Windows 7 What’s New Guide

Microsoft Corporation

Published: June 2009

Abstract

This document covers many new and changed Windows 7 features of interest to IT professionals, including DirectAccess, BranchCache and other networking technologies, VHD boot and other deployment technologies, and AppLocker, Biometrics, and other security technologies.

Copyright Information

Contents

What's New for IT Pros in Windows 7 Release Candidate

Users are becoming increasingly computer savvy, and they expect more from the technology they use at work. They expect to be able to work from home, from branch offices, and on the road, without a decrease in productivity. As the needs of users have changed, the demands on IT professionals have increased. Today, IT pros are being asked to provide more capabilities and support greater flexibility, while continuing to minimize cost and security risks. With Windows® 7, IT pros can meet the diverse needs of their users in a way that is more manageable. Businesses can enable employees to work more productively at their desks, at home, on the road, or in a branch office. Security and control are enhanced, reducing the risk associated with data on lost computers or external hard drives. Desktop management is streamlined, so it takes less work to deploy Windows 7 and keep it running smoothly. Because Windows 7 is based on the Windows Vista® foundation, companies that have already deployed Windows Vista will find that Windows 7 is highly compatible with existing hardware, software, and tools.

Note

For a complete view of Windows 7 resources, articles, demos, and guidance, please visit the Springboard Series for Windows 7 on the Windows Client TechCenter.

For a Web version of this document, see the Windows 7 What’s New Guide in the Windows Client TechCenter Library (http://go.microsoft.com/fwlink/?LinkId=152703).

What can IT pros do with Windows 7?

Windows 7 contains many new and changed features of interest to IT pros. Following are some of the key management tasks that can be improved or enabled with Windows 7.

Make end users productive anywhere

Windows 7 enables end users to be productive no matter where they are or where the data they need resides. They can work faster and with fewer interruptions because Windows 7 improves performance and reliability. They do not have to look in multiple places to find information because a single search can examine a SharePoint site on a company intranet and files on their computers. With DirectAccess, mobile users are able to simply and securely access corporate resources when they are out of the office. Users in branch offices with slow connections can be more productive by using BranchCache™ in Windows 7 to cache frequently accessed files and Web pages.

For more information about DirectAccess and BranchCache, see What's New in Networking.

Enhance security and control

Windows 7 builds on the security foundation of Windows Vista, delivering increased flexibility in securing computers and data. In addition to protecting internal computer hard disk drives, BitLocker™ Drive Encryption can encrypt external USB drives and hard disks—and provide recovery keys so that the data is accessible when it is needed. For enterprises that demand the highest levels of compliance, IT pros can use new application-blocking tools to dictate which applications are allowed to run on end user computers, providing another way to limit the risk of malicious software.

Streamline desktop management with the Microsoft Desktop Optimization Pack

Whether IT pros manage and deploy desktop computers, portable computers, or virtual environments, Windows 7 makes the job easier while enabling them to use the same tools and skills they use with Windows Vista. Advanced image management and deployment tools enable IT pros to add, remove, and report on drivers, language packs, and updates—and deploy those system images to user computers by using less network bandwidth. New scripting and automation capabilities based on Windows PowerShell™ 2.0 reduce the costs of managing and troubleshooting computers. For IT pros that use client virtualization, Windows 7 helps them more easily maintain virtual machine images and provide a richer user experience over remote connections.

The Microsoft Desktop Optimization Pack, which is updated at least once a year, completes the enterprise experience. By using Windows 7 and the Microsoft Desktop Optimization Pack together, enterprises can optimize their desktop infrastructure and gain the flexibility to address their unique business needs. Companies can quickly prepare to deploy Windows 7 by immediately deploying Windows Vista and the Microsoft Desktop Optimization Pack. Customers who are already running Windows Vista will find that Windows 7 delivers strong compatibility with Windows Vista software and devices, and that Windows 7 can be managed with many of the same tools that they use to manage Windows Vista. Companies that are using the Microsoft Desktop Optimization Pack will have an even greater advantage when moving to Windows 7 because they can more easily migrate settings and applications.

New and changed features in Windows 7

This section provides information about the new and changed features in Windows 7.

For more information about key new and changed features in Windows 7, see the following topics:

- What's New in AppLocker
- What's New in Biometrics
- What's New in Certificates
- What's New in Deployment Tools
- What's New in Group Policy

What's New in AppLocker

What are the major changes?

AppLocker™ is a new feature in Windows® 7 and Windows Server® 2008 R2 that replaces the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as .exe files, scripts, Windows Installer files (.msi and .msp files), and DLLs.

What does AppLocker do?

Using AppLocker, you can:

- Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create rules based on the publisher and file version attributes that are persistent through updates, or you can create rules that target a specific version of a file.

  Important

  AppLocker rules specify which files are allowed to run. Files that are not included in rules are not allowed to run.

- Assign a rule to a security group or an individual user.

  Note

  You cannot assign AppLocker rules to Internet zones, individual computers, or registry paths.

- Create exceptions for .exe files. For example, you can create a rule that allows all Windows processes to run except Regedit.exe.

- Use audit-only mode to identify files that would not be allowed to run if the policy were in effect.
- Import and export rules.

Who will be interested in this feature?

AppLocker can help organizations that want to:

- Limit the number and type of files that are allowed to run by preventing unlicensed or malicious software from running and by restricting the ActiveX controls that are installed.
- Reduce the total cost of ownership by ensuring that workstations are homogeneous across their enterprise and that users are running only the software and applications that are approved by the enterprise.
- Reduce the possibility of information leaks from unauthorized software.

AppLocker may also be of interest to organizations that currently use Group Policy objects (GPOs) to manage Windows-based computers or have per-user application installations.

Are there any special considerations?

- By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. Administrators should maintain an up-to-date list of allowed applications.
- Expect an increase in the number of help desk calls initially because of blocked applications. As users begin to understand that they cannot run applications that are not allowed, the help desk calls may decrease.
- There is minimal performance degradation because of the runtime checks.
- Because AppLocker is similar to the Group Policy mechanism, administrators should understand Group Policy creation and deployment.
- AppLocker rules cannot be used to manage computers running a Windows operating system earlier than Windows 7.
- If AppLocker rules are defined in a GPO, only those rules are applied. To ensure interoperability between Software Restriction Policies rules and AppLocker rules, define Software Restriction Policies rules and AppLocker rules in different GPOs.
- When an AppLocker rule is set to **Audit only**, the rule is not enforced. When a user runs an application that is included in the rule, the application is opened and runs normally, and information about that application is added to the AppLocker event log.

Which editions include AppLocker?

AppLocker is available in all editions of Windows Server 2008 R2 and in some editions of Windows 7.

What's New in Biometrics

For enhanced convenience, Windows® 7 enables administrators and users to use fingerprint biometric devices to log on to computers, grant elevation privileges through User Account Control (UAC), and perform basic management of the fingerprint devices. Administrators can manage fingerprint biometric devices in Group Policy settings by enabling, limiting, or blocking their use.

What's new in biometrics?

A growing number of computers, particularly portable computers, include embedded fingerprint readers. Fingerprint readers can be used for identification and authentication of users in Windows. Until now, there has been no standard support for biometric devices or for biometric-enabled applications in Windows. Computer manufacturers had to provide software to support biometric devices in their products. This made it more difficult for users to use the devices and administrators to manage the use of biometric devices.

Windows 7 includes the Windows Biometric Framework that exposes fingerprint readers and other biometric devices to higher-level applications in a uniform way, and offers a consistent user experience for discovering and launching fingerprint applications. It does this by providing the following:

- A **Biometric Devices** Control Panel item that allows users to control the availability of biometric devices and whether they can be used to log on to a local computer or domain.
- Device Manager support for managing drivers for biometric devices.
- Credential provider support to enable and configure the use of biometric data to log on to a local computer and perform UAC elevation.
- Group Policy settings to enable, disable, or limit the use of biometric data for a local computer or domain. Group Policy settings can also prevent installation of biometric device driver software or force the biometric device driver software to be uninstalled.
- Biometric device driver software available from Windows Update.

Who will want to use biometric devices?

Fingerprint biometric devices offer a convenient way for users to log on to computers and grant elevation through UAC.

What are the benefits of the new biometric features?

The new biometric features provide a consistent way to implement fingerprint biometric–enabled applications and manage fingerprint biometric devices on stand-alone computers or on a network. The Windows Biometric Framework makes biometric devices easier for users and for administrators to configure and control on a local computer or in a domain.

What's the impact of these changes on biometrics?

The introduction of the Windows Biometric Framework allows the integration of fingerprint biometric devices in Windows. It offers a consistent user experience for logging on to Windows and performing UAC elevation. In addition, it provides a common set of discovery and integration points that offers a more consistent user experience across devices and applications. The Windows Biometric Framework also includes management functions that allow administrators to control the deployment of biometric fingerprint devices in the enterprise.

What's New in Certificates

What's new in certificates?

- Windows® 7 introduces HTTP enrollment protocols that enable policy-based certificate enrollment across Active Directory forest boundaries and over the Internet. These changes enable new certificate enrollment scenarios that allow organizations to expand the accessibility of existing public key infrastructure (PKI) deployments and reduce the number of certification authorities (CAs).
- Improvements to the certificate selection user interface and filtering logic provide a simplified user experience when an application presents multiple certificates.

Who will want to use these new features?

HTTP enrollment

Enterprises with a new or existing PKI can use HTTP enrollment in these new deployment scenarios:

- In multiple-forest environments, client computers can enroll for certificates from CAs in a different forest.
- In extranet deployments, mobile workers and business partners can request and renew certificates over the Internet.

Certificate selection

Internet browsers and many other applications use the **Certificate Selection** dialog box to prompt users for certificate selection when multiple certificates are available. The **Certificate Selection** dialog box presents a list of certificates to choose from, but selecting the correct certificate can be a confusing task that often results in support calls and a poor user experience. Organizations encountering these issues can benefit from the improvements in certificate selection.

What are the benefits of the new and changed features?

HTTP enrollment

Organizations that have multiple-forest environments and a per-forest PKI can use HTTP enrollment to allow certificate enrollment across forest boundaries and consolidate their PKI to use fewer CAs.

Organizations that issue certificates to mobile workers, business partners, or online customers can use HTTP enrollment to allow certificate enrollment over the Internet and simplify the enrollment process for remote users.

The new HTTP enrollment protocols are based on open Web services standards and can be implemented by organizations that want to provide online certificate services and registration authority services.

Certificate selection

The certificate selection experience includes improvements in the filtering logic and the user interface. Improved filtering logic is intended to reduce the number of certificates that are presented to the user, ideally resulting in a single certificate that requires no user action. Filter criteria can be specified by the application and include certificate purpose, validity period, and certification path. If more than one certificate meets the filter criteria, the **Certificate Selection** dialog box displays details of each certificate such as subject, issuer, and validity period as well as a graphic that distinguishes between smart card certificates and certificates that are installed on the computer.

What's the impact of these changes on certificates?

HTTP enrollment

HTTP enrollment requires deployment of the certificate enrollment Web services included in Windows Server 2008 R2. For more information, see **What's New in Active Directory Certificate Services (AD CS) in Windows Server 2008 R2**. Administrators use Group Policy to distribute the locations of the certificate enrollment Web services to domain members. Windows 7 also supports Lightweight Directory Access Protocol (LDAP) enrollment that is compatible with existing CAs running Windows Server 2003 or Windows Server 2008.

