Table of contents

10 things to consider before rolling out Windows Vista in your organization 2
10 reasons you should upgrade to Vista (and 10 reasons you shouldn't) 4
10 things you should do before installing Windows Vista on a computer 6
10 things you should know about Internet Explorer 7 Security 9
10 things you should know about the Vista firewall 11
10 things you should know about Vista's Windows Meeting Space 13
10 things you should know about User Account Control in Vista 14
10 things you should know about Windows Vista's service hardening 16
10 things you should know about Vista's Network Access Protection (NAP) 17
10 things you should know about Windows Defender in Vista 19

10 things to consider before rolling out Windows Vista in your organization

By Debra Littlejohn Shinder, MCSE, MVP

Despite the delays and uncertainties about exactly when it was going to happen, Vista is now upon us. Organizations are already making upgrade plans, especially those that pride themselves on being early adopters. But there are some things you need to consider before taking the plunge.

1 Is your hardware up to snuff?

Vista is famous—or perhaps, more accurately, infamous—for its hefty hardware requirements. Certainly, minimum system requirements are more demanding than for any previous Windows operating system.

In reality, there are two separate sets of hardware requirements, one for machines that are merely "Vista Capable" and one for those that are "Vista Premium Ready." Whereas the latter requires a 1GHz processor, a GB of RAM and a high end video card, requirements for the former are a bit more easily (and inexpensively) attainable. It's important to remember that, although the eye candy afforded by Aero Glass is very cool, it's probably not really necessary for most business applications.

Before you start making plans to upgrade all of your organization's workstations to Vista, you should check out the exact system requirements on Microsoft's Windows Vista Enterprise Hardware Planning Guidance Web site.

2 Which edition(s) of Vista do you need?

Selecting the right edition of Windows XP was pretty simple. There were four basic varieties: Home Edition, Professional Edition, Tablet PC Edition, and Media Center Edition. If the computer needed to join a Windows domain, the first and last editions were out (MCE 2004 could join a domain, but 2005 could not). Unless you were installing on a Tablet PC, there was no need for TPCE. The logical choice for the vast majority of systems on a business network was XP Pro.

Things get slightly more complicated with Vista. Now there are five editions: Home Basic, Home Premium, Business, Enterprise, and Ultimate. Although you probably won't want to use the Home editions on a company network, you may be less certain whether to choose Business, Enterprise, or Ultimate. Business Edition is roughly comparable to XP Pro, whereas Enterprise Edition includes extra features, such as BitLocker Drive Encryption (an added layer of security for corporate laptops), application compatibility tools, SUA (Subsystem for UNIX-based applications), and advanced multi-language support. Ultimate is a superset with all the features of all editions (including Media Center), which may be more than you need for your business PCs. You'll find more information on the editions here.

3 Understand Vista licensing

With Vista, Microsoft is adding an Enterprise Edition that will be available only to customers with a Software Assurance or Microsoft Enterprise Agreement. For smaller businesses, the Windows Anytime Upgrade license, which allows you to upgrade some editions of Vista to a higher edition, may be of interest (for example, you can upgrade Home Basic to Home Premium, or Business to Ultimate). See Microsoft's Windows Anytime Upgrade FAQs for more details on the plan.

4 What about application compatibility?

When it comes down to it, the applications, not the operating system, matter most in terms of getting the job done. One important consideration in rolling out a new OS is to ensure that your essential programs will run on it without problems.

Vista's built-in compatibility modes will help you install and run apps that were written for previous versions of Windows. Microsoft has created the Application Compatibility Toolkit to help you identify applications that may need enhancements to work with Vista's User Account Control (UAC) feature and to fix those programs. You can also use technologies such as Virtual PC/Virtual Server or Terminal Services as a workaround for incompatible applications.

Nonetheless, it's important to test your mission-critical applications beforehand and ensure that they will work with Vista—or develop a plan to replace them or implement a workaround if they don't. For application compatibility resources, see this overview.

5 Assess the network infrastructure

Although there's no requirement that you do so, upgrading to Vista may provide you with motivation to move to IPv6. Vista includes much better support for the new Internet Protocol. With XP/Server 2003, IPv6 support requires installing a separate protocol, whereas the TCP/IP stack in Vista/Longhorn Server supports dual IP architecture and both IPv4 and IPv6 are enabled by default.

The United States. has been much slower than Asian countries to move to IPv6, but there are many reasons to do so now. A transition to IPv6 not only enhances IP security, it also allows doing away with NAT and makes it easier to incorporate video and audio into applications. For a list of advantages of IPv6, see IPv6 — The evolution of the Internet.

6 Who needs Vista (and who doesn't)?

You may not want or need to upgrade all desktop systems in the your organization to Vista at once. In fact, there's a lot to be said for implementing an OS upgrade in a large company one step at a time. Upgrades shouldn't be done randomly, though. Part of your rollout plan should include assessing which users can benefit most from Vista's new features, are most in need of Vista's security enhancements, or otherwise should take priority in the rollout process.

Clerical personnel who spend most of their computer time in a word processing or spreadsheet program may be perfectly content—and just as productive—continuing to use their current OS for awhile.

7 Are your users prepared?

Such considerations as cost, hardware, and infrastructure are important when you're making the decision to roll out a new OS, but don't forget the people factor. A minority of computer users embrace new technology eagerly and can't wait to be the first on the block to try and master the latest and greatest. But most users, like human beings in general, are resistant to change, even if the change is for the better.

Upgrading to a new operating system always requires a learning period, regardless of how intuitive the software is, and Vista introduces some major interface changes and new ways of doing things that may frustrate your less tech-savvy users. For example, those new to Vista are likely to be confused or annoyed by the dialog boxes that AUC pops up whenever they try to perform a task that requires administrative rights, even if they're logged on as administrators.

