Internet Explorer Technical Articles

Technical Articles

Internet Explorer Technical Articles

- Deploying Windows Live Toolbars in the Enterprise
- Solutions for Virtualizing Internet Explorer
- Deploying Pinned Websites
- Internet Explorer 9 Preinstallation Techniques

Deploying Windows Live Toolbars in the Enterprise

Applies To: Internet Explorer

This article contains information about the Windows® Live™ Toolbar. The Toolbar is an end-user application that adds Windows Live™ Search and other useful Web tools, including at-a-glance preview information about a user's Windows Live social network and e-mail, to the Internet Explorer® browser window. The Toolbar includes functionality that enterprise administrators can use to customize the Toolbar and to control which features are available to enterprise end users.

In This Article

Custom Buttons

Installation

Group Policy Settings

Registry Key Locations

Group Policy Registry Values

Windows Live™ Toolbar

This document is intended for Windows system administrators and provides guidance on how to install and configure the Toolbar for end-users. By defining enterprise-wide policies for the Toolbar, you can determine which buttons and features users can access. For example, you can disable the feature that allow search suggestions from Windows Live™ Search history, or enable users to share their favorite web pages with their Windows Live social network. You can configure Group Policy before deploying the Toolbar, or at any subsequent time.

Important
Group Policy features are supported in Windows Live Toolbar version 14.00.8052.1208.

Custom Buttons

The Windows Live™ Toolbar Custom Button Software Developer's Toolkit (SDK) available at this Microsoft Web site provides the ability to create custom buttons using XML. For example, you can create custom buttons that enable shortcut access to a Web site, the ability to search a Web site directly from the Toolbar by using Windows Live™ Search, or the ability to display information in the button's menu or in an HTML window.

For example, you could create a custom button that directs new employees to a new hire orientation Web page, that displays a corporate purchasing web page, or that shows important phone numbers from your intranet. Other buttons could use the Internet to show the local weather and traffic conditions or provide headlines from an external news source.

Installing Windows Live Toolbar

You can run a command-line option to deploy Windows Live Toolbar in an enterprise. The following example installs the Window Live Toolbar portion of the Windows Live Suite: `wlsetup-all.exe/appselect:toolbar/quiet`

Configuring Group Policy Settings

The Toolbar uses Microsoft® Group Policy and the Active Directory directory service to deliver and apply configurations to users and computers. The Toolbar enables you to use a Group Policy administrative template file (.adm) available at this Microsoft Web site to enable, disable, or configure settings and sets the value of the Toolbar keys in each targeted machine's registry. You configure the settings by right-clicking a setting and then clicking **Properties**. Alternatively, you can use other administration tools, such as logon scripts, to directly modify the registry settings of user machines. For the Group Policy to take effect, you need to restart Internet Explorer. The Windows Live Toolbar Elevation Helper process (wltuser.exe) must be stopped and restarted for the Toolbar policy to take effect.

The following table defines the settings that are available in the Toolbar's Group Policy administrative template.

Setting	Description

Don't allow users to install custom buttons	Enabling this policy removes all user-installed custom buttons from the Toolbar and hides the button that accesses the Windows Live Gallery button. End-users are prevented from installing custom buttons. Buttons located in `%Appdata%\Microsoft\Windows Live Toolbar\Custom Buttons` do not appear in the Toolbar and only buttons located in `%programfiles%\Windows Live\Toolbar\Custom Buttons` appear in the user's Toolbar. This provides administrators with a method to deploy buttons. Administrator-deployed buttons cannot be uninstalled but the user may configure, hide, unhide and re-order button settings.
Turn off Windows Live buttons	This policy enables administrators to disable all Windows Live buttons so that the buttons are not visible and the user cannot install additional Toolbar buttons. When this policy is disabled or not configured, the user can **Show** or **Hide** Windows Live buttons in the Toolbar.
Don't allow changes to the search region	Enabling this policy prevents users from changing the default country and region setting used by Windows Live Search.
Don't allow search suggestions from search history	Enabling this policy prevents displaying suggestions based on search history. When this policy is disabled or not configured, then the user may disable the search history feature via the **Options** dialog box.
Don't allow search suggestions from popular Live search queries	Enabling this policy disallows displaying search suggestions from popular searches in the results pane. When this policy is disabled or not configured, the user may disable popular search suggestions from the **Options** dialog box.
Don't allow search filters in custom buttons	Enabling this policy disallows custom button search filters, which can be used to filter Toolbar search results so that only certain types of results are returned. For example, users can enable filters so that only news results are returned by search.
Don't allow users to sign in to Toolbar with Windows Live ID	Enabling this policy disallows Windows Live ID account sign-in and sign-out functionality.
Don't allow users to configure Windows Live Toolbar	Enabling this policy removes the user's ability to configure Toolbar settings using the **Options** dialog box.
Don't allow users to send feedback to Microsoft	This policy allows you to disable the feature that enables users to send feedback to Microsoft.
Don't allow Microsoft to collect information on browser and Toolbar usage	Enabling this policy prevents the Toolbar from returning quality monitoring and search instrumentation data to Microsoft.

Turn off Smart Menus in Windows Live Toolbar	Enabling this policy disables the **Smart Menu** feature which enables users to get additional contextual information about a Web page they're browsing in Internet Explorer.
Turn off Windows Live Toolbar Maps Button	This policy disables the **Maps** button which can be used to automatically map addresses found on a Web page.
Turn off Windows Live Toolbar address detection for Maps button and Smart Menus	This policy disables functionality that automatically detects any postal addresses found on the current web page for use with the **Maps** button or **Smart Menu** feature.
Turn off syncing of Internet Explorer favorites with Windows Live	Enabling this policy prevents the use of the Toolbar's Internet Explorer favorites synchronization feature.

Registry Key Locations

The following list describes approved registry key locations for the Toolbar.

Computer Policy Settings

HKLM\Software\Policies

HKLM\Software\Microsoft Windows\CurrentVersion\Policies\Microsoft\Windows Live\Toolbar

User Policy Settings

HKCU\Software\Policies\Microsoft\Windows Live\Toolbar

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Microsoft\Windows Live\Toolbar

Group Policy Registry Values

The following table describes registry key values for the Toolbar.

Registry Key	Description	Type	Policy Enabled Value
UserCustomButton	Disallow user installed custom buttons	REG_DWORD	1
SearchRegion	Turn off default search country/regions setting	REG_DWORD	1
SuggestUserHistory	Turn off suggestions from user search history	REG_DWORD	1
SuggestPopular	Turn off suggestions from popular searches	REG_DWORD	1
CustomSearchScopes	Turn off custom button search scopes	REG_DWORD	1
LiveSignIn	Turn off Live sign-in	REG_DWORD	1
Options	Disable access to Toolbar options	REG_DWORD	1
FeedbackLink	Disable feedback link	REG_DWORD	1
UsageData	Prevent sending instrumentation data	REG_DWORD	1

SmartMenus	Turn off Smart Menus	REG_DWORD	1
UsageData	Prevent instrumentation collection and reporting	REG_DWORD	1
SyncFavorites	Disable favorites sync	REG_DWORD	1
WindowsLiveButtonsBar	Disable Windows Live buttons	REG_DWORD	1

See Also
Other Resources
Windows Live™ Toolbar Custom Button Software Developer's Toolkit (SDK)
Active Directory Administrative Template for Windows Live Toolbar

Solutions for Virtualizing Internet Explorer

With new features and benefits, the Windows® 7 operating system drives lower total cost of ownership by helping users stay productive anywhere, enhancing security and control, and simplifying computer management across an organization. Windows Internet Explorer® 8, the default browser for Windows 7, provides improved security and new features. These new versions of Windows and Internet Explorer can increase efficiency and enhance an organization's productivity and security.

However, migrating to a new operating system can be a challenge, and it brings with it the need to support older software. For example, your organization may be required by a regulatory agency to use the same software to obtain business data that was originally obtained using an older version of the operating system. You may also rely on an application that was built for previous versions of Internet Explorer, such as Windows Internet Explorer 7 or Microsoft® Internet Explorer 6, and cannot easily run in Internet Explorer 8.

Your organization may not currently have the time or resources needed to rebuild, refit, or upgrade such applications within the timeframe required to roll out a new operating system. You may find that you are already maintaining older hardware that you need to support your older applications—this requires the effort of IT staff and can be very costly.

Microsoft provides solutions that let you run previous versions of Windows (and Internet Explorer) by using virtualization on your current hardware and software. By using these solutions, you can continue to run Internet Explorer 7 or Internet Explorer 6 in a virtual environment; you can then continue to run your older applications seamlessly, while you benefit from the newer technologies in Windows 7 and Internet Explorer 8.

This white paper looks at several Microsoft virtualization options that let you run Internet Explorer 7 and Internet Explorer 6—Microsoft® Enterprise Desktop Virtualization (MED-V), Windows XP Mode, and Terminal Services. This paper details these options, including benefits, costs, limitations, and licensing considerations, and helps you decide which option is best for your organization.

Additionally, this white paper provides a series of appendices with prescriptive guidance and best practices—including step-by-step instructions—for setting up each virtualization solution and for running it securely.

Virtualizing Internet Explorer

Application compatibility is one of the main reasons why organizations may be reluctant to upgrade to the latest version of the Windows operating system. Organizations may rely on an important line-of-business (LOB) application that must run in the operating system, for example, or they may have a critical intranet site that was built to run in Internet Explorer 6. Additionally, they may not have the time or the resources they need to rebuild, refit, or upgrade these applications.

If your organization is considering an upgrade to Windows 7 but is concerned about the expense, time, and IT staff effort needed to maintain your older (or legacy) LOB applications, using a virtualization option might be a an effective solution until you can run your applications natively.

The three Microsoft virtualization options most appropriate for virtualizing Internet Explorer 7 and Internet Explorer 6 are MED-V, Windows XP Mode, and Terminal Services. The following table summarizes these options.