Certificate selection

Applications that use the **CryptUIDlgSelectCertificate** function automatically use the new **Certificate Selection** dialog box and generally do not require changes. A new flag has been added to the API so that applications can use the legacy **Certificate Selection** dialog box; however, this requires that the application be modified and distributed to users. Additionally, optional parameters can be used to specify criteria for the **CertSelectCertificateChains** function, which is used to select certificates to be displayed by the **CryptUIDlgSelectCertificate** function. For more information, see CertSelectCertificateChains Function on MSDN.

What's New in Deployment Tools

This topic provides information on the key feature changes in two deployment tools: Windows Automated Installation Kit (Windows AIK) and Windows Deployment Services.

Microsoft Deployment Toolkit (MDT) is the recommended process and toolset to automate desktop and server deployment. For more information on MDT 2010, which can be used to deploy Windows 7, see the Microsoft Deployment Toolkit.

Deployment Tools for Windows 7

Windows Automated Installation Kit (Windows AIK)

New Features in the Windows AIK

Windows Deployment Services

What's New in Windows Deployment Services

What's New in Group Policy

What are the major changes?

The following changes are available in Windows Server® 2008 R2 and in Windows® 7 with Remote Server Administration Tools (RSAT):

- Windows PowerShell Cmdlets for Group Policy: Ability to manage Group Policy from the Windows PowerShell™ command line and to run PowerShell scripts during logon and startup
- Group Policy Preferences: Additional types of preference items
- Starter Group Policy Objects: Improvements to Starter GPOs
- Administrative Template Settings: Improved user interface and additional policy settings

What does Group Policy do?

Group Policy provides an infrastructure for centralized configuration management of the operating system and applications that run on the operating system.

Who will be interested in this feature?

The following groups might be interested in these changes:

- IT professionals who have to manage users and computers in a domain environment
- Dedicated Group Policy administrators
- IT generalists
- Support personnel

Are there any special considerations?

You can manage local and domain Group Policy by using domain-based versions of Windows Server 2008 R2. Although the Group Policy Management Console (GPMC) is distributed with Windows Server 2008 R2, you must install Group Policy Management as a feature through Server Manager.

You can also manage local and domain Group Policy by using Windows 7. For managing local Group Policy, the Group Policy Object Editor has been replaced by the Local Group Policy Editor. To manage domain Group Policy, you must first install the GPMC. The GPMC is included with RSAT, which is available for download:

- Windows Server 2008 R2 Remote Server Administration Tools for Windows 7
- Windows Server 2008 Remote Server Administration Tools for Windows Vista with SP1

RSAT enables IT administrators to remotely manage roles and features in Windows Server 2008 R2 from a computer that is running Windows 7. RSAT includes support for the remote management of computers that are running either a Server Core installation or the full installation option of Windows Server 2008 R2. The functionality RSAT provides is similar to Windows Server 2003 Administration Tools Pack.

Installing RSAT does not automatically install the GPMC. To install the GPMC after you install RSAT, click **Programs** in **Control Panel**, click **Turn Windows features on or off**, expand **Remote Server Administration Tools**, expand **Feature Administration Tools**, and select the **Feature Administration Tools** and **Group Policy Management Tools** check boxes.

Which editions include this feature?

Group Policy is available in all editions of Windows Server 2008 R2 and Windows 7. Both local and domain-based Group Policy can be managed by using any version of Windows Server 2008 R2 and any version of Windows 7 that supports RSAT.

Does it function differently in some editions?

Without RSAT, only local Group Policy can be managed using Windows 7. With RSAT, both local and domain-based Group Policy can be managed using any edition of Windows 7 that supports RSAT.

Is it available in both 32-bit and 64-bit versions?

Group Policy is available in both 32-bit and 64-bit versions of Windows Server 2008 R2. The choice of a 32-bit or 64-bit version does not affect interoperability, scalability, security, or manageability for Group Policy.

Windows PowerShell Cmdlets for Group Policy

What do the Windows PowerShell Group Policy cmdlets do?

Windows PowerShell is a Windows command-line shell and scripting language that you can use to automate many of the same tasks that you perform in the user interface by using the Group Policy Management Console (GPMC). To help you perform these tasks, Group Policy in Windows Server 2008 R2 provides more than 25 cmdlets. Each cmdlet is a simple, single-function command-line tool.

You can use the Group Policy cmdlets to perform the following tasks for domain-based Group Policy objects (GPOs):

- Maintaining GPOs: GPO creation, removal, backup, and import.
- Associating GPOs with Active Directory® containers: Group Policy link creation, update, and removal.
- Setting inheritance flags and permissions on Active Directory organizational units (OUs) and domains.
- Configuring registry-based policy settings and Group Policy Preferences Registry settings: Update, retrieval, and removal.
- Creating and editing Starter GPOs.

Are there any special considerations?

To use the Windows PowerShell Group Policy cmdlets, you must be running either Windows Server 2008 R2 on a domain controller or on a member server that has the GPMC installed, or Windows 7 with Remote Server Administration Tools (RSAT) installed. RSAT includes the GPMC and its cmdlets.

You must also use the **Import-Module grouppolicy** command to import the Group Policy module before you use the cmdlets at the beginning of every script that uses them and at the beginning of every Windows PowerShell session.

You can use the **GPRegistryValue** cmdlets to change registry-based policy settings and the **GPPrefRegistryValue** cmdlets to change registry preference items. For information about the registry keys that are associated with registry-based policy settings, see the Group Policy Settings Reference. This reference is a downloadable spreadsheet.

Note

> For more information about the Group Policy cmdlets, you can use the **Get-Help**<*cmdlet-name*> and **Get-Help**<*cmdlet_name*>**-detailed** cmdlets to display basic and detailed Help.

What policy settings have been added or changed?

New policy settings now enable you to specify whether Windows PowerShell scripts run before non-Windows PowerShell scripts during user computer startup and shutdown, and user logon and logoff. By default, Windows PowerShell scripts run after non-Windows PowerShell scripts.

Group Policy settings

Setting name	Location	Default value	Possible values
Run Windows PowerShell scripts first at computer startup, shutdown	Computer Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which computer startup and shutdown scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\Startup** and **Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\Shutdown**.

Setting name	Location	Default value	Possible values
Run Windows PowerShell scripts first at user logon, logoff	Computer Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which user logon and logoff scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logon** and **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logoff**.
Run Windows PowerShell scripts first at user logon, logoff	User Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which user logon and logoff scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logon** and **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logoff**.
Startup (**PowerShell Scripts** tab)	Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last
Shutdown (**PowerShell**	Computer Configuration\Policies\Windows	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell

Setting name	Location	Default value	Possible values
Scripts tab)	Settings\Scripts (Startup/Shutdown)\		scripts last
Logon (**PowerShell Scripts** tab)	User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last
Logoff (**PowerShell Scripts** tab)	User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last

Additional references

- Windows PowerShell Technology Center: This Web site is an entry point for Windows PowerShell documentation, such as information about deployment, operations, training, support, and communities.
- Windows PowerShell blog: This Web site is an entry point for Windows PowerShell blogs that includes information about current Windows PowerShell developments, best practices, training, and other resources.
- Group Policy Technology Center: This Web site is an entry point for Group Policy documentation, such as information about deployment, operations, training, support, and communities.
- Group Policy Settings Reference: This document lists Group Policy settings described in administrative template (ADMX) files and security settings. This spreadsheet includes all administrative template policy settings for Windows Server 2008 R2 and Windows Vista.

Group Policy Preferences

What are the major changes?

The following new types of preference items can be managed by using Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT). The client-side extensions for these new types of preference items are included in Windows Server 2008 R2 and Windows 7:

- Power Plan (Windows Vista and later) preference items
- Scheduled Task (Windows Vista and later) preference items
- Immediate Task (Windows Vista and later) preference items
- Internet Explorer 8 preference items

What do Group Policy Preferences do?

Group Policy Preferences let you manage drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language. You can use preference items to reduce scripting and the number of custom system images needed, standardize management, and help secure your networks. By using preference item-level targeting, you can streamline desktop management by reducing the number of Group Policy objects needed.

What new functionality does this feature provide?

Windows Server 2008 R2 and Windows 7 with RSAT improve several preference extensions with the addition of new types of preference items, providing support for power plans; scheduled tasks and immediate tasks for Windows 7, Windows Server 2008, and Windows Vista; and Windows Internet Explorer 8.

Power Plan (Windows Vista and later) preference items

Windows Server 2008 R2 and Windows 7 with RSAT improve the Power Options preference extension with the addition of Power Plan (Windows Vista and later) preference items.

Why is this change important?

You can use Power Plan preference items to configure default sleep and display options for managing power consumption for computers, reducing power consumption and benefitting the environment. With Power Plan preference items, you can let users make changes to those default options. Although you can also manage power options by using enforced policy settings, some user roles (such as mobile users) might need the flexibility to change those settings on their own.

The user interface for Power Plan preference items resembles that for advanced power settings in **Power Options** in **Control Panel**. This similarity makes the functionality easier to learn. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which a Power Plan preference item is applied.

Are there any dependencies?

Power Plan preference items can only be used to manage power consumption for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Power Options (Windows XP) preference items and Power Scheme (Windows XP) preference items instead.

Scheduled Task (Windows Vista and later) preference items

Windows Server 2008 R2 and Windows 7 with RSAT improve the Scheduled Tasks preference extension with the addition of Scheduled Task (Windows Vista and later) preference items.

Why is this change important?

You can use Scheduled Task (Windows Vista and later) preference items to create, replace, update, and delete tasks and their associated properties. Although you can still use Scheduled Task preference items to manage tasks for Windows 7, Windows Server 2008, and Windows Vista, Scheduled Task (Windows Vista and later) preference items provide a user interface similar to the Task Scheduler in Windows 7, Windows Server 2008, and Windows Vista, together with the options that it provides. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which a Scheduled Task preference item is applied.

Are there any dependencies?

Scheduled Task (Windows Vista and later) preference items can only be used to manage tasks for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Scheduled Task preference items instead.

Immediate Task (Windows Vista and later) preference items

Windows Server 2008 R2 and Windows 7 with RSAT improve the Scheduled Tasks preference extension with the addition of Immediate Task (Windows Vista and later) preference items.

Why is this change important?

You can use Immediate Task (Windows Vista and later) preference items to create tasks to be run immediately upon the refresh of Group Policy—and then removed. Previously, Immediate Task preference items were not supported for Windows Server 2008 and Windows Vista. Immediate Task (Windows Vista and later) preference items provide an intuitive user interface similar to the Task Scheduler in Windows 7, Windows Server 2008, and Windows Vista, together with the options that it provides. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which an Immediate Task preference item is applied.

Are there any dependencies?

Immediate Task (Windows Vista and later) preference items can only be used to manage tasks for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Immediate Task (Windows XP) preference items instead.

Internet Explorer 8 preference items

Windows Server 2008 R2 and Windows 7 with RSAT improve the Internet Settings preference extension with the addition of Internet Explorer 8 preference items.