It's important to prepare users for the transition through education, training, and policies that don't make it harder on them than necessary. For instance, you can allow those who prefer it to switch back to the classic Windows theme to make the desktop look more familiar.

8 Are support personnel ready?

It's not just end users who must be prepared before the rollout. Your help desk and other tech support personnel are going to be hit with a plethora of questions and requests for assistance. Even if they're well trained and completely versed in the new OS, they need to be prepared for a much large volume of work than usual. You might consider adding more support personnel temporarily during and immediately after the upgrade.

9 Is your data safe?

Sure, if all goes well, the OS upgrade will leave all your precious data intact. But what if all doesn't go well? The most elementary, but surprisingly oft-overlooked, consideration is whether all of your data is properly backed up "just in case." That doesn't just mean having a backup program and a bunch of tapes that you shuffle every week or so. It means actually doing test restorations to ensure that those backups will work if and when you need them.

10 What will it really cost?

When all the other considerations are in, you can start to calculate how much it will cost to do the upgrade. Don't forget that the bottom line cost includes a lot more than the licensing fees. It also includes the cost of any necessary hardware upgrades, application modifications (or moving to new applications or new versions of the old ones), changes to the network infrastructure (if applicable), consultants you hire to help with the rollout, user training (including cost productivity while those users are away from their usual tasks), training of support personnel and IT administrators, and administrative overhead of handling all these preparations, including application compatibility testing, backup testing, and so forth.

Once you have a realistic cost estimate, you can intelligently decide whether the benefits of upgrading are worth it or whether your company is better off using XP (or even Windows 2000) for awhile longer and waiting for the first service pack or beyond before you take the Vista plunge.

10 reasons you should upgrade to Vista (and 10 reasons you shouldn't)

By Josh Hoskins

Windows Vista is coming, and there are plenty of reasons to upgrade. There are also plenty of reasons not to. Although some organizations are actively preparing for Vista, others are planning to stay the course with their current operating systems. Still others are planning to move to an entirely new environment. Whatever your decision, it's always helpful to know what you are getting into or giving up. Here's a look at 10 reasons why you should upgrade to Windows Vista... and 10 reasons why you shouldn't.

Why you should upgrade to Windows Vista

1 Security

One of primary design focuses for Vista was to create the most secure environment possible. Many basic aspects of Windows (such as running as an Administrator) have been changed to help produce this environment. Not only that, Internet Explorer 7 has many new features designed to help protect you while you are online.

2 Enhanced networking

Microsoft has rewritten its TCP/IP network stack for Vista to provide better performance. In addition, Vista has dramatically changed how users interact with the network devices in their PC and on their network. Now users can take advantage of the new built-in tools to help diagnose network problems. This will cut down on help desk calls and in some cases, speed up support. The help desk can use the information provided by the diagnostic tools to help in their troubleshooting.

3 Aero Glass user interface

The Aero Glass interface in Windows Vista is a major step forward for Windows in GUI design. Your Windows desktop has never looked better than it will under a Vista version supporting Aero Glass. Not only do things look better, but the whole layout of the GUI has been changed to make everything easier to find and more intuitive to use.

4 Integrated Sidebar and Search

Most of us have already installed a third-party search application, RSS reader, and sidebar or gadget dock in Windows XP. These features have been integrated into the OS itself and look fabulous under Aero Glass. You'll no longer need to open a browser to see your stocks or check on the weather. They will be constantly displayed (and updated) from the Windows Sidebar. Searching for your documents has never been easier, either, now that the integrated search function in Windows supports the indexing features of many newer search applications.

5 Windows Reliability and Performance Monitor

IT professionals are already familiar with Performance Monitor, but now the power of this utility has been brought to the masses. The new Windows Reliability and Performance Monitor can easily be set by a user to automatically take a baseline performance reading of their new PC. And when performance begins to suffer, this tool will help then diagnose what is causing the problem.

6 500 new GPO objects

Many companies rely on Active Directory and its Group Policy capabilities to enforce standards on their desktops. Windows Vista makes this even better by including more than 500 new Group Policy Objects.

7 BitLocker

As we've seen over the past few years, laptops are one of the biggest security holes for IT departments. The new BitLocker technology in Windows Vista can help mitigate this risk by encrypting data and making the computer unusable to anyone not in possession of the startup key (which can be typed in or stored on a USB key).

8 Continual support

Being the newest OS from Microsoft, Vista will be eligible for support longer than any other Windows OS available. Along with support from Microsoft, there will be support from the Internet at large, as people will be using Windows Vista for quite awhile into the foreseeable future. This offers some peace of mind, knowing that you can get help should you run into any issues.

9 ReadyBoost (USB drive as memory)

Microsoft has a new way to help you boost performance on your OS without requiring you to buy a lot of new expensive hardware. You can now plug in removable memory (USB key, compact flash, SD card, etc.) and assign all or part of it to use ReadyBoost. This means that the memory will be used as a prefetch section between your RAM and hard drive. In testing, this has shown that it can offer a great speed boost to many systems, especially those with limited RAM.

10 DirectX 10

DirectX 10 will be available only on Windows Vista. DirectX is useful for a variety of graphics and video functions, including business applications such as video conferencing. And if you must have the latest and greatest in games, the upgrade to Windows Vista is a no-brainer, as this is the only way you can get it. DirectX 10 also claims to fix the “small batch problem” from previous versions. It has claimed that this could lead to DirectX 10 games that can perform six times better than the same game running in DirectX 9 on Windows XP.

Why you shouldn't upgrade to Windows Vista

1 Stiff hardware requirements

Vista has the harshest hardware requirements of any Microsoft operating system to date. To use all of the features of Windows Vista, you need a 1 GHz processor, 1 GB of RAM, and a DirectX 9-capable video card. Although this will allow you to run everything, you'll get better performance with a faster processor and more RAM. Since the Aero Glass interface requires a DirectX 9-capable GPU, a lot of older desktops and laptops won't be able to use Aero Glass, even if they meet the other requirements.

