For IT professionals: Planning guide for Microsoft Office 2010

Microsoft Corporation

Published: December 2010

Author: Microsoft Office System and Servers Team (itspdocs@microsoft.com)

Abstract

This book contains information about how to plan a deployment of Microsoft Office 2010. The audience for this book includes IT generalists, IT operations, help desk and deployment staff, IT messaging administrators, consultants, and other IT professionals.

The content in this book is a copy of selected content in the Office 2010 Resource Kit technical library (*http://go.microsoft.com/fwlink/?LinkId=181453*) as of the publication date. For the most current content, see the technical library on the Web.

Microsoft

Contents

Getting help

Every effort has been made to ensure the accuracy of this book. This content is also available online in the Office System TechNet Library, so if you run into problems you can check for updates at:

http://technet.microsoft.com/office

If you do not find your answer in our online content, you can send an e-mail message to the Microsoft Office System and Servers content team at:

itspdocs@microsoft.com

If your question is about Microsoft Office products, and not about the content of this book, please search the Microsoft Help and Support Center or the Microsoft Knowledge Base at:

http://support.microsoft.com

Planning the deployment of Office 2010

This section provides an overview of the Setup architecture for Office 2010, and information about how to plan for desktop configurations, security, and applications including Microsoft Access 2010, Microsoft Excel 2010, and Microsoft Outlook 2010. It also provides planning information for migration and upgrading from previous versions of Office, as well as planning for virtualization and Remote Desktop Services.

In this section:

Article	Description
Setup architecture overview for Office 2010	Provides an overview of the Setup architecture for Office 2010, setup sequence of events, language-neutral design and deployment of multiple languages, customization methods, required local installation source, and updates process.
Plan a migration and upgrade strategy for Office 2010	Provides information about how to plan the installation of the Microsoft Office 2010 suites, and how to migrate the user data, such as user and computers settings and documents created from the previously installed versions of Microsoft Office.
Plan desktop configurations for Office 2010	Provides information and guidelines about items to consider before you deploy Office 2010.
Plan for volume activation of Office 2010	Provides an overview of Microsoft Volume Licensing and Office Activation Technologies for Office 2010 and how describes how to plan for volume activation.

Setup architecture overview for Office 2010

The basic Setup architecture in Microsoft Office 2010 is the same as the architecture introduced in the 2007 Microsoft Office system. The Setup architecture streamlines all aspects of installing, customizing, and maintaining Office. The Setup program unifies and manages the complete installation process. This includes customizing users' Office configuration, deploying multiple languages at the same time, and applying software updates to new installations. This article contains an overview of the Setup architecture, setup sequence of events, language-neutral design and deployment of multiple languages, customization methods, required local installation source, and updates process.

The Setup architecture helps administrators manage areas such as the following more efficiently:

- Deployment process so that Office is installed in the most efficient way for their environment.
- Customization of Office so that users get optimal configuration on their computers.
- Deployment of language-specific features for users who are located in offices around the world.
- Deployment of Office in a way that makes future maintenance, including software updates, as efficient as possible.

In versions of Office earlier than the 2007 Office system, a single Office product such as Microsoft Office Standard was contained in a single *Windows Installer (MSI) file*. An MSI file is a relational database that Windows Installer uses to install a product. As with the 2007 Office system, the Office 2010 products consist of multiple MSI files, and no single MSI file represents a complete product. A language-neutral core package (MSI file) is combined with one or more language-specific packages to make a complete product. For example, an Office product such as Microsoft Office Professional Plus 2010 consists of the core package plus one or more language-specific packages. Setup assembles the individual packages, orchestrates a seamless installation, and handles customization and maintenance tasks during and after installation of Office on users' computers.

Office 2010 introduces native 64-bit versions of Office products to support 64-bit processors, which are becoming the standard for systems ranging from servers to desktop computers. Office 2010 also provides support for 32-bit Office 2010 applications that run on 64-bit Windows operating systems by using Windows-32-on-Windows-64 (WOW64). WOW64 is the x86 emulator that enables 32-bit Windows-based applications to run seamlessly on 64-bit Windows. Office 2010 lets users continue to use existing third-party Office add-ons, which are primarily 32-bit because no 64-bit versions are available yet for many add-ons. Providing support for 32-bit Office 2010 running on 64-bit operating systems prevents blocking the 32-bit add-ons. For more information about 64-bit editions of Office 2010, see 64-bit editions of Office 2010 (*http://technet.microsoft.com/library/faab55b2-bb6c-4636-811e-24f6939548d1(Office.14).aspx*).

In this article:

Setup process

Typically, the first step in a corporate installation of Office is to create a network installation point — a task as simple as copying all the files and folders from the Office product CD to a shared network location. At a minimum, the network installation point contains the language-neutral core package plus language-specific folders for one language. This installation point serves as the initial source for all users who install Office.

In the simplest scenario, you deploy an Office product from the network installation point with one language version and a single set of customizations for all users. Setup handles this scenario automatically. If you deploy multiple products or languages, you can add them to the same network installation point and specify exactly which products and languages to include in the installation. In all of these scenarios, Setup performs the same tasks to assemble the correct set of MSI files and to complete the installation.

Note:
The Office 2010 does not let you create an administrative installation point by running Setup with the **/a** command-line option to extract compressed source files, as was possible with Office versions earlier than the 2007 Office system. All installations now occur from the compressed source.

In this section:

Setup sequence of events

The basic Setup sequence of events is as follows and occurs in the same order in every deployment scenario:

1. Run Setup.
2. Check prerequisites.
3. Read XML data.
4. Build the feature tree.

5. Create a local installation source on the user's computer.
6. Install Office.
7. Apply the customization file.
8. Apply software updates.

Run Setup

Setup.exe is the program that begins all the mechanisms of the installation process. It is located at the root of the network installation point. You run Setup one time for each Office product that you install. When it runs, Setup searches the network installation point for an Office product to install. If the installation point contains more than one Office product, Setup gives the user a choice of products to install.

You can circumvent the selection process and determine which Office product is installed by pointing Setup.exe to the Config.xml file in a core product folder. For example, if you want to install Microsoft Office Professional Plus 2010, you can use the following command line:

\\server\share\Office14ProPlus\setup.exe /config
\\server\share\Office14ProPlus\Pro.WW\Config.xml

where **Office14ProPlus** is the root of the network installation point.

In versions of Office earlier than the 2007 Office system, Setup.exe called Windows Installer (Msiexec.exe) to install Office. Although Setup still uses Windows Installer, Setup bypasses the Windows Installer executable program. The Msiexec.exe command line cannot be used to install the Office 2010 (or the 2007 Office system).

Note:
This version of Setup.exe recognizes only a few command-line options. For more information, see Setup command-line options for Office 2010 (*http://technet.microsoft.com/library/0f489f42-4c01-41d1-8b52-3a2a2da8f731(Office.14).aspx*).

Check prerequisites

When Setup starts, it checks for several installation prerequisites. This includes minimum operating system requirements and administrative permissions. A user must be an administrator of the client computer to install Office, or you must use a tool such as Microsoft Systems Management Server (SMS) or Microsoft System Center Configuration Manager 2007 to run the installation by using elevated permissions.

When you run Setup.exe from the x64 folder, Setup determines whether there are 32-bit Office applications installed. If Setup detects 32-bit Office applications, it displays an error message that informs users that they must first uninstall all 32-bit Office applications if they want to continue with the installation of Office 2010 64-bit. The error lists the installed 32-bit Office applications. If Setup does not detect 32-bit Office applications, it installs the 64-bit edition of Office 2010.

When you run Setup.exe from the x32 folder, Setup determines whether there are 64-bit Office 2010 applications installed. If Setup detects 64-bit Office 2010, an error message displays and Setup is blocked. If Setup does not detect 64-bit Office 2010, it installs the 32-bit edition of Office 2010. For more information, see 64-bit Setup process (*http://technet.microsoft.com/library/faab55b2-bb6c-4636-811e-24f6939548d1.aspx#BKMK_SetupProc*) in 64-bit editions of Office 2010 (*http://technet.microsoft.com/library/faab55b2-bb6c-4636-811e-24f6939548d1(Office.14).aspx*).

Note

- To install Office on computers where users lack administrative permissions, you must run Setup in a context that provides it with administrative permissions. After Office is installed, users without administrative permissions can run all installed features. This includes installing features on demand.
- For example, in organizations where users are not the administrators of their computers, administrators can use the following methods of providing Office Setup with the appropriate permissions:

Read XML data

Setup collects information about each package on the installation point, collects default settings for the installation, and incorporates customizations that you specify. Setup collects all this information in the form of XML data from several sources:

- **Setup.xml and Package.xml files for each package** Each folder on the installation point — both the folder for the language-neutral core package and the folder for each language-specific package — contains a Setup.xml and a *Package*.xml file (for example, ProPlusWW.xml for Microsoft Office Professional Plus 2010). Information in these files enables Setup to do the following:
  - Identify a product and the available languages for that product.
  - Match language-neutral and language-specific elements to create complete features.
  - Build a consolidated feature tree.
  - Collect the set of MSI files that are required for the installation.

  Note:
  The Setup.xml and *Package*.xml files are signed and cannot be modified. Altering these files causes Setup to fail.
- **Setup customization file** Early in the installation process, Setup determines whether you have specified a Setup customization file (.msp file) for the product that is being installed. A Setup customization .msp file is created when administrators use the Office Customization Tool (OCT) to customize an installation of Office 2010. The OCT is part of the *Setup program* and is the recommended tool for most customizations. The customization file contains all the modifications that you specify for an installation. This includes customizations that control the installation process.

The OCT is available in volume licensed versions of Office 2010. To determine whether your Office 2010 installation is a volume licensed version, check the Office 2010 installation disk to see whether it contains a folder named Admin. If the Admin folder exists, the disk is a volume license edition; otherwise, the disk is a retail edition.

If no customization file is specified on the command line or in the Config.xml file, Setup searches the Updates folder on the installation point for a customization file specific to the product that is being installed. By default, the Updates folder is included on the installation point. In most cases, it is the recommended location in which to store both a Setup customization .msp file and software updates for all the Office products included on the installation point.

Important

- If you plan to deploy multiple Setup customization files (.msp files), you can place only one customization .msp file for each Office 2010 product that you are installing in the Updates folder for an initial installation. Only one Setup customization .msp file (patch) for each Office 2010 product that you are installing is supported in the Updates folder. You must deploy the rest of the customization .msp files for a product after the Office installation is completed.
- If you are deploying multiple Office 2010 products, such as Microsoft Office Professional Plus 2010 and Microsoft Visio Professional 2010, you can include one customization .msp file for Office Professional Plus 2010 and one customization .msp file for Visio Professional 2010 in the Updates folder. The customization .msp files that you place in the Updates folder will be deployed first. Therefore, they must include any Setup customizations that cannot be changed after the installation, for example, the installation location.
- If you are deploying an initial installation of Office 2010 and you also want to deploy Office 2010 software updates, such as service packs and hotfixes, Setup can apply the product updates as part of the installation process. You can place the Office 2010 product updates in the Updates folder. In scenarios such as this where the Updates folder includes both one Setup customization .msp file and product updates, Setup applies only the Setup customization .msp file with the initial installation and the product updates are applied after the installation is complete.

Setup uses XML data appended to the customization file to determine how to install the product — for example, whether to run quietly or which features to display in the feature tree. Settings in a customization file overwrite default settings contained in the Setup.xml and *Package*.xml files.

For more information about Setup customization files, see Streamlined customization model. For information about how to use the OCT, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

- **Config.xml file** Each core product folder contains a Config.xml file that directs Setup to install that product. You can edit Config.xml to customize the installation process. For example, you can use elements in Config.xml to specify which products or languages to include in the installation. Settings in Config.xml take precedence over settings in a customization file and default settings contained in the Setup.xml and *Package*.xml files.

For more information about how and when to edit Config.xml, see Config.xml file in Office 2010 (*http://technet.microsoft.com/library/e16af71c-fed4-40da-a886-95e596c3999e(Office.14).aspx*).

Build the feature tree

Setup uses the information that is contained in the XML files to create a single feature tree that includes all the available applications and features in the product. You view the feature tree and specify which applications and features to install on users' computers by using the Office Customization Tool. If you let users run Setup interactively, they view the feature tree with your modifications in the Setup user interface.

For more information about how to specify which Office features to install, see Configure feature installation states for Office 2010 (*http://technet.microsoft.com/library/5e377afe-3c09-447d-82b9-06400fbf1138(Office.14).aspx*).

Create a local installation source on the user's computer

Setup calls a program named **Office Source Engine** (**Ose.exe**) to create a required local installation source (LIS) on the user's computer. To create the local installation source, Setup copies files from the installation point to a *hidden* folder on the user's computer. The default location is **\MSOCache\All Users** at the root of the drive on which Office is installed. Later, Setup uses Windows Installer to install Office from this local installation source.

The local installation source provides several important benefits:

- After Office is installed, Setup can repair, reinstall, or add Office features by using the local source.
- Users who are applying software updates are less likely to be prompted for a network or CD source because an installation source is available locally.
- You can deploy the local installation source in advance and trigger the installation of Office on users' computers later to reduce the load on the network. In this scenario, you can even run Setup from the local installation source. This lets users complete the Office installation by using no network connection.

For more information about the local installation source, see Required local installation source.

Install Office

When the installation starts, Setup checks for required disk space and feature dependencies, and then calls Windows Installer to install the correct set of packages (MSI files) on the user's computer from the local installation source. Setup uses the XML data described previously to determine which set of MSI files to include. The progress bar that Setup displays to users during the installation takes the whole installation process into account. This includes applying customizations and software updates from the Updates folder.

Note:

Although Setup uses Windows Installer to install Office, Windows Installer alone cannot install the individual MSI files independent of Setup.

Apply the customization file

During the installation process, Setup applies the customization file to the user's configuration. The result resembles the effect of applying a Windows Installer transform (MST file) in previous versions of Office: your customizations become the default configuration for users. In addition to the XML data that customizes the installation process, the customization file might include default user settings, feature installation states, Microsoft Outlook profiles, and other modifications to the user's configuration.

Customization files are product-specific; Setup applies only those files that are relevant to the product being installed.

Note:

If you plan to deploy multiple Setup customization .msp patches, you can place only one Setup customization .msp file for each Office 2010 product in the Updates folder for an initial installation. You must deploy the rest of the customization .msp files after the Office installation is complete. As mentioned previously, only one customization for each product patch in the Updates folder is supported. The customization .msp file that you place in the Updates folder will be deployed first so it must include any Setup customizations that cannot be changed after the installation, for example, the installation location.

If you create different configurations for different groups of users, we recommend that you store the customization files in another location and then use the **/adminfile** option on the Setup command line to specify the file that you want. For example:

\\server\share\Office14\setup.exe /adminfile \\server\share\Office14\MyUpdates\Engineering.msp

where **Office14** is the root of the network installation point.

Note:

When you precache the local installation source, Setup copies the Updates folder from the network installation point to the local installation source. In this manner, your customizations can be included in offline installation scenarios. This is the only circumstance in which Setup caches the customization file on the local computer before the installation. For more information, see Precache the local installation source for Office 2010 (*http://technet.microsoft.com/library/ff0a01a5-33d8-407c-ac52-50edccb32786(Office.14).aspx*).

Apply software updates

At the end of the installation process, Setup checks the Updates folder on the installation point for software updates (.msp files). Unlike Setup customization files that you create by using the Office Customization Tool, software updates are distributed by Microsoft to enhance the product.

If you are deploying Office to users and must also have to deploy a set of software updates, Setup can apply the updates as part of the initial installation process. Costing (estimated required disk space) and progress bar indicators all take this step of the installation process into account. From a user's

perspective, the complete process is a single event. This model preserves the original installation point and still lets you give new users the most up-to-date version of the product.

Note:
The Updates folder is used only for initial or new installations of Office 2010. The Updates folder can contain only one Setup customization .msp patch, and multiple service packs and hotfixes that are in .msp format only.

For more information about the software update process, see Consolidated update process.

Including more than one product on the installation point

If the network installation point contains more than one Office 2010 product, Setup searches all folders and subfolders for Config.xml and Setup.xml files and then prompts the user to select a product to install. If you are installing more than one Office product, it is more efficient to store all the products on the same installation point and then customize Setup to install a specific Office product on users' computers.

Note:
When you copy multiple Office products to the same installation point, you might be prompted to overwrite shared Setup files. Because these files are duplicated among all Office 2010 products, you do not need to recopy any of the duplicate folders. This efficient design saves space and ensures consistency when you create and replicate network installation points.

Running Setup interactively

You can choose to run the installation quietly so that users see little or none of the process. However, if you let users view the Setup user interface, the choices that you make affect several aspects of Setup behavior. For example:

- If more than one Office product is available on the installation point and a user runs Setup.exe without command-line options, Setup gives the user a choice of products to install.
- If more than one language is available on the installation point, Setup matches the language of Office to the Windows user locale on the user's computer. This is by default. However, if a user selects the **Customize** installation option, the **Languages** tab in the Setup interface gives the user a choice of all available languages on the network installation point.
- If you enter a product key and accept the Microsoft Customer License Terms in the customization file or Config.xml, those Setup screens are not displayed to the user during Setup.
- If you use a customization file to hide and lock certain features, those features are not displayed in the feature tree.

To find out more about how to customize display settings, see Customize Setup before installing Office 2010 (*http://technet.microsoft.com/library/9c14db60-b591-41f9-a94b-50627d2daa81(Office.14).aspx*).

Language-neutral design

In Office 2010 (and in the 2007 Office system), an Office product such as Office Professional Plus 2010 is organized as follows:

- Language-neutral elements are grouped in one core package (MSI file).
- Language-specific elements are organized in separate packages by application.

This arrangement of files simplifies international deployments. The most basic installation of an Office product consists of the core package plus one language. Adding more languages is as simple as copying additional Single Language Packs (SLPs) to the network installation point — all work with the core product in exactly the same way. All language versions of Office, including the English language version, are deployed in the same manner. Setup combines the language-neutral core package with the language-specific packages in a seamless installation process.

Important:
The current Office 2010 release includes English, Chinese, French, German, Japanese, Spanish, and Russian language sources *only*. Later releases will provide additional languages.

In this section:

Language versions of Office

Every Office product must include at least one set of language-specific packages. You cannot deploy just the core package (MSI file) by itself. On the Office product CD and the network installation point, these language packages are contained in folders. Each folder name includes a language tag, in the form *ll-cc* (for example, *en-us* for English U.S.), that identifies the language. Each folder also contains a set of installation files.

For example, the Office Professional Plus 2010 product is spread out among the files in these folders. Elements that are not specific to any language, such as Winword.exe (the executable file for Microsoft Word 2010), reside in the core ProPlus.WW package. Other elements, such as Help and the user interface for Word 2010, reside in the appropriate language-specific package for Word or for shared Office features.

Both language-neutral and language-specific elements are required to make a functionally complete feature. Winword.exe by itself does not represent a Word application that anyone can use. Similarly, the core Office Professional Plus 2010 MSI file in the ProPlus.WW folder does not represent a complete Office product.

Setup assembles all these parts into a whole product. The Package.xml and Setup.xml files in each folder contain information that Setup uses to assemble complete features, build a consolidated feature tree, and collect the correct set of MSI files for the installation. After collecting the XML data and assembling the required MSI files, Setup uses Windows Installer to install Office on the user's computer. From a user's perspective, this process happens automatically and seamlessly.

You cannot deploy an individual application in Office 2010 by detaching the language-specific folder that contains the individual MSI file, such as the Word.en-us folder. However, you can determine which applications and features are installed on users' computers by customizing the installation.

Note:
None of the MSI files on an Office installation point can be installed independently by using Windows Installer or any other method. Also, none of the digitally signed XML files (Setup.xml and *Package*.xml) can be edited or altered. In Office 2010, Setup is required to collect the files and installation information and to orchestrate the installation process.

Language packs for Office

Language-specific packages are used in two contexts: in the language version of an Office product, and in the Single Language Pack (SLP) for that language. For example, the French version of Office Professional Plus 2010 will include a language-specific folder for each application and for shared features in Office Professional Plus 2010. The same folders will be included in the French SLP, which will include language-specific folders for other products in Office 2010.

Language packs can be deployed as separate products, or they can be used to deploy an Office product in multiple languages. You are not required to enter a unique product key for language packs, whether you are deploying them separately or as part of the installation of another product.

Note:
In versions of Office earlier than the 2007 Office system, enterprise customers added languages by deploying Multilanguage User Interface (MUI) packs after a U.S. English version of Office was installed. Localized versions, such as the Japanese version of Office Standard Edition, were not identical to the core version with a Japanese MUI pack. This design was simplified and improved in the 2007 Office system and is the same in Office 2010.

Streamlined customization model

In versions of Microsoft Office earlier than the 2007 Office system, several tools were required to customize Setup and to manage Office after installation. The 2007 Office system introduced a consistent, streamlined model. In Office 2010 (as in the 2007 Office system), administrators can use Setup to install, customize, and manage Office. To enforce specific user and computer settings, administrators can use Group Policy (see Using Group Policy).

In this section:

- Using the Office Customization Tool
  - Customizing a new installation
  - Making changes to an existing Office installation
- Using the Config.xml file to customize Office
- Using Setup command-line options
- Using Group Policy

Using the Office Customization Tool

You customize an Office installation by using the Office Customization Tool, a component of Setup, which is included in volume licensed versions of Office 2010 client. Start the OCT by running Setup with the **/admin** command-line option. By using the OCT, create a Setup customization file (.msp file), which you place in the Updates folder in the network installation point. As mentioned previously, the Updates folder is used only for initial or new installations of Office 2010, and only one customization patch in the Updates folder is supported. A Setup customization file is an expanded form of a Windows Installer .msp file. Each file is configured for a specific product, such as Office Professional Plus 2010 or OneNote 2010. When you run Setup to install an Office product, Setup looks in the Updates folder for a customization file that corresponds to the product that you are installing. As Setup installs the product, it applies the customizations from this file. You can create more than one Setup customization file to configure Office for different groups of users. When you run Setup, you specify the appropriate customization file to use for each installation by using the Setup command-line option **/adminfile**, or by using Config.xml (see Using the Config.xml file to customize Office).

For complete details on how to use the OCT to create a Setup customization file, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

Customizing a new installation

By using a Setup customization file that you create with the OCT, you can modify the way Setup installs Office on a user's computer the first time. For example, the OCT lets you customize Office in the following ways:

- Direct Setup to run without user interaction (quietly).
- Predefine the product key and accept the Microsoft Software License Terms on behalf of the user.
- Specify where to install Office files on the user's computer.
- Choose whether to remove previous versions of Office before you install the Office 2010.
- Determine which Office features are installed.
- Specify the default values for a large number of user options, including Microsoft Outlook settings.

Note:
Office 2010 does not support side-by-side installations of 64-bit and 32-bit Office, including across applications. For example, there is no support for side-by-side installations of the 2007 Office system 32-bit with Office 2010 64-bit, or for Microsoft SharePoint Workspace 2010 64-bit and Microsoft Excel 2010 32-bit. You cannot use the Office 2010 customization tools to configure side-by-side installations or customizations of 64-bit and 32-bit Office. For example, you cannot create a custom side-by-side installation by using 64-bit Microsoft Office Professional 2010 and 32-bit Visio 2010 single image. For more information about 64-bit Office 2010, see 64-bit editions of Office 2010 (*http://technet.microsoft.com/library/faab55b2-bb6c-4636-811e-24f6939548d1(Office.14).aspx*).

For information about how to customize Setup, see Customize Setup before installing Office 2010 (*http://technet.microsoft.com/library/9c14db60-b591-41f9-a94b-50627d2daa81(Office.14).aspx*).

Making changes to an existing Office installation

If you need to make changes to an existing Office installation, use the same tool that you used to customize the original installation: Run the OCT to update a Setup customization file or to create a new one. Then apply the customization file to the user's computer exactly as you would a software update, and the user's existing Office installation is updated with your customizations. This means that the customizations available when you install Office are also available when you modify Office after installation.

Note:
There are some customizations that Setup applies only when you are installing Office for the first time. These include: specifying where to install Office on the user's computer, defining the product key, and removing previous versions of Office applications. The OCT identifies which customizations apply only to a new installation.

Using the Config.xml file to customize Office

You can use the Config.xml file to make changes to your Office installation. You can customize most of the same options that you can with the Office Customization Tool, including a few additional ones not available in the OCT.

Using the Config.xml file is the recommended method for performing the following installation tasks:

- Instructing Setup to copy the *local installation source* to the user's computer without installing Office.
- Specifying the path of the network installation point.
- Selecting which product or language to install.
- Changing where Setup looks for Setup customization files and updates.
- Making last-minute or one-off customizations that do not warrant running the OCT to create a new customization file.

If you put the Config.xml file in the same folder as Setup.exe, Setup finds and uses the file. You can also specify the location of the file by using the **/config** Setup command-line option.

Note:
If you specify both a Setup customization file and the Config.xml file, the customizations that you define in Config.xml take precedence over the same customizations in the customization file.

For a complete description of the contents and format of the Config.xml file, see Config.xml file in Office 2010 (*http://technet.microsoft.com/library/e16af71c-fed4-40da-a886-95e596c3999e(Office.14).aspx*).

Using Setup command-line options

Setup recognizes only a few command-line options in the Office 2010. This is the same as for 2007 Office system. The OCT is the primary tool to configure Setup properties and specify other customizations.

You can use Setup.exe commands to perform the following tasks:

- Run the Office Customization Tool to create a Setup customization (.msp) file.
- Apply the specified Setup customization file to the installation. For example, you can specify a path of a specific customization file (.msp file) or to the folder where you store customization files.
- Specify the Config.xml file that Setup uses during the installation.
- Run Setup in maintenance mode and make changes to an existing Office installation.
- Run Setup to repair the specified product from the user's computer.
- Run Setup to remove the specified product from the user's computer.

For more information about the Setup.exe commands, see Setup command-line options for Office 2010 (*http://technet.microsoft.com/library/0f489f42-4c01-41d1-8b52-3a2a2da8f731(Office.14).aspx*). For information about Windows Installer properties that were used in previous versions of Office, and about properties that can be used when you install Office 2010, see Setup properties in Office 2010 (*http://technet.microsoft.com/library/41f07f9b-f0d0-489d-a185-d7b96f21f561(Office.14).aspx*).

Using Group Policy

Administrators can use Group Policy settings to define and maintain an Office configuration on users' computers. Group Policy is used to configure the Office 2010 policy settings contained in Administrative Templates, and the operating system enforces those policy settings. In an Active Directory environment, administrators can apply policy settings to groups of users and computers in a site, domain, or organizational unit to which a Group Policy object is linked. True policy settings are written to the approved registry keys for policy, and these settings have access control list (ACL) restrictions that prevent non-administrator users from changing them. This allows administrators to create highly restricted or lightly managed configurations.

Administrators can use policy settings for the Office 2010 applications to manage most options that configure the Office user interface, including the following:

- Menu commands and their corresponding toolbar buttons
- Shortcut keys
- Most options in the **Options** dialog box

Note:
Most of the Office 2010 policy settings are also available in the OCT (OPA settings). To configure initial default settings in a Setup customization .msp file, administrators can use the OCT. However, users can modify most of the settings after the installation. Use Group Policy if you want to enforce specific configurations. Group Policy settings have precedence over OCT settings.

Required local installation source

In Office 2010, Setup creates a local installation source on the user's computer as part of the default installation process. Setup installs all Office 2010 products in a two-step process. First, Setup copies compressed installation source files to the user's computer. Second, Setup calls Windows Installer to perform the actual installation from the local installation source. After the installation is complete, the local installation source remains available for any Setup operations that require access to an original source. Minimum disk space requirements include the local installation source.

Note:
In Microsoft Office 2003, large organizations typically installed the product from an administrative installation point; installing from a local installation source was optional. In the Office 2010, however, the administrative installation option no longer exists, and the local installation source is a required part of the design.

The local installation source makes the process of distributing software updates more efficient and reliable. Neither the network installation point nor the user's local installation source is ever updated directly. Users' installations remain synchronized when they apply the client version of software updates.

Additional benefits of having a complete installation source always available on the local computer include the following:

- You can deploy the local installation source to users before they install Office. This minimizes the effect on the network and ensures that all users install the product and begin to use Office 2010 applications at exactly the same time.
- Users can perform maintenance tasks, such as applying software updates, without being prompted for their Office CD or a network source.
- Traveling users, or users who have slow or intermittent network connections, can run Setup without access to the network if they have a local installation source installed in advance.

These benefits come at minimal cost. Although the local installation source does use some hard disk space, creating the local installation source and installing Office takes approximately the same amount of time as installing Office by itself.

In this section:

Creating a local installation source on users' computers

When users install Office from the CD or from a network installation point, Setup creates the local installation source by using a program called the Office Source Engine (Ose.exe) to copy required installation files to a *hidden* folder on the local computer. The default location is \MSOCache\All Users at the root of the drive on which Office is installed.

Each package that comprises an Office product — both the language-neutral core package and one or more language-specific packages — has a separate download code and is cached in the subfolder under MSOCache\All Users. Setup always caches a complete local installation source, which includes all the files associated with the product that is being installed. If the installation point includes multiple languages, Setup caches only the packages for the languages that are installed on the user's computer.

When additional Office products are installed on the user's computer, those products are cached in the same local installation source.

Note:
If a user installs a second Office product on a different drive, Setup creates a second local installation source at the root of that drive. In this scenario, shared files might be duplicated between the two local installation sources. However, this design ensures that each local installation source is complete and functions correctly.

Users cannot unintentionally delete the local installation source or remove it by using the Setup user interface or the Windows Disk Cleanup Wizard. If the MSOCache folder is deleted or corrupted, Setup automatically re-creates or repairs the folder the next time that a source is required. If users do not have sufficient disk space, they are prompted to free some space. You can rely on the fact that every user has access to a source when you distribute new updates or customizations.

Note:
Once the local installation source is created, its location on the user's computer is fixed. Unless the user specifies a different drive, additional Office products installed later are always added to the existing MSOCache\All Users folder.

Deploying the local installation source by itself

Because Setup performs the installation of Office from the local installation source, you can minimize the demand on the network by deploying the installation source beforehand. For example by using your usual method for running Setup on users' computers, you can distribute the local installation source to one group of users at a time. Once all users have a precached source, you can have everyone run Setup to install Office at the same time. In this scenario, most of the installation activity occurs on the local computer instead of over the network.

For more information, see Precache the local installation source for Office 2010 (*http://technet.microsoft.com/library/ff0a01a5-33d8-407c-ac52-50edccb32786(Office.14).aspx*).

You can also run Setup directly from the local installation source on the local computer. Running Setup locally means that no activity, including loading Setup files and reading metadata, occurs over the network. In this scenario, you must identify the subfolder in MSOCache\All Users that contains the core product that you want to install. Each core product subfolder contains a copy of the Setup program, and running Setup from a specific folder installs that product. This method lets users install Office without relying on a network connection.

For more information, see Run Setup from the local installation source to install Office 2010 (*http://technet.microsoft.com/library/7897ccea-d9e2-4cdf-bb63-53090da8fd0d(Office.14).aspx*).

Consolidated update process

In versions of Office earlier than the 2007 Office system, you made a number of choices to ensure that client computers received the latest Office software updates and that client computers did not become out of sync with the administrative installation point. You might have configured Setup to chain software updates with new installations of Office, or you might have applied updates to the administrative installation point and reinstalled Office on all the client computers.

The architecture introduced in the 2007 Office system makes this process much simpler. In Office 2010 (as in the 2007 Office system), you create a *network installation point* that you never have to update. Instead, a simple copy operation makes software updates available for new installations. You update existing installations independent of the network installation point so you do not have to worry about keeping client computers synchronized with the installation source.

In this section:

- Applying Office updates during new installations
- Updating existing Office installations

Applying Office updates during new installations

When you obtain Office software updates from Microsoft, copy the updates into the Updates folder in the root of the network installation point. The existing files in the network installation point remain the same as when you first copied them from the Office CD.

Note:
You can use the Updates folder to incorporate the installation of updates with an *initial installation* of the Office 2010 products. Only Windows Installer update files that are contained in this folder are installed with the initial installation. Therefore, you must extract the updates from Microsoft Self-Extractor packages. You can also place a Setup customization .msp patch in the Updates folder to customize initial installations.

When you run Setup to install Office on a client computer, Setup looks in the Updates folder for software updates and incorporates the updates automatically as it installs Office. If there are multiple updates in the folder, Setup applies only those updates that are targeted at the Office product being installed. If the Updates folder includes both a Setup customization .msp patch and product updates, Setup applies only the Setup customization .msp patch with the initial installation and the product updates are applied after the installation completes. Setup also applies the updates in the correct sequential order. The result is that the user receives the latest updates with the new installation of Office.

Tip:

To direct Setup to look for software updates in a folder other than the Updates folder, use the **SetupUpdates** element in the Config.xml file. For more information, see SetupUpdates element (*http://technet.microsoft.com/library/e16af71c-fed4-40da-a886-95e596c3999e.aspx#ElementSetupUpdates*) in Config.xml file in Office 2010 (*http://technet.microsoft.com/library/e16af71c-fed4-40da-a886-95e596c3999e(Office.14).aspx*).

Updating existing Office installations

Once Office is installed, you apply software updates directly to the client computer without returning to the network installation point. You do this through a deployment management program such as Microsoft Systems Management Server or System Center Configuration Manager 2007, by using Windows Server Update Services, or by updating computers directly from the Internet by using Microsoft Update.

Note:
After Office is installed on a client computer, reinstalling Office reapplies only those software updates that were applied with the original installation. If you copied new software updates in the Updates folder, they are not applied during the reinstallation.

See Also

Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*)

Config.xml file in Office 2010 (*http://technet.microsoft.com/library/e16af71c-fed4-40da-a886-95e596c3999e(Office.14).aspx*)

Setup command-line options for Office 2010 (*http://technet.microsoft.com/library/0f489f42-4c01-41d1-8b52-3a2a2da8f731(Office.14).aspx*)

Setup properties in Office 2010 (*http://technet.microsoft.com/library/41f07f9b-f0d0-489d-a185-d7b96f21f561(Office.14).aspx*)

Setup changes introduced in the 2007 Office system (*http://technet.microsoft.com/library/5623705c-ac5c-453c-a623-385b08b28b31(Office.14).aspx*)

Customization overview for Office 2010 (*http://technet.microsoft.com/library/72a93ebf-389a-491a-94c8-d7da02642139(Office.14).aspx*)

Plan a migration and upgrade strategy for Office 2010

This section provides information about how to plan the installation of the Microsoft Office 2010 suites, and how to migrate the user data, such as user and computers settings and documents created from the previously installed versions of Microsoft Office.

In this section:

Article	Description
Plan an upgrade to Office 2010	Describes the upgrade process for Microsoft Office 2010, including the various upgrade options and data migration paths.
Migrate user data registry keys in Office 2010	Lists the registry keys that are migrated when you use either the in-place upgrade or the uninstall-upgrade of Office 2010.
Choose an option for deploying Office 2010	Provides areas of functionality you can use to deploy Office 2010, including network share, Group Policy startup scripts, managed deployment, application virtualization, and presentation virtualization.

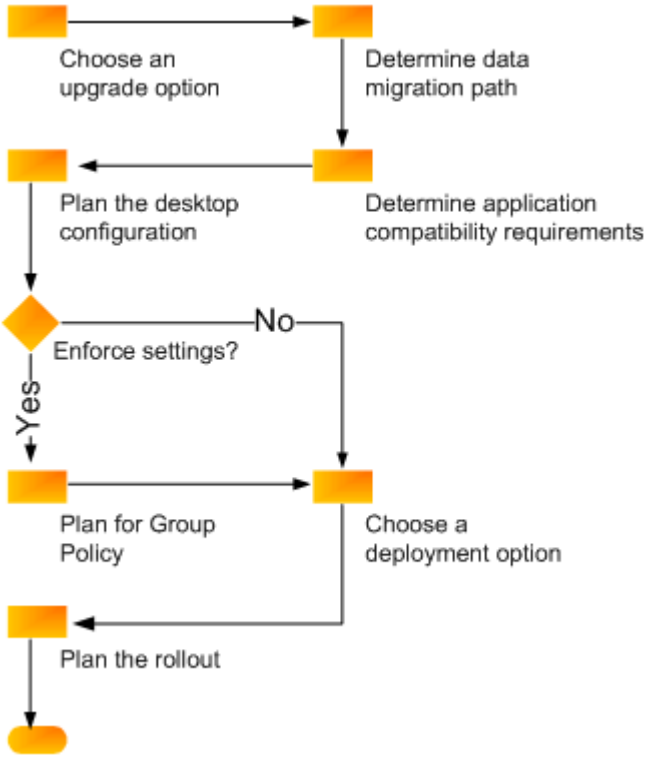
Plan an upgrade to Office 2010

This article describes the upgrade process for Microsoft Office 2010, including the various upgrade options and data migration paths.

In this article:

Overview of the upgrade process

The following diagram shows the tasks involved for planning an upgrade to Office 2010.



The process of upgrading to Office 2010 can be divided into two primary tasks:

- Install the new Microsoft Office 2010 suites.
- Migrate the user data, such as user and computers settings and documents created from the previously installed version of Microsoft Office.

When you plan an upgrade strategy, first decide on the option for upgrading to Office 2010 that is best for the organization. The upgrade type then helps determine the available choices for data migration and how data migration is performed.

Compare upgrade options and understand data migration

The options for upgrading to Office 2010 can be categorized into the following three areas:

- **In-place upgrade** The earlier version of Office, such as the 2007 Microsoft Office system, is installed on computers.
- **Uninstall upgrade** The earlier version of Office, such as the 2007 Office system, is first uninstalled before the upgrade to Office 2010.
- **New operating system upgrade** The computers get a new version of the operating system, such as Windows 7, and an upgrade to Office 2010.

The following table lists the upgrade options and how the migration of the user and computer settings data takes place.

Upgrade option	Migration of user and computer settings data
In-place upgrade	Migration performed during installation of Office 2010
Uninstall-upgrade	Migration performed during first use of each Office 2010 application
New operating system upgrade	Migration performed after the new operating system and Office 2010 are installed.

Migration of data to Office 2010 includes both the user and computer settings and the documents that were created from earlier versions of Office. For a list of the registry keys that are migrated, see Migrate user data registry keys in Office 2010.

The documents created from the previously installed version of Office remain on the computers in their current formats and can be migrated or converted, as needed, at another time if an in-place upgrade or uninstall upgrade is used. When performing a new operating system upgrade, you must move the documents from the source computers to a migration store before you install the new operating system and upgrade the computers to Office 2010.

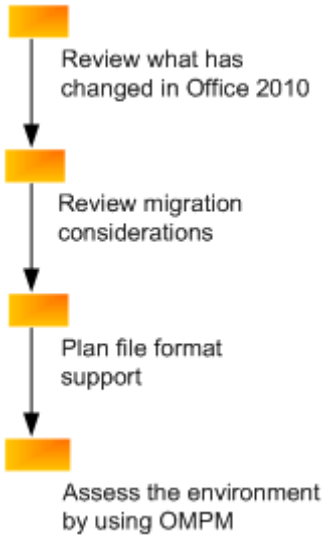
After you decide on the best option for the organization, you have to determine the best migration strategy for the documents created by using earlier versions of Office.

Important:

Migration to Office 2010 is currently not supported by using either the User State Migration Tool (USMT) version 4.0, or the Microsoft Deployment Toolkit (MDT) 2010. We recommend that you do not attempt to use either tool for your Office 2010 migration at this time. This article will be updated when a fix is available.

Migrate documents

The following diagram shows the tasks involved in planning to migrate documents to Office 2010.



These tasks are further defined in the following steps:

1. **Review what has changed** When you plan your document migration, first review changes to the Office 2010 applications that you plan to install, such as what is new, changed, or removed. For more information, see Changes in Office 2010 (*http://technet.microsoft.com/library/0dee24b3-09af-485b-b5ed-d4b879dcc8f6(Office.14).aspx*).
2. **Review migration considerations** Next, review any application-specific migration considerations. For more information, see migration considerations for each application in Product and feature changes in Office 2010 (*http://technet.microsoft.com/library/258c6715-637c-468a-9fc9-f109dc7927c5(Office.14).aspx*).
3. **Plan file format support** After you review the changes and migration considerations, determine a strategy for file format support after you upgrade to Office 2010. For more information, see FAQ: File format (*http://go.microsoft.com/fwlink/?LinkId=166107*).
4. **Assess by using OMPM** Finally, use the Office Migration Planning Manager (OMPM) to examine the files in your environment, and then and decide whether to archive them, convert them in bulk by using the Office File Converter available in OMPM, or convert them manually.

See Also

Migrate user data registry keys in Office 2010

Migrate user data registry keys in Office 2010

The registry keys for Microsoft Office 2003 and 2007 Microsoft Office system applications that are included and excluded by using either the in-place upgrade or the uninstall-upgrade option are listed in this article.

Important:
Migration to Office 2010 is currently not supported by using either the User State Migration Tool (USMT) version 4.0, or the Microsoft Deployment Toolkit (MDT) 2010. We recommend that you do not attempt to use either tool for your Office 2010 migration at this time. This article will be updated when a fix is available.

In this article:

Microsoft Office 2003 settings

Common Settings <include>

HKCU\Software\Microsoft\Office\Common* [*]
HKCU\Software\Microsoft\Office\11.0* [*]
HKCU\Software\Microsoft\Shared Tools* [*]
HKCU\Software\Microsoft\Shared Tools\Proofing Tools\Custom Dictionaries [*]
HKCU\Software\Microsoft\Office\11.0\Common\Internet* [*]
%APPDATA%\Microsoft\Office [*.acl]
%APPDATA%\Microsoft\Office\Recent [*]
%APPDATA%\Microsoft\Proof* [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{4FFB3E8B-AE75-48F2-BF13-D0D7E93FA8F9}* [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}* [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{87EF1CFE-51CA-4E6B-8C76-E576AA926888}* [*]

Common Settings <exclude>

HKCU\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries* [*]
HKCU\Software\Microsoft\Office\11.0\Shortcut Bar [LocalPath]
HKCU\Software\Microsoft\Office\11.0\Common\Internet [LocationOfComponents]
HKCU\Software\Microsoft\Office\11.0\Common\Open Find* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Internet [UseRWHlinkNavigation]
HKCU\Software\Microsoft\Office\11.0\Common\InternetServer Cache* [*]

Access 2003 <include>

HKCU\Software\Microsoft\Office\11.0\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\Access* [*]
HKCU\Software\Microsoft\Office\11.0\Access* [*]
HKCU\Software\Microsoft\Office\11.0\CMA* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings\ [Microsoft Access]
%APPDATA%\Microsoft\Office [Access11.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Access\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Access\Recent Templates* [Template*]

Access 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\Access\Settings [MRU*]

Excel 2003 <include>

HKCU\Software\Microsoft\Office\11.0\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\11.0\Excel* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings\ [Microsoft Excel]
%APPDATA%\Microsoft\Excel\ [EXCEL11.xlb]
%APPDATA%\Microsoft\Office\ [EXCEL11.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Excel\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Excel\Recent Templates* [Template*]

Excel 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\Excel\Recent Files* [*]

FrontPage 2003 <include>

HKCU\Software\Microsoft\FrontPage* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings [Microsoft FrontPage]
%APPDATA%\Microsoft\FrontPage\State [CmdUI.PRF]
%APPDATA%\Microsoft\Office [fp11.pip]
%APPDATA%\Microsoft\FrontPage\Snippets [FPSnippetsCustom.xml]

FrontPage 2003 <exclude>

HKCU\Software\Microsoft\FrontPage [WecErrorLog]
HKCU\Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent File List* [*]
HKCU\Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent Web List* [*]

OneNote 2003 <include>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Common\LanguageResources [SKULanguage]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\OneNote* [*]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings\ [Microsoft Office OneNote]
%APPDATA%\Microsoft\Office\ [OneNot11.pip]
%APPDATA%\Microsoft\OneNote\ [Preferences.dat]
%APPDATA%\Microsoft\OneNote\ [Toolbars.dat]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\Recent Templates* [Template*]

OneNote 2003 <exclude>

HKCU\software\Microsoft\Office\%OFFICEVERSION%\OneNote\Options\Save\ [BackupLastAutoBackupTime]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\OneNote\Options\Save\ [BackupFolderPath]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\OneNote\General\ [LastCurrentFolderForBoot]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\OneNote\General\ [Last Current Folder]

Outlook 2003 <include>

HKCU\Software\Microsoft\Office\11.0\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\Outlook* [*]
HKCU\Software\Microsoft\Office\11.0\Outlook* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings [Microsoft Outlook]
HKCU\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts* [*]
HKCU\Software\Microsoft\Office\11.0\Outlook\Journal* [*]
%APPDATA%\Microsoft\Signatures* [*]
%CSIDL_LOCAL_APPDATA%\Microsoft\FORMS [frmcache.dat]
%APPDATA%\Microsoft\Outlook [outcmd11.dat]
%APPDATA%\Microsoft\Outlook [outcmd.dat]
%APPDATA%\Microsoft\Outlook [views.dat]
%APPDATA%\Microsoft\Outlook [OutlPrint]
%APPDATA%\Microsoft\Office [MSOut11.pip]
%APPDATA%\Microsoft\Outlook [*.rwz]
%APPDATA%\Microsoft\Outlook [*.srs]
%APPDATA%\Microsoft\Outlook [*.NK2]
%APPDATA%\Microsoft\Outlook [*.xml]
HKCU\Software\Microsoft\Exchange* [*]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [001e023d]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [001f023d]

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [*]

Outlook 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\Outlook [FirstRunDialog]
HKCU\Software\Microsoft\Office\11.0\Outlook [Machine Name]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles*\0a0d020000000000c000000000000046 [111f031e]
HKCU\Identities* [LDAP Server]
HKCU\Software\Microsoft\Internet Account Manager\Accounts* [LDAP Server]
HKCU\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts* [LDAP Server]

PowerPoint 2003 <include>

HKCU\Software\Microsoft\Office\11.0\PowerPoint* [*]
HKCU\Software\Microsoft\Office\11.0\PowerPoint\RecentFolderList [Default]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings [Microsoft PowerPoint]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\PowerPoint\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\PowerPoint\Recent Templates* [Template*]

PowerPoint 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\PowerPoint\Recent File List* [*]
HKCU\Software\Microsoft\Office\11.0\PowerPoint\RecentFolderList* [*]

Project 2003 <include>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings [Microsoft Project]
%APPDATA%\Microsoft\Office [MSProj11.pip]
%APPDATA%\Microsoft\MS Project\11* [*]

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent Templates* [Template*]

Project 2003 <exclude>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent File List [*]

Publisher 2003 <include>

HKCU\Software\Microsoft\Office\11.0\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\11.0\Publisher* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings [Microsoft Publisher]
%APPDATA%\Microsoft\Office [*.acl]
%APPDATA%\Microsoft\Publisher [pubcmd.dat]
%APPDATA%\Microsoft\Office\ [*.jsp]

Publisher 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\Publisher\Recent File List* [*]

Visio 2003 <include>

HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio* [*]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings\ [Microsoft Office Visio]
CSIDL_APPDATA\Microsoft\Office\[Visio11.pip]
CSIDL_LOCAL_APPDATA\Microsoft\Visio\ [content.dat]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Visio\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Visio\Recent Templates* [Template*]

Visio 2003 <exclude>

HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [LastFile*]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [MyShapesPath]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [UserDictionaryPath1]

Word 2003 <include>

HKCU\Software\Microsoft\Office\11.0\Common\LanguageResources [SKULanguage]
HKCU\Software\Microsoft\Office\11.0\Word* [*]
HKCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings [Microsoft Word]
%APPDATA%\Microsoft\Templates [Normal.dot]
%APPDATA%\Microsoft\Office [Word11.pip]
%APPDATA%\Microsoft\Office [WordMa11.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Word\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Word\Recent Templates* [Template*]

Word 2003 <exclude>

HKCU\Software\Microsoft\Office\11.0\Word\Options [PROGRAMDIR]

Microsoft Office 2007 settings

Common Settings <include>

HKCU\Software\Microsoft\Office\Common* [*]
HKCU\Software\Microsoft\Office\12.0\Common* [*]
HKCU\Software\Microsoft\Shared Tools* [*]
%APPDATA%\Microsoft\Office [*.acl]
%APPDATA%\Microsoft\Office\Recent [*]
%APPDATA%\Microsoft\Templates* [*]
%APPDATA%\Microsoft\Proof* [*]

%APPDATA%\Microsoft\UProof* [*]
HKCU\Software\Microsoft\Shared Tools\Proofing Tools*\Custom Dictionaries [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{4FFB3E8B-AE75-48F2-BF13-D0D7E93FA8F9}* [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}* [*]
HKCU\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{87EF1CFE-51CA-4E6B-8C76-E576AA926888}* [*]

Common Settings <exclude>

HKCU\Software\Microsoft\Office\12.0\Shortcut Bar [LocalPath]
HKCU\Software\Microsoft\Office\12.0\Common\Internet [LocationOfComponents]
HKCU\Software\Microsoft\Office\12.0\Common\Open Find* [*]
HKCU\Software\Microsoft\VBA\6.0\Common
%CSIDL_LOCAL_APPDATA%\Microsoft\Office [*.qat]

Access 2007 <include>

%APPDATA%\Microsoft\Office [Access11.pip]
HKCU\Software\Microsoft\Office\Access* [*]
HKCU\Software\Microsoft\Office\12.0\Access* [*]
HKCU\Software\Microsoft\Office\12.0\CMA* [*]
HKCU\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\ [Microsoft Access]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Access\File MRU* [*]

Access 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\Access\Settings [MRU*]

Excel 2007 <include>

HKCU\Software\Microsoft\Office\12.0\Excel* [*]
HKCU\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\ [Microsoft Excel]
%APPDATA%\Microsoft\Excel\ [EXCEL11.xlb]
%APPDATA%\Microsoft\Office\ [EXCEL11.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Excel\File MRU* [*]

Excel 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\Excel\Recent Files* [*]

OneNote 2007 <include>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings\ [Microsoft Office OneNote]
%APPDATA%\Microsoft\Office\ [OneNot12.pip]
%APPDATA%\Microsoft\OneNote\%OFFICEVERSION%\ [Preferences.dat]
%APPDATA%\Microsoft\OneNote\%OFFICEVERSION%\ [Toolbars.dat]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\Recent Templates* [*]
%APPDATA%\Microsoft\MS Project\12* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\Recent Templates* [Template*]

OneNote 2007 <exclude>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\General\ [LastMyDocumentsPathUsed]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\OneNote\Options\Paths\ [BackupFolderPath]

Outlook 2007 <include>

HKCU\Software\Microsoft\Office\Outlook* [*]
HKCU\Software\Microsoft\Office\12.0\Outlook* [*]

HKCU\Software\Microsoft\Office\12.0\Common\Toolbars\Settings [Microsoft Outlook]
HKCU\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts* [*]
%APPDATA%\Microsoft\Signatures* [*]
%CSIDL_LOCAL_APPDATA%\Microsoft\FORMS [frmcache.dat]
%APPDATA%\Microsoft\Outlook [outcmd11.dat]
%APPDATA%\Microsoft\Outlook [outcmd.dat]
%APPDATA%\Microsoft\Outlook [views.dat]
%APPDATA%\Microsoft\Outlook [OutlPrint]
%APPDATA%\Microsoft\Office [MSOut11.pip]
HKCU\Software\Microsoft\Exchange* [*]
%APPDATA%\Microsoft\Outlook [*.rwz]
%APPDATA%\Microsoft\Outlook [*.srs]
%APPDATA%\Microsoft\Outlook [*.NK2]
%APPDATA%\Microsoft\Outlook [*.xml]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [*]
HKCU\Software\Microsoft\Office\12.0\Outlook\Journal* [*]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [001e023d]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles* [001f023d]

Outlook 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\Outlook [FirstRunDialog]
HKCU\Software\Microsoft\Office\12.0\Outlook [Machine Name]
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles*\0a0d020000000000c000000000000046 [111f031e]
HKCU\Identities* [LDAP Server]
HKCU\Software\Microsoft\Internet Account Manager\Accounts* [LDAP Server]
HKCU\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts* [LDAP Server]

PowerPoint 2007 <include>

HKCU\Software\Microsoft\Office\12.0\PowerPoint* [*]
HKCU\Software\Microsoft\Office\12.0\PowerPoint\RecentFolderList [Default]
HKCU\Software\Microsoft\Office\12.0\Common\Toolbars\Settings [Microsoft PowerPoint]
%APPDATA%\Microsoft\PowerPoint [PPT11.pcb]
%APPDATA%\Microsoft\Office [PowerP11.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\PowerPoint\File MRU* [*]

PowerPoint 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\PowerPoint\Recent File List* [*]
HKCU\Software\Microsoft\Office\12.0\PowerPoint\RecentFolderList* [*]

Project 2007 <include>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings [Microsoft Office Project]
%APPDATA%\Microsoft\Office [MSProj12.pip]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent Templates* [Template*]

Project 2007 <exclude>

HKCU\Software\Microsoft\Office\%OFFICEVERSION%\MS Project\Recent File List [*]

Publisher 2007 <include>

HKCU\Software\Microsoft\Office\12.0\Publisher* [*]
HKCU\Software\Microsoft\Office\12.0\Common\Toolbars\Settings [Microsoft Publisher]
%APPDATA%\Microsoft\Office [*.acl]

%APPDATA%\Microsoft\Publisher [pubcmd.dat]
%APPDATA%\Microsoft\Office [Publis11.pip]
%APPDATA%\Microsoft\Office\ [*.jsp]

Publisher 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\Publisher\Recent File List* [*]

Visio 2007 <include>

HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio* [*]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Common\Toolbars\Settings\ [Microsoft Office Visio]
%APPDATA%\Microsoft\Office\ [Visio12.pip]
%CSIDL_LOCAL_APPDATA%\Microsoft\Visio\ [content.dat]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Visio\Recent Templates* [*]
HKCU\Software\Microsoft\Office\%OFFICEVERSION%\Visio\Recent Templates* [Template*]

Visio 2007 <exclude>

HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [LastFile*]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [MyShapesPath]
HKCU\software\Microsoft\Office\%OFFICEVERSION%\Visio\Application\ [UserDictionaryPath1]

Word 2007 <include>

HKCU\Software\Microsoft\Office\12.0\Word* [*]
%APPDATA%\Microsoft\Templates* [*]
%APPDATA%\Microsoft\QuickStyles* [*]
%APPDATA%\Microsoft\Document Building Blocks* [*]
%APPDATA%\Microsoft\Bibliography* [*]
%APPDATA%\Microsoft\Office [Word11.pip]
%APPDATA%\Microsoft\Office [WordMa11.pip]

Word 2007 <exclude>

HKCU\Software\Microsoft\Office\12.0\Word\Data [PROGRAMDIR]
HKCU\Software\Microsoft\Office\12.0\Word\Options [PROGRAMDIR]

Choose an option for deploying Office 2010

You can use five areas of functionality to deploy Microsoft Office 2010: network share, Group Policy startup scripts, managed deployment, application virtualization, and presentation virtualization. You can use any of these options or a combination of them, such as the managed deployment option to deploy and manage virtual Office 2010 applications. We do not support Office 2010 deployment by means of Group Policy Software Installation (GPSI). A workable alternative to GPSI is to assign computer startup scripts. This article describes each of the deployment options.

For a visual representation of the deployment options, see Deployment Options for Microsoft Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=168621*), which includes diagrams, descriptions, advantages, limitations, recommendations, and tools.

Deployment options

Determine which of the following deployment options works best for your organization.

Network share

A simple way to deploy Office 2010 is to create a network installation point and copy the contents of the Microsoft Office CD onto the network share. Make sure that the network share is accessible by the targeted resources: users/computers.

Group Policy startup scripts

Administrators can use Group Policy to assign computer startup scripts to deploy Office 2010. A script can be written in any language that is supported by the client computer. Windows Script Host-supported languages, such as Microsoft Visual Basic Scripting Editing (VBScript) and JScript, and command files are the most common.

Managed deployment

Administrators can use change and configuration management software, such as Microsoft System Center Essentials and Microsoft System Center Configuration Manager, to deploy Office 2010 applications. The choice of System Center Essentials or Configuration Manager depends in part on the size of your organization.

Applicationvirtualization

Administrators can use Microsoft Application Virtualization (App-V) as part of a deployment option to allow users to run Office 2010 applications on their desktops. Microsoft Application Virtualization streams applications on demand to the desktop, from which the application is run. However, the application is not installed on the desktop.

Presentationvirtualization

Administrators can use Windows Server 2008 Terminal Services as a deployment option to allow users to operate the Office 2010 applications from their workstations. Terminal Services is run on a shared server and presents the application user interface on a remote system, such as a local workstation. Microsoft Application Virtualization for Terminal Services allows for the optimization of the Office 2010 application through the sequencing process of application virtualization and then uses Terminal Services to deliver the application as a presentation virtualization.

Plan desktop configurations for Office 2010

This section provides information and guidelines about items to consider before you deploy Microsoft Office 2010.

In this section:

Article	Description
Plan for OneNote 2010	Describes how to plan a deployment of Microsoft OneNote 2010.
Plan for Outlook 2010	Guides you through the things to consider when you deploy Microsoft Outlook 2010.
Plan for spelling checker settings in Office 2010	Describes how to use either Group Policy or the Office Customization Tool (OCT) to manage the behavior of spelling checker in Office 2010.
Plan for SharePoint Workspace 2010	Describes how to plan a deployment of Microsoft SharePoint Workspace 2010.
Plan customizations and options for Visio 2010	Describes some of the customizations and options that are available in Microsoft Visio 2010.
Plan security for Office 2010	Describes several new security controls in Office 2010 that help you plan a robust defense against threats while maintaining information worker productivity.
Plan Group Policy for Office 2010	Provides information about how to use Group Policy to configure and enforce settings for Office 2010 applications.
Plan for multilanguage deployment of Office 2010	Discusses planning considerations for deploying Office 2010 with multiple languages.
Plan for virtualization for Office 2010	Describes what virtualization is, how you can use virtualization in your organization, and which method and type is best for your environment.
Plan for Remote Desktop Services (Terminal Services)	Provides information about how to plan the deployment of Office 2010 by using Remote Desktop Services (Terminal Services).

Article	Description
Plan for accessibility in Office 2010	Provides an overview of the Microsoft Office Accessibility Checker, which can make Office 2010 products more accessible to users who have disabilities.

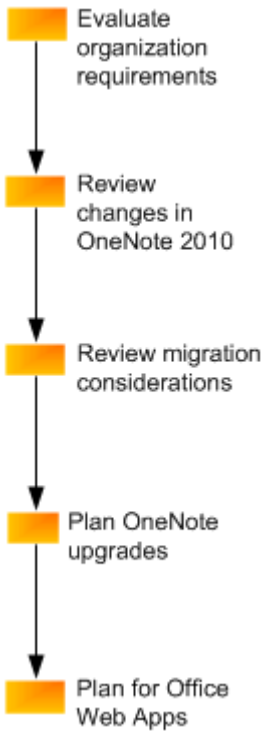
Plan for OneNote 2010

This article provides information about the planning process for deploying Microsoft OneNote 2010.

In this article:

Planning overview

The following figure summarizes the planning steps for deploying OneNote 2010 in the enterprise.



Evaluate your organization’s requirements

The planning process typically begins with an evaluation of your current environment to help determine your organization’s requirements. Issues to consider include the following:

- Ensuring that computers meet the system requirements for Microsoft Office 2010.
- Whether you are upgrading from an earlier version of the product.
- Migration considerations, such as file formats and user data settings migration.
- Security considerations, such as whether to prevent users from sharing documents across the Internet.
- Multilanguage requirements.

System requirements for OneNote 2010

Information about system requirements for OneNote 2010 is available in Microsoft OneNote 2010 in System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).

For information about the tools that are available to help you assess hardware and software in your environment, see Assessment tools for Office 2010 (*http://technet.microsoft.com/library/b0dffc14-da76-4588-a40c-35ef734937a7(Office.14).aspx*).

Upgrading to OneNote 2010

If you are performing an upgrade from an earlier version of Microsoft OneNote, see Plan OneNote upgrades later in this article for information about the new file format in OneNote 2010 and recommendations for upgrades from Microsoft Office OneNote 2007 and OneNote 2003.

Security considerations

To help you plan for Office 2010 application security in your organization, you will find information about security threats and the new security controls that are available in Office 2010 in these articles: Security overview for Office 2010, Understand security threats and countermeasures for Office 2010, and Plan security for Office 2010.

Multilanguage requirements

The Office 2010 language-neutral architecture simplifies deployment in multiple languages. An Office 2010 product, such as Microsoft Office Professional Plus 2010, consists of a language-neutral core package plus one or more language-specific packages. For information about how to deploy Office 2010 applications in multiple languages, see Plan for multilanguage deployment of Office 2010, and Customize language setup and settings for Office 2010 (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d(Office.14).aspx*).

Review changes in OneNote 2010

As part of planning for OneNote 2010, you should review the changes in the current release. For a description of what is new, what is changed, and what is removed in OneNote 2010, see Changes in OneNote 2010 (*http://technet.microsoft.com/library/8f57bbaa-c01b-42f8-a6f2-cc92e449d1c2(Office.14).aspx*).

Review migration considerations

The next step in the planning process is to review migration considerations for users who are migrating from previous versions of OneNote to OneNote 2010. For information about the issues to consider, see Migration considerations (*http://technet.microsoft.com/library/8f57bbaa-c01b-42f8-a6f2-cc92e449d1c2.aspx#BKMK_Migration*) in Changes in OneNote 2010 (*http://technet.microsoft.com/library/8f57bbaa-c01b-42f8-a6f2-cc92e449d1c2(Office.14).aspx*).

Plan OneNote upgrades

OneNote 2010 uses a new file format for saving files than in previous versions of the product, and many of the new OneNote 2010 features (such as math equations, versioning, linked note taking, and multilevel subpages) require the new format. The new file format lets you share your notebooks on the Web, so that you can use a Web browser to view and edit your notebook files. By default, new OneNote 2010 notebooks that you create are saved in the new file format.

The following sections provide information about upgrading from earlier versions of the product.

Upgrading from OneNote 2007

OneNote 2010 lets you view, open, and edit notebooks that are saved in the Microsoft Office OneNote 2007 file format. You can convert Office OneNote 2007 notebooks to OneNote 2010, and you can also convert them back to the Office OneNote 2007 format.

By default, existing Office OneNote 2007 notebooks are not automatically converted when you update from Office OneNote 2007 to OneNote 2010. Note that you cannot use Office OneNote 2007 to open and use notebooks that are saved in the OneNote 2010 file format.

One issue to consider is whether you need to share your notebooks with Office OneNote 2007 users. The recommendations for addressing this issue are as follows:

- If you plan to share notebooks with Office OneNote 2007 users who do not have OneNote 2010 installed, we recommend that you do not upgrade those notebooks.
- If you do not need to share notebooks with users of earlier versions of OneNote, we recommend that you convert existing notebooks to the OneNote 2010 format. This enables all of the new product features.

If you open an Office OneNote 2007 notebook, the application title bar displays "**[Compatibility Mode]**" to indicate that the file format is Office OneNote 2007.

To change the format of a notebook, right-click the notebook on the navigation bar, and then select **Properties**. In the **Notebook Properties** dialog, you can change the notebook format from Office OneNote 2007 to OneNote 2010, and you can also convert it back to the Office OneNote 2007 format.

Upgrading from OneNote 2003

OneNote 2003 notebooks are read-only in OneNote 2010 (and in Office OneNote 2007). This means that you cannot edit files that use the OneNote 2003 format in OneNote 2010 or in Office OneNote 2007.

To be able to continue to edit your OneNote 2003 notes when you upgrade from OneNote 2003 to OneNote 2010, you must upgrade your notebook to the OneNote 2010 format or the Office OneNote 2007 format. To do this, open the notebook in OneNote 2010, and then click the Information Bar that appears at the top of every page in your OneNote 2003 notebook.

OneNote 2003 notebooks that are converted to either the OneNote 2010 or the Office OneNote 2007 format cannot be changed back. Therefore, we recommend that you make a backup copy of the notebooks before you convert the files to a newer format.

Plan for OneNote Web App

Microsoft OneNote Web App is an online companion to OneNote 2010 that enables you to access and do light editing or sharing of OneNote notebooks from almost anywhere. By using OneNote Web App, you can access and edit notebooks from a Web browser, even on computers on which the full version of OneNote is not installed. Users can view, share, and work on documents with other users online across personal computers, mobile phones, and the Web.

Microsoft Office Web Apps are available to users through Windows Live and to business customers who have Office 2010 volume licensing and document management solutions that are based on Microsoft SharePoint 2010 Products. Business customers can run Office Web Apps installed on a server that is running Microsoft SharePoint Server 2010 or Microsoft SharePoint Foundation 2010. In enterprise environments, running Office Web Apps on servers that are running SharePoint 2010 Products enables better administrative control of the organization's data.

This section provides information about system requirements, and links to resources for downloading, deploying, and using Microsoft Office Web Apps.

We recommend that you read the following articles about Office Web Apps deployment if you plan to deploy OneNote Web App in your environment: Understanding Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185473*), Planning Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185475*), and Deploy Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185483*).

In this section:

- System requirements for Office Web Apps
- Resources for deploying and using Office Web Apps

System requirements for Office Web Apps

The following table lists the system requirements for Office Web Apps.

System requirements	Details
Supported operating systems	Windows Server 2008 Windows Server 2008 R2 and Windows Server 2008 with Service Pack 2 (SP2)
Hardware	Processor: 64-bit; dual processor; 3 GHz RAM: 4 GB for stand-alone; 8 GB for farm Hard disk: 80 GB
Software	SharePoint Foundation 2010 -or- SharePoint Server 2010
Browser support	Internet Explorer 7.0 or later on Windows Safari 4.0 or later on Mac Firefox 3.5 or later on Windows, Mac, and Linux

Resources for deploying and using Office Web Apps

The following table lists resources for download information and documentation to help you plan, deploy, and use Office Web Apps and OneNote Web App in your organization.

Resource	Description
Microsoft Office Web Apps (Beta) (*http://go.microsoft.com/fwlink/?LinkId=183997*)	Download for Office Web Apps.
Understanding Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185473*)	Information to help you understand an Office Web Apps on-premises solution and how it can benefit users in your organization.
Planning Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185475*)	Information to help you plan an Office Web Apps on-premises solution in your organization.
Deploy Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185483*)	Information to help you deploy Office Web Apps in your organization.

Resource	Description
Manage Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185498*)	Information to help you manage Office Web Apps in your organization.

Considerations for using OneNote with SharePoint products

This section summarizes the key issues that you need to consider when you use OneNote 2010 with SharePoint 2010 Products.

Turn off Require Check Out

Co-authoring allows multiple users to collaborate on the same document at any time, without interfering with each other's changes or locking out other users. When you set up and manage co-authoring, you need to consider the following:

Check Out When a user checks out a document from a SharePoint Server 2010 library for editing, this locks the document for editing to that user only, which prevents co-authoring. The **Require Check Out** setting should not be enabled in document libraries where co-authoring will be used. By default, **Require Check Out** is not enabled in SharePoint Server 2010. Users should not check out documents manually when co-authoring is being used.

Versioning

Unlike Microsoft Word 2010 and Microsoft PowerPoint 2010, OneNote 2010 stores version information within the OneNote file itself. For this reason, administrators should follow these recommended practices when storing OneNote notebooks in a SharePoint Server 2010 document library:

- Do not enable minor versioning. This is the default setting in SharePoint Server 2010.
- If major versioning is enabled, we recommend that you set a reasonable maximum number of versions to store. The complete version history of the file is stored in each major version that SharePoint creates, which can result in sub-optimal storage efficiency. If you want to enable major versions, we recommend that you select the **Keep the following number of major versions** setting. This prevents an unbounded number of versions from being created because of prolonged editing of the file, which could exceed the site storage quota. By default, major versioning is not enabled in SharePoint Server 2010.

For more information about how to plan for version control and check-out, see Versioning, content approval, and check-out planning (SharePoint Server 2010) (*http://go.microsoft.com/fwlink/?LinkId=186210*).

Mixed Environment with Microsoft Office OneNote 2007

OneNote 2010 is compatible with the Office OneNote 2007 file format and supports co-authoring with Office OneNote 2007 users. In mixed environments, notebooks must be saved in the Office OneNote 2007 file format so that Office OneNote 2007 and OneNote 2010 users can work together on the notebook. By upgrading to the OneNote 2010 file format, however, users gain a number of key features, including compatibility with the OneNote Web App which allows users without the full version of OneNote installed to edit and co-author notebooks.

OneNote 2010 includes the ability to upgrade Office OneNote 2007 files to OneNote 2010 files at any time, providing an easy upgrade path for organizations that are moving from a mixed environment to a unified environment on Office 2010.

See Also

Changes in OneNote 2010 (*http://technet.microsoft.com/library/8f57bbaa-c01b-42f8-a6f2-cc92e449d1c2(Office.14).aspx*)

Changes in Office 2010 (*http://technet.microsoft.com/library/0dee24b3-09af-485b-b5ed-d4b879dcc8f6(Office.14).aspx*)

Deploy Office Web Apps (Installed on SharePoint 2010 Products) (*http://go.microsoft.com/fwlink/?LinkId=185483*)

Microsoft OneNote 2010 Beta Help blog (*http://go.microsoft.com/fwlink/?LinkId=167111*)

Plan for Outlook 2010

An organization's messaging environment helps shape the Microsoft Outlook 2010 deployment. This section provides information about planning to deploy Outlook 2010 and factors to consider when you upgrade, install the application for the first time, plan for roaming or remote users, decide when to install, and plan for security.

In this section:

Article	Description
Planning overview for Outlook 2010	Provides an overview of the planning process and guides you through the factors to consider when you plan the deployment of Outlook 2010.
Determine when to install Outlook 2010	Describes the requirements, advantages, and disadvantages of various strategies you can use in the deployment of Outlook 2010.
Determine which features to enable or customize in Outlook 2010	Provides an initial list of some of the Microsoft Outlook features that you might need to configure and deploy with Microsoft Outlook 2010.
Plan an Exchange deployment in Outlook 2010	Provides information to consider when you plan a Cached Exchange Mode deployment of Outlook 2010.
Plan to automatically configure user accounts in Outlook 2010	Describes the two discovery mechanisms to automatically configure user accounts in Outlook 2010: Autodiscover and Common Settings Discover.
Plan for compliance and archiving in Outlook 2010	Discusses the planning considerations to deploy Retention Policy and Personal Archive features with Outlook 2010 and Microsoft Exchange Server 2010.
Plan for security and protection in Outlook 2010	Describes features in Outlook 2010 that can help keep an organization’s e-mail messaging secure.

Planning overview for Outlook 2010

A close review of the organization's messaging requirements will help you plan the optimal Microsoft Outlook 2010 deployment. This article guides you through the things to consider when you deploy Outlook 2010.

In this article:

Determining an organization’s needs

The organization's messaging environment helps shape the Outlook 2010 deployment. Factors to consider include whether you are upgrading Outlook, installing the application for the first time, planning for roaming or remote users, or choosing a combination of these and other factors.

Upgrade or initial installation

If you are upgrading to Outlook 2010 from an earlier version of Microsoft Outlook, consider whether you will migrate previous settings, modify user profiles, and use new customization options. The Office Customization Tool (OCT) enables you to migrate users' current settings and make other customizations, such as define new Microsoft Exchange servers or customize new features. User settings are migrated automatically by default, except for security settings.

If you are deploying Outlook on client computers for the first time, each user needs an Outlook profile to store information about e-mail messaging server connections and other important Outlook settings. You use the OCT or deploy an Outlook Profile (.prf) file to define profile settings for users.

Migrating data

If the organization uses a different mail client, you might have to migrate data from those clients to Outlook 2010. The importers that are provided in Outlook (for example, for Eudora Light) might be helpful. Importers cannot be configured to run automatically. You use importers to migrate data for individual users.

Remote and roaming users

You can customize Outlook to optimize the experience for remote and roaming users, and to set up Outlook for multiple users on the same computer.

You might want to configure features such as Outlook Anywhere (known as RPC over HTTP in earlier versions of Outlook) and Cached Exchange Mode for remote users. These features enhance the user experience when Outlook is used over slower or less reliable connections. By using Outlook Anywhere, you can configure connections that enable users to connect more securely from the Internet to Exchange servers in your organization without using a virtual private network (VPN) connection. Cached Exchange Mode is an Outlook feature that was introduced with Office Outlook 2003 that creates a local copy of users' mailboxes. Cached Exchange Mode is recommended for all configurations, but especially benefits remote users. The feature enables users to have more reliable access to their Outlook data, whether or not they are connected to a network.

When multiple users share the same computer, use Windows logon features on the computer's operating system to manage user logon verification. Unless you deploy application virtualization, users must use the same version of Outlook because only one version of Outlook can be installed on the same computer. To learn more about how to set up multiple Outlook users on the same computer, see Using Outlook on a computer you share with other people (*http://go.microsoft.com/fwlink/?LinkId=100528*).

Multilingual requirements

Microsoft Office 2010 provides broad support to deploy in international or multilingual environments. As with the 2007 Microsoft Office system, the Office 2010 product consists of the language-neutral core package plus one or more language-specific packages. In addition to the proofing tools included in each language version, you can download and deploy proofing tools for other languages to help multilingual groups work with and edit files in many languages.

Outlook 2010 supports Unicode throughout the product to help multilingual organizations seamlessly exchange messages and other information in a multilingual environment.

Client and messaging server platforms

Some features of Outlook 2010 (for example, Cached Exchange Mode) require Microsoft Exchange Server as a messaging platform. Although Outlook 2010 works well with earlier versions of Exchange, some features of Outlook 2010 require specific versions of Exchange. Because of this and other improved integration with Exchange throughout Outlook 2010, we recommend that you combine Outlook 2010 with the latest version of Exchange.

Deployment customization decisions for Outlook 2010 depend on which version of Exchange Server you use. If you currently use Exchange Server as your messaging server and you have not upgraded to Exchange 2003 or a later version, consider coordinating the Exchange Server upgrade with the deployment timing for Outlook 2010. Exchange Server 2003 is the earliest version of Exchange Server that can be used with Outlook 2010.

Choosing when and how to install Outlook

You have options for when and how you install Outlook 2010. For example, consider whether it would be best for the organization to do the following:

- Install or upgrade Outlook for different groups of users in stages, or at the same time.
- Install Outlook as a stand-alone application.
- Install Outlook before, during, or after Office 2010 installation.

Each organization has a different environment and might make different choices about timing Outlook 2010 upgrades. For example, you might have a messaging group that is responsible for upgrading Outlook and a separate group that plans deployment for other Microsoft Office applications. In this case, it might be easier to upgrade Outlook separately from the rest of Office, instead of to attempt to coordinate deployment between the two groups.

Note that Outlook 2010 cannot coexist with previous versions of Outlook on the same computer. If you have to use previous versions, do not install Outlook 2010 or deploy Outlook 2010 with application virtualization. For more information, see Determine when to install Outlook 2010.

Customizing Outlook settings and profiles

You can customize an Outlook installation to handle Outlook user settings and profiles in two ways:

- Specify Outlook user settings in the OCT.
- Specify options for managing new and existing Outlook profiles in the OCT or use an Outlook Profile file (.prf).

For example, you can enable Outlook users to migrate their current profiles and settings while default profiles and settings are defined for new Outlook users. You can also modify existing profiles and establish new default profiles for new Outlook users. If you deploy Outlook 2010 with Microsoft Exchange Server 2010, you can add more than one Exchange account for a profile by using the OCT or .prf file.

When you use the OCT to customize Outlook, you save choices and other installation preferences in the customization file that is applied during Setup. Later, you update settings and profile information by opening the file in the OCT and saving a new copy of the file.