Virtualization Option	Benefits	Limitations	Basic Requirements	Recommendation for Size
MED-V	Most robust option Seamless Web solution with automatic URL redirection for applications that run on only Internet Explorer 6 (no user training necessary) Centrally managed via a MED-V management server Flexible—can have different virtual machines for different users if other applications are required	Older computers might not meet the system requirements to run the virtualized XP instance Does not work on a virtualized operating system	Requires both client and server Required 2 GB of RAM on the host Part of MDOP 2009 volume licensing; a Software Assurance benefit, available for enterprise customers	Recommended for enterprise environments

Windows XP Mode	User can start Internet Explorer directly from desktop or Start menu Windows XP Mode and Windows Virtual PC are free downloads for Windows 7 Professional, Windows 7 Enterprise, or Windows 7 Ultimate	Not as centrally managed as other options Older hardware might not support Windows XP Mode Needs to be installed individually on each computer Requires some user training	Requires only client computer Recommended 2 GB of RAM and 15 GB of hard disk space	Suitable for small to medium-sized implementations
Terminal Services	Easy to configure Centrally managed Some enterprises already have Terminal Services deployed	All resources to run Internet Explorer on server side Clients need network access to the server resources Requires user training Requires purchase of Windows Server® 2003 Client Access Licenses to expand Terminal Services option	Requires both client and server; requires	Suitable for any size organization

Table 1. Virtualization options.

What About Other Virtualization Options?

Because Internet Explorer is integrated into the operating system, application virtualization options are not appropriate for virtualizing Internet Explorer 7 and Internet Explorer 6. (For more information, see the Knowledge Base article Running Multiple Versions of Internet Explorer on Single Operating System Is Unsupported.

It is necessary to virtualize the entire operating system to obtain a previous version of Internet Explorer. By doing so, you prevent system conflicts that can occur if Internet Explorer is treated as an application. To reduce the cost of ownership of those operating systems, you can use Software Restriction Policies in Windows XP and Group Policy Settings in Internet Explorer 6 to lock down the virtualized environment.

The following table provides a comparison of desktop virtualization and compatibility issues. In the table, machine virtualization (or full virtualization) includes Windows Virtual PC, Windows XP Mode, and MED-V. Session virtualization includes Terminal Services.

	Machine virtualization	**Session virtualization**	**Application virtualization**
Description	A virtual machine simulates enough hardware to allow an unmodified guest operating system to run in isolation	Applications and data are accessed on a remote computer over a network	Application is encapsulated from underlying hardware
Runs earlier version of Internet Explorer	Yes	Yes, with earlier (legacy) server	No
Application-to-operating system incompatibilities	Yes	Yes, with earlier server	No
Application-to-application conflicts	No	Yes, using one server per application	Yes

16-bit applications on 64-bit hosts	Yes, with 32-bit virtual machine	Yes, with 32-bit virtual machine	No
Enterprise manageability	Only with MED-V	Yes	Yes

Table 2. Comparison of desktop virtualization options.

Virtualize with MED-V

Benefits	Limitations	Basic Requirements	Recommendation for Size
Most robust option Seamless web solution with automatic URL redirection for applications that run on only Microsoft® Internet Explorer® 6 (no user training necessary) Centrally managed via a MED-V management server Flexible—can have different virtual machines for different users if other applications are required	Older computers might not meet the system requirements to run the virtualized XP instance Does not work on a virtualized operating system	Requires both client and server Required 2 GB of RAM on the host Part of MDOP 2009 volume licensing; a Software Assurance benefit, available for enterprise customers	Recommended for enterprise environments

Microsoft Enterprise Desktop Virtualization (MED-V), a core component of the Microsoft Desktop Optimization Pack (MDOP) for Microsoft Software Assurance, is the most robust and scalable solution for virtualizing Internet Explorer 7 and Internet Explorer 6. It provides a centrally managed solution that is intended for enterprise customers. If you use MED-V for virtualization, you can run Windows® 7 and still run older applications seamlessly, directly from a Windows 7 desktop. Users continue to work as they always have and as they launch their browser, MED-V determines whether to leave the URL in Internet Explorer 8 or whether it should redirect and display it in Internet Explorer 6 or Internet Explorer 7 on the MED-V workspace. The MED-V policy that is created and managed by the administrator determines the who, what, and how of applications from the MED-V workspace. By using MED-V, you retain the productivity benefits of the newest operating system, yet you can use older applications that might be best suited for your work.

You can learn more about MED-V with the MED-V Overview video, the How Do I: Use Microsoft Enterprise Desktop Virtualization (MED-V)? video, and the MED-V Quick Start Guide. For more information about MED-V, see the MED-V home page.

What Is MED-V?

MED-V delivers applications in a virtual machine instance that runs an earlier version of the operating system, such as .

MED-V builds on top of Windows Virtual PC so that you can run two operating systems on one physical device, adding virtual image delivery, provisioning, and centralized management. From the user's perspective, these applications and web sites are accessible from the standard desktop **Start** menu or in their browser and appear side by side with native applications, so there is minimal change to the user experience.

MED-V requires both a server and client computer and deployment considerations should be made for how clients will access the MED-V management server. Clients need to meet the system requirements for running a virtual instance of another operating system. But while these considerations need to be made MED-V remains the most robust and seamless of the virtualization options.

You can learn about MED-V in the SolutionAccelerators Infrastructure Planning and Design documentation.

Benefits of Using MED-V

As previously stated, you can use MED-V to run Internet Explorer 7 or Internet Explorer 6 in a virtual environment with a previous operating system version, seamlessly integrated into the Windows 7 desktop. The following list addresses some of the benefits of using MED-V:

- **MED-V is easy to provision and deploy.** MED-V provides a way to automate the first-time setup of virtual machines at the endpoint, including assignment of a unique computer name, performing initial network setup, and joining the virtual machine to a corporate domain.

  With MED-V, you can customize images in heterogeneous desktop environments, and you can adjust the Virtual PC memory allocation based on available RAM on the host computer.

  Application and website provisioning is based on Active Directory users/groups. You can assign a virtual image and define which applications are available to the user and which web sites should be redirected to Internet Explorer 6 or Internet Explorer 7.

- **MED-V is centrally managed.** You can centrally define usage permissions and virtual machine settings and centrally monitor endpoint clients. There are also helpdesk tools to diagnose and troubleshoot virtual machines.

- **With MED-V, you can maintain a minimal inventory.** While you do have additional operating systems, you are generally not burdened with many extra images to manage. While language packs or Internet Explorer 7 may require more images, many customers find that they need only a single additional image.

  MED-V provides an administrator console for virtual image management and a central image repository for image storage, versioning, and delivery (which can be based on Internet Information Services [IIS] web servers, System Center Configuration Manager, or alternative deployment technologies). Integration with makes it possible to provision virtual images based on group membership or user identity.

- **You can use standard image maintenance.** With MED-V, you can continue using Windows Server® Update Services (WSUS) to deploy the latest Microsoft product updates or System Center Configuration Manager. The MED-V workspace is managed as any other desktop in the enterprise.

For more information, see the Microsoft Enterprise Desktop Virtualization Evaluation Guide. Also, see the Links for Further Information later in this document.

Limitations of MED-V

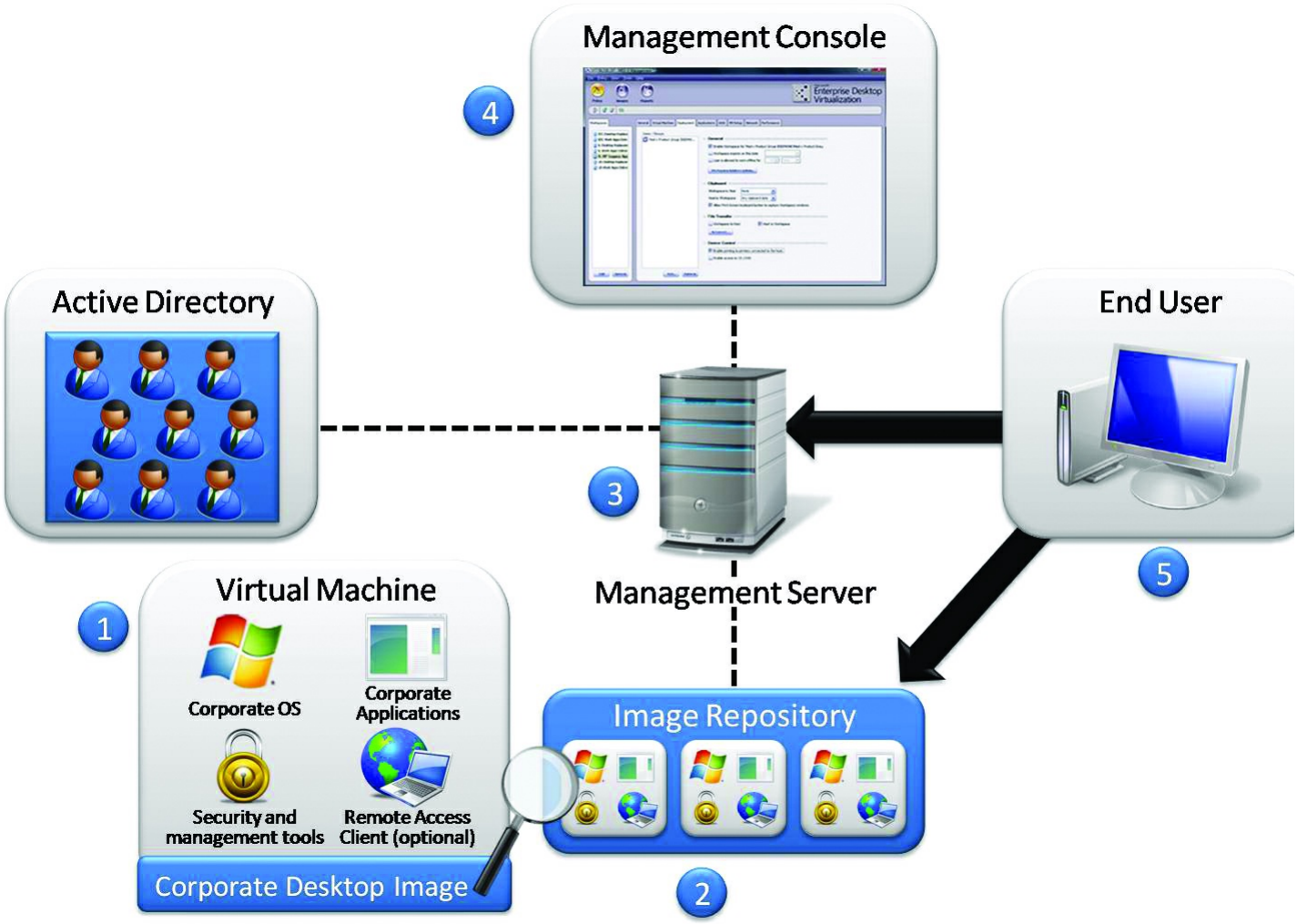
MED-V utilizes client machine resources, and this may be an issue for under-powered hardware. Starting the virtual machine on the client side can take a few minutes; it therefore might be beneficial to set the MED-V preference to leave the virtual machine running for the best user experience.