Why is this change important?

You can use Internet Explorer 8 preference items to update Internet options for Internet Explorer 8. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which an Immediate Task preference item is applied.

What works differently?

Internet Explorer 8 and Internet Explorer 7 have different default settings, so that the corresponding types of preference items have different default settings as well.

Are there any dependencies?

Internet Explorer 8 preference items can only be used to manage Internet options for Internet Explorer 8. To manage Internet options for earlier versions of Internet Explorer, use Internet Explorer 7 preference items or Internet Explorer 5 and 6 preference items.

Starter Group Policy Objects

What are the major changes?

System Starter Group Policy objects (GPOs) for the following scenarios are available in Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT):

- Windows Vista Enterprise Client (EC)
- Windows Vista Specialized Security Limited Functionality (SSLF) Client
- Windows XP Service Pack 2 (SP2) EC
- Windows XP SP2 SSLF Client

What do System Starter GPOs do?

System Starter GPOs are read-only Starter GPOs that provide a baseline of settings for a specific scenario. Like Starter GPOs, System Starter GPOs derive from a GPO, let you store a collection of Administrative template policy settings in a single object, and can be imported.

What new functionality does this feature provide?

System Starter GPOs are included as part of Windows Server 2008 R2 and Windows 7 with RSAT and do not have to be downloaded and installed separately.

Why is this change important?

The System Starter GPOs included with Windows Server 2008 R2 and Windows 7 with RSAT provide recommended Group Policy settings for the following scenarios described in either the Windows Vista Security Guide or the Windows XP Security Guide:

- The computer and user Group Policy settings that are recommended for the Windows Vista EC client environment are contained in the Windows Vista EC Computer and Windows Vista EC User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows Vista SSLF client environment are contained in the Windows Vista SSLF Computer and Windows Vista SSLF User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows XP SP2 EC environment are contained in the Windows XP SP2 EC Computer and Windows XP SP2 EC User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows XP SP2 SSLF client environment are contained in the Windows XP SP2 SSLF Computer and Windows XP SP2 SSLF User System Starter GPOs.

What works differently?

You no longer have to download these System Starter GPOs because they are included in Windows Server 2008 R2 and Windows 7 with RSAT.

Additional references

- For more information about the EC and SSLF client scenarios for Windows Vista and the recommended policy settings, see the Windows Vista Security Guide (http://go.microsoft.com/fwlink/?LinkID=121852).
- For more information about the EC and SSLF client scenarios for Windows XP and the recommended policy settings, see the Windows XP Security Guide (http://go.microsoft.com/fwlink/?LinkID=121854).

Administrative Template Settings

What are the major changes?

The following changes are available in Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT):

- Improved user interface
- Support for multi-string registry and QWORD value types

What do Administrative templates do?

Administrative templates (.ADMX files) are registry-based policy settings that appear under the Administrative Templates node of both the Computer and User Configuration nodes. This hierarchy is created when the Group Policy Management Console reads XML-based Administrative template files.

What new functionality does this feature provide?

Administrative templates now provide an improved user interface and support for the multi-string (REG_MULTI_SZ) value and QWORD registry types.

Improved user interface

In previous releases of Windows, the properties dialog box for an Administrative template policy setting included three separate tabs: **Setting** (for enabling or disabling a policy setting and setting additional options), **Explain** (for learning more about a policy setting), and **Comment** (for entering optional information about the policy setting). In Windows Server 2008 R2, these options are available in a single location in the properties dialog box instead of in three separate tabs. This dialog box is now resizable.

Additionally, the **Explain** field, which provides additional information about a policy setting, is now called **Help**.

Why is this change important?

By providing all options required for configuring policy settings in a single location, the improved Administrative templates user interface reduces the administrative time that is required to configure and learn more about policy settings.

Support for multi-string and QWORD registry value types

Administrative templates now provide support for the multi-string (REG_MULTI_SZ) and QWORD registry value types.

Why is this change important?

This change expands Group Policy management options by enabling organizations to use Administrative template policy settings to manage applications that use the REG_MULTI_SZ and QWORD registry value types.

Support for the REG_MULTI_SZ registry value type enables you to perform the following tasks when you configure Administrative template policy settings:

- Enable a policy setting, enter multiple lines of text, and sort entries.
- Edit an existing configured setting, and add new line items.
- Edit an existing configured setting, and edit individual line items.

- Edit an existing configured setting, select one or more entries, and delete selected entries. The entries do not have to be contiguous.

Support for the QWORD registry value type enables you to use Administrative template policy settings to manage 64-bit applications.

What policy settings have been added or changed?

For Group Policy in Windows Server 2008 R2 and Windows 7 with RSAT, more than 300 Administrative template policy settings were added. To learn whether specific policy settings were added or changed for the technologies that are documented in this guide, review the appropriate technology-specific topics.

What's New in Handwriting Recognition

What's new in handwriting recognition?

Windows® 7 provides many Tablet PC improvements for handwriting recognition, including:

- Support for handwriting recognition, personalization, and text prediction in new languages.
- Support for handwritten math expressions.
- Personalized custom dictionaries for handwriting recognition.
- New integration capabilities for software developers.

In Windows Vista, handwriting recognition is supported for eight Latin languages: English (United States and United Kingdom), German, French, Spanish, Italian, Dutch, and Brazilian Portuguese, and four East Asian languages: Japanese, Chinese (Simplified and Traditional), and Korean. For Windows 7, 14 additional languages are supported: Norwegian (Bokmål and Nynorsk), Swedish, Finnish, Danish, Polish, Portuguese (Portugal), Romanian, Serbian (Cyrillic and Latin), Catalan, Russian, Czech, and Croatian. Windows 7 users can launch the Tablet Input Panel (TIP), write in their desired language for which a recognizer is available, and insert the converted, recognized text into applications such as Microsoft Outlook® or Word.

In Windows Vista, personalization for handwriting recognition is supported only for United States English and United Kingdom English for the Latin languages. For Windows 7, six additional Latin languages for which base recognizers shipped in Windows Vista will receive the benefits of the Personalization features. Additionally, personalization will be included for all 14 new languages in Windows 7. Personalization improves a user's handwriting experience significantly as the recognizer learns how and what a user writes.

When using the soft (on-screen) keyboard in Windows 7, Text Prediction helps you enter text more efficiently. Users typing a few letters will be offered a list of words that match. Based on the words users input frequently and the corrections that they make, Windows 7 will become even better at predicting what a user types over time. When using the soft keyboard, Windows 7 supported languages for Text Prediction are expanded beyond the support of United States English and United Kingdom English in Windows Vista to include the following: French, German, Italian, Korean, Simplified Chinese, Traditional Chinese, and Japanese. New languages supported for Text Prediction with pen input include Simplified Chinese and Traditional Chinese. Text Prediction for Simplified Chinese and Traditional Chinese offers both word completion and next word prediction. Users will benefit from this feature as it significantly speeds up handwriting input for these languages.

Windows 7 enables users who work with math expressions to use handwriting recognition to input math expressions via the Math Input Panel, a new accessory. The Math Input Panel recognizes handwritten math expressions, provides a rich correction experience, and inserts math expressions into target programs. Math Input Control, which offers the same recognition and correction functionality, enables developers to integrate math handwriting recognition into programs directly for a higher degree of control and customization.

In Windows Vista, the ability of users to add a new word to the built-in dictionaries is limited. Windows 7 allows users to create custom dictionaries, enabling them to replace or augment the built-in vocabulary by using their own specialized wordlists.

Windows 7 exposes many Tablet PC enhancements for access by software developers, so they can make their applications more useful. For example, updated Ink Analysis APIs in Windows 7 enhance and accelerate the development of ink-enabled applications—and make it easier to integrate basic shape recognition features. Through these capabilities, users will benefit from more options in programs that can use the unique capabilities of a Tablet PC.

What's New in Networking

What are the major changes?

The Windows Server® 2008 R2 and Windows® 7 operating systems include networking enhancements that make it easier for users to get connected and stay connected regardless of their location or type of network. These enhancements also enable IT professionals to meet the needs of their business in a secure, reliable, and flexible way.

New networking features covered in this topic include:

- DirectAccess, which enables users to access an enterprise network without the extra step of initiating a virtual private network (VPN) connection.
- VPN Reconnect, which automatically re-establishes a VPN connection as soon as Internet connectivity is restored, saving users from re-entering their credentials and re-creating the VPN connection.
- BranchCache™, which enables updated content from file and Web servers on a wide area network (WAN) to be cached on computers at a local branch office, increasing application response time and reducing WAN traffic.

- URL-based Quality of Service (QoS), which enables you to assign a priority level to traffic based on the URL from which the traffic originates.
- Mobile broadband device support, which provides a driver-based model for devices that are used to access a mobile broadband network.
- Multiple active firewall profiles, which enable the firewall rules most appropriate for each network adapter based on the network to which it is connected.

Who will be interested in these features?

The following groups might be interested in these features:

- IT managers
- System architects and administrators
- Network architects and administrators
- Security architects and administrators
- Application architects and administrators
- Web architects and administrators

What does DirectAccess do?

With the DirectAccess feature introduced in Windows Server 2008 R2, domain member computers running Windows 7 can connect to enterprise network resources whenever they connect to the Internet. During access to network resources, a user connected to the Internet has virtually the same experience as if connected directly to an organization's local area network (LAN). Furthermore, DirectAccess enables IT professionals to manage mobile computers outside of the office. Each time a domain member computer connects to the Internet, before the user logs on, DirectAccess establishes a bi-directional connection that enables the client computer to stay up to date with company policies and receive software updates.

Security and performance features of DirectAccess include authentication, encryption, and access control. IT professionals can configure the network resources to which each user can connect, granting unlimited access or allowing access only to specific servers or networks. DirectAccess also offers a feature that sends only the traffic destined for the enterprise network through the DirectAccess server. Other Internet traffic is routed through the Internet gateway that the client computer uses. This feature is optional, and DirectAccess can be configured to send all traffic through the enterprise network.

Are there any special considerations?

The DirectAccess server must be running Windows Server 2008 R2, must be a domain member, and must have two physical network adapters installed. Dedicate the DirectAccess server only to DirectAccess and do not have it host any other primary functions. DirectAccess clients must be domain members running Windows 7. Use the Add Features Wizard in Server Manager to install the DirectAccess Management console, which enables you to set up the DirectAccess server and monitor DirectAccess operations after setup.

Infrastructure considerations include the following:

- **Active Directory Domain Services (AD DS).** At least one Active Directory® domain must be deployed. Workgroups are not supported.
- **Group Policy.** Group Policy is recommended for deployment of client settings.
- **Domain controller.** At least one domain controller in the domain containing user accounts must be running Windows Server 2008 or later.
- **Public key infrastructure (PKI).** A PKI is required to issue certificates. External certificates are not required. All SSL certificates must have a certificate revocation list (CRL) distribution point that is reachable via a publicly resolvable fully qualified domain name (FQDN) while either local or remote.
- **IPsec policies.** DirectAccess uses IPsec to provide authentication and encryption for communications across the Internet. It is recommended that administrators be familiar with IPsec.
- **IPv6.** IPv6 provides the end-to-end addressing necessary for clients to maintain constant connectivity to the enterprise network. Organizations that are not yet ready to fully deploy IPv6 can use IPv6 transition technologies such as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Teredo, and 6to4 to connect across the IPv4 Internet and to access IPv4 resources on the enterprise network. IPv6 or transition technologies must be available on the DirectAccess server and allowed to pass through the perimeter network firewall.

What does VPN Reconnect do?

VPN Reconnect is a new feature of Routing and Remote Access service (RRAS) that provides users with seamless and consistent VPN connectivity, automatically reestablishing a VPN when users temporarily lose their Internet connection. Users who connect using wireless mobile broadband will benefit most from this capability. With VPN Reconnect, Windows 7 automatically reestablishes active VPN connections when Internet connectivity is reestablished. Although the reconnection might take several seconds, it is transparent to users.

VPN Reconnect uses IPsec tunnel-mode with Internet Key Exchange version 2 (IKEv2), which is described in RFC 4306, specifically taking advantage of the IKEv2 mobility and multihoming extension (MOBIKE) described in RFC 4555.

Are there any special considerations?

VPN Reconnect is implemented in the RRAS role service of the Network Policy and Access Services (NPAS) role of a computer running Windows Server 2008 R2. Infrastructure considerations include those for NPAS and RRAS. Client computers must be running Windows 7 to take advantage of VPN Reconnect.

What does BranchCache do?

With BranchCache, content from Web and file servers on the enterprise WAN is stored on the local branch office network to improve response time and reduce WAN traffic. When another client at the same branch office requests the same content, the client can access it directly from the local network without obtaining the entire file across the WAN. BranchCache can be set up to operate in either a *distributed cache* mode or a *hosted cache* mode. Distributed cache mode uses a peer-to-peer architecture. Content is cached at the branch office on the client computer that firsts requests it. The client computer subsequently makes the cached content available to other local clients. Hosted cache mode uses a client/server architecture. Content requested by a client at the branch office is subsequently cached to a local server (called the *hosted cache server*), where it is made available to other local clients. In either mode, before a client retrieves content, the server where the content originates authorizes access to the content, and content is verified to be current and accurate using a hash mechanism.

Are there any special considerations?

BranchCache supports HTTP, including HTTPS, and Server Message Block (SMB), including signed SMB. Content servers and the hosted cache server must be running Windows Server 2008 R2, and client computers must be running Windows 7.

What does URL-based QoS do?

QoS marks IP packets with a Differentiated Services Code Point (DSCP) number that routers then examine to determine the priority of the packet. If packets are queued at the router, higher priority packets are sent before lower priority packets. With URL-based QoS, IT professionals can prioritize network traffic based on the source URL, in addition to prioritization based on IP address and ports. This gives IT professionals more control over network traffic, ensuring that important Web traffic is processed before less-important traffic, even when that traffic originates at the same server. This can improve performance on busy networks. For example, you can assign Web traffic for critical internal Web sites a higher priority than external Web sites. Similarly non-work-related Web sites that can consume network bandwidth can be assigned a lower priority so that other traffic is not affected.

What does mobile broadband device support do?

The Windows 7 operating system provides a driver-based model for mobile broadband devices. Earlier versions of Windows require users of mobile broadband devices to install third-party software, which is difficult for IT professionals to manage because each mobile broadband device and provider has different software. Users also have to be trained to use the software and must have administrative access to install it, preventing standard users from easily adding a mobile broadband device. Now, users can simply connect a mobile broadband device and immediately begin using it. The interface in Windows 7 is the same regardless of the mobile broadband provider, reducing the need for training and management efforts.

What do multiple active firewall profiles do?

Windows Firewall settings are determined by the profile that you are using. In previous versions of Windows, only one firewall profile can be active at a time. Therefore, if you have multiple network adapters connected to different network types, you still have only one active profile—the profile providing the most restrictive rules. In Windows Server 2008 R2 and Windows 7, each network adapter applies the firewall profile that is most appropriate for the type of network to which it is connected: Private, Public, or Domain. This means that if you are at a coffee shop with a wireless hotspot and connect to your corporate domain network by using a VPN connection, then the Public profile continues to protect the network traffic that does not go through the tunnel, and the Domain profile protects the network traffic that goes through the tunnel. This also addresses the issue of a network adapter that is not connected to a network. In Windows 7 and Windows Server 2008 R2, this unidentified network will be assigned the Public profile, and other network adapters on the computer will continue to use the profile that is appropriate for the network to which they are attached.

What's New in Service Accounts

One of the security challenges for critical network applications such as Exchange and Internet Information Services (IIS) is selecting the appropriate type of account for the application to use.

On a local computer, an administrator can configure the application to run as Local Service, Network Service, or Local System. These service accounts are simple to configure and use but are typically shared among multiple applications and services and cannot be managed on a domain level.

If you configure the application to use a domain account, you can isolate the privileges for the application, but you need to manually manage passwords or create a custom solution for managing these passwords. Many SQL Server and IIS applications use this strategy to enhance security, but at a cost of additional administration and complexity.

In these deployments, service administrators spend a considerable amount of time in maintenance tasks such as managing service passwords and service principal names (SPNs), which are required for Kerberos authentication. In addition, these maintenance tasks can disrupt service.

What's new in service accounts?

Two new types of service accounts are available in Windows Server® 2008 R2 and Windows® 7—the managed service account and the virtual account. The managed service account is designed to provide crucial applications such as SQL Server and IIS with the isolation of their own domain accounts, while eliminating the need for an administrator to manually administer the service principal name (SPN) and credentials for these accounts. Virtual accounts in Windows Server 2008 R2 and Windows 7 are "managed local accounts" that can use a computer's credentials to access network resources.

Who will want to use service accounts?

Administrators will want to use managed service accounts to enhance security while simplifying or eliminating password and SPN management.

Virtual accounts simplify service administration by eliminating password management and allowing services to access the network with the computer's account credentials in a domain environment.

What are the benefits of new service accounts?

In addition to the enhanced security that is provided by having individual accounts for critical services, there are four important administrative benefits associated with managed service accounts:

- Managed service accounts allow administrators to create a class of domain accounts that can be used to manage and maintain services on local computers.
- Unlike with regular domain accounts in which administrators must reset passwords manually, the network passwords for these accounts will be reset automatically.
- Unlike with normal local computer and user accounts, the administrator does not have to complete complex SPN management tasks to use managed service accounts.
- Administrative tasks for managed service accounts can be delegated to non-administrators.

What's the impact of these changes on account management?

Managed service accounts can reduce the amount of account management needed for critical services and applications.

Are there any special considerations for using the new service account options?

To use managed service accounts and virtual accounts, the client computer on which the application or service is installed must be running Windows Server 2008 R2 or Windows 7. In Windows Server 2008 R2 and Windows 7, one managed service account can be used for services on a single computer. Managed service accounts cannot be shared between multiple computers and cannot be used in server clusters where a service is replicated on multiple cluster nodes.

Windows Server 2008 R2 domains provide native support for both automatic password management and SPN management. If the domain is running in Windows Server 2003 mode or Windows Server 2008 mode, additional configuration steps will be needed to support managed service accounts. This means that:

- If the domain controller is running Windows Server 2008 R2 and the schema has been upgraded to support managed service accounts, both automatic password and SPN management are available.
- If the domain controller is on a computer running Windows Server 2008 or Windows Server 2003 and the Active Directory schema has been upgraded to support this feature, managed service accounts can be used and service account passwords will be managed automatically. However, the domain administrator using these server operating systems will still need to manually configure SPN data for managed service accounts.

To use managed service accounts in Windows Server 2008, Windows Server 2003, or mixed-mode domain environments, the following schema changes must be applied:

- Run **adprep /forestprep** at the forest level.
- Run **adprep /domainprep** in every domain where you want to create and use managed service accounts.
- Deploy a domain controller running Windows Server 2008 R2 in the domain to manage managed service accounts by using Windows PowerShell cmdlets.

  For more information, see **AdPrep**.

For more information about managing SPNs, see Service Principal Names.

What's New in Smart Cards

Windows® 7 includes new features that make smart cards easier to use and to deploy, and makes it possible to use smart cards to complete a greater variety of tasks. The new smart card features are available in all versions of Windows 7.

What's new in smart cards?

Windows 7 features enhanced support for smart card–related Plug and Play and the Personal Identity Verification (PIV) standard from the National Institute of Standards and Technology (NIST).

This means that users of Windows 7 can use smart cards from vendors who have published their drivers through Windows Update without needing special middleware. These drivers are downloaded in the same way as drivers for other devices in Windows.

When a PIV-compliant smart card is inserted into a smart card reader, Windows attempts to download the driver from Windows Update. If an appropriate driver is not available from Windows Update, a PIV-compliant minidriver that is included with Windows 7 is used for the card.

Who will want to use smart cards?

Network administrators who want to enhance the security of the organization's computers, particularly portable computers used by remote users, will appreciate the simplified deployment and use scenarios made possible by smart card Plug and Play PIV support. Users will appreciate the ability to use smart cards to perform critical business tasks in a secure manner.

What are the benefits of the new and changed features?

The new smart card support options in Windows 7 include:

- **Encrypting drives with BitLocker Drive Encryption.** In the Windows 7 Enterprise and Windows 7 Ultimate operating systems, users can choose to encrypt their removable media by turning on BitLocker and then choosing the smart card option to unlock the drive. At run time, Windows retrieves the correct minidriver for the smart card and allows the operation to complete.
- **Smart card domain logon by using the PKINIT protocol.** In Windows 7, the correct minidriver for a smart card is retrieved automatically, enabling a new smart card to authenticate to the domain without requiring the user to install or configure additional middleware.
- **Document and e-mail signing.** Windows 7 users can rely on Windows to retrieve the correct minidriver for a smart card at run time to sign an e-mail or document. In addition, XML Paper Specification (XPS) documents can be signed without the need for additional software.
- **Use with line-of-business applications.** In Windows 7, any application that uses Cryptography Next Generation (CNG) or CryptoAPI to enable the application to use certificates can rely on Windows to retrieve the correct minidriver for a smart card at run time so that no additional middleware is needed.

What's the impact of these changes on smart card usage?

Smart card usage is expanding rapidly. To encourage more organizations and users to adopt smart cards for enhanced security, the process to provision and use new smart cards is simplified and supports more end user scenarios.

What's New in User Account Control

What's new in User Account Control?

Before the introduction of User Account Control (UAC), when a user was logged on as an administrator, that user was automatically granted full access to all system resources. While running as an administrator enabled a user to install legitimate software, the user could also unintentionally or intentionally install a malicious program. A malicious program installed by an administrator can fully compromise the computer and affect all users.

With the introduction of UAC, the access control model changed to help mitigate the impact of a malicious program. When a user attempts to start an administrator task or service, the **User Account Control** dialog box asks the user to click either **Yes** or **No** before the user's full administrator access token can be used. If the user is not an administrator, the user must provide an administrator's credentials to run the program. Because UAC requires an administrator to approve application installations, unauthorized applications cannot be installed automatically or without the explicit consent of an administrator.

In Windows® 7 and Windows Server® 2008 R2, UAC functionality is improved to:

- Increase the number of tasks that the standard user can perform that do not prompt for administrator approval.
- Allow a user with administrator privileges to configure the UAC experience in the Control Panel.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for local administrators in Admin Approval Mode.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for standard users.

Who will want to use UAC?

UAC helps standard users and administrators protect their computers by preventing programs that may be malicious from running. The improved user experience makes it easier for users to perform daily tasks while protecting their computers.

UAC helps enterprise administrators protect their network by preventing users from running malicious software.

What are the benefits of the new and changed features?

By default, standard users and administrators access resources and run applications in the security context of standard users. When a user logs on to a computer, the system creates an access token for that user. The access token contains information about the level of access that the user is granted, including specific security identifiers (SIDs) and Windows privileges.

When an administrator logs on, two separate access tokens are created for the user: a standard user access token and an administrator access token. The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs have been removed. The standard user access token is used to start applications that do not perform administrative tasks (standard user applications).

When the user runs applications that perform administrative tasks (administrator applications), the user is prompted to change or "elevate" the security context from a standard user to an administrator, called Admin Approval Mode. In this mode, the administrator must provide approval for applications to run on the secure desktop with administrative privileges. The improvements to

UAC in Windows 7 and Windows Server 2008 R2 result in an improved user experience when configuring and troubleshooting your computer.

The built-in Administrator account in Windows Server 2008 R2 does not run in Admin Approval Mode

The built-in Administrator account in Windows Server 2008 R2, which is the first account created on a server, does not run in Admin Approval Mode. All subsequently created administrator accounts in Windows Server 2008 R2 do run in Admin Approval Mode.

The built-in Administrator account is disabled by default in Windows 7

The built-in Administrator account is disabled by default in Windows 7. If the built-in Administrator account is the only active local administrator account during an upgrade from Windows XP, Windows 7 leaves the account enabled and places the account in Admin Approval Mode. The built-in Administrator account, by default, cannot log on to the computer in Safe Mode.

Behavior of computers that are not domain members

When there is at least one configured local administrator account, the disabled built-in Administrator account cannot log on in Safe Mode. Instead, any local administrator account can be used to log on. If the last local administrator account is inadvertently demoted, disabled, or deleted, Safe Mode allows the disabled built-in Administrator account to log on for disaster recovery.

Behavior of computers that are domain members

The disabled built-in Administrator account in all cases cannot log on in Safe Mode. A user account that is a member of the **Domain Admins** group can log on to the computer to create a local administrator if none exists.

Important

If the domain administrator account has never logged on to the client computer, you must start the computer in Safe Mode with Networking to cache the credentials on the client computer.

Note

After the computer is removed from the domain, it reverts back to the non-domain member behavior.

All subsequent user accounts are created as standard users in Windows 7

Standard user accounts and administrator user accounts can use UAC enhanced security. In new Windows 7 installations, by default, the first user account created is a local administrator account in Admin Approval Mode (UAC enabled). All subsequent accounts are then created as standard users.

Reduced number of UAC prompts

Windows 7 and Windows Server 2008 R2 reduce the number of UAC prompts that local administrators and standard users must respond to.

To reduce the number of prompts that a local administrator must respond to:

- File operation prompts are merged.
- Internet Explorer prompts for running application installers are merged.
- Internet Explorer prompts for installing ActiveX® controls are merged.

The default UAC setting allows a standard user to perform the following tasks without receiving a UAC prompt:

- Install updates from Windows Update.
- Install drivers that are downloaded from Windows Update or included with the operating system.
- View Windows settings. (However, a standard user is prompted for elevated privileges when changing Windows settings.)
- Pair Bluetooth devices to the computer.
- Reset the network adapter and perform other network diagnostic and repair tasks.

Configure UAC experience in Control Panel

Windows Vista® offers two levels of UAC protection to the user: on or off. Windows 7 and Windows Server 2008 R2 introduce additional prompt levels that are similar to the Internet Explorer security zone model. If you are logged on as a local administrator, you can enable or disable UAC prompts, or choose when to be notified about changes to the computer. There are four levels of notification to choose from:

- **Never notify me**. You are not notified of any changes made to Windows settings or when software is installed.
- **Only notify me when programs try to make changes to my computer**. You are not notified when you make changes to Windows settings, but you do receive notification when a program attempts to make changes to the computer.
- **Always notify me**. You are notified when you make changes to Windows settings and when programs attempt to make changes to the computer.

- **Always notify me and wait for my response**. You are prompted for all administrator tasks on the secure desktop. This choice is similar to the current Windows Vista behavior.

The following table compares the number of UAC prompts for user actions in Windows 7 and Windows Server 2008 R2 with the number of UAC prompts in Windows Vista Service Pack 1.

Actions	Only notify me when programs try to make changes to my computer	Always notify me
Change personalization settings	No prompts	Fewer prompts
Manage your desktop	No prompts	Fewer prompts
Set up and troubleshoot your network	No prompts	Fewer prompts
Use Windows Easy Transfer	Fewer prompts	Same number of prompts
Install ActiveX controls through Internet Explorer	Fewer prompts	Fewer prompts
Connect devices	No prompts	No prompts if drivers are on Windows Update, or similar number of prompts if drivers are not on Windows Update
Use Windows Update	No prompts	No prompts
Set up backups	No prompts	Same number of prompts
Install or remove software	No prompts	Fewer prompts

Change the behavior of UAC messages for local administrators

If you are logged on as a local administrator, you can change the behavior of UAC prompts in the local security policies for local administrators in Admin Approval Mode.

- **Elevate without prompting**. Applications that are marked as administrator applications and applications that are detected as setup applications are run automatically with the full administrator access token. All other applications are automatically run with the standard user token.
- **Prompt for credentials on the secure desktop**. The **User Account Control** dialog box is displayed on the secure desktop. To give consent for an application to run with the full administrator access token, the user must enter administrative credentials. This setting supports compliance with Common Criteria or corporate policies.
- **Prompt for consent on the secure desktop**. The **User Account Control** dialog box is displayed on the secure desktop. To give consent for an application to run with the full

administrator access token, the user must click **Yes** or **No** on the **User Account Control** dialog box. If the user is not a member of the local **Administrators** group, the user is prompted for administrative credentials. This setting supports compliance with Common Criteria or corporate policies.

- **Prompt for credentials**. This setting is similar to **Prompt for credentials on the secure desktop**, but the **User Account Control** dialog box is displayed on the desktop instead.
- **Prompt for consent**. This setting is similar to **Prompt for consent on the secure desktop**, but the **User Account Control** dialog box is displayed on the desktop instead.
- **Prompt for consent for non-Windows binaries**. The **User Account Control** dialog box is displayed on the desktop for all files that are not digitally signed with the Windows digital certificate.

Change the behavior of UAC messages for standard users

If you are logged on as a local administrator, you can change the behavior of UAC prompts in the local security policies for standard users.

- **Automatically deny elevation requests**. Administrator applications cannot run. The user receives an error message that indicates a policy is preventing the application from running.
- **Prompt for credentials**. This is the default setting. For an application to run with the full administrator access token, the user must enter administrative credentials in the **User Account Control** dialog box that is displayed on the desktop.
- **Prompt for credentials on the secure desktop**. For an application to run with the full administrator access token, the user must enter administrative credentials in the **User Account Control** dialog box that is displayed on the secure desktop.

What's the impact of these changes on UAC?

In response to customer requests, the improved UAC allows users to perform their daily tasks with fewer prompts and gives administrators more control over how UAC prompts users.

What's New in Virtual Hard Disks

The Microsoft virtual hard disk (.vhd) file format is a publicly available format specification that specifies a virtual hard disk encapsulated in a single file, capable of hosting native file systems and supporting standard disk operations. Virtual hard disk files are used by Hyper-V™ in Windows Server 2008, Microsoft Virtual Server, and Microsoft Virtual PC for virtual disks connected to a virtual machine. The .vhd file format is also used by Microsoft Data Protection Manager, Windows Server Backup, and many other Microsoft and non-Microsoft solutions.

What's new in virtual hard disks?

In Windows® 7, a virtual hard disk can be used as the running operating system on designated hardware without any other parent operating system, virtual machine, or hypervisor. You can use the Windows 7 disk management tools (the DiskPart command-line tool and the Disk Management snap-in) to create a .vhd file. You can deploy a Windows 7 image (in .wim format) to the virtual hard disk, and you can copy the .vhd file to multiple systems. You can configure the Windows 7 boot manager for a native or physical boot of the Windows image that is contained in the virtual hard disk. Furthermore, you can connect the .vhd file to a virtual machine for use with the Hyper-V role in Windows Server® 2008 R2. Native-boot .vhd files are not designed or intended to replace full image deployment on all client or server systems. Previous versions of Windows do not support a native boot from a virtual hard disk and require a hypervisor and virtual machine in order to boot from a .vhd file.

For instructions, see **Walkthrough: Deploy a Virtual Hard Disk for Native Boot** and **Add a Native-Boot Virtual Hard Disk to the Boot Menu**.

Who will want to use virtual hard disks?

Enterprise environments already managing and using .vhd files for virtual machine deployment will find the most benefit from the disk management support for .vhd files and native-boot virtual hard disk capabilities. Many data center customers are transitioning to virtual machines on a server running Hyper-V in order to consolidate servers and lower energy costs. Native virtual hard disk support in the disk management utilities and core storage system simplify creation and image management in .vhd files.

While moving an increasing number of applications to virtual machines, enterprise environments still operate a significant part of the data center on physical computers. IT administrators have to maintain two sets of images: one set based on the .wim format for physical computers, and another set based on the .vhd format for virtual machines. The common image format supporting both physical and virtual machines provides flexibility in image deployment while simplifying the process of image management.

Developers and testers are using virtual machines to test new system and application software. Virtual machines provide a convenient, isolated test environment and reduce the need for dedicated test hardware. But sometimes you need to run tests on a physical computers to access a specific hardware device, like the graphics card, or to get accurate performance profiling. A common image format that runs on both virtual and physical machines also benefits developers and testers. A native boot from a virtual hard disk enables booting a Windows 7 image from a file without creating a separate physical disk partition in which to install Windows.

What are the benefits of the new and changed features?

Native support for virtual hard disks simplifies image management and reduces the number of images to catalog and maintain. To create a virtual hard disk on Windows Server 2008, you install the Hyper-V server role, use Hyper-V Manager to create a .vhd file, and then start the virtual machine to install a version of Windows from the CD/DVD onto a partition in the virtual hard disk. In Windows 7, the native support for the .vhd format means that you can create and modify .vhd files without installing the Hyper-V server role. You can attach .vhd files using the disk management tools, and you can service the Windows image inside the virtual hard disk. The deployment tools in the Windows Automated Installation Kit (Windows AIK) can be used to apply a Windows image to the virtual hard disk, and to apply updates to the system image in the .vhd file.

The Windows image applied to a .vhd file can boot in a virtual machine on a server running Hyper-V or can boot natively on a physical computer without the use of a hypervisor. In order to boot the Windows system in either a virtual or physical computer, the boot environment must be initialized correctly for each scenario.

What are the dependencies?

The steps for deploying a Windows 7 or Windows Server 2008 R2 image to a .vhd file depends on the Windows deployment tools, including Imagex.exe. Imagex.exe is used to capture a Windows operating system partition into a Windows Image (.wim) file format, and to apply a .wim file to a file system partition (which may reside inside a .vhd file).

Imagex.exe is one of the tools in the Windows Automated Installation Kit (Windows AIK). You must install the latest version of the Windows AIK at **Windows Automated Installation Kit for Windows 7 Beta**. The Windows AIK download is an ISO image that you burn to a DVD and then install on your system. After installing the Windows AIK, ImageX.exe is located in the Windows AIK\PE Tools directory.

A native boot of Windows 7 from a .vhd file also requires the Windows 7 boot environment. The Windows 7 boot environment is initialized during a full operating system installation and includes the Windows Boot Manager, Boot Configuration Data (BCD), and other supporting files.

What's the impact of these changes on virtual hard disks?

The support for virtual hard disks as a native format targets key scenarios in the enterprise where the IT staff is well versed with different imaging technologies and tools to manage their client and servers. A managed enterprise environment also employs technologies like folder redirection and roaming profiles to manage the user’s data outside the deployed virtual hard disk images. There are recommendations and limitations for virtual hard disks in the **Frequently Asked Questions: Virtual Hard Disks** topic.

What's New in Windows PowerShell

Windows PowerShell™ is a command-line shell and scripting language designed especially for system administration. Built on the Microsoft .NET Framework, Windows PowerShell helps IT professionals control and automate the administration of Windows operating systems and of applications that run on Windows.

The simple command tools in Windows PowerShell, called *cmdlets*, let you manage the computers in your enterprise from the command line. Windows PowerShell *providers* let you access data stores, such as the registry and the certificate store, as easily as you access the file system. In addition, Windows PowerShell has full support for all Windows Management Instrumentation (WMI) classes.

Windows PowerShell is fully extensible. You can write your own cmdlets, providers, functions, and scripts, and you can package them in modules to share with other users.

Windows® 7 includes Windows PowerShell 2.0. It also includes other cmdlets, providers, and tools that you can add to Windows PowerShell so that you can use and manage other Windows technologies such as Active Directory® Domain Services, Windows® BitLocker™ Drive Encryption, the DHCP Server service, Group Policy, Remote Desktop Services, and Windows Server Backup.

What's new in Windows PowerShell?

The following changes are available in Windows PowerShell in Windows 7:

- **New cmdlets.** Windows PowerShell includes more than 100 new cmdlets, including Get-Hotfix, Send-MailMessage, Get-ComputerRestorePoint, New-WebServiceProxy, Debug-Process, Add-Computer, Rename-Computer, Reset-ComputerMachinePassword, and Get-Random.
- **Remote management.** You can run commands on one computer or hundreds of computers with a single command. You can establish an interactive session with a single computer. And, you can establish a session that can receive remote commands from multiple computers.
- **Windows PowerShell Integrated Scripting Environment (ISE).** Windows PowerShell ISE is a graphical user interface for Windows PowerShell that lets you run commands, and write, edit, run, test, and debug scripts in the same window. It offers up to eight independent execution environments and includes a built-in debugger, multiline editing, selective execution, syntax colors, line and column numbers, and context-sensitive Help.
- **Background jobs.** With Windows PowerShell background jobs, you can run commands asynchronously and "in the background" so you can continue to work in your session. You can run background jobs on a local or remote computer, and you can store the results locally or remotely.
- **Debugger.** The Windows PowerShell debugger can help you debug functions and scripts. You can set and remove breakpoints, step through code, check the values of variables, and display a call-stack trace.

- **Modules.** Windows PowerShell modules let you organize your Windows PowerShell scripts and functions into independent, self-contained units. You can package your cmdlets, providers, scripts, functions, and other files into modules that you can distribute to other users. Modules are easier for users to install and use than Windows PowerShell snap-ins. Modules can include any type of file, including audio files, images, Help files, and icons. Modules run in a separate session to avoid name conflicts.
- **Transactions.** Windows PowerShell now supports transactions, which let you manage a set of commands as a logical unit. A transaction can be committed, or it can be completely undone so that the affected data is not changed by the transaction.
- **Events.** Windows PowerShell includes a new event infrastructure that lets you create events, subscribe to system and application events, and then listen, forward, and act on the events synchronously and asynchronously.
- **Advanced functions.** Advanced functions behave just like cmdlets, but they are written in the Windows PowerShell scripting language instead of in C#.
- **Script internationalization.** Scripts and functions can display messages and Help text to users in multiple languages.
- **Online Help.** In addition to Help at the command line, the Get-Help cmdlet has a new Online parameter that opens a complete and updated version of each Help topic on Microsoft TechNet.

Who will want to use Windows PowerShell?

The following groups might be interested in these changes:

- IT professionals who want to manage Windows at the command line and automate administrative tasks.
- Developers who want to use the extensive Windows PowerShell scripting language to build .NET Framework applications and extend Windows PowerShell.
- All users who want to learn Windows PowerShell to manage their system, write scripts to automate their tasks, and create new tools without having to learn a programming language.

What are the benefits of the new and changed features?

Windows PowerShell provides these new management features, among many others.

Remote Management

Windows PowerShell remote management lets users connect to and run Windows PowerShell commands on all of their computers. IT professionals can use it to monitor and maintain computers, distribute updates, run scripts and background jobs, collect data, and make uniform, optimized changes to one computer or to hundreds of computers.

Windows PowerShell ISE

Windows PowerShell ISE makes it easier and more efficient to use Windows PowerShell. Beginners will appreciate the syntax colors and the context-sensitive Help. Multiline editing makes it easy to try the examples that you copy from the Help topics and from other sources. Advanced users will appreciate the availability of multiple execution environments, the built-in debugger, and the extensibility of the Windows PowerShell ISE object model.

Modules

Windows PowerShell modules make it easier for cmdlet and provider authors to organize and distribute tools and solutions. And, they make it easier for users to install the tools and add them to their Windows PowerShell sessions. IT professionals can use modules to distribute tested and approved solutions throughout their enterprise and share them with other professionals in the community.

Transactions

Windows PowerShell transactions let you use Windows PowerShell to make changes that might have to be rolled back or committed as a unit, such as database updates and changes to the registry.

What's the impact of these changes on Windows PowerShell?

Windows PowerShell has the following system and feature requirements:

- Windows PowerShell requires the Microsoft .NET Framework 2.0.
- Windows PowerShell ISE, the graphical user interface program for Windows PowerShell, requires the Microsoft .NET Framework 3.5 with Service Pack 1.
- The Out-GridView cmdlet requires the Microsoft .NET Framework 3.5 with Service Pack 1.
- The Get-WinEvent cmdlet requires Windows Vista or later versions of Windows and the Microsoft .NET Framework 3.5.
- The Export-Counter cmdlet runs only on Windows 7 and later versions of Windows.
- The WMI-based remoting features of Windows PowerShell require no configuration and run on all versions of Windows that support Windows PowerShell. The WS-Management-based remoting features require both the local and remote computers to run Windows Vista or a later version of Windows. Also, you must enable and configure WS-Management on all participating computers. For more information, see About_Remote.
- Several cmdlets work only when the current user is a member of the Administrators group on the computer or when the current user can provide the credentials of a member of the Administrators group. This requirement is explained in the Help topics for the affected cmdlets.

What's New in Windows Search, Browse, and Organization

What's new in Windows Search, Browse, and Organization?

Windows® 7 introduces a number of new features and enhancements that can help IT professionals deploy and maintain desktop search, browse, and organization functionality:

- Improvements in the performance and stability of the indexer.
- Improvements in the performance and relevance of the search experience.
- The introduction of federated search and search connectors.
- The introduction of aggregation and visualizations to improve the organization of search results.
- The introduction of libraries to help with organization.
- Improvements in the performance and user interface of Windows Explorer.
- Additional Group Policy settings, available on all supported operating systems.
- Reduced impact on the server running Microsoft Exchange Server when indexing uncached (classic online) e-mail.
- The ability to index delegate mailboxes for e-mail.
- Support for indexing encrypted documents of local file systems.
- Support for indexing digitally signed e-mail of MAPI-enabled e-mail clients such as Microsoft Outlook®.
- An expanded ability to do fast remote queries of file shares, including on Windows Vista®, Windows Server® 2008, Windows® XP with Windows Search 4.0 installed, and earlier versions.

The Windows Search Service enables you to perform fast file searches on a server from computers running Windows 7 or Windows Server® 2008 R2, or from computers that have Windows Desktop Search installed and are running Windows Vista, Windows Server 2008, Windows XP, Windows Server® 2003 R2, or Windows Server® 2003.

Note

Indexing of uncached e-mail is also known as classic online e-mail. In Windows® 7, there is less impact on Microsoft Exchange Server when indexing uncached e-mail. In contrast to uncached or classic online e-mail, cached e-mail uses a local Offline Folder file (.ost) to keep a local copy of your Exchange Server mailbox on your computer, which permits indexing of e-mail locally.

Who will want to use Windows Search, Browse, and Organization?

This feature is intended for IT professionals. Improvements in search are also relevant to home users.

Before deploying Windows Search, Browse, and Organization in Windows 7, administrators should consider several factors, including the following:

- The role of desktop search within your enterprise search strategy.
- Which data stores or services you want to publish for direct client access in Windows Explorer by using the OpenSearch standard.
- Current document storage practices and how they relate to libraries.
- The importance of file storage encryption to your organization.
- The importance of e-mail encryption and signing to your organization.

What are the benefits of the new and changed features?

A brief overview of the major new features and capabilities for Windows Search, Browse, and Organization in Windows 7 is provided in the following table.

Feature	New in Windows 7
Improvements in the performance and user interface of Windows Explorer	The navigation is better organized and more intuitive, everyday tasks are easier to access, and there are numerous improvements in the presentation of end user content.
The introduction of libraries to help with organization	Libraries make it quicker and easier to find files. Built on the existing **My Documents** experience, libraries work like folders do but have additional functionality. In addition to browsing files by using the hierarchical folder structure, you can also browse metadata such as date, type, author, and tags. Users can include files from multiple storage locations in their libraries without having to move or copy the files from original storage locations.
Improvements in the search experience	The search experience is integrated into everyday tasks through Windows Explorer, the **Start** menu, and the introduction of new libraries. Search results take relevance into account, making it faster to find what you are

Feature	New in Windows 7
	looking for. Other improvements to the experience include the introduction of highlighted matches in the searched document, a search builder to construct advanced queries, and arrangement views. Arrangement views allow you to pivot search results, list the most recent searches, and provide broader **Start** menu scope including Control Panel tasks.
The introduction of federated search and search connectors	Windows 7 enables searching for content on remote indices. Integrating federated search into Windows gives users the benefits of using familiar tools and workflows to search remote data. This enhanced integration provides the added benefit of highlighting matches within the searched document. Windows 7 enables federated search via the public OpenSearch standard. Other improvements are the consistent UI for remote search results within Windows Explorer and the ability to drag and drop files listed in the search results between different locations.
Indexing of uncached (classic online) e-mail	Before users can search for e-mail, the Windows indexing service must index the e-mail store, which involves collecting the properties and content of e-mail items within the store. This initial indexing is later followed by smaller incremental indexing (as e-mail arrives, is read, and deleted, and so on) to keep the index current. Windows 7 minimizes the impact on the server running Exchange Server by reducing the number of remote procedure calls (RPC) required to index e-mail messages and attachments. Because e-mail messages are indexed in native formats (HTML, RTF, and text) there is no load on the server to convert mail types. Windows indexes public folders only when they are cached locally.
Remote query	Windows 7 extends the ability to search across remote desktops. Windows 7 or Windows

Feature	New in Windows 7
	Search 4.0 (available on Windows Vista and Windows XP) enables users to query remote computers running on supported operating systems; Windows Vista allows users to search remote computers only if they are running Windows Vista.
Support for indexing encrypted files	Windows 7 fully supports indexing encrypted files on local file systems, allowing users to index and search the properties and contents of encrypted files. Users can manually configure Windows to include encrypted files in indexing, or administrators can configure this by using Group Policy.
Support for indexing digitally signed e-mail	Windows 7 allows users to search all content in digitally signed e-mail messages. This includes the message body and any attachments. A computer that is running Windows Vista Service Pack 1 (SP1) and Windows Search 4.0 functions as follows: • Users can search all digitally signed e-mail messages that they have sent. This search includes all message content. • Users can search all digitally signed e-mail messages that they have received. However, these searches are limited to certain properties, such as subject, sender, or recipients. Users cannot search the message body or attachment contents.

What's the impact of these changes on Windows Search, Browse, and Organization?

There are significant improvements in how you use Windows Search, Browse, and Organization in Windows 7:

- Closer integration with everyday workflows.
- More relevant search results.
- Highlighted search terms to easily identify results.
- An integrated advanced query builder.

In Windows 7, there is a new emphasis on organization with the introduction of libraries and the multiple improvements in the arrangement views and visualization of data.

Note

Windows 7 does not support indexing the content of encrypted e-mail messages or any S/MIME receipts that are received on S/MIME signed messages that you send.

What's New in Windows Security Auditing

What are the major changes?

There are a number of auditing enhancements in Windows Server® 2008 R2 and Windows® 7 that increase the level of detail in security auditing logs and simplify the deployment and management of auditing policies. These enhancements include:

- **Global Object Access Auditing.** In Windows Server 2008 R2 and Windows 7, administrators can define computer-wide system access control lists (SACLs) for either the file system or registry. The specified SACL is then automatically applied to every single object of that type. This can be useful both for verifying that all critical files, folders, and registry settings on a computer are protected, and for identifying when an issue with a system resource occurs.
- **"Reason for access" reporting.** This list of access control entries (ACEs) provides the privileges on which the decision to allow or deny access to the object was based. This can be useful for documenting the permissions, such as group memberships, that allow or prevent the occurrence of a particular auditable event.
- **Advanced audit policy settings.** These 53 new settings can be used in place of the nine basic auditing settings under **Local Policies\Audit Policy** to allow administrators to more specifically target the types of activities they want to audit and eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

The following sections describe these enhancements in greater detail.

What do these auditing enhancements do?

In Windows XP, administrators have nine categories of security auditing events that they can monitor for success, failure, or both success and failure. These events are fairly broad in scope and can be triggered by a variety of similar actions, some of which can generate a large number of event log entries.

In Windows Vista® and Windows Server 2008, the number of auditable events is expanded from nine to 50, which enables an administrator to be more selective in the number and types of events to audit. However, unlike the nine basic Windows XP events, these new audit events are not integrated with Group Policy and can only be deployed by using logon scripts generated with the Auditpol.exe command-line tool.

In Windows Server 2008 R2 and Windows 7, all auditing capabilities have been integrated with Group Policy. This allows administrators to configure, deploy, and manage these settings in the Group Policy Management Console (GPMC) or 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.

Audit policy enhancements in Windows Server 2008 R2 and Windows 7 allow administrators to connect business rules and audit policies. For example, applying audit policy settings on a domain or OU basis will allow administrators to document compliance with rules such as:

- Track all group administrator activity on servers with finance information.
- Track all the files that are accessed by defined groups of employees.
- Confirm that the correct SACL is applied to every file, folder, and registry key when they are accessed.

Who will be interested in this feature?

Auditing enhancements in Windows Server 2008 R2 and Windows 7 support the needs of IT professionals who are responsible for implementing, maintaining, and monitoring the ongoing security of an organization's physical and information assets.

These settings can help administrators answer questions such as the following:

- Who is accessing our assets?
- What assets are they accessing?
- When and where did they access them?
- How did they obtain access?

Security awareness and the desire to have a forensic trail are significant motivators behind these questions. The quality of this information is required and evaluated by auditors in a growing number of organizations.

Are there any special considerations?

A number of special considerations apply to various tasks associated with auditing enhancements in Windows Server 2008 R2 and Windows 7:

- **Creating an audit policy.** To create an advanced Windows security auditing policy, you must use the GPMC or Local Security Policy snap-in on a computer running Windows Server 2008 R2 or Windows 7. (You can use the GPMC on a computer running Windows 7 after installing the Remote Server Administration Tools.)
- **Applying audit policy settings.** If you are using Group Policy to apply the advanced audit policy settings and global object access settings, client computers must be running Windows Server 2008 R2 or Windows 7. In addition, only computers running Windows Server 2008 R2 or Windows 7 can provide "reason for access" reporting data.

- **Developing an audit policy model.** To plan advanced security audit settings and global object access settings, you must use the GPMC targeting a domain controller running Windows Server 2008 R2.
- **Distributing the audit policy.** After a Group Policy object (GPO) that includes advanced security auditing settings has been developed, it can be distributed by using domain controllers running any Windows server operating system. However, if you cannot put client computers running Windows 7 in a separate OU, you should use Windows Management Instrumentation (WMI) filtering to ensure that the advanced policy settings are applied only to client computers running Windows 7.

Note

Advanced audit policy settings can also be applied to client computers running Windows Vista. However, the audit policies for these client computers must be created and applied separately by using Auditpol.exe logon scripts.

Important

Using both the basic audit policy settings under **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 Advanced Audit Policy Configuration settings, you should enable the **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings** policy setting under **Local Policies\Security Options**. This will prevent conflicts between similar settings by forcing basic security auditing to be ignored.

In addition, to plan and deploy security event auditing policies, administrators need to address a number of operational and strategic questions, including:

- Why do we need an audit policy?
- Which activities and events are most important to our organization?
- Which types of audit events can we omit from our auditing strategy?
- How much administrator time and network resources do we want to devote to generating, collecting, and storing events, and analyzing the data?

Which editions include this feature?

All versions of Windows Server 2008 R2 and Windows 7 that can process Group Policy can be configured to use these security auditing enhancements. Versions of Windows Server 2008 R2 and Windows 7 that cannot join a domain do not have access to these features. There is no difference in security auditing support between 32-bit and 64-bit versions of Windows 7.

What new functionality does this feature provide?

The following new functionality is provided by Windows Server 2008 R2 and Windows 7: Global Object Access Auditing, "reason for access" settings, and advanced audit policy settings.

Global Object Access Auditing

With Global Object Access Auditing, administrators can define computer SACLs per object type for either the file system or 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 setting. For example, a policy setting "track all changes made by group administrators" will be enough to show that this policy is in effect.

Resource SACLs are also useful for diagnostic scenarios. For example, setting a Global Object Access Auditing policy to log all the activity for a specific user and enabling the Access Failures audit policies in a resource (file system, registry) will 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 (or a single registry setting SACL and a Global Object Access Auditing policy) 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.

"Reason for access" settings

There are several events in Windows to audit whenever an operation was successful or unsuccessful. The events usually include the user, the object, and the operation, but they lack the reason why the operation was allowed or denied. Forensics analysis and support scenarios are improved in Windows Server 2008 R2 and Windows 7 by logging the reason, based on specific permissions, why someone had access to corporate resources.

Advanced audit policy settings

In Windows Server 2008 R2 and Windows 7, enhanced audit policies can be configured and deployed by using domain Group Policy, which reduces management cost and overhead and significantly enhances the flexibility and effectiveness of security auditing.

The following sections describe the new events and event categories that are available in the **Advanced Audit Policy Configuration** node of Group Policy.

Account logon events

The events in this category help document domain attempts to authenticate account data, either to a domain controller or a local Security Accounts Manager (SAM). Unlike logon and logoff events, which track attempts to access a particular computer, events in this category report on the account database that is being used.

Setting	Description
Credential Validation	Audit events generated by validation tests on user account logon credentials.
Kerberos Service Ticket Operations	Audit events generated by Kerberos service ticket requests.
Other Account Logon Events	Audit events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets.
Kerberos Authentication Service	Audit events generated by Kerberos authentication ticket-granting ticket (TGT) requests.

Account management events

The settings in this category can be used to monitor changes to user and computer accounts and groups.

Setting	Description
User Account Management	Audit changes to user accounts.
Computer Account Management	Audit events generated by changes to computer accounts, such as when a computer account is created, changed, or deleted.
Security Group Management	Audit events generated by changes to security groups.
Distribution Group Management	Audit events generated by changes to distribution groups. **Note** Events in this subcategory are logged only on domain controllers.
Application Group Management	Audit events generated by changes to application groups.
Other Account Management Events	Audit events generated by other user account changes that are not covered in this category.

Detailed tracking events

Detailed tracking events can be used to monitor the activities of individual applications to understand how a computer is being used and the activities of users on that computer.

Setting	Description
Process Creation	Audit events generated when a process is created or starts. The name of the application or user that created the process is also audited.
Process Termination	Audit events generated when a process ends.
DPAPI Activity	Audit events generated when encryption or decryption requests are made to the Data Protection application interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information. For more information about DPAPI, see Windows Data Protection.
RPC Events	Audit inbound remote procedure call (RPC) connections.

DS access events

DS access events provide a low-level audit trail of attempts to access and modify objects in Active Directory® Domain Services (AD DS). These events are logged only on domain controllers.

Setting	Description
Directory Service Access	Audit events generated when an AD DS object is accessed. Only AD DS objects with a matching SACL are logged. Events in this subcategory are similar to the Directory Service Access events available in previous versions of Windows.
Directory Service Changes	Audit events generated by changes to AD DS objects. Events are logged when an object is created, deleted, modified, moved, or undeleted.
Directory Service Replication	Audit replication between two AD DS domain

Setting	Description
	controllers.
Detailed Directory Service Replication	Audit events generated by detailed AD DS replication between domain controllers.

Logon/logoff events

Logon and logoff events allow you to track attempts to log on to a computer interactively or over a network. These events are particularly useful for tracking user activity and identifying potential attacks on network resources.

Setting	Description
Logon	Audit events generated by user account logon attempts on a computer.
Logoff	Audit events generated by closing a logon session. These events occur on the computer that was accessed. For an interactive logon, the security audit event is generated on the computer that the user account logged on to.
Account Lockout	Audit events generated by a failed attempt to log on to an account that is locked out.
IPsec Main Mode	Audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.
IPsec Quick Mode	Audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations.
IPsec Extended Mode	Audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations.
Special Logon	Audit events generated by special logons.
Other Logon/Logoff Events	Audit other events related to logon and logoff that are not included in the Logon/Logoff category.

Setting	Description
Network Policy Server	Audit events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock.

Object access events

Object access events allow you to track attempts to access specific objects or types of objects on a network or computer. To audit a file, directory, registry key, or any other object, you must enable the Object Access category for success and failure events. For example, the File System subcategory needs to be enabled to audit file operations, and the Registry subcategory needs to be enabled to audit registry access.

Proving that this policy is in effect to an external auditor is difficult. There is no easy way to verify that the proper SACLs are set on all inherited objects.

Setting	Description
File System	Audit user attempts to access file system objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Write, Read, or Modify, and the account making the request match the settings in the SACL.
Registry	Audit attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL.
Kernel Object	Audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. **Note** The **Audit: Audit the access of global system objects** policy setting controls the default SACL of kernel objects.
SAM	Audit events generated by attempts to access

Setting	Description
	Security Accounts Manager (SAM) objects.
Certification Services	Audit Active Directory Certificate Services (AD CS) operations.
Application Generated	Audit applications that generate events by using the Windows Auditing application programming interfaces (APIs). Applications designed to use the Windows Auditing API use this subcategory to log auditing events related to their function.
Handle Manipulation	Audit events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events.
File Share	Audit attempts to access a shared folder. However, no security audit events are generated when a folder is created, deleted, or its share permissions are changed.
Detailed File Share	Audit attempts to access files and folders on a shared folder. 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 established between a client and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.
Filtering Platform Packet Drop	Audit packets that are dropped by Windows Filtering Platform (WFP).
Filtering Platform Connection	Audit connections that are allowed or blocked by WFP.
Other Object Access Events	Audit events generated by the management of Task Scheduler jobs or COM+ objects.

Policy change events

Policy change events allow you to track changes to important security policies on a local system or network. Because policies are typically established by administrators to help secure network resources, any changes or attempts to change these policies can be an important aspect of security management for a network.

Setting	Description
Audit Policy Change	Audit changes in security audit policy settings.
Authentication Policy Change	Audit events generated by changes to the authentication policy.
Authorization Policy Change	Audit events generated by changes to the authorization policy.
MPSSVC Rule-Level Policy Change	Audit events generated by changes in policy rules used by Windows Firewall.
Filtering Platform Policy Change	Audit events generated by changes to WFP.
Other Policy Change Events	Audit events generated by other security policy changes that are not audited in the Policy Change category.

Privilege use events

Privileges on a network are granted for users or computers to completed defined tasks. Privilege use events allow you to track the use of certain privileges on one or more computers.

Setting	Description
Sensitive Privilege Use	Audit events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a client computer, or generating security audits.
Non Sensitive Privilege Use	Audit events generated by the use of non-sensitive privileges (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station.
Other Privilege Use Events	Not used.

System events

System events allow you to track high-level changes to a computer that are not included in other categories and that have potential security implications.

Setting	Description
Security State Change	Audit events generated by changes in the security state of the computer.
Security System Extension	Audit events related to security system extensions or services.
System Integrity	Audit events that violate the integrity of the security subsystem.
IPsec Driver	Audit events that are generated by the IPsec filter driver.
Other System Events	Audit any of the following events: • Startup and shutdown of the Windows Firewall. • Security policy processing by the Windows Firewall. • Cryptography key file and migration operations.

Miscellaneous Changes in Windows 7

The following sections of this document discuss additional new and changed features in Windows 7:

- Background Intelligent Transfer Service
- AppLocker
- Windows PowerShell 2.0
- Group Policy
- Windows Update Standalone Agent
- Windows Search, Browse, and Organization

Background Intelligent Transfer Service

Background Intelligent Transfer Service (BITS) 4.0 leverages the BranchCache infrastructure to provide peer-to-peer file transfer functionality. It does not interoperate with the BITS 3.0 peer caching solution that was included with Windows Vista and Windows Server® 2008.

Note

As a result of this change, any enterprise application or service (such as Windows Server Update Services) that uses BITS 3.0 peer caching must download files directly from the originating server rather than retrieve it from a peer computer. To avoid or correct this issue, use a Windows Server 2008 R2 computer that has BranchCache installed.

AppLocker

AppLocker is the next version of the Software Restriction Policies feature, which provides access control for applications. For more information, see **What is AppLocker?**.

Improvements to AppLocker include:

- **AppLocker PowerShell cmdlets**. These cmdlets are used in conjunction with the AppLocker user interface as building blocks to help author, test, maintain, and troubleshoot AppLocker policy. For more information, see **AppLocker PowerShell Cmdlets**.
- **Audit only enforcement mode.** This setting helps you determine which applications are used in an organization and test rules that you create before you deploy them. When the AppLocker policy for a rule collection is set to Audit only, rules for that rule collection are not enforced. Rules can be imported into AppLocker and tested before they are deployed by using the Audit only enforcement mode. For more information, see “Scenario 2: Using Auditing to Track Which Applications Are Used” in the **AppLocker Step-by-Step Guide**.

Windows PowerShell 2.0

Windows PowerShell 2.0 is compatible with Windows PowerShell 1.0; however, existing scripts and applications need to be updated to accommodate the following changes:

- The value of the PowerShellVersion registry entry in HKLM\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine is changed to **2.0**.
- New cmdlets and variables have been added that might conflict with variables and functions in profiles and scripts.
- The **-ieq** operator performs a case insensitive comparison on characters.
- The **Get-Command** cmdlet gets functions by default, in addition to cmdlets.
- Native commands that generate a user interface cannot be piped to the **Out-Host** cmdlet.
- The new **Begin**, **Process**, **End**, and **Dynamic Param** language keywords might conflict with similar words that are used in scripts and functions. Parsing errors may occur if these words are interpreted as language keywords.
- Cmdlet name resolution has changed. Windows PowerShell 1.0 generated a runtime error when two Windows PowerShell snap-ins exported cmdlets with the same name. In Windows PowerShell 2.0, the last cmdlet that is added to the session runs when you type the command name. To run a command that does not run by default, qualify the cmdlet name with the name of the snap-in or module in which it originated.

- A function name followed by **-?** gets the Help topic for the function, if one is included in the function.
- Parameter resolution for Microsoft .NET Framework methods have changed. In Windows PowerShell 1.0, if you called an overloaded .NET method with more than one best-fit syntax, no error was reported. In Windows PowerShell 2.0, an ambiguity error is reported. In addition, in Windows PowerShell 2.0, the algorithm for choosing the best fit method has been revised significantly to minimize the number of ambiguities.
- If you are enumerating a collection in the pipeline, and you try to modify the collection, Windows PowerShell 2.0 throws an exception. For example, the following commands would work in Windows PowerShell 1.0, but they would fail after the first pipeline iteration in Windows PowerShell 2.0:

  ```
  $h = @{Name="Hello"; Value="Test"}

  $h.keys | foreach-object {$h.remove($_)}
  ```

  To avoid this error, create a subexpression for the enumerator by using the **$()** characters as follows:

  ```
  $($h.keys) | foreach-object {$h.remove($_)}
  ```

Group Policy

In Windows 7, Group Policy has been improved in the following ways:

- **New Windows PowerShell cmdlets**. This feature applies to Windows 7 Enterprise, Windows 7 Professional, and Windows 7 Ultimate. Prior to Windows 7, Group Policy management and automation was accomplished through the Group Policy Management Console (GPMC) or with scripts written against the GPMC COM interfaces. Windows 7 introduces a set of 25 new cmdlets, which allow IT administrators to manage and automate Group Policy through Windows PowerShell. With these cmdlets, an IT administrator can backup, restore, report on, and configure (through registry settings) Group Policy objects. This functionality is added when the GPMC is installed.
- **ADMX support for Reg_QWORD & Reg_MultiSZ**. Prior to Windows 7, a registry key that was of type QWORD or MultiSZ could not be configured through Group Policy Administrative Templates (ADMX). The ADMX schema has been updated to support the QWORD and MultiSZ registry types.
- **Improvements to the ADMX editor**. This feature applies to Windows 7 Enterprise, Windows 7 Professional, and Windows 7 Ultimate. Prior to Windows 7, the ADMX editor was displayed as a non-resizable, tabbed dialog box. UI text was often clipped, and Help content was difficult to find. The new ADMX editor is displayed in a resizable window that prevents text clipping. Information about settings, including Help and comments, is easier to find.
- **Improvements to Group Policy Preferences**. This feature applies to Windows 7 Enterprise, Windows 7 Professional, and Windows 7 Ultimate. New features have been added to Group Policy Preferences to allow configuring Internet Explorer 8. There is also new functionality available in Scheduled Tasks and Power Plans for Windows 7. IT pros can use Group Policy

Preferences to centrally configure the Internet Explorer 8, Scheduled Tasks, and Power Plans settings. This functionality is added when GPMC is installed. Additionally, the Group Policy Preference Client-Side Extensions are included in Windows 7, so IT administrators do not need to deploy the extensions through Windows Update or the Download Center.

For more information, see **What's New in Group Policy in Windows 7**.

Windows Update Stand-alone Installer

The Windows Update Stand-alone Installer (Wusa.exe) provides the following improvements in Windows 7:

- **Uninstall support**. Prior to Windows 7, **wusa.exe** included install support only. In Windows 7, **wusa.exe** includes uninstall support so that administrators can uninstall updates from a command line. Users can uninstall an update by providing the path to the .msu file or by providing the package number (from the Microsoft Knowledge Base) of the update to be uninstalled.

  Use the following command to uninstall an update by specifying the full path to the update:

  ```
  wusa.exe /uninstall <Path>
  ```

  Use the following command to uninstall an update by specifying the update package number from the Microsoft Knowledge Base:

  ```
  wusa.exe /uninstall /kb:<KB Number>
  ```

- **Additional command-line parameters**. New parameters are available in Windows 7 to enable logging, extract the contents of an .msu file, and control the restart behavior when an update is installed in quiet mode.

Command-Line Parameter	Windows Vista	Windows 7
/log	Not available. Logging could only be enabled through tracing tools.	New parameter enables logging through the **Wusa.exe** tool.
/extract	Not available. Contents of .msu files could only be extracted by using the **expand.exe** tool.	New parameter enables .msu files to be extracted through the **Wusa.exe** tool.
/quiet	Supports the **/norestart** option only.	Extended to support the **/forcerestart**, **/warnrestart**, and **/promptrestart** options.

- **Extended error information**. The **Wusa.exe** tool provides extended information in error scenarios for better diagnosis.

Error	Error Code in Windows Vista	Error Code in Windows 7
Update is already installed.	1 (S_FALSE)	0x240006 (WU_S_ALREADY_INSTALLED)
Update is not applicable.	1 (S_FALSE)	0x80240017 (WU_E_NOT_APPLICABLE)

Note

An update was released to provide the error codes for Windows 7 on computers that are running Windows Vista. For more information about the update, see article 949545 in the Microsoft Knowledge base (http://go.microsoft.com/fwlink/?LinkId=151807).

Windows Search, Browse, and Organization

Windows 7 introduces many features and enhancements to help IT pros deploy and maintain desktop search, browse, and organization functionality. Key improvements to Windows Search, Browse, and Organization include:

- Closer integration with everyday workflows.
- Improvements in the performance and relevance of the search experience.
- Introduction of aggregation and visualizations to improve organization.
- Introduction of federated search to remote indices.

For more information, see What's New in Windows Search, Browse, and Organization.