For more information about how to configure Outlook profiles, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

Important

- There is a known issue in which an additional Exchange account is added to the Outlook profile when a user who already has an exchange account in the profile is upgraded from Outlook 2003 or Outlook 2007. This issue can occur while you are upgrading Outlook and applying customizations by using a custom OCT file (.msp) or .prf file that is configured to “Modify Profile" and "Define changes to make to the existing default profile.”

- To prevent multiple Exchange accounts from being created in one profile when you upgrade users to Outlook 2010, you must create a .prf file and set the properties BackupProfile=False and UniqueService=Yes. For the steps to do this, see Multiple Exchange accounts created in Outlook 2010 with existing Outlook profiles after upgrading from an earlier Office version using a custom MSP (*http://go.microsoft.com/fwlink/?LinkId=199704*).

Configuring subscriptions and other sharing features

As with Office Outlook 2007, Outlook 2010 includes features that let you easily subscribe to new sources of content and share the features with users inside and outside your organization. Content sources include Microsoft SharePoint Foundation 2010 and SharePoint Foundation 2010 contacts, tasks, and calendars, together with local and Internet-based calendars (iCals).

Really Simple Syndication (RSS) is another sharing feature that enables users to subscribe to internal or Internet-based sources of syndicated content (.xml files) to avoid having to check a site for new information. You can deploy specific RSS feeds or calendar subscriptions to users, configure settings to manage how users can share these subscriptions or content, specify how often the servers update users' copies of the data, and more.

Using Outlook with Remote Desktop Services (Terminal Services)

Remote Desktop Services in Windows Server enables you to install a single volume licensed copy of Outlook 2010 on a Remote Desktop Services-enabled computer. Instead of having Outlook run on local computers, multiple users connect to the server and run Outlook from that server.

To achieve optimal results when you use Outlook with Remote Desktop Services, pay attention to how you customize your Outlook configuration. For example, in Outlook 2010 you can configure Cached Exchange Mode with Remote Desktop Services. However, you will have to provide sufficient disk space to accommodate each user’s mailbox on the Remote Desktop Session Host server computer (terminal server). Note that Outlook might be part of an environment that includes other applications that are provided on the same Remote Desktop Session Host computer.

Collaboration Data Objects dependencies

Collaboration Data Objects (CDO) is not supported in Outlook 2010. Although some solutions that depend on CDO 1.2.1 might continue to run, CDO 1.2.1 is not designed for a multiple Exchange account environment and unexpected results can occur. For Outlook solutions, use the Outlook object model instead of CDO 1.2.1.

AutoArchive

Outlook mailboxes grow as users create and receive items. To keep mailboxes manageable, users need another place to store — or archive — older items that are important but not frequently used. It is typically most convenient to automatically move these older items to the archive folder and to discard items whose content has expired and is no longer valid. Outlook 2010 AutoArchive can manage this

process automatically for users. However, we recommend that you use the Personal Archive feature in Microsoft Exchange Server 2010 Messaging Records Management (MRM) because it eliminates the need for Personal Folder files (.pst). By using Personal Archive in Exchange Server 2010, the e-mail archive folders are stored online so that users can access the archived files by using Microsoft Outlook Web App or from a secondary computer by using Outlook 2010. By using either of these client applications, users can view an archive mailbox and move or copy messages between their primary mailboxes and the archive. If you plan to deploy Outlook 2010 with Exchange Server 2010, consider using the Exchange Server 2010 Personal Archive feature instead of Outlook 2010 AutoArchive. For more information, see Understanding Personal Archive: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=169269*).

If you choose to use the AutoArchive feature in Outlook 2010, you can configure the settings to customize Outlook 2010 AutoArchive by using the Outlook Group Policy template (Outlk14.adm). Or you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the settings.

Outlook data files (.pst)

If you plan to deploy Outlook 2010 with Exchange Server 2010, we recommend that you use the Personal Archive feature in Exchange Server 2010 Messaging Records Management (MRM) because it eliminates the need for Outlook data files (.pst). By using the Personal Archive in Exchange Server 2010, the e-mail archive is stored online so that users can access the archived files by using Microsoft Outlook Web App or from a secondary computer by using Outlook 2010. By using either of these client applications, users can view an archive mailbox and move or copy messages between their primary mailboxes and the archive. For more information, see Understanding Personal Archive: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=169269*).

If you plan to deploy Outlook 2010 with Exchange Server 2003 or Exchange Server 2007, you can configure .pst files to be stored locally (recommended) or on a network share. Only consider storing .pst files on a network share if the network has high bandwidth and reliability. If a user's .pst file is stored on a network share and the user loses the connection to the network, the user's Outlook experience could be degraded and unsaved changes might be lost.

Retention policies

Retention policy settings can help users follow retention policy guidelines that your organization establishes for document retention. With Outlook 2010, you cannot deploy AutoArchive-based retention settings through Outlook 2010 by using Group Policy. If you need to deploy retention policies, explore the Messaging Records Management (MRM) features in Exchange Server 2010. For more information, see Messaging Records Management: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=169263*).

Security and privacy considerations

Outlook includes many security and privacy features.

The Trust Center for Office

The Trust Center, introduced with the 2007 Office system, provides a central location for security and privacy options. The Very High, High, Medium, and Low security levels that were used in earlier versions of Office have been replaced with a more streamlined security system.

Limiting viruses and junk e-mail messages for users

Outlook 2010 includes features that are designed to help minimize the spread of viruses and to help users avoid junk e-mail.

As in Office Outlook 2007, in Outlook 2010 you can configure virus-prevention and other security settings in Group Policy to support the needs of an organization. You can also use the Outlook Security Template to configure settings, as in earlier releases of Outlook. By using either configuration method, you can, for example, modify the list of file types that are blocked in e-mail messages.

The Object Model (OM) Guard that helps prevent viruses from using the Outlook Address Book (OAB) to spread is updated. Outlook checks for up-to-date antivirus software to help determine when to display OAB access warnings and other Outlook security warnings.

Outlook 2010 has several features to help users reduce receipt of junk e-mail messages. Outlook 2010 includes a Junk E-mail Filter for users that replaces the rules used in previous versions of Outlook to filter mail. Messages caught by the filter are moved to the Junk E-mail folder, where they can be viewed or deleted later. Outlook 2010 includes a Postmarking feature that was introduced with Office Outlook 2007 that can help the Junk E-mail filter determine valid e-mail messages.

Junk e-mail senders can include a Web beacon in HTML e-mail messages that includes external content, such as graphic images. When users open or view the e-mail, the Web beacons verify that their e-mail addresses are valid. This increases the probability that they will receive more junk e-mail messages. Outlook 2010 reduces the probability that users will become targets for future junk e-mail by blocking automatic picture downloads from external servers by default.

Outlook 2010 helps protect against issues created by phishing e-mail messages and deceptive domain names. By default, Outlook screens phishing e-mail messages — e-mail that seems to be legitimate but is designed to capture personal information, such as a user's bank account number and password. Outlook also helps prevent the receipt of e-mail messages from deceptive users by warning about suspicious domain names in e-mail addresses. Outlook 2010 supports internationalized domain names (IDNs) in e-mail addresses. IDNs allow people to register and use domain names in their native languages instead of online English. IDN support allows phishers to send homograph attacks, a situation in which a look-alike domain name is created using alphabet characters from different languages, not just English, with the intention of deceiving users into thinking they are visiting a legitimate Web site.

For more information about how to plan for security and privacy in Outlook 2010, see Plan for security and protection in Outlook 2010.

Configuring cryptographic features

Outlook provides cryptographic features for sending and receiving security-enhanced e-mail messages over the Internet or local intranet. You can customize features in an Outlook 2010 deployment to set cryptographic options that are appropriate for your organization.

You can also implement additional features to help enhance security in e-mail messaging. For example, you can provide security labels that match your organization's security policy. An Internal Use Only label might be implemented as a security label to apply to e-mail messages that are not to be sent or forwarded outside your company.

Restricting permission on e-mail messages

Information Rights Management (IRM) helps users prevent sensitive e-mail messages and other 2007 Office system content, such as documents and worksheets, from being forwarded, edited, or copied by unauthorized people. In Outlook 2010, users can use IRM to mark e-mail messages with Do not forward, which automatically restricts permission for recipients to forward, print, or copy the message. In addition, you can define customized Office-wide IRM permission policies for your organization's needs and can deploy the new permission policies for users to use with e-mail messages or other Office documents.

Outlook 2010 and e-mail protocols and servers

Outlook 2010 can be used with a wide variety of e-mail servers and services. The primary e-mail servers and services supported by Outlook include the following:

- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol version 3 (POP3)
- Internet Mail Access Protocol version 4 (IMAP4)
- Messaging Application Programming Interface (MAPI) for Exchange Server (version 2003 and later)
- Other messaging and information sources, including Hewlett-Packard OpenMail. Use of these additional service providers is made possible by the way in which Outlook 2010 uses the MAPI extensibility interface.

HTTP is supported with the installation of the Outlook Connector.

Users can use Outlook 2010 without an e-mail server to use the Contacts, Tasks, and Calendar features in a stand-alone configuration.

Upgrading from an earlier version of Outlook

You can install Outlook 2010 over any previous installation of Outlook. As in other Office 2010 applications, user settings stored in the registry are migrated. If a MAPI profile already exists on a user's computer, you typically can configure a deployment to continue to use the profile. However, if you are upgrading from an Internet Mail Only installation of Outlook 2000 or earlier, you might have to re-create user profiles. Outlook 2010 cannot coexist with previous versions of Outlook on the same computer. If you determine that users need a previous version, do not install Outlook 2010 or deploy Outlook 2010 with application virtualization.

When you upgrade users from an earlier version of Outlook, you must make choices about configuring user profiles, consider Cached Exchange Mode issues, and be aware of fax and forms changes.

For an overview of feature changes and migration considerations, see Changes in Outlook 2010 (*http://technet.microsoft.com/library/97a37b3c-972b-4cea-be0b-6a5ff2a1f9bb(Office.14).aspx*).

Upgrading with Cached Exchange Mode enabled

The process of upgrading users to Outlook 2010 with Cached Exchange Mode already enabled in Office Outlook 2003 or Office Outlook 2007 is straightforward. If you do not change Cached Exchange Mode settings, the same settings are kept for Outlook 2010. There is no change to the .ost or OAB file format, and you do not need to re-create these files during an upgrade.

However, if ANSI Outlook data files (.ost) are in the organization's environment, you might have to take additional steps when you migrate files to Outlook 2010. Users with non-Unicode (ANSI) formatted data files (.ost) and large Exchange mailboxes can experience errors when Outlook attempts to synchronize their mailboxes to their .ost files. We recommend that you upgrade users' .ost files to the Unicode format because Outlook Unicode files do not have the 2-gigabyte (GB) size limit of Outlook ANSI files. Unicode is the default file format for Outlook 2010. For information about how to force an upgrade of an existing non-Unicode (ANSI) formatted .ost file to Unicode format, see the section "To force upgrade of non-Unicode ANSI format .ost files to Unicode" (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034.aspx#UpgradeANSI*) in the article Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

For additional Cached Exchange Mode planning considerations, see Plan an Exchange deployment in Outlook 2010.

Additional issues to consider when planning an upgrade

To prepare for an upgrade, you must decide on the following additional issues:

- Should you upgrade to Exchange Server 2010 to take advantage of new features such as integrated e-mail archive, centralized rights management, support for multiple Exchange accounts, MailTips, Voice Mail Preview and Protected Voice Mail? For more information about Exchange Server 2010, see Microsoft Exchange 2010 (*http://go.microsoft.com/fwlink/?LinkId=163579*).

- Should you make changes to Outlook user profiles as part of your upgrade? For example, you might define a new Exchange server or enable new features of Outlook 2010. For more information about customizing Outlook profiles, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).
- How should you create and store a backup of your existing installation? Before you upgrade to any new release, we recommend that you back up existing data. For more information about backing up Outlook files, see Back up Outlook data with the Microsoft Outlook Personal Folders Backup tool (*http://go.microsoft.com/fwlink/?LinkId=81366*).
- How will users learn about the new interface and features of Office 2010? For more information, see Office.com (*http://go.microsoft.com/fwlink/?LinkId=169378*).
- Will any discontinued features or new or changed functionality affect when and how you upgrade? For a list of changes from earlier versions of Outlook, see Changes in Outlook 2010 (*http://technet.microsoft.com/library/97a37b3c-972b-4cea-be0b-6a5ff2a1f9bb(Office.14).aspx*).
- Will you have to assess and remediate Outlook add-ins in your environment?
    - Outlook 2010 enforces a new fast shutdown process for add-ins. The new shutdown process prevents add-ins from causing long delays by holding on to resources after the user exits Outlook. Although this change could adversely affect some existing add-ins, add-in vendors and IT administrators can resolve those effects by forcing Outlook to revert to the standard add-in shutdown process. For more information about the new shutdown process, see Shutdown Changes for Outlook 2010 (*http://go.microsoft.com/fwlink/?LinkId=203255*). For more information about add-in assessment and remediation, see Application compatibility assessment and remediation guide for Office 2010 (*http://technet.microsoft.com/library/b0d56d5f-f780-483e-8f95-dc7360a05208(Office.14).aspx*).
    - Exchange Client Extensions (ECEs) do not load in Outlook 2010. Some third-party applications such as archiving or security solutions use ECEs and must be updated for Outlook 2010. For more information, see Announcing the deprecation of Exchange Client Extensions (*http://go.microsoft.com/fwlink/?LinkId=203888*).
    - If you are installing 64-bit Outlook, 32-bit MAPI applications must be updated to 64-bit. For more information, see 64-bit editions of Office 2010 (*http://technet.microsoft.com/library/faab55b2-bb6c-4636-811e-24f6939548d1(Office.14).aspx*) and Building MAPI Applications on 32-Bit and 64-Bit Platforms (*http://go.microsoft.com/fwlink/?LinkId=203889*).

Upgrading from other mail and scheduling programs

You can upgrade to Outlook 2010 from other e-mail and scheduling programs. The process can be simplified with the use of the import feature in Outlook.

The following table lists migration paths supported by Outlook 2010.

Software program	Version
Outlook Express	4. *x*, 5. *x*, 6. *x*
Eudora Pro, Eudora Light	2. *x*, 3. *x*, 4. *x*, 5. *x*, 6. *x*, 7. *x*

Note:
You cannot import Microsoft Mail files to Outlook 2010, and you cannot share information between Outlook 2010 and Schedule Plus.

See Also

Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*)

Changes in Outlook 2010 (*http://technet.microsoft.com/library/97a37b3c-972b-4cea-be0b-6a5ff2a1f9bb(Office.14).aspx*)

Plan an Exchange deployment in Outlook 2010

Determine when to install Outlook 2010

You can install Microsoft Outlook 2010 before, during, or after an installation of other applications in Microsoft Office 2010. You can also deploy Outlook 2010 to different groups of users at different times.

Note that installing Outlook 2010 without Microsoft Word 2010 limits Outlook 2010 functionality in the following ways: 1) The Outlook 2010 e-mail editor has fewer features, and 2) Internet Fax functionality is not available.

This article describes the requirements, advantages, and disadvantages of each installation strategy.

In this article:

Installing Outlook with Office

You can install Outlook 2010 as part of an overall upgrade to Office 2010. Outlook 2010 is included in most editions of the Microsoft Office system.

Install Outlook 2010 with Office 2010 to eliminate the additional steps that you must follow to create separate application deployments.

Installing Outlook before Office

You might install Outlook 2010 in the following scenarios before you deploy other applications in Office 2010:

- To test custom solutions that rely on previous versions of Office applications (such as Microsoft Office Word 2007 or Microsoft Office Excel 2007) before you install the current version.
- When your messaging support group has the resources to install Outlook 2010 now, but the desktop applications support group must install the rest of Office later. Note that Outlook 2010 cannot coexist with previous versions of Microsoft Outlook. If users or tools require a previous version, do not install Outlook 2010 until your environment can support Outlook 2010 or deploy Outlook 2010 with application virtualization.

To install Outlook 2010 before you install Office 2010, do the following:

1. Customize Office Setup to install only Outlook 2010 from a network installation point.
2. Use the Office Customization Tool (OCT) to create or update a Setup customization file that installs Office 2010 from the same network installation point.

For details about how to install Office 2010 applications in stages, see Stage deployment of applications in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=162650*).

Advantages of installing Outlook before Office

If you deploy Outlook 2010 quickly, users can start to use new features without waiting for testing or technical support to become available for a complete upgrade.

Disadvantages of installing Outlook before Office

Installing Outlook 2010 before you install the rest of Office 2010 has several disadvantages:

- When you deploy the other Office 2010 applications later, you must customize the installation process to preserve your original Outlook 2010 settings.
- The Outlook 2010 editor has reduced functionality unless Word 2010 is also installed. For more information, see Using Outlook 2010 with or without Word 2010 installed (*http://go.microsoft.com/fwlink/?LinkId=195840*).
- Attachment Preview in Outlook 2010 does not work for Microsoft Office 2003 file types or earlier.
- When you use the same network installation point for Outlook 2010 and Office 2010, you must take additional steps to modify the installation options.

Installing Outlook after Office

You can wait to install Outlook 2010 until after you have installed the Office 2010. If any of the following scenarios applies to your organization, you might consider delaying your deployment of Outlook 2010:

- You plan to coordinate your Outlook 2010 deployment with a future upgrade of Microsoft Exchange Server.
- You want to convert IBM Lotus Notes to a Exchange Server solution before you upgrade to Outlook 2010.
- The desktop support group has the resources to upgrade to the Office 2010 now, but the messaging support group must wait to deploy Outlook 2010.

To install Outlook 2010 after you install Office 2010, do the following:

1. Customize Office Setup to install only Office 2010 without Outlook 2010 from a network installation point.
2. Use the OCT to create or update a Setup customization file that installs Outlook 2010 from the same network installation point.

For details about how to install Office 2010 applications in stages, see Stage deployment of applications in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=162650*).

Advantages of installing Outlook after Office

In many organizations, it makes sense to coordinate an Outlook 2010 deployment with an upgrade of an e-mail server, instead of with an upgrade of other desktop applications. For example, if you plan to upgrade to a new version of Exchange Server, you might plan an Outlook 2010 upgrade to follow immediately afterward — independently from an upgrade of other Office 2010 applications — to take advantage of features that work together between the e-mail server and client.

Disadvantages of installing Outlook after Office

When you install Office without Outlook 2010, you must use the OCT to customize Setup. This ensures that previous versions of Outlook are not removed from users' computers.

Regardless of when or how you install Outlook 2010 separately from Office 2010, you must perform additional steps to manage customizations to the installation process.

Staging an Outlook deployment

Some groups in an organization might be ready to immediately upgrade to Outlook 2010, but other groups might need more time. The following situations might warrant a staged deployment of Outlook 2010:

- The usual policy is to stage upgrades to help ensure a smooth rollout of new software throughout the organization.
- You have remote systems support groups (for example, in regional sales offices) that require autonomy in scheduling upgrades for their areas.
- Some groups want to wait until after a project deadline before they make changes to their local computers.
- You have limited resources for staging and upgrading systems throughout an organization.

Advantages of staging a deployment

Staging your Outlook 2010 deployment gives you more flexibility in managing your upgrading resources. In addition, pilot users immediately become familiar with the new features and productivity improvements of Outlook 2010.

In most circumstances, users encounter no significant technical problems when they work with different versions of Outlook. Outlook 2010 users can communicate seamlessly with users of Office Outlook 2007 and Office Outlook 2003. However, if users have delegate access in Outlook, the person who grants Delegate permissions and the delegate have to use the same version of Outlook.

Disadvantages of staging a deployment

You must consider the logistics of scheduling and managing a staged deployment. An organization might require additional resources to support users on different versions of the same product; for example, it might need additional training for Help desk staff.

For details about how to install Office 2010 applications in stages, see Stage deployment of applications in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=162650*).

See Also

Planning overview for Outlook 2010

Stage deployment of applications in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=162650*)

Determine which features to enable or customize in Outlook 2010

This article contains an initial list of some of the Microsoft Outlook features that you might need to configure and deploy with Microsoft Outlook 2010, such as Contact Cards and the Outlook Social Connector. For security and protection features, see Plan for security and protection in Outlook 2010.

You can customize the installation of Outlook 2010 by using Group Policy or the Office Customization tool (OCT). To enforce settings, use Group Policy with the Outlook 2010 Group Policy template (Outlk14.adm), and for some settings, such as those for Contact Cards, the Microsoft Office 2010 Group Policy template (Office14.adm).

- For information about how to download the Outlook 2010 administrative template, and about other Office 2010 Administrative Templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://technet.microsoft.com/library/2aa26c81-d80c-4be4-9114-8ea205ef47f2(Office.14).aspx*).
- For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*).

To configure default settings, in which case users can change the settings, use the OCT. The OCT settings are in corresponding locations of the Group Policy settings on the **Modify user settings** page of the OCT. For more information about the OCT, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

Contact Cards and Outlook Social Connector are two new features that you can configure by using Group Policy and the OCT. The Outlook 2010 features, Quick Steps and Clean Up, cannot be configured by using Group Policy or the OCT. Also, the MailTips feature is only administratively configurable through Microsoft Exchange Server 2010. However, users can customize their settings for these three features in Outlook 2010. To access user settings for Clean Up and MailTips, on the **File** tab, click **Options**, and then click **Mail**. To manage Quick Steps in Outlook 2010, on the **Home** tab, in the **Quick Steps** group, click the lower-right expand button.

For more information about how to configure MailTips in Exchange Server 2010, see Understanding MailTips (*http://go.microsoft.com/fwlink/?linkId=181931*) and Managing MailTips (*http://go.microsoft.com/fwlink/?linkId=181934*).

In this article:

- Instant Search
- Navigation Pane
- Outlook Social Connector
- Search Folders
- SharePoint Server Colleague add-in

AutoArchive

Outlook 2010 AutoArchive helps determine how e-mail is managed in user mailboxes. You can configure AutoArchive settings for users in your organization, determining, for example, how frequently to run AutoArchive and whether to prompt users before they run AutoArchive.

If you plan to deploy Outlook 2010 with Exchange Server 2010, consider using the Exchange Server 2010 Personal Archive feature instead of Outlook 2010 AutoArchive. For more information, see Understanding Personal Archive: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=169269*).

For planning compliance and archiving considerations, see Plan for compliance and archiving in Outlook 2010.

By default, AutoArchive is turned on and runs automatically at scheduled intervals, removing older and expired items from folders. Older items are those that reach the archiving age that a user specifies (the default archiving age varies by the kind of Outlook item). Expired items are mail and meeting items whose content is no longer valid after a certain date, such as a mail item set to expire two months ago that still appears in a user's Inbox.

Users can specify an expiration date on items in Outlook 2010 at the time they create or send the item or at a later date. When the item expires, it is unavailable and shows in the folder list with a strike-through mark on the item.

When AutoArchive runs, it can delete items or move items to an archive folder, depending on the settings that you specify.

The archive file is an Outlook data file (.pst file) that appears as **Archive Folders** in the Outlook 2010 folder list. The first time that AutoArchive runs, Outlook 2010 creates the archive file automatically in the following location:

%UserProfile%\AppData\Local\Microsoft\Outlook\Archive.pst

You can lock down the settings to customize AutoArchive by using the Outlook Group Policy template (Outlk14.adm). The settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Other\AutoArchive**. Or, you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the settings. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

The settings that you can configure for AutoArchive are shown in the following table.

Option	Description
Turn on AutoArchive	Set AutoArchive to run for users, with a frequency specified by the **Run AutoArchive every <x> days** setting.
Run AutoArchive every <*x*> days	Specify an AutoArchive interval in number of days.
Prompt before AutoArchive runs	Notify users that AutoArchive will run, rather than running silently.
Delete expired items (e-mail folders only)	Delete expired e-mail messages, instead of moving them to an archive folder.
Archive or delete old items	Move Outlook items to the archive file or delete the items.
Show archive folder in folder list	Display the archive folder in the user's Outlook folder list.
Clean out items older than	Specify how long to keep items before archiving or deleting them.
Permanently delete old items	Permanently delete items, instead of moving them to the Deleted Items folder.

Contact Cards

In Microsoft Office 2010, Contact Cards appear when you rest the mouse pointer over a name, for example a sender's name in an e-mail message or the author's name in an Office 2010 document. If you install Office 2010 with Office Communicator 2007 R2, Office or Communicator Server 2007 R2, Contact Cards displays a person's availability and lets you easily start a conversation directly through instant messaging, voice call, or video. When you expand the Contact Card, you can view the **Contact**, **Organization**, and **Member Of** tabs. The **Contact** tab is the default view and it displays information such as department, office location, and work telephone number. The **Organization** tab displays the contact's manager and contacts that share the same manager. The **Member Of** tab displays the distribution lists for which the contact is a member. In Office 2010, you can customize Contact Cards to turn off certain features and specify where presence icons are displayed. For the **Contact** tab on the Contact Card, you can replace labels and values. The specific settings that you can configure for Contact Cards are described in the following two sections. Note that there is a known issue with the Group Policy and OCT settings for customizing the **Contact** tab; however, a workaround is available. To customize the **Contact** tab, you must manually deploy the appropriate registry keys. See Contact Card Contact Tab customization workaround (*http://go.microsoft.com/fwlink/?LinkId=184612*).

Contact Card

In Group Policy, the settings in the following table are found under **User Configuration\Administrative Templates\Microsoft Office 2010\Contact Card**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Configure presence icon	Specify where the presence icons are displayed. **Display all** Display the presence icons. **Display some** Display only in the Contact Card and in lists in Microsoft SharePoint 2010 Products. **Display None** Do not display presence icons.
Display legacy GAL dialog	Enable to display the global address list (GAL) dialog box instead of the Contact Card when users double-click a contact in Outlook.
Do not display Hover Menu	Enable to stop the Hover Menu from displaying when a user pauses on a contact's presence icon or display name with the cursor.
Do not display photograph	Enable to not display the contact photograph on the Contact Card, e-mail header, reading pane, fast search results, GAL dialog box, and **File** tab.
Remove Member Of tab	Enable to remove the **Member Of** tab on the Contact Card.
Remove Organization tab	Enable to remove to **Organization** tab on the Contact Card.
Turn off click to IM option	Enable to remove the Instant Messaging (IM) option from the Contact Card and Outlook ribbon.
Turn off click to telephone	Enable to remove the telephone option from the Contact Card and Outlook ribbon.
Turn off presence integration	Enable to turn off IM presence integration for Office 2010 applications.

Contact tab

There is a known issue with the Group Policy and OCT settings for customizing the **Contact** tab; however, a workaround is available. To customize the **Contact** tab, you must manually deploy the appropriate registry keys. See Contact Card Contact Tab customization workaround (*http://go.microsoft.com/fwlink/?LinkId=184612*).

The following **Contact** tab settings under **User Configuration\Administrative Templates\Microsoft Office 2010\Contact Card** in Group Policy and in the corresponding locations on the **Modify user settings** page of the OCT will be fully functional in a later release of the Administrative Templates.

To customize the Contact Card **Contact** tab in Outlook 2010, use the **replace MAPI property settings** option. To customize the Contact Card **Contact** tab for other Office 2010 applications such as Microsoft Word 2010, use the **replace AD attribute settings** option.

For information about Active Directory attributes, see Property Sets in Exchange 2007 (*http://go.microsoft.com/fwlink/?LinkId=183812*) and Attributes defined by Active Directory (Windows) (*http://go.microsoft.com/fwlink/?LinkId=183814*). For information about MAPI properties, see Mail User Properties (*http://go.microsoft.com/fwlink/?LinkId=183815*)

Option	Description
Move Calendar Line	Enable and set the line number to move the **Calendar** field value to another location on the Contact Card. This action will replace the field value that was in that location.
Move Location Line	Enable and set the line number to move the **Location** field value to another location on the Contact Card. This action will replace the field value that was in that location.
Replace Label - Title	Enable and enter a new label name for the **Title** (title, department) field.
Replace Label - Office	Enable and enter a new label name for the **Office** (office location) field.
Replace Label - Work	Enable and enter a new label name for the **Work** (work phone) field.
Replace Label - Mobile	Enable and enter a new label name for the **Mobile** (mobile phone) field.
Replace Label - Home	Enable and enter a new label name for the **Home** (home phone) field.
Replace Label – E-mail	Enable and enter a new label name for the **E-mail** (e-mail address) field.
Replace Label - Calendar	Enable and enter a new label name for the **Calendar** (calendar free/busy information) field.
Replace Label - Location	Enable and enter a new label name for the **Location** (location information) field.

Option	Description
Replace AD attribute – “title, department”	Enable and enter the Active Directory (AD) attribute to replace the **Title** field value. For example, to display the e-mail alias, enter the AD attribute: **sAMAccountName**. If you enable this setting, also set **Replace MAPI property – “title, department”**.
Replace AD attribute – “office location”	Enable and enter the Active Directory (AD) attribute to replace the **Office** field value. If you enable this setting, also set **Replace MAPI property – “office location”**.
Replace AD attribute – “work phone”	Enable and enter the Active Directory (AD) attribute to replace the **Work** field value. If you enable this setting, also set **Replace MAPI property – “work phone”**.
Replace AD attribute – “mobile phone”	Enable and enter the Active Directory (AD) attribute to replace the **Mobile** field value. If you enable this setting, also set **Replace MAPI property – “mobile phone”**.
Replace AD attribute – “home phone”	Enable and enter the Active Directory (AD) attribute to replace the **Home** field value. If you enable this setting, also set **Replace MAPI property – “home phone”**.
Replace AD attribute – “e-mail address”	Enable and enter the Active Directory (AD) attribute to replace the **E-mail** field value. If you enable this setting, also set **Replace MAPI property – “e-mail address”**.
Replace AD attribute – “calendar free/busy information”	Enable and enter the Active Directory (AD) attribute to replace the **Calendar** field value. If you enable this setting, also set **Replace MAPI property – “calendar free/busy information”**.
Replace AD attribute – “location information”	Enable and enter the Active Directory (AD) attribute to replace the **Location** field value. If you enable this setting, also set **Replace MAPI property – “location information”**.

Option	Description
Replace MAPI property – “title, department”	Enable and enter the MAPI property to replace the **Title** field value. For example, to display the e-mail alias, enter the MAPI property: **0x3a00001f**. If you enable this setting, also set **Replace AD attribute – “title, department”**.
Replace MAPI property – “office location”	Enable and enter the MAPI property to replace the **Office** field value. If you enable this setting, also set **Replace AD attribute – “office location”**.
Replace MAPI property – “work phone”	Enable and enter the MAPI property to replace the **Work** field value. If you enable this setting, also set **Replace AD attribute – “work phone”**.
Replace MAPI property – “mobile phone”	Enable and enter the MAPI property to replace the **Mobile** field value. If you enable this setting, also set **Replace AD attribute – “mobile phone”**.
Replace MAPI property – “home phone”	Enable and enter the MAPI property to replace the **Home** field value. If you enable this setting, also set **Replace AD attribute – “home phone”**.
Replace MAPI property – “e-mail address”	Enable and enter the MAPI property to replace the **E-mail** field value. If you enable this setting, also set **Replace AD attribute – “e-mail address”**.
Replace MAPI property – “calendar free/busy information”	Enable and enter the MAPI property to replace the **Calendar** field value. If you enable this setting, also set **Replace AD attribute – “calendar free/busy information”**.
Replace MAPI property – “location information”	Enable and enter the MAPI property to replace the **Location** field value. If you enable this setting, also set **Replace AD attribute – “location information”**.

Conversation view

The Conversation view provides a threaded view of e-mail messages in an Microsoft Outlook folder. To access the Conversation view in Outlook 2010, click **View**, and then select the **Show as Conversations** check box.

The settings that you can configure for Conversation view in Group Policy and the OCT are shown in the following table. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Preferences\E-mail Options**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Configure Cross Folder Content in Conversation view	Enable and select the e-mail folder content to include in Conversation view. **On and cross-store** E-mail displayed is from all connected Outlook data files whether they are cached on the local computer or online. **Off** E-mail displayed in Conversation view is only from the current folder (such as the Inbox). **On and current** E-mail displayed in Conversation view is only from the current Outlook data file being viewed. **On and local** E-mail displayed is only from the current Outlook data file being viewed and any other local Outlook data file (such as a personal data file (.pst)).
Do not use Conversational arrangement in Views	There is a known issue with the explanatory text for this setting, which will be corrected in a later release of the Administrative Templates. If you do not configure this setting, the Outlook 2010 views will display Date view as the default. Enable to turn off Conversation view to prevent users from using Conversation View in Outlook 2010. Disable to turn on Conversation View as the default Outlook 2010 view.

Global Address List synchronization

Outlook 2010 synchronizes its **Contacts** folder entries to contacts in the Exchange Global Address List (GAL) when they have matching SMTP addresses. This synchronization is one-way: from the GAL to the Outlook **Contacts** folder.

Discrepancies in contact phone numbers might arise when the phone entries in users' Outlook **Contacts** folder are created in a different format from the one that is used in the corporate GAL. For example, a locale might require one type of phone number prefix format for calling from within the country and another prefix format for calling from outside the country.

If a user creates his or her Outlook 2010 contacts with the prefix formats that are required to dial from outside the country, a "move correction" takes place when Outlook 2010 contacts are updated by using details from the GAL.

In a move correction, the telephone numbers that the user creates in his or her Outlook contacts are overwritten and moved to an adjacent phone number field. For example, the telephone number in the "Business" field is moved to the "Business 2" field. For more information about move corrections, see Contact corrections that Outlook makes during GAL synchronization.

After synchronization, you cannot reverse the changes in bulk. However, a user can manually update Outlook contacts, or if there are many differences, the user's Exchange mailbox can be restored. A programmatic solution is possible, but requires complex data validation to pull the previous values from the **Notes** field. These solutions quickly become unfeasible for a large enterprise.

However, if contact synchronization is a large issue in your organization, you can disable GAL synchronization for Outlook 2010, either before you deploy Microsoft Office 2010, or when you see potential for this situation occurring.

Contact corrections that Outlook makes during GAL synchronization

If an Outlook contact is updated through GAL synchronization, Outlook "corrects" contact fields that do not match by using one of the following methods:

- **Normal correction** In a normal correction, Outlook logs the old value of the field in the **Notes** field and then updates the field by using the new value from the GAL.
- **Move correction** In a move correction, Outlook moves the old value of the field to an adjacent field. If this action is unsuccessful, Outlook performs a normal correction. If all fields in a contact group are full, the move correction becomes a normal correction

For the following fields, a *move* correction is the default correction method that is used. For all other fields Outlook always performs a *normal* correction.

Business Phone Group

Business Phone

Business 2 Phone

Other Phone

Home Phone Group

- Home Phone
- Home 2 Phone
- Other Phone

Mobile Phone Group

- Mobile Phone
- Other Phone

Business Address Group

- Business Address
- Other Address

Home Address Group

- Home Address
- Other Address

Configuring GAL synchronization

By default, GAL synchronization is enabled in Outlook 2010. You can disable GAL synchronization with Outlook contacts by configuring the **Block Global Address List synchronization** setting in Group Policy. After you apply this Group Policy setting, users cannot change the configuration.

If you use the OCT to disable GAL synchronization, users can enable it in the user interface (UI). To do this, they click the **View** tab on the ribbon, click the drop-down arrow next to the **People Pane** button, select the **Account Settings** command from the list, and then click the **Settings** button at the bottom of the **Social Network Accounts** dialog box. You can configure the GAL synchronization settings in the following table. In Group Policy, you can find the settings under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Social Connector**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT. For the steps to configure these settings, see Disable global address list synchronization for Outlook 2010 (*http://technet.microsoft.com/library/8709aafb-fef9-4f35-9e25-7ef42db242db(Office.14).aspx*).

Option	Description
Block Global Address List synchronization	Enable to block the synchronization of contacts between Outlook and the GAL. If you disable or do not configure this setting, GAL synchronization is allowed.
Set GAL contact synchronization interval	Enable to control how often (in minutes) contact information is synchronized between Outlook and connected social networks. By default, if you disable or do not configure this policy, contact information is synchronized one time per day or every 1,440 minutes.

You can configure GAL sync to prompt before updating, instead of updating without prompting, (which is default behavior) by configuring the registry settings that are listed in the following table. For the steps to deploy the registry data, see Disable global address list synchronization for Outlook 2010 (*http://technet.microsoft.com/library/8709aafb-fef9-4f35-9e25-7ef42db242db(Office.14).aspx*).

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	DWORD	Software\Microsoft\Office\Outlook\SocialConnector	ScheduleContactGALSync	Configures the GAL synchronization configuration. However, the user can override the configuration through the user interface by clicking the **View** tab on the ribbon, clicking the drop-down arrow next to the **People Pane** button, selecting the **Account Settings** command, and then clicking the **Settings** button in the **Social Network Accounts** dialog box. 0 = Do not synchronize contacts with the GAL 1 = Automatically update contacts with the latest GAL information 2 = Prompt before updating contacts with the latest GAL information
HKEY_CURRENT_USER	String	Software\Microsoft\Office\Outlook\SocialConnector	GalSyncExcludedLocales	For country codes, see ISO 3166-1 alpha-3 (*http://go.microsoft.com/fwlink/?LinkId=197158*). **Important:** This registry value is only honored when the **ScheduleContactGALSync** key does not exist. The **ScheduleContactGALSync** is created if the user manually sets GAL synchronization options through the user interface.

Internet Calendars

An Internet Calendar (iCal) is a calendar that you can publish to an Internet site, where other users can view it or subscribe to it. You can create an iCal from your calendar, send it as an attachment in an e-mail message, upload to Office.com, or upload it to a WebDAV server to publish it. You can also receive an iCal file as a file attachment in an e-mail message or download an iCal file to subscribe to a third-party calendar. For more information, see Introduction to publishing Internet Calendars (*http://go.microsoft.com/fwlink/?LinkId=193168*).

With Outlook 2010, you can customize iCal subscription features. You can disable iCal subscriptions in Outlook 2010 if, for example, you are concerned about bandwidth usage and want to delay introducing iCal subscriptions. By default, iCal subscriptions are enabled. You can also deploy iCal subscriptions as default subscriptions that users can change or delete. Or, you can lock down iCal subscriptions so that users cannot make changes or remove them. However, users can add new iCal subscriptions. By default, there are no iCal subscriptions. However, users can add and remove them.

Outlook 2010 sets the synchronization interval so that each iCal subscription is updated at the publisher's recommended interval. Users can override the default interval unless you disallow that option. If users set the update frequency to a short interval, it can cause performance problems.

By enabling the **Override published sync interval** option in Group Policy, you can enforce the publisher's update intervals so that users cannot change the intervals. This setting is used for all iCal subscriptions. You cannot set this option differently for different subscriptions.

The settings that you can configure for iCal in Group Policy and the OCT are shown in the following table. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Account Settings\Internet Calendars**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Options	Description
Automatically download attachments	Enable to automatically download attachments (such as graphics) on Internet Calendar appointments.
Default Internet Calendar subscriptions	Enable and add the URLs that are to be added to each user's profile as an Internet Calendar subscription.
Disable roaming of Internet Calendars	Enable so that Internet Calendars are available only on the client that originally linked them.
Do not include Internet Calendar integration in Outlook	Enable to prevent users from subscribing to Internet Calendars in Outlook.
Override published sync interval	Enable to prevent users from overriding the sync interval published by Internet Calendar providers.

Instant Search

In Microsoft Outlook 2010, users can use the Instant Search feature to quickly locate an item, such as an e-mail message, a task, or an appointment. Items that match the search are highlighted. Users can filter results by typing additional letters (known as *wordwheeling*).

Instant Search in Outlook 2010 works by accessing indexed content. Indexing Outlook content results in quicker search results. By default, the text of all unrestricted Outlook items — including attachments — is indexed, a process that starts when Outlook 2010 runs for the first time. You can turn off full text indexing, or you can turn off only attachments indexing. Indexing occurs in the background and only when there is additional processing capacity available on the user's computer.

The following Windows settings determine how Outlook manages search indexing:

- **HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Search\PreventIndexingOutlook**
- **HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Search\PreventIndexingEmailAttachments**

Encrypted items and items that are restricted by using Information Rights Management (IRM) are not indexed.

If you install Outlook 2010 on a computer that is running Windows Vista or Windows 7, you can configure searching indexing options for Outlook by using Group Policy or the OCT.

The settings that you can configure for Instant Search are shown in the following table. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Preferences\Search Options**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Change color used to highlight search matches	Selects the background color that will be used for highlighting matches in search results (default is yellow).
Do not display hit highlights in search results	Turns off search hit highlighting.
Do not include display search results as the user types	Do not display search results as the user types a search query (turn off Word Wheel functionality).
Do not include the Online Archive in All Mail item search	Enable to set the default action in All Mail Item search not to include search results from the Online Archive.

Option	Description
Expand scope of searches	Expand the scope for Instant Search to all folders in the current module (for example, Mail or Calendar). By default, Instant Search in Outlook returns results only from the selected folder.
Prevent clear signed message and attachment indexing	Do not index of the body and attachments of clear-text signed messages. The sender, subject line, and date will continue to be indexed and searchable.
Prevent installation prompts when Windows Desktop Search component is not present	When Outlook starts, do not prompt users by using a dialog box that asks whether users want to download Windows Desktop Search (if it is not already installed). Also, remove the links in Outlook that let users download Windows Desktop Search.
Turn off automatic search index reconciliation	Turn off the automatic verification of the integrity of the Outlook search index, which runs every 72 hours.

Navigation Pane

You can configure the modules in the Navigation Pane in Outlook 2010 (such as Calendar, Mail, and so on) to appear in a specific order for users, or to display only certain modules.

You can use the *Office Customization Tool* (OCT) **Add registry entries** option to distribute registry keys that specify how modules are displayed. You cannot use Group Policy to lock down Navigation Pane options.

The following table lists the registry settings that you can configure for a custom installation.

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	REG_DWORD	Software\Microsoft\Office\14.0\Outlook\Preferences	NumBigModules	Controls how many large buttons (each representing a Navigation Pane module) appear on the Navigation Pane. The default is 4. The maximum number that you can specify to be displayed is **8**.

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	REG_SZ	Software\Microsoft\Office\14.0\Outlook\Preferences	ModuleOrder	Determines the order in which the modules are displayed on the Navigation Pane. The data is an ordered list of indexes, where each position represents a Navigation Pane module, and the number in that position determines where the matching module appears. The default is **1,2,3,4,5,6,7,8**. The index positions match this list: Mail, Calendar, Contacts, Tasks, Notes, Folder List, Shortcuts, Journal. For example, if the user switches Mail to be the third module showing, and Contacts to be the first, the registry value has this data: **3,2,1,4,5,6,7,8**
HKEY_CURRENT_USER	REG_SZ	Software\Microsoft\Office\14.0\Outlook\Preferences	ModuleVisible	Determines whether a module is visible on the Navigation Pane. The values match the positions that are used in the module ordering list. The default is **1,1,1,1,1,1,1,0**. For example, the first position determines whether Mail is shown.

Root	Data type	Key	Value name	Value data
				By default, the Journal is not shown in the Navigation Pane. You can choose to not display other modules also. For example, to not display **Contacts**, **Tasks**, **Notes**, or **Shortcuts**, set this data: **1,1,0,0,0,1,0,0**.

Outlook Social Connector

The Outlook Social Connector is an add-in that exposes social network data including friends, profiles, activities, and status information from social networks in Outlook 2010. In the People Pane at the bottom of an e-mail message, you can see information about the sender such as their picture, name, and title; view your communication history with this person including meetings and attachments; and view their activity feeds from social networks.

To take advantage of the features that are available with the Outlook Social Connector, you must run Outlook 2010 in Cached Exchange Mode with Windows Desktop Search and have Microsoft SharePoint Server 2010 My Site configured for users. In this configuration, local items — such as e-mail messages, meetings, and attachments from the sender — will be included in the communication history. Additionally, with My Site configured you can view the activity feed from the sender's My Site.

If you run Outlook 2010 in Online Mode, only items related to the sender that are stored on the server will be shown in the communication history. Also, only activity feed information about the sender from on-demand social network providers, such as Facebook, can be shown. Activity feeds from My Site will not be available.

To include information from users' My Site in the Outlook Social Connector, you must run Outlook 2010 in Cached Exchange Mode with Windows Desktop Search and set the **MySiteHost** registry key as described in the following table.

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	REG_SZ	Software\Policies\Microsoft\Office\14.0\common\Portal\Link Providers\MySiteHost	URL	Your My Site URL – for example, http://Office/MySite.

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	REG_SZ	Software\Policies\Microsoft\Office\14.0\common\Portal\Link Providers\MySiteHost	DisplayName	Optional: The name to display to the user in the Outlook Social Connector – for example, MySite.

You can control the social network providers from which users can view activity feeds. You can prevent activity feeds from all social network providers by enabling the **Prevent social network connectivity** setting in Group Policy. Or, you can deploy specific providers by using the **Specify list of social network providers to load** setting in the OCT and prevent other providers from being installed by using the **Block specific social network providers** setting in Group Policy.

You can also control whether to allow the Outlook Social Connector or social network providers to prompt users for updates or manage the updates yourself by using the **Do not show social network info-bars** setting in Group Policy.

The settings that you can configure for Conversation view in Group Policy and the OCT are shown in the following table. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Social Connector**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Block Global Address List synchronization	Block synchronization between Outlook and the global address list.
Block network activity synchronization	Block synchronization of activity information between Outlook and social networks.
Block social network contact synchronization	Block synchronization of contacts between Outlook and social networks.
Block specific social network providers	Specify the list of social network providers to block by Program ID (ProgID). A provider's ProgID is registered under **HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\SocialConnector\SocialNetworks**.
Do not allow on-demand activity synchronization	Prevent on-demand synchronization of activity information between Outlook and social networks.

Option	Description
Do not download photos from Active Directory	Do not download contact photos from Active Directory.
Do not show social network info-bars	Enable to prevent displaying information-bar messages that will prompt users to upgrade the Outlook Social Connector when updates are available or to install or update social network providers.
Prevent social network connectivity	Enable to turn off social network connectivity in the Outlook Social Connector. Outlook Social Connector will still allow personal information management (PIM) aggregation so that users can view information about a chosen contact from their Outlook 2010 data files (for example, e-mail messages exchanged and meetings with that contact).
Set GAL contact synchronization interval	Control how often contact information is synchronized between Outlook and connected social networks (in minutes). By default, if you disable or do not configure this policy, contact information is synchronized one time per day or 1,440 minutes.
Specify activity feed synchronization interval	Control how often activity feed information is synchronized between Outlook and connected social networks (in minutes). By default, if you disable or do not configure this policy, activity information is synchronized every 60 minutes.
Specify list of social network providers to load	Enter a list of social network providers (by ProgID) that will be loaded by the Outlook Social Connector. A provider's ProgID is registered under **HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\SocialConnector\SocialNetworks**.
Turn off Outlook Social Connector	Enable to turn off the Outlook Social Connector.

Search Folders

Outlook folders are where items are stored — such as new e-mail messages (Inbox folder), sent e-mail messages (Sent Items folder), or saved e-mail messages (folders that you can create). Search Folders are virtual folders that contain views of all e-mail items that match specific search criteria. E-mail messages are not stored in Search Folders.

Search Folders display the results of previously defined search queries of your Outlook 2010 folders. The e-mail messages remain stored in one or more Outlook folders. Each Search Folder is a saved search that is kept up to date. By default, Search Folders monitor all Outlook folders for new items that match the criteria of the Search Folder. However, you can configure which folders are monitored. In Outlook 2010, click **Folder**, and then click **Customize This Search Folder**.

When users create a Search Folder, they have several default Search Folder options to choose from, such as Mail with attachments or Mail from specific people. They can also create custom Search Folders. To create a Search Folder in Outlook 2010, click **Folder** in the ribbon, and then click **New Search Folder**.

By default, Search Folders remain active for 1,000 days. You can configure how long Search Folders remain active for Cached Exchange Mode accounts and for online Exchange Server accounts. You can specify the number of days after which Search Folders become dormant — that is, items listed in the Search Folder are no longer up to date with current searches of Outlook folders. A dormant Search Folder appears in italic in a user's navigation pane. When a user opens a dormant Search Folder, the view is refreshed and the elapsed time count begins again.

The time period that you specify with this setting begins the last time that a user clicked the Search Folder. You can specify a different number of days for users in Exchange Online Mode and in Cached Exchange Mode. Separate counts are maintained for each Search Folder for each mode. If you enable and specify zero days for the option **Keep search folders in Exchange online**, Search Folders in Exchange Online Mode are always dormant. Similarly, if you specify zero days for the option **Keep search folders in offline**, Search Folders in Cached Exchange Mode are always dormant.

You can also limit the number of Search Folders allowed in each user mailbox, or you can disable the Search Folders user interface completely.

Note:
If users use Search Folders in Online Mode (using a mailbox on the Exchange Server) instead of in Cached Exchange Mode, the number of users who can be supported by the Exchange Server might be decreased.

The settings that you can configure for Search Folders in Group Policy and the OCT are shown in the following table. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Search Folders**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Do not create Search Folders when users start Outlook	A known issue exists for this policy setting. Default Search Folders are removed in Outlook 2010. This policy does not affect new or existing profiles in Outlook 2010.
Keep search folders in Exchange online	Specify the number of days to keep a Search Folder active when Outlook is running in Online Mode.
Keep search folders offline	Specify the number of days to keep a Search Folder active Outlook is running in offline or cached mode.

Option	Description
Maximum Number of Online Search Folders per Mailbox	Specify the maximum number of Search Folders for Exchange. Does not affect the number of Search Folders on a client computer.

SharePoint Server Colleague add-in

The Microsoft SharePoint Server Colleague add-in in Outlook 2010 scans the user's **Sent Items** folder to look for names and keywords along with the frequency of those names and keywords. The list of possible colleagues is updated periodically and stored under the user's profile on the user's local computer. This list is accessed through the **Add Colleagues** page on a user's SharePoint My Site intranet site where they can choose the colleagues that they want to add to their My Site page. The user can approve or reject contact names and keywords adding them to the **Ask Me About** Web Part. For more information, see Plan user profiles (SharePoint Server 2010) (*http://go.microsoft.com/fwlink/?LinkId=182364*) and Manage the information you share through your My Site and profile (*http://go.microsoft.com/fwlink/?LinkId=198208*).

By default, the SharePoint Server 2010 Colleague add-in is installed and turned on when you install Outlook 2010. However, to use the SharePoint Server 2010 Colleague add-in, you must have both SharePoint Server 2010 and Outlook 2010 installed. You must also deploy the My Site URL registry data that is listed in the following table. For the steps to deploy the registry data, see Enable SharePoint Server 2010 Colleague in Outlook 2010 (*http://technet.microsoft.com/library/4abf0200-cc1d-438a-835a-e1ea3410176a(Office.14).aspx*).

Root	Data type	Key	Value name	Value data
HKEY_CURRENT_USER	REG_SZ	Software\Policies\Microsoft\Office\14.0\common\Portal\Link Providers\MySiteHost	URL	Your My Site URL – for example, *http://Office/MySite*.
HKEY_CURRENT_USER	REG_SZ	Software\Policies\Microsoft\Office\14.0\common\Portal\Link Providers\MySiteHost	DisplayName	Optional: The name to display to the user – for example, *MySite*.

The settings to disable or lock down the SharePoint Server Colleague add-in by using Group Policy are listed in the following table and are found under the Microsoft Office 2010 settings: **User Configuration\Administrative Templates\Microsoft Office 2010\Server Settings\SharePoint Server**. Or, you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the settings. The OCT settings are in the corresponding location on the **Modify user settings** page of the OCT under the Microsoft Office 2010 settings. For the steps to configure these settings, see Configure Colleagues for My Site (*http://technet.microsoft.com/library/4abf0200-cc1d-438a-835a-e1ea3410176a.aspx#BKMK_ConfigureEMailAnalyzer*).

Option	Description
Enable Colleague Import Outlook Add-in to work with Microsoft SharePoint Server	Enable this setting to turn on the SharePoint Server Colleague add-in for Outlook 2010. Disable this setting to turn off this feature. If you do not set this option, the Colleague add-in is turned on by default.
Maximum number of days to scan from today to determine the user's colleagues for recommendation	Enable this setting to specify how many days prior to today to scan the Outlook sent items for the user's colleague recommendation list. For example, if you use the default, which is 20 days, the SharePoint Server Colleague add-in will scan items sent in the last 20 days. The larger the number of days specified, the more accurate the recommendation. The smaller the number of days, the faster the recommendations are generated.
Maximum number of items to scan from today to determine the user's colleagues for recommendation	Enable this setting to specify the maximum number of sent items to scan for the user's colleague recommendation list.
Maximum number of recipients in an Outlook item to scan to determine the user's colleagues for recommendation	Enable this setting to specify the maximum number of recipients in an Outlook sent item to scan for the user's colleague recommendation list.
Maximum number of rows fetched per request while populating a lookup in the SharePoint list control	Enable this setting to specify the maximum number of rows to retrieve per request while populating the SharePoint list control.
Minimum time before starting Colleague recommendation scan	Enable this setting to specify the minimum idle time (in milliseconds) to wait before the SharePoint Server Colleague add-in begins to scan the Outlook Sent Items folder.

Option	Description
Minimum time to wait before rescanning the Outlook mailbox for new recommendations	Enable this setting to specify the minimum time (in hours) to wait before rescanning the Outlook**Sent Items** folder for new colleague recommendations.

See Also

Plan for security and protection in Outlook 2010

Configure user settings for Office 2010 (*http://technet.microsoft.com/library/29cdde97-d1a7-4683-9c34-bd0bd78c41cc(Office.14).aspx*)

Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://technet.microsoft.com/library/2aa26c81-d80c-4be4-9114-8ea205ef47f2(Office.14).aspx*)

Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*)

Group Policy overview for Office 2010

Plan an Exchange deployment in Outlook 2010

Microsoft Outlook 2010 offers two basic connectivity modes when you are connected to a Microsoft Exchange Server computer: Cached Exchange Mode or Online Mode.

This article discusses which connectivity mode might be appropriate for your environment and also provides planning considerations and settings for Cached Exchange Mode deployments in Outlook 2010.

In this article:

Overview

When an Outlook 2010 account is configured to use Cached Exchange Mode, Outlook 2010 works from a local copy of a user's Microsoft Exchange mailbox stored in an offline data file (.ost file) on the user's computer, together with the Offline Address Book (OAB). The cached mailbox and OAB are updated periodically from the Exchange Server computer.

Cached Exchange Mode was introduced in Outlook 2003 to provide users a better online and offline experience. Cached Exchange Mode lets users move between connected and disconnected environments without interrupting their experience in Outlook. Also, it insulates users from network latency and connectivity issues while they are using Outlook.

In contrast, Online Mode works directly by using information from the server. When new information is required in Outlook, a request is made to the server and the information is displayed. Mailbox data is only cached in memory and never written to disk.

Cached Exchange Mode or Online Mode can be selected by the user during account setup or by changing the account settings. The mode can also be deployed by using the Office Customization Tool (OCT) or Group Policy.

Important

- There is a known issue in which an additional Exchange account is added to the Outlook profile when a user who already has an exchange account in the profile is upgraded from Outlook 2003 or Outlook 2007. This issue can occur while you are upgrading Outlook and applying customizations by using a custom OCT file (.msp) or .prf file that is configured to “Modify Profile" and "Define changes to make to the existing default profile.”
- To prevent multiple Exchange accounts from being created in one profile when you upgrade users to Outlook 2010, you must create a .prf file and set the properties BackupProfile=False and UniqueService=Yes. For the steps to do this, see Multiple Exchange accounts created in Outlook 2010 with existing Outlook profiles after upgrading from an earlier Office version using a custom MSP (*http://go.microsoft.com/fwlink/?LinkId=199704*).

Choosing between Cached Exchange Mode and Online Mode

When to use Cached Exchange Mode

Cached Exchange Mode is the premier configuration in Outlook 2010. We recommend it in all circumstances, except those specifically indicated in When to use Online Mode later in this article.

Although we recommend Cached Exchange Mode in most user configurations, it is especially valuable in the following scenarios:

- Portable computer users who frequently move in and out of connectivity.
- Users who frequently work offline or without connectivity.
- Users who have high-latency connections (greater than 500ms) to the Exchange Server computer.

When to use Online Mode

Online Mode is the legacy method of connecting to Microsoft Exchange. It is a fully supported configuration in Office Outlook 2003, Outlook 2007, and Outlook 2010. Online Mode has value in certain scenarios in which the behavior of Cached Exchange Mode is unwanted. Example scenarios include the following:

- “Kiosk” scenarios in which a particular computer has many users who access different Outlook accounts and the delay to download e-mail messages to a local cache is unacceptable.
- Heavily regulated compliance or secure environments in which data must not be stored locally for any reason. In these environments, we recommend that you evaluate Encrypting File System (EFS) or BitLocker in addition to Cached Exchange Mode as a potential solution.
- Very large mailboxes on computers that do not have enough hard disk space for a local copy of the mailbox.

- Very large mailboxes (greater than 25 GB) on which performance considerations become an issue in Cached Exchange Mode.
- Virtualized or Remote Desktop Services (Terminal Services) environments that run Outlook 2007 or Outlook 2003. Cached Exchange Mode is not supported when you run Outlook 2007 or Outlook 2003 on a computer running Remote Desktop Services (Terminal Services).
- Virtualized or Remote Desktop Services (Terminal Services) environments that run Outlook 2010 on which disk size or disk input/output (I/O) limitations prevent running Cached Exchange Mode at the desired scale.

If you work with a very large mailbox, you can reduce the size of the local data file by using synchronization filters. For more information, see Create a synchronization filter (*http://go.microsoft.com/fwlink/?LinkID=193917*) and Optimizing Outlook 2007 Cache Mode Performance for a Very Large Mailbox (*http://go.microsoft.com/fwlink/?LinkID=193918*).

If you work with a very large mailbox on which performance considerations become an issue in Cached Exchange Mode, see How to troubleshoot performance issues in Outlook (*http://go.microsoft.com/fwlink/?LinkID=193920*).

Special considerations

Outlook 2010 supports running in Cached Exchange Mode in a Remote Desktop Services (Terminal Services) environment that has multiple users. When you configure a computer running Remote Desktop Services (Terminal Services) to use Cached Exchange Mode, you must consider additional storage space that is required and disk I/O requirements of multiple client access.

By default, new Exchange accounts that are set up on a computer running Remote Desktop Services (Terminal Services) will use Online Mode. Upon setup, the user can decide to enable Cached Exchange Mode or this setting can be controlled by using the **Use Cached Exchange Mode for new and existing Outlook profiles** option in the Office Customization Tool or Group Policy.

In very limited bandwidth environments, Cached Exchange Mode can be configured to download only e-mail headers and a 256-character preview of the message body. For more information, see Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

Even when it is configured in Cached Exchange Mode, Outlook 2010 must contact the server directly to do certain operations. These operations will not function when Outlook is not connected and can take longer to complete on high-latency connections. These operations include the following:

- Working with Delegate mailbox data stores.
- Working with Shared Folders that have not been made available offline. For more information, see Configure Offline Availability for a Shared Folder(*http://go.microsoft.com/fwlink/?LinkID=193926*).
- Retrieving Free/Busy information.
- Setting, modifying, or canceling an Out of Office message.
- Accessing Public Folders.
- Retrieving rights to a rights-protected message.

- Editing rules.
- Retrieving MailTips.

How Cached Exchange Mode can help improve the Outlook user experience

Use of Cached Exchange Mode provides the following key benefits:

- Shields the user from network and server connection issues.
- Facilitates switching from online to offline for mobile users.

By caching the user's mailbox and the OAB locally, Outlook no longer depends on continuous network connectivity for access to user information. While connected, Outlook continuously updates users' mailboxes so that the mailboxes are kept up to date. If a user disconnects from the network — for example, by removing a portable computer, such as a laptop, from a docking station — the latest information is automatically available offline.

In addition to using local copies of mailboxes to improve the user experience, Cached Exchange Mode optimizes the type and amount of data sent over a connection with the server. For example, if the **On slow connections, download only headers** setting is configured in the Office Customization Tool, Outlook changes the type and amount of data sent over the connection.

Note:
Outlook checks the network adapter speed on the user's computer to determine a user's connection speed, as supplied by the operating system. Reported network adapter speeds of 128 kilobytes (KB) or lower are defined as slow connections. Under some circumstances, the network adapter speed might not accurately reflect data throughput for users. For more information about adjusting the behavior of Outlook in these scenarios, see Managing Outlook behavior for perceived slow connections later in this article.

Outlook can adapt to changing connection environments by offering different levels of optimization, such as disconnecting from a corporate local area network (LAN), going offline, and then re-establishing a connection to the server over a slower, dial-up connection. As the Exchange Server connection type changes — for example, to LAN, wireless, cellular, or offline — transitions are seamless and do not require changing settings or restarting Outlook.

For example, a user might have a portable computer at work with a network cable connection to a corporate LAN. In this scenario, the user has access to headers and full items, including attachments. The user also has quick access and updates to the computer that runs Exchange Server. If a user disconnects the portable computers from the LAN, Outlook switches to **Trying to connect** mode. The user can continue to work uninterruptedly with the data in Outlook. If a user has wireless access, Outlook can re-establish a connection to the server and then switch back to **Connected** mode.

If the user later connects to the Exchange Server computer over a dial-up connection, Outlook recognizes that the connection is slow and automatically optimizes for that connection by downloading

only headers and by not updating the OAB. In addition, Outlook 2010 and Office Outlook 2007 include optimizations to reduce the amount of data that is sent over the connection. The user does not need to change settings or restart Outlook in this scenario.

Outlook 2010 also includes the **Need Password** mode. A **Need Password** message is displayed when Outlook is in a disconnected state and requires user credentials to connect; for example, when a user clicks **Cancel** in a credentials authentication dialog box. When Outlook is disconnected but is not offline, a user-initiated action (such as clicking **Send/Receive** or the **Type Password** button on the ribbon) causes Outlook to prompt again for the password and to display a **Trying to connect** message until the user can successfully authenticate and connect.

Outlook features that can reduce the effectiveness of Cached Exchange Mode

Some Outlook features reduce the effectiveness of Cached Exchange Mode because they require network access or bypass Cached Exchange Mode functionality. The primary benefit of using Cached Exchange Mode is that the user is shielded from network and server connection issues. Features that rely on network access can cause delays in Outlook responsiveness that users would not otherwise experience when they use Cached Exchange Mode.

The following features might rely on network access and can cause delays in Outlook unless users have fast connections to Exchange Server data:

- Delegate access, when folders are not cached locally (local cache is the default).
- Opening another user's calendar or folder that is not cached locally (local cache is the default).
- Using a public folder that is not cached.

For more information, see Managing Outlook folder sharing in Synchronization, disk space, and performance considerations later in this article.

We recommend that you disable or do not implement the following features, or combination of features, if you deploy Cached Exchange Mode:

- **The toast alert feature with digital signatures on e-mail messages** Outlook must check a server to verify a digital signature. By default, when new messages arrive in a user's Inbox, Outlook displays a toast message that contains a part of an e-mail message. If the user clicks the toast message to open a signed e-mail message, Outlook uses network access to check for a valid signature on the message.
- **Multiple Address Book containers** The Address Book typically contains the global address list (GAL) and user Contacts folders. Some organizations configure subsets of the GAL, which display in the Address Book. These subset address books can also be included in the list that defines the search order for address books. If subset address books are included in the search order list, Outlook might need to access the network to check these address books every time that a name is resolved in an e-mail message that a user is composing.

- **Custom properties on the General tab in Properties dialog box for users** The **Properties** dialog box appears when you double-click a user name (for example, on the **To** line of an e-mail message). This dialog box can be configured to include custom properties unique to an organization, such as a user's cost center. However, if you add properties to this dialog box, we recommend that you not add them to the **General** tab. Outlook must make a remote procedure call (RPC) to the server to retrieve custom properties. Because the **General** tab shows by default when the **Properties** dialog box is accessed, an RPC would be performed every time that the user accessed the **Properties** dialog box. As a result, a user who runs Outlook in Cached Exchange Mode might experience noticeable delays when he or she accesses this dialog box. To help avoid such delays, you create a new tab on the **Properties** dialog box for custom properties, or include custom properties on the **Phone/Notes** tab.

Certain Outlook add-ins can affect Cached Exchange Mode. Some add-ins can access Outlook data by using the object model to bypass the expected functionality of the **Download only headers** and **On slow connections, download only headers** settings in Cached Exchange Mode. For example, full Outlook items, not only headers, download if you use Microsoft ActiveSync technology to synchronize a hand-held computer, even over a slow connection. In addition, the update process is slower than if you download the items in Outlook, because one-time-only applications use a less-efficient kind of synchronization.

Synchronization, disk space, and performance considerations

Cached Exchange Mode uses a local copy of the user’s Exchange mailbox, and in some cases, you can improve the performance of cached mode for your whole organization or for a group of users; for example, users who work remotely.

Manual synchronization of Exchange accounts no longer necessary

Cached Exchange Mode works independently of existing Outlook Send/Receive actions to synchronize users' .ost and OAB files with Exchange Server data. Send/Receive settings update users' Outlook data in the same way the settings did in earlier versions of Outlook.

Users who have Send/Receive-enabled Exchange accounts and who synchronize Outlook data by pressing F9 or by clicking **Send/Receive** might not realize that manual synchronization is no longer necessary. In fact, network traffic and server usage can be adversely affected if users repeatedly execute Send/Receive requests to Exchange Server. To minimize the effects, inform users that manual Send/Receive actions are unnecessary in Cached Exchange Mode. This might be especially helpful for remote users who typically used Outlook in offline mode with earlier Outlook versions and used Send/Receive to synchronize the data or just before they disconnected from the network. This kind of data synchronization now occurs automatically in Cached Exchange Mode.

Another way to manage the issue is to disable the Send/Receive option for users. However, we do not recommend this because it can create problems for some users; for example, when you upgrade

current Outlook users with POP accounts and existing customized Send/Receive groups to Outlook 2010. In this situation, if you disable the Send/Receive option, users cannot download POP e-mail messages or HTTP e-mail messages by using the Outlook Connector.

Offline Address Book access advantages

Cached Exchange Mode enables Outlook to access the local Offline Address Book (OAB) for user information, instead of requesting the data from Exchange Server. Local access to user data greatly reduces the need for Outlook to make RPCs to the Exchange Server computer, and lessens much of the network access that is required for users in Exchange online mode or in previous versions of Outlook.

When users have a current OAB installed on their computers, only incremental updates to the OAB are needed to help prevent unnecessary server calls. Outlook in Cached Exchange Mode synchronizes the user's OAB with updates from the Exchange Server copy of the OAB every 24 hours. You can help control how often users download OAB updates by limiting how often you update the Exchange Server copy of the OAB. If there is no new data to synchronize when Outlook checks, the user's OAB is not updated.

Note:
We recommend that users use the default Unicode OAB. The ANSI OAB files do not include some properties that are in the Unicode OAB files. Outlook must make server calls to retrieve required user properties that are not available in the local OAB, which can result in significant network access time when users do not have a Full Details OAB in Unicode format.

Offline folder (.ost file) recommendations

When you deploy Cached Exchange Mode for Outlook, be aware that users' local .ost files can increase 50 percent to 80 percent over the size of the mailbox reported in Exchange Server. The format Outlook uses to store data locally for Cached Exchange Mode is less space-efficient than the server data file format. This results in the use of more disk space when mailboxes are downloaded to provide a local copy for Cached Exchange Mode.

When Cached Exchange Mode first creates a local copy of a user's mailbox, the user's current .ost file, if one exists, is updated. If users currently have non-Unicode ANSI-formatted .ost files, we recommend that you upgrade their .ost files to Unicode. Non-Unicode (ANSI) Outlook files have a limit of 2 gigabytes (GB) of data storage. The maximum size for Unicode .ost files is configurable, with the default being 50 GB of data storage.

Also, make sure that users' .ost files are located in a folder that has sufficient disk space to accommodate users' mailboxes. For example, if users' hard drives are partitioned to use a smaller drive for system programs (the system drive is the default location for the folder that contains the .ost file), specify a folder on another drive that has more disk space as the location of users' .ost files.

- For more information about how to deploy .ost files in a location other than the default location, see To configure a default .ost location by using Group Policy (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034.aspx#ConfigureDefaultOST*) in Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).
- To determine whether your users' .ost files are in ANSI or Unicode format, see How to determine the mode that Outlook 2007 or Outlook 2003 is using for offline folder files (*http://go.microsoft.com/fwlink/?LinkId=159924*).
- For information about how to force an upgrade of an existing non-Unicode (ANSI) formatted .ost file to Unicode format, see To force upgrade of non-Unicode ANSI format .ost files to Unicode (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034.aspx#UpgradeANSI*) in Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).
- For more information about how to configure the Unicode .ost file size, see How to configure the size limit for both (.pst) and (.ost) files in Outlook 2007 and in Outlook 2003 (*http://go.microsoft.com/fwlink/?LinkId=159750*).

Managing performance issues

Most users will find that Cached Exchange Mode performs faster than online mode. However, many factors influence a user's perception of Cached Exchange Mode performance, including hard disk size and speed, CPU speed, .ost file size, and the expected level of performance.

For troubleshooting tips about diagnosing and addressing performance issues in Outlook, see Microsoft Knowledge Base article 940226: How to troubleshoot performance issues in Outlook 2007 (*http://go.microsoft.com/fwlink/?linkid=100887*) and Performance tips for deploying Outlook 2007 (*http://go.microsoft.com/fwlink/?LinkId=160227*).

Managing Outlook folder sharing

In Outlook 2010 and Office Outlook 2007, by default, shared non-mail folders that users access in other mailboxes are downloaded and cached in the user's local .ost file when Cached Exchange Mode is enabled. Only shared Mail folders are not cached. For example, if a coworker shares a calendar with another user and the user opens it, Outlook 2010 starts caching the folder locally so that the user has offline access to the folder and is insulated from network issues. However, if a manager delegates access to his or her Inbox to a team member, accessing the folder is an online task and can cause response delays.

Cached non-mail folders, such as Calendar, enable offline access and can provide a much more reliable experience on slow or unreliable networks. But be aware that they take a little more time to populate initially; more data is synchronized, so the local .ost file size increases; and in scenarios with slow connections or where the user is offline, the non-mail folder is not current until the latest changes are synchronized and downloaded.

You can configure this option (**Download shared non-mail folders**) in the Office Customization Tool (OCT) when you customize your Cached Exchange Mode deployment.

You can also enable shared mail folders for users if it is necessary. However, the cautionary notes earlier in this article regarding the sharing of non-mail folders also apply to the sharing of mail folders. Local .ost file size increases for users who have shared folders enabled. For information about how to enable this setting, see Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

For more information, see You cannot cache shared mail folders in Outlook 2007 (*http://go.microsoft.com/fwlink/?linkid=159948*).

Public Folder Favorites considerations

Cached Exchange Mode can be configured to download and synchronize the public folders included in users' Favorites folders for Outlook Public Folders. By default, Public Folder Favorites are not synchronized. However, you might want to enable this option if your organization uses public folders extensively. You can configure an option to download Public Folder Favorites in the .ost when you customize your Cached Exchange Mode deployment.

If users' Public Folders Favorites folders include large public folders, their .ost files can also become large. This can adversely affect Outlook performance in Cached Exchange Mode. Before you configure Cached Exchange Mode to enable this option, ensure that users are selective about the public folders that are included in their Public Folder Favorites. Also, ensure that users' .ost files are large enough, and are in folders that have sufficient disk space, to accommodate the additional storage requirements for the public folder downloads.

Managing Outlook behavior for perceived slow connections

Outlook is configured to determine a user's connection speed by checking the network adapter speed on the user's computer, as supplied by the operating system. If the reported network adapter speed is 128 KB or lower, the connection is defined as a slow connection.

When a slow connection to an Exchange Server computer is detected, Outlook helps users have a better experience if they reduce the amount of less-critical information that is synchronized with the Exchange Server computer. Outlook makes the following changes to synchronization behavior for slow connections:

- Switches to downloading only headers.
- Does not download the Offline Address Book or OAB updates.
- Downloads the body of an item and associated attachments only when it is requested by the user.

Outlook continues to synchronize the Outlook data with mobile devices, and some client-side rules might run.

Note:
We recommend that you do not synchronize mobile devices with the **Cached Exchange Download only headers** setting enabled. When you synchronize a mobile device — for example, by using ActiveSync — full items are downloaded in Outlook, and the synchronization process is less efficient than with regular Outlook synchronization to users' computers.

The **Download only headers** setting for synchronization is designed for Outlook users who have dial-up connections or cellular wireless connections, to minimize network traffic when there is a slow or expensive connection. Under some circumstances, the network adapter speed might not accurately reflect data throughput for users. For example, if a user's computer is connected to a local area network (LAN) for fast access to local file servers, the network adapter speed is reported as fast because the user is connected to a LAN. However, the user's access to other locations on an organization's network, including the Exchange Server computer, might use a slow link, such as an ISDN connection. For such a scenario, where users' actual data throughput is slow although their network adapters report a fast connection, you might want to configure an option to change or lock down the behavior of Outlook; for example, by disabling automatic switching to downloading only headers by using the Group Policy Object Editor option, **Disallow On Slow Connections Only Download Headers**. Similarly, there might be connections that Outlook has determined are slow but which provide high data throughput to users. In this case, you might also disable automatic switching to downloading only headers. You can configure the **On slow connections, download only headers** option in the OCT, or lock down the option by using Group Policy Object Editor to set **Disallow On Slow Connections Only Download Headers**. For more information about how to customize this setting, see Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

Options for staging a Cached Exchange Mode deployment

Stage the rollout over time if you plan to upgrade a large group of users from a deployment of Outlook without Cached Exchange Mode to Outlook 2010 with Cached Exchange Mode enabled. Outlook without Cached Exchanged Mode is the case for Outlook 2002 or earlier, or Office Outlook 2003, or for Office Outlook 2007 without Cached Exchange Mode installed. A staged rollout over time helps your organization's Exchange Server computers manage the requirements of creating or updating users' .ost files.

Caution:
If most user accounts are updated to use Cached Exchange Mode at the same time and then start Outlook at the same time (for example, on a Monday morning after a weekend upgrade), the Exchange Server computers have significant performance issues. These performance issues can sometimes be reduced; for example, if most of the users in your organization have current .ost files. But in general, we recommend staging deployment of Cached Exchange Mode over a period of time.

The following scenarios include examples of how you can deploy Cached Exchange Mode to avoid a large initial performance impact on the Exchange Server computers and, in some cases, minimize the time users spend waiting for the initial synchronization:

- **Retain Outlook .ost files when you deploy Cached Exchange Mode.** Because existing .ost files are merely updated with the latest mailbox information when Outlook with Cached Exchange Mode starts for the first time, retaining these .ost files when you deploy Cached Exchange Mode can help reduce the load on your organization's Exchange Server computers. Users who already have .ost files will have less Outlook information to synchronize with the server. This scenario works best when most users already have .ost files that have been synchronized recently with Exchange Server. To retain .ost files while you deploy Outlook with Cached Exchange Mode, do not specify a new Exchange Server computer when you customize Outlook profile information in the OCT. Or, when you customize Outlook profiles in the OCT, clear the **Overwrite existing Exchange settings if an Exchange connection exists (only applies when modifying the profile)** check box. (If you specify an Exchange Server computer when you configure and deploy Outlook with this option enabled, Outlook replaces the Exchange service provider in the MAPI profile, which removes the profile's entry for existing .ost files.) If you are currently using non-Unicode (ANSI) .ost files, we recommend that you upgrade users' .ost files to Unicode for improved performance and functionality. In this case, the old non-Unicode (ANSI) .ost files cannot be retained; they would be re-created in the Unicode format.