2 Learning curve

Vista is a different animal from previous Windows operating systems. Many of the tools are the same or similar, but there is still a lot to learn. If your IT department is already stretched thin, taking the time to learn and implement Windows Vista may not be worth it right now.

3 No loss of WinXP support

Vista will be supported longer than XP, but XP still has two years of mainstream support from Microsoft. And a wealth of information on WinXP (and other operating systems) is already available on the internet. If you and your staff are comfortable with XP, there's little reason to upgrade to Vista for continued support at the moment.

4 Application incompatibility

Many popular applications do not work on Vista. Applications like ITunes and Nero have issues running on Vista. In fact, nearly every program involved in ripping or recoding media have issues with Vista. If these major

applications are having compatibility issues, how many more small applications--those you may use everyday--will have problems, too?

5 DRM issues

Peter Gutmann from the UK's *The Register* has called Window Vista's new DRM the "longest suicide note in history." Even though great strides have been made for PCs in the living room as an entertainment device, Vista has put crippling DRM into place when playing next generation (HD-DVD and BluRay) content. When playing this content, the component output and S/PDIF output is disabled, effectively crippling Windows Vista as an entertainment system.

6 Notebook battery drain

Windows Vista requires more hardware power to run--and notebook battery life goes down the more you require of your PC's hardware. Even just running the Aero Glass interface will drain your battery faster, due to the additional GPU processing. Any dedicated road warrior should consider this before upgrading.

7 Not so innovative

You can download many advanced search applications for free. Even Microsoft has released one. Google has a nice sidebar with a built-in RSS reader available for free. Yahoo widgets (formally Konfabulator) allow you to change your desktop into a virtual workspace with all manner of data and tools available at your fingertips. Apple's OS X is by far the leader in modern desktops. Even Aero Glass cannot compare to the smoothness of OS X (which is more than five years old). Sun's Project Looking Glass can provide a minimal 3d desktop for XP for free.

8 Cost

Vista is expensive. There's no way around this. Microsoft has tried to mitigate this by releasing different versions of Vista with different price points. Unfortunately, many of these are feature crippled and cause more confusion than necessary. If you want Vista, expect to pay up to $400 for one of the top versions.

9 A new video card for DirectX 10

DirectX 10 being Vista-only means that many gamers are waiting patiently on the newest OS. Unfortunately, not only will they have to pay for the OS, but they will also have to buy a new video card that supports DirectX 10. Currently, only NVIDIA’s 8800 chipset is DirectX 10 compatible, with the lowest model (the GTS) having a retail price of $399.

10 Slower game performance

Aero Glass is one of the cornerstones of Windows Vista, but it puts a load on your video card that will affect game performance. There are several reports of Microsoft telling developers that current games will run 10 percent to 15 percent slower on Vista than on Windows XP as a result. It remains to be seen whether this performance hit will continue to be an issue on games designed specifically for Vista.

10 things you should do before installing Windows Vista on a computer

By Steven Pittsley

Windows Vista may well be the most comprehensive operating system ever produced by Microsoft, and the eye candy offered by the 3-D Aero Glass graphics are very slick. But enhanced functionality and graphical improvements come at a price--and that price is usually high-end hardware. If you plan to take advantage of all that Windows Vista offers, that's definitely true. The minimum requirements to run Microsoft’s latest flagship will be much steeper than any previous operating system.

Microsoft has created two distinct hardware classifications for PC manufacturers to use for their new systems. A PC can be either Vista Capable or Premium Ready. The standard Vista Capable machines have more scaled down hardware requirements than the Premium Ready machines. Other than being cheaper and a bit slower than their beefy Premium Ready siblings, the biggest difference between the two systems is that Vista Capable machines can't use the exciting new Aero Glass graphics.

Here are 10 factors to address as you prepare your existing computers to run Windows Vista. Many of the hardware requirements are surprisingly easy to meet, despite the demands of the operating system. The biggest hurdle to run Windows Vista will be the graphics card requirement, although this requirement is less stringent if

you don't plan to use the new Aero Glass graphics. In general, a majority of existing PCs will be fully capable of running Windows Vista with standard 2-D graphics. It may not be as pleasing to the eye, but it's likely to be pleasing to your pocket book.

1 Analyze your machine for upgrade readiness

Before doing anything else, you should download and run the Windows Upgrade Advisor utility. This software will examine your computer and provide you with a summary of what versions of Windows Vista the computer is capable of running. Note that the Upgrade Advisor only indicates whether or not the PC will run Windows Vista. It does not indicate which requirements the PC doesn't meet.

2 Check the CPU

The CPU requirements for Windows Vista are not earth shattering by any means. To be considered Vista Capable, the computer must have a CPU of at least 800 MHz. Those that are Premium Ready require a processor of at least 1 GHz. Most computers that have been sold in recent years will meet this requirement with ease.

3 Make sure you have enough memory

Memory is another fairly easy-to-meet hardware requirement for Windows Vista. To be considered Vista Capable, the PC must have at least 512 MB of RAM. Premium Ready machines must have a minimum of 1 GB of system RAM. Most modern PCs will either meet this requirement or be capable of a relatively inexpensive upgrade.

4 Evaluate your graphics adapter

Those of you looking forward to the new 3-D Aero Glass graphics will need to make sure that your graphics adapter is DirectX 9 capable. WDDM (a Windows display driver model for writing drivers) compatibility is also recommended. To be considered Premium Ready, the graphics adapter must have a minimum of 128 MB of video RAM. Vista Capable cards require only 64 MB of video RAM. Unless you plan on using the Aero Glass graphics, there is no reason to upgrade your existing video adapter if it's Vista Capable.

5 Verify that you have sufficient hard drive space

With hard drive capacity constantly increasing, available space is usually not a major concern. However, you should still be aware of the minimum space requirements for Windows Vista.

Take a moment to verify that your system has enough free space. To install Windows Vista, the hard drive must be at least 40 GB in size and have a minimum of 15 GB of free space.

6 Make sure you've got a DVD drive

Windows Vista ships on a DVD, so to install the new operating system, the computer must have a DVD drive. This is another requirement that should be fairly easy to meet, since DVD drives have become commonplace or require only a fairly inexpensive upgrade.

7 Sort out the versions

Determining which version of Windows Vista to install can be a bit more complex than it was with previous versions of Windows. Windows Vista will have five editions:

- **Windows Vista Home Basic**. This version of Vista provides basic operating system functionality. If you don't need advanced features, such as Aero Glass, this is the choice for you. Average home users will choose this version, although stepping up to Windows Vista Home Premium will offer more functionality.
- **Windows Vista Home Premium**. This version is sort of a cross between Windows XP Home and Windows XP Professional. It offers much more functionality than the Vista Home Basic edition and is probably the version that most average to advanced home users will install.
- **Windows Vista Business**. This version is comparable to Windows XP Professional. It offers standard business functionality and will be a staple on the corporate desktop.
- **Windows Vista Enterprise**. The Vista Enterprise version offers advanced functionality such as BitLocker Drive Encryption for laptops, application compatibility tools, and multi-language support.
- **Windows Vista Ultimate**. The Vista Ultimate version combines the best of the home and business editions into one feature-rich operating system. This version also includes the Windows Media Center.

8 Check application compatibility

To make your Windows Vista installation go as smoothly as possible, you should ensure that your existing applications will run under Vista before installing it. You can download and run the Application Compatibility Toolkit to help you identify applications that may not run under Windows Vista.

9 Don't overlook data backups

Backing up your data is one of the most critical steps in upgrading your operating system. Unfortunately, this step is often overlooked in the excitement of installing the latest operating system. In addition to backing up your data, it's best to verify that you have all of the installation media from your existing software and the appropriate licensing information before you start the installation.

10 Remember the notebooks

Notebook computers must meet all of the same hardware specifications as desktop PCs. The one problem with notebooks, however, is that If the graphics card isn't compatible, there is little that you can do to upgrade the system.

10 things you should know about Internet Explorer 7 Security

By Debra Littlejohn Shinder, MCSE, MVP

Some sensationalistic reports of a security flaw immediately followed Internet Explorer 7's final release, but the vulnerability turned out to be in Outlook Express rather than IE. In fact, Microsoft has put a great deal of effort into making IE 7 more secure. Here are some of the new IE 7 security features and what they can do for you.

1 Default protection from potentially dangerous Active X controls

Active X controls that haven't been checked out and verified as safe no longer run automatically by default; instead they're automatically disabled by the Active X opt-in feature.

2 Per-zone control of Active X opt in

You can disable Active X opt-in on a per-zone basis. It's enabled by default on the Internet and Restricted Sites zones for better security and disabled on the Intranet and Trusted Sites zones.

3 Site and zone locking for Active X controls

Developers can now make their Active X controls more secure by restricting a control to run only on a particular site (site locking) or only in a specific security zone (zone locking).

4 Protection against phishing

IE 7 introduces the Phishing Filter, which helps protect users from being fooled into entering personal information or passwords that can be collected and used for identity theft. The Phishing Filter automatically checks the Web sites you visit against a list of known phishing sites and issues a warning if the site has been identified as a phishing site. If you prefer not to have sites checked automatically, you can check specific sites when you suspect they might be phishing sites.

5 Cross-domain security

A attack tactic called cross-domain scripting is prevented by new IE 7 security mechanisms that force scripts to run in the their original security context even if they're redirected to a different security domain.

6 Locked down security zones

Security zones in IE 7 are locked down tighter than before, with higher default security settings, disabling of the Intranet zone on non-domain computers, and an interface that makes it harder to select low or medium low security.

7 Better SSL/TLS notification and digital certificate info

Users of IE 7 can more easily determine whether a Web site is secured by SSL/TLS and get information on the digital certificates issued to the site. Sites with high assurance certificates cause the address bar to turn green.

8 Privacy protection features

Three new registry keys, called Feature Control keys, prevent HTML from getting a user's personal information. In addition, you can easily clear out information you've entered in Web pages, as well as the browser cache (Temporary Internet Files), history, cookies and other personal info, with a single click.

9 Address bars

All browser windows in IE7 contain address bars, so it's harder for a malicious site to conceal its identity by hiding the URL of the site.

10 International character alert

IE 7 supports international characters, but to prevent spoofing that exploits the similarity of characters in different languages, the browser warns you that the characters are in another language when international character sets are used.

10 things you should know about the Vista firewall

By Debra Littlejohn Shinder, MCSE, MVP

Microsoft has made significant changes to the Windows Firewall in Vista that enhance security and make it more configurable and customizable for advanced users, while retaining the simplicity required by novices. Here are some key aspects of the changes.

1 Two interfaces to meet different needs

The Vista firewall has two separate graphical configuration interfaces: a basic configuration interface accessible through the Security Center and Control Panel and an advanced configuration interface accessible as a snap-in when you create a custom MMC. This prevents novice users from inadvertently making changes that could disrupt their connectivity or put them at risk, while providing a way for advanced users to customize firewall settings more granularly and control outbound as well as inbound traffic. You can also use commands in the netsh advfirewall context to configure the Vista firewall from the command line or create scripts to automatically configure the firewall on a group of machines. You can also control the Vista firewall settings through Group Policy.

2 Basic configuration options

With the basic configuration interface, you can turn the firewall on or off or set it to block all programs with no exceptions, and you can create exceptions (programs, services, or ports that you specifically unblock) and specify the scope of each exception (whether it applies to traffic from all computers, including those on the Internet, only computers on your local network/subnet, or only computers that you identify by IP address or subnet. Here you can also specify which connections you want the firewall to protect, and configure security logging and ICMP settings.

3 Secure by default

The Windows Firewall in Vista defaults to a secure configuration, while still supporting best usability. By default, most inbound connections are blocked and outbound connections are allowed. The Vista firewall works in conjunctions with Vista's new Windows Service Hardening feature, so that if the firewall detects behavior that is prohibited by the Windows Service Hardening network rules, the firewall will block that behavior. The firewall also fully supports a pure IPv6 network environment.

4 ICMP message blocking

By default, incoming ICMP echo requests are allowed through the firewall, and all other ICMP messages are blocked. This is because the Ping tool is routinely used to send echo request messages for troubleshooting purposes. However, hackers can also send echo request messages to locate target hosts. You can block echo request messages (or unblock other ICMP messages if they're needed for diagnostic purposes) through the Advanced tab on the basic configuration interface.

5 Multiple firewall profiles

The Vista Firewall With Advanced Security MMC snap-in allows you to set up multiple firewall profiles on your computer, so that you can have a different firewall configuration for different situations. This is especially useful for portable computers. For example, you may want a more secure configuration when you're connected to a public wi-fi "hotspot" than when you're connected to your home network. You can create up to three firewall profiles: one for connecting to a Windows domain, one for connecting to a private network, and one for connecting to a public network.

6 IPSec features

With the advanced configuration interface, you can customize IPSec settings to specify the security methods to be used for both integrity and encryption, determine the lifetime for keys in minutes and sessions, and select the desired Diffie-Hellman key exchange algorithm. Data encryption for IPSec connections is not enabled by default, but you can enable it and select which algorithms are to be used are data integrity and encryption. Finally, you can select to authenticate the user, computer, or both via Kerberos, require computer certificates from a CA that you specify, or create custom authentication settings.

7 Security rules

A wizard guides you through the steps of creating security rules to control how and when secure connections are to be created between individual computers or groups of computers. You can restrict connections on such criteria as domain membership or health and exempt specified computers from connection authentication requirements. You can set up rules to require authentication between two specific computers (server-to-server) or use tunnel rules to authenticate connections between gateways. You can also create custom rules if none of the predefined rule types is appropriate.

8 Custom authentication rules

When you make a custom authentication rule, you specify individual computers or groups of computers (by IP address or address range) to be the endpoints of the connection. You can either request or require authentication for inbound connections, outbound connections or both. For example, you can require authentication for inbound connections but only request it for outbound connections. When authentication is requested, the connection will be authenticated if possible, but will still be allowed through unauthenticated if it is not.

9 Inbound and outbound rules

You can create inbound and outbound rules to block or allow connections for specific programs or ports. You can use the preconfigured rules or make your own custom rules. The New Rule Wizard guides you through the steps of creating a rule. You can apply a rule to programs, ports or services, and you can have the rule apply to all programs or to a specific program. You can block all connections for that program, allow all connections, or allow only secure connections and require encryption to protect the confidentiality of the data sent over the connection. You can configure both source and destination IP addresses for both inbound and outbound traffic. Likewise, you can configure rules for both source and destination TCP and UDP ports.

10 AD-based rules

You can create rules to block or allow connections based on Active Directory user, computer, or group accounts, as long as the connection is secured by IPSec with Kerberos v5 (which includes the Active Directory account information). You can also use the Windows Firewall With Advanced Security to enforce Network Access Protection (NAP) policy.

10 things you should know about Vista's Windows Meeting Space

By Debra Littlejohn Shinder, MCSE, MVP

Windows Meeting Space is a new application built into Windows Vista that makes it easy for up to 10 collaborators to share their desktops, applications, files, and presentations and to pass private notes to one another over the network. Here are some highlights of WMS features and functionality.

1 Windows Meeting Space is just for Vista

Windows Meeting Space replaces Microsoft NetMeeting. It's available only to users of the Windows Vista operating system, since it's built on Vista's peer-to-peer networking technology and uses Vista features, such as WS-Discovery.

2 Windows Meeting Space is easy to set up and use

The first time you open the program, it automatically performs tasks required for using WMS, such as configuring the firewall to allow Meeting Space communications and enabling People Near Me and file replication. If no network is detected, it will even create an ad hoc wireless network for WMS communications.

3 Windows Meeting Space contains built-in security mechanisms

You can select to receive invitations only from trusted contacts (those who have provided digital certificates verifying their identities) and require participants to enter a password before being allowed to join a meeting. All Meeting Space communications are encrypted so that only authorized persons can see the shared desktops, applications, and files.

4 You can make your meetings invisible

Windows Meeting Space lets you configure visibility options. If you make a meeting invisible, Vista users near you won't be able to see it in the list of available meetings and will have to be explicitly invited to join.

5 Windows Meeting Space offers multiple options for joining meetings

There are three ways to join a meeting

- Through the list of available meetings displayed in the WMS interface
- Via an e-mailed invitation
- Via an invitation file that's been shared or transferred

6 You can deliver a presentation during a meeting

To run a presentation during a meeting, you can either connect to a network projector or display a presentation on your desktop and share the desktop or the presentation application with other meeting participants.

7 You can distribute handouts to meeting participants

To share handouts, just select the file(s) you want to distribute and they'll be copied to each meeting participant's computer. Any participant can edit the handouts, and changes will be propagated to other participants' copies without changing the original file.

8 Windows Meeting Space requires IPv6

IPv6 is installed and enabled by default in Windows Vista. However, for meetings within the local subnet (People Near Me), you don't need to have a formal IPv6 infrastructure in place.

9 You can share your desktop or an application with meeting participants

When you share your desktop, other meeting participants can see all of the items on it, similar to Remote Assistance. But unlike RA, they won't be able to control your desktop unless you explicitly give them control. You'll be notified in the Meeting Space interface that you're sharing your desktop, and you can see how your shared session looks on other computers. If you don't want other meeting participants to see your entire desktop, you can select a file or application to share instead.

10 Admins have numerous ways to control the use of Windows Meeting Space

Administrators can use Group Policy to restrict or control the use of Windows Meeting Space. Options include disabling WMS entirely, disabling sharing of handouts, and enforcing password length and complexity requirements. You can also set rules for types of files that can be shared via the Attachment Manager or record WMS activities and information in a log file.

10 things you should know about User Account Control in Vista

By Deb Shinder, MCSE, MVP

User Account Control (UAC) is at the heart of Windows Vista's focus on security, but it may also be one of Vista's most misunderstood new features. Love it or hate it, you'll need to learn more about it to balance security and user-friendliness in your Vista deployment. Let's take a look at 10 things you need to know about UAC before you roll out Vista, whether on an individual machine or throughout an organization.

1 UAC cuts the risk of logging on as an administrator

It's a common problem: Users who have administrative accounts tend to log on with those accounts, even if they also have regular user accounts and realize that using a standard user account for routine tasks is a better security practice. It's just more convenient, and human nature puts a high priority on convenience.

With User Account Control, some of the risk of logging on as an admin is ameliorated because Vista performs most tasks with regular user privileges even when someone is logged on as an administrator.

2 The logon process has changed

Although it appears the same to the user--you still enter your account name and password in the same way--the Vista logon process has changed under the hood. Now when you log on with an administrative account, you not only get an access token for that account, but you also get a standard user access token. The standard token is used to launch Explorer.exe, so all child processes will run with that token's privileges unless privileges are elevated by responding to a UAC prompt.

3 It's easier to tell which tasks require admin privileges

Vista makes it easier to know which actions will require elevated privileges. Options in dialog boxes for which you must have administrative privileges are marked with a shield-shaped icon to indicate that if you select that option, you'll need to respond to the UAC prompt (or, if Group Policy is so configured, you may not be able to perform the operation at all when logged on as a standard user).

4 Administrator Approval Mode is the default

By default, Vista runs with standard user privileges, even when you're logged on as an administrator. If a task requires administrative privileges, a dialog box asks for your permission to continue the action. This prevents malware from elevating privileges without your knowledge.

5 You can make it more secure

You can change the behavior of UAC by editing Group Policy (the local security policy or domain policy). You can increase security by requiring that a user enter administrative credentials to elevate privileges, rather than just clicking the Continue button, even when already logged on as an administrator. Users logged on with standard user accounts will, by default, be prompted to enter administrative credentials when they try to perform a task that requires elevated privileges. In a domain environment, the default is to disallow the elevation of privileges. You can change these behaviors by editing Group Policy, too.

6 You can increase security even more

By default, both signed and unsigned executable files will run with elevated privileges when you respond to the prompt. However, in a high security environment, this behavior can be changed by editing Group Policy so that Vista will elevate only executables that are signed and valid. When you enable this policy, Vista will check the executable's digital certificate whenever that application requests elevation of privileges.

7 You can make it less secure (but more convenient)

It's not recommended, but if you're in an environment that you're absolutely certain is free of malware, you can edit Group Policy to allow those logged on as administrators to perform tasks with elevated privileges without being required to respond to the UAC prompt. This essentially negates the extra security provided by UAC when logged on as an administrator and exposes the system to the same security threats that exist when you log on with an admin account in pre-Vista versions of Windows. However, it does do away with the sometimes annoying dialog boxes and makes it more convenient for admins who are, for example, installing a lot of software.

8 You can turn off UAC or the Secure Desktop

When UAC prompts for permission to elevate privileges, the desktop is locked so that it can receive messages only from Windows processes. No other software can interact with the desktop at this time, and it goes dark to indicate this. By editing Group Policy, you can disable the Secure Desktop. The prompt will still pop up but will be displayed on the interactive desktop.

It's also possible (although not recommended) to turn off UAC completely. This is done by disabling the policy to Run All Administrators In Administrator Approval Mode.

9 Legacy applications may need to be marked

Pre-Vista applications that were not written to be aware of UAC may have to be specially configured to work with Vista. If the programs need to perform tasks that require administrative privileges, you need to mark them with a requested execution level to prompt users for approval. This can be done with the Application Compatibility Toolkit, available as a free download from Microsoft. For more details, see TechNet's Windows Application Compatibility page.

10 UAC is not a substitute for other security measures

UAC provides extra protection; for example, it makes it more difficult for malicious software to do harm. However, it's not a substitute for antivirus and anti-spyware programs, and you should still use a good, properly configured firewall. To be effective, security must be multi-layered, and UAC is only one element of a good client security plan.

10 things you should know about Windows Vista's service hardening

By Deb Shinder, MCSE, MVP

Service hardening is one of many new security mechanisms in Windows Vista and the next generation of Windows server, currently known as Longhorn Server. Because it's not always desirable or possible to disable Windows services that provide attackers with an exploitable point of attack, the new operating systems include features that make it more difficult for service exploits to do damage. Here are a few facts you should know about service hardening.

1 SCM manages services

Windows services are programs that are managed by the Service Control Manager (SCM), which maintains a database of installed services and manages each service's state. Usually services start automatically when Windows boots and run continuously, making them always available and thus attractive to attackers.

2 Higher privileges = greater exposure

In previous Windows operating systems, most services ran under the LocalSystem account, which has a high level of privileges. That meant that if the service were compromised, attackers could do major damage because they would have access to almost everything.

3 Vista and Longhorn Server run services with lowest possible privileges

In Vista and Longhorn, many of the services that used to run under LocalSystem now run under the NetworkService or LocalService accounts, which have a lower level of privileges. Services run with the lowest possible privileges. Any privileges that a service doesn't need are removed, which helps reduce the attack surface.

4 Vista protects services by using "isolation" techniques

Isolation techniques includes Session 0 isolation, which prevents user applications from running in Session 0 (the first session created when Windows starts up). Only services and other applications that are not associated with a user session can run there. This protects the services from the actions of other applications.

5 Vista assigns a Security Identifier (SID) to each service

Assigning an SID to each service allows services to be separated from one another and enables the operating system to apply the Windows access control model to restrict services' access to resources in the same way user and group accounts' access can be restricted.

6 In Vista, access control lists (ACLs) can now be applied to services

An ACL is a set of access control entries (ACEs). Every resource on the network has a security descriptor that contains the ACLs assigned to it. Permissions defining who or what can access that resource are stored in the ACL.

7 Vista allows the application of network firewall policies to services

The policy is linked to the service's SID. This allows you to control how the service is allowed to access the network and prevent it from using the network in ways it's not supposed to, such as sending outbound network traffic. The Vista Firewall is integrated with the service hardening feature.

8 Specific services can be restricted so that they can't make edits to the registry, write to system files, and so forth

If a service needs to perform those actions to function properly, it can be restricted so that it can write only to specific areas of the registry or a file system. Services can also be prevented from making changes to configuration settings and performing other actions that can be exploited by an attacker.

9 Each service is pre-assigned a service hardening profile

This profile defines what the service should and shouldn't be allowed to do. Based on this profile, the SCM assigns the services only the privileges they must have. This all happens transparently, with no configuration or administrative overhead required.

10 Service hardening does not prevent attackers from compromising services

The Windows Firewall and other protective layers are designed to prevent that. The purpose of service hardening is to reduce the level of damage that can be done if the service *does* become compromised. It provides inner layer protection in Vista's multilayered security strategy.

10 things you should know about Vista's Network Access Protection (NAP)

By Debra Littlejohn Shinder, MCSE, MVP

Microsoft's Network Access Protection (NAP) is built into the Windows Longhorn Server and Windows Vista client operating systems and expands upon the functionality of the Network Access Quarantine Control feature in Windows Server 2003. NAP allows you to monitor the health status of all computers that attempt to connect to your network—not just remote access clients—and ensure that they're compliant with your health policies. Noncompliant computers can be given access to a restricted network where you can place resources they can use to gain compliance.

Here are 10 basic facts you need to know before deploying NAP on your network.

1 NAP is a supplemental feature

NAP does not take the place of other network security mechanisms, such as firewalls, anti-malware programs, and intrusion detection systems. It does not in any way prevent unauthorized access to your network. Instead, it helps protect your network from attacks and malicious software that can be introduced by authorized users who connect to your network via unpatched, misconfigured, or unprotected computers.

2 NAP can be deployed in two modes: monitoring mode or isolation mode

If you configure a monitoring policy, authorized users are given access to the network even if their computers are found noncompliant, but the noncompliant status is logged so that administrators can instruct the users to bring the computers into compliance. In isolation mode, noncompliant computers are given access only to the restricted network, where they can find resources to gain compliance.

3 You can select compliance criteria for the computers that connect to your network

Compliance criteria include requirements for service packs and security updates, antivirus software, anti-spyware protection, firewalls, and Windows Automatic Updates. The criteria are configured on the System Health Validator (SHV) on the NAP server.

4 The NAP server must run Windows Longhorn Server

The NAP server is a Network Policy Server (NPS). NPS is Longhorn's replacement for Internet Authentication Service (IAS) in Windows Server 2003 and provides authentication and authorization. NAP services include the NAP Administration Server and the NAP Enforcement Server. The System Health Validator (SHV) runs on the server.

5 NAP requires that the client computers have NAP client software installed

The NAP client is built into Windows Vista, and a NAP client for Windows XP is expected to be made available with the release of Windows Longhorn Server. The System Health Agent (SHA) runs on the client. If you have computers on the network running operating systems that don't support NAP, you can exempt them from the health status requirements by creating exceptions, so that those computers can still access the network. If no exceptions are made for them, non-NAP capable computers will have access to the restricted network only.

6 The SHA prepares a Statement of Health (SoH) based on the health status of the client computer

The NAP software submits the SoH to the SHV. The SHV communicates with the Policy Server and determines whether the health status provided in the SoH meets the requirements of your health policy. If it does, the computer is allowed full access to the network. If not (in isolation mode), the computer is given access to the restricted network where it can download the updates or software needed to come into compliance. The computers on the restricted network that contain these resources are called *remediation servers*.

7 You can use health certificates to prove compliance

In this case, you need a Longhorn server running Internet Information Services (IIS) and Certificate Services to act as a CA and issue the health certificates. This server is called the Health Registration Authority (HRA). The NAP client sends the SoH to the HRA, which sends it to the NPS server. The NPS server communicates with the Policy Server to find out if the SoH is valid. If it is, the HRA obtains a health certificate for the client, which can be used to initiate IPSec-based communications.

8 There are four types of NAP enforcement

IPSec enforcement relies on the HRA and X.509 certificates. **802.1x enforcement** relies on an EAPHost NAP enforcement client and is used for clients connecting through an 802.1x access point. (This can be a wireless access point or an Ethernet switch.) Restricted access profiles are placed on noncompliant clients using packet filters or VLAN identifiers to restrict them to the restricted network. **VPN enforcement** relies on VPN servers to enforce the health policy when a computer attempts to make a VPN connection to the network. **DHCP enforcement** relies on the DHCP servers to enforce the health policy when a computer leases or renews its IP address. You can use one, some, or all of the enforcement methods on a given network.

9 Only computers that connect to the network via one of the four enforcement methods will have their access restricted if they're noncompliant

DHCP enforcement is the easiest to deploy and most comprehensive because most computers will need to lease IP addresses (all except those assigned static addresses), but IPSec enforcement is the strongest enforcement method. When a computer's access is restricted, it will still have access to the DNS and DHCP servers, as well as the remediation servers. You can, however, place secondary DNS servers or forwarding servers on the restricted network, rather than primary DNS servers.

10 NAP is different from Network Access Quarantine Control in Windows Server 2003

NAP can be applied to all the systems on the network, not just remote access clients. With NAP, you can also monitor and control the health status of visiting laptops and even on-site desktop computers. It's also easier to deploy because it doesn't require the creation of custom scripts and manual configuration with command-line tools, as does NAQC. In addition, third-party software vendors can use the NAP APIs to create NAP-compatible health status validation and network access limitation components. NAP and NAQC can be used simultaneously, but generally NAP will serve as a replacement for NAQC.

10 things you should know about Windows Defender in Vista

By Debra Littlejohn Shinder, MCSE, MVP

Windows Vista comes with a built-in anti-spyware application called Windows Defender, to help you protect your computer against malicious software designed to gather information about you and your system for the purpose of advertising or even identity theft. Defender is an integral part of Vista's heightened security. Here are 10 things you need to know to use Defender to your best advantage.

1 Windows Defender is only one part of a multilayered security strategy

Defender is designed to detect and remove or quarantine known and suspected spyware programs that may be installed on your computer without your knowledge. It does not prevent all attacks against your computer.

Defender should be used in conjunction with other security mechanisms such as a firewall, antivirus software, and encryption.

2 Defender is enabled on Vista by default

You can turn Defender on and off and configure its properties and behavior through the Windows Defender Control Panel applet. It can also be accessed through the Security Center in Vista. The interface is simple, with a one-click button to scan immediately for spyware and the ability to schedule automatic scans on a daily basis or on a selected day of the week at a time of your choosing.

3 Defender can perform three types of scans

A Quick Scan looks in the locations where spyware is most commonly found. This saves time and catches most spyware. A Full Scan checks every drive and folder on the computer. This is the most thorough option but it can take quite some time, depending on the size of your hard disk(s) and the number of files you have. During the scan, there may be a performance hit on other activities you perform on the computer. A custom scan allows you to select the specific drive(s) or folder(s) you want to scan. If Defender detects spyware during a Custom Scan, it will then perform a Quick Scan to remove or quarantine it.

4 You can specify how you want Defender to perform a scan

You can choose whether Defender should scan files and folders that have been archived. You can select to use heuristics methods to identify software that is likely to be spyware, based on patterns and behavior, in addition to using definition files that identity known spyware. In addition, you can choose whether to create a restore point before removing detected items, so that if a file that's necessary to one of your legitimate programs is removed by mistake, it will be easy to fix the problem. You can also specify files and folders that Defender should skip altogether when performing a scan.

5 Real-time protection alerts you immediately if a suspected spyware program attempts to install itself or run on your computer

Real-time protection is enabled by default, but you can choose whether to use it and you can select which security agents should be turned on to monitor various aspects of the system. A number of security agents are available to monitor such items as startup programs, security-related configuration settings, IE add-ons, IE configuration settings, downloaded files and programs, services and drivers, application registration files, Windows utilities, or any program that's started.

6 Administrators can control how Defender runs on user machines

Admins can allow all users to use Windows Defender to scan the computer, choose actions for Defender to take when suspected spyware is detected. and review Defender's activities. They can also restrict the use of Defender with administrative privileges. By default, everyone is allowed to use Windows Defender.

7 You can view the activities Windows Defender has performed via the History page

On the History page, you'll see a list of programs and activities that includes a description of detected items, advice regarding what to do about each item, and resources such as the file location and registry keys associated with the program. You'll see the alert level, what action was taken on what date, and the current status of the item. You can also review a list of items you've permitted to run via the Allowed Items link. You can see what you've prevented from running, and remove or restore these items, via the Quarantined Items link.

8 Windows Defender classifies possible spyware threats according to four alert levels

Severe means it's a malicious program that can damage your computer. **High** means it's a program that might collect your personal information or change your settings. Software classified as Severe or High alert should be removed immediately. **Medium** pertains to programs that might collect personal information but may also be part of a trusted program. **Low** alert signifies software that might collect information or change settings but that was installed in accordance with a licensing agreement you accepted. You should review programs flagged as Medium or Low alert and decide whether you want to block or remove them. Some programs are not yet classified.

9 You should have Defender check for new definitions on a regular basis

To be effective, anti-spyware software uses definitions files that must be kept up to date because new spyware threats appear on a frequent basis. Best practice is to have Defender automatically check for new definitions through Windows Update before performing a scheduled scan. You can also check for new definitions manually. If you rely on manual updating only, you should check for new definitions at least once per week.

10 Microsoft relies on the SpyNet community of Defender users to help expand the spyware database

You're not required to participate in SpyNet to use Defender, but if you do, Defender will send information to Microsoft about the suspected spyware it detects and the actions you apply to each. You can join the SpyNet community easily via the Tools | Settings options, and you can select either a basic or advanced membership. With an advanced membership, you'll receive an alert when Defender detects software that hasn't been analyzed, and more detailed information is sent to Microsoft about detected software.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for our Windows Vista Report newsletter
- Check out all of TechRepublic's free newsletters
- "Installing Windows Vista: The good, the bad, and the ugly" (TechRepublic download)
- "Vista's Aero Glass: Is it all it's cracked up to be?" (TechRepublic article)
- "Get an in-depth look at Vista firewall's advanced configuration features" (TechRepublic download)
- "Vista's Windows Meeting Space offers enhanced functionality for real-time collaboration" (TechRepublic download)

Version history

Version: 1.0
Published: January 23, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team