

Windows 7 Manageability Overview

Published: February 2009

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Active Directory, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Vista, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

|  |
| --- |
| **Windows 7 Manageability Overview** |
|  |

Windows 7 introduces a number of manageability improvements that can reduce total cost of ownership by helping to increase automation, improve user productivity, and provide flexible administrative control to meet compliance requirements. This paper provides an overview of each of these improvements.

IT professionals are often responsible for repetitive and time-consuming tasks. Windows 7’s comprehensive scripting abilities enhance the productivity of IT professionals by automating those tasks, which reduces errors while improving administrative efficiency:

* Microsoft® Windows PowerShell™ 2.0 enables IT professionals to easily create and run scripts on a local PC or on remote PCs across the network. Complex tasks or repetitive management and troubleshooting tasks are automated.
* Group Policy scripting enables IT professionals to manage Group Policy Objects (GPOs) and registry-based settings in an automated manner, thus improving the efficiency and accuracy of GPO management.

In addition to its powerful scripting capabilities, Windows 7 includes several features that improve user productivity and reduce costs:

* Built-in Windows Troubleshooting Packs enable end-users to solve many common problems on their own, and IT professionals can create custom Troubleshooting Packs, thus extending this capability to internal applications.
* Improvements to the System Restore tool inform users of applications that might be affected when returning Windows to an earlier state.
* The new Problem Steps Recorder enables users to record screenshots, click-by-click, that reproduce a problem so IT can troubleshoot solutions.
* Improvements to the Resource Monitor and Reliability Monitor enable IT professionals to more quickly diagnose performance, compatibility, and resource limitation problems

For IT departments to address their ever-increasing security needs and meet compliance requirements, Windows 7 also supports the following features:

* AppLocker™ enables IT professionals to more flexibly set policy on which applications and scripts users can run or install, providing a more secure and manageable desktop.
* Auditing improvements enable IT professionals to use Group Policy to configure more comprehensive auditing of files and registry access.
* Administrators can require users to encrypt removable storage devices with BitLocker To Go™ via Group Policy.
* Group Policy Preferences define the default configuration, which users can change, and provide centralized management of mapped network drives, scheduled tasks, and other Windows components that are not Group Policy-aware.
* DirectAccess seamlessly connects mobile computers to the internal network, allowing IT professionals to manage them if the user has an Internet connection

Altogether, the improvements introduced by Windows 7 can reduce the time IT professionals spend maintaining and troubleshooting, improve user productivity, and enable IT departments to better meet compliance requirements.

**Increased Automation**

One of the best ways to improve the efficiency of IT professionals is through the use of automation. With automation, tasks that previously required hours of an IT professional’s time can be handled in seconds. By detecting a problem and automatically taking steps to resolve it, a process that an IT professional had previously performed manually can be entirely automated. An added benefit is that automation also reduces the possibility for human error.

Scripting is the most flexible and powerful automation tool for IT professionals, and Windows 7 includes an improved version of the Windows scripting environment: Windows PowerShell 2.0. Unlike traditional programming languages designed for full-time developers, PowerShell is a scripting language designed to be used by systems administrators and it does not require an understanding of complex development languages such as Microsoft Visual Basic®, Visual C++®, or C#.

Because PowerShell can use Windows Management Interface (WMI), scripts can perform almost any management task an IT professional would want to automate. You can call command-line tools from PowerShell, enabling full control over any aspect of the system that supports management. PowerShell can even leverage the full .NET Framework, providing access to thousands of powerful objects.

To develop or run a PowerShell script, it must be installed on the computer. PowerShell 2.0 is available as a download for Windows XP, Windows Server® 2003, and Windows Vista, and it ships with Windows Server 2008. In Windows 7, PowerShell 2.0 is built into the operating system, therefore, IT professionals can create, distribute, and run PowerShell scripts on computers running Windows 7 without having to deploy or service additional software to the PCs across their organization.

Some of the tasks administrators use PowerShell for with Windows 7 include:

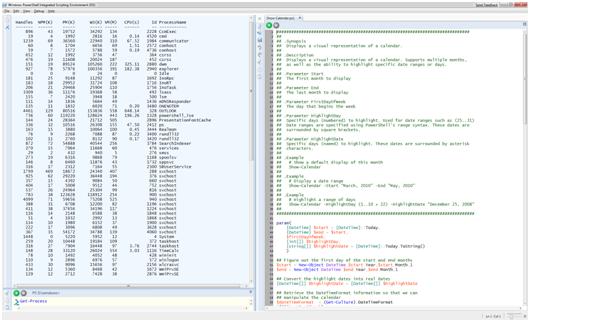
* Remotely creating a System Restore point prior to troubleshooting
* Remotely restoring a computer to a System Restore point to resolve a problem that cannot be easily fixed
* Remotely querying for installed updates
* Editing the registry using transactions, which ensure that a group of changes are implemented
* Remotely examining system stability data from the reliability database

The sections that follow describe key improvements to PowerShell in Windows 7 to help IT professionals automate time-consuming tasks.

**PowerShell Integrated Scripting Environment**

PowerShell scripts are standard text files. With Windows Vista and earlier versions of Windows, the built-in editor was Notepad. While Notepad is perfect for quickly editing text files, and it is sufficient for writing scripts, a more robust editor would enable IT professionals to learn, create, and debug scripts more efficiently.

Windows 7 includes the PowerShell Integrated Scripting Environment (ISE), a graphical PowerShell development environment with debugging capabilities and an interactive console, as shown in Figure 1.



**Figure 1:** The Windows PowerShell ISE

The editor provides several features to simplify script development:

* **Integrated environment.** A one-stop shop for interactive shell tasks, as well as for editing, running, and debugging scripts.
* **Syntax coloring.** Keywords, objects, properties, cmdlets, variables, strings, and other tokens appear in different colors to improve readability and reduce errors.
* **Unicode support.** Unlike the command line, the ISE fully supports Unicode, complex script, and right-to-left languages.
* **Selective invocation.** The user can select any portion of a PowerShell script, run it, and see the results in the Output pane.
* **Multiple sessions.** The user can start up to eight independent sessions (PowerShell tabs) within the ISE. This enables IT professionals to manage multiple servers, each in its own environment, from within the same application.
* **Script Editor.** The script editor includes tab completion, automatic indenting, line numbers, search-and-replace, and go-to line, among other features.
* **Debugging.** The integrated visual script debugger allows the user to set breakpoints, step through the script (step into, step over, and step out), check the call stack, and hover over variables to inspect their value.
* **Object model.** The ISE comes with a complete object model, which allows the user to write PowerShell scripts to manipulate the ISE itself.
* **Customizability.** The ISE is fully customizable, from the size and placement of the panes to the text size and the background colors.

These features make it easier to learn scripting and provide a more robust development environment out-of-the-box.

**PowerShell Cmdlets**

Cmdlets (pronounced command-lets) are one of the most powerful features of PowerShell. A cmdlet is a task-oriented command that is used in the Windows PowerShell environment. For example, PowerShell includes cmdlets that:

* Append text to a file
* Read and write XML files
* Manage services
* Manage files and folders

PowerShell 2.0 supports over 500 new cmdlets to manage client computers and servers, edit the registry and file system, perform WMI calls, and connect the powerful .NET Framework development environment. You can also extend PowerShell by creating custom cmdlets or use community-developed extensions.

**PowerShell Remoting**

In the past, in order to manage a remote computer, you would have to connect to it using Remote Desktop. This makes large-scale (or automated) management difficult. PowerShell 2.0 introduces PowerShell Remoting, which lets you run PowerShell commands for automated or interactive remote management. Today, efficient administrators do the majority of computer management across the network. With Windows 7 and PowerShell 2.0, you can run cmdlets on remote computers using the standard management protocol WS-Management (WS-MAN). This allows you to create scripts that run on one or many remote computers and to take control of a remote PowerShell session to execute commands directly on that computer. Uses include:

* Creating a System Restore point during a help desk call so that you can restore the computer to the current state if necessary
* Changing firewall rules to protect computers from a newly discovered vulnerability

Another option for running PowerShell scripts on remote Windows 7 computers is to use logon, logoff, startup, and shutdown scripts defined in GPOs. Earlier versions of Windows supported specifying only command files for these scripts. PowerShell provides far more flexibility and power than is available in command files

**PowerShell Eventing**

Many applications support immediate notifications of important actions or events. These are commonly exposed as WMI events, or events on a .NET object. Additionally, Windows itself exposes helpful notifications around file activity, services, processes, and more. These events form the foundation of many diagnostic and system management tasks. In Windows 7, PowerShell 2.0 supports this by listening, acting on, and forwarding management and system events. IT professionals can create PowerShell scripts that respond synchronously (immediately after the event is added) or asynchronously (at some later time) to system events. If you register for an event through PowerShell remoting, you can even have those event notifications automatically forwarded to a centralized machine.

With PowerShell, the flexibility is unlimited. For example, you can create a script that performs directory management if files are added to or removed from a certain location. You can create a script that performs a management task only if a specific event is added multiple times, or if different events occur within a specified amount of time. You can even create scripts that respond to events created by your own internal applications to perform management tasks specific to your organization’s needs.

In addition to these capabilities, PowerShell’s eventing supports WMI and .NET Framework events that cover more detailed notifications than those available in the standard event logs. For example, PowerShell can access eventing related to services starting and stopping, processes launching, files changing, and more.

**Automating Management of GPOs**

IT professionals in medium and large organizations often need to create many GPOs that define computer settings ranging from the computer desktop to screen saver timeouts. Microsoft provides the Group Policy Object Editor and the Group Policy Management Console (GPMC) tools to allow administrators to create and update GPOs. However, since there are thousands of possible settings, updating multiple GPOs can be time-consuming, repetitive, and error-prone.

Before Windows 7, automating GPOs was limited to the management of the GPOs themselves. For example, IT professionals could create or link a GPO, but could not change configuration settings within them. Accessing the GPMC application programming interfaces (APIs) also required the skill set of an application developer.

After installing the Windows Server 2008 R2 Remote Server Administration Tools (RSAT) (a download from microsoft.com that includes the GPMC for Windows 7) you can use PowerShell to automate both the management of GPOs and the configuration of registry-based settings (settings available through ADM or ADMX administrative templates). This functionality enables IT professionals to take complete control over GPOs using these cmdlets:

**GPO Cmdlets**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Backup-GPO | Block-GPInheritance | Copy-GPO | Get-GPO | Get-GPOReport |
| Get-GPPermissions | Get-GPPrefRegistryValue | Get-GPRegistryValue | Get-GPResultantSetOfPolicy | Get-GPStarterGPO |
| Import-GPO | New-GPLink | New-GPO | New-GPStarterGPO | Remove-GPLink |
| Remove-GPO | Remove-GPPrefRegistryValue | Remove-GPRegistryValue | Rename-GPO | Restore-GPO |
| Set-GPLink | Set-GPPermissions | Set-GPPrefRegistryValue | Set-GPRegistryValue | Get-GPInheritance |

Perhaps your organization needs to create different GPOs for multiple business units, and each GPO varies by two different settings: the delay before the screensaver starts, and whether a password is required to unlock the screensaver. In an organization with six business units, each with different business requirements, administrators would normally have to manually create the GPOs, and define the settings for each, from within the UI, which can be very time-consuming. With Windows 7 and PowerShell, an administrator can write a PowerShell script that uses an array containing the business unit names and unique GPO settings. The script can then iterate through the array and create each GPO in just seconds.

**Executing PowerShell via Group Policy**

When Group Policy was delivered with Windows 2000, it allowed administrators to execute batch file-based scripts at user logon or logoff, as well as at computer startup and shutdown. This enabled administrators to configure parts of the environment or execute additional programs during those times. Windows 7 introduces support for executing PowerShell scripts as well, giving administrators more comprehensive tools for real-time configuration during these system events.

**Keep Users Productive**

For most people, computers are an integral part of their workday. If computer problems do arise, these people can become unproductive very quickly. Clearly, IT must rapidly resolve problems when they occur; however, the cost of IT involvement in solving problems needs to be minimized as well.

Windows 7 provides many new and improved tools that can help users and IT professionals get back to being productive while minding the bottom line. Users can solve many problems on their own without calling the help desk; when IT help is necessary, it allows IT professionals to rapidly diagnose and solve problems.

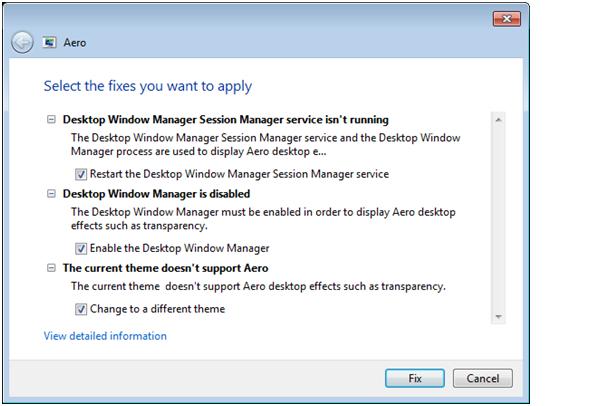
For users, advanced troubleshooting enables them to easily resolve the most common issues, but IT or developers can also develop custom troubleshooting packs to address issues common within their environments. Typically, IT professionals must spend time with users to understand the conditions that cause problems to occur. Windows 7’s new Problem Steps Recorder enables users to record the steps they take in order to reproduce the problem, which is significantly more efficient. Improved versions of System Restore and automatic installation of the Windows RE can reduce the time required to solve system and startup problems. For IT professionals, enhanced versions of Resource Monitor and Reliability Monitor reduce the time required to diagnose problems.

**Advanced and Customized Troubleshooting**

A central goal of any IT organization is to reduce costs while making sure users increase productivity. One way to achieve this goal is to resolve problems quickly, with as little IT intervention as possible. The Windows Troubleshooting Platform, new to Windows 7, is an extensible and powerful platform that IT departments, software developers, and third parties can customize through the use of PowerShell. The Windows Troubleshooting Platform has two key components: Windows Troubleshooting Packs and Windows Troubleshooting Pack Builder.

**Windows Troubleshooting Packs**

Windows Troubleshooting Packs are a collection of PowerShell scripts that attempt to diagnose a problem and, if possible, solve the problem with the user’s approval. Troubleshooting Packs can also perform ongoing maintenance of a specific feature. Windows 7 includes 20 built-in Troubleshooting Packs that address more than 100 root causes of problems. Microsoft designed the Troubleshooting Packs to correlate to the top 10 categories of Microsoft support calls, including Power Efficiency, Application Compatibility, Networking, and Sound. As shown in Figure 2, Troubleshooting Packs can diagnose complex problems, including those caused by multiple conditions, and prompt the user with tips on how to resolve each of them. A list of Windows Troubleshooting Packs that ship with Windows 7 follows the figure.



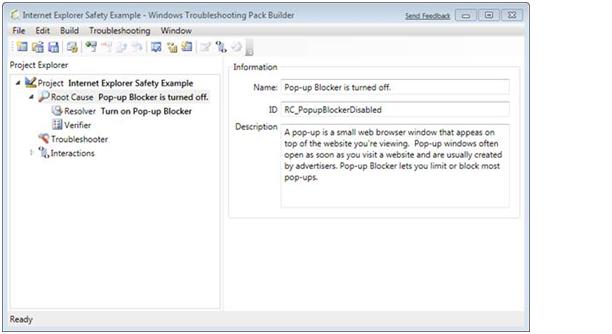
**Figure 2:** A Windows Troubleshooting Pack diagnosing a problem

**Windows 7 Troubleshooting Packs**

|  |  |
| --- | --- |
| Aero | Troubleshoot problems that prevent your computer from displaying Aero animations and effects. |
| Play Sound | Troubleshoot problems that prevent your computer from playing sound. |
| Record Sound | Troubleshoot problems that prevent your computer from recording sound. |
| Printer | Troubleshoot problems that prevent you from using a printer |
| performance | Adjust settings in Windows that can help improve overall speed and performance |
| Maintenance | Clean up unused files and shortcuts and perform other maintenance tasks |
| Power | Adjust power settings to improve battery life and reduce power consumption |
| Homegroup Networking | Troubleshoot problems that prevent you from viewing computer or shared files in a homegroup |
| Hardware and Device | Troubleshoot problems with hardware and devices |
| Browse the Web | Troubleshoot problems that prevent you from browsing the Web with Internet Explorer |
| Web browsing safely | Adjust settings to improve browser safety in Internet Explorer |
| Windows Media Player Library | Troubleshoot problems that prevent music and movies from being shown in the Windows Media Player Library |
| Windows Media Player Setting | Reset Windows Media player back to default settings |
| Play a DVD in Windows Media Player | Troubleshoot problems that prevent playing a DVD in Windows Media Player |
| Connection to a workplace using DirectAccess | Connect to your workplace network over the Internet |
| Connection to a shared folder | Access shared files and folders on other computers |
| Incoming connections to this computer | Allow other computers to connect to your computer |
| Network adapter | Troubleshoot Ethernet, wireless, or other network adapters |
| Internet connections | Connect to the Internet or to a particular Web site |
| Program Compatibility Troubleshooter | Troubleshoot a program that doesn't work in this version of Windows |

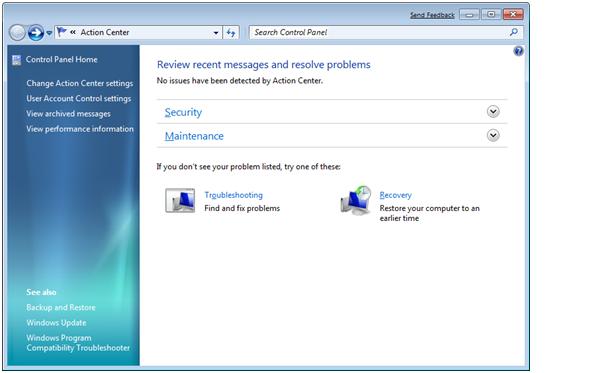
**Windows Troubleshooting Pack Builder**

The Windows Troubleshooting Pack Builder (as shown in Figure 3) is a development kit, included with the Windows Software Development Kit (SDK), that includes a graphical tool for IT professionals and developers building Windows Troubleshooting Packs. The toolkit simplifies adding Troubleshooting Pack metadata and links to the PowerShell Integrated Scripting Environment (discussed earlier in this paper) for authoring detection, resolution, and verification scripts. Because PowerShell is so powerful, you can examine and configure almost any element of the Windows and application environment. You can deploy troubleshooting packages, using Group Policy Preferences (discussed later) to copy them to the local hard drive, or simply store then on a central file server.



**Figure 3:** Windows Troubleshooting Pack Builder, part of the Windows Troubleshooting Toolkit

Troubleshooting can be manually initiated by users from the Help and Support Center or from the Action Center, as shown in Figure 4. Troubleshooting can also be initiated from within applications, allowing organizations to design Windows 7 diagnostic tools as a feature of their line-of-business applications. IT professionals can execute Troubleshooting Packs remotely and use Group Policy settings to limit users to diagnosing, but not fixing, problems.



**Figure 4:** Windows Action Center

IT Professionals can also run Troubleshooting Packs on a scheduled basis to automate maintenance. For example, you can use Troubleshooting Packs to remove temporary files, check a hard disk for errors, or verify the system time.

Microsoft hosts the Windows Online Troubleshooting Service, which provides Windows 7 users with new Troubleshooting Packs, and updates to those that ship with the product, to diagnose newly discovered problems. Administrators can disable this function through Group Policy.

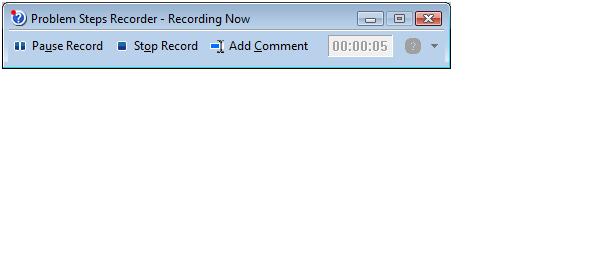
Like applications, Troubleshooting Packs can be signed using a certificate issued by a trusted Certification Authority (CA). Administrators can then use Group Policy settings to run Troubleshooting Packs only from trusted publishers. Troubleshooting Packs can be distributed to local computers, published on an intranet Web site, or stored on a shared folder.

Besides simplifying troubleshooting for end-users, administrators can use Troubleshooting Packs to speed complex diagnostic and testing procedures by running them interactively from a command prompt or silently using an answer file. In such cases, administrators can run Troubleshooting Packs while logged on to the local computer or remotely from across the network.

**Problem Steps Recorder**

Typically, the most complicated aspect of troubleshooting is reproducing the conditions that demonstrate a problem, especially if the affected user is working remotely or communicating by telephone. If IT can’t reproduce a user’s problem, they can’t easily diagnose its source.

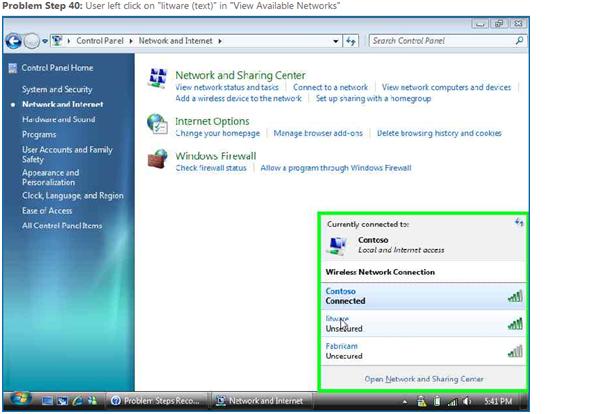
Windows 7’s solution to this impasse is the Problem Steps Recorder, shown in Figure 5. Users simply run the recorder to log the steps taken when an reproducible problem occurs. Users click Start Record, reproduce the problem, enter comments where appropriate, click Stop Record, and then send the recording via e-mail or share to their IT professional.



**Figure 5:** The Problem Steps Recorder

Every time a user clicks or types, a screenshot of the action is recorded, along with accompanying logs and software configuration data. Users’ text comments to describe something happening on the computer that isn’t recorded—for example, poor responsiveness or excessive paging—are also captured.

The Problem Steps Recorder creates a .MHT file (a type of HTML document that includes images in a single file) compressed in a zip archive. The IT professional can open the .MHT file, as shown in Figure 6, to view screenshots and get an exact description of the user’s actions.



**Figure 6:** Recorded Problem Steps

The Problem Steps Recorder can save the IT professional a significant amount of time. Furthermore, it helps overcome language barriers, allowing IT professionals to diagnose problems regardless of language differences

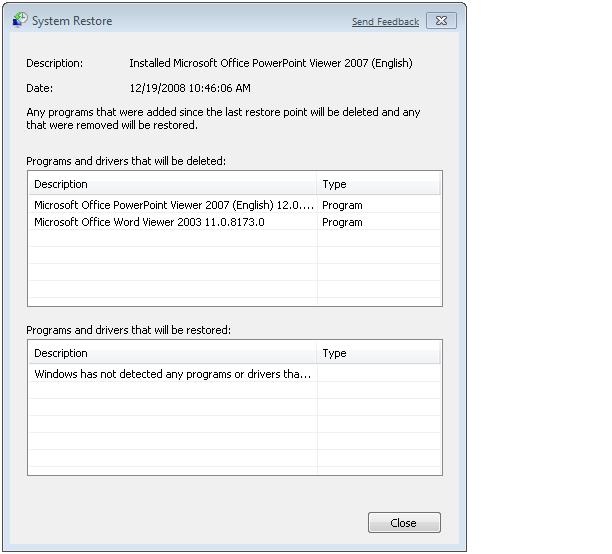
**System Restore**

Occasionally, a user might experience reliability problems. For example, an installation might update a driver with a less-reliable version or an application might overwrite files with incompatible versions. In some cases, uninstalling an update or application will not reverse every change that has been made. Windows Vista included Windows System Restore to store “snapshots” of the system on the local hard drive, either at regular intervals or to a point before the system updates or application/device driver installations were downloaded.

In rolling back all system changes made since the restore point, previous versions of System Restore also reversed system changes unrelated to the problem:

* Applications and drivers that were installed after the System Restore point will be removed
* Applications and drivers removed after the System Restore point will be restored

These earlier versions of Windows made it difficult for users or IT professional to determine which components would be affected by restoring to a System Restore point. Users were predictably frustrated when they discovered that some of their applications were no longer available. Often, these users called the support center for help—once again consuming the IT professional’s time. With Windows 7, the user or IT professional can view a list of software changes (based on applications listed in Add/Remove Programs) before rolling Windows 7 back to an earlier state, as shown in Figure 7. By offering a more complete explanation of a System Restore outcome, such as removing an application that should be preserved, an IT professional can choose a different restore point or make certain to reinstall the application afterward.



**Figure 7:** System Restore description of applications that will be affected by a system restore

In Windows 7, restore points will also be available from system images created by the end users (similar to Complete PC backups in Windows Vista), allowing System Restore to roll-back to a point further back in time than the local System Restore storage would allow. In other words, backups to external hard disks can be used for restore points, too.

Like many other aspects of Windows 7, System Restore enables IT professionals to be more effective and productive through the use of PowerShell. PowerShell can create a System Restore point or restore a computer to a System Restore point, even remotely.

Therefore, while on a support call, IT professionals can connect to a computer from across the network and create a System Restore point before making any changes that might negatively affect the computer’s stability. Scripts that perform troubleshooting or configuration tasks can automatically create a System Restore point to allow changes to be easily restored. Finally, an IT professional could use a PowerShell script to restore a computer to an earlier System Restore point, even across the network.

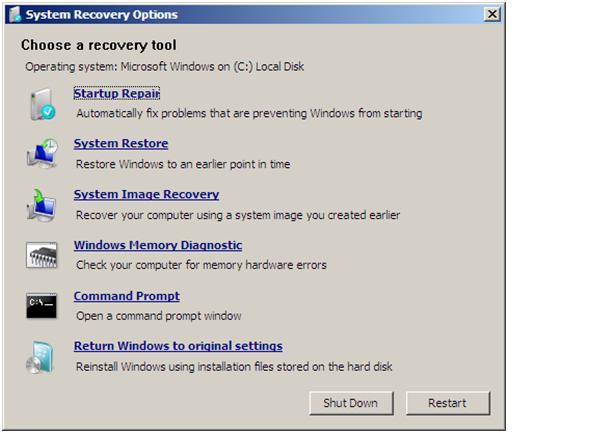
**Windows Recovery Environment**

A computer that fails to start is one of the most challenging troubleshooting scenarios IT professionals face, and most frustrating to users—especially mobile users who are far from the support staff. If users can’t start Windows, they can’t access software troubleshooting tools to diagnose and resolve the problem. More important, they can’t give that important sales presentation or create that budget.

To help users easily resolve startup problems, Windows Vista introduced two tools: the Windows Recovery Environment and the Startup Repair tool. Users or IT professionals can start Windows RE by booting a computer from the Windows Vista DVD. The tools included with Windows RE can often automatically fix startup problems, requiring no troubleshooting from the IT professional.

Although Windows RE can reduce the time required to repair a corrupted instance of Windows Vista, many users either don’t have the Windows Vista DVD available or they didn’t install Windows RE on a separate partition of the PC’s hard drive. Furthermore, Windows Vista did not include a straightforward way to install Windows RE. If remote users call the support center because Windows won’t start on their mobile computer, it would be extremely difficult for IT to resolve the issue. With proper planning, however, IT professionals can install Windows RE onto a partition on a computer’s hard disk, thus making it available without the Windows Vista DVD.

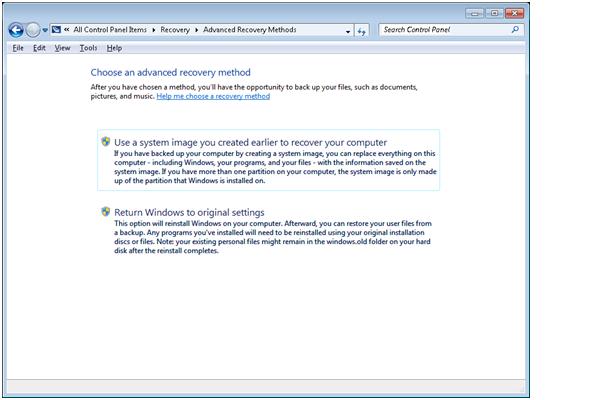
Like Windows Vista, Windows 7 includes Windows RE, including improved versions of the system recovery tools, as shown in Figure 8. The most significant improvement is that Windows RE is automatically installed on the local hard disk as part of the Windows 7 setup, ensuring that the tools are available even if the Windows 7 DVD is not. Now, regardless of how Windows 7 is installed, users can be confident that Windows RE, and tools such as Startup Repair, are always available. Naturally, if the hard disk is not functioning, IT professionals can still start Windows RE from the Windows 7 DVD.



**Figure 8:** System Recovery Options, launched from Windows RE

With Windows 7, if a remote user can’t start Windows, an IT professional can talk the user through the process of starting Windows RE from the computer’s hard disk. In such cases, the system recovery tools can often automatically resolve the problem without requiring any manual troubleshooting. Within minutes, the user will be able to start Windows 7.

These tools also allow users to start Windows RE from the Recovery Control Panel when they want to restore their systems from a system image backup or to factory condition. The Recovery Control Panel guides users through the process of backing up their local user files, restarting the computer to Windows RE, and launching the appropriate recovery application. (See Figure 9.) The Recovery Control Panel is assessable from the Action Center, so IT and support professionals can easily walk remote users through the process of restoring their computers over the phone.

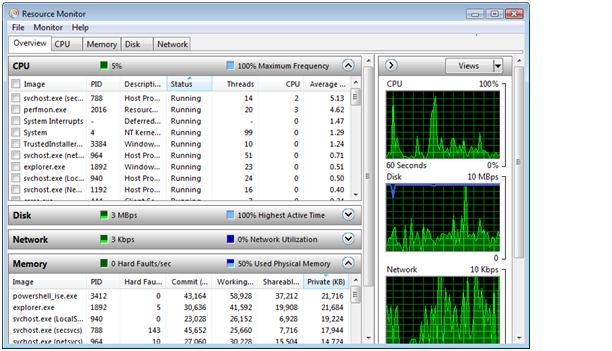


**Figure 9:** The Recovery Control Panel screen, which provides users with system restore options

**Resource Monitor**

To troubleshoot resource issues more thoroughly, IT professionals need deep insight into a computer’s inner workings. The more complex the problem, the more detailed the information to solve it must be. While Task Manager is sufficient to identify which process is using the most processor time, IT professionals often need a more powerful tool to identify which process is generating the most disk or network I/O to solve the problem at hand.

Windows 7 includes an enhanced version of Resource Monitor, which provides this sort of detailed resource utilization information on a process-by-process basis. As shown in Figure 10, this data is displayed in a format that provides rapid access to a great deal of information that can be used to easily drill down into process-specific details.



**Figure 10:** Resource Monitor

Within seconds, you can use Resource Monitor to view:

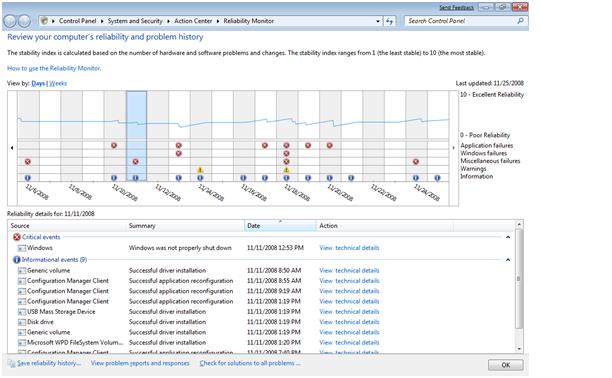
* Which processes are using the most processor time and memory
* Which services are hosted within a SvcHost.exe process
* Which handles (including devices, registry keys, and files) a process is accessing
* Which modules (including DLLs) a process is accessing
* Which processes are reading and writing the most data to the disk
* How much network data each process is sending and receiving
* Which processes are listening for incoming network connections or have network connections open
* How much memory each process is using

In addition, you can end processes and search online for information about a process. With Resource Monitor, IT professionals can quickly identify the source of performance and resource utilization problems, reducing the time required to troubleshoot complex issues.

**Reliability Monitor**

Windows Vista introduced the Reliability Monitor, a tool that provides a timeline of system events that correlate with the overall stability of the PC. These events include the installation or removal of software and device drivers, application failures, and unclean shutdowns. The Reliability Monitor has proved to be valuable to IT professionals because it allows them to quickly trace problems back to the system change that caused them.

With Windows 7, Reliability Monitor is now integrated with Problem Reports And Solutions to better correlate system changes, events, and potential resolutions. In Figure 11, Reliability Monitor is shown providing details about events on a specific day, including a failed application installation and security updates.



**Figure 11:** Reliability Monitor

Windows 7 also enhances Reliability Monitor by exposing the reliability data via the Windows Management Interface. Using WMI, you can gather reliability data remotely and process it using PowerShell scripts and WMI-related cmdlets. Now, IT professionals can leverage WMI to centrally collect or inspect the reliability of Windows 7 computers throughout the network, either proactively or during a support call.

Other management tools, such as Microsoft System Center Operations Manager, can centrally monitor the reliability data from all Windows 7 computers. Alternatively, you can create your own PowerShell scripts to monitor reliability and take appropriate action. By centrally monitoring reliability data, you can identify unreliable computers that are affecting user productivity, even if the users don’t bother to call the support center.

**Flexible Administrative Control**

Whether defined by government regulations, customer service level agreements, or internal security requirements, many organizations have compliance requirements and must centrally define and enforce configuration settings across the organization. Windows 7 includes improved features and new technologies to help IT professionals efficiently meet their compliance requirements:

* AppLocker simplifies controlling which applications users can run by providing flexible publisher rules.
* Improved auditing enables IT professionals to use Group Policy to configure which files and registry values are audited.
* BitLocker improvements provide data encryption enforcement, including on removable storage devices.

Group Policy Preferences also extend the reach of Group Policy to applications and Windows components not normally manageable via Group Policy, such as mapped network drives; local user account passwords and group membership; scheduled tasks; and registry settings. Finally, with the proliferation of remote workers, it is critical for IT professionals to enforce configuration settings on mobile PCs when they’re not directly connected to the corporate network. DirectAccess keeps mobile PCs connected to the internal network, allowing IT professionals to download software updates, apply Group Policy settings, and provide remote management.

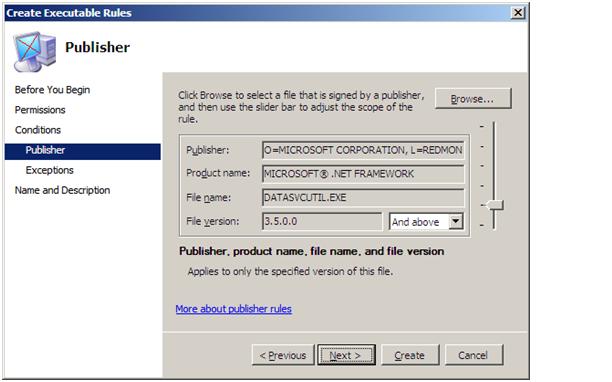
Combined, these improvements give IT professionals the flexibility they need to address most of the configuration management issues that occur today.

**AppLocker**

If users run unauthorized software, their computers can become far less manageable and secure. They also run sluggishly, which reduces user productivity and generates more calls to the support center. And, most important, running this software is a violation of compliance rules.

With AppLocker in Windows 7, administrators have more flexibility than ever to specify exactly which applications and scripts users can run. Administrators can even grant users the right to install specific applications and limit their ability to install others. This enables IT to build and sustain more standardized desktop environments.

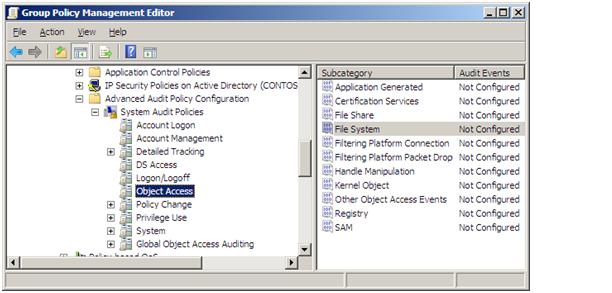
AppLocker includes a number of rules. Its Publisher Rules grant access to an application based on its digital signature, making it possible for a single rule to allow multiple versions of an application to run (even future versions that have not yet been released). As shown in Figure 12, you can create a rule that allows users to run versions 3.5 and later of an application if it is signed with a specific certificate. AppLocker’s Publisher Rules improve productivity by allowing IT to deploy new versions of an application without having to update the rules.



**Figure 12:** An AppLocker rule

**Enhanced Auditing**

Windows 7 provides detailed auditing to give IT professionals insight into who can access information, why a user was denied access, and who has changed an object. In previous versions of Windows, detailed auditing could only be configured using scripts. With Windows 7, you can use Group Policy settings to enable auditing for subcategories, as shown in Figure 13. This auditing is designed to assist organizations in meeting regulatory and business requirements.



**Figure 13:** Configuring auditing using Group Policy

IT professionals can also use Group Policy settings to configure which files, registry keys, and other objects will be audited. With previous versions of Windows, IT professionals had to manually configure resource auditing or write scripts that enabled auditing and run them on every computer.

**Enforced Data Encryption**

Administrators can use Group Policy settings to centrally configure BitLocker and BitLocker To Go for removable storage encryption. Some of the configuration options are:

* Specifying specific requirements for system volumes, non-system volumes, and removable storage
* Requiring strong passwords, a smart card, or domain user credentials to protect removable storage devices
* Setting a minimum PIN length for booting from the system volume
* Specifying the passphrase complexity and length requirements for non-system volumes
* Configuring how non-system volumes can be recovered
* Requiring BitLocker encryption for removable storage devices, as shown in Figure 14, while still allowing unencrypted devices to be opened in read-only mode



**Figure 14:** Requiring BitLocker encryption for a removable drive

**Group Policy Preferences**

IT professionals use Group Policy settings to centrally and consistently configure computers. Because users aren’t allowed to change Group Policy settings, they are perfect for mandating configurations. However, an organization might determine that not all elements of a computer’s configuration should be mandated. Often, IT departments simply want to configure default settings, but allow users to change those settings for their preferences. For example, IT might configure mobile computers to go into standby mode when their lids are closed. However, as a matter of preference, some users would want to change that.

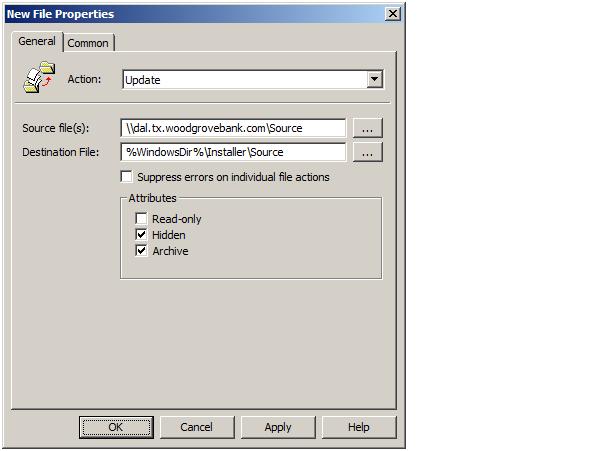
IT professionals typically specify defaults in operating system images prior to deployment. Often, they must configure many different operating system images to provide specific default settings for different groups of users. Alternatively, IT professionals can create scripts that map network drives, create scheduled tasks, or define registry settings. Whichever method is used, managing all these preferences is cumbersome.

With Windows 7, you can use Group Policy Preferences to configure defaults for non-Group Policy-aware Windows components, including:

* Mapped network drives
* Scheduled tasks
* Shortcuts
* Environment variables
* Power options
* Printers
* Regional options
* Folder options
* Open Database Connectivity (ODBC) data sources
* Registry settings
* Start menu settings
* Internet settings
* Local users and groups

Unlike traditional Group Policy settings, Group Policy Preferences assign defaults that users can change. IT can leverage Group Policy Preferences to reduce the number of Windows images required for deployment, because they can define Group Policy Preferences to configure default settings, rather than creating separate Windows images for different configurations.

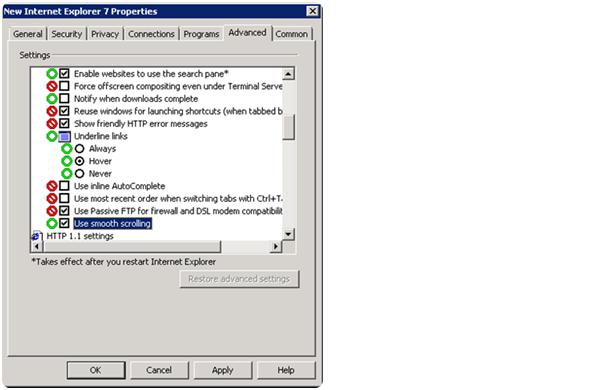
Besides defining preferences, you can create, replace, update, and delete files, groups of files, and folders. The straightforward user interface, shown in Figure 15, allows you to synchronize files from across the network to the destination you specify. For example, you could use this interface to copy a custom dictionary to the %AppData% folder within each user profile. The folder’s interface allows you to regularly delete the contents of a folder, which is useful for cleaning temporary files.



**Figure 15:** Configuring Group Policy settings with a graphical user interface

Group Policy Preferences can be assigned to different groups of users or computers within a GPO without requiring the use of WMI filters. For example, an administrator could configure a preference that applies only to mobile computers.

Many Group Policy Preferences are configurable using the same user interface that users would access to configure an application. For example, you can use Group Policy Preferences to configure Internet Explorer options using a graphical user interface similar to that provided by Internet Explorer itself, as shown in Figure 16. Similarly, you can specify devices using a browser similar to Device Manager.



**Figure 16:** Configuring Group Policy Preferences

There are, however, a number of key differences between Group Policy Preferences and Group Policy settings.

**Comparison of Group Policy Preferences and Group Policy Settings**

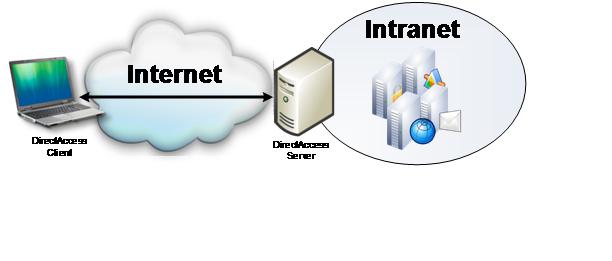
|  |  |  |
| --- | --- | --- |
|  | Group Policy Preferences | Group Policy Settings |
| Enforcement | Preferences are not enforced; users can change settings | Settings are enforced; the user interface to change settings is disabled |
| Flexibility | Easily import or create preferences for registry settings and files | Adding settings requires application support and creating administrative templates; users cannot create settings to manage files or folders |
| Targeting | Individual preferences can be targeted to specific users and groups | Targeting users requires writing WMI queries |
| User interface | Provides a familiar, easy-to-use interface for most preferences | Provides an alternative user interface for most settings |

**DirectAccess**

Mobile computers are a challenge for IT departments because they can only be managed when they are connected to the internal network. Users who work away from the main office or who travel for extended periods of time might not connect to the internal network for weeks or months. As a result, these mobile computers don’t download updated Group Policy settings, critical updates, or anti-malware definitions.

Traditionally, remote users connect to internal network resources with a Virtual Private Network (VPN). However, using a VPN can be cumbersome for users because it requires several steps, and several seconds (or even minutes), for authentication to occur.

Windows 7, together with Windows Server 2008 R2, introduces DirectAccess (see Figure 17), a new solution that enables users to have the same experience working remotely as they would working in the office. Taking advantage of technologies such as IPv6 and IPSec, DirectAccess provides remote computers with automatic, seamless access to the internal network across the Internet without connecting to a Virtual Private Network (VPN), while providing secure and flexible network infrastructure for enterprises.



**Figure 17:** DirectAccess in Windows 7

For example, if a remote user connects to a wireless hotspot at a local coffee shop, DirectAccess will detect that an Internet connection is available and automatically establish a connection to the DirectAccess server on the edge of the internal network. The user will be able to access internal resources that administrators have granted remote access such as internal shares, Web sites, and applications.

The IT Department can manage the mobile computer by updating Group Policy settings and distributing software updates when the Internet connection is established, even before the user is logged on. This flexibility gives IT the opportunity to service remote machines on a regular basis and ensures that mobile users stay up to date with company policies.

User data normally stored within a internal server via Folder Redirection and cached locally via Offline Files And Folders will also benefit from having each file automatically synchronized (backed up) with the server because the network connection is persistent. Users will appreciate DirectAccess because it keeps them automatically connected to internal resources. IT professionals will appreciate DirectAccess because it greatly improves the manageability of mobile computers by connecting them to the internal network, any time the user has an Internet connection. Mobile computers stay connected, managed, and up-to-date.

**Summary**

Windows 7 is designed to reduce cost and increase IT department productivity by increasing automation and providing tools to make troubleshooting and resolving issues quickly. Windows PowerShell 2.0, an enterprise-scale scripting engine, is included with Windows 7 and enables IT professionals to automate almost any aspect of system management. IT professionals can even automate the creation and configuration of Group Policy objects, simplifying policy definition for organizations with a complex Group Policy structure.

Windows 7 also helps users be more productive. In particular, IT professionals can use PowerShell to create customized Windows Troubleshooting Packs that are designed to resolve issues common to their specific environment. Because troubleshooting is extensible, IT professionals and line-of-business application developers can design solutions that users can access to diagnose and even resolve problems with internal applications. And users who solve their own problem using the Windows Troubleshooting Platform don’t need to call the support center.

For those problems that still require a call to the support center, Windows 7 enables IT professionals to quickly diagnose and solve problems. Anyone who has struggled to reproduce the problem a user describes will appreciate the Problem Steps Recorder, which captures click-by-click screenshots showing what user actions led to the problem. Improvements to Resource Monitor and Reliability Monitor will enable IT professionals to quickly identify which processes are causing problems and what system changes might have caused them. Updates to System Restore enable users or IT professionals to see which applications and drivers will be affected before a restore point is activated. Windows Recovery Environment is installed by default so that it can be accessed in an emergency or when a Windows 7 DVD is not available.

Windows 7 also includes significant enhancements to Group Policy, the tool IT departments use to centrally manage computers running Windows. If you strive for a more managed and secure desktop environment that restricts which applications users can run, AppLocker will enable you to create more flexible rules that can apply to any version of an application—even versions that have not yet been released. Group Policy Preferences define default settings for users, providing a simple way to establish an initial configuration that users can update, without requiring you to modify deployment images. You can also use Group Policy to require BitLocker encryption, even for removable storage devices such as USB flash drives. Finally, by enabling DirectAccess, mobile computers can continue to be managed, receiving updated Group Policy settings on a regular basis, syncing data files with the server, and receiving software updates, because they will be automatically connected to your internal network every time the computer connects to the Internet.

These technologies enable Windows 7 to accomplish a simple, universal goal: reduce desktop support costs by making IT professionals more productive.