  For information about how to force an upgrade of an existing non-Unicode (ANSI) formatted .ost file to Unicode format, see "Force upgrade of non-Unicode ANSI format .ost files to Unicode" in Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

- **Provide seed .ost files to remote users, and then deploy Cached Exchange Mode after users have installed the .ost files that you provide.** If most users in your organization do not currently have .ost files or are not using Cached Exchange Mode, you can deploy Outlook 2010 with Cached Exchange Mode disabled. Then, before the date on which you plan to deploy Cached Exchange Mode, you provide initial, or seed, .ost files to each user with a snapshot of the user's mailbox; for example, by providing or mailing to the user a CD that contains the file together with installation instructions. You might also want to provide a recent version of your organization's Office Address Book (OAB) with Full Details. You configure and deploy Cached Exchange Mode when users confirm that they have installed the files.

  When you update your Outlook deployment to use Cached Exchange Mode later, Exchange Server updates users' existing .ost files and there is much less data to synchronize than there would be if a new .ost file and OAB were created for each user. To create individual CDs for each user's .ost file can be time-consuming. Therefore, this seed-file deployment option might be most useful for select groups of remote users who would otherwise spend lots of time waiting for the initial mailbox and OAB synchronization, perhaps at a high cost, depending on their remote connection scenario.

  For more information about how to create initial .ost files, see Providing an initial OST file for an Outlook Cached Exchange Mode deployment (*http://go.microsoft.com/fwlink/?LinkId=74518*). The

article describes the creation initial .ost files for Office Outlook 2003. The process works similarly for Office Outlook 2007 and Outlook 2010.

- **Deploy Outlook with Cached Exchange Mode to groups of users over time.** You can balance the workload on the Exchange Server computers and the local area network by upgrading groups of users to Cached Exchange Mode over time. You can reduce the network traffic and server-intensive work of populating .ost files with users' mailbox items and downloading the OAB by rolling out the new feature in stages. The way that you create and deploy Cached Exchange Mode to groups of users depends on your organization's usual deployment methods. For example, you might create groups of users in Microsoft Systems Management Server (SMS), to which you deploy a SMS package that updates Outlook to use Cached Exchange Mode. You deploy SMS to each group over a period of time. To balance the load as much as you can, choose groups of users whose accounts are spread across groups of Exchange Server computers.

Upgrading current Cached Exchange Mode users to Outlook 2010

The process of upgrading users to Outlook 2010 with Cached Exchange Mode already enabled in Office Outlook 2003 or Office Outlook 2007 is straightforward. If you do not change Cached Exchange Mode settings, the same settings are kept for Outlook 2010. There is no change to the .ost or OAB file format, and you do not need to re-create these files during an upgrade.

However, note that the option to share non-mail folders was introduced in Office Outlook 2007 and is enabled by default. Therefore, existing Office Outlook 2003 profiles with Cached Exchange Mode will have this setting enabled when users are upgraded. This could be problematic if:

- Users in your organization use ANSI .ost files.
- Users' .ost files are close to the size limit.
- Your organization uses shared folders extensively.

When these factors are all present, downloading shared non-mail folders can create performance issues and other problems.

For new Outlook 2010 profiles or for upgrading existing Office Outlook 2003 profiles, use the OCT to disable the non-mail folder sharing option and therefore help prevent problems with downloading non-mail folders. When upgrading existing Office Outlook 2007 profiles, you can disable this setting by using the Group Policy Object Editor.

In addition, be aware that caching for shared non-mail folders works differently from other caching for Cached Exchange Mode. With shared non-mail folders, replication to the local .ost file starts only when the user clicks the shared folder. Once a user has activated caching for the folder by clicking it, Outlook updates the folder just like other Outlook folders are synchronized in Cached Exchange Mode. However, if the user does not go to the folder at least once every 45 days (the default value), the local data will be not be updated further until the user clicks the folder again.

You can configure the **Synchronizing data in shared folders** option in Group Policy.

For more information about how to configure Cached Exchange Mode by using Group Policy, see Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

Deploying Cached Exchange Mode to users who already have .ost files

Some Outlook users who connect to Exchange Server in online mode might have .ost files. If these users have a non-Unicode (ANSI) formatted .ost file and large Exchange mailboxes, they might experience errors when Outlook attempts to synchronize their mailboxes to their .ost files. We recommend that you upgrade users' .ost files to the Unicode format as Outlook Unicode files do not have the 2-GB size limit that Outlook ANSI files do. Unicode is the default file format for Outlook 2010. For information about how to force an upgrade of an existing non-Unicode (ANSI) formatted .ost file to Unicode format, see To force upgrade of non-Unicode ANSI format .ost files to Unicode (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034.aspx#UpgradeANSI*) in Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

Configuring Cached Exchange Mode

You can lock down the settings to customize Cached Exchange Mode by using the Outlook Group Policy Administrative template (Outlk14.adm). Or, you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the settings.

By using Group Policy, you can help prevent users from enabling Cached Exchange Mode in Outlook 2010, and you can enforce download options for Cached Exchange Mode or configure other Cached Exchange Mode options. For example, you can specify the default times between Exchange Server synchronizations when data changes on an Exchange Server computer or on the client computer.

For steps to lock down settings by using Group Policy, see Configure Cached Exchange Mode in Outlook 2010 (*http://technet.microsoft.com/library/c6f4cad9-c918-420e-bab3-8b49e1885034(Office.14).aspx*).

The following table shows some of the settings that you can configure for Cached Exchange Mode. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Account Settings\Exchange\Cached Exchange Mode**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Disallow Download Full Items	Enable to turn off the **Download Full Items** option in Outlook. To find this option, click the **Send/Receive** tab, and then click **Download Preferences**.

Option	Description
Disallow Download Headers	Enable to turn off the **Download Headers** option in Outlook. To find this option, click the **Send/Receive** tab.
Disallow Download Headers then Full Items	Enable to turn off the **Download Headers then Full Items** option in Outlook. To find this option, click the **Send/Receive** tab, and then click **Download Preferences**.
Disallow On Slow Connections Only Download Headers	Enable to turn off the **On Slow Connections Download Only Headers** option in Outlook. To find this option, click the **Send/Receive** tab, and then click **Download Preferences**.
Download Public Folder Favorites	Enable to synchronize Public Folder Favorites in Cached Exchange Mode.
Download shared non-mail folders	Enable to synchronize shared non-mail folders in Cached Exchange Mode.
Use Cached Exchange Mode for new and existing Outlook profile	Enable to configure new and existing Outlook profiles to use Cached Exchange Mode. Disable to configure new and existing Outlook profiles to use Online Mode.

The following table shows some additional settings that you can configure for Exchange connectivity. In Group Policy, the settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Account Settings\Exchange**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Option	Description
Automatically configure profile based on Active Directory Primary SMTP address	Enable to prevent users from changing the SMTP e-mail address used to set up a new account from the one retrieved from Active Directory.
Configure Outlook Anywhere user interface options	Enable to let users view and change user interface (UI) options for Outlook Anywhere.
Do not allow an OST file to be created	Enable to prevent offline folder use.
Restrict legacy Exchange account	Enable to restrict which account is the first account that is added to the profile.

Option	Description
Set maximum number of Exchange accounts per profile	Enable to set the maximum number of Exchange accounts allowed per Outlook profile.
Synchronizing data in shared folders	Enable to control the number of days that elapses without a user accessing an Outlook folder before Outlook stops synchronizing the folder with Exchange.

Additional resources

For more information about how to plan a Cached Exchange Mode deployment, see the following resources.

- When you use Office Outlook 2003, Office Outlook 2007, or Outlook 2010 with Exchange Server-based systems, you can use Cached Exchange Mode and other features to enhance the user experience regarding issues such as high latency, loss of network connectivity, and limited network bandwidth. To learn about these improvements, see Client Network Traffic with Exchange 2003 white paper (*http://go.microsoft.com/fwlink/?LinkId=79063*).
- Outlook 2010 includes the ability to automatically configure user accounts. To learn how the discovery mechanisms work and how to modify an XML file to configure Autodiscover for your organization, see Plan to automatically configure user accounts in Outlook 2010.

Cached Exchange Mode in a Remote Desktop Session Host environment: planning considerations (white paper)

This white paper is an addendum to the document Remote Desktop Session Host Capacity Planning in Windows Server 2008 R2 (*http://go.microsoft.com/fwlink/?LinkId=196861*). Use it while you evaluate the deployment of Outlook 2010 in Cached Exchange Mode to your Remote Desktop Session Host (RDSH) environment. This white paper covers the three major areas that you should consider during your deployment planning:

- Storage footprint
- Performance impact
- Networked storage

Download this white paper as a Microsoft Word document (.docx): Cached Exchange Mode in a Remote Desktop Session Host environment: planning considerations (*http://go.microsoft.com/fwlink/?LinkId=200170*).

Plan to automatically configure user accounts in Outlook 2010

This article describes the two discovery mechanisms to automatically configure user accounts in Microsoft Outlook 2010: Autodiscover and Common Settings Discover.

In this article:

Overview

As with Microsoft Office Outlook 2007, Outlook 2010 includes the ability to automatically configure user accounts. Outlook 2010 uses one of two discovery mechanisms to automatically configure accounts: Autodiscover and Common Settings Discover.

Autodiscover is a standards-based XML file that can be configured by an administrator for an Internet service provider (ISP) or a corporation, or dynamically generated by a service, such as the Client Access server role in Microsoft Exchange Server 2007 or Microsoft Exchange Server 2010. This is the recommended mechanism for settings discovery, because it provides optimal performance. It also minimizes the possibility of configuration error on the client computer, because the settings are defined explicitly and deliberately by the administrator of the mail servers.

Common Settings Discover is less configurable, and less sophisticated, but configures most mail servers around the world based on common settings. It tries encrypted connections first. If these connections fail, it prompts the user to try connections that are not encrypted, and tries the same servers again without encryption. Many ISPs today do not require encryption, but have it enabled so that users can configure their accounts by using encryption.

For information about how to deploy and manage the Autodiscover service for Exchange Server 2007, see Overview of Autodiscover Service: Exchange 2007 Help (*http://go.microsoft.com/fwlink/?linkId=183290*). For Exchange Server 2010, see Understanding the Autodiscover Service: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?linkId=183289*).

Using Autodiscover with DNS

Autodiscover in Outlook 2010 is an XML file that is put in one of two locations, based on the domain name provided by the user. For the Internet, Autodiscover relies on the Domain Name System (DNS) to

find the XML file. The XML file location is based on the e-mail address that the user provides. For example, if barbara@contoso.com is entered as the user's e-mail address, Outlook 2010 looks for the XML file in the following locations and in the following order:

1. https://contoso.com/autodiscover/autodiscover.xml
2. https://autodiscover.contoso.com/autodiscover/autodiscover.xml

If your company also has a Web site at the root domain (for example, contoso.com), the second option (the Autodiscover "host (A) resource record" solution) lets you run the Web server and the Autodiscover file or service on separate servers. For smaller companies, the additional management of having separate DNS records can be ignored, and a single server can run both the Web site and the Autodiscover service (for example, the option 1 listed previously).

The connection must be established by using Secure Sockets Layer (SSL), and a valid SSL certificate must be present. SSL is required because a company or an Internet service provider (ISP) could choose to provide only encrypted access to their mail servers. In this scenario, if Outlook 2010 first checks non-SSL locations or allows failover to a non-SSL location, and a user types an e-mail address and password in a vulnerable security situation such as a man-in-the-middle attack, the automatic configuration service in Outlook 2010 could weaken security by being the weakest link in the connection chain if a non-SSL connection is allowed. Without an encrypted connection, the automatic configuration service could allow a non-encrypted Web site to configure mail server settings and allow authentication with a user name and password to the non-encrypted site. Instead, SSL is required by the Autodiscover protocol to maintain the compatibility with companies and ISPs that demand secure configuration routines.

However, if a company or an ISP chooses to host many e-mail domains, Outlook 2010 can follow an HTTP redirect or DNS Service (SRV) resource record (this DNS SRV record lookup functionality is included in Office Outlook 2007 Service Pack 1 and later versions) that is not encrypted to a secure Web site that stores the settings. For example, suppose that contoso.com is a hosted e-mail domain, and that the hosting service runs the Autodiscover file at hoster.com. In this scenario, the **autodiscover** prefix can be used by the hosting company to direct Outlook 2010 to a secure site that contains the Autodiscover settings.

- HTTP redirect: http://autodiscover.contoso.com/autodiscover/autodiscover.xml --> redirects to https://autodiscover.hoster.com/autodiscover/autodiscover.xml
- DNS SRV: _autodiscover._tcp.contoso.com --> points to https://autodiscover.hoster.com/autodiscover/autodiscover.xml

In both examples, users will see a warning dialog box in Outlook 2010 stating that they are being redirected to autodiscover.hoster.com for server settings. The dialog box provides the option to allow the redirection and lets users ignore future prompts about the redirect site (in this example, autodiscover.hoster.com).

Autodiscover protocol details

In a domain environment that has Service Connection Point (SCP) configured, an SCP lookup will be performed first. Otherwise, the first connection attempt is always an HTTPS POST verb to *domain*,

where the user has entered the e-mail address *e-mail@domain*. If the settings are successfully retrieved, no additional network calls are made. If the settings are not retrieved, an HTTPS POST verb is performed to autodiscover.*domain*. If settings are not retrieved from this site, a final HTTP GET and DNS SRV record lookup is performed only to the autodiscover.*domain* site. This HTTP GET and DNS SRV record lookup can only redirect to a secure site. (If settings are present at the HTTP location, Outlook 2010 will not configure them because the connection was not encrypted.)

Outlook 2010 can follow up to 10 redirects of any type. That is, you can follow an HTTPS POST redirect, HTTP GET redirect, or use the Autodiscover redirect XML schema tags detailed later in this article. After 10 redirections cannot obtain the settings, the settings discovery fails.

Static XML vs. Web service XML

The POST verb is used so that Outlook 2010 can issue a request to a dynamic Web service, such as the Client Access server role in Exchange 2007 and Exchange Server 2010. However, if a static XML file is sufficient or if you are not running an Autodiscover Web service, the XML response returned in a customized 405 (POST verb not supported) response from any Web server will also work as the configuration XML used by Outlook 2010.

Using Autodiscover locally

It is possible to configure the registry on your computer to look for a local XML file that defines the server settings. However, we strongly recommend that the settings be hosted on a live server instead so that they can be easily updated. For testing purposes, adding entries to the registry can force Outlook 2010 to use local XML files to configure an e-mail domain that is not configured on the server. The server overrides the local XML for better security and configuration control.

For example, to provide contoso.com e-mail address settings from a local XML file, you could configure the following registry value:

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Autodiscover]
"contoso.com"="%PROGRAMFILES%\Microsoft Office\Office14\contoso.xml"

In this example, the XML settings file is located here: %PROGRAMFILES%\Microsoft Office\Office14\contoso.xml. A sample XML settings file is provided later in this article.

Precedence for XML settings

Outlook 2010 configures the server type based on the order in which servers are defined in the Autodiscover XML settings file. For example, if a mail service provider enables users to log on by using both the POP3 protocol and the IMAP protocol, but prefers that users use the POP3 protocol, the POP3 settings should be listed first in the Autodiscover file.

Autodiscover transaction summary

The order of operations for Autodiscover settings discovery in Outlook 2010 is summarized as follows:

1. Automatically retrieve the e-mail address from the Active Directory directory service if the computer is joined to a domain.
2. Retrieve the name of the Exchange Server computer if found, and store the name for later.
3. Look for Service Connection Point (SCP) objects or SCP pointer objects that correspond to the user's e-mail address, and find the correct Autodiscover server to connect to. Then,, connect to the server and retrieve the settings.
4. If the previous step fails, try DNS discovery of Autodiscover XML (allowing for 10 redirects).
   a. HTTPS POST: https://*domain*/autodiscover/autodiscover.xml
   b. HTTPS POST: https://autodiscover.*domain*/autodiscover/autodiscover.xml
   c. HTTP GET: http://autodiscover.*domain*/autodiscover/autodiscover.xml (only to follow redirects, not to obtain settings)
   d. DNS SRV lookup: _autodiscover._tcp.*domain* (only to follow the redirect to which the SRV resource record points)
5. If the previous step fails, try local XML discovery and use the XML found on the local computer, if applicable.
6. If the previous step fails but the name of the Exchange Server computer is found in step 2, configure the Exchange account based on the name of the Exchange Server computer.
7. If the previous step is not applicable, try Common Settings Discover, as described in Common Settings Discover later in this article.

The Autodiscover XML schema

The XML schema for Autodiscover in Outlook 2010 is described in the following sections.

POST request sent by Outlook

When retrieving XML settings to configure an e-mail account, Outlook 2010 always uses a POST verb. The HTTP POST is as shown in the following code sample.

```
<!-- REQUEST TO SERVER. In HTTP POST DATA -->

<?xml version="1.0" encoding="utf-8" ?>

<Autodiscover

xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006">

<Request>

<AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscover/outlook/responsesc

hema/2006a</AcceptableResponseSchema>


<!-- EMailAddress: Optional

This tag indicates the user's email address.
```

```
-->
<EMailAddress>JohnDoe@sample.com</EMailAddress>
</Request>
</Autodiscover>
```

XML response schema

A server might respond to an Outlook 2010 POST in several ways. If a static XML file is sufficient, such as a POP3 service that is provided by an Internet service provider (ISP) where the server names are the same for all users, a customized 405 POST error message that has the XML content will be sufficient. If an Autodiscover service is running, the response might be dynamically calculated based on the user's POST shown in the previous section. Regardless, the response schema is as shown in the following code sample.

```
<!-- RESPONSE FROM THE SERVER -->
<?xml version="1.0" encoding="utf-8" ?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
<!-- Response: Required
This tag serves as an indication that the retrieved XML is an Autodiscovery Response
-->
<Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
<!-- User: Optional
This tag gives user-specific information.  Autodiscover must be UTF-8 encoded.
-->
<User>
<!-- DisplayName: Optional
The server may have a good formal display name.  The client can decide to accept it or change
it.  This will save the user time in the default case.
-->
<DisplayName>John Doe</DisplayName>
</User>

<!-- Account: Required
This tag specifies the type of account, such as Email vs Newsgroups, vs SIP server, etc.
-->
```

<Account>

<!-- AccountType: Required

This value indicates the type of the account.

VALUES:

email: The values under this Account tag indicate configuration settings for an email server.

nntp: The values under this Account tag indicate configuration settings for a NNTP server. (not used by Outlook 2007)

-->

<AccountType>**email | nntp**</AccountType>

<!-- Action: Required

This value indicates if the goal of this account results is to provide the settings or redirect to another web server that can provide results.

VALUES:

redirectUrl: If this value is specified, then the URL tag will specify the http: or https: URL containing the Autodiscover results to be used. In order to prevent the server from being able to send the client into an infinite loop, the client should stop redirecting after 10 redirects.

redirectAddr: If this value is specified, then the XML tag will specify the e-mail address that Outlook should use to execute Autodiscover again. In other words, the server is telling the client that the e-mail address the client should really be using for Autodiscover is not the one that was posted, but the one specified in this tag.

settings: If this value is specified, then the XML will contain the settings needed to configure the account. The settings will primarily be under the PROTOCOL tag.

-->

<Action>**redirectUrl | redirectAddr | settings**</Action>

<!-- RedirectUrl: Required if ACTION tag has value of 'redirectUrl'. Otherwise this tag must not exist.

The value will be a https: URL that the client should use to obtain the Autodiscover settings or a http: URL that the client should use for further redirection.

-->

<RedirectUrl>**redirect.URL**</RedirectUrl>

<!-- RedirectAddr: Required if ACTION tag has value of 'redirectAddr'. Otherwise this tag must not exist.

The value will be an email address that the client should use to rediscover settings using the Autodiscover protocol.

-->

<RedirectAddr>**email@address**</RedirectAddr>

<!-- Image: Optional

This is a JPG picture to brand the ISP configuration experience with. The client can choose whether or not they download this picture to display. (not used by Outlook 2007)

-->

<Image>**http://path.to.image.com/image.jpg**</Image>

<!-- ServiceHome: Optional

This is a link to the ISP's Home Page. The client can choose whether or not they expose this link to the user. (not used by Outlook 2007)

-->

<ServiceHome>**http://web.page.com**</ServiceHome>

<!-- Protocol: Required if ACTION tag has value of 'settings'. Otherwise, this tag must not exist.

The tag encloses the specifications for a single account type. The list of Protocol tags are in order of preference of the server. The client may over ride the preference.

-->

<Protocol>

<!-- TYPE: Required.

The value here specifies what kind of mail account is being configured.

POP3: The protocol to connect to this server is POP3. Only applicable for AccountType=email.

SMTP: The protocol to connect to this server is SMTP. Only applicable for AccountType=email.

IMAP: The protocol to connect to this server is IMAP. Only applicable for AccountType=email.

DAV: The protocol to connect to this server is DAV. Only applicable for AccountType=email.

WEB: Email is accessed from a web browser using an URL from the SERVER tag. Only applicable for AccountType=email. (not used by Outlook 2007)

NNTP: The protocol to connect to this server is NNTP. Only applicable for AccountType=nntp. (not used by Outlook 2007)

-->

<Type>**POP3 | SMTP | IMAP | DAV | WEB | NNTP**</Type>

<!-- ExpirationDate: Optional.

The value here specifies the last date which these settings should be used. After that date, the settings should be rediscovered via Autodiscover again. If no value is specified, the default will be no expiration.

-->

<ExpirationDate>**YYYYMMDD**</ExpirationDate>

<!-- TTL: Optional.

The value here specifies the time to live in hours that these settings are valid for. After that time has elapsed (from the time the settings were retrieved), the settings should be rediscovered via Autodiscovery again. A value of 0 indicates that no rediscovery will be required. If no value is specified, the default will be a TTL of 1 hour.

-->

<TTL>**168**</TTL>

<!-- Server: Required.

The value here specifies the name of the mail server corresponding to the server type specified above.

For protocols such as POP3, SMTP, IMAP, or NNTP, this value will be either a hostname or an IP address.

For protocols such as DAV or WEB, this will be an URL.

-->

<Server>**mail.contoso.com**</Server> <!--IP Addr or DNS name of server-->

<!-- Port: Optional.

The value specifies the Port number to use. If no value is specified, the default settings will be used depending on the mail server type. This value is not used if the SERVER tag contains an URL.

-->

<Port>**110**</Port>

<!-- LoginName: Optional.

This value specifies the user's login. If no value is specified, the default will be set to the string preceding the '@' in the email address. If the Login name contains a domain, the format should be <Username>@<Domain>. Such as JoeUser@SalesDomain.

-->

<LoginName>**johndoe**</LoginName>

<!-- DomainRequired: Optional. Default is off.

If this value is true, then a domain is required during authentication. If the domain is not specified in the LOGINNAME tag, or the LOGINNAME tag was not specified, the user will need to enter the domain before authentication will succeed.

-->

<DomainRequired>**on | off**</DomainRequired>

<!-- DomainName: Optional.

This value specifies the user's domain. If no value is specified, the default authentication will be to use the e-mail address as a UPN format <Username>@<Domain>. Such as JoeUser@SalesDomain.

-->

<DomainName></DomainName>

<!-- SPA: (Secure Password Authentication) Optional.

This value specifies whether or not secure password authentication is needed.

If unspecified, the default is set to on.

-->

<SPA>**on | off**</SPA>

<!-- SSL: Optional.

This value specifies whether secure login is needed.

If unspecified, the default is set to on.

-->

<SSL>on | off</SSL>

```
<!-- AuthRequired: Optional.
This value specifies whether authentication is needed (password).
If unspecified, the default is set to on.
-->
<AuthRequired>on | off</AuthRequired> <!-- Optional: Is Authentication required? -->

<!-- UsePOPAuth: Optional.
This value can only be used for SMTP types.
If specified, then the authentication information provided for the POP3 type account will also
be used for SMTP.
-->
<UsePOPAuth>on | off</UsePOPAuth>

<!-- SMTPLast: Optional.  Default is off.
If this value is true, then the SMTP server requires that email be downloaded before sending
email via the SMTP server.  This is often required because the SMTP server verifies that the
authentication succeeded when downloading email.
-->
<SMTPLast>on | off</SMTPLast>
</Protocol>
</Account>
</Response>
</Autodiscover>
```

Sample XML responses

The XML response that is returned depends on the configuration defined by the ISP.

ISP with POP3 and SMTP service

The following XML file would be configured as a custom 405 error response at either https://contoso.com/autodiscover/autodiscover.xml or https://autodiscover.contoso.com/autodiscover/autodiscover.xml.

```
<?xml version="1.0" encoding="utf-8" ?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
```

```
<Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
<Account>
<AccountType>email</AccountType>
<Action>settings</Action>
<Protocol>
<Type>POP3</Type>
<Server>mail.contoso.com</Server>
<Port>995</Port>
<DomainRequired>off</DomainRequired>
<SPA>off</SPA>
<SSL>on</SSL>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>SMTP</Type>
<Server>mail.contoso.com</Server>
<Port>587</Port>
<DomainRequired>off</DomainRequired>
<SPA>off</SPA>
<SSL>on</SSL>
<AuthRequired>on</AuthRequired>
<UsePOPAuth>on</UsePOPAuth>
<SMTPLast>on</SMTPLast>
</Protocol>
</Account>
</Response>
</Autodiscover>
```

ISP with POP3, IMAP, and SMTP services with POP3 preference for clients

The following XML file would be configured exactly as described in the previous section.

```
<?xml version="1.0" encoding="utf-8" ?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
```

```
<Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
<Account>
<AccountType>email</AccountType>
<Action>settings</Action>
<Protocol>
<Type>POP3</Type>
<Server>mail.contoso.com</Server>
<Port>995</Port>
<DomainRequired>off</DomainRequired>
<SPA>off</SPA>
<SSL>on</SSL>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>IMAP</Type>
<Server>mail.contoso.com</Server>
<Port>993</Port>
<DomainRequired>off</DomainRequired>
<SPA>off</SPA>
<SSL>on</SSL>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>SMTP</Type>
<Server>mail.contoso.com</Server>
<Port>587</Port>
<DomainRequired>off</DomainRequired>
<SPA>off</SPA>
<SSL>on</SSL>
<AuthRequired>on</AuthRequired>
<UsePOPAuth>on</UsePOPAuth>
<SMTPLast>on</SMTPLast>
```

```
</Protocol>

</Account>

</Response>

</Autodiscover>
```

XML redirect to a common XML file location

To redirect users to a common XML file location, the following XML file should be configured at a hosted domain location, at a URL that is not encrypted. By using this XML file, a message is displayed to users explaining that they are being redirected to another site for Autodiscover settings.

For example, if the hosted domain location was hoster.com providing contoso.com e-mail addresses, the file would be located at http://autodiscover.contoso.com/autodiscover/autodiscover.xml. The contents of the file, in this example, would be as shown in the following code sample.

```
<?xml version="1.0" encoding="utf-8" ?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">

<Response

xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">

<Account>

<AccountType>email</AccountType>

<Action>redirectUrl</Action>

<RedirectUrl>https://autodiscover.hoster.com/autodiscover/autodiscover.xml</RedirectUrl>

</Account>

</Response>

</Autodiscover>
```

Users can instead be redirected by configuring an ordinary HTTP 302 redirect at the source location. Outlook 2010 follows both 302 redirects and redirectUrl tags in an XML response.

Note that the XML file contents for all Autodiscover responses must be named Autodiscover.xml.

Common Settings Discover

If the required settings for automatically configuring a user account in Outlook 2010 cannot be found by the methods described in the previous Autodiscover sections, a fallback algorithm is used to detect servers by using common names and well-known ports.

In Outlook 2010, the automatic configuration of a Webmail account will set the account type to IMAP by default for IMAP-supported Webmail accounts such as Google Gmail. If users prefer POP3 settings, they can manually adjust the protocol settings after the settings are determined by Outlook 2010 by selecting the **Manually configure server settings** option in the **Add New Account** dialog box. To make this selection straightforward for users, mail service providers that provide both POP3 and IMAP

protocols should use the same server names for each protocol. Then, the user needs only to change a selection box, switching from IMAP to POP3.

Outlook 2010 tries a variety of incoming and outgoing server settings in parallel to maximize performance and minimize wait time for the user. The settings that Outlook 2010 attempts to configure for users are listed in the following tables. All encrypted settings are tried first, and mutually exclusively. Then, settings that are not encrypted are tried, if the user consents.

IMAP settings

First, encrypted settings are tried. For an IMAP server, the connection permutations are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	993	SSL	SPA
	email@domain	993	SSL	no SPA
	email@domain	993	TLS	SPA
	email@domain	993	TLS	no SPA
	email@domain	143	SSL	SPA
	email@domain	143	SSL	no SPA
	email@domain	143	TLS	SPA
	email@domain	143	TLS	no SPA
	email	993	SSL	SPA
	email	993	SSL	no SPA
	email	993	TLS	SPA
	email	993	TLS	no SPA
	email	143	SSL	SPA
	email	143	SSL	no SPA
	email	143	TLS	SPA
	email	143	TLS	no SPA
imap.*domain*	*email@domain*	993	SSL	SPA
	email@domain	993	SSL	no SPA
	email@domain	993	TLS	SPA

Server	User name	Port	TLS/SSL	SPA
	email@domain	993	TLS	no SPA
	email@domain	143	SSL	SPA
	email@domain	143	SSL	no SPA
	email@domain	143	TLS	SPA
	email@domain	143	TLS	no SPA
	email	993	SSL	SPA
	email	993	SSL	no SPA
	email	993	TLS	SPA
	email	993	TLS	no SPA
	email	143	SSL	SPA
	email	143	SSL	no SPA
	email	143	TLS	SPA
	email	143	TLS	no SPA
domain	*email@domain*	993	SSL	SPA
	email@domain	993	SSL	no SPA
	email@domain	993	TLS	SPA
	email@domain	993	TLS	no SPA
	email@domain	143	SSL	SPA
	email@domain	143	SSL	no SPA
	email@domain	143	TLS	SPA
	email@domain	143	TLS	no SPA
	email	993	SSL	SPA
	email	993	SSL	no SPA
	email	993	TLS	SPA
	email	993	TLS	no SPA
	email	143	SSL	SPA
	email	143	SSL	no SPA

Server	User name	Port	TLS/SSL	SPA
	email	143	TLS	SPA
	email	143	TLS	no SPA

Next, permutations that are not encrypted are tried, after the user is asked to continue with connection attempts that are not encrypted. The IMAP settings that are not encrypted that Outlook 2010 attempts to configure are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	143	Clear	SPA
	email@domain	143	Clear	no SPA
	email	143	Clear	SPA
	email	143	Clear	no SPA
imap.*domain*	*email@domain*	143	Clear	SPA
	email@domain	143	Clear	no SPA
	email	143	Clear	SPA
	email	143	Clear	no SPA
domain	*email@domain*	143	Clear	SPA
	email@domain	143	Clear	no SPA
	email	143	Clear	SPA
	email	143	Clear	no SPA

POP3 settings

First, encrypted settings are tried. For a POP3 server, the connection permutations are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	995	SSL	SPA
	email@domain	995	SSL	no SPA
	email@domain	995	TLS	SPA

Server	User name	Port	TLS/SSL	SPA
	email@domain	995	TLS	no SPA
	email@domain	110	SSL	SPA
	email@domain	110	SSL	no SPA
	email@domain	110	TLS	SPA
	email@domain	110	TLS	no SPA
	email	995	SSL	SPA
	email	995	SSL	no SPA
	email	995	TLS	SPA
	email	995	TLS	no SPA
	email	110	SSL	SPA
	email	110	SSL	no SPA
	email	110	TLS	SPA
	email	110	TLS	no SPA
pop3.*domain*	*email@domain*	995	SSL	SPA
	email@domain	995	SSL	no SPA
	email@domain	995	TLS	SPA
	email@domain	995	TLS	no SPA
	email@domain	110	SSL	SPA
	email@domain	110	SSL	no SPA
	email@domain	110	TLS	SPA
	email@domain	110	TLS	no SPA
	email	995	SSL	SPA
	email	995	SSL	no SPA
	email	995	TLS	SPA
	email	995	TLS	no SPA
	email	110	SSL	SPA
	email	110	SSL	no SPA

Server	User name	Port	TLS/SSL	SPA
	email	110	TLS	SPA
	email	110	TLS	no SPA
pop.*domain*	*email@domain*	995	SSL	SPA
	email@domain	995	SSL	no SPA
	email@domain	995	TLS	SPA
	email@domain	995	TLS	no SPA
	email@domain	110	SSL	SPA
	email@domain	110	SSL	no SPA
	email@domain	110	TLS	SPA
	email@domain	110	TLS	no SPA
	email	995	SSL	SPA
	email	995	SSL	no SPA
	email	995	TLS	SPA
	email	995	TLS	no SPA
	email	110	SSL	SPA
	email	110	SSL	no SPA
	email	110	TLS	SPA
	email	110	TLS	no SPA
domain	*email@domain*	995	SSL	SPA
	email@domain	995	SSL	no SPA
	email@domain	995	TLS	SPA
	email@domain	995	TLS	no SPA
	email@domain	110	SSL	SPA
	email@domain	110	SSL	no SPA
	email@domain	110	TLS	SPA
	email@domain	110	TLS	no SPA
	email	995	SSL	SPA

Server	User name	Port	TLS/SSL	SPA
	email	995	SSL	no SPA
	email	995	TLS	SPA
	email	995	TLS	no SPA
	email	110	SSL	SPA
	email	110	SSL	no SPA
	email	110	TLS	SPA
	email	110	TLS	no SPA

Next, permutations that are not encrypted are tried, after the user is asked to continue with connection attempts that are not encrypted. The POP3 settings that are not encrypted that Outlook 2010 attempts to configure are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	110	Clear	SPA
	email@domain	110	Clear	no SPA
	email	110	Clear	SPA
	email	110	Clear	no SPA
pop3.*domain*	*email@domain*	110	Clear	SPA
	email@domain	110	Clear	no SPA
	email	110	Clear	SPA
	email	110	Clear	no SPA
pop.*domain*	*email@domain*	110	Clear	SPA
	email@domain	110	Clear	no SPA
	email	110	Clear	SPA
	email	110	Clear	no SPA
domain	*email@domain*	110	Clear	SPA
	email@domain	110	Clear	no SPA
	email	110	Clear	SPA

Server	User name	Port	TLS/SSL	SPA
	email	110	Clear	no SPA

SMTP settings

First, encrypted settings are tried. For an SMTP server, the connection permutations are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	587	SSL	SPA
	email@domain	587	SSL	no SPA
	email@domain	587	TLS	SPA
	email@domain	587	TLS	no SPA
	email@domain	25	SSL	SPA
	email@domain	25	SSL	no SPA
	email@domain	25	TLS	SPA
	email@domain	25	TLS	no SPA
	email	587	SSL	SPA
	email	587	SSL	no SPA
	email	587	TLS	SPA
	email	587	TLS	no SPA
	email	25	SSL	SPA
	email	25	SSL	no SPA
	email	25	TLS	SPA
	email	25	TLS	no SPA
	Anonymous	587	SSL	not applicable
	Anonymous	587	TLS	not applicable
	Anonymous	25	SSL	not applicable
	Anonymous	25	TLS	not applicable
smtp.*domain*	*email@domain*	587	SSL	SPA

Server	User name	Port	TLS/SSL	SPA
	email@domain	587	SSL	no SPA
	email@domain	587	TLS	SPA
	email@domain	587	TLS	no SPA
	email@domain	25	SSL	SPA
	email@domain	25	SSL	no SPA
	email@domain	25	TLS	SPA
	email@domain	25	TLS	no SPA
	email	587	SSL	SPA
	email	587	SSL	no SPA
	email	587	TLS	SPA
	email	587	TLS	no SPA
	email	25	SSL	SPA
	email	25	SSL	no SPA
	email	25	TLS	SPA
	email	25	TLS	no SPA
	Anonymous	587	SSL	not applicable
	Anonymous	587	TLS	not applicable
	Anonymous	25	SSL	not applicable
	Anonymous	25	TLS	not applicable
domain	*email@domain*	587	SSL	SPA
	email@domain	587	SSL	no SPA
	email@domain	587	TLS	SPA
	email@domain	587	TLS	no SPA
	email@domain	25	SSL	SPA
	email@domain	25	SSL	no SPA
	email@domain	25	TLS	SPA
	email@domain	25	TLS	no SPA

Server	User name	Port	TLS/SSL	SPA
	email	587	SSL	SPA
	email	587	SSL	no SPA
	email	587	TLS	SPA
	email	587	TLS	no SPA
	email	25	SSL	SPA
	email	25	SSL	no SPA
	email	25	TLS	SPA
	email	25	TLS	no SPA
	Anonymous	587	SSL	not applicable
	Anonymous	587	TLS	not applicable
	Anonymous	25	SSL	not applicable
	Anonymous	25	TLS	not applicable

Next, permutations that are not encrypted are tried, after the user is asked to continue with connection attempts that are not encrypted. The SMTP settings that are not encrypted that Outlook 2010 attempts to configure are as shown in the following table.

Server	User name	Port	TLS/SSL	SPA
mail.*domain*	*email@domain*	25	Clear	SPA
	email@domain	25	Clear	no SPA
	email	25	Clear	SPA
	email	25	Clear	no SPA
	Anonymous	25	Clear	not applicable
smtp.*domain*	*email@domain*	25	Clear	SPA
	email@domain	25	Clear	no SPA
	email	25	Clear	SPA
	email	25	Clear	no SPA
	Anonymous	25	Clear	not applicable

Server	User name	Port	TLS/SSL	SPA
domain	*email@domain*	25	Clear	SPA
	email@domain	25	Clear	no SPA
	email	25	Clear	SPA
	email	25	Clear	no SPA
	Anonymous	25	Clear	not applicable

See Also

Overview of Autodiscover Service: Exchange 2007 Help (*http://go.microsoft.com/fwlink/?linkId=183290*)

Understanding the Autodiscover Service: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?linkId=183289*)

Plan for compliance and archiving in Outlook 2010

This article discusses the planning considerations to deploy Retention Policy and Personal Archive features with Microsoft Outlook 2010 and Microsoft Exchange Server 2010. These features together can provide a great way to enable users to stay in compliance with mail retention policies, and have the space to store their business-critical information by using the Personal Archive.

Even if your organization does not strictly enforce compliance, the Personal Archive is a great solution to migrate your organization away from personal Microsoft Outlook data files (.pst) or third-party archiving solutions. The Personal Archive enables users to archive their e-mail messages in a managed location for backup, data recovery, and compliance needs.

Retention Policy and Personal Archive are available only when you use Outlook 2010 as part of Microsoft Office Professional 2010 or Microsoft Office Professional Plus 2010 with an Exchange Server 2010 account, and the Exchange administrator has enabled Retention Policy and Online Archive.

In this article:

Planning a Retention Policy deployment

Retention Policy is an effective way to let you enforce e-mail retention policies on messages stored on a server that is running Exchange Server 2010. Additionally, Retention Policy can be used as an aid to help users stay under their mailbox quota. Retention Policy can be applied at the mailbox, folder, and individual e-mail level, and is only supported for e-mail messages. Other message types, such as calendar or tasks items, are not supported with Outlook 2010 and Exchange Server 2010. To enforce Retention Policy, e-mail messages must be stored in a mailbox or personal archive on an Exchange Server computer.

As part of planning a Retention Policy deployment, consider the following key steps:

- Work with your company’s legal or compliance department to define policies.
- Determine which combination of mailbox, folder, and user policies is appropriate.
- Upgrade the users to Retention Policy.
- Inform the users about Retention Policy.
- For users under investigation, place them on Retention Hold or Legal Hold.

Defining your Retention Policies

Deciding on which Retention Policies have to be available for your organization, departments, and users should be a conversation that you have with your legal or compliance department. Your company might be subject to government or additional regulation that can be enforced by using Retention Policies. Because departments can be under different regulations, you should organize your policies into logical, easy-to-manage groups. Once you understand the policies that your company must follow, you can determine how to best implement those policies.

Personal Tags are the policies that you can give to users to apply to individual messages and folders they have created. When you define the policies that users will follow, we recommend no more than 10 Personal Tags be used. More than that can overwhelm users. Furthermore, in the Assign Policy gallery on the ribbon, Outlook will only show 10 Personal Tags at a time. If a user has to access more than 10 Personal Tags, they can select **More Retention Policies** in the Assign Policy gallery.

Determining which types of policies to create

Now that you know which groups of users need which Retention Policies, you can determine how you want to implement those policies.

There are three major types of Retention Policies.

1. **Default Policy Tag** This is a policy that is deployed by the Exchange administrator and is applied to all user-created folders and all e-mail messages in a user's mailbox. This policy cannot be changed by the user. This is the only policy type that guarantees all e-mail messages will have at least one policy applied to them.
2. **Retention Policy Tag** This is a type of policy that can be applied to the following special folders in the user's mailbox:
   - Inbox
   - Drafts
   - Sent Items
   - Deleted Items
   - Junk E-mail
   - Outbox
   - RSS Feeds
   - Sync Issues
   - Conversation History

   Note:
   Policies on these special folders cannot be changed by the user even if there is no Retention Policy Tag applied to the folder.
3. **Personal Tag** This is a type of policy that will appear in the Retention Policy user interface (UI) for the user to apply to folders that they create and to individual e-mail messages.

a. Users cannot apply these policies to any of the special folders listed under Retention Policy Tag earlier in this section.
b. Users can apply these policies to e-mail messages within special folders, but not the folder itself.
c. Users can apply these policies to their own user-created folders.

Note:
Search folders do not support retention policies because they do not contain actual e-mail messages.

Personal Tags

For users to set a Retention Policy on a folder or e-mail message, they must be provided with one or more Personal Tags. By default, the Ribbon Assign Policy gallery shows the first 10 policies (Personal Tags) in alphabetical order. This menu list shows the most recently used policies. However, as additional policies are used, they will be displayed in alphabetical order on the ribbon. When a user applies a policy to a folder by using the folder properties dialog box, the full list of available Personal Tags is shown.

The Personal Tags that are created for the user should have names that clearly describe the type of content that requires the policy. For example, if e-mail messages that mention a patent have to be retained for 7 years, create a policy that is titled “Patent Information” and set it for 2,555 days. Outlook will automatically translate the number of days into a human-readable format and append the length after the title. So, in Outlook, the policy will appear as **Patent Information (7 years)**.

You should also add a description of the policy so that users can get more clarification on which e-mail messages are in scope for that Personal Tag. The description should describe in detail the type of content that falls under that policy. For example:
Policy: Patent Information (7 years)
Description: All email messages that are related to a patent.

This is the order in which a policy takes precedence on an e-mail message:

1. Policy on the e-mail (Personal Tag)
2. Policy on the folder that contains the e-mail
3. Policy on the parent of that folder, and the parent folders above
4. Policy on the mailbox (Default Policy Tag)

For example: A user has a folder named **Financial Documents** with the **Finance (– 3 years)** Retention Policy applied to it. One of the e-mail messages in the folder describes finance department policy and resides in the Financial Documents folder for easy reference. The user can mark that e-mail message with a Retention Policy of **Reference (– Never)** so that the e-mail messages are never deleted, even though the folder policy is **Finance (– 3 years)**.

Distribution lists

If your organization uses Distribution Lists, a Personal Tag that deletes e-mail messages after 1-4 weeks can help users manage their mailbox quota easier. Users can create an Outlook rule to automatically apply the policy to e-mail messages or to have messages delivered to a folder that has the policy applied.

Retention policy warm up period and training

Training users on Retention Policy is important to make sure that they know how to use the system correctly, and that they understand when and why their e-mail messages are being deleted. You should make sure that users understand why the data is being retained or destroyed so that they can apply Personal Tags appropriately, and that they know what content will be destroyed after a certain time.

Suggested steps:

1. Assign policies to user's mailboxes and put their mailboxes on **Retention Hold**. This will prevent any policy from deleting e-mail messages. For more information, see Place a Mailbox on Retention Hold (*http://go.microsoft.com/fwlink/?LinkId=195158*).
2. Give users instructions on how to use Retention Policy. Explain that during the warm-up period, users must apply policies to folders and messages otherwise old message could be deleted. For more information, see Assign Retention Policy to E-mail Messages (*http://go.microsoft.com/fwlink/?LinkId=195157*).
3. A few days before the end of the warm-up period, remind users of the warm-up deadline.
4. At the deadline, remove users from Retention Hold.

Because it can take users some time to adjust to any new system, instituting a warm-up time period to help users ease into working with Retention Policy is very important. Users must be able to apply the correct Personal Tags to the correct folders and get used to the idea of their information being automatically deleted. We recommended that you give users at least 3 months of using Retention Policy with their e-mail before you remove the Retention Hold from users' mailboxes. This way, users can see and have access to the Retention Policy features before any of their information is destroyed. This makes it easier for users to integrate Retention Policy into their workflow and understand what is occurring to their e-mail messages.

Warning:
If you do not have a warm-up period, important e-mail messages could be deleted before the user was able to apply a longer policy.

Similarly, during any period in which users will not be monitoring their e-mail messages, such as being away on extended vacation or parental leave, their mailboxes should be put on Retention Hold. This is so that their information is not accidentally deleted. When they return to work and have had enough time to go through their e-mail messages, turn off Retention Hold.

Important

- If you use a Default Policy Tag, or Retention Policy Tag on the user's mailbox or special folders, and the user uses cached mode to connect to Exchange, there will be an initial degradation in performance in Outlook while their Outlook profile is updated with the policy information. The time that is required to process the data file depends on its size and the speed of the computer. Users should be informed of the performance impact as their mailbox is updated.
- Or, you can delete the user's Outlook profile and create a new profile for that account. When the user starts Outlook, Outlook will download the e-mail messages with the policy information already added. Depending on the size of the account's mailbox, this might be faster than updating the existing account. However, after you create a new profile with that account, all messages must be indexed again to enable searching in Outlook.

Educating users about Retention Policy

Users should be informed about the following aspects of Retention Policy because it will affect their experience and the ultimate effectiveness of your company's Retention Policies. For more information, see Assign Retention Policy to E-mail Messages (*http://go.microsoft.com/fwlink/?LinkId=195157*).

- Users should check and change, if it is necessary, the Retention Policies on their folders so that messages are not accidentally deleted at the end of the warm-up period.
- During the warm-up period, the Retention Policies will not automatically delete messages.
- The Default Policy Tag will delete all e-mail messages that are older than the policy length unless the users change the Retention Policy on their folders or individual e-mail messages. The retention length of the Default Policy Tag should be clearly stated.
- It is not possible for users to change the folder policy on special folders such as the Inbox, Sent Items, and Deleted Items folders. If there is a policy on the special folders, the policy should be clearly stated.
- If users want messages in a special folder to have a different policy, they can manually apply a Personal Tag to those messages.
- If a user adds a Personal Tag to an e-mail message, that Personal Tag will take precedence over the folder policy, or the Default Policy Tag.
- Retention Policy only applies to e-mail messages. Therefore, all meetings and appointments on their calendars will not be deleted.
- Subfolders inherit their parent folder's Retention Policy.
- Retention Policy does not delete messages in Outlook data files (.pst).
- Users can apply a Retention Policy to a message by using the Assign Policy gallery in the ribbon.
- Users can apply a Retention Policy to folders they have created by using **Set Folder Policy** in the Assign Policy gallery.
- Users can get a list of all messages that will expire within 30 days by selecting **View Items Expiring Soon** in the Assign Policy gallery.

- Users can determine which Retention Policy is being applied to a message by looking under the CC line in the Reading Pane or at the bottom on the reading inspector.

Users under legal hold or investigation

There are two options for legal hold with Outlook 2010 and Exchange Server 2010: Retention Hold and Litigation Hold. Retention Hold makes it obvious to the user that the mailbox has been put on hold. Litigation Hold is silent and does not indicate to the user that the mailbox is under investigation.

The following table summarizes which features are available with Retention Hold and Litigation Hold. The Recoverable Items and Copy on Write features are explained in the following sections.

Feature	Retention Hold	Litigation Hold
Retention policies are enforced on the server	No	Yes. Deletions are captured in a hidden folder in the user's mailbox so they are not destroyed.
Archive policies are enforced on the server	No	Yes
The Recoverable Items container can empty itself	Yes	No
Copy on Write is turned on	No	Yes

Recover Deleted Items

The Recover Deleted Items folder in Exchange, previously known as the Dumpster, provides a holding area for items that are deleted by the user in Outlook, Microsoft Outlook Web Access (OWA), and other e-mail clients. Users can recover items they have deleted in Outlook and OWA by accessing the Recover Deleted Items folder. For more information, see Recover Deleted Items (*http://go.microsoft.com/fwlink/?LinkId=195172*).

By default, the Recover Deleted Items folder keeps deleted items for 14 days or until the storage quota for the folder is reached. The Recover Deleted Items folder will remove items on a first in, first out (FIFO) basis if the folder storage quota is exceeded. If Litigation Hold for a user's mailbox is turned on, the Recover Deleted Items folder cannot be purged by using either of these methods. This ensures that the data that was deleted can be searched and recovered. For more information, see Understanding Legal Hold (*http://go.microsoft.com/fwlink/?LinkId=195174*).

Copy on Write

With Exchange Server 2010, you can ensure that all versions of an e-mail message are saved with the Copy on Write feature. This feature will copy the original version of an e-mail message that was

modified and store it in a hidden folder named Versions. The properties on an e-mail message that can trigger a copy can be found in Understanding Legal Hold (*http://go.microsoft.com/fwlink/?LinkId=195174*). This functionality is automatically turned on by using Litigation Hold.

Using Retention Hold

If you have a user whose e-mail messages are subject to investigation and should not be deleted, Retention Hold can be turned on for that user's mailbox. By using Retention Hold, you can display a comment in the Backstage view, which will inform the user of the Retention Hold status. If users have a Personal Archive, they will have to manually move messages to the archive. Retention Hold prevents the server from letting Retention and Archive policies to delete or move messages.

While a user's mailbox is on Retention Hold, that user's mailbox quota should be increased to let them to keep e-mail messages that are relevant to the investigation.

When a user is put on Retention Hold, they should be informed of the following:

- Retention Policies and Archive Polices will no longer delete or move messages.
- The user can manually move messages to the Personal Archive, if they have one.

Using Litigation Hold

If you have a user who is frequently under legal investigation or is part of many investigations at the same time, Litigation Hold is a way to ensure that all of the user's e-mail messages are being retained without affecting the e-mail user experience. By using Litigation Hold, Outlook does not inform the user that the user's mailbox is on hold. This can be useful in internal investigation.

Because Retention and Archive policies let users delete and move messages, Litigation Hold enables the user to work as if they are not under investigation. The Recover Deleted Items folder captures all deleted items, and the Copy on Write feature captures all versions of e-mail messages. The combination of these features relieves the burden of maintaining information that might be pertinent to a legal investigation. For more information, see Understanding Legal Hold (*http://go.microsoft.com/fwlink/?LinkId=195174*).

Planning a Personal Archive deployment

A Personal Archive can be used to replace Outlook data files (.pst) used to archive e-mail messages in your organization. Also, it can give users additional room for e-mail messages that they must keep for compliance reasons.

As part of planning a Personal Archive deployment, consider the following key steps:

- Determine your organization's archive policies.
- Educate users about the Personal Archive.
- Manage the Outlook data files (.pst) in your organization.

Determining your archive policies

By default, the following archive policies are created for a user when they are given a Personal Archive:

- **Default Policy (– 2 years)** The default archive policy applies to a user's entire mailbox. It archives all e-mail messages for which the received date is older than 2 years.
- **Personal Tags** By default, the following Personal Tags are given to users to apply to their folders and e-mail messages.
  - 6 months
  - 1 year
  - 2 years
  - 5 years
  - Never

Archive policies cannot be applied through Exchange to special folders in the user's mailbox, such as the Inbox and Sent Items folders. By default, all folders in the user's mailbox will inherit the Default Policy. But the user can change the policy on any folder or e-mail message by using Personal Tags.

Educating users about the Personal Archive

Users should be informed about the following aspects of the Personal Archive, because it will affect their experience and the way they use the feature. We recommend a warm-up period during which archive policies are set on users' mailbox folders. This is so that users are not surprised when e-mail messages are moved to the archive overnight.

- The Personal Archive cannot be used when the user is offline, or if a connection to the user's Exchange Server computer cannot be established.
- Over a 24 hour window, Exchange Server automatically moves e-mail messages that are ready to be archived. Therefore, users who set an archive policy on a folder will not see an immediate result of this action.
- There is no way for the user to archive messages immediately by using Exchange Server. Messages that must be archived immediately must be moved to the archive by the user.
- AutoArchive will not be available to the user and will not archive messages. If users have set up AutoArchive to delete or move messages to an Outlook data file (.pst), they must apply the appropriate Retention and Archive policies to achieve the same effect.
- Folders that are created in the archive have the same Retention Policy as they did in the mailbox. Similarly, messages in the archive have the same Retention Policy (if one was applied) as they did in the mailbox. Messages with a Retention Policy will expire in the Personal Archive.

Outlook data files (.pst) in your organization

To ensure that your organization's e-mail is not moved out of the user's mailbox or your organization's compliance infrastructure, you can deploy the **DisableCrossAccountCopy** registry key. This will prevent the user from saving the information to an Outlook data file (.pst), or from copying it to another

e-mail account in Outlook. You can deploy this registry key by manually adding it to the user's registry or by using the **Prevent copying or moving items between accounts** setting in Group Policy.

This registry key provides more control than the two typically used registry keys **DisablePST** and **PSTDisableGrow** in Outlook 2010. Because it prevents users from moving data out of restricted accounts without limiting their .pst use, users are able to use personal e-mail accounts in Outlook that might deliver e-mail messages to a .pst file. They are also able to read messages and copy messages from their existing .pst file. The **DisableCrossAccountCopy** registry key is recommended to completely replace the need for **DisablePST** and **PSTDisableGrow** for these reasons. Optionally, you can also prevent users from copying data out of their synchronized lists in Microsoft SharePoint 2010 Products.

The **DisableCrossAccountCopy** registry key is located in **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook**.

Registry entry	Type	Value	Description	Deployment
DisableCrossAccountCopy	REG_MULTI_SZ	There are three string values that can be defined for this registry key: 1. An asterisk (*****) will restrict copying or moving messages out of any account or Outlook data file (.pst). 2. Domain name of e-mail account to be restricted. You can specify the domain of the accounts that you want to restrict. For example, **contoso.com**. 3. **SharePoint** This string will restrict copying or moving data out of all SharePoint lists.	Defines accounts or Outlook data files (.pst) where moving or copying data out of that location is not allowed.	This registry key can be deployed by manually adding it to the user's registry or by using the **Prevent copying or moving items between accounts** setting in Group Policy.

Or, you can set the **DisableCrossAccountCopy** in Group Policy by enabling the **Prevent copying or moving items between accounts** setting under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Account Settings\Exchange**.

If your organization has already deployed the **DisablePST** or **PSTDisableGrow** registry keys, they will not affect the behavior of the **DisableCrossAccountCopy** key. If you have users who do not use Outlook 2010, all three keys can be deployed at the same time. However, for most organizations, the **DisablePST** and **PSTDisableGrow** registry keys are unnecessary.

The following is the list of ways that copying or moving e-mail messages out of an account or Outlook data file (.pst) will be restricted:

- Users cannot drag-and-drop messages from a restricted account into another account or Outlook data file (.pst).
- Users cannot use the **Move** menu to move or copy messages from a restricted account into another account or Outlook data file (.pst).
- When using AutoArchive, all accounts that have been restricted will not have the option to archive data.
- In the **Mailbox Cleanup** menu of the Backstage view, the Archive option will not list restricted accounts as an option for archiving.
- Rules will not move messages out of the restricted accounts.
- Users will be unable to export messages out of restricted accounts.
- The Clean Up feature will not delete redundant parts of e-mail conversations in restricted accounts.

To prevent users from moving or copying messages from restricted accounts to their computers, you can deploy the **DisableCopyToFileSystem** registry key.

The **DisableCopyToFileSystem** registry key is located in **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook**.

Registry entry	Type	Value	Description	Deployment
DisableCopyToFileSystem	REG_MULTI_SZ	There are three string values that can be defined for this registry key: 1. An asterisk (*****) will restrict a user from dragging messages from any account or Outlook data file (.pst) to the computer.	Defines accounts or Outlook data files (.pst) where dragging messages to the computer is not allowed.	This registry key can be deployed by manually adding it to the user's registry.

Registry entry	Type	Value	Description	Deployment
		2. Domain name of e-mail account to be restricted. You can specify the domain of the accounts that you want to restrict. For example, **contoso.com**. 3. **SharePoint** This string will restrict dragging data out of all SharePoint lists to the computer.		

See Also

Place a Mailbox on Retention Hold (*http://go.microsoft.com/fwlink/?LinkId=195158*)

Understanding Legal Hold (*http://go.microsoft.com/fwlink/?LinkId=195174*)

Understanding Retention Tags and Retention Policies: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=195435*)

Understanding Personal Archive: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=169269*)

Plan for security and protection in Outlook 2010

This section describes features in Microsoft Outlook 2010 that can help keep an organization's e-mail messaging secure.

In this section:

Article	Description
Choose security and protection settings for Outlook 2010	Describes how to customize many of the security-related features in Outlook 2010, including how the security settings are enforced, which kind of ActiveX controls can run, custom forms security, and programmatic security settings.
Plan attachment settings in Outlook 2010	Describes how to configure Outlook 2010 attachment security settings by using Group Policy and the Outlook 2010 template (Outlk14.adm).
Plan for e-mail messaging cryptography in Outlook 2010	Describes how to configure security features in Outlook 2010 to help users send and receive cryptographic e-mail messages.
Plan for limiting junk e-mail in Outlook 2010	Discusses how the Outlook 2010 Junk E-mail Filter works, and which settings you can configure for the Junk E-mail Filter and for automatic picture download.

Choose security and protection settings for Outlook 2010

You can customize many of the security-related features in Microsoft Outlook 2010. This includes how the security settings are enforced, which kind of ActiveX controls can run, custom forms security, and programmatic security settings. You can also customize Outlook 2010 security settings for attachments, Information Rights Management, junk e-mail, and encryption, which are covered in additional articles listed in Additional settings later in this article.

Caution:
By default, Outlook is configured to use high security-related settings. High security levels can result in limitations to Outlook functionality, such as restrictions on e-mail message attachment file types. Be aware that lowering any default security settings might increase the risk of virus execution or virus propagation. Use caution, and read the documentation before you modify these settings.

In this article:

Overview

By default, Outlook is configured to use high security-related settings. High security levels can result in limitations to Outlook functionality, such as restrictions on e-mail message attachment file types. You might need to lower default security settings for your organization. However, be aware that lowering any default security settings might increase the risk of virus execution or propagation.

Before you begin configuring security settings for Outlook 2010 by using Group Policy or the Outlook Security template, you must configure the Outlook Security Mode in Group Policy. If you do not set the Outlook Security Mode, Outlook 2010 uses the default security settings and ignores any Outlook 2010 security settings that you have made.

For information about how to download the Outlook 2010 adminstrative template, and about other Office 2010 Administrative Templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://technet.microsoft.com/library/2aa26c81-d80c-4be4-9114-8ea205ef47f2(Office.14).aspx*). For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*).

Specify how security settings are enforced in Outlook

As with Microsoft Office Outlook 2007, you can configure security options for Outlook 2010 by using Group Policy (recommended) or modify security settings by using the Outlook Security template and publish the settings to a form in a top-level folder in Exchange Server public folders. Unless you have Office Outlook 2003 or earlier versions in your environment, we recommend that you use Group Policy to configure security settings. To use either option, you must enable the Outlook Security Mode setting in Group Policy and set the Outlook Security Policy value. Default security settings in the product are enforced if you do not enable this setting. The Outlook Security Mode setting is in the Outlook 2010 Group Policy template (Outlk14.adm) under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings**. When you enable the **Outlook Security Mode** setting, you have the four Outlook Security Policy options, which are described in the following table.

Outlook Security Mode option	Description
Outlook Default Security	Outlook ignores any security-related settings configured in Group Policy or when using an Outlook Security template. This is the default settings.
Use Outlook Security Group Policy	Outlook uses the security settings from Group Policy (recommended).
Use Security Form from 'Outlook Security Settings' Public Folder	Outlook uses the settings from the security form published in the designated public folder.
Use Security Form from 'Outlook 10 Security Settings' Public Folder	Outlook uses the settings from the security form published in the designated public folder.

Customize security settings by using Group Policy

When you use Group Policy to configure security settings for Outlook 2010, consider the following factors:

- **Settings in Outlook Security template must be manually migrated to Group Policy.** If you previously used the Outlook Security template to manage security settings and now choose to use

Group Policy to enforce settings in Outlook 2010, you must manually migrate the settings that you configured earlier to the corresponding Group Policy settings for Outlook 2010.

- **Customized settings configured by using Group Policy might not be active immediately.** You can configure Group Policy to refresh automatically (in the background) on users' computers while users are logged on, at a frequency that you determine. To ensure that new Group Policy settings are active immediately, users must log off and log back on to their computers.
- **Outlook checks security settings only at startup.** If security settings are refreshed while Outlook is running, the new configuration is not used until the user closes and restarts Outlook.
- **No customized settings are applied in Personal Information Manager (PIM)-only mode.** In PIM mode, Outlook uses the default security settings. No administrator settings are necessary or used in this mode.

Special environments

When you use Group Policy to configure security settings for Outlook 2010, consider whether your environment includes one or more of the scenarios shown in the following table.

Scenario	Issue
Users who access their mailboxes by using a hosted Exchange Server	If users access mailboxes by using a hosted Exchange Server, you might use the Outlook Security template to configure security settings or use the default Outlook security settings. In hosted environments, users access their mailboxes remotely; for example, by using a virtual private network (VPN) connection or by using Outlook Anywhere (RPC over HTTP). Because Group Policy is deployed by using Active Directory and in this scenario, the user's local computer is not a member of the domain, Group Policy security settings cannot be applied. Also, by using the Outlook Security template to configure security settings, users automatically receive updates to security settings. Users cannot receive updates to Group Policy security settings unless their computer is in the Active Directory domain.
Users with administrative rights on their computers	Restrictions to Group Policy settings are not enforced when users log on with administrative rights. Users with administrative rights can also change the Outlook security settings on their computer and can remove or alter the restrictions that you have configured. This is true not only for Outlook security settings, but for all Group Policy settings. Although this can be problematic when an organization intends to have standardized settings for all users, there are mitigating factors: • Group Policy overrides local changes at the next logon. Changes to Outlook security settings revert to the Group Policy settings when the user logs on.

Scenario	Issue
	• Overriding a Group Policy setting affects only the local computer. Users with administrative rights affect only security settings on their computer, not the security settings for users on other computers. • Users without administrative rights cannot change policies. In this scenario, Group Policy security settings are as secure as settings configured by using the Outlook Security template.
Users who access Exchange mailboxes by using Outlook Web App	Outlook and Outlook Web App do not use the same security model. OWA has separate security settings stored on the Exchange Server computer.

How administrator settings and user settings interact in Outlook 2010

Security settings that are defined by the user in Outlook 2010 work as if they are included in the Group Policy settings that you define as the administrator. When there is a conflict between the two, settings with a higher security level override settings with a lower security level.

For example, if you use the Group Policy Attachment Security setting **Add file extensions to block as Level 1** to create a list of Level 1 file name extensions to be blocked, your list overrides the default list provided with Outlook 2010 and overrides the user's settings for Level 1 file name extensions to block. Even if you allow users to remove file name extensions from the default Level 1 group of excluded file types, users cannot remove file types that were added to the list.

For example, if the user wants to remove the file name extensions .exe, .reg, and .com from the Level 1 group, but you use the **Add Level 1 file extensions** Group Policy setting to add .exe as a Level 1 file type, the user can only remove .reg and .com files from the Level 1 group in Outlook.

Working with Outlook COM add-ins

A Component Object Model (COM) add-in should be coded so that it takes advantage of the Outlook trust model to run without warning messages in Outlook 2010. Users might continue to see warnings when they access Outlook features that use the add-in, such as when they synchronize a hand-held device with Outlook 2010 on their desktop computer.

However, users are less likely to see warnings in Outlook 2010 than in Office Outlook 2003 or earlier versions. The Object Model (OM) Guard that helps prevent viruses from using the Outlook Address Book to propagate themselves is updated in Office Outlook 2007 and Outlook 2010. Outlook 2010 checks for up-to-date antivirus software to help determine when to display address book access warnings and other Outlook security warnings.

The OM Guard cannot be modified by using the Outlook security form or Group Policy. However, if you use default Outlook 2010 security settings, all COM add-ins that are installed in Outlook 2010 are trusted by default. If you customize security settings by using Group Policy, you can specify COM add-ins that are trusted and that can run without encountering the Outlook object model blocks.

To trust a COM add-in, you include the file name for the add-in, in a Group Policy setting with a calculated hash value for the file. Before you can specify an add-in as trusted by Outlook, you must install a program to calculate the hash value. For information about how to do this, see Manage trusted add-ins for Outlook 2010 (*http://technet.microsoft.com/library/96604a08-00aa-48dd-81dc-2d9379f474fe(Office.14).aspx*).

If you enforce customized Outlook security settings with the Microsoft Exchange Server security form published in an Exchange Server public folder, you can learn how to trust COM add-ins. Scroll down to the **Trusted Code tab** section in the Microsoft Office 2003 Resource Kit article, Outlook Security Template Settings (*http://go.microsoft.com/fwlink/?LinkId=75744*).

If the user continues to see security prompts after the add-in is included in the list of trusted add-ins, you must work with the COM add-in developer to resolve the problem. For more information about coding trusted add-ins, see Important Security Notes for Microsoft Outlook COM Add-in Developers (*http://go.microsoft.com/fwlink/?LinkId=74697*).

Customize ActiveX and custom forms security in Outlook 2010

You can specify ActiveX and custom forms security settings for Outlook 2010 users. Custom forms security settings include options for changing how Outlook 2010 restricts scripts, custom controls, and custom actions.

Customize how ActiveX controls behave in one-off forms

When Outlook receives a message that contains a form definition, the item is a one-off form. To help prevent unwanted script and controls from running in one-off forms, Outlook does not load ActiveX controls in one-off forms by default.

You can lock down the settings to customize ActiveX controls by using the Group Policy Outlook 2010 template (Outlk14.adm). Or you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the settings. In Group Policy, use the **Allow ActiveX One Off Forms** setting under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security**. In the OCT, the **Allow ActiveX One Off Forms** setting is in corresponding location on the **Modify user settings** page of the OCT. For more information about the OCT, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

When you enable **Allow ActiveX One Off Forms** setting, you have three options, which are described in the following table.

Option	Description
Allows all ActiveX Controls	Allows all ActiveX controls to run without restrictions.
Allows only Safe Controls	Allows only safe ActiveX controls to run. An ActiveX control is safe if it is signed with Authenticode and the signer is listed in the Trusted Publishers List.
Load only Outlook Controls	Outlook loads only the following controls. These are the only controls that can be used in one-off forms. • Controls from fm20.dll • Microsoft Office Outlook Rich Format Control • Microsoft Office Outlook Recipient Control • Microsoft Office Outlook View Control

If you do not configure any of these options, the default is to load only Outlook controls.

Customize custom forms security settings

You can lock down the settings to configure security for custom forms by using the Group Policy Outlook 2010 template (Outlk14.adm). Or you can configure default settings by using the OCT, in which case users can change the settings. In Group Policy, the settings are under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Custom Form Security**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT. The settings that you can configure for scripts, custom controls, and custom actions are shown in the following table:

Option	Description
Allow scripts in one-off Outlook forms	Run scripts in forms where the script and the layout are contained in the message. If users receive a one-off form that contains script, users are prompted to ask whether they want to run the script.
Set Outlook object model Custom Actions execution prompt	Specifies what occurs when a program attempts to run a custom action by using the Outlook object model. A custom action can be created to reply to a message and circumvent the programmatic send protections previously described. Select one of the following: • **Prompt user** enables the user to receive a message and decide whether to allow programmatic send access.

Option	Description
	• **Automatically approve** always allows programmatic send access without displaying a message. • **Automatically deny** always denies programmatic send access without displaying a message. • **Prompt user based on computer security** enforces the default configuration in Outlook 2010.

Customize programmatic settings in Outlook 2010

As an administrator of Outlook 2010, you can configure programmatic security settings to manage restrictions for the Outlook object model. The Outlook object model lets you programmatically manipulate data that is stored in Outlook folders.

Note:
The Exchange Server Security template includes settings for Collaboration Data Objects (CDO). However, using CDO with Outlook 2010 is not supported.

You can use Group Policy to configure programmatic security settings for the Outlook object model. In Group Policy, load the Outlook 2010 template (Outlk14.adm). The Group Policy settings are located under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Programmatic Security**. These settings cannot be configured by using the Office Customization Tool.

The following are descriptions of the Group Policy options for programmatic settings. You can choose one of the following settings for each item:

- **Prompt user** Users receive a message allowing them to choose whether to allow or deny the operation. For some prompts, users can choose to allow or deny the operation without prompts for up to 10 minutes.
- **Automatically approve** Outlook automatically grants programmatic access requests from any program. This option can create a significant vulnerability, and we do not recommend it.
- **Automatically deny** Outlook automatically denies programmatic access requests from any program and the user does not receive a prompt.
- **Prompt user based on computer security** Outlook relies on the setting in the "Programmatic Access" section of the Trust Center. This is the default behavior.

The settings that you can configure for programmatic security settings for the Outlook object model are shown in the following table.

Option	Description
Configure Outlook object model prompt when accessing an address book	Specifies what happens when a program attempts to gain access to an address book by using the Outlook object model.
Configure Outlook object model prompt when accessing the **Formula** property of a **UserProperty** object	Specifies what happens when a user adds a Combination or Formula custom field to a custom form and binds it to an Address Information field. By doing this, code can be used to indirectly retrieve the value of the Address Information field by getting the Value property of the field.
Configure Outlook object model prompt when executing Save As	Specifies what happens when a program attempts to programmatically use the Save As command to save an item. When an item has been saved, a malicious program could search the file for e-mail addresses.
Configure Outlook object model prompt when reading address information	Specifies what happens when a program attempts to gain access to a recipient field, such as **To**, by using the Outlook object model.
Configure Outlook object model prompt when responding to meeting and task requests	Specifies what happens when a program attempts to send mail programmatically by using the Respond method on task requests and meeting requests. This method is similar to the Send method on mail messages.
Configure Outlook object model prompt when sending mail	Specifies what happens when a program attempts to send mail programmatically by using the Outlook object model.

Additional settings

The following table lists the articles that cover additional security settings not included in this article.

Feature	Related resources
ActiveX controls	Plan security settings for ActiveX controls for Office 2010
Attachments	Plan attachment settings in Outlook 2010
Cryptography	Plan for e-mail messaging cryptography in Outlook 2010
Digital signatures	Plan digital signature settings for Office 2010

Feature	Related resources
Junk e-mail	Plan for limiting junk e-mail in Outlook 2010
Information Rights Management	Plan for Information Rights Management in Office 2010
Protected view	Plan Protected View settings for Office 2010

See Also

Plan security for Office 2010

Plan attachment settings in Outlook 2010

In Microsoft Outlook 2010, you can specify that attachments to Outlook items (such as e-mail messages or appointments) are restricted based on the file type of the attachment. A file type can have either a Level 1 or Level 2 restriction. You can also configure what users can do with attachment restrictions. For example, you could allow users to change the restrictions for a group of attachment file types from Level 1 (user cannot view the file) to Level 2 (user can open the file after saving it to disk).

Note:
To enforce attachment settings, you must first configure the method that Outlook 2010 uses to enforce security settings by using Group Policy. For information about how to set the Outlook 2010 method to enforce security settings, see Specify how security settings are enforced in Outlook in Choose security and protection settings for Outlook 2010.

This article is for Outlook administrators. To learn more about why some Outlook attachments are blocked, see Blocked attachments: The Outlook feature you love to hate (*http://go.microsoft.com/fwlink/?LinkId=81268*). To learn how to share files that have restricted file types, see Blocked attachments in Outlook (*http://go.microsoft.com/fwlink/?LinkId=188575*).

In this article:

Overview

There is restricted access to some attachments in items (such as e-mail messages or appointments) in Outlook 2010. Files that have specific file types can be categorized as Level 1 (the user cannot view the file) or Level 2 (the user can open the file after saving it to disk).

By default, Outlook 2010 classifies several file types as Level 1 and blocks files that have those extensions from being received by users. Examples include .cmd, .exe, and .vbs file name extensions. As an administrator, you can use Group Policy to manage how a file type is categorized for e-mail attachment blocking. For example, you can change a file type categorization from Level 1 to Level 2 or create a list of Level 2 file types. There are no Level 2 file types by default.

You can configure Outlook 2010 attachment security settings by using Group Policy and the Outlook 2010 template (Outlk14.adm). Most of the attachment security settings are the found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Attachment Security**. Settings to prevent users from customizing attachment security settings and to use Protected View for attachments received from internal senders are found under

User Configuration\Administrative Templates\Microsoft Outlook 2010\Security. Attachment security settings cannot be configured by using the Office Customization Tool (OCT).

For more information about Protected View, see Plan Protected View settings for Office 2010.

For information about how to download the Outlook 2010 adminstrative template, and about other Office 2010 Administrative Templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://technet.microsoft.com/library/2aa26c81-d80c-4be4-9114-8ea205ef47f2(Office.14).aspx*). For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*).

Add or remove Level 1 file name extensions

Level 1 files are hidden from the user. The user cannot open, save, or print a Level 1 attachment. (If you specify that users can demote a Level 1 attachment to a Level 2 attachment, Level 2 restrictions apply to the file.) If a user receives an e-mail message or appointment that has a blocked attachment, the InfoBar at the top of the item displays a list of the blocked files. (The InfoBar does not appear on a custom form.) When you remove a file type from the Level 1 list, attachments that have that file type are no longer blocked. For the default list of Level 1 file types, see Attachment file types restricted by Outlook 2010 (*http://technet.microsoft.com/library/bc667b4c-1645-42be-8dc0-af56dc11ef5b(Office.14).aspx*).

The settings in the following table let you add or remove Level 1 file types from the default list. In Group Policy, these settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Attachment Security**. These settings cannot be configured by using the OCT.

Option	Description
Add file extensions to block as Level 1	Specifies the file types (usually three letters) you want to add to the Level 1 file list. Do not enter a period before each file name extensions. If you enter multiple file name extensions, separate them with semicolons.
Remove file extensions blocked as Level 1	Specifies the file types (usually three letters) you want to remove from the Level 1 file list. Do not enter a period before each file type. If you enter multiple file types, separate them with semicolons.

Add or remove Level 2 file name extensions

With a Level 2 file type, the user is required to save the file to the hard disk before the file is opened. A Level 2 file cannot be opened directly from an item.

When you remove a file type from the Level 2 list, it becomes a regular file type that can be opened, saved, and printed in Outlook 2010. There are no restrictions on the file.

The settings in the following table let you add or remove Level 2 file types from the default list. In Group Policy, these settings are found under **User Configuration\Administrative Templates\ Microsoft Outlook 2010\Security\Security Form Settings\Attachment Security**. These settings cannot be configured by using the OCT.

Option	Description
Add file extensions to block as Level 2	Specifies the file name extension (usually three letters) you want to add to the Level 2 file list. Do not enter a period before each file name extension. If you enter multiple file name extensions, separate them with semicolons.
Remove file extensions blocked as Level 2	Specifies the file name extension (usually three letters) you want to remove from the Level 2 file list. Do not enter a period before each file name extension. If you enter multiple file name extensions, separate them with semicolons.

Configure additional attachment file restrictions

The settings in the following table are additional settings that you can configure for attachments in Group Policy. In Group Policy, these settings are found under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Attachment Security**. These settings cannot be configured by using the OCT.