MED-V requires that you manage an extra operating system, which means extra inventory, patching, antivirus software, and so on. However, MED-V can be managed with the same tools that you are managing the MED-V host with, as an example you can patch the MED-V workspace with Windows Server Update Services (WSUS), as described in Appendix 5: Updating Using Windows Server Update Services.

MED-V does not work on a virtualized operating system through virtualized desktop infrastructure (VDI). VDI clients are already virtual, so they cannot host a virtual instance. This means that if you are using VDI for user desktops, you cannot host MED-V.

MED-V Solution Components

Figure 1 shows the components of a MED-V solution.



The MED-V includes the following components:

- **Administrator-defined virtual machine.** This virtual machine encapsulates a full desktop environment, including an operating system, applications, and optional management and security tools.
- **Image repository.** The image repository stores all virtual images on a standard IIS server and enables virtual images version management, client-authenticated image retrieval, and efficient download (of a new image or updates). The image repository is optional; alternative deployment methods that deliver the image to the MED-V host can be used including distribution with System Center Configuration Manager.
- **Management Server.** The Management Server associates virtual images from the image repository along with administrator usage policies to Active Directory users or groups. The Management Server also aggregates clients' events and stores them in an external database (Microsoft SQL Server®) for monitoring; reporting is an optional feature. Note that additional policy servers may be required for large deployments.
- **Management Console.** The Management Console makes it possible for administrators to control the Management Server and the image repository.
- **User.** Applications installed in the virtual machine are seamlessly available through the standard desktop **Start** menu and are integrated with other applications on the user desktop. Web applications can also be automatically redirected to Internet Explorer 6 or Internet Explorer 7 in the MED-V workspace, providing seamless compatibility.

How Does MED-V Work?

When a user launches MED-V, the MED-V client contacts the MED-V management server. The management server returns the policy to the client. Through the policy, the MED-V client identifies which virtual machine it should use, what applications should be published to the host, and how those should be displayed. Based on the policy, the client looks to see if the virtual machine is available locally (pre-distributed with System Center Configuration Manager). If not, the client attempts to download it from the image server. After the virtual machine is available, it is configured for that user (machine rename, domain joined, and so on) and then the user can begin accessing applications in the MED-V workspace.

Step-by-step guidance for using MED-V to virtualize Internet Explorer 6 and Internet Explorer 7 is provided in Appendix 1: How to Use MED-V.

After MED-V is deployed, the user experience is completely seamless—designated URLs are automatically redirected to the MED-V workspace in Internet Explorer 6 or Internet Explorer 7.

Licensing Considerations

MED-V software is part of MDOP 2009 volume licensing; MED-V is an SA benefit, available for enterprise customers.

MDOP customers can download the software at the Microsoft® Volume Licensing Site (MVLS).

MDOP is available for test and evaluation for Microsoft Developer Network (MSDN®) and TechNet subscribers in accordance with MSDN and TechNet agreements.

System Requirements

Following are the detailed system requirements for MED-V version 1 (V1). For more detailed information, see the MED-V Architecture Overview.

- Management Server
  - Operating system: Windows Server 2008 R2, Windows Server 2008 Standard, or Windows Server 2008 Enterprise (x86 and 64-bit) editions
  - Recommended hardware: Dual processor (2.8 gigahertz [GHz]), 4 GB RAM
  - Active Directory: Management server should be joined to a domain
- Additional Server Components
  - Image repository: web server(s) based on IIS (optional, used if the administrator selects a deployment method other than the Image Server)

    - Reporting database (optional): SP2 Enterprise Edition or Express, Standard, or Enterprise editions
    - Additional policy server for larger deployments
- Client
    - 2 GB RAM
    - Operating system:
        - Windows 7
        - Windows Vista® with Service Pack 1 (SP1) (Enterprise, Home Basic, Home Premium, Business, Ultimate)
        - with SP2 or SP3 (Professional, Home)
    - Microsoft Virtual PC: Microsoft Virtual PC 2007 SP1 with KB958162 (or newer) is required
- Guest Operating System
    - with SP2 or SP3—32-bit
    - Microsoft Windows 2000 SP4—32-bit

Virtualize with Windows XP Mode

Benefits	Limitations	Basic Requirements	Recommendation for Size
User can start Internet Explorer® directly from desktop or Start menu Windows® XP Mode and Windows Virtual PC are free downloads for Windows 7 Professional, Windows 7 Enterprise, or Windows 7 Ultimate	Not as centrally managed as other options Older hardware might not support Windows XP Mode Needs to be installed individually on each computer Requires some user training	Requires only client computer Recommended 2 GB of RAM and 15 GB of hard disk space	Suitable for small to medium-sized implementations

Windows XP Mode is suitable for small- to medium-sized organizations that have limited server infrastructure. Windows XP Mode uses a new version of Virtual PC to provide seamless access to Internet Explorer 7 or Internet Explorer 6, either through a virtual desktop or directly through the Windows 7 desktop.

To learn more about Windows XP Mode, see Windows 7 Features: Windows XP Mode. Also, see Links for Further Information.

What Is Windows XP Mode?
Windows XP Mode is a virtual machine package for Windows Virtual PC that contains a pre-installed, licensed copy of Windows® XP Professional SP3 as its guest operating system. Pre-installed integration components let applications running within the virtualized environment appear in the operating system Start menu as if they were running directly on the host computer.

Be aware that Windows XP Mode applications run in a Terminal Services session in the virtualized instance. The applications are accessed via Remote Desktop Protocol by a client running on the Windows 7 host computer.

For step-by-step guidance for using Windows XP Mode, see Appendix 2: How to Use Windows XP Mode.

Benefits of Using Windows XP Mode
Windows XP Mode is a free option that requires only the Windows XP Mode download and Windows Virtual PC. Both are available as free downloads at Windows XP Mode. Windows XP Mode runs in a separate window on the Windows 7 desktop, much like a program, except it is a fully functional version of the operating system. In Windows XP Mode, you can run Internet Explorer 7 or Internet Explorer 6, access your physical computer's CD/DVD drive, install programs, save files, and perform other tasks as if you were using a computer running .

When you install a program in Windows XP Mode, Internet Explorer 7 or Internet Explorer 6 appear in both the Windows XP Mode list of programs and in the Windows 7 list of programs.

Be aware that Windows Virtual PC includes some new improvements, such as the ability to access the computer's physical hard disk drives (including the host operating system's volumes) through a virtual machine and USB support. You can learn more at Windows 7 Features: Windows XP Mode. Also, see Links for Further Information.

Limitations
Depending on the state of the virtual machine, it may take some time to load Internet Explorer 6. The Windows XP Mode option is not as centrally managed as other options; therefore, managing and patching Windows XP Mode can be more cumbersome.

Licensing Considerations
There are no special licensing requirements for using Windows XP Mode; it is free if you have Windows 7 Premium, Windows 7 Enterprise, or Windows 7 Ultimate. For more information, see Install and use Windows XP Mode in Windows 7.

System Requirements for Windows XP Mode
Following are the system requirements for Windows XP Mode.

- Windows 7 (Premium, Professional, Enterprise, or Ultimate)

- Windows Virtual PC
- Windows XP Mode (a virtual machine supplied by Microsoft®)

Microsoft also recommends a minimum of 2 GB of RAM on the host computer and 15 GB of disk space for each Windows XP Mode instance. However, if the only workload that the Windows XP Mode virtual machine will be providing is Internet Explorer, the virtual machine may require less RAM than the base recommendation. Be aware that if your computer does not meet the requirements, Windows Virtual PC and Windows XP Mode will not work correctly, even though you might be able to download and install them.

To find out which edition of Windows 7 you are running, click the Start button, right-click Computer, and then click Properties. The edition of Windows 7 you are running is displayed under Windows edition near the top of the window. If you are not running Windows 7 Professional, Windows 7 Enterprise, or Windows 7 Ultimate, you might consider using the Windows Anytime Upgrade to upgrade your edition of Windows 7 to Windows 7 Professional or Windows 7 Ultimate. (Windows 7 Enterprise is not available in Windows Anytime Upgrade.)

Be aware that while hardware-assisted virtualization is not required, it can significantly improve performance.

Virtualize with Terminal Services

Benefits	Limitations	Basic Requirements	Recommendation for Size
Easy to configure Centrally managed Some enterprises already have Terminal Services deployed	All resources to run Internet Explorer® on server side Clients need network access to the server resources Requires user training Requires purchase of Windows Server® 2003 Client Access Licenses to expand Terminal Services option	Requires both client and server; requires Windows Server 2003	Suitable for any size organization

Terminal Services (known as Remote Desktop Services in the and Windows Server 2008 R2 operating systems) is a centralized application deployment and remote access solution that uses presentation virtualization, which separates where the application is used from where it is run. Terminal Services is best suited to a medium-sized to large-sized organization with a light server infrastructure, where the client computers have access to the server resources.

You must run Terminal Services in Windows Server 2003, because Internet Explorer 6 is the default version of Internet Explorer included in Windows Server 2003 (includes Internet Explorer 7 and Windows Server 2008 R2 includes Internet Explorer 8).

For step-by-step guidance and best practices for using Terminal Services, see Appendix 3: How to Use Terminal Services.

Benefits of Using Terminal Services

When you use Terminal Services to virtualize Internet Explorer 6, all the activities on the networks and all the development and management issues related to the network are handled by the central computer or server. This central server makes it easy to configure and centrally manage. After Terminal Services are applied to the computer, clients can connect on the local area network (LAN) connection, virtual private network (VPN) connection, or through a wide area network (WAN) connection. The benefits of using Terminal Services include:

- **Rapid, Centralized Deployment.** When you use Terminal Services, all resources necessary to run the instance of Internet Explorer are located on the server side. Centrally deployed applications are easy to patch and upgrade.
- **Low-Bandwidth Access to Data.** Terminal Services reduce the amount of network bandwidth that is required for data access.

Limitations

Using Terminal Services to virtualize Internet Explorer 6 is not as seamless as the other virtualization options. You must connect to a new desktop to access Internet Explorer 6, and you must minimize the remote desktop session to access the local desktop. Be aware, however, that you can run the Remote Desktop Protocol (RDP) session with the optimal resolution for your applications or sites. Additionally, you can configure this RDP session to run only Internet Explorer and no other applications (including the Start menu and desktop), and you do not have to open the RDP session in full screen mode.

Because most Microsoft operating systems ship with versions of Internet Explorer, the Windows Server 2003 operating system must be used to virtualize Internet Explorer 6. This means you cannot take advantage of the Terminal Services RemoteApp™ capabilities in the and Windows Server 2008 R2 operating systems. You must use a traditional Terminal Services RDP session. (To virtualize Internet Explorer 7, you can use or Windows Server 2008 R2 and a TSweb/RemoteApp RDP session, though this document does not cover these technologies.)

Licensing Considerations

Terminal Services is licensed on a per-device or per-user basis and is not available on a per-server or concurrent basis. Each device or user, whether the device or user connects directly to the terminal server or indirectly via another server, requires appropriate licenses to be assigned to it. In this scenario, the required licenses include Terminal Services for Windows Server 2003.

For more information, see Licensing Terminal Sever in Windows Server 2003 R2.

System Requirements for Terminal Services

The system requirements for Terminal Services are the requirements for the Windows Server 2003 operating system. These can be found at System Requirements.

Be aware that Terminal Services can be virtualized. While hardware-assisted virtualization is not required, it can improve performance.

Solutions for Virtualizing Internet Explorer - Summary

Your business may rely on applications that were built for Internet Explorer® 7 or Internet Explorer 6, and the applications cannot easily run in the current version of Internet Explorer 8. If this is the case, but you still want to take advantage of the improved security, new features, and technologies included in Internet Explorer 8 and Windows® 7, virtualization solutions might be the right choice for you.

With Microsoft virtualization solutions such as MED-V and Windows XP Mode, you can continue to use Internet Explorer 7 or Internet Explorer 6 on a virtual machine. You can also use Terminal Services to virtualize Internet Explorer 6. With these options, you can continue running your applications that run only on Internet Explorer 7 or Internet Explorer 6 while continuing to enjoy the new features and technologies that Internet Explorer 8 includes, or you can use operating systems that come with Internet Explorer 8 as the default browser.

Links for Further Information

The following links can provide you with more information about using virtualization solutions.

MED-V Information
For general information about MED-V, see the Microsoft Desktop Optimization Pack (MDOP) tab on the Windows Enterprise site.

For the latest content and expert advice, see Microsoft Desktop Optimization Pack (MDOP) on the Windows Client TechCenter.

The Official MDOP Blog provides information on a variety of topics.

For information about MED-V on TechNet, see Microsoft Enterprise Desktop Virtualization.

For a list of the benefits of MED-V, see Enhancing deployment and management for virtual PCs in enterprise environments.

To create a test environment and explore the basic MED-V product features, see Quick Start Guide (Quick start policy XML file).

To evaluate product deployment and management options, see the Evaluation Guide.

For additional technical resources, refer to the MED-V Team Blog.

For a screencast series, see Mad About MED-V. This screencast series covers four topics: concept and architecture, user experience, configuring workspace policy, and creating the deployment package.

For more about MED-V on TechNet, see MED-V Planning, Deployment, and Operations Guide.

For an overview, watch the MED-V Overview video. Also watch the Microsoft Enterprise Desktop Virtualization (MED-V) Administration Video Series.

To see MED-V in action, watch the video Microsoft Enterprise Desktop Virtualization (MED-V) Overview.

For case studies, see TUV NORD Group: Global Firm Reduces Hardware and IT Costs with Desktop Virtualization and the Microsoft IT Showcase article.

For an analyst's view, see the paper Introduction to the Benefits of Local Desktop Virtualization.

Windows XP Mode Information
For general information, see Windows XP Mode.

To download Windows XP Mode, see Download Windows XP Mode.

For installation information, see Install and Use Windows XP Mode in Windows 7. See also Windows Virtual PC.

For an overview video, see the Windows XP Mode Overview walkthrough on the Windows Client TechCenter.

Terminal Services Information
For general information, see Windows Server 2003 Terminal Services.

For papers, downloads, and news, see Remote Desktop Services on TechNet.

For an overview, see Terminal Services Overview.

For licensing information, see Windows Server 2003 Terminal Server Licensing.

Appendices

This section contains the following appendices:

- Appendix 1: How to Use MED-V
- Appendix 2: How to Use Windows XP Mode
- Appendix 3: How to Use Terminal Services
- Appendix 4: Securing Internet Explorer
- Appendix 5: Updating Using Windows Server Update Services

Appendix 1: How to Use MED-V

The following section provides high level information about how to set up and use MED-V to virtualize Internet Explorer® 7 and Internet Explorer 6 and provides best practices for running and securing your implementation. The configuration described in the sections that follow all assume that an Active Directory domain is already deployed.

How to Deploy and Configure MED-V
Instructions for deploying and configuring MED-V can be found at MED-V Deployment and Configuration on TechNet. Following is a summary of the high-level steps:

1. Install and configure the MED-V Server component.
2. Configure the Image Web Distribution Server.
3. Install MED-V Client and MED-V Management Console.
4. Create Virtual PC Image for MED-V.
5. Create MED-V Workspace.
6. Test, pack, and upload Virtual PC Image.
7. Create and configure MED-V policy.
8. Test Internet Explorer access from client workstation.

Also see the MED-V Quick Start Guide and the Microsoft Enterprise Desktop Virtualization (MED-V) Administration Video Series.

How to Define Internet Explorer 6 or Internet Explorer 7 URL Redirection with MED-V
A core function of MED-V is to redirect a URL from Internet Explorer 8 on a MED-V host to Internet Explorer 6 or Internet Explorer 7 on the guest, allowing companies to move to Windows® 7. This is done by configuring a policy in the MED-V Management Console where it is then applied to MED-V users throughout the company. MED-V policy dictates the who, what, and how of applications – who will receive the policy, what applications or websites they will see or be redirected to, and how those will be seen by the user. In the case of redirecting websites, an administrator defines which sites should be redirected to the guest and what happens when the user types or selects a different site in the guest. The user simply interacts with the browser they are presented with, and the MED-V policy defined by the administrator manages the users' experience.

The following screen shot shows a sample MED-V policy configuration in the MED-V Management Console, which can be used to publish Internet Explorer 6 to the host operating system. A workspace is defined and assigned to users (see the left pane for Workspaces in the following screenshot), and then the administrator can define what applications can be seen on the MED-V host from the MED-V workspace. This is done by selecting the applications tab and identifying the shortcuts that will be created on the MED-V host. In the published applications section, a shortcut to Internet Explorer 6 has been created, which allows the user to seamlessly launch Internet Explorer6 from the MED-V host. Publishing this shortcut is optional for automatic redirection but it demonstrates how any applications from the guest can be published to the host.

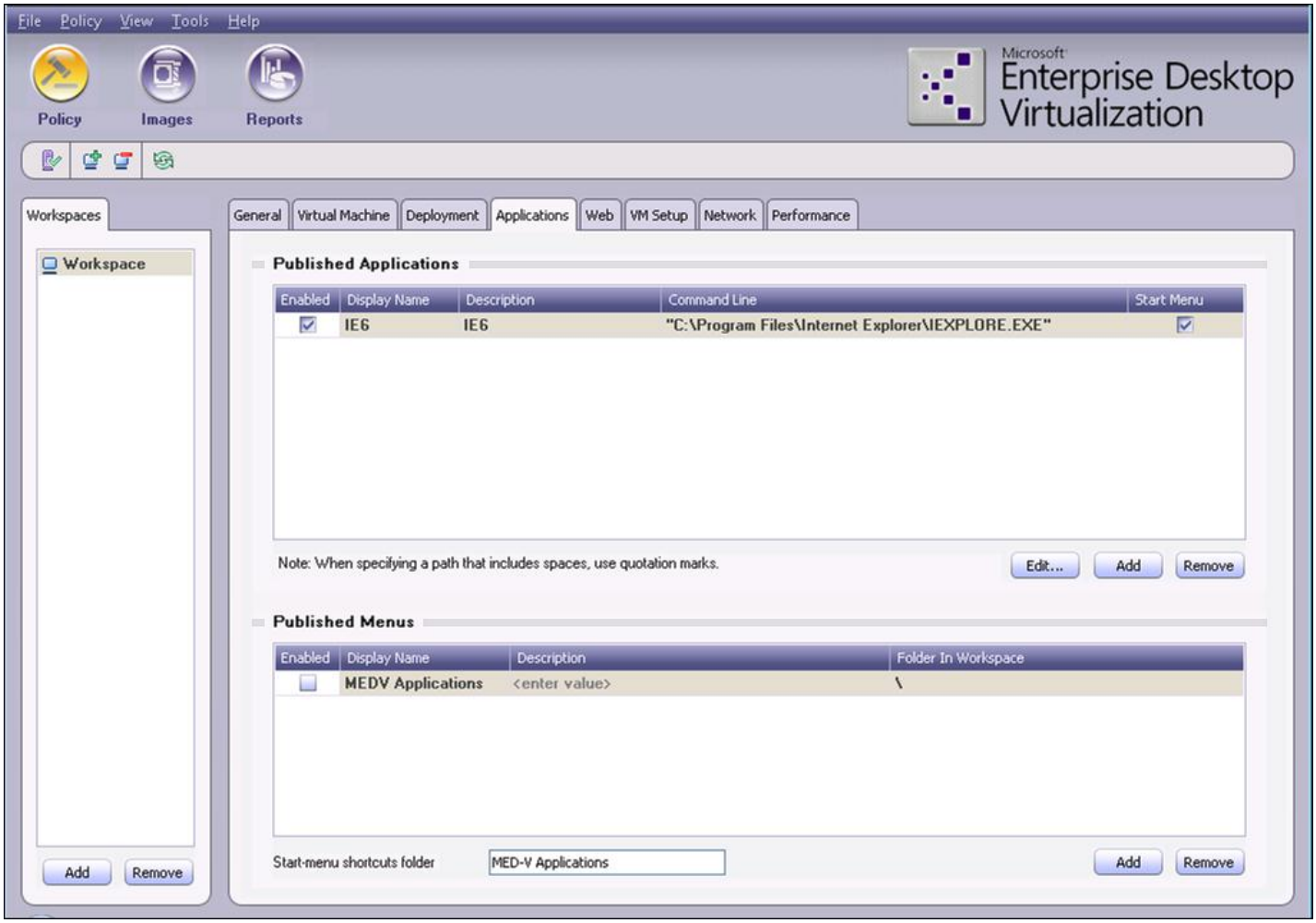


Figure 2. Applications tab.

The following screen shot shows a sample MED-V policy configuration, which redirects all guest browser requests for http://site1 to the MED-V Internet Explorer instance. An administrator can define a domain name or an IP address that will be redirected automatically from the MED-V host to the guest. Other features include the ability to force all other URLs browsed in the guest to be automatically redirected to the MED-V host as well as any “mailto” links. MED-V identifies the correct browser to deliver the content based on the MED-V policy.

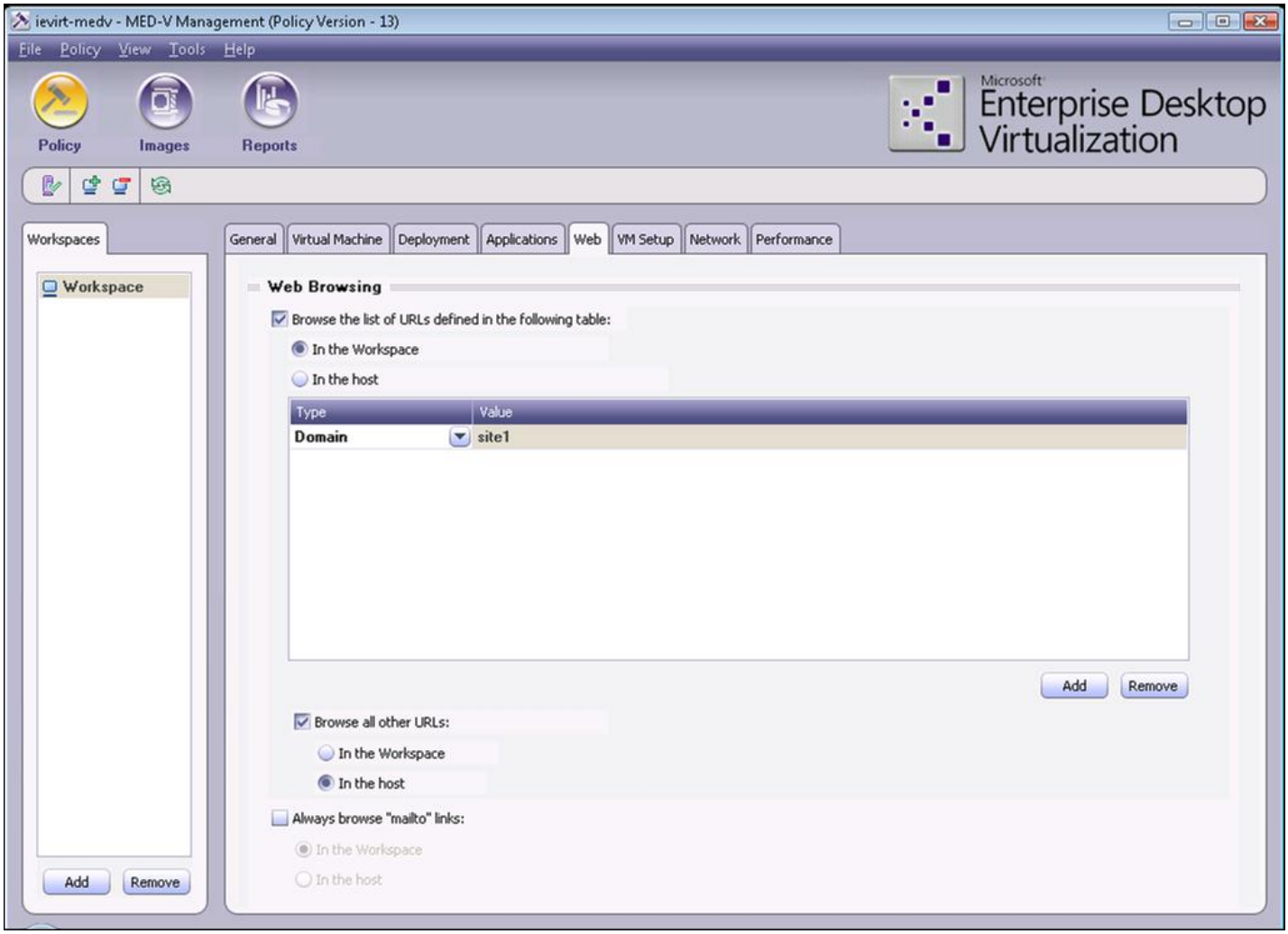


Figure 3. Web tab.

Appendix 2: How to Use Windows XP Mode

The following section provides steps for setting up and using Windows® XP Mode to virtualize Internet Explorer® 6 and Internet Explorer 7 and provides best practices for running and securing your implementation. The configuration described in the sections that follow all assume that an Active Directory domain is already deployed. Be aware that if you follow the instructions in the Configure Windows XP Mode section to add a Windows XP Mode virtual machine to the domain, the virtual machine can then be managed in a separate organizational unit (OU) for configuration and updates.

How to Use Windows XP Mode to Virtualize Internet Explorer 6

The following procedures show the general steps for using Windows XP Mode to virtualize Internet Explorer 6.

Install Windows XP Mode

1. From the Windows Virtual PC Website, download the appropriate version of Windows Virtual PC and download Windows XP Mode.
2. Install Windows Virtual PC.
3. Install WindowsXPMode_en-us.exe.

Configure Windows XP Mode

1. Click **Start**, **All Programs**, **Windows Virtual PC**, and then **Windows XP Mode**.
2. Accept the licensing terms, and then type and confirm a password for XPMUser.
3. Select **Help protect my computer by turning on Automatic Updates now. (recommended)**, and then click **Start Setup**.
4. Wait for Windows XP Mode to configure and boot to the desktop.
5. Click **Start**, right-click **My Computer**, and then click **Properties**.
6. Click the **Computer Name** tab, and click **Change**.
7. Select **Domain**. In the **Domain** field, type your domain name.
8. When prompted for credentials, type the name and password of an account that has permission to join the domain.
9. When prompted to restart your computer, click **Yes**, and wait for the virtual machine to reboot.
10. Right-click **Start**, and then click **Open All Users**.
11. Double-click **Programs**.
12. Drag and drop the **Internet Explorer** icon from the desktop to the **Programs** folder, and close the **Programs** window.
13. Click **Start**, and then click **Log Off**. Click the **X** button in the upper-right corner to put the virtual machine in hibernation.

Test Internet Explorer 6

1. On the Windows 7 workstation, click **Start**, **All Programs**, **Windows Virtual PC**, **Windows XP Mode Applications**, and then click **Internet Explorer (Windows XP Mode)**.
2. Type the password that was defined during the setup of Windows XP Mode.
3. Select the **Remember my credentials** check box.
4. In the **menu** bar, click **Help**, and then click **About Internet Explorer**.
5. Verify that the desired version of Internet Explorer is running.

Customize Internet Explorer 6

1. From the **Tools** menu, select **Internet Options**.
2. In the **Home page address** field, enter the URL address for your desired home page. Close the Internet Explorer window.

3. Click **Start**, **All Programs**, **Windows Virtual PC**, and then **Windows XP Mode Applications**.
4. Right-click **Internet Explorer (Windows XP Mode)**, and then drag to the desktop.
5. Select **Copy here**.

How to Secure Windows XP Mode
Windows XP Mode is an actual instance of running in a virtual machine, and it must be treated as such for security purposes. Use the following guidance to secure your applications:

Secure Windows XP Mode

- Ensure that the appropriate antivirus/anti-malware software is installed on the operating system in the virtual machine. Be aware that the local security software on the host machine does not protect it.
- Ensure that the virtual machine gets all the security updates through automatic updates or WSUS.
- Ensure that any applications installed in the virtual machine get vendor updates when needed.
- Disable unneeded services on the operating system running in the virtual machine.

Additionally, be sure to follow all the security guidelines in the Windows XP Security Compliance Management Toolkit.

Appendix 3: How to Use Terminal Services

The following section provides steps for setting up and using Terminal Services to virtualize Internet Explorer® 7 and Internet Explorer 6 and provides best practices for running and securing your implementation. The configuration described in the sections that follow all assume that an Active Directory domain is already deployed.

Using Terminal Services to Virtualize Internet Explorer 6
For the detailed steps for installing and configuring Terminal Services, see Guidelines for Deploying Terminal Server. The following list includes the high-level steps.

Terminal Services to Virtualize Internet Explorer 6

1. Install Terminal Services.
2. Install the Terminal Services Licensing Server.
3. Configure Terminal Services licensing.
4. Configure the access group.

Secure Terminal Services

1. Create an Active Directory group for users that will use Internet Explorer in Terminal Services.
2. In **Terminal Services Configuration**, click **Connections** to modify the properties for the RDP-TCP connection.
3. On the **Permissions** tab, add the group and grant **Guest Access** permissions. Remove any other groups that do not require remote desktop access.
4. Secure the RDP-TCP connection by configuring the following to fit your requirements:
    a. Restrict the number of client sessions that can remain active on the server.
    b. Set session time limits.
    c. Configure encryption levels.
    d. Set additional permissions for users and groups on the terminal server.
5. Right-click **My Computer**, and then click **Properties**.
6. On the **Remote** tab, clear the **Enable Remote Desktop on this Computer** check box.

Create .RDP File and Test Access

1. From any computer on the network, click **Start**, and then click **Run**.
2. Type **MSTSC**, and then press **ENTER**.
3. In the **Computer** field, type the name of your Terminal Services server.
4. Click the **Options** button.
5. Select the **Allow me to save credentials** check box.
6. Click the **Display** tab, and configure as desired.
7. Click the **Local Resources** tab, and configure as desired.

Note
It is recommended that you allow access to local drives so that you can download to local workstation from the Terminal Services Internet Explorer session.

8. Click the **Programs** tab.
9. In the program path and file name field, type **c:\program files\internet explorer\iexplore.exe**.

Note
You can also include a URL after the above path to define a default website. For example: c:\program files\internet explorer\iexplore.exe" http://intranet/

10. Click the **Experience** tab, and then select the appropriate setting for your network speed.
11. Click the **General** tab.
12. Click **Save As**, and save the RDP file.
13. Double-click the RDP file, and then click **Connect**.
14. Log on and test connectivity. Internet Explorer should start upon log on.
15. Close the RDP session.
16. Copy the RDP file and distribute via your preferred method (e-mail, network share, and so on).
17. After distributing the RDP file, users can right-click the file, click **Edit**, type credentials, and then click **Save**.

Appendix 4: Securing Internet Explorer

Make sure that you have a secure browsing experience that is in line with your company policies. For example, you can disable any Internet Explorer® features that are not required, use security zones, and prohibit downloads.

For more information about security settings, see Working with Internet Explorer 6 Security Settings. For more information about setting policies, see Internet Explorer Policy Settings.

Appendix 5: Updating Using Windows Server Update Services

With Windows Server® Update Services (WSUS), IT administrators can deploy the latest Microsoft® product updates to computers that are running the Windows® operating system. By using WSUS, you can fully manage the distribution of updates that are released through Microsoft Update to computers in your network.

Updating Using Windows Server Update Services
To keep WSUS from automatically updating Internet Explorer 7 or Internet Explorer 6 to Internet Explorer 8, you need create a separate update group for your computers running Internet Explorer 7 and Internet Explorer 6 to make sure that Internet Explorer version updates are not applied to them.

The high-level steps are the following.

To update by using Windows Server Update Services

1. Create a custom Organizational Unit (OU).
2. Add all computers running Terminal Services or Windows XP Mode to the OU. If you are using MED-V, add the MED-V images to the OU.
3. Right-click the custom OU and Group Policy object (GPO) configuration.
4. Create a group in WSUS, and limit Internet Explorer version update approval to this group.

For more information, see Managing Windows Server Update Services.

Revision History

The following changes have been made to this white paper.

Version 1.1
The following summarizes changes made to the 1.1 version of this white paper.

- The following sections were updated:
    - Virtualize with MED-V
    - Appendix 1: How to Use Med-V
    - Basic Requirements for XP Mode
- The **Appendix 4: How to Lock Down Virtualized Internet Explorer Content Access** section was removed.

Version 1.2
The following summarizes changes made to the 1.2 version of this white paper.

- Links to Internet Explorer 6 to Internet Explorer 8 Application Compatibility Remediation white paper were removed.

Deploying Pinned Websites

Windows® Internet Explorer® 9 takes websites out of the browser box and makes them more like applications in Window 7. You can pin websites to the Windows 7 taskbar for quick access. You pin a website simply by dragging its tab to the taskbar. Some websites can also extend the icon's Jump List. For more information about adding and removing pinned sites, see Pin a Website to your Taskbar.

The ability to pin websites to the Windows 7 taskbar can help make end users in businesses more productive. As an IT professional, for example, you can pin intranet websites to the taskbar to make them immediately available to users. In this article, you learn how to deploy pinned websites by using Lite Touch Installation in the Microsoft Deployment Toolkit (MDT) 2010.

Note
Original Equipment Manufacturers (OEMs) are not permitted to customize the browser by pinning websites to the taskbar. OEMs that install Internet Explorer 9 as part of a Windows product, under an OEM license agreement with Microsoft, should use the OEM Preinstallation Kit (OPK) Addendum for Internet Explorer 9 as their guide for customizations that are allowed for Internet Explorer 9 preinstalled on computers.

Deploying pinned websites in MDT 2010

Pinning websites only works with Windows 7 and Internet Explorer 9, so this article requires that you have a fully stocked MDT 2010 deployment share that contains Windows 7. You can add Internet Explorer 9 to the deployment share as an application, or you can slipstream Internet Explorer 9 into the Windows 7 image:

- To learn how to add Internet Explorer 9 to an MDT 2010 deployment share as an update, see Using Software Distribution Tools to Install Internet Explorer 9 in the TechNet library.

- To learn how to add the Internet Explorer 9 update to a Windows 7 image, see Internet Explorer 9 Preinstallation Techniques in the TechNet Library. After you update the Windows 7 image with the Internet Explorer 9 update, you must still add the image to your deployment share.

Deploying pinned websites in MDT 2010 is a three-step process:

1. Create a .website file for each website that you want to deploy. When you pin a website to the taskbar, Windows 7 creates a .website file that describes how the icon should look and feel.

2. Copy the .website files to the Start menu on each target computer for all users. This article uses the legacy OEM folders as a quick and easy way to copy files during deployment to target computers. Alternatively, you could write a script that copies the files, and add that script to the task sequence. Using the OEM folders is much simpler and requires no script code.

3. Edit the task sequence of your Unattend.xml answer files to pin the websites to the taskbar. In particular, you want to add each .website file to the TaskbarLinks item in Unattend.xml during oobeSystem phase. You can add up to three .website files to the TaskbarLinks item.

Figure 1 shows a successful Windows 7 deployment using MDT 2010. Notice that the taskbar already includes the Bing™ and MSN® icons pinned to the taskbar. These websites are immediately available to end users, although they must click each icon to populate its Jump List. You can also pin intranet websites and SharePoint sites. These pinned websites will be available to every user who logs on to the computer.

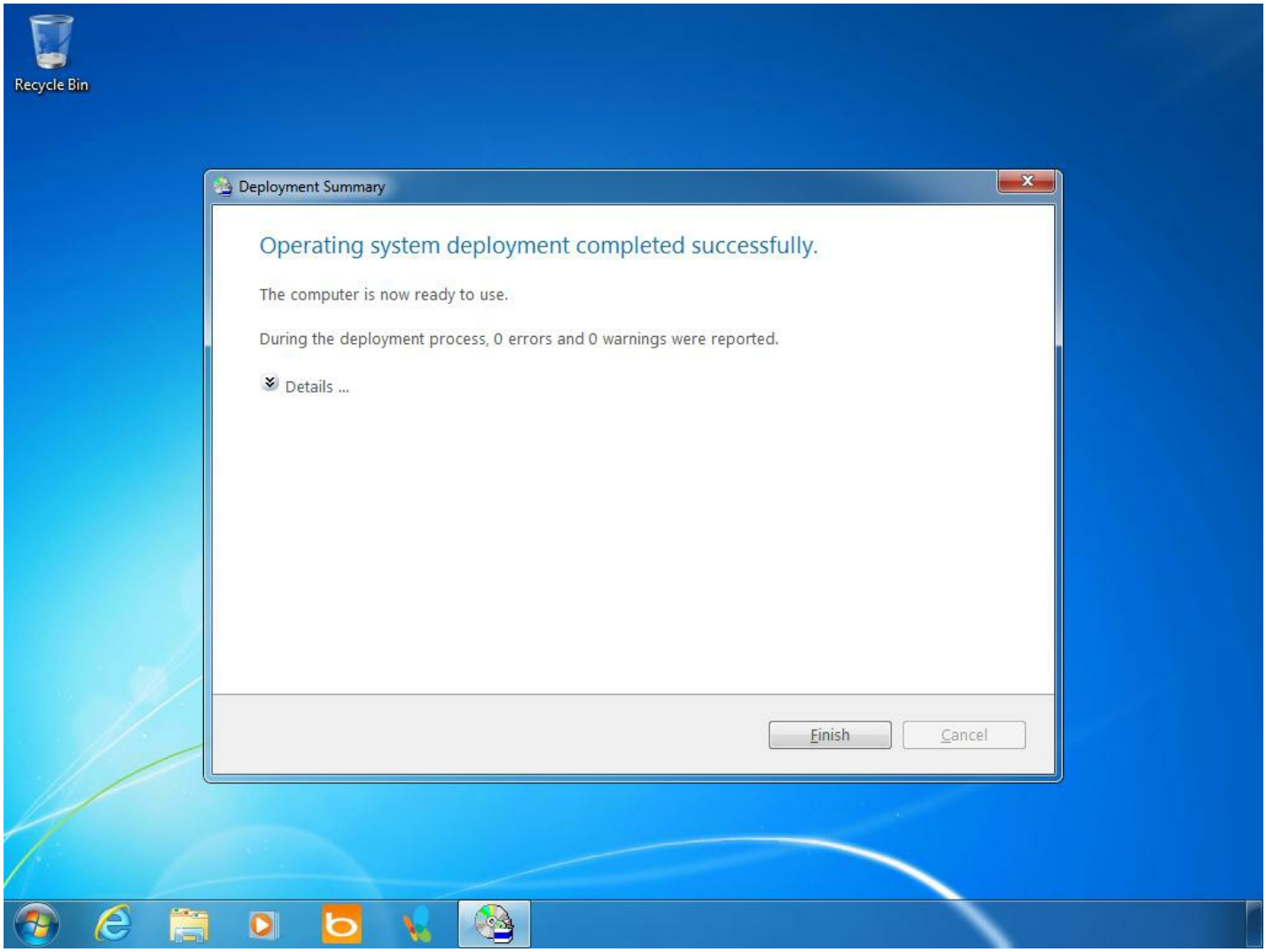


Figure 1. Websites pinned during a Windows 7 deployment by using MDT 2010.

Step 1: Creating .website files

The first step is to create a .website file for each website that you want to pin to the Windows 7 taskbar during deployment. A .website file is like a shortcut, except it's a plain text file that describes not only the website's URL but also how the icon looks.

To create each .website file:

1. Open the website in Internet Explorer 9.
2. Drag the website's tab and drop it on the Windows 7 taskbar.
3. Open the following folder in Windows Explorer, and copy the .website files to your desktop:

   %USERPROFILE%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar

To follow the examples in this article, you will want to pin the Bing (http://www.bing.com/) and MSN (http://www.msn.com/) websites to the taskbar. Then, copy the Bing.website and MSN.com.website to your desktop. You'll add these files to your deployment share in the next step.

Step 2: Copying .website files to the Start menu

After you've copied the .website files to the desktop, you must enable the deployment share to copy them to the Start menu on each target computer. You can create a script that copies the files to target computers' Start menus, and add that script to the task sequence. For more information on using a script to customize your deployment share, see the MDT 2010.

An easier way that requires no script code is to use the legacy OEM folder. The MDT 2010 documentation describes this folder in detail. MDT 2010 automatically copies the contents of the OEM folder to target computers during installation. Everything in the subfolder named $$ goes in the target computer's %SYSTEMROOT% folder, and everything in the subfolder named $1 goes in the %SYSTEMDRIVE$ folder. For more information, see Customizing and Automating Installations.

Here, you'll take advantage of the $1 folder to copy the .website files to the Start menu for all users (%SYSTEMDRIVE%\ProgramData\Microsoft\Windows\Start Menu).

To copy .website files to the Start menu

1. Open the MDT 2010 deployment share in Windows Explorer.
2. In the OEM folder, create the path $1\ProgramData\Microsoft\Windows\Start Menu \Websites. If the OEM folder does not exist, create it at the root of the deployment share.

3. Copy the .website files you created earlier (Bing.website and MSN.com.website) from the desktop to OEM\$1\ProgramData\Microsoft\Windows\Start Menu\Websites in the deployment share, as shown in Figure 2.

The .website files remain on the Start menu after deployment.

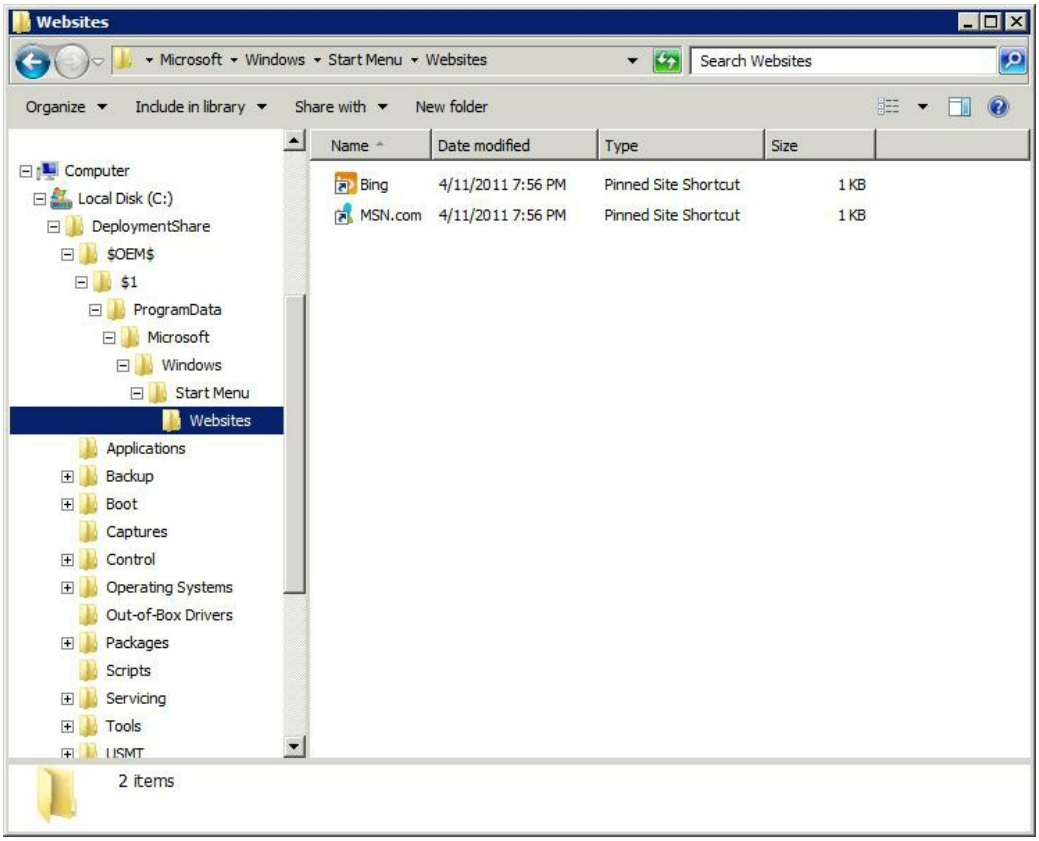


Figure 2. Copying .website files to the Start menu for all users.

Step 3: Pinning .website files to the Taskbar

With the .website files ready to copy to the Start menu on target computers for all users, the last step is to edit the Unattend.xml answer files to pin those .website files to the taskbar. You will need to complete the following steps for each task sequence during which you want to pin these websites to the taskbar:

1. In the Deployment Workbench of MDT 2010, open the deployment share containing the task sequence during which you want to deploy pinned websites, and click **Task Sequences**.

2. In the right pane of the Deployment Workbench, right-click the task sequence, and click **Properties**.

3. On the **OS Info** tab, click **Edit Unattend.xml** to open the Unattend.xml file in Windows System Image Manager (Windows SIM).

4. Add **TaskbarLinks** to the **oobeSystem** phase of the Unattend.xml file. In the **Windows Image** pane, under **Microsoft-Windows-Shell-Setup**, right-click **TaskbarLinks**, and then click **Add Setting to Pass 7 oobeSystem**.

5. In the **TaskbarLinks Properties** pane, add the path of the .website files that you created earlier. You can only add three links to the **TaskbarLinks** item. Additionally, remember to use a path relative to the target computer and not the deployment share. For example, add the following (shown in Figure 3):

   - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Websites\Bing.website
   - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Websites\MSN.com.website

6. On the **File** menu, click **Save Answer File**, and close Windows SIM.

7. To close the task sequence, click **OK**.

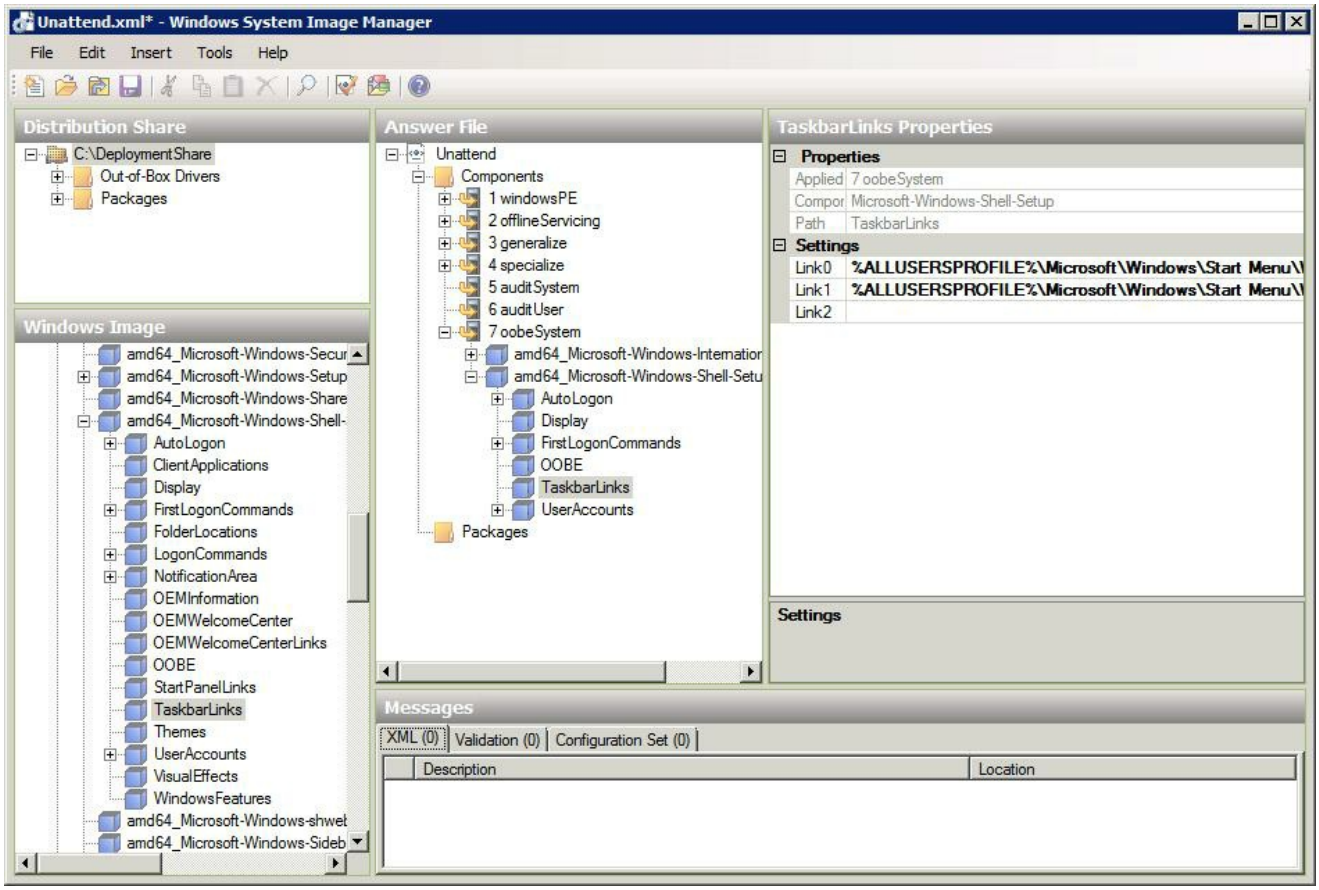


Figure 3. Adding TaskbarLinks to an Unattend.xml file.

Updating intranet websites for pinning

The MDT 2010 deployment share and task sequences are now ready to pin websites to the taskbar during deployment. This pinning feature can include intranet sites important in your organization.

You can make your intranet websites act more like applications by extending them to fully support the Windows 7 taskbar. This includes creating custom Jump Lists, thumbnail previews, and notifications. For more information about extending your intranet websites, see:

- Pinned Sites on MSDN
- Economics of Web: Build a Pinned Site in Less than a Day on the Windows Blog

Also, for more ideas, see Pinned Sites on Internet Explorer Gallery.

Internet Explorer 9 Preinstallation Techniques

This document provides information and instructions necessary for IT Professionals to preinstall the Windows® Internet Explorer® 9 Internet browser, as well as any additional Internet components on Windows 7, or Windows Server 2008. Also, this document provides a list of unattend settings that can be used to automate configuration and deployment of Internet Explorer 9.

Preinstalling Internet Explorer 9 on Windows 7 or Windows Server 2008 R2
You can preinstall Internet Explorer 9 on Windows 7 by slipstreaming Internet Explorer 9 into the operating-system image.

1. Install the Windows Automated Installation Kit (Windows AIK) that matches your local computer configuration.

2. Copy the .wim file that contains Windows 7 to a location on your local drive. For example, `C:\Slipstreaming\Win7x86ENU\install.wim`.

3. Create a folder for the mounted image. For example: `C:\Slipstreaming\Mount`.

4. Download Internet Explorer 9 and put it in a directory in the C:\Slipstreaming directory. For example, C:\Slipstreaming\IE9-Windows7-x86-enu.exe

5. Open a Command Prompt window and extract the cabinet (.cab) file from the Internet Explorer setup executable, by typing:

   ```
   <Path_to_IE90_Setup> /x:<CAB_File_Location>
   ```

   where *Path_to_IE90_Setup* is the location of your Internet Explorer 9 setup executable and the *CAB_File_Location* where to store the extracted .cab file.

   For example: `C:\Slipstreaming\IE9-Windows7-x86-enu.exe /x:C:\Slipstreaming\IE9Win7x86ENU`

Important
You cannot extract the x64-based Internet Explorer cabinet files on an x86-based computer. Instead, you must extract the cabinet files on an x64-based computer. However, you can, extract the x86-based Internet Explorer cabinet files on either an x86-based or x64-based computer.

6. Open an elevated command prompt to run the Deployment Image Servicing and Management (DISM) tool. Click **Start**, point to **All Programs**, point to **Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.

7. Mount your Windows 7 offline image, by using the following command-line text:

   ```
   Dism /Mount-Wim /WimFile:<Filepath> /index:<Index_Number> /MountDir:<Mount_Location>
   ```

   where <*Filepath*> is the full path of your Windows image, <*Index_Number*> is a numeric value for the operating-system image indexed in the .wim file, and <*Mount_Location*> is the location where you want to store the mounted image.

   For example: `Dism /Mount-Wim /WimFile: C:\Slipstreaming\Win7x86ENU\install.wim /index:1 /MountDir:C:\Slipstreaming\Mount`

Important
If you are not sure of your operating-system index number, you can type the following text into a Command Prompt window to retrieve the index number for the image that you want to modify: `Dism /Get-WimInfo /WimFile: <path_to_wim>` For example: `Dism /Get-WimInfo /WimFile:C:\Slipstreaming\Win7x86ENU\install.wim`

8. Download the Internet Explorer prerequisite files for Windows 7 and Windows Server® 2008 R2 into a directory within

the C:\Slipstreaming directory, for example C:\Slipstreaming\Prereqs.

- For Windows 7, the following prerequisites must be installed: KB2454826, KB2484033, KB2488113, KB2467023, and KB2505438. These prerequisites are available in the Internet Explorer 9 .iso file.
- For Windows 7 Service Pack 1 (SP1), the following prerequisites must be installed: KB2484033, KB2488113, and KB2505438. These prerequisites are available in the Internet Explorer 9 .iso file.
- For Windows Server® 2008 R2, the following prerequisites must be installed: KB2454826, KB2484033, KB2488113, KB2467023, and KB2505438. Another update, KB2483177, is not required, but without this update installed media codecs will not be available. This update requires that Desktop Experience is enabled. These prerequisites are available in the Internet Explorer 9 .iso file.
- For Windows Server 2008 R2 SP1, the following prerequisites must be installed: KB2484033, KB2488113, and KB2505438. Another update, KB2483177, is not required, but without this update installed media codecs will not be available. This update requires that Desktop Experience is enabled. These prerequisites are available in the Internet Explorer 9 .iso file.

9. For each of the prerequisite files from the previous step, in the Command Prompt window, type the following text to add the prerequisite to the Internet Explorer 9 package:

   ```
   Dism /Image:<mounted image> /Add-Package /PackagePath:<MSU_File_Location>
   ```

   For example: `Dism /Image:C:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Slipstreaming\Prereqs\Windows6.1-KB2454826-v2-x86.msu`

10. In the Command Prompt window, type the following text to add the Internet Explorer 9 package to the image:

    ```
    Dism /Image:<mounted image> /Add-Package /PackagePath:<CAB_File_Location>
    ```

    For example: `Dism /Image:C:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Slipstreaming\IE9Win7x86ENU\IE9-Win7.cab`

11. In the Command Prompt window, type the following command to commit the changes and unmount the image:

    ```
    Dism /Unmount-WIM /MountDir:<mounted image> /Commit
    ```

    where <*mounted image*> is the location of the Mount folder you created in an earlier step.

    For example: `Dism /Unmount-WIM /MountDir:C:\Slipstreaming\Mount /Commit`

12. Configure your Internet Explorer 9 installation as part of your installation image by creating and using an answer file and performing an unattended installation.

Preinstalling Internet Explorer 9 on a localized version of Windows 7 or Windows Server 2008 R2

You can preinstall Internet Explorer 9 on a localized version of Windows 7 by slipstreaming Internet Explorer 9 into the operating-system image.

1. Install the Windows AIK that matches your local computer configuration.
2. Copy the .wim file that contains Windows 7 to your local drive. For example, C:\Slipstreaming\Win7x64DEU\install.wim.
3. Create a folder for the mounted image. For example:

   - `C:\Slipstreaming\Mount`

4. Download Internet Explorer 9 and put it in a directory in the C:\Slipstreaming directory. For example, C:\Slipstreaming\IE9-Windows7-x64-deu.exe

5. Open an elevated **Command Prompt** window and extract and expand the cabinet (.cab) file from the Internet Explorer setup executable, by typing:

   ```
   <Path_to_IE90_Setup> /x:<CAB_File_Location>
   ```

   where *Path_to_IE90_Setup* is the location of your Internet Explorer 9 setup executable and *CAB_File_Location* is the location to store the extracted .cab files.

   For example: `C:\Slipstreaming\IE9-Windows7-x64-deu.exe /x:C:\Slipstreaming\IE9Win7x64DEU`

   There are two or more CAB files to install:

   - `C:\Slipstreaming\IE9Win7x64DEU\IE9-Win7.CAB` contains the neutral and English versions of Internet Explorer.
   - `C:\Slipstreaming\IE9Win7x64DEU\ielangpack-DEU.CAB` contains the localized support files.

   > **Note**
   > There might be more than one localized package. Some languages have a different fallback language than English. For example, Catalan has fallback-language settings for either French or Spanish. The parent language and the LIP for the Internet Explorer package should be installed.

6. Open an elevated command prompt to run the Deployment Image Servicing and Management (DISM) tool. Click **Start**, point to **All Programs**, point to **Windows AIK**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**.

7. Mount your Windows 7 offline image, by using the following command:

   ```
   Dism /Mount-Wim /WimFile:<Filepath> /index:<Index_Number> /MountDir:<Mount_Location>
   ```

   where <*Filepath*> is the full path to your Windows image file, <*Index_Number*> is a numeric value for the operating-system image indexed in the .wim file, and <*Mount_Location*> is the location where you want to store the mounted image.

   For example: `Dism /Mount-Wim /WimFile:C:\Slipstreaming\Win7x64DEU\install.wim /index:1 /MountDir:C:\Slipstreaming\Mount`

   > **Important**
   > If you are not sure of your operating-system index number, you can use the following command to retrieve the index number for the image that you want to modify: `Dism /Get-WimInfo /WimFile:<path_to_wim>`
   >
   > For example: `Dism /Get-WimInfo /WimFile:C:\Slipstreaming\Win7x64DEU\install.wim`

8. Download the Internet Explorer prerequisite files for Windows 7 and Windows Server 2008 R2 into a directory within the C:\Slipstreaming directory, for example `C:\Slipstreaming\Prereqs`:

   - For Windows 7, the following prerequisites are required to be installed: KB2454826, KB2484033, KB2488113, KB2467023, and KB2505438.These prerequisites are available in the Internet Explorer 9 .iso file.
   - For Windows 7 SP1, the following prerequisites must be installed: KB2484033, KB2488113, and KB2505438. These

prerequisites are available in the Internet Explorer 9 .iso file.

- For Windows Server 2008 R2, the following prerequisites are required to be installed: KB2454826, KB2484033, KB2488113, KB2467023, and KB2505438. Another update, KB2483177, is not required, but without this update installed media codecs will not be available. This update requires that Desktop Experience is enabled. These prerequisites are available in the Internet Explorer 9 .iso file.

- For Windows Server 2008 R2 SP1, the following prerequisites must be installed: KB2484033, KB2488113, and KB2505438. Another update, KB2483177, is not required, but without this update, installed media codecs will not be available. This update requires that Desktop Experience is enabled. These prerequisites are available in the Internet Explorer 9 .iso file.

9. For each of the prerequisite files from the previous step, in the Command Prompt window, type the following text to add the prerequisite to the Internet Explorer 9 package: `Dism /Image:<mounted image> /Add-Package /PackagePath:<MSU_File_Location>`

   For example: `Dism /Image:C:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Slipstreaming\Prereqs\Windows6.1-KB2454826-v2-x64.msu`

10. In the Command Prompt window, type the following text to add the Internet Explorer 9 language-neutral package: `Dism /Image:<mounted image> /Add-Package /PackagePath:<CAB_File_Location>`

    For example: `Dism /Image:C:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Slipstreaming\IE9Win7x64DEU\IE9-Win7.CAB`

11. Internet Explorer localized files have a dependency that requires that the supporting Windows localized files to be installed before a localized Internet Explorer package can be installed.

    If you are slipstreaming Internet Explorer into a fully localized build of Windows and the supporting Windows localized language files are already installed on the system, you can skip this step. You must install Windows language packs (LIPs and MUI files) before you install any other updates, because the language-specific updates will not be applied in the resulting image. If you are installing a LIP, you must change the file name extension from .mlc to .cab.

    You can add a language package by using the command: `Dism /Image:<mount folder> /Add-Package /PackagePath:<path to language pack cab file>`

    For example: `Dism /Image:C:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Downloads\Langpacks\de-de\lp.cab`

12. Add the Internet Explorer language package by using the command: `Dism /Image:<mount folder> /Add-Package /PackagePath:<path to language pack cab file>`

    For example: `Dism /image:c:\Slipstreaming\Mount /Add-Package /PackagePath:C:\Slipstreaming\IE9Win7x64DEU\ielangpack-DEU.cab`

13. In the Command Prompt window, type the following command to commit the changes and unmount the image:

    `Dism /Unmount-WIM /MountDir:<mounted image> /Commit`

    where *<mounted image>* is the location of the Mount folder you created in an earlier step.

    For example: `Dism /Unmount-WIM /MountDir:C:\Slipstreaming\Mount /Commit`

14. Configure your Internet Explorer 9 installation as part of your installation image by creating and using an answer file and performing an unattended installation.

Unattended Installation Settings and Internet Explorer 9

The following table shows settings in the Microsoft-Windows-IE-InternetExplorer component that are new in Internet Explorer 9. You can use these settings to modify the way Internet Explorer 9 browser appears and behaves to the end user.

New Internet Explorer setting	Description
Microsoft-Windows-IE-InternetExplorer/SearchScopes/Scope/`ShowTopResult`	Specifies whether the *TopResult* feature is used with search requests.
Microsoft-Windows-IE-InternetExplorer/SearchScopes/Scope/`TopResultURL`	Specifies the complete URL of the page that shows the *TopResult* search results.

The following table shows changes in existing Internet Explorer settings.

Changed setting	Description of setting	Description of change
Microsoft-Windows-IE-InternetExplorer/`EnableLinksBar`	Specifies whether the **Favorites** bar appears.	The default value is changed to `false`.
Microsoft-Windows-IE-InternetExplorer/`ShowCommandBar`	Specifies whether the **Command** bar appears.	The default value is changed to `false`.
Microsoft-Windows-IE-InternetExplorer/`ShowStatusBar`	Specifies whether the **Status** bar appears.	The default value is changed to `false`.
Microsoft-Windows-IE-InternetExplorer/`SmallCommandBarIcons`	Specifies whether small icons on the **Command Bar** are used.	The default value is changed to `true`.