



Threats and Countermeasures Guide: Security Settings in Windows 7 and Windows Server 2008 R2

Microsoft Corporation

Published: May 2011

Authors: Starr Andersen, Greg Marshall, Eric Mitchell, Roland Winkler

Abstract

The purpose of this guide is to provide you with a reference to security settings that provide countermeasures for specific threats against current versions of the Windows operating systems.

Microsoft

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveX, Aero, AppLocker, BitLocker, BranchCache, Internet Explorer, MS-DOS, Outlook, ReadyBoost, SQL Server, Win32, Windows, Windows Live, Windows Media, Windows NT, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

| | |
|--|-----|
| Threats and Countermeasures Guide: Security Settings in Windows Server 2008 R2 and Windows 7 | 4 |
| Threats and Countermeasures Guide: Account Policies | 7 |
| Threats and Countermeasures Guide: Advanced Security Audit Policy..... | 29 |
| Threats and Countermeasures Guide: User Rights | 63 |
| Threats and Countermeasures Guide: Security Options..... | 106 |
| Threats and Countermeasures Guide: Event Log..... | 202 |
| Threats and Countermeasures Guide: System Services..... | 211 |
| Threats and Countermeasures Guide: Software Restriction Policies..... | 352 |
| Threats and Countermeasures Guide: Application Control Policies | 355 |
| Threats and Countermeasures Guide: External Storage Devices..... | 357 |
| Threats and Countermeasures Guide: Additional Resources | 376 |

Threats and Countermeasures Guide: Security Settings in Windows Server 2008 R2 and Windows 7

This guide is a reference to the security settings in Windows Server® 2008 R2 and Windows® 7 that provide countermeasures for specific threats against the current versions of the operating systems.



Note

For a web version of this document, see [Threats and Countermeasures Guide](#) in the Windows Server Technical Library.

Many of the countermeasures that are described in this guide are not intended for specific computer roles in the companion guides, or in some cases, for any roles at all. These countermeasures help ensure compatibility, usability, manageability, availability, or performance.

Generally, as security increases, functionality decreases, and vice versa. However, there are exceptions, and some security countermeasures actually help improve functionality.

Each section begins with a brief explanation of what is in the section, followed by a list of subsection headings, each of which corresponds to a setting or group of settings. Each subsection includes a brief explanation of what the countermeasure does and the following subsections:

- **Vulnerability** Explains how an attacker might exploit a feature or its configuration.
- **Countermeasure** Explains how to implement the countermeasure.
- **Potential impact** Explains the possible negative consequences of countermeasure implementation.

For example, the section **Domain Level Account Policies** begins with the following subsections:

Account Policies

- Enforce password history
 - Vulnerability
 - Countermeasure
 - Potential impact

- Maximum password age
 - Vulnerability
 - Countermeasure
 - Potential impact

This pattern is repeated throughout this guide. Settings that are closely related are presented in a single subsection. For example, in the **Security Options** section, four related settings are placed into the same subsection as follows:

Microsoft network client and server: Digitally sign communications

- Microsoft network client: Digitally sign communications (always)
- Microsoft network server: Digitally sign communications (always)
- Microsoft network client: Digitally sign communications (if server agrees)
- Microsoft network server: Digitally sign communications (if client agrees)

This guide focuses on Group Policy settings that are considered security settings, and those that are intended to help organizations manage their environments are not documented. This guide examines only the settings and features in Windows Server 2008 R2 and Windows 7 that can help organizations secure their enterprises against specific threats. Settings and features that were added in service packs after the release of Windows 7 and Windows Server 2008 R2, or functionalities that may have been added by software released after those service packs, may not be discussed in this guide. Also, management features and those security features that are not configurable by administrators are not described in this guide.

The information that is provided within this guide should help you and members of your organization understand the countermeasures that are available in the current versions of the operating systems.

Section overviews

This guide consists of the following sections, which provide a reference to the settings that you should consider when planning the security policy for your organization.

| | |
|---|--|
| Threats and Countermeasures Guide: Account Policies | This section discusses the Group Policy settings that are applied at the domain level: password policies, account lockout policies, and Kerberos |
|---|--|

| | |
|---|---|
| | protocol authentication policies. |
| Threats and Countermeasures Guide: Advanced Security Audit Policy | This section discusses the use of advanced audit policy settings, which are now integrated with Group Policy to monitor and enforce your security measures. It describes the various settings, and it provides examples of how audit information is modified when the settings are changed. |
| Threats and Countermeasures Guide: User Rights | This section discusses the various logon rights and privileges that are provided by the Windows 7 and Windows Server 2008 R2 operating systems, and it provides guidance about which accounts should be assigned these rights. |
| Threats and Countermeasures Guide: Security Options | This section provides guidance about security settings for digital data signatures, Administrator and Guest account names, drive access, driver installation behavior, and logon prompts. |
| Threats and Countermeasures Guide: Event Log | This section provides guidance about how to configure the settings that relate to the various event logs on computers running Windows Server 2008 R2 or Windows 7. |
| Threats and Countermeasures Guide: System Services | Windows Server 2008 R2 and Windows 7 include a variety of system services. Many of these services are configured to run by default, but others are not present unless you install specific components. This section describes the various services included with the operating systems so that you can best decide which ones to leave enabled and which ones can be safely disabled. |
| Threats and Countermeasures Guide: Software | This section provides a brief overview of the |

| | |
|---|---|
| Restriction Policies | Software Restriction Policy feature that is available in Windows Server 2008 R2 and Windows 7. It provides links to additional resources about how to design and use policy settings to control which applications can be used in your organization. |
| Threats and Countermeasures Guide: Application Control Policies | This section provides a brief overview of the AppLocker™ feature that is available in Windows Server 2008 R2 and Windows 7. It provides links to additional resources about how to design and use policy settings to control which applications can be used in your organization. |
| Threats and Countermeasures Guide: External Storage Devices | This section describes Group Policy settings that can be used to limit, prevent, or allow the use of external storage devices in networked computers. |
| Threats and Countermeasures Guide: Additional Resources | This section provides links to additional information sources about Windows security topics from Microsoft that you may find useful. |

Threats and Countermeasures Guide: Account Policies

This section of the Threats and Countermeasures Guide discusses Group Policy settings that are applied at the domain level. The default setting values for these policies, which are collectively referred to as Account Policies settings, are included in the built-in Default Domain Controllers Policy Group Policy Object (GPO).

Account Policies overview

There are three folders in the Account Policies folder:

- [Password Policy](#)

- [Account Lockout Policy](#)
- [Kerberos Policy](#)

A single Windows Server® 2008 R2 domain can have one of each of these policies. If these policies are set at any level below the domain level in Active Directory® Domain Services, they affect only local accounts on member servers.

The Account Policies settings in Group Policy are applied at the domain level. Default values are present in the built-in Default Domain Controllers Policy GPO for Password Policy settings, Account Lockout Policy settings, and Kerberos Policy settings. The domain Account Policies settings become the default local Account Policies settings of any computer that is running the Windows® operating system and that is a member of the domain.

**Note**

Each domain can have only one Account Policies setting. The Default Domain Policy is the policy that is enforced by the domain controllers in the domain by default. The Account Policies setting must be defined in the Default Domain Policy or in a new policy that is linked to the root of the domain and given precedence over the Default Domain Policy. These domain-wide Account Policies settings (Password Policy, Account Lockout Policy, and Kerberos Policy) are enforced by the domain controllers in the domain. Therefore, domain controllers always retrieve the values of these Account Policies settings from the Default Domain Policy GPO.

The only exception to this rule is when another Account Policies setting is defined for an organizational unit (OU). The Account Policies settings for the OU affect the local policy on any computers that are contained in the OU. For example, if an OU policy defines a maximum password age that differs from the domain-level Account Policies settings, the OU policy is applied and enforced only when users log on to the local computer. The default local computer policies apply only to computers that are in a workgroup or in a domain where neither an OU Account Policies setting nor a domain policy applies.

The following sections discuss the settings for each of the policies that is in the Account Policies folder.

Password Policy settings

In Windows and many other operating systems, the most common method to authenticate a user's identity is to use a secret passphrase or password. A secure network environment requires all users to use strong passwords. A strong password has at least 10 characters, and it includes a combination of letters, numbers, and symbols. These passwords help prevent the compromise of user accounts and administrative accounts by unauthorized people who use

manual methods or automated tools to guess weak passwords. Strong passwords that are changed regularly reduce the likelihood of a successful password attack.

Windows Server 2008 R2 and Windows Server 2008 support fine-grained password policies. This feature provides organizations with a way to define different password and account lockout policies for different sets of users in a domain. In the Active Directory domains in Windows 2000 and Windows Server 2003, only one password policy and account lockout policy could be applied to all users in the domain. Fine-grained password policies apply only to user objects (or inetOrgPerson objects if they are used instead of user objects) and global security groups.

Fine-grained password policies include attributes for all the settings that can be defined in the Default Domain Policy (except Kerberos protocol settings) as well as account lockout settings. When you specify a fine-grained password policy, you must specify all of these settings. By default, only members of the Domain Admins group can set fine-grained password policies. However, you can also delegate the ability to set these policies to other users. The domain functional level must be Windows Server 2008 or Windows Server 2008 R2 to use fine-grained password policies. Fine-grained password policies cannot be applied to an organizational unit (OU) directly.

To apply a fine-grained password policy to users of an OU, you can use a shadow group. A shadow group is a global security group that is logically mapped to an OU to enforce a fine-grained password policy. You add users of the OU as members of the newly created shadow group and then apply the fine-grained password policy to this shadow group. You can create additional shadow groups for other OUs as needed. If you move a user from one OU to another, you must update the membership of the corresponding shadow groups.

Fine-grained password policies do not interfere with custom password filters that you might use in the same domain. Organizations that have deployed custom password filters to domain controllers running Windows 2000 or Windows Server 2003 can continue to use those password filters to enforce additional restrictions for passwords. For more information about fine-grained password policies, see [AD DS: Fine-Grained Password Policies](#).

You can enforce the use of strong passwords through an appropriate password policy. There are password policy settings that control the complexity and lifetime of passwords, such as the **Passwords must meet complexity requirements** policy setting.

You can configure the password policy settings in the following location by using the Group Policy Management Console (GPMC) on your domain controller:

Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy

If individual groups require distinct password policies, these groups should be separated into another domain or forest based on any additional requirements.

Enforce password history

This policy setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused.

Possible values:

- User-specified value between 0 and 24
- Not Defined

On domain controllers, the default value for this policy setting is 24. On stand-alone servers, the default value for this policy setting is 0.

Vulnerability

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users can use the same small number of passwords repeatedly. If you do not also configure the **Minimum password age** policy setting, users might repeatedly change their passwords until they can reuse their original password.



Note

After an account has been compromised, a simple password reset might not be enough to restrict a malicious user because the malicious user might have modified the user's environment so that the password is changed back to a known value automatically at a certain time. If an account has been compromised, it is best to delete the account and assign the user a new account after all affected systems have been restored to normal operations and verified that they are no longer compromised.

Countermeasure

Configure the **Enforce password history** policy setting to 24, the maximum setting, to help minimize the number of vulnerabilities that are caused by password reuse.

For this policy setting to be effective, you should also configure effective values for the **Minimum password age** and **Maximum password age** policy settings.

Potential impact

The major impact of configuring the **Enforce password history** policy setting to 24 is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization, but this makes them easier to guess. Also, an excessively low value for the **Maximum password age** policy setting is likely to increase administrative overhead because users who forget their passwords might ask the help desk to reset them frequently.

Maximum password age

This policy setting determines the maximum number of days that a password can be used before the user must change it. Its value must be more than the **Minimum password age** value.

Possible values:

- User-specified number of days between 0 and 999
- Not Defined

The default value for this policy setting is 42.

Vulnerability

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the **Maximum password age** policy setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by a malicious user for as long as the valid user is authorized access.

Countermeasure

Configure the **Maximum password age** policy setting to a value that is suitable for your organization's business requirements.

Potential impact

If the **Maximum password age** policy setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization because users might write their passwords in an unsecured location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows

potential attackers more time in which to discover user passwords or to use compromised accounts.

Minimum password age

This policy setting determines the minimum number of days that a password must be used before the user is allowed to change it. Its value must be less than the **Maximum password age** value.

Configure this policy setting to a number that is greater than 0, and set the **Enforce password history** policy setting. If you configure the **Enforce password history** policy setting to 0, users are not required to choose a new unique password when prompted to change their password. If password history is used, users must enter a new unique password when they change their password.

Possible values:

- User-specified number of days between 0 and 998
- Not Defined

The default value for this policy setting is 1 on domain controllers and 0 on stand-alone servers.

Vulnerability

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately passwords are compromised, and if an attacker is targeting a specific individual user account with foreknowledge of data about that user, reuse of old passwords can cause a security breach.

To address password reuse, you must use a combination of security settings. Using this policy setting with the **Enforce password history** policy setting prevents the easy reuse of old passwords. For example, if you configure the **Enforce password history** policy setting to ensure that users cannot reuse any of their last 12 passwords, but you do not configure the **Minimum password age** policy setting to a number that is greater than 0, they could change their password 13 times in a few minutes and reuse the password they started with. You must configure this policy setting to a number that is greater than 0 for the **Enforce password history** policy setting to be effective.

Countermeasure

Configure the **Minimum password age** policy setting to a value of at least 2 days. Users should know about this limitation and contact the help desk if they need to change their password during that 2-day period. If you configure the number of days to 0, immediate password changes would be allowed, which we do not recommend.

Potential impact

If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the **User must change password at next logon** check box, or the user cannot change the password until the next day.

Minimum password length

This policy setting determines the fewest number of characters that can make up a password for a user account. Some prefer using a passphrase rather than a password. Passphrases can be quite long and they can include spaces, punctuation marks, and Unicode characters. Therefore, a phrase such as "I want to drink a \$5 beverage!" is a valid passphrase. Such a phrase is considerably stronger than an 8 or 10 character string and is easier to remember.

The longer a password is, the better security it provides, especially if it includes a character combination of uppercase and lowercase letters, digits, symbols, and punctuation. The following table shows the amount of time that it would take a computer that is performing a brute force attack (at 10 million character combinations per second) to discover a password for a user account.

| Password length | Alphanumeric case-sensitive (62 characters) | Alphanumeric case-sensitive including symbols (96 characters) |
|-----------------|---|---|
| 2 | Instant | Instant |
| 3 | Instant | Instant |
| 4 | Less than 2 seconds | 8.5 seconds |
| 5 | 1.5 minutes | 13.5 minutes |
| 6 | 1.5 hours | 22 hours |
| 7 | 4 days | 87 days |
| 8 | 253 days | 23 years |

**Note**

A computer that could perform a brute force attack at a rate of 1 billion character combinations per second would take 83.5 days to discover an eight-symbol password that includes a combination of uppercase and lowercase letters, digits, symbols, and punctuation.

Possible values:

- User-specified number between 0 and 14
- Not Defined

The default value for this policy setting is 7 on domain controllers and 0 on stand-alone servers.

Vulnerability

Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Countermeasure

Configure the **Minimum password length** policy setting to a value of 8 or more. If the number of characters is set to 0, no password will be required.

In most environments, we recommend an 8-character password because it is long enough to provide adequate security but not too difficult for users to easily remember. This configuration provides adequate defense against a brute force attack. Using the **Passwords must meet complexity requirements** policy setting in addition to the **Minimum password length** policy setting helps reduce the possibility of a dictionary attack.

**Note**

Some jurisdictions have established legal requirements for password length as part of establishing computer security regulations.

Potential impact

Requirements for extremely long passwords can actually decrease the security of an organization because users might leave the information in an unsecured location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of Help Desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases. They are often easier to remember, and due to the larger number of character combinations, they are much harder to discover.

**Note**

Older versions of Windows such as Windows 98 and Windows NT® 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Passwords must meet complexity requirements

This policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password.

If this policy setting is enabled, passwords must meet the following requirements:

- The password is at least six characters long.
- The password contains characters from three of the following four categories:
 - Uppercase characters
 - Lowercase characters
 - Numerals
- Non-alphanumeric and Unicode characters, which include the following characters as well as other accented characters and characters not present in common keyboards: (() ` ~ ! @ # \$ % ^ & * - + = | \ { } [] : ; ' < > , . ? / € Γ f λ and space). This group also includes extended characters that can only be specified by using keystroke combinations.
- The password does not contain three or more consecutive characters from the user's account name or display name. If the account name is fewer than three characters long, this check is not performed because the rate at which passwords would be rejected would be

too high. When a check is performed against the user's full name, several characters separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, number signs, and tabs. A token that is three or more characters long 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. Because 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.

These complexity requirements are enforced when a password is changed or a new password is created.

For specific instructions about how to configure password policy settings, see [Apply or modify password policy](#).

For more information, see:

- [Strong passwords](#)
- [Password best practices](#)
- [Apply or modify password policy](#)
- [Security Configuration Manager tools](#)

The rules that are included in the Windows Server 2008 R2 policy cannot be directly modified. However, you can create a new version of the Passfilt.dll file to apply a different set of rules. For more information about how to create your own password filter, see [Password Filters](#).

Possible values:

- Enabled
- Disabled
- Not Defined

By default, this policy setting is enabled on domain controllers and disabled on stand-alone servers.

Vulnerability

Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

Countermeasure

Configure the **Passwords must meet complexity requirements** policy setting to **Enabled** and advise users to use a variety of characters in their passwords.

When combined with a **Minimum password length** of 8, this policy setting ensures that the number of different possibilities for a single password is so great that it is difficult (but not impossible) for a brute force attack to succeed. (If the **Minimum password length** policy setting is increased, the average amount of time necessary for a successful attack also increases.)

Potential impact

If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetical characters or might have problems entering passwords that contain accented characters or symbols on keyboards with different layouts. However, all users should be able to comply with the complexity requirement with minimal difficulty.

If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row symbols. (Upper row symbols are those that require you to press and hold the SHIFT key and then press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments.

The use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in increased Help Desk requests. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 0128–0159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Store password using reversible encryption for all users in the domain

This policy setting determines whether the following Windows operating systems use reversible encryption when they store passwords:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 Server
- Windows 7 Professional

- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows Vista® Business N
- Windows Vista Ultimate
- Windows Vista Enterprise
- Windows XP Professional
- Windows 2000 Professional

The **Store password using reversible encryption for all users in the domain** policy setting provides support for application protocols that require knowledge of the user's password for authentication purposes. However, encrypted passwords that are stored in a way that is reversible can potentially be decrypted by an attack that obtains the encrypted version and is able to find the encryption key. Also, a successful brute force attack could obtain not only a usable password (one that is able to perform authentications to the domain), but one that is identical to the actual user's password (which could give insight into the user's password selection criteria, or be usable in other systems that are sharing the same password). A knowledgeable attacker who was able to break this encryption could then log on to network resources with the compromised account.



Caution

Do not enable this policy setting unless business requirements outweigh the need to protect password information.

Use of Challenge Handshake Authentication Protocol (CHAP) through remote access or Internet Authentication Service (IAS) services requires that this policy setting be enabled. CHAP is an authentication protocol that can be used by Microsoft Remote Access and Network Connections. It is also required when using Digest authentication in Internet Information Services (IIS). Both IAS and IIS support more secure methods of authentication that do not require reversible encryption. If possible, move those services to a different authentication protocol instead of enabling this policy setting.

Possible values:

- Enabled
- Disabled
- Not Defined

The default value for this policy setting is **Disabled**.

Vulnerability

Enabling this policy setting allows the operating system to store passwords in a format that can weaken your overall security.

Countermeasure

Disable the **Store password using reversible encryption for all users in the domain** policy setting.

Potential impact

If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest authentication in IIS, you must configure this policy setting to **Enabled**. Application of this policy through Group Policy on a user-by-user basis increases security risks because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Account Lockout Policy settings

More than a few unsuccessful password submissions during an attempt to log on to a computer might represent an attacker's attempts to determine an account password by trial and error. The Windows operating system can track logon attempts, and you can configure the operating system to disable the account for a preset period of time after a specified number of failed attempts. Account lockout policy settings control the threshold for this response and what action to take after the threshold is reached.

You can configure the account lockout policy settings in the following location within the GPMC:

Computer Configuration\Windows Settings\Account Policies\Account Lockout Policy

Account lockout duration

This policy setting determines the number of minutes that a locked-out account remains locked before it is automatically unlocked. The available range is from 1 to 99,999 minutes. To specify that the account will be locked out until an administrator manually unlocks it, configure the value to 0. If the **Account lockout threshold** policy setting is defined, the **Account lockout duration** must be greater than or equal to the value for the **Reset account lockout counter after** policy setting.

Possible values:

- User-defined value in minutes between 0 and 99,999

- Not Defined

This policy setting is dependent on the **Account lockout threshold** policy setting that is being defined, and it must be greater than or equal to the value specified for the **Reset lockout counter after** policy setting.

Vulnerability

A denial-of-service (DoS) condition can be created if an attacker abuses the **Account lockout threshold** and repeatedly attempts to log on with a specific account. After you configure the **Account lockout threshold** policy setting, the account will be locked after the specified number of failed attempts. If you configure the **Account lockout duration** policy setting to 0, the account remains locked until an administrator unlocks it manually.

Countermeasure

Configure the **Account lockout duration** policy setting to an appropriate value for your environment. To specify that the account will remain locked until an administrator manually unlocks it, configure the value to 0. When the **Account lockout duration** policy setting is configured to a non-zero value, automated attempts to guess account passwords are delayed for this interval before resuming attempts against a specific account. Using this policy setting in combination with the **Account lockout threshold** policy setting makes automated password guessing attempts more difficult.

Potential impact

Although it may seem like a good idea to configure the **Account lockout duration** policy setting to 0 so that accounts cannot be automatically unlocked, such a configuration can increase the number of requests that your organization's Help Desk receives to unlock accounts that were locked by mistake.

Account lockout threshold

This policy setting determines the number of failed logon attempts that causes a user account to become locked. A locked account cannot be used until it is reset by an administrator or until the lockout duration for the account expires. You can specify up to 999 failed logon attempts, or you can set the value to 0 to specify that the account is never locked out. When you define **Account lockout threshold** policy, you must also define the **Reset lockout counter after** and the **Account lockout duration** policy settings.

Failed password attempts against workstations or member servers that have been locked by pressing CTRL+ALT+DELETE or by password-protected screen savers do not count as failed logon attempts unless the **Interactive logon: Require Domain Controller authentication to unlock workstation** policy setting is enabled in the **Security Options** section of Group Policy. If it is,

repeated failed password attempts to unlock the workstation count against the account lockout threshold.

Possible values:

- User-defined value between 0 and 999
- Not Defined

The default value for this policy setting is 0.

Vulnerability

Online brute force password attacks can use automated methods to try millions of password combinations for any user account. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed.

However, a DoS attack could be performed on a domain that has an account lockout threshold configured. An attacker could programmatically attempt a series of password attacks against all users in the organization. If the number of attempts is greater than the account lockout threshold, the attacker might be able to lock out every account without needing any special privileges or being authenticated in the network.



Note

Offline password attacks are not countered by this policy setting.

Countermeasure

Because vulnerabilities can exist when this value is configured as well as when it is not configured, two distinct countermeasures are defined. Any organization should weigh the choice between the two, based on their identified threats and the risks that they want to mitigate. The two countermeasure options are:

- Configure the **Account lockout threshold** policy setting to 0. This configuration ensures that accounts will not be locked out, and it prevents a DoS attack that intentionally attempts to lock out accounts. This configuration also helps reduce Help Desk calls because users cannot accidentally lock themselves out of their accounts. Because it does not prevent a brute force attack, this configuration should be chosen only if both of the following criteria are explicitly met:
 - The password policy requires all users to have complex passwords of 8 or more characters.
 - A robust audit mechanism is in place to alert administrators when a series of failed logons occur in the environment.

- Configure the **Account Lockout Threshold** policy setting to a sufficiently high value to provide users with the ability to accidentally mistype their password several times before the account is locked, but ensure that a brute force password attack still locks the account. A good recommendation for such a configuration is 50 invalid logon attempts, which prevents accidental account lockouts and reduces the number of Help Desk calls, but does not prevent a DoS attack.

We recommend this option if your organization cannot implement complex password requirements and an audit policy that alerts administrators to a series of failed logon attempts. Using this type of policy must be accompanied by a good, fast process that can be implemented to unlock locked accounts when needed on weekends, at night, or during holidays to help mitigate massive lockouts caused by an attack on your systems.

Potential impact

If this policy setting is enabled, a locked-out account is not usable until it is reset by an administrator or until the account lockout duration expires. This policy setting will likely generate a number of additional Help Desk calls. In fact, locked accounts cause the greatest number of calls to the Help Desk in many organizations.

If you configure the **Account lockout threshold** policy to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place. If you configure this policy setting to a number greater than zero, an attacker can easily lock out any accounts for which the account name is known. This is especially dangerous considering that no privileges other than access to the network are necessary to lock the accounts.

Reset account lockout counter after

This policy setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers account lockouts is reset to 0. This reset time must be less than or equal to the **Account lockout duration** policy setting configuration.

Possible values:

- User-defined number of minutes between 1 and 99,999
- Not Defined

Vulnerability

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times.

Countermeasure

Configure the **Reset account lockout counter after** policy setting to 30.

Potential impact

If you do not configure this policy setting or if the value is configured to an interval that is too long, an attacker could attempt to log on to each user's account numerous times and lock out their accounts, a DoS attack might succeed, or administrators might have to manually unlock all locked-out accounts. If you configure this policy setting to a reasonable value, users can perform new attempts to log on after a failed logon within a reasonable time, without making brute force attacks feasible at high speeds. Be sure that you notify users of the values that are used for this policy setting so that they wait for the lockout timer to expire before they call the Help Desk.

Kerberos Policy settings

The Kerberos protocol authentication provides the default mechanism for domain authentication services and the authorization data that is necessary for a user to access a resource and perform a task on that resource. If the lifetime of Kerberos protocol tickets is reduced, the risk of a legitimate user's credentials being stolen and successfully used by an attacker decreases. However, authorization overhead increases.

In most environments, the Kerberos Policy settings do not need to be changed. These policy settings are applied at the domain level, and the default values are configured in the Default Domain Policy GPO in a default installation of Windows server operating systems beginning with the Active Directory domain in Windows Server 2003.

You can configure the Kerberos Policy settings in the following location within the Group Policy Management Console (GPMC):

Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy

**Note**

The Kerberos Policy settings also can be specified in the Local Group Policy Editor. Any policy setting that is specified there is superseded by domain policy settings.

Enforce user logon restrictions

This policy setting determines whether the Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional because the extra step takes time and can slow down network access to services.

Possible values:

- Enabled
- Disabled
- Not Defined

The default value for this policy setting is **Enabled**.

Vulnerability

If you disable this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on.

Countermeasure

Enable the **Enforce user logon restrictions** policy setting.

Potential impact

None. This is the default configuration.

Maximum lifetime for service ticket

This policy setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The policy setting must be 10 minutes or greater, and it must be less than or equal to the value of the **Maximum lifetime for user ticket** policy setting.

If a client computer presents an expired session ticket when it requests a connection to a server, the server returns an error message and the client computer must request a new session ticket from the KDC. However, after a connection is authenticated, it does not matter whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Operations are not interrupted if the session ticket that authenticated the connection expires during the connection.

Possible values:

- User-defined value in minutes between 0 and 99,999
- Not Defined

The default value for this policy setting is 600. If you configure this policy setting to 0, service tickets do not expire.

Vulnerability

If you configure the value for the **Maximum lifetime for service ticket** policy setting too high, users might be able to access network resources outside of their logon hours. Also, users whose

accounts were disabled might continue to have access to network services with valid service tickets that were issued before their accounts were disabled.

Countermeasure

Configure the **Maximum lifetime for service ticket** policy setting to 600 minutes.

Potential impact

None. This is the default configuration.

Maximum lifetime for user ticket

This policy setting determines the maximum amount of time (in hours) of a user's ticket-granting ticket (TGT). When a user's TGT expires, a new one must be requested or the existing one must be renewed.

Possible values:

- User-defined value in hours between 0 and 99,999
- Not Defined

The default value for this policy setting is 10.

Vulnerability

If you configure the value for the **Maximum lifetime for user ticket** policy setting too high, users might be able to access network resources outside of their logon hours. Also, users whose accounts were disabled might continue to have access to network services with valid user tickets that were issued before their accounts were disabled. If you configure this value too low, ticket requests to the KDC may affect the performance of your KDC and present an opportunity for a DoS attack.

Countermeasure

Configure the **Maximum lifetime for user ticket** policy setting with a value between 4 and 10 hours.

Potential impact

Reducing this policy setting from the default value reduces the likelihood that the TGT will be used to access resources that the user does not have rights to. However, it requires more frequent requests to the KDC for TGTs on behalf of users. Most KDCs can support a value of 4 hours without too much additional burden.

Maximum lifetime for user ticket renewal

This policy setting determines the period of time (in days) during which a user's TGT can be renewed.

Possible values:

- User-defined value in minutes between 0 and 99,999
- Not Defined

The default value for this policy setting is 7.

Vulnerability

If the value for the **Maximum lifetime for user ticket renewal** policy setting is too high, users might be able to renew very old user tickets.

Countermeasure

Configure the **Maximum lifetime for user ticket renewal** policy setting to 7 days.

Potential impact

None. This is the default configuration.

Maximum tolerance for computer clock synchronization

This policy setting determines the maximum time difference (in minutes) that the Kerberos protocol allows between the time on the client computer's clock and the time on the domain controller in Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 that provides Kerberos protocol authentication.

Possible values:

- User-defined value in minutes between 1 and 99,999
- Not Defined

The default value for this policy setting is 5.



Note

If you configure this policy setting and then restart the computer, this policy setting reverts to the default value.

Vulnerability

To prevent "replay attacks," which are attacks in which an authentication credential is resubmitted by a malicious user or program to gain access to a protected resource, the Kerberos

authentication protocol uses time stamps as part of its protocol definition. For time stamps to work properly, the clocks of the client computer and the domain controller need to be closely synchronized. Because the clocks of two computers are often not synchronized, administrators can use this policy to establish the maximum acceptable difference for the Kerberos protocol between the clocks on the client computer and a domain controller. If the difference between the clocks is less than the maximum time difference that is specified in this policy setting, any time stamp that is used in a session between the two computers is considered to be authentic.

Countermeasure

Configure the **Maximum tolerance for computer clock synchronization** policy setting to 5 minutes.

Potential impact

None. This is the default configuration.

Additional references

The following links provide additional information about topics that relate to securing domain controllers that run Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2:

- [Modify Security Policies in Default Domain Controllers Policy](#)
- [Best Practice Guide for Securing Windows Server Active Directory Installations](#)

Threats and Countermeasures Guide: Advanced Security Audit Policy

This section of the Threats and Countermeasures Guide discusses advanced security audit policy settings, which are located in **Security Settings\Advanced Audit Policy Configuration**.

Establishing an organizational computer system audit policy is an important facet of information security. Configuring audit policy settings that monitor the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.

In Windows Server® 2008 R2 and Windows® 7, all auditing capabilities are integrated with Group Policy settings. This allows administrators to configure, deploy, and manage these settings in the Group Policy Management Console (GPMC) or the Local Security Policy snap-in for a domain, site, or organizational unit (OU). Windows Server 2008 R2 and Windows 7 make it easier for IT professionals to track when precisely defined, significant activities take place on the network. These features include:

- Advanced audit policy settings, which allow administrators to apply and manage detailed audit policy settings in a more narrowly defined manner than previously through their existing Group Policy framework.
- "Reason for access" auditing, which enables administrators to specify and identify the permissions that were used to generate a particular object access security event.
- Global object access auditing, which allows administrators to define system access control lists (SACLs) for an entire computer file system or registry.

Previous versions of Windows had fewer, although still useful, security auditing options, for example:

- Security auditing was enabled through nine basic settings under **Security Settings\Local Policies\Audit Policy**. For more information, see [Audit Policy Settings Under Local Policies\Audit Policy](#).
- Additional basic audit policy settings are also available under **Security Settings\Local Policies\Security Options**. For more information, see [Audit Policy Settings Under Local Policies\Security Options](#).
- In Windows Vista and Windows Server 2008, the number of auditable events was expanded from nine to 53, which enabled an administrator to be more selective in the number and types of events to audit. However, these new audit events were not integrated with Group Policy, and they can only be deployed by using logon scripts that are generated with the Auditpol.exe command-line tool.

**Note**

For instructions on how to use Auditpol.exe to create detailed audit policies for computers running Windows Vista and how to distribute those settings by using a script, see [article 921469](#) in the Microsoft Knowledge Base.

The nine local audit policy settings under **Security Settings\Local Policies\Audit Policy** can still be used if client computers do not support advanced audit policy settings. However, where possible it is recommended that you use the more precise auditing capabilities that are provided by the advanced audit policy settings.

**Important**

Using both the basic audit policy settings under **Security Settings\Local Policies\Audit Policy** and the advanced settings under **Advanced Audit Policy Configuration** can cause unexpected results. Therefore, the two sets of audit policy settings should not be combined. If you use the **Advanced Audit Policy Configuration** settings, you should enable the **Audit: Force audit policy subcategory settings (Windows Vista or later)** policy setting under **Security Settings\Local Policies\Security Options**. This setting will override audit policy settings under **Security Settings\Local Policies\Audit Policy** and prevent conflicts between similar settings by forcing basic security auditing to be ignored.

For more information about using the basic security audit policy, see the Audit Policy section of [Threats and Countermeasures Guide: Security Settings in Windows Server 2008 and Windows Vista](#).

When you implement advanced audit policy settings:

- Specify the categories and subcategories of the events that you want to audit. The event categories and subcategories that you select constitute your audit policy.
- Set the size and behavior of the Security log. You can view the Security log with Event Viewer.
- Determine which objects you want to audit access of and what type of access you want to audit, if you want to audit directory service access or object access. For example, if you want to audit all attempts by users to open a particular file, you can configure audit policy settings in the object access event category so that both successful and failed attempts to read a file are recorded.

The Security log records an audit event whenever users perform certain specified actions. For example, the modification of a file or a policy can trigger an event that shows the action that was performed, the associated user account, and the date and time of the action. These events can be both successful and failed attempts to perform actions.

Regular security analyses enable administrators to track and determine whether adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer that relate to security, which administrators can use to adjust the security levels. More important, this information can help detect any security oversights that may occur in the computer over time. For example, security levels may be temporarily changed to enable immediate resolution of an administration or network issue. However, such changes are often forgotten and never undone. If security levels are not properly reset, a computer may no longer meet the requirements for enterprise security.

Establishing and enabling audit policy settings that record deviations from your enterprise security policy are extremely important for any enterprise network. Audit logs may provide the only indication that a security breach has occurred by recording changes on file permissions, installation of programs, and escalation of privileges. Even if the breach is discovered by means other than auditing, proper audit settings can generate an audit log that may contain important information about the breach, how it occurred, and which systems were affected.

In many cases, failure events are much more informative than success events because failures typically indicate errors. For example, successful logon to a computer by a user would typically be considered normal. However, if someone unsuccessfully tries to log on to a computer multiple times, it may indicate an attacker's attempt to break into the computer with someone else's account credentials. The Event Log in Group Policy is used to define attributes that relate to the Application, Security, and System logs, such as maximum log size, access rights for each log, and retention settings and methods. Auditing events are stored in the Security event log. For more information about the Event Log, see the [Threats and Countermeasures Guide: Event Log](#) section in this guide.

Before any audit processes are implemented, an organization should determine how to collect, organize, and analyze the data. There is little value in large volumes of audit data if there is no underlying plan to use it. Also consider that audit settings can affect computer performance. The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server. Therefore, you should perform some performance tests before you deploy new audit settings in your production environment. A final consideration is the amount of storage space that you can allocate to store the data that is collected during auditing. Depending on the setting you choose, auditing data can accumulate quickly and can fill up available disk space.

The following sections describe the options and issues for configuring advanced security audit policy settings for better system management and security.

Advanced audit policy settings

The vulnerabilities, countermeasures, and potential impacts of all the advanced audit policy settings are similar. The options for each of the audit settings are identical:

- **Success** An audit event is generated when the requested action succeeds.
- **Failure** An audit event is generated when the requested action fails.
- **Not configured** No audit event is generated for the associated action.

Vulnerability

If audit policy settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if security audit policy settings are configured so that events are generated for all activities, the Security log will be filled with data and difficult to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit policy settings for a large number of objects.

If failure auditing is used and the **Audit: Shut down system immediately if unable to log security audits** policy setting in the **Security Options** section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures to fill the Security log and force the computer to shut down, creating a denial-of-service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Countermeasure

Enable advanced security audit policy settings that support the organizational security policy for all the computers in your organization. Identify the components that you need to monitor to enable your organization to hold users accountable for their actions while they use organizational resources. These components should allow IT departments to detect unauthorized activity efficiently and track events in log files. For more information about identifying security auditing priorities, and selecting and implementing security auditing settings to address those needs, see [Planning and Deploying Advanced Security Auditing Policies](#).

Potential impact

If no audit policy settings are configured or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too detailed, critically important entries in the Security log may be obscured by the large number of log entries created by routine activities and computer performance, and the available amount of

data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.



Important

Applying advanced audit policy settings replaces any comparable basic or local security audit policy settings. If you subsequently change the advanced audit policy setting to **Not configured**, you will need to complete the following steps to restore the original basic security audit policy settings:

1. Confirm that all Advanced Audit Policy settings are set to **Not configured**.
2. Delete all audit.csv files from the %SYSVOL% folder on the domain controller.
3. Reconfigure and apply local security audit policy settings.

Audit account logon events

Use this category of audit policy settings to record each instance of a user logging on to or logging off from another computer when that computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.

Failure audits are useful for intrusion detection. However, this configuration of the policy setting also creates the potential for a DoS attack. When the **Audit: Shut down system immediately if unable to log security audits** policy setting in the **Security Options** section of Group Policy is also enabled, an attacker could generate millions of logon failures to fill the Security log and force the computer to shut down.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|-----------------------------|--|-----------------|
| Audit Credential Validation | This security policy setting determines whether the operating system generates audit events on credentials that are submitted for a user | Not configured |

| Name | Description | Default setting |
|---------------------------------------|--|-----------------|
| | <p>account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.</p> <p>Because domain accounts are used much more frequently than local accounts in enterprise environments, most of the Account Logon events in a domain environment occur on the domain controllers that are authoritative for the domain accounts. However, these events can occur on any computer, and they may occur in conjunction with Logon/Logoff events, or on separate computers.</p> | |
| Audit Kerberos Authentication Service | <p>This security policy setting allows you to generate audit events for Kerberos authentication ticket-granting ticket (TGT) requests. If you configure this policy setting, an audit event is generated after a Kerberos protocol authentication TGT request. Success audits record successful attempts and Failure audits record unsuccessful attempts.</p> | Not configured |

| Name | Description | Default setting |
|--|--|-----------------|
| Audit Kerberos Service Ticket Operations | This security policy setting determines whether the operating system generates security audit events for Kerberos protocol service ticket requests. Events are generated every time Kerberos is used to authenticate a user who attempts to access a protected network resource. Kerberos protocol service ticket operation audit events can be used to track user activity. | Not configured |
| Audit Other Account Logon Events | This security policy setting allows you to audit events that are generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos protocol tickets. Examples include new Remote Desktop sessions and Remote Desktop disconnections, locking and unlocking a workstation, invoking or dismissing a screen saver, detection of a Kerberos protocol replay attack, in which a Kerberos protocol request with identical information was received twice, access to a wireless network that is granted to a user or computer account, or access to a wired 802.1x network that is granted | Not configured |

| Name | Description | Default setting |
|------|--------------------------------|-----------------|
| | to a user or computer account. | |

Audit account management

This category of security audit policy settings enables auditing of each account management event on a computer.

Success audits should be enabled on all computers in your enterprise. When an organization responds to security incidents, it is critical that they be able to track who created, changed, or deleted an account. Failure audits generate an event when any account management action fails.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|------------------------------------|---|-----------------|
| Audit Application Group Management | This security policy setting determines whether the operating system generates audit events when application group management tasks are performed, such as when an application group is created, changed, or deleted; or a member is added to or removed from an application group. | Not configured |
| Audit Computer Account Management | This security policy setting determines whether the operating system generates audit events when a computer account is created, changed, or deleted. This policy setting is useful for tracking account-related changes to computers that are members of a | Not configured |

| Name | Description | Default setting |
|---------------------------------------|---|-----------------|
| | domain. | |
| Audit Distribution Group Management | This security policy setting determines whether the operating system generates audit events when a distribution group is created, changed, or deleted; or a member is added to or removed from a distribution group. These audit events are only logged on domain controllers. | Not configured |
| Audit Other Account Management Events | <p>This security policy setting determines whether the operating system generates user account management audit events when:</p> <ul style="list-style-type: none"> • The password hash of an account is accessed. This typically happens when the Active Directory® Migration Tool (ADMT) is moving password data. • The Password Policy Checking application programming interface (API) is called. Calls to this function could be part of an attack from a malicious application that is testing whether password complexity policy settings are being applied. • Changes are made to domain policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy or Computer Configuration\Windows | Not configured |

| Name | Description | Default setting |
|---------------------------------|---|-----------------|
| | Settings\Security Settings\Account Policies\Account Lockout Policy. | |
| Audit Security Group Management | <p>This security policy setting determines whether the operating system generates audit events when a security group is created, changed, or deleted; a member is added to or removed from a security group; or a group's type is changed.</p> <p>Security groups can be used for access control permissions and also as distribution lists.</p> | Success |
| Audit User Account Management | <p>This security policy setting determines whether the operating system generates audit events when a user account is created, changed, deleted, renamed, disabled, enabled, locked out, or unlocked; a user account password is set or changed; a security identifier (SID) history is added to a user account; the Directory Services Restore Mode password is set; permissions on accounts that are members of administrators groups are changed; or Credential Manager credentials are backed up or restored.</p> <p>This policy setting is essential for tracking events that involve provisioning and managing user</p> | Success |

| Name | Description | Default setting |
|------|-------------|-----------------|
| | accounts. | |

Audit process tracking

This category of audit policy settings enables auditing of detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

When enabled, the Audit process tracking settings can generate a large number of events. However, the information that these policy settings generate can be very beneficial during an incident response because they provide a detailed log of the processes that were started and when they were started.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|------------------------|--|-----------------|
| Audit DPAPI Activity | This security policy setting determines whether the operating system generates audit events when encryption or decryption calls are made into the data protection application interface (DPAPI), which is used to protect secret information such as stored passwords and key information. For more information about DPAPI, see Windows Data Protection . | Not configured |
| Audit Process Creation | This security policy setting determines whether the operating system generates audit events when a process is | Not configured |

| Name | Description | Default setting |
|---------------------------|---|-----------------|
| | created (starts), and the name of the program or user that created it. | |
| Audit Process Termination | This security policy setting allows you to generate audit events when an attempt is made to end a process. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when a process ends. | Not configured |
| Audit RPC Events | This security policy setting determines whether the operating system generates audit events when inbound remote procedure call (RPC) connections are made. | Not configured |

Audit directory service access

This category of security audit policy settings enables auditing of user access of an Active Directory object that has an associated SACL.



Note

A SACL is list of users and groups for which actions on an object are to be audited on a network that is running the Windows operating system.


Success audits generate an event when a user successfully accesses an Active Directory object that has a SACL that indicates that the user should be audited for the requested action. Failure audits generate an event for each unsuccessful attempt. (Both types of events are created before the user is notified that the request succeeded or failed.) If you enable this policy setting


and configure SACLs on directory objects, a large volume of entries can be generated in the Security logs on domain controllers. You should enable these settings only if you actually intend to use the information that is created.

**Note**

You can configure a SACL on an Active Directory object through the **Security** tab in that object's **Properties** dialog box. This method is analogous to **Audit object access**, except that it applies only to Active Directory objects and not to file system and registry objects.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|--|--|-----------------|
| Audit Detailed Directory Service Replication | This security policy setting can be used to generate security audit events with detailed tracking information about the data that is replicated between domain controllers. This audit subcategory can be useful to diagnose replication issues, but it can create a very high volume of event data. | Not configured |
| Audit Directory Service Access | <p>This security policy setting determines whether the operating system generates events when an Active Directory Domain Services (AD DS) object is accessed.</p> <p> Important Audit events will only be generated on objects with configured SACLs, and only when they are</p> | Not configured |

| Name | Description | Default setting |
|-------------------------------------|---|-----------------|
| | accessed in a manner that matches the SACL settings. | |
| Audit Directory Service Changes | <p>This security policy setting determines whether the operating system generates audit events when objects in AD DS are created, deleted, modified, moved, or undeleted.</p> <p>Changes to Active Directory objects are important events to track to understand the state of the network policy. Directory Service Changes auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed.</p> <p> Important Audit events will only be generated on objects with configured SACLs, and only when they are accessed in a manner that matches the SACL settings.</p> | Not configured |
| Audit Directory Service Replication | This security policy setting determines whether the operating system generates audit events when replication between two domain controllers begins and ends. | Not configured |


Audit logon and logoff events

This category of security audit policy settings enables auditing of each instance that a user logs on, logs off, or connects over the network connection. Instances are generated where the account exists, either on the domain controller if the account is a domain account or on the local computer if the account is a local computer account, and "logon events" are generated on the computer where the user is logging on or off. If you log successful account logon events on a domain controller, workstation logon attempts do not generate logon events. Only interactive and network logon attempts to the domain controller itself generate logon events on the domain controller.

Success audits provide useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged on to which computer. Failure audits are useful for intrusion detection. However, the configuration of failure events also creates a potential DoS condition. When the **Audit: Shut down system immediately if unable to log security audits** policy setting in the **Security Options** section of Group Policy is also enabled, an attacker could generate millions of logon failures to fill the Security log, and force the server to shut down.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|---------------------------|---|-----------------|
| Audit Account Lockout | This security policy setting allows you to audit security events that are generated by a failed attempt to log on to an account that is locked out. Account lockout events are essential for understanding user activity and detecting potential attacks. | Success |
| Audit IPsec Extended Mode | This security policy setting determines whether the operating system generates audit events for the results of the Internet Key Exchange | Not configured |

| Name | Description | Default setting |
|------------------------|--|--|
| | (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations. | |
| Audit IPsec Main Mode | This security policy setting determines whether the operating system generates events for the results of the IKE protocol and AuthIP during Main Mode negotiations. | Not configured |
| Audit IPsec Quick Mode | This security policy setting determines whether the operating system generates audit events for the results of the IKE protocol and AuthIP during Quick Mode negotiations. | Not configured |
| Audit Logoff | <p>This security policy setting determines whether the operating system generates audit events when logon sessions are terminated. These events occur on the computer that was accessed. In the case of an interactive logon, these would be generated on the computer that was logged on to.</p> <p>Logon events are essential to understanding user activity and detecting potential attacks. Logoff events are not 100 percent reliable. For example, the computer can be</p> | <p>Success</p> <p> Note There is no failure event in this subcategory because failed logoffs (such as when a system abruptly shuts down) do not generate an audit record.</p> |

| Name | Description | Default setting |
|-----------------------------|--|--|
| | turned off without a proper logoff and shutdown taking place; in this case, a logoff event will not be generated. | |
| Audit Logon | <p>This security policy setting determines whether the operating system generates audit events when a user attempts to log on to a computer. For an interactive logon, events are generated on the computer that was logged on to. For network logon, such as accessing a share, events are generated on the computer hosting the resource that was accessed.</p> <p>Logon events are essential to tracking user activity and detecting potential attacks.</p> | <p>Success for client computers</p> <p>Success and Failure for servers</p> |
| Audit Network Policy Server | <p>This security policy setting determines whether the operating system generates audit events for RADIUS (IAS) and Network Access Protection (NAP) activity on user access requests (Grant, Deny, Discard, Quarantine, Lock, and Unlock).</p> <p>NAP events can be used to understand the overall health of the network.</p> | Success and Failure |

| Name | Description | Default setting |
|---------------------------------|--|-----------------|
| Audit Other Logon/Logoff Events | <p>This security policy setting determines whether the operating system generates audit events for other logon or logoff events, such as when a Remote Desktop session disconnects or connects, a workstation is locked or unlocked, a screen saver is invoked or dismissed, a user is granted access to a wireless network, a user is granted access to a wired 802.1x network, or a replay attack is detected. The latter indicates that a Kerberos protocol request was received twice with identical information. This condition could also be caused by network misconfiguration.</p> | Not configured |
| Audit Special Logon | <p>This security policy setting determines whether the operating system generates audit events when a special logon is used or a member of a special group logs on.</p> <p>A special logon is a logon that has administrator-equivalent privileges, and it can be used to elevate a process to a higher level.</p> <p>Special Groups is a Windows feature that enables the administrator to find out when</p> | Success |

| Name | Description | Default setting |
|------|---|-----------------|
| | <p>a member of a certain group has logged on. The administrator can set a list of group security identifiers (SIDs) in the registry. If any of these SIDs is added to a token during logon and this auditing subcategory is enabled, a security event is logged. For more information about this feature, see article 947223 in the Microsoft Knowledge Base.</p> <p>Users who hold special privileges can potentially make changes to the system. It is recommended to track their activity.</p> | |

Audit object access

This security audit policy setting enables auditing of the event that is generated by a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

Success audits generate an event when a user successfully accesses an object that has a SACL. Failure audits generate an event for each unsuccessful attempt (some failure events are to be expected during normal computer operations). For example, many applications (such as Microsoft Office Word) always attempt to open files with both Read and Write privileges. If the applications are unable to do so, they then try to open the files with Read-only privileges. If you enable failure auditing and the appropriate SACL on the file, a failure event is recorded when such an event occurs.

Although you can also audit registry keys, we do not recommend auditing them unless you have advanced computer knowledge and know how to use the registry.

You can audit access to objects that are stored in the Internet Information Services (IIS) metabase. To enable metabase object auditing, you must enable the **Audit object access** policy

on the target computer, and then you must set SACLs on the specific metabase objects that you want to monitor.

If you do not configure the policy settings in this category selectively, a large volume of entries can be generated in the Security logs on computers in your organization. Therefore, you should only enable these settings if you actually intend to use the information that is logged.





Note


You must perform a two-step process to enable auditing an object, such as a file, folder, printer, or registry key. After you enable the **Audit object access** policy, you must modify the SACLs of the objects that you want to monitor. For example, to audit any attempts by users to open a particular file, you can configure a Success or Failure audit attribute directly on the file that you want to monitor for that particular event by using Windows Explorer or Group Policy.


The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|------------------------------|---|-----------------|
| Audit Application Generated | This security policy setting determines whether the operating system generates audit events when applications attempt to use the Windows Auditing application programming interfaces (APIs) to create, delete, or initialize an application client context, or for application operations. The level, volume, relevance, and importance of these audit events depend on the application that is generating them. The operating system logs the events as they are generated by the application. | Not configured |
| Audit Certification Services | This security policy setting | Not configured |

| Name | Description | Default setting |
|---------------------------|--|-----------------|
| | generates events when a wide variety of Active Directory Certificate Services (AD CS) operations are performed, such as when AD CS starts, shuts down, is backed up, or is restored; certificates are requested, issued, or revoked; and security permissions for AD CS role services are modified. | |
| Audit Detailed File Share | <p>This security policy setting allows you to audit attempts to access files and folders on a shared folder. Detailed File Share audit events include detailed information about the permissions or other criteria that are used to grant or deny access.</p> <p> Note The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection that is established between a client computer and file share.</p> | Not configured |
| Audit File Share | This security policy setting determines whether the operating system generates audit events when a shared folder is accessed. Audit events are not | Not configured |

| Name | Description | Default setting |
|-------------------------------------|--|-----------------|
| | generated when shared folders are created, deleted, or when share folder permissions change. Combined with File System auditing, File Share auditing allows you to track what content was accessed, the source (IP address and port) of the request, and the user account that was used for access. | |
| Audit File System | <p>This security policy setting determines whether the operating system audits user attempts to access file system objects. These events are essential for tracking activity for file objects that are sensitive or valuable, and these events require extra monitoring.</p> <p> Note Audit events are only generated for objects that have configured SACLs, and only if the type of access requested (such as Write, Read, or Modify) and the account that makes the request match the settings in the SACL.</p> | Not configured |
| Audit Filtering Platform Connection | This security policy setting determines whether the operating system generates audit events when connections are allowed or blocked by the | Not configured |

| Name | Description | Default setting |
|--------------------------------------|--|-----------------|
| | Windows Filtering Platform, such as when an application is blocked from accepting incoming connections, a connection is allowed or blocked, a binding to a local port is allowed or blocked, or an application or service is allowed or blocked from listening on a port for incoming connections. | |
| Audit Filtering Platform Packet Drop | This security policy setting allows you to audit packets that are dropped by the Windows Filtering Platform. A high rate of dropped packets may indicate attempts to gain unauthorized access to computers on your network. | Not configured |
| Audit Handle Manipulation | <p>This security policy setting determines whether the operating system generates audit events when a handle to an object is opened or closed. Enabling Audit Handle Manipulation also enables the logging of "reason for access" data within generated events. Only objects with configured SACLs generate these events, and only if the attempted handle operation matches the SACL.</p> <p> Note Handle Manipulation events are only generated for object types where</p> | Not configured |

| Name | Description | Default setting |
|----------------------------------|---|-----------------|
| | the corresponding File System or Registry Object Access subcategory is enabled. For more information, see Audit File System or Audit Registry . | |
| Audit Kernel Object | <p>This security policy setting allows you to audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events.</p> <p> Note The audits generated are usually only useful to developers.</p> | Not configured |
| Audit Other Object Access Events | This security policy setting determines whether the operating system generates audit events for the management of Task Scheduler jobs or COM+ objects. | Not configured |
| Audit Registry | This security policy setting determines whether the operating system audits user attempts to access registry objects. Audit events are only generated for objects that have configured SACLs specified, and only if the type of access requested (such as Write, Read, or Modify) and the account that | Not configured |

| Name | Description | Default setting |
|-----------|---|-----------------|
| | makes the request match the settings in the SACL. | |
| Audit SAM | This security policy setting allows you to audit events that are generated by attempts to access Security Accounts Manager (SAM) objects including SAM_ALIAS (a local group), SAM_GROUP (a group that is not a local group), SAM_USER (a user account), SAM_DOMAIN (a domain), and SAM_SERVER (a computer account). | Not configured |


Audit policy change

This category of security audit policy setting enables auditing of every incidence of a change to user rights assignment policies, Windows Firewall policies, audit policies, or trust policies.


Audit this to record attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies. Success audits are useful for accounting purposes, and they can help you determine who successfully modified policies in the domain or on individual computers. Failure audits generate an event when a change to user rights assignment policies, audit policies, or trust policies fails.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|---------------------------|--|-----------------|
| Audit Audit Policy Change | This security policy setting determines whether the operating system generates audit events when changes are made to the | Not configured |

| Name | Description | Default setting |
|------------------------------------|---|-----------------|
| | audit policy, including permissions and audit settings on the audit policy object, changing the system audit policy, registration and de-registration of security event sources, changing per-user audit settings, changing the value of CrashOnAuditFail, and changing audit settings on an object. | |
| Audit Authentication Policy Change | <p>This security policy setting determines whether the operating system generates audit events when changes are made to authentication policy, including creation, modification, and removal of forest and domain trusts; changes to the Kerberos protocol policy under Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy, or namespace collision, such as when an added trust collides with an existing namespace name. In addition, audit events are logged when any of the following user rights are granted to a user or group: Access this computer from the network, Allow logon locally, Allow logon through Remote Desktop, Logon as a batch job, or Logon as a service.</p> <p> Note This setting is useful for</p> | Success |

| Name | Description | Default setting |
|--|--|-----------------|
| | tracking changes in domain and forest level trust and for privileges that are granted to user accounts or groups. | |
| Audit Authorization Policy Change | This security policy setting determines whether the operating system generates audit events when user rights are assigned or removed, and when the Encrypting File System (EFS) policy is changed. | Not configured |
| Audit Filtering Platform Policy Change | This security policy setting determines whether the operating system generates audit events for IPsec services status changes, changes to IPsec settings, changes to the Windows Filtering Platform engine and providers, and IPsec Policy Agent service activities. | Not configured |
| Audit MPSSVC Rule-Level Policy Change | This security policy setting determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe), which is used by Windows Firewall. The tracked activities include active policies when the Windows Firewall service starts; changes to the Windows Firewall settings, Group Policy settings, rules, and exception list; and rules ignored or not applied by the Windows Firewall service. | Not configured |

| Name | Description | Default setting |
|----------------------------------|---|-----------------|
| |  Note Changes to firewall rules are important to understand the security state of the computer and how well it is protected against network attacks. | |
| Audit Other Policy Change Events | This security policy setting determines whether the operating system generates events for security policy changes that are not otherwise audited in the Policy Change category, such as Trusted Platform Module (TPM) configuration changes, kernel-mode cryptographic self-tests, and cryptographic provider operations. | Not configured |

Audit privilege use

This category of audit policy setting enables auditing of each instance of a user who exercises a user right.

Success audits generate an event when the exercise of a user right succeeds. Failure audits generate an event for an unsuccessful exercise. If you enable this policy setting, the volume of events that is generated can be very large and cumbersome. You should enable this setting only if you plan to use the information that is generated.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|-----------------------------------|--|-----------------|
| Audit Sensitive Privilege Use | <p>This security policy setting allows you to audit events that are generated when a privileged service is called or when sensitive user rights such as the following are used:</p> <ul style="list-style-type: none"> Act as part of the operating system Back up files and directories Create a token object Debug programs Impersonate a client after authentication Manage auditing and security log Take ownership of files or other objects | Not configured |
| Audit Non-Sensitive Privilege Use | <p>This security policy setting allows you to audit events that are generated by the use of non-sensitive user rights, such as:</p> <ul style="list-style-type: none"> Access Credential Manager as a trusted caller Access this computer from the network Add workstations to the domain Allow log on locally | Not configured |

| Name | Description | Default setting |
|----------------------------------|---|-----------------|
| | Change the system time Force shutdown from a remote system Perform volume maintenance tasks | |
| Audit Other Privilege Use Events | This security policy setting is not used in this version of Windows. | Not configured |

System

This category of audit policy settings enables auditing the restart or shutdown of users' computers, or events that affect either computer security or the Security log. For example, if malicious software tried to change a setting on your computer without your permission, System event auditing would record it.






Note


Because few additional events are recorded if both failure and success audits are enabled for system events, and because all such events are very significant, you should enable these policy settings on all computers in your organization.

The following table describes the settings that are included in this category and their default settings. For more information about the events that are generated by these settings, see the [Security Audit Policy Reference](#).

| Name | Description | Default setting |
|--------------------|---|-----------------|
| Audit IPsec Driver | This security policy setting determines whether the operating system audits the activities of the IPsec driver, and it reports any of the following events: Startup and shutdown of IPsec services | Not configured |

| Name | Description | Default setting |
|-----------------------------|---|---------------------|
| | <p>Packets that are dropped due to integrity check failure</p> <p>Packets that are dropped due to replay check failure</p> <p>Packets that are dropped due to being in plaintext</p> <p>Packets that are received with an incorrect Security Parameter Index (SPI). (This can indicate malfunctioning hardware or interoperability problems.)</p> <p>Failure to process IPsec filters</p> <p> Security A high rate of packet drops by the IPsec filter driver may indicate attempts to gain access to the network by unauthorized systems.</p> | |
| Audit Other System Events | This security policy setting determines whether the operating system audits the startup and shutdown of the Windows Firewall service and driver, security policy processing by the Windows Firewall service, and cryptography key file and migration operations. | Success and Failure |
| Audit Security State Change | This security policy setting determines whether the operating system audits changes in the security state of a system, and it reports system startup and | Success |

| Name | Description | Default setting |
|---------------------------------|---|-----------------|
| | <p>shutdown, changes of system time, and system recovery from CrashOnAuditFail.</p> <p> Important Some auditable activity may not be recorded when a system reboots due to CrashOnAuditFail.</p> | |
| Audit Security System Extension | <p>This security policy setting determines whether the operating system audits events that are related to security system extensions. This can include when a security extension code is loaded (such as an authentication, notification, or security package).</p> <p>It also includes when a service is installed. An audit log is generated when a service is registered with the Service Control Manager. The audit log contains information about the service name, binary, type, start type, and service account.</p> <p> Important Attempts to install or load security system extensions or services that are critical system events that could indicate a security breach.</p> <p>These events are expected to appear more often on a domain controller than on client computers</p> | Not configured |

| Name | Description | Default setting |
|------------------------|---|---------------------|
| | or member servers. | |
| Audit System Integrity | <p>This security policy setting determines whether the operating system audits events that violate the integrity of the security subsystem, which can include any of the following events:</p> <p>Audited events are lost due to a failure of the auditing system.</p> <p>A process uses an invalid local procedure call (LPC) port in an attempt to impersonate a client computer, reply to a client computer's address space, read to a client computer's address space, or write from a client computer's address space.</p> <p>A remote procedure call (RPC) integrity violation is detected.</p> <p>A code integrity violation with an invalid hash value of an executable file is detected.</p> <p>Cryptographic tasks are performed.</p> <p> Important Violations of security subsystem integrity are critical and could indicate a potential security attack.</p> | Success and Failure |

Global Object Access Auditing

Global Object Access Auditing policy settings allow administrators to define computer SACLs per object type for the file system or the registry. The specified SACL is then automatically applied to every object of that type.

Auditors will be able to prove that every resource in the system is protected by an audit policy by just viewing the contents of the Global Object Access Auditing policy settings. For example, the policy setting **Track all changes made by group administrators** shows that this policy is in effect.


Resource SACLs are also useful for diagnostic scenarios. For example, setting a Global Object Access Auditing policy setting to log all the activity for a specific user and enabling the Object Access audit policy for a resource (file system or registry) to track **Access denied** events can help administrators quickly identify which object in a system is denying a user access.




Note

If both a file or folder SACL and a Global Object Access Auditing policy setting (or a single registry setting SACL and a Global Object Access Auditing policy setting) are configured on a computer, the effective SACL is derived from combining the file or folder SACL and the Global Object Access Auditing policy. This means that an audit event is generated if an activity matches either the file or folder SACL or the Global Object Access Auditing policy.

The following table describes the settings that are included in this category and their default settings. For more information about using Global Object Access Auditing, see the [Advanced Security Auditing Step-by-Step Guide](#).

| Name | Description | Default setting |
|-------------|--|-----------------|
| File System | <p>This security policy setting allows you to configure a global SACL on the file system for an entire computer.</p> <p> Note This policy setting must be used in combination with the File System security policy setting</p> | Not configured |

| Name | Description | Default setting |
|----------|---|-----------------|
| | under Object Access. | |
| Registry | <p>This security policy setting allows you to configure a global SACL on the registry for a computer.</p> <p> Note This policy setting must be used in combination with the Registry security policy setting under Object Access.</p> | Not configured |

Additional references

The following links provide additional information about security audit policy settings:

- For more security audit policy information, see [Security Auditing](#) in the Windows Server 2008 and Windows Server 2008 R2 Technical Library.
- For an overview of Windows Server 2008 auditing and compliance issues, see the TechNet magazine article [Auditing and Compliance in Windows Server 2008](#).
- [Security Audit Events for Windows 7 and Windows Server 2008 R2](#) is a downloadable reference spreadsheet that lists all events that appear in the Security log and are logged with a source of Security-Auditing.
- [Article 947223](#) in the Microsoft Knowledge Base describes how to audit when members of identified special groups log on to the computer.

Threats and Countermeasures Guide: User Rights

This section of the Threats and Countermeasures Guide discusses user rights. User rights govern the methods by which a user can log on to a system. User rights are applied at the local computer level, and they allow users to perform tasks on a computer or a domain. User rights include logon rights and privileges. Logon rights control who is authorized to log on to a computer and how they can log on. Privileges control access to computer and domain resources

and can override permissions that have been set on specific objects. Privileges are managed in Group Policy under **User Rights Assignment**.

An example of a logon right is the ability to log on to a computer locally. An example of a privilege is the ability to shut down the computer. Both types of user rights are assigned by administrators to individual users or groups as part of the security settings for the computer.

User Rights Assignment Settings

Each user right has a constant name and Group Policy setting associated with it. The constant names are used when referring to the user right in log events. You can configure the user rights assignment settings in the following location within the Group Policy Management Console (GPMC): **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**.

The following table identifies the user right Group Policy setting and its associated constant name.

| Group Policy Setting | Constant Name |
|---|---------------------------------|
| Access Credential Manager as a trusted caller | SeTrustedCredManAccessPrivilege |
| | |
| Access this computer from the network | SeNetworkLogonRight |
| Act as part of the operating system | SeTcbPrivilege |
| Add workstations to domain | SeMachineAccountPrivilege |
| Adjust memory quotas for a process | SeIncreaseQuotaPrivilege |
| Allow log on locally | SeInteractiveLogonRight |
| Allow log on through Remote Desktop Services | SeRemoteInteractiveLogonRight |
| Back up files and directories | SeBackupPrivilege |
| Bypass traverse checking | SeChangeNotifyPrivilege |

| Group Policy Setting | Constant Name |
|--|-----------------------------------|
| Change the system time | SeSystemtimePrivilege |
| Change the time zone | SeTimeZonePrivilege |
| Create a pagefile | SeCreatePagefilePrivilege |
| Create a token object | SeCreateTokenPrivilege |
| Create global objects | SeCreateGlobalPrivilege |
| Create permanent shared objects | SeCreatePermanentPrivilege |
| Create symbolic links | SeCreateSymbolicLinkPrivilege |
| Debug programs | SeDebugPrivilege |
| Deny access to this computer from the network | SeDenyNetworkLogonRight |
| Deny log on as a batch job | SeDenyBatchLogonRight |
| Deny log on as a service | SeDenyServiceLogonRight |
| Deny log on locally | SeDenyInteractiveLogonRight |
| Deny log on through Remote Desktop Services | SeDenyRemoteInteractiveLogonRight |
| Enable computer and user accounts to be trusted for delegation | SeEnableDelegationPrivilege |
| Force shutdown from a remote system | SeRemoteShutdownPrivilege |
| Generate security audits | SeAuditPrivilege |
| Impersonate a client after authentication | SeImpersonatePrivilege |
| Increase a process working set | SeIncreaseWorkingSetPrivilege |

| Group Policy Setting | Constant Name |
|---|---------------------------------|
| Increase scheduling priority | SeIncreaseBasePriorityPrivilege |
| Load and unload device drivers | SeLoadDriverPrivilege |
| Lock pages in memory | SeLockMemoryPrivilege |
| Log on as a batch job | SeBatchLogonRight |
| Log on as a service | SeServiceLogonRight |
| Manage auditing and security log | SeSecurityPrivilege |
| Modify an object label | SeRelabelPrivilege |
| Modify firmware environment values | SeSystemEnvironmentPrivilege |
| Perform volume maintenance tasks | SeManageVolumePrivilege |
| Profile single process | SeProfileSingleProcessPrivilege |
| Profile system performance | SeSystemProfilePrivilege |
| Remove computer from docking station | SeUndockPrivilege |
| Replace a process level token | SeAssignPrimaryTokenPrivilege |
| Restore files and directories | SeRestorePrivilege |
| Shut down the system | SeShutdownPrivilege |
| Synchronize directory service data | SeSyncAgentPrivilege |
| Take ownership of files or other objects | SeTakeOwnershipPrivilege |

Access Credential Manager as a trusted caller

This policy setting is used by Credential Manager during Backup and Restore. No accounts should have this privilege because it is assigned only to Winlogon. Saved credentials of users may be compromised if this privilege is given to other entities.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

If an account is given this right, the user of the account can create an application that calls into Credential Manager and is then provided the credentials for another user.

Countermeasure

Do not define the **Access Credential Manager as a trusted caller** policy setting for any accounts besides Credential Manager.

Potential impact

None. Not Defined is the default configuration.

Access this computer from the network

This policy setting determines which users can connect to the computer from the network. This capability is required by a number of network protocols, including Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

Possible values:

- User-defined list of accounts
- Not Defined

By default, the members of the following groups have this right on desktop computers and servers:

- Administrators
- Backup Operators
- Everyone

- Users

By default, the members of the following groups have this right on domain controllers:

- Administrators
- Authenticated Users
- Enterprise Domain Controllers
- Everyone
- Pre-Windows 2000 Compatible Access

Vulnerability

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the **Access this computer from the network** user right is required for users to connect to shared printers and folders. If this user right is assigned to the **Everyone** group, anyone in the group can read the files in those shared folders. This situation is unlikely because the groups that are created by a default installation of Windows Server® 2008 R2 and Windows® 7 do not include the **Everyone** group. However, if a computer is upgraded to Windows Server 2008 R2 or Windows 7 and the original computer includes the **Everyone** group as part of its defined users and groups, that group is transitioned as part of the upgrade process, and it is present on the system.

Countermeasure

Restrict the **Access this computer from the network** user right to only those users and groups who require access to the computer. For example, if you configure this policy setting for the Administrators and Users groups, users who log on to the domain can access resources that are shared from servers in the domain if members of the Domain Users group are included in the local Users group.

**Note**

If you are using IPsec to help secure network communications in your organization, ensure that a group that includes computer accounts is given this right. This right is required for successful computer authentication. Assigning this right to **Authenticated Users** or **Domain Computers** meets this requirement.

Potential impact

If you remove the **Access this computer from the network** user right on domain controllers for all users, no one can log on to the domain or use network resources. If you remove this user right on member servers, users cannot connect to those servers through the network. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers that they need to access the network.

Act as part of the operating system

This policy setting determines whether a process can assume the identity of any user and thereby gain access to the resources that the user is authorized to access. Typically, only low-level authentication services require this user right. Potential access is not limited to what is associated with the user by default. The calling process may request that arbitrary additional privileges be added to the access token. The calling process may also build an access token that does not provide a primary identity for auditing in the system event logs.

Possible values:

- User-defined list of accounts
- Not Defined

The default value for this user right is Not Defined.

Vulnerability

Users with the **Act as part of the operating system** user right can take complete control of the computer and erase evidence of their activities.

Countermeasure

Restrict the **Act as part of the operating system** user right to as few accounts as possible, and it should not be assigned to the Administrators group under typical circumstances. When a service

requires this user right, configure the service to log on with the Local System account, which has this privilege inherently. Do not create a separate account and assign this user right to it.

Potential impact

There should be little or no impact because the **Act as part of the operating system** user right is rarely needed by any accounts other than the Local System account.

Add workstations to domain

This policy setting determines which users can add a computer to a specific domain. For it to take effect, it must be assigned so that it applies to at least one domain controller. A user who is assigned this user right can add up to 10 workstations to the domain. Users can also join a computer to a domain if they have the Create Computer Objects permission for an organizational unit (OU) or for the Computers container in the directory. Users who are assigned this permission can add an unlimited number of computers to the domain regardless of whether they have the **Add workstations to domain** user right.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Authenticated Users group have this user right.

Vulnerability

The **Add workstations to domain** user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could install Windows on his or her computer and then add the computer to the domain. The user would know the password for the local administrator account, could log on with that account, and then add his or her domain account to the local Administrators group.

Countermeasure

Configure this setting so that only authorized members of the IT team are allowed to add computers to the domain.

Potential impact

For organizations that have never allowed users to set up their own computers and add them to the domain, this countermeasure has no impact. For those that have allowed some or all users to configure their own computers, this countermeasure forces the organization to establish a formal process for these procedures going forward. It does not affect existing computers unless they are removed from and re-added to the domain.

Adjust memory quotas for a process

This policy setting determines which users can adjust the maximum amount of memory that is available to a process. Although this capability is useful when you must tune computers, it has potential for abuse.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the following groups have this right:

- Administrators
- Local Service
- Network Service

Vulnerability

A user with the **Adjust memory quotas for a process** user right can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. This privilege could be used to start a denial-of-service (DoS) attack.

Countermeasure

Restrict the **Adjust memory quotas for a process** user right to users who require it to perform their jobs, such as application administrators who maintain database management systems or domain administrators who manage the organization's directory and its supporting infrastructure.

Potential impact

Organizations that have not restricted users to roles with limited privileges may find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET

or IIS, you may need to assign the **Adjust memory quotas for a process** user right to additional accounts that are required by those components. IIS requires that this privilege be explicitly assigned to the IWAM_<ComputerName>, Network Service, and Service accounts. Otherwise, this countermeasure should have no impact on most computers. Additionally, some applications might require a service account with this user right to run. If this user right is necessary for a user account, it can be assigned to a local computer account instead of to a domain account. Before you remove a user account from the list of accounts with this right, ensure that those user accounts are not being used as service accounts.

Allow log on locally

This policy setting determines which users can start an interactive session on the computer. Users who do not have this right are still able to start a remote interactive session on the computer if they have the **Allow logon through Remote Desktop Services** right.

Possible values:

- User-defined list of accounts
- Not Defined

By default, the members of the following groups have this right on workstations and servers:

- Administrators
- Backup Operators
- Users

By default, the members of the following groups have this right on domain controllers:

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators

Vulnerability

Any account with the **Allow log on locally** user right can log on to the console of the computer. If you do not restrict this user right to legitimate users who must log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Countermeasure

For domain controllers, assign the **Allow log on locally** user right only to the Administrators group. For other server roles, you may choose to add Backup Operators as well as Administrators. For end-user computers, you should also assign this right to the Users group.

Alternatively, you can assign groups such as Account Operators, Server Operators, and Guests to the **Deny log on locally** user right.

Potential impact

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. If you have installed optional components such as ASP.NET or IIS, you may need to assign the **Allow log on locally** user right to additional

accounts that are required by those components. IIS requires that this user right be assigned to the IUSR_<ComputerName> account. You should confirm that delegated activities are not adversely affected by any changes that you make to the **Allow log on locally** user rights assignments.

Allow log on through Remote Desktop Services

This policy setting determines which users can log on to the computer through a Remote Desktop connection. You should not assign this user right to additional users or groups. Instead, it is a best practice to add users to or remove users from the Remote Desktop Users group to control who can open a Remote Desktop connection to the computer.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Administrators group have this right on domain controllers, workstations, and servers. The Remote Desktops Users group also has this right on workstations and servers.

Vulnerability

Any account with the **Allow log on through Remote Desktop Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who must log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Countermeasure

For domain controllers, assign the **Allow log on through Remote Desktop Services** user right only to the Administrators group. For other server roles and end-user computers, add the Remote Desktop Users group. For servers that have the Remote Desktop (RD) Session Host role service enabled and do not run in Application Server mode, ensure that only authorized IT personnel who must manage the computers remotely belong to either of these groups.



Caution

For RD Session Host servers that run in Application Server mode, ensure that only users who require access to the server have accounts that belong to the Remote Desktop Users group because this built-in group has this logon right by default.

Alternatively, you can assign the **Deny log on through Remote Desktop Services** user right to groups such as Account Operators, Server Operators, and Guests. However, be careful when you use this method because you could block access to legitimate administrators who also belong to a group that has the **Deny log on through Remote Desktop Services** user right.

Potential impact

Removal of the **Allow log on through Remote Desktop Services** user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities are not adversely affected.

Back up files and directories

This policy setting determines which users can circumvent file and directory permissions to back up the computer. This user right is effective only when an application attempts access through the NTFS backup application programming interface (API) through a backup tool such as NTBACKUP.EXE. Otherwise, standard file and directory permissions apply.

Possible values:

- User-defined list of accounts
- Not Defined

By default, this right is granted to Administrators and Backup Operators on workstations and servers. On domain controllers, Administrators, Backup Operators, and Server Operators have this right.

Vulnerability

Users who can back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Countermeasure

Restrict the **Back up files and directories** user right to members of the IT team who must back up organizational data as part of their day-to-day job responsibilities. If you are using backup software that runs under specific service accounts, only these accounts (and not the IT staff) should have the **Back up files and directories** user right.

Potential impact

Changes in the membership of the groups that have the **Back up files and directories** user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators can still perform backup operations.

Bypass traverse checking

This policy setting determines which users can pass through folders without being checked for the Traverse Folder special access permission when they navigate an object path in the NTFS file system or in the registry. This user right does not allow the user to list the contents of a folder. It only allows the user to traverse folders.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The default configuration for the **Bypass traverse checking** setting is to allow all users, including the Everyone group, to bypass traverse checking. Permissions to files and folders are controlled through the appropriate configuration of file system access control lists (ACLs) because the ability to traverse the folder does not provide any Read or Write permissions to the user. The only scenario in which the default configuration could lead to a mishap would be if the administrator who configures permissions does not understand how this policy setting works. For example, the administrator might expect that users who are unable to access a folder are unable to access the contents of any child folders. Such a situation is unlikely, and, therefore, this vulnerability presents little risk.

Countermeasure

Organizations that are extremely concerned about security may want to remove the Everyone group, and perhaps the Users group, from the list of groups that have the **Bypass traverse checking** user right. Taking explicit control over traversal assignments can be an effective way to limit access to sensitive information. Access-based enumeration can also be used. If you use access-based enumeration, users cannot see any folder or file to which they do not have access. For more information about this feature, see [Access-based Enumeration](#).

Potential impact

The Windows operating systems, as well as many applications, were designed with the expectation that anyone who can legitimately access the computer will have this user right. Therefore, we recommend that you thoroughly test any changes to assignments of the **Bypass traverse checking** user right before you make such changes to production systems. In particular, IIS requires this user right to be assigned to the Network Service, Local Service, IIS_WPG, IUSR_<ComputerName>, and IWAM_<ComputerName> accounts. (It must also be assigned to the ASPNET account through its membership in the Users group.) We recommend that you leave this policy setting at its default configuration.

Change the system time

This policy setting determines which users can adjust the time on the computer's internal clock. It is not required to change the time zone or other display characteristics of the system time.

Possible values:

- User-defined list of accounts
- Not Defined

By default on workstations and servers, members of the Administrators and Local Service groups have this right. On domain controllers, members of the Administrators, Server Operators, and Local Service groups have this right.

Vulnerability

Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requester and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos protocol tickets.

The risk from these types of events is mitigated on most domain controllers, member servers, and end-user computers because the Windows Time Service automatically synchronizes time with domain controllers in the following ways:

- All desktop client computers and member servers use the authenticating domain controller as their inbound time partner.

- All domain controllers in a domain nominate the primary domain controller (PDC) emulator operations master as their inbound time partner.
- All PDC emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner.
- The PDC emulator operations master at the root of the domain is authoritative for the organization. Therefore, we recommend that you configure this computer to synchronize with a reliable external time server.

This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time Service or reconfigure it to synchronize with a time server that is not accurate.

Countermeasure

Restrict the **Change the system time** user right to users with a legitimate need to change the system time, such as members of the IT team.

Potential impact

There should be no impact because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Change the time zone

This policy setting determines which users can adjust the time zone that is used by the computer for displaying the local time, which is the computer's system time plus the time zone offset.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Administrators and Users group have this right.

Vulnerability

Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones.

Countermeasure

Countermeasures are not required because system time is not affected by this setting.

Potential impact

None. Not Defined is the default configuration.

Create a page file

This policy setting determines which users can create and change the size of a page file. Specifically, it determines whether they can specify a page file size for a particular drive in the **Performance Options** box located on the **Advanced** tab of the **System Properties** dialog box or through using internal application interfaces (APIs).

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Administrators group have this right.

Vulnerability

Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

Countermeasure

Restrict the **Create a page file** user right to members of the Administrators group.

Potential impact

None. Restricting this right to members of the Administrators group is the default configuration.

Create a token object

This policy setting determines which accounts a process can use to create a token, and which accounts it can then use to gain access to any local resources when the process uses `NtCreateToken()` or other token-creation APIs.

Possible values:

- User-defined list of accounts
- Not Defined

This user right is used internally by the operating system; by default, it is not assigned to any user groups.

Vulnerability



Caution

A user account that is given this user right has complete control over the system, and it can lead to the system being compromised. We highly recommend that you do not assign any user accounts this right.

The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their privileges or create a DoS condition.

Countermeasure

Do not assign the **Create a token object** user right to any users. Processes that require this user right should use the Local System account, which already includes it, instead of a separate user account that has this user right assigned.

Potential impact

None. Not Defined is the default configuration.

Create global objects

This policy setting determines which users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Administrators group have this right, as do Local Service and Network Service accounts.

Vulnerability

Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption.

Countermeasure

Restrict the **Create global objects** user right to members of the local Administrators and Service groups.

Potential impact

None. Restricting the **Create global objects** user right to members of the local Administrators and Service groups is the default configuration.

Create permanent shared objects

This policy setting determines which users can create directory objects in the object manager. Users who have this capability can create permanent shared objects, including devices, semaphores, and mutexes. This user right is useful to kernel-mode components that extend the object namespace, and they have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right to any users.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Users who have the **Create permanent shared objects** user right could create new shared objects and expose sensitive data to the network.

Countermeasure

Do not assign the **Create permanent shared objects** user right to any users. Processes that require this user right should use the System account, which already includes this user right, instead of a separate user account.

Potential impact

None. Not Defined is the default configuration.

Create symbolic links

This policy setting determines which users can create a symbolic link from the currently logged on computer to a file or folder in a different location.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the Administrators group have this right.

Vulnerability

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a DoS attack.

Countermeasure

Do not assign the **Create symbolic links** user right to standard users. Restrict this right to trusted administrators. You can use the **fsutil** command to establish a **symlink** file system setting that controls the kind of symbolic links that can be created on a computer. For more information about **fsutil** and symbolic links, type **fsutil behavior set symlinkevaluation /?** at an elevated command prompt.

Potential impact

None. Not defined is the default configuration.

Debug programs

This policy setting determines which users can attach to or open any process, even those they do not own. This user right provides access to sensitive and critical operating-system components.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The **Debug programs** user right can be exploited to capture sensitive computer information from system memory or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information or to insert rootkit code. By default, the **Debug programs** user right is assigned only to administrators, which helps mitigate risk from this vulnerability.

Countermeasure

Remove the accounts of all users and groups that do not require the **Debug programs** user right.

Potential impact

If you revoke this user right, no one can debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the **Debug programs** user right to a separate Group Policy for that OU.

Deny access to this computer from the network

This policy setting determines which users are prevented from accessing this computer over the network.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

Countermeasure

Assign the **Deny access to this computer from the network** user right to the following accounts:

- ANONYMOUS LOGON
- Built-in local Administrator account
- Local Guest account
- All service accounts

An important exception to this list is any service accounts that are used to start services that must connect to the computer over the network. For example, if you have configured a shared folder for Web servers to access and present content within that folder through a Web site, you may need to allow the account that runs IIS to log on to the server with the shared folder from the network. This user right is particularly effective when you must configure servers and workstations on which sensitive information is handled because of regulatory compliance concerns.

Potential impact

If you configure the **Deny access to this computer from the network** user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks are not negatively affected.

Deny log on as a batch job

This policy setting determines which accounts are prevented from logging on by using a batch-queue tool, which is a feature in Windows 7 and Windows Server 2008 R2 that is used to schedule and start jobs automatically one or more times in the future. The ability to log on by using a batch-queue tool is needed for any accounts that are used to start scheduled jobs by means of the Task Scheduler.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Accounts that have the **Deny log on as a batch job** user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Countermeasure

Assign the **Deny log on as a batch job** user right to the local Guest account.

Potential impact

If you assign the **Deny log on as a batch job** user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks are not affected adversely.

Deny log on as a service

This policy setting determines which users are prevented from logging on to the computer as a service.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Countermeasure

We recommend that you not assign the **Deny log on as a service** user right to any accounts, which is the default configuration. Organizations that are extremely concerned about security may want to assign this user right to groups and accounts that they are certain will never need to log on as a service.

Potential impact

If you assign the **Deny log on as a service** user right to specific accounts, services may not start and a DoS condition could result.

Deny log on locally

This policy setting determines which users are prevented from logging on directly at the computer's console.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who must log on to the console

of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Countermeasure

Assign the **Deny log on locally** user right to the local guest account. If you have installed optional components such as ASP.NET, you may want to assign this user right to additional accounts that are required by those components.

Potential impact

If you assign the **Deny log on locally** user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that are configured with the Web Server role. You should confirm that delegated activities are not adversely affected.

Deny log on through Remote Desktop Services

This policy setting determines which users are prevented from logging on to the computer through a Remote Desktop connection.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, malicious users might download and run software that elevates their privileges.

Countermeasure

Assign the **Deny log on through Remote Desktop Services** user right to the built-in local guest account and all service accounts. If you have installed optional components such as ASP.NET, you may want to assign this user right to additional accounts that are required by those components.

Potential impact

If you assign the **Deny log on through Remote Desktop Services** user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right cannot connect to the computer through Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks are not negatively affected.

Enable computer and user accounts to be trusted for delegation

This policy setting determines which users can change the **Trusted for Delegation** setting on a user or computer object in Active Directory® Domain Services (AD DS). Users and computers that are assigned this user right must also have write access to the account control flags on the object.

Delegation of authentication is a capability that client and server applications use when they have multiple tiers. It allows a public-facing service to use client credentials to authenticate to an application or database service. For this configuration to be possible, both client and server must run under accounts that are trusted for delegation.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Countermeasure

The **Enable computer and user accounts to be trusted for delegation** user right should be assigned only if there is a clear need for its functionality. When you assign this right, you should investigate the use of constrained delegation to control what the delegated accounts can do. On domain controllers, this right is assigned to the Administrators group by default.



Note

There is no reason to assign this user right to anyone on member servers and workstations that belong to a domain because it has no meaning in those contexts. It is only relevant on domain controllers and stand-alone computers.

Potential impact

None. Not Defined is the default configuration.

Force shutdown from a remote system

This policy setting determines which users can shut down a computer from a remote location on the network.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

Countermeasure

Restrict the **Force shutdown from a remote system** user right to members of the Administrators group or other specifically assigned roles that require this capability, such as non-administrative operations center staff.

Potential impact

If, on a domain controller, you remove the **Force shutdown from a remote system** user right from the Server Operator group, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities are not adversely affected.

Generate security audits

This policy setting determines which accounts can be used by a process to generate audit records in the Security log. You can use the information in the Security log to trace unauthorized computer access.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Accounts that can 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, attackers could use this method to remove evidence of their unauthorized activities. If the computer is configured to shut down when it is unable to write to the Security log and it is not configured to automatically back up the log files, this method could be used to create a DoS condition.

Countermeasure

Ensure that only the Local Service and Network Service accounts have the **Generate security audits** user right assigned to them.

Potential impact

None. Restricting the **Generate security audits** user right to the Local Service and Network Service accounts is the default configuration.

Impersonate a client after authentication

This policy setting determines which programs are allowed to impersonate a user or another specified account and act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user cannot cause a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.

Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.

A user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user.
- The user in this logon session logged on to the network with explicit credentials to create the access token.
- The requested level is less than Impersonate, such as Anonymous or Identify.

Because of these factors, users do not usually need to have this user right assigned.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

An attacker with the **Impersonate a client after authentication** user right could create a service, trick a client computer into connecting to the service, and then impersonate that computer to elevate the attacker's level of access to that of the computer.

Countermeasure

On member servers, ensure that only the Administrators and Service groups (SERVICE, Local Service, and Network Service) have the **Impersonate a client after authentication** user right assigned to them.

Potential impact

In most cases, this configuration has no impact. If you have installed optional components such as ASP.NET or IIS, you may need to assign the **Impersonate a client after authentication** user right to additional accounts that are required by those components, such as IUSR_<ComputerName>, IIS_WPG, ASP.NET, or IWAM_<ComputerName>.

Increase a process working set

This policy setting determines which users can increase or decrease the size of a process's working set. The working set of a process is the set of memory pages currently visible to the process in physical RAM memory. These pages are resident, and they are available for an application to use without triggering a page fault. The minimum and maximum working set sizes affect the virtual memory paging behavior of a process.

Possible values:

- User-defined list of accounts
- Not Defined

By default, standard users have this right.

Vulnerability

Increasing the working set size for a process decreases the amount of physical memory that is available to the rest of the system.

Countermeasure

Increase user awareness of the impact of increasing a process working set and how to recognize when their system is adversely affected by changing this setting.

Potential impact

None. Allowing standard users to increase the process working set is the default configuration.

Increase scheduling priority

This policy setting determines which users can increase the base priority class of a process. It is not a privileged operation to increase relative priority within a priority class. This user right is not required by administrative tools that are supplied with the operating system, but it might be required by software development tools.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

Countermeasure

Verify that only Administrators have the **Increase scheduling priority** user right assigned to them.

Potential impact

None. Restricting the **Increase scheduling priority** user right to members of the Administrators group is the default configuration.

Load and unload device drivers

This policy setting determines which users can dynamically load and unload device drivers. This user right is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer.



Note

This right does not apply to Plug and Play device drivers.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Device drivers run as highly privileged code. A user who has the **Load and unload device drivers** user right could unintentionally install malicious software that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.



Note

You must have this user right or be a member of the local Administrators group to install a new driver for a local printer or to manage a local printer and configure defaults for options such as duplex printing.

Countermeasure

Do not assign the **Load and unload device drivers** user right to any user or group other than Administrators on member servers. On domain controllers, do not assign this user right to any user or group other than Domain Admins.

Potential impact

If you remove the **Load and unload device drivers** user right from the Print Operators group or other accounts, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks are not negatively affected.

Lock pages in memory

This policy setting determines which accounts can use a process to keep data in physical memory, which prevents the computer from paging the data to virtual memory on disk. If you assign this user right, significant degradation of computer performance can occur.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Users with the **Lock pages in memory** user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

Countermeasure

Do not assign the **Lock pages in memory** user right to any accounts.

Potential impact

None. Not Defined is the default configuration.

Log on as a batch job

This policy setting determines which accounts can log on by using a batch-queue tool such as the Task Scheduler service. When an administrator uses the Add Scheduled Task Wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the **Log on as a batch job** user right. When the scheduled time arrives, the Task Scheduler service logs on the user as a batch job instead of as an interactive user, and the task runs in the user's security context.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The **Log on as a batch job** user right presents a low-risk vulnerability. For most organizations, the default setting of Not Defined is sufficient. Members of the local Administrators group have this right by default.

Countermeasure

You should allow the computer to manage this logon right automatically if you want to allow scheduled tasks to run for specific user accounts. If you do not want to use the Task Scheduler in this manner, configure the **Log on as a batch job** user right for only the Local Service account.

For IIS servers, you should configure this policy locally instead of through domain-based Group Policy settings so that you can ensure that the local IUSR_<ComputerName> and IWAM_<ComputerName> accounts have this logon right.

Potential impact

If you configure the **Log on as a batch job** setting by using domain-based Group Policy settings, the computer cannot assign the user right to accounts that are used for scheduled jobs in the Task Scheduler. If you install optional components such as ASP.NET or IIS, you may need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the IIS_WPG group and the IUSR_<ComputerName>, ASPNET, and IWAM_<ComputerName> accounts. If this user right is not assigned to this group and these accounts, IIS cannot run some COM objects that are necessary for proper functionality.

Log on as a service

This policy setting determines which service accounts can register a process as a service. In Windows Server 2008 R2 and Windows 7, only the Network Service account has this right by default. Any service that runs under a separate user account must be assigned this user right.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Log on as a service allows accounts to start network services or services that run continuously on a computer, even when no one is logged on to the console. The risk is reduced by the fact that only users with administrative privileges can install and configure services. An attacker who has already attained that level of access could configure the service to run with the Local System account.

Countermeasure

By definition, the Network Service account has the **Log on as a service** user right. This right is not granted through the Group Policy setting. You should minimize the number of other accounts that are granted this user right.

Potential impact

On most computers, restricting the **Log on as a service** user right to the Local System, Local Service, and Network Service built-in accounts is the default configuration, and there is no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the **Log on as a service** user right to additional accounts that are required by those components. IIS requires that this user right be explicitly granted to the ASPNET user account.

Manage auditing and security log

This policy setting determines which users can specify object access audit options for individual resources such as files, Active Directory objects, and registry keys. Object access audits are not performed unless you enable them by using either the GPMC or the Auditpol command-line tool. A user who is assigned this user right can also view and clear the Security log in Event Viewer. For more information about audit policy, see the [Threats and Countermeasures Guide: Advanced Security Audit Policy](#) section of this guide.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Anyone with the **Manage auditing and security log** user right can clear the Security log to erase important evidence of unauthorized activity.

Countermeasure

Ensure that only the local Administrators group has the **Manage auditing and security log** user right.

Potential impact

Restricting the **Manage auditing and security log** user right to the local Administrators group is the default configuration.



Warning

If groups other than the local Administrators group have been assigned this user right, removing this user right might cause performance issues with other applications. Before removing this right from such a group, investigate whether any applications are dependent on this right.

Modify an object label

This policy setting determines which users can modify the integrity label of objects, such as files, registry keys, or processes that are owned by other users. The integrity label is used by the Windows Integrity Controls (WIC) feature, and it is new to Windows 7. WIC keeps lower-integrity processes from modifying higher-integrity objects by assigning one of six possible labels to objects on the system.

The following list describes the integrity levels from lowest to highest integrity:

- **Untrusted** Default assignment for processes that are logged on anonymously.
- **Low** Default assignment for processes that interact with the Internet.
- **Medium** Default assignment for standard user accounts and any object not explicitly designated with a lower or higher integrity level.
- **High** Default assignment for administrator accounts and processes that request to run using administrative rights.
- **System** Default assignment for Windows kernel and core services.
- **Installer** Used by setup programs to install software. It is important that only trusted software is installed on computers because objects that are assigned the Installer integrity level can install, modify, and uninstall all other objects.

Possible values:

- User-defined list of accounts
- Not Defined

By default, no user accounts are given this right.

Vulnerability

Anyone with the **Modify an object label** user right can change the integrity level of a file or process so that it becomes elevated or decreased to a point where it can be deleted by lower-level processes. Either of these states effectively circumvents the protection offered by Windows Integrity Controls and makes your system vulnerable to attacks by malicious software. If malicious software is set with an elevated integrity level such as Trusted Installer or System, administrator accounts do not have sufficient integrity levels to delete the program from the system. In that case, use of the **Modify an object label** right is mandated so that the object can be relabeled. However, the relabeling must occur by using a process that is at the same or a higher level of integrity than the object that you are attempting to relabel.

Countermeasure

Do not give any group this right. If necessary, implement it for a constrained period of time to a trusted individual to respond to a specific organizational need.

Potential impact

None. Not Defined is the default configuration.

Modify firmware environment values

This security setting determines who can modify firmware environment values. The effect of the setting depends on the processor.

On x86-based computers, the only firmware environment value that can be modified by assigning this user right is the **Last Known Good Configuration** setting, which should only be modified by the system.

On Itanium-based computers, boot information is stored in nonvolatile RAM. Users must be assigned this user right to run bootcfg.exe and to change the **Default Operating System** setting on **Startup and Recovery** in **System Properties**.

On all computers, this user right is required to install or upgrade Windows.



Note

This security setting does not affect who can modify the system environment variables and user environment variables that are displayed on the **Advanced** tab of **System Properties**.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Anyone who is assigned the **Modify firmware environment values** user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

Countermeasure

Ensure that only the local Administrators group is assigned the **Modify firmware environment values** user right.

Potential impact

None. Restricting the **Modify firmware environment values** user right to the members of the local Administrators group is the default configuration.

Perform volume maintenance tasks

This policy setting determines which users can perform volume or disk management tasks, such as defragmenting an existing volume, creating or removing volumes, and running the Disk Cleanup tool.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

A user who is assigned the **Perform volume maintenance tasks** user right could delete a volume, which could result in the loss of data or a DoS condition. Also, disk maintenance tasks can be used to modify data on the disk such as user rights assignments that might lead to escalation of privileges.

Countermeasure

Ensure that only the local Administrators group is assigned the **Perform volume maintenance tasks** user right.

Potential impact

None. Restricting the **Perform volume maintenance tasks** user right to the local Administrators group is the default configuration.

Profile single process

This policy setting determines which users can sample the performance of an application process. Typically, you do not need this user right to use the Performance console. However, you do need this user right if System Monitor is configured to collect data through Windows Management Instrumentation (WMI).

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The **Profile single process** user right presents a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might want to attack directly. Attackers may be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion-detection system. They could also identify other users who are logged on to a computer.

Countermeasure

Ensure that only the local Administrators group is assigned the **Profile single process** user right.

Potential impact

If you remove the **Profile single process** user right from the Power Users group or other accounts, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks are not negatively affected.

Profile system performance

This policy setting determines which users can sample the performance of computer system processes. This privilege is required by the Performance console only if it is configured to collect data through WMI. Typically, you do not need this user right to use the Performance console. However, you must have this user right if System Monitor is configured to collect data through WMI.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The **Profile system performance** user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might want to attack directly. Attackers may also be able to determine what processes are active on the computer so that they could identify countermeasures to avoid, such as antivirus software or an intrusion detection system.

Countermeasure

Ensure that only the local Administrators group is assigned the **Profile system performance** user right.

Potential impact

None. Restricting the **Profile system performance** user right to the local Administrators group is the default configuration.

Remove computer from docking station

This policy setting determines which users of a portable computer need to log on and then click **Eject PC** on the **Start** menu to undock the computer.

Possible values:

- User-defined list of accounts
- Not Defined

By default, members of the following group have this right:

- Local Administrators

Vulnerability

Anyone who has the **Remove computer from docking station** user right can log on and then remove a portable computer from its docking station. If this setting is not defined, it has the same effect as if everyone were granted this right.

However, the value of implementing this countermeasure is reduced by the following factors:

- If attackers can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system starts.
- This setting does not affect servers because they typically are not installed in docking stations.
- An attacker could steal the computer and the docking station together.
- Computers that can be mechanically undocked can be physically removed by the user whether or not they use the Windows undocking functionality.

Countermeasure

Ensure that only the local Administrators group and the user account to which the computer is allocated are assigned the **Remove computer from docking station** user right.

Potential impact

By default, only members of the local Administrators group are granted this right. Other user accounts must be explicitly granted the right as necessary. If your organization's users are not members of the local Administrators groups on their portable computers, they cannot remove their own portable computers from their docking stations without shutting them down first. Therefore, you may want to assign the **Remove computer from docking station** privilege to the local Users group for portable computers.

Replace a process level token

This policy setting determines which parent processes can replace the access token that is associated with a child process.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Users with the **Replace a process level token** user right can start processes as other users whose credentials they know.

Countermeasure

For member servers, ensure that only the Local Service and Network Service accounts have the **Replace a process level token** user right.

Potential impact

On most computers, restricting the **Replace a process level token** user right to the Local Service and Network Service built-in accounts is the default configuration, and there is no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the **Replace a process level token** user right to additional accounts. For example, IIS requires that the Service, Network Service, and IWAM_<ComputerName> accounts be explicitly granted this user right.

Restore files and directories

This security setting determines which users can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories, and determines which users can set any valid security principal as the owner of an object.

Granting this user right to an account is similar to granting the account the following permissions to all files and folders on the system:

- Traverse Folder/Execute File
- Write



Caution

Users with this user right can overwrite registry settings, hide data, and gain ownership of system objects. We strongly recommend that you only assign this user right to trusted users.

By default, this right is granted to the Administrators and Backup Operators groups. On domain controllers, it is also granted to the Server Operators group.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

An attacker with the **Restore files and directories** user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data,

data corruption, or a DoS condition. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install programs that provide for continued access to the computer.



Note

Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Countermeasure

Ensure that only the local Administrators group is assigned the **Restore files and directories** user right unless your organization has clearly defined roles for backup and for restore personnel.

Potential impact

If you remove the **Restore files and directories** user right from the Backup Operators group and other accounts, users who are not members of the local Administrators group cannot load data backups. If your organization delegates the restoration of backups to a subset of your IT staff, you should verify that this change does not negatively affect the ability of your organization's personnel to do their jobs.

Shut down the system

This policy setting determines which users can shut down the local computer.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Although the **Shut down the system** user right requires the ability to log on to the server, you should be very careful about which accounts and groups that you allow to shut down a domain controller.

When a domain controller is shut down, it is no longer available to process logons, process Group Policy settings, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single-Master Operations (FSMO) roles, you

can disable key domain functionality, such as processing logons for new passwords—the primary domain controller (PDC) emulator role.

For other server roles, especially those where non-administrators have rights to log on to the server (such as RD Session Host servers), it is critical that this privilege be removed from users that do not have a legitimate reason to restart the servers.

Countermeasure

Ensure that only the Administrators and Backup Operators groups are assigned the **Shut down the system** user right on member servers, and ensure that only the Administrators group is assigned the user right on domain controllers.

Potential impact

The impact of removing these default groups from the **Shut down the system** user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities are not adversely affected.

Synchronize directory service data

This policy setting determines which users and groups have the authority to synchronize all directory service data, regardless of the protection on the objects and properties. This privilege is required to use LDAP directory synchronization (dirsync) services.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

The **Synchronize directory service data** user right affects domain controllers; only domain controllers should be able to synchronize directory service data. Domain controllers have this user right inherently because the synchronization process runs in the context of the **System** account on domain controllers. Attackers who have this user right can view all information that is stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

Countermeasure

Ensure that no accounts are assigned the **Synchronize directory service data** user right.

Potential impact

None. Not Defined is the default configuration.

Take ownership of files or other objects

This policy setting determines which users can take ownership of any securable object in the computer, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads.

Possible values:

- User-defined list of accounts
- Not Defined

Vulnerability

Any users with the **Take ownership of files or other objects user right** can take control of any object, regardless of the permissions on that object, and then make any changes that they want to make that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Countermeasure

Ensure that only the local Administrators group has the **Take ownership of files or other objects** user right.

Potential impact

None. Restricting the **Take ownership of files or other objects** user right to the local Administrators group is the default configuration.

Threats and Countermeasures Guide: Security Options

Security Options

The Security Options section of Group Policy configures computer security settings for digital data signatures, Administrator and Guest account names, access to floppy disk and CD/DVD drives, driver installation behavior, and logon prompts.

Security Options settings

You can configure the Security Options policy settings in the following location within the Group Policy Object Editor or the Group Policy Management Console:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

The Security Options item of Group Policy contains the following policies:

- [Accounts: Administrator account status](#)
- [Accounts: Guest account status](#)
- [Accounts: Limit local account use of blank passwords to console logon only](#)
- [Accounts: Rename administrator account](#)
- [Accounts: Rename guest account](#)
- [Audit: Audit the access of global system objects](#)
- [Audit: Audit the use of Backup and Restore privilege](#)
- [Audit: Force audit policy subcategory settings \(Windows Vista or later\) to override audit policy category settings](#)
- [Audit: Shut down system immediately if unable to log security audits](#)
- [DCOM: Machine Access Restrictions in Security Descriptor Definition Language \(SDDL\)](#)
- [DCOM: Machine Launch Restrictions in Security Descriptor Definition Language \(SDDL\)](#)
- [Devices: Allow undock without having to log on](#)
- [Devices: Allowed to format and eject removable media](#)
- [Devices: Prevent users from installing printer drivers](#)

- [Devices: Restrict CD-ROM access to locally logged-on user only](#)
- [Devices: Restrict floppy access to locally logged-on user only](#)
- [Domain controller: Allow server operators to schedule tasks](#)
- [Domain controller: LDAP server signing requirements](#)
- [Domain controller: Refuse machine account password changes](#)
- [Domain member: Digitally encrypt or sign secure channel data \(multiple related settings\)](#)
- [Domain member: Disable machine account password changes](#)
- [Domain member: Maximum machine account password age](#)
- [Domain member: Require strong \(Windows 2000 or later\) session key](#)
- [Interactive logon: Display user information when the session is locked](#)
- [Interactive logon: Do not display last user name](#)
- [Interactive logon: Do not require CTRL+ALT+DEL](#)
- [Interactive logon: Message text for users attempting to log on and Message title for users attempting to log on](#)
- [Interactive logon: Number of previous logons to cache \(in case domain controller is not available\)](#)
- [Interactive logon: Prompt user to change password before expiration](#)
- [Interactive logon: Require Domain Controller authentication to unlock workstation](#)
- [Interactive logon: Require smart card](#)
- [Interactive logon: Smart card removal behavior](#)
- [Microsoft network client and server: Digitally sign communications \(four related settings\)](#)
- [Microsoft network client: Send unencrypted password to third-party SMB servers](#)
- [Microsoft network server: Amount of idle time required before suspending session](#)
- [Microsoft network server: Disconnect clients when logon hours expire](#)
- [Microsoft network server: Server SPN target name validation level](#)
- [Network access: Allow anonymous SID/Name translation](#)
- [Network access: Do not allow anonymous enumeration of SAM accounts](#)
- [Network access: Do not allow anonymous enumeration of SAM accounts and shares](#)

- [Network access: Do not allow storage of passwords or credentials for network authentication](#)
- [Network access: Let Everyone permissions apply to anonymous users](#)
- [Network access: Named Pipes that can be accessed anonymously](#)
- [Network access: Remotely accessible registry paths](#)
- [Network access: Remotely accessible registry paths and sub-paths](#)
- [Network access: Restrict anonymous access to Named Pipes and Shares](#)
- [Network access: Shares that can be accessed anonymously](#)
- [Network access: Sharing and security model for local accounts](#)
- [Network security: Allow Local System to use computer identity for NTLM](#)
- [Network security: Allow Local System NULL session fallback](#)
- [Network Security: Allow PKU2U authentication requests to this computer to use online identities](#)
- [Network security: Configure encryption types allowed for Kerberos](#)
- [Network security: Do not store LAN Manager hash value on next password change](#)
- [Network security: Force logoff when logon hours expire](#)
- [Network security: LAN Manager authentication level](#)
- [Network security: LDAP client signing requirements](#)
- [Network security: Minimum session security for NTLM SSP based \(including secure RPC\) clients](#)
- [Network security: Minimum session security for NTLM SSP based \(including secure RPC\) servers](#)
- [Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication](#)
- [Network security: Restrict NTLM: Add server exceptions in this domain](#)
- [Network Security: Restrict NTLM: Audit Incoming NTLM Traffic](#)
- [Network Security: Restrict NTLM: Audit NTLM authentication in this domain](#)
- [Network Security: Restrict NTLM: Incoming NTLM traffic](#)
- [Network Security: Restrict NTLM: NTLM authentication in this domain](#)
- [Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers](#)
- [Recovery console: Allow automatic administrative logon](#)

- [Recovery console: Allow floppy copy and access to all drives and all folders](#)
- [Shutdown: Allow system to be shut down without having to log on](#)
- [Shutdown: Clear virtual memory pagefile](#)
- [System cryptography: Force strong key protection for user keys stored on the computer](#)
- [System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing](#)
- [System objects: Default owner for objects created by members of the Administrators group](#)
- [System objects: Require case insensitivity for non-Windows subsystems](#)
- [System objects: Strengthen default permissions of internal system objects \(e.g. Symbolic Links\)](#)
- [System settings: Optional subsystems](#)
- [System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies](#)
- [User Account Control: Admin Approval Mode for the Built-in Administrator account](#)
- [User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop](#)
- [User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode](#)
- [User Account Control: Behavior of the elevation prompt for standard users](#)
- [User Account Control: Detect application installations and prompt for elevation](#)
- [User Account Control: Only elevate executables that are signed and validated](#)
- [User Account Control: Only elevate UIAccess applications that are installed in secure locations](#)
- [User Account Control: Run all administrators, in Admin Approval Mode](#)
- [User Account Control: Switch to the secure desktop when prompting for elevation](#)
- [User Account Control: Virtualize file and registry write failures to per-user locations](#)

Accounts: Administrator account status

This policy setting enables or disables the Administrator account for normal operational conditions. If you start a computer in Safe Mode, the Administrator account is always enabled, regardless of how you configure this policy setting.

Possible values:

- Enabled

- Disabled
- Not Defined

Vulnerability

The built-in Administrator account cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. This account has a well-known security identifier (SID), and there are non-Microsoft tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on. All other accounts that are members of the Administrator's group have the safeguard of locking out the account if the number of failed logons exceeds its configured maximum.

Countermeasure

Disable the **Accounts: Administrator account status** policy setting so that the built-in Administrator account cannot be used in a normal system startup.

If it is very difficult to maintain a regular schedule for periodic password changes for local accounts, you can disable the built-in Administrator account instead of relying on regular password changes to protect it from attack.

Potential impact

Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in Safe Mode to fix the problem that caused the secure channel to fail.

If the current Administrator password does not meet the password requirements, you cannot enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Accounts: Guest account status

This policy setting enables or disables the Guest account.

Possible values:

- Enabled
- Disabled

- Not Defined

Vulnerability

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group are accessible over the network, which could lead to the exposure or corruption of data.

Countermeasure

Disable the **Accounts: Guest account status** policy setting so that the built-in Guest account cannot be used.

Potential impact

All network users must be authenticated before they can access shared resources. If you disable the Guest account and the **Network Access: Sharing and Security Model** option is set to **Guest Only**, network logons fail, such as those performed by the Microsoft Network Server (SMB Service). This policy setting should have little impact on most organizations because **Disabled** is the default setting.

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

This policy setting enables or disables remote interactive logons by network services such as Terminal Services or Remote Desktop Services, Telnet, and File Transfer Protocol (FTP) for local accounts that have blank passwords. If you enable this policy setting, a local account must have a non-blank password to perform an interactive or network logon from a remote client.

Possible values:

- Enabled
- Disabled
- Not Defined



Caution

This policy setting does not affect interactive logons that are performed physically at the console or logons that use domain accounts. It is possible for non-Microsoft applications that use remote interactive logons to bypass this policy setting.

Vulnerability

Blank passwords are a serious threat to computer security, and they should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings

for Active Directory® domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

Countermeasure

Enable the **Accounts: Limit local account use of blank passwords to console logon only** policy setting.

Potential impact

None. This is the default configuration.

Accounts: Rename administrator account

This policy setting determines whether a different account name is associated with the SID for the Administrator account.

Possible values:

- *User-defined text*
- Not Defined

Vulnerability

If you rename the Administrator account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The user who installs the operating system specifies an account that is the first member of the Administrator group and has full rights to configure the computer. The account may not have the name Administrator, so this countermeasure is applied by default on new Windows® 7 installations. If a computer is upgraded from a previous version of Windows to Windows 7, the account with the name Administrator is retained with all the rights and privileges that were defined for the account in the previous installation.

The built-in Administrator account cannot be locked; regardless of how many times an attacker might use an incorrect password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are non-Microsoft tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Countermeasure

Specify a new name in the **Accounts: Rename administrator account** policy setting to rename the Administrator account.

Potential impact

You must provide users who are authorized to use this account with the new account name. (The guidance for this policy setting assumes that the Administrator account was not disabled.)

Accounts: Rename guest account

This policy setting determines that the account name is associated with the SID for the Guest account.

Possible values:

- *User-defined text*
- Not Defined

Vulnerability

Because the Guest account name is well known, it provides a vector for a malicious user to access network resources and attempt to elevate privileges or install software that could be used for a later attack on your system.

Countermeasure

Specify a new name in the **Accounts: Rename guest account** policy setting to rename the Guest account. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Potential impact

There should be little impact because the Guest account is disabled by default.

Audit: Audit the access of global system objects

If you enable this policy setting, a default system access control list (SACL) is applied when the computer creates system objects such as mutexes, events, semaphores, and MS-DOS® devices. If you also enable the **Audit object access** audit setting, access to these system objects is audited.

Global system objects, also known as "base system objects" or "base named objects," are temporary kernel objects that have had names assigned to them by the application or system component that created them. These objects are most commonly used to synchronize multiple applications or multiple parts of a complex application. Because they have names, these objects

are global in scope, and therefore, they are visible to all processes on the computer. These objects all have a security descriptor, but typically they have a NULL SACL. If you enable this policy setting at startup, the kernel assigns a SACL to these objects when they are created.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

A globally visible named object, if incorrectly secured, could be acted upon by malicious software by using the name of the object. For instance, if a synchronization object such as a mutex had a poorly chosen discretionary access control list (DACL), malicious software could access that mutex by name and cause the program that created it to malfunction. However, the risk of such an occurrence is very low.

Countermeasure

Enable the **Audit: Audit the access of global system objects** policy setting.

Potential impact

If you enable the **Audit: Audit the access of global system objects** policy setting, a large number of security events could be generated, especially on busy domain controllers and application servers. Such an occurrence could cause servers to respond slowly and force the Security log to record numerous events of little significance. This policy setting can only be enabled or disabled, and there is no way to choose which events are recorded. Even organizations that have the resources to analyze events that are generated by this policy setting are not likely to have the source code or a description of what each named object is used for. Therefore, it is unlikely that most organizations would benefit by enabling this policy setting.

Audit: Audit the use of Backup and Restore privilege

This policy setting enables or disables auditing of the use of all user privileges, including Backup and Restore, when the **Audit privilege use** policy setting is in effect. If you enable both policy settings, an audit event is generated for every file that is backed up or restored.

If you enable this policy setting in conjunction with the **Audit privilege use** policy setting, any exercise of user rights is recorded in the Security log. If you disable this policy setting, actions by users who have Backup or Restore privileges are not audited, even if **Audit privilege use** is enabled.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

When the Backup and Restore function is used, it creates a copy of the file system that is identical to the target of the backup. Making regular Backup and Restore volumes is an important part of your incident response plan. However, a malicious user could use a legitimate backup copy to gain access to information or to impersonate a legitimate network resource to compromise your enterprise.

Countermeasure

Enable the **Audit: Audit the use of Backup and Restore privilege** policy setting. Alternatively, implement automatic log backup by configuring the **AutoBackupLogFiles** registry key. If you enable this option when the **Audit privilege use** policy setting is also enabled, an audit event is generated for every file that is backed up or restored. This information could help you to identify an account that was used to accidentally or maliciously restore data in an unauthorized manner.

For more information about configuring this key, see [article 100879](#) in the Microsoft Knowledge Base.

Potential impact

If you enable this policy setting, a large number of security events could be generated, which could cause servers to respond slowly and force the Security event log to record numerous events of little significance. If you increase the Security log size to reduce the chances of a system shutdown, an excessively large log file may affect system performance.

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

In Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, audit policies can be managed in a more precise way by using the audit policy subcategories. Setting audit policies at the category level overrides the subcategory audit policy feature. The registry value **SCENoApplyLegacyAuditPolicy**, allows audit policies to be managed by using subcategories without requiring a change to Group Policy settings. This registry value can be set to prevent the application of category-level audit policies from Group Policy and from the Local Security Policy administrative tool.

There are 40 auditing subcategories that provide more precise details about activities on a computer. The following table lists these subcategories.

| Category–Subcategory | Description | Default Setting |
|----------------------------------|---|---------------------|
| System–Security System Extension | Reports the loading of extension code such as authentication packages by the security subsystem. | No Auditing |
| System–System Integrity | Reports on violations of integrity of the security subsystem. | Success and Failure |
| System–IPsec Driver | Reports on the activities of the Internet Protocol security (IPsec) driver. | No Auditing |
| System–Other System Events | Reports on other system events. | Success and Failure |
| System–Security State Change | Reports changes in security state of the system, such as when the security subsystem starts and stops. | Success |
| Logon/Logoff–Logon | Reports when a user attempts to log on to the system. | Success |
| Logon/Logoff–Logoff | Reports when a user logs off from the system. | Success |
| Logon/Logoff–Account Lockout | Reserved for future use. | No Auditing |
| Logon/Logoff–IPsec Main Mode | Reports the results of Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations. | No Auditing |

| Category–Subcategory | Description | Default Setting |
|--|---|-----------------|
| Logon/Logoff–IPsec Quick Mode | Reports the results of IKE protocol and AuthIP during Quick Mode negotiations. | No Auditing |
| Logon/Logoff–IPsec Extended Mode | Reports the results of AuthIP during Extended Mode negotiations. | No Auditing |
| Logon/Logoff–Special Logon | Reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. | Success |
| Logon/Logoff–Network Policy Server | Reports events that are generated by RADIUS and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock. Auditing this setting results in a medium or high volume of records on servers running Network Policy Server. | No Auditing |
| Logon/Logoff–Other Logon/Logoff Events | Reports other logon/logoff-related events, such as disconnecting and reconnecting to Remote Desktop Services or Terminal Services sessions, using RunAs to run processes under a different account, and locking and unlocking a workstation. | No Auditing |
| Object Access–File System | Reports when file system objects are accessed. Only file system | No Auditing |

| Category–Subcategory | Description | Default Setting |
|--------------------------------------|--|-----------------|
| | objects with SACLs cause audit records to be generated, and only when they are accessed in a manner that matches their SACL. | |
| Object Access–Registry | Reports when registry objects are accessed. Only registry objects with SACLs cause audit records to be generated, and only when they are accessed in a manner that matches their SACL. | No Auditing |
| Object Access–Kernel Object | Reports when kernel objects such as processes and mutexes are accessed. Only kernel objects with SACLs cause audit records to be generated, and only when they are accessed in a manner that matches their SACL. Typically kernel objects are only given SACLs if the AuditBaseObjects or AuditBaseDirectories auditing options are enabled. | No Auditing |
| Object Access–SAM | Reports when SAM objects are accessed. | No Auditing |
| Object Access–Certification Services | Reports when Certification Services operations are performed. | No Auditing |
| Object Access–Application Generated | Reports when applications attempt to generate audit events by using the Windows auditing application programming interfaces (APIs). | No Auditing |

| Category–Subcategory | Description | Default Setting |
|--|--|-----------------|
| Object Access–Handle Manipulation | Reports when a handle to an object is opened or closed. Only objects with SACLs cause these events to be generated and only if the attempted handle operation matches the SACL. Handle Manipulation events are only generated for object types where the corresponding Object Access subcategory is enabled; for example, File System or Registry. | No Auditing |
| Object Access–File Share | Reports when a file share is accessed. | No Auditing |
| Object Access–Filtering Platform Packet Drop | Reports when packets are dropped by the Windows Filtering Platform (WFP). These are high-volume events, so log file size should be monitored closely when auditing these events. | No Auditing |
| Object Access–Filtering Platform Connection | Reports when connections are allowed or blocked by WFP. These are high-volume events, so log file size should be monitored closely when auditing these events. | No Auditing |
| Object Access–Other Object Access Events | Reports other object access-related events such as Task Scheduler jobs and COM+ objects. | No Auditing |
| Detailed Tracking–Process Termination | Reports when a process terminates. | No Auditing |

| Category–Subcategory | Description | Default Setting |
|--|--|-----------------|
| Detailed Tracking– DPAPI Activity | Reports encrypted or decrypted calls into the data protections application programming interface (DPAPI). DPAPI protects secret information such as stored password and key information. | No Auditing |
| Detailed Tracking–RPC Events | Reports remote procedure call (RPC) connection events. | No Auditing |
| Detailed Tracking–Process Creation | Reports the creation of a process and the name of the program or user that created it. | No Auditing |
| Policy Change–Audit Policy Change | Reports changes in the audit policy including SACL changes. | Success |
| Policy Change–Authentication Policy Change | Reports changes in the authentication policy. | Success |
| Policy Change–Authorization Policy Change | Reports changes in the authorization policy including permissions (DACL) changes. | No Auditing |
| Policy Change–MPSSVC Rule-Level Policy Change | Reports changes in policy rules that are used by the Microsoft Protection Service (MPSSVC.exe). This service is used by Windows Firewall. | No Auditing |
| Policy Change–Filtering Platform Policy Change | Reports the addition and removal of objects from WFP, including startup filters. These are high-volume events, so log file size should be monitored closely when auditing these events. | No Auditing |

| Category–Subcategory | Description | Default Setting |
|---|--|-----------------|
| Policy Change–Other Policy Change Events | Reports other types of security policy changes, such as configuration of the Trusted Platform Module (TPM) or cryptographic providers. | No Auditing |
| Account Management–User Account Management | Reports each event of user account management, such as when a user account is created, changed, deleted, renamed, disabled, or enabled, or when a password is set or changed. | Success |
| User Account Management–Computer Account Management | Reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. | No Auditing |
| User Account Management–Security Group Management | Reports each event of security group management, such as when a security group is created, changed, or deleted, or when a member is added to or removed from a security group. | Success |
| User Account Management–Distribution Group Management | Reports each event of distribution group management, such as when a distribution group is created, changed, or deleted, or when a member is added to or removed from a distribution group. | No Auditing |
| User Account Management–Application Group Management | Reports each event of application group management on a computer, such as when an | No Auditing |

| Category–Subcategory | Description | Default Setting |
|---|---|-----------------|
| | application group is created, changed, or deleted, or when a member is added to or removed from an application group. | |
| User Account Management–Other Account Management Events | Reports other account management events. | No Auditing |
| DS Access–Directory Service Changes | Reports changes to objects in Active Directory Domain Services (AD DS). Directory Service Changes auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause an audit to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause an audit to be generated due to settings to the object class in the schema. | No Auditing |
| DS Access–Directory Service Replication | Reports when replication between two domain controllers begins and ends. | No Auditing |
| DS Access–Detailed Directory Service Replication | Reports details about the information that is replicating between domain controllers. These are high-volume events, so log file size should be monitored closely when auditing these events. | No Auditing |

| Category–Subcategory | Description | Default Setting |
|--|---|-----------------|
| DS Access–Directory Service Access | Reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. | No Auditing |
| Account Logon–Kerberos Ticket Events | Reports the results of validation tests on Kerberos protocol tickets that are submitted for a user account logon request. | No Auditing |
| Account Logon–Other Account Logon Events | Reports the events that occur in response to credentials that are submitted for a user account logon request. These events do not relate to credential validation or Kerberos protocol tickets, because those events have separate subcategories that can be audited). | No Auditing |
| Account Logon–Credential Validation | Reports the results of validation tests on credentials that are submitted for a user account logon request. | No Auditing |
| Privilege Use–Sensitive Privilege Use | <p>Reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:</p> <ul style="list-style-type: none"> • Act as part of the operating system • Back up files and directories • Create a token object | No Auditing |

| Category–Subcategory | Description | Default Setting |
|---|--|-----------------|
| | <ul style="list-style-type: none"> • Debug programs • Enable computer and user accounts to be trusted for delegation • Generate security audits • Impersonate a client after authentication • Load and unload device drivers • Manage auditing and security log • Modify firmware environment values • Replace a process-level token • Restore files and directories • Take ownership of files or other objects <p>Auditing this subcategory creates a high volume of events, so log file size should be monitored closely when auditing these events.</p> | |
| Privilege Use–Non Sensitive Privilege Use | <p>Reports when a user account or service uses a nonsensitive privilege. The following list identifies the user rights that are considered nonsensitive privileges:</p> <ul style="list-style-type: none"> • Access Credential Manager as a trusted caller • Access this computer from | No Auditing |

| Category–Subcategory | Description | Default Setting |
|----------------------|--|-----------------|
| | <p>the network</p> <ul style="list-style-type: none"> • Add workstations to domain • Adjust memory quotas for a process • Allow log on locally • Allow log on through Terminal Services or Remote Desktop Services • Bypass traverse checking • Change the system time • Create a pagefile • Create global objects • Create permanent shared objects • Create symbolic links • Deny access this computer from the network • Deny log on as a batch job • Deny log on as a service • Deny log on locally • Deny log on through Terminal Services or Remote Desktop Services • Force shutdown from a remote system • Increase a process working set • Increase scheduling priority | |

| Category–Subcategory | Description | Default Setting |
|-----------------------------------|---|-----------------|
| | <ul style="list-style-type: none"> • Lock pages in memory • Log on as a batch job • Log on as a service • Modify an object label • Perform volume maintenance tasks • Profile single process • Profile system performance • Remove computer from docking station • Shut down the system • Synchronize directory service data <p>Auditing this subcategory creates a high volume of events, so log file size should be monitored closely when auditing these events.</p> | |
| Privilege Use–Other Privilege Use | This category is reserved for future use. No events are currently mapped to this subcategory. | No Auditing |

Vulnerability

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events, and the key information that needed to be audited was difficult to find.

Countermeasure

Enable audit policy subcategories as needed to track specific events.

Potential impacts

The individual audit policy subcategories are now exposed in the Group Policy tools interface. Administrators can deploy a custom audit policy that applies detailed security auditing settings. If you attempt to modify an auditing setting by using Group Policy after you enable this setting, the Group Policy auditing setting is ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable the **SCENoApplyLegacyAuditPolicy** key.



Important

Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable Success or Failure auditing for all of the Privilege Use subcategories, the high volume of audit events that are generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

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

This policy setting enables or disables shutting down the computer if it is unable to log security events. The Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certifications require that the computer prevent the occurrence of auditable events if the audit system is unable to log them. The way that Windows meets this requirement is to halt the computer and display a Stop error if the audit system fails. If you enable this policy setting, the computer stops if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the Security log is full, and its specified retention method is **Do Not Overwrite Events** or **Overwrite Events by Days**.

When this policy setting is enabled, the following Stop error displays if the security log is full and an existing entry cannot be overwritten:

STOP: C0000244 {Audit Failed}

An attempt to generate a security audit failed.

To recover, an administrator must log on, archive the log (optional), clear the log, and disable this option to allow the computer to be restarted. At that point, it may be necessary to manually clear the Security log before you can configure this policy setting to Enabled.

Possible values:

- Enabled
- Disabled

- Not Defined

Vulnerability

If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Countermeasure

Enable the **Audit: Shut down system immediately if unable to log security audits** policy setting to ensure that security auditing information is captured for review.

Potential impact

If you enable this policy setting, the administrative burden can be significant, especially if you also configure the **Retention method for the Security log** to **Do not overwrite events** (clear log manually). This configuration causes a repudiation threat (for example, a backup operator could deny that they backed up or restored data) to become a denial-of-service (DoS) vulnerability because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is abrupt, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system maintains its integrity when this type of computer shutdown occurs, there is no guarantee that every data file for every application will still be in a usable form when the computer restarts.

DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)

This policy setting allows administrators to define additional computer-wide access controls that govern access to all Distributed Component Object Model (DCOM)–based applications on a computer. These controls restrict call, activation, or launch requests on the computer. A simple way to think about these access controls is that an additional access check call is performed against a computer-wide access control list (ACL) on each call, activation, or launch of any COM server on the computer. If the access check fails, the call, activation, or launch request is denied. (This check is in addition to any access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to access any COM server on the computer. This policy setting controls access permissions to cover call rights.

These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through the `CoInitializeSecurity` function or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific server.

These ACLs also provide a centralized location for an administrator to set a general authorization policy that applies to all COM servers on the computer.

This policy setting allows you to specify an ACL in two ways. You can type the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. We recommend that you use the built-in user interface to specify the ACL content that you want to apply with this setting.

The default ACL settings vary, depending on the version of the Windows operating system you are running.

Vulnerability

Many COM applications include some security-specific code (for example, to call `CoInitializeSecurity`), but they use weak settings that often allow unauthenticated access to the process. In earlier versions of Windows, administrators could not override these settings to force stronger security without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls.

Also, COM infrastructure includes the Remote Procedure Call System Service (RPCSS), a system service that runs during and after computer startup. This service manages activation of COM objects and the running object table, and it provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote access, these interfaces can be called by anyone, including unauthenticated users. As a result, RPCSS can be attacked by malicious users who use remote, unauthenticated computers.

Countermeasure

To protect individual COM-based applications or services, set the **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** policy setting to an appropriate computer-wide ACL.

Potential impact

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications or components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific call permissions that ACL assigns correct permissions to appropriate users. If the permissions are incorrect, you must change your application-specific permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)

This policy setting is similar to the **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** policy setting in that it allows administrators to define additional computer-wide access controls that govern access to all DCOM-based applications on a computer. However, the ACLs that are specified in this policy setting control local and remote COM launch requests (not access requests) on the computer. A simple way to think about this access control is that an additional access check call is performed against a computer-wide ACL on each launch of any COM server on the computer. If the access check fails, the call, activation, or launch request is denied. (This check is in addition to any access check that is run against the server-specific ACLs.) In effect, it provides a minimum authorization standard that must be passed to launch any COM server on the computer. The **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)** policy setting differs in that it provides a minimum access check that is applied to attempts to access an already launched COM server.

These computer-wide ACLs provide a way to override weak security settings that are specified by a specific application through `CoInitializeSecurity` or application-specific security settings. They provide a minimum security standard that must be passed, regardless of the settings of the specific COM server. These ACLs provide a centralized location for an administrator to set a general authorization policy that applies to all COM servers on the computer.

The **DCOM: Machine Launch Restrictions in the Security Descriptor Definition Language (SDDL)** policy setting allows you to specify an ACL in two ways. You can type the security descriptor in SDDL, or you can choose users and groups and grant or deny them Local Access and Remote Access permissions. We recommend that you use the built-in user interface to specify the ACL content that you want to apply with this policy setting.

The default ACL settings vary, depending on the version of the Windows operating system you are running.

Vulnerability

Many COM applications include some security-specific code (for example, to call `CoInitializeSecurity`), but they use weak settings that often allow unauthenticated access to the process. In earlier versions of Windows, administrators could not override these settings to force stronger security without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls.

COM infrastructure includes the RPCSS, a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table, and it provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote component

activation, these interfaces can be called by anyone, including unauthenticated users. As a result, RPCSS can be attacked by malicious users by using remote, unauthenticated computers.

Countermeasure

To protect individual COM-based applications or services, set this policy setting to an appropriate computer-wide ACL.

Potential impact

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications or components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific launch permissions ACL assigns activation permission to appropriate users. If it does not, you must change your application-specific launch permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

Devices: Allow undock without having to log on

This policy setting enables or disables the ability of a user to remove a portable computer from a docking station without logging on. If you enable this policy setting, users can press a docked portable computer's physical eject button to safely undock the computer. If you disable this policy setting, the user must log on to receive permission to undock the computer. Only users who have the **Remove Computer from Docking Station** privilege can obtain this permission.



Note

Disabling this policy setting only reduces theft risk for portable computers that cannot be mechanically undocked. Computers that can be mechanically undocked can be physically removed by the user whether or not they use the Windows undocking functionality.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

If this policy setting is enabled, anyone with physical access to portable computers in docking stations could remove them and possibly tamper with them.

Countermeasure

Disable the **Devices: Allow undock without having to log on** policy setting.

Potential impact

Users who have docked their computers must log on to the local console before they can undock their computers. For computers that do not have docking stations, this policy setting has no impact.

Devices: Allowed to format and eject removable media

This policy setting determines who is allowed to format and eject removable media.

Possible values:

- Administrators
- Administrators and Power Users
- Administrators and Interactive Users
- Not Defined

Vulnerability

Users could move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices eject media when a mechanical button is pressed diminishes the advantage of this policy setting.

Countermeasure

Configure the **Devices: Allowed to format and eject removable media** policy setting to **Administrators**.

Potential impact

Only administrators can format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they must be informed of the change in policy.

Devices: Prevent users from installing printer drivers

This policy setting determines who is allowed to install a printer driver when adding a network printer. For a computer to print to a network printer, that network printer driver must be installed on the local computer. If you enable this policy setting, only members of the Administrators, Power Users, or Server Operators groups are allowed to install a printer driver when they add a network printer. If you disable this policy setting, all users can install printer

drivers when they add a network printer. This policy setting prevents typical users from downloading and installing untrusted printer drivers.



Note

This policy setting has no impact if an administrator has configured a trusted path to download drivers. If you use trusted paths, the print subsystem attempts to use the trusted path to download the driver. If the trusted path download succeeds, the driver is installed on behalf of any user. If the trusted path download fails, the driver is not installed and the network printer is not added.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only administrators, not users, to do so on servers because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver.

Countermeasure

Enable the **Devices: Prevent users from installing printer drivers** policy setting.

Potential impact

Only members of the Administrators, Power Users, or Server Operators groups can install printers on the servers. If this policy setting is enabled but the driver for a network printer already exists on the local computer, users can still add the network printer.

Devices: Restrict CD-ROM access to locally logged-on user only

This policy setting determines whether a CD is accessible to local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable CDs. If this policy setting is enabled and no one is logged on interactively, the CD can be accessed over the network.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

A remote user could potentially access a mounted CD that contains sensitive information. This risk is small because CD drives are not automatically made available as shared drives; administrators must deliberately choose to share the drive. However, administrators can deny network users the ability to view data or run applications from removable media on the server.

Countermeasure

Enable the **Devices: Restrict CD-ROM drive access to locally logged-on user only** policy setting.

Potential impact

Users who connect to the server over the network cannot use any CD drives that are installed on the server when someone is logged on to the local console of the server. System tools that require access to the CD drive will fail. For example, the Volume Shadow Copy service attempts to access all CD and floppy disk drives that are present on the computer when it initializes, and if the service cannot access one of these drives, it fails. This condition causes the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies also fail. This policy setting would not be suitable for a computer that serves as a CD media player for network users.

Devices: Restrict floppy access to locally logged-on user only

This policy setting determines whether removable floppy disks are accessible to local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable floppy disks. If this policy setting is enabled and no one is logged on interactively, a floppy disk can be accessed over the network.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

A remote user could potentially access a mounted floppy disk that contains sensitive information. This risk is small because floppy disk drives are not automatically shared;

administrators must deliberately choose to share the drive. However, administrators can deny network users the ability to view data or run applications from removable media on the server.

Countermeasure

Enable the **Devices: Restrict floppy access to locally logged-on user only** policy setting.

Potential impact

Users who connect to the server over the network cannot use any floppy disk drives that are installed on the server when someone is logged on to the local console of the server. System tools that require access to floppy disk drives fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy disk drives that are present on the computer when it initializes, and if the service cannot access one of these drives, it fails. This condition causes the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies also fail.

Domain controller: Allow server operators to schedule tasks

This policy setting determines whether server operators are allowed to submit jobs by means of the AT command. If you enable this policy setting, jobs that are created by server operators by means of the AT command run in the context of the account that runs the Task Scheduler service. By default, that is the Local System account. If you enable this policy setting, server operators could perform tasks that the Local System account can do, but that they typically cannot do, such as add their account to the local Administrators group.



Note

This security option setting affects only the AT schedule tool. It does not affect the Task Scheduler tool.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Tasks that run under the context of the Local System account can affect resources that are at a higher privilege level than the user account that scheduled the task.

Countermeasure

Disable the **Domain controller: Allow server operators to schedule tasks** policy setting.

Potential impact

The impact should be small for most organizations. Users (including those in the Server Operators group) can still create jobs by means of the Task Scheduler snap-in. However, those jobs run in the context of the account with which the user authenticates when setting up the job.

Domain controller: LDAP server signing requirements

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing.

Possible values:

- None
- Require signature
- Not Defined

Vulnerability

Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. You could also implement Internet Protocol security (IPsec) authentication header mode (AH tunnel mode), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Countermeasure

Configure the **Domain controller: LDAP server signing requirements** policy setting to **Require signature**.

Potential impact

Clients that do not support LDAP signing cannot run LDAP queries against the domain controllers.

Domain controller: Refuse machine account password changes

This policy setting enables or disables a domain controller from accepting password change requests for computer accounts.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

If you enable this policy setting on all domain controllers in a domain, domain members cannot change their computer account passwords, and those passwords are more susceptible to attack.

Countermeasure

Disable the **Domain controller: Refuse machine account password changes** policy setting.

Potential impact

None. This is the default configuration.

Domain member: Digitally encrypt or sign secure channel data (multiple related settings)

The following policy settings determine whether a secure channel can be established with a domain controller that cannot sign or encrypt secure channel traffic:

- **Domain member: Digitally encrypt or sign secure channel data (always)**
- **Domain member: Digitally encrypt secure channel data (when possible)**
- **Domain member: Digitally sign secure channel data (when possible)**

If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** policy setting, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data.

To protect authentication traffic from man-in-the-middle, replay, and other types of network attacks, computers that are running the Windows operating system create a communication channel through NetLogon called "secure channels." These channels authenticate computer accounts, and they also authenticate user accounts when a remote user connects to a network resource and the user account exists in a trusted domain. This authentication is called "pass-through authentication," and it allows a computer that has joined a domain to have access to the user account database in its domain and in any trusted domains.



Note

To enable the **Domain member: Digitally encrypt or sign secure channel data (always)** policy setting on a member workstation or server, all domain controllers in the domain that the member belongs to must sign or encrypt all secure channel data. This

requirement means that all such domain controllers cannot run an operating system earlier than Microsoft Windows NT® 4.0 with Service Pack 6a (SP6a).

If you enable the **Domain member: Digitally encrypt or sign secure channel data (always)** policy setting, the **Domain member: Digitally sign secure channel data (when possible)** policy setting is automatically enabled.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted, but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

Countermeasure

Select one of the following settings as appropriate for your environment to configure the computers in your domain to encrypt or sign secure channel data:

- **Domain member: Digitally encrypt or sign secure channel data (always)**
- **Domain member: Digitally encrypt secure channel data (when possible)**
- **Domain member: Digitally sign secure channel data (when possible)**

Potential impact

Using digital encryption and signing the secure channel is a good idea where they are supported. The secure channel protects domain credentials as they are sent to the domain controller. However, operating systems earlier than Windows NT 4.0 with SP6a do not support digital encryption and signing the secure channel. Microsoft Windows® 98 Second Edition client computers do not support it unless they have the Active Directory Client Extension installed. Therefore, you cannot enable the **Domain member: Digitally encrypt or sign secure channel**

data (always) policy setting on domain controllers that support Windows 98 client computers as members of the domain. Potential impacts can include the following:

- The ability to create or delete trust relationships is disabled with clients running versions of Windows earlier than Windows NT 4.0 with SP6a.
- Logons are disabled from client computers running versions of Windows earlier than Windows NT 4.0 with SP6a.
- The ability to authenticate other domains' users is disabled from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain.

You can enable this policy setting after you eliminate all client computers running Windows 98 or Windows 95 from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the policy settings, **Domain member: Digitally encrypt secure channel data (when possible)** and **Domain member: Digitally encrypt sign channel data (when possible)**, on all computers in the domain that support the above settings and client computers running versions of Windows earlier than Windows NT 4.0 with SP6a. Applications that run on these versions of Windows are not affected.

Domain member: Disable machine account password changes

This policy setting enables or disables blocking the periodic changing of computer account passwords. If you enable this policy setting, the domain member cannot change its computer account password. If you disable this policy setting, the domain member is allowed to change its computer account password as specified by the **Domain Member: Maximum age for computer account password** policy setting, which is every 30 days by default.



Caution

Do not enable the **Domain member: Disable machine account password changes** policy setting. Computer account passwords are used to establish secure channel communications between members and domain controllers, and within the domain, they establish a secure channel between the domain controllers. After such communications are established, the secure channel transmits sensitive information that is needed to make authentication and authorization decisions.

Do not use the **Domain member: Disable machine account password changes** policy setting in an attempt to support dual-boot scenarios that use the same computer account. If you want to support such a scenario for two installations that are joined to the same domain, use different computer names for the two installations.

This policy setting was added to Windows to make it easier for organizations that store prebuilt computers that are put into production months later. It eliminates the need for those computers to rejoin the domain. This policy setting is also sometimes used with imaged computers or those with hardware- or software-level change prevention. Correct imaging procedures make the use of this policy unnecessary for imaged computers.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

The default requirement for domain accounts is to change the password every 30 days. If you disable this policy setting, computers retain the same passwords as their computer accounts. Computers that cannot automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

Countermeasure

Verify that the **Domain member: Disable machine account password changes** policy setting is configured to **Disabled**.

Potential impact

None. This is the default configuration.

Domain member: Maximum machine account password age

This policy setting determines the maximum allowable age for a computer account password.

Possible values:

- User-defined number of days between 0 and 999
- Not Defined

Vulnerability

In Active Directory domains, each computer and every user has an account and password. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker has more time to undertake a brute force attack to guess the password of one or more computer accounts.

Countermeasure

Configure the **Domain member: Maximum machine account password age** policy setting to 30 days.

Potential impact

None. This is the default configuration.

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

This policy setting determines whether a secure channel can be established with a domain controller that cannot encrypt secure channel traffic with a strong, 128-bit session key. If you enable this policy setting, you can establish a secure channel only with a domain controller that can encrypt secure channel data with a strong key. If you disable this policy setting, 64-bit session keys are allowed.



Note

To enable this policy setting on a member workstation or server, all domain controllers in the domain to which the member belongs must be able to encrypt secure channel data with a strong, 128-bit key.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdrop. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or it can be redirected.)

Countermeasure

Enable the **Domain member: Require strong (Windows 2000 or later) session key** policy setting.

If you enable this policy setting, all outgoing secure channel traffic requires a strong encryption key. If you disable this policy setting, the key strength is negotiated. You should enable this policy setting only if the domain controllers in all trusted domains support strong keys. By default, this policy setting is disabled.

Potential impact

Computers that have this policy setting enabled cannot join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT domains may not work properly. Computers that do not support this policy setting cannot join domains in which the domain controllers have this policy setting enabled.

Interactive logon: Display user information when the session is locked

When a Windows session is locked (which means the user at the computer pressed CTRL+ALT+DEL and the secure desktop is now displayed), user information is displayed. By default, this information is in the form of **<user name> is logged on**. The user display name is the user's **Full name** as set on the **Properties** page for that user. These settings do not apply to the display of the logon tiles, which are displayed on the desktop after using the Switch User feature. The information that is displayed can be changed to meet your security requirements by using the following possible values.

Possible values:

- User display name, domain and user names
- User display name only
- Do not display user information
- Not Defined

Vulnerability

When a computer displays the secure desktop in an unsecured area, certain user information can be readily available to anyone looking at the monitor, either physically or through a remote connection. The displayed user information could include the domain user account name or the full name of the user who locked the session or who had logged on last.

Countermeasure

Enabling this policy setting allows the operating system to hide certain user information from being displayed on the secure desktop (after the computer has been started or when the session has been locked by using CTRL+ALT+DEL). However, user information is displayed if the Switch User feature is used so that the logon tiles are displayed for each logged on user.

You might consider enabling the **Interactive logon: Do not display last user name** policy setting, which will prevent Windows from displaying the logon name and logon tile of the last user to log on.

Potential impact

If you do not enable this policy setting, the effect will be the same as enabling the policy setting and selecting the **User display name, domain and user names** option.

If the policy setting is enabled and set to **Do not display user information**, the user name of the user who is currently logged on is not displayed on the secure desktop when the computer is locked. However, if the **Interactive logon: Do not display last user name** policy setting is not enabled, the user name of the last user who logged on is still displayed. Depending on how the logon tiles are configured, they could provide visual clues as to who is logged on. In addition, if the **Interactive logon: Do not display last user name** policy setting is not enabled, then the **Switch user** feature will show user information.

Interactive logon: Do not display last user name

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or portable computers in your organization.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

An attacker with access to the console (for example, someone with physical access or someone who can connect to the server through Remote Desktop Services or Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute force attack to try to log on.

Countermeasure

Enable the **Interactive logon: Do not display last user name** policy setting.

Potential impact

Users must always type their user names when they log on to the servers.

Interactive logon: Do not require CTRL+ALT+DEL

The CTRL+ALT+DEL key combination establishes a trusted path to the operating system for users to type their user name and password. When this policy setting is enabled, users are not

required to use this key combination to log on to the network. However, this configuration poses a security risk because it provides an opportunity for users to log on with weaker logon credentials. When this policy is disabled, users must press CTRL+ALT+DEL before they log on to Windows, or they must use a smart card, a tamper-proof device that stores security information, to log on.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

This policy setting makes it easier for users with certain types of physical impairments to log on to computers that run the Windows operating system. However, if users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path.

If this policy setting is enabled, an attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Countermeasure

Disable the **Interactive logon: Do not require CTRL+ALT+DEL** policy setting.

Potential impact

Unless they use a smart card to log on, users must simultaneously press CTRL+ALT+DEL before the logon dialog box is displayed.

Interactive logon: Message text for users attempting to log on and Message title for users attempting to log on

There are two separate policy settings that relate to logon displays:

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

The first policy setting specifies a text message that displays to users when they log on, and the second policy setting specifies a title for the title bar of the text message window. Many

organizations use this text for legal purposes; for example, to warn users about the ramifications of misuse of company information, or to warn them that their actions may be audited.

Possible values:

- User-defined text
- Not Defined

Vulnerability

Users often do not understand the importance of security practices. However, the display of a warning message before logon may help prevent an attack by warning malicious or uninformed users about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Countermeasure

Configure the **Interactive logon: Message text for users attempting to log on** and **Interactive logon: Message title for users attempting to log on** policy settings to an appropriate value for your organization.



Note

Any warning message that displays should be approved by your organization's legal and human resources representatives.

Potential impact

Users see a message in a dialog box before they can log on to the server console.



Note

Client computers running Windows 2000 cannot interpret and display messages that exceed 512 characters in length and contain carriage-return, line-feed sequences. You must use a computer that is running Windows 2000 to create a logon message policy that applies to other computers running Windows 2000. If you create a logon message policy on a computer that is running Windows 2000, and you discover that it does not display properly on other computers running Windows 2000, you must first change the policy setting to **Not Defined**, and then reconfigure the setting by using a computer running Windows 2000. If you do not do this, the changes do not take effect properly.

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

This policy setting determines the number of individual users who can log on to a Windows domain by using cached account information. Logon information for domain accounts can be cached locally so that if a domain controller cannot be contacted on subsequent logons, a user can still log on. This policy setting determines the number of individual users whose logon information is cached locally.

If a domain controller is unavailable and a user's logon information is cached, the user is prompted with the following message:

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available.

If a domain controller is unavailable and a user's logon information is not cached, the user is prompted with this message:

The system cannot log you on now because the domain <DOMAIN_NAME> is not available.

Possible values:

- User-defined number between 0 and 50
- Not Defined

Vulnerability

The number that is assigned to this policy setting indicates the number of users whose logon information is cached locally by the servers. If the number is set to 10, the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session.

Users who access the server console have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to attempt to determine user passwords.

To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Countermeasure

Configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy setting to **0**, which disables the local caching of logon

information. Additional countermeasures include enforcement of strong password policies and physically secure locations for the computers.

Potential impact

Users cannot log on to any computers if there is no domain controller available to authenticate them. Organizations can configure this value to **2** for end-user computers, especially for mobile users. A configuration value of **2** means that the user's logon information is still in the cache, even if a member of the IT department has recently logged on to the computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Interactive logon: Prompt user to change password before expiration

This policy setting determines how many days in advance that users are warned their password is about to expire. With this advanced warning, the user has time to construct a sufficiently strong password.

Possible values:

- User-defined number of days between 1 and 999
- Not Defined

Vulnerability

If user passwords are configured to expire periodically in your organization, users need to be warned when this is about to happen, or they may be locked out of the computer inadvertently when their passwords expire. This condition could lead to confusion for users who access the network locally, or it could make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Countermeasure

Configure the **Interactive logon: Prompt user to change password before expiration** policy setting to 14 days.

Potential impact

Users see a dialog-box prompt to change their password each time that they log on to the domain when their password is configured to expire in 14 or fewer days.

Interactive logon: Require Domain Controller authentication to unlock workstation

This policy setting enables or disables the requirement for a domain account to contact a domain controller to unlock a computer. Logon information is required to unlock a locked computer. If you enable this setting, a domain controller must authenticate the domain account

that is being used to unlock the computer. If you disable this setting, logon-information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configured the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy setting to a value that is greater than zero, the user's cached credentials are used to unlock the computer.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

By default, the computer caches (in memory) the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account—such as user rights assignments, account lockout, or the account being disabled—are not considered or applied after the account is authenticated. User privileges are not updated, and (more important) disabled accounts are still able to unlock the console of the computer.

Countermeasure

Configure the **Interactive logon: Require Domain Controller authentication to unlock workstation** policy setting to **Enabled** and configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy setting to **0**.

Potential impact

When the console on a computer is locked by a user or automatically by a screen-saver timeout, the console can be unlocked only if the user can authenticate to the domain controller. If no domain controller is available, users cannot unlock their workstations. If you configure the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy setting to **0**, users whose domain controllers are unavailable (such as mobile or remote users) cannot log on.

Interactive logon: Require smart card

This policy setting enables or disables the requirement for users to log on to a computer with a smart card. The use of smart cards instead of passwords for authentication dramatically increases security because current technology makes it extremely difficult for an attacker to impersonate another user. Smart cards that require personal identification numbers (PINs)

provide two-factor authentication: the user must possess the smart card and know its PIN. Attackers who capture the authentication traffic between the user's computer and the domain controller find it extremely difficult to decrypt the traffic, and if they do, the next time that the user logs on to the network a new session key is generated to encrypt traffic between the user and the domain controller.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

It can be difficult to make users choose strong passwords, and even strong passwords are vulnerable to brute force attacks if an attacker has sufficient time and computing resources.

Countermeasure

For users with access to computers that contain sensitive data, issue smart cards and configure the **Interactive logon: Require smart card** policy setting to **Enabled**.

Potential impact

All users of a computer with this policy setting enabled must use smart cards to log on to the local computer, which means that the organization must have a reliable public key infrastructure (PKI) in addition to smart cards and smart card readers for these users. These requirements are significant challenges because expertise and resources are required to plan for and deploy these technologies. For more information about deploying smart cards, see [Windows Vista Smart Card Infrastructure](#).

Interactive logon: Smart card removal behavior

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

Possible values:

- No Action
- Lock Workstation
- Force Logoff
- Disconnect if a remote Terminal Services session

- Not Defined

By default, this policy setting is Not Defined, which is equivalent to the No Action setting.

**Note**

The Smart Card Removal Policy service must be started for this policy setting to work.

Vulnerability

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources by using those credentials.

Countermeasure

Configure the **Interactive logon: Smart card removal behavior** policy setting to **Lock Workstation**.

If you select **Lock Workstation** for this policy setting, the workstation locks when the smart card is removed. Users can leave the area, take their smart card with them, and still maintain a protected session. This behavior is similar to the setting that requires users to log on when resuming work on the computer after the screen saver has started.

If you select **Force Logoff** for this policy setting, the user is automatically logged off when the smart card is removed. This policy setting is useful when a computer is deployed as a public access point, such as a kiosk or other type of shared computer.

Potential impact

If you select **Force Logoff**, users must reinsert their smart cards and reenter their PINs when they return to their workstations.

Microsoft network client and server: Digitally sign communications (four related settings)

There are four separate policy settings that relate to packet-signing requirements for Server Message Block (SMB) communications:

- **Microsoft Network Client: Digitally Sign Communications (Always)**
- **Microsoft Network Server: Digitally Sign Communications (Always)**
- **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)**
- **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)**

Implementation of digital signatures in high-security networks helps prevent the impersonation of clients and servers, known as "session hijacking."

Possible values for each of these policy settings are:

- Enabled
- Disabled
- Not Defined

Vulnerability

Session hijacking uses tools that allow attackers who have access to the same network as the client computer or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned Server Message Block (SMB) packets and then modify the traffic and forward it so that the server might perform objectionable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource-sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission does not take place.

Countermeasure

Configure the policy settings as follows:

- Disable **Microsoft Network Client: Digitally Sign Communications (Always)**.
- Disable **Microsoft Network Server: Digitally Sign Communications (Always)**.
- Enable **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)**.
- Enable **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)**.

In highly secure environments, we recommend that you configure all of these policy settings to **Enabled**. However, that configuration may cause slower performance on client computers and prevent communications with earlier SMB applications and operating systems.



Note

An alternative countermeasure that could protect all network traffic is to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing.

Potential impact

The Windows implementation of the SMB file and print-sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client computer and the server.

Implementing SMB signing may negatively affect performance because each packet must be signed and verified. If these policy settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server, performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems cannot connect. However, if you completely disable all SMB signing, computers are vulnerable to session-hijacking attacks.

Microsoft network client: Send unencrypted password to third-party SMB servers

This policy setting enables or disables sending plaintext passwords by the SMB redirector to non-Microsoft SMB servers that do not support password encryption during authentication.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

If you enable this policy setting, the server can transmit plaintext passwords across the network to other computers that offer SMB services. These other computers might not use any of the SMB security mechanisms.

Countermeasure

Disable the **Microsoft network client: Send unencrypted password to connect to third-party SMB servers** policy setting.

Potential impact

Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Microsoft Windows 95 may not be able to communicate with the servers in your organization by means of the SMB protocol.

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

This policy setting determines the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. The session automatically reestablishes when activity in client computer resumes. A value of 0 disconnects an idle session as quickly as possible. The maximum value is 99999, which is 208 days which in effect disables the policy setting.

Possible values:

- User-defined period of time in minutes
- Not Defined

By default, this policy is not defined, which means that the system allows 15 minutes of idle time for servers and an undefined time for workstations.

Vulnerability

Each SMB session consumes server resources, and numerous null sessions slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Countermeasure

The default behavior on a server mitigates this threat by design.

Potential impact

There is little impact because SMB sessions are reestablished automatically if the client resumes activity.

Microsoft network server: Disconnect clients when logon hours expire

This policy setting enables or disables the forced disconnection of users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service are forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions are maintained after the client's logon hours expire. If you enable this policy setting, you should also enable **Network security: Force logoff when logon hours expire**.

Possible values:

- Enabled
- Disabled

- Not Defined

By default, this policy setting is enabled.

Vulnerability

If your organization configures logon hours for users, it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually continue to use those resources with sessions that were established during allowed hours.

Countermeasure

Enable the **Microsoft network server: Disconnect clients when logon hours expire** policy setting.

Potential impact

If logon hours are not used in your organization, this policy setting has no impact. If logon hours are used, existing user sessions are forcibly terminated when their logon hours expire.

Microsoft network server: Server SPN target name validation level

This policy setting controls the level of validation that a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session by using the Server Message Block (SMB) protocol.

Possible values:

- Off
- Accept if provided by client
- Required from client

By default, this policy setting is not defined.

Vulnerability

This policy setting controls the level of validation that a computer with shared folders or printers (the server) performs on the SPN that is provided by the client computer when it establishes a session by using the SMB protocol. The level of validation can help prevent a class of attacks against SMB servers (referred to as SMB relay attacks). This policy setting will affect SMB1 and SMB2.

Countermeasure

If you set **Accept if provided by client**, the SMB server will accept and validate the SPN that is provided by the SMB client and allow a session to be established if it matches the SMB server's

list of SPNs. If the SPN does not match, the session request for that SMB client computer will be denied.

If you set **Required from client**, the SMB client computer must send an SPN name in session setup, and the SPN name that is provided must match the SMB server that is being requested to establish a connection. If no SPN is provided by the client computer, or the SPN that is provided does not match, the session is denied.

Potential impact

All Windows operating systems support a client SMB component and a server SMB component. This policy setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Because the SMB protocol is widely deployed, setting the options to **Accept if provided by client** or **Required from client** will prevent some clients from successfully authenticating to some servers in your environment.

Network access: Allow anonymous SID/Name translation

This policy setting enables or disables the ability of an anonymous user to request SID attributes for another user.

Possible values:

- Enabled
- Disabled
- Not Defined

By default, this policy setting is enabled on domain controllers, and it is disabled on workstations and member servers.

Vulnerability

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password-guessing attack.

Countermeasure

Disable the **Network access: Allow anonymous SID/Name translation** policy setting.

Potential impact

Disabled is the default configuration for this policy setting on member computers; therefore, it has no impact on them. The default configuration for domain controllers is **Enabled**. If you disable this policy setting on domain controllers, computers running versions of Windows earlier than Windows Server 2003 may not communicate with domains that have computers running Windows Server 2003. For example, the following computers may not work:

- Remote Access Service servers running Windows NT 4.0
- Servers that host Microsoft SQL Server® and run on computers that are running Windows NT 3.x or Windows NT 4.0
- Servers that host Remote Access Service or Microsoft SQL Server and run on computers that are running Windows 2000 and are located in Windows NT domains

Network access: Do not allow anonymous enumeration of SAM accounts

This policy setting determines which additional permissions are granted for anonymous connections to the computer. The Windows operating system allows anonymous users to perform certain activities, such as querying the Security Accounts Manager (SAM) database store of user accounts and security descriptors for users on the local computer, and then enumerating the results. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. However, even if this policy setting is enabled, anonymous users still have access to any resources that have permissions that explicitly include the special built-in group ANONYMOUS LOGON.

In Windows 2000, a similar policy setting called **Additional Restrictions for Anonymous Connections** managed a registry value called **RestrictAnonymous**, which was located in the **HKLM\SYSTEM\CurrentControlSet\Control\LSA** registry key. In Windows Server 2003, the policy settings **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Do not allow anonymous enumeration of SAM accounts and shares** replaced the Windows 2000 policy setting. They manage the registry values **RestrictAnonymousSAM** and **RestrictAnonymous**, respectively, which are located in the **HKLM\System\CurrentControlSet\Control\Lsa** registry key.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. Social engineering attackers try to deceive users in some way to obtain passwords or some form of security information.

Countermeasure

Enable the **Network access: Do not allow anonymous enumeration of SAM accounts** policy setting.

Potential impact

It is impossible to establish trust with domains that are running Windows NT 4.0. Also, client computers that run earlier versions of the Windows operating system such as Windows NT 3.51 and Windows 95 experience problems when they try to use resources on the server.

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

This policy setting determines whether anonymous enumeration of Security Accounts Manager (SAM) accounts and shared folders is allowed. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. You can enable this policy setting if you do not want to allow anonymous enumeration of SAM accounts and shared folders. However, even if it is enabled, anonymous users still have access to any resources that have permissions that explicitly include the special built-in group ANONYMOUS LOGON.

In Windows 2000, a similar policy setting called **Additional Restrictions for Anonymous Connections** managed a registry value called **RestrictAnonymous**, which was located in the **HKLM\SYSTEM\CurrentControlSet\Control\LSA** registry key. In Windows Server 2003, the policy settings **Network access: Do not allow anonymous enumeration of SAM accounts** and **Network access: Do not allow anonymous enumeration of SAM accounts and shares** replaced the Windows 2000 policy setting. They manage the registry values **RestrictAnonymousSAM** and **RestrictAnonymous**, respectively, which are located in the **HKLM\System\CurrentControlSet\Control\Lsa** registry key.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social-engineering attacks.

Countermeasure

Enable the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** policy setting.

Potential impact

It is impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain are unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously are unable to list the shared network resources on those servers. The users must be authenticated before they can view the lists of shared folders and printers.

Network access: Do not allow storage of passwords or credentials for network authentication

This policy setting determines whether the **Stored User Names and Passwords** feature can save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the **Stored User Names and Passwords** feature in Windows does not store passwords and credentials.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Passwords that are cached can be accessed by users when they are logged on to their computer. Although this information may sound obvious, a problem can arise if the user unknowingly runs malicious software that reads the passwords and forwards them to an unauthorized user.



Note

The chances of success for this exploit and others that involve malicious software are reduced significantly for organizations that effectively implement and manage an enterprise antivirus solution combined with sensible software restriction policies. For more information about software restriction policies, see the section **Software Restriction Policies**.

Countermeasure

Enable the **Network access: Do not allow storage of passwords or credentials for network authentication** policy setting.

Potential impact

Users are forced to type passwords whenever they log on to network resources that are not accessible to their domain account. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory–based domain account.

Network access: Let Everyone permissions apply to anonymous users

This policy setting determines what additional permissions are granted for anonymous connections to the computer. If you enable this policy setting, anonymous users can enumerate the names of domain accounts and shared folders and perform certain other activities. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust.

By default, the token that is created for anonymous connections does not include the Everyone SID. Therefore, permissions that are assigned to the Everyone group do not apply to anonymous users. If you enable this policy setting, the Everyone SID is added to the token that is created for anonymous connections, and anonymous users can access any resource for which the Everyone group has been assigned permissions.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

An unauthorized user could anonymously list account names and shared resources, and then use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

Countermeasure

Disable the **Network access: Let Everyone permissions apply to anonymous users** policy setting.

Potential impact

None. This is the default configuration.

Network access: Named Pipes that can be accessed anonymously

This policy setting determines which communication sessions, or pipes, have attributes and permissions that allow anonymous access.

Possible values:

- User-defined list of shared folders
- Not Defined

For this policy setting to take effect, you must also enable the **Network access: Restrict anonymous access to named pipes and shares** policy setting.

Vulnerability

You can restrict access over named pipes such as COMNAP and LOCATOR to help prevent unauthorized access to the network. The following list describes available named pipes and their purpose. These named pipes were granted anonymous access in earlier versions of Windows and some legacy applications may still use them.

| Named pipe | Purpose |
|------------|--|
| COMNAP | SNABase named pipe (Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers.) |
| COMNODE | SNA Server named pipe |
| SQL\QUERY | Default named pipe for SQL Server |
| SPOOLSS | Named pipe for the Print Spooler service |
| EPMAPPER | End Point Mapper named pipe. |
| LOCATOR | Remote Procedure Call Locator service named pipe |
| TrlWks | Distributed Link Tracking Client named pipe |
| TrkSvr | Distributed Link Tracking Server named pipe |

Countermeasure

Configure the **Network access: Named Pipes that can be accessed anonymously** policy setting to a null value (enable the policy setting but do not specify named pipes in the text box).

Potential impact

This configuration disables null-session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes no longer function. This may break trust between domains in a mixed-mode environment.

Network access: Remotely accessible registry paths

This policy setting determines which registry paths are accessible when an application or process references the WinReg key to determine access permissions.

Possible values:

- User-defined list of paths
- Not Defined

Vulnerability

An attacker could use information in the registry to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Countermeasure

Configure the **Network access: Remotely accessible registry paths** policy setting to a null value (enable the policy setting but do not enter any paths in the text box).

Potential impact

Remote management tools require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail.



Note

If you want to allow remote access, you must also enable the Remote Registry service.

Network access: Remotely accessible registry paths and sub-paths

This policy setting determines which registry paths and subpaths are accessible when an application or process references the WinReg key to determine access permissions.

Possible values:

- User-defined list of paths
- Not Defined

Vulnerability

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs that are assigned throughout the registry are fairly restrictive and help protect the registry from access by unauthorized users reduces the risk of such an attack.

Countermeasure

Configure the **Network access: Remotely accessible registry paths and sub-paths** policy setting to a null value (enable the policy setting but do not enter any paths in the text box).

Potential impact

Remote management tools require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail.

**Note**

If you want to allow remote access, you must also enable the Remote Registry service.

Network access: Restrict anonymous access to Named Pipes and Shares

This policy setting enables or disables the restriction of anonymous access to only those shared folders and pipes that are named in the **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously** policy settings.

This policy setting controls null session access to shared folders on your computers by adding RestrictNullSessAccess with the value **1** in the registry key

HKLM\System\CurrentControlSet\Services\LanManServer\Parameters. This registry value toggles null session shared folders on or off to control whether the Server service restricts unauthenticated clients' access to named resources.

Possible values:

- Enabled
- Disabled
- Not Defined

This policy setting is enabled by default.

Vulnerability

Null sessions are a weakness that can be exploited through shared folders (including the default shared folders) on computers in your environment.

Countermeasure

Enable the **Network access: Restrict anonymous access to Named Pipes and Shares** policy setting.

Potential impact

You can enable this policy setting to restrict null-session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries.

If you choose to enable this policy setting and are supporting Windows NT 4.0 domains, determine whether any of the named pipes in the following list are required to maintain trust relationships between the domains, and then add the pipe to the **Network access: Named pipes that can be accessed anonymously**:

- COMNAP–SNA session access
- COMNODE–SNA session access
- SQL\QUERY–SQL instance access
- SPOOLSS–Spooler service
- LLSRPC–License Logging service
- Netlogon–Net Logon service
- Lsarpc–LSA access
- Samr–Remote access to SAM objects
- browser–Computer Browser service

In operating systems earlier than Windows Server 2003 with Service Pack 1 (SP1), these named pipes were allowed anonymous access by default. In later operating systems, these pipes must be explicitly added if needed.

Network access: Shares that can be accessed anonymously

This policy setting determines which shared folders can be accessed by anonymous users.

Possible values:

- User-defined list of shared folders
- Not Defined

Vulnerability

Any shared folders that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Countermeasure

Configure the **Network access: Shares that can be accessed anonymously** policy setting to a null value.

Potential impact

There should be little impact because this is the default configuration. Only authenticated users have access to shared resources on the server.

Network access: Sharing and security model for local accounts

This policy setting determines how network logons that use local accounts are authenticated. If you configure this policy setting to Classic, network logons that use local account credentials authenticate with those credentials. If you configure this policy setting to Guest only, network logons that use local accounts are automatically mapped to the Guest account. The Classic model provides precise control over access to resources and enables you to grant different types of access to different users for the same resource. Conversely, the Guest only model treats all users equally as the Guest user account, and they all receive the same level of access to a given resource, which can be either Read Only or Modify.

The default configuration for a stand-alone computer is Guest only. The default configuration for domain members is Classic.



Notes

This policy setting does not affect network logons that use domain accounts. Nor does this policy setting affect interactive logons that are performed remotely through services such as Telnet, Terminal Services or Remote Desktop Services. This setting also has no effect on computers running Windows 2000.

When the computer is not joined to a domain, this policy setting also tailors the **Sharing** and **Security** tabs in Windows Explorer to correspond to the sharing and security model that is being used.

Possible values:

- Classic: Local users authenticate as themselves

- Guest only: Local users authenticate as Guest
- Not Defined

Vulnerability

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they do not have Write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Countermeasure

For network servers, configure the **Network access: Sharing and security model for local accounts** policy setting to **Classic – local users authenticate as themselves**. On end-user computers, configure this policy setting to **Guest only – local users authenticate as guest**.

Potential impact

None. This is the default configuration.

Network security: Allow Local System to use computer identity for NTLM

This policy setting allows Local System services that use SPNEGO (Negotiate) to use the computer identity when reverting to NTLM authentication.

If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

If you do not configure this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows Server 2008 R2 or Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, signing and encryption are supported to provide data protection.

Countermeasure

You can configure the **Network security: Allow Local System to use computer identity for NTLM** security policy setting to allow Local System services that use Negotiate to use the computer identity when reverting to NTLM authentication.

Potential impact

If you do not configure this policy setting, services running as Local System that use the default credentials and a NULL session revert to NTLM authentication for Windows operating systems earlier than Windows Vista or Windows Server 2008. This might cause some authentication requests between Windows operating systems to fail and display an error.

Network security: Allow Local System NULL session fallback

This policy setting controls what values are used when a service connects to different versions of Windows operating systems from computers running Windows Server 2008 R2 and Windows 7.

If **Network security: Allow Local System to use computer identity for NTLM** is set to disabled, then services running as Local System will fall back to using NULL session authentication when transmitting data to servers running versions of Windows earlier than Windows Vista or Windows Server 2008. NULL session does not establish a unique session key for each authentication and thus cannot provide integrity or confidentiality protection. This setting determines whether services that request the use of these faculties are allowed to perform signature or encryption functions with well-known key for application compatibility.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

If this setting is enabled, then a system-generated session key is created when connecting with a NULL session, which provides no protection but allows applications to sign and encrypt data without errors. Data intended to be protected may be exposed.

Countermeasure

You can configure the computer to use the machine identity for Local System with the policy **Network security: Allow Local System to use computer identity for NTLM**. If that is not possible, then this policy can be used to prevent data from being exposed in transit that was protected with a well-known key.

Potential impact

If you enable this policy, services that use NULL session with Local System could fail to authenticate because they will be prohibited from using signing and encryption.

This policy applies to Windows Server 2008 and Windows Vista (SP1 and later). When your environment no longer requires support for NT 4, this policy should be disabled. By default it is disabled on Windows 7 and Windows Server 2008 R2.

Network Security: Allow PKU2U authentication requests to this computer to use online identities

This policy setting determines whether the PKU2U authentication protocol requests will be allowed between computers running Windows 7.

If you enable this policy setting, this will allow authentication to successfully complete between the two (or more) computers that have established a peer relationship through the use on online IDs. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation, and it associates the user's certificate to a security token and the logon process completes.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Enabling this policy setting allows a user account on one computer to be associated with an online identity, such as Windows Live ID, so that the account can log on to a peer computer (if

the peer computer is likewise configured) without the use of a Windows logon account (domain or local). Although this can be beneficial for workgroups or home groups, using this feature in a domain might circumvent your established security policies.

Countermeasure

Set this policy to **Disabled** or do not configure this security policy for all domain-joined computers.

Potential impact

If you disable or do not enable this policy setting, the PKU2U protocol will not be used to authenticate between peer computers, which forces users to follow domain-defined access control policies. If you enable this policy setting, you will allow your users to use PKU2U to authenticate by using local certificates between computers that are not part of a domain. This allows users to share resources between computers.

Network security: Configure encryption types allowed for Kerberos

This policy setting determines which set of encryption types will be allowed for processing Kerberos authentication requests.

Possible values:

- DES_CBC_CRC
- DES_CBC_MD5
- RC4_HMAC_MD5
- AES128_HMAC_SHA1
- AES256_HMAC_SHA1
- Future encryption types

The following table describes these values.

| Value | Description |
|-------------|--|
| DES_CBC_CRC | Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. Windows 7 and Windows Server 2008 R2 |

| Value | Description |
|-------------------------|---|
| | systems do not support DES by default. |
| DES_CBC_MD5 | Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. Windows 7 and Windows Server 2008 R2 systems do not support DES by default. |
| RC4_HMAC_MD5 | Supported in Windows 2000 Server, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. |
| AES128_HMAC_SHA1 | Not supported in Windows 2000 Server, Windows XP, or Windows Server 2003. Supported in Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. |
| AES256_HMAC_SHA1 | Not supported in Windows 2000 Server, Windows XP, or Windows Server 2003. Supported in Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. |
| Future encryption types | As of the release of Windows Server 2008 R2 and Windows 7, this is reserved by Microsoft for additional encryption types that might be implemented. |

Vulnerability

Windows Server 2008 R2 and Windows 7 do not support the DES cryptographic suites by default because stronger cryptographic suites are available. However, to enable Kerberos protocol interoperability with non-Windows versions of Kerberos, these suites can be enabled. Doing so might open attack vectors on computers running Windows Server 2008 R2 and Windows 7.

Countermeasure

Do not configure this policy setting. This will force computers running Windows Server 2008 R2 and Windows 7 to use the AES or RC4 cryptographic suites. You can also disable DES for your computers running Windows Vista and Windows Server 2008.

Potential impact

If you do not select any of the encryption types, computers running Windows Server 2008 R2 and Windows 7 might have Kerberos protocol authentication failures when connecting with computers running non-Windows versions of Kerberos.

If you do select any encryption type, you will lower the effectiveness of encryption for Kerberos authentication.

Contemporary non-Windows implementations of Kerberos support RC4 and AES 128-bit and AES 256-bit encryption. Most implementations, including MIT Kerberos and Windows Kerberos, are deprecating DES encryption.

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

This policy setting determines whether LAN Manager is prevented from storing hash values for the new password the next time the password is changed. Hash values are representation of the password after the encryption algorithm is applied that corresponds to the format specified by the algorithm. To decrypt the hash value, the encryption algorithm must be determined and then reversed. The LAN Manager hash is relatively weak and prone to attack compared to the cryptographically stronger NTLM hash.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

The SAM file can be targeted by attackers who seek access to user name and password hashes. Such attacks use special tools to discover passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks are not prevented by enabling this policy setting because LAN Manager hashes are much weaker than NTLM hashes, but it is much more difficult for these attacks to succeed.

Countermeasure

Enable the **Network security: Do not store LAN Manager hash value on next password change** policy setting. Require that all users set new passwords the next time they log on to the domain so that LAN Manager hashes are removed.

Potential impact

Earlier operating systems such as Windows 95, Windows 98, and Windows Millennium Edition, in addition to some non-Microsoft applications, cannot connect to the system.

Network security: Force logoff when logon hours expire

This policy setting enables or disables the forced disconnection of users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB server are disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions are maintained after the client's logon hours expire.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

If you disable this policy setting, users can remain connected to the computer outside of their allotted logon hours.

Countermeasure

Enable the **Network security: Force logoff when logon hours expire** policy setting. This policy setting does not apply to administrator accounts.

Potential impact

When a user's logon time expires, SMB sessions terminate. The user cannot log on to the computer until the next scheduled access time commences.

Network security: LAN Manager authentication level

This policy setting determines which challenge/response authentication protocol is used for network logons. LAN Manager allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the

default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory uses LAN Manager (LM), NTLM, or NTLM version 2 (NTLMv2).

LAN Manager authentication includes the LM, NTLM, and NTLMv2 variants, and it is the protocol that is used to authenticate all Windows client computers when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to domains based on earlier versions of Windows
- Authenticate to computers that do not run the Windows 2000, Windows Server 2003, Windows Vista, or Windows XP operating systems
- Authenticate to computers that are not in the domain

Possible values:

- Send LM & NTLM responses
- Send LM & NTLM - use NTLMv2 session security if negotiated
- Send NTLM responses only
- Send NTLMv2 responses only
- Send NTLMv2 responses only. Refuse LM
- Send NTLMv2 responses only. Refuse LM & NTLM
- Not Defined

The **Network security: LAN Manager authentication level** policy setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that client computers use, the session security level that the computers negotiate, and the authentication level that servers accept. The following table identifies the policy settings, describes the setting, and identifies the security level that is used in the corresponding registry setting if you choose to use the registry to control this setting instead of the policy setting.

| Setting | Description | Registry security level |
|--------------------------|---|-------------------------|
| Send LM & NTLM responses | Client computers use LM and NTLM authentication, and they | 0 |

| Setting | Description | Registry security level |
|--|---|-------------------------|
| | never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. | |
| Send LM & NTLM – use NTLMv2 session security if negotiated | Client computers use LM and NTLM authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. | 1 |
| Send NTLM response only | Client computers use NTLM authentication only, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. | 2 |
| Send NTLMv2 response only | Client computers use NTLMv2 authentication only, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. | 3 |
| Send NTLMv2 response only. Refuse LM | Client computers use NTLMv2 authentication only, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM authentication, and they will accept only NTLM and NTLMv2 authentication. | 4 |
| Send NTLMv2 response only. Refuse LM & NTLM | Client computers use NTLMv2 authentication only, and they | 5 |

| Setting | Description | Registry security level |
|---------|---|-------------------------|
| | use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM and NTLM authentication, and they will accept only NTLMv2 authentication. | |

Vulnerability

Beginning with Windows Vista, this policy setting is undefined. Beginning with Windows Server 2008, this policy setting is configured to **Send NTLMv2 responses only**. In Windows 2000, Windows Server 2003, and Windows XP, client computers are configured by default to send LM and NTLM authentication responses (client computers running Windows 95 and Windows 98 send only LM).

The default setting on servers allows all client computers to authenticate with servers and use their resources. However, this means that LM responses—the weakest form of authentication response—are sent over the network, and it is potentially possible for attackers to intercept that traffic to reproduce the user's password more easily.

The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with the LM and NTLM protocols for network authentication.

You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for client computers and servers running these earlier versions of Windows, client computers and servers that are members of the domain use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Countermeasure

Configure the **Network security: LAN Manager Authentication Level** policy setting to **Send NTLMv2 responses only**. We and a number of independent organizations strongly recommend this level of authentication when all client computers support NTLMv2.

For more information about how to enable NTLMv2 on earlier versions of Windows, see [article 239869](#) in the Microsoft Knowledge Base. Windows NT 4.0 requires Service Pack 4 (SP4) to

support NTLMv2, and the Windows 95 and Windows 98 operating systems need the directory service client installed to support NTLMv2.

Potential impact

Clients that do not support NTLMv2 authentication cannot authenticate in the domain and access domain resources by using LM and NTLM.

Network security: LDAP client signing requirements

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. These different levels of data signing are described in the following list:

- **None.** The LDAP BIND request is issued with the caller-specified options.
- **Negotiate signing.** If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.
- **Require signing.** This level is the same as Negotiate signing. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is returned a message that the LDAP BIND command request failed.



Note

This policy setting does not have any impact on `ldap_simple_bind` or `ldap_simple_bind_s`. Microsoft LDAP clients do not use `ldap_simple_bind` or `ldap_simple_bind_s` to communicate with a domain controller.

Possible values:

- None
- Negotiate signing
- Require signature
- Not Defined

Vulnerability

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network

infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Countermeasure

Configure the **Network security: LDAP server signing requirements** policy setting to **Require signature**.

Potential impact

If you configure the server to require LDAP signatures, you must also configure the client computer. If you do not configure the client computer, it cannot communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts.

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

This policy setting allows a client computer to require the negotiation of 128-bit encryption, or NTLMv2 session security. These values are dependent on the **Network security: LAN Manager Authentication Level** policy setting value.

Possible values:

- Require 128-bit encryption
- Require NTLMv2 session security
- Not Defined

Vulnerability

Network traffic that uses the NTLM Security Support Provider (NTLM SSP) could be exposed such that an attacker who has gained access to the network can create man-in-the-middle attacks.

Countermeasure

Enable all options that are available for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** policy setting.

Potential impact

If this policy setting is configured, client computers that are enforcing these settings cannot communicate with older servers that do not support these settings.

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

This policy setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the **LAN Manager Authentication Level security** setting value.

Possible values:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128-bit encryption
- Not Defined

Vulnerability

Network traffic that uses the NTLM Security Support Provider (NTLM SSP) could be exposed such that an attacker who has gained access to the network can create man-in-the-middle attacks.

Countermeasure

Enable all four options that are available for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** policy setting.

Potential impact

If this policy setting is configured, older client computers that do not support these security settings cannot communicate with this computer.

Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication

This policy setting allows you to create an exception list of remote servers to which client computers are allowed to use NTLM authentication if any of the deny options are set in the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** policy setting.

When you can enter a list of remote servers to which client computers are allowed to use NTLM authentication, the policy is defined and enabled.

Possible values:

- User-defined list of remote servers
- Not Defined

Vulnerability

When it has been determined that the NTLM authentication protocol should not be used from a client to any remote servers because you are required to use a more secure protocol, such as Kerberos protocol, there might be some applications on the client computer that still use NTLM. If so, and you set **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** to any of the Deny options, those applications will fail because the outbound NTLM authentication traffic from the client computer will be blocked.

If you define an exception list of servers to which client computers are allowed to use NTLM authentication, then NTLM authentication traffic will continue to flow between the servers and those applications on the client computers. The servers then are vulnerable to any malicious attack that takes advantage of security weaknesses in NTLM.

Countermeasure

When you use **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** in audit-only mode, you can determine by reviewing which applications on the client computers are making NTLM authentication requests to the remote servers in your environment. When assessed, you will have to determine on a case-by-case basis if NTLM authentication still minimally meets your security requirements. If not, then the application has to be upgraded to use something other than NTLM authentication.

Potential impact

Defining a list of servers for this policy setting will enable NTLM authentication traffic from the application on the client computer that uses those servers, and this might result in a security vulnerability.

If this list is not defined and **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** is enabled, then applications on client computers that use NTLM will fail to authenticate to those servers that they have used in the past.

Network security: Restrict NTLM: Add server exceptions in this domain

This policy setting allows you to create an exception list of servers in this domain to which client computers are allowed to use NTLM pass-through authentication if any of the deny options are set in the **Network Security: Restrict NTLM: NTLM authentication in this domain** policy setting.

When you enter a list of remote servers to which clients are allowed to use NTLM authentication, the policy is defined and enabled.

Possible values:

- User-defined list of servers to which clients are allowed to use NTLM authentication
- Not Defined

Vulnerability

When it has been determined that the NTLM authentication protocol should not be used within a domain because you are required to use a more secure protocol, such as Kerberos protocol, there might be some client applications that still use NTLM. If so, and you set **Network Security: Restrict NTLM: NTLM authentication in this domain** to any of the Deny options, those applications will fail because the outbound NTLM authentication traffic from the client will be blocked.

If you define an exception list of servers in this domain to which client computers are allowed to use NTLM pass-through authentication, then NTLM authentication traffic will continue to flow between the servers and those applications on the client computers. The servers then are vulnerable to any malicious attack that takes advantage of security weaknesses in NTLM.

Countermeasure

When you use **Network Security: Restrict NTLM: NTLM authentication in this domain** in audit-only mode, you can determine by reviewing which applications on the client computers are making NTLM authentication requests to the pass-through authentication servers. When assessed, you will have to determine on a case-by-case basis if NTLM authentication still minimally meets your security requirements. If not, then the application has to be upgraded to use something other than NTLM authentication.

Potential impact

Defining a list of servers for this policy setting will enable NTLM authentication traffic between those servers and any application on the client computer that uses those servers and might result in a security vulnerability.

If this list is not defined and **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** is enabled, then applications on the client computers that use NTLM will fail to authenticate to those servers that they have used in the past.

Network Security: Restrict NTLM: Audit Incoming NTLM Traffic

This policy setting allows you to audit a member or remote server for NTLM traffic that is coming in from client computer-based services. The policy works in conjunction with the **Network Security: Restrict NTLM: Incoming NTLM traffic** policy setting that restricts the traffic.

Possible values:

- Disable
- Enable auditing for domain accounts
- Enable auditing for all accounts
- Not Defined

Vulnerability

Enabling this policy setting will reveal through logging which servers and client computers within your network or domain handle NTLM traffic. The identity of these computers can be used in malicious ways if NTLM authentication traffic is compromised. The policy setting does not prevent or mitigate any vulnerability because it is for audit purposes only.

Countermeasure

Restrict access to the log files when this policy setting is enabled in your production environment.

Potential impact

If you do not enable or configure this policy setting, no NTLM authentication traffic information will be logged. If you do enable this policy setting, only auditing functions will occur; no security enhancements will be implemented.

Network Security: Restrict NTLM: Audit NTLM authentication in this domain

This policy setting allows you to audit NTLM authentication requests that come from member servers to a domain controller. The policy setting works in conjunction with the **Network security: Restrict NTLM: NTLM authentication in this domain** policy setting that restricts the traffic.

Possible values:

- Disable
- Enable for domain accounts to domain servers
- Enable for domain accounts

- Not Defined

Vulnerability

Enabling this policy setting will reveal through logging which servers and client computers within your network or domain handle NTLM traffic. The identity of these computers can be used in malicious ways if NTLM authentication traffic is compromised. The policy setting does not prevent or mitigate any vulnerability because it is for audit purposes only.

Countermeasure

Restrict access to the log files when this policy setting is enabled in your production environment.

Potential impact

If you do not enable or configure this policy setting, no NTLM authentication traffic information will be logged. If you enable this policy setting, only auditing functions will occur; no security enhancements will be implemented.

Network Security: Restrict NTLM: Incoming NTLM traffic

This policy setting allows you to deny or allow NTLM traffic on the targeted server that is coming from client computers, other member servers, or a domain controller.

Possible values:

- Allow all
- Deny all domain accounts
- Deny all accounts
- Not Defined

Vulnerability

Malicious attacks on NTLM authentication traffic resulting in a compromised server can occur only if the server handles NTLM requests. If those requests are denied, this attack vector is eliminated.

Countermeasure

When it has been determined that the NTLM authentication protocol should not be used within a network because you are required to use a more secure protocol, such as Kerberos protocol, you can select from several options based on your security goals to restrict NTLM usage.

Potential impact

If you configure this policy setting, numerous NTLM authentication requests could fail within your network, which could degrade productivity. Before implementing this change through this policy setting, set **Network security: Restrict NTLM: Audit Incoming NTLM Traffic** to the same option so that you can review the log for the potential impact, perform an analysis of servers, and create an exception list of servers to exclude from the **Network security: Restrict NTLM: Add server exceptions in this domain** policy setting.

Network Security: Restrict NTLM: NTLM authentication in this domain

This policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller. This policy setting does not affect interactive logon to this domain controller.

Possible values:

- Disable
- Deny for domain accounts to domain servers
- Deny for domain accounts
- Deny for domain servers
- Deny all
- Not Defined

Vulnerability

Malicious attacks on NTLM authentication traffic resulting in a compromised server or domain controller can occur only if the server or domain controller handles NTLM requests. If those requests are denied, this attack vector is eliminated.

Countermeasure

When it has been determined that the NTLM authentication protocol should not be used within a network because you are required to use a more secure protocol, such as the Kerberos protocol, then you can select from several options based on your security goals to restrict NTLM usage within the domain.

Potential impact

If you configure this policy setting, numerous NTLM authentication requests could fail within the domain, which could decrease productivity. Before implementing this change through this policy setting, set **Network security: Restrict NTLM: Audit NTLM authentication in this domain** to the same option so that you can review the log for the potential impact, perform an analysis of

servers, and create an exception list of servers to exclude from this policy setting by using **Network security: Restrict NTLM: Add server exceptions in this domain**.

Audited and blocked events are recorded on this computer in the Operational log located in **Applications and Services Log\Microsoft\Windows\NTLM**.

Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers

This policy setting allows you to deny or audit outgoing NTLM traffic from a computer running Windows 7 or Windows Server 2008 R2 to any remote server running the Windows operating system.

Possible values:

- Allow all
- Audit all
- Deny all
- Not Defined

Vulnerability

Malicious attacks on NTLM authentication traffic resulting in a compromised server or domain controller can occur only if the server or domain controller handles NTLM requests. If those requests are denied, this attack vector is eliminated.

Countermeasure

When it has been determined that the NTLM authentication protocol should not be used within a network because you are required to use a more secure protocol, such as Kerberos protocol, you can select from several options, based on your security goals, to restrict NTLM usage to servers.

Potential impact

If you configure this policy setting to deny all requests, numerous NTLM authentication requests to remote servers could fail, which could decrease productivity. Before implementing this restriction through this policy setting, select **Audit all** so that you can review the log for the potential impact, perform an analysis of servers, and create an exception list of servers to exclude from this policy by using **Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication**.

Audited and blocked events are recorded on this computer in the Operational log located in **Applications and Services Log\Microsoft\Windows\NTLM**.

Recovery console: Allow automatic administrative logon

This policy setting determines whether the Administrator account password must be provided before access to the computer is granted. If you enable this policy setting, the Administrator account is automatically logged on to the computer at the Recovery Console; no password is required.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

The Recovery Console can be very useful when you must troubleshoot and repair computers that do not start. However, allowing automatic logon to the Recovery Console can make it possible for someone to assume full control of the server.

Countermeasure

Disable the **Recovery console: Allow automatic administrative logon** policy setting.

Potential impact

Users must enter a user name and password to access the Recovery Console.

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

This policy setting enables or disables the Recovery Console SET command, 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.** Suppresses the prompt that typically displays before an existing file is overwritten.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

An attacker who can cause the system to restart into the Recovery Console could steal sensitive data and leave no audit or access trail.

Countermeasure

Disable the **Recovery console: Allow floppy copy and access to drives and folders** policy setting.

Potential impact

Users who have started a server through the Recovery Console and logged on with the built-in Administrator account cannot copy files and folders to a floppy disk.

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

This policy setting determines whether a computer can be shut down without having to log on to Windows. If you enable this policy setting, the **Shut down** command is available on the Windows logon screen. If you disable this policy setting, the **Shut down** command is removed from the Windows logon screen. This configuration requires that users are able to log on to the computer successfully and they have the **Shut down the system** user right before they can perform a computer shutdown.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Users who can access the console locally could shut down the computer.

Attackers who have access to the local console could restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable.

Countermeasure

Disable the **Shutdown: Allow system to be shut down without having to log on** policy setting.

Potential impact

Operators must log on to servers to shut them down or restart them.

Shutdown: Clear virtual memory pagefile

This policy setting determines whether the virtual memory paging file is cleared when the computer is shut down. Virtual memory support uses a system paging file to swap pages of memory to disk when they are not used. On a running computer, this paging file is opened exclusively by the operating system, and it is well protected. However, computers that are configured to allow other operating systems to start should verify that the system paging file is cleared as the computer shuts down. This confirmation ensures that sensitive information from process memory that might be placed in the paging file is not available to an unauthorized user who manages to directly access the paging file after shutdown.

When you enable this policy setting, the system paging file is cleared when the system shuts down normally. Also, this policy setting forces the computer to clear the hibernation file (hiberfil.sys) when hibernation is disabled on a portable computer.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Important information that is kept in real memory may be written periodically to the paging file to help the operating system handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file.



Caution

An attacker who has physical access to the computer could bypass this countermeasure by unplugging the computer from its power source.

Countermeasure

Enable the **Shutdown: Clear virtual memory pagefile when system shuts down** policy setting. This configuration causes the operating system to clear the pagefile when the computer is shut down. The amount of time that is required to complete this process depends on the size of the pagefile. Because the process overwrites the storage area used by the pagefile several times, it could be several minutes before the computer completely shuts down.

Potential impact

It takes longer to shut down and restart the computer, especially on computers with large paging files. For a computer with 2 gigabytes (GB) of RAM and a 2-GB paging file, this policy setting could increase the shutdown process by 20 to 30 minutes, or more. For some organizations this downtime violates their internal service level agreements. Therefore, use caution before you implement this countermeasure in your environment.

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

This policy setting determines whether users can use private keys, such as their Secure/Multipurpose Internet Mail Extensions (S/MIME) key, without a password.

Possible values:

- User input is not required when new keys are stored and used
- User is prompted when the key is first used
- User must enter a password each time they use a key
- Not Defined

Vulnerability

If a user's account is compromised or the user's computer is inadvertently left unsecured, the malicious user can use the keys that are stored for the user to access protected resources.

Countermeasure

Configure the **System cryptography: Force strong key protection for user keys stored on the computer** policy setting to **User must enter a password each time they use a key** so that users must provide a password that is distinct from their domain password every time they use a key. This configuration makes it more difficult for an attacker to access locally stored user keys, even if the attacker takes control of the user's computer and determines the logon password.

Potential impact

Users must type their password every time they access a key that is stored on their computer. For example, if users use an S/MIME certificate to digitally sign their email, they are forced to type the password for that certificate every time they send a signed email message. For some organizations, the overhead that is involved by using this configuration may be too high. At a minimum, this policy setting should be set to **User is prompted when the key is first used**.

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

This policy setting determines whether the TLS/SSL Security Support Provider supports only the Federal Information Processing Standard (FIPS)-compliant strong cipher suite known as TLS_RSA_WITH_3DES_EDE_CBC_SHA, which means that the provider only supports the TLS protocol as a client and as a server, if applicable. It uses only the Triple Data Encryption Standard (3DES) encryption algorithm for the TLS traffic encryption, only the Rivest-Shamir-Adleman (RSA) public key algorithm for the TLS key exchange and authentication, and only the Secure Hash Algorithm version 1 (SHA-1) hashing algorithm for the TLS hashing requirements.

When this policy setting is enabled, the Encrypting File System (EFS) service supports only the 3DES encryption algorithm for encrypting file data. By default, the implementation of EFS beginning with Windows Server 2003 uses the Advanced Encryption Standard (AES) with a 256-bit key.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

You can enable this policy setting to ensure that the computer uses the most powerful algorithms that are available for digital encryption, hashing, and signing. Use of these algorithms minimizes the risk of compromise of digitally encrypted or signed data by an unauthorized user.

Countermeasure

Enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy setting.

Potential impact

Client computers that have this policy setting enabled cannot communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms cannot use servers that require the algorithms for network communications. For example, many Apache-based Web servers are not configured to support TLS. If you enable this policy setting, you must also configure your Web browser to use TLS.

This policy setting also affects the encryption level that is used for the Remote Desktop Protocol (RDP). The Remote Desktop Connection tool uses the RDP to communicate with servers that run

Remote Desktop Services or Terminal Services and client computers that are configured for remote control. RDP connections fail if both computers are not configured to use the same encryption algorithms.

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

This policy setting determines whether the Administrators group or an object creator is the default owner of any system objects that are created.

Possible values:

- Administrators group
- Object creator
- Not Defined

Vulnerability

If you configure this policy setting to the Administrators group, it is impossible to hold individuals accountable for the creation of new system objects.

Countermeasure

Configure the **System objects: Default owner for objects created by members of the Administrators group** policy setting to **Object creator**.

Potential impact

When system objects are created, the ownership reflects which account created the object instead of the more generic Administrators group. A consequence of this policy setting is that objects become orphaned when user accounts are deleted. For example, when a member of the information technology group leaves, any objects that they created anywhere in the domain have no owner.

This situation could become an administrative burden because administrators must manually take ownership of orphaned objects to update their permissions. This potential burden can be minimized if you can ensure that Full Control is always assigned to new objects for a domain group such as Domain Admins.

System objects: Require case insensitivity for non-Windows subsystems

This policy setting enables or disables the enforcement of case insensitivity for all subsystems. The Microsoft Win32® subsystem is case-insensitive. However, the kernel supports case sensitivity for other subsystems, such as Portable Operating System Interface for UNIX (POSIX).

If you enable this policy setting, case insensitivity is enforced for all directory objects, symbolic links, IO, and file objects. If you disable this policy setting, case insensitivity is not enforced, but the Win32 subsystem does not become case sensitive.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Because Windows is case insensitive but the POSIX subsystem supports case sensitivity, failure to enable this policy setting makes it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of uppercase and lowercase letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files is available.

Countermeasure

Enable the **System objects: Require case insensitivity for non-Windows subsystems** policy setting.

Potential impact

All subsystems are forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that are case sensitive.

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

This policy setting determines the strength of the default DACL for objects. The Windows operating system maintains a global list of shared computer resources (such as MS-DOS device names, mutexes, and semaphores) so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions. If you enable this policy setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create.

Possible values:

- Enabled
- Disabled

- Not Defined

Vulnerability

This policy setting is enabled by default to protect against a known vulnerability that can be used with hard links or symbolic links. Hard links are actual directory entries in the file system. With hard links, the same data in a file system can be referred to by different file names. Symbolic links are text files that provide a pointer to the file that is interpreted and followed by the operating system as a path to another file or directory.

Because symbolic links are a separate file, they can exist independently of the target location. If a symbolic link is deleted, its target location remains unaffected. When this policy setting is disabled, it is possible for a malicious user to destroy a data file by creating a link that looks like a temporary file that the system automatically creates, such as a sequentially named log file, but points to the data file that the malicious user wants to eradicate. When the system writes the files with that name, the data is overwritten.

Enabling **System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)** prevents an attacker from exploiting programs that create files with predictable names by not allowing them to write to objects that they did not create.

Countermeasure

Enable the **System objects: Strengthen default permissions of global system objects (e.g., Symbolic Links)** policy setting.

Potential impact

None. This is the default configuration.

System settings: Optional subsystems

This policy setting determines which subsystems support your applications. You can use this security setting to specify as many subsystems as your environment demands.

Possible values:

- User-defined list of subsystems
- Not Defined

Vulnerability

The POSIX subsystem is an Institute of Electrical and Electronic Engineers (IEEE) standard that defines a set of operating system services. The POSIX subsystem is required if the server supports applications that use that subsystem.

The POSIX subsystem introduces a security risk that relates to processes that can potentially persist across logons. If a user starts a process and then logs out, there is a potential that the next user who logs on to the computer could access the previous user's process. This would allow the second user to take actions on the process by using the privileges of the first user.

Countermeasure

Configure the **System settings: Optional subsystems setting** to a null value. The default value is POSIX.

Potential impact

Applications that rely on the POSIX subsystem no longer operate. For example, Microsoft Services for Unix (SFU) installs an updated version of the POSIX subsystem that is required, so you must reconfigure this setting in Group Policy for any servers that use SFU.

System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. This security setting enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, you can create a certificate rule that allows or disallows Microsoft Authenticode®-signed software to run, based on the digital certificate that is associated with the software. For certificate rules to work in software restriction policies, you must enable this security setting.

Possible values:

- Enabled
- Disabled
- Not Defined

Vulnerability

Without the use of software restriction policies, users and computers might be exposed to the running of unauthorized software that could include malicious software such as viruses and Trojan horses.

Countermeasure

Enable the **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies** policy setting.

Potential impact

If you enable certificate rules, software restriction policies check a certificate revocation list (CRL) to verify that the software's certificate and signature are valid. This checking process may negatively affect performance when signed programs start. To disable this feature, you can edit the software restriction policies in the appropriate GPO. On the **Trusted Publishers Properties** dialog box, clear the **Publisher** and **Timestamp** check boxes.

User Account Control: Admin Approval Mode for the Built-in Administrator account

This policy setting determines the behavior of Admin Approval mode for the built-in Administrator account.

Possible values:

- Enabled
- Disabled

When this policy setting is enabled, the built-in Administrator account logs on in Admin Approval Mode. In this mode, the local Administrator account functions like a standard user account, but it has the ability to elevate privileges without logging on by using a different account. In this mode, any operation that requires elevation of privilege displays a prompt that allows the administrator to permit or deny the elevation of privilege.

When this policy setting is disabled, the built-in Administrator account logs on in XP-compatible mode, and it runs all applications by default with full administrative privileges. By default, this policy setting is set to **Disabled**. However, if a computer is upgraded from a previous version of Windows to Windows 7 and the Administrator account is the only account on the computer, the built-in Administrator account remains enabled, and this policy setting is also enabled.

Vulnerability

One of the risks that User Account Control (UAC) is intended to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for malicious programs is to discover the password of the Administrator account because that user account was created for all installations of the Windows operating system. To address this risk, the built-in Administrator account is disabled in Windows 7. In Windows Server 2008 R2, the Administrator account is enabled, and the password must be changed the first time the administrator logs on. In a default installation of Windows 7, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.

- If the computer is joined to a domain, no local administrator accounts are created. The enterprise or domain administrator must log on to the computer and create a local administrator account if one is warranted.

After Windows 7 is installed, the built-in Administrator account can be enabled, but we strongly recommend that this account remain disabled.

Countermeasure

Enable the **User Account Control: Admin Approval Mode for the Built-in Administrator account** policy setting if you have the built-in Administrator account enabled.

Potential impact

Users who log on by using the local Administrator account are prompted for consent whenever a program requests an elevation in privilege.

User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop

This security setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts that are being used by a standard user.



Note

This policy setting does not change the behavior of the UAC elevation prompt for administrators.

Possible values:

- Enabled
- Disabled or Not Configured

When this policy setting is enabled, UIA programs including Windows Remote Assistance can automatically disable the secure desktop for elevation prompts. Unless you have also disabled elevation prompts, the prompts appear on the interactive user's desktop instead of the secure desktop, and they appear on the remote administrator's view of the desktop during a Windows Remote Assistance session, and the remote administrator can provide the appropriate credentials for elevation.

If you plan to enable this policy setting, you should also review the effect of the **User Account Control: Behavior of the elevation prompt for standard users** policy setting. If it is configured as **Automatically deny elevation requests**, elevation requests are not presented to the user. If you disable this policy setting, the secure desktop can only be disabled by the user of the interactive

desktop or by disabling the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting. By default, this policy setting is set to **Enabled**.

Vulnerability

UIA programs are designed to interact with the Windows operating system and with application programs on behalf of a user. This policy setting allows UIA programs to bypass the secure desktop to increase usability in certain cases, but allowing elevation requests to appear on the regular interactive desktop instead of the secure desktop increases the risk that a malicious program could intercept data that is being transferred between the UI and the application.

Because UIA programs must be able to respond to prompts regarding security issues, such as the UAC elevation prompt, UIA programs must be highly trusted. To be considered trusted, a UIA program must be digitally signed. By default, UIA programs can be run only from the following protected paths:

- Program Files, including subfolders
- Program Files (x86), including subfolders, in 64-bit versions of Windows only
- Windows\System32

The requirement to be in a protected path can be disabled by the **User Account Control: Only elevate UIAccess applications that are installed in secure locations** policy setting. Although this policy setting applies to any UIA program, it is used primarily in certain Windows Remote Assistance scenarios. The Windows Remote Assistance program is a UIA program.

Countermeasure

Disable the **User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop** policy setting.

Potential impact

If a user requests remote assistance from an administrator and the remote assistance session is established, any elevation prompts appear on the interactive user's secure desktop and the administrator's remote session is paused. To avoid pausing the remote administrator's session during elevation requests, the user can select the **Allow IT Expert to respond to User Account Control prompts** check box when setting up the remote assistance session. However, selecting this check box requires that the interactive user respond to an elevation prompt on the secure desktop. If the interactive user is a standard user, the user does not have the required credentials to allow elevation.

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode

This policy setting determines the behavior of the elevation prompt for accounts that have administrative credentials.

Possible values:

- Elevate without prompting
- Prompt for credentials
- Prompt for consent

The default value for this policy setting is **Prompt for consent**.

Vulnerability

One of the risks that the UAC feature tries to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This policy setting notifies the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Countermeasure

Configure the **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** policy setting to **Prompt for consent**.

Potential impact

This is the default behavior. Administrators should be made aware that they will be prompted for consent.

User Account Control: Behavior of the elevation prompt for standard users

This policy setting determines the behavior of the elevation prompt for standard users.

Possible values:

- Automatically deny elevation requests
- Prompt for credentials

The default configuration for this policy setting is **Prompt for credentials**.

Vulnerability

One of the risks that UAC tries to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This policy setting

notifies the user that a program requires the use of elevated privilege operations, and it requires that the user be able to supply administrative credentials for the program to run.

Countermeasure

Configure the **User Account Control: Behavior of the elevation prompt for standard users to Automatically deny elevation requests**. This policy setting requires the user to log on with an administrative account to run programs that require elevation of privilege. As a security best practice, standard users should not have knowledge of administrative passwords. However, if your users have both standard and administrator-level accounts, we recommend setting **Prompt for credentials** so that the users do not choose to always log on with their administrator accounts, and they use the standard user account instead.

Potential impact

Users must provide administrative passwords to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are affected are identified and standard operating procedures are modified to support least privilege operations.

User Account Control: Detect application installations and prompt for elevation

This policy setting determines the behavior of application installation detection for the entire system. If this policy setting is enabled, application installation packages that require an elevation of privilege to install are detected and the user is prompted for administrative credentials.

Enterprises that are running standard user desktops that capitalize on delegated installation technologies (such as Group Policy Software Install (GPSI) or SMS) can disable this feature. In this case, installer detection is unnecessary and it is not required.

Possible values:

- Enabled
- Disabled

The default configuration for this policy setting is **Enabled**.

Vulnerability

Some malicious software may attempt to install itself after being given permission to run, for example, malicious software with a trusted application shell. The user may give permission for the program to run because the program is trusted and is then prompted for installation of an unknown component. This provides another way to trap the software before it can do damage.

Countermeasure

Enable the **User Account Control: Detect application installations and prompt for elevation** policy setting.

Potential impact

Users must provide administrative passwords to install programs.

User Account Control: Only elevate executables that are signed and validated

This policy setting enforces public key infrastructure (PKI) signature checks on any interactive application that requests elevation of privilege. Enterprise administrators can control the applications that are allowed to run through the population of certificates in the local computer's Trusted Publishers store. If this policy setting is enabled, the PKI certificate chain validation of a given executable file is enforced before it is permitted to run.

Possible values:

- Enabled
- Disabled

The default configuration for this policy setting is **Disabled**.

Vulnerability

Intellectual property, personally identifiable information, and other confidential data is normally manipulated by applications on the computer, and elevated credentials are required to get access to the information. Users and administrators inherently trust applications that are used with these information sources and provide their credentials. If one of these applications is replaced by a rogue application that appears identical to the trusted application, the confidential data and the user's administrative credentials could be compromised.

Countermeasure

Enable the **User Account Control: Only elevate executables that are signed and validated** policy setting.

Potential impact

Enabling this policy setting requires that you have a PKI and that your enterprise administrators have populated the Trusted Publishers store with the certificates for the allowed applications. Some older applications are not signed, and they cannot be used in an environment that is hardened with this policy setting.

You should carefully test your applications in a preproduction environment before implementing this policy setting. For information about the steps that are required to test

application compatibility, make application compatibility fixes, and sign installer packages to prepare your organization for UAC deployment, see [Understanding and Configuring User Account Control in Windows Vista](#).

Control over the applications that are installed on the desktop and the hardware that joins your domain should provide similar protection from the vulnerability that is addressed by this policy setting. Additionally, the level of protection that is provided by this policy setting is not an assurance that all rogue applications will be found.

User Account Control: Only elevate UIAccess applications that are installed in secure locations

This policy setting enforces the requirement that applications that request running with a UIAccess integrity level (by means of a marking of UIAccess=true in their application manifest), must reside in a secure location on the file system. Relatively secure locations are limited to the following directories:

- Program Files, including subdirectories
- Windows\system32
- Program Files (x86), including subdirectories for 64-bit versions of Windows



Note

The Windows operating system enforces a PKI signature check on any interactive application that requests running with a UIAccess integrity level regardless of the state of this security setting.

Possible values:

- Enabled
- Disabled

The default configuration for this policy setting is **Enabled**.

Vulnerability

UIAccess integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. When this policy setting is enabled, an application that has the UIAccess flag set to true in its manifest can interchange information with applications that are running at a higher privilege level, such as logon prompts and privilege elevation prompts. This ability is required to support accessibility features (such as screen readers) that are transmitting user interfaces to

alternative forms, but it is not required by most applications. A process that is started with UIAccess rights has the following capabilities:

- To set the foreground window.
- To drive any application window by using the SendInput function.
- To use read input for all integrity levels by using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.
- To set journal hooks.
- To use AttachThreadInput to attach a thread to a higher integrity input queue.

Countermeasure

Enable the **User Account Control: Only elevate UIAccess applications that are installed in secure locations** policy setting.

Potential impact

If the application that requests UIAccess meets the UIAccess policy setting requirements, the application can bypass most of the UIPI restrictions. If the application does not meet the security restrictions, the application is started without UIAccess rights, and it can interact only with applications at the same or lower privilege level.

User Account Control: Run all administrators in Admin Approval Mode

This policy setting determines the behavior of all UAC policies for the entire system. Admin Approval Mode and all other UAC policies are dependent on this option being enabled. Changing this policy setting requires restarting the computer.

Possible values:

- Enabled
- Disabled



Note

If this security setting is configured to **Disabled**, the Security Center notifies the user that the overall security of the operating system has been reduced.

The default configuration for this policy setting is **Enabled**.

Vulnerability

This policy setting turns UAC on or off. If this setting is disabled, UAC is not used, and any security benefits and risk mitigations that are dependent on UAC are not present on the system.

Countermeasure

Enable the **User Account Control: Run all users, including administrators, as standard users** policy setting.

Potential impact

Users and administrators must learn to work with UAC prompts and adjust their work habits to use least privilege operations.

User Account Control: Switch to the secure desktop when prompting for elevation

This policy setting determines whether the elevation request prompts appears on the interactive user desktop or the secure desktop.

Possible values:

- Enabled
- Disabled

The default configuration for this policy setting is **Enabled**.

Vulnerability

Elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malicious software.

Countermeasure

Enable the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting. The secure desktop helps protect against input and output spoofing by presenting the credentials dialog box in a protected section of memory that is accessible only by trusted system processes.

Potential impact

None. This is the default configuration.

User Account Control: Virtualize file and registry write failures to per-user locations

This policy setting enables or disables redirecting the Write failures of earlier applications to defined locations in the registry and file system. This feature mitigates those applications that historically ran as administrator and wrote runtime application data back to either %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software\.

Virtualization facilitates the running of applications that cannot run with standard user privileges. An administrator who runs only standard user applications may choose to disable this feature because it is unnecessary.

Possible values:

- Enabled
- Disabled

The default configuration for this policy setting is **Enabled**.

Vulnerability

Earlier applications might not write data to secure locations.

Countermeasure

Enable the **User Account Control: Virtualize file and registry write failures to per-user locations** policy setting.

Potential impact

None. This is the default configuration.

Threats and Countermeasures Guide: Event Log

This section of the Threats and Countermeasures Guide discusses event log settings. The event logs record events that happen on the computer. Examining the events in these logs can help you trace activity, respond to events, and keep your systems secure. Configuring these logs properly can help you manage the logs more efficiently and use the information that they provide more effectively.

Windows® 7 and Windows Server® 2008 R2 have event systems that save event log files as XML files that can be reported on and managed as part of a collective reporting schema. There are several additional log providers and categories that you can monitor.

Event Viewer in Windows 7 and Windows Server 2008 R2 tracks information in a number of logs, including:

- **Windows Logs**

This provider contains the following event logs from the operating system:

- **Application** Events in this Windows log are classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that is not necessarily significant, but it might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service.

- **Security** This Windows log contains security-related events, called "audit events," which are described as successful or failed, depending on the event, such as whether a user's attempt to log on to the Windows operating system was successful.
- **Setup** This Windows log records events that are related to installing programs and services on a computer. Computers that are configured as domain controllers display additional logs in this category.
- **System** This Windows log records system events that are sent by the Windows operating system and Windows system services. They are classified as error, warning, or information.
- **Forwarded Events** This Windows log records events that are forwarded to this log by other computers.
- **Applications and Services Logs**

The Applications and Services Log is a new category of event log provider. Each application or service that is installed on the computer can have an individual log. These logs store events from a single application or service rather than events that might have system-wide impact. This category of logs includes four subtypes for which the application or service can provide events: Administrative, Operational, Analytic, and Debug logs.

- **Administrative** Events in the Administrative channel indicate a problem and a well-defined solution that an administrator can act on. An example of an administrative event is an event that occurs when an application fails to connect to a printer. These events are well documented or they include a message that gives the reader direct instructions about what must be done to rectify the problem.
- **Operational** Events found in the Operational channel are used for analyzing and diagnosing a problem or occurrence. They can be used to trigger tools or tasks based on the problem or occurrence. An example of an operational event is an event that occurs when a printer is added or removed from a system.
- **Analytic** Events found in the Analytic channel aid in performance evaluations and troubleshooting. These events are published in high volume, so they should only be enabled and logged for limited amounts of time as part of a diagnostic process. They describe program operation and they may indicate problems that cannot be handled by user intervention.
- **Debug** Events found in the Debug channel can be used by developers to troubleshoot issues with their programs.



Note

Analytic and Debug logs are hidden and disabled by default. To use these logs, first start Event Viewer, click the **View** menu, and then select **Show Analytic and Debug Logs**.

Then select the Analytic or Debug log that you want to enable, and on the **Action** menu, click **Properties**. In the **Properties** dialog box, select **Enable logging**, and click **OK**.

Each of these logs has attributes, such as maximum log size, access rights, and retention settings and methods, which can be defined in the appropriate Event Log section in Group Policy.

Event Log Settings

You can configure the event log settings in the following location within the Group Policy Management Console:

Computer Configuration\Administrative Templates\Windows Components\Event Log Service

Subordinate folders exist for the following event logs by default:

- Application
- Security
- Setup
- System

An identical set of policy settings is available for each event log. The Setup folder has an additional policy setting that allows logging to be turned on. The following sections describe the options and issues for configuring event log settings for better system management and security.



Note

The event log Group Policy settings in Windows Server 2003 are still supported on Windows 7 and Windows Server 2008 R2. However, if the new Group Policy settings for the Event Log Service are also specified, they take precedence.

Maximum log size (KB)

This policy setting specifies the maximum sizes of the log file. An individual log file size can be specified for each of the Application, Security, Setup, and System event log channels. The user interfaces (UIs) of the Local Group Policy Editor and the Microsoft Management Console (MMC) Event Viewer snap-in allow you to enter values as large as 2 terabytes. If this setting is not configured, event logs have a default maximum size of 20 megabytes.

Although there is no simple equation to determine the best log size for a particular server or client computer, you can calculate a reasonable size by multiplying the average event size by the average number of events per month, assuming that you back up your logs on a monthly

schedule. The average event takes up about 500 bytes within each log, and the log file sizes must be a multiple of 64 KB. If you can estimate the average number of events that are generated each day for each type of log in your organization, you can determine a good size for each type of log file.

For example, if your file server generates a Security log of 5,000 events per day and you want to ensure that at least four weeks of data are available at all times, you should configure the log size to about 70 MB (calculated as 500 bytes * 5000 events per day * 28 days = 70,000,000 bytes). Then check the servers occasionally over the following four weeks to verify that your calculations are correct and that the logs retain enough events for your needs. Event log size and log wrapping should be defined to match the business and security requirements that you determined when you designed your organization's security plan.

Possible values:

- Enabled
- Disabled
- Not Configured

If you enable this policy setting, specify a user-defined value in KBs between 1,024 and 2,147,483,647, which must be a multiple of 64. If this policy setting is disabled or not configured, the maximum size of the log file is set to the local configuration value. The local administrator can change this value by using the log's **Properties** dialog box, and it defaults to 20 MBs.

Vulnerability

If you significantly increase the number of objects to audit in your organization and if you enabled the **Audit: Shut down system immediately if unable to log security audits** policy setting, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer is unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the **Audit: Shut down system immediately if unable to log security audits** policy setting that is described in [Threats and Countermeasures Guide: Security Options](#) and increase the Security log size.

Countermeasure

Enable sensible log-size policies for all computers in your organization so that legitimate users can be held accountable for their actions, unauthorized activity can be detected and tracked, and computer problems can be detected and diagnosed. [Article 957662](#) in the Microsoft Knowledge Base provides guidance for the maximum size of event logs that you should configure on your server.

Potential impact

When event logs fill to capacity, by default the computer overwrites the oldest entries with the most recent ones. To mitigate the risk of loss of older data, you can configure the computer to automatically back up the log when it becomes full.

Ideally, all specifically monitored events should be sent to a server that uses System Center Operations Manager 2007 or a similar automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, you can gather forensic information about the attacker's activities.

Log access

This policy setting determines which user accounts have access to log files and what usage rights are granted. Individual access rights can be specified for each of the Application, Security, Setup, and System event log channels.

Possible values:

- Enabled
- Disabled
- Not Configured

Enabling this setting allows you to enter a security descriptor for the log file. The security descriptor controls who can read, write, or clear the event log. You enter the security descriptor by using Security Definition Description Language (SDDL). The following example shows the default SDDL string for the Application log:

```
O:BAG:SYD:(D;; 0xf0007;;;AN) (D;; 0xf0007;;;BG) (A;; 0xf0007;;;SY) (A;; 0x5;;;BA) (A;; 0x7;;;SO) (A;; 0x3;;;IU) (A;; 0x2;;;BA) (A;; 0x2;;;LS) (A;; 0x2;;;NS)
```

In this example, the first ACE denies Anonymous Users read, write, and clear access to the log. The sixth ACE permits Interactive Users to read and write to the log. For more information about SDDL syntax and about how to construct an SDDL string, see the MSDN topic [Security Descriptor String Format](#).

If this policy setting is disabled or not configured for the Application or Setup logs, all authenticated users can write, read, and clear the log. If this policy setting is disabled or not configured for the Security log, only system software and administrators can read or clear the log.

Vulnerability

Attackers who successfully log on to a computer can learn important information about the computer if they are able to view the event logs. They could then use this information to implement additional exploits.

Countermeasure

Identify which log files are valued in your organization. The Security event log has the most restrictive default settings, but events in the Application log or Setup log may also be useful for forensic investigation. Configure the SID to match the user account that is trusted to manage and monitor those logs.

Potential impact

Users may not be able to access event log data for troubleshooting information.

Retain old events

This policy setting controls event log behavior when the log file reaches its maximum size. When this policy setting is enabled and a log file reaches its maximum size, new events are not written to the log and are lost. When this policy setting is disabled and a log file reaches its maximum size, new events overwrite old events.

Possible values:

- Enabled
- Disabled
- Not Configured



Note

Old events may or may not be retained according to the **Backup log automatically when full** policy setting. You should only configure this setting if you archive the log at scheduled intervals and you ensure that the maximum log size is large enough to accommodate the interval.

Vulnerability

Retaining old events introduces a greater risk of a denial-of-service attack by filling up the event log, and it prevents critical information about an attack from being logged due to lack of space.

Countermeasure

Configure the **Retain old events** policy setting for the policies of all four event logs to **Not Configured**. If you decide that you must retain old events logs, configure the **Backup log automatically when full** policy setting to mitigate the risk that is associated with this policy setting.

Potential impact

None. This is the default configuration.

Backup log automatically when full

This policy setting controls event log behavior when the log file reaches its maximum size, and it takes effect only if the **Retain old events** policy setting is enabled. If you enable this policy setting and the **Retain old events** policy setting is enabled, the event log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the **Retain old events** policy setting is enabled, new events are discarded and the old events are retained. When this policy setting is not configured and the **Retain old events** policy setting is enabled, new events are discarded and the old events are retained.

Possible values:

- Enabled
- Disabled
- Not Configured

Vulnerability

If you significantly increase the number of objects to audit in your organization, there is a risk that the Security log will reach its capacity and force the computer to shut down. If such a shutdown occurs, the computer is unusable until an administrator clears the Security log. To prevent such a shutdown, you can disable the **Audit: Shut down system immediately if unable to log security audits** policy setting that is described in [Threats and Countermeasures Guide: Security Options](#), and then increase the Security log size.

Countermeasure

If you enable the **Retain old events** policy setting and enable and specify a **Maximum log size** policy setting, you should also enable the **Backup log automatically when full** policy setting to ensure that all valued events are recorded and retained and that there is no loss of service due to lack of storage for event logs.

Ideally, all significant events are sent to a monitoring server that uses Operations Manager 2007 or other automated monitoring tool.

Potential impact

Computers must have enough local storage to create a backup file or access to a network storage location to create the backup file. If the events cannot be logged because the disk is full or unavailable, the events are lost. Security events are the exception to this rule if you have enabled the **Audit: Shut down system immediately if unable to log security audits** policy setting, in which case the affected computer shuts down.

Additional references

The following links provide additional information about event logging in Windows 7 and Windows Server 2008 R2:

- For more information about SDDL, see [Security Descriptor String Format](#).
- For more information about events in Windows 7 and Windows Server 2008 R2, see [Event Viewer and Resulting Internet Communication in Windows 7 and Windows Server 2008 R2](#).

Threats and Countermeasures Guide: System Services

System services are programs that load automatically as part of an application's startup process or as the operating system's startup process to support the tasks that are required of the operating system. Services have been an attractive target for creators of malicious software, such as viruses, who want to attack the Windows® operating systems. There are a number of reasons for this situation:

- Services are typically long running. Often, they start when the system starts and stop when it shuts down.
- Services are often network facing, making them especially vulnerable to remote attacks.
- Services typically run in a high-privilege account such as Local System.

To address this situation, the design of the core services was modified to accomplish the following goals:

- Limiting access to services by user applications. Session 0 isolation requires services and user applications to run in separate sessions.
- "Hardening" services to limit the ability of a compromised service to damage a system. There are two complementary ways to accomplish this goal:
 - Running with least privilege allows services to run with only the privileges that they require.
 - Isolating services from other services or applications by using a unique service identity that can restrict access to service resources. For example, service isolation allows an antivirus service to maintain exclusive access to its signature definition files.

This section of this guide identifies the function and purpose of commonly used services and explains which services are enabled in Windows Server® 2008 R2 and Windows 7.

When you first install Windows Server 2008 R2 or Windows 7, some services are installed and configured to run by default when the computer starts. There are fewer services installed by default in a Server Core installation option of the Windows Server 2008 R2 operating system than in the full installation option of Windows Server 2008 R2. In addition, Server Core installation supports a limited subset of roles and services, and it has a smaller attack surface than a full installation.

By default, Windows Server 2008 R2 is installed without any server roles enabled and with a minimum number of services running. You should install only the server roles and features that

are required for the workload of each server. Even with this reduction in default services, your server may not need all of the services that are installed by default. You should disable any unneeded services to enhance security in your environment.

Windows services overview

A service must log on to access resources and objects in the operating system, and most services are not designed to have their default logon accounts changed. If you change the default account, it is likely that the service will fail. If you select an account that does not have the **Log on as a service** user right, the Services snap-in automatically grants that user right to the account. However, this configuration does not guarantee that the service will start. The Windows operating systems include three local accounts that are used as the logon accounts for various system services:

- **Local System account.** The Local System account is a powerful account that has full access to the computer and represents the computer on the network. If a service uses the Local System account to log on to a domain controller, that service has access to the entire domain. Some services are configured by default to use the Local System account, and this should not be changed. The Local System account does not have a user-accessible password.
- **Local Service account.** The Local Service account is a built-in account that is similar to an authenticated user account. It has the same level of access to resources and objects as members of the Users group. This limited access helps protect a computer if individual services or processes are compromised. Services that use the Local Service account access network resources as a null session with anonymous credentials. The name of this account is NT AUTHORITY\Local Service, and it does not have a user-accessible password.

The Local Service account supports the following privileges by default.

| Privilege | Description |
|-------------------------------|--|
| SeAssignPrimaryTokenPrivilege | Replace a process-level token |
| SeIncreaseQuotaPrivilege | Adjust memory quotas for a process |
| SeAuditPrivilege | Generate security audits |
| SeChangeNotifyPrivilege | Bypass traverse checking (This privilege is inherited through membership in the Everyone group.) |
| SeNetworkLogonRight | Access this computer from the network (This privilege is inherited through membership in the Everyone group.) |
| SeBatchLogonRight | Log on as a batch job |

- Network Service account.** The Network Service account is also a built-in account that is similar to an authenticated user account. Like the Local Service account, it has the same level of access to resources and objects as members of the Users group, which helps to protect the computer. Services that use the Network Service account access network resources with the credentials of the computer account. The name of the account is NT AUTHORITY\Network Service, and it does not have a user-accessible password.

The Network Service account supports the following privileges by default.

| Privilege | Description |
|-------------------------------|--|
| SeAssignPrimaryTokenPrivilege | Replace a process-level token |
| SeIncreaseQuotaPrivilege | Adjust memory quotas for a process |
| SeAuditPrivilege | Generate security audits |
| SeChangeNotifyPrivilege | Bypass traverse checking (This privilege is inherited through membership in the Everyone group.) |
| SeNetworkLogonRight | Access this computer from the network (This privilege is inherited through membership in the Everyone group.) |
| SeInteractiveLogonRight | Log on as a service |
| SeImpersonatePrivilege | Impersonate a client after authentication |

Services are attractive targets for creators of malicious software such as viruses because they usually run in the background and average users do not interact with them, they interact with the application that uses them. Ideally, service developers should limit the risk that is presented by misuse of a service by developing services that run using a lower-privilege account such as the Local Service account or the Network Service account. However, many services require some privileges that only the Local System account supports.

If you are developing a service that requires a privilege provided by the Local System account, it should be developed to run with least privilege to reduce the potential attack surface presented by malicious use of the service. Running with least privilege means that services are not required to retain the default set of privileges that are supported by a standard account. Instead, service developers can select an account that has the privileges they require and then remove all other unnecessary privileges. Running with least privilege can be used for any type of service account (Local Service, Network Service, Local System, a domain, or a local account).

When a service starts, the required privileges are registered with the Service Control Manager (SCM), which grants a set of privileges that is stored in the process token for the service.

The privilege check uses one of the following methods:

- For stand-alone services, the SCM checks the list of required privileges against the process token. Any that were not specified as required are removed from the token.
- For shared-process services, such as services that are hosted in svchost, the list of privileges is a compilation of the required privileges for all services in the group. The only privileges that the SCM removes from the process token are those that no member of the group has specified as required.
- If a service does not specify a required set of privileges, by default the SCM assumes that the service requires all of the privileges that are associated with the account. This assures backward compatibility. However, if a service group contains a mixture of services with defined privileges and without defined privileges, the entire group uses the privileges that are associated with the account.

If a service requires privileges that are not in the process token, the SCM does not start the service. For example, a process that is part of a service group running under the Network Service account could specify SeLoadDriverPrivilege as a required privilege. However, if other processes in the group did not specify required privileges, the process token for the group contains only those privileges that are defined for the Network Service account. SeLoadDriverPrivilege is not supported by a Network Service process token, so the start attempt for that process fails. Administrators must understand this issue when they make configuration changes such as changing the service image of a shared-process service while the target service process is running. The service can start only if the target service process supports the specified privileges.

Service isolation

Many services require access to objects that are available only to high-privilege accounts. For example, a service might have to write to a registry key that provides write access to administrators only. Services typically gained access to such objects by running in a high-privilege account such as the Local System account or by weakening the security on the objects to allow access by services that are running in a generic lower-privilege account.

These approaches increased the risk that an attacker or malicious software could gain control of the system. The only way for an administrator to mitigate this risk was to create an account specifically for the service and allow access to the objects only for that account. However, this approach created manageability issues, most notably password management, because the administrator no longer had the advantages of using built-in operating system accounts.

Service isolation mitigates this issue by providing services a way to access specific objects without having to run in a high-privilege account or weaken the objects' security protection. For example, service isolation allows an antivirus service to run in a lower-privilege account than the

Local System account but still maintain complete access to its signature definition files or registry keys that would normally be accessible to administrators only.

A service isolates an object for its exclusive use by securing the resource—such as file or registry key access—with an access control entry that contains a service security ID (SID). This ID is referred to as a per-service SID. A per-service SID is derived from the service's name and it is unique to that service.

After a SID has been assigned to a service, the service owner can modify the required objects' access control lists (ACLs) to allow access to the SID. For example, a registry key in `HKEY_LOCAL_MACHINE\SOFTWARE` would normally be accessible only to services with administrative privileges. By adding the per-service SID to the key's ACL, the service can run in a lower-privilege account but still have access to the key.

If a per-service SID is enabled, it is added to the service's process token. To be added to the process token, a per-service SID must be enabled when the service's process is started. If a process hosts multiple services with enabled SIDs, all the SIDs are added to the process token. Per-service SIDs also allow a process token to be converted to a restricted token by adding one or more SIDs to the restricted token list.

Restricted SIDs

A per-service SID provides good isolation and allows the service to run in a lower-privilege account. However, because the process token also contains the SID for the account, a per-service SID does not prevent the service from accessing other resources that are accessible to the account. Consider the following scenario:

Service X runs in the Local Service account and has a service SID enabled. In addition to having access to objects that have specifically granted this service access (by using the per-service SID), it also has access to all objects that grant access to the Local Service account. As a result, if this service was compromised, the attacker could cause damage by accessing the resources that are not related to the service.

To mitigate this problem and reduce the damage potential of compromised services, the Windows operating system uses a hybrid approach that combines write-restricted tokens and per-service SIDs to provide restricted SIDs for services.

When a service enables a restricted SID, the per-service SID of that service is added to both the normal and restricted SID lists of the write-restricted service process token. This ensures that the service can write only to objects that have explicitly granted write access to one of the SIDs in the restricted list. Returning to the preceding example, by enabling restricted SIDs, service X

can no longer write to any objects that grant write access to the Local Service account because those objects do not explicitly grant write access to the per-service SID of service X.



Important

If you change the default service settings, key services may not run correctly. It is especially important to use caution if you change the **Startup type** and **Log on as** settings of services that are configured to start automatically.

System service settings

System services are described differently from the other settings in this guide because the vulnerability, countermeasure, and potential impact statements are almost identical for all services. The following are some general rules for managing system services vulnerabilities, countermeasures, and potential impacts.

For each system service, you can assign a service startup type. The possible values for these settings are:

- **Automatic.** Service automatically starts when the computer is restarted.
- **Automatic (Delayed start).** Service starts automatically when the computer is restarted, but delays the start of the service until after higher priority services and drivers are started.
- **Manual.** Service does not start until a program starts it or it is explicitly started by the user.
- **Disabled.** The service cannot be started.
- Not Defined

You can use the **sc config** command to set the service startup type from a Command Prompt window. For more information, see [sc config](#).

Vulnerability

Any service or application is a potential point of attack.



Important

Additional services that you enable may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.

Countermeasure

Disable all unnecessary services. On your server, install only the server roles and features that are required to support the server's workload.

Do not set permissions on service objects

There are graphical user interface (GUI)–based tools that you can use to edit services. We recommend that you not alter the permissions on the services that are included with the operating system because the default permissions are already quite restrictive.

To modify the properties of system services, you can use the following tools as appropriate:

- Use the Security Configuration Wizard that is provided with Windows Server 2008 R2. We recommend this approach when you must configure services and network port filters for various server roles.
- Run the Security Templates snap-in or Local Group Policy Editor on a server that is running Windows Server 2008 R2. We recommend this approach when you must configure services for security templates or Group Policy settings that are applied to Windows 7.

Potential impact

If some services (such as the Security Accounts Manager) are disabled, you cannot restart the computer. If other critical services are disabled, the computer may be unable to authenticate with domain controllers. If you want to disable some system services, you should test the changed settings on nonproduction computers before you change them in a production environment.

Descriptions of system services

The following subsections describe the services that are included with Windows Server 2008 R2 and Windows 7.

- [ActiveX Installer](#)
- [Adaptive Brightness](#)
- [Application Experience](#)
- [Application Host Helper Service](#)
- [Application Identity](#)
- [Application Information](#)
- [Application Layer Gateway Service](#)

- [Application Management](#)
- [ASP.NET State Service](#)
- [Background Intelligent Transfer Service \(BITS\)](#)
- [Base Filtering Engine](#)
- [BitLocker Drive Encryption Service](#)
- [Block Level Backup Engine Service](#)
- [Bluetooth Support Service](#)
- [BranchCache](#)
- [Certificate Propagation](#)
- [Client for NFS](#)
- [Certificate Services](#)
- [Cluster Service](#)
- [CNG Key Isolation](#)
- [COM+ Event System](#)
- [COM+ System Application](#)
- [Computer Browser](#)
- [Credential Manager](#)
- [Cryptographic Services](#)
- [DCOM Server Process Launcher](#)
- [Desktop Window Manager Session Manager](#)
- [DHCP Client](#)
- [DHCP Server](#)
- [Diagnostic Policy Service](#)
- [Diagnostic Service Host](#)
- [Diagnostic System Host](#)
- [Disk Defragmenter](#)

- [Distributed File System](#)
- [Distributed File System Replication](#)
- [Distributed Link Tracking Client](#)
- [Distributed Link Tracking Server](#)
- [Distributed Transaction Coordinator](#)
- [DNS Client](#)
- [DNS Server](#)
- [Encrypting File System](#)
- [Extensible Authentication Protocol](#)
- [Fax Service](#)
- [Function Discovery Provider Host](#)
- [Function Discovery Resource Publication](#)
- [Group Policy Client](#)
- [Group Policy](#)
- [Health Key and Certificate Management](#)
- [HomeGroup Listener](#)
- [HomeGroup Provider](#)
- [HTTP SSL](#)
- [Human Interface Device Access](#)
- [IIS Admin Service](#)
- [IKE and AuthIP IPsec Keying Modules](#)
- [Indexing Service](#)
- [Interactive Services Detection](#)
- [Internet Connection Sharing](#)
- [Intersite Messaging](#)
- [IP Helper](#)

- [IPsec Policy Agent](#)
- [KtmRm for Distributed Transaction Coordinator](#)
- [Link-Layer Topology Discovery Mapper](#)
- [LPD Service](#)
- [Media Center Extender Service](#)
- [Message Queuing](#)
- [Message Queuing Triggers](#)
- [Microsoft .NET Framework NGEN](#)
- [Microsoft FTP Service](#)
- [Microsoft Software Shadow Copy Provider](#)
- [Microsoft iSCSI Initiator Service](#)
- [Multimedia Class Scheduler](#)
- [Microsoft Fibre Channel Platform Registration Service](#)
- [Net.Msmq Listener Adapter](#)
- [Net.Pipe Listener Adapter](#)
- [Net.Tcp Listener Adapter](#)
- [Net.Tcp Port Sharing Service](#)
- [Netlogon](#)
- [Network Access Protection Agent](#)
- [Network Connections](#)
- [Network List Service](#)
- [Network Location Awareness](#)
- [Network Store Interface Service](#)
- [Offline Files](#)
- [Parental Controls](#)
- [Peer Name Resolution Protocol](#)

- [Peer Networking Grouping](#)
- [Peer Networking Identity Manager](#)
- [Performance Counter DLL Host](#)
- [Performance Logs & Alerts](#)
- [Plug and Play](#)
- [PnP-X IP Bus Enumerator](#)
- [PNRP Machine Name Publication Service](#)
- [Portable Device Enumerator Service](#)
- [Power](#)
- [Print Spooler](#)
- [Problem Reports and Solutions Control Panel Support](#)
- [Program Compatibility Assistant Service](#)
- [Protected Storage](#)
- [Quality Windows Audio Video Experience](#)
- [Remote Access Auto Connection Manager](#)
- [Remote Access Connection Manager](#)
- [Remote Desktop Configuration](#)
- [Remote Desktop Services](#)
- [Remote Desktop Services UserMode Port Redirector](#)
- [Remote Procedure Call \(RPC\)](#)
- [Remote Procedure Call \(RPC\) Locator](#)
- [Remote Registry](#)
- [RIP Listener](#)
- [Resultant Set of Policy Provider](#)
- [Routing and Remote Access](#)
- [RPC Endpoint Mapper](#)

- [SeaPort](#)
- [Secondary Logon](#)
- [Secure Socket Tunneling Protocol Service](#)
- [Security Accounts Manager](#)
- [Security Center](#)
- [Server](#)
- [Shell Hardware Detection](#)
- [Simple TCP/IP Services](#)
- [Smart Card](#)
- [Smart Card Removal Policy](#)
- [SNMP Service](#)
- [SNMP Trap](#)
- [Software Protection](#)
- [Special Administration Console Helper](#)
- [SPP Notification Service](#)
- [SSDP Discovery](#)
- [Storage Service](#)
- [Superfetch](#)
- [System Event Notification Service](#)
- [Tablet PC Input Service](#)
- [Task Scheduler](#)
- [TCP/IP NetBIOS Helper](#)
- [Telephony](#)
- [Themes](#)
- [Thread Ordering Server](#)
- [TPM Base Services](#)

- [UPnP Device Host](#)
- [User Profile Service](#)
- [Virtual Disk Service](#)
- [Volume Shadow Copy](#)
- [WLAN AutoConfig](#)
- [WMI Performance Adapter](#)
- [WWAN AutoConfig](#)
- [Web Management Service](#)
- [WebClient](#)
- [Windows Audio](#)
- [Windows Audio Endpoint Builder](#)
- [Windows Backup](#)
- [Windows Biometric Service](#)
- [Windows CardSpace](#)
- [Windows Color System](#)
- [Windows Connect Now - Config Registrar](#)
- [Windows Defender](#)
- [Windows Driver Foundation - User-mode Driver Framework](#)
- [Windows Error Reporting Service](#)
- [Windows Event Collector](#)
- [Windows Event Log](#)
- [Windows Firewall](#)
- [Windows Font Cache Service](#)
- [Windows Image Acquisition \(WIA\)](#)
- [Windows Installer](#)
- [Windows Internet Name Service \(WINS\)](#)

- [Windows Management Instrumentation](#)
- [Windows Media Center Receiver Service](#)
- [Windows Media Center Scheduler Service](#)
- [Windows Media Player Network Sharing Service](#)
- [Windows Modules Installer](#)
- [Windows Presentation Foundation Font Cache](#)
- [Windows Process Activation Service](#)
- [Windows Remote Management \(WS-Management\)](#)
- [Windows Search](#)
- [Windows Time](#)
- [Windows Update \(Automatic Updates\)](#)
- [Wired AutoConfig](#)
- [Workstation](#)
- [World Wide Web Publishing Service](#)



Note

If a service is not started, other services that depend on that service also fail to start. Therefore, if you change the status of one service, you may affect other seemingly unrelated services. Applications and programs may also create dependencies on services that are different from the default configuration documented in the following service descriptions. To check the dependencies for a service, in the **Services** Control Panel or the MMC snap-in (services.msc), click **Properties**, and then click the **Dependencies** tab.

ActiveX Installer

The ActiveX® Installer (AxInstSV) service provides User Account Control validation for the installation of ActiveX controls from the Internet, and it enables managing the ActiveX control installation that is based on Group Policy settings. This service's startup type is **Manual**, so it will start when requested by an application. If this service is disabled, the installation of ActiveX controls will behave according to the default browser settings. When the ActiveX Installer service is started in its default configuration, it logs on by using the Local System account.

This service is included in all versions of Windows 7, but it is not included in Windows Server 2008 R2.

For more information about working with this service, see [Administering the ActiveX Installer Service in Windows 7](#).

The ActiveX Installer service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Adaptive Brightness

The Adaptive Brightness (SensrSvc) service monitors ambient light sensors to detect changes in ambient light and adjust the display brightness. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions. The default startup type for this service is **Manual**. When the Adaptive Brightness service is started in its default configuration, it logs on by using the Local Service account. This service is not dependent on any other system service, nor is any service dependent on it.

This service is supported in all versions of Windows 7 except Windows 7 Starter operating system. This service is not included in Windows Server 2008 R2.

For more information about working with this service, see [Windows 7 Brightness Control for Integrated Displays](#).

Application Experience

The Application Experience (AELookupSvc) service is a part of the Application Compatibility Administrator. It processes application compatibility lookup requests for applications as they start, provides support for computers that are running programs in compatibility mode, reports on compatibility issues, and automatically applies software updates to programs.

The Application Experience service must be active for application compatibility software updates to be applied. You cannot customize this service; the operating system uses it internally. This service does not use any network, Internet, or Active Directory® Domain Services (AD DS) resources.

If you disable the Application Experience service, the service continues to run, but no calls are made to the service. You cannot stop the actual process.

This service is installed by default and its startup type is **Manual**. When the Application Experience service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Application Host Helper Service

The Application Host Helper Service (AppHostSvc) provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, the IIS configuration history feature will not work, and you will be unable to use Application Pool-specific access control entries to lock down files or directories.

This service is not installed by default. After it is installed, the Application Host Helper Service startup type is **Automatic**. When the Application Host Helper Service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Application Identity

The Application Identity (AppIDSvc) service determines and verifies the identity of an application. Disabling this service will prevent AppLocker™ from being enforced. This service is installed by default and its startup type is **Manual**. When the Application Identity service is started in its default configuration, it logs on by using the Local Service account.

The Application Identity service is dependent on the following system components:

- AppID Driver
- Flt Mgr
- System Attribute Cache
- Cryptographic Services
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Application Information

The Application Information (Appinfo) service facilitates running interactive applications with additional administrative privileges. If this service is stopped, users cannot start applications

with the additional administrative privileges that they may require to perform certain user tasks. For example, if this service is disabled, system tools like Services and Regedit cannot run.

To enable this service after it has been disabled, you must start the computer in Safe Mode to get access to the Services snap-in console.

The default startup type for this service is **Manual** and it is started by applications that request additional privileges. When the Application Information service is started in its default configuration, it logs on by using the Local System account by default.

The Application Information service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- User Profile Service

Application Layer Gateway Service

The Application Layer Gateway Service (ALG) is a subcomponent of the Windows networking subsystem. It provides support for non-Microsoft plug-ins to allow network protocols to pass through the firewall and work behind Internet Connection Sharing. This service is installed by default and its startup type is **Manual**.

When the Application Layer Gateway Service is started in its default configuration, it logs on by using the Local Service account.

This service is not dependent on any other system service, nor is any service dependent on it.

The following table identifies the application protocol, network protocol, and ports that are used by the Application Layer Gateway Service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
| FTP Control | TCP | 21 |

Application Management

The Application Management (AppMgmt) service provides software installation services such as Assign, Publish, and Remove. It processes requests to enumerate, install, and remove

applications that are deployed through an organization's network by using Group Policy. When you use **Get Programs** from the Windows Control Panel to install programs from the network on a domain-joined computer, Windows calls this service to retrieve the list of deployed applications on your network. The service is also called when you use Control Panel to remove an application, or when a component (such as the shell) makes an installation request for an application to handle a file name extension, Component Object Model (COM) class, or programmatic identifier (<ProgID> key) that is not present on the computer. The service is started by the first call, and it does not stop after it is started.

If the Application Management service stops or if you disable it, users cannot install, remove, or enumerate applications that are deployed in AD DS. This service is installed by default, but it is not started unless an application requests it.

When the Application Management service is started in its default configuration, it log on by using the Local System account.

This service is available on Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise in addition to all versions of Windows Server 2008 R2. It is not available on Windows 7 Starter, Windows 7 Home Basic, or Windows 7 Home Premium.

This service is not dependent on any other system service, nor is any service dependent on it.

ASP.NET State Service

The ASP.NET State Service (aspnet_state) provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.

This service is not installed by default on Windows 7 or Windows Server 2008 R2. Once installed, its startup type is **Manual**.

When the ASP.NET State Service is started in its default configuration, it logs on by using the Network Service account.

This service is available on Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise in addition to all versions of Windows Server 2008 R2. It is not available on Windows 7 Starter or Windows 7 Home Basic.

This service is not dependent on any other system service, nor is any service dependent on it.

The following table identifies the application protocol, network protocol, and ports used by the ASP.NET State Service:

| Application protocol | Network protocol | Ports |
|-----------------------|------------------|-------|
| ASP.NET Session State | TCP | 42424 |

Background Intelligent Transfer Service

The Background Intelligent Transfer Service (BITS) is a background file-transfer mechanism and queue manager. BITS transfers files asynchronously between a client and an HTTP server. By default, requests to BITS are submitted and the files are transferred through otherwise idle network bandwidth so that other network-related activities, such as browsing, are not affected.

BITS suspends the transfer if a connection is lost or if the user logs off. The BITS connection is persistent and transfers information while the user is logged off, across network disconnects, and during computer restarts. When the user logs on, BITS resumes the user's transfer job.

BITS uses a queue to manage file transfers. You can prioritize transfer jobs within the queue and specify whether the files are transferred in the foreground or background. Background transfers are optimized by BITS, which increases and decreases (or throttles) the rate of transfer, based on the amount of idle network bandwidth that is available. If a network application begins to consume more bandwidth, BITS decreases its transfer rate to preserve the user's interactive experience.

BITS provides one foreground and three background priority levels that you can use to prioritize transfer jobs. Higher priority jobs preempt lower priority jobs. Jobs at the same priority level share transfer time, and round-robin scheduling prevents blockage of the transfer queue by a large job. Lower priority jobs do not receive transfer time until all higher priority jobs are complete or in an error state.

This service is installed by default and its startup type is **Manual**. When the Background Intelligent Transfer Service is started in its default configuration, it logs on by using the Local System account.

If BITS stops, features such as Windows Update cannot automatically download programs and other information. This functionality also means that the computer cannot receive automatic updates from the organization's Windows Server Update Services server if one has been configured through Group Policy. If you disable this service, any services that explicitly depend on it fail to transfer files unless they have a fail-safe mechanism to transfer files directly through other methods.

BITS is dependent upon the following system components:

- COM+ Event System
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Base Filtering Engine

The Base Filtering Engine (BFE) service manages firewall and IPsec policies and implements user-mode filtering. Stopping or disabling the BFE service significantly reduces the security of the system and results in unpredictable behavior in IPsec management and firewall applications.

The BFE is the core of the Windows Filtering Platform in Windows 7 and Windows Server 2008 R2. This service is installed by default and its startup type is **Automatic**. When the Base Filtering Engine service is started in its default configuration, it logs on by using the Local Service account.

The BFE service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following components are dependent upon the BFE service:

- Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) IPsec Keying Modules
- Internet Connection Sharing (ICS)
- IPsec Policy Agent
- Routing and Remote Access
- Windows Firewall

This service should not be disabled.

BitLocker Drive Encryption Service

The BitLocker™ Drive Encryption Service (BDESVC) allows BitLocker to prompt users for various actions when they access their hard disk drives and it supports unlocking BitLocker-protected drives automatically without user interaction. Additionally, the service supports storing recovery

information to Active Directory Domain Services, if available. If necessary, it ensures that the most recent recovery certificates are used. Stopping or disabling the service prevents users from using these features of BitLocker.

This service is installed by default and its startup type is **Manual**. When the BitLocker Drive Encryption Service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Block Level Backup Engine Service

The Block Level Backup Engine Service (wbengine) performs block-level backup and recovery of data. This service is used by the **Backup and Restore** feature in the Control Panel of Windows 7 and by the Windows Server Backup feature of Windows Server 2008 R2. It allows for backups to occur at the hard disk drive level, instead of by files, and it uses a process similar to disk imaging.

This service is installed by default and its startup type is **Manual**. When the Block Level Backup Engine Service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Bluetooth Support Service

The Bluetooth Support Service (bthserv) supports the discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated. If Bluetooth devices are not used with the computer, this service can be disabled.

This service is installed by default and its startup type is **Manual**. When the Bluetooth Support Service is started in its default configuration, it logs on by using the Local Service account.

The Bluetooth Support Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

BranchCache

The BranchCache™ (PeerDistSvc) service caches network content from peer computers on the local subnet. This enables clients in a branch office to securely retrieve files that are cached locally. If this service is stopped or disabled, remote computers will need to connect directly to host servers to retrieve data.

This service is installed by default on computers running Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise, and its startup type is **Manual**. When the BranchCache service is started in its default configuration, it logs on by using the Network Service account.

The Branch Cache service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

BranchCache is a feature in Windows 7 and Windows Server 2008 R2. For more information, see the [BranchCache technology center](#).

Certificate Propagation

The Certificate Propagation (CertPropSvc) service propagates certificates from smart cards to resources that request them. The Certification Propagation service applies when a user is logged-on and inserts a smart card into a reader that is attached to the computer. The certificates are read from the smart card and added to the user's personal store by the service.

If the Group Policy setting "Turn on root certificate propagation from smart card" is enabled, Root Certificates are also propagated to the machine root trust store. Root certificate propagation is responsible for the following specific smart card deployment scenarios, where public key infrastructure (PKI) trust has not yet been established:

- Joining the domain
- Accessing a network remotely

In both cases, the computer is not joined to a domain, and therefore, trust is not being managed by Group Policy. The objective is to authenticate to a remote server (the domain controller or the RADIUS server), and root certificate propagation provides the ability to use the smart card to include the missing trust chain.

When a user inserts a smart card, the Certificate Propagation service copies any root certificates on the card to the **Smart Card Trusted Roots** certificate stores on the local computer. This process establishes a trust relationship with the organization.

This service is installed by default and its startup type is **Manual**. However, if you have deployed smart cards as part of your authentication policy, we recommend that you configure this setting with the **Automatic** startup type. When started in the default configuration it will log on using the Local System account.

The Certification Propagation service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Client for NFS

The Client for NFS (NfsClnt) service enables the computer to access files in network file system (NFS) shared folders, and it is part of the Services for UNIX support in Windows 7 and Windows Server 2008 R2.

This service is not installed by default on Windows 7. It is installed by default on Windows Server 2008 R2. In both operating systems, its startup type is by default **Manual**.

When the Client for NFS service is started in its default configuration, it logs on by using the Network Service account.

This service is available on Windows 7 Ultimate and Windows 7 Enterprise, in addition to all versions of Windows Server 2008 R2.

Certificate Services

The Certificate Services service supports the Active Directory Certificate Services (AD CS) server role as part of Windows Server 2008 R2 to enable a business to act as its own certification authority (CA). It issues and manages digital certificates for smart card logon and for applications such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), Encrypting File System (EFS), IPsec.

The AD CS server role is not installed by default. Administrators must install it through Server Manager, at which time the Certificate Services role service is also installed. If Certificate Services stops or if you disable it after installation, certificate requests are not accepted and

certificate revocation lists (CRLs) and delta CRLs are not published. If the service stops long enough for CRLs to expire, existing certificates fail to validate.

Certificate Services relies on RPC and on DCOM to communicate with clients by using random TCP ports that are higher than port 1024.

Certificate Services is not supported on a Server Core installation of Windows Server 2008, but it is supported on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocol, network protocol, and ports used by Certificate Services:

| Application protocol | Network protocol | Ports |
|-----------------------------------|------------------|---|
| RPC | TCP | 135 |
| Randomly allocated high TCP ports | TCP | Random port number between 1024 and 65535 |

Cluster Service

The Cluster Service (ClusSvc) supports the Failover Clustering feature in nextrefserver_7 that controls server cluster operations and manages the cluster database. A cluster is a collection of independent computers that work together to provide load-balancing and failover support. Applications that can run on a cluster, such as Microsoft Exchange Server and Microsoft SQL Server, use the cluster to present a single virtual computer to users.

The cluster software spreads data and computation tasks among the nodes of the cluster. When a node fails, other nodes provide the services and data that were formerly provided by the missing node. When a node is added or repaired, the cluster software assigns some data and computation tasks to that node.

There are two types of cluster solutions for the Windows operating systems that support different application styles: server clusters and Network Load Balancing (NLB) clusters. Server clusters provide a highly available environment for applications that must run reliably for long periods of time (such as databases or file servers), and they provide failover support with tightly integrated cluster management. NLB clusters provide a highly available and highly scalable

environment for other types of applications such as public-facing Web servers, and balance the client requests among a set of identical servers.

The Cluster Service is not installed or enabled by default. If the Cluster Service stops after it is installed, clusters are unavailable.

The Cluster Service is an optional feature on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocol, network protocol, and ports that are used by the Cluster Service:

| Application protocol | Network protocol | Ports |
|-----------------------------------|------------------|---|
| Cluster Services | UDP | 3343 |
| RPC | TCP | 135 |
| Cluster administrator | UDP | 137 |
| Randomly allocated high UDP ports | UDP | Random port number between 1024 and 65535 |

CNG Key Isolation

The CNG Key Isolation (xxx) service is hosted in the Local Security Authority (LSA) process as part of system cryptography support. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC).

Common Criteria is an international standard (ISO/IEC 15408) for computer security. It is based on a framework in which computer system users can specify their security requirements, vendors can then implement and make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. This provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard manner.

The CNG Key Isolation service stores and uses long-lived keys in a secure process that complies with Common Criteria requirements. To comply with Common Criteria requirements, the long-

lived keys must be isolated so that they are never present in the application process. Cryptography Next Generation (CNG) currently supports storing asymmetric private keys by using the Microsoft software key storage provider (KSP) that is included in Windows Server 2008 R2 and Windows 7, and installed by default.

Key isolation is enabled by default in Windows Server 2008 R2 and Windows 7. Also, non-Microsoft KSPs are not loaded in the key isolation service (which is the Local Security Authority, or LSA, process). Only the Microsoft KSP is loaded in the key isolation service.

The LSA process is used as the key isolation process to maximize performance. All access to private keys goes through the key storage router, which exposes a comprehensive set of functions for managing and using private keys.

CNG stores the public portion of the stored key separately from the private portion. The public portion of a key pair is maintained in the key isolation service, and it is accessed by using lightweight remote procedure call (LRPC). The key storage router uses LRPC when calling into the key isolation process. All access to private keys goes through the private key router, and it is audited by CNG.

This service is installed by default and its startup type is **Manual**.

When the CNG Key Isolation service is started in its default configuration, it logs on by using the Local System account.

The CNG Key Isolation service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following components are dependent upon the CNG Key Isolation service:

- Extensible Authentication Protocol
- Wired AutoConfig
- WLAN AutoConfig

COM+ Event System

The COM+ Event System (EventSystem) service provides automatic event distribution to COM components that subscribe to it. COM+ events extend the COM+ programming model to support late-bound events or method calls between the publisher or subscriber and the event

system. The event system notifies event consumers as information becomes available, and it does not repeatedly poll the server.

The COM+ Event System service handles most of the event semantics for the publisher and the subscriber. Publishers offer to publish event types, and subscribers request event types from specific publishers. Subscriptions are maintained outside the publisher and the subscriber, and they are retrieved when needed, which simplifies the programming model for both. The subscriber is not required to contain the logic to build subscriptions—it is possible to build a subscriber as easily as a COM component. The life cycle of the subscription is separate from that of the publisher or the subscriber. You can build subscriptions before the subscriber or publisher is activated.

This service is installed by default and its startup type is **Automatic**. When started in its default configuration it logs on by using the Local Service account. When the COM+ Event System services stops, the System Event Notification service closes and cannot provide logon and logoff notifications. The Volume Shadow Copy Service, which is needed for Windows Backup and backup applications that rely on the Windows Backup API, also requires this service.

The COM+ Event System service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following components are dependent upon the COM+ Event System service:

- Background Intelligent Transfer Service
- COM+ System Application
- SPP Notification Service
- System Event Notification Service

COM+ System Application

The COM+ System Application (COMSysApp) service manages the configuration and tracking of COM+ based components. If this service stops, most COM+ based components do not function properly. The Volume Shadow Copy Service, which is needed for Windows Backup and backup applications that rely on the Windows Backup API, requires this service.

This service is installed by default and its startup type is **Manual**. When started in its default configuration it logs on by using the Local System account.

The COM+ System Application service is dependent upon the following system components:

- COM+ Event System
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- System Event Notification Service

Computer Browser

The Computer Browser (Browser) service maintains an up-to-date list of computers on your network, and it supplies the list to programs that request it. The Computer Browser service is used by Windows-based computers that must view network domains and resources. Computers that are designated as browsers maintain browse lists, which contain all shared resources that are used on the network.

There are several roles that a computer might perform in a browsing environment. Under some conditions, such as failure or shutdown of a computer that is designated for a specific browser role, browsers or potential browsers may change to a different operational role.

On Windows 7-based computers, the Computer Browser service is installed by default and its startup type is **Manual**. On computers running Windows Server 2008 R2, it is disabled. When the Computer Browser service is started in its default configuration, it logs on by using the Local System account. If it stops, the browser list is not updated or maintained.

The Computer Browser service is dependent upon the following system components:

- Server
- Security Accounts Manager
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Server SMB 1.xxx Driver
- Server SMB 2.xxx Driver
- srvnet
- Workstation

- Browser Support Driver
- Network Store Interface Service
- NSI proxy service driver
- SMB 1.x MiniRedirector
- SMB 2.0 MiniRedirector
- SMB MiniRedirector Wrapper and Engine
- Redirected Buffering Sub System
- Mup

The following table identifies the application protocol, network protocols, and ports used by the Computer Browser service:

| Application protocol | Network protocol | Ports |
|--------------------------|------------------|-------|
| NetBIOS Datagram Service | UDP | 138 |
| NetBIOS Name Resolution | UDP | 137 |
| NetBIOS Session Service | TCP | 139 |

Credential Manager

The Credential Manager (VaultSvc) service provides secure storage and retrieval of credentials to users, applications, and security service packages.

This service is installed by default and its startup type is **Manual**. When started in its default configuration, it logs on by using the Local System account.

The Credential Manager service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the Credential Manager service.

- Windows Biometric Service

Cryptographic Services

The Cryptographic Services (CryptSvc) service provides key-management services for the computer. Cryptographic Services is composed of the following management services:

- **Catalog Database Service.** This service adds, removes, and looks up catalog files, which are used to sign all the files in the operating system. Windows File Protection (WFP), Driver Signing, and setup use this service to verify signed files. You cannot stop this service during setup. If the service stops after setup, it restarts when it is requested by an application.
- **Protected Root Service.** This service adds and removes Trusted Root Certification Authority certificates. The service displays a service message box with the certificate's name and thumbprint. If you click **OK**, the certificate is added or removed from your current list of trusted root authorities. Only Local System accounts have write access to the list. If this service stops, the current user cannot add or remove Trusted Root Certification Authority certificates.
- **Automatic Root Certificate Update Service.** This service retrieves root certificates as needed from Windows Update. This service can be used in support secure-sockets-layer (SSL) sessions to help ensure that server certificates are kept up-to-date. If this service stops, root certificates must be updated manually.
- **Key Service.** This service allows administrators to enroll for certificates on behalf of the local computer account. The service provides several functions that are required for enrollment, such as enumeration of available certification authorities, enumeration of available computer templates, and the ability to create and submit a certificate request in the local computer context. Only administrators can enroll on behalf of the local computer account. The Key Service also allows administrators to remotely install Personal Information Exchange (PFX) files on the computer. If this service stops, autoenrollment cannot automatically acquire the default set of computer certificates.

The Cryptographic Services service is installed by default and its startup type is **Automatic**. When Cryptographic Services service is started in its default configuration, it logs on by using the Network Service account. If it stops, the management services that are referenced in the preceding paragraphs do not function properly.

The Cryptographic Services service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the Cryptographic Services service:

- Application Identity service

DCOM Server Process Launcher

The DCOM Server Process Launcher (DCOMLaunch) service launches COM and DCOM servers in response to object activation requests. This service is installed by default and its startup type is **Automatic**. When the DCOM Server Process Launcher service is started in its default configuration, it logs on by using the Local System account.

If the DCOM Server Process Launcher service stops, remote procedure calls and DCOM requests on the local computer do not function properly. In particular, the Windows Firewall service fails if this service stops. This service is required and cannot be stopped from the Services console. If this service stops, the computer restarts.

The Remote Procedure Call (RPC) service is dependent upon the DCOM Server Process Launcher service.

Desktop Window Manager Session Manager

The Desktop Window Manager Session Manager (UxSms) service provides Desktop Window Manager startup and maintenance services. The service supports the Themes service, and it checks that applications are compatible with the Windows Aero desktop experience. If an application is not compatible with Aero, this service causes it to revert to a classic Windows theme that it supports.

If the computer does not support Aero graphics, performance might be by disabling this service.

This service is installed by default and its startup type is **Automatic**. When the Desktop Window Manager Session Manager service is started in its default configuration, it logs by on using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

DHCP Client

The DHCP Client (Dhcp) service manages network configuration. It registers and updates IP addresses and Domain Name System (DNS) names for the computer. You do not have to manually change the IP settings for a client computer, such as a portable computer, that connects from different locations throughout the network. The client computer is automatically given a new IP address, regardless of the subnet that it reconnects to (if a DHCP server is accessible from the subnets). There is no need to manually configure settings for DNS or WINS. The DHCP server can provide these settings to the client computer if the DHCP server is

configured to issue such information. To enable this option on the client computer, click **Obtain DNS Server Address Automatically**. No conflicts are caused by duplicate IP addresses.

If the DHCP Client service stops, the computer does not receive dynamic IP addresses and automatic DNS updates stop being registered on the DNS server.

By default this service is installed by default and its startup type is **Automatic**. When the DHCP Client service is started in its default configuration, it logs on by using the Local Service account.

The DHCP Client service is dependent upon the following system components:

- Ancillary Function Driver for Winsock
- Net I/O Legacy TDI Support Drive
- TCP/IP Protocol Driver
- Network Store Interface Service
- NSI proxy service driver

The WinHTTP Web Proxy Auto-Discovery Service is dependent upon the DHCP Client Service.

DHCP Server

The DHCP Server (DHCP Server) service allocates IP addresses, and it enables advanced configuration of network settings (such as setting for DNS servers and WINS servers) to DHCP clients automatically. DHCP uses a client/server model. The network administrator establishes one or more DHCP servers that maintain TCP/IP configuration information and provide the information to client computers. The server database includes the following:

- Valid configuration parameters for all client computers on the network.
- Valid IP addresses that are maintained in a pool for assignment to client computers, plus reserved addresses for manual assignment.
- Duration of the lease that is offered by the server. The lease defines the length of time that the assigned IP address is valid.

DHCP is an IP standard that is designed to reduce the complexity of address configuration administration. It uses a server computer to centrally manage IP addresses and other related configuration details for your network.

DHCP includes the Multicast Address Dynamic Client Allocation Protocol (MADCAP), which is used to perform multicast address allocation. When registered client computers are dynamically

assigned IP addresses through MADCAP, they can participate efficiently in the data stream process, such as for real-time video or audio network transmissions.

With a DHCP server installed and configured on your network, DHCP-enabled client computers can obtain their IP addresses and related configuration parameters dynamically each time they start and join the network. DHCP servers provide this configuration in the form of an address-lease offer to the client computers.

If the DHCP Server service stops, the server no longer issues IP addresses or other configuration parameters automatically. This service is only installed and activated if you install the DHCP server role.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports that are used by the DHCP Server service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
| DHCP Server | UDP | 67 |
| MADCAP | UDP | 2535 |

Diagnostic Policy Service

Diagnostic Policy Service (DPS) enables problem detection, troubleshooting, and resolution for components in the Windows operating system. If this service is stopped, diagnostics cannot function. Diagnostic Policy Service supports the Network Diagnostic Framework that is used to troubleshoot network connectivity issues.

This service is installed by default and its startup type is **Automatic**. When Diagnostic Policy Service is started in its default configuration, it logs by on using the Local Service account.

This service is not dependent on any other system service, nor is any service dependent on it.

Diagnostic Service Host

The Diagnostic Service Host (WdiServiceHost) service enables problem detection, troubleshooting, and resolution for Windows components. If this service is stopped, diagnostics

cannot function. The Diagnostic Service Host service is part of the Network Diagnostic Framework that is used to troubleshoot network connectivity issues. When a user selects **Diagnose and Repair** from the Network and Sharing Center or the Network Connection context menu, the Diagnostic Policy Service starts the Diagnostic Service Host service. The service continues to run until the computer is restarted.

This service is installed by default and its startup type is **Manual**. When the Diagnostic Service Host service is started in its default configuration, it logs by on using the Local Service account.

This service is not dependent on any other system service, nor is any service dependent on it.

Diagnostic System Host

The Diagnostic System Host (WdiSystemHost) service enables problem detection, troubleshooting, and resolution for Windows components. If this service is stopped, diagnostics cannot function. The Diagnostic System Host service is part of the Network Diagnostic Framework that is used to troubleshoot network connectivity issues.

This service is installed by default and its startup type is **Manual**. When the Diagnostic System Host service is started in its default configuration, it logs by on using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Disk Defragmenter

The Disk Defragmenter (defragsvc) service is used to defragment disks on a schedule that is maintained by the Task Scheduler, which controls when it starts and stops.

This service is installed by default and its startup type is **Manual**. When the Disk Defragmenter service is started in its default configuration, it logs by on using the Local System account.

The Disk Defragmenter service is dependent upon the following system components:

- Remote Procedure Call (RPC) service
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Distributed File System

The Distributed File System (Dfs) service manages logical volumes that are distributed across a local or wide area network, and it is required for the AD DS SYSVOL shared resource. Distributed

File System (DFS) is a distributed service that integrates disparate shared files into a single logical namespace.

This namespace is a logical representation of the network storage resources that are available to users on the network. If the Distributed File System service stops, you are unable to access shared files or network data through the logical namespace. To access the data when the service is stopped, you must know the names of all the servers and all the shared files in the namespace, and you must access each of these targets independently. This service is installed as part of the File Services role.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports that are used by the Distributed File System service:

| Application protocol | Network protocol | Ports |
|-----------------------------------|------------------|---|
| NetBIOS Datagram Service | UDP | 138 |
| NetBIOS Session Service | TCP | 139 |
| LDAP Server | TCP | 389 |
| LDAP Server | UDP | 389 |
| SMB | TCP | 445 |
| RPC | TCP | 135 |
| Randomly allocated high TCP ports | TCP | Random port number between 1024 and 65535 |

Distributed File System Replication

The Distributed File System Replication (DFSR) service is a state-based, multi-master file replication engine that automatically copies updates to files and folders between computers that are participating in a common replication group. This service is installed as part of the File Services role.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2. The following table identifies the application protocols, network protocols, and ports used by the Distributed File System service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------------------------------|
| RPC | TCP | 135 |
| RPC | TCP | 5722 (domain controller only) |

| | | |
|-----------------------------------|-----|---|
| Randomly allocated high TCP ports | TCP | Random port number between 1024 and 65535 |
|-----------------------------------|-----|---|

Distributed Link Tracking Client

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

When you create a shortcut to a file on an NTFS volume, distributed link tracking inserts a unique object identifier (ID) into the target file, which is known as the link source. The file that refers to the target file (known as the link client) also internally stores information about the object ID. Distributed link tracking can use this object ID to locate the link source file in the following scenarios:

- When the link source file is renamed.
- When the link source file is moved to another folder on the same volume or a different volume of the same computer.
- When the link source file is moved to another computer in the network.



Note

Unless the computer is in a domain where the Distributed Link Tracking Server service is available, this form of link tracking is less reliable over time.

- When the shared network folder that contains the link source file is renamed.
- When the computer that contains the link source file is renamed.

For all of the preceding scenarios, the link source file must be located on a fixed NTFS volume. The NTFS volumes cannot be located on removable media.



Note

The Distributed Link Tracking Client service monitors activity on NTFS volumes and stores maintenance information in a file called Tracking.log, which is located in a hidden folder called System Volume Information at the root of each volume. This folder is protected by permissions that allow only the computer to access it. The folder is also used by other Windows services, such as the Indexing Service.

If the Distributed Link Tracking Client service stops links to content on that computer are not maintained or tracked.

This service is installed by default and its startup type is **Automatic**. When the Distributed Link Tracking Client service is started in its default configuration, it logs by on using the Local System account.

The Distributed Link Tracking Client service is dependent upon the following system components:

- Remote Procedure Call
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Distributed Link Tracking Server

The Distributed Link Tracking Server (TrkSvr) service stores information so files that are moved between volumes can be tracked for each volume in the domain. When enabled, the Distributed Link Tracking Server service runs on each domain controller in a domain. This service enables the Distributed Link Tracking Client service to track linked documents that have been moved to a location in another NTFS volume in the same domain.

The Distributed Link Tracking Server service is disabled by default. If you enable it, you must do so on all domain controllers of a domain. If the Distributed Link Tracking Server service is enabled on a domain controller that is upgraded to a newer version of Windows Server, the service must be re-enabled manually.

If the Distributed Link Tracking Server service is enabled and then later disabled, you must purge its entries in AD DS. For more information, see [article 312403](#) in the Microsoft Knowledge Base.

If the Distributed Link Tracking Server service stops or if you disable it, links that are maintained by the Distributed Link Tracking Client service eventually become less reliable.

The Distributed Link Tracking Server service is part of the AD DS server role.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2. The following table identifies the application protocols, network protocols, and ports used by the Distributed Link Tracking Server service:

| Application protocol | Network protocol | Ports |
|-----------------------------------|------------------|---|
| RPC | TCP | 135 |
| Randomly allocated high TCP ports | TCP | Random port number between 1024 and 65535 |

Distributed Transaction Coordinator

The Distributed Transaction Coordinator (MSDTC) service coordinates transactions that are distributed across multiple computers and resource managers, such as databases, message queues, and file systems. This service is necessary if transactional components are to be configured through COM+. It is also required for transactional queues in Message Queuing (also known as MSMQ) and SQL Server operations that span multiple computers.

If this service stops, transactions that use this service are not performed. Clustered installations of Microsoft Exchange, SQL Server, or other applications that make use of transaction services may be affected if this service stops.

This service is installed by default and its startup type is **Manual**. When the Distributed Transaction Coordinator service is started in its default configuration, it logs on by using the Network Service account.

This service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Security Accounts Manager

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports used by the Distributed Transaction Coordinator service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
|----------------------|------------------|-------|

| | | |
|-----------------------------------|-----|---|
| RPC | TCP | 135 |
| Randomly allocated high TCP ports | TCP | random port number between 1024 – 65535 |

aiici

DNS Client

The DNS Client (Dnscache) service resolves and caches Domain Name System (DNS) names for the computer. The DNS Client service must run on every computer that performs DNS name resolution. DNS name resolution is needed to locate domain controllers in AD DS domains. The DNS Client service is also needed to enable the location of the devices that are identified through DNS name resolution. Windows 7 includes both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) protocol stacks that are installed and enabled by default. DNS name queries and registrations can involve IPv4 address records (A records) and IPv6 address records (AAAA records).

If the DNS Client service stops, the computer cannot resolve DNS names or locate Active Directory domain controllers, and users cannot log on to the computer.

Computers must perform both A and AAAA queries to determine the best method of connectivity to the endpoint that is wanted. By obtaining IPv4 and IPv6 addresses, there is an increased chance of access to the wanted endpoint if one of the addresses is unreachable. The DNS Client service minimizes the impact on DNS servers when performing DNS name queries through the following behavior:

- If the host has only link-local or Teredo IPv6 addresses assigned, the DNS Client service sends a single query for A records. For more information, see the [Teredo Overview](#) on Microsoft TechNet.
- If the host has at least one IPv6 address assigned that is not a link-local or Teredo address, the DNS Client service sends a DNS query for A records and then a separate DNS query to the same DNS server for AAAA records. If an A record query times out or has an error (other than name not found), the corresponding AAAA record query is not sent.

This service is installed by default and its startup type is **Automatic**. When the DNS Service is started in its default configuration, it logs on by using the Network Service account.

The DNS Client service is dependent upon the following system components:

- NetIO Legacy TDI Support Driver
- TCP/IP Protocol Driver
- Network Store Interface Service
- NSI proxy service driver

DNS Server

The DNS Server (DNS) service enables DNS name resolution. It answers queries and update requests for DNS names. DNS servers locate devices that are identified by their DNS names and locate domain controllers in AD DS.

If the DNS Server service stops or if you disable it, DNS updates do not occur. The DNS Server service is not required to run on every computer. However, if there is no authoritative DNS server for a particular portion of the DNS namespace, the location of the devices that use DNS names in that portion of the namespace fail. Absence of an authoritative DNS server for the DNS namespace that is used to name Active Directory domains results in an inability to locate domain controllers in that domain.

The DNS Server service is only installed and activated if you install the DNS Server role.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports used by the DNS Server service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
| DNS | UDP | 53 |
| DNS | TCP | 53 |

Encrypting File System

The Encrypting File System (EFS) service provides the core file encryption technology that is used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications are unable to access encrypted files.

This service is installed by default and its startup type is **Manual**. When you select a file or folder to encrypt with EFS, the service will start, and its startup type is changed to **Automatic**.

When the EFS service is started in its default configuration, it logs on by using the Local System account.

The EFS service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Extensible Authentication Protocol

The Extensible Authentication Protocol (EapHost) service provides network authentication in such scenarios as 802.1x wired and wireless, virtual private network (VPN), and Network Access Protection (NAP). The Extensible Authentication Protocol (EAP) also provides APIs that are used by network access clients, including wireless and VPN clients, during the authentication process.

EAP supports authentication schemes such as Generic Token Card, One Time Password (OTP), Message Digest 5 (MD5)-Challenge, Transport Layer Security (TLS) for smart card and digital certificate-based authentication, and future authentication technologies. EAP is a critical technology component for establishing secure connections. If you disable this service, the computer is prevented from accessing networks that require EAP authentication.

This service is installed by default and its startup type is **Manual**. When the Extensible Authentication Protocol service is started in its default configuration, it logs on by using the Local System account.

The Extensible Authentication Protocol service is dependent upon the following system components:

- CNG Key Isolation
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher

- RPC Endpoint Mapper

The following components are dependent upon the Extensible Authentication Protocol service:

- Wired AutoConfig
- WLAN AutoConfig

Fax Service

The Fax Service is a Telephony API (TAPI)-compliant service, and it provides fax capabilities from users' computers. The Fax Service allows users to send and receive faxes from their desktop applications through a local fax device or a shared network fax device. The service offers the following features:

- Fax distribution and receipt
- Fax activity tracking and monitoring
- Inbound fax routing
- Server and device configuration management
- Archiving of sent faxes

If you disable the print spooler or telephony service, the Fax Service does not start successfully. If this service stops, users cannot send or receive faxes. This service is installed by default and its startup type is **Manual**. It stops when there is no fax activity and restarts on an as-needed basis. On server operating systems, the Fax Service is installed with the Fax Server role. For more information, see [Install the Fax Server Role](#).

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The Fax Service is dependent upon the following system components:

- Plug and Play
- Print Spooler
- HTTP
- Remote Procedure Call
- DCOM Server Process Launcher
- RPC Endpoint Mapper

- Telephony

The following table identifies the application protocols, network protocols, and ports used by the Fax Service:

| Application protocol | Network protocol | Ports |
|-----------------------------------|------------------|---|
| NetBIOS Session Service | TCP | 139 |
| SMB | TCP | 445 |
| RPC | TCP | 135 |
| Randomly allocated high TCP Ports | TCP | Random port number between 1024 and 65535 |

Function Discovery Provider Host

The Function Discovery Provider Host (fdPHost) service provides the host process for Function Discovery providers. The Function Discovery Provider Host service provides a uniform programmatic interface for enumerating system resources, such as hardware devices, whether they are connected locally or through a network. It enables applications to discover and manage lists of devices or objects that are sorted by functionality or class. Applications and users can use the Function Discovery Provider Host service to discover what functions their system can perform, regardless of the underlying device or software architecture.

The Function Discovery Provider Host service supports an extensible discovery provider model. The providers that are included in the system provide an abstraction layer over existing standards such as Plug and Play, Simple Service Discovery Protocol (SSDP), Web Services Dynamic Discovery (WS-Discovery), and the registry. You can create custom providers to expose your organization's resources through the Function Discovery Provider Host service.

The service is installed by default, and its startup type is **Manual**. When the Function Discovery Provider Host service is started in its default configuration, it logs on by using the Local Service account.

The Function Discovery Provider Host service is dependent upon the following system components:

- HTTP

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent upon the Function Discovery Provider Host service:

- HomeGroup Provider
- Media Center Extender Service
- PnP-X IP Bus Enumerator

Function Discovery Resource Publication

The Function Discovery Resource Publication (FDResPub) service publishes information about a computer and the resources that are attached to that computer so that they can be discovered over the network. If this service is stopped, those resources cannot be published and they cannot be discovered by other computers on the network.

This service is installed by default and its startup type is **Manual**. When the Function Discovery Resource Publication service is started in its default configuration, it logs on by using the Local Service account.

The Function Discovery Resource Publication service is dependent upon the following system components:

- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon this service:

- HomeGroup Provider

Group Policy Client

The Group Policy Client (gpsvc) service is responsible for applying settings that are configured by administrators for the computer and users through Group Policy. If the service is stopped or disabled, the settings are not applied, and applications and components cannot be managed

through Group Policy. Components or applications that depend on Group Policy might not function if this service is stopped or disabled.

The Group Policy Client service is installed by default and its startup type is **Automatic**. When the Group Policy Client service is started in its default configuration, it logs by on using the Local System account. The service cannot be disabled or modified through the Services snap-in console.

The Group Policy Client service is dependent upon on the following system components:

- Mup
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Group Policy

The Group Policy service on domain controllers supports the application of Group Policy settings to client computers in the domain. To successfully apply Group Policy settings, a client must be able to contact a domain controller over the DCOM, ICMP, LDAP, SMB, and RPC protocols. If these protocols are unavailable or blocked between the client and a relevant domain controller, the Group Policy service will not apply or refresh. For a cross-domain logon, where a computer is in one domain and the user account is in another, these protocols may be required for the client, the resource domain, and the account domain to communicate. Internet Control Message Protocol (ICMP) is used for slow link detection.

This service is installed by default and its startup type is **Manual**. When the Group Policy service is started in its default configuration, it logs on by using the Local System account.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports used by the Group Policy service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|---------------------------|
| DCOM | TCP plus UDP | Random ports between 1024 |

| | | |
|-------------|------|--|
| | | and 65535 |
| ICMP (ping) | ICMP | Used for slow link detection |
| LDAP | TCP | 389 |
| SMB | TCP | 445 |
| RPC | TCP | 135 or a random port number between 1024 and 65535 |

Health Key and Certificate Management

The Health Key and Certificate Management (hkmsvc) service provides X.509 certificate and key management services for the Network Access Protection Agent (NAP) service as part of the Network Access Protection platform. Enforcement technologies that use X.509 certificates may not function properly if this service is not installed or is disabled.

The NAP platform helps administrators validate and enforce compliance with system health policies for network access and communication. Administrators can create solutions to validate computers that connect to or communicate on their networks, to provide needed updates or access to needed resources, and to limit the network access of computers that are noncompliant.

This service is installed by default and its startup type is **Manual**. When the Health Key and Certificate Management service is started in its default configuration, it logs on by using the Local System account.

The Health Key and Certificate Management service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

HomeGroup Listener

The HomeGroup Listener service makes local computer changes that are associated with configuring and maintaining computers that are joined to a homegroup. If this service is stopped or disabled, the computer will not work properly in a homegroup and the homegroup might not

work properly. It is recommended that this service be running if the computer is part of a homegroup.

This service is installed by default and its startup type is **Manual**. When the HomeGroup Listener service is started in its default configuration, it logs on by using the Local System account.

The HomeGroup Listener service is dependent upon the following system components:

- Server
- Security Accounts Manager
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Server SMB 1.xxx Driver
- Server SMB 2.xxx Driver
- srvnet

HomeGroup Provider

The HomeGroup Provider service performs networking tasks that are associated with configuring and maintaining homegroups. If this service is stopped or disabled, the computer will be unable to detect other homegroups, and the homegroup might not work properly. It is recommended that this service be running if the computer is part of a homegroup.

This service is installed by default and its startup type is **Manual**. When the HomeGroup Provider service is started in its default configuration, it logs on by using the Local Service account.

The HomeGroup Provider service is dependent on the following system components:

- Function Discovery Provider Host
- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Function Discovery Resource Publication

- Network List Service
- Network Location Awareness
- Network Store Interface Service
- NSI proxy service driver
- TCP/IP Protocol Driver

HTTP SSL

The HTTP SSL (HTTPFilter) service enables IIS to perform Secure Sockets Layer (SSL) functions. SSL is an open standard that establishes encrypted communications channels to help prevent the interception of critical information, such as credit card numbers. Primarily, it protects data that is transmitted for electronic financial transactions on the Internet, although it is designed to work on other Internet services as well.

If the HTTP SSL service stops, IIS does not perform SSL functions. This service is installed when IIS is installed, and it is not present or active otherwise. You can configure this service through the Internet Information Services (IIS) snap-in.

This service is available on a Server Core installation of Windows Server 2008 R2 in addition to the Web, Standard, Enterprise, and Datacenter editions of Windows Server 2008 and Windows Server 2008 R2.

The following table identifies the application protocols, network protocols, and ports used by the HTTP SSL service:

| Application protocol | Network Protocol | Ports |
|----------------------|------------------|-------|
| HTTPS | TCP | 443 |

Human Interface Device Access

The Human Interface Device Access (hidserv) service enables generic input access to Universal Serial Bus (USB) devices such as keyboards and mice. The service activates and maintains predefined keyboard keys, remote controls, and other multimedia devices.

If the Human Interface Device Access service stops, keyboard keys that are controlled by this service no longer function. For instance, the Back key, Forward key, and other keys on USB keyboards and volume buttons on USB speakers do not function.

This service is installed by default and its startup type is **Manual**. When The Human Interface Device Access service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

IIS Admin Service

The IIS Admin Service (IISADMIN) allows administration of Internet Information Services (IIS) components such as FTP, application pools, websites, web service extensions, and Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) virtual servers. If you stop or disable this service, you cannot run web, FTP, NNTP, or SMTP sites.

The IIS Admin Service is not installed by default. It is installed when you install IIS an optional feature of the operating system. After this service is installed, its startup type is **Automatic**. When the IIS Admin Service is started, it logs on by using the Local System account by default.

The IIS Admin Service is dependent upon the following system components:

- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Security Accounts Manager

IKE and AuthIP IPsec Keying Modules

The IKE and AuthIP IPsec Keying Modules (IKEEXT) service hosts the IKE and AuthIP keying modules. These modules are used for authentication and key exchange in IPsec. Stopping or disabling the IKE and AuthIP IPsec Keying Modules service disables the IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKE and AuthIP IPsec Keying Modules service may result in an IPsec failure and may compromise the security of the system. We strongly recommend that you have the IKEEXT service running.

This service is installed by default and its startup type is **Manual**. When the IKE and AuthIP IPsec Keying Modules service is started in its default configuration, it logs on by using the Local System account.

The IKE and AuthIP IPsec Keying Modules service is dependent upon the following system components:

- Base Filtering Engine
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Indexing Service

The Indexing Service (CISVC) indexes the 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 document search capability on local and remote computers and a search index for content that is shared on the web. The service builds indexes of all textual information in files and documents. After the initial index build is complete, the Indexing Service maintains the indexes whenever a file is created, modified, or deleted.

The Indexing Service has been replaced by Windows Search in Windows 7 and Windows Server 2008 R2. The Indexing Service is still available; however, it must be explicitly installed. After it is installed, its default startup type is **Automatic**. When the Indexing Service is started it logs on by using the Local System account by default.

The Indexing Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Interactive Services Detection

The Interactive Services Detection (UI0Detect) service enables notification of user input for interactive services, which enables access to dialog boxes that are created by interactive services. If this service is stopped, notifications of new interactive service dialog boxes no longer function and there might no longer be access to interactive service dialog boxes. This service supports the service isolation feature.

In Windows XP, Windows Server 2003, and earlier versions of the Windows operating system, all services run in the same session as the first user who logs on to the console. This session is called Session 0. Running services and user applications together in Session 0 poses a security

risk because services run at elevated privilege; and therefore, they are targets for malicious users who are looking for a way to elevate their own privilege level.

The Windows 7 and Windows Server 2008 R2 operating systems mitigate this security risk by isolating services in Session 0 and making Session 0 noninteractive. In these operating systems, only system processes and services run in Session 0. The first user logs on to Session 1, and subsequent users log on to subsequent sessions. This means that services never run in the same session as users' applications. Therefore, users are protected from attacks that originate in application code.

Because Session 0 is no longer a user session, services that run in Session 0 do not have access to the video driver. This means that any attempt that a service makes to render graphics fails. For example, if a device installer runs in Session 0 and the installation program creates a dialog box in Session 0 that requires user input to continue, the device installation never completes because the user does not see the dialog box. From the user's perspective, the device installer has stopped responding because it has stopped progressing and the user has no way to resume it. Basically, any functionality in a service or a service-hosted driver that assumes the user is running in Session 0 does not work correctly in Windows 7 and Windows Server 2008 R2.

As a result of this issue, the option to enable the Interactive Service Detection service is available for customers who have services from earlier versions of Windows that send user interaction dialog boxes to Session 0 instead of to the corresponding user's session.

This service is installed by default and its startup type is **Manual**. The service starts only when a visible dialog box that is not a command window is detected. If the service is started, users are notified when a dialog box or window (including a command window) appears in Session 0. Information about each of the last 10 dialog boxes appears in turn if more information is shown. This helps to ensure that when you test the deployment of the new operating you are aware of services from earlier operating systems in their environment, and they have the opportunity to contact the vendors for updated services.

The service detects these visible dialog boxes or windows and sends a notification to the user. Users may choose to:

- Respond to the dialog box immediately by clicking a button to switch to Session 0, interact with the task dialog box, and then switch back to their session.
- Be reminded again in five minutes. The reminders continue until the dialog box closes.

If this service is disabled, users do not receive notifications when the devices or services send dialog boxes to Session 0.

When the Interactive Services Detection service is started in its default configuration, it logs on by using the Local System account, and it is allowed to interact with the desktop.

This service is not dependent on any other system service, nor is any service dependent on it.

Internet Connection Sharing

The Internet Connection Sharing (SharedAccess) service provides network address translation, addressing, name resolution, and intrusion prevention services for a home network or small office network.

This service is installed by default and its startup type is **Disabled**. When the Internet Connection Sharing service is started in its default configuration, it logs on by using the Local System account.

The Internet Connection Sharing service is dependent upon the following system components:

- Base Filtering Engine
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Network Connections
- Network Store Interface Service
- NSI proxy service driver
- Remote Access Connection Manager
- Secure Socket Tunneling Protocol Service
- Telephony
- Plug and Play
- Windows Management Instrumentation

Intersite Messaging

The Intersite Messaging (IsmServ) service enables message exchanges between computers in an environment with servers that are running the Windows Server operating system. This service is used for mail-based replication between sites. AD DS includes support for replication between sites through SMTP over IP transport. SMTP support is provided by the SMTP service, which is a component of IIS.

The set of transports that are used for communication between sites must be extensible. Therefore, each transport is defined in a separate add-in dynamic link library (DLL) file. These add-in DLL files are loaded into the Intersite Messaging service, which runs on all domain controllers that can perform communication between sites. The Intersite Messaging service directs send-and-receive requests to the appropriate transport add-in DLL files, which then route the messages to the Intersite Messaging service on the destination computer.

If the Intersite Messaging service stops, messages are not exchanged, intersite messaging replication does not work, and site-routing information is not calculated for other services.

This service is installed by default on computers running Windows Server 2008 R2, but it is disabled until the server is promoted to the domain controller role. When the Intersite

Messaging service is started in its default configuration, it logs on by using the Local System account.

The Intersite Messaging service is dependent on the following system components:

- DCOM Server Process Launcher
- RPC Endpoint Mapper

IP Helper

The IP Helper (iphlpvc) service offers IPv6 connectivity over an IPv4 network. IPv6 solves many IPv4 issues regarding address depletion, security, autoconfiguration, and extensibility. This service allows IPv6-enabled sites and hosts to communicate through IPv6 over an IPv4 infrastructure—for example, the Internet. This is often referred to as "6to4." IPv6 sites and hosts can use their 6to4 address prefix and the Internet to communicate. They do not need to obtain an IPv6 global address prefix from an Internet service provider (ISP) to connect to the IPv6-enabled portion of the Internet.

6to4 is a tunneling technique that is described in RFC 3056. The 6to4 hosts do not require any manual configuration, and they use a standard autoconfiguration to create 6to4 addresses. The 6to4 technique uses the global address prefix of 2002:WWXX:YYZZ::/48, where WWXX:YYZZ is the colon-hexadecimal representation of a public IPv4 address (w.x.y.z) that is assigned to a site or host, also known as the Next Level Aggregator (NLA) portion of a 6to4 address.

The IP Helper service also supports 6over4, also known as IPv4 multicast tunneling, a technique that is described in RFC 2529. The 6over4 technique allows IPv6 and IPv4 nodes to communicate through IPv6 over an IPv4 infrastructure. It uses the IPv4 infrastructure as a multicast-capable link. For 6over4 to work correctly, the IPv4 infrastructure must be IPv4 multicast-enabled.

If the IP Helper service stops, the computer only has IPv6 connectivity if it is connected to a native IPv6 network.

This service is installed by default and its startup type is **Automatic**. When the IP Helper service is started in its default configuration, it logs on by using the Local System account.

The IP Helper service is dependent upon the following system components:

- NetIO Legacy TDI Support Driver
- TCP/IP Protocol Driver
- Network Store Interface Service
- NSI proxy service driver

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Management Instrumentation

IPsec Policy Agent

The IPsec Policy Agent (PolicyAgent) service provides end-to-end security between clients and servers on TCP/IP networks, manages IPsec policy settings, starts the Internet Key Exchange (IKE), and coordinates IPsec policy settings with the IP security driver. The service is controlled by using the NET START and NET STOP commands.

IPsec operates at the Internet Protocol layer of the operating system, and it is transparent to other operating system services and applications. The service provides packet filtering, and it can negotiate security between computers on IP networks.

If the IPsec Policy Agent service stops, TCP/IP security between clients and servers on the network is impaired.

This service is installed by default and its startup type is **Manual** on computers running Windows Server 2008 R2 or Windows 7. When the IPsec Policy Agent service is started in its default configuration, it logs on by using the Network Service account.

The IPsec Policy Agent service is dependent upon the following system components:

- Base Filtering Engine
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- TCP/IP Protocol Driver

KtmRm for Distributed Transaction Coordinator

The KtmRm for Distributed Transaction Coordinator (KtmRm) service coordinates transaction between the Microsoft Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). This service supports the KTM feature in Windows 7 and Windows Server 2008 R2. The KTM enables the development of applications that use transactions. The transaction engine is within the kernel, but you can develop kernel-mode transactions or user-mode transactions within a single host or among distributed hosts.

The KTM implements Transactional NTFS (TxF) and Transactional Registry (TxR). TxF allows transacted file system operations within the NTFS file system. TxR allows transacted registry operations. KTM enables client applications to coordinate file system and registry operations with a transaction that results in better error recovery during data transfer and in the event of system failure.

This service is installed by default and its startup type is **Manual**. When the KtmRm for Distributed Transaction Coordinator service is started in its default configuration, it logs on by using the Network Service account.

The KtmRm for Distributed Transaction Coordinator service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Security Accounts Manager

Link-Layer Topology Discovery Mapper

The Link-Layer Topology Discovery Mapper (lltdsvc) service creates a network map, which includes computer and device connectivity information and metadata that describes each computer and device. If this service is disabled, the network map does not function properly.

This service is installed by default and its startup type is **Manual**. When the Link-Layer Topology Discovery Mapper service is started in its default configuration, it logs on by using the Local Service account.

The Link-Layer Topology Discovery Mapper service is dependent upon the following system components:

- Link-Layer Topology Discovery Mapper I/O Driver
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

LPD Service

The LPD Service (LPDSVC) enables client computers to print to the Line Printer Daemon (LPD) service on this server by using TCP/IP and the Line Printer Remote (LPR) protocol. This service is part of the **Print and Documents Services** feature of the operating system.

This service is not installed by default. It can be added by using the **Turn Windows Features on or off** option in the **Control Panel**. After this service is installed, its default startup type is **Manual**. When the LPD Service is started it logs on by using the Local System account by default.

The LPD Service is dependent upon the following system components:

- Print Spooler
- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- TCP/IP Protocol Driver

Media Center Extender Service

The Media Center Extender Service (Mcx2Svc) allows Media Center Extenders to locate and connect to the computer. This service is available in Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise. It is not available in Windows 7 Starter or Windows 7 Home Basic.

This service is installed by default and its startup type is **Disabled**. When Media Center Extender Service is started in its default configuration, it logs on by using the Local Service account.

The Media Center Extender Service is dependent upon the following system components:

- Function Discovery Provider Host
- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- PnP-X IP Bus Enumerator
- Remote Desktop Services
- Terminal Device Driver
- SSDP Discovery

Message Queuing

The Message Queuing (MSMQ) service is a messaging infrastructure and development tool that creates distributed messaging applications for the Windows operating system. Such applications can communicate across heterogeneous networks and send messages between computers that may be temporarily unable to connect to each other. This service provides guaranteed message delivery, efficient routing, security, and priority-based messaging.

For remote reading, Message Queuing 4.0 uses encrypted RPC by default. In situations where encrypted RPC cannot be used, (for example, where a workgroup computer is part of the remote read process), the message is passed to the remote computer as plaintext and message security is not guaranteed. A plaintext message that has reached its destination queue can be read only by users who have the necessary access rights to read messages from the queue.

We recommend that servers enable Message Queuing 4.0 in secured remote reading mode. In secured remote reading mode, the computer only listens to the secure remote read interface. The effect of this is that only Message Queuing 4.0 and Message Queuing 3.0 on servers running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 can remotely receive messages from queues on the computer. Remote reads from MSMQ 1.0 client computers, MSMQ 2.0 client computers, and Message Queuing 3.0 client computers running Windows XP are not supported. For information about enabling your server to use only the secured mode, see [Enable Secured Remote Read](#).

If the Message Queuing service stops, distributed messages are unavailable. If you disable this service, any services that explicitly depend on it do not start. Also, the COM+ Queued

Components service, some functionality of Windows Management Instrumentation (WMI), and the Message Queuing Triggers service are affected.

Message Queuing is an optional feature in Windows 7 and Windows Server 2008 R2. It is not installed or enabled by default. It can be added through the **Turn Windows Features on or off** dialog box in the **Programs** area of Control Panel. When this service is installed, its default startup type is **Automatic**. When the Message Queuing service is started it logs on using the Network Service account by default.

The Message Queuing service is dependent upon the following system components:

- Message Queuing Access Control
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Event Log

The following services are dependent upon the Message Queuing service:

- Message Queuing Triggers
- Net.Msmq Listener Adapter

Message Queuing Triggers

The Message Queuing Triggers (MSMQTriggers) service provides a rule-based system to monitor messages that arrive in a Message Queuing service queue. The Message Queuing Triggers service enables the invocation of a Component Object Model (COM) component or an executable, depending on the queue's defined filters for the incoming messages.

The Message Queuing Triggers service is installed as part of the Message Queuing service on Windows Server 2008 R2. In Windows 7, the Message Queuing Triggers feature must be installed through the **Turn Windows Features on or off** dialog box in the **Programs** area of Control Panel.

If the Message Queuing Triggers service stops, you cannot apply rule-based monitoring or invoke programs to process messages automatically.

Microsoft .NET Framework NGEN

This service supports the Microsoft .NET Framework Native Image Generator (NGEN) feature of the .NET Framework Common-Language Runtime. It is used to create platform-specific, optimized versions of .NET Framework applications that have faster performance than applications that have to be compiled by the just-in-time compiler before they can be run.

The service runs either in low priority for important compilations or in idle priority for non-important compilations. After all optimizations that are in the queue are completed, the service shuts down.

This service is installed by default, and the service startup type is **Manual**. You might have several versions of this service installed by different .NET applications. This service has been renamed **Native Image Service** in .NET Framework 4.

Microsoft FTP Service

The Microsoft FTP Service (ftpsvc) enables the computer to be a File Transfer Protocol (FTP) server. If this service is stopped, the computer cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

This service is not installed by default. When installed, the default service startup type is **Automatic**. When the Microsoft FTP Service is started it logs on using the Local System account by default.

The Microsoft FTP Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Microsoft Software Shadow Copy Provider

The Microsoft Software Shadow Copy Provider (swprv) service manages software-based shadow copies that are taken by the Volume Shadow Copy Service. A shadow copy is a snapshot of a disk volume that represents a consistent read-only point-in-time for that volume. This point-in-time snapshot stays constant and allows an application, such as backup software, to copy data from the shadow copy.

There are two general classes of shadow copies:

- **Hardware.** A hardware shadow copy is a mirror of two or more disks that are split into separate volumes. One of the volumes remains the working set, and the other volume can be mounted separately.
- **Software.** A software shadow copy uses a copy-on-write scheme to copy all sectors of a volume that change over time into a differential area on disk. When the shadow copy is mounted, all unchanged sectors are read from the original volume and all sectors that have changed are read from the differential area.

Shadow copies can resolve three classic data backup challenges:

- The need to back up files that were opened for exclusive access. Backup of an open file is a challenge because it is likely in a state of change. Without a shadow copy or a way to suspend the application, backups often become corrupted.

- The need to maintain a computer's availability during the shadow copy.
- Use of the same communications channels as snapshots to facilitate information transfer between application and backup tools.

If the Microsoft Software Shadow Copy Provider service stops, software-based volume shadow copies cannot be managed, which could cause Windows Backup to fail.

This service is installed by default, and its startup type is **Manual**. When the Microsoft Software Shadow Copy Provider service is started in its default configuration, it logs on by using the Local System account.

The Microsoft Software Shadow Copy Provider service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Microsoft iSCSI Initiator Service

The Microsoft iSCSI Initiator Service (MSiSCSI) manages iSCSI sessions from a computer to remote iSCSI target devices. If this service is stopped, the computer cannot log on or access iSCSI targets. If this service is disabled, any services that explicitly depend on it fail to start.

You can use iSCSI to connect storage devices over a network (LAN, WAN, or the Internet) by using TCP/IP. iSCSI devices can be disks, tapes, CDs, or other storage devices on network connected systems.

The Microsoft iSCSI Initiator Service ensures that all volumes and devices listed as "favorite targets" are available to the computer. The iSCSI Initiator properties are configured from the Administrative Tools Control Panel. To use an Internet storage device, you must unblock the appropriate firewall ports.

The IP network that is used by iSCSI does not include a default security mechanism. Because iSCSI is a plaintext protocol, iSCSI presents an attack surface that should be secured if you decide to use this service. To help secure IP packets (the data stream), you can use the challenge-handshake authentication protocol (CHAP), RADIUS authentication, or Internet Protocol security (IPsec). IPsec can be combined with either CHAP or RADIUS authentication.

This service is installed by default and the service startup type is **Manual**.

This service is not dependent on any other system service, nor is any service dependent on it.

Multimedia Class Scheduler

The Multimedia Class Scheduler (MMCSS) service enables relative prioritization of work based on system-wide task priorities. This is intended mainly for multimedia applications. If this service is stopped, individual tasks return to their default priority.

Users expect multimedia applications to offer a smooth playback experience. If the playback has pauses or jerky movements, users are dissatisfied with the experience, and will not use that content delivery method. Early versions of media players suffered from a lack of bandwidth; but the common issue now is a lack of CPU processing time. Demand for the CPU processing time by concurrently running applications such as antivirus programs, content indexing, or email applications, can interfere with media rendering and playback.

To provide a better playback experience, the operating system provides the Multimedia Class Scheduler service to manage the CPU priorities of multimedia threads. An application registers with the Multimedia Class Scheduler service by using APIs that indicate its multimedia characteristics, which must match one of those listed by name under the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows  
NT\Currentversion\Multimedia\SystemProfile\Tasks
```


The task keys are:

- Audio
- Capture
- Distribution
- Games
- Playback
- Pro Audio
- Window Manager

The task keys specify how much preference is given to each multimedia type for CPU and graphics processor resources.

The Multimedia Class Scheduler service also ensures that other concurrently running threads get an adequate portion of CPU time so that the system and other applications remain responsive. Therefore, the Multimedia Class Scheduler service reserves 20 percent of CPU time for other activity.

This service is installed by default and its startup type is **Automatic**. When the Multimedia Class Scheduler service is started in its default configuration, it logs on by using the Local System account.

The following component is dependent upon the Multimedia Class Scheduler service:

- Windows Audio

Microsoft Fibre Channel Platform Registration Service

The Microsoft Fibre Channel Platform Registration Service (FCRegSvc) registers the platform with all available Fibre Channel fabrics and maintains the registrations. A fabric is a network topology where devices are connected to each other through one or more high-efficiency data paths. The Microsoft Fibre Channel Platform Registration Service supports storage area networks.

This service is installed by default on Windows Server 2008 R2, and the service startup type is **Manual**.

Net.Msmq Listener Adapter

The Net.Msmq Listener Adapter (NetMsmqActivator) service receives activation requests over the net.msmq and msmq.formatname protocols and passes them to the Windows Process Activation Service.

The Net.Msmq Listener Adapter (NetMsmqActivator) service is not installed by default. It can be added by using the **Turn Windows Features on or off** option in the **Control Panel**. After it is installed, its default startup type is **Automatic**. When the Net.Msmq Listener Adapter service is started it logs on using the Network Service account by default.

The Net.Msmq Listener Adapter service is dependent upon the following system components:

- Message Queuing
- Message Queuing Access Control
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Event Log
- Windows Process Activation Service

Net.Pipe Listener Adapter

The Net.Pipe Listener Adapter (NetPipeActivator) service receives activation requests over the net.pipe protocol and passes them to the Windows Process Activation Service.

This service is not installed by default. It can be added by using the **Turn Windows Features on or off** option in the **Control Panel**. After it is installed, its default startup type is **Automatic**. When the Net.Pipe Listener Adapter service is started in its default configuration, it logs on by using the Local Service account.

The Net.Pipe Listener Adapter service is dependent upon the following system components:

- Windows Process Activation Service
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Net.Tcp Listener Adapter

The Net.Tcp Listener Adapter (NetTcpActivator) service receives activation requests over the net.tcp protocol and passes them to the Windows Process Activation Service.

This service is not installed by default. It can be added using the **Turn Windows Features on or off** option in the **Control Panel**. After it is installed, its default startup type is **Automatic**. When the Net.Tcp Listener Adapter service is started in its default configuration, it logs on by using the Local Service account.

The Net.Tcp Listener Adapter service is dependent upon the following system components:

- Net.Tcp Port Sharing Service
- Windows Process Activation Service
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Net.Tcp Port Sharing Service

The Net.Tcp Port Sharing Service (NetTcpPortSharing) provides the ability for multiple user processes to share TCP ports over the net.tcp protocol. This service allows a net.tcp port to be shared and secured, similar to how HTTP traffic uses port 80.

The Net.Tcp Port Sharing Service is available on all operating systems that support .NET Framework 3.0, but the service is not enabled by default. As a security precaution, an administrator must manually enable the Net.Tcp Port Sharing Service prior to first use. Although the Net.Tcp Port Sharing Service provides a layer of processing between applications and the network, applications that use port sharing should be secured as if they were listening on the network directly. Specifically, applications that use port sharing should evaluate the process privileges under which they run. When possible, run your application by using the built-in Network Service account, which runs with the minimal set of process privileges required for network communication.

This service is installed by default with Windows 7, and its startup type is **Disabled**. When the Net.Tcp Listener Adapter service is installed it modifies the startup type of this service to **Manual** and started. It is also available for installation as role service for the Application Server role on Windows Server 2008 R2.

This service is not dependent upon any other system components.

The following system component is dependent upon the Net.Tcp Port Sharing Service:

- Net.Tcp Listener Adapter

Netlogon

The Netlogon service maintains an encrypted channel between the computer and the domain controller that it uses to authenticate users and services. It passes user credentials through the encrypted channel to a domain controller and returns the domain security identifiers and user rights (this is commonly referred to as pass-through authentication).

If the Netlogon service stops, the computer cannot authenticate users and services, and the domain controller cannot register DNS records. If this happens, the domain controller may deny NTLM authentication requests, and client computers cannot discover domain controllers.

This service is installed by default and its startup type is **Manual**. However, after the computer joins a domain, its startup type is **Automatic**.

When the Netlogon service is started in its default configuration, it logs on by using the Local System account.

The Netlogon service is dependent upon the following system components:

- Workstation
- Browser Support Driver
- Network Store Interface Service
- NSI proxy service driver
- SMB 1.x MiniRedirector
- SMB MiniRedirector Wrapper and Engine
- Redirected Buffering Sub System
- Mup
- SMB 2.0 MiniRedirector

Network Access Protection Agent

The Network Access Protection Agent (napagent) service enables Network Access Protection (NAP) functionality on client computers. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its

configuration is updated. Depending on the configuration the NAP health policy and network policy, client computers might be automatically updated to comply with organizational software security policies such as mandatory updates, antivirus, signatures, and firewall configurations, so that users quickly regain full network access without having to manually update their computer.

This service is installed by default and its startup type is **Manual**. If you have a NAP infrastructure in place, its startup type is **Automatic**.

When the Network Access Protection Agent service is started in its default configuration, it logs on by using the Network Service account.

The Network Access Protection Agent service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Network Connections

The Network Connections (Netman) service is installed by default on computers running Windows Server 2008 R2 or Windows 7. This service manages objects in the Network Connections folder, from which you can view both network and remote connections. This service is responsible for client network configuration, and it displays the connection status in the notification area of the taskbar. You can also view and configure network interface settings through this service.

This service is installed by default and its startup type is **Manual**. The Network Connections interface is invoked at startup. If this service stops, configuration of LAN, dial-up, and VPN connections are unavailable to client computers. If you disable this service, the following issues might result:

- Network connection status indicator in the notification area will not display correctly.
- Connections do not display in the Network Connections folder, which prevents dial-out access and configuration of LAN settings.
- Other services that use Network Connections to check for Network Location-specific Group Policy settings do not function properly.
- Events that pertain to media connection and disconnection are not received.
- Internet connection sharing does not function correctly.

- The ability to configure incoming connections, wireless settings, or your home network is unavailable.
- New connections are not created.
- Any services that explicitly depend on this service do not start.

The Network Connections service is dependent upon the following system components:

- Network Store Interface Service
- NSI proxy service driver
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the Network Connections service:

- Internet Connection Sharing (ICS)

Network List Service

The Network List Service (netprofm) identifies the networks to which the computer has connected, collects and stores properties for these networks, and notifies applications when these properties change. This service, along with the Network Location Awareness service, enables the display of the status of network connections in the notification area. This service is part of the Network Diagnostics Framework.

This service is installed by default and its startup type is **Manual**.

When the Network List Service is started in its default configuration, it logs on by using the Local Service account.

The Network List Service is dependent upon the following system components:

- Network Location Awareness
- Network Store Interface Service
- NSI proxy service driver
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

- TCP/IP Protocol Driver

The following system component is dependent upon the Network List Service:

- HomeGroup Provider

Network Location Awareness

The Network Location Awareness (NlaSvc) service collects and stores network configuration information, such as IP address and domain name changes, in addition to location change information. This service notifies compatible applications when this information changes so that they can reconfigure themselves to use the current network connection. If this service stops, network location awareness functionality is not available.

This service is installed by default on Windows 7 and Windows Server 2008 R2, and its startup type is **Automatic**. If you configure this service with a startup type of **Manual**, dependent services usually start it.

When the Network Location Awareness service is started in its default configuration, it logs on by using the Network Service account.

The Network Location Awareness service is dependent upon the following system components:

- Network Store Interface Service
- NSI proxy service driver
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- TCP/IP Protocol Driver

The following system components are dependent upon the Network Location Awareness service:

- Network List Service
- HomeGroup Provider
- WWAN AutoConfig

Network Store Interface Service

The Network Store Interface Service (nsi) delivers network notification to client computers. The service keeps track of the network interfaces that are available on the computer, stores routing information for each interface, and communicates this information with other services that require it. Stopping this service causes loss of network connectivity.

This service is installed by default and its startup type is **Automatic**.

When Network Store Interface Service is started in its default configuration, it logs on by using the Local Service account.

The Network Store Interface service is dependent upon the following system component:

- NSI proxy service driver

The following system components are dependent upon the Network Store Interface service:

- DHCP Client
- WinHTTP Web Proxy Auto-Discovery Service
- DNS Client
- IP Helper
- Network Connections
- Internet Connection Sharing (ICS)
- Network Location Awareness
- Network List Service
- HomeGroup Provider
- WWAN Autoconfig
- Workstation
- Computer Browser
- Netlogon
- Remote Desktop Configuration

Offline Files

The Offline Files (CscService) service performs maintenance activities in the Offline Files cache, responds to user logon and logoff events, and dispatches events to accounts or logs that are configured to receive events related to Offline Files activities and changes in cache state.

The Offline Files service enables the user to designate particular network folders (and their subfolders) to be available offline. When the user is connected to the network, the Offline Files service automatically synchronizes the folders to the local hard disk drive. When the computer disconnects from the network, the Offline Files service provides access to the content from the locally cached copy. When the computer reconnects to the network, the service automatically synchronizes any changes that have been made in an offline file with the online version, and it updates the offline versions with recent changes to online versions.

We recommend that you use the Encrypting File System (EFS) to encrypt the Offline Files cache so that the files in the cache can only be accessed by the user on whose behalf it is cached.

This service is installed by default and its startup type is **Automatic** on computers running Windows 7 Professional, Windows 7 Ultimate, or Windows 7 Enterprise operating systems. The Offline Files service is not available on computers running the Windows 7 Starter, Windows 7 Home Basic, or Windows 7 Home Premium operating systems.

When the Offline Files service is started in its default configuration, it logs on by using the Local System account.

The Offline Files service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Parental Controls

The Parental Controls (WPCSvc) service provides backwards compatibility for Windows Vista parental controls. If you did not use Windows Vista parental controls, this service can be disabled.

This service is installed by default and its startup type is **Manual**.

When the Parental Controls service is started in its default configuration, it logs on by using the Local Service account.

The Parental Controls service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Peer Name Resolution Protocol

The Peer Name Resolution Protocol (PNRPsvc) service enables peer name resolution over the Internet without using a server. If this service is disabled, some peer-to-peer and collaborative applications may not function. This protocol enables the naming of computers and services without relying on a DNS server. This allows for flexible, informal, temporary networks of nearby computers for collaboration, data sharing, and data storage.

Security in peer-to-peer networks is difficult to establish. If computers in your organization are allowed to connect to peer-to-peer networks, a security policy about the types of information that is shared and the types of peer-to-peer networks that are compliant with your policy should be explicitly designed and communicated to your users. This helps users make decisions about which peer-to-peer networks they can trust.

A trusted peer-to-peer network should meet the following industry standards for establishing trust:

- Uses a trusted authentication method to identify the network and its users. Your security policy should identify which form of authentication is the minimally acceptable method.
- Supports different authorization levels to allow for control over who shares information by using the network.
- Supports encrypted data transmission so that when users collaborate over this network, their information is not as susceptible to capture by unauthorized users.

Provides some form of data-integrity checking, such as digital signatures, to ensure that the data was not modified in transit.

This service is installed by default and its startup type is **Manual**.

When the Peer Name Resolution Protocol service is started in its default configuration, it logs on by using the Local Service account.

The Peer Name Resolution Protocol service is dependent upon the following system component:

- Peer Networking Identity Manager

The following system components are dependent upon the Peer Name Resolution Protocol service:

- Peer Networking Grouping
- PNRP Machine Name Publication Service

Peer Networking Grouping

The Peer Networking Grouping (p2psvc) service supports peer "grouping," which is a technology that allows a developer to create a private peer-to-peer network. Administrators create the groups and invite members to join after verifying their credentials. Each member has a specific certificate, which is called a Group Member Certificate (GMC). The GMC ensures that all records exchanged between peers are digitally signed. The public key of a peer is contained in the structures that are passed as part of the communication between peers. The groups are opened and closed by the administrator as needed. This service supports the HomeGroup feature in Windows 7.

This service is installed by default and its startup type is **Manual**.

When the Peer Networking Grouping is started in its default configuration, it logs on by using the Local Service account.

The Peer Networking Grouping service is dependent upon the following system components:

- Peer Name Resolution Protocol
- Peer Networking Identity Manager

Peer Networking Identity Manager

The Peer Networking Identity Manager (p2pimsvc) service provides the identity service for peer networking. It allows the creation, enumeration, and manipulation of peer identities in a peer-to-peer application. An individual user can have several peer identities. This service supports the HomeGroup feature in Windows 7.

This service is installed by default and its startup type is **Manual**.

When the Peer Networking Identity Manager service is started in its default configuration, it logs on by using the Local Service account.

The Peer Networking Identity Manager service is not dependent upon any other system component.

The following system components are dependent upon the Peer Networking Identity Manager service:

- Peer Name Resolution Protocol
- Peer Networking Grouping
- PNRP Machine Name Publication Service

Performance Counter DLL Host

The Performance Counter DLL Host (PerfHost) service enables remote users and 64-bit applications to query the performance counters that are provided by 32-bit applications. If this service is stopped, only local users and 32-bit applications will be able to query the performance counters provided by 32-bit applications.

This service is installed by default on computers running the 64-bit version of Windows 7, and its startup type is **Manual**.

When the Performance Counter DLL Host service is started in its default configuration, it logs on by using the Local Service account.

The Performance Counter DLL Host service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Performance Logs & Alerts

The Performance Logs & Alerts (pla) service collects performance data from local or remote computers, based on preconfigured schedule parameters, and then writes the data to a log or triggers an alert. This service starts and stops each named performance data collection according to the information that is contained in the named log collection setting. This service only runs if at least one collection is scheduled.

If the Performance Logs & Alerts service stops or if you disable it, performance information is not collected. Also, any data collections that are currently active are terminated, and future scheduled collections will not occur.

This service is installed by default and its startup type is **Manual**.

When the Performance Logs & Alerts service is started in its default configuration, it logs on by using the Local Service account.

The Performance Logs & Alerts service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Plug and Play

The Plug and Play (PlugPlay) service enables a computer to recognize and adapt to hardware changes with little or no user input. This service enables you to add or remove devices without any detailed knowledge of the computer hardware, and you do not need to manually configure the hardware or the operating system. For example, you can plug in a USB keyboard, and the Plug and Play service detects the new device, finds a driver for it, and installs it. Or if you dock a portable computer and use the docking station's Ethernet card to connect to the network, you do not need to change any configuration settings. Later, you can undock the same computer and use a modem to connect to the network—again, without any manual configuration changes.

You cannot stop or disable the service through the Services snap-in console because of the impact on operating system stability. If this service stops, the Device Manager interface appears blank and no hardware devices are displayed.

This service is installed by default and its startup type is **Automatic**.

The Plug and Play service is not dependent upon any other system components.

The following system components are dependent upon the Plug and Play service:

- Fax
- Smart Card
- Tablet PC Input Service
- Telephony
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Internet Connection Sharing (ICS)

- Routing and Remote Access
- Virtual Disk
- Windows Audio Endpoint Builder
- Windows Audio
- Windows Driver Foundation–User-Mode Driver Framework
- Windows Biometric Service
- WWAN Autoconfig

PnP-X IP Bus Enumerator

The PnP-X IP Bus Enumerator (IPBusEnum) service manages the virtual network bus. It discovers network-connected devices by using SSDP or the WS-Discovery protocol and gives them presence in Plug and Play. If this service is stopped or disabled, presence of network-connected devices is not maintained in Plug and Play, and all Plug and Play scenarios stop functioning.

This service is installed by default in Windows 7, and the service startup type is **Manual**. In Windows Server 2008 R2, this service is installed, but disabled.

When the PnP-X IP Bus Enumerator is started in its default configuration, it logs on by using the Local System account.

The PnP-X IP Bus Enumerator service is dependent upon the following system components:

- Function Discovery Provider Host
- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the PnP-X IP Bus Enumerator service:

- Media Center Extender Service

PNRP Machine Name Publication Service

The PNRP Machine Name Publication Service (PNRPAutoReg) publishes a computer name by using the Peer Name Resolution Protocol (PNRP). You can publish the computer name as a

secured or unsecured peer name. The peer name configuration is managed by the following netsh command: **p2p pnrp peer**.

This service is installed by default and its startup type is **Manual**.

When the PNRP Machine Name Publication Service is started in its default configuration, it logs on by using the Local Service account.

The PNRP Machine Name Publication Service is dependent upon the following system components:

- Peer Name Resolution Protocol
- Peer Networking Identity Manager

Portable Device Enumerator Service

The Portable Device Enumerator Service (WPDBusEnum) enforces Group Policy settings for removable mass-storage devices. It enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content by using removable mass-storage devices. This service enables you to specify which portable storage devices are allowed to be connected to systems that are managed with Group Policy.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When the Portable Device Enumerator Service is started in its default configuration, it logs on by using the Local System account.

The Portable Device Enumerator Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Power

The Power service manages the power policy and power policy notification delivery.

This service is installed by default, and its startup type is **Automatic** on Windows 7 and **Manual** on Windows Server 2008 R2.

When the Power service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Print Spooler

The Print Spooler (Spooler) service manages all local and network print queues and controls all print jobs. The print spooler communicates with printer drivers and input/output (I/O) components, such as the USB port and the TCP/IP protocol suite, and it is the center of the Windows printing subsystem.

If the Print Spooler service stops, you cannot print or send faxes from your local computer. When the Print Spooler service stops on a server that runs Remote Desktop Services, the Easy Print feature will not work correctly.

The Printer Pruner feature of AD DS relies on the Print Spooler service. For the Printer Pruner to operate across the organization and allow orphaned queues to be scavenged on an unmanaged basis, every site in the organization must have at least one domain controller that runs the Print Spooler service.

This service is installed by default in Windows Server 2008 R2 and Windows 7, and its startup type is **Automatic**. If you configure the service startup type to **Disabled** or **Manual**, it does not automatically start when print jobs are submitted.

When the Print Spooler service is started in its default configuration, it logs on by using the Local System account, and it is allowed to interact with the desktop.

The Print Spooler service is dependent upon the following system components:

- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent upon the Print Spooler service:

- Fax
- LPD Service

Problem Reports and Solutions Control Panel Support

The Problem Reports and Solutions Control Panel Support (wercplsupport) service provides support for viewing, sending, and deleting system-level reports for the Problem Reports and Solutions Control Panel. This service is part of the Windows Diagnostic Infrastructure.

This service is installed by default and its startup type is **Manual**.

When the Problem Reports and Solutions Control Panel Support service is started, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Program Compatibility Assistant Service

The Program Compatibility Assistant Service (PcaSvc) provides support for the Program Compatibility Assistant. If this service is stopped, the Program Compatibility Assistant does not function properly. The Program Compatibility Assistant Service attempts to find software and driver updates that improve the compatibility of applications with Windows 7. The Program Compatibility Assistant Service runs automatically when it detects that an older program is attempting to run in Windows 7 and is encountering problems. Then it makes changes to the computer's configuration so that the program can run better.

This service is installed by default and its startup type is **Manual**.

When the Program Compatibility Assistant Service is started in its default configuration, it logs on by using the Local System account.

The Program Compatibility Assistant Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Protected Storage

The Protected Storage service protects sensitive information that is stored, such as private keys, and prevents access by unauthorized services, processes, or users. The service provides a set of software libraries that allow applications to retrieve security and other information from personal storage locations, and it hides the implementation and details about the storage.

The storage location that is provided by this service is protected from modification. The Protected Storage service uses the Hash-Based Message Authentication Code (HMAC) and the Secure Hash Algorithm 1 (SHA1) cryptographic hash function to encrypt the user's master key. This component requires no configuration.

If the Protected Storage service stops, private keys are inaccessible, the Certificate Services service does not operate, Secure/Multipurpose Internet Mail Extensions (S/MIME) and SSL do not work, and smart card logon fails.

This service is installed by default and its startup type is **Manual**.

When the Protected Storage service is started in its default configuration, it logs on by using the Local System account.

The Protected Storage service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Quality Windows Audio Video Experience

The Quality Windows Audio Video Experience (qWave) service is a networking platform for audio/video (A/V) streaming applications on IP home networks.

The platform for the Quality Windows Audio Video Experience service enhances A/V streaming performance and reliability by ensuring network Quality of Service (QoS) for A/V applications. It provides mechanisms for admission control, run-time monitoring and enforcement, application feedback, and traffic prioritization. The platform for the Quality Windows Audio Video Experience service provides the functionality for socket-based applications to gather in-depth, real-time information of a variable bandwidth network, allowing it to dynamically adapt to changing network conditions. It also allows applications to prioritize packets to make better use of the available bandwidth.

This service is installed by default and its startup type is **Manual**.

When the Quality Windows Audio Video Experience service is started in its default configuration, it logs on by using the Local Service account.

The Quality Windows Audio Video Experience service is dependent upon the following system components:

- Link-Layer Topology Discovery Mapper I/O Driver
- QoS Packet Scheduler
- QWAVE driver
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Remote Access Auto Connection Manager

The Remote Access Auto Connection Manager (RasAuto) service detects unsuccessful attempts to connect to a remote network or computer, and it provides alternative methods for connection. When a program fails in an attempt to reference a remote DNS or NetBIOS name or address or when network access is unavailable, the service displays a dialog box that allows you to make a dial-up or VPN connection to the remote computer.

The Remote Access Auto Connection Manager service maintains a local database of connections that were previously used to reach named computers or shared folders. When the service detects an unsuccessful attempt to reach a remote computer or shared folder, it offers to dial the connection that was last used to reach this remote device. It is started automatically on an as-needed basis. If you disable the Remote Access Auto Connection Manager service, you must manually establish connections to remote computers when you want to access them.

This service is installed by default and its startup type is **Manual**.

When the Remote Access Auto Connection Manager service is started in its default configuration, it logs on by using the Local System account.

The Remote Access Auto Connection Manager service is dependent on the following system components:

- Remote Access Auto Connection Driver
- Remote Access Connection Manager
- Secure Socket Tunneling Protocol Service
- Telephony
- Plug and Play
- Remote Procedure Call (RPC)

- DCOM Server Process Launcher
- RPC Endpoint Mapper

Remote Access Connection Manager

The Remote Access Connection Manager (RasMan) service manages dial-up and VPN connections from the computer to the Internet or other remote networks. When you double-click a connection in the Network Connections folder and then click the **Connect** button, the Remote Access Connection Manager service dials the connection or sends a VPN connection request. It then handles subsequent negotiations with the remote access server to set up the connection.

The Remote Access Connection Manager service is inactive when no requests are pending. The Network Connections folder calls this service to enumerate the set of connections and to display the status of each one.

If the Remote Access Connection Manager service stops or if you disable it, the computer cannot make dial-up or VPN connections to a remote network or accept inbound connection requests. Also, the Network Connections folder does not display any VPN or dial-up connections, and the Internet Options Control Panel does not allow the user to configure any options that pertain to dial-up or VPN connections.

This service is installed by default and its startup type is **Manual**.

When the Remote Access Connection Manager service is started in its default configuration, it logs on by using the Local System account.

The Remote Access Connection Manager service is dependent upon the following system components:

- Secure Socket Tunneling Protocol Service
- Telephony
- Plug and Play
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent upon the Remote Access Connection Manager service:

- Internet Connection Sharing (ICS)
- Remote Access Auto Connection Manager
- Routing and Remote Access

Remote Desktop Configuration

The Remote Desktop Configuration (SessionEnv) service is responsible for all Remote Desktop Services and Remote Desktop-related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, remote desktop themes, and remote desktop certificates.

This service is installed by default and its startup type is **Manual**.

When the Remote Desktop Configuration service is started in its default configuration, it logs on by using the Local System account.

The Remote Desktop Configuration service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Workstation
- Browser Support Driver
- Network Store Interface Service
- NSI proxy service driver
- SMB 1.x MiniRedirector
- SMB MiniRedirector Wrapper and Engine
- Redirected Buffering Sub System
- Mup
- SMB 2.0 MiniRedirector

Remote Desktop Services

The Remote Desktop Services (TermService) service allows users to connect interactively to a remote computer. To prevent remote use of this computer: in the Control Panel, in **System properties**, clear the check boxes on the **Remote** tab.

This service is installed by default and its startup type is Manual.

When the Remote Desktop Services service is started in its default configuration, it logs on by using the Local System account.

The Remote Desktop Services service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Terminal Device Driver

The following system components are dependent on the Remote Desktop Services service:

- Remote Desktop
- Remote Desktop Session Host Server
- Media Center Extender Service
- Remote Desktop Services UserMode Port Redirector

Remote Desktop Services UserMode Port Redirector

The Remote Desktop Services UserMode Port Redirector (UmRdpService) service allows the redirection of printers, drives, and ports for Remote Desktop connections.

This service is installed by default with Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise in addition to all versions of Windows Server 2008 R2. It is not available on Windows 7 Starter, Windows 7 Home Basic, or Windows 7 Home Premium.

Its service startup type is Manual.

When started in the default configuration it will log on using the Local System account.

The Remote Desktop Services UserMode Port Redirector service is dependent upon the following system components:

- Remote Desktop Services

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Terminal Device Driver
- Terminal Service Device Redirector Driver
- Redirected Buffering Sub System
- Mup

Remote Procedure Call (RPC)

The Remote Procedure Call (RPCSS) service is an interprocess communication (IPC) mechanism that enables data exchange and solicits functionality from another process. That process can be on the same computer, on the local area network, or across the Internet. The Remote Procedure Call (RPC) service serves as the RPC endpoint mapper and COM Service Control Manager (SCM).

You cannot stop or disable the Remote Procedure Call (RPC) service. The service runs under the Network Service account. If this service is not available, the operating system does not load.

The Remote Procedure Call (RPC) service is dependent on the following system components:

- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent on the Remote Procedure Call (RPC) service:

- ActiveX Installer
- Application Identity
- Application Information
- Background Intelligent Transfer Service
- Base Filtering Engine
- Bluetooth Support Service
- Certificate Propagation
- CNG Key Isolation
- COM+ Event System

- COM+ System Application
- Computer Browser
- Credential Manager
- Cryptographic Services
- Disk Defragmenter
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- Encrypting File System (EFS)
- Extensible Authentication Protocol
- Fax
- Function Discovery Provider Host
- Function Discovery Resource Publication
- Group Policy Client
- Health Key and Certificate Management
- HomeGroup Listener
- HomeGroup Provider
- IIS Admin Service
- IKE and AuthIP IPsec Keying Modules
- Indexing Service
- Internet Connection Sharing (ICS)
- IP Helper
- IPsec Policy Agent
- KtmRm for Distributed Transaction Coordinator
- Link-Layer Topology Discovery Mapper
- LPD Service
- Media Center Extender Service

- Message Queuing
- Message Queuing Triggers
- Microsoft FTP Service
- Microsoft Software Shadow Copy Provider
- Net.Msmq Listener Adapter
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter
- Network Access Protection Agent
- Network Connections
- Network List Service
- Network Location Awareness
- Offline Files
- Parental Controls
- Performance Logs & Alerts
- PnP-X IP Bus Enumerator
- Portable Device Enumerator Service
- Print Spooler
- Program Compatibility Assistant Service
- Protected Storage
- Quality Windows Audio Video Experience
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode Port Redirector
- Remote Registry

- RIP Listener
- Routing and Remote Access
- Security Accounts Manager
- Security Center
- Server
- Shell Hardware Detection
- Smart Card Removal Policy
- Software Protection
- SPP Notification Service
- Superfetch
- System Event Notification Service
- Tablet PC Input Service
- Task Scheduler
- Telephony
- Telnet
- User Profile Service
- Virtual Disk
- Volume Shadow Copy
- Windows Audio
- Windows Backup
- Windows Biometric Service
- Windows Color System
- Windows Connect Now–Config Registrar
- Windows Defender
- Windows Firewall
- Windows Image Acquisition (WIA)

- Windows Installer
- Windows Live Family Safety
- Windows Management Instrumentation
- Windows Media Center Scheduler Service
- Windows Process Activation Service
- Windows Remote Management (WS-Management)
- Windows Search
- Windows Update
- Wired AutoConfig
- WLAN AutoConfig
- World Wide Web Publishing Service
- WWAN AutoConfig

Remote Procedure Call (RPC) Locator

The Remote Procedure Call (RPC) Locator service enables RPC clients that use the RpcNs* APIs to locate RPC servers. RpcNs* APIs are not used internally in the Windows operating system, so you only need to start this service if non-Microsoft applications require this service.

In Windows Vista and Windows 7, this service does not provide any functionality, and it is present only for application compatibility. In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service managed the RPC name service database.

If the Remote Procedure Call (RPC) Locator service stops or if you disable it, RPC clients that must locate RPC services on other computers cannot locate servers, or they may fail to start.

RPC clients that rely on RpcNs* APIs from the same computer may not find RPC servers that support a given interface. If the service stops or if you disable it on a domain controller, RPC clients that use the RpcNs* APIs and the domain controller may experience interruption of service when they try to locate clients.

This service is installed by default, and the startup type is **Manual**.

This service is not dependent on any other system service, nor is any service dependent on it.

Remote Registry

The Remote Registry service enables remote users who have the appropriate permissions to modify registry settings on the domain controller. The service's default configuration allows only members of the Administrators and Backup Operators groups to access the registry remotely. This service is required for the Microsoft Baseline Security Analyzer (MBSA) tool. MBSA enables you to verify which patches are installed on each of the servers in your organization.

If the Remote Registry service stops, only the registry on the local computer can be modified. If you disable this service, any services that explicitly depend on the service cannot start, but registry operations on your local computer are not affected. However, other computers or devices cannot connect to your local computer's registry.

This service is installed by default, and its startup type is **Automatic**.

The Remote Registry service is dependent upon the following system components:

When the Remote Registry service is started in its default configuration, it logs on by using the Local Service account.

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

RIP Listener

The RIP Listener (iprip) service listens for route updates that are sent by routers that use the Routing Information Protocol (RIP). RIP Listener is an optional networking component that you can install through the **Turn Windows features on or off** item in Control Panel. When started, the RIP Listener service listens for RIP v1 and RIP v2 traffic, and it uses the received RIP messages to update its routing tables.

This service is installed by default and its startup type is **Automatic**.

When the RIP Listener service is started in its default configuration, it logs on by using the Local Service account.

The RIP Listener service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Resultant Set of Policy Provider

The Resultant Set of Policy Provider (RSOPProv) service enables you to connect to a domain controller, access the WMI database for that computer, and simulate the application of a given set of Group Policy settings which is known as the Resultant Set of Policy (RSOP). This simulation is commonly referred to as the RSOP Planning mode.

If this service stops on a domain controller, the RSOP Planning mode simulation is unavailable on that domain controller. RSOP must run only on domain controllers; member servers and workstations do not need to run this service to be included in the planning mode simulation.

This service is installed by default in Windows Server 2008 R2 and its startup type is **Manual**.

When the Resultant Set of Policy Provider service is started in its default configuration, it logs on by using the Local System account.

The Resultant Set of Policy Provider service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Routing and Remote Access

The Routing and Remote Access (RemoteAccess) service provides multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services. This service also provides dial-up and VPN remote access services. Your server can use this service to function as a remote access server, a VPN server, a gateway, or a branch-office router.

From a routing perspective, the Routing and Remote Access service supports the Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) routing protocols, and it controls the routing tables for the TCP/IP stack-forwarding engine.

The Routing and Remote Access service must be explicitly enabled to support remote access scenarios. If you support remote access and this service stops, the computer cannot accept incoming RAS, VPN, or dial-on-demand connections, and routing protocols are not received or transmitted.

The Routing and Remote Access service is installed by default, and its startup type is **Disabled**.

The Routing and Remote Access service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

RPC Endpoint Mapper

The RPC Endpoint Mapper (RpcEptMapper) service resolves RPC interface identifiers to transport endpoints. You cannot stop or disable the RPC Endpoint Mapper service. The service runs under the Network Service account. If this service is not available, the operating system does not load.

This service is installed by default and its startup type is **Automatic**.

The RPC Endpoint Mapper service is not dependent on any other system components.

The following system components are dependent on the RPC Endpoint Mapper service:

- ActiveX Installer
- Application Identity
- Application Information
- Background Intelligent Transfer Service
- Base Filtering Engine
- Bluetooth Support Service
- Certificate Propagation
- CNG Key Isolation
- COM+ Event System
- COM+ System Application
- Computer Browser
- Credential Manager
- Cryptographic Services
- Disk Defragmenter
- Distributed Link Tracking Client
- Distributed Transaction Coordinator

- Encrypting File System (EFS)
- Extensible Authentication Protocol
- Fax
- Function Discovery Provider Host
- Function Discovery Resource Publication
- Group Policy Client
- Health Key and Certificate Management
- HomeGroup Listener
- HomeGroup Provider
- IIS Admin Service
- IKE and AuthIP IPsec Keying Modules
- Indexing Service
- Internet Connection Sharing (ICS)
- IP Helper
- IPsec Policy Agent
- KtmRm for Distributed Transaction Coordinator
- Link-Layer Topology Discovery Mapper
- LPD Service
- Media Center Extender Service
- Message Queuing
- Message Queuing Triggers
- Microsoft FTP Service
- Microsoft Software Shadow Copy Provider
- Net.Msmq Listener Adapter
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter

- Network Access Protection Agent
- Network Connections
- Network List Service
- Network Location Awareness
- Offline Files
- Parental Controls
- Performance Logs & Alerts
- PnP-X IP Bus Enumerator
- Portable Device Enumerator Service
- Print Spooler
- Program Compatibility Assistant Service
- Protected Storage
- Quality Windows Audio Video Experience
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode Port Redirector
- Remote Procedure Call (RPC)
- Remote Registry
- RIP Listener
- Routing and Remote Access
- Security Accounts Manager
- Security Center
- Server
- Shell Hardware Detection

- Smart Card Removal Policy
- Software Protection
- SPP Notification Service
- Superfetch
- System Event Notification Service
- Tablet PC Input Service
- Task Scheduler
- Telephony
- Telnet
- User Profile Service
- Virtual Disk
- Volume Shadow Copy
- Windows Audio
- Windows Backup
- Windows Biometric Service
- Windows Color System
- Windows Connect Now—Config Registrar
- Windows Defender
- Windows Firewall
- Windows Image Acquisition (WIA)
- Windows Installer
- Windows Live Family Safety
- Windows Management Instrumentation
- Windows Media Center Scheduler Service
- Windows Process Activation Service
- Windows Remote Management (WS-Management)

- Windows Search
- Windows Update
- Wired AutoConfig
- WLAN AutoConfig
- World Wide Web Publishing Service
- WWAN AutoConfig

SeaPort

The SeaPort service enables detecting, downloading, and installing up-to-date configuration files for Microsoft search enhancement applications. It also provides server communication for the Customer Experience Improvement Program. If this service is disabled, search enhancement features such as search history may not work correctly.

This service is not installed by default. It is installed with Windows Live Essentials as an enhancement to the default Windows Search service. After it is installed, its startup type is **Automatic**.

When the SeaPort service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Secondary Logon

The Secondary Logon (seclogon) service enables processes to be started under alternate credentials. This allows a user to create processes in the context of different security principals. A common use of this service is by administrators who may log on as restricted users but must have administrative privileges to run a specific application. They can use a secondary logon to temporarily run such applications. If the service is disabled, this type of logon access is unavailable and calls to the `CreateProcessWithLogonW` API fail.

This service starts when a program or application is started by using the **Run as different user** option in the extended context menu (which can be opened by holding down the shift key when you right-click an item).

This service is installed by default and its startup type is **Manual**.

When the Secondary Logon service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Secure Socket Tunneling Protocol Service

The Secure Socket Tunneling Protocol Service (SstpSvc) provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers by using virtual private networking (VPN). If this service is disabled, users will not be able to use SSTP to access remote servers.

This service is installed by default and its startup type is **Manual**.

When the Secure Socket Tunneling Protocol Service is started in its default configuration, it logs on by using the Local Service account.

The Secure Socket Tunneling Protocol Service is not dependent on any other system service.

The following system components are dependent on the Secure Socket Tunneling Protocol Service.

- Remote Access Connection Manager
- Internet Connection Sharing
- Remote Access Auto Connection Manager
- Routing and Remote Access

Security Accounts Manager

The Security Accounts Manager (SamSs) service is a protected subsystem that manages user and group account information. The startup of the Security Accounts Manager service signals to other services that it is ready to accept requests.

Do not attempt to disable this service. If you disable this service, other services in the computer may not start correctly.

This service is installed by default and its startup type is **Automatic**.

When the Security Accounts Manager service is started in its default configuration, it logs on by using the Local System account.

The Security Accounts Manager service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher

- RPC Endpoint Mapper

The following system components are dependent upon the Security Accounts Manager service:

- Distributed Transaction Coordinator
- KtmRm for Distributed Transaction Coordinator
- Server
- Computer Browser
- HomeGroup Listener

Security Center

The Security Center (wscsvc) service monitors and reports security health settings on the computer. The health settings include whether the firewall is turned on, the current status of the installed antivirus application, the current status of the installed antispyware application, the current Windows Update setting, whether User Account Control is turned on, and whether the recommended Internet settings are in use.

The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service. The Action Center uses the service to provide alerts in the notification area and a graphical view of the security health states in the Action Center Control Panel. Network Access Protection (NAP) uses this service to report the security health states of client computers to the NAP Network Policy Server to make network quarantine decisions. The service also has a public API that allows external consumers to programmatically retrieve the aggregated security health state of the system.

If you disable the Security Center service, the protected components continue to function in accordance with their specific configuration settings. However, no centralized monitor service is provided.

This service is installed by default and its startup type is **Automatic (Delayed Start)**.

When the Security Center service is started in its default configuration, it logs on by using the Local Service account.

The Security Center service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

- Windows Management Instrumentation

Server

The Server service provides RPC support, file printing, and named-pipe sharing over the network. It allows local resources, such as disks and printers, to be shared so that other users on the network can access them. It also allows named-pipe communication for applications that run between computers. Named-pipe communication reserves memory for the output of one process to be used as input for another process. The input-acceptance process does not need to be local to the computer.

If the Server service stops or if you disable it, the computer cannot share local files and printers with other computers on the network, and it cannot satisfy remote RPC requests.

The Server service is installed by default and its startup type is **Automatic**.

When the Server service is started in its default configuration, it logs on by using the Local System account.

The Server service is dependent upon the following system components:

- Security Accounts Manager
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Server SMB 1.xxx Driver
- Server SMB 2.xxx Driver

The following system components are dependent on the Server service:

- Computer Browser
- HomeGroup Listener

Shell Hardware Detection

The Shell Hardware Detection (ShellHWDetection) service monitors and provides notification for AutoPlay hardware events. AutoPlay is a feature that detects content such as pictures, music, or video files on a removable storage device. AutoPlay then automatically starts applications to play or display that content, which simplifies the use of specialized peripheral devices such as MP3 players and digital photo readers. The service also makes it easier for users because they

do not need to know beforehand what software applications are needed to access various content types.

AutoPlay supports a variety of media content types and applications. Independent hardware vendors (IHVs) and independent software vendors (ISVs) can extend this support to include their devices and applications. A user can configure AutoPlay for any combination of pictures, music files, and video.

Media and device types that are supported by AutoPlay include:

- Removable storage devices, including a USB flash drive, an external or removable drive, a CF card, or other types of external storage devices that can be easily removed from a computer
- PC cards
- External hot-plug USB or 1394 fixed drives
- Supported content types, which include:
 - Pictures (.jpg, .bmp, .gif, and .tif files)
 - Music files (.mp3 and .wma files)
 - Video (.mpg and .asf files)

If the service stops, the Hardware AutoPlay functionality does not work and shell performance is also affected.

This service is installed by default on Windows 7 and Windows Server 2008 R2, and its startup type is **Automatic**.

When the Shell Hardware Detection service is started in its default configuration, it logs on by using the Local System account.

The Shell Hardware Detection service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the Shell Hardware Detection Service:

- Windows Image Acquisition (WIA)

Simple TCP/IP Services

Simple TCP/IP Services (simptcp) implements support for the following protocols and ports:

- 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

When you enable Simple TCP/IP Services, all five protocols are enabled on all adapters. There is no ability to selectively enable specific services or enable the service on per-adapter basis.

If you stop or disable Simple TCP/IP Services, the rest of the operating system is unaffected. We recommend that you do not install this service unless you specifically need a computer to support communication with other computers that use the referenced protocols.

This service is not installed by default, and it must be added through the **Turn Windows Features on or off** dialog box in the **Programs** area of Control Panel.

When Simple TCP/IP Services is started it logs on by using the Local Service account by default.

Simple TCP/IP Services is dependent upon the following system component:

- Ancillary Function Driver for Winsock

Smart Card

The Smart Card (SCardSvr) service manages and controls access to a smart card that is inserted into a smart card reader that is connected to the computer. The smart card subsystem is based on Personal Computer/Smart Card (PC/SC) Workgroup consortium standards. For more information, see [PC/SC Workgroup](#).

The Resource Manager component manages the access to readers and smart cards. To manage these resources, the Resource Manager performs the following functions:

- Identifies and tracks resources
- Allocates readers and resources across multiple applications
- Supports transaction primitives to access services that are available on a given card

If this service stops, the computer is unable to read smart cards.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When the Smart Card service is started in its default configuration, it logs on by using the Local Service account.

The Smart Card service is dependent upon the following system component:

- Plug and Play

Smart Card Removal Policy

The Smart Card Removal Policy (SCPolicySvc) service allows the system to be configured to lock the user desktop, disconnect from Remote Desktop sessions, or log off the user upon smart card removal. Users who walk away from computers that are running an active logon session create a security risk. To enforce the security of your system, it is best practice for users to disconnect from Remote Desktop sessions and log off or lock their computers when they leave. The Smart Card Removal Policy service allows you to force users to comply with this practice when they remove their smart cards.



Note

If you decide to force the logoff, users must ensure that they have saved changes to documents and other files before they remove their smart cards. Otherwise, they may lose any changes they have made.

Whether you use the Smart Card Removal Policy service depends on how your users interact with their computers. For example, this policy might be used for computers in an open floor or kiosk environment. This policy may not be necessary when users have dedicated computers or exclusive use of multiple computers. You can use a password-protected screensaver or other means to lock the computers of these users.

This service is installed by default and its startup type is **Manual**.

When the Smart Card Removal Policy service is started in its default configuration, it logs on by using the Local System account.

The Smart Card Removal Policy service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

SNMP Service

The SNMP Service allows inbound Simple Network Management Protocol (SNMP) requests to be serviced by the local computer. This service includes agents that monitor activity in network devices and report to the network console workstation. It also provides a way to manage network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally located computer that runs network management software. SNMP performs management services through a distributed architecture of management computers and agents.

The SNMP Service also includes an SNMP agent that allows remote, centralized management of computers and services.

The SNMP Service is only installed on the computer if you manually install the optional SNMP feature. If the SNMP service stops or if you disable it, the computer no longer responds to SNMP requests. If the computer is being monitored by network management tools that rely on SNMP, they cannot collect data from the computer nor control its functionality through the service.

When this service is installed, its startup type is **Automatic**.

When the SNMP Service is started in its default configuration, it logs on by using the Local System account.

SNMP Trap

The SNMP Trap service receives trap messages, which contain information about specific events and are generated by local or remote SNMP agents. The service forwards the messages to SNMP management programs that run on the computer. When configured for an agent, the SNMP service generates trap messages if any specific events occur, and these messages are sent to a trap destination. For example, an agent can be configured to initiate an authentication trap if an unrecognized management computer sends a request for information. Trap destinations consist of the computer name, and the IP address of the management computer. The trap destination must be a network-enabled host that runs SNMP management software. Trap destinations can be configured by a user, but the events (such as restarting the computer) that generate trap messages are internally defined by the SNMP agent.

If the service stops or if you disable it, SNMP-based programs on the computer do not receive SNMP trap messages from other computers. If this computer monitors network devices or server applications with SNMP traps, significant computer events are lost.

This service is installed by default and its startup type is **Manual**.

When the SNMP Trap service is started in its default configuration, it logs on by using the Local Service account.

Software Protection

The Software Protection (sppsvc) service enables downloading, installing, and enforcing digital licenses for the Windows operating system and applications. If the service is disabled, the operating system and licensed applications will run in a notification mode. It is strongly recommended that you not disable the Software Protection service.

This service is installed by default and its startup type is **Automatic**.

When the Software Protection service is started in its default configuration, it logs on by using the Network Service account.

The Software Protection service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Special Administration Console Helper

The Special Administration Console Helper (sacsvr) service provides the ability to perform remote management tasks on a computer that is running Windows Server 2008 R2, if the computer's functions are halted due to a Stop error message. The Windows Emergency Management Services component supports two out-of-band console interfaces: the Special Administration Console (SAC) and **!SAC**, which offers a subset of SAC commands for use when the server has been halted.

The SAC and **!SAC** components accept input and send output through the out-of-band port. SAC is a separate entity from **!SAC** and the command-line environments in Windows Server 2008 R2. After a specific failure point is reached, Emergency Management Services components determine when to shift from SAC to **!SAC**. **!SAC** becomes available automatically if SAC fails to load or does not function.

The Special Administration Console Helper service allows you to create inbound communication channels through the Command Prompt window. If the Special Administration Console Helper service stops, SAC services are not available.

This service is installed by default in Windows Server 2008 R2, and its startup type is **Manual**.

When the Special Administration Console Helper service is started in its default configuration, it logs on by using the Local System account.

SPP Notification Service

The SPP Notification Service (sppuinotify) provides activation and notification for software licensing.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When The SPP Notification Service is started in its default configuration, it logs on by using the Local Service account.

The SPP Notification is dependent on the following system components:

- COM+ Event System
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

SSDP Discovery

The SSDP Discovery (SSDPSRV) service discovers networks devices and services that use the simple service discovery protocol (SSDP), such as Universal Plug and Play (UPnP) devices. For example, the UPnP Device Host service uses SSDP to locate and identify UPnP-certified network devices and service. The SSDP Discovery service also announces SSDP devices and services that are running on the local computer.

The service is started only when the computer attempts to locate and configure UPnP-certified devices. If you disable this service, the computer is cannot find UPnP-certified devices on the network and the UPnP Device Host service cannot find and interact with UPnP-certified devices.

This service is installed by default in Windows 7, and its startup type is **Manual**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Disabled**.

When the SSDP Discovery service is started in its default configuration, it logs on by using the Local Service account.

The SSDP Discovery service is dependent on the following system component:

- HTTP

The following system components are dependent on the SSDP Discovery service:

- Media Center Extender Service

- UPnP Device Host

Storage Service

The Storage Service (StorSvc) enforces Group Policy settings for storage devices. It is only available for computers running Windows 7 Professional or Windows 7 Enterprise.

This service is installed by default and its startup type is **Manual**.

When the Storage Service is started in its default configuration, it logs on by using the Local System account.

Superfetch

The Superfetch (Sysmain) service maintains and improves system performance. The Superfetch service is part of a collection of performance-enhancing features that address responsiveness issues related to demand paging. We do not recommend using the Superfetch service on servers unless the server is being used as a workstation.

This service is installed by default in Windows 7, and its startup type is **Automatic**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Disabled**.

When the Superfetch service is started in its default configuration, it logs on by using the Local System account.

The Superfetch service is dependent on the following system components:

- File Information FS MiniFilter
- FltMgr
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

System Event Notification Service

The System Event Notification Service (SENS) monitors and tracks computer events such as logon, network, and power events in the Windows operating system. It also notifies the COM+ Event System service subscribers for these events.

If the System Event Notification service stops, subscribers to the COM+ Event System service do not receive event notifications and the following problems occur:

- The following Win32 APIs do not work: IsNetworkAlive and IsDestinationReachable. These APIs are typically used by mobile applications on portable computers.
- ISENS* interfaces do not work, and SENS logon and logoff notifications fail.
- SyncMgr (Mobsync.exe) does not work properly due to its dependency on network connectivity information and logon notifications from SENS.
- The COM+ Event System fails when it tries to notify SENS of events.
- The Volume Shadow Copy Service does not load properly, which causes the Windows Server Backup API to fail.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Automatic**.

When the System Event Notification Service is started in its default configuration, it logs on by using the Local System account.

The System Event Notification service is dependent upon the following system components:

- COM+ Event System
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent upon the System Event Notification Service:

- COM+ System Application

Tablet PC Input Service

The Tablet PC Input Service (TabletInputService) enables Tablet PC pen-and-ink functionality. This allows any edition of Windows 7 to be installed on a Tablet PC. It also allows users to use an external pen and touch input device.

If the computer does not have tablet functionality or an external pen and touch input device, you should consider disabling this service.

This service is installed by default and its startup type is **Manual**.

When the Tablet PC Input Service is started in its default configuration, it logs on by using the Local Service account.

The Tablet PC Input Service is dependent upon the following system components:

- Plug and Play
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Task Scheduler

The Task Scheduler (Schedule) service enables you to configure and schedule automated tasks on the computer. The service monitors whatever criteria you choose, and it carries out the tasks when the criteria are met.

The Task Scheduler service supports a security isolation model that runs tasks in separate sessions according to their security content. As part of this isolation mode, tasks performed for different users are started in separate sessions, completely isolated from one another and from tasks that are running in the SYSTEM context. If passwords are required, they are encrypted and stored in Credential Manager, and they are retrieved as necessary.

If the Task Scheduler service stops, scheduled tasks do not run at their scheduled times or intervals.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Automatic**.

When the Task Scheduler service is started in its default configuration, it logs on by using the Local System account. It cannot be configured to log on using another account.

The Task Scheduler service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Event Log

TCP/IP NetBIOS Helper

The TCP/IP NetBIOS Helper (lmhosts) service provides support for the NetBIOS over TCP/IP (NetBT) service, and it provides NetBIOS name resolution for clients on your network. It enables users to share files, print, and log on to the network. Specifically, the service performs DNS name resolution and pings a set of IP addresses that return a list of accessible IP addresses to provide support for the NetBT service.

If this service stops or if you disable it, client computers that use applications that rely on NetBIOS or WINS may not be able to share files or printers, or log on to their computers

This service is installed by default in Windows Server 2008 R2 and Windows 7, and its startup type is **Automatic**.

When the TCP/IP NetBIOS Helper service is started in its default configuration, it logs on by using the Local Service account.

The TCP/IP NetBIOS Helper service is dependent upon the following system components:

- Ancillary Function Driver for Winsock
- NetBT
- NetIO Legacy TDI Support Driver
- TCP/IP Protocol Driver

Telephony

The Telephony (TapiSrv) service provides support for programs that control telephony devices on the local computer and on servers that are also running the service through the LAN. This service is required for dial-up modem connectivity.

This service is installed by default, and its startup type is **Manual**.

When the Telephony (TapiSrv) service is started in its default configuration, it logs on by using the Network Service account.

The Telephony service is dependent upon the following system components:

- Plug and Play
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent upon the Telephony service:

- Fax
- Remote Access Auto Connection Manager
- Remote Access Connection Manager

- Internet Connection Sharing (ICS)

Themes

The Themes service provides theme-management services for the graphic user interface. A desktop theme is a predefined set of icons, fonts, colors, sounds, and other elements that give the computer desktop a unified and distinctive look.

In Windows 7, if the Themes service stops or if you disable it, the visual style (including the windows, buttons, scrollbars, **Start** button, and other controls) revert to the Windows Classic visual style.

This service is installed by default in Windows 7, and its startup type is **Automatic**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Disabled**.

When the Themes service is started in its default configuration, it logs on by using the Local System account.

Thread Ordering Server

The Thread Ordering Server (THREADORDER) service provides ordered execution for a group of threads within a specific period of time. It ensures that each client thread runs once during the specific period and in a relative order.

This service is installed by default and its startup type is **Manual**.

When the Thread Ordering Server service is started in its default configuration, it logs on by using the Local Service account.

This service is not dependent on any other system service, nor is any service dependent on it.

TPM Base Services

TPM Base Services (TBS) enables access to the Trusted Platform Module (TPM), which provides hardware-based cryptographic services to system components and applications. TPM Base Services component centralizes TPM access across applications. It also virtualizes certain limited TPM resources. TPM Base Services uses priorities that are specified by calling applications to cooperatively schedule TPM access.

TPM Base Services is an optional system service that allows transparent sharing of the TPM resources. It simultaneously shares these resources among multiple applications on the same physical computer, even if those applications run on different virtual machines.

TPM Base Services runs as a system service in the Windows Server 2008 R2 and Windows 7 operating systems. It provides services to other components as an API exposed through remote procedure calls (RPC).

If this service is stopped or disabled, an application cannot use keys that are protected by the TPM.

This service installed by default and its startup type is **Manual**.

When TPM Base Services is started in its default configuration, it logs on by using the Local Service account.

This service is not dependent on any other system service, nor is any service dependent on it.

UPnP Device Host

The UPnP Device Host (upnphost) service supports peer-to-peer UPnP functionality for network devices. This service simplifies device and network service installation and management and accomplishes device and service discovery and control through driverless, standards-based protocol mechanisms.

UPnP-certified devices can automatically configure network addresses, announce their presence on a network subnet, and enable the exchange of device and service descriptions. When the UPnP Device Host service is installed, a computer can act as a UPnP-certified control point to discover and control the devices through a web or application interface.

This service is installed by default in Windows 7, and its startup type is **Manual**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Disabled**.

When the UPnP Device Host service is started in its default configuration, it logs on by using the Local Service account.

The UPnP Device Host service is dependent upon the following system components:

- HTTP
- SSDP Discovery

User Profile Service

The User Profile Service (ProfSvc) is responsible for loading and unloading user profiles. If this service is stopped or disabled, users cannot successfully log on or log off, applications may have problems getting to users' data, and components that are registered to receive profile event notifications do not receive them. This service should not be stopped or disabled.

This service is installed by default and its startup type is **Automatic**.

When the User Profile Service is started in its default configuration, it logs on by using the Local System account.

The User Profile Service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system component is dependent on the User Profile Service:

- Application Information

Virtual Disk Service

The Virtual Disk Service (VDS) provides a single interface to manage block storage virtualization, whether it is managed in the operating system software, the redundant array of independent disks (RAID) storage hardware subsystems, or other virtualization engines.

VDS provides a vendor-neutral and technology-neutral interface to manage logical volumes (software) and logical units (hardware). You can use this interface to manage bind operations, topology discovery and tracking, volume status, and fault tracking.

The service is started only when an application attempts to use VDS. When the service stops, VDS is no longer available.

This service is installed by default in Windows Server 2008 R2 or Windows 7, and its startup type is **Manual**.

When VDS is started in its default configuration, it logs on by using the Local System account.

VDS is dependent upon the following system components:

- Plug and Play
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Volume Shadow Copy

The Volume Shadow Copy (VSS) service manages and implements volume shadow copies and it manages the volume snapshots. If the service is stopped, shadow copies will be unavailable for backup and the backup process may not succeed. The features and applications of the Windows operating system that use VSS include the following:

- [Windows Server Backup](#)
- [Shadow Copies of Shared Folders](#)
- [System Center Data Protection Manager](#)
- [System Restore](#)

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When the Volume Shadow Copy service is started in its default configuration, the service logs on by using the Local System account.

The Volume Shadow Copy service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

WLAN AutoConfig

The WLAN AutoConfig (Wlansvc) service provides the logic that is required to configure, discover, connect to, and disconnect from a wireless local area network (WLAN) as defined by IEEE 802.11 standards. It also contains the logic to turn the computer into a software access point so that other devices or computers can wirelessly connect to the computer by using a WLAN adapter that can support this. Stopping or disabling the WLAN AutoConfig service will make all WLAN adapters on the computer inaccessible from the networking UI in the Windows operating system. It is strongly recommended that you have the WLAN AutoConfig service running if the computer has a WLAN adapter.

This service is installed by default and its startup type is **Manual**.

When the WLAN AutoConfig service is started in its default configuration, it logs on by using the Local System account.

The WLAN AutoConfig service is dependent upon the following system components:

- Extensible Authentication Protocol
- CNG Key Isolation
- Native WiFi Filter
- NDIS Usermode I/O Protocol
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

WMI Performance Adapter

The WMI Performance Adapter (wmiApSrv) service provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.

This service is installed by default and its startup type is **Manual**.

When the WMI Performance Adapter service is started in its default configuration, it logs on by using the Local System account.

WWAN AutoConfig

The WWAN AutoConfig (WwanSvc) service manages mobile broadband (GSM and CDMA) data card and embedded module adapters and connections by automatically configuring the networks. It is strongly recommended that this service be kept running for the best user experience of mobile broadband devices.

This service is installed by default and its startup type is **Manual**.

When the WWAN AutoConfig service is started in its default configuration, it logs on by using the Local Service account

The WWAN AutoConfig service is dependent upon the following system components:

- NDIS Usermode I/O Protocol
- Network Location Awareness
- Network Store Interface Service
- NSI proxy service driver
- Remote Procedure Call (RPC)

- DCOM Server Process Launcher
- RPC Endpoint Mapper
- TCP/IP Protocol Driver
- Plug and Play

Web Management Service

The Web Management Service (WMSVC) enables remote and delegated management capabilities so that administrators can manage the web server, sites, and applications that are present on this computer. This service supports Internet Information Services.

This service is not installed by default, and it must be added through the **Turn Windows Features on or off** dialog box in the **Programs** area of Control Panel. This service is not available on computers running Windows 7 Starter or Windows 7 Home Basic.

When the Web Management Service is started in its default configuration, it logs on by using the Local Service account.

The Web Management Service is dependent upon the following system component:

- HTTP

WebClient

The WebClient (WebClient) service enables Win32 applications to access documents on the Internet. The service extends the network capability of the Windows operating system by allowing standard Win32 applications to create, read, and write files on Internet file servers through the use of WebDAV (a file-access protocol that is described in XML and uses HTTP for communication). Because it uses standard HTTP, WebDAV communicates by using an existing Internet infrastructure, such as firewalls and routers.

This service is installed by default in Windows 7, and its startup type is **Manual**.

When the WebClient service is started in its default configuration, it logs on by using the Local Service account.

The WebClient service is dependent upon the following system components:

- WebDav Client Redirector Driver
- Redirected Buffering Sub System
- Mup

Windows Audio

The Windows Audio (AudioSrv) service provides support for sound and related Windows Audio event functions. This service manages events that are compatible with Plug and Play for audio devices such as sound cards and global audio effects (GFX) for Windows audio application program interfaces. Examples of GFXs are equalization (EQ), bass enhancement, and speaker correction. The service loads, unloads, saves, and restores states for the GFXs on a per-session basis.

Through the Multimedia Control Panel, users can accomplish the following:

- Enable or disable a GFX
- Select among several GFX filters if more than one GFX is available that is designed for the specific audio hardware (A GFX driver's .inf file specifies the target hardware for the GFX.)

You cannot stop the Windows Audio service after it is started. If you disable this service, audio functionality may be affected, including the inability to hear sound or process GFXs.

This service is installed by default in Windows 7, and its startup type is **Automatic**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Manual**.

When the Windows Audio service is started in its default configuration, it logs on by using the Local Service account.

The Windows Audio service is dependent upon the following system components:

- Multimedia Class Scheduler
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Audio Endpoint Builder
- Plug and Play

Windows Audio Endpoint Builder

The Windows Audio Endpoint Builder (AudioEndpointBuilder) service manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects do not function properly. The term endpoint device refers to a hardware device at one end of a data path that originates or terminates at an application program. Examples of audio endpoint devices are speakers, headphones, microphones, and CD players.

The audio system keeps track of endpoint devices and dynamic changes in the configuration of audio hardware that has jack-presence detection. The system enumerates an endpoint device that remains plugged in. When the user unplugs an endpoint device, the system ceases to enumerate it. This feature improves the reliability of the audio system, giving more predictable capture and playback experiences across different devices.

This service is installed by default in Windows 7, and its startup type is **Automatic**. The service is installed by default in Windows Server 2008 R2, and its startup type is **Manual**.

When the Windows Audio Endpoint Builder service is started in its default configuration, it logs on by using the Local System account.

The Windows Audio Endpoint Builder service is dependent upon the following system component:

- Plug and Play

The following system component is dependent upon the Windows Audio Endpoint Builder service:

- Windows Audio

Windows Backup

The Windows Backup (SDRSVC) service supports backup features provided in Windows 7 that allows data files and system images to be stored separately from the computer. This protects the files and images in case of system failure or data loss.

Having a regular backup policy is essential for disaster recovery scenarios, but backups are also a security risk. Your security policy must address how data backups are going to be protected so that they are not used to remove confidential information from your data center or your organization. Backup copies that are on removable media should be placed in a secure storage area that only trusted personnel have access to, and they should be encrypted. If possible, desktops and portable computers should be backed up on network servers, which are backed up in a secure storage area. If that is not feasible, your users should be informed about best practices for securely backing up data, and you should provide a secure location to store their backup copies.

This service is installed by default and its startup type is **Manual**.

When the Windows Backup service is started in its default configuration, it logs on by using the Local System account.

The Windows Backup service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Biometric Service

The Windows Biometric Service (WbioSrv) gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

The service is installed by default and its startup type is **Manual**.

When the Windows Biometric Service is started in its default configuration, it logs on by using the Local System account.

The Windows Biometric Service is dependent upon the following system components:

- Credential Manager
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Driver Foundation–User-Mode Driver Framework
- Plug and Play
- User-Mode Driver Frameworks Platform Driver

Windows CardSpace

The Windows CardSpace (idsvc) service enables the creation, management, and disclosure of digital identities. Windows CardSpace is client software that enables users to provide their digital identity to online services in a simple and secure way.

This service is installed by default and its startup type is **Manual**.

When the Windows CardSpace service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Windows Color System

The Windows Color System (WcsPlugInService) service hosts non-Microsoft Windows Color System color device model and gamut map model plug-in modules. These plug-in modules are vendor-specific extensions to the Windows Color System baseline color device and gamut map models. The Windows Color System system provides for more precise color mapping and gradation. Non-Microsoft vendors such as printer manufacturers and photo finishers can use this feature in applications and drivers to explicitly call the color that they want rendered.

Stopping or disabling the WcsPlugInService service disables this extensibility feature, and the Windows Color System uses its baseline model processing rather than the vendor's requested processing. This might result in inaccurate color rendering.

This service is installed by default and its startup type is **Manual**.

When the Windows Color System service is started in its default configuration, it logs on by using the Local Service account.

The Windows Color System service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Connect Now—Config Registrar

The Windows Connect Now—Config Registrar (WCNCSVC) service acts as a registrar for the Windows Connect Now service, and it issues network credentials to the enrollee in the service. The Windows Connect Now technology enables a streamlined configuration of secured wireless networks and easier provisioning of wireless hardware. It also supports configuration of devices on out-of-band Ethernet and in-band wireless networks. WCNCSVC hosts the Windows Connect Now Configuration, which is the implementation of Wi-Fi Protected Setup protocol that is provided by Microsoft. This is used to configure wireless LAN settings for an access point or a Wi-Fi device. The service is started programmatically as needed.

Windows Connect Now—NET in Windows 7 communicates with access points and wireless stations by using UPnP architecture, authenticates with them by using a personal identification number (PIN), and provides wireless settings that are based on user selection.

This service is installed by default and its startup type is **Manual**.

When Windows Connect Now–Config Registrar service is started in its default configuration, it logs on by using the Local Service account.

The Windows Connect Now–Config Registrar service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Defender

The Windows Defender (WinDefend) service scans the computer and helps protect the computer against pop-ups, slow performance, and security threats that are caused by spyware and other unwanted software.

This service is installed by default and its startup type is **Automatic**.

When the Windows Defender service is started in its default configuration, it logs on by using the Local System account.

The Windows Defender service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Driver Foundation–User-Mode Driver Framework

The Windows Driver Foundation–User-Mode Driver Framework (wudfsvc) service manages user-mode driver host processes. User-Mode Driver Framework (UMDF) supports the creation of user-mode drivers that support protocol-based or serial bus-based devices. Such drivers handle the same types of I/O requests as kernel-mode drivers, and they are installed by INF files like kernel-mode drivers. The UMDF supports protocol device classes such as cameras and portable music players. Moving drivers for such devices into user mode can simplify the drivers and improve the overall stability of the operating system.

This service is installed by default and its startup type is **Automatic**.

When the Windows Driver Foundation–User-Mode Driver Framework service is started in its default configuration, it logs on by using the Local System account.

The Windows Driver Foundation–User-Mode Driver Framework is dependent upon the following system components:

- Plug and Play
- User-Mode Driver Frameworks Platform Driver

The following system component relies on the Windows Driver Foundation–User-Mode Driver Framework:

- Windows Biometric Service

Windows Error Reporting Service

The Windows Error Reporting Service (WerSvc) reports errors when programs stop working or responding, and it enables existing solutions to be delivered. It also generates logs for the Problem Reports and Solutions diagnostic and repair service. If this service is stopped, programs and services that rely on this service will not report errors correctly, and the results of diagnostic services and repairs for those programs and services will not be displayed.

Windows Error Reporting is a feature that allows Microsoft to track and address errors that are related to the operating system, Windows features, and applications. Windows Error Reporting gives users the opportunity to send data about errors to Microsoft and to receive information about solutions. Solution information can include instructions for working around an issue, or a link to the Windows Update website or another website for updated drivers, patches, or Microsoft Knowledge Base articles. Developers at Microsoft can use Windows Error Reporting as a problem-solving tool to address customer issues in a timely manner and to improve the quality of Microsoft products.

Windows Error Reporting has "consent levels" that an administrator can configure to control how Windows Error Reporting sends data to Microsoft. These settings are configured on the **Problem Reporting settings** page of the **Action Center** Control Panel. These settings can also be configured through Group Policy under **Computer Configuration** or **User Configuration** in **Administrative Templates\Windows Components\Windows Error Reporting\Consent**.

User Account Control affects how Windows Error Reporting works. A standard user does not have the same ability to report errors as an administrator. If a prompt appears when a user is logged on as an administrator, the user can choose to report application and operating system errors. If a prompt appears for a user who is not logged on as an administrator, the user can choose to report application errors plus errors for operating system software that does not require administrative credentials to run.

The administrator also has the option to specify a list of programs for which error reports should never be sent.

This service is installed by default and its startup type is **Manual**. When the Windows Error Reporting service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Windows Event Collector

The Windows Event Collector (Wecsvc) service manages persistent subscriptions to events from remote sources that support the WS-Management protocol. This includes event logs, hardware, and event sources that use the Intelligent Platform Management Interface (IPMI). This service stores forwarded events in a local event log. If the service is stopped or disabled, event subscriptions cannot be created, and forwarded events cannot be accepted.

The Event Collector service on the local computer uses the WS-Management protocol to send an event subscription request to a remote computer. The remote computer must be able to receive this information. This subscription request is passed to the Event Forwarder, which is a WS-Management plug-in. The plug-in then creates an event subscription on the remote computer, which is based on the subscription request made by the local computer. Any events delivered to the remote computer are then sent to the Event Collector service on the local computer.

Event collection allows administrators to get events from remote computers and store them in a centralized place. The events are stored in the local event log of the collector computer and persisted in the local event log. The destination log path for the events is a property of the subscription. All data in the received event is saved in the collector computer event log. Additional information that is related to forwarding the event is also added to the event.

This service is installed by default, and its startup type is **Manual**.

When the Windows Event Collector service is started in its default configuration, it logs on by using the Network Service account.

The Windows Event Collector is dependent upon the following system components:

- HTTP
- Windows Event Log

Windows Event Log

The Windows Event Log (Eventlog) service enables event log messages that are issued by programs and components in the Windows operating system that are to be viewed in Event Viewer. These event log messages contain information that can help diagnose issues with applications, services, and the operating system.

You cannot stop the Windows Event Log service. If you disable the service, it would be impossible to track events, which significantly reduces the ability to successfully diagnose computer issues. Also, security events would not be audited, and you could not view previous event logs with the Event Viewer console.

This service is installed by default and its startup type is **Automatic**.

When the Windows Event Log service is started in its default configuration, it logs on by using the Local Service account.

The following table identifies the application protocols, network protocols, and ports that are used by the Windows Event Log service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
| RPC/named pipes | TCP | 139 |
| RPC/ named pipes | TCP | 445 |
| RPC/ named pipes | UDP | 137 |
| RPC/ named pipes | UDP | 138 |

The following system components are dependent upon the Windows Event Log Service:

- Operations Manager Audit Forwarding Service
- Task Scheduler
- Windows Event Collector

Windows Firewall

The Windows Firewall (MpsSvc) service helps to protect the computer by preventing unauthorized users from gaining access to the computer through the Internet or a network. For

an overview of the changes in Windows Firewall in Windows 7 and Windows Server 2008 R2, see [What's New in Windows Firewall with Advanced Security](#).

This service is installed by default and the startup type is **Automatic**.

When the Windows Firewall service is started in the default configuration, it logs on by using the Local Service account.

The Windows Firewall service is dependent upon the following system components:

- Base Filtering Engine
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Windows Firewall Authorization Driver

Windows Font Cache Service

The Windows Font Cache Service (FontCache) optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, although doing so will degrade application performance.

This service is installed by default and its startup type is **Manual**.

When the Windows Font Cache Service is started in its default configuration, it logs on by using the Local Service account.

Windows Image Acquisition (WIA)

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

The Windows Image Acquisition (WIA) service supports Small Computer System Interface (SCSI), IEEE 1394, USB, and serial digital still-image devices. Image scanners and digital cameras are examples of still-image devices. Support for infrared, parallel, and serial still-image devices is provided by the existing infrared, parallel, and serial interfaces.

If the service stops, events from imaging devices are not captured and processed. If there is a device that is supported by the Windows Image Acquisition service installed on the computer, the service starts automatically at startup. Also, it restarts any time that a Windows Image Acquisition-enabled application is started.

This service is installed by default in Windows 7, and its startup type is **Manual**.

When the Windows Image Acquisition service is started in its default configuration, it logs on by using the Local Service account.

The Windows Image Acquisition service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Shell Hardware Detection

Windows Installer

The Windows Installer (msiserver) service manages the installation and removal of applications. It applies a set of centrally defined setup rules during the installation process that specify how applications are installed and configured. You can also use this service to modify, repair, or remove existing applications. The Windows Installer technology consists of the Windows Installer service for the Windows operating system and the Windows Installer Package (a .msi file) that contains application setup and installation information.

The Windows Installer service is also an extensible software management system. It manages the installation, addition, and deletion of software components, monitors file resiliency, and maintains basic disaster recovery by way of rollbacks. It supports the installation and operation of software from multiple sources, and developers who want to install custom applications can customize it.

Applications that use the installer start the service. If this service stops, applications that use it cannot be installed, removed, repaired, or modified. Also, a number of applications use this service when they are active, and they may not run if the Windows Installer service stops.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When the Windows Installer service is started in its default configuration, it logs on by using the Local System account.

The Windows Installer service is dependent upon the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher

- RPC Endpoint Mapper

Windows Internet Name Service (WINS)

The Windows Internet Name Service (WINS) enables NetBIOS name resolution. If your organization has computers that require NetBIOS name resolution, you can use Server Manager to install this feature on servers running Windows Server 2008 R2. However, we recommend that you investigate the use of DNS alternatives to WINS, such as a search suffix list or a global names zone. For more information about using DNS clients, see [Understanding DNS Client Settings](#).

Windows Management Instrumentation

The Windows Management Instrumentation (Wmi) service provides a common interface and object model to access management information about operating systems, devices, applications, and services. Windows Management Instrumentation (WMI) is an infrastructure that provides the ability to build management applications and instrumentation.

The WMI infrastructure is a component in the Windows operating system that moves and stores information about managed objects. It is composed of the Windows Management Instrumentation service and the WMI repository. The Windows Management Instrumentation service acts as an intermediary between the providers, management applications, and the WMI repository, and it places information from a provider into the WMI repository. The service accesses the WMI repository in response to queries and instructions from management applications, and the service can pass information directly between a provider and a management application. In contrast, the WMI repository acts as a storage area for information from the various providers.

The Windows Management Instrumentation service provides access to the management data through a number of interfaces, including COM APIs, scripts, and command-line interfaces. It is compatible with previous management interfaces and protocols, such as Simple Network Management Protocol (SNMP). The service installs and runs automatically on computers running Windows 7 or Windows Server 2008 R2. If the service stops, most Windows-based software cannot function properly.

This service is installed by default and its startup type is **Automatic**.

When the Windows Management Instrumentation service is started in its default configuration, it logs on by using the Local System account.

The Windows Management Instrumentation service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent on the Windows Management Instrumentation service:

- Internet Connection Sharing (ICS)
- IP Helper
- Security Center

Windows Media Center Receiver Service

The Windows Media Center Receiver Service (ehRecvr) supports the Windows Media Center so that you can receive TV and radio programs on the computer.

This service is installed by default in Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise, it and its startup type is **Manual**. This service is not available in Windows 7 Starter or Windows 7 Home Basic.

When the Windows Media Center Receiver Service is started in its default configuration, it logs on by using the Network Service account.

The Windows Media Center Receiver Service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Media Center Scheduler Service

The Windows Media Center Scheduler Service (ehSched) supports the Windows Media Center so that you can start and stop TV program recordings on schedule.

This service is installed by default in Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise, it and its startup type is **Manual**. This service is not available in Windows 7 Starter or Windows 7 Home Basic.

When the Windows Media Center Receiver Service is started in its default configuration, it logs on by using the Network Service account.

The Windows Media Center Scheduler Service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Media Player Network Sharing Service

The Windows Media Player Network Sharing Service (WMPNetworkSvc) shares Windows Media Player libraries with other networked players and media devices by using the UPnP architecture.

This service is installed by default in all editions of Windows 7, and its startup type is **Automatic** on Windows 7 Home Premium and Windows 7 Professional. In all other editions of Windows 7, its startup type is **Manual**.

When the Windows Media Player Network Sharing Service is started in its default configuration, it logs on by using the Network Service account.

The Windows Media Player Network Sharing Service is dependent on the following system component:

- HTTP

Windows Modules Installer

The Windows Modules Installer (TrustedInstaller) service enables installation, modification, and removal of Windows updates and optional components. If this service is disabled, installation or removal of Windows updates may fail for this computer.

This service is installed by default, and its startup type is **Manual**.

When the Windows Modules Installer service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it.

Windows Presentation Foundation Font Cache

The Windows Presentation Foundation Font Cache service optimizes performance of the Windows Presentation Foundation (WPF) application by caching commonly used font data. You may have multiple versions of this service, such as Windows Presentation Foundation Font Cache 3.0.0.0 and Windows Presentation Foundation Font Cache 4.0.0.0, to support applications

that are created with different versions of WPF. WPF applications will start this service if it is not already running. It can be disabled, but doing so degrades the performance of WPF applications.

This service is installed by default in Windows 7, and its startup type is **Manual**.

When the Windows Presentation Foundation Font Cache service is started in its default configuration, it logs on by using the Local Service account.

The Windows Presentation Foundation Font Cache service is not dependent on any other system service, nor is any service dependent on it.

Windows Process Activation Service

The Windows Process Activation Service (WAS) manages the activation and lifetime of the worker processes that contain applications that host Windows Communication Foundation (WCF) services. The Windows Process Activation Service process model generalizes the IIS process model for the HTTP server by removing the dependency on HTTP. This allows WCF services to use both HTTP and non-HTTP protocols, such as Net.Tcp, in a hosting environment that supports message-based activation, and it provides the ability to host a large number of applications on a computer.

This service is not installed by default. For security, you should not run the Windows Process Activation Service unless your system supports the .NET Framework 3.5.1 application or IIS 7.0. The .NET Framework 3.5.1 and IIS 7.0 automatically install the Windows Process Activation Service as needed. You should not install the Windows Process Activation Service by itself.

When the Windows Process Activation Service is started in its default configuration, it logs on by using the Local System account.

The Windows Process Activation Service is dependent upon on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

The following system components are dependent upon the Windows Process Activation Service:

- Net.Msmq Listener Adapter
- Net.Pipe Listener Adapter
- Net.Tcp Listener Adapter

- World Wide Web Publishing Service

Windows Remote Management (WS-Management)

The Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard Web services protocol that is used to manage remote software and hardware. The Windows Remote Management service listens on the network for WS-Management requests and processes them. The Windows Remote Management service must be configured with a listener by using the Winrm command-line tool or by using a Group Policy setting for it to listen to the network.

The Windows Remote Management service provides access to WMI data, and it enables event collection. Event collection and subscription to events require that the service is running. The Windows Remote Management service messages use HTTP and HTTPS as transports. This service does not depend on IIS, but it is preconfigured to share a port with IIS on the same computer. The Windows Remote Management service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should verify that websites hosted on IIS do not use the /wsman URL prefix.

A server that has a baseboard management controller (BMC) that supports the WS-Management standard, can be managed by applications and scripts using the Windows Remote Management service to communicate directly with the BMC, even when the operating system is offline (for example, before the system boots or if there is a system failure).

When a server does not have a BMC, the Windows Remote Management service can still connect to WMI remotely in situations where the DCOM communication is impeded, for example, across a firewall. This usage is possible because the WS-Management standard uses a single port that is configurable by the system administrator.

The Windows Remote Management service exposes an application programming interface (API) for scripting. The scripting API communicates with WMI by using syntax that is different from standard WMI scripts. The syntax for the Windows Remote Management service is documented in the [WinRM section of MSDN](#). Hardware management uses a plug-in to expose WMI classes to the Windows Remote Management service. To call these classes, the WMI namespace and class must be converted into a Uniform Resource Identifier (URI).

As a security measure, you should configure the Windows Remote Management service to use the HTTPS protocol.

This service is installed by default, and its startup type is **Manual**.

When the Windows Remote Management service is started in its default configuration, it logs on by using the Network Service account.

The Windows Remote Management service is dependent on the following system components:

- HTTP
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Search

The Windows Search (WSearch) service supports the Instant Search feature, and it provides content indexing and property caching for file, email, and other content (by means of extensibility APIs). If the service is stopped or disabled, Windows Explorer cannot display virtual folder views of items, and Windows Explorer reverts to an item-by-item search.

The content that is indexed is based on the file and data types that are supported through add-ins included in the Windows Search service and the default inclusion and exclusion rules for folders in the file system. For example, the filters that are included in the Windows Search service support more than 200 common types of data, including support for Microsoft Office documents, Office Outlook email (in conjunction with the MAPI protocol handler), plaintext files, and HTML.

The main component of Windows Search is the indexer process, which is implemented as a Windows service running in the Local System account. The process is always running for all users even if no user is logged on. This enables the Windows Search service to maintain one index that is shared among all users, with security restrictions on content access, and to process remote queries from client computers on the network.

The Windows Search service includes a number of features to ensure that it protects the user experience and system performance when indexing. The following conditions cause the service to slow or pause indexing:

- High CPU usage by processes that are not search related
- High system I/O rate including file reads and writes, pagefile and file cache I/O, and mapped file I/O
- Low memory availability
- Low battery life

- Low disk space on the drive that is storing the index

The Windows Search service is installed by default, and its startup type is **Automatic**. When started in the default configuration, it logs on by using the Local System account.

The Windows Search service is dependent on the following system components:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Windows Time

The Windows Time (W32Time) service maintains date and time synchronization on networked computers that are running the Windows operating system. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or time stamp, can be assigned to network validation and resource access requests. The implementation of NTP and the integration of time providers make the Windows Time service reliable and scalable for administrators. For computers that are not joined to a domain, you can configure the Windows Time service to synchronize time with an external time source.

If the Windows Time service stops or if you disable it, date and time synchronization is unavailable in the network or from an external NTP server. There are two possible scenarios:

- If you stop the Windows Time service on a workstation, the workstation cannot synchronize its time with another source, but no other external server is affected.
- If you stop the Windows Time service on a domain controller, the same effect as in the previous scenario applies, but domain members are also unable to synchronize time with it. This inability to synchronize may adversely affect time synchronization in the organization.

This service is installed by default in Windows 7 and Windows Server 2008 R2, and its startup type is **Manual**.

When the Windows Time service is started in its default configuration, it logs on by using the Local Service account.

Windows Update (Automatic Updates)

The Windows Update (wuauserv) service enables the download and installation of security updates for the Windows operating system and Microsoft Office software. It automatically provides the latest updates, drivers, and enhancements to computers that are running the Windows operating system. When an Internet connection is available, the operating system

searches for applicable updates. Depending on the configuration settings, the service may notify the user before download, notify the user before installation, or automatically install the updates.

You can disable the Windows Update service through the Control Panel. You can also use the Local Group Policy Editor to configure an intranet server that is configured with Windows Server Update Services (WSUS) to host updates from the Microsoft Update sites. This setting lets you specify a server on your network to function as an internal update service.

If the Windows Update service stops or if you disable it, updates are not automatically downloaded to the computer. You must manually search for, download, and install applicable updates.

This service is installed by default and its startup type is **Automatic**.

When the Windows Update service is started in its default configuration, it logs on by using the Local System account.

The following system components are dependent upon the Windows Update service:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

WinHTTP Web Proxy Auto-Discovery Service

The WinHTTP Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc) implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol that enables an HTTP client to automatically discover a proxy configuration.

If the WinHTTP Web Proxy Auto-Discovery Service stops or if you disable it, the WPAD protocol runs within the HTTP client's process instead of an external service process, and there is no loss of functionality.

This service is installed by default, and its startup type is **Manual**.

When the WinHTTP Web Proxy Auto-Discovery service is started in its default configuration, it logs on by using the Local Service account.

The WinHTTP Web Proxy Auto-Discovery service is dependent upon the following system components:

- DHCP Client

- Ancillary Function Driver Winsock
- NetIO Legacy TDI Support Driver
- TCP/IP Protocol Driver
- Network Store Interface Service
- NSI proxy service driver

Wired AutoConfig

The Wired AutoConfig (dot3svc) service performs IEEE 802.1X authentication on Ethernet interfaces. By using the Wired Network (IEEE 802.3) Policies, Group Policy settings, and client-side extensions in Windows Server 2008 R2, you can specify network settings for computers running Windows 7 and Windows Server 2008 R2. (The computers must connect to an Ethernet network through an 802.1X-compatible switch in an Active Directory environment.)



Note

You cannot configure computers running Windows XP or Windows Server 2003 by using Wired Network (IEEE 802.3) Policies.

If your current wired network deployment enforces 802.1x authentication, the Wired AutoConfig service should be configured to run to establish Layer 2 connectivity and provide access to network resources. Wired networks that do not enforce 802.1x authentication are unaffected by the Wired AutoConfig service.

This service is installed by default and its startup type is **Manual**.

When the Wired AutoConfig service is started in its default configuration, it logs on by using the Local System account.

The Wired AutoConfig service is dependent upon the following system components:

- Extensible Authentication Protocol
- CNG Key Isolation
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- NDIS Usermode I/O Protocol

WLAN Autoconfig

The WLAN Autoconfig service enables automatic configuration of Wireless Network (IEEE 802.11) Policies. Microsoft has worked with wireless communications vendors to automate the network adapter configuration process, which associates the network adapter with an available network and improves the wireless roaming experience in the Windows operating system.

The wireless network adapter and its Network Driver Interface Specification (NDIS) driver provide support for NDIS object identifiers (also known as OIDs) that query and set device and driver behavior. The network adapter scans for available networks and passes the information to the Windows operating system. The WLAN Autoconfig service configures the network adapter for an available network. When two networks cover the same area, the user can configure a preferred network order. The computer tries each network in order until it determines an active one. It is also possible to limit association to only the configured, preferred networks.

In Windows Server 2008 R2 and Windows 7, the WLAN AutoConfig service enumerates wireless adapters, and it manages wireless connections and the wireless profiles that contain the settings required to configure a wireless client to connect to wireless networks. The WLAN AutoConfig System Services Group Policy settings in Windows Server 2008 R2 enable administrators to specify the service startup type of the WLAN AutoConfig service for domain member computers running Windows 7 and Windows Server 2008 R2 that have wireless network adapters and the associated Windows 7 adapter drivers installed.

WLAN AutoConfig Group Policy settings enable administrators to prevent domain member users from altering the startup mode of the WLAN AutoConfig service.

This service is installed by default and its startup type is **Manual**.

When the WLAN AutoConfig service is started in its default configuration, it logs on by using the Local System account.

The WLAN AutoConfig service is dependent upon the following system components:

- Extensible Authentication Protocol
- CNG Key Isolation
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- Native WiFi Filter

- NDIS Usermode I/O Protocol

WMI Performance Adapter

The WMI Performance Adapter (wmiApSrv) service provides performance library information from WMI high-performance providers. Applications and services can provide performance counters in two ways: they can write a WMI high-performance provider or write a performance library. Consumers of high-performance data also have two ways to request performance data: through WMI or through the Performance Data Helper (PDH) APIs. There are mechanisms that are in place to enable the two models to interact, so that clients that access counters through each model can still detect the counters provided by the other model. The reverse adapter is one of those mechanisms.

The WMI Performance Adapter service transforms performance counters that are supplied by WMI high-performance providers into counters that can be consumed by PDH through the Reverse Adapter Performance Library. This approach provides PDH clients, such as Sysmon, with the ability to consume performance counters from any WMI high-performance providers on the computer.

If the WMI Performance Adapter service stops, WMI performance counters are unavailable.

This service is installed by default and its startup type is **Manual**.

When the WMI Performance Adapter service is started in its default configuration, it logs on by using the Local System account.

This service is not dependent on any other system service, nor is any service dependent on it

Workstation

The Workstation (LanmanWorkstation) service creates and maintains client network connections and communications. The Workstation service is a user-mode wrapper for the Microsoft Networks redirector. It loads and performs configuration functions for the redirector, supports network connections to remote servers, supports the WNet APIs, and provides redirector statistics.

This service is installed by default, and its startup type is **Automatic**.

If the Workstation service stops, clients cannot establish connections to remote servers or access files through named pipes. Clients and programs cannot access files and printers on other remote computers, but TCP/HTTP connectivity is not affected. Internet browsing and Web Client access still work.

The Workstation service is dependent upon the following system components:

- Browser Support Driver
- Network Store Interface Service
- NSI proxy service driver
- SMB 1.x MiniRedirector
- SMB 2.0 MiniRedirector
- SMB MiniRedirector Wrapper and Engine
- Redirected Buffering Sub System
- Mup

The following system components are dependent on the Workstation service:

- Computer Browser
- Netlogon
- Remote Desktop Configuration

World Wide Web Publishing Service

The World Wide Web Publishing Service (W3SVC) provides web connectivity and administration of websites through the IIS snap-in. This service provides HTTP services for applications that are running on the Windows operating system, and it contains a process manager and a configuration manager. The process manager controls the processes in which custom applications and simple websites reside. The configuration manager reads the stored computer configuration and ensures that Windows is configured to route HTTP requests to the appropriate application pools or operating system processes.

This service can monitor the processes that contain custom applications and provide recycling services for these applications. Recycling is a configuration property of an application pool, which can be based on memory limits, request limits, processing time, or time of day. The service queues HTTP requests if custom applications stop responding, and it attempts to restart custom applications.

You can configure the ports that are used by this service through the Internet Information Services (IIS) Manager snap-in. If the administrative website is enabled, a virtual website is created that uses HTTP traffic on TCP port 8098.

The following table identifies the application protocol, network protocol, and ports used by the World Wide Web Publishing Service:

| Application protocol | Network protocol | Ports |
|----------------------|------------------|-------|
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |

This service is an optional component that can be installed on Windows Server 2008 R2 or Windows 7 as part of the IIS Web Server package. If the World Wide Web Publishing Service stops, the operating system cannot serve any form of web request.

The World Wide Web Publishing Service is dependent upon the following system components:

- Windows Process Activation Service
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

Threats and Countermeasures Guide: Software Restriction Policies

This topic for the IT professional discusses security threats against the Software Restrictions Policies feature in the Windows operating system and countermeasures that you can take to mitigate those threats in Windows Server® 2008 R2 and Windows® 7.

Overview

Software restriction policies provide a policy-driven system to specify which programs are allowed to run on the local computer and which are not. The policy settings were introduced in Windows Server 2003 and Windows XP. In Windows Vista and Windows Server 2008, the default hash rule algorithm was upgraded from Message Digest version 5 (MD5) to the Secure Hash Algorithm-256 (SHA256). SHA-256 is a 256-bit (32-byte) message digest hash, and it is meant to provide 128 bits of security against collision attacks. It is considered much stronger than MD5, which has known vulnerabilities. MD5 is still supported for compatibility with Windows XP. In addition, certificate rules can be activated from within the Software Restriction Policies snap-in extension instead of from within the Local Security Policies snap-in.

No improvements to Software Restriction Policies were made for Windows Server 2008 R2 and Windows 7. However, AppLocker™, which is an improved application control policy feature, was introduced.

Software Restriction Policies settings

The increased use of networks and the Internet in daily business computing means that it is more likely than ever that an organization's users can encounter malicious software. Software restriction policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojan horses, and other types of malicious software.

You can configure the Software Restriction Policies settings in the following location within the Group Policy Management Console:

Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies

Vulnerability

People use computer networks to collaborate in many ways; they use email, instant messaging, and peer-to-peer applications. As these collaboration opportunities increase, so does the risk from viruses, worms, and other forms of malicious software. Email and instant messaging can

transport unsolicited malicious software, which can take many forms—from native Windows executable (.exe) files, to macros in word processing (.doc) documents, to script (.vbs) files.

Viruses and worms are often transmitted in email messages, and they frequently include social engineering techniques that trick users into performing an action that activates the malicious software. The amount and variety of forms that malicious software can take make it difficult for users to know what is safe to run and what is not. When activated, malicious software can damage content on a hard disk drive, flood a network with requests to cause a denial-of-service (DoS) attack, send confidential information to the Internet, or compromise the security of a computer.



Note

Software restriction policies do not prevent restricted processes that run under the System account. For example, if a malicious program has set up a malicious service that starts under the Local System account, it starts successfully even if there is a software restriction policy configured to restrict it.

Countermeasure

Create a sound design for software restriction policies on end-user computers in your organization, and then thoroughly test the policies in a lab environment before you deploy them in a production environment.

A policy consists of a default rule that specifies whether programs are allowed to run and exceptions to that rule. The default rule can be set to **Unrestricted** (the program is allowed to run) or **Disallowed** (the program is not allowed to run).

Setting the default rule to **Unrestricted** allows an administrator to define exceptions (programs that are not allowed to run). A more secure approach is to set the default rule to **Disallowed**, and specify only the programs that are known and trusted to run.

There are two ways to use software restriction policies:

1. If an administrator knows all of the programs that should run, then a software restriction policy can be applied to allow only this list of trusted applications.
2. If all the applications that users might run are not known, then administrators can disallow undesired applications or file types as needed.

Software Restriction Policies has four rules with which to identify software. The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the

default rule. Each rule can include descriptive text to help communicate why the rule was created.

A software restriction policy supports the following four ways to identify software:

1. Hash: A cryptographic fingerprint of the file.
2. Certificate: A software publisher certificate that is used to digitally sign a file.
3. Path: The local or universal naming convention (UNC) path of where the file is stored.
4. Zone: The Internet zone as specified through Internet Explorer.

Potential impact

A flawed software restriction policy implementation can disable necessary applications or allow malicious software to run. Therefore, it is important that organizations dedicate sufficient resources to manage and troubleshoot the implementation of such policies.



Note

Although software restriction policies are an important tool that can enhance the security of computers, they are not a replacement for other security measures such as antivirus programs, firewalls, and restrictive access control lists (ACLs).

Additional references

The following links provide additional information about designing and using software restriction policies:

- For information about implementing software restriction policies on computers running Windows Vista, see [Using Software Restriction Policies to Protect Against Unauthorized Software](#).
- For information about methods, including software restriction policies, to defend your computer against malicious software, see Chapter 2 of the [Windows Vista Security Guide](#).

Threats and Countermeasures Guide: Application Control Policies

This security policy reference topic for the IT professional describes the security considerations for the application control policy settings that are managed by AppLocker™, including vulnerabilities, countermeasures, and potential impact in Windows Server® 2008 R2 and Windows® 7.

Application Control Policies settings

The increased use of networks and the Internet in daily business computing means that it is more likely than ever that an organization's users will encounter malicious software. Application control policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojan horses, and other types of malicious software.

Application control policies specify which programs are allowed to run on the local computer and which are not.

You can configure the Application Control Policies settings in the following location within the Group Policy Management Console (GPMC):

Computer Configuration\Windows Settings\Security Settings\Application Control Policies

Vulnerability

Computer networks are used to collaborate in many different ways, such as email, instant messaging, and peer-to-peer applications. As these collaboration opportunities increase, so does the risk from viruses, worms, and other forms of malicious software. Email and instant messaging can transport unsolicited malicious software, which can take many forms such as Windows executable files, macros in word processing documents, and script files.

Viruses and worms are often transmitted in email messages, and they frequently include social engineering techniques that trick users into performing an action that activates the malicious software. The amount and variety of forms that malicious software can take make it difficult for users to know what is safe to run and what is not. When activated, malicious software can damage content on a hard disk drive, flood a network with requests to cause a denial-of-service (DoS) attack, send confidential information to the Internet, or compromise the security of a computer.

Countermeasure

Create a sound design for your application control policies on end-user computers in your organization, and then thoroughly test the policies in a lab environment before you deploy them in a production environment.

Potential impact

A flawed application control policy implementation can disable necessary applications or allow malicious or unintended software to run. Therefore, it is important that organizations dedicate sufficient resources to manage and troubleshoot the implementation of such policies.

Additional References

For a listing of documentation about application control policies in Windows Server 2008 R2, see [AppLocker](#) in the Windows Server Technical Library.

Threats and Countermeasures Guide: External Storage Devices

This section of the Threats and Countermeasures Guide discusses Group Policy settings that can be used by administrators to limit, prevent, or allow the use of external storage devices in networked computers.

Overview

A growing variety of external storage devices can be connected to personal computers and servers that are running the Windows® operating system. Many users now expect to be able to install and use these devices in the office, at home, and in other locations. For administrators, these devices pose potential security and manageability challenges, such as:

- Protecting against data loss due to unauthorized copying of the organization's data.
- Restricting users' ability to copy or load unauthorized data and applications to the organization's servers and client computers.
- Preventing users from installing device drivers for unauthorized devices.
- Preventing users from installing device drivers from unauthorized locations.
- Help protect against potential malware programs, such as Conficker, which are capable of using external storage devices to install themselves in the system and spread throughout the network.

The Group Policy settings discussed in this section can be used to limit, prevent, or enable these situations. The default value for these policy settings is **Not configured**.

These policy settings are located in the following locations under **Computer Configuration\Administrative Templates\System**:

- **Device Installation\Device Installation Restrictions**
- **Device Redirection\Device Redirection Restrictions**
- **Driver Installation**
- **Enhanced Storage Access**
- **Removable Storage Access**

These policy settings are located in the following locations under **Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies**:

- **Turn off AutoPlay**
- **Don't set the always do this check box**
- **Turn off AutoPlay for non-volume devices**
- **Default behavior for AutoRun**

Additional Group Policy settings that can be used to manage the installation or use of external storage devices are covered in other sections of this guide. These policy settings include:

- **Load and unload device drivers** in [Threats and Countermeasures Guide: User Rights](#)
- **Devices: Allowed to format and eject removable media** in [Threats and Countermeasures Guide: Security Options](#)
- **Devices: Restrict CD-ROM access to locally logged-on user only** in [Threats and Countermeasures Guide: Security Options](#)
- **Devices: Restrict floppy access to locally logged-on user only** in [Threats and Countermeasures Guide: Security Options](#)

Also in [Threats and Countermeasures Guide: System Services](#), there is information about the following services that can be used to manage external storage devices:

- The SSDP Discovery service, which supports peer-to-peer Plug and Play functionality for network devices and services.
- The Portable Device Enumerator Service, which enforces Group Policy settings for removable mass-storage devices.
- The Windows Update service, which enables the download and installation of security updates for Windows and Office, in addition to device drivers and device driver updates.

For more information that can assist you in managing external storage devices, see the following sections of [Using Windows 7 and Windows Server 2008 R2: Controlling Communication with the Internet](#):

- [Device Manager, Hardware Wizards, and Resulting Internet Communication in Windows 7 and Windows Server 2008 R2](#)
- [Plug and Play and Resulting Internet Communication in Windows 7 and Windows Server 7](#)
- [Windows Update and Resulting Internet Communication in Windows 7 and Windows Server 2008 R2](#)

Device installation restrictions

A rapidly growing number and variety of new devices can be installed on a computer. To support these devices and the legitimate user scenarios that they enable, Microsoft® has simplified the process whereby authenticated users can locate and install device drivers that allow these devices to work with the Windows operating system. This simplified installation process is designed to reduce network support costs, because administrators no longer need to install devices on behalf of users or grant administrator permissions to users so that they can install and manage devices. However, many organizations still require some restrictions for device installation, based on a device or device class.

Possible values:

- Enabled
- Disabled
- Not configured

Vulnerability

Allowing users to manage and use external devices without restrictions can expose an organization to the following risks:

- **Data theft.** It is easier for users to make unauthorized copies of company data if they can install unapproved devices that support removable media. For example, if users can install a CD-R device, they can burn copies of company data onto a recordable CD.
- **Increase support costs.** Allowing users to install and use devices that your Help Desk is not prepared to support can increase user confusion and expose the network to unapproved software that is associated with those devices.

Countermeasure

To address these concerns, you can configure Device Installation Restrictions Group Policy settings to do the following:

- **Prevent installation of all devices.**

In this scenario, the administrator wants to prevent standard users from installing any device but allow administrators to install or update devices. To implement this scenario, you must configure two computer policies: one that prevents all users from installing devices and a second policy to exempt administrators from the restrictions.

- **Allow users to install only authorized devices.**

In this scenario, the administrator wants to allow users to install only the devices that are included on a list of authorized devices. To complete this scenario, you configure and apply a Group Policy setting that includes a list of authorized devices so that users can install only the devices that you specify.

- **Prevent installation of only prohibited devices.**



In this scenario, the administrator wants to allow standard users to install most devices but prevent them from installing devices that are included on a list of prohibited devices. To complete this scenario, you must configure and apply a Group Policy setting that includes a list of prohibited devices so that users can install any device except those that you specify.

- **Control the use of removable media storage devices.**

In this scenario, the administrator wants to prevent standard users from writing data to removable storage devices or devices with removable media, such as a USB memory drive or a CD or DVD burner. To complete this scenario, you configure and apply a computer policy to allow Read access but deny Write access to a specific device or to an external writable device on a computer.

The following table provides a brief description of the device installation policy settings that are used to implement these scenarios.

| Policy setting | Description |
|---|---|
| Prevent installation of devices not described by other policy settings | This policy setting controls the installation of devices that are not specifically described by any other policy setting. If you enable this policy setting, users cannot install or update the driver for devices unless they are described by either the Allow installation of devices that match these device IDs policy setting or the Allow installation of devices for these device classes policy setting. |
| Allow administrators to override device installation policy | This policy setting allows members of the local Administrators group to install and update the drivers for any device, regardless of other policy settings. If you enable this policy setting, administrators can use the Add Hardware Wizard or the Update Driver Wizard to install |

| Policy setting | Description |
|--|---|
| | and update the drivers for any device. |
| Prevent installation of devices that match these device IDs | <p>This policy setting specifies a list of Plug and Play hardware IDs and compatible IDs for devices that users cannot install. If you enable this policy setting, users cannot install or update the driver for a device if any of its hardware IDs or compatible IDs match one in this list.</p> <p> Note This policy setting takes precedence over any other policy settings that allow users to install a device. This policy setting prevents users from installing a device even if it matches another policy setting that would allow installation of that device.</p> |
| Prevent installation of drivers matching these device setup classes | <p>This policy setting specifies a list of Plug and Play device setup class GUIDs for devices that users cannot install. If you enable this policy setting, users cannot install or update drivers for a device that belongs to any of the listed device setup classes.</p> <p> Note This policy setting takes precedence over any other policy settings that allow users to install a device. This policy setting prevents users from installing a device, even if it matches another policy setting that would allow installation of that device.</p> |
| Allow installation of devices that match any of these device IDs | This policy setting specifies a list of Plug and Play hardware IDs and compatible IDs that |

| Policy setting | Description |
|--|---|
| | <p>describe devices that users can install. This policy setting is intended to be used only when the Prevent installation of devices not described by other policy settings policy setting is enabled, and it does not take precedence over any policy setting that would prevent users from installing a device. If you enable this policy setting, users can install and update any device with a hardware ID or compatible ID that matches an ID in this list if that installation has not been specifically prevented by the Prevent installation of devices that match these device IDs policy setting, the Prevent installation of devices for these device classes policy setting, or the Prevent installation of removable devices policy setting. If another policy setting prevents users from installing a device, users cannot install it even if the device is also described by a value in this policy setting.</p> |
| <p>Allow installation of devices using drivers for these device classes</p> | <p>This policy setting specifies a list of device setup class GUIDs that describe devices that users can install. This policy setting is intended to be used only when the Prevent installation of devices not described by other policy settings policy setting is enabled, and it does not take precedence over any policy setting that would prevent users from installing a device. If you enable this policy setting, users can install and update any device with a device setup class that matches one of the device setup class GUIDs in this list if that installation has not been specifically prevented by the Prevent installation of devices that match these device IDs policy setting, the Prevent installation of devices for these device classes</p> |

| Policy setting | Description |
|----------------|--|
| | policy setting, or the Prevent installation of removable devices policy setting. If another policy setting prevents users from installing a device, users cannot install it even if the device is also described by a value in this policy setting. |



Note

These policy settings affect all users who log on to the computer where the policy settings are applied. You cannot apply these policies to specific users or groups except for the **Allow administrators to override device installation policy** policy setting. This policy exempts members of the local Administrators group from any of the device installation restrictions that you apply to the computer by configuring other policy settings as described in this section.

Potential Impact

Inform users about the external hardware that they can and cannot use so that device restrictions do not generate unnecessary Help Desk calls. In addition, because new devices and updated device drivers are being introduced all the time, it may be necessary to define, review, and update organization-wide device standards and update the device installation Group Policy settings on a regular basis.

Device Redirection Restrictions

Device Redirection Restriction Group Policy settings are designed to extend the Device Installation Restriction Group Policy settings described in the previous section by further defining and limiting the locations from which device drivers can be installed.

Possible values:

- Enabled
- Disabled
- Not configured

Vulnerability

If approved locations are not available, users might install device drivers from unapproved locations.

Countermeasure

To address these concerns, you can configure the following Device Redirection Restrictions Group Policy settings to prevent users from obtaining device drivers from unapproved locations.

| Policy setting | Description |
|--|---|
| Prevent redirection of devices that match any of these device Ids | This policy setting prevents the redirection of specific USB devices. If you enable this policy setting, an alternate driver for the USB device cannot be loaded. |
| Prevent redirection of USB devices | This policy setting prevents the redirection of USB devices. If you enable this policy setting, an alternate driver for USB devices cannot be loaded. |

Potential Impact

If the primary location that you specify for the device driver that supports a particular device is not available, the user cannot obtain the device driver from an alternate location. The user will only be able to install and use the specified device if the primary location you define is available.

Driver Installation

You can configure a computer policy on your computer to allow specified users to install devices from specific device setup classes. In addition, you can manage whether a user or administrator receives the prompt to search Windows Update or Windows Server Update Services (WSUS) for device drivers when one is not found locally. When you enable this policy setting, Windows Update or WSUS is searched without asking the user for permission first. This policy setting only affects a computer on which searching Windows Update or WSUS is enabled.

Possible values:

- Enabled


- Disabled
- Not configured

Vulnerability

In some networks, allowing non-administrators to allow some classes of device drivers is considered a vulnerability. In addition, the ability to control whether a prompt appears allowing a user or administrator to decide whether to search Windows Update for a device driver if none is available locally can give them better control of which device drivers are installed.

Countermeasure

The following Group Policy settings can help you control whether non-administrators can install drivers for specified classes of devices and whether users or administrators receive a prompt when a device driver is not found locally.

| Policy setting | Description |
|---|---|
| Allow non-administrators to install drivers for these device setup classes | This policy setting allows administrators to specify a list of device setup class GUIDs that describe device drivers that non-administrator members of the built-in Users group can install on the system. If you enable this policy setting, members of the Users group can install new drivers for the specified device setup classes. The drivers must be signed according to the Windows Driver Signing Policy or be signed by publishers that are already in the TrustedPublisher store. |
| Turn off Windows Update device driver search prompt | <p>This policy setting specifies whether the administrator will be prompted before using Windows Update to search for device drivers.</p> <p> Note This policy setting has an effect only if the Turn off Windows Update device driver searching policy setting in Administrative</p> |

| Policy setting | Description |
|----------------|---|
| | <p>Templates\System\Internet Communication Management\Internet Communication settings is disabled or not configured.</p> <p>If you enable this policy setting, administrators will not be prompted to search Windows Update.</p> |

Potential Impact

Enabling non-administrators to install device drivers can reduce the number of help desk calls when users attempt to install hardware, but it increases the risk that non-approved devices are installed.

Enhanced Storage Access

Enhanced Storage devices are devices that support the IEEE 1667 protocol to provide functions such as authentication at the hardware level of the storage device. These devices enhance data protection if a device is lost or stolen.

Possible values:

- Enabled
- Disabled
- Not configured

Vulnerability



These devices can be very small, such as USB flash drives, to provide a convenient way to store and carry data. At the same time, the small size makes it very easy for the device to be lost, stolen, or misplaced. By supporting authentication at the device level, it becomes less likely that the data on the device will be compromised, even if the device is lost or stolen.

Countermeasure

The Enhanced Storage Access policy settings enable you to use Group Policy to administer policies for Enhanced Storage devices that support certificate and password authentication silos in your organization.

For definitions of various storage devices, see [Definitions](#) for Storage Silo Drivers in the MSDN Library.

The following Group Policy settings control the behavior of Enhanced Storage devices.

| Policy setting | Description |
|---|--|
| Allow Enhanced Storage certificate provisioning | <p>This policy setting allows users to provision certificates on devices that support the Certificate Authentication Silo.</p> <p> Note This policy setting is applicable only to Enhanced Storage devices that support the Certificate Authentication Silo.</p> |
| Allow only USB root hub connected Enhanced Storage devices | <p>This policy setting allows only Enhanced Storage devices that are connected to USB root hubs.</p> |
| Configure list of approved Enhanced Storage devices | <p>This policy setting allows you to configure a list of devices by manufacturer and product ID that are allowed on the computer.</p> <p> Note Manufacturer ID is a six-character value. Product ID is up to 40 characters in length. To specify that all devices by a manufacturer are allowed, type the manufacturer ID. To specify that only specific devices by a manufacturer are allowed, type the manufacturer ID, a hyphen, and the product ID or IDs of the allowed devices; for example:</p> |

| Policy setting | Description |
|---|---|
| | <Manufacturer ID>-<Product ID>. The manufacturer ID and the product ID values are case-sensitive. Contact the device manufacturer to get the manufacturer and product ID values. |
| Configure list of approved IEEE 1667 silos | <p>This policy setting allows you to create a list of approved silos that can be used on the computer.</p> <p>The Certificate Authentication Silo is always on the approved list.</p> |
| Do not allow password authentication of Enhanced Storage devices | This policy setting blocks the use of a password to unlock an Enhanced Storage device. |
| Do not allow non-Enhanced Storage removable devices | This policy setting limits the use of removable devices to Enhanced Storage devices and blocks the use of other storage devices on the computer. |
| Lock Enhanced Storage when the machine is locked | This policy setting locks the device when the computer is locked. |

Potential Impact

Enhanced Storage devices can enhance data protection, but they may require additional user education to use properly.

Removable Storage Access

Removable storage such as CD, DVD, and USB drives support a wide variety of scenarios, including data backup, software installation (especially when network access is not available), and easy access to multimedia training materials.

Possible values:

- Enabled
- Disabled
- Not configured

Vulnerability

Removable storage devices such as read-only and read-write CD and DVD drives, USB drives, and tape drives can pose security concerns such as the risk of introducing malware onto network computers, the installation of unapproved software, and data theft.

Countermeasure

An administrator can apply Group Policy settings to control whether users can read from or write to any device with removable media. These policy settings can be used to help prevent sensitive or confidential material from being written to removable media.

You can apply these policy settings at the computer level so they affect every user who logs on to the computer. You can also apply them at the user level and limit enforcement to specific user accounts.



Important



These removable storage access policies do not affect software that runs in the System account context, such as the ReadyBoost® technology in Windows. However, any software that runs under the security context of the current user might be affected by these restrictions. For example, if the **Removable Disks: Deny write access** policy setting is in effect for a user, even if that user is an administrator, then the BitLocker™ setup program cannot write its startup key to a USB drive. You might want to consider applying the restrictions to only users and groups other than the local Administrators group.


The **Removable Storage Access** policy settings also include a setting to allow an administrator to force a restart. If a device is in use when a restricting policy is applied, the policy might not be enforced until the computer is restarted. Use the policy setting to force a restart if you do not want to wait until the next time the user restarts the computer. If the restricting policies can be enforced without restarting the computer, then the restart option is ignored.

The policy settings can be found in two locations. The policy settings found in **Computer Configuration\Administrative Templates\System\Removable Storage Access** affect a computer and every user who logs on to it. The policy settings found in **User Configuration\Administrative**

Templates\System\Removable Storage Access affect only the users to whom the policy setting is applied, including groups if Group Policy is applied by using Active Directory Domain Services.

The following Group Policy settings enable you to control Read or Write access to removable storage drives. Each device category supports two policies: one to deny Read access and one to deny Write access.

| Policy settings | Description |
|--|---|
| Time (in seconds) to force reboot | <p>This policy setting sets the amount of time (in seconds) that the system will wait to restart to enforce a change in access rights to removable storage devices. The restart is only forced if the restricting policies cannot be applied without it.</p> <p> Note If the policy change affects multiple devices, the change is enforced immediately on all devices that are not currently in use. If any of the affected devices are in use so that the change cannot be immediately enforced, then this policy to restart the computer will be enforced, if it was enabled by the administrator.</p> |
| CD and DVD: Deny execute access | <p>This policy setting allows you to deny Read or Write access to devices in the CD and DVD removable storage class, including USB connected devices.</p> <p> Important Some non-Microsoft CD and DVD burner software interacts with the hardware in a way that is not prevented by this policy setting. If you want to prevent all writing to CD or DVD burners, you might want to</p> |

| Policy settings | Description |
|---|---|
| | consider applying Group Policy to prevent the installation of that software. |
| CD and DVD: Deny read access | This policy setting allows you to deny Read access to devices in the CD and DVD removable storage class, including USB connected devices. |
| CD and DVD: Deny write access | <p>This policy setting allows you to deny Write access to devices in the CD and DVD removable storage class, including USB connected devices.</p> <p> Important Some non-Microsoft CD and DVD burner software interacts with the hardware in a way that is not prevented by the policy. If you want to prevent all writing to CD or DVD burners, you might want to consider applying a Group Policy setting to prevent the installation of that software.</p> |
| Custom Classes: Deny read access | This policy setting allows you to deny Read access to any device with a Device Setup Class GUID that is found in the lists you provide. |
| Custom Classes: Deny write access | This policy setting denies Write access to custom removable storage classes that you specify. |
| Floppy Drives: Deny execute access | This policy setting allows you to deny Execute access to devices in the Floppy Drive class, including USB connected devices. |
| Floppy Drives: Deny read access | This policy setting allows you to deny Read access to devices in the Floppy Drive class, |

| Policy settings | Description |
|---|---|
| | including USB connected devices. |
| Floppy Drives: Deny write access | This policy setting allows you to deny Write access to devices in the Floppy Drive class, including USB connected devices. |
| Removable Disks: Deny execute access | This policy setting allows you to deny Execute access to removable devices that emulate hard disks, such as USB memory drives or external USB hard disk drives. |
| Removable Disks: Deny read access | This policy setting allows you to deny Read access to removable devices that emulate hard disks, such as USB memory drives or external USB hard disk drives. |
| Removable Disks: Deny write access | This policy setting allows you to deny Write access to removable devices that emulate hard disks, such as USB memory drives or external USB hard disk drives. |
| Tape Drives: Deny execute access | This policy setting allows you to deny Execute access to tape drives, including USB connected devices. |
| Tape Drives: Deny read access | This policy setting allows you to deny Read access to tape drives, including USB connected devices. |
| Tape Drives: Deny write access | This policy setting allows you to deny Write access to tape drives, including USB connected devices. |
| WPD Devices: Deny read access | This policy setting allows you to deny Read access to devices in the Windows Portable Device class, such as media players, mobile phones, and Windows CE devices. |

| Policy settings | Description |
|--|--|
| WPD Devices: Deny write access | This policy setting allows you to deny Write access to devices in the Windows Portable Device class, such as media players, mobile phones, and Windows CE devices. |
| All Removable Storage classes: Deny all access | This policy setting takes precedence over any of the policy settings in this list, and if enabled, it denies Execute, Read, and Write access to any device that is identified as using a removable storage device. |
| All Removable Storage: Allow direct access in remote sessions | This policy setting grants users direct access to removable storage devices in remote sessions. |

Potential Impact

Removable storage devices such as CD and DVD drives, removable disks, mobile phones, and tape drives have proliferated in the last few years, and users have come to rely on them to copy and transfer data from location to location. Restricting a user's ability to use these devices to read or write data may prevent or make it more difficult for them to complete some legitimate organization tasks, such as viewing DVD-based training materials or backing up data. If you implement removable storage device restrictions, you may need to provide alternate means, such as providing training kiosks or providing network-based backup, for these tasks to be completed.

AutoPlay and AutoRun policies

AutoPlay and AutoRun capabilities offer users simplified access to resources on removable storage devices.

Possible values:


- Enabled
- Disabled
- Not configured

Vulnerability

AutoPlay and AutoRun capabilities can pose potential risks when malware is present on these devices, and they are allowed to run without user intervention.

The AutoPlay and AutoRun policy settings enable you to use Group Policy to administer policies for files that are stored on enhanced storage devices or that are downloaded to computers in your organization.

The following Group Policy settings control the behavior of AutoPlay and AutoRun.

| Policy setting | Description |
|--|--|
| Turn off AutoPlay | <p>Turns off the AutoPlay feature.</p> <p>AutoPlay begins reading from a drive as soon as you insert media into the drive. As a result, the setup file of programs and the music on audio media start immediately.</p> <p>If you enable this setting, you can disable AutoPlay on CD-ROM and removable media drives, or disable AutoPlay on all drives.</p> <p>This setting disables AutoPlay on additional types of drives. You cannot use this setting to enable AutoPlay on drives when it is disabled by default.</p> <p> Note This setting appears in the Computer Configuration and the User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration.</p> |
| Don't set the always do check box | <p>If this policy is enabled, the "Always do this..." check box in AutoPlay will not be set by default when the dialog is shown.</p> |

| Policy setting | Description |
|---|---|
| Turn off AutoPlay for non-volume devices | <p>If this policy is enabled, AutoPlay will not be enabled for non-volume devices like MTP devices. If you disable or not configure this policy, AutoPlay will continue to be enabled for non-volume devices.</p> |
| Default behavior for AutoRun | <p>Sets the default behavior for AutoRun commands. AutoRun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.</p> <p>The default behavior in Windows Vista and later is to prompt the user whether the AutoRun command is to be run.</p> <p>If you disable or do not configure this policy, Windows Vista will prompt the user whether the AutoRun command is to be run.</p> <p>If you enable this policy, an Administrator can change the default behavior in Windows for AutoRun to:</p> <ol style="list-style-type: none"> 1. Completely disable AutoRun commands 2. Automatically execute the AutoRun command. |

Potential Impact

Restricting or blocking AutoPlay and AutoRun capabilities can enhance system security, but they may require additional user education to determine when such files can be run safely.

Threats and Countermeasures Guide: Additional Resources

This topic is for IT professionals. It lists companion resources to the Windows Server® 2008 R2 and Windows® 7 Threats and Countermeasures Security Guide.

The Threats and Countermeasures Guide explains the most significant security countermeasures that are available in Windows Server 2008 R2 and Windows 7. You can use the Security Configuration Wizard (SCW) to create security policies and import them into a Group Policy Object (GPO) that is linked to the parent organizational unit (OU) for the member server to manage most of the recommended settings. Because some hardening procedures cannot be applied through Group Policy, the guide also discusses some manual configuration settings.

The Threats and Countermeasures Guide is not intended to be a comprehensive reference to all of the features and considerations that you must take into account when securing the Windows Server 2008 R2 and Windows 7 operating systems. When you construct your information and network security plans for your environment, you may also find useful information in the following locations:

- [Secure Windows Server](#)
- [Microsoft Security Compliance Manager](#)
- [Microsoft Safety & Security Center](#)
- [Enterprise Security Best Practices](#)
- [10 Immutable Laws of Security](#)
- [Windows Client Security and Control](#)
- [Windows Server 2008 and Windows Server 2008 R2 Technical Library](#)
- [Server and Domain Isolation](#)
- [Selecting the Right NAP Architecture](#)
- [Windows Server Virtualization](#)
- [Windows Smart Card Technical Reference](#)
- [Group Policy Settings Reference for Windows and Windows Server](#)