Option	Description
Display Level 1 attachments	Enables users to access all attachments that have Level 1 file types by first saving the attachments to disk, and then opening them (as with Level 2 attachments).
Allow users to demote attachment	Enables users to create a list of attachment file name extensions to demote from Level 1 to Level 2. If you do not configure this Group Policy setting, the default behavior in Outlook is to ignore the user's list. The registry key in which users create the list of file

Option	Description
s to Level 2	types to demote is: **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\Level1Remove**. In the registry key, users specify the file name extensions (usually three letters) to remove from the Level 1 file list, separated with semicolons.
Do not prompt about Level 1 attachments when sending an item	Prevents users from receiving a warning when they send an item that contains a Level 1 attachment. This option affects only the warning. Once the item is sent, recipients might be unable to view or access the attachment, depending on their security settings. If you want users to be able to post items to a public folder without receiving this prompt, you must enable this setting and the **Do not prompt about Level 1 attachments when closing an item** setting.
Do not prompt about Level 1 attachments when closing an item	Prevents users from receiving a warning when they close an e-mail message, appointment, or other item that contains a Level 1 attachment. This option affects only the warning. Once the item is closed, the user cannot view or gain access to the attachment. If you want users to be able to post items to a public folder without receiving this prompt, you must enable this setting and the **Do not prompt about Level 1 attachments when sending an item** setting.
Display OLE package objects	Displays OLE objects that have been packaged. A package is an icon that represents an embedded or linked OLE object. When you double-click the package, the program that was used to create the object either plays the object (for example, if the object is a sound file) or opens and displays the object. Allowing Outlook to display OLE package objects can be problematic, because the icon can be easily changed and used to disguise malicious files.

The settings in the following table are found in Group Policy under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security**. These settings cannot be configured by using the OCT.

Action	Description
Prevent users from customizing attachment security settings	When enabled, users cannot customize the list of file types that are allowed as attachments in Outlook, regardless of how you have configured other Outlook security settings.
Use Protected View for attachments received from	When enabled, attachments received from senders within your organization open in Protected View. This setting only applies to

Action	Description
internal senders	Microsoft Outlook accounts that connect to a Microsoft Exchange Server computer.

See Also

Choose security and protection settings for Outlook 2010

Attachment file types restricted by Outlook 2010 (*http://technet.microsoft.com/library/bc667b4c-1645-42be-8dc0-af56dc11ef5b(Office.14).aspx*)

Plan Protected View settings for Office 2010

Plan for e-mail messaging cryptography in Outlook 2010

Microsoft Outlook 2010 supports security-related features to help users send and receive cryptographic e-mail messages. These features include cryptographic e-mail messaging, security labels, and signed receipts.

Note:
To obtain full security functionality in Microsoft Outlook, you must install Outlook 2010 with local administrative rights.

In this article:

About Cryptographic messaging features in Outlook 2010

Outlook 2010 supports cryptographic messaging features that enable users to do the following:

- **Digitally sign an e-mail message.** Digital signing provides nonrepudiation and verification of contents (the message contains what the person sent, without any changes).
- **Encrypt an e-mail message.** Encryption helps ensure privacy by making the message unreadable to anyone other than the intended recipient.

Additional features can be configured for security-enhanced messaging. If your organization provides support for these features, security-enhanced messaging enables users to do the following:

- **Send an e-mail message that uses a receipt request.** This helps verify that the recipient is validating the user's digital signature (the certificate that the user applied to a message).
- **Add a security label to an e-mail message.** Your organization can create a customized S/MIME V3 security policy that adds labels to messages. An S/MIME V3 security policy is code that you add to Outlook. It adds information to the message header about the sensitivity of the message. For more information, see Security labels and signed receipts later in this article.

How Outlook 2010 implements cryptographic messaging

The Outlook 2010 cryptography model uses public key encryption to send and receive signed and encrypted e-mail messages. Outlook 2010 supports S/MIME V3 security, which allows users to exchange security-enhanced e-mail messages with other S/MIME e-mail clients over the Internet or intranet. E-mail messages encrypted by the user's public key can be decrypted only by using the associated private key. This means that when a user sends an encrypted e-mail message, the recipient's certificate (public key) encrypts it. When a user reads an encrypted e-mail message, the user's private key decrypts it.

In Outlook 2010, users are required to have a security profile to use cryptographic features. A security profile is a group of settings that describes the certificates and algorithms used when a user sends messages that use cryptographic features. Security profiles are configured automatically if the profile is not already present when:

- The user has certificates for cryptography on his or her computer.
- The user begins to use a cryptographic feature.

You can customize these security settings for users in advance. You can use registry settings or Group Policy settings to customize Outlook to meet your organization's cryptographic policies and to configure (and enforce, by using Group Policy) the settings that you want in the security profiles. These settings are described in Configuring Outlook 2010 cryptographic settings later in this article.

Digital IDs: A combination of public/private keys and certificates

S/MIME features rely on digital IDs, which are also known as digital certificates. Digital IDs associate a user's identity with a public and private key pair. The combination of a certificate and private/public key pair is called a digital ID. The private key can be saved in a security-enhanced store, such as the Windows certificate store, on the user's computer, or on a Smart Card. Outlook 2010 fully supports the X.509v3 standard, which requires that public and private keys are created by a certification authority in an organization, such as a Windows Server 2008 computer that is running Active Directory Certificate Services or by a public certification authority such as VeriSign. For information about which option might be best for your organization, see Digital certificate: Self-signed or issued by CAs in Plan digital signature settings for Office 2010.

Users can obtain digital IDs by using public Web-based certification authorities such as VeriSign and Microsoft Certificate Services. For more information about how users can obtain a digital ID, see the Outlook Help topic Get a digital ID (*http://go.microsoft.com/fwlink/?LinkId=185585*). As an administrator, you can provide digital IDs to a group of users.

When certificates for digital IDs expire, users typically must obtain updated certificates from the issuing certification authority. If your organization relies on Windows Server 2003 Certificate Authority (CA) or Active Directory Certificate Services (AD CS) in Windows Server 2008 for certificates, Outlook 2010 automatically manages certificate update for users.

Managing cryptographic digital IDs

Outlook 2010 provides ways for users to manage their digital IDs — the combination of a user's certificate and public and private encryption key set. Digital IDs help keep users' e-mail messages secure by letting them exchange cryptographic messages. Managing digital IDs includes the following:

- Obtaining a digital ID. For more information about how users can obtain a digital ID, see the Outlook Help topic Get a digital ID (*http://go.microsoft.com/fwlink/?LinkId=185*585).
- Storing a digital ID, so you can move the ID to another computer or make it available to other users.
- Providing a digital ID to other users.
- Exporting a digital ID to a file. This is useful when the user is creating a backup or moving to a new computer.
- Importing a digital ID from a file into Outlook. A digital ID file might be a user's backup copy or might contain a digital ID from another user.
- Renewing a digital ID that has expired.

A user who performs cryptographic messaging at more than one computer must copy his or her digital ID to each computer.

Places to store digital IDs

Digital IDs can be stored in three locations:

- **Microsoft Exchange Global Address Book** Certificates generated by CA or by AD CS are automatically published in the global address book (GAL). Externally generated certificates can be manually published to the global address book. To do this in Outlook 2010, on the **File** tab, click **Options**, and then click **Trust Center**. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings**. On the **E-mail Security** tab, under **Digital IDs (Certificates)**, click the **Publish to GAL** button.
- **Lightweight Directory Access Protocol (LDAP) directory service** External directory services, certificate authorities, or other certificate providers can publish their users' certificates through an LDAP directory service. Outlook allows access to these certificates through LDAP directories.
- **Microsoft Windows file** Digital IDs can be stored on users' computers. Users export their digital ID to a file from Outlook 2010. To do this, on the **File** tab, click **Options**, and then click **Trust Center**. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings**. On the **E-mail Security** tab, under **Digital IDs (Certificates)**, click the **Import/Export** button. Users can encrypt the file when they create it by providing a password.

Providing digital IDs to other users

If a user wants to exchange cryptographic e-mail messages with another user, they must have each other's public key. Users provide access to their public key through a certificate.

There are several ways to provide a digital ID to other users, including the following:

- **Use a certificate to digitally sign an e-mail message.** A user provides his or her public key to another user by composing an e-mail message and digitally signing the message by using a certificate. When Outlook users receive the signed message, they right-click the user's name on the **From** line, and then click **Add to Contacts**. The address information and the certificate are saved in the Outlook user's contacts list.
- **Provide a certificate by using a directory service, such as the Microsoft Exchange Global Address Book.** Another alternative is for a user to automatically retrieve another user's certificate from an LDAP directory on a standard LDAP server when he or she sends an encrypted e-mail message. To gain access to a certificate in this manner, users must be enrolled in S/MIME security with digital IDs for their e-mail accounts.

  A user can also obtain certificates from the global address book.

Importing digital IDs

Users can import a digital ID from a file. This is useful, for example, if a user wants to send cryptographic e-mail messages from a new computer. Each computer from which the user sends cryptographic e-mail messages must have the user's certificates installed. Users export their digital ID to a file from Outlook 2010. To do this, on the **File** tab, click **Options**, and then click **Trust Center**. Under **Microsoft Outlook Trust Center**, click **Trust Center Settings**. On the **E-mail Security** tab, under **Digital IDs (Certificates)**, click the **Import/Export** button.

Renewing keys and certificates

A time limit is associated with each certificate and private key. When the keys provided by CA or by AD CS approach the end of the designated time period, Outlook displays a warning message and offers to renew the keys. Outlook prompts the user, offering to send the renewal message to the server on each user's behalf.

If users do not choose to renew a certificate before it expires, or if they use another certification authority instead of in CA or AD CS, the user must contact the certification authority to renew the certificate.

Security labels and signed receipts

Outlook 2010 includes support for S/MIME V3 Enhanced Security Services (ESS) extensions about security labels and signed receipts. These extensions help you provide security-enhanced e-mail communications within your organization and to customize security to fit your requirements.

If your organization develops and provides S/MIME V3 security policies to add custom security labels, the code in the security policies can enforce attaching a security label to an e-mail message.

Two examples of security labels include the following:

- An Internal Use Only label might be implemented as a security label to apply to mail that should not be sent or forwarded outside your company.
- A label can specify that certain recipients cannot forward or print the message, if the recipient also has the security policy installed.

Users can also send security-enhanced receipt requests with messages to verify that the recipients recognize the user's digital signature. When the message is received and saved (even if it is not yet read) and the signature is verified, a receipt implying that the message was read is returned to the user's Inbox. If the user's signature is not verified, no receipt is sent. When the receipt is returned, because the receipt is also signed, you have verification that the user received and verified the message.

Configuring Outlook 2010 cryptographic settings

You can control many aspects of Outlook 2010 cryptography features to help configure more secure messaging and message encryption for your organization by using the Outlook 2010 Group Policy template (Outlook14.adm). For example, you can configure a Group Policy setting that requires a security label on all outgoing mail or a setting that disables publishing to the global address list. You can also use the Office Customization Tool (OCT) to configure default settings, which enables users to change the settings. Also, there are cryptography configuration options that can only be configured by using registry key settings.

For more information about how to download the Outlook 2010 adminsitrative template, and about other Office 2010 Administrative Templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://technet.microsoft.com/library/2aa26c81-d80c-4be4-9114-8ea205ef47f2(Office.14).aspx*). For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*).

For more information about the OCT, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

You can lock down the settings in the following table to customize cryptography. In the OCT, on the **Modify user settings** page, these settings are under **Microsoft Outlook 2010\Security\Cryptography**. In Group Policy, these settings are under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Cryptography**.

Cryptography option	Description
Always use TNEF formatting in	Always use transport neutral encapsulation format (TNEF) for S/MIME messages instead of the format specified by the user.

Cryptography option	Description
S/MIME messages	
Do not check e-mail address against address of certificates being used	Do not verify user's e-mail address by using address of certificates that are used for encryption or signing.
Do not display **'Publish to GAL'** button	Disable the **Publish to GAL** button on the **E-mail Security** page of the Trust Center.
Do not provide Continue option on Encryption warning dialog boxes	Disable the **Continue** button on encryption settings warning dialog boxes. Users will not be able press **Continue** to send the message.
Enable Cryptography Icons	Display Outlook cryptography icons in the Outlook user interface (UI).
Encrypt all e-mail messages	Encrypt outgoing e-mail messages.
Ensure all S/MIME signed messages have a label	Require all S/MIME-signed messages to have a security label. Users can attach labels to e-mail messages in Outlook 2010. To do this, on the **Options** tab, in the **More Options** group, under **Security**, click the **Security Settings** button. In the **Security Properties** dialog box, select **Add digital signature to this message**. Under **Security Label** for **Policy**, select a label.
Fortezza certificate policies	Enter a list of policies allowed in the policies extension of a certificate that indicate the certificate is a Fortezza certificate. List policies separated by semicolons.
Message formats	Choose message formats to support: S/MIME (default), Exchange, Fortezza, or a combination of these formats.
Message when Outlook	Enter a message to display to users (maximum 255 characters).

Cryptography option	Description
cannot find the digital ID to decode a message	
Minimum encryption settings	Set to the minimum key length for an encrypted e-mail message. Outlook will display a warning message if the user tries to send a message by using an encryption key that is below the minimum encryption key value set. The user can still choose to ignore the warning and send by using the encryption key originally chosen.
Replies or forwards to signed/encrypted messages are signed/encrypted	Enable to turn on signing/encryption when replying/forwarding a signed or encrypted message, even if the user is not configured for S/MIME.
Request an S/MIME receipt for all S/MIME signed messages	Request a security-enhanced receipt for outgoing signed e-mail messages.
Require SUITEB algorithms for S/MIME operations	Use only Suite-B algorithms for S/MIME operations.
Required Certificate Authority	Set the name of the required certification authority (CA). When a value is set, Outlook disallows users from signing e-mail by using a certificate from a different CA.
Run in FIPS compliant mode	Require Outlook to run in FIPS 140-1 mode.
S/MIME interoperability with external clients:	Specify the behavior for handling S/MIME messages: **Handle internally**, **Handle externally**, or **Handle if possible**.

<table>
<tr><th>Cryptography option</th><th>Description</th></tr>
<tr><td>S/MIME receipt requests behavior</td><td>Specify an option for how S/MIME receipt requests are handled:
Open message if receipt can't be sent
Don't open message if receipt can't be sent
Always prompt before sending receipt
Never send S/MIME receipts</td></tr>
<tr><td>Send all signed messages as clear signed messages</td><td>Send signed e-mail messages in clear text.</td></tr>
<tr><td>Sign all e-mail messages</td><td>Require digital signatures on all outgoing e-mail messages.</td></tr>
<tr><td>Signature Warning</td><td>Specify an option for when signature warnings display to users:
Let user decide if they want to be warned. This option enforces the default configuration.
Always warn about invalid signatures.
Never warn about invalid signatures.</td></tr>
<tr><td>URL for S/MIME certificates</td><td>Provide a URL at which users can obtain an S/MIME receipt. The URL can contain three variables (%1, %2, and %3), that will be replaced by the user's name, e-mail address, and language, respectively.
When you specify a value for URL for S/MIME certificates, use the following parameters to send information about the user to the enrollment Web page.

<table><tr><th>Parameter</th><th>Placeholder in URL string</th></tr><tr><td>User display name</td><td>%1</td></tr><tr><td>SMTP e-mail name</td><td>%2</td></tr><tr><td>User interface language ID</td><td>%3</td></tr></table>
For example, to send user information to the Microsoft enrollment Web page, set the URL for S/MIME certificates entry to the following value, including the parameters:
<code>www.microsoft.com/ie/certpage.htm?name=%1&email=%2&helplcid=%3</code></td></tr>
</table>

Cryptography option	Description
	For example, if the user's name is Jeff Smith, e-mail address is someone@example.com, and user interface language ID is 1033, the placeholders are resolved as follows: `www.microsoft.com/ie/certpage.htm?name=Jeff%20Smith&email=someone@example.com&helplcid=1033`

The settings in the following table are in Group Policy under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Cryptography\Signature Status dialog box**. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Cryptography option	Description
Attachment Secure Temporary Folder	Specify a folder path for the Secure Temporary Files Folder. This overrides the default path and we do not recommend it. If you must use a specific folder for Outlook attachments, we recommend that: • You use a local directory (for best performance). • You place the folder under the Temporary Internet Files folder (to benefit from the enhanced security on that folder). • The folder name is unique and difficult to guess.
Missing CRLs	Specify the Outlook response when a certificate revocation list (CRL) is missing: warning (default) or display error. Digital certificates contain an attribute that shows where the corresponding CRL is located. CRLs contain lists of digital certificates that have been revoked by their controlling certification authorities (CAs), typically because the certificates were issued incorrectly or their associated private keys were compromised. If a CRL is missing or unavailable, Outlook cannot determine whether a certificate has been revoked. Therefore, an incorrectly issued certificate or one that has been compromised might be used to gain access to data.
Missing root certificates	Specify the Outlook response when a root certificate is missing: neither error nor warning (default), warning or display error.
Promote Level 2 errors as errors, not warnings	Specify the Outlook response for Level 2 errors: display error or warning (default). Potential Error Level 2 conditions include the following: • Unknown Signature Algorithm • No Signing Certification Found

Cryptography option	Description
	• Bad Attribute Sets • No Issuer Certificate Found • No CRL Found • Out of Date CRL • Root Trust Problem • Out of Date CTL
Retrieving CRLs (Certificate Revocation Lists)	Specify how Outlook behaves when CRL lists are retrieved: • Use system default. Outlook relies on the CRL download schedule that is configured for the operating system. • When online always retrieve the CRL. This option is the default configuration in Outlook. • Never retrieve the CRL.

Configuring additional cryptography settings

The following section provides additional information about configuration options for cryptography.

Security policy settings for general cryptography

The following table shows additional Windows registry settings that you can use for your custom configuration. Theses registry settings are located in **HKEY_CURRENT_USER\Software\Microsoft\Cryptography\SMIME\SecurityPolicies\Default**. There is no corresponding Group Policy.

Registry entry	Type	Value	Description
ShowWithMultiLabels	DWORD	0, 1	Set to **0** to attempt to display a message when the signature layer has different labels set in different signatures. Set to **1** to prevent display of message. Default is **0**.
CertErrorWithLabel	DWORD	0, 1, 2	Set to **0** to process a message that has a certificate error when the message has a label. Set to **1** to deny access to a message that has a certificate error. Set to **2** to ignore the message label and grant access to the message. (The user still sees a certificate error.) Default is **0**.

See Also

Plan for security and protection in Outlook 2010

Plan security for Office 2010

Plan digital signature settings for Office 2010

Get a digital ID (*http://go.microsoft.com/fwlink/?LinkId=185585*)

Plan for limiting junk e-mail in Outlook 2010

This article discusses how the Outlook 2010 Junk E-mail Filter works, and which settings you can configure for the Junk E-mail Filter and automatic picture download to meet the needs of your organization.

This article is for Outlook administrators. To configure Outlook junk e-mail options on your computer, see Junk E-mail Filter options (*http://go.microsoft.com/fwlink/?LinkId=81371*).

In this article:

Overview

Microsoft Outlook 2010 includes features that can help users avoid receiving and reading junk e-mail messages. These include the Junk E-mail Filter and the ability to disable automatic content download from external servers.

Automatic picture download settings help reduce the risk of Web beacons activating in e-mail messages by automatically blocking the download of pictures, sounds, and other content from external servers in e-mail messages. By default, automatic content download is disabled.

Note:
Outlook 2010 automatically saves active content that you choose to download from the Internet. Like Office Outlook 2007 and earlier versions, Outlook 2010 prompts you before it downloads active content that can serve as a Web beacon. However, unlike Office Outlook 2007 and earlier versions, when you close the item, you are not prompted to save the changes. Instead, the downloaded content is automatically saved.

The Junk E-mail Filter helps users avoid reading junk e-mail messages. By default, the filter is turned on, and the protection level is set to Low, which is designed to filter the most obvious junk e-mail messages. The filter replaces the rules for processing junk e-mail messages in previous versions of Outlook (before Microsoft Office Outlook 2003). The filter incorporates technology built into the software to evaluate e-mail messages to determine whether the messages are likely to be junk e-mail, in addition to filtering lists that automatically block or accept messages to or from specific senders.

The Junk E-mail Filter contains two parts:

- Three Junk e-mail Filter lists: Safe Senders, Safe Recipients, and Blocked Senders.

- The Junk E-mail Filter that evaluates whether an unread message should be treated as junk e-mail based on several factors that include the message content and whether the sender is included in Junk E-mail Filter lists.

All settings for the Junk E-mail Filter are stored in each user's Outlook profile. You can override the profile settings by using Group Policy or set default Junk E-mail Filter configurations by using the Office Customization Tool (OCT).

The Junk E-mail Filter is provided for a subset of Outlook 2010 account types. The types are listed in the following section, *Supported account types*. The filter works best when it is used with Microsoft Exchange Server 2003 and later versions. Note that Exchange Server 2003 is the earliest version of Exchange Server that can be used with Outlook 2010.

When Outlook users are upgraded to Outlook 2010, existing Junk E-mail Filter lists are maintained, unless you deploy new lists to users.

Supported account types

Outlook 2010 supports junk e-mail filtering for the following account types:

- Microsoft Exchange Server e-mail accounts in Cached Exchange Mode
- Microsoft Exchange Server e-mail accounts when mail is delivered to a personal Outlook Data File (.pst)
- HTTP accounts
- POP accounts
- Windows Live Hotmail accounts
- IMAP accounts

The following account types are not supported for the Outlook 2010 Junk E-mail Filter:

- Microsoft Exchange Server e-mail accounts in Online mode
- Third-party MAPI providers

Support in Exchange Server

If users use Cached Exchange Mode or download to a personal Outlook Data File (.pst), the Junk E-mail Filter lists that are available from any computer are also used by the server to evaluate mail. This means that if a sender is a member of a user's Blocked Senders list, mail from that sender moves to the Junk E-mail folder on the server and is not evaluated by Outlook 2010. In addition, Outlook 2010 uses the Junk E-mail Filter to evaluate e-mail messages.

Configuring the Junk E-mail Filter user interface

You can specify several options to configure how the Junk E-mail Filter works for your users.

These include the following:

- Set the Junk E-mail Filter protection level.
- Permanently delete suspected junk e-mail messages or move the messages to the Junk E-mail folder.
- Trust e-mail messages from users' Contacts.

The default values for the Junk E-mail Filter are designed to help provide a positive experience for users. However, you can configure these settings to different defaults and set other options and policies when you deploy Outlook 2010 to your organization.

Junk e-mail settings are set only one time. When the user first starts Outlook 2010, the settings are configured in the profile that the user selects. Other profiles the user has, or may create later, do not include the settings that you have configured. Instead, default settings are used.

Default values for the Junk E-mail Filter settings are as follows:

- Junk E-mail protection level: Set to LOW
- Permanently delete Junk E-mail: Set to OFF
- Trust E-mail from Contacts: Set to OFF

You can use the OCT to configure these options to specify default values for users, or the options can be enforced by Group Policy. For information about how to configure options for the Junk E-mail Filter, see Configure junk e-mail settings in Outlook 2010 (*http://technet.microsoft.com/library/d5538a83-5d2f-4acb-b372-8741afe1f212(Office.14).aspx*).

Important

You can configure the following settings for the Outlook 2010 Junk E-mail filter. In the OCT, on the **Modify user settings** page, these settings are under **Microsoft Outlook 2010\Outlook Options\Preferences\Junk E-mail**. In Group Policy, these settings are under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Preferences\Junk E-mail**.

Junk e-mail option	Description
Add e-mail recipients to users' Safe Senders Lists	Automatically add all e-mail recipients to users' Safe Senders Lists.
Hide Junk Mail UI	In Group Policy, disable junk e-mail filtering and hide related settings in Outlook.
Hide warnings about suspicious domain names in e-mail addresses	Enable to hide warnings about suspicious domain names in the e-mail addresses.
Junk Mail Import List	Option in the OCT. You must enable this setting to enable other junk e-mail settings configured in the OCT or in Group Policy.

Junk e-mail option	Description
Junk E-mail protection level	Select the level of junk e-mail protection for users: No Protection, Low, High, Trusted Lists Only.
Overwrite or Append Junk Mail Import List	Change default from overwrite Junk Mail Import list to append to the list.
Permanently delete Junk E-mail	Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder.
Specify path to Blocked Senders list	Specify a text file that contains a list of e-mail addresses to append to or overwrite the Blocked Senders list.
Specify path to Safe Recipients list	Specify a text file that contains a list of e-mail addresses to append to or overwrite the Safe Recipients list.
Specify path to Safe Senders list	Specify a text file that contains a list of e-mail addresses to append to or overwrite the Safe Senders list.
Trust E-mail from Contacts	Trust e-mail addresses included in users' Contacts folders.

Deploying default Junk E-mail Filter lists

You can deploy default Junk E-mail Filter lists to your users. The Junk E-mail Filter uses these lists as follows:

- **Safe Senders list** E-mail messages that were received from the e-mail addresses in the list or from any e-mail address that includes a domain name in the list are never treated as junk e-mail.
- **Safe Recipients list** E-mail messages sent to the e-mail addresses in the list or to any e-mail address that includes a domain name in the list are never treated as junk e-mail.
- **Blocked Senders list** E-mail messages that were received from the e-mail addresses in the list or from any e-mail address that includes a domain name in the list are always treated as junk e-mail.

If a domain name or e-mail address is a member of both the Blocked Senders list and the Safe Senders list, the Safe Senders list takes precedence over the Blocked Senders list. This reduces the risk that mail that users want might be treated as junk e-mail by mistake. The lists are stored on the Exchange server and are available if users roam.

To deploy the Junk E-mail Filter lists, you create the lists on a test computer and distribute the lists to your users. You can distribute the lists by putting the lists on a network share, or if you have remote users not connected to the domain, you can use the OCT to add the files by using the **Add files** option. The lists that you provide are default lists. If you deploy the lists by using Group Policy, users can

change the lists during their Outlook session. When users restart Outlook, Group Policy will append the list by default or, if you have enabled **Overwrite or Append Junk Mail Import List**, their changes will be overwritten with the original list that you deployed. For information about how to create and deploy default lists, see Configure junk e-mail settings in Outlook 2010 (*http://technet.microsoft.com/library/d5538a83-5d2f-4acb-b372-8741afe1f212(Office.14).aspx*).

Configuring Automatic picture download

Messages in HTML format often include pictures or sounds. Sometimes these pictures or sounds are not included in the message, but are instead downloaded from a Web server when the e-mail message is opened or previewed. This is typically done by legitimate senders to avoid sending extra-large messages.

However, junk e-mail senders can use a link to content on external servers to include a Web beacon in e-mail messages, which notifies the Web server when users read or preview the message. The Web beacon notification validates the user's e-mail address to the junk e-mail sender, which can result in more junk e-mail being sent to the user.

This feature, to not automatically download pictures or other content, can also help users avoid viewing potentially offensive material (for external content linked to the message) and, if they are on a low bandwidth connection, to decide whether an image warrants the time and bandwidth to download it. Users can view the blocked pictures or content in a message by clicking the InfoBar under the message header or by right-clicking the blocked image.

By default, Outlook 2010 does not download pictures or other content automatically, except when the external content comes from a Web site in the Trusted Sites zone, or from an address or domain specified in the Safe Senders List. You can change this behavior so that content from any of the zones (Trusted Sites, Local Intranet, and Internet) will be downloaded automatically or blocked automatically.

You can configure the following settings for automatic picture download. In the OCT, on the **Modify user settings** page, these settings are under **Microsoft Outlook 2010\Security\Automatic Picture Download Settings**. In Group Policy, these settings are under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Automatic Picture Download Settings**.

Automatic picture download option	Description
Automatically download content for e-mail from people in Safe Senders and Safe Recipients lists	Enable this option to automatically download content when e-mail message is from someone in the user's Safe Senders list or to someone in the user's Safe Recipients list.
Block Trusted Zones	Disable this option to include Trusted Zones in the Safe Zones for Automatic Picture Download.
Display pictures and external content in HTML e-mail	Enable this option to automatically display external content in HTML mail.

Automatic picture download option	Description
Do not permit download of content from safe zones	Disable this option to automatically download content for sites in Safe Zones (as defined by Trusted Zones, Internet, and Intranet settings).
Include Internet in Safe Zones for Automatic Picture Download	Automatically download pictures for all Internet e-mail.
Include Intranet in Safe Zones for Automatic Picture Download	Automatically download pictures for all Intranet e-mail

For information about how to configure automatic picture download, see Configure junk e-mail settings in Outlook 2010 (*http://technet.microsoft.com/library/d5538a83-5d2f-4acb-b372-8741afe1f212(Office.14).aspx*).

See Also

Configure junk e-mail settings in Outlook 2010 (*http://technet.microsoft.com/library/d5538a83-5d2f-4acb-b372-8741afe1f212(Office.14).aspx*)

Plan for spelling checker settings in Office 2010

Depending on your objectives, you can use either Group Policy or the Office Customization Tool (OCT) to manage the behavior of spelling checker in Office 2010. To determine which of these tools to use, you must decide whether or not you want users to be able to change your configurations:

- Group Policy enables you to set *policies*, which are configurations that users cannot change.
- The OCT enables you to set *preferences*, which are configurations that users can change through the user interface (UI). Preferences are deployed during Office 2010 setup.

The Office 2010 Group Policy and OCT settings are available in the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316*) download package. The download package also contains an Excel 2010 workbook ("Office2010GroupPolicyAndOCTSettings.xls") that has more information about the settings. It includes registry information that can be useful if you want to configure spelling checker options by using a script.

In this article:

The sections in this article are grouped by application. Each section contains a table that lists the setting names, descriptions, the behavior that occurs when you enable, disable, or do not configure the setting, and the location of the setting in the Group Policy object editor and OCT.

Note

- The locations in the Group Policy Object Editor apply when you invoke the Group Policy Object Editor to configure a GPO. To configure local Group Policy, use the Local Group Policy Editor. To configure domain-based Group Policy, use the Group Policy Management Console (GPMC). Either tool invokes the Group Policy Object Editor when you configure a GPO. For more information, see Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*) and Group Policy overview for Office 2010.
- The locations in the OCT are available on the Modify user settings page. For more information about the OCT, see Office Customization Tool in Office 2010.

- For more information about the spelling checker options that users can change through the UI, see Choose how spelling and grammar checking work (http://go.microsoft.com/fwlink/?linkID=202126).

Office 2010 general spelling checker settings

The following table lists the settings that apply globally to Office 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
Improve proofing tools	Controls whether the Help Improve Proofing Tools feature sends usage data to Microsoft.	Data is sent to Microsoft if users decide to participate in the Customer Experience Improvement Program (CEIP).	Data is not collected or sent to Microsoft.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection
Flag Repeated Words	Allows users to flag or ignore repeated words.	Spelling checker flags repeated words.	Spelling checker does not flag repeated words.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling
Ignore words in UPPERCASE	Allows users to ignore words that are written in UPPERCASE.	Spelling checker ignores words that are written in UPPERCASE.	Spelling checker does not ignore words that are written in UPPERCAS	Same as if it is enabled, except users can change	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
			E.	the setting through the UI.		
Ignore words with numbers	Allows users to ignore words that contain numbers.	Spelling checker ignores words that contain numbers.	Spelling checker does not ignore words that contain numbers.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling
Ignore Internet and file addresses	Allows users to ignore URLs and file paths.	Spelling checker ignores URLs and file paths.	Spelling checker does not ignore URLs and file paths.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling
Suggest from main dictionary only.	Allows users to select words from the main dictionary only.	Spelling checker lets users select words from the main dictionary only.	Spelling checker lets users select words from other sources.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data Collection	Microsoft Office 2010\Tools | Options | Spelling

InfoPath 2010 spelling checker settings

The following table lists the settings that apply to InfoPath 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
Hide spelling errors	Allows users to hide spelling errors (the wavy line under a misspelled word)	Spelling errors (the wavy lines under a misspelled word) are hidden.	Spelling errors are designated by a wavy line that is under the misspelled word.	Same as if it is enabled, except users can change the setting through the UI.	Microsoft InfoPath 2010\InfoPath Options\Spelling & Grammar	Microsoft InfoPath 2010\InfoPath Options\Spelling & Grammar
Disable commands	Allows the administrator to disable UI options.	The administrator can disable the following UI option: Home tab | Spelling Menu | Set Proofing Language	UI option is enabled.	Same as if it is disabled, except users can change the setting through the UI.	Microsoft InfoPath 2010\Disable Items in User Interface\Predefined	Not available in the OCT.

OneNote 2010 spelling checker settings

The following table lists the settings that apply to OneNote 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
OneNote Spelling Options	Determines the following spelling	One or more options	One or more options	Same as enabling the “Check	Microsoft OneNote 2010\OneNote	Microsoft OneNote 2010\OneNote

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
	options for users • No spell checking • Check spelling as you type • Hide spelling errors • Check spelling but hide errors	can be enabled.	can be disabled.	spelling as you type" option, but users can change this through the UI.	Options\Spelling	Options\Spelling

Outlook 2010 spelling checker settings

The following table lists the settings that apply to Outlook 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
General	Enables or disables the following spelling options for users: • Always check spelling before sending	One or more options can be enabled.	One or more options can be disabled.	Both options are enabled, but users can change this through the UI.	Microsoft Outlook 2010\Outlook Options\Spelling	Microsoft Outlook 2010\Outlook Options\Spelling

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
	• Ignore original message text in software					

PowerPoint 2010 spelling checker settings

The following table lists the settings that apply to PowerPoint 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
Use contextual spelling	Enables or disables contextual spelling for users.	Contextual spelling is enabled for users.	Contextual spelling is disabled for users.	Same as if it is enabled, except users can change through the UI.	Microsoft PowerPoint 2010\PowerPoint Options\Proofing	Microsoft PowerPoint 2010\PowerPoint Options\Proofing
Check spelling as you type	Enables PowerPoint 2010 to check the spelling while the user types.	**Check spelling as you type** is enabled for users.	**Check spelling as you type** is disabled for users.	Same as if it is enabled, except users can change through the UI.	Microsoft PowerPoint 2010\PowerPoint Options\Proofing	Microsoft PowerPoint 2010\PowerPoint Options\Proofing

Publisher 2010 spelling checker settings

The following table lists the settings that apply to Publisher 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
Check spelling as you type	Enables or disables the following options: • Check spelling as you type. • Hide spelling errors. • "Check spelling as you type" and "Hide spelling errors" are both enable.	One or more of the options can be enabled.	One or more of the options can be disabled.	Check spelling as you type is enabled, but users can change this through the UI.	Microsoft Publisher 2010\Publisher Options\L_Proofing	Microsoft Publisher 2010\Publisher Options\L_Proofing

Word 2010 spelling checker settings

The following table lists the settings that apply to Word 2010.

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
Check grammar with spelling	Allows users to configure spelling checker to check the grammar at the same time that they check the spelling.	Spelling checker checks for grammar when it checks	Spelling checker does not check	Same as if it is enabled, except users can	Microsoft Word 2010\Word Options\Proofing\Auto Format as you type\Automatically as you type	Microsoft Word 2010\Word Options\Proofing

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
		spelling.	for grammar when it checks spelling.	change through the UI.		
Delay before starting background spelling checker	Allows the administrator to add a delay, expressed in milliseconds.Milliseconds (e.g. 5000 milliseconds = 5 seconds), before background spelling checker starts.)	The administrator can specify a delay in milliseconds, between 0 – 2147483647.	There is no delay.	There is no delay.	Microsoft Word 2010\Word Options\Proofing\Auto Format as you type\Automatically as you type	Microsoft Word 2010\Word Options\Proofing

See Also

Group Policy overview for Office 2010

Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*)

Plan for proofing tools

Plan for SharePoint Workspace 2010

When you plan a Microsoft SharePoint Workspace 2010 deployment, consider your organization's needs and objectives, especially in the context of the deployment options that are discussed here.

The following references may also be helpfu:

- For information about how to deploy SharePoint Workspace 2010 after planning your objectives, see Configure and customize SharePoint Workspace 2010 (*http://technet.microsoft.com/library/5290b730-b9fd-4228-93e0-7ace1766aa85(Office.14).aspx*).
- For information about how to deploy SharePoint Workspace 2010 for a Microsoft Groove Server-managed environment, see Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*).

In this article:

Topology options for SharePoint Workspace 2010

SharePoint Workspace 2010 is a client for Microsoft SharePoint Server 2010 and Microsoft SharePoint Foundation 2010 that supports online and offline collaboration. SharePoint Workspace enables anytime synchronization of local content with documents and lists on a SharePoint site. SharePoint Workspace also provides options that support peer collaboration through the creation of Groove workspaces and shared folders that do not require SharePoint connections. SharePoint Workspace is included with Microsoft Office Professional Plus 2010. See SharePoint Workspace 2010 overview (*http://technet.microsoft.com/library/650cb781-4dbd-45ac-b8d3-2ce9b3a16600(Office.14).aspx*) for more information about SharePoint Workspace.

Planning a SharePoint Workspace 2010 deployment begins with selecting a topology that best supports your collaboration strategy. To start, consider the operating environment and your organization's requirements.

The following table lists key decision factors:

Capability	Requirement
Is SharePoint Server 2010 or SharePoint Foundation 2010 used in the organization?	Yes|No
Do some team contributors have to work offline?	Yes|No
Do you have to support flexible, agile peer collaboration, where users have to connect from different locales and time zones?	Yes|No
Does the organization permit the use of peer collaboration software?	Yes|No
Does team collaboration have to extend outside a private network or LAN to trusted partners and field sites?	Yes|No
Is Active Directory used in your organization?	Yes|No
Are valuable contributions expected from clients that have no access to the organization's SharePoint sites?	Yes|No
Is centralized management of peer collaboration necessary for the organization's security and management infrastructure?	Yes|No

The following table shows how various SharePoint Workspace topologies address these requirements:

SharePoint Workspace topologies and capabilities

Topology	Capabilities
SharePoint Workspace as a SharePoint client	This topology supports or builds upon: • Access to SharePoint Server 2010 or SharePoint Foundation 2010 document libraries and lists. • Team contributors who work online and offline.
SharePoint Workspace as a peer collaboration client	This topology supports or builds upon: • Team contributors working online and offline. • Flexible, agile peer collaboration. Groove workspaces support multiple communication protocols and organizations can control which ports are open for peer message transport. • Team collaboration that is extended outside a private network to trusted partners and field sites.

Topology	Capabilities
	• Valuable contributions from clients that have no access to the organization's SharePoint sites.
SharePoint Workspace as a SharePoint and peer collaboration client	This topology supports or builds upon: • Access to SharePoint Server 2010 or SharePoint Foundation 2010 document libraries and lists. • Team contributors working online and offline. • Flexible, agile peer collaboration. Groove workspaces support multiple communication protocols. This lets organizations control which ports are open for peer message transport. • Team collaboration that extends outside a private network to trusted partners and field sites. • Valuable contributions from clients that have no access to the organization's SharePoint sites.
SharePoint Workspace and Groove Server as a managed collaboration system	This topology supports or builds upon: • Centralized management of peer collaboration to address the organization's security and management requirements. • Team contributors working online and offline. • Flexible, agile peer collaboration. • Team collaboration extended outside a private network to trusted partners and field sites. • Valuable contributions from clients that have no access to the organization's SharePoint sites. • Existing integration with Active Directory system. For more information about this deployment topology, see Groove Server 2010 (*http://technet.microsoft.com/library/fa057d58-5620-4f1a-aef2-126cad6a8b31(Office.14).aspx*).

The next four sections of this article describe how the listed SharePoint Workspace deployment topologies map to collaboration needs.

SharePoint Workspace as a SharePoint client

SharePoint Workspace as a SharePoint client is most suitable for organizations with SharePoint team members and partners who have to contribute content from outside the corporate infrastructure — from data that is collected in the field or from locations that do not have a SharePoint server connection. This topology provides SharePoint Workspace users with the following collaboration option:

- The ability to easily create a SharePoint workspace that establishes a connection between a SharePoint server and a SharePoint Workspace client. This enables a single SharePoint team member or partner to take SharePoint site content onto a local computer. By using a SharePoint workspace, a contributor can add, change, and delete content for a SharePoint document library or list whether online or offline, regardless of connectivity to a SharePoint server. Synchronization of content updates between the SharePoint Workspace client and SharePoint sites occurs automatically when the client is online so that contributors can share the work that they performed while offline as easily as they can share the work that they generate while connected to the Internet.

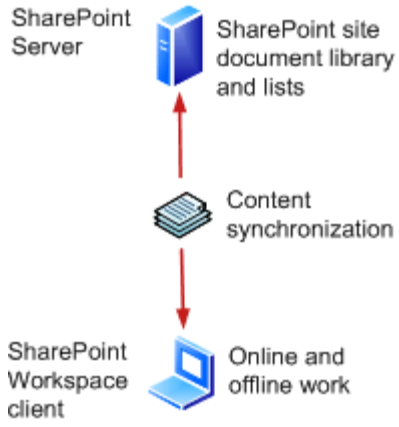
Note:
The SharePoint Workspace client lets users create SharePoint workspaces and peer workspaces. Peer workspace types can be Groove workspaces or Shared Folders, as described in SharePoint Workspace as a SharePoint and peer collaboration client. To deploy SharePoint Workspace exclusively as a SharePoint client, supporting SharePoint workspaces only, you can include with your deployment a policy that prohibits peer workspace options, as described in Configure and customize SharePoint Workspace 2010 (*http://technet.microsoft.com/library/5290b730-b9fd-4228-93e0-7ace1766aa85(Office.14).aspx*).

For this configuration, a basic level of client management can be achieved by using Windows and Active Directory tools.

SharePoint workspaces rely on SharePoint Workspace communications and dynamics technology to support individual client-to-SharePoint connections that enable SharePoint Workspace users to work with and synchronize SharePoint document and list content on their local computers. Figure 1 shows a basic setup of SharePoint Workspace to Microsoft SharePoint Server 2010.

Figure 1.

SharePoint Workspace connection to SharePoint



SharePoint Workspace as a peer collaboration client

SharePoint Workspace as a peer collaboration client is most suitable for organizations that have to provide information workers with a well-equipped, easy-to-use collaboration environment where neither Microsoft SharePoint Server 2010 nor Microsoft SharePoint Foundation 2010 is available. This topology gives Groove_2nd_NoVer users two peer collaboration options:

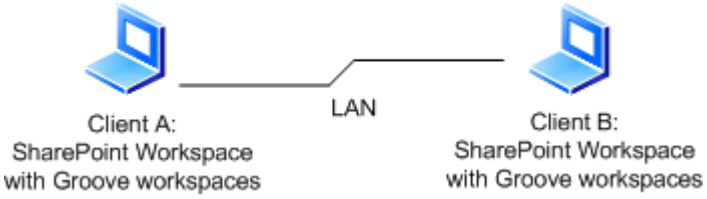
- The ability to easily and quickly create Groove workspaces where information workers can collaborate safely with trusted peers without the need of a virtual private network (VPN) and with access to a full set of local online and offline collaboration tools. Groove workspace collaboration tools support document creation and sharing, online discussions, meeting management, and Microsoft InfoPath forms, in an environment of real-time collaboration among team members and partners located inside or outside the corporate firewall.
- The ability to create Shared Folders where SharePoint Workspace users can collaborate on content within designated Windows folders on workspace member desktops.

For this configuration, a basic level of client management can be achieved by using Windows and Active Directory tools.

For peer collaboration through Groove workspaces and Shared Folders, SharePoint Workspace builds on its communications and dynamics foundation and provides a workspace manager module with a set of tools, a contacts manager, a message manager, and an implementation of standards-based Public Key Infrastructure (PKI) to help secure Groove workspaces and authenticate workspace members. Groove workspace data resides on client computers and built-in security provisions ensure that workspace member data is encrypted over the network. The core capabilities of SharePoint Workspace tools and components can be used on two client computers that are directly connected over a local area network (LAN), as shown in Figure 2.

Figure 2.

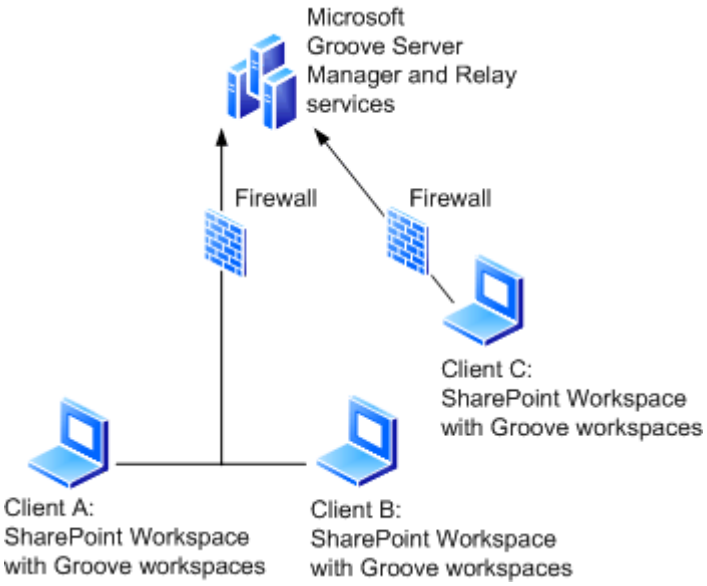
Groove workspace peer connections on a LAN



To sustain peer communications for Groove workspaces and Shared Folders, when a client is connected to a wide area network (WAN), offline, or behind a firewall, SharePoint Workspace relies on supporting Microsoft Groove Server Manager and Relay services, as shown in Figure 3. These servers, Microsoft-hosted or installed onsite, help ensure timely communication regardless of user context or Internet-wide environmental conditions.

Figure 3.

Groove workspace connections beyond a LAN



SharePoint Workspace as a SharePoint and peer collaboration client

SharePoint Workspace as a SharePoint and peer collaboration client is most suitable for organizations that have to synchronize client desktop content with SharePoint document libraries and lists while extending collaboration to ad hoc teams that work outside the SharePoint document framework. This option merges the previously described topologies to give SharePoint Workspace users the following collaboration options:

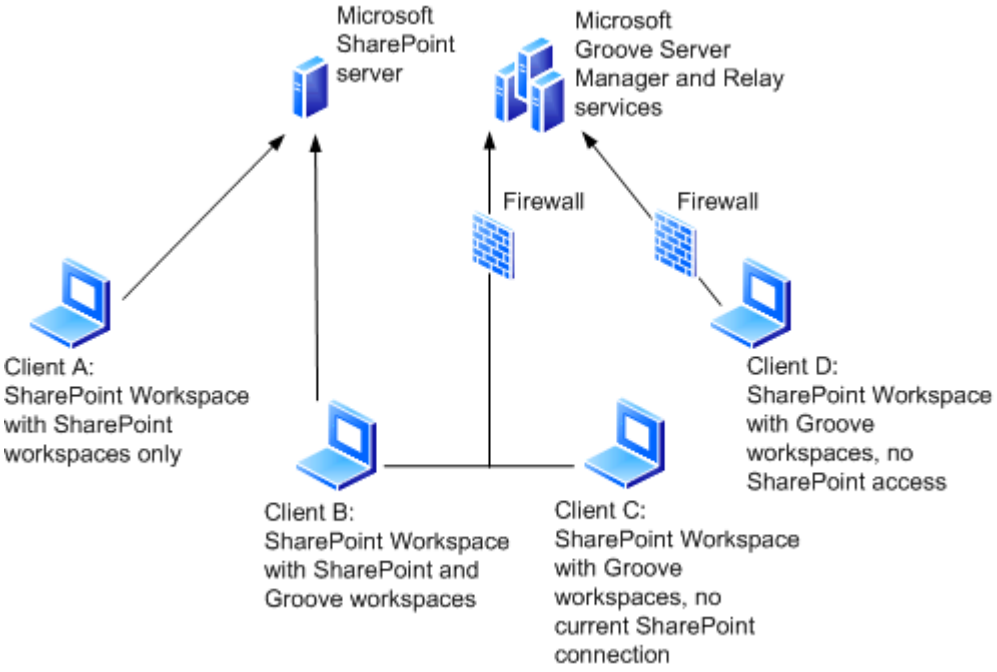
- The ability to create a SharePoint workspace that establishes a connection between a SharePoint server and a SharePoint Workspace client. This enables a single SharePoint team member or partner to take SharePoint site content onto a local computer, as described in SharePoint Workspace as a SharePoint client.
- The ability to easily create Groove workspaces where trusted peers can collaborate safely without the need of a VPN, as described in SharePoint Workspace 2010 overview (*http://technet.microsoft.com/library/650cb781-4dbd-45ac-b8d3-2ce9b3a16600(Office.14).aspx*).
- The ability to create Shared Folder workspaces where SharePoint Workspace users can collaborate on content within designated Windows folders on workspace member desktops.

For this configuration, a basic level of client management can be achieved by using Windows and Active Directory tools.

SharePoint Workspace communications and dynamics modules, together with TCP/IP protocols summarized in Network settings for SharePoint Workspace 2010, support message transport and content synchronization between individual clients and SharePoint servers, and between client peers. Figure 4 shows a SharePoint Workspace client/server system that involves a SharePoint server, Groove Server Relay and management services, and four SharePoint Workspace clients:

Figure 4.

SharePoint Workspace with SharePoint and Groove servers



SharePoint Workspace and Groove Server as a managed collaboration system

When Groove workspaces and Shared Folders are used, installation of Microsoft Groove Server 2010 onsite as part of SharePoint Workspace deployment provides optimal client administration. Groove Server provides two applications that facilitate SharePoint Workspace deployment and operation in an enterprise: Groove Server Manager provides management, reporting, and policy distribution services, and Groove Server Relay facilitates client communications. This system can function with or without SharePoint Server and can be extended to partners outside corporate firewalls. For more information about Groove Server 2010, see Groove Server 2010 (*http://technet.microsoft.com/library/fa057d58-5620-4f1a-aef2-126cad6a8b31(Office.14).aspx*).

The following table shows how SharePoint Workspace topology options can serve a range of scenarios.

SharePoint Workspace scenarios and topologies

Scenario	Description	Chosen topology and required components
Financial services company	• Scope: City-wide • Size: 2,000 employees • SharePoint Workspace users: 1,000 • SharePoint infrastructure in place	**SharePoint Workspace as SharePoint client only** Required components: • SharePoint Server • SharePoint Workspace clients
State higher-education system	• Scope: State-wide • Size: 4,000 employees • SharePoint Workspace users: 2,000 • No existing SharePoint installation	**SharePoint Workspace as a peer collaboration client** Required components: • SharePoint Workspace clients that have Internet connectivity
Regional healthcare system	• Scope: Region • Size: 10,000 employees • SharePoint Workspace users: 8,000 • SharePoint infrastructure in place	**SharePoint Workspace as a SharePoint and peer collaboration client** Required components: • SharePoint Server • SharePoint Workspace clients • Internet connectivity
Multinational corporation	• Scope: Global • Size: 500,000 employees • SharePoint Workspace users: 50,000	**Groove Server and SharePoint Workspace as a SharePoint managed collaboration system** Required components: • Microsoft Groove Server 2010

Scenario	Description	Chosen topology and required components
	• IT department: Yes	• SharePoint Workspace clients • Active Directory system (recommended) • Internet connectivity (recommended)

Network settings for SharePoint Workspace 2010

Microsoft SharePoint Workspace 2010 automatically configures Windows Firewall network ports for optimal operation. To verify client port connections or to configure Microsoft SharePoint Server and SharePoint Workspace ports for SharePoint workspaces only, start the Windows Firewall Control Panel add-in and configure settings as necessary.

For more information about SharePoint Workspace protocols, see Microsoft protocol documents (*http://go.microsoft.com/fwlink/?LinkId=162294*).

The following table describes which ports are required for which protocols in SharePoint Workspace.

Client port settings for SharePoint Workspace 2010

SharePoint Workspace client port settings	Protocols supported	Description
80/TCP - Outgoing	Microsoft File Synchronization by SOAP over HTTP Protocol (MS-FSSHTTP) Microsoft Groove HTTP Encapsulation of Simple Symmetric Transport Protocol (MS-GRVHENC)	Supports the following communications: • For SharePoint workspaces — Synchronization of document and list content between Microsoft SharePoint Server and SharePoint Workspace clients. • For Groove workspaces and Shared Folders — Transmission of SSTP messages among SharePoint Workspace clients and Groove Relay servers when neither SSTP port 2492/TCP nor port 443/TCP is available. Encapsulates SSTP transmissions in HTTP. • For Groove workspaces and Shared Folders — SOAP

SharePoint Workspace client port settings	Protocols supported	Description
		communication between SharePoint Workspace clients and Groove management servers.
443/TCP - Outgoing	HTTPS Microsoft Groove HTTP Encapsulation of Simple Symmetric Transport Protocol Security Protocol (MS-GRVSSTPS)	Supports the following communications: • For SharePoint workspaces — Synchronization of SSL-protected content between Microsoft SharePoint Server and SharePoint Workspace clients. • For Groove workspaces and Shared Folders — Transmission of SSTP messages among SharePoint Workspace clients and relay servers when SSTP port 2492/TCP is not available. Utilizes Secure HTTP Tunneling technology.
2492/TCP - Incoming and outgoing	Microsoft Groove Simple Symmetric Transport Protocol (MS-GRVSSTP)	Supports the following communications: • For Groove workspaces and Shared Folders — Transmission of SSTP messages among SharePoint Workspace clients and relay servers.
1211/UDP - Incoming and outgoing	Local Area Network Device Presence Protocol (LANDPP)	Supports following communications: • For Groove workspaces and Shared Folders — Local area network (LAN) device presence detection between SharePoint Workspace clients.

Scalability and performance considerations

This section provides system capacity information to help you plan for optimal system performance within the scope of expected SharePoint workspace usage in your organization. In this discussion, performance refers to document open, save, and update times, as well as upload and download times.

Performance and scalability

SharePoint Workspace stores downloaded SharePoint library documents in the common Office Document Cache (ODC) on the client device. The number of SharePoint Workspace documents that are stored in this cache has a direct impact on client system memory and performance. Because the ODC supports multiple Office applications, the implications of cache utilization by one Office application can extend to other Office applications on the system. In the case of SharePoint Workspace 2010, as more documents are stored in the ODC for synchronization, system memory fills up and performance decreases. As the number of cached SharePoint documents approaches 1,800, depending on file size, types, and contents, available memory and performance may decrease significantly. This approximate upper limit is based on tests in a controlled environment. The limit may be higher or lower in actual scenarios with documents of different sizes, types, and contents.

The size and number of documents that are synchronized with SharePoint can vary widely, even in a single organization. To anticipate and mitigate client performance and operational problems, try to plan for the expected maximum use case by implementing usage guidelines to prevent overloading the cache and related resources.

SharePoint Workspace 2010 hardware requirements are intended for most basic use cases, where the cache may contain fewer than 500 files and file size averages no more than 300 KB. These requirements specify client installation on a single-core processor of 256 MHz, with 256 MB of RAM and a 1.5 GB drive. To optimize for a better user experience in a heavier use environment, the following equipment is recommended as a minimum:

- Dual core processor, 2GHz
- 4 GB RAM
- 200 GB hard disk drive

If you expect to support client document caches that hold more than 500 documents on average, and some of them contain more than 300 KB of text, possibly with complex graphics and video clips, you should consider the higher-level hardware requirements.

The suggested limits are the result of tests conducted on the following hardware:

Intel Xeon CPU E5410 @ 2.33GHz, 4GB RAM, Single Disk 200GB

If necessary, you can take the following step to help control SharePoint Workspace performance:

- Limit file downloads to headers only by setting the following DWORD value in the Registry: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Groove\DefaultDocumentLibraryContentDownloadSettingHeadersOnly

Warning:
Serious problems might occur if you modify the registry incorrectly. These problems could require you to reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk. Always make sure that you back up the registry before you modify it, and that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, see the Microsoft Knowledge Base article Windows registry information for advanced users (*http://support.microsoft.com/kb/256986*).

For information about baseline SharePoint Workspace hardware requirements, see System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).

For information about the built-in mechanisms provided by SharePoint Server 2010 and SharePoint Workspace 2010, see Performance monitoring and throttling.

For information about SharePoint Server system requirements, see Deployment for SharePoint Server 2010 (*http://go.microsoft.com/fwlink/?LinkId=188459*).

Performance monitoring and throttling

SharePoint Server 2010 moderates the flow of client communications by throttling requests when built-in server health monitors indicate that server performance is lagging because of heavy workload. When SharePoint workspaces are used, SharePoint Workspace clients respond to SharePoint Server back-off signals by adjusting the frequency of server requests. SharePoint Workspace synchronization frequency adjustments reflect SharePoint workspace activity and SharePoint site changes, in such a way that the periodicity is lower when activity is minimal than when activity is greater. These adjustments reduce overall client bandwidth usage while they improve server performance.

In the case of Groove workspaces, SharePoint Workspace provides built-in performance provisions and relies on Groove Server Relay services, hosted by Microsoft or installed onsite, to optimize communications. To optimize performance, SharePoint Workspace transmits Groove workspace data directly from client to client when network conditions allow it. When data is addressed to a client that cannot be reached directly, SharePoint Workspace sends data over relay servers that optimize message transmission. Total bandwidth use under conditions of high traffic is often less when relay servers help in message transmission.

For more information about SharePoint performance monitoring and throttling, see Plan for caching and performance (*http://technet.microsoft.com/en-us/library/ee424404.aspx*).

Security considerations

SharePoint Workspace client exchanges with SharePoint sites rely on synchronization protocol and external mechanisms for security, such as those provided by VPNs or Secure Socket Layer (SSL) technology. Therefore, we recommend SSL encryption for SharePoint connections from outside a

corporate domain. You can configure Group Policy settings that apply across an Active Directory organizational unit, as described in Configure and customize SharePoint Workspace 2010 (*http://technet.microsoft.com/library/5290b730-b9fd-4228-93e0-7ace1766aa85(Office.14).aspx*). In addition, you can secure the SharePoint site from unauthorized access by setting access control lists appropriately. For guidance about how to set access control for users to synchronize with SharePoint libraries and lists, see Security and protection for SharePoint Foundation 2010 (*http://technet.microsoft.com/library/3f3744aa-6785-48c0-b16d-7bdddff577ca(Office.14).aspx*) or Security and protection for SharePoint Server 2010 (*http://technet.microsoft.com/library/c12253e2-2bc6-4e53-8fae-26829915481e(Office.14).aspx*).

SharePoint Workspace uses strong cryptographic and encryption technologies to protect SharePoint Workspace accounts, which are the secure repositories for each user's cryptographic keys, identity, contacts, messages, and unique workspace identifiers. Windows authentication and users' Windows logon credentials are used to unlock SharePoint Workspace accounts.

SharePoint Workspace 2010 does not encrypt SharePoint Workspace 2010 documents and other binary files, including SharePoint workspace content, on disk. Therefore, consider using BitLocker Drive Encryption to encrypt all content on client data drives. For more information see BitLocker Drive Encryption (*http://go.microsoft.com/fwlink/?LinkId=163122*). You can strengthen protection by blocking Windows Search in the SharePoint Workspace Data directory, to prevent generation of Search indexes that are not encrypted. However, be aware that content shared with other clients that are not equally protected will remain not encrypted and searchable.

For Groove workspaces and Shared Folders, SharePoint Workspace uses native symmetric and public key cryptographic technologies to authenticate, encrypt, and protect transmissions between clients over the network. Strong encryption protects the following content on-disk: Groove instant messages, Groove invitations, Groove Discussion and Notepad entries, archived Groove workspaces, and Forms tool templates.

SharePoint Workspace user authentication

SharePoint Workspace 2010 uses Windows logon and the Data Protection API (DPAPI) to authenticate the user and access the SharePoint Workspace account. This single sign-on user (SSO) logon means that additional SharePoint Workspace-specific credentials are not required.

For authenticating SharePoint Workspace users to SharePoint Server, SharePoint Workspace supports the following SharePoint Server methods: Windows authentication and forms-based authentication. Typically, Windows authentication is used for internal SharePoint Workspace user access to SharePoint sites. Forms-based authentication can be used for external SharePoint Workspace user access to SharePoint sites.

For authenticating SharePoint Workspace users to one another (for Groove workspaces, Shared Folders, and messaging), SharePoint Workspace relies on its native public key infrastructure (PKI).

For more information about Single Sign-On for SharePoint Server, see Enterprise Single Sign-On (*http://go.microsoft.com/fwlink/?LinkId=162302*).

For more information about forms-based authentication, see Configure Forms Based Authentication (*http://go.microsoft.com/fwlink/?LinkID=149721*).

Alternate access mapping

SharePoint Server supports alternate access mapping, which lets you define multiple URLs per site. When SharePoint workspaces are used, you can take advantage of this capability to ensure that SharePoint Workspace can synchronize with multiple SharePoint Server site URLs. Defining multiple URLs is useful for deployment scenarios in which the URL of a web request received by Internet Information Services (IIS) differs from the URL that was typed by a SharePoint user; for example, in scenarios that include reverse proxy publishing and load balancing.

If you have defined Alternate Access Mappings (AAM) for Microsoft SharePoint Server or SharePoint Foundation in the context of a Unified Access Gateway (UAG) server, you must configure the UAG server so that the correct alternate access mappings for target SharePoint server URLs are retained when remote SharePoint Workspace users try to access and synchronize content on a SharePoint site through the UAG.

To avoid synchronization problems for offline SharePoint Workspace 2010 clients who reconnect to SharePoint through UAG after working offline, disable address link translation for the following pages on the Unified Access Gateway server:

- /_vti_bin/Lists.asmx
- /_vti_bin/Webs.asmx

For more information about alternate access mapping, see Planning alternate access mappings (*http://go.microsoft.com/fwlink/?LinkID=114854*).

SharePoint list and library actions and settings

The following SharePoint Server 2010 actions and settings apply to SharePoint Workspace 2010:

- File Synchronization via SOAP over HTTP Protocol — This protocol must be enabled to support synchronization of SharePoint library and list content with SharePoint workspaces on SharePoint Workspace clients.
- Remote Differential Compression (RDC) — This Windows feature should be enabled to support File Synchronization via SOAP over HTTP Protocol.
- Site Actions: **Sync to SharePoint Workspace** — SharePoint Workspace users connected to the SharePoint site can click **Sync to SharePoint Workspace** to create a SharePoint workspace on a local computer, or to synchronize content if a local SharePoint workspace already exists for the site. From the local workspace, the user can add, change, or delete content regardless of connectivity to the SharePoint site. Synchronization with the SharePoint site occurs automatically at set intervals while the user is connected, or the user can click the **Sync** tab in the SharePoint workspace to force synchronization.

  Note:

Sync to SharePoint Workspace is also available as a ribbon option from a SharePoint document library or list.

- Site Actions/Site Settings/Site Administration/Search and offline availability/**Offline Client Availability** — SharePoint site administrators must select this setting to enable SharePoint Workspace clients to access the site.
- Secure Socket Layer (SSL) protection — SSL protection is recommended for the incoming port 80 interface that will support SharePoint communications with SharePoint Workspace clients.

Search options

SharePoint Workspace content can be searched by using Windows Search 4.0 or later versions. By default, Windows Search crawling (index creation) is enabled for some SharePoint Workspace content. SharePoint Workspace users can access Windows Search 4.0 by clicking **Search** on the **Home** tab of the ribbon, unless prevented from doing this by a Windows policy. Administrators can block Windows Search of SharePoint Workspace content and can override any user search setting by deploying an Active Directory GPO, as described in Configure and customize SharePoint Workspace 2010 (*http://technet.microsoft.com/library/5290b730-b9fd-4228-93e0-7ace1766aa85(Office.14).aspx*). For information about how to use Windows Search, see the Windows Search Administrator Guides (*http://go.microsoft.com/fwlink/?LinkID=164567*).

SharePoint Workspace backup and recovery

All SharePoint Workspace account information resides on client computers. Account information includes cryptographic keys and user identity information. SharePoint Workspace provides mechanisms for user account backup and recovery. In addition, users can back up Groove workspaces as workspace archives.

To help safeguard SharePoint Workspace user accounts, encourage SharePoint Workspace users to observe the following best practices:

- Enable SharePoint Workspace account recovery. The **Enable account recovery** setting can be accessed in SharePoint Workspace 2010 through the **Account Preferences** option and gives users a secure method for regaining access to accounts if a Windows logon must be reset. The **Enable account recovery** check box should remain selected on all clients, because it enables account recovery. Consider warning users against clearing this setting.

  Note:

  Enable account recovery also supports account portability and the ability to use the account on multiple computers. For organizations that must prevent users from porting their account to another computer, Microsoft Groove Server 2010 provides a policy that restricts managed accounts to a single computer. For information about how to deploy Groove Server at your site, see Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*).

- Back up SharePoint Workspace user accounts to a file in a secure location. SharePoint Workspace supports account recovery in the event of a lost or corrupted account, by providing an option that enables users to save their accounts to a .grv file. Encourage users to regularly save their accounts to file in a secure location. Users can save their account by clicking the **File** tab on the ribbon and, in the Manage Account drop-down menu, selecting Account Preferences. Then they select **Save Account as File** on the **Account** tab, entering a file name and a password, for initial account recovery, when they are prompted. Note that **Enable account recovery** must be selected in the user's account preferences for a reset code to be sent and the account to be recovered if the password is forgotten. When this setting is enabled SharePoint Workspace sends a reset code to the e-mail address that was provided in the Account Configuration Wizard when the account was created. Users can then reset a recovered account.

To help safeguard Groove workspaces, encourage users to periodically back up each Groove workspace by clicking the **File** tab on the ribbon, selecting **Share**, and then configuring the **Workspace as Archive** option. For more information about how to back up and recover Groove workspaces, see SharePoint Workspace product help at Microsoft products online (*http://go.microsoft.com/fwlink/?LinkId=162269*).

Note:
Groove workspace data and tools reside on client computers. Therefore, if other team members share a Groove workspace, the lost workspace can be retrieved from another client computer.

See Also

SharePoint Workspace 2010 overview (*http://technet.microsoft.com/library/650cb781-4dbd-45ac-b8d3-2ce9b3a16600(Office.14).aspx*)

Configure and customize SharePoint Workspace 2010 (*http://technet.microsoft.com/library/5290b730-b9fd-4228-93e0-7ace1766aa85(Office.14).aspx*)

Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*)

Microsoft protocol documents (*http://go.microsoft.com/fwlink/?LinkId=162294*)

SharePoint Workspace and ODC (*http://blogs.msdn.com/b/sharepoint_workspace_development_team/archive/2010/03/12/sharepoint-workspace-and-the-office-document-cache.aspx*)

Plan customizations and options for Visio 2010

This article describes some of the customizations and options that are available in Microsoft Visio 2010.

In this article:

Application settings

In Visio 2010, there are several ways to customize the application settings that you work with, from the application's appearance and behavior, to the rules that help you manage the work that you create.

Backgrounds and Borders & Titles galleries

The Backgrounds and Borders & Titles galleries on the **Design** tab are populated from the built-in stencils. However, the galleries can be customized by putting a stencil in the user's My Shapes folder (which is in the Documents or My Documents folder).

The stencils must be named as follows:

_BCKGRND.VSS for the Backgrounds gallery

_BORDERS.VSS for the Borders & Titles gallery

Note:
The files names must begin with an underscore.

If Visio finds a stencil that has this exact file name (which must be the same file name in all languages) in the My Shapes folder, it will use it to populate the gallery, instead of the stencil that was included with Visio 2010.

Warning:
The Shapes in these galleries have special behaviors that require knowledge of the Visio ShapeSheet to replicate.

To get a basis for the customized gallery content, follow these steps:

1. Find the stencils that are included with Visio 2010, found in \Program Files\Microsoft Office\Office14\Visio Content\1033 (for English).
2. Copy the files to your \My Shapes folder:
   a. Backgrounds (US and Metric)

BCKGRN_U.VSS

BCKGRN_M.VSS

b. Borders & Title (US and Metric)

BORDRS_U.VSS

BORDRS_M.VSS

3. Rename and customize the files.

Custom themes

In Microsoft Office Visio 2007, the introduction of the Themes feature made it easy to apply a professionally designed look to a diagram. In Visio 2010, the Themes feature takes advantage of the Microsoft Office Fluent user interface (UI) and is one of the features that demonstrates the Live Preview capability.

Visio custom themes are stored in the document, not in an external file. The way to deploy a custom theme is to define it in a Visio document and then save it as a template (*.vst) for use in the organization. The way that you create templates in Visio 2010 has not changed from Office Visio 2007 or earlier versions.

To create a custom theme that will be stored as a template, follow these steps:

1. Click the **Design** tab.
2. Click **Colors**.
3. Click **Create New Theme Colors**.
4. Select the theme name and colors, and then click **OK**.
5. Click **Effects**.
6. Click **Create New Theme Effects**.
7. Select the desired effects, and then click **OK**.

All users will have to start their new drawings from that template to use the custom theme.

Custom validation rules

In Visio 2010, you can deploy custom templates that contain validation rule sets and rules to ensure that diagrams comply with certain company standards. A validation rule represents one kind of requirement that your diagram should follow. When a user runs validation, Visio displays a list of issues for requirements that have not been met.

A validation rule defines a logical test to be performed against the contents of the diagram. The validation rules are packaged together in rule sets. There can be multiple rule sets in a document. Each rule set can be active or inactive (off) and multiple sets can be active at the same time. Each rule set in a document has a unique name. The same rule might appear in multiple rule sets in a document, and the same rule set can appear in multiple documents that use the application. Microsoft Visio Premium 2010 provides rules in the Basic Flowchart, Cross-Functional Flowchart, Six Sigma Diagram, Microsoft

SharePoint Workflow, and BPMN diagram templates. Custom rules and rule sets can be added to any template.

When validation is performed, Visio checks each rule active in the document against all the targets found in the document. For each target that does not meet the requirements specified by the rule, Visio creates a validation issue. All issues found during validation are displayed for the user in a single list.

Validation can be initiated by the user via the command button on the ribbon when the user wants to check their document for issues. These issues can be left unfixed or specifically ignored, which will suppress the issue for subsequent validation runs.

To access the validation feature, follow these steps:

1. On the **Process** tab, select the **Issues Window**. This will open the Validation Window below the drawing.
2. Then, on the **Process** tab, click the **Check Diagram** button.

When validation is triggered, there is no particular order of rules processed or shapes processed. However, a progress bar is shown after the operation takes longer than three seconds. The operation is stoppable, and Visio will display any issues found to this point.

If Visio finds more errors in the document than it can display in the Issues Window (currently 32767), validation is stopped automatically. A dialog box will display the message: “Diagram validation has been stopped because there are too many issues for Visio to track.”

Once validation has stopped (complete or incomplete), if issues are found, Visio opens the Issues Window if it is currently not open and displays the issues.

Diagram templates

When you start Visio 2010, the first thing that you see is the new screen in the Microsoft Office Backstage view, where you can choose a template for the diagram that you will create. It resembles the Office Visio 2007 Getting Started screen. Visio 2010 documents are created in either U.S. units or metric units. The only SKU that contains both U.S. units and metric units is U.S. English (en-us). When you use this SKU, and create a new diagram, you can choose which units that you want to use. There is a setting and a Group Policy that can be customized to create the default as one of those two units when it is available and when the installation is en-us.

Customize Quick Shapes

The Shapes Window is redesigned in Visio 2010. Within the Shapes Window is a group named Quick Shapes. Quick Shapes is a subset of shapes that are used more frequently in a given stencil.

Quick Shapes can be customized through the user interface and these customizations are stored in the registry. The Quick Shapes count information for stencils is stored in the published components table and is the count used by default.

When a user customizes the stencil through the UI, Visio saves the Quick Shapes count and the master sort order in the registry under **HKCU\Software\Microsoft\Office\14.0\Visio\Quick Shapes** by using the following format:

Name:	Full file path of the stencil file
Type:	REG_BINARY
Data:	The Quick Shapes count and the sequence of master IDs, represented in binary form. The Quick Shapes count and each master ID are represented in 4 bytes

Trusted documents

Trusted documents is an improved feature in Office 2010 that interacts with document security features. It enables active content (for example, macros and ActiveX controls) in a document, based on the trust decision on the file, and can remember the selection every time that you open the document. Office versions earlier than the 2007 Office system prompted you for macros and other kinds of active content prior to opening a document every time.

In Office 2010, if you create or open a document that contains a macro, or receive a document that uses a data connection to a trusted server, and you have enabled the content in the trust record, you will not be prompted with a security notification for the content any more. When you use trusted documents, the trust is recorded on a per-file basis. The trust record is added to the Current User section of your local registry and contains the file's full path and other data, such as the creation time of the document.

Note:
Trust records are stored on a specific computer, so you will get prompted again if you open the file on another computer.

There are two entry points to make a document trusted. To make a document trusted, follow these steps:

1. On the Message Bar, click **Enable Content**.
2. Click the Message Bar for details. This will open the Backstage view.

   In the Backstage view, click **Enable Content**. This will display two additional options:

   a. Enable all content and make it a trusted document.

   b. Click the **Advanced Options** button to enable content for one time (similar to the 2007 Office system).

Trusting documents on a network share is riskier than trusting documents on your local hard disk drive because other users who have access to the network locations can modify the contents of your file. For this reason, a security warning is displayed the first time that you try to trust a document on a network location. In the Trust Center, you can disallow documents on a network location from being trusted.

This causes Office to show you the security notification every time that you open a document on a network location.

In the Trust Center, you can modify settings to allow or disallow documents on a network from being trusted, disable the trusted documents feature, or reset all trusted documents so that they are no longer trusted. All these settings can be configured by the administrator by using Group Policy.

SharePoint and the Repository

In Visio 2010, you can save files to Microsoft SharePoint 2010 Products by using the Backstage view. To save files, follow these steps:

1. Click the **File** tab.
2. Click **Save & Send**.
3. Click **Save to SharePoint**.
4. Save the drawing as:

   Drawing (*.vsd) or Web Drawing (*.vdw)
5. The **Save As** dialog box lets you confirm or refine your selection.

   If you select Web Drawing (*.vdw), ensure that you have SharePoint 2010 Products and Visio Services to have your diagram display in the browser.

See Also

Changes in Visio 2010 (*http://technet.microsoft.com/library/a125e33f-d851-4aea-9672-5aa4a6d9bc72(Office.14).aspx*)

Plan security for Office 2010

An organization's success often depends on the productivity of its information workers and the integrity and confidentiality of its intellectual property. Many IT departments find it difficult to satisfy these business needs because protection often comes at the expense of productivity. This section describes the new security controls that are available in Microsoft Office 2010 to help you plan a robust defense against threats while maintaining information worker productivity.

In this section:

Article	Description
Security overview for Office 2010	Provides an overview of new security controls in Microsoft Office 2010 that make it easier for IT professionals to build a robust defense against threats while maintaining information worker productivity.
Understand security threats and countermeasures for Office 2010	Provides information to help you plan for a secure desktop configuration for Office 2010, including which security risks and threats are relevant to Office 2010, and which might pose a risk to the organization's business assets or processes.
Plan Trusted Locations settings for Office 2010	Provides information about how to use the Trusted Locations feature in Office 2010 to differentiate safe files from potentially harmful files.
Plan Trusted Publishers settings for Office 2010	Provides information about how to use the Trusted Publishers feature in Office 2010 to designate content publishers that you trust.
Plan security settings for add-ins for Office 2010	Describes how to control the way add-ins behave, or to prevent users from running add-ins, by modifying the Office 2010 add-in settings.
Plan security settings for ActiveX controls for Office 2010	Describes how to change the way Microsoft ActiveX controls behave in Office 2010 by modifying ActiveX control settings.
Plan security settings for VBA macros for Office 2010	Describes how to control the way Visual Basic for Applications (VBA) and VBA macros behave by modifying Microsoft Office 2010 VBA and VBA macros settings.

Article	Description
Plan COM object categorization for Office 2010	Describes how to control the behavior of certain COM objects in Office 2010 by using COM object categorization.
Plan Protected View settings for Office 2010	Provides information about how to configure Protected View, a new security feature in Office 2010 that helps mitigate exploits to your computer by opening files in a restricted environment so they can be examined before the files are opened for editing.
Plan Office File Validation settings for Office 2010	Provides information about how to configure Office File Validation, a new security feature in Office 2010 that helps prevent file format attacks by scanning Office binary file formats before the files are opened.
Plan password complexity settings for Office 2010	Provides information about settings to enforce strong passwords, such as password length and complexity rules, when you use the **Encrypt with Password** feature in Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.
Plan cryptography and encryption settings for Office 2010	Provides information about cryptography and encryption in Microsoft Office 2010, and describes the settings that you can use to encrypt data.
Plan digital signature settings for Office 2010	Provides information about how to digitally sign documents by using Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.
Plan privacy options for Office 2010	Describes how to configure privacy options in Office 2010 to meet an organization's security requirements.
Plan file block settings for Office 2010	Provides information about Group Policy and Office Customization Tool (OCT) settings that you can configure to block specific file format types for Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.
Plan for Information Rights Management in Office 2010	Provides a summary of Information Rights Management (IRM) technology and how it works in Office applications.
Plan for security and protection in Outlook 2010	Describes features in Microsoft Outlook 2010 that can help keep an organization's e-mail messaging secure.

Article	Description
Security articles for end users (Office 2010)	Lists and categorizes key Office 2010 security-related articles, videos, and training courses that IT administrators might want to share with end users.

Security overview for Office 2010

An organization's financial success often depends on the productivity of its information workers and the integrity and confidentiality of its intellectual property. Many IT departments find it difficult to satisfy these business needs because protection often comes at the expense of productivity. When too many security controls are implemented, worker productivity decreases. When too few security controls are implemented, worker productivity increases, but your attack surface also increases, forcing higher remediation costs and a higher total cost of ownership (TCO). Fortunately, several new security controls in Microsoft Office 2010 make it easier for IT professionals to build a robust defense against threats while maintaining information worker productivity.

Four of the new controls help harden and reduce the attack surface and help mitigate exploits. These new controls include the following:

Data Execution Prevention (DEP) support for Office applications A hardware and software technology that helps harden the attack surface by helping to protect against malicious code exploits.

Office File Validation A software component that helps reduce the attack surface by identifying files that do not follow a valid file format definition.

Expanded file block settings Settings managed in the Trust Center and through Group Policy that help reduce the attack surface by providing more specific control over the file types that an application can access.

Protected View A feature that helps mitigate attacks by enabling users to preview untrusted or potentially harmful files in a sandbox environment.

In addition to these new controls, Office 2010 provides several security improvements that further harden the attack surface by helping to ensure the integrity and confidentiality of data. These security enhancements include the following:

- Cryptographic agility
- Trusted time stamping support for digital signatures
- Domain-based password complexity checking and enforcement
- Encryption-strengthening enhancements
- Improvements to the Encrypt with Password feature
- Integrity checking of encrypted files

Office 2010 also provides several security improvements that have a direct affect on information worker productivity. Improvements in the Message Bar user interface, Trust Center user interface settings, and a trust model that persists users' trust decisions are some examples of the new features that help make security decisions and actions less intrusive to information workers. In addition, many of the new and enhanced security controls can be managed through Group Policy settings. This makes it easier for you to enforce and maintain the organization's security architecture.

In this article:

Layered defense is key

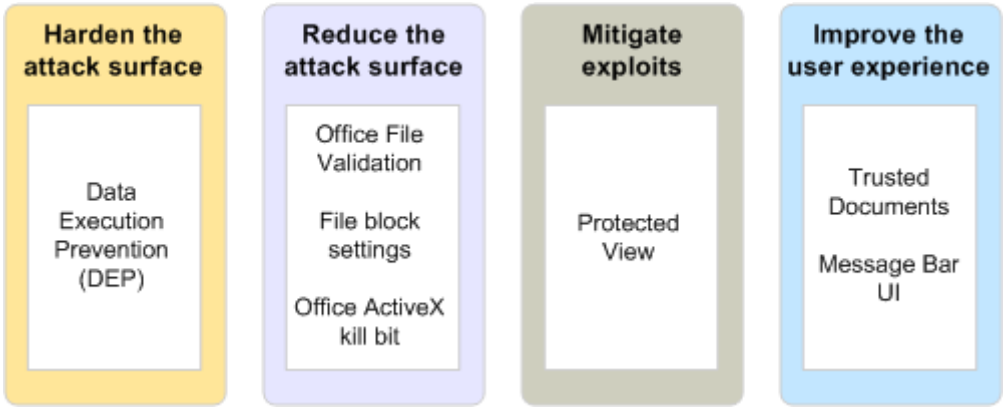
Defense in depth, a central tenet of any effective security architecture, is a security strategy that implements multiple overlapping layers of defense against unauthorized users and malicious code. In mid-sized and large organizations, the layers of defense typically include the following:

- Perimeter network protection, such as firewalls and proxy servers
- Physical security measures, such as restricted data centers and server rooms
- Desktop security tools, such as personal firewalls, virus scanning programs, and spyware-detection programs

A defense-in-depth strategy helps ensure that security threats are met with multiple and redundant security controls. For example, if a worm breaches the perimeter firewall and gains access to the internal network, it still has to pass through the virus-scanning program and the personal firewall to damage a desktop computer. A similar mechanism is built into the security architecture of Office 2010.

A four-layer approach

The security architecture of Office 2010 helps you extend the defense-in-depth strategy beyond desktop security tools by providing countermeasures for a layered defense. When implemented, these countermeasures take effect the moment a user attempts to open a file by using an Office 2010 application, and they continue to provide multiple layers of defense until the file is open and ready for editing. The following figure shows the four defensive layers that are built into the Office 2010 security architecture. It also shows some countermeasures that you can implement for each layer.



Hardening the attack surface

This defensive layer helps harden the attack surface of Office 2010 applications by using a countermeasure known as Data Execution Prevention (DEP). DEP helps prevent buffer overflow exploits by identifying files that attempt to run code from a part of memory reserved only for data. By default, DEP is enabled in Office 2010. You can manage DEP settings in the Trust Center or through Group Policy settings.

Reducing the attack surface

This defensive layer helps reduce the attack surface of Office 2010 applications by limiting the kinds of files that applications can open and by preventing applications from running certain kinds of code that is embedded in files. To do this, Office applications use the following three countermeasures:

- **Office File Validation** This software component scans files for format differences and based on the implemented setting can prevent a file from being opened for editing if the format is not valid. A file that contains a file format exploit against an Office 2010 application is one example of a file that is not valid. By default, Office File Validation is enabled and is primarily managed through Group Policy settings.
- **File block settings** Introduced in the 2007 Microsoft Office system to help reduce the attack surface, these settings enable you to prevent applications from opening and saving certain file types. In addition, you can specify what will occur if you allow a file type to be opened. For example, you can specify whether a file type is opened in Protected View and whether editing is allowed. Several new file block settings have been added in Office 2010. You can manage file block settings in the Trust Center and through Group Policy settings.
- **Office ActiveX kill bit** This new Office 2010 feature enables you to prevent specific ActiveX controls from running in Office 2010 applications without affecting how those controls run in Microsoft Internet Explorer. By default, Office ActiveX kill bit is not configured. However, you can configure this countermeasure by modifying the registry.

Mitigating exploits

This defensive layer helps mitigate exploits by opening potentially harmful files in an isolated sandbox environment. This sandbox environment, known as Protected View, enables users to preview files before they open them for editing in an application. By default, Protected View is enabled. However, you can turn it off and manage it in the Trust Center and through Group Policy settings.

Improving the user experience

This defensive layer mitigates exploits by reducing the number of security decisions users make and by improving the way users make security decisions. For example, documents that are considered untrustworthy are automatically opened in Protected View without any user feedback. Users can read and close these documents without making any security decisions, which in most cases means that they can effectively finish their work without being confronted with security prompts. If a user wants to edit a document that is in Protected View they can select the option to allow editing. Once editing is allowed, the document will not be opened in Protected View again. If the document contains active content, such as ActiveX controls and macros, a Message Bar appears that prompts the user whether to enable the active content. Once active content is enabled, the user will not be prompted again with

the Message Bar for active content. You can configure Message Bar settings and Trusted Documents settings in the Trust Center and through Group Policy settings.

Enhanced hardening countermeasures

In addition to the countermeasures described in the previous section, Office 2010 provides several new and enhanced countermeasures for further hardening of the attack surface. These countermeasures help harden the attack surface by protecting the integrity and confidentiality of data.

Integrity countermeasures

Integrity settings help you mitigate threats to the integrity of business data and business processes. Malicious users attack the integrity of these assets by corrupting documents, presentations, and spreadsheets. For example, a malicious user might attack the integrity of business data or business processes by replacing a file with a similar file that contains corrupted data or information. Two countermeasures have been improved and enhanced — digital signatures and integrity checking of encrypted files — to help you mitigate integrity threats.

Digital signature improvements

Trusted time stamping is now supported in digital signatures, which makes Office documents compatible with the W3C XML Advanced Electronic Signatures (XAdES) standard. Trusted time stamping helps ensure that digital signatures remain valid and legally defensible even if the certificate that is used to sign the document expires. Trusted time stamping support is available only in Microsoft Excel 2010, Microsoft Access 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010. To take advantage of this feature, you must use a time-stamping authority.

In addition to time stamping support, Office 2010 includes several improvements in the user interface that make managing and implementing digital signatures easier for users. You can also configure and manage trusted time stamping through several new Group Policy settings.

Integrity checking of encrypted files

Administrators can now decide whether to implement a hash-based message authentication code (HMAC) when a file is encrypted, which can help determine whether someone has tampered with a file. The HMAC is fully compliant with Windows Cryptographic API: Next Generation (CNG), enabling administrators to configure the cryptographic provider, hash, and context that are used to generate the HMAC. These parameters are configurable through Group Policy settings.

Confidentiality countermeasures

Confidentiality settings help you mitigate threats to information that you do not want disclosed either publicly or privately, such as e-mail correspondence, project planning information, design specifications, financial information, customer data, and personal and private information. Several countermeasures have been improved and enhanced to help you mitigate confidentiality threats.

Cryptographic enhancements

Several Office 2010 applications are now cryptographically agile and support CNG, which means that administrators can specify any cryptographic algorithm for encrypting and signing documents. In addition, several Office 2010 applications now support Suite B cryptography.

Encrypt with Password improvements

The Encrypt with Password feature is now compliant with the ISO/IEC 29500 and ISO/IEC 10118-3:2004 requirements. This feature is also interoperable between Office 2010 and the 2007 Office system with Service Pack 2 (SP2), but only if the host operating systems support the same cryptographic providers. In addition, Office 2010 includes several changes in the user interface that make the Encrypt with Password feature easier for users to understand and implement.

Password complexity checking and enforcement

Passwords used by the Encrypt with Password feature can now be checked for length and complexity, and enforced by domain-based password policies. This applies only to passwords that are created by using the Encrypt with Password feature. You can use several new Group Policy settings to manage password complexity checking and enforcement.

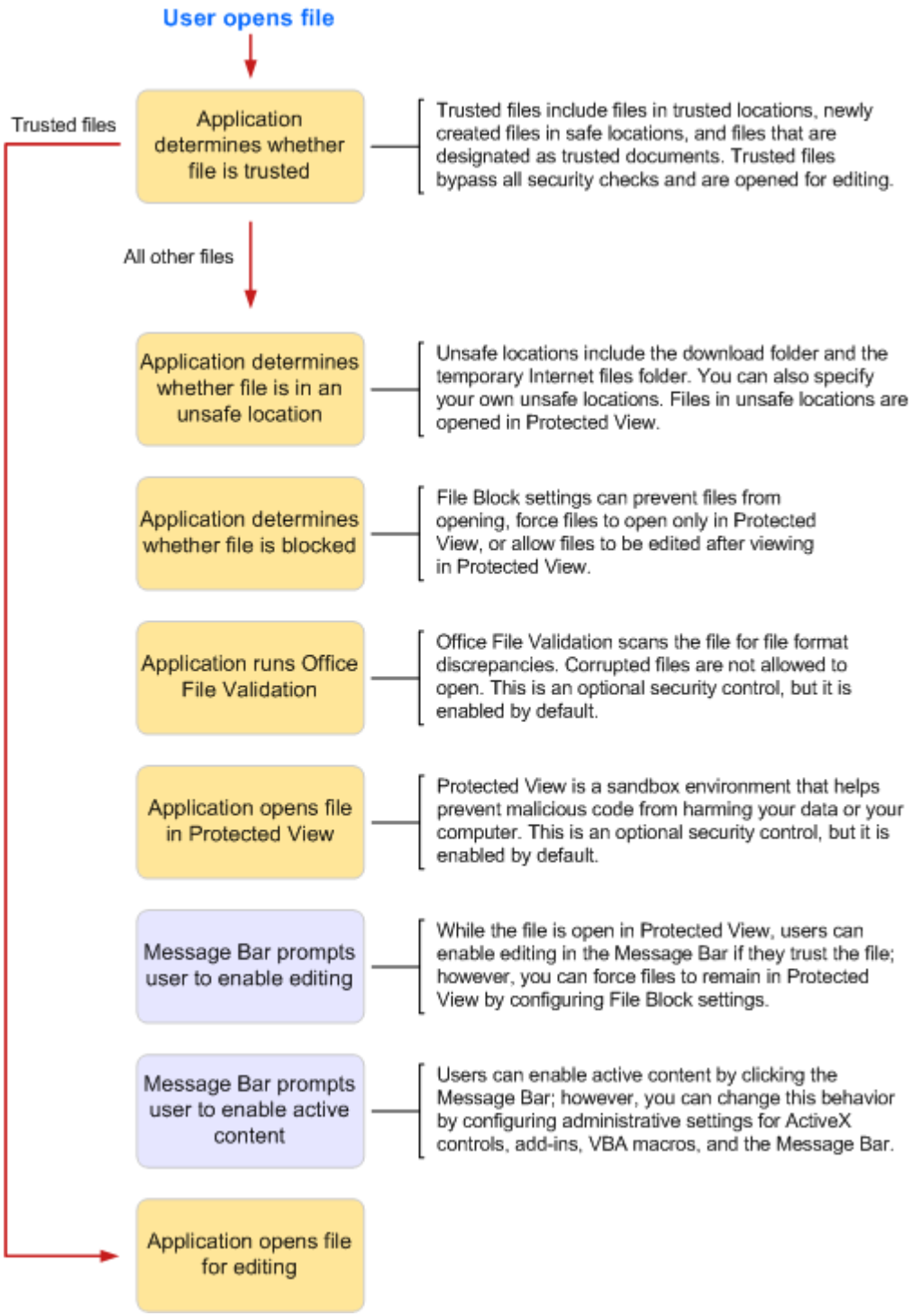
Encryption enhancements

The encryption mechanism is enhanced, which helps ensure that the encryption/decryption key is never stored as plain text in a file. In general, these encryption enhancements are transparent to users and administrators.

Helping users make better security decisions

One of the benefits of a layered defense is its stepwise ability to weaken and slow security attacks, which gives you more time to identify attack vectors and deploy alternative countermeasures (if needed). Another benefit of a layered defense is its intrinsic ability to reduce the number of security decisions users have to make. In its default security configuration, Office 2010 makes most of the security decisions, not the user. As a result, users have fewer opportunities to make inaccurate security decisions and are more productive.

The following figure shows a high-level view of the main security controls that are implemented when a user opens a file in Excel 2010, PowerPoint 2010, or Word 2010. Security controls that require no user input are yellow; security controls that require user input are light blue. The figure shows the default behavior of Office 2010. You can change this default behavior to suit the organization’s security requirements and architecture. Also, this figure does not show all of the security controls that can be implemented, such as DEP, encryption, or Information Rights Management.



As shown in the previous figure, documents must pass through several defensive layers before users are required to make a security decision. If users do not have to edit a document, they can read the

document in Protected View and then close it without making any security decisions. Several key features make this efficient workflow possible.

Improved trust model When users attempt to open a file, Office 2010 evaluates the file's trust state. By default, trusted files bypass most security checks and are opened for editing without requiring any security decisions by the user. Untrusted files must undergo the security checks that make up the layered defense. Documents that are considered untrustworthy are automatically opened in Protected View without any user feedback. If a user wants to edit a document that is in Protected View, the user can select the option to allow editing. Once editing is allowed, the document will not be opened in Protected View again. If the document contains active content, such as ActiveX controls and macros, a Message Bar appears that prompts the user whether to enable the active content. Once active content is enabled, the user will not be prompted again with the Message Bar for active content. In the 2007 Office system you can use the trusted locations and trusted publishers features to designate trusted files and trusted content. In Office 2010, you can also use a new feature known as Trusted Documents. Trusted Documents lets users designate a file as trusted after viewing the file in Protected View. When a user designates a file as being trusted, the trust decision persists with the file so that the user does not have to make the trust decision again the next time that they open the file.

Note:

Trusted files do not bypass antivirus checking or ActiveX kill-bit checking. If a file is trusted, it is scanned by the local antivirus scanning program (if available) and any ActiveX controls that have a kill-bit set are disabled.

Transparent countermeasures Several of the new countermeasures in Office 2010 are invisible to the user and require no user interaction. For example, Office 2010 applications evaluate untrusted files for file format differences by using a new technology known as Office File Validation. This technology runs autonomously when a user opens an untrusted file. If no potential file format differences are detected, users have no indication that this technology scanned the file.

Note:

In some cases, the Office File Validation feature might ask a user for permission to send file scan information to Microsoft to help improve the feature's ability to detect exploits. You can prevent these prompts from occurring by configuring Group Policy settings.

Sandbox previewing environment Untrusted files are opened in a sandbox previewing environment known as Protected View. Users can read files in this sandbox environment, and they can copy content to the clipboard. However, they cannot print files or edit them. In most cases, previewing a document is sufficient for users and they can close the file without answering any security questions. For example, even if a file contains an untrusted Visual Basic for Applications (VBA) macro, a user does not have to enable the VBA macro to preview the content in Protected View.

In most cases, the default security configuration in Office 2010 is a suitable defense-in-depth solution, which provides multiple layers of defense without impinging too much on user productivity. However, some organizations might have to modify the default security configuration to meet more strict security requirements or to reduce security and provide more flexibility to users. For example, if the organization consists mostly of expert users who do not have to preview files in sandbox environment, you can

disable Protected View. We do not recommend this (and it might be very risky), but it helps reduce the number of security decisions users make. Likewise, if the organization requires a locked-down security environment, you can modify the security settings so that all untrusted documents must be opened in Protected View and can never leave Protected View. This might provide more protection, but it also hinders a user's ability to edit a file. Regardless of the organization's particular security requirements, the multilayered countermeasures in Office 2010 let you effectively balance security and productivity; that is, you can increase or decrease the frequency and the kind of security decisions users have to make without completely compromising the security architecture.

Giving the administrator full control

Most large and mid-sized organizations use some centralized management tool, such as domain-based Group Policy settings, to deploy and manage their security configurations. Using domain-based Group Policy settings helps ensure that the computers in the organization have a consistent configuration and enables you to enforce the security configuration — two requirements of an effective security strategy. To that end, Office 2010 provides an expanded suite of Group Policy settings to help you effectively deploy and manage the security configuration.

The following table shows the different ways that you can manage the new security controls in Office 2010. It also shows which applications support the new security features.

Security feature	Configurable in the Trust Center?	Configurable through Group Policy settings?	Applies to which applications?
Data Execution Prevention	Yes	Yes	All Office 2010 applications.
Office File Validation	No	Yes	Excel 2010 PowerPoint 2010 Word 2010
File block settings	Yes	Yes	Excel 2010 PowerPoint 2010 Word 2010
Office ActiveX kill bit	No	No (must be configured in the registry)	Microsoft Access 2010 Excel 2010 PowerPoint 2010 Microsoft Visio 2010 Word 2010

Security feature	Configurable in the Trust Center?	Configurable through Group Policy settings?	Applies to which applications?
Protected View	Yes	Yes	Excel 2010 PowerPoint 2010 Word 2010
Trusted Documents	Yes	Yes	Access 2010 Excel 2010 PowerPoint 2010 Visio 2010 Word 2010
Encryption (cryptographic agility) settings	No	Yes	Access 2010 Excel 2010 InfoPath 2010 OneNote 2010 PowerPoint 2010 Word 2010
Time stamping of digital signatures	No	Yes	Excel 2010 InfoPath 2010 PowerPoint 2010 Word 2010
Integrity checking of encrypted files	No	Yes	Excel 2010 PowerPoint 2010 Word 2010
Password complexity and enforcement	No	Yes	Excel 2010 PowerPoint 2010 Word 2010

Migrating security and privacy settings from Office 2003

Office 2010 contains many security features that can help protect documents and help make desktops more secure. Some of these security features were introduced in the 2007 Office system, and have been enhanced in Office 2010. Other security features are new to Office 2010. If you are migrating to

Office 2010 from Microsoft Office 2003 or an earlier version of Office, it might be helpful to understand when various Office 2010 security and privacy features were introduced.

The following table shows the main security and privacy features that were added or enhanced in the 2007 Office system and Office 2010.

Security feature	Description	Feature status in the 2007 Office system	Feature status in Office 2010	For more information see…
Trust Center	A central console in the user interface that enables users to view and configure security settings and privacy options.	Introduced in the 2007 Office system	Enhanced and expanded settings in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=160365*)
Message Bar	A user interface element that gives users notifications and warnings when they open a document that contains potentially harmful content.	Introduced in the 2007 Office system	Enhanced the message bar user interface in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=161330*)
Trusted Locations	A security feature that enables you to differentiate safe and unsafe	Introduced in the 2007 Office system	No significant changes in Office 2010	Plan Trusted Locations and Trusted Publishers in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=160295*)

Security feature	Description	Feature status in the 2007 Office system	Feature status in Office 2010	For more information see…
	documents.			
File block settings	A suite of security settings that enable you to prevent users from opening or saving certain kinds of files.	Introduced in the 2007 Office system	Enhanced and expanded settings in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=161330*)
Document Inspector	A privacy tool that can help users remove personal information and hidden information from a document.	Introduced in the 2007 Office system	Enhanced the user interface in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkID=161331*)
Global and application-specific settings for ActiveX controls	Enables you to disable all ActiveX controls, configure ActiveX control initialization, and configure ActiveX control prompts.	Introduced in the 2007 Office system	No significant functional changes in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=161332*)
Enhanced global and application-specific settings for	Enables you to disable VBA and configure macro warnings	Introduced in the 2007 Office system	No significant functional changes in Office	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=161332*)

Security feature	Description	Feature status in the 2007 Office system	Feature status in Office 2010	For more information see…
VBA macros	settings.		2010	
Application-specific settings for add-ins	Enables you to disable add-ins, require that add-ins are signed by a trusted publisher, and configure add-in warnings.	Introduced in the 2007 Office system	No significant functional changes in Office 2010	Overview of security in the 2007 Office system (*http://go.microsoft.com/fwlink/?LinkId=161332*)
Data Execution Prevention (DEP)	A hardware and software technology that helps harden the attack surface by preventing viruses and worms that exploit buffer overflow vulnerabilities.	Not available in 2007 Office system applications	Introduced in Office 2010	Data Execution Prevention in Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=193251*)
Office File Validation	A countermeasure that scans files for format differences and prevents files from being opened for editing if the format is not valid.	Not available in 2007 Office system applications	Introduced in Office 2010	Plan Office File Validation settings for Office 2010
Office	An Office	Available	Introduce	How to stop an ActiveX control from running

Security feature	Description	Feature status in the 2007 Office system	Feature status in Office 2010	For more information see…
ActiveX kill bit	feature that administrators can use to prevent specific ActiveX controls from running within Office applications.	in 2007 Office system applications as an Internet Explorer ActiveX kill bit	d in Office 2010 as an Office ActiveX kill bit	in Internet Explorer (*http://go.microsoft.com/fwlink/?LinkId=160644*)
Protected View	An Office feature that helps mitigate attacks by enabling users to preview untrusted or potentially harmful files in a sandbox environment.	Not available in 2007 Office system applications	Introduced in Office 2010	Plan Protected View settings for Office 2010
Trusted Documents	A security tool that enables users to designate safe documents.	Not available in 2007 Office system applications	Introduced in Office 2010	Trusted Documents in Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=193508*)
Trusted time stamping of digital signatures	Helps ensure that digital signatures remain valid and legally defensible even if the	Not available in 2007 Office system applications	Introduced in Office 2010	Plan digital signature settings for Office 2010

Security feature	Description	Feature status in the 2007 Office system	Feature status in Office 2010	For more information see…
	certificate that you used to sign the document expires.			
Integrity checking of encrypted files	Enables you to implement a hash-based message authentication code (HMAC) when a file is encrypted.	Not available in 2007 Office system applications	Introduced in Office 2010	Plan cryptography and encryption settings for Office 2010
Password complexity checking and enforcement	Enables you to check and enforce passwords for length and complexity by using domain-based password policies.	Not available in 2007 Office system applications	Introduced in Office 2010	Plan password complexity settings for Office 2010
Cryptographic agility	Enables you to specify cryptographic settings for encrypting documents.	Not available in 2007 Office system applications	Introduced in Office 2010	Plan cryptography and encryption settings for Office 2010

Understand security threats and countermeasures for Office 2010

A secure desktop configuration is an important part of any organization's defense-in-depth strategy. But before you can plan for a secure desktop configuration that includes Microsoft Office 2010, you must understand which security risks and threats are relevant to Office 2010, and then determine which of those security risks and threats pose a risk to the organization's business assets or business processes. You also have to determine which privacy risks and threats pose a risk to users' personal and private information.

In this article:

Information security risks

Most IT professionals and IT security specialists categorize information security risks into three broad categories:

- **Confidentiality risks** These risks represent threats to an organization’s intellectual property from unauthorized users and malicious code that attempt to access what is said, written, and created in an organization.
- **Integrity risks** These risks represent threats to your business resources from unauthorized users and malicious code that attempt to corrupt the business data on which your organization relies. Integrity risks jeopardize any business asset that contains critical information for an organization, such as database servers, data files, and e-mail servers.
- **Availability risks** These risks represent threats to business processes by unauthorized users and malicious code that attempt to disrupt the way that you do business and how information workers complete their work. Business intelligence processes, application features and capabilities, and document workflow processes can all be threatened by availability risks.

To help ensure that your organization is protected from all three of these risk categories, a defense-in-depth security strategy is recommended; that is, a security strategy that includes multiple overlapping layers of defense against unauthorized users and malicious code. Layers typically include the following:

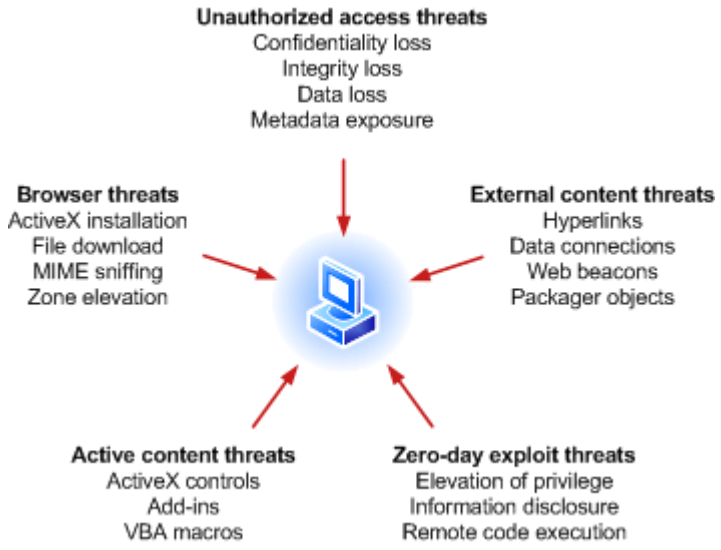
- Perimeter network protection, such as firewalls and proxy servers.
- Physical security measures, such as physically secure data centers and server rooms.
- Desktop security tools, such as personal firewalls, virus scanning programs, and spyware detection.

If Office 2010 is part of an organization's environment, the defense-in-depth strategy must also include the mitigation mechanisms that are provided with Office 2010. These mitigation mechanisms include many technologies, settings, and features. By using these mechanisms, you can help mitigate threats to Office 2010 applications and help protect the intellectual property, business resources, and business processes that are at the heart of the business.

By default, the Office 2010 security model helps an organization mitigate all three kinds of risk. However, every organization has different infrastructure capabilities, different productivity demands, and different desktop security requirements. To determine exactly how the organization can mitigate these business risks, you have to evaluate the threats and threat agents that exploit these risks.

Threats to desktop productivity applications

The security model for Office 2010 helps you mitigate five kinds of productivity software security threats. Each of these threat types include several threat agents, which can be exploited by various security attacks. The following illustration shows the security threats and examples of the most common threat agents.



Most organizations face some potential risk from five kinds of security threats. However, most organizations deal with unique combinations of threat agents and potential security attacks or exploits.

Active content threats

Active content threats are common desktop security threats. Typical threat agents include ActiveX controls, add-ins, and VBA macros. These threat agents can be exploited by programmers who write malicious code or create malicious programs, which then run on users' computers. Active content

threats pose a potential risk to any size organization, especially organizations that let users do the following:

- Run ActiveX controls, add-ins, or VBA macros.
- Open e-mail attachments.
- Share documents across a public network, such as the Internet.
- Open documents from sources outside the organization, such as clients, vendors, or partners.

Unauthorized access threats

Unauthorized access threats occur when unauthorized users attempt to gain access to information. Potential targets of unauthorized users include the following:

- **Document files** If unauthorized users gain access to document files, they can delete, replace, or corrupt the files. For example, a malicious programmer might use a file format attack to exploit an unauthorized access threat in a document.
- **Information within documents** This information includes text, graphics, comments, revisions, annotations, custom XML data, hidden text, watermarks and header and footer information. When unauthorized users access the information within documents, they might access sensitive data, such as company confidential data, and personal or private information about users. They can also alter, corrupt, or delete information, and they can use their access to add active content to documents saved in trusted locations.
- **Metadata** Information associated with documents, including document properties such as author name, organization name, document editing time, or document version number. Unauthorized users who gain access to metadata might access sensitive personal or company data. They can also corrupt or remove metadata.

Most organizations face unauthorized access threats, although many organizations do not take sufficient measures to mitigate them because they perceive the threat to be minimal or consider the administrative cost for mitigating the threat excessive. These perceptions could lead to unsafe practices and circumstances such as the following:

- The organization's network security architecture cannot prevent an intruder or attacker from gaining access to your internal network, which increases the risk that an intruder or attacker might gain access to your organization's documents.
- The organization lets users send, receive, or share proprietary documents over the Internet, including financial data, project plans, presentations, or drawings.
- The organization does not prevent users from connecting portable computers to public networks, which increases the risk that an unidentifiable attacker might gain access to the documents that are saved on those portable computers.
- The organization does not prevent users from taking documents that contain proprietary information out of the office.
- There is a chance that an unauthorized attacker or intruder can gain access to documents that contain proprietary information.

External content threats

External content threats include any threat agent that links a document to another document, a database, or a Web site across an intranet or a public network, such as the Internet. External content threats are exploited through the following threat agents:

- **Hyperlinks** An attacker typically exploits this threat agent by creating hyperlinks to documents that are not trusted or Web sites that contain malicious code or content.
- **Data connections** An attacker typically exploits this threat agent by creating data connections to data sources or databases, and then by using such connections to maliciously manipulate or extract data.
- **Web beacons** A typical scenario for exploiting this threat agent is for an attacker to embed an invisible link to a remote image in an e-mail message. When a user opens the message, the link becomes active and downloads the remote image. In the process, user information can be sent to the remote computer, such as the user's e-mail address and the IP address of their computer.
- **Packager objects** An attacker can exploit this threat agent by having an embedded object run malicious code.

External threats pose a risk if the organization:

- Gives users unrestricted access to public networks, such as the Internet.
- Does not prevent users from receiving e-mail messages that contain embedded images and HTML.
- Does not prevent users from using data connections in spreadsheets or other documents.

Browser threats

These threats can exist when an application or a document programmatically uses the functionality of a Web browser, such as Microsoft Internet Explorer. Browser threats pose a risk to applications and documents because any threats that exist for the browser also exist for the application or document that hosts the browser. Browser threats include many threat agents, and can be exploited through various security attacks. Examples of these threat agents include ActiveX control installation, file downloads, MIME sniffing, zone elevation, and add-on installation.

Browser threats pose a risk if your organization:

- Allows users to run ActiveX controls, add-ins, or macros that use browser functionality.
- Develops and distributes Office solutions that use browser functionality.

Zero-day exploit threats

Zero-day exploits can be launched when a security vulnerability is found that has not yet been addressed by a software update, such as a Microsoft security bulletin or service pack. Zero-day exploits can take several forms, including the following:

- Remote code execution
- Elevation of privilege

- Information disclosure

Malicious programmers and users can exploit security vulnerabilities through various security attacks. Until a security bulletin or a service pack is released to respond to the security vulnerability, the vulnerability can pose a potential threat to your organization.

Default countermeasures in Office 2010

Office 2010 provides many countermeasures that help mitigate threats to your business assets and business processes. A *countermeasure* is a security feature or a security control that mitigates one or more security threats. You can usually change the behavior of countermeasures by configuring settings in the Office Customization Tool (OCT) or through Group Policy by using the Office 2010 Administrative Templates.

Many of the countermeasures in Office 2010 mitigate a specific kind of threat in one particular application. For example, Microsoft InfoPath 2010 includes a countermeasure that warns users about the possible presence of Web beacons in forms. You can change the behavior of this countermeasure by configuring the **Beaconing UI for forms opened in InfoPath** setting in the OCT or through Group Policy.

Other countermeasures mitigate broader kinds of threats that are common to several applications. For example, the Protected View feature enables users to view the content of untrusted documents, presentations, and workbooks without enabling unsafe content or malicious code to harm the computer. This countermeasure is used by Microsoft Excel 2010, Microsoft PowerPoint 2010, Microsoft Word 2010, and Microsoft Outlook 2010 when you preview attachments for Excel 2010, PowerPoint 2010, Microsoft Visio 2010, and Word 2010. You can change its behavior by configuring several settings in the OCT or through Group Policy.

The following sections describe the most frequently used countermeasures in Office 2010.

ActiveX control settings

You can use ActiveX control settings to disable ActiveX controls and change the way ActiveX controls are loaded into Office 2010 applications. By default, trusted ActiveX controls are loaded in safe mode with persistent values and users are not notified that the ActiveX controls loaded. Untrusted ActiveX controls load differently depending on how the ActiveX control is marked and whether a VBA project exists in the file together with the ActiveX control. The default behavior of untrusted ActiveX controls is as follows:

- If an ActiveX control is marked Safe for Initialization (SFI) and it is contained in a document that does not contain a VBA project, the ActiveX control is loaded in safe mode with persistent values. The Message Bar does not appear and users are not notified about the presence of the ActiveX control. All ActiveX controls in the document must be marked SFI for this behavior to occur.
- If an ActiveX control is marked Unsafe for Initialization (UFI) and it is contained in a document that does not contain a VBA project, users are notified in the Message Bar that ActiveX controls are disabled. However, users can click the Message Bar to enable ActiveX controls. If a user enables

ActiveX controls, all ActiveX controls (those marked UFI and SFI) are loaded in safe mode with persistent values.

- If an ActiveX control marked UFI or SFI is contained in a document that also contains a VBA project, users are notified in the Message Bar that ActiveX controls are disabled. However, users can click the Message Bar to enable ActiveX controls. If a user enables ActiveX controls, all ActiveX controls (those marked SFI and UFI) are loaded in safe mode with persistent values.

Important:
If a kill bit is set in the registry for an ActiveX control, the control is not loaded and cannot be loaded in any circumstance. The Message Bar does not appear and users are not notified about the presence of the ActiveX control.

To change the default behavior of ActiveX controls, see Plan security settings for ActiveX controls for Office 2010.

Add-in settings

You can use add-in settings to disable add-ins, require add-ins be signed by a trusted publisher, and disable notifications for add-ins. By default, installed and registered add-ins can run without requiring user intervention or warning. To change this default behavior, see Plan security settings for add-ins for Office 2010.

Cryptography and encryption settings

These settings will be available when Office 2010 is officially released.

Data Execution Prevention settings

You can use Data Execution Prevention (DEP) settings to disable DEP in Office 2010 applications. DEP is a hardware and software countermeasure that helps prevent malicious code from running. By default, DEP is enabled in Office 2010 applications and we recommend that you do not change this default setting.

Digital signature settings

These settings will be available when Office 2010 is officially released.

External content settings

You can use external content settings to change the way Office 2010 applications access external content. External content is any kind of content that is accessed remotely, such as data connections and workbook links, hyperlinks to Web sites and documents, and links to images and media. By default, when a user opens a file that contains links to external content, the Message Bar notifies the user that the links are disabled. Users can enable the links by clicking the Message Bar. We recommend that you do not change these default settings.

File Block settings

You can use File Block settings to prevent specific file types from being opened or saved. You can also use these settings to prevent or force certain file types from opening in Protected View. By default, Excel 2010, PowerPoint 2010, and Word 2010 force several kinds of files to open only in Protected View. Users cannot open these file types for editing.

Office File Validation settings

You can use Office File Validation settings to disable the Office File Validation feature and change how the Office File Validation feature handles files that do not pass validation. You can also use these settings to prevent the Office File Validation feature from prompting users to send validation information to Microsoft. By default, the Office File Validation feature is enabled. Files that do not pass validation are opened in Protected View and users can edit files after they are opened in Protected View. For more information about Office File Validation settings, see Plan Office File Validation settings for Office 2010.

Password complexity settings

You can use password complexity settings to enforce password length and complexity for passwords that are used with the Encrypt with Password feature. Password complexity settings let you enforce password length and complexity at the domain level if the organization has established password complexity rules through domain-based Group Policy, or at a local level if the organization has not implemented domain-based password complexity Group Policy. By default, Office 2010 applications do not check password length or complexity when a user encrypts a file by using the Encrypt with Password feature.

Privacy options

You can use privacy options to prevent the **Welcome to Microsoft Office 2010** dialog box from appearing the first time that a user starts Office 2010. This dialog box lets users enroll in various Internet-based services that help protect and improve Office 2010 applications. You can also use privacy options to enable the Internet-based services that appear in the **Welcome to Microsoft Office 2010** dialog box. By default, the **Welcome to Microsoft Office 2010** dialog box appears when a user starts Office 2010 for the first time, and users can enable the recommended Internet-based services, enable a subset of these services, or make no configuration changes. If a user makes no configuration changes, the following default settings take effect:

- Office 2010 applications do not connect to Office.com for updated Help content.
- Office 2010 applications do not download small programs that help diagnose problems and error message information is not sent to Microsoft.
- Users are not enrolled in the Customer Experience Improvement Program.
- When users implement a search query from the Help system, information about which Office 2010 applications are installed is not sent to Microsoft to improve Office.com search results.

To change this default behavior, or to suppress the **Welcome to Microsoft Office 2010 dialog** box, see Plan privacy options for Office 2010.

Protected View settings

You can use Protected View settings to prevent files from opening in Protected View and force files to open in Protected View. You can also specify whether you want scripts and programs that run in Session 0 to open in Protected View. By default, Protected View is enabled and all untrusted files open in Protected View. Scripts and programs running in Session 0 do not open in Protected View. For more information about Protected View settings, see Plan Protected View settings for Office 2010.

Note:
You can also use File Block settings to prevent or force specific file types from opening in Protected View.

Trusted Documents settings

You can use Trusted Documents settings to disable the Trusted Documents feature and prevent users from trusting documents that are stored on network shares. Trusted documents bypass most security checks when they are opened and all active content is enabled (antivirus checking and ActiveX kill-bit checking are the two checks that cannot be bypassed). By default, the Trusted Documents feature is enabled, which means users can designate safe files as trusted documents. In addition, users can designate files on network shares as trusted documents. We recommend that you do not change these default settings.

Trusted Locations settings

You can use Trusted Locations settings to designate safe locations for files. Files that are stored in trusted locations bypass most security checks when they are opened and all content in the file is enabled (antivirus checking and ActiveX kill-bit checking are the two checks that cannot be bypassed). By default, several locations are designated as trusted locations. Also, trusted locations that are on a network, such as shared folders, are disabled. To change this default behavior, and find out which locations are designated as trusted locations by default, see Plan Trusted Locations settings for Office 2010.

Trusted Publishers settings

You can use Trusted Publishers settings to designate certain kinds of active content as being safe, such as ActiveX controls, add-ins, and VBA macros. When a publisher signs active content with a digital certificate, and you add the publisher's digital certificate to the Trusted Publishers list, the active content is considered trusted. By default, there are no publishers on the Trusted Publishers list. You must add publishers to the Trusted Publishers list to implement this security feature. To implement the Trusted Publishers feature, see Plan Trusted Publishers settings for Office 2010.

VBA macro settings

You can use VBA macro settings to change the way VBA macros behave, disable VBA, and change the way VBA macros behave in applications that are started programmatically. By default, VBA is enabled and trusted VBA macros are allowed to run without notification. Trusted VBA macros include VBA macros that are signed by a trusted publisher, stored in a trusted document, or stored in a document that is in a trusted location. Untrusted VBA macros are disabled, but a notification in the Message Bar lets users enable untrusted VBA macros. In addition, VBA macros are allowed to run in applications that are started programmatically.

To change this default behavior, see Plan security settings for VBA macros for Office 2010.

See Also

Security overview for Office 2010

Plan Trusted Locations settings for Office 2010

If you want to differentiate safe files from potentially harmful files, you can use the Trusted Locations feature in Microsoft Office 2010. The Trusted Locations feature lets you designate trusted file sources on the hard disks of users' computers or on a network share. When a folder is designated as a trusted file source, any file that is saved in the folder is assumed to be a trusted file. When a trusted file is opened, all content in the file is enabled and active, and users are not notified about any potential risks that might be contained in the file, such as unsigned add-ins and Microsoft Visual Basic for Applications (VBA) macros, links to content on the Internet, or database connections.

In this article:

About planning Trusted Locations settings

Office 2010 provides several settings that let you control the behavior of the Trusted Locations feature. By configuring these settings, you can do the following:

- Specify trusted locations globally or on a per-application basis.
- Allow trusted locations to exist on remote shares.
- Prevent users from designating trusted locations.
- Disable the Trusted Locations feature.

The Trusted Locations feature is available in the following applications: Microsoft Access 2010, Microsoft Excel 2010, Microsoft InfoPath 2010, Microsoft PowerPoint 2010, Microsoft Visio 2010, and Microsoft Word 2010.

The following list describes the default configuration for the Trusted Locations feature:

- Trusted Locations is enabled.
- Users cannot designate network shares as trusted locations. However, users can change this setting in the Trust Center.
- Users can add folders to the Trusted Locations list.
- Both user-defined and policy-defined trusted locations can be used.

In addition, several folders are designated as trusted locations in a default installation of Office 2010. The default folders for each application are listed in the following tables. (InfoPath 2010 and Visio 2010 have no default trusted locations.)

Access 2010 trusted locations

The following table lists the default trusted locations for Access 2010.

Default trusted locations	Folder description	Trusted subfolders
Program Files\Microsoft Office\Office14\ACCWIZ	Wizard databases	Not allowed

Excel 2010 trusted locations

The following table lists the default trusted locations for Excel 2010.

Default trusted locations	Folder description	Trusted subfolders
Program Files\Microsoft Office\Templates	Application templates	Allowed
Users*user_name*\Appdata\Roaming\Microsoft\Templates	User templates	Not allowed
Program Files\Microsoft Office\Office14\XLSTART	Excel startup	Allowed
Users*user_name*\Appdata\Roaming\Microsoft\Excel\XLSTART	User startup	Not allowed
Program Files\Microsoft Office\Office14\STARTUP	Office startup	Allowed
Program Files\Microsoft Office\Office14\Library	Add-ins	Allowed

PowerPoint 2010 trusted locations

The following table lists the default trusted locations for PowerPoint 2010.

Default trusted locations	Folder description	Trusted subfolders
Program Files\Microsoft Office\Templates	Application templates	Allowed
Users*user_name*\Appdata\Roaming\Microsoft\Templates	User templates	Allowed
Users*user_name*\Appdata\Roaming\Microsoft\Addins	Add-ins	Not allowed
Program Files\Microsoft Office\Document Themes 14	Application themes	Allowed

Word 2010 trusted locations

The following table lists the default trusted locations for Word 2010.

Default trusted locations	Folder description	Trusted subfolders
Program Files\Microsoft Office\Templates	Application templates	Allowed
Users*user_name*\Appdata\Roaming\Microsoft\Templates	User templates	Not allowed
Users*user_name*\Appdata\Roaming\Microsoft\Word\Startup	User startup	Not allowed

Note:
For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*).

Implement Trusted Locations

To implement Trusted Locations, you must determine the following:

- The applications for which you want to configure Trusted Locations.
- The folders that you want to designate as trusted locations.
- The folder sharing and folder security settings that you want to apply to your trusted locations.
- The restrictions that you want to apply to trusted locations.

Determine the applications that you want to configure

Use the following guidelines to help determine the applications for which you want to configure Trusted Locations:

- Trusted Locations affect all content in a file, including add-ins, ActiveX controls, hyperlinks, links to data sources and media, and VBA macros. Moreover, files opened from trusted locations skip file validation checks, File Block checks, and do not open in Protected View.
- Each application provides the same settings for configuring Trusted Locations. This means that you can independently customize Trusted Locations for each application.
- You can disable Trusted Locations for one or more applications, and implement Trusted Locations for other applications.

Determine the folders to designate as trusted locations

Use the following guidelines to help determine the folders that you want to designate as trusted locations:

- You can specify trusted locations on a per-application basis or globally.
- One or more applications can share a trusted location.
- To prevent malicious users from adding files to a trusted location or from modifying files that are saved in a trusted location, you must apply operating system security settings to any folder that you designate as a trusted location.
- By default, only trusted locations that are on users' hard disks are allowed. To enable trusted locations on network shares, you must enable the **Allow Trusted Locations not on the computer** setting.
- We do not recommend that you specify root folders, such as drive C, or the whole Documents or My Documents folder as trusted locations. Instead, create a subfolder within those folders and specify only that folder as a trusted location.

In addition, you must use the guidelines in the following sections if you want to:

- Use environment variables to specify trusted locations.
- Specify Web folders (that is, http://paths) as trusted locations.

Use environment variables to specify trusted locations

You can use environment variables by using Group Policy and the OCT to specify trusted locations. However, when you use environment variable within the OCT, you must change the value type that is used to store trusted locations in the registry for environment variables to work correctly. If you use an environment variable to specify a trusted location, and you do not make the necessary registry modification, the trusted location appears in the Trust Center. But it is unavailable and it appears as a relative path that contains the environment variables. After you change the value type in the registry, the trusted location appears in the Trust Center as an absolute path and is available.

To use environment variables to specify trusted locations

1. Use Registry Editor to locate the trusted location that is represented by an environment variable.

   To open Registry Editor, click **Start**, click **Run**, type **regedit**, and then click **OK**.

   Trusted locations that are configured by using the OCT are stored in the following location:

   HKEY_CURRENT_USER/Software/Microsoft/Office/14.0/application_name/Security/Trusted Locations

   Where *application_name* can be Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, or Microsoft Word.

   Trusted locations are stored in registry entries named Path, and they are stored as String Value (REG_SZ) value types. Be sure to locate each Path entry that uses environment variables to

specify a trusted location.

2. Change the Path value type.

   Applications in the Office 2010 cannot recognize environment variables that are stored as String Value (REG_SZ) value types. For applications to recognize environment variables, you must change the value type of the Path entry so that it is an Expandable String Value (REG_EXPAND_SZ) value type. To do this, follow these steps:

   a. Write down or copy the value of the Path entry. This should be a relative path that contains one or more environment variables.

   b. Delete the Path entry.

   c. Create a newPathentry of type Expandable String Value (REG_EXPAND_SZ).

   d. Modify the new Path entry so that it has the same value that you wrote down or copied in the first step.

   Be sure to make this change for each Path entry that uses environment variables to specify a trusted location.

Specify Web folders as trusted locations

You can specify Web folders (that is, http://paths) as trusted locations. However, only those Web folders that support Web Distributed Authoring and Versioning (WebDAV) or FrontPage Server Extensions Remote Procedure Call (FPRPC) protocols are recognized as trusted locations. Use the following guidelines if you are not sure whether a Web folder supports the WebDAV or FPRPC protocols:

- If an application is opened by Internet Explorer, check the most recently used files list. If the most recently used files list indicates that the file is located on a remote server, rather than in the Temporary Internet Files folder, it is likely that the Web folder supports WebDAV in some form. For example, if you click a document while browsing Internet Explorer, and the document opens in Word 2010, the most recently used files list should show that the document is located on the remote server and not in the local Temporary Internet Files folder.
- Try to use the **Open** dialog box to browse to the Web folder. If the path supports WebDAV, you probably can browse to the Web folder or you are prompted for credentials. If the Web folder does not support WebDAV, navigation fails and the dialog box closes.

Note:
Sites that are created with Windows SharePoint Services and Microsoft SharePoint Server can be designated as trusted locations.

Determine folder sharing and folder security settings

All folders that you specify as trusted locations must be secured. Use the following guidelines to determine which sharing settings and security settings that you have to apply to each trusted location:

- If a folder is shared, configure sharing permissions so that only authorized users have access to the shared folder. Be sure to use the principle of least privilege and grant permissions that are appropriate to a user. That is, grant Read permission to those users who do not have to modify trusted files, and grant Full Control permission to those users who have to modify trusted files.
- Apply folder security permissions so that only authorized users can read or modify the files in trusted locations. Make sure to use the principle of least privilege and to grant permissions that are appropriate to a user. That is, grant Full Control permissions to only those users who have to modify files; and grant more-restrictive permissions to those users who need only to read files.

Determine restrictions for trusted locations

Office 2010 provides several settings that enable you to restrict or control the behavior of trusted locations. Use the following guidelines to determine how to configure these settings.

Setting name: Allow mix of policy and user locations

Description: This setting controls whether trusted locations can be defined by users, the OCT, and Group Policy, or if they must be defined by Group Policy alone. By default, users can designate any location as a trusted location and a computer can have any combination of user-created, OCT-created, and Group Policy-created trusted locations.

Impact: If this setting is disabled, all trusted locations that are not created by Group Policy are disabled and users cannot create new trusted locations in the Trust Center. Disabling this setting will cause some disruption for users who have defined their own trusted locations in the Trust Center. Applications treat such locations as they treat any other untrusted locations, which means that users see Message Bar warnings about content such as ActiveX controls and VBA macros when they open files, and they have to choose whether to enable controls and macros or leave them disabled This is a global setting that applies to all applications for which you configure trusted locations.

Guidelines: Organizations that have a highly restrictive security environment typically disable this setting. Organizations that manage their desktop configurations through Group Policy typically disable this setting.

Setting name: Allow Trusted Locations not on the computer

Description: This setting controls whether trusted locations on the network can be used. By default, trusted locations that are network shares are disabled. But users can still select the **Allow Trusted Locations on my network** check box in the Trust Center, which will enable users to designate network shares as trusted locations. This is not a global setting. You must configure this setting on a per-application basis for Access 2010, Excel 2010, PowerPoint 2010, Visio 2010, and Word 2010.

Impact: Disabling this setting disables all trusted locations that are network shares and prevents users from selecting the **Allow Trusted Locations on my network** check box in the Trust Center. Disabling this setting will cause some disruption for users who have defined their own trusted locations in the Trust Center. If you disable this setting, and a user attempts to designate a network share as a trusted location, a warning informs the user that the current security settings do not allow the creation of Trusted Locations that are remote paths or network paths. If an administrator

designates a network share as a trusted location through Group Policy or by using the OCT, and this setting is disabled, the trusted location is disabled. Applications treat such locations like any other untrusted locations, which means that users see Message Bar warnings about content such as ActiveX controls and VBA macros when they open files, and they have to choose whether to enable controls and macros or leave them disabled.

Guidelines: Organizations that have a highly restrictive security environment typically disable this setting.

Note:
You can also use the **Remove all Trusted Locations written by the OCT during installation** setting to delete all trusted locations that have been created by configuring the OCT.

Disable Trusted Locations

Office 2010 provides a setting that enables you to disable the Trusted Locations feature. This setting must be configured on a per-application basis for Access 2010, Excel 2010, PowerPoint 2010, Visio 2010, and Word 2010. Use the following guidelines to determine whether you should use this setting.

Setting name: Disable all Trusted Locations

Description: This setting lets administrators disable the Trusted Locations feature on a per-application basis. By default, the Trusted Locations feature is enabled and users can create trusted locations.

Impact: Enabling this setting disables all trusted locations, including trusted locations that are:

- Created by default during setup.
- Created by using the OCT.
- Created by users through the Trust Center.
- Created by using Group Policy.

Enabling this setting also prevents users from configuring Trusted Locations settings in the Trust Center. If you enable this setting, make sure that you notify users that they cannot use the Trusted Locations feature. If users have been opening files from trusted locations, and you enable this setting, users might start seeing warnings in the Message Bar and they might be required to respond to Message Bar warnings to enable content, such as ActiveX controls, add-ins, and VBA macros.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan Trusted Publishers settings for Office 2010

If an organization uses published content, such as Microsoft ActiveX controls, add-ins, and Visual Basic for Applications (VBA) macros, you can use the Trusted Publishers list to designate content publishers that you trust. A *publisher* is any developer, software company, or organization that has created and distributed a digitally signed ActiveX control, add-in, or VBA macro. A *trusted publisher* is any publisher that has been added to the Trusted Publishers list. When a user opens a file, and the file contains active content that is created by a trusted publisher, the trusted publisher's content is enabled and users are not notified about any potential risks that might be contained in the file.

In this article:

About planning Trusted Publishers settings

To designate a publisher as a trusted publisher, you have to add the publisher's certificate to the Trusted Publishers list. In this context, the publisher's certificate is the digital certificate (.cer file) that the publisher used to digitally sign their published content. In most cases, you can obtain the .cer file from the publisher, or you can export it from the .cab, .dll, .exe, or .ocx file that is associated with the published content. If you are unsure which published content the organization uses, you might also have to determine whether any other published content runs with the organization's Microsoft Office 2010 applications and then obtain certificates for that published content.

There are two methods you can use to add a publisher's certificate to the Trusted Publishers list: the Office Customization Tool (OCT) or Group Policy. The OCT provides no settings for managing certificates other than adding a trusted publisher's certificate to the Trusted Publishers list. If you want to manage certificate trust or if you want to establish specific trust relationships to satisfy business scenarios, you must use Group Policy. For more information about how to add trusted publishers to the Trusted Publishers list and how to manage trusted root certificates, see Manage Trusted Root Certificates (*http://go.microsoft.com/fwlink/?LinkId=164939*) and Manage Trusted Publishers (*http://go.microsoft.com/fwlink/?LinkId=164941*).

Obtain certificates from known publishers

You can usually obtain a certificate for published content by asking the publisher to send it to you. If you cannot obtain the certificate in this manner, and you know the name of the digitally signed .cab, .dll, .exe, or .ocx file that contains the published content, you can use the following procedure to export the certificate file.

Important:
This procedure assumes the computer runs the Windows Vista operating system.

To export a certificate from a .dll file

1. Right-click the file that the publisher has signed, and then click **Properties**.
2. Click the **Digital Signatures** tab.
3. In **Signature list**, click the certificate, and then click **Details**.
4. In the **Digital Signature Details** dialog box, click **View Certificate**.
5. Click the **Details** tab, and then click **Copy to File**.
6. On the Certificate Explore Wizard welcome page, click **Next**.
7. On the Export File Format page, click **DER encoded binary X.509 (.CER)**, and then click **Next**.
8. On the File to Export page, type a path and name for the .cer file, click **Next**, and then click **Finish**.

Make sure that you save all of the .cer files on a network share that can be accessed by client computers during installation.

Determine which certificates must be added to the Trusted Publishers list

In some cases, you might not know whether an organization uses published content or you might not know which published content to add to the Trusted Publishers list. This is usually relevant only if you have a highly restrictive environment and you require that all published content be signed. You can test Office 2010 applications for digitally signed content by using the following procedure.

Important:
The following procedure assumes Word 2010 is running, but you can perform the same procedure on other Office 2010 applications.

To identify published content and add the content publisher to the Trusted Publishers list

1. On a test computer or a client computer that is running the standard configuration for the organization (including any add-ins that users need), enable the Require Application Add-Ins to be signed by Trusted Publisher setting in the Trust Center by doing the following:
   - Click the **File** tab, click **Options**, click **Trust Center**, click **Trust Center Settings**, click **Add-ins**, click **Require Application Add-ins to be signed by Trusted Publisher**, and then click **OK**.
2. Exit and restart Word. If add-ins are installed, the Message Bar displays the following message: **Security Warning Some active content has been disabled. Click here for more details.**.
3. On the Message Bar, click **Some active content has been disabled. Click here for more**

details..

4. Click the **File** tab and in the Backspace View, click **Enable Content**, and then click **Advanced Options**.
5. In the **Security Alerts – Multiple Issues** dialog box, install each certificate to the Trusted Publishers list by following these steps for each add-in that shows a valid digital signature:
   a. Click **Show Signature Details**.
   b. In the **Digital Signature Details** window, click **View Certificate**.
   c. In the **Certificate** window, click **Install Certificate**.
   d. In the Certificate Import Wizard, click **Next**, click **Place all certificates in the following store**, click **Browse**, click **Trusted Publishers**, click **OK**, click **Next**, and then click **Finish**.
6. Prepare the certificate files for distribution:
   a. Click the **File** tab, click **Options**, click **Trust Center**, click **Trust Center Settings**, and then click **Trusted Publishers**.
   b. For each certificate, select the certificate, click **View**, and then follow these steps:
   a. In the **Certificate** window, on the **Details** tab, click **Copy to File**.
   b. In the Certificate Export Wizard, click **Next**, and then click **Next** again to accept the default file format, enter a file name, select a location to store the file, and then click **Finish**.

Related Trusted Publishers settings

The following settings are often used with Trusted Publishers settings:

Require that application add-ins are signed by trusted publisher

This setting restricts add-ins to only those that are signed by a trusted publisher.

Disable Trust Bar notification for unsigned application add-ins

This setting prevents users from seeing Message Bar warnings about add-ins that are not signed by a trusted publisher.

VBA macro warning settings

This setting restricts VBA macros to only those that are signed by a trusted publisher.

Disable all ActiveX

This setting restricts ActiveX controls to only those that are signed by a trusted publisher.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan security settings for add-ins for Office 2010

If you want to control the way add-ins behave, or prevent users from running add-ins, you can modify Microsoft Office 2010 add-in settings.

In this article:

About planning add-in settings

Microsoft Office 2010 provides several settings that enable you to control the behavior of add-ins. By configuring these settings, you can do the following:

- Disable add-ins on a per-application basis.
- Require that add-ins are signed by a trusted publisher.
- Disable notifications for unsigned add-ins.

Add-in settings can be configured only on a per-application basis. There are no global add-in settings.

For detailed information about the settings that are discussed in this article, see Security policies and settings in Office 2010. For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010.

By default, any add-in that is installed and registered can run without user intervention or warning. Installed and registered add-ins can include the following:

- Component Object Model (COM) add-ins
- Visual Studio Tools for Office (VSTO) add-ins
- Automation add-ins
- RealTimeData (RTD) servers
- Application add-ins (for example, .wll, .xll, and .xlam files)
- XML expansion packs
- XML style sheets

This default behavior is the same as selecting the **Trust all installed add-ins and templates** setting in Microsoft Office 2003 or an earlier Microsoft Office system.

Disable add-ins on a per-application basis

Office 2010 provides a setting that enables you to disable add-ins. Use the following guidelines to determine whether to use this setting.

Setting name: Disable all application add-ins

Description: This setting disables all add-ins. By default, all installed and registered add-ins can run.

Impact: If you enable this setting, add-ins are disabled and users are not notified that add-ins are disabled. Enabling this setting could cause significant disruptions for users who work with add-ins. If users have business-critical add-ins installed, you might be unable to enable this setting.

Guidelines: Most organizations use the default configuration for this setting and do not change this setting.

Require that application add-ins are signed by trusted publisher

Office 2010 provides a setting that enables you to require that all add-ins be signed by a trusted publisher. Use the following guidelines to determine whether to use this setting.

Setting name: Require that application add-ins are signed by trusted publisher

Description: This setting controls whether add-ins must be digitally signed by a trusted publisher. By default, the publisher of an add-in does not have to be on the Trusted Publishers list for an add-in to run.

Impact: When you enable this setting, add-ins that are signed by a publisher that is on the Trusted Publishers list will run without notification. Unsigned add-ins and add-ins that are signed by a publisher that is not on the Trusted Publishers list will be disabled. But users are prompted to enable the add-ins. Enabling this setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting.

Disable notifications for unsigned add-ins

Office 2010 provides a setting that enables you to prevent users from seeing Message Bar warnings when unsigned add-ins are not able to run. Use the following guidelines to determine whether to use this setting.

Setting name: Disable Trust Bar Notification for unsigned application add-ins

Description: This setting controls whether to notify users when unsigned application add-ins are loaded or silently disable such add-ins without notification. By default, a warning appears in the Message Bar when an unsigned add-in attempts to run.

Impact: If you enable this setting, users will not see a warning in the Message Bar when an unsigned add-in attempts to run and users will be unable to enable the unsigned add-in. Enabling this setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting if they require all add-ins be signed by a trusted publisher.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Plan security settings for ActiveX controls for Office 2010

You can change the way Microsoft ActiveX controls behave in Microsoft Office 2010 by modifying ActiveX control settings.

In this article:

About planning settings for ActiveX controls

Office 2010 provides several security settings that let you to control how ActiveX controls behave and how users are notified about potentially unsafe ActiveX controls. By configuring these settings, you can do the following:

- Disable ActiveX controls.
- Modify how ActiveX controls are initialized based on the safe mode parameters and the Safe for Initialization (SFI) and Unsafe for Initialization (UFI) parameters.

For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*).

By default, trusted ActiveX controls are loaded in safe mode with persistent values and users are not notified that the ActiveX controls loaded. A trusted ActiveX control is any ActiveX control that is signed by a trusted publisher or contained in a document that is opened from a trusted location or considered to be a trusted document. Untrusted ActiveX controls load differently depending on how the ActiveX control is marked and whether a VBA project exists in the file together with the ActiveX control. The default behavior of untrusted ActiveX controls is as follows:

- If an ActiveX control is marked Safe for Initialization (SFI) and it is contained in a document that does not contain a VBA project, the ActiveX control is loaded in safe mode with persistent values. The Message Bar does not appear and users are not notified about the presence of the ActiveX control. All ActiveX controls in the document must be marked SFI for this behavior to occur.
- If an ActiveX control is marked Unsafe for Initialization (UFI) and it is contained in a document that does not contain a VBA project, users are notified in the Message Bar that ActiveX controls are disabled. However, users can click the Message Bar to enable ActiveX controls. If a user enables ActiveX controls, all ActiveX controls (those marked UFI and SFI) are loaded in safe mode with persistent values.

- If an ActiveX control marked UFI or SFI is contained in a document that also contains a VBA project, users are notified in the Message Bar that ActiveX controls are disabled. However, users can click the Message Bar to enable ActiveX controls. If a user enables ActiveX controls, all ActiveX controls (those marked SFI and UFI) are loaded in safe mode with persistent values.

Important:
If a kill bit is set in the registry for an ActiveX control, the control is not loaded and cannot be loaded in any circumstance. In addition, the Message Bar does not appear and users are not notified about the presence of the ActiveX control.

Disable ActiveX controls

Office 2010 provides a setting that enables you to disable ActiveX controls. Disabling ActiveX controls prevents all ActiveX controls in a file from initializing (that is, loading) when a file is opened. It also prevents users from adding ActiveX controls to a document. In some cases, a disabled ActiveX control might appear in a file as a red x or some other symbol. However, the control is disabled and no action occurs if a user clicks the symbol. Also, when you disable ActiveX controls, users are not notified that ActiveX controls are disabled.

Use the following guidelines to determine whether to disable ActiveX controls.

Setting name: Disable all ActiveX

Description: This setting controls whether ActiveX controls are disabled in Office 2010. This is a global setting and cannot be configured on a per-application basis.

Impact: If you enable this setting, ActiveX controls do not initialize and users are not notified that the ActiveX controls are disabled. Also, users cannot insert ActiveX controls into documents. ActiveX controls can provide additional functionality in documents. Therefore, disabling them can reduce functionality for users. You should ensure that users are aware that this setting is enabled, because they are not notified by the application that ActiveX controls have been disabled. It is also important to determine whether ActiveX controls are used to provide business-critical functionality before you enable this setting.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting.

Note:
If you enable this setting, ActiveX controls are disabled in files that are saved in trusted locations.

You can also use the Office COM kill bit, which was introduced in Office 2010, to prevent specific COM objects, including ActiveX controls, from running within Office 2010 applications. This capability was available in the 2007 Office system. However, it was dependent on the Internet Explorer ActiveX kill bit setting. Now, with Office 2010, you can independently control through the registry which COM objects will not be able to run by using Office 2010. If, for example, the kill bit is set for the same ActiveX control in both locations, Office and Internet Explorer, and there is a conflict between the two settings, the

Office COM kill bit has precedence. A common scenario where you would see the Office COM kill bit set is when you apply an update that is included in a Microsoft Security Bulletin to address a specific Office 2010 security issue.

Warning:
We do not recommend *unkilling* (undoing the kill action on) a COM object. If you do this, you might create security vulnerabilities. The kill bit is typically set for a reason that might be critical, and because of this, extreme care must be used when you unkill an ActiveX control.

It is possible to add an AlternateCLSID (also known as a “Phoenix bit”) when you need to correlate the CLSID of a new ActiveX control, which was modified to mitigate the security threat, to the CLSID of the ActiveX control to which the Office COM kill bit was applied. Office 2010 supports using the AlternateCLSID only with ActiveX control COM objects. For more information about kill bit behavior, including AlternateCLSID, see How to stop an ActiveX control from running in Internet Explorer (*http://go.microsoft.com/fwlink/?LinkId=183124*).

Because the following procedure is highly technical, do not continue unless you are very comfortable with the procedure.

Important:
This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs.

The location for setting the Office COM kill bit in the registry is **HKLM/Software/Microsoft/Office/Common/COM Compatibility/{CLSID}**, where CLSID is the class identifier of the COM object. To enable the Office COM kill bit, you need to add the registry key, including the CLSID of the ActiveX control, and add the value of 0x00000400 to the Compatibility Flags REG_DWORD.

Note:
The behavior of the kill bit (both Internet Explorer and Office COM) can be affected by enabling COM categorization in Office 2010. For more information, see Plan COM object categorization for Office 2010.

Controls you may want to consider putting onto the Office deny list:

Microsoft HTA Document 6.0 - 3050F5C8-98B5-11CF-BB82-00AA00BDCE0B

htmlfile - 25336920-03F9-11CF-8FD0-00AA00686F13

htmlfile_FullWindowEmbed - 25336921-03F9-11CF-8FD0-00AA00686F13

mhtmlfile - 3050F3D9-98B5-11CF-BB82-00AA00BDCE0B

Web Browswer Control - 8856F961-340A-11D0-A96B-00C04FD705A2

DHTMLEdit - 2D360200-FFF5-11d1-8d03-00a0c959bc0a

Change the way ActiveX controls are initialized

Office 2010 provides a setting that enables you to control the way ActiveX controls are initialized based on SFI, UFI, and safe mode parameters. SFI, UFI, and safe mode are parameters that developers can configure when they create ActiveX controls. ActiveX controls that are marked SFI use safe data sources to initialize. A safe data source is one that is trusted, known, and does not cause a security breach. Controls that are not marked SFI are considered UFI.

Safe mode is another security mechanism that developers can use to help ensure the safety of ActiveX controls. When a developer creates an ActiveX control that implements safe mode, the control can be initialized in two ways: in safe mode and in unsafe mode. When an ActiveX control is initialized in safe mode, certain restrictions that limit functionality are imposed on the control. Conversely, when an ActiveX control is initialized in unsafe mode, there are no restrictions on its functionality. For example, an ActiveX control that reads and writes files might only be able to read files if it is initialized in safe mode, and it might be able to read and write files when it is initialized in unsafe mode. Only ActiveX controls that are SFI can be initialized in safe mode. ActiveX controls that are UFI are always initialized in unsafe mode.

If the default initialization for ActiveX controls is insufficient for your organization but you do not want to disable ActiveX controls, use the following guidelines to determine how you can change the way ActiveX controls are initialized.

Setting name: ActiveX control initialization

Description: This setting specifies how ActiveX controls are initialized for all Office 2010 applications. This is a global setting and cannot be configured on a per-application basis. You can select one of six possible initialization security levels for this setting:

- **Security level 1** Regardless of how the control is marked, load it and use persistent values (if any). This setting prevents users from being prompted.
- **Security level 2** If the control is marked SFI, load the control in safe mode and use persistent values (if any). If the control is not marked SFI, load in unsafe mode with persistent values (if any), or use the default (first-time initialization) settings. This level resembles the default configuration, but unlike the default configuration this setting prevents users from being notified.
- **Security level 3** If the control is marked SFI, load the control in unsafe mode and use persistent values (if any). If the control is not marked SFI, prompt the user and advise them that it is marked unsafe. If the user decides No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings.
- **Security level 4** If the control is marked SFI, load the control in safe mode and use persistent values (if any). If the control is not marked SFI, prompt the user and advise them that it is marked unsafe. If the user decides No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings.
- **Security level 5** If the control is marked SFI, load the control in unsafe mode and use persistent values (if any). If the control is not marked SFI, prompt the user and advise them that

it is marked unsafe. If the user decides No at the prompt, do not load the control. Otherwise, load it with persistent values.

- **Security level 6** If the control is marked SFI, load the control in safe mode and use persistent values (if any). If the control is not marked SFI, prompt the user and advise them that it is marked unsafe. If the user decides No at the prompt, do not load the control. Otherwise, load it with persistent values.

Impact: If a control is not marked SFI, the control could adversely affect a computer — or it could mean that the developers did not test the control in all situations and cannot know for sure whether it might be compromised in the future. In addition, some ActiveX controls do not respect the safe mode registry setting, and therefore might load persistent data even though you configure this setting so that ActiveX controls initialize in safe mode. Enabling this setting and selecting security level 2, 4, or 6 only increases security for ActiveX controls that are accurately marked as SFI. In situations that involve malicious or poorly designed code, an ActiveX control might be inaccurately marked as SFI.

Guidelines: Most organizations enable this setting and select security level 2, which uses the same initialization criteria as the default configuration but does not notify users in the Message Bar. Organizations that have a highly restrictive security environment typically disable this setting, which is the default configuration.

Related ActiveX control settings

Several other settings affect how ActiveX controls behave in Office 2010 applications. If you are modifying ActiveX control settings because you have a special security environment, you might want to evaluate the following settings:

Load controls in Forms3 This setting determines how ActiveX controls are initialized in UserForms.

Disable all Trust Bar notifications for security issues This setting prevents users from seeing Message Bar warnings, including warnings about unsafe ActiveX controls.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan security settings for VBA macros for Office 2010

If you want to control the way Visual Basic for Applications (VBA) and VBA macros behave, you can modify Microsoft Office 2010 VBA and VBA macros settings for the following applications: Microsoft Access 2010, Microsoft Excel 2010, Microsoft PowerPoint 2010, Microsoft Publisher 2010, Microsoft Visio 2010, and Microsoft Word 2010.

In this article:

About planning VBA and VBA macro settings

Office 2010 provides several settings that enable you to control the behavior of VBA and VBA macros. By configuring these settings, you can do the following:

- Change the security warning settings for VBA macros. This includes disabling VBA macros, enabling all VBA macros, and changing the way that users are notified about VBA macros.
- Disable VBA.
- Change how VBA macros behave in applications that are started programmatically through Automation.
- Change how antivirus software scans encrypted VBA macros.

For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*).

By default, VBA is enabled and trusted VBA macros are allowed to run. This includes VBA macros in documents that are saved in a trusted location, VBA macros in trusted documents, and VBA macros that meet the following criteria:

- The macro is signed by the developer with a digital signature.
- The digital signature is valid.
- This digital signature is current (not expired).
- The certificate associated with the digital signature was issued by a reputable certification authority (CA).

- The developer who signed the macro is a trusted publisher.

Note:
The default security setting for macros is different in Microsoft Outlook 2010. For more information, see the Outlook 2010 security documentation.

VBA macros that are not trusted are not allowed to run until a user clicks the Message Bar and selects to enable the VBA macro.

Change the security warning settings for VBA macros

Office 2010 provides a setting that enables you to change the security warning settings and the behavior of VBA macros. Use the following guidelines to determine how to configure this setting if you want to change how users are notified about untrusted VBA macros or change the default behavior of VBA macros.

Setting name: VBA Macro Notification Settings

Description: This setting controls how applications warn users about Visual Basic for Applications (VBA) macros. You configure this setting on a per-application basis for Access 2010, Excel 2010, PowerPoint 2010, Publisher 2010, Visio 2010, and Word 2010. You can select one of four possible options for this setting:

Disable all with notification The application displays the Trust Bar for all macros, whether signed or unsigned. This is the default setting.

Disable all except digitally signed macros The application displays the Trust Bar for digitally signed macros. This allows users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified or given the ability to enable the unsigned macros.

Disable all without notification The application disables all macros, whether signed or unsigned, and does not notify users.

Enable all macros (not recommended) All macros are enabled, whether signed or unsigned. This option can significantly reduce security by letting dangerous code to run undetected.

Impact: If you enable this setting and select the **Disable all except digitally signed macros** option, documents and templates that contain unsigned macros lose all functionality supplied by those macros. To prevent this loss of functionality, users can put files that contain macros in a trusted location.

Important:
If **Disable all except digitally signed macros** is selected, users cannot open unsigned Access 2010 databases.

If you select **Disable all without notification**, documents and templates that contain unsigned and signed macros lose all functionality supplied by those macros. This is true even if a macro is signed and the publisher is listed in the Trusted Publisher list.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting and select the **Disable all except digitally signed macros** option. Organizations that do not let users run macros typically enable this setting and select **Disable all without notification**.

Disable VBA

Office 2010 provides a setting that enables you to disable VBA. By default, VBA is enabled. Use the following guidelines to determine how to configure this setting if you want to disable VBA.

Setting name: Disable VBA for Office applications

Description: This setting disables VBA in Excel 2010, Microsoft Outlook 2010, PowerPoint 2010, Publisher 2010, Microsoft SharePoint Designer 2010, and Word 2010, and prevents any VBA code from running in these applications. You cannot configure this setting on a per-application basis. It is a global setting. Enabling this setting does not install or remove any VBA-related code from a user's computer.

Impact: If you enable this setting, VBA code does not run. If your organization has business-critical requirements for using documents that have VBA code, do not enable this setting.

Guidelines: Organizations that have a highly restrictive security environment typically enable this setting.

Change how VBA macros behave in applications that are started programmatically

Office 2010 provides a setting that enables you to change the way VBA macros behave in applications that have been started programmatically through Automation. By default, when a separate program is used to programmatically start Excel 2010, PowerPoint 2010, or Word 2010, any macros can run in the application that was programmatically started. Use these guidelines to determine how to configure this setting if you want to do the following:

- Prevent macros from running in applications that are programmatically started through Automation.
- Allow VBA macros to run according to the VBA macro security settings that are configured for the applications that are programmatically started through Automation.

Setting name: Automation security

Description: This setting controls whether macros can run in an application that is opened programmatically by another application. This setting is a global setting and applies to Excel 2010, PowerPoint 2010, and Word 2010. You cannot configure this setting on a per-application basis. You can choose one of three possible options for this setting:

Disable macros by default All macros are disabled in the programmatically opened application.

Macros enabled (default) Macros are allowed to run in the programmatically opened application. This option enforces the default configuration.

Use application macro security level Macro functionality is determined according to how you configure the **VBA macro warning settings** setting for each application.

Impact: If you enable this setting and select the **Disable macros by default** option, macros will not run in applications that are programmatically started. This can be a problem if an application is started programmatically and then opens a document or a template that contains macros. In this case, the functionality that is provided by the macros is not available. The same situation might occur if you select the **Use application macro security level** option and you disable macros using the **VBA macro warning settings** setting.

Guidelines: Most organizations enable this setting and select the **Use application macro security level** option. However, organizations that have a highly restrictive security environment typically enable this setting and select the **Disable macros by default** option.

Change how encrypted VBA macros are scanned for viruses

Office 2010 provides a setting that enables you to modify the way encrypted VBA macros are scanned by antivirus software in Excel 2010, PowerPoint 2010, and Word 2010. By default, if a document, presentation, or workbook is encrypted and contains VBA macros, the VBA macros are disabled unless an antivirus program is installed on the client computer. In addition, encrypted VBA macros are scanned by the client computer's antivirus program when a user opens a document that contains encrypted macros. Use these guidelines to determine how to configure this setting if you want to do the following:

- Allow all encrypted VBA macros to run without being scanned by an antivirus program.
- Scan encrypted VBA macros if an antivirus program is installed, but enable encrypted VBA macros if no antivirus program is installed.

Setting name: Scan encrypted macros in Excel Open XML documents, Scan encrypted macros in PowerPoint Open XML documents, Scan encrypted macros in Word Open XML documents

Description: This setting controls the way encrypted VBA macros undergo virus scanning. This setting is a per-application setting and can be configured for Excel 2010, PowerPoint 2010, and Word 2010. You can choose one of three possible options for this setting:

Scan encrypted macros (default). All encrypted VBA macros are disabled unless they are scanned by an antivirus program. This option enforces the default configuration.

Scan if antivirus software available. Encrypted VBA macros are disabled unless they are scanned by an antivirus program. However, if no antivirus program is installed on the client computer, all encrypted VBA macros are enabled.

Load macros without scanning. Encrypted VBA macros are enabled and are not scanned, regardless of whether an antivirus program is installed on the client computer.

Impact: If you enable this setting and select the **Load macros without scanning** option, security could be significantly reduced by encrypted macros that have not been scanned for viruses. The same is

true if the client computer does not have an antivirus program installed and you enable this setting and select the **Scan if antivirus software available** option.

Guidelines: Most organizations use the default configuration for this setting and do not change this setting.

Related VBA macro settings

Several other settings affect how VBA macros behave in Office 2010 applications. If you are modifying VBA macro settings because you have a special security environment, you might want to evaluate the following settings:

Trust access to VBA project

This setting determines whether automation clients can access the VBA project.

Disable all Trust Bar notifications for security issues

This setting prevents users from seeing Message Bar warnings, including warnings about unsafe VBA macros.

Note:
For the latest information about policy settings, refer to theMicrosoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Plan COM object categorization for Office 2010

You can control the behavior of certain COM objects in Microsoft Office 2010 by using COM object categorization. COM objects can include ActiveX, Object Linking and Embedding (OLE), Excel RealTimeData (RTD) servers, and Office Web Components (OWC) data source providers. For example, you can create a security allow list, which will only allow the specified COM objects to load or you could choose to override the Internet Explorer kill bit.

In this article:

About COM object categorization

Office 2010 will first check whether any of the Group Policy settings for COM object categorization is configured. If any of the settings are enabled to use COM object categorization, Office 2010 will verify the specified COM objects are categorized correctly within the registry.

To enable COM object categorization within your organization, you first need to determine how to best configure the Group Policy security settings for the needs of your organization. Then, you need to add the category id for the targeted COM objects within the registry.

Configure Group Policy security settings for COM object categorization

There are four COM object categorization Group Policy settings:

- **Check OWC data source providers**
- **Check Excel RTD servers**
- **Check OLE objects**
- **Check ActiveX objects**

Check OWC data source providers and **Check Excel RTD servers** can be configured to be either enabled or disabled. Enabling these settings will force Office 2010 to only load the COM objects that are categorized correctly.

Check OLE objects and **Check ActiveX objects** have additional options when you select **Enabled**. These options are listed in the following table.

Option	Description
Do not check	Office loads (OLE/ActiveX) objects without checking if they are categorized correctly before loading.
Override IE kill bit list (default behavior)	Office uses the category list to override Internet Explorer kill bit checks.
Strict allow list	Office loads only Active X objects that are categorized correctly.

The **Override IE kill bit list** option lets you specifically list which OLE or ActiveX controls will be allowed to load within Office 2010 as long as they are categorized correctly, even if they are on the Internet Explorer kill bit list. Use this control when you want to allow a COM object that is designated as unsafe to load in Internet Explorer. However, you know that the COM object is safe to load in Microsoft Office. Office also checks whether the Office COM kill bit is enabled. For more information about the Office COM kill bit, see Plan security settings for ActiveX controls for Office 2010. If the Office COM kill bit is enabled and there is no alternate CLSID, also known as a “Phoenix bit,” the COM object will not load. For more information about kill bit behavior, see How to stop an ActiveX control from running in Internet Explorer (*http://go.microsoft.com/fwlink/?LinkId=183124*).

Use the **Strict allow list** option when you want to create a security allow list to only allow the specified controls to load and to disallow all other OLE or ActiveX objects, not on the list, from loading.

If you enable any of the COM object categorization settings within Group Policy, the next step is to add the COM object categorization in the registry.

Add COM object categorization in registry

Each Group Policy setting has a corresponding COM object categorization setting within the registry. These settings are listed in the following table.

Group Policy setting	Category ID (CATID)
Check OWC data source providers	{A67A20DD-16B0-4831-9A66-045408E51786}
Check Excel RTD servers	{8F3844F5-0AF6-45C6-99C9-04BF54F620DA}
Check OLE objects	{F3E0281E-C257-444E-87E7-F3DC29B62BBD}
Check ActiveX objects	{4FED769C-D8DB-44EA-99EA-65135757C156}

Except when the Group Policy setting is either configured to **disabled** or **enabled | Do not check**, you need to add a correct CATID for the designated COM objects. In the registry, you add a key (if it does not already exist) named Implemented Categories to the CLSID of the COM object. Then, you add a subkey that contains the CATID to the Implemented Categories key.

For example, if you create an allow list and allow only the OLE object, Microsoft Graph Chart, to be used in Office, you would first look up the CLSID for that COM object in the following location in the registry:

HKEY_CLASSES_ROOT\CLSID

The CLSID for the Microsoft Graph Chart is {00020803-0000-0000-C000-000000000046}. The next step is to either verify that either the key, Implemented Categories, already exists or create one if it does not. The path in this example will be:

HKEY_CLASSES_ROOT\CLSID\{00020803-0000-0000-C000-000000000046}\Implemented Categories

Finally, you would add a new subkey for the CATID that corresponds to the Check OLE object Group Policy setting to the Implemented Categories key. The final path and values for this example will be:

HKEY_CLASSES_ROOT\CLSID\{00020803-0000-0000-C000-000000000046}\Implemented Categories\{F3E0281E-C257-444E-87E7-F3DC29B62BBD}

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

Plan Protected View settings for Office 2010

If you want to change how the sandbox preview feature in Microsoft Office 2010 behaves, you can configure Protected View settings. Protected View is a new security feature in Office 2010 that helps mitigate exploits to your computer by opening files in a restricted environment so they can be examined before they are opened for editing in Microsoft Excel 2010, Microsoft PowerPoint 2010, or Microsoft Word 2010.

In this article:

About planning Protected View settings

Protected View helps mitigate several kinds of exploits by opening documents, presentations, and workbooks in a sandbox environment. A *sandbox* is a piece of computer memory or a specific computer process that is isolated from certain operating system components and applications. Because of this isolation, programs and processes that run in a sandbox environment are considered less dangerous. Sandbox environments are frequently used to test new applications and services that might make a computer unstable or fail. Sandbox environments are also used to prevent applications and processes from harming a computer.

When a file is opened in Protected View, users can view the file content but they cannot edit, save, or print the file content. Active file content, such as ActiveX controls, add-ins, database connections, hyperlinks, and Visual Basic for Applications (VBA) macros, is not enabled. Users can copy content from the file and paste it into another document. In addition, Protected View prevents users from viewing the details of digital signatures that are used to sign a document, presentation, or workbook.

Default behavior of Protected View

By default, Protected View is enabled in Excel 2010, PowerPoint 2010, and Word 2010. However, files open in Protected View only under certain conditions. In some cases, files bypass Protected View and are opened for editing. For example, files that are opened from trusted locations and files that are trusted documents bypass several security checks and are not opened in Protected View.

By default, files open in Protected View if any one of the following conditions is true:

- **A file skips or fails Office File Validation** Office File Validation is a new security feature that scans files for file format exploits. If Office File Validation detects a possible exploit or some other unsafe file corruption, the file opens in Protected View.

- **AES zone information determines that a file is not safe** Attachment Execution Services (AES) adds zone information to files that are downloaded by Microsoft Outlook or Microsoft Internet Explorer. If a file's zone information indicates that the file originated from an untrusted Web site or the Internet, the downloaded file opens in Protected View.
- **A user opens a file in Protected View** Users can open files in Protected View by selecting **Open in Protected View** in the **Open** dialog box, or by holding down the SHIFT key, right-clicking a file, and then selecting **Open in Protected View**.
- **A file is opened from an unsafe location** By default, unsafe locations include the user's Temporary Internet Files folder and the downloaded program files folder. However, you can use Group Policy settings to designate other unsafe locations.

In some cases, Protected View is bypassed even if one or more of the previously listed conditions are met. Specifically, files do not open in Protected View if any one of the following is true:

- A file is opened from a trusted location.
- A file is considered a trusted document.

Change Protected View behavior

We recommend that you do not change the default behavior of Protected View. Protected View is an important part of the layered defense strategy in Office 2010, and is designed to work with other security features such as Office File Validation and File Block. However, we recognize that some organizations might have to change Protected View settings to suit special security requirements. To that end, Office 2010 provides several settings that let you change how the Protected View feature behaves. You can use these settings to do the following:

- Prevent files that are downloaded from the Internet from opening in Protected View.
- Prevent files that are stored in unsafe locations from opening in Protected View.
- Prevent attachments opened in Microsoft Outlook 2010 from opening in Protected View.
- Add locations to the list of unsafe locations.

In addition, you can use File Block settings and Office File Validation settings to force files to open in Protected View. For more information, see Force files to open in Protected View later in this article.

Note:
For detailed information about the settings that are discussed in this article, see Security policies and settings in Office 2010. For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010.

Prevent files from opening in Protected View

You can change Protected View settings so that certain files bypass Protected View. To do so, enable the following settings:

Do not open files from the Internet zone in Protected View This setting forces files to bypass Protected View if the AES zone information indicates that the file was downloaded from the Internet zone. This setting applies to files that are downloaded by using Internet Explorer, Outlook Express, and Outlook.

Do not open files in unsafe locations in Protected View This setting forces files to bypass Protected View if the files are opened from an unsafe location. You can add folders to the unsafe locations list by using the **Specify list of unsafe locations** setting, which is discussed later in this article.

Turn off Protected View for attachments opened in Outlook This setting forces Excel 2010. PowerPoint 2010, and Word 2010 files that are opened as Outlook 2010 attachments to bypass Protected View.

These settings do not apply if File Block settings force the file to open in Protected View. Also, these settings do not apply if a file fails Office File Validation. You can configure each of these settings on a per-application basis for Excel 2010, PowerPoint 2010, and Word 2010.

Force files to open in Protected View

The File Block and Office File Validation features have settings that let you force files to open in Protected View when certain conditions are met. You can use these settings to determine the circumstances under which files open in Protected View.

Use File Block to force files to open in Protected View

The File Block feature lets you prevent users from opening or saving certain file types. When you use File Block settings to block a file type, you can choose one of three file block actions:

- Blocked and not allowed to open.
- Blocked and opened only in Protected View (users cannot enable editing).
- Blocked and opened in Protected View (users can enable editing).

By selecting the second or third option, you can force blocked file types to open in Protected View. You can configure File Block settings only on a per-application basis for Excel 2010, PowerPoint 2010, and Word 2010. For more information about File Block settings, see Plan File Block settings for Office 2010.

Use Office File Validation settings to force files to open in Protected View

Office File Validation is a new security feature that scans files for file format exploits before they are opened by an Office 2010 application. By default, files that fail Office File Validation are opened in Protected View and users can enable editing after previewing the file in Protected View. However, you can use the **Set document behavior if file validation fails** setting to change this default behavior. You can use this setting to select one of three possible options for files that fail Office File Validation:

- **Block completely** Files that fail Office File Validation cannot be opened in Protected View or opened for editing.
- **Open in Protected View and disallow editing** Files that fail Office File Validation are opened in Protected View but users cannot edit the files.
- **Open in Protected View and allow editing** Files that fail Office File Validation are opened in Protected View and users are allowed to edit the files. This is the default.

By selecting the second option, you can restrict Protected View behavior for files that fail Office File Validation. You can configure this Office File Validation setting only on a per-application basis for Excel 2010, PowerPoint 2010, and Word 2010. For more information about Office File Validation settings, see Plan Office File Validation settings for Office 2010.

Add files to the list of unsafe files

You can use the **Specify list of unsafe locations** setting to add locations to the unsafe locations list. Files that are opened from unsafe locations are always opened in Protected View. The unsafe locations feature does not prevent users from editing a document; it only forces a document to open in Protected View before it is edited. This is a global setting that applies to Excel 2010, PowerPoint 2010, and Word 2010.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Understand security threats and countermeasures for Office 2010

Plan Office File Validation settings for Office 2010

Plan Office File Validation settings for Office 2010

If you want to change how Microsoft Office 2010 validates files that are stored in Microsoft Office binary file formats, you can configure Office File Validation settings. Office File Validation is a new security feature in Office 2010 that helps prevent file format attacks by scanning Office binary file formats before they are opened in Microsoft Excel 2010, Microsoft PowerPoint 2010, or Microsoft Word 2010.

In this article:

About planning Office File Validation settings

Office File Validation helps detect and prevent a kind of exploit known as a file format attack or file fuzzing attack. File format attacks exploit the integrity of a file, and they occur when someone modifies the structure of a file with the intent of adding malicious code. Usually the malicious code is run remotely and is used to elevate the privilege of restricted accounts on the computer. As a result, an attacker could gain access to a computer that they did not previously have access to. This could enable an attacker to read sensitive information from the computer's hard disk drive or install malware, such as a worm or a key logging program. The Office File Validation feature helps prevent file format attacks by scanning and validating files before they are opened. To validate files, Office File Validation compares a file's structure to a predefined file schema, which is a set of rules that determine what a readable file looks like. If Office File Validation detects that a file's structure does not follow all rules described in the schema, the file does not pass validation.

File format attacks occur most frequently in files that are stored in Office binary file formats. For this reason, Office File Validation scans and validates the following kinds of files:

- Excel 97-2003 Workbook files. These files have an .xls extension and include all Binary Interchange File Format 8 (BIFF8) files.
- Excel 97-2003 Template files. These files have an .xlt extension and include all BIFF8 files.
- Microsoft Excel 5.0/95 files. These files have an .xls extension and include all BIFF5 files.
- PowerPoint 97-2003 Presentation files. These files have a .ppt extension.
- PowerPoint 97-2003 Show files. These files have a .pps extension.
- PowerPoint 97-2003 Template files. These files have a .pot extension.
- Word 97-2003 Document files. These files have a .doc extension.

- Word 97-2003 Template files. These files have a .dot extension.

Office 2010 provides several settings that let you change how the Office File Validation feature behaves. You can use these settings to do the following:

- Disable Office File Validation.
- Specify document behavior when a file fails validation.
- Prevent Office 2010 from sending Office File Validation information to Microsoft.

Note:
For detailed information about the settings that are discussed in this article, see Security policies and settings in Office 2010. For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010.

By default, Office File Validation is enabled in Excel 2010, PowerPoint 2010, and Word 2010. Any files that fail validation are opened in Protected View and users can choose to enable editing for files that fail validation but are opened in Protected View. Also, users are prompted to send Office File Validation information to Microsoft. Information is collected only for files that fail validation.

We recommend that you do not change the default settings for Office File Validation. However, some organizations might have to configure Office File Validation settings to suit special security requirements. Specifically, organizations that have the following security requirements might have to change the default settings for the Office File Validation feature:

- Organizations that restrict access to the Internet. Office File Validation prompts users to send validation error information to Microsoft approximately every two weeks. This could violate an organization's Internet access policies. In this case, you might need to prevent Office File Validation from sending the information to Microsoft. For more information, see Turn off Office File Validation reporting later in this article.
- Organizations that have highly restrictive security environments. You can configure Office File Validation so that files that fail validation cannot be opened or can only be opened in Protected View. This is a more restrictive than the default settings for Office File Validation and might be suitable to organizations that have a locked-down security environment. For more information about how to change document behavior, see Change document behavior when validation fails later in this article.
- Organizations that do not want their files sent to Microsoft. If users allow it, Office File Validation sends a copy of all files that fail validation to Microsoft. You can configure Office File Validation so that users are not prompted to send validation information to Microsoft.

Turn off Office File Validation

You can use the **Turn off file validation** setting to disable Office File Validation. This setting must be configured on a per-application basis for Excel 2010, PowerPoint 2010, and Word 2010. This setting prevents files that are stored in the Office binary file format from being scanned and validated. For

example, if you enable the **Turn off file validation** setting for Excel 2010, Office File Validation does not scan or validate Excel 97-2003 Workbook files, Excel 97-2003 Template files, or Microsoft Excel 5.0/95 files. If a user opens one of those file types, and the file contains a file format attack, the attack will not be detected or prevented unless some other security control detects and prevents such an attack.

We recommend that you do not turn off Office File Validation. Office File Validation is a key part of the layered defense strategy in Office 2010 and should be enabled on all computers throughout an organization. If you want to prevent files from being validated by the Office File Validation feature, we recommend that you use the Trusted Locations feature. Files that are opened from trusted locations skip Office File Validation checks. You can also use the Trusted Documents feature to prevent a file from being validated by Office File Validation. Files that are considered to be trusted documents do not undergo Office File Validation checks.

Change document behavior when validation fails

You can use the **Set document behavior if file validation fails** setting to change how documents behave when they fail validation. When you enable this setting, you can select one of the following three options:

- **Block files completely** Files that fail validation do not open in Protected View and users cannot open files for editing.
- **Open files in Protected View and disallow edit** Files open in Protected View so users can see the content of the file, but users cannot open files for editing.
- **Open files in Protected View and allow edit** Files open in Protected View and users can choose to open files for editing. This option represents the default behavior of the Office File Validation feature.

If you select the **Open files in Protected View and disallow edit** option, users see the following text in the Message Bar when a file fails validation:

Protected View Office has detected a problem with this file. Editing it may harm your computer. Click for more details.

If a user clicks the Message Bar, the Microsoft Office Backstage view appears, which provides a more lengthy description of the problem and lets users enable the file for editing.

If you select the **Block files completely** option, users see the following text in a dialog box when a file fails validation:

Office has detected a problem with this file. To help protect your computer this file cannot be opened.

Users can expand the dialog box and see a more detailed explanation of why the file does not open, or they can close the dialog box by clicking **OK**.

Turn off Office File Validation reporting

You can use the **Turn off error reporting for files that fail file validation** setting to suppress the dialog box that prompts users to send information to Microsoft. This setting also prevents validation information from being sent to Microsoft.

Every time that a file fails validation, Office 2010 collects information about why the file failed validation. Approximately two weeks after a file fails validation, Office 2010 prompts users to send Office File Validation information to Microsoft. The validation information includes such things as the file types, file sizes, how long it took to open the files, and how long it took to validate the files. Copies of the files that failed validation are also sent to Microsoft. Users see the list of files when they are prompted to send validation information to Microsoft. Users can decline to send validation information to Microsoft, which means no information about failed validations is sent to Microsoft and no files are sent to Microsoft. If an organization restricts Internet access, has restrictive Internet access policies, or does not want files sent to Microsoft, you might have to enable the **Turn off error reporting for files that fail file validation** setting.

Important:
The Office File Validation feature can occasionally indicate that a file failed validation when in fact the file is valid. The validation reporting feature helps Microsoft improve the Office File Validation feature and minimize the occurrence of false positive results.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan password complexity settings for Office 2010

Microsoft Office 2010 provides settings to allow you to enforce strong passwords, such as password length and complexity rules, when you use the **Encrypt with Password** feature in Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010. By using these settings, you can have Office 2010 applications enforce local password requirements or the domain-based requirements that are specified in the Password Policy settings in Group Policy.

In this article:

About planning password length and complexity settings

By default, there are no restrictions on password length or password complexity for the **Encrypt with Password** feature, which means that users can encrypt a document, presentation, or workbook without specifying a password. However, we recommend that organizations change this default setting and enforce password length and complexity to help ensure that strong passwords are used with the **Encrypt with Password** feature.

Many organizations enforce strong passwords for log on and authentication by using domain-based group policies. If this is the case, we recommend that the organization use the same password length and complexity requirements for the **Encrypt with Password** feature. For more information about strong passwords, including recommendations for determining password length and complexity, see Creating a Strong Password Policy (*http://go.microsoft.com/fwlink/?LinkId=166269*).

Caution:
When you establish password policies, you need to balance the need for strong security with the need to make the password policy easy for users to implement. If a password is forgotten or an employee leaves an organization without providing the passwords used to save and encrypt the data, the data is inaccessible until the correct password is available to decrypt the data.

Enforce password length and complexity

When you configure the password settings that Office 2010 provides to enforce password length and complexity, you have the option to use the settings that are included with Office 2010 or in combination with the password settings that are available in the domain-based Group Policy object. If you already

enforce strong passwords for domain log on and authentication, we recommend that you configure the password length and complexity settings for Office 2010 the same as they are configured for the Password Policy Group Policy object for the domain.

The password settings included with Office 2010 are listed as follows:

- **Set minimum password length**
- **Set password rules level**
- **Set password rules domain time-out**

You can configure the Office 2010 password settings by using the Office Customization Tool (OCT) or the Office 2010 Administrative Templates for local or domain-based group policies. For information about how to configure security settings in the OCT and the Office 2010 Administrative Templates, see Configure security for Office 2010.

The password settings available for the Password Policy Group Policy object on the domain are listed as follows:

- **Enforce password history**
- **Maximum password age**
- **Minimum password age**
- **Minimum password length**
- **Password must meet complexity requirements**
- **Store passwords using reversible encryption**

You can use the Group Policy Object Editor to configure the domain-based Password Policy settings (**GPO** | **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Account Policies** | **Password Policy**). For more information, see Group Policy Object Editor Technical Reference (*http://go.microsoft.com/fwlink/?LinkId=188682*).

The **Set password rules level** setting in Office 2010 determines the password complexity requirements and whether the Password Policy Group Policy object for the domain will be used.

To enforce password length and complexity for the **Encrypt with Password** feature, you must do the following:

- Determine the minimum password length that you want to enforce locally.
- Determine the password rules level.
- Determine the password time-out value for domain-based password enforcement. (This is an optional task. You might need to configure this value if there is a custom password filter installed on your domain controller and the default time to wait when contacting a domain controller of 4 seconds is insufficient.)

Determine minimum password length requirement

To enforce password length and complexity, you must first determine the minimum password length that you want to enforce locally. The **Set minimum password length** setting lets you do this. When you enable this setting, you can specify a password length between 0 and 255. However, specifying a minimum password length does not enforce password length. To enforce password length or complexity, you must change the **Set password rules level** setting, which is discussed in the following section.

Caution:
When you establish password policies, you need to balance the need for strong security with the need to make the password policy easy for users to implement. If a password is forgotten or an employee leaves an organization without providing the passwords used to save and encrypt the data, the data is inaccessible until the correct password is available to decrypt the data.

Determine the password rules level

After you set a minimum password length for local enforcement, you must determine the rules by which password length and complexity are enforced. The **Set password rules level** setting lets you do this. When you enable this setting, you can select one of four levels, which are as follows:

- **No password checks** Password length and complexity is not enforced. This is the same as the default configuration.
- **Local length check** Password length is enforced but not password complexity. In addition, password length is enforced only on a local basis according to the password length requirement specified in the **Set minimum password length** setting.
- **Local length and complexity checks** Password length is enforced on a local basis according to the password length requirement specified in the **Set minimum password length** setting. Password complexity is also enforced on a local basis, which means that passwords must contain characters from at least three of the following character sets:
  - Lowercase a–z
  - Uppercase A–Z
  - Digits 0–9
  - Non-alphabetical characters

  This setting works only if you specify a password length of at least six characters in the **Set minimum password length** setting.
- **Local length, local complexity, and domain policy checks** Password length and complexity is enforced according to the domain-based Password Policy settings that are set in Group Policy. If a computer is offline or cannot contact a domain controller, the local password length and complexity requirements are enforced exactly as they are described for the **Local length and complexity checks** setting.

If you want to enforce password length and password complexity by using domain-based settings, you must configure Password Policy settings in Group Policy. Domain-based enforcement has several advantages over local enforcement. Some of the advantages include the following:

- Password length and complexity requirements are the same for log on and authentication as they are for the **Encrypt with Password** feature.
- Password length and complexity requirements are enforced the same way throughout the organization.
- Password length and complexity requirements can be enforced differently according to organizational units, sites, and domains.

To learn more about enforcing password length and complexity by using domain-based Group Policy, see Enforcing strong password usage throughout your organization (*http://go.microsoft.com/fwlink/?LinkId=166262*).

Determine domain time-out value

If you use domain-based Group Policy settings to enforce password length and complexity for the **Encrypt with Password** feature and there is a custom password filter installed on your domain controller, you might need to configure the **Set password rules domain time-out** setting. The domain time-out value determines how long an Office 2010 application waits for a response from a domain controller before it uses the local password length and complexity settings for enforcement. You can use the **Set password rules domain time-out** setting to change the domain time-out value. By default, the time-out value is 4000 millisecond (4 seconds), which means that an Office 2010 application will use local password length and complexity settings for enforcement if a domain controller does not respond within 4000 milliseconds.

Note:
The domain time-out value has no effect unless you enable the **Set minimum password length** setting, enable the **Set password rules level** setting, and then select the **Local length, local complexity, and domain policy checks** option.

Related password length and complexity settings

The following settings are often used when an organization enforces password length and complexity:

Cryptographic agility settings These settings let you specify the cryptographic providers and algorithms that are used to encrypt documents, presentations, and workbooks.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan cryptography and encryption settings for Office 2010

Microsoft Office 2010 contains settings that let you control the way that data is encrypted when you use Microsoft Access 2010, Microsoft Excel 2010, Microsoft OneNote 2010, Microsoft PowerPoint 2010, Microsoft Project 2010, and Microsoft Word 2010. This article discusses cryptography and encryption in Office 2010, describes the settings that you can use to encrypt data, and provides information about compatibility with previous versions of Microsoft Office. For information about Microsoft Outlook 2010, see Plan for e-mail messaging cryptography in Outlook 2010.

As you plan your encryption settings, consider the following guidelines:

- We recommend that you do *not* change the default encryption settings unless your organization's security model requires encryption settings that differ from the default settings.
- We recommend that you enforce password length and complexity to help ensure that strong passwords are used when you encrypt data. For more information, see Plan password complexity settings for Office 2010.
- We recommend that you do *not* use RC4 encryption. For more information, see Compatibility with previous versions of Office later in this article.
- There is not an administrative setting that lets you force users to encrypt documents. However, there is an administrative setting that lets you remove the ability to add passwords to documents and, therefore, disallow the encryption of documents. For more information, see Cryptography and encryption settings later in this article.
- Saving documents in trusted locations does not affect encryption settings. If a document is encrypted and it is saved in a trusted location, a user must provide a password to open the document.

In this article:

About cryptography and encryption in Office 2010

The available encryption algorithms to use with Office depend on the algorithms that can be accessed through the APIs (application programming interface) in the Windows operating system. Office 2010, in addition to maintaining support for Cryptography API (CryptoAPI), also includes support for CNG (CryptoAPI: Next Generation), which was first made available in the 2007 Microsoft Office system with Service Pack 2 (SP2).

CNG allows for more agile encryption, where different encryption and hashing algorithms supported on the host computer can be specified to be used during the document encryption process. CNG also allows for better extensibility encryption, where third-party encryption modules can be used.

When Office uses CryptoAPI, the encryption algorithms depend on those that are availablein a CSP (Crypto Service Provider), which is part of the Windows operating system. The following registry key contains a list of CSPs that are installed on a computer:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Cryptography/Defaults/Provider

The following CNG encryption algorithms, or any other CNG cipher extension installed on the system, can be used with Office 2010 or the 2007 Office system SP2:

AES, DES, DESX, 3DES, 3DES_112, and RC2

The following CNG hashing algorithms, or any other CNG cipher extension that is installed on the system, can be used with Office 2010 or the 2007 Office system SP2:

MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA256, SHA384, and SHA512

Although there are Office 2010 settings to change how encryption is performed, when you encrypt Open XML Format files (.docx, .xslx, .pptx, and so on) the default values — AES (Advanced Encryption Standard), 128-bit key length, SHA1, and CBC (cipher block chaining) — provide strong encryption and should be fine for most organizations. AES encryption is the strongest industry-standard algorithm that is available and was selected by the National Security Agency (NSA) to be used as the standard for the United States Government. AES encryption is supported on Windows XP SP2, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008.

Cryptography and encryption settings

The following table lists the settings that are available to change the encryption algorithms when you use Microsoft Office versions that access CryptoAPI. This includes Office versions up to and including Office 2010.

Setting	Description
Encryption type for password-protected Office Open XML files	This setting lets you specify an encryption type for Open XML files from the available cryptographic service providers (CSP). This setting is required when you use a custom COM encryption add-in. For more information, see the “2007 Office System Encryption Developers Guide,” which is available as part of the SharePoint Server 2007 SDK (*http://go.microsoft.com/fwlink/?LinkID=107614&clcid=0x409*). This setting is also required if you use the 2007 Office system SP1 or use a version of the Compatibility Pack that is older than the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats (*http://go.microsoft.com/fwlink/?LinkID=78517&clcid=0x409*) and you want to change the encryption algorithm to something other than the default.

Setting	Description
Encryption type for password-protected Office 97-2003 files	This setting lets you specify an encryption type for Office 97–2003 (binary) files from the available cryptographic service providers (CSP). The only supported encryption algorithm when you use this setting is RC4, which, as previously mentioned, we do not recommend.

In Office 2010, if you must change the **Encryption type for password-protected Office Open XML files** setting, you first must enable the **Specify encryption compatibility** setting and select the **Use legacy format** option. The **Specify encryption compatibility** setting is available for Access 2010, Excel 2010, PowerPoint 2010, and Word 2010. The following table lists the settings that are available to change the encryption algorithms when you use Office 2010. These settings apply to Access 2010, Excel 2010, OneNote 2010, PowerPoint 2010, Project 2010, and Word 2010.

Note:
All of the following settings, except for the **Set parameters for CNG context** and **Specify CNG random number generator algorithm** settings, are applicable even when you use a supported operating system for Office 2010, such as Windows XP SP3, which does not include support for CNG. In this case, Office 2010 uses CryptoAPI instead of CNG. These settings apply only when you use Office 2010 for encryption of Open XML files.

Setting	Description
Set CNG cipher algorithm	This setting lets you configure the CNG cipher algorithm that is used. The default is AES.
Configure CNG cipher chaining mode	This setting lets you configure the cipher chaining mode that is used. The default is **Cipher Block Chaining (CBC)**.
Set CNG cipher key length	This setting lets you configure the number of bits to use when you create the cipher key. The default is 128 bits.
Specify encryption compatibility	This setting lets you specify the compatibility format. The default is **Use next generation format**.
Set parameters for CNG context	This setting lets you specify the encryption parameters that should be used for the CNG context. To use this setting, a CNG context first has to be created by using CryptoAPI: Next Generation (CNG). For more information, see CNG Cryptographic Configuration Functions (*http://go.microsoft.com/fwlink/?LinkID=192996&clcid=0x409*).

Setting	Description
Specify CNG hash algorithm	This setting lets you specify the hash algorithm that is used. The default is SHA1.
Set CNG password spin count	This setting lets you specify the number of times to spin (rehash) the password verifier. The default is 100000.
Specify CNG random number generator algorithm	This setting lets you configure the CNG random number generator to use. The default is RNG (Random Number Generator).
Specify CNG salt length	This setting lets you specify the number of bytes of salt that should be used. The default is 16.

In addition to the CNG settings that were listed in the previous table, the CNG setting that is listed in the following table can be configured for Excel 2010, PowerPoint 2010, and Word 2010.

Setting	Description
Use new key on password change	This setting lets you specify if a new encryption key should be used when the password is changed. The default is not to use a new key on password changes.

You can use the setting that is listed in the following table to remove the ability to add passwords to documents and, therefore, disallow encryption of documents.

Setting	Description
Disable password to open UI	This setting controls whether Office 2010 users can add passwords to documents. By default users can add passwords.

Note:
For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*).

Compatibility with previous versions of Office

If you have to encrypt Office documents, we recommend that you save the documents as Open XML Format files (.docx, .xlsx, .pptx, and so on) instead of Office 97–2003 format (.doc, .xls, .ppt, and so on). The encryption that is used for binary documents (.doc, .xls, .ppt) uses RC4. It is not recommended, as discussed in Security Considerations sections 4.3.2 and 4.3.3 of the Office Document Cryptography Structure Specification (*http://go.microsoft.com/fwlink/?LinkId=192287*). Documents that are saved in the older Office binary formats can only be encrypted by using RC4 to maintain compatibility with older versions of Microsoft Office. AES, the default and recommended encryption algorithm, is used to encrypt Open XML Format files.

Office 2010 and the 2007 Office system let you save documents as Open XML Format files. In addition, if you have Microsoft Office XP or Office 2003, you can use the Compatibility Pack to save documents as Open XML Format files.

Documents that are saved as Open XML Format files and encrypted by using Office 2010 can only be read by Office 2010, Office 2007 SP2, and Office 2003 with the Office 2007 SP2 compatibility pack. To ensure compatibility with all previous versions of Office, you can create a registry key (if it does not already exist) under **HKCU\Software\Microsoft\Office\14.0\<application>\Security\Crypto** called **CompatMode** and disable it by setting it to **0**. The values that you can enter for <application> represent the specific Office application that you are configuring this registry key for. For example, you can enter Access, Excel, PowerPoint, or Word. It is important to realize that, when you set **CompatMode** to **0**, Office 2010 uses an Office 2007 compatible encryption format, instead of the enhanced security that is provided by default when you use Office 2010 to encrypt Open XML Format files. If you have to configure this setting for compatibility reasons, we recommend that you also use a third-party encryption module that allows for enhanced security, such as AES encryption.

If your organization uses the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats to encrypt Open XML Format files, you should review the following information:

- By default, the Compatibility Pack uses the following settings to encrypt Open XML Format files:
  - **Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype),AES 128,128** (on the Windows XP Professional operating system).
  - **Microsoft Enhanced RSA and AES Cryptographic Provider,AES 128,128** (on Windows Server 2003 and Windows Vista operating systems).
- Users are not notified that the Compatibility Pack uses these encryption settings.
- The graphical user interface on earlier versions of Office might display incorrect encryption settings for Open XML Format files if the Compatibility Pack is installed.
- Users cannot use the graphical user interface in earlier versions of Office to change the encryption settings for Open XML Format files.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Office Document Cryptography Structure Specification (*http://go.microsoft.com/fwlink/?LinkId=192287*)

Plan digital signature settings for Office 2010

You can digitally sign documents by using Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010. You can also add a signature line or signature stamp by using Excel 2010, Microsoft InfoPath 2010, and Word 2010. Microsoft Office 2010 includes support for XAdES (XML Advanced Electronic Signatures), which is a set of extensions to the XML-DSig standard. This was first supported in the 2007 Microsoft Office system.

In this article:

What is a digital signature?

You can digitally sign a document for many of the same reasons why you might place a handwritten signature on a paper document. A digital signature is used to help authenticate the identity of the creator of digital information — such as documents, e-mail messages, and macros — by using cryptographic algorithms.

Digital signatures are based on digital certificates. Digital certificates are verifiers of identity issued by a trusted third party, which is known as a certification authority (CA). This works similarly to the use of printed identity documents. For example, a trusted third party such as a government entity or employer issues identity documents — such as driver's licenses, passports and employee ID cards — on which other people rely to verify that a person is whom he or she claims to be.

What digital signatures accomplish

Digital signatures help establish the following authentication measures:

- **Authenticity** The digital signature and its underlying digital certificate helps ensure that the signer is whom he or she claims to be. This helps prevent other people from pretending to be the originator of a particular document (the equivalent of forgery on a printed document).
- **Integrity** The digital signature helps ensure that the content has not been changed or tampered with since it was digitally signed. This helps prevent documents from being intercepted and changed without knowledge of the originator of the document.
- **Non-repudiation** The digital signature helps prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content. This helps prove that the originator of the document is the true originator and not someone else, regardless of the claims of the signer. A signer cannot repudiate the signature on that document without repudiating his or her digital key and, therefore, other documents signed with that key.

Requirements for digital signatures

To establish these conditions, the content creator must digitally sign the content by creating a signature that satisfies the following criteria:

- The digital signature is valid. A CA that is trusted by the operating system must sign the digital certificate on which the digital signature is based.
- The certificate that is associated with the digital signature is not expired or contains a time stamp indicating the certificate was valid at the time of signing.
- The certificate that is associated with the digital signature is not revoked.
- The signing person or organization (known as the publisher) is trusted by the recipient.

Word 2010, Excel 2010, and PowerPoint 2010 detect these criteria for you and warn you if there seems to be a problem with the digital signature. Information about problematic certificates can easily be viewed in a certificate task pane that appears in the Office 2010 application. Office 2010 applications let you add multiple digital signatures to the same document.

Digital signatures in the business environment

The following scenario shows how digital signing of documents can be used in a business environment:

1. An employee uses Excel 2010 to create an expense report. The employee then creates three signature lines: one for herself, one for her manager, and one for the accounting department. These lines are used to identify that the employee is the originator of the document, that no changes will occur in the document as it moves to the manager and the accounting department, and that there is proof that both the manager and the accounting department have received and reviewed the document.
2. The manager receives the document and adds her digital signature to the document, confirming that she has reviewed and approved it. She then forwards it to the accounting department for payment.
3. A representative in the accounting department receives the document and signs it, which confirms receipt of the document.

This example demonstrates the ability to add multiple signatures to a single Office 2010 document. In addition to the digital signature, the signer of the document can add a graphic of her actual signature, or use a Tablet PC to actually write a signature into the signature line in the document. There is also a “rubber stamp” feature that can be used by departments, which indicates that a member of a specific department received the document.

Compatibility issues

Office 2010, just as the 2007 Office system, uses the XML-DSig format for digital signatures. In addition, Office 2010 has added support for XAdES (XML Advanced Electronic Signatures). XAdES is a set of tiered extensions to XML-DSig, the levels of which build upon the previous to provide more reliable digital signatures.

For more information about the levels of XAdES that are supported in Office 2010, see Using digital signatures later in this article. For more information about the details of XAdES, see the specification for XML Advanced Electronic Signatures (XAdES) (*http://go.microsoft.com/fwlink/?LinkId=186631*).

It is important to be aware that digital signatures created in Office 2010 are incompatible with versions of Microsoft Office earlier than the 2007 Office system. For example, if a document is signed by using an application in Office 2010 or in the 2007 Office system and opened by using an application in Microsoft Office 2003 that has the Office Compatibility Pack installed, the user will be informed that the document was signed by a newer version of Microsoft Office and the digital signature will be lost.

The following figure shows a warning that the digital signature is removed when the document is opened in an earlier version of Office.

Also, if XAdES is used for the digital signature in Office 2010, the digital signature would not be compatible with the 2007 Office system unless you configure the Group Policy setting, **Do not include XAdES reference object in the manifest**, and set it to **Disabled**. For more information about the digital signature Group Policy settings, see Configure digital signatures later in this article.

If you need digital signatures created in Office 2010 to be compatible with Office 2003 and earlier versions, you can configure the Group Policy setting, **Legacy format signatures**, and set it to **Enabled**. This Group Policy setting is located under User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\Signing. After this setting is set to **Enabled**, the Office 2010 applications use the Office 2003 binary format to apply digital signatures to Office 97–2003 binary documents created in Office 2010.

Digital certificate: Self-signed or issued by CAs

Digital certificates can be either self-signed or issued by CAs in an organization, such as a Windows Server 2008 computer that is running Active Directory Certificate Services, or a public CA, such as VeriSign or Thawte. Self-signed certificates are typically used by people and small businesses that do not want to set up a public key infrastructure (PKI) for their organizations and do not want to purchase a commercial certificate.

The primary drawback of using self-signed certificates is that they are only useful if you exchange documents with those who know you personally and are confident that you are the actual originator of the document. By using self-signed certificates, there is no third party that validates the authenticity of your certificate. Each person who receives your signed document must manually decide whether to trust your certificate.

For larger organizations, two primary methods for obtaining digital certificates are available: certificates that are created by using a corporate PKI and commercial certificates. Organizations that want to share signed documents only among other employees in the organization might prefer a corporate PKI to reduce costs. Organizations that want to share signed documents with people outside of their organization might prefer to use commercial certificates.

Certificates created by using a corporate PKI

Organizations have the option to create their own PKI. In this scenario, the company sets up one or more certification authorities (CAs) that can create digital certificates for computers and users throughout the company. When combined with the Active Directory directory service, a company can create a complete PKI solution so that all corporate-managed computers have the corporate CA chain installed and that both users and computers are automatically assigned digital certificates for document signing and encryption. This allows for all employees in a company to automatically trust digital certificates (and, therefore, valid digital signatures) from other employees in the same company.

For more information, see Active Directory Certificate Services (*http://go.microsoft.com/fwlink/?LinkId=188299*).

Commercial certificates

Commercial certificates are purchased from a company whose line of business is to sell digital certificates. The main advantage of using commercial certificates is that the commercial certificate vendor's root CA certificate is automatically installed on Windows operating systems, which enables these computers to automatically trust these CAs. Unlike the corporate PKI solution, commercial certificates enable you to share your signed documents with users who do not belong to your organization.

There are three kinds of commercial certificates:

- **Class 1** Class 1 certificates are issued to people who have valid e-mail addresses. Class 1 certificates are appropriate for digital signatures, encryption, and electronic access control for non-commercial transactions where proof of identity is not required.
- **Class 2** Class 2 certificates are issued to people and devices. Class 2 individual certificates are appropriate for digital signatures, encryption, and electronic access control in transactions where proof of identity based on information in the validating database is sufficient. Class 2 device certificates are appropriate for device authentication; message, software, and content integrity; and confidentiality encryption.
- **Class 3** Class 3 certificates are issued to people, organizations, servers, devices, and administrators for CAs and root authorities (RAs). Class 3 individual certificates are appropriate for digital signatures, encryption, and access control in transactions where proof of identity must be assured. Class 3 server certificates are appropriate for server authentication; message, software, and content integrity; and confidentiality encryption.

For more information about commercial certificates, see Digital ID – Office Marketplace (*http://go.microsoft.com/fwlink/?LinkId=119114*).

Using digital signatures

You can digitally sign documents by using Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010. You can also add a signature line or signature stamp using Excel 2010, Microsoft InfoPath 2010, and Word 2010. Digitally signing a document that has a digital certificate but does not have a signature line or stamp is known as creating an invisible digital signature. Both methods, visible and invisible digital signatures, use a digital certificate for signing the document. The difference is the graphical representation within the document when a visible digital signature line is used. For more information about how to add a digital signature, see Add or remove a digital signature in Office files (*http://go.microsoft.com/fwlink/?LinkId=187659*).

By default, Office 2010 creates XAdES-EPES digital signatures, whether a self-signed certificate or a certificate signed by a CA is used during the creation of the digital signature.

The XAdES digital signature levels, based on the XML-DSig digital signature standard, available in Office 2010 are listed in the following table. Each of the levels builds upon the previous level and contains all the capabilities of the previous levels. For example, XAdES-X also contains all of the capabilities of XAdES-EPES, XAdES-T, and XAdES-C, in addition to the new functionality introduced with XAdES-X.

Signature level	Description
XAdES-EPES (Base)	Adds information about the signing certificate to the XML-DSig signature. This is the default for Office 2010 signatures.
XAdES-T (Timestamp)	Adds a time stamp to the XML-DSig and XAdES-EPES sections of the signature, which helps protect against certificate expiration.
XAdES-C (Complete)	Adds references to certification chain and revocation status information.
XAdES-X (Extended)	Adds a time stamp to the XML-DSig SignatureValue element, and the –T and –C sections of the signature. The additional time stamp protects the additional data from repudiation.
XAdES-X-L (Extended Long Term)	Stores the actual certificate and certificate revocation information together with the signature. This allows for certificate validation even if the certificate servers are no longer available.

Time stamp digital signatures

The ability with Office 2010 to add a time stamp to a digital signature allows for helping to extend the lifespan of a digital signature. For example, if a revoked certificate has previously been used for the creation of the digital signature, which contains a time stamp from a trusted time stamp server, the digital signature could still be considered valid if the time stamp occurred before the revocation of the certificate. To use the time stamp functionality with digital signatures, you must complete the following:

- Set up a time stamp server that is compliant with RFC 3161
- Use the Group Policy setting, **Specify server name**, to enter the location of the time stamp server on the network.

You can also configure additional time stamp parameters by configuring one or more of the following Group Policy settings:

- **Configure time stamping hashing algorithm**
- **Set timestamp server timeout**

If you do not configure and enable **Configure time stamping hashing algorithm**, the default value of SHA1 will be used. If you do not configure and enable **Set timestamp server timeout**, the default time that Office 2010 will wait for the time stamp server to respond to a request is 5 seconds.

Configure digital signatures

In addition to the Group Policy settings for configuring time stamp related–settings, there are other Group Policy settings to configure how digital signatures are configured and controlled in an organization. The setting names and descriptions are listed in the following table.

Setting	Description
Require OCSP at signature generation time	This policy setting lets you determine whether Office 2010 requires OCSP (Online Certificate Status Protocol) revocation data for all digital certificates in a chain when digital signatures are generated.
Specify minimum XAdES level for digital signature generation	This policy setting lets you specify a minimum XAdES level that Office 2010 applications must reach in order to create an XAdES digital signature. If unable to reach the minimum XAdES level, the Office application does not create the signature.
Check the XAdES portions of a digital signature	This policy setting lets you specify whether Office 2010 checks the XAdES portions of a digital signature, if present, when validating a digital signature for a document.

Setting	Description
Do not allow expired certificates when validating signatures	This policy setting lets you configure whether Office 2010 applications accept expired digital certificates when verifying digital signatures.
Do not include XAdES reference object in the manifest	This policy setting lets you determine whether an XAdES reference object should appear in the manifest. You must configure this setting to **Disabled** if you want the 2007 Office system to be able to read Office 2010 signatures that contain XAdES content; otherwise, the 2007 Office system will consider signatures that contain XAdES content invalid.
Select digital signature hashing algorithm	This policy setting lets you configure the hashing algorithm that Office 2010 applications use to confirm digital signatures.
Set signature verification level	This policy setting lets you set the verification level that is used by Office 2010 applications when validating a digital signature.
Requested XAdES level for signature generation	This policy setting lets you specify a requested or desired XAdES level in creating a digital signature.

Additional digital signature related Group Policy settings are listed as follows:

- **Key Usage Filtering**
- **Set default image directory**
- **EKU filtering**
- **Legacy format signatures**
- **Suppress Office Signing Providers**
- **Suppress external signature services menu item**

For more information about each Group Policy setting, see the help files that are contained with the Administrative Template files for Office 2010. For more information about the Administrative Template files, see Group Policy overview for Office 2010.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

Plan privacy options for Office 2010

If you want to suppress the **Welcome to Microsoft Office 2010** dialog box that appears the first time that a user starts Microsoft Office 2010, you can configure privacy options. The **Welcome to Microsoft Office 2010** dialog box, also known as the Opt-in wizard or the **Recommended Settings** dialog box, lets users enable or disable several Internet-based services that help protect and improve Office 2010 applications.

In this article:

About planning privacy options

The first time that a user starts Office 2010, the following dialog box appears:

If users select **Use Recommended Settings**, the following security settings and privacy options are enabled:

- Recommended and important updates are automatically installed for the Windows Vista and newer operating systems and Office 2010 applications. Users are notified about new optional software. For Windows XP, high priority updates are installed.

- Applications are able to connect to Office.com for updated Help content and can receive targeted Help content for Office 2010 applications that are installed.
- Applications are able to periodically download small files that help determine system problems and prompt users to send error reports to Microsoft.
- Users are signed up for the Customer Experience Improvement Program.

If users select **Install Updates Only**, recommended and important updates are automatically installed for the Windows Vista operating systems and newer Windows operating systems and Office 2010 applications. Users are notified about new optional software. For Windows XP, only high priority updates are installed. However, privacy options are not changed in Office 2010 applications, which means that the default privacy options take effect. If users select **Don't Make Changes**, automatic updating is not changed in the Windows Security Center and privacy options are not changed in Office 2010, which means that the default privacy options take effect.

The default privacy options for Office 2010 applications are as follows:

- Office 2010 applications do not connect to Office.com for updated Help content and office applications are not detected on your computer to give users improved search results.
- Office 2010 applications do not download small programs that help diagnose problems and error message information is not sent to Microsoft.
- Users are not enrolled in the Customer Experience Improvement Program.

Because the **Welcome to Microsoft Office 2010** dialog box lets users enable or disable several Internet-based services, you might want to prevent the dialog box from appearing and configure these services individually. If you suppress the dialog box, we recommend that you enable all of the Internet-based services, which you can do by configuring privacy options.

Note:
For information about how to configure security settings in the Office Customization Tool (OCT) and the Office 2010 Administrative Templates, see Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*).

Suppress the Welcome to Microsoft Office 2010 dialog box

You can suppress the **Welcome to Microsoft Office 2010** dialog box by enabling the **Suppress recommended settings dialog** setting. This Group Policy setting is located in the Group Policy Object Editor under User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\Miscellaneous. This setting prevents the **Welcome to Microsoft Office 2010** dialog box from appearing the first time that a user starts Office 2010. If you enable this setting, the automatic updating feature remains unchanged and the privacy options that control Internet-based services are not enabled.

If you suppress the **Welcome to Microsoft Office 2010** dialog box without enabling certain privacy options, you disable several features that improve Office 2010 applications and you could expose a

computer to security threats. Therefore, if you enable this setting we recommend that you also enable all of the privacy options that are discussed in Configure privacy options.

Most organizations enable this setting, including organizations that have a highly restrictive security environment or a security environment that restricts Internet access.

Configure privacy options

Office 2010 provides several settings that let you control the disclosure of private information. These settings are often known as privacy options. You can enable or disable each of these settings to suit your organization's security requirements. However, if you suppress the **Welcome to Microsoft Office 2010** dialog box, we recommend that you enable all these settings.

Setting name: Online content options. This Group Policy setting is located in the Group Policy Object Editor under User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\ Tools | Options | General | Service Options… \ Online Content.

- **Description**: This setting controls whether the Office 2010 Help system can download Help content from Office.com. You can select one of three possible options for this setting:

  Never show online content or entry points. The Help system does not connect to Office.com to download content. This is the default setting if you suppress the **Welcome to Microsoft Office 2010** dialog box or if users select **Don't make changes** or **Install Updates Only** on the **Welcome to Microsoft Office 2010** dialog box.

  Search only offline content whenever available. The Help system does not connect to Office.com to download content.

  Search online content whenever available. The Help system connects to Office.com for content when the computer is connected to the Internet.

- **Impact**: If you enable this setting and select **Never show online content or entry points** or **Search only offline content whenever available**, users cannot access updated Help topics through the Help system and you cannot get templates from Office.com.
- **Guidelines**: Most organizations enable this setting and select **Search online content whenever available**. This is the recommended configuration for this setting. However, organizations that have a highly restrictive security environment, or a security environment that restricts Internet access, typically enable this setting and select **Never show online content or entry points**.

Setting name: Automatically receive small updates to improve reliability. This Group Policy setting is located in the Group Policy Object Editor under User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\ Privacy\Trust Center.

Description: This setting controls whether client computers periodically download small files that enable Microsoft to diagnose system problems.

Impact: If you enable this setting, Microsoft collects information about specific errors and the IP address of the computer. No personally identifiable information is transmitted to Microsoft other than the IP address of the computer requesting the update.

Guidelines: Most organizations enable this setting, which is the recommended configuration. Organizations that have a highly restrictive security environment, or a security environment that restricts Internet access, typically disable this setting.

Setting name: Enable Customer Experience Improvement Program. This Group Policy setting is located under User Configuration\Administrative Templates\(ADM\ADMX)\Microsoft Office 2010\Privacy\Trust Center.

Description: This setting controls whether users participate in the CEIP to help improve Office 2010. When users participate in the CEIP, Office 2010 applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and improve the products and features customers use most often. Participating in the CEIP does not collect users' names, addresses, or any other identifying information except the IP address of the computer that is used to send the data.

Impact: If you enable this setting, users participate in the CEIP.

Guidelines: Most organizations enable this setting, which is the recommended configuration. Organizations that have a highly restrictive security environment, or a security environment that restricts Internet access, typically do not enable this setting.

Related privacy options

Several other settings are related to privacy disclosure in Office 2010 applications. If you are changing privacy options because you have a special security environment, you might want to evaluate the following settings:

Protect document metadata for password protected files This setting determines whether metadata is encrypted when you use the Encrypt with Password feature.

Protect document metadata for rights managed Office Open XML files This setting determines whether metadata is encrypted when you use the Restrict Permission by People feature.

Warn before printing, saving, or sending a file that contains tracked changes or comments This setting determines whether users are warned about comments and tracked changes before they print, save, or send a document.

Make hidden markup visible This setting determines whether all tracked changes are visible when you open a document.

Prevent document inspectors from running This setting lets you disable Document Inspector modules.

Note:
For the latest information about policy settings, refer to the Microsoft Excel 2010 workbook Office2010GroupPolicyAndOCTSettings_Reference.xls, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316&clcid=0x409*) download page.

See Also

Security overview for Office 2010

Configure security for Office 2010 (*http://technet.microsoft.com/library/14675abe-a72c-4d01-aa41-ebd35ffc9165(Office.14).aspx*)

Plan file block settings for Office 2010

This article provides information about Group Policy and Office Customization Tool (OCT) settings that you can configure to block specific file format types for Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010 users.

In this article:

Blocking file format types by using Group Policy or the OCT

You can block specific types of files for Excel 2010, PowerPoint 2010, and Word 2010, and determine how users can open and save these blocked files, by configuring settings in Group Policy or the OCT. Although you can use block file format settings to manage file usage in many scenarios, these settings are most commonly used to:

- Force an organization to use specific file formats.
- Mitigate zero-day security attacks (which are attacks that occur during between the time that a vulnerability becomes publicly known and a software update or service pack is available) by temporarily preventing users from opening specific types of files.
- Prevent an organization from opening files that have been saved in earlier and pre-release (beta) Microsoft Office formats.

Planning considerations for configuring file block settings

Consider the following overall guidelines as you plan your file block settings:

- Decide if you want users to be able to make changes to your configurations:
  - If you have used Group Policy to configure file block settings (*policies*), users cannot change your configurations.
  - If you have used the OCT to make file block settings (*preferences*), users can make changes to the settings in the Trust Center UI.
- Block open settings do not apply to files that are opened from trusted locations.
- Block file format settings are application-specific. You cannot prevent users from using other applications to open or save file types or formats that are blocked. For example, you can enable block file format settings that prevent users from opening .dot files in Word 2010, but users will still be able to open .dot files by using Microsoft Publisher 2010, which uses a converter to read the .dot file.

- Disabling notifications in the Message Bar does not affect block file format settings. The block file format warning dialog box appears before any notification appears in the Message Bar.

Group Policy and OCT settings

This section describes how to find the settings in Group Policy and the OCT, and lists the settings for Excel 2010, PowerPoint 2010, and Word 2010.

How to find the settings

Unless otherwise noted, the location of the settings are as follows:

- For Group Policy, the settings are available under the **User Configuration/Administrative Templates** node of the Group Policy Object Editor.

  Note:
  The locations in the Group Policy Object Editor presented in this article apply when you invoke the Group Policy Object Editor to edit a GPO. To edit local Group Policy, use the Local Group Policy Editor. To edit domain-based Group Policy, use the Group Policy Management Console (GPMC). Either tool invokes the Group Policy Object Editor when you edit a GPO. For more information, see Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*) and Group Policy overview for Office 2010.

- For the OCT, the policy settings are available on the **Modify user settings** page.

Once in Group Policy and the OCT, the specific path of the folder that contains the file block settings for Excel 2010, PowerPoint 2010, and Word 2010 are parallel:

- Excel 2010 file block settings:
  - **Microsoft Excel 2010\Excel Options\Security\Trust Center\File Block Settings**
- PowerPoint 2010 file block settings:
  - **Microsoft PowerPoint 2010\PowerPoint Options\Security\Trust Center\File Block Settings**
- Word 2010 file block settings:
  - **Microsoft Word 2010\Word Options\Security\Trust Center\File Block Settings**

Note:
By default, users can set default file block settings in the Trust Center user interface (UI) for Excel 2010, PowerPoint 2010, and Word 2010 (on the **File** tab, click **Options**, click **Trust Center**, click **Trust Center Settings**, and then click **File Block Settings**). You can disable the file block options in Trust Center options by configuring the settings through Group Policy. If you configure the settings through the OCT, users will still have the option of specifying file type behavior through the Trust Center UI. For more information, see What is File Block? (*http://go.microsoft.com/fwlink/?LinkId=195498*).

About the “Set default file block behavior” setting

The “Set default file block behavior” setting specifies how blocked files open (for example: does not open, opens in protected view, or opens in protected view but can be edited). If you enable this setting, the default file block behavior you specify applies to any file format that users block in the Trust Center UI. It also applies to a specific file format only if you both enable its file format setting (for more information about individual file format settings, see the tables in this article) and select the **Open/Save blocked, use open policy** option. Otherwise, if you configure an individual file format setting, it overrides the **Set default file block behavior** setting configuration for that file type.

Note:
The options under **Open behavior for selected types** in the Trust Center UI, under **File Block**, map directly to the options in the **Set default file block behavior** setting. You can disable these UI options for users by enabling the “Set default file block behavior” setting in Group Policy.

Excel 2010 settings

The following table lists the file block settings in Group Policy and the OCT that you can configure for Excel 2010 users. With the exception of the **Set default file block behavior** setting, file setting names correspond to the file types that they can block.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
Set default file block behavior	• Blocked file formats set by users in the Trust Center UI • Individual file types, if you enable its setting and select **Open/Save blocked, use open policy** **Note:** Individual file type settings override this setting.	• Blocked files are not opened. • Blocked files open in Protected View and cannot be edited. • Blocked files open in Protected View and can be edited.	Blocked files are not opened (users cannot open blocked files).
Excel 2007 and later workbooks and templates	*.xlsx *.xltx	• Do not block: The file type is not blocked. • Save blocked: Saving of the	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 2007 and later macro-enabled workbooks and templates	• *.xlsm • *.xltm	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 2007 and later add-in files	• *.xlam	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Excel 2007 and later binary workbooks	• *.xlsb	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
OpenDocument Spreadsheet files	• *.ods	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		and saving of the file type is blocked, and the option to edit is enabled.	
Excel 97–2003 add-in files	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Excel 97–2003 workbooks and templates	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 95–97 workbooks and templates	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Excel 95 workbooks	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 4 workbooks	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled.	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		• Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 4 worksheets	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Excel 3 worksheets	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 2 worksheets	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 4 macrosheets and add-in files	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Excel 3 macrosheets and add-in files	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		behavior setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Excel 2 macrosheets and add-in files	• *.xls • *.xla • *.xlt • *.xlm • *.xlw • *.xlb	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		and saving of the file type is blocked, and the option to edit is enabled.	
Web pages and Excel 2003 XML spreadsheets	• *.mht • *.mhtml • *.htm • *.html • *.xml • *.xlmss	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
XML files	• *.xml	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	
Text files	• *.txt • *.csv • *.prn	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Excel add-in files	• *.xll (.dll)	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
dBase III / IV files	• *.dbf	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
Microsoft Office query files	• *.iqy • *.dqy • *.oqy • *.rqy	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Microsoft Office data connection files	• *.odc	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Other data source	• *.udl	• Do not block: The file type is	File format

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
files	• *.dsn • *.mdb • *.mde • *.accdb • *.accde • *.dbc • *.uxdc	not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	type is not blocked.
Offline cube files	• *.cub	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Dif and Sylk files	• *.dif • *.slk	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Legacy converters for Excel	• All file formats that are opened through a converter	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Microsoft Office Open XML converters for Excel	• All file formats that are opened through an OOXML converter	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options:	If you disable or do not configure this setting
		disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	

PowerPoint 2010 settings

The following table lists the file block settings in Group Policy and the OCT that you can configure for PowerPoint 2010 users. With the exception of the **Set default file block behavior** setting, file setting names correspond to the file types that they can block.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
Set default file block behavior	• Blocked file formats set by users in the Trust Center UI • Individual file types, if you enable its setting and select **Open/Save blocked, use open policy** Note: individual file type settings override this setting.	• Blocked files are not opened. • Blocked files open in Protected View and cannot be edited. • Blocked files open in Protected View and can be edited.	Blocked files are not opened (users cannot open blocked files).
PowerPoint 2007 and later presentations, shows, templates, themes, and add-ins	• *.pptx • *.pptm • *.potx • *.ppsx	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
	• *.ppam • *.thmx • *.xml	open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
OpenDocument Presentation files	• *.odp	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open.	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		• Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
PowerPoint 97–2003 presentations, shows, templates and add-in files	• *.ppt • *.pot • *.pps • *.ppa	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
Web pages	• *.mht • *.mhtml • *.htm • *.html	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Outline files	• *.rtf • *.txt • *.doc • *.wpd • *.docx • *.docm • *.wps	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		behavior setting.	
Legacy converters for PowerPoint	• Presentation files older than PowerPoint 97	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Graphic Filters	• *.jpg • *.png • *.tif • *.bmp • *.wmf • *.emf	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked.	File format type is not blocked.
Microsoft Office Open XML converters for	• All file formats that are opened through	• Do not block: The file type is not blocked.	File format type is not

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
PowerPoint	an OOXML converter	• Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	blocked.

Word 2010 settings

The following table lists the file block settings in Group Policy and the OCT that you can configure for Word 2010 users. With the exception of the **Set default file block behavior** setting, file setting names correspond to the file types that they can block.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
Set default file block behavior	• Blocked file formats set by users in the	• Blocked files are not opened. • Blocked files open in	Blocked files are not opened (users cannot

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
	Trust Center UI • Individual file types, if you enable its setting and select **Open/Save blocked, use open policy**  **Note:** Individual file type settings override this setting.	Protected View and cannot be edited. • Blocked files open in Protected View and can be edited.	open blocked files).
Word 2007 and later documents and templates	• *.docx • *.dotx • *.docm • *.dotm • *.xml (Word Flat Open XML)	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
OpenDocument text files	• *.odt	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Word 2007 and later binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Word 2003 binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		and saving of the file type is blocked, and the option to edit is enabled.	
Word 2003 and plain XML documents	• *.xml	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Word XP binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		default file block behavior setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Word 200 binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Word 97 binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Word 95 binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Word 6.0 binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		and saving of the file type is blocked, and the option to edit is enabled.	
Word 2.0 and earlier binary documents and templates	• *.doc • *.dot	• Do not block: The file type is not blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.
Web pages	• *.htm • *.html • *.mht • *.mhtml	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set**	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		default file block behavior setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
RTF files	• *.rtf	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Plain text files	*.txt	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting.	File format type is not blocked.
Legacy converters for Word	• All file formats that are opened through a converter	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the	File format type is not blocked.

Setting name	File format extension	If you enable this setting, you can select one of the following options	If you disable or do not configure this setting
		option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	
Office Open XML converters for Word	• All file formats that are opened through an OOXML converter	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked. • Open/Save blocked, use open policy: Both opening and saving of the file type is blocked. The file opens based on the configuration of the **Set default file block behavior** setting. • Block: Both opening and saving of the file type is blocked, and the file does not open. • Open in Protected View: Both opening and saving of the file type is blocked, and the option to edit the file type is disabled. • Allow editing and open in Protected View: Both opening and saving of the file type is blocked, and the option to edit is enabled.	File format type is not blocked.

See Also

Plan security for Office 2010

Group Policy overview for Office 2010

Enforce settings by using Group Policy in Office 2010

Office Customization Tool in Office 2010

Plan for Information Rights Management in Office 2010

In many businesses, sensitive information such as employee medical and financial records, payroll information, and private personal data is protected only by limiting access to the networks or computers where the information is stored. Information Rights Management (IRM) technology in Microsoft Office 2010 helps organizations and information workers control sensitive information electronically by enabling users to specify permissions for accessing and using documents and messages.

This article contains a summary of IRM technology and how it works in Office applications, together with links to more information about how to set up and install the required servers and software to implement IRM in Office 2010.

In this article:

IRM overview

Information Rights Management (IRM) is a persistent file-level technology from Microsoft that uses permissions and authorization to help prevent sensitive information from being printed, forwarded, or copied by unauthorized people. Once permission for a document or message is restricted by using this technology, the usage restrictions travel with the document or e-mail message as part of the contents of the file.

Note

- The ability to create content or e-mail messages that have restricted permission by using IRM is available in Microsoft Office Professional Plus 2010, and in the stand-alone versions of Microsoft Excel 2010, Microsoft Outlook 2010, Microsoft PowerPoint 2010, Microsoft InfoPath 2010, and Microsoft Word 2010. IRM content that is created in Office 2010 can be viewed in Microsoft Office 2003, the 2007 Microsoft Office system, or Office 2010.
- For more information about IRM and Active Directory Rights Management Services (AD RMS) features that are supported in Office 2010, Office 2007, and Office 2003, see AD RMS and Microsoft Office Deployment Considerations (*http://go.microsoft.com/fwlink/?LinkId=153314*).

IRM support in Office 2010 helps organizations and knowledge workers address two fundamental needs:

- **Restricted permission for sensitive information** IRM helps prevent sensitive information from unauthorized access and reuse. Organizations rely on firewalls, logon security-related measures, and other network technologies to help protect sensitive intellectual property. A basic limitation of using these technologies is that legitimate users who have access to the information can share it with unauthorized people. This could lead to a potential breach of security policies.
- **Information privacy, control, and integrity** Information workers often work with confidential or sensitive information. By using IRM, employees do not have to depend on the discretion of other people to ensure that sensitive materials remain inside the company. IRM eliminates users' ability to forward, copy, or print confidential information by helping to disable those functions in documents and messages that use restricted permission.

For information technology (IT) managers, IRM helps enable the enforcement of existing corporate policies about document confidentiality, workflow, and e-mail retention. For CEOs and security officers, IRM reduces the risk of having key company information fall into the hands of the wrong people, whether by accident, thoughtlessness, or through malicious intent.

How IRM works in Office 2010

Office users apply permissions to messages or documents by using options on the ribbon; for example, by using the **Restrict Editing** command on the **Review** tab in Word. The protection options available are based on *permission policies* that you customize for your organization. Permission policies are groups of IRM rights that you package together to apply as one policy. Office 2010 also provides several predefined groups of rights, such as **Do Not Forward** in Microsoft Outlook 2010.

Using IRM with an RMS server

Enabling IRM in your organization typically requires access to a rights management server that runs Windows Rights Management Services (RMS) for Windows Server 2003 or Active Directory Rights Management Services (AD RMS) for Windows Server 2008. (It is also possible to use IRM by using Windows Live ID to authenticate permissions, as described in the next section.) The permissions are enforced by using authentication, typically by using Active Directory directory service. Windows Live ID can authenticate permission if Active Directory is not implemented.

Users do not have to have Office to be installed to read protected documents and messages. For users who run Windows XP or earlier versions, the Excel viewer (*http://go.microsoft.com/fwlink/?LinkId=184596*) and Word viewer (*http://go.microsoft.com/fwlink/?LinkId=184595*) enable Windows users who have the correct permission to read some documents that have restricted permission, without using Office software. Users running Windows XP or earlier versions can use Microsoft Outlook Web App or the Rights Management Add-on for Internet Explorer (*http://go.microsoft.com/fwlink/?LinkId=82926*) to read e-mail messages that have restricted permissions, without using Outlook software. For users who run Windows 7, Windows Vista Service Pack 1, Windows Server 2008, or Windows Server 2008 R2, this

functionality is already available. The Active Directory Rights Management Services client software is included with these operating systems.

In Office 2010, organizations can create the permissions policies that appear in Office applications. For example, you might define a permission policy named **Company Confidential**, which specifies that documents or e-mail messages that use the policy can only be opened by users inside the company domain. There is no limit to the number of permission policies that can be created.

Note:
Windows SharePoint Services 3.0 supports using IRM on documents that are stored in document libraries. By using IRM in Windows SharePoint Services, you can control which actions users can take on documents when they open them from libraries in Windows SharePoint Services 3.0. This differs from IRM applied to documents stored on client computers, where the owner of a document can choose which rights to assign to each user of the document. For more information about how to use IRM with document libraries, see Plan document libraries (Windows SharePoint Services) (*http://go.microsoft.com/fwlink/?LinkId=183051*).

With AD RMS on Windows Server 2008, users can share rights-protected documents between companies that have a federated trust relationship. For more information, see Active Directory Rights Management Services Overview (*http://go.microsoft.com/fwlink/?LinkId=183052*) and Federating AD RMS (*http://go.microsoft.com/fwlink/?LinkId=183053*).

Also with AD RMS, Microsoft Exchange Server 2010 offers new IRM-protected e-mail functionality including AD RMS protection for Unified Messaging voice mail messages and Microsoft Outlook protection rules that can automatically apply IRM-protection to messages in Outlook 2010 before they leave the Microsoft Outlook client. For more information, see What's New in Exchange 2010 (*http://go.microsoft.com/fwlink/?LinkId=183062*) and Understanding Information Rights Management: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=183063*).

For more information about how to install and configure RMS servers, see Windows Server 2003 Rights Management Services (RMS) (*http://go.microsoft.com/fwlink/?LinkId=73121*) and Windows Server 2008 Active Directory Rights Management Services (*http://go.microsoft.com/fwlink/?LinkId=180006*).

Using IRM without a local RMS server

In a typical installation, Windows Server 2003 with RMS or Windows Server 2008 with AD RMS enables using IRM permissions with Office 2010. If an RMS server is not configured on the same domain as the users, Windows Live ID can authenticate permission, instead of Active Directory. Users must have access to the Internet to connect to the Windows Live ID servers.

You can use Windows Live ID accounts when you assign permissions to users who need access to the contents of a restricted file. When you use Windows Live ID accounts for authentication, each user must specifically be granted permission to a file. Groups of users cannot be assigned permission to access a file.

Setting up IRM for Office 2010

Applying IRM permissions to documents or e-mail messages requires the following:

- Access to RMS for Windows Server 2003 or AD RMS for Windows Server 2008 to authenticate permissions. Or, authentication can be managed by using the Windows Live ID service on the Internet.
- Rights Management (RM) client software. RM client software is included in Windows Vista and later versions or available as an add-in for Windows XP and Windows Server 2003.
- Microsoft Office 2003, 2007 Microsoft Office system, or Office 2010. Only specific versions of Office enable users to create IRM permissions.

Setting up RMS server access

Windows RMS or AD RMS manages licensing and other administrative server functions that work with IRM to provide rights management. An RMS-enabled client program, such as Office 2010, lets users create and view rights-protected content.

To learn more about how RMS works and how to install and configure an RMS server, see Windows Server 2003 Rights Management Services (RMS) (*http://go.microsoft.com/fwlink/?LinkId=73121*), Windows Server 2008 Active Directory Rights Management Services (*http://go.microsoft.com/fwlink/?LinkId=180006*), and Understanding Information Rights Management: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=183062*).

Installing the Rights Management client software

RM client software is included in Windows Vista and later versions of Windows. Separate installation and configuration of the necessary RMS client software is required on Windows XP and Windows Server 2003 to interact with RMS or AD RMS on the computer that is running Windows or the Windows Live ID service on the Internet.

Download the RMS Client Service Pack (*http://go.microsoft.com/fwlink/?LinkId=82927*) to enable users on Windows XP and Windows Server 2003 to run applications that restrict permission based on RMS technologies.

Defining and deploying permissions policies

As in Office 2003 and the 2007 Office system, Office 2010 includes predefined groups of rights that users can apply to documents and messages, such as **Read** and **Change** in Microsoft Word 2010, Microsoft Excel 2010, and Microsoft PowerPoint 2010. You can also define custom IRM permissions policies to provide different packages of IRM rights for users in your organization.

You create and manage rights policy templates by using the administration site on your RMS or AD RMS server.

For information about how to create, configure, and post custom permissions policy templates, see Windows Server 2003 Rights Management Services (RMS) (*http://go.microsoft.com/fwlink/?LinkId=73121*) and Windows Server 2008 AD RMS Rights Policy Templates Deployment Step-by-Step Guide (*http://go.microsoft.com/fwlink/?LinkId=183068*). For Exchange Server 2010 Outlook protection rules, see Understanding Outlook Protection Rules: Exchange 2010 Help (*http://go.microsoft.com/fwlink/?LinkId=183067*). The rights that you can include in permissions policy templates for Office 2010 are listed in the following sections.

Permissions rights

Each IRM permissions right listed in the following table can be enforced by Office 2010 applications configured on a network that includes a server that runs RMS or AD RMS.

IRM right	Description
Full Control	Gives the user every right listed in this table, and the right to change permissions that are associated with content. Expiration does not apply to users who have Full Control.
View	Allows the user to open IRM content. This corresponds to Read Access in the Office 2010 user interface.
Edit	Allows the user to configure the IRM content.
Save	Allows the user to save a file.
Extract	Allows the user to make a copy of any part of a file and paste that part of the file into the work area of another application.
Export	Allows the user to save content in another file format by using the **Save As** command. Depending on the application that uses the file format that you select, the content might be saved without protection.
Print	Allows the user to print the contents of a file.
Allow Macros	Allows the user to run macros against the contents of a file.
Forward	Allows an e-mail recipient to forward an IRM e-mail message and to add or remove recipients from the To: and Cc: lines.
Reply	Allows e-mail recipients to reply to an IRM e-mail message.
Reply All	Allows e-mail recipients to reply to all users on the To: and Cc: lines of an IRM e-mail message.
View Rights	Gives the user permission to view the rights associated with a file. Office ignores this right.

Predefined groups of permissions

Office 2010 provides the following predefined groups of rights that users can choose from when they create IRM content. The options are available in the **Permission** dialog box for Word 2010, Excel 2010, and PowerPoint 2010. In the Office application, click the **File** tab, click **Info**, click the **Protect Document** button, select **Restriction Permission by People**, click **Restrict Access**, and then click **Restrict permission to this document** to enable the permission options listed in the following table.

IRM predefined group	Description
Read	Users with Read permission only have the View right.
Change	Users with Change permission have View, Edit, Extract, and Save rights.

In Outlook 2010, users can select the following predefined group of rights when they create an e-mail item. The option is accessed from the e-mail by clicking the **File** tab, **Info**, and then **Set Permissions**.

IRM predefined group	Description
Do Not Forward	In Outlook, the author of an IRM e-mail message can apply Do Not Forward permission to users in the To:, Cc:, and Bcc: lines. This permission includes the View, Edit, Reply, and Reply All rights.

Advanced permissions

Other IRM permissions can be specified in the advanced **Permission** dialog box in Word 2010, Excel 2010, and PowerPoint 2010. In the initial **Permission** dialog box, click **More Options**. For example, users can specify an expiration date, let other users to print or copy content, and so on.

By default, Outlook enables messages to be viewed by a browser that supports Rights Management.

Deploying rights policy templates

When the rights policy templates are complete, post them to a server share where all users can access the templates or copy them to a local folder on the user's computer. The IRM policy settings that are available in the Office Group Policy template (Office14.adm) file can be configured to point to the location where the rights policy templates are stored (either locally or on an available server share). For information, see Configure Information Rights Management in Office 2010 (*http://technet.microsoft.com/library/27c84179-87fd-483e-a34d-806c4646ce9d(Office.14).aspx*).

Configuring IRM settings for Office 2010

You can lock down many settings to customize IRM by using the Office Group Policy template (Office14.adm). You can also use the Office Customization Tool (OCT) to configure default settings, which enables users to configure the settings. In addition, there are IRM configuration options that can only be configured by using registry key settings.

Office 2010 IRM settings

The settings that you can configure for IRM in Group Policy and by using the OCT are listed in the following table. In Group Policy, these settings are under **User Configuration\Administrative Templates\Microsoft Office 2010\Manage Restricted Permissions**.

The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

IRM option	Description
Active Directory time-out for querying one entry for group expansion	Specify the time-out value for querying an Active Directory entry when expanding a group.
Additional permissions request URL	Specify the location where a user can obtain more information about how to access the IRM content.
Allow users with earlier versions of Office to read with browsers…	Enable users without Office 2010 to view rights-managed content by using the Rights Management Add-in for Windows Internet Explorer.
Always expand groups in Office when restriction permission for documents	Group name is automatically expanded to display all the members of the group when users apply permissions to a document by selecting a group name in the **Permission** dialog box.
Always required users to connect to verify permission	Users opening a rights-managed Office document must connect to the Internet or local area network to confirm by RMS or Windows Live ID that they have a valid IRM license.
Disable Microsoft Passport service for content with restricted permission	If enabled, users cannot open content created by a Windows Live ID authenticated account.
Never allow users to specify groups when restricting permission for documents	Return an error when users select a group in the **Permission** dialog box: "You cannot publish content to Distribution Lists. You may only specify e-mail addresses for individual users."

IRM option	Description
Prevent users from changing permission on rights managed content	If enabled, users can consume content that already includes IRM permissions, but cannot apply IRM permissions to new content nor configure the rights on a document.
Specify Permission Policy Path	Display in the **Permission** dialog box permission policy templates found in the folder that is specified.
Turn off Information Rights Management user interface	Disable all Rights Management-related options within the user interface of all Office applications.
URL for location of document templates displayed when applications do not recognize rights-managed documents	Provide the path of a folder that contains customized plain-text wrapper templates to be used by previous versions of Office that do not support rights-managed content.

For more information about how to customize these settings, see Configure Information Rights Management in Office 2010 (*http://technet.microsoft.com/library/27c84179-87fd-483e-a34d-806c4646ce9d(Office.14).aspx*).

Office 2010 IRM registry key options

The following IRM registry settings are located in **HKCU\Software\Microsoft\Office\14.0\Common\DRM**.

Registry entry	Type	Value	Description
CorpCertificationServer	String	URL to corporate certification server	Typically, Active Directory is used to specify the RMS server. This setting lets you override the location of the Windows RMS specified in Active Directory for certification.
RequestPermission	DWORD	1 = The box is checked. 0 = The box is cleared.	This registry key toggles the default value of the **Users can request additional permissions from** check box.
CloudCertificationServer	String	URL to custom cloud certification server	No corresponding Group Policy setting.

Registry entry	Type	Value	Description
CloudLicenseServer	String	URL of the licensing server	No corresponding Group Policy setting.
DoNotUseOutlookByDefault	DWORD	0 = Outlook is used 1 = Outlook is not used	The **Permission** dialog box uses Outlook to validate e-mail addresses entered in that dialog box. This causes an instance of Outlook to be started when restricting permissions. Disable the option by using this key.

The following IRM registry setting is located in **HKCU\Software\Microsoft\Office\12.0\Common\DRM\LicenseServers**. There is no corresponding Group Policy setting.

Registry entry	Type	Value	Description
LicenseServers	Key/Hive. Contains DWORD values that have the name of a license server.	Set to the server URL. If the value of the DWORD is 1, Office will not prompt to obtain a license (it will only get it). If the value is zero or there is no registry entry for that server, Office prompts for a license.	Example: If 'http://contoso.com/_wmcs/licensing = 1' is a value for this setting, a user trying to obtain a license from that server to open a rights-managed document would not be prompted for a license.

The following IRM registry setting is located in **HKCU\Software\Microsoft\Office\12.0\Common\Security**. There is no corresponding Group Policy setting.

Registry entry	Type	Value	Description
DRMEncryptProperty	DWORD	1 = The file metadata is encrypted. 0 = The metadata is stored in plaintext. The default value is 0.	Specify whether to encrypt all metadata stored inside a rights-managed file.

For Open XML Formats (for example, docx, xlsx, pptx, and so on), users can decide to encrypt the Microsoft Office metadata stored inside a rights-managed file. Users can encrypt all Office metadata. This includes hyperlink references, or leave content as not encrypted so other applications can access the data.

Users can choose to encrypt the metadata by setting a registry key. You can set a default option for users by deploying the registry setting. There is no option for encrypting some of the metadata: all metadata is encrypted or none is encrypted.

In addition, the **DRMEncryptProperty** registry setting does not determine whether non-Office client metadata storage — such as the storage that is created in Microsoft SharePoint 2010 Products — is encrypted.

This encryption choice does not apply to Microsoft Office 2003 or other previous file formats. Office 2010 handles earlier formats in the same manner as 2007 Office system and Microsoft Office 2003.

Configuring IRM settings for Outlook 2010

In Outlook 2010, users can create and send e-mail messages that have restricted permission to help prevent messages from being forwarded, printed, or copied and pasted. Office 2010 documents, workbooks, and presentations that are attached to messages that have restricted permission are also automatically restricted.

As an Microsoft Outlook administrator, you can configure several options for IRM e-mail, such as disabling IRM or configuring local license caching.

The following IRM settings and features can be useful when you configure rights-managed e-mail messaging:

- Configure automatic license caching for IRM.
- Help enforce an e-mail message expiration period.
- Do not use Outlook for validating e-mail addresses for IRM permissions.

Note:
To disable IRM in Outlook, you must disable IRM for all Office applications. There is no separate option to disable IRM only in Outlook.

Outlook 2010 IRM settings

You can lock down most settings to customize IRM for Outlook by using the Outlook Group Policy template (Outlk14.adm) or the Office Group Policy template (Office14.adm). Or, you can configure default settings for most options by using the Office Customization Tool (OCT), which enables users to configure the settings. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

Location	IRM option	Description
Microsoft Outlook 2010\Miscellaneous	Do not download rights permissions license information for IRM e-mail during Exchange folder sync	Enable to prevent license information from being cached locally. If enabled, users must connect to the network to retrieve license information to open rights-managed e-mail messages.
Microsoft Outlook 2010\Outlook Options\ E-mail Options\ Advanced E-mail Options	When sending a message	To enforce e-mail expiration, enable and enter the number of days before a message expires. The expiration period is enforced only when users send rights-managed e-mail and then the message cannot be accessed after the expiration period.

For more information about how to customize these settings, see Configure Information Rights Management in Office 2010 (*http://technet.microsoft.com/library/27c84179-87fd-483e-a34d-806c4646ce9d(Office.14).aspx*).

Outlook 2010 IRM registry key options

The **Permission** dialog box uses Outlook to validate e-mail addresses that are entered in that dialog box. This causes an instance of Outlook to start when permissions are restricted. You can disable this option by using the registry key that is listed in the following table. There is no corresponding Group Policy or OCT setting for this option.

The following IRM registry setting is located in **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\DRM**.

Registry entry	Type	Value	Description
DoNotUseOutlookByDefault	DWORD	0 = Outlook is used 1 = Outlook is not used	Disable the option by using this key.

See Also

Configure Information Rights Management in Office 2010
(*http://technet.microsoft.com/library/27c84179-87fd-483e-a34d-806c4646ce9d(Office.14).aspx*)

Windows Server 2003 Rights Management Services (RMS)
(*http://go.microsoft.com/fwlink/?LinkId=73121*)

Windows Server 2008 Active Directory Rights Management Services
(*http://go.microsoft.com/fwlink/?LinkId=180006*)

Understanding Information Rights Management: Exchange 2010 Help
(*http://go.microsoft.com/fwlink/?LinkId=183062*)

Plan document libraries (Windows SharePoint Services)
(*http://go.microsoft.com/fwlink/?LinkId=183051*)

Security articles for end users (Office 2010)

IT pros can share the Microsoft Office 2010 security resources that are listed in this article with end users in their organizations. These resources include articles, videos, and training courses that are designed to assist end users who use Product Short Name 2010 applications. The resources are listed in a series of tables that are organized into the following categories:

- **Overview**
- **New Security Features**
- **Outlook/Access/Excel/PowerPoint/Visio/Word**
- **Access only**

To see a list of all security and privacy related articles for a specific program, such as Word, PowerPoint, or another Office program, go to the Office.com (*http://go.microsoft.com/fwlink/?LinkId=205394*) website, select the **support** tab, select **All Support**, select the application you want, and then select **Security and privacy**.

Overview

Resource	Description
Office 2010 Security: Protecting your files (*http://go.microsoft.com/fwlink/?LinkId=202501*)	Self-paced training that assists the user in becoming familiar with the security features that help protect files in Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.
View my options and settings in the Trust Center (*http://go.microsoft.com/fwlink/?LinkId=202800*)	Discusses the Trust Center, where you can find security and privacy settings for Office 2010 programs.

New Security Features

Resource	Feature
What is Protected View? (*http://go.microsoft.com/fwlink/?LinkId=202497*)	**Protected View**, a new security feature in Office 2010 that helps protect your computer by opening files in a restricted environment so they can be examined before they are opened for editing in Excel, PowerPoint, or Word.

Resource	Feature
Office 2010 Security video: file validation (*http://go.microsoft.com/fwlink/?LinkId=202789*)	**Office File Validation**, a new security feature in Office 2010 that helps protect your computer by scanning and validating Office binary file formats before they are opened.

Outlook

Resource	Description
How Outlook helps protect you from viruses, spam, and phishing (*http://go.microsoft.com/fwlink/?LinkId=202522*)	Describes how Outlook 2010 helps protect your computer from viruses, spam, and phishing.
Blocked attachments in Outlook	Describes the default behavior of Outlook 2010, which does not allow you to receive certain kinds of files as attachments.
Encrypt e-mail messages (*http://go.microsoft.com/fwlink/?LinkID=188575*)	Explains how message encryption works in Outlook 2010 and includes procedures for encrypting e-mail messages.
Introduction to IRM for e-mail messages (*http://go.microsoft.com/fwlink/?LinkId=203142*)	Explains what Information Rights Management (IRM) is and how you can use it to restrict permission to content in e-mail messages in Microsoft Outlook.

Access, Excel, PowerPoint, Visio, and Word

Resource	Description
Enable or disable ActiveX settings in Office files (*http://go.microsoft.com/fwlink/?LinkId=202803*)	Explains how to work with ActiveX controls that are in your files, how to change their settings, and how to enable or disable them by using the Message Bar and the Trust Center.
Enable or disable macros in Office files (*http://go.microsoft.com/fwlink/?LinkId=202804*)	Describes the risks involved when you work with macros, and how to enable or disable macros in the Trust Center.
Trusted documents (*http://go.microsoft.com/fwlink/?LinkId=202805*)	Explains what trusted documents are, when to use them, and how to configure their settings.

Resource	Description
Add, remove, or modify a trusted location for your files (*http://go.microsoft.com/fwlink/?LinkId=202806*)	Describes trusted locations, how and where you can create them, and the precautions that you should take before you use a trusted location.
Active content types in your files (*http://go.microsoft.com/fwlink/?LinkId=202807*)	Lists active-content types that can be blocked by the Trust Center and cause Message Bars to appear when you open files. Active content types include macros, add-ins, and data connections.

Access only

Resource	Description
Introduction to Access 2010 security (*http://go.microsoft.com/fwlink/?LinkId=204464*)	Summarizes the security features that are offered by Access 2010, and explains how to use the tools that Access provides for helping to secure a database.
Decide whether to trust a database (*http://go.microsoft.com/fwlink/?LinkId=204613*)	Discusses how trust works in Access 2010, how it differs from security in earlier versions of Access, and what factors that you should consider when you decide whether to trust a database.
Set or change Access 2003 user-level security in Access 2010 (*http://go.microsoft.com/fwlink/?LinkId=204614*)	Explains how the Access 2003 security features work, and how to start and use them in Access 2010.
How database objects behave when trusted and untrusted (*http://go.microsoft.com/fwlink/?LinkId=204615*)	Explains how, by default, Access 2010 disables several database objects unless you apply a digital signature to them or you place the database in a trusted location. The article also lists the components that Access disables.
Show trust by adding a digital signature (*http://go.microsoft.com/fwlink/?LinkId=204616*)	Explains how to create your own security certificate to show that you believe that a database is safe and that its content can be trusted.

Plan Group Policy for Office 2010

Group Policy is an infrastructure that is used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers in an Active Directory directory service environment. The Group Policy infrastructure consists of a Group Policy engine and several individual extensions. These extensions are used to configure Group Policy settings, either by modifying the registry through the Administrative Templates extension, or setting Group Policy settings for security settings, software installation, folder redirection, Internet Explorer Maintenance, wireless network settings, and other areas. This section provides information for IT administrators who plan to use Group Policy to configure and enforce settings for Microsoft Office 2010 applications.

In this section:

Article	Description
Group Policy overview for Office 2010	Provides a brief overview of how to use Group Policy to configure and enforce settings for Office 2010 applications.
Planning for Group Policy in Office 2010	Discusses the key planning steps for managing Office 2010 applications by using Group Policy.
FAQ: Group Policy (Office 2010)	Provides answers to common questions about how Group Policy works with Office 2010
Downloadable book: Group Policy for Office 2010	Provides a description of and a link to the downloadable book *Group Policy for Office 2010*.

Group Policy overview for Office 2010

This article provides a brief overview of Group Policy concepts. The intended audience for this article is the IT administrator who plans to use Group Policy to configure and enforce settings for Microsoft Office 2010 applications.

In this article:

Local and Active Directory-based Group Policy

Group Policy is an infrastructure that is used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers in an Active Directory directory service environment. The Group Policy infrastructure consists of a Group Policy engine and several individual extensions. These extensions are used to configure Group Policy settings, either by modifying the registry through the Administrative Templates extension, or setting Group Policy settings for security settings, software installation, folder redirection, Internet Explorer Maintenance, wireless network settings, and other areas.

Each installation of Group Policy consists of two extensions:

- A server-side extension of the Group Policy Object Editor Microsoft Management Console (MMC) snap-in, used to define and set the policy settings applied to client computers.
- A client-side extension that the Group Policy engine calls to apply policy settings.

Group Policy settings are contained in Group Policy objects (GPOs), which are linked to selected Active Directory containers such as sites, domains, or organizational units (OUs). When a GPO is created, it is stored in the domain. When the GPO is linked to an Active Directory container, such as an OU, the link is a component of that Active Directory container. The link is not a component of the GPO. The settings within GPOs are evaluated by the affected targets by using the hierarchical nature of Active Directory. For example, you can create a GPO named *Office 2010 settings* that contains only configurations for Office 2010 applications. You can then apply that GPO to a specific site so that users contained in that site receive the Office 2010 configurations that you specified in the *Office 2010 settings* GPO.

Every computer has a local GPO that is always processed, regardless of whether the computer is a member of a domain or is a stand-alone computer. The local GPO cannot be blocked by domain-based

GPOs. However, settings in domain GPOs always take precedence, because they are processed after the local GPO.

Note:
Windows Vista, Windows Server 2008, and Windows 7 provide support for managing multiple local GPOs on stand-alone computers. For more information, see Step-by-Step Guide to Managing Multiple Local Group Policy Objects (*http://go.microsoft.com/fwlink/?LinkId=182215*).

Although you can configure local GPOs on individual computers, maximum benefits of Group Policy are obtained in a Windows Server 2003 or Windows Server 2008-based network that has Active Directory installed.

Group Policy processing

Group Policy for computers is applied at computer startup. Group Policy for users is applied when users log on. In addition to the initial processing of Group Policy at startup and logon, Group Policy is applied subsequently in the background periodically. During a background refresh, a client-side extension reapplies the policy settings only if it detects that a change occurred on the server in any of its GPOs or its list of GPOs. For software installation and folder redirection, Group Policy processing occurs only during computer startup or user logon.

Group Policy settings are processed in the following order:

- **Local GPO** Each computer has a GPO that is stored locally. This GPO processes for both computer and user Group Policy.
- **Site** GPOs linked to the site to which the computer belongs are processed next. Processing is completed in the order specified by the administrator, on the **Linked Group Policy Objects** tab for the site in Group Policy Management Console (GPMC). The GPO that has the lowest link order is processed last and has the highest precedence. For information about how to use GPMC, see Group Policy management tools later in this article.
- **Domain** Multiple domain-linked GPOs are processed in the order specified by the administrator, on the **Linked Group Policy Objects** tab for the domain in GPMC. The GPO that has the lowest link order is processed last and has the highest precedence.
- **Organizational units** GPOs linked to the OU that is highest in the Active Directory hierarchy are processed first, and then GPOs that are linked to its child OU are processed, and so on. GPOs linked to the OU that contains the user or computer are processed last.

The processing order is subject to the following conditions:

- Windows Management Instrumentation (WMI) or security filtering applied to GPOs.
- Any domain-based GPO (not local GPO) can be enforced by using the **Enforce** option, so that its policy settings cannot be overwritten. Because an Enforced GPO is processed last, no other settings can write over the settings in that GPO. If more than one Enforced GPO exists, the same setting in each GPO can be set to a different value. In this case, the link order of the GPOs determines which GPO contains the final settings.

- At any domain or OU, Group Policy inheritance can be selectively designated as **Block Inheritance**. However, because Enforced GPOs are always applied and cannot be blocked, blocking inheritance does not prevent the application of policy settings from Enforced GPOs.

Policy inheritance

Policy settings in effect for a user and computer are the result of the combination of GPOs applied at a site, domain, or OU. When multiple GPOs apply to users and computers in those Active Directory containers, the settings in the GPOs are aggregated. By default, settings deployed in GPOs linked to higher-level containers (parent containers) in Active Directory are inherited to child containers and combine with settings deployed in GPOs linked to the child containers. If multiple GPOs attempt to set a policy setting that has conflicting values, the GPO with the highest precedence sets the setting. GPOs that are processed later have precedence over GPOs that are processed earlier.

Synchronous and asynchronous processing

Synchronous processes can be described as a series of processes in which one process must finish running before the next one begins. Asynchronous processes can run on different threads at the same time, because their outcome is independent of other processes. Administrators can use a policy setting for each GPO to change the default processing behavior so that processing is asynchronous instead of synchronous.

Under synchronous processing, there is a time limit of 60 minutes for all of Group Policy to finish processing on the client computer. Client-side extensions that have not finished processing after 60 minutes are signaled to stop. In this case, the associated policy settings might not be fully applied.

Fast Logon Optimization feature

By default, the Fast Logon Optimization feature is set for both domain and workgroup members. The result is the asynchronous application of policy when the computer starts and the user logs on. This application of policy is similar to a background refresh. It can reduce the length of time it takes for the logon dialog box to appear and the length of time it takes for the desktop to become available to the user.

Administrators can disable the Fast Logon Optimization feature by using the **Always wait for the network at computer startup and logon** policy setting, which is accessed in the **Computer Configuration\Administrative Templates\System\Logon** node of Group Policy Object Editor.

Slow links processing

Some Group Policy extensions are not processed when the connection speed falls below specified thresholds. The default value for what Group Policy considers a slow link is any rate slower than 500 Kilobits per second (Kbps).

Group Policy refresh interval

By default, Group Policy is processed every 90 minutes, with a randomized delay of up to 30 minutes — for a total maximum refresh interval of up to 120 minutes.

For security settings, after you have edited security settings policies, the policy settings are refreshed on the computers in the OU to which the GPO is linked:

- When a computer restarts.
- Every 90 minutes on a workstation or server and every 5 minutes on a domain controller.
- By default, security policy settings delivered by Group Policy are also applied every 16 hours (960 minutes), even if a GPO has not changed.

Triggering a Group Policy refresh

Changes made to the GPO must first replicate to the appropriate domain controller. Therefore, changes to Group Policy settings might not be immediately available on users' desktops. In some scenarios, such as application of security policy settings, it might be necessary to apply policy settings immediately.

Administrators can trigger a policy refresh manually from a local computer without waiting for the automatic background refresh. To do this, administrators can type **gpupdate** at the command line to refresh the user or computer policy settings. You cannot use GPMC to trigger a policy refresh.

The **gpupdate** command triggers a background policy refresh on the local computer from which the command is run. The **gpupdate** command is used in Windows Server 2003 and Windows XP environments.

The application of Group Policy cannot be pushed to clients on demand from the server.

Changing how Group Policy processes GPOs

The primary method for specifying which users and computers receive the settings from a GPO is by linking the GPO to sites, domains, and OUs.

You can change the default order by which GPOs are processed by using any of the following methods:

- Change the link order.
- Block inheritance.
- Enforce a GPO link.
- Disable a GPO link.
- Use security filtering.
- Use Windows Management Instrumentation (WMI) filtering.
- Use loopback processing.

Each of these methods is described in the following subsections.

Change the link order

The GPO link order in a site, domain, or OU controls when links are applied. Administrators can change the precedence of a link by changing the link order, that is, by moving each link up or down in the list to the appropriate location. The link that has the higher order (1 is the highest order) has the higher precedence for a site, domain, or OU.

Block inheritance

Applying block inheritance to a domain or OU prevents GPOs linked to higher sites, domains, or organizational units from being automatically inherited by the child-level Active Directory container.

Enforce a GPO link

You can specify that the settings in a GPO link take precedence over the settings of any child object by setting that link to **Enforced**. GPO links that are enforced cannot be blocked from the parent container. If GPOs contain conflicting settings and do not have enforcement from a higher-level container, the settings of the GPO links at the higher-level parent container are overwritten by settings in GPOs linked to child OUs. By using enforcement, the parent GPO link always has precedence. By default, GPO links are not enforced.

Disable a GPO link

You can completely block how users apply a GPO for a site, domain, or OU by disabling the GPO link for that domain, site, or OU. This does not disable the GPO. If the GPO is linked to other sites, domains, or OUs, they will continue to process the GPO if the links are enabled.

Use security filtering

You can use security filtering to specify that only specific security principles in a container where the GPO is linked apply the GPO. Administrators can use security filtering to narrow the scope of a GPO so that the GPO applies only to a single group, user, or computer. Security filtering cannot be used selectively on different settings in a GPO.

The GPO applies to a user or computer only if that user or computer has both **Read** and **Apply Group Policy** permissions on the GPO, either explicitly or effectively through group membership. By default, all GPOs have **Read** and **Apply Group Policy** set to **Allowed** for the Authenticated Users group, which includes users and computers. This is how all authenticated users receive the settings of a new GPO when the GPO is applied to an OU, domain, or site.

By default, Domain Admins, Enterprise Admins, and the local system have full control permissions, without the **Apply Group Policy** access-control entry (ACE). Administrators are also members of Authenticated Users. This means that, by default, administrators receive the settings in the GPO. These

permissions can be changed to limit the scope to a specific set of users, groups, or computers within the OU, domain, or site.

The Group Policy Management Console (GPMC) manages these permissions as a single unit and displays the security filtering for the GPO on the **GPO Scope** tab. In GPMC, groups, users, and computers can be added or removed as security filters for each GPO.

Use Windows Management Instrumentation filtering

You can use Windows Management Instrumentation (WMI) filtering to filter the application of a GPO by attaching a WMI Query Language (WQL) query to a GPO. The queries can be used to query WMI for multiple items. If a query returns true for all queried items, the GPO is applied to the target user or computer.

A GPO is linked to a WMI filter and applied on a target computer, and the filter is evaluated on the target computer. If the WMI filter evaluates to false, the GPO is not applied (except if the client computer is running Windows 2000. In this case, the filter is ignored and the GPO is always applied). If the WMI filter evaluates to true, the GPO is applied.

The WMI filter is a separate object from the GPO in the directory. A WMI filter must be linked to a GPO to apply, and a WMI filter and the GPO to which it is linked must be in the same domain. WMI filters are stored only in domains. Each GPO can have only one WMI filter. The same WMI filter can be linked to multiple GPOs.

Note:
WMI is the Microsoft implementation of the Web-Based Enterprise Management industry initiative that establishes management infrastructure standards and lets you combine information from various hardware and software management systems. WMI exposes hardware configuration data such as CPU, memory, disk space, and manufacturer, and also software configuration data from the registry, drivers, file system, Active Directory, the Windows Installer service, networking configuration, and application data. Data about a target computer can be used for administrative purposes, such as WMI filtering of GPOs.

Use loopback processing

You can use this feature to ensure that a consistent set of policy settings is applied to any user who logs on to a specific computer, regardless of the user's location in Active Directory.

Loopback processing is an advanced Group Policy setting that is useful on computers in some closely managed environments, such as servers, kiosks, laboratories, classrooms, and reception areas. Setting loopback causes the **User Configuration** policy settings in GPOs that apply to the computer to be applied to every user logging on to that computer, instead of (in **Replace** mode) or in addition to (in **Merge** mode) the **User Configuration** settings of the user.

To set loopback processing, you can use the **User Group Policy loopback processing mode** policy setting, which is accessed under **Computer Configuration\Administrative Templates\System\Group Policy** in Group Policy Object Editor.

To use the loopback processing feature, both the user account and the computer account must be in a domain running Windows Server 2003 or a later version of Windows. Loopback processing does not work for computers that are joined to a workgroup.

Administrative Templates

The Administrative Templates extension of Group Policy consists of an MMC server-side snap-in that is used to configure policy settings and a client-side extension that sets registry keys on target computers. Administrative Templates policy is also known as registry-based policy or registry policy.

Administrative Template files

Administrative Template files are Unicode files that consist of a hierarchy of categories and subcategories to define how options display through the Group Policy Object Editor and GPMC. They also indicate the registry locations that are affected by policy setting configurations, which include the default (not configured), enabled, or disabled values of the policy setting. The templates are available in three file versions: .adm, .admx, and .adml. The .adm files can be used for computers that are running any Windows operating system. The .admx and .adml files can be used on computers that are running at least Windows Vista or Windows Server 2008. The .adml files are the language-specific versions of .admx files.

The functionality of the administrative template files is limited. The purpose of .adm, .admx, or .adml template files is to enable a user interface to configure policy settings. Administrative Template files do not contain policy settings. The policy settings are contained in Registry.pol files that are located in the Sysvol folder on domain controllers.

The Administrative Templates server-side snap-in provides an **Administrative Templates** node that appears in Group Policy Object Editor under the **Computer Configuration** node and under the **User Configuration** node. The settings under **Computer Configuration** manipulate registry settings for the computer. Settings under **User Configuration** manipulate registry settings for users. Although some policy settings require simple UI elements such as text boxes to enter values, most policy settings contain only the following options:

- **Enabled** The policy is enforced. Some policy settings provide additional options that define the behavior when the policy is activated.
- **Disabled** Enforces the opposite behavior as the **Enabled** state for most policy settings. For example, if **Enabled** forces a feature's state to **Off**, **Disabled** forces the feature's state to **On**.
- **Not configured** The policy is not enforced. This is the default state for most settings.

The Administrative Template files are stored in the locations on the local computer, as shown in the following table.

File type	Folder
.adm	%systemroot%\Inf
.admx	%systemroot%\PolicyDefinitions
.adml	%systemroot%\PolicyDefinitions\<language-specific folder, e.g., *en-us*>

You can also store and use .admx and .adml files from a central store in the folders on the domain controller, as shown in the following table.

File type	Folder
.admx	%systemroot%\sysvol\domain\policies\PolicyDefinitions
.adml	%systemroot%\sysvol\domain\policies\PolicyDefinitions\<language-specific folder, for example, *en-us*>

For more information about how to store and use the templates from a central store, see “Group policy and sysvol” in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).

Administrative Template files for Office 2010

Administrative Template files specifically for Office 2010 are available as a separate download and let you:

- Control entry points to the Internet from Office 2010 applications.
- Manage security in the Office 2010 applications.
- Hide settings and options that are unnecessary for users to perform their jobs and that might distract them or result in unnecessary support calls.
- Create a highly managed standard configuration on users’ computers.

To download the Office 2010 administrative templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*).

The Office 2010 Administrative Templates are as shown in the following table.

Application	Administrative Template files
Microsoft Access 2010	access14.admx, access14.adml, access14.adm
Microsoft Excel 2010	excel14.admx, excel14.adml, excel14.adm
Microsoft InfoPath 2010	inf14.admx, inf14.adml, inf14.adm
Microsoft Office 2010	office14.admx, office14.adml, office14.adm
Microsoft OneNote 2010	onent14.admx, onent14.adml, onent14.adm
Microsoft Outlook 2010	outlk14.admx, outlk14.adml, outlk14.adm
Microsoft PowerPoint 2010	ppt14.admx, ppt14.adml, ppt14.adm
Microsoft Project 2010	proj14.admx, proj14.adml, proj14.adm
Microsoft Publisher 2010	pub14.admx, pub14.adml, pub14.adm
Microsoft SharePoint Designer 2010	spd14.admx, spd14.adml, spd14.adm
Microsoft SharePoint Workspace 2010	spw14.admx, spw14.adml, spw14.adm
Microsoft Visio 2010	visio14.admx, visio14.adml, visio14.adm
Microsoft Word 2010	word14.admx, word14.adml, word14.adm

True policies vs. user preferences

Group Policy settings that administrators can fully manage are known as *true policies*. Settings that users can configure (but might reflect the default state of the operating system at installation time) are known as *preferences*. Both true policies and preferences contain information that modifies the registry on users' computers.

True policies

Registry values for true policies are stored under the approved registry keys for Group Policy. Users cannot change or disable these settings.

For computer policy settings:

- **HKEY_LOCAL_MACHINE\Software\Policies** (the preferred location)
- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies**

For user policy settings:

- **HKEY_CURRENT_USER\Software\Policies** (the preferred location)

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies**

For Office 2010, true policies are stored in the following registry locations.

For computer policy settings:

- **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\14.0**

For user policy settings:

- **HKEY_CURRENT_USER\Software\Policies\ Microsoft\Office\14.0**

Preferences

Preferences are set by users or by the operating system at installation time. The registry values that store preferences are located *outside* the approved Group Policy keys. Users can change their preferences.

If you configure preference settings by using a GPO, it does not have system access control list (SACL) restrictions. Therefore, users might be able to change these values in the registry. When the GPO goes out of scope (if the GPO is unlinked, disabled, or deleted), these values are not removed from the registry.

To view preferences in Group Policy Object Editor, click the **Administrative Templates** node, click **View**, click **Filtering**, and then clear the **Only show policy settings that can be fully managed** check box.

Group Policy management tools

Administrators use the following tools to administer Group Policy:

- **Group Policy Management Console** Used to manage most Group Policy management tasks.
- **Group Policy Object Editor** Used to configure policy settings in GPOs.

Group Policy Management Console

Group Policy Management Console (GPMC) simplifies the management of Group Policy by providing a single tool to manage core aspects of Group Policy, such as scoping, delegating, filtering, and manipulating inheritance of GPOs. GPMC can also be used to back up (export), restore, import, and copy GPOs. Administrators can use GPMC to predict how GPOs will affect the network and to determine how GPOs have changed settings on a computer or user. GPMC is the preferred tool for managing most Group Policy tasks in a domain environment.

GPMC provides a view of GPOs, sites, domains, and OUs across an enterprise, and can be used to manage either Windows Server 2003 or Windows 2000 domains. Administrators use GPMC to perform all Group Policy management tasks, except for configuring individual policy settings in Group Policy objects. This is performed with Group Policy Object Editor, which you open within GPMC.

Administrators use GPMC to create a GPO and has no initial settings. An administrator can also create a GPO and link the GPO to an Active Directory container at the same time. To configure individual

settings in a GPO, an administrator edits the GPO by using Group Policy Object Editor from within GPMC. Group Policy Object Editor is displayed with the GPO loaded.

An administrator can use GPMC to link GPOs to sites, domains, or OUs in Active Directory. Administrators must link GPOs to apply settings to users and computers in Active Directory containers.

GPMC includes the following Resultant Set of Policies (RSoP) features that are provided by Windows:

- **Group Policy Modeling** Simulates which policy settings are applied under circumstances specified by an administrator. Administrators can use Group Policy Modeling to simulate the RSoP data that would be applied for an existing configuration, or they can analyze the effects of simulated, hypothetical changes to the directory environment.
- **Group Policy Results** Represents the actual policy data that is applied to a computer and user. Data is obtained by querying the target computer and retrieving the RSoP data that was applied to that computer. The Group Policy Results capability is provided by the client operating system and requires Windows XP, Windows Server 2003, or later versions of the operating system.

Group Policy Object Editor

Group Policy Object Editor is an MMC snap-in that is used to configure policy settings in GPOs. The Group Policy Object Editor is contained in gpedit.dll, and is installed with Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 operating systems.

To configure Group Policy settings for a local computer that is not a member of a domain, use Group Policy Object Editor to manage a local GPO (or multiple GPOs in computers that are running Windows Vista, Windows 7, or Windows Server 2008). To configure Group Policy settings in a domain environment, GPMC (which invokes Group Policy Object Editor) is the preferred tool for Group Policy management tasks.

Group Policy Object Editor gives administrators a hierarchical tree structure for configuring Group Policy settings in GPOs, and consists of the following two main nodes:

- **User Configuration** Contains settings that are applied to users when users log on and periodic background refresh.
- **Computer Configuration** Contains settings that are applied to computers at startup and periodic background refresh.

These two main nodes are additionally divided into folders that contain the different kinds of policy settings that can be set. These folders include the following:

- **Software Settings** Contains software installation settings.
- **Windows Settings** Contains Security settings and Scripts policy settings.
- **Administrative Templates** Contains registry-based policy settings

System requirements for GPMC and Group Policy Object Editor

The Group Policy Object Editor is part of GPMC and is invoked when you edit a GPO. You can run GPMC on Windows XP, Windows Server 2003, Windows Vista, Windows 7, and Windows Server 2008. The requirements vary per Windows operating system as follows:

- GPMC is part of the Windows Vista operating system. However if you have installed Service Pack 1 or Service Pack 2 on Windows Vista, GPMC is removed. To reinstall it, install the Microsoft Remote Server Administration Tools for Windows Vista (*http://go.microsoft.com/fwlink/?LinkId=89361*).
- The GPMC is included with Windows Server 2008 and later. However, this feature is *not* installed with the operating system. Use Server Manager to install the GPMC. For information about how to install GPMC, see Install the GPMC (*http://go.microsoft.com/fwlink/?LinkID=187926*).
- To install GPMC on Windows 7, install the Remote Server Administration Tools for Windows 7 (*http://go.microsoft.com/fwlink/?LinkId=180743*).
- To install GPMC on Windows XP or Windows Server 2003, install the Group Policy Management Console with Service Pack 1 (*http://go.microsoft.com/fwlink/?LinkId=88316*).

For more information about how to use GPMC and the Group Policy Object Editor, see Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*).

Office Customization Tool and Group Policy

Administrators can use either the Office Customization Tool (OCT) or Group Policy to customize user configurations for Office 2010 applications:

- **Office Customization Tool (OCT)** Used to create a Setup customization file (.msp file). Administrators can use the OCT to customize features and configure user settings. Users can modify most of the settings after the installation. This is because the OCT configures settings in publicly available parts of the registry, such as **HKEY_CURRENT_USER/Software/Microsoft/Office/14.0**. This tool is typically used in organizations that do not manage desktop configurations centrally. For more information, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).
- **Group Policy** Used to configure the Office 2010 policy settings that are contained in Administrative Templates, and the operating system enforces those policy settings. In an Active Directory environment, administrators can apply policy settings to groups of users and computers in a site, domain, or OU to which a Group Policy object is linked. True policy settings are written to the approved registry keys for policy, and these settings have SACL restrictions that prevent users who are not administrators from changing them. Administrators can use Group Policy to create highly managed desktop configurations. They can also create lightly managed configurations to address the business and security requirements of their organizations. For more information about the OCT, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

See Also

Windows Server Group policy (*http://go.microsoft.com/fwlink/?LinkId=177635*)

Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*)

Group Policy Documentation Survival Guide (*http://go.microsoft.com/fwlink/?LinkId=116313*)

Planning for Group Policy in Office 2010

Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*)

Planning for Group Policy in Office 2010

This article discusses the key planning steps for managing Microsoft Office 2010 applications by using Group Policy.

In this article:

Planning for Group Policy

Group Policy enables IT administrators to apply configurations or policy settings to users and computers in an Active Directory directory service environment. Configurations can be made specifically to Office 2010. For more information, see Group Policy overview for Office 2010.

Planning for the deployment of Group Policy-based solutions includes several steps:

1. Define your business objectives and security requirements.
2. Evaluate your current environment.
3. Design managed configurations based on your business and security requirements.
4. Determine the scope of application of your solution.
5. Plan for testing, staging, and deploying your Group Policy solution.
6. Involving key stakeholders in planning and deploying the solution.

Define business objectives and security requirements

Identify your specific business and security requirements and determine how Group Policy can help you manage standard configurations for the Office 2010 applications. Identify the resources (groups of users and computers) for which you are managing Office settings by using Group Policy and define the scope of your project.

Evaluate your current environment

Examine how you currently perform management tasks related to configurations for Microsoft Office applications to help you determine which kinds of Office policy settings to use. Document the current practices and requirements. You will use this information to help you design managed configurations, in the next step. Items to include are as follows:

- Existing corporate security policies and other security requirements. Identify which locations and publishers are considered secure. Evaluate your requirements for managing Internet Explorer feature control settings, document protection, privacy options, and blocking file format settings.
- Messaging requirements for the organization. Evaluate requirements for configuring user interface settings, virus-prevention, and other security settings for Office Outlook 2007 by using Group Policy. For example, Group Policy provides settings for limiting the size of .pst files, which can improve performance on the workstation.
- User requirements for Office applications for the various kinds of user roles. This depends largely on users' job requirements and the organization's security requirements.
- Default file save options to use for Microsoft Access 2010, Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.
- Access restrictions to set for Office 2010 user interface items; for example, including disabling commands, menu items, and keyboard shortcuts.
- Software installation issues, if you are considering this deployment method. Although Group Policy can be used to install software applications in small-sized organizations that have Active Directory installed, there are some limitations, and you must determine whether it is an appropriate solution for your deployment requirements. For more information, see "Identifying issues pertaining to software installation" in Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).

  If you manage large numbers of clients in a complex or rapidly changing environment, Microsoft System Center Configuration Manager 2010 is the recommended method for installing and maintaining Office 2010 in medium- and large-sized organizations. System Center Configuration Manager 2010 offers additional functionality, including inventory, scheduling, and reporting features.

  Another option for deployment of Office 2010 in Active Directory environments is to use Group Policy computer startup scripts.
- Whether to use Group Policy or the OCT. Although both Group Policy and the OCT can be used to customize user configurations for the Office 2010 applications, there are important differences:
  - Group Policy is used to configure Office 2010 policy settings contained in Administrative Templates, and the operating system enforces those policy settings. These settings have system access control list (SACL) restrictions that prevent non-administrator users from changing them. Use Group Policy for configuring settings that you want to enforce.
  - The OCT is used to create a Setup customization file (.msp file). Administrators can use the OCT to customize features and configure user settings. Users can modify most of the settings

after the installation. We recommend that you use the OCT for preferred or default settings only.

For more information, see Office Customization Tool and Group Policy.

- Whether to use *local* Group Policy to configure Office settings. You can use local Group Policy to control settings in environments that include stand-alone computers that are not part of an Active Directory domain. For more information, see Group Policy overview for Office 2010.

Design managed configurations based on business and security requirements

Understanding your business requirements, security, network, IT requirements, and your organization's current Office application management practices helps you identify appropriate policy settings for managing the Office applications for users in your organization. The information that you collect during the evaluation of your current environment step helps you design your Group Policy objectives.

When you define your objectives for using Group Policy to manage configurations for Office applications, determine the following:

- The purpose of each Group Policy object (GPO).
- The owner of each GPO — the person who is responsible for managing the GPO.
- The number of GPOs to use. Keep in mind that the number of GPOs applied to a computer affects startup time, and the number of GPOs applied to a user affects the amount of time needed to log on to the network. The greater the number of GPOs that are linked to a user — especially the greater the number of settings within those GPOs — the longer it takes to process the GPOs when a user logs on. During the logon process, each GPO from the user's site, domain, and organizational unit (OU) hierarchy is applied, provided both the Read and Apply Group Policy permissions are set for the user.
- The appropriate Active Directory container to which to link each GPO (site, domain, or OU).
- The location of Office applications to install, if you are deploying the Office 2010 with Group Policy Software Installation.
- The location of computer startup scripts to execute, if you are deploying Office 2010 by assigning Group Policy computer startup scripts.
- The kinds of policy settings contained in each GPO. This depends on your business and security requirements and how you currently manage settings for Office applications. We recommend that you configure only settings that are considered critical for stability and security and that you keep configurations to a minimum. Also consider using policy settings that can improve performance on the workstation, such as controlling Outlook .pst file size, for example.
- Whether to set exceptions to the default processing order for Group Policy.
- Whether to set filtering options for Group Policy to target specific users and computers.

To help you plan for ongoing administration of GPOs, we recommend that you establish administrative procedures to track and manage GPOs. This helps ensure that all changes are implemented in a prescribed manner.

Determine the scope of application

Identify Office 2010 policy settings that apply to all corporate users (such as any application security settings that are considered critical to the security of your organization) and those that are appropriate for groups of users based on their roles. Plan your configurations according to the requirements that you identify.

In an Active Directory environment, you assign Group Policy settings by linking GPOs to sites, domains, or OUs. Most GPOs are typically assigned at the organizational unit level, so make sure that your OU structure supports your Group Policy-based management strategy for Office 2010. You might also apply some Group Policy settings at the domain level, such as security-related policy settings or Outlook settings that you want to apply to all users in the domain.

Test and stage Group Policy deployments

Planning for testing and staging is a critical part of any Group Policy deployment process. This step includes creating standard Group Policy configurations for Office 2010 applications and testing the GPO configurations in a *non-production* environment before you deploy to users in the organization. If necessary, you can filter the scope of application of GPOs and define exceptions to Group Policy inheritance. Administrators can use Group Policy Modeling (in Group Policy Management Console) to evaluate which policy settings would be applied by a specific GPO, and Group Policy Results (in Group Policy Management Console) to evaluate which policy settings are in effect.

Group Policy provides the ability to affect configurations across hundreds and even thousands of computers in an organization. Consequently, it is critical that you use a change management process and rigorously test all new Group Policy configurations or deployments in a non-production environment before you move them into your production environment. This process ensures that the policy settings contained in a GPO produce the expected results for the intended users and computers in Active Directory environments.

As a best practice for managing Group Policy implementations, we recommend that you stage Group Policy deployments by using the following pre-deployment process:

- Deploy new GPOs in a test environment that reflects the production environment as closely as possible.
- Use Group Policy Modeling to evaluate how a new GPO will affect users and interoperate with existing GPOs.
- Use Group Policy Results to evaluate which GPO settings are applied in the test environment.

For more information, see “Using Group Policy Modeling and Group Policy Results to evaluate Group Policy settings” in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).

Involve key stakeholders

Group Policy deployments in enterprises are likely to have cross-functional boundaries. As part of preparing for your deployment, it is important to consult key stakeholders from the various functional teams in your organization and ensure they participate during the analysis, design, test, and implementation phases, as appropriate.

Make sure that you conduct reviews of the policy settings that you plan to deploy for managing the Office 2010 applications with your organization's security and IT operations teams to ensure that the configurations suit the organization and that you apply as strict a set of policy settings as necessary to protect the network resources.

See Also

Group Policy overview for Office 2010

Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*)

FAQ: Group Policy (Office 2010)

Find answers to frequently asked questions (FAQ) about Group Policy and Microsoft Office 2010.

Q: When should I use Group Policy instead of Office Configuration Tool (OCT)?

A: Although both Group Policy and the OCT can be used to customize user configurations for the Microsoft Office 2010 applications, each is used for a specific configuration scenario.

- **Group Policy is recommended for settings that you want to enforce**. Group Policy is used to configure Office 2010 policy settings that are contained in Administrative Templates. The operating system enforces those policy settings. Many settings have system access control list (SACL) restrictions that prevent non-administrator users from changing them. In some cases, the settings can be changed by users. See True policies vs. user preferences for more information.
- **OCT is recommended for preferred or default settings only**. The OCT is used to create a Setup customization file (.msp file). Administrators can use the OCT to customize features and configure user settings. Users can configure most of the settings after the installation.

Q: Where can I find a list of Group Policies that are available for Office 2010?

A: Refer to the Microsoft Excel 2010 workbook *Office2010GroupPolicyAndOCTSettings_Reference.xls*, which is available in the **Files in this Download** section on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool download page (*http://go.microsoft.com/fwlink/?LinkID=189156*).

You can download Group Policy-related documentation from the Group Policy for Microsoft Office 2010 download page (*http://go.microsoft.com/fwlink/?LinkId=204009*).

Q: What is the difference between the two workbooks Office2010GroupPolicyAndOCTSettings_Reference.xls and Office2010GroupPolicyAndOCTSettings.xls?

A: Always use *Office2010GroupPolicyAndOCTSettings_Reference.xls*. This workbook is more up-to-date and is available for separate download on the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool download page (*http://go.microsoft.com/fwlink/?LinkID=189156*).

The workbook *Office2010GroupPolicyAndOCTSettings.xls* is integrated into the Group Policy templates download package and is now out-of-date.

Q: What is the difference between .adm, .admx, and .adml administrative template files?

A: These files are designed for use with specific operating systems on the computer that you use to manage Group Policy settings.

- The .adm files can be used by administrative computers that are running any Windows operating system.
- The .admx and .adml files can be used by administrative computers that are running at least Windows Vista or Windows Server 2008. The .adml files are the language-specific versions of .admx files. The .admx files hold the settings, and the .adml files apply the settings for the specific language.

You can find more information about .admx files in the Managing Group Policy ADMX Files Step-by-Step Guide. (*http://go.microsoft.com/fwlink/?LinkID=164569*)

Q: Do the Office 2010 .admx template files work with the 2007 Office system? Or must I download the 2007 Office system template files separately?

A: You must use the template files that match the version of Office that you are deploying. We do not recommend that you use the Office 2010 template files to configure the 2007 Office system.

Q: How do I install the Office 2010 Group Policy templates?

A. Step-by-step instructions for starting Policy Management Console (GPMC), creating a Group Policy Object (GPO), and loading Office 2010 Administrative Templates to a GPO are provided in the topic Enforce settings by using Group Policy in Office 2010 (*http://technet.microsoft.com/library/873a5392-1b1a-47a1-a863-1f29ef116d0e(Office.14).aspx*). The topic describes two locations for storing Group Policy templates:

- In an Administrative Templates *central store* in the Sysvol folder of the domain controller
- In the PolicyDefinitions folder in the local computer

You can find more detailed information about creating a central store in Scenario 2: Editing Domain-Based GPOs Using ADMX Files (*http://go.microsoft.com/fwlink/?LinkId=207184*).

If you want to take a quick look at the templates on your local computer, follow these steps after you download the template files:

To view the .admx and .adml template files on a computer that runs at least Windows Vista or Windows Server 2008

1. Copy the .admx and .adml files to the PolicyDefinitions folder in the local computer:
   a. Copy .admx files to this location: %systemroot%\PolicyDefinitions (for example, C:\Windows\PolicyDefinitions)
   b. Copy .adml files to this location: %systemroot%\PolicyDefinitions*ll-cc* (where *ll-cc* represents the language identifier, such as en-us for English United States)
2. Open the gpedit.msc console and expand **Administrative Templates** (under **Computer Configuration** and **User Configuration**) to view the Office 2010 policies.

To view the .adm template files on a computer that is running any Windows operating system

1. Open the gpedit.msc console, right-click **Administrative Templates** in the Computer Configuration or User Configuration node, and then select **Add/Remove Templates**.
2. Click **Add** and locate the folder on your computer where you stored the .adm files.
3. Select the templates that you want in the language of your choice, click **Open**, and then click **Close**. The .adm files are displayed under the respective **Administrate Templates** nodes in a subnode called **Classic Administrative Templates (ADM)**.

Q: How can I map a specific UI element in Office 2010 to a Group Policy setting?

A. Although it has not been updated for Office 2010, a list of 2007 Office system Group Policy settings and associated user interface settings is available as a downloadable workbook. The workbook also provides the associated registry key information for user interface options that are managed by Group Policy settings, and indicates the locations of the Office 2003 user interface elements (such as toolbars and menus) in the 2007 Office system user interface for Access, Excel, Outlook, PowerPoint, and Word. Click the following link to view and download the Office2007PolicySettingsAndUIOptions.xlsx workbook: http://go.microsoft.com/fwlink/?LinkId=106122 (*http://go.microsoft.com/fwlink/?LinkId=106122*).

Q: How can I use Group Policy to disable commands and menu items?

You can use Group Policy settings to disable commands and menu items for Office 2010 applications by specifying the toolbar control ID (TCID) for the Office 2010 controls. You can also disable keyboard shortcuts by setting the **Custom | Disable** shortcut keys policy setting and adding the virtual key code and modifier for the shortcut. A virtual key code is a hardware-independent number that uniquely

identifies a key on the keyboard. A modifier is the value for a modifier key, such as ALT, CONTROL, or SHIFT.

To download a list the control IDs for built-in controls in all applications that use the Ribbon, visit Office 2010 Help Files: Office Fluent User Interface Control Identifiers (*http://go.microsoft.com/fwlink/?LinkID=181052*).

For more information, see Disable user interface items and shortcut keys in Office 2010 (*http://technet.microsoft.com/library/ab942894-fd65-4ebd-ba32-cfc07de97c36(Office.14).aspx*)

Q. Why does Microsoft not support the use of Group Policy Software Installation to deploy Office 2010?

A: Using the Software Installation extension of Group Policy is not supported in Office 2010 because of changes to the Office setup architecture and customization model. If you have an Active Directory environment, you can use a Group Policy computer startup script as an alternative. Group Policy computer startup scripts provide solutions for organizations that need an automated way to deploy Office_2nd_CurrentVer to many computers but who do not have desktop management applications, such as Microsoft System Center Essentials or System Center Configuration Manager or a third-party software management tool.

For more information, see Deploy Office 2010 by using Group Policy computer startup scripts (*http://technet.microsoft.com/library/305a57fb-e616-400c-8b8b-d7789a715910(Office.14).aspx*). For information about all Office deployment methods, see Deploy Office 2010 (*http://technet.microsoft.com/library/90ae3e01-b598-478c-af6f-8d24de33a9c3(Office.14).aspx*).

Q. What are the advantages and limitations of deploying Office 2010 using Group Policy computer startup scripts?

Advantages:

- A script can be written in any language that is supported by the client computer. Windows Script Host-supported languages, such as VBScript and JScript, and command files are the most common.
- Scripts take advantage of Active Directory Domain Services (AD DS) and Group Policy infrastructure.
- AD DS handles the elevation of rights that are required for application installation.
- Administrators can use a similar scripting process to apply updates and service packs for each computer in the domain or organizational unit.
- A script can be written in any language that is supported by the client computer, such as VBScript and JScript, provided they are Windows Script Host-supported languages.

Disadvantages:

- Group Policy invokes the script and has limited awareness of the installation status afterward.
- Product uninstalls and installs for multiple computers have to be done by using a command-line script or batch file.
- It might be difficult to determine exactly which updates and service packs were applied to each client computer.

Downloadable book: Group Policy for Office 2010

Group Policy for Office 2010 provides information about the Group Policy settings for Microsoft Office 2010. The audiences for this book are IT professionals who plan, implement, and maintain Office installations in their organizations.

The content in this book is a copy of selected content in the Office 2010 Resource Kit as of the publication date. For the most current content, see the Office 2010 Resource Kit (*http://technet.microsoft.com/library/9df1c7d2-30a9-47bb-a3b2-5166b394fbf5(Office.14).aspx*) on the web.

Downloadable book: Group Policy for Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=204009*)

Plan for multilanguage deployment of Office 2010

This article discusses planning considerations for deploying Microsoft Office 2010 with multiple languages.

In this article:

Plan Setup

The language-neutral design of Office 2010 helps simplify the deployment of Office products in multiple languages. Instead of creating a series of installations, you enable Setup to coordinate a single installation of multiple language versions.

All language-specific components for a particular language are contained in a Microsoft Office 2010 Language Pack. Each Office 2010 Language Pack includes language-specific folders for all Office 2010 products that are available in that language. Folders are identified by a language tag appended to the folder name. For a complete list of language tags, see Language identifiers and OptionState Id values in Office 2010 (*http://technet.microsoft.com/library/f5fee727-df49-4ef7-b073-dd6c08dfecfa(Office.14).aspx*).

You copy all the Office 2010 Language Packs that you need to a network installation point that contains at least one complete Office 2010 product. By default, Setup automatically installs the language version that matches the Windows user locale that is set on each user's computer. Or, you can override this default behavior and manage the distribution of multiple language versions more precisely. For example, you can:

- Install more than one language on a single computer.
- Specify which languages to install on users' computers, regardless of the language of the operating system, which is specified by user locale.
- Specify custom settings once and then apply them to all language versions that you deploy in your organization.
- Deploy different languages to different groups of users.
- Deploy the Microsoft Office 2010 Proofing Tools Kit for additional languages.

To identify which deployment solution is appropriate for your scenario, see the model poster Deploy Multilanguage Packs for Microsoft Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=168622*).

To determine which companion proofing languages are included in an Office 2010 Language Pack, see Companion proofing languages for Office 2010 (*http://technet.microsoft.com/library/3f4de10b-757a-4ce5-b9b7-1baafeb4753e(Office.14).aspx*).

Each Office 2010 Language Pack contains the proofing tools for one or more additional languages. For example, the Office 2010 Language Pack - Danish contains the proofing tools for English and German, in addition to Danish. All Office 2010 Language Packs contain the proofing tools for English. For more information about proofing tools, see Plan for proofing tools.

Before it installs a language version of an Office 2010 product, Setup determines whether the user has the required operating system support for that language. Setup stops the installation if there is no support. For example, if a user has not enabled support for East Asian languages, Setup does not install the Japanese version of Office 2010.

It is important to plan which languages will be needed at the beginning of your deployment. There are special steps that you must take if you have to change users' configurations after the initial deployment and include additional languages as part of your customizations. For more information, see Add or remove languages after deploying Office 2010 (*http://technet.microsoft.com/library/aef95370-7f15-434f-9311-e792555645d7(Office.14).aspx*).

Understanding the Setup logic for Shell UI language

Whenever you deploy the Office 2010 from a network installation point that contains more than one language version, Setup must determine which language to use for the Setup user interface. By default, Setup uses that same language for the Office 2010 installation language and for the Shell user interface (Shell UI). The Shell UI includes core elements of Office 2010 that register with the operating system, such file name extensions, Tool Tips, and right-click menu items.

If your objective is to install only one language version of Office 2010 on each client computer and if you do not specify any additional languages in the Config.xml file, Setup uses the following logic to determine which language to use:

- Setup matches the language of the user locale.
- If there is no match, Setup looks for a close match. If the user locale is set to English (Canada), for example, Setup might install Office 2010 in English (U.S).
- If there is no close match, Setup looks for a language in the following subkey in the Windows registry:

  HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources

  If the **InstallLanguage** entry has not been added to the **LanguageResources** subkey and set to a particular language (LCID), Setup prompts the user to select a language (in an interactive installation), or the installation fails (in a quiet installation).

If your objective is to install more than one language version of Office 2010 on each client computer, you should edit the Config.xml file and set the **<AddLanguage>** element for each language that you want to include. However, when you add more than one language in the Config.xml file, you must specify which of those languages Setup should use for the Shell UI. If the Shell UI language is not specified, the installation fails.

You specify a language for the Shell UI by setting the **ShellTransform** attribute of the **<AddLanguage>** element. In this case, the language of the Setup user interface follows the logic described previously. However, the languages installed on the computer and the language of the Shell UI are determined by the entries in the Config.xml file.

Setup always installs Office 2010 in the language of the Shell UI, in addition to any other installation languages. For example, if the Shell UI is set to French, the user can select additional installation languages on the **Languages** tab; however, the user cannot remove French.

For specific steps on how to customize Setup for different scenarios, see applicable sections in Customize language setup and settings for Office 2010 (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d(Office.14).aspx):*

- Deploy a default language version of Office (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d.aspx#BKMK_DeployDefaultLanguageVersionOfOffice*)
- Specify which languages to install (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d.aspx#BKMK_SpecifyLanguagesToInstall*)
- Deploy different languages to different groups of users (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d.aspx#BKMK_DeployDifferentLanguages*)

Plan customizations

When a user starts an Office 2010 application for the first time, Setup applies default settings that match the language installed on the computer and the language specified by the Windows user locale setting.

Four main language settings affect the way users work with Office 2010:

- **Primary editing language** When more than one language version of Office 2010 is installed on the computer, this setting determines the language in which users work with Office applications and documents.
- **Enabled editing languages** Users can specify more than one language for editing Office 2010 documents. Depending on the languages selected, this setting might require that the user has installed additional proofing tools.
- **User interface language** This setting determines the language in which the user interface (menus and dialog boxes) is displayed.
- **Help language** This setting determines the language in which users view Help topics.

You can configure these language settings for users in advance. If you specify custom language settings when you install Office, by applying a Setup customization file (.msp file) or by setting policies, Office 2010 does not overwrite your settings with the default settings when users start the applications for the first time.

Methods of customizing language settings

You configure language settings by using one of the following methods:

- **Group policies** Group Policies enforce default language settings. Users in your organization cannot permanently change settings managed by policy. The settings are reapplied every time that the user logs on.

  The following policies help you manage language settings in the Office 2010:

  - **Display menus and dialog boxes in** Located in the Display Language folder. This determines the language of the user interface.
  - **Display help in** Located in the Display Language folder. This determines the language of online Help. If this policy is not configured, the Help language uses the user interface language.
  - **Enabled Editing Languages** Located in the Editing Languages folder. This enables editing languages from the list of languages supported by Office.
  - **Primary Editing Language** Located in the Enabled Editing Languages folder. This specifies the language in which users work with Office applications and documents when more than one language version is available on the computer.
- **Office Customization Tool (OCT)** You use the OCT to create a Setup customization file (.msp file) that Setup applies during the installation. Settings specified in the OCT are the default settings. Users can change the settings after the installation.

- **Language Settings tool** If you do not enforce language settings by policy, users who work in Office 2010 applications can use the Language Settings tool to change their language settings.

For specific steps on how to use these tools to customize Office 2010 for multiple language deployments, see Customize language setup and settings for Office 2010 (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d(Office.14).aspx*).

Enable users to view the new language settings on first open

Typically, after you configure language settings by using one of the methods described in this article, Setup applies default settings that match the language that is installed on the computer when a user starts an Office 2010 application for the first time. This means the new language settings will display the next (second) time that the user starts the Office 2010 application.

If you want users to view the new language settings the first time that they open an Office 2010 application, you can deploy the following registry settings to their computers when you deploy an initial Office 2010 installation, or before they have to use an Office 2010 application. You can deploy these registry settings by using a script or batch file, Group Policy, or the OCT. The registry settings that you must configure are the following DWORD values under the **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources** key:

UILanguage

HelpLanguage

FollowSystemUI

For each of these values, for **Value** name specify the LCID (locale identifier) that corresponds to the language that you want to use. For a list of LCIDs, see Language identifiers and OptionState Id values in Office 2010 (*http://technet.microsoft.com/library/f5fee727-df49-4ef7-b073-dd6c08dfecfa(Office.14).aspx*). LCIDs are decimal values. Therefore, you must also set the **Base** option to **Decimal**.

Customize language-specific settings related to user locale

In addition to using the **Primary Editing Language** setting, the Office 2010 also configures language-related settings, such as number format, to match the user locale of the operating system. This behavior is controlled by the **LangTuneUp** entry in the **LanguageResources** subkey in the Windows registry. If you do not want user locale to affect default settings, you can reset the value of **LangTuneUp** when you install Office 2010. If the **LangTuneUp** entry does not exist, Office 2010 creates the entry the first time that an application starts and sets the value to **OfficeCompleted**.

The **LangTuneUp** entry can have one of two values:

- **OfficeCompleted** Settings based on user locale are not applied to Office 2010 as a whole. However, individual applications still check for new input method editors (IMEs) and language scripts, and still apply application settings that are specific to the user locale. For example, applications ensure that newly installed keyboards have the appropriate editing languages enabled, and Word uses fonts in Normal.dot based on user locale.

- **Prohibited** No settings related to user locale are modified by Office 2010 or by any individual Office 2010 application.

In some scenarios, ignoring the user locale setting can help maintain a standard configuration across a multilingual organization. Setting the **LangTuneUp** entry to **Prohibited** ensures that language settings remain consistent and macros are more compatible internationally.

For example, if your organization is based in the United States and you want to standardize settings internationally, you can deploy Office 2010 with **Primary Editing Language** set to **en-us** (U.S. English) and **LangTuneUp** set to **Prohibited**. In this scenario, users receive the same default settings, regardless of their user locale.

Ignoring user locale is not always the best option. For example, users who read and enter Asian characters in Office 2010 documents might not always have the Asian fonts they must have to display characters correctly. If the installation language on the user's computer does not match the language that was used in the document and **LangTuneUp** is set to **Prohibited**, Office 2010 does not display fonts in the non-default language. If your Office 2010 installations need to support multiple Asian language user locales, make sure **LangTuneUp** continues to be set to **OfficeCompleted**. To help ensure that users do not change the default value, set the corresponding policy.

Plan for proofing tools

Proofing tools let users edit documents in more than 50 languages. Depending on the language, these editing tools might include spelling and grammar checkers, thesauruses, and hyphenators. Proofing tools might also include language-specific editing features such as Language AutoDetect, AutoSummarize, and Intelligent AutoCorrect.

The Office 2010 Proofing Tools Kit provides a single resource from which you can install any of the proofing tools. You can install proofing tools on a local computer or deploy tools to a group of users. You can also customize and install the tools for one user or all users in your organization.

Determining the method for deploying proofing tools

You can deploy additional proofing tools for users who have to edit documents in languages other than those already installed on their computers. You can deploy additional proofing tools from either of these sources:

- **Office 2010 Language Pack** Use this option if users need both the user interface and the proofing tools for the language, or if one language pack can provide all the proofing tool languages that you need. Be aware that each language version of the Office 2010 includes proofing tools for a set of companion languages. For example, when you deploy the English version of an Office 2010 product, users receive proofing tools for both Spanish and French in addition to English. Depending on the number of user interface languages that you want to deploy and the included companion languages, Office 2010 Language Packs might provide all of the proofing tools that you need.

  For a list of companion languages, see Companion proofing languages for Office 2010 (*http://technet.microsoft.com/library/3f4de10b-757a-4ce5-b9b7-1baafeb4753e(Office.14).aspx*). If a

language pack has all the proofing tool languages that you need, deploy a language pack by using the instructions that fit your scenario in Customize language setup and settings for Office 2010 (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d(Office.14).aspx*).

- **Office 2010 Proofing Tools Kit** This product contains the proofing tools for all of the languages that are available with Office 2010. Use this option if you do not need the user interface for the language and you must have many proofing tools that are not included in the set of companion languages for any languages installed or included in an additional language pack that you could install.

The Office 2010 Multi-Language Pack contains all of the Office 2010 Language Packs. Individual Office 2010 Language Packs, the Office 2010 Multi-Language Pack, and Office 2010 Proofing Tools Kit are available for purchase in major retail stores and their Web sites, and also through Microsoft volume licensing programs.

The hard disk space requirement to install proofing tools is 1 gigabyte (GB). However, the overall disk space depends on whether you deploy proofing tools from a language pack or from the Office 2010 Proofing Tools Kit. As with most products in the Office 2010, the complete Office 2010 Proofing Tools Kit package is cached to the local installation source (LIS).

Note:
Proofing tools do not include bilingual dictionaries or word breakers. Those tools are part of the language version or language pack.

Customizing Setup for Office 2010 Proofing Tools Kit

To customize the Setup of the Office 2010 Proofing Tools Kit, modify the Config.xml file in the ProofKit.WW folder. For each set of proofing tools that you do not want to install, in the **OptionState** element, set the **State** attribute to **Absent**.

Syntax

<OptionState
Id="*optionID***"**
State="Absent" | **"Advertise"** | **"Default"** | **"Local"**
[**Children="force"**]
/>

OptionState attributes

The following table shows **OptionState** attributes, values, and descriptions.

Attribute	Value	Description
Id	*optionID*	An item that the user can choose to install. See Proofing Tools Config.xml OptionState Id values (*http://technet.microsoft.com/library/f5fee727-df49-4ef7-b073-dd6c08dfecfa.aspx#BKMK_OptionStateID*) in Language identifiers and OptionState Id values in Office 2010 (*http://technet.microsoft.com/library/f5fee727-df49-4ef7-b073-dd6c08dfecfa(Office.14).aspx*).
State	**Absent**	The feature is not installed.
	Advertise	The feature is installed the first time that it is used.
	Default	The feature returns to its default installation state.
	Local	The feature is installed on the user's computer.
Children	**force**	All child features of the feature are set to the specified state.

Note:
The default value for the **State** attribute is **Local**.

Example Config.xml file for Office 2010 Proofing Tools Kit

The following example Config.xml file shows every language that has the **OptionState** element **State** attribute set to **Absent**. If you decide to copy this example into the Config.xml file for the Office 2010 Proofing Tools Kit, set the **State** attribute for each set of proofing tools that you want to deploy to **Local** (or **Default** or **Advertise**, if preferred).

```
<Configuration Product="ProofKit">

  <!-- <Display Level="full" CompletionNotice="yes" SuppressModal="no" AcceptEula="no" /> -->
```

```
  <!-- <Logging Type="standard" Path="%temp%" Template="Microsoft Office Proofing Tools Kit
Setup(*).txt" /> -->
  <!-- <USERNAME Value="Customer" /> -->
  <!-- <COMPANYNAME Value="MyCompany" /> -->
  <!-- <INSTALLLOCATION Value="%programfiles%\Microsoft Office" /> -->
  <!-- <LIS CACHEACTION="CacheOnly" /> -->
  <!-- <LIS SOURCELIST ="\\server1\share\Office;\\server2\share\Office" /> -->
  <!-- <DistributionPoint Location="\\server\share\Office" /> -->
  <!-- <OptionState Id="OptionID" State="absent" Children="force" /> -->
    <OptionState Id="IMEMain_1028" State="Absent" Children="force"/>
    <OptionState Id="IMEMain_1041" State="Absent" Children="force"/>
    <OptionState Id="IMEMain_1042" State="Absent" Children="force"/>
    <OptionState Id="IMEMain_2052" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1025" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1026" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1027" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1028" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1029" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1030" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1031" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1032" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1033" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1035" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1036" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1037" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1038" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1040" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1041" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1042" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1043" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1044" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1045" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1046" State="Absent" Children="force"/>
```

```
    <OptionState Id="ProofingTools_1048" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1049" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1050" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1051" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1053" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1054" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1055" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1056" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1058" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1060" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1061" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1062" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1063" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1069" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1081" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1087" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1094" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1095" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1097" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1099" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1102" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_1110" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_2052" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_2068" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_2070" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_2074" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_3076" State="Absent" Children="force"/>
    <OptionState Id="ProofingTools_3082" State="Absent" Children="force"/>
  <!-- <Setting Id="Setup_Reboot" Value="IfNeeded" /> -->
  <!-- <Command Path="%windir%\system32\msiexec.exe" Args="/i \\server\share\my.msi"
QuietArg="/q" ChainPosition="after" Execute="install" /> -->
</Configuration>
```

Precaching the local installation source for the Office 2010 Proofing Tools Kit

When you deploy the Office 2010 Proofing Tools Kit, Setup creates a local installation source on the user's computer — a copy of the compressed source files for the Office 2010 Proofing Tools Kit. Once the files have been copied to the user's computer, Setup completes the installation from the local installation source. You can minimize the load on the network by deploying the local installation source separately, before you deploy the Office 2010 Proofing Tools Kit. To precache the local installation source for the Office 2010 Proofing Tools Kit, see Precache the local installation source for Office 2010 (*http://technet.microsoft.com/library/ff0a01a5-33d8-407c-ac52-50edccb32786(Office.14).aspx*). Use the Setup.exe and Config.xml files from the ProofKit.WW folder on the Office 2010 Proofing Tools Kit CD.

See Also

Language identifiers and OptionState Id values in Office 2010 (*http://technet.microsoft.com/library/f5fee727-df49-4ef7-b073-dd6c08dfecfa(Office.14).aspx*)

Companion proofing languages for Office 2010 (*http://technet.microsoft.com/library/3f4de10b-757a-4ce5-b9b7-1baafeb4753e(Office.14).aspx*)

Customize language setup and settings for Office 2010 (*http://technet.microsoft.com/library/1c423975-1848-4060-999c-cafcadf3047d(Office.14).aspx*)

Add or remove languages after deploying Office 2010 (*http://technet.microsoft.com/library/aef95370-7f15-434f-9311-e792555645d7(Office.14).aspx*)

International reference for Office 2010 (*http://technet.microsoft.com/library/db99b5fd-ae5d-43b9-ac5f-2adce6e00868(Office.14).aspx*)

Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*)

Precache the local installation source for Office 2010 (*http://technet.microsoft.com/library/ff0a01a5-33d8-407c-ac52-50edccb32786(Office.14).aspx*)

Plan for virtualization for Office 2010

Microsoft Application Virtualization (App-V) provides the administrative capability to make applications available to end-user computers without having to install the applications directly on those computers. This section provides contains information to help you plan a deployment of Microsoft Office 2010 by using Application Virtualization.

In this section:

Article	Description
Overview of virtualization to deploy Office 2010	Describes what virtualization is, how you can use virtualization in your organization, and which method and type of Microsoft Application Virtualization (App-V) you can use to deploy Office 2010 in your organization.
Methods to deploy Office 2010 by using Application Virtualization	Provides information about methods to deploy Office 2010 by using Microsoft Application Virtualization (App-V) in specific environments and how to deploy by using an Application Virtualization Management Server or an Application Virtualization Streaming Server.
Application Virtualization application packages	This article contains technical guidance for using Microsoft Application Virtualization (App-V) to create an Office 2010 package.

Overview of virtualization to deploy Office 2010

This article describes what virtualization is, how you can use virtualization in your organization, and which method and type can be implemented in your environment. For a visual representation of this information, see Virtualization Overview, Methods, and Models (*http://go.microsoft.com/fwlink/?LinkId=168624*).

In this article:

About virtualization

Virtualization is the capability to run an application or a computer in a virtual environment without affecting the components that already exist on that particular desktop or server. Virtualizing computing resources can be done in two ways:

- **Application virtualization** Application virtualization is where a software application is packaged to run in a self-contained, virtual environment that contains all the information that is needed to run the application on the client computer without installing the software application locally.
- **Desktop virtualization** Desktop virtualization is where the software application, operating system, and hardware configuration is packaged to run in a self-contained, virtual environment. When a layer is created between the hardware and the operating system that is being installed, you are able to run multiple operating systems with applications on a single computer.

Virtualization types and technologies

The enterprise can deploy with one virtual delivery method or it can have multiple virtual environments in combination with one another.

Desktop, Presentation, Application

The virtualization types and technologies that are available for client support are as follows:

- **Desktop** Desktop virtualization is any kind of technology that creates an additional isolated operating system environment on a standard desktop. Virtual PC is still very common to use for capturing an entire desktop, specific hardware components, or only the Users Profile and applying it to another device, desktop, or operating system. Virtual PC can create a primary system that has guest accounts for multiple operating system images that support legacy software without interrupting end-user functionality with upgrades to newer released versions of applications or application compatible issues. For more information, see Windows Virtual PC (*http://go.microsoft.com/fwlink/?LinkId=156041*).
- **Presentation** Presentation virtualization involves separating user profiles, with the data and application settings, from the user's computer. The key to enabling this is Remote Desktop Services (formerly known as Terminal Services), one of the core virtualization technologies available in Windows Server 2008. Presentation mode is typically for thin client connections or multiuser applications, where any application combination, or virtualized desktop environment that uses both the operating system and an application, is run in one location while having it controlled in another. Remote Desktop Services presents each user with screen images that can be individual applications or entire desktops, while the user's computer sends keystrokes and mouse movements back to the server. For more information, see Select Desktop or Presentation Virtualization (*http://go.microsoft.com/fwlink/?LinkId=156042*).
- **Application** Application virtualization enables you to virtualize individual applications, plug-ins, upgrades, and updates, and then stream them to a client computer in chunks for faster availability. For remote users, such as consultants or users traveling with portable computers, application virtualization can be "packaged" as an *.msi to distribute via a USB drive, CD, or file server. For more information, see Choose Application or Desktop Virtualization (*http://go.microsoft.com/fwlink/?LinkId=156043*).

Each of these methods of virtualization keeps the application in its own protected environment.

There are also the server-side virtualization types (Hyper-V and Virtual Server), which are not discussed in this article. For more information about server-side virtualization types, see the following articles:

- Virtual Server 2005 Technical Library (*http://go.microsoft.com/fwlink/?LinkId=156044*)
- Hyper-V as it applies to Windows Server 2008 (*http://go.microsoft.com/fwlink/?LinkId=156045*)

Application Virtualization

Microsoft Application Virtualization (App-V) is an enterprise-level application virtualization solution and is part of the Microsoft Desktop Optimization Pack (MDOP). App-V enables applications to run on a single instance of the operating system, turning applications into centrally managed services that are never installed, that never conflict, and that are streamed on-demand to end-users. App-V supports legacy applications and their extension points, whereas virtualized applications will not conflict with one another, do not affect the system, can be completely removed, and easily repaired or upgraded.

App-V is best used for applications that run on the current or target operating system, but have conflict issues either with other applications or some installed files. By decoupling the physical desktop from the software or hardware, you can create an isolated environment unseen by the end-user, and then run an application by using a desktop computer or server that has Remote Desktop Services (formerly known as Terminal Services) enabled without ever installing the application on the client operating system.

Microsoft Office 2010 includes the traditional Setup.exe method of deployment, and also supports delivery through virtualization via streaming or deploying Office applications to the end-user without the need of a CD or Setup.exe file.

For applications that cannot be run on the operating system and need an older version of the operating system, see Microsoft Enterprise Desktop Virtualization (MED-V) (*http://go.microsoft.com/fwlink/?LinkId=156031*), which is a component of MDOP (see Microsoft Desktop Optimization Pack (*http://go.microsoft.com/fwlink/?LinkId=156032*). MED-V enables you to deploy applications by using the Virtual PC tool.

To use Microsoft Application Virtualization in the enterprise, Office 2010 will require the Application Virtualization Desktop Client (Deployment Kit) configured on each device.

For more information about virtual environments, see About Virtual Environments (*http://go.microsoft.com/fwlink/?LinkId=156039*).

Virtualization delivery methods

Delivery of Microsoft Office 2010 can be done via several delivery methods.

For information about computer or server virtualization, see the following resources:

- Windows Virtual PC (*http://go.microsoft.com/fwlink/?LinkId=156041*)
- Virtualization with Hyper-V (*http://go.microsoft.com/fwlink/?LinkId=156049*)
- Hyper-V as it applies to Windows Server 2008 (*http://go.microsoft.com/fwlink/?LinkId=156045*)
- Virtual Server 2005 Technical Library (*http://go.microsoft.com/fwlink/?LinkId=156044*)

Delivery methods

Within each kind of virtualization, there is a delivery method that provides a virtual environment to the desktop.

For a visual representation of delivery methods, see Virtualization Overview, Methods, and Models (*http://go.microsoft.com/fwlink/?LinkId=168624*).

Delivery methods for virtualization are as follows:

- **Presentation delivery** Enables a virtualized application to be accessed via Remote Desktop Services from a desktop computer. Applications are run from one central server location that provides screen images of the application or a desktop and are controlled by the desktop.

  For more information about Remote Desktop Services (formerly known as Terminal Services) presentation virtualization, see Remote Desktop Services (*http://go.microsoft.com/fwlink/?LinkId=156050*).

- **Streaming delivery** Application virtualization is the process where a software application is "packaged" and stored on a file server, application server, or alternative source drive, such as in Microsoft System Center Configuration Manager 2007 and delivered in small sequenced bundles as needed. For more information, see System Center Configuration Manager (*http://go.microsoft.com/fwlink/?LinkId=156051*).

  When end-users open a document that is running the virtual application for the first time, a quick scroll bar is displayed that shows what percentage of the virtual application has streamed to their computer. The application will load so that end-users can start their work. If there are features that the end-user needs that were not in the initial feature block, the rest of the application will stream in the background, into their local cache.

  A sequenced package contains several files. This includes one .sft file, one .sprj file, one Manifest.xml file, and then several .osd and .ico files.

  - The .sft file contains all the application files that contain all assets and state organized into streamable feature blocks.
  - The .osd file contains the description of the application, which includes environment dependencies, package location, shell integration, and scripts.
  - The .ico file contains the icons associated with each shortcut or file type association (FTA) defined in an .osd file or the Manifest.xml file. These are extracted from application resources.
  - The .sprj file is the sequencing project file that references the .osd default package setting list of all parser items, classifications, and exclusions.

- The Manifest.xml file, which publishes parameters for the applications in a package, includes the definition of shell integration (for example, FTAs, shortcuts, Dynamic Data Exchange (DDE), and so on).

- **Stand-alone delivery** The process where a software application is “packaged” and delivered via CD, USB drive, and so on, to be stored locally on the users cached drive for full access when they are disconnected from the network.

  For a visual representation of the stand-alone delivery method for mobile users, see Virtualization Overview, Methods, and Models (*http://go.microsoft.com/fwlink/?LinkId=168624*).

When you create a stand-alone package, an additional file is added to the package. The .msi file is created to publish and load (“install”) the virtual application package in a stand-alone environment.

Virtualization changes and updates

Microsoft Application Virtualization (App-V), formerly known as Microsoft SoftGrid Application Virtualization, provides access to centralized policy-based management, which enables administrators to add or remove access to any given application regardless of its location (for example, desktop, portable computer, or offline users).

App-V includes integration with Microsoft System Center Configuration Manager 2007, which can enable deployments of App-V applications from Configuration Manager 2007.

For more information about the major highlights in App-V and new features, see Application Virtualization Overview (*http://go.microsoft.com/fwlink/?LinkId=156034*).

Enhancements from SoftGrid

The following table lists some of the improvements in App-V. For a detailed list of the improvements, see Microsoft Application Virtualization - New Features (*http://go.microsoft.com/fwlink/?LinkId=156036*).

New feature	Supported in App-V 4.x
Virtualized Windows Services	Yes. Enables users to virtualize all aspects of any Windows-based application.
Virtualized Transactional User Profiles	Yes. Reduces the size of Windows profiles while enabling seamless roaming between computers.
End-User Pre-Caching	Yes. Enables users to initiate precached applications for offline use.
Batch Sequencing	Yes. Enables “sequence once, run anywhere” on multiple Windows operating systems, reducing the work required to virtualize applications.
Licensing Model	Enables central licensing with the added Security Protection Platform (SPP).
Support for Windows 7	Yes (App-V 4.5).
Support for Office 2010	Yes (App-V 4.6) x86, and for x64 Office or x86 deployments to x64 computers (under WoW64).
Active Updates	Yes. Updates an application version without having to disconnect the user.
SharePoint and Outlook Fast Search	Yes.
Access Control	Yes. Controls access to applications that were only pre-authorized by IT, even in offline mode.

Application virtualization client architecture

Depending on the needs of your organization, combining virtualization technologies is possible. Determine what you must have based on the virtualization characteristics for your situation. For more information, see Combining Virtualization Technologies (*http://go.microsoft.com/fwlink/?LinkId=156054*).

Virtualizing an application puts a layer between the operating system and the application itself. This provides the following benefits:

- More flexibility in running applications, which in the past might have had conflicts with other applications.
- Applications can be installed and removed more easily, because they are not affecting any of the local files on the desktop.
- Less regression testing.
- More customization on deployment of applications.

When an application is published on a local client computer, the application remains in a virtual environment. However, it is executed locally by using local resources. Even though the application is in a virtual environment, it is still able to interact with other locally installed programs.

The virtual environment for each application contains the registry settings and .ini files, .dll files, and the Group Policy settings file. The application reads from and writes to this virtual environment without affecting any of those settings on the local client computer. The only items that the App-V–enabled application will read from and write to outside its space are the System Services (for example, cut-and-paste, OLE, and printers) and the Profile Data. The local system files (for example, registry, .ini, and .dll) will only be read when it is necessary.

See Also

Planning and Deployment Guide for the Application Virtualization System (*http://go.microsoft.com/fwlink/?LinkId=156611*)

Electronic Software Distribution-Based Scenario (*http://go.microsoft.com/fwlink/?LinkId=156046*)

Application Virtualization Server-Based Scenario (*http://go.microsoft.com/fwlink/?LinkId=156047*)

Stand-Alone Delivery Scenario for Application Virtualization Clients (*http://go.microsoft.com/fwlink/?LinkId=156048*)

Microsoft Application Virtualization Sequencing Guide (*http://go.microsoft.com/fwlink/?LinkId=156052*)

Best practices to use for sequencing in Microsoft SoftGrid (*http://go.microsoft.com/fwlink/?LinkId=156053*)

Methods to deploy Office 2010 by using Application Virtualization

This article provides information about specific methods for deploying Microsoft Application Virtualization (App-V) in environments that have no servers available to support other methods to deploy virtual applications, and in environments that plan to deploy virtualized applications from a connected server, such as an Application Virtualization Management Server or an Application Virtualization Streaming Server.

For information to help you better understand and deploy App-V and its components, see Planning and Deployment Guide for the Application Virtualization System (*http://go.microsoft.com/fwlink/?LinkID=156611&clcid=0x409*). The guide also provides step-by-step procedures for implementing the key deployment methods.

For information about how to specifically deploy Office 2010 by using App-V, see Deploy Office 2010 by using Microsoft Application Virtualization (*http://technet.microsoft.com/library/b8b513fe-0306-407c-bd87-617a79b29ffa(Office.14).aspx*).

Deployment methods

The virtual application package content can be placed on one or more Application Virtualization servers so that it can be streamed down to the clients on demand and cached locally. File servers and Web servers can also be used as streaming servers, or the content can be placed directly on the end user's computer — for example, if you are using an electronic software distribution (ESD) system, such as Microsoft System Center Configuration Manager 2007.

The following are some deployment methods and resources:

- **ESD-based deployment** For more information, see Electronic Software Distribution-Based Scenario (*http://go.microsoft.com/fwlink/?LinkID=156046&clcid=0x409*).
- **Server-based deployment** For more information, see Application Virtualization Server-Based Scenario (*http://go.microsoft.com/fwlink/?LinkID=156047&clcid=0x409*).
- **Stand-alone deployment** For more information, see Stand-Alone Delivery Scenario for Application Virtualization Clients (*http://go.microsoft.com/fwlink/?LinkID=156048&clcid=0x409*).

See Also

Deploy Office 2010 by using Microsoft Application Virtualization (*http://technet.microsoft.com/library/b8b513fe-0306-407c-bd87-617a79b29ffa(Office.14).aspx*)

Planning and Deployment Guide for the Application Virtualization System (*http://go.microsoft.com/fwlink/?LinkID=156611&clcid=0x409*)

Application Virtualization application packages

This article contains technical guidance for using Microsoft Application Virtualization (App-V) to create a Microsoft Office 2010 package.

In this article:

Application virtualization sequencer

The Microsoft Application Virtualization Sequencer is a wizard-based tool that administrators use to create virtualized applications and application packages that are streamed to the App-V client computers.

During the sequencing process, the administrator puts the Sequencer program in monitor mode and installs the application to be sequenced on the sequencing computer. Next, the administrator starts the sequenced application and starts its most frequently used functions so that the monitoring process can configure the primary feature block. The primary feature block contains the minimum content that is required for an application, or multiple applications, to run. When these steps are complete, the administrator stops the monitoring mode, and then saves and tests the sequenced application to verify correct operation.

Application virtualization packages

The Sequencer produces the application package, which consists of several files, described in the following list. The .sft, .osd, and .ico files are stored in a shared content folder on the App-V Management Server and are used by the App-V client computer to access and run sequenced applications.

The **.ico** (icon) files specifies the application icons that appear on the App-V client desktop, and are used in the **Start** menu shortcuts and for file types. When you double-click the files or shortcuts, you start the shortcut to the corresponding .osd file, which starts the data streaming and the application. The experience of starting an App-V–enabled application is identical to starting a locally stored application.

The **.osd** (Open Software Description) file provides the information that is needed to locate the .sft file for the application and set up and start the application. This information includes the application name, the name and path of the executable file, the name and path of the .sft file, the suite name, the supported operating systems, and general comments about the application.

The **.sft** file contains the assets that include one or more Windows-based applications. The App-V Sequencer, without altering the source code, packages these asset files into chunks of data that can be streamed to the App-V client. The file is divided into two distinct blocks. The first block, which is known as the *primary feature block*, consists of the application's most-used features, as configured during package creation.

The **.sprj** (Sequencer project) file is generated when a project is saved. The .sprj file contains a list of files, directories, and registry entries that are excluded by the Sequencer. Load this file into the Sequencer to add, change, delete, or upgrade any of the applications in the suite. A common example might be when you use the .sprj files to add service packs to the application.

The manifest file (XML based) describes all of the applications, file-type associations, and icons that are used by the package.

Creating an Office 2010 system package

Microsoft Office 2010 uses the Office Software Protection Platform (SPP) service. This is the same activation technology that is used to activate volume editions of Windows Vista and Windows 7 and is contained in the Microsoft Office 2010 Deployment Kit for App-V (*http://go.microsoft.com/fwlink/?LinkID=186371&clcid=0x409*).

Before you can sequence a package, ensure that you have the minimum configuration necessary, and follow the guidelines provided in Best Practices for the Application Virtualization Sequencer (*http://go.microsoft.com/fwlink/?LinkID=192229*).

You must install and configure the Microsoft Office 2010 Deployment kit for App-V on the sequencing computer. The deployment kit includes both the required SPP licensing components that are required for Office license activation (*http://go.microsoft.com/fwlink/?LinkID=182959*) and the Office 2010 integration features. This product must also be installed on the client computers to which virtualized Office 2010 packages will be deployed and streamed.

To create a system package, you must have a minimum of an electronic software distribution (ESD) server or an App-V Management Server, a sequencing computer, and a client computer each running the same version of Windows. Ensure that your environment meets all the relevant conditions listed in the following table.

Architecture of sequencing computer	Architecture of computer that is running Office	Architecture of client computer	Licensing support	Virtual proxy support
x86-based computer	x86-based computer	x86-based computer	Yes	Yes
		x 64 (Office will run through WoW64)	Yes	Yes

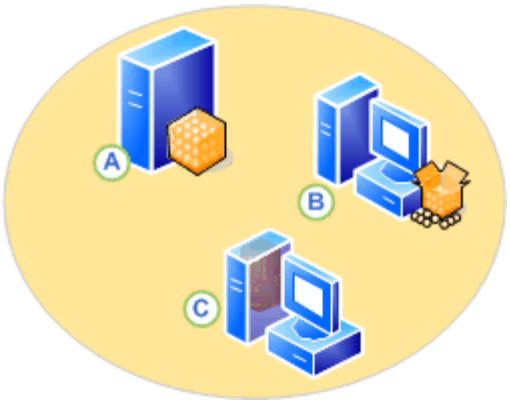
Architecture of sequencing computer	Architecture of computer that is running Office	Architecture of client computer	Licensing support	Virtual proxy support
x64-based computer	x86-based computer	x64-based computer (Office will run through WoW64)	Yes	Yes
	x64-based computer	x64-based computer	Yes	No

Important:
Packages that are sequenced on x64-based computers can only be deployed to x64-based client computers. Packages that are sequenced on x86-based computers can be deployed to x86-based client computers or x64-based client computers.

Note:
Virtual proxies are optional. However, virtual proxies are only supported on 32-bit computers that are running Office 2010.

The following figure and table describe the minimum requirements and are followed by the procedures necessary to create a system package.

- Prepare a computer for sequencing
- Install the deployment kit
- Sequence the Office 2010 system package



Computer	Description	Required operating system
A	Represents the Electronic Software Distribution (ESD) server or App-V Management Server	Running Windows Server 2008
B	Represents the client computer setup as the sequencing computer	Running the same Windows version as C
C	Represents the receiving client computer for the virtualized application package	Running the same Windows version as B

Use the following procedure to prepare a computer for sequencing.

To prepare a computer for sequencing

1. Ensure that you have Windows Search 4.0 (*http://go.microsoft.com/fwlink/?LinkID=169358*) installed, and set the **Windows Search** service to **Manual** or to **Automatic**.
2. Download the XPS Viewer by installing the Microsoft XML Paper Specification Essentials Pack (*http://go.microsoft.com/fwlink/?LinkID=169359*).
3. Set the Windows Update service to **Disabled**.
4. Install the App-V 4.6 Sequencer.
5. Download the Deployment Kit (*http://go.microsoft.com/FWLINK/?LinkID=186371*) and extract the .exe file.
6. After you extract the .exe file, you should have an OffVirt.msi file.

Use the following procedure to install the deployment kit that enables Office 2010 client products to be sequenced and deployed by using App-V. The kit includes the components that are required for Office license activation.

To install the deployment kit

1. Open an elevated command prompt.

   Click **All Programs** and **Accessories**, right-click **Command Prompt**, and then click on **Run as Administrator**. Or, open the **Start** menu, type **cmd** in the search box area, and then press **CTRL+SHIFT+ENTER**.
2. Browse to the directory that contains the Offvirt.msi file.
3. Run the following command to install the deployment kit:

Msiexec /i OffVirt.msi [feature flags][licensing flags]

Note

You must install the version of the deployment kit that matches the operating system architecture of your computer. For example, if you intend to sequence either Office 32-bit or 64-bit on a 64-bit operating system computer, you must use the 64-bit version of the deployment kit because it matches the operating system version.

Use the feature flags for the architecture that matches your sequencing station operating system:

32-bit:ADDLOCAL=Click2runMapi,Click2runOWSSupp,Click2runWDS,OSpp,OSpp_Core

64-bit:ADDLOCAL=Click2runMapi,Click2runOWSSupp,Click2runWDS,Ospp,OSpp_Core,OSppWoW64

For more information about the Office 2010 system volume activation and to determine which activation and licensing flags to use, see Office license activation (*http://go.microsoft.com/fwlink/?LinkID=182959*).

The following table lists the Office 2010 product applications and Office 2010 product suites together with their corresponding licensing flag for KMS activation. To configure the appropriate license properties for KMS, specify the values that correspond to the Office 2010 product that you are sequencing, and set the flag value from the following table to 1.

For example: **msiexec /i Offvirt.msi PROPLUS=1 VISIOPREM=1**

KMS activation

Product application	Flag	Value		Product suite	Value	Flag
Access	Access	0 or 1		Office Professional Plus	0 or 1	PROPLUS
Excel	Excel	0 or 1		Office Small Business Basics	0 or 1	SMALLBUSBASICS
SharePoint Workspace	GROOVE	0 or 1		Office Standard	0 or 1	STANDARD
InfoPath	InfoPath	0 or 1				
OneNote	OneNote	0 or 1				
Outlook	Outlook	0 or 1				
PowerPoint	PowerPoint	0 or 1				
Project	PROJECTPRO	0 or 1				

Professional						
Project Standard	PROJECTSTD	0 or 1				
Publisher	Publisher	0 or 1				
SharePoint Designer	SPD	0 or 1				
Visio Premium	VISIOPREM	0 or 1				
Visio Professional	VISIOPRO	0 or 1				
Visio Standard	VISIOSTD	0 or 1				
Word	Word	0 or 1				

The following table lists the flags and values for MAK activation. If the Office client computers will be using MAK activation, you must install the product key by using one of the methods listed in the following table.

MAK activation

Flag	Value
PIDKEYS Multiple product keys are semicolon delimited. Ex. PIDKEYS=X-X-X-X-X;Y-Y-Y-Y-Y	XXXXX-XXXXX-XXXXXX-XXXXXX-XXXXXXX
USEROPERATIONS	0 or 1

1. Use the Volume Activation Management Tool (VAMT) 2.0, to install product keys on client computers that stream the Office 2010 system. To download the tool, see Volume Activation Tool (*http://go.microsoft.com/FWLINK/?LinkID=83292*).
2. Deploy one or more MAKs keys by using PIDKEYS property, semicolon delimited, as shown in the table. In the following example, the Professional Plus and the Visio MAK keys are being entered, followed by the USEROPERATIONS property set to 1 to allow the client to activate.

   msiexec /i OffVirt.msi PIDKEYS=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx;yyyyy-yyyyy-yyyyy-yyyyy-yyyyy-yyyyyy USEROPERATIONS=1

3. Mixed KMS/MAK deployments are supported. For example: use KMS for PROPLUS and MAK for Visio:

   msiexec /i OffVirt.msi PROPLUS=1 PIDKEYS=yyyyy-yyyyyy-yyyyyy-yyyyyy-yyyyyy-yyyyyy

Note:
UserOperations=1 means non-administrative users can activate Office. UserOperations=0 means only administrators can activate Office.

Use the following procedure to sequence the Office 2010 system on the sequencing computer.

To sequence the Office 2010 system

1. On the sequencing computer, click **Start**, select all programs, select **Microsoft Application Virtualization**, and then click **Microsoft Application Virtualization Sequencer**. This will open the application virtualization sequencing wizard.
2. Click **Create Package** to create a new package for an application.
3. On the **Package Information** dialog box, specify the name of the package.
4. For the installation folder, install to a new directory by using an 8.3 format such as Q:\Temp123.wxp, and then click **OK**.

   Note:
   We recommend that you select a virtual drive assignment and use it consistently; typically, this is the Q:\ drive.
5. On the **Monitoring Installation** dialog box, click **Begin Monitoring** to monitor the installation phase.
6. Start the setup.exe for the Office 2010 system.
7. At the **Choose the installation that you want** prompt, click **Customize**.

   Note:
   In the Office installation procedure, make sure that you select **Install to hard disk drive** if you want that feature installed.
8. Click the **File Location** tab, and configure the path to match the installation directory that you selected in step 4. Then click **Install**.

The following procedure to configure the first start use settings (for example, customizing user settings) is optional, but should be performed during monitoring. If you do not need the optional steps, go to To create the Primary Feature Block later in this article.

Optional steps

1. Start virtual applications during monitoring. Click **Start**, and then click **Run**.
2. Enter the actual path of the virtual application, and select the executable virtual file to start the virtual application.

For example, to start Word, type **q:\Temp123.wxp\Office14\WINWORD.EXE**, and then press ENTER.

3. Configure additional proxies while the sequencer is still monitoring.

Use the following procedure, which is done while on the sequencing computer, to configure additional proxies. These steps must occur during the monitoring process to have these keys correctly persisted in a deleted state in the virtual registry. Proxies enable Fast Search in Outlook Search, integration with SharePoint (openin and, editing documents), and other features.

To configure additional proxies

1. Configure SharePoint proxy registry settings by creating the following virtual registry keys on the sequencer server while the sequencer is still monitoring, and then delete these registry keys so that the sequencer monitors the deletion of the newly added keys.
   - If you are sequencing a 32-bit operating system, the keys are as follows:

     HKEY_CLASSES_ROOT\CLSID\{9203C2CB-1DC1-482d-967E-597AFF270F0D}\TreatAs

     HKEY_CLASSES_ROOT\CLSID\{BDEADEF5-C265-11D0-BCED-00A0C90AB50F}\TreatAs
   - If you are sequencing a 64-bit operating system, the keys are as follows:

     HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{9203C2CB-1DC1-482d-967E-597AFF270F0D}\TreatAs

     HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{BDEADEF5-C265-11D0-BCED-00A0C90AB50F}\TreatAs
2. Add new proxy applications for proxy support on the **Configure Applications** page, and select the **Applications root** directory. Click **Add**, and then add the following applications:

   Note:
   To quickly locate the path, click **Browse**. Copy and paste the application path into the **File name** field.
   - Instant Search (Virtual Search host)

     Application Path: %commonprogramfiles%\microsoft shared\virtualization handler\VirtualSearchHost.exe

     Name: Specify a name. The default name is “Search MAPI Protocol Handler Host”
   - Virtual SharePoint Proxy

     Application Path: %commonprogramfiles%\microsoft shared\virtualization handler\VirtualOWSSuppManager.exe

     Name: Specify a name. The default name is “Microsoft SharePoint Client Support Manager”
   - Simple MAPI

     Application Path: %commonprogramfiles%\microsoft shared\virtualization

handler\MapiServer.exe

Name: Specify a name. The default name is “Microsoft Virtual Office Simple MAPI Proxy Server”

- Virtual Mail Control Panel Item

  Application Path: %windir%\system32\Control.exe %SFT_MNT%\short path\Office14\mlcfg32.cpl

  Name: Specify a name. The default name is “Windows Control Panel”

Note

To add the parameter **%SFT_MNT%\short path\Office14\mlcfg32.cpl** to the application path, browse to the Control.exe application path, and click **OK**. Append the parameter in the **Application Path** field.

The short path is the 8.3 directory on which you installed Office 2010. For example, if you installed Office 2010 to Q:\Temp123.wxp, the short path would be Temp123.wxp.

- Office Document Cache

  Application Path: Q:\short path\Office14\MSOSync.exe

  Name: Specify a name. The default name is “Microsoft Office Document Cache”

3. Set the Office Document Cache application to start automatically.

   Expand the Office Document Cache element in the **Applications** tree.
4. Select **Shortcuts**. Edit the shortcut location to be **Start Menu\Programs\Startup**.
5. Synchronize all application .osd file versions with the proxy .osd version.

   Right-click the Office installation file (Setup.exe), and then select **Properties**.
6. Click the **Version** tab. Change the version of all .osd files to match that version.

   For example: If the version of Setup.exe is 14.0.4763.1000, make sure that the version number of all proxy application .osd files and Office .osd files are set to 13.04.764.1000.
7. Click **Next**.

Use the following procedures to create the primary feature block that contains the minimum content required for an application or multiple applications to run. We recommend that you do not start OneNote, Outlook, and SharePoint because of the customization settings that are better preserved. During this step, do not press **F1**.

To create the Primary Feature Block

1. On the **Application** page, click **Next**.
2. Select and start the preferred applications to generate the primary feature block for each application.
3. Click **Next**.

4. After sequencing is complete, click **Finish**.
5. To save the package, click **Package**, and then click **Save As**.

To configure the Office 2010 registry setting

1. Verify that the following virtual registry key is set to **Merge with Local**.

   If you are sequencing on a 32-bit operating system, the registry key is as follows:

   MACHINE\Software\Microsoft\Office\14.0

   If you are sequencing on a 64-bit operating system, the registry key is as follows:

   MACHINE\Software\Wow6443Node\Microsoft\Office\14.0

2. Right-click the registry key, select **Key**, and then verify that the **Merge with Local Key** check box is selected.

   Important:
   If you are deploying Office 2010 to a computer that already has the 2007 Office system installed (coexistence with Office 2010), follow these steps. Otherwise, skip the rest of these steps and continue.

3. During monitoring, create the following registry subkey:

   HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles

   If you are sequencing on a 64-bit version of Windows, also create the following subkey:

   HKEY_CURRENT_USER\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles

   For App-V 4.6, make sure that the subkey is set to **Override local key**.

   For App-V 4.5, set the parent key **…\CurrentVersion\Windows Messaging Subsystem** to merge with the local key.

   Set the subkey **…\CurrentVersion\Windows Messaging Subsystem\Profiles** to merge with the local key.

   Important:
   The following steps must be performed during monitoring to have the key persist in a deleted state in the virtual registry.

4. On the **Tools** menu, click **Sequencing Wizard.**
5. Click **Next**.
6. Click **Begin Monitoring**.
7. Create the following virtual registry subkey, and then delete it so that the sequencer monitors the deletion of the newly added key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\Microsoft.OMSAddin

8. Click **Stop Monitoring**, continue to click **Next**, and then click **Finish** to return to the advanced sequencer properties page.

   Note:
   You might have to add some of these XML nodes if they currently do not exist.

9. For each .osd file, add **TRUE** to the following Element text of the tag:

   SOFTPKG -> IMPLEMENTATION -> VIRTUALENV -> POLICIES -> LOCAL_INTERACTION_ALLOWED

Use the following procedure to configure the client computer to run the Office 2010 sequenced package.

To configure a client computer to run Office 2010

1. Install the App-V client on the client computer, if you have not already done this.
2. Browse to the directory that contains the Offvirt.msi file.
3. At the command prompt, run the following command:

   msiexec /i OffVirt.msi [Licensing flags]

   You must enter a correct licensing flag from the list in the following table to correctly configure the deployment kit. Otherwise, functionality might be incorrect.

   KMS activation

Product application	Flag	Value		Product suite	Value	Flag
Access	Access	0 or 1		Office Professional Plus	0 or 1	PROPLUS
Excel	Excel	0 or 1		Office Small Business Basics	0 or 1	SMALLBUSBASICS
SharePoint Workspace	GROOVE	0 or 1		Office Standard	0 or 1	STANDARD
InfoPath	InfoPath	0 or 1				
OneNote	OneNote	0 or 1				
Outlook	Outlook	0 or 1				
PowerPoint	PowerPoint	0 or 1				

Project Professional	PROJECTPRO	0 or 1				
Project Standard	PROJECTSTD	0 or 1				
Publisher	Publisher	0 or 1				
SharePoint Designer	SPD	0 or 1				
Visio Premium	VISIOPREM	0 or 1				
Visio Professional	VISIOPRO	0 or 1				
Visio Standard	VISIOSTD	0 or 1				
Word	Word	0 or 1				

The following table lists the flags and values for MAK activation. If the Office clients will be using MAK activation, you must install the product key by using one of the methods listed in the table.

MAK activation

Flag	Value
PIDKEYS Multiple product keys are semicolon delimited. Ex. PIDKEYS=X-X-X-X-X;Y-Y-Y-Y-Y	XXXXX-XXXXX-XXXXXX-XXXXXX-XXXXXXX
USEROPERATIONS	0 or 1

a. Use the Volume Activation Management Tool (VAMT) 2.0 to install product keys on client computers that stream the Office 2010 system. To download this tool, see Volume Activation Tool (*http://go.microsoft.com/FWLINK/?LinkID=83292*) on the Microsoft Download Web site.

b. Deploy one or more MAK keys by using the PIDKEYS property, semicolon delimited, as shown in the previous table. In the following example, the Professional Plus and the Visio MAK keys are being entered, followed by the USEROPERATIONS property set to 1 to

allow the client to become active.

msiexec /i OffVirt.msi PIDKEYS=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx;yyyyy-yyyyy-yyyyy-yyyyy-yyyyy-yyyyyy USEROPERATIONS=1

c. Mixed KMS/MAK deployments are supported. If you want, some client computers can use KMS activation, and other client computers can use MAK. For example: use KMS for PROPLUS and MAK for Visio:

msiexec /i OffVirt.msi PROPLUS=1 PIDKEYS=yyyyy-yyyyyy-yyyyyy-yyyyyy-yyyyyy-yyyyyy

4. Enable the proxies on the client computer only if you configured proxies during the sequencing step.

To enable the virtual proxies for the package, open an elevated command prompt and run the following command:

msiexec /I path of the OffVirt.msi\OffVirt.msi ADDDEFAULT=Click2runOneNoteProxy,Click2runOutlookProxies,Click2RunWDSProxy, Click2runOWSSuppProxies PACKAGEGUID={SFT package GUID} PACKAGEVERSION=versions found in OSD files for proxies, Outlook, and OneNote OUTLOOKNAME=application name for Outlook from OSD ONENOTENAME=application name for OneNote from OSD MAPISERVER=MAPI proxy application name VIRTUALSEARCHHOST=Search proxy application name MLCFG32CPL=application name for virtual mail configuration OWSSUPPServer=application name for SharePoint proxy

For example:

msiexec /i c:\OffVirt.msi ADDDEFAULT=Click2runOneNoteProxy,Click2runOutlookProxies,Click2runWDSProxy,Click2runOWSSuppProxies PACKAGEGUID={5971AF75-7831-4AE9-906F-0F30C7DD0CA5} PACKAGEVERSION=14.0.4763.1000 OUTLOOKNAME=”Microsoft Outlook 2010” ONENOTENAME=”Microsoft OneNote 2010” MAPISERVER=”Microsoft Virtual Office Simple Mapi Proxy Server” VIRTUALSEARCHHOST=”Search MAPI Protocol Handler Host” MLCFG32CPL=”Windows Control Panel” OWSSUPPServer=”Microsoft SharePoint Client Support Manager”

Creating application dependencies by using Dynamic Suite Composition

Dynamic Suite Composition provides a tool for administrators to control which virtual applications will be combined to create a unified, virtual working environment for an application set. Dynamic Suite Composition lets you specify mandatory or optional dependencies between virtual applications. After a virtual application is run on the client computer, it will also start the dependent virtual application’s environment and allow the combination of both virtual environments.

The Dynamic Suite Composition tool comes as part of the App-V resource kit. It reduces the risk of mistyping and the complexity that is associated with editing XML directly. The following is a sample exercise to configure two separate virtualized packages to integrate together:

1. On the App-V server, click **Start**, and then click **Microsoft App-V DSC Tool**.
2. In the Package Roots field, click **Select**, and then click **Add Folder**.
3. Expand **Computer**, select **Content** where the stored packages are listed, click **OK**, and then click **Done** to build the list of available packages.
4. In the **Primary Package** box, select the first package from **D:\Content\...**.
5. In the **Secondary Packages Available** box, select the second package from **D:\Content\...**, and then click **Add**.
6. Click **Save**, click **OK** to confirm, and then click **Exit** to complete the procedure.

See Also

Proof of Concept Jumpstart Kit v1.1 (*http://go.microsoft.com/fwlink/?LinkId=195525*)

Plan for Remote Desktop Services (Terminal Services)

A terminal server is the server that hosts Windows-based programs or the full Windows desktop for Terminal Services clients. Users can connect to a terminal server to run programs, to save files, and to use network resources on that server. When a user accesses a program on a terminal server, the program execution occurs on the server. Only keyboard, mouse, and display information is transmitted over the network. Each user sees only their individual session. The session is managed transparently by the server operating system and is independent of any other client session.

The Terminal Services role, now named Remote Desktop Services in Windows Server 2008 R2, provides the ability to host multiple, concurrent client sessions in Windows. By using Remote Desktop Services, users can access the Remote Desktop Session Host server (terminal server) from within a corporate network or from the Internet.

In this section:

Article	Description
Plan to deploy Office 2010 in a Remote Desktop Services (Terminal Services) environment	Describes the best practices and recommended guidelines to use when you plan a deployment of Microsoft Office 2010 in a Remote Desktop Services environment.
Setup customizations of Office 2010 related to Remote Desktop Services (Terminal Services)	Describes the customizations of Office 2010 that are related to Remote Desktop Services.

Plan to deploy Office 2010 in a Remote Desktop Services (Terminal Services) environment

This article describes the best practices and recommended guidelines to use when you plan a deployment of Microsoft Office 2010 in a Remote Desktop Services environment (formerly known as Terminal Services).

In this article:

Planning a Remote Desktop Services environment

Use the best practices and recommended guidelines in the following sections to plan an effective Remote Desktop Services environment for Office 2010.

Evaluating licensing requirements

Remote Desktop Services deployments of Microsoft Office require a volume license key to function correctly. In the 2007 Microsoft Office system, installations were able to complete on an operating system with Remote Desktop Services configured even if a non-volume license key (for example, retail) was used. However, when users started an application, they were presented with the following message:

“This copy of Microsoft Office Program cannot be used on Terminal Server. Please contact your local authorized Microsoft retailer for more information.”

In Office 2010, a setup time check is introduced. If the permissions associated with the product key do not allow for Remote Desktop Services, the Setup program is blocked immediately indicating that the SKU is not supported on the computer that is running Remote Desktop Services.

Evaluating software requirements

Be sure that you understand the requirements for the server and client computers before you install Office 2010 on a Remote Desktop Services-enabled computer.

Server requirements

You can run Office 2010 on a computer that is running Windows Server 2003 with Server Pack (SP) 1 or later versions. You cannot install or run Office 2010 on a server operating system that was released earlier than Windows Server 2003.

Deploying on Remote Desktop Services requires a review of the design changes in Office 2010, and a review of the server requirements depending on the version of Windows Server (2003 or 2008) that you intend to use. Depending on the current server hardware, which will support multiple concurrent sessions, the performance will be much affected. Processor and memory requirements will vary depending on the workload. The following table shows the results of some recent tests.

Windows Server version	Core processor	Memory	Concurrent sessions
Windows Server 2008	32	256 GB	1140
Windows Server 2008	16	256 GB	860
Windows Server 2003	16 (does not support 32)		
Windows Server 2003	4	16 GB	150

Remote Desktop Services could be configured to load balance on a Remote Desktop Session Host (RD Session Host) server farm depending on the customers' deployment needs.

As Windows Server 2003 RD Session Host server capacity and scaling shows, the number of concurrent sessions depends on many factors, such as workload and configuration. To support thousands of concurrent sessions, an RD Session Host server farm configuration should be used.

To view the Windows Server 2008 tuning guide, which now has a reference for general training of RD Session Host server knowledge worker workload (the Office-based workload) on Windows Server 2008, see Performance Tuning Guidelines for Windows Server 2008 (*http://go.microsoft.com/fwlink/?LinkId=135703*).

To learn about how Microsoft IT deployed Windows Server 2008 Terminal Services at Microsoft, see How MSIT uses Terminal Services as a Scalable Remote Access Solution (*http://go.microsoft.com/fwlink/?LinkId=135705*).

To learn more about the Remote Desktop Load Simulation Toolset, see Remote Desktop Load Simulation Tools (*http://go.microsoft.com/fwlink/?LinkId=178956*).

Client requirements

One advantage of running Office 2010 on a Remote Desktop Services-enabled computer is that older, less robust client computers can access the Remote Desktop Services-enabled computer. Specifically, any computer that supports the Remote Desktop Protocol (RDP) can connect to a Remote Desktop Services-enabled computer.

Evaluating recommended guidelines and best practices

Be sure that you review the following guidelines and best practice to plan an effective deployment of Office 2010 in a Remote Desktop Services environment.

The following paper, available for download, guides you on capacity planning of RD Session Host in Windows Server 2008 R2. It describes the most relevant factors that influence the capacity of a given deployment. Remote Desktop Session Host Capacity Planning in Windows Server 2008 R2 (*http://go.microsoft.com/fwlink/?LinkId=185079&clcid=0x409*)

For Microsoft Outlook 2010, the most scalable and optimized configuration for large deployments is Outlook running in Online Mode against the Exchange Server. However, Customers who deploy Outlook 2010 now have the supported option of enabling Cached Exchange Mode when Outlook 2010 is installed in a Remote Desktop environment. This may be ideal for small deployments where Outlook is connecting over a high latency connection to an Exchange Server that is located remotely. For more information, see Cached Exchange Mode in a Remote Desktop Session Host environment: planning considerations (white paper).

Single point of failure

Running Office 2010 on a single Remote Desktop Services-enabled computer can create a single point of failure if the Remote Desktop Services-enabled computer becomes unavailable or fails. In this event, all information workers who are connected to the Remote Desktop Services-enabled computer could lose connectivity with Office 2010 applications and could lose data. You can lessen the risk by using Windows Clustering, which uses server clusters and Network Load Balancing to help ensure that Remote Desktop Services–enabled computer safely fail over. For example, if you deploy a clustered and load-balanced server farm that consists of four Remote Desktop Services-enabled computers and one of the Remote Desktop Services-enabled computers becomes unavailable, the client connection will fail over to one of the other three Remote Desktop Services-enabled computers.

Remote Desktop Session Host server hardware

A Remote Desktop Services-enabled computer requires significantly more memory and processing resources than a typical server. In addition, although Remote Desktop Services is designed to be bandwidth efficient, the amount of data that the client exchanges with the Remote Desktop Services-enabled computers can be considerable and can affect performance. Consequently, before you roll out Office 2010 in a Remote Desktop Services environment, you should perform thorough capacity testing to ensure that the RD Session Host servers (terminal servers) have sufficient disk space, processing power, memory, and network bandwidth.

Remote Desktop Session Host server installation requirements

You must install the Remote Desktop Session Host (RD Session Host) server component on your server before you install Office 2010. You must also add every user who logs on to the Remote Desktop Services-enabled computer to the Remote Desktop Users group. Adding users to the Remote Desktop Users group enables the users to use Remote Desktop Connection to connect to the Remote Desktop Services-enabled computer and run Office 2010. If you do not add users to the Remove

Desktop users group, users are denied access to the Remote Desktop Services-enabled computer. For more information about how to install and configure Remote Desktop Services (Terminal Services), see Guidelines for Deploying Terminal Server (http://go.microsoft.com/fwlink/?LinkId=88006).

Configuring Remote Desktop Session Host server

The Remote Desktop Services Application Server mode was modified in the latest version with two steps in the feature work.

TSDisabled is a list of features that will not be installed by default, and will not appear in the feature tree for customized installs so they cannot be manually enabled.

TSAbsent is a list of features that will not be installed by default. However, they will appear in the feature tree (defaulted to absent) and can be manually turned back on via customization.

Disabled versus Absent

The following is a list of Office 2010 features that are either disabled or the default is set to absent on RD Session Host server configurations.

TSDisabled: OutlookVBScript

TSAbsent: PPTSoundFiles

Customizing the Office 2010 installation

Before you install Office 2010 on a Remote Desktop Services-enabled computer, you must be sure that the installation states are configured correctly for the features and applications that you are installing. Changing the installation state for a feature or an application does not require special tools and can be done during a manual installation or through the Office Customization Tool (OCT).

When users run Office 2010 on a Remote Desktop Services-enabled computer, they cannot install, configure, or uninstall features or applications. This is because the features and applications are installed on the RD Session Host server and not on the client computer, and users do not have administrative right to install, configure or uninstall software on the RD Session Host server (terminal server). Consequently, you must be sure that the installation state for each feature and application is configured as **Run from my computer** (that is fully installed) or **Not Available** (that is, not installed). If the installation state for a feature or application is configured as **Installed on First use**, users will see the following warning if they attempt to use the feature or run the application:

“Only administrators have permission to add, remove, or configure server software during a terminal service remote session.”

Likewise, if you change the installation state for an add-in to be installed on first use, the following error appears when a user tries to load the add-in:

“Microsoft Office cannot run this add-in. An error occurred and this feature is no longer functioning correctly. Please contact your system administrator.”

You can configure installation states during a manual installation by clicking **Customize** on the **Choose the installation you want** page. For more information about how to perform a manual installation on a Remote Desktop Services-enabled computer, see the following section.

Installing Office 2010 on a Remote Desktop Services-enabled computer

There are two ways that you can install Office 2010 on a Remote Desktop Services-enabled computer:

- Run the Setup program and manually step through the installation process.
- Automate the Setup program by using the customization (.msp) file, which you create with the OCT.

In either case, you must configure the Remote Desktop Services-enabled computer for install mode before you install Office 2010. Install mode ensures that an applications configurations (.ini) files are copied to the system directory so the files can be used as master copies for user-specific .ini files.

The first time that a user runs an application on an RD Session Host server (terminal server), the application searches the root directory for its .ini files. If the .ini files are not found in the root directory, but are found in the system directory, Remote Desktop Services copies the .ini files to the root directory. This ensures that each user has a unique copy of the applications .ini files. The application creates new .ini files in the users root directory. It is important that each user has a unique copy of the .ini files for an application. This prevents instances where different users might have incompatible application configuration (for example, different default directories or screen resolution).

Perform a manual installation of Office 2010

The following procedure describes how to manually install Office 2010 on a Remote Desktop Services-enabled computer. It is assumed that you have installed Remote Desktop Services and that you run the Setup program from the Office 2010 installation CD or from a network installation point.

To manually install Office 2010

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add or Remove Programs**, and then click **Add New Program**.
3. Click **Next**.
4. Click **Browse**.
5. Locate the Setup program (Setup.exe) for Office 2010. This can be on the Office 2010 installation CD or on a network installation point.
6. Click **Setup.exe**, and then click **Open**.
7. On the **Enter your Product Key** page, type the product key, and then click **Continue**.
8. On the **Read the Microsoft Software License Terms** page, click the **I accept the terms of this agreement** check box, and then click **Continue**.
9. On the **Choose the Installation you want** page, click **Customize**.

10. On the **Install Options** tab, click an application or feature and change the installation state to either **Run from my computer** or **Not available**.
11. If you want to customize other settings, click the **File Location** tab or the **User Information** tab, and then make the changes that you want.
12. To start the installation, click **Install Now**.
13. When the installation is complete, click **Close** to close the Setup program.
14. On the **After Installation** page, click **Next**.
15. On the **Finish Admin Install** page, click **Finish**.

It is important that you perform the last two steps. These steps configure the Remote Desktop Services-enabled computer for execute mode.

Perform an automated installation of Office 2010

The following procedures show how to perform an automated installation of Office 2010 on a Remote Desktop Services-enabled computer. It is assumed that you have created a Setup customization (.msp) file and have configured the installation states for features and applications as recommended earlier in this article. It is also assumed that you run the Setup program from a network installation point which you have already created.

First, configure the Remote Desktop Services-enabled computer for install mode.

Configure the Remote Desktop Services-enabled computer for install mode

1. Click **Start**, click **Run**, type **Cmd**, and then click **OK**.
2. At the command prompt, type the following command, and then press ENTER:

   Change user /install

Next, run the automated installation exactly as you would on a client computer.

When the automated installation is complete, configure the Remote Desktop Services-enabled computer for execute mode.

Configure the Remote Desktop Services-enabled computer for execute mode

1. Click **Start**, click **Run**, type **Cmd**, and then click **OK**.
2. At the command prompt, type the following command, and then press ENTER:

   Change user /execute

Note:
With Interactive Installations, by default, the user name field is populated with the currently logged-on users' information. This is also true for the user name set in the Config.xml file.

Any user name that is provided during Setup is written to the registry key **HKCU\Software\Microsoft\Office\Common\UserInfo**.

Remote Desktop Services mirrors this registry key to **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\TerminalServer\Install\Software\Microsoft\Office\Common\UserInfo**.

Any new users then receive the defaults from the **HKLM UserInfo** key in their own user profiles. Because a user name already exists, any new Remote Desktop Services users will not be prompted to input their own names, and instead they get the default user name of the administrator.

To resolve this issue for new users in a current Remote Desktop Services deployment, the administrator of the computer that is running Remote Desktop Services should remove values from the registry key **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\TerminalServer\Install\Software\Microsoft\Office\Common\UserInfo**.

To resolve the issue for all users in a new Remote Desktop Services deployment, the administrator of the computer that is running Remote Desktop Services should perform one of the following tasks:

- During installation, select **Customize**, and then clear the user name and initial values.
- Use a Config.xml file that has the user name and initials set to empty values.
- After installation, remove the values from the registry key **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\TerminalServer\Install\Software\Microsoft\Office\Common\UserInfo**.

See Also

Whitepaper Release: Application Virtualization 4.5 for Terminal Services (*http://go.microsoft.com/fwlink/?LinkId=185972&clcid=0x409*)

Setup customizations of Office 2010 related to Remote Desktop Services (Terminal Services)

Remote Desktop Services deployments of Microsoft Office 2010 require a volume license key to function correctly. This article describes customizations that are related to Remote Desktop Services (formerly known as Terminal Services).

In this article:

Install on first use

When you deploy Office 2010 to a multiple-user Remote Desktop Services-enabled computer, it is best to set the installation state (**Install On Demand** | **Advertise** | **Setting**) feature to use **Run from my computer**.

The installation state of **Install on first use** does not guarantee a successful installation of Office 2010.

Screen flickering

When you use PowerPoint 2010 that is connected to a Windows Server 2003 terminal server session by using a third-party client, such as a Citrix ICA client, the screen will flicker.

This can occur when you run Windows Presentation Foundation (WPF) applications in the terminal server session.

For information about the cause and resolution of this problem, see Microsoft Knowledge Base article 955692: Your screen flickers when you start WPF applications in a Windows Server 2003 terminal server session (*http://go.microsoft.com/fwlink/?LinkId=184709&clcid=0x409*).

TSAbsent and TSDisabled

The behavior enforced by the TSAbsent and TSDisabled can be overridden by using a custom Config.xml or Setup customization (.msp) file.

For example, by default OutlookVBScript is TSDisabled. However, you can override this by using Config.xml or .msp file.

The Remote Desktop Session Host server attributes on specific options are meant to modify default states. The attributes do not enforce a specific state.

The following Office 2010 features are either disabled or the default is set to absent on Remote Desktop Session Host server configurations.

- TSDisabled: OutlookVBScript
- TSAbsent: PPTSoundFiles

See Also

Plan to deploy Office 2010 in a Remote Desktop Services (Terminal Services) environment

Plan for accessibility in Office 2010

The Accessibility Checker in Microsoft Office 2010 lets users create more accessible documents for people who have disabilities. The Accessibility Checker (like a spelling checker, but for accessibility issues) is a core feature of Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.

In this article:

Increase the visibility of violations

The settings that are provided in Control what the checker reports later in this article are used to control the Accessibility Checker. Of these settings, most are about stopping the Accessibility Checker from performing a particular check.

The policy setting **Increase the visibility of Accessibility Checker violations** controls how strongly an accessibility error will be emphasized in the user interface. If enabled, you can specify what happens when a document, workbook, or spreadsheet has accessibility errors, as shown here:

- Accessibility violations do not change the **Prepare for Distribution** area in the Microsoft Office Backstage view (default).
- Accessibility errors cause the **Prepare for Distribution** area to be strongly emphasized in the Backstage view.
- Accessibility errors or warnings cause the **Prepare for Distribution** area to be less strongly emphasized in the Backstage view.

If disabled or not configured, the Accessibility Checker user interface is presented in its normal state.

Important:
Group Policy settings can be used to control the Accessibility Checker. For Excel 2010, PowerPoint 2010, and Word 2010, the Group Policy settings are located in the gpedit node <AppName>\File tab\Check Accessibility.

Control what the checker reports

The following tables provide the complete Group Policy settings that can be used to control the Accessibility Checker for Excel 2010, PowerPoint 2010, and Word 2010.

Group Policy settings for Excel 2010

Setting for Excel 2010	Associated registry key	Description
Stop checking for alt text accessibility information	AltText	If enabled, the Accessibility Checker does not verify whether objects such as images and shapes contain alternative text. If disabled or not configured, objects are checked for alternative text and issues found appear in the Accessibility Checker.
Stop checking for table header accessibility information	TableHeaders	If enabled, the Accessibility Checker does not verify whether tables have a header row specified. If disabled or not configured, tables are checked for header rows and issues found appear in the Accessibility Checker.
Stop checking to ensure workbooks allow programmatic access	ProgrammaticAccess	If enabled, the Accessibility Checker does not check whether workbooks have blocked programmatic access through Digital Rights Management (DRM). If disabled or not configured, workbooks are checked for programmatic access and issues found appear in the Accessibility Checker.
Stop checking for merged cells	MergedCells	If enabled, the Accessibility Checker does not check whether tables have merged cells. If disabled or not configured, worksheets are checked for merged cells and issues found appear in the Accessibility Checker.
Stop checking to ensure hyperlink text is meaningful	MeaningfulHyperlinks	If enabled, the Accessibility Checker does not check whether hyperlinks have meaningful text. If disabled or not configured, hyperlink text is checked and issues found appear in the Accessibility Checker.
Stop checking to ensure non-default sheet names	SheetNames	If enabled, the Accessibility Checker does not check whether worksheets with content have non-default names. If disabled or not configured, worksheet names are checked and issues found appear in the Accessibility Checker.

Setting for Excel 2010	Associated registry key	Description
Stop checking for blank table rows used as formatting	BlankTableRows	If enabled, the Accessibility Checker does not check whether blank table rows are used as formatting. If disabled or not configured, tables are checked for blank rows and issues found appear in the Accessibility Checker.

Group Policy settings for PowerPoint 2010

Setting for PowerPoint 2010	Associated registry key	Description
Stop checking for alt text accessibility information	AltText	If enabled, the Accessibility Checker does not verify whether objects such as images and shapes contain alt text. If disabled or not configured, objects are checked for alternative text and issues found appear in the Accessibility Checker.
Stop checking to ensure hyperlink text is meaningful	HyperlinkText	If enabled, the Accessibility Checker does not check whether hyperlinks have meaningful text. If disabled or not configured, hyperlink text is checked and issues found appear in the Accessibility Checker.
Stop checking for media files which might need captions	ClosedCaptions	If enabled, the Accessibility Checker does not flag media files that might need caption information. If disabled or not configured, presentations are scanned for media files and issues found appear in the Accessibility Checker.
Stop checking for table header accessibility information	HeaderRow	If enabled, the Accessibility Checker does not verify whether tables have a header row specified. If disabled or not configured, tables are checked for header rows and issues found appear in the Accessibility Checker.

Setting for PowerPoint 2010	Associated registry key	Description
Stop checking for blank table rows and columns	BlankRowCol	If enabled, the Accessibility Checker does not verify whether blank rows and blank columns have been inserted into tables. If disabled or not configured, tables are checked for blank rows and blank columns and issues found appear in the Accessibility Checker.
Stop checking for merged and split cells	SimpleStructure	If enabled, the Accessibility Checker does not verify whether tables have merged or split cells. If disabled or not configured, tables are checked for merged and split cells and issues found appear in the Accessibility Checker.
Stop checking that slide titles exist	HasTitle	If enabled, the Accessibility Checker does not verify whether every slide has a title placeholder. If disabled or not configured, slides are checked for titles and issues found appear in the Accessibility Checker.
Stop checking to ensure each slide has a unique title	UniqueTitle	If enabled, the Accessibility Checker does not verify whether every slide has a unique title. If disabled or not configured, slide titles are checked for uniqueness and issues found appear in the Accessibility Checker.
Stop checking to ensure a meaningful order of objects on slides	NonPlaceholderShapes	If enabled, the Accessibility Checker does not check whether a slide has non-placeholder objects which might be read back out of order. If disabled or not configured, slides are checked for objects which might be read back out of order and issues found appear in the Accessibility Checker.
Stop checking to ensure presentations allow programmatic access	IRM	If enabled, the Accessibility Checker does not check whether presentations have blocked programmatic access through DRM. If disabled or not configured, presentations are checked for programmatic access and issues found appear in the Accessibility Checker.

Group Policy settings for Word 2010

Setting for Word 2010	Associated registry key	Description
Stop checking for alt text accessibility information	AltText	If enabled, the Accessibility Checker does not verify whether objects such as images and shapes contain alt text. If disabled or not configured, objects are checked for alternative text and issues found appear in the Accessibility Checker.
Stop checking to ensure hyperlink text is meaningful	MeaningfulHyperlinks	If enabled, the Accessibility Checker does not verify whether hyperlinks have meaningful text. If disabled or not configured, hyperlink text is checked and issues found appear in the Accessibility Checker.
Stop checking for table header accessibility information	TableHeaders	If enabled, the Accessibility Checker does not verify whether tables have a header row specified. If disabled or not configured, tables are checked for header rows and issues found appear in the Accessibility Checker.
Stop checking for blank table rows and columns	BlankTableCells	If enabled, the Accessibility Checker does not verify whether blank rows and blank columns have been inserted into tables. If disabled or not configured, tables are checked for blank rows and blank columns and issues found appear in the Accessibility Checker.
Stop checking for merged and split cells	2DTableStructure	If enabled, the Accessibility Checker does not verify whether tables have merged or split cells. If disabled or not configured, tables are checked for merged and split cells and issues found appear in the Accessibility Checker.
Stop checking to ensure documents allow programmatic access	ProgrammaticAccess	If enabled, the Accessibility Checker does not check whether documents have blocked programmatic access through DRM. If disabled or not configured, documents are checked for programmatic access and issues found appear in the Accessibility Checker.

Setting for Word 2010	Associated registry key	Description
Stop checking to ensure long documents use styles for structure	StylesAsStructure	If enabled, the Accessibility Checker does not check whether long documents have used styles to define content structure. If disabled or not configured, documents are checked for style usage and issues found appear in the Accessibility Checker.
Stop checking to ensure styles have been used frequently	HeadingSpacing	If enabled, the Accessibility Checker does not check whether documents that use styles have used them frequently enough to accurately represent the document's content structure. If disabled or not configured, the frequency of style usage is checked and issues found appear in the Accessibility Checker.
Stop checking to ensure headings are succinct	SuccinctHeadings	If enabled, the Accessibility Checker does not check whether headings in a document are succinct. If disabled or not configured, document headings are checked for length and issues found appear in the Accessibility Checker.
Stop checking whether objects are floating	FloatingObjects	If enabled, the Accessibility Checker does not check whether a document has objects that are floating instead of inline. If disabled or not configured, objects are checked for floating text wrapping properties and issues found appear in the Accessibility Checker.
Stop checking whether blank characters are used for formatting	BlankCharacters	If enabled, the Accessibility Checker does not check whether multiple consecutive white-space characters are used for formatting. If disabled or not configured, documents are checked for consecutive white-space usage and issues found appear in the Accessibility Checker.
Stop checking for image watermarks	ImageWatermarks	If enabled, the Accessibility Checker does not check whether a document has image watermarks.

Setting for Word 2010	Associated registry key	Description
		If disabled or not configured, documents are checked for watermarks and issues found appear in the Accessibility Checker.
Stop checking to ensure heading styles do not skip style level	HeadingOrder	If enabled, the Accessibility Checker does not check whether headings in a document are used in order. If disabled or not configured, the ordering of headings in a document is checked and issues found appear in the Accessibility Checker.
Stop checking for tables used for layout	LayoutTablesReadingOrder	If enabled, the Accessibility Checker does not flag layout tables (that is, tables that have no style applied). If disabled or not configured, tables that have no styles are flagged and violations appear in the Accessibility Checker.

See Also

Accessibility Investments and Document Accessibility (blog) (*http://blogs.technet.com/office2010/archive/2010/01/07/office-2010-accessibility-investments-document-accessibility.aspx*)

Accessibility and the Ribbon (*http://go.microsoft.com/fwlink/?LinkId=188457*)

Plan for volume activation of Office 2010

Microsoft policy requires the activation of all editions of Microsoft Office 2010 client software, including Volume License editions. For Office 2010, volume activation takes place through Office Activation Technologies, which is based on the Software Protection Platform (SPP) used in Windows Vista and Windows Server 2008.

In this section:

Article	Description
Volume activation overview for Office 2010	Provides an overview of Microsoft Volume Licensing and Office Activation Technologies for Office 2010.
Plan volume activation of Office 2010	Describes how to plan for volume activation by using Office Activation Technologies.
Plan MAK independent activation of Office 2010	Describes how to plan for a deployment of Office 2010 by using Multiple Activation Key (MAK) independent activation.
Plan MAK proxy activation of Office 2010	Describes how to plan for a deployment of Office 2010 by using MAK proxy activation.
Plan KMS activation of Office 2010	Describes how to plan for a deployment of Office 2010 by using Management Service (KMS) activation.
Scenario: Core network - KMS activation of Office 2010	Describes how to plan KMS activation in a core network for volume activation of Office 2010.
Scenario: Secure network - KMS or MAK activation of Office 2010	Describes how to plan KMS or MAK activation in a secure network for volume activation of Office 2010.
Scenario: Roaming or disconnected computers - KMS or MAK activation of Office 2010	Describes how to plan KMS or MAK activation in roaming or disconnected computers for volume activation of Office 2010.
Scenario: Test or development lab - KMS or MAK activation of Office 2010	Describes how to plan KMS or MAK activation in a test or development lab network for volume activation of Office 2010.

Article	Description
FAQ: Volume activation of Office 2010	Provides answers to frequently asked questions (FAQ) about the various aspects of volume activation of Office 2010.

See Also

Volume activation quick start guide for Office 2010 (*http://technet.microsoft.com/library/dbff777c-3a2d-4d8e-a7be-6c45900c73c2(Office.14).aspx*)

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Volume activation overview for Office 2010

Microsoft includes product activation technologies in the following products sold through the Volume Licensing channel: Windows 7, Windows Vista, Windows Server 2008 R2, Windows Server 2008, and now Microsoft Office 2010 client products. Activation establishes a relationship between the software's product key and a particular installation of that software on a device. This article provides an overview of volume licensing and the two kinds of volume activation that is available.

In this article:

Volume Licensing overview

Microsoft Volume Licensing offers programs that are customized to the size and purchasing preference of organizations. These programs provide simple, flexible, and affordable solutions that enable organizations to easily manage licenses. Some editions of Office 2010 are available only through the volume licensing channel. To become a volume licensing customer, organizations must set up a volume licensing agreement with Microsoft.

By obtaining software licenses through Microsoft Volume Licensing programs, organizations pay only for the software license, instead of the media included in boxed software. In addition to reducing overall cost by eliminating these physical costs, purchasing in volume provides more customized purchasing options and improved software administration.

With some Volume Licensing programs, organizations can also purchase Software Assurance (*http://go.microsoft.com/fwlink/?LinkId=184005*). This is a comprehensive maintenance offering that helps organizations get the most out of their software investment. It combines the latest software with telephone support, partner services, training, and information technology (IT) tools. Organizations can choose Software Assurance at the time of purchase and begin to use the benefits immediately for the term of the license agreement.

Depending on the Volume Licensing program chosen, organizations might receive media, and have the option to obtain media (or supplemental media), documentation, and product support separately as needed.

For more information about Volume Licensing, see Microsoft Volume Licensing (*http://go.microsoft.com/fwlink/?LinkId=8523*). For step-by-step information about how to activate Volume License editions of Office 2010 client products, see Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*). If you are already familiar with Windows Volume Activation through Key Management Service (KMS) and Multiple Activation Key (MAK), see Volume activation quick start guide for Office 2010 (*http://technet.microsoft.com/library/dbff777c-3a2d-4d8e-a7be-6c45900c73c2(Office.14).aspx*) for instructions that are specific to Office 2010.

Changes in activation policy

Activation for the 2007 Microsoft Office system was required only for Microsoft software purchased from retail stores and OEMs. Product keys entered in Microsoft Office Enterprise 2007 bypassed activation. For Office 2010, the activation method uses Office Activation Technologies, based on the Software Protection Platform introduced in Windows Vista and Windows Server 2008.

Microsoft policy requires the activation of all editions of Office 2010 client software. This includes those obtained through the Volume Licensing program. This requirement applies to Office 2010 running on both physical computers and virtual computers. Activation is not required for any Office 2010 server products, such as Microsoft SharePoint Server 2010 and Microsoft Project Server 2010, or any version of Microsoft Exchange Server.

Why is activation necessary?

Counterfeiting is a significant problem for the software industry. According to a study by the Business Software Alliance, 41 percent of all personal computer software installed worldwide during 2008 was obtained illegally. Though the financial effects are serious to software manufacturers and vendors, with losses estimated at US $50 billion in 2008, the effect of counterfeit software goes beyond revenue loss to software manufacturers. Many consumers who have a counterfeit copy of Microsoft software are unwitting victims of a crime. Additionally, counterfeit software is increasingly becoming a vehicle for the distribution of viruses and malware that can target unsuspecting users, potentially exposing them to corruption or loss of personal or business data and identity theft.

Adding the activation requirement to Microsoft software helps prevent keys from being widely leaked. This minimizes the use of counterfeit software. For more information about the Business Software Alliance study, see Sixth Annual BSA and IDC Global Software Piracy Study (*http://go.microsoft.com/fwlink/?LinkId=155960*).

Privacy

All methods of activation used by Microsoft are designed to help protect user privacy. The data that is collected is used to confirm that you have a legally licensed copy of the software. It is then aggregated for statistical analysis. Microsoft does not use this information to identify you or contact you.

Office Activation Technologies

Office Activation Technologies provide methods for activating products that are licensed under Microsoft Volume Licensing programs. Most Office Volume Licensing customers are familiar with Volume License Keys (VLKs) that were issued under a specific license agreement. This key effectively "bypassed" activation. For Office 2010, Office Activation Technologies help automate and manage the activation process while addressing the piracy and product key management problems that arose with keys issued for Office Enterprise 2007.

You can use the following methods to activate Office 2010 by using Office Activation Technologies, which are the same methods that are used for Windows Vista, Windows Server 2008, and later versions of Windows. The kind of product key entered determines the activation method:

- **Key Management Service (KMS)** A computer serves as the KMS host, which requires an Office 2010 KMS host key to be installed and activated. This establishes a local activation service in your environment. Office 2010 client computers connect to the local KMS host for activation.
- **Multiple Activation Key (MAK)** With a MAK key, Office 2010 client computers activate online by using the Microsoft hosted activation servers or by telephone.
- **A combination of KMS and MAK** For example, desktop computers that are running Office 2010 will have the KMS client key installed, whereas portable computers that are running Office 2010 will have the MAK key installed.

To learn about which volume activation method to use, see Plan volume activation of Office 2010

Key Management Service (KMS)

KMS enables product activations on the local network. This eliminates the need for individual computers to connect to Microsoft for product activation. It is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. A computer is required to be configured as a KMS host. The KMS host contains a customer-specific volume license key (KMS host key) for each product to be activated and connects one time to Microsoft hosted servers for activation. Computers that are running Windows Server 2003, Volume License editions of Windows 7, or Windows Server 2008 R2 operating systems can be configured as Office 2010 KMS hosts.

Only one Office KMS host key is required to activate all Volume License editions of Office 2010 client products.

Important:
The Office 2010 KMS host key is not specific to the operating system. It is designed to be used on any of the operating systems that were mentioned earlier, including both 32-bit and 64-bit editions.

Office 2010 KMS clients

KMS clients are computers that are running Volume License editions of Office 2010, which are preinstalled with a KMS client key. KMS clients connect to an organization's KMS host to request activation. Office 2010 KMS clients can be installed on the operating systems listed in System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).

By default, a KMS client key has already been installed in Volume License editions of Office 2010. No action is required by the end user, and you do not have to enter a product key for Office 2010 KMS clients. The only action required by the administrator is the initial activation of the KMS host.

For more information, see Plan a KMS deployment in Plan volume activation of Office 2010.

Multiple Activation Key (MAK)

A unique MAK key is given to an organization for each Volume License edition of Office 2010. Each computer must then activate one time with the Microsoft hosted activation services. Associated with each key is a count of the number of activations. For example, a MAK key for an Office 2010 product that has 100 activations allows the organization to install the key on 100 computers and activate each one.

MAK is appropriate for organizations with computers that are not connected to the corporate network for long periods of time, such as portable computers. For this to work, a MAK key must be installed instead of the default KMS client key that is used in Volume License editions of Office 2010. There are two ways to activate computers by using MAK. The first method is *MAK independent activation*, which requires that each computer independently connect and activate with Microsoft, either over the Internet or by telephone.

The second method is *MAK Proxy activation*, which is performed by using the Volume Activation Management Tool (VAMT) 2.0 (*http://go.microsoft.com/fwlink/?LinkId=183042*). VAMT 2.0 supports Office 2010 MAK proxy activation. By using this method, a computer collects activation information from multiple computers on the network and then sends a centralized activation request on their behalf. In this setup, the VAMT 2.0 console is the only computer that connects to Microsoft hosted servers. For more information, see Plan a MAK activation in Plan volume activation of Office 2010.

With MAK activation, there is no requirement to periodically renew activation. You must reactivate if significant hardware changes (such as replacing the hard disk drive) are detected or you re-install the operating system. Each reactivation will decrement the number of activations associated with the key. If you save and reapply the confirmation ID from the MAK proxy activation through VAMT 2.0, you can reactivate the same computer without decrementing the number of activations associated with the key, because no connection with Microsoft is made. In addition, you must request more activation allowances when the number of activations passes the predetermined limit. You also have to manage the installation of MAK keys and you might have to manually activate systems by using a telephone when no Internet connection is available.

Note:
Only VAMT 2.0 and later versions can support Office 2010.

Volume License product keys

If you use Volume License editions of Office 2010, planning for volume activation must be part of your Office 2010 deployment process. KMS host keys and MAKs are issued under a specific license agreement to enable organizations to use the licensed products. These keys can be used only with volume licensing products. They cannot be used with retail software or software that is preinstalled on a new computer by an original equipment manufacturer (OEM), unless the organization has an agreement with the OEM to preinstall Volume License editions of the products.

To obtain your KMS host key and MAK keys, go to the Web site where you downloaded Office 2010.

See Also

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*)

Troubleshoot volume activation for Office 2010 (*http://technet.microsoft.com/library/976fc06b-faed-4682-b41f-4a19d8eb3302(Office.14).aspx*)

Office 2010 Volume Activation forum (*http://go.microsoft.com/fwlink/?LinkId=180346*)

Office 2010 forums (*http://go.microsoft.com/fwlink/?LinkId=180345*)

Plan volume activation of Office 2010

This article describes how to plan the testing for Office Activation Technologies. Before you read this article, we recommend that you read Volume activation overview for Office 2010. We also highly recommend that you read the Windows Volume Activation Planning Guide (*http://go.microsoft.com/fwlink/?LinkId=183040*).

In this article:

Plan a deployment

If you are planning a Windows deployment of Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2, you will probably have the same considerations for Windows as for Microsoft Office 2010. To help determine which activation method — Key Management Service (KMS) or Multiple Activation Key (MAK) or both — to use for Windows, see the Windows Volume Activation Planning Guide (*http://go.microsoft.com/fwlink/?LinkId=183040*). Most likely, Office 2010 will use the same method.

A volume activation deployment includes the following steps:

1. Learn about product activation.
2. Review available activation models.
3. Evaluate client connectivity.
4. Map the physical computer or virtual machine to an activation method.
5. Determine product key needs.
6. Determine monitoring and reporting needs.

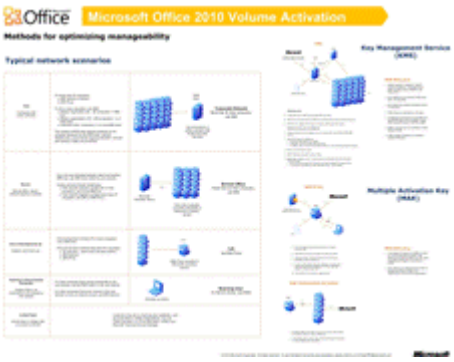
Most of the information is covered in the Windows Volume Activation Planning Guide (*http://go.microsoft.com/fwlink/?LinkId=183040*). This article provides an overview of the technology.

When you plan for Office Activation Technologies, think about the following information:

- The KMS activation threshold for Office 2010 is five computers. This means that Office 2010 client computers will become activated only after five or more client computers have requested activation.
- There is no need to enter a product key for Office 2010 KMS clients. You only need to enter a KMS host key on your KMS host computer.
- If you decide to use MAK, enter the product key either through the Office Customization Tool (OCT) or the Config.xml file. After Office 2010 installation, the product key can be changed by using the

Volume Activation Management Tool (VAMT) 2.0 or the Office Software Protection Platform script (ospp.vbs). For more information about ospp.vbs, see Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*).

For a visual representation of the volume activation methods for Office 2010 and typical network scenarios, see Volume Activation of Microsoft Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=188811*).



Review activation methods

Office Activation Technologies provide two activation methods:

- **Key Management Service (KMS)** A server-client model in which a computer serves as the KMS host, which requires a KMS host key to be installed and activated. This establishes a local activation service in your environment. Office 2010 client computers connect to the local Office 2010 KMS host for activation.
- **Multiple Activation Key (MAK)** With a MAK key, Office 2010 client computers activate online by using the Microsoft hosted activation servers or by telephone.

The kind of key installed determines the activation method. All Office 2010 volume license editions have the KMS client key pre-installed. You do not have to enter a product key if you are deploying KMS clients. If you want to use MAK activation, you have to enter the correct MAK key.

A combination of KMS and MAK can also be used. For example, Office 2010 running on desktops has the KMS client key installed, whereas Office 2010 running on portable computers has the MAK key installed.

The model chosen depends on the size, network infrastructure, connectivity, and security requirements. You can choose to use only one or a combination of these activation models. Typically, the same activation method for a particular instance of Windows would be used for Office. For more information about how to decide which activation method to use, see the Windows Volume Activation Planning Guide (*http://go.microsoft.com/fwlink/?LinkId=183040*).

Key Management Service (KMS)

KMS is a server-client model in which a computer serves as the KMS host. KMS activation requires TCP/IP connectivity. By default, KMS hosts use DNS to publish the KMS service, and client computers connect to the KMS host for activation by using anonymous remote procedure calls (RPCs) through TCP communications port **1688**, which is the default port number when you enable the firewall on a KMS host. You can use the default settings, which require little or no administrative action, or manually configure KMS hosts and clients based on network configuration and security requirements.

To be licensed, the KMS client must be activated. The following table describes the license state of the Office 2010 KMS client with respect to activation.

License state	Description
Licensed	By default, the KMS client attempts activation with the KMS host one time every seven days. (The number of days is configurable.) This design allows the maximum possible time for the client to be in the licensed state. Once the KMS client is successfully activated, it remains in the licensed state for 180 days. When in the licensed state, users do not see any notification dialog boxes prompting them to activate. After 180 days, the activation attempt process resumes. If activation is continually successful, the entire activation experience is transparent to the end-user.
Out-of-tolerance	If activation does not occur during the 180-day period, Office 2010 goes into the out-of-tolerance state for 30 days. Users then see notifications requesting activation.
Unlicensed notification	If activation does not occur during the out-of tolerance state, Office 2010 goes into the unlicensed notification state. Users then see notifications requesting activation and a red title bar.

The KMS host must be installed with a KMS host key and activated before accepting KMS activation requests from KMS clients. For information about how to set up a KMS host, see Prepare and configure the KMS host (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section2*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).

Important

- The KMS host key for Office 2010 is not specific to a particular operating system. It is designed to be used on any of the operating systems supported as an Office 2010 KMS host, including both 32-bit and 64-bit editions:

Publication of the KMS service

The KMS service uses service (SRV) resource records (RRs) in DNS to store and communicate the locations of KMS hosts. KMS hosts use dynamic updates, if available, to publish the KMS SRV RRs. If

dynamic updates are not available or if the KMS host does not have permissions to publish the RRs, you must publish the DNS records manually or configure client computers to connect to specific KMS hosts. This might require changing permissions on DNS to let more than one KMS host publish SRV records.

Note:
DNS changes might take time to propagate to all DNS hosts, depending on the complexity and topology of the network.

Client discovery of KMS

The first time that a KMS client queries DNS for KMS information, it randomly selects a KMS host from the list of SRV RRs that DNS returns. The address of a DNS server that contains the SRV RRs can be listed as a suffixed entry on KMS clients, which allows advertisement of SRV RRs for KMS in one DNS server and KMS clients that have other primary DNS servers to find it.

You can add **priority** and **weight** parameters to the **DnsDomainPublishList** registry value for KMS hosts on Volume License editions of Windows 7 or Windows Server 2008 R2. Doing so enables you to establish KMS host priority groupings and weighting within each group, which specifies the order in which to use KMS hosts and balances traffic among multiple KMS hosts. If you are using priority and weight parameters, we recommend that KMS caching be disabled on the client. This allows the client to query DNS every time that activation is attempted, which will honor the priority and weight parameters, instead of directly contacting the cached KMS host that last resulted in successful activation.

If the KMS host that a client selects does not respond, the KMS client removes that KMS host from its list of SRV RRs and randomly selects another KMS host from the list. If the priority and weight parameters are set, the KMS client will use them while finding another KMS host. Otherwise, KMS hosts are selected randomly. After a KMS host responds, the KMS client caches the name of the KMS host and uses it for subsequent activation and renewal attempts if caching is enabled. If the cached KMS host does not respond on a subsequent renewal, the KMS client discovers a new KMS host by querying DNS for KMS SRV RRs.

KMS activation thresholds

The minimum requirement for Office 2010 KMS activation is a KMS host and at least five KMS clients in a network environment. Five or more computers that are running Office 2010 volume editions must contact the KMS host within 30 days for their activation requests to be successful. When five clients have connected to a KMS host, clients that later connect to the KMS host receive responses that allow the clients to be activated. Due to the re-activation schedule, the original five clients also become activated when they request activation from the KMS host again.

After initializing KMS, the KMS activation infrastructure is self-maintaining. The KMS service can be co-hosted with other services. A single KMS host can support hundreds of thousands of KMS clients. Most organizations can deploy merely two KMS hosts for their entire infrastructure (one main KMS host and one backup host for redundancy).

KMS activation renewal

KMS activations are valid for 180 days. This is called the *activation validity interval*. To remain activated, KMS clients must renew their activation by connecting to the KMS host at least one time every 180 days. By default, KMS client computers attempt to renew their activation every seven days. After a client's activation is renewed, the activation validity interval begins again.

Use KMS for computers that are running Windows and Office 2010 client products

When you use KMS to activate computers that are running both Windows and Office 2010, you have the following options for Office 2010:

- Use the same KMS host on a computer that is running Windows Server 2003, Volume License editions of Windows 7 or Windows Server 2008 R2 (recommended).
- Use separate KMS hosts for computers that are running Windows and Office 2010.

Important:
If you already have a KMS host that is set up to activate Windows products, you still have to install the Office 2010 KMS host license files, enter the Office 2010 KMS host key, and activate the key. To do this, go to the Microsoft Office 2010 KMS Host License Pack (*http://go.microsoft.com/fwlink/?LinkID=169244*) Web site, and then download and run KeyManagementServiceHost.exe.

The operating systems supported as an Office 2010 KMS host are as follows:

- Windows Server 2008 R2
- Volume editions of Windows 7
- Windows Server 2003

If you are already using a computer that is running as your Windows KMS host and you want to co-host the Office 2010 KMS host, follow the steps in Prepare and configure the KMS host (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section2*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).

Multiple Activation Key (MAK)

A MAK key is used for one-time activation with the Microsoft hosted activation services. Each MAK key has a predetermined number of allowed activations. This number is based on Volume Licensing agreements and may not match the organization's exact license count. Each activation that uses a MAK key with the Microsoft hosted activation service counts toward the activation limit. Once Office 2010 is activated, no re-activation is required unless the hardware changes significantly.

There are two ways to activate computers by using a MAK key:

- **MAK Independent Activation** MAK independent activation requires that each computer independently connect and be activated with Microsoft, either over the Internet or by telephone.

MAK independent activation is best suited for computers in an organization that do not maintain a connection to the corporate network.

- **MAK Proxy Activation by using VAMT 2.0** This enables a centralized activation request on behalf of multiple computers that have one connection to Microsoft. MAK Proxy activation is configured by using VAMT 2.0. MAK Proxy activation is appropriate for environments in which security concerns might restrict direct access to the Internet or the corporate network. It is also suited for development and test labs that do not have this connectivity.

MAK architecture

MAK activation requires that a MAK key is installed on a client computer and instructs that computer to activate itself against Microsoft hosted activation servers over the Internet. In MAK Proxy activation, a MAK key must be installed on the client computer by any of the methods previously described. VAMT 2.0 obtains the installation ID (IID) from the target computer, sends the IID to Microsoft on behalf of the client, and obtains a confirmation ID (CID). The tool then activates the client by installing the CID. The CID is saved and can be used later, for example, to activate test computers that have been re-imaged after 90 days.

VAMT 2.0

VAMT 2.0 is a Microsoft Management Console (MMC) snap-in that allows a graphical user interface (GUI) to easily manage Windows and Office 2010 client products with volume license keys installed. You may specify a group of products to activate by using Active Directory Domain Services (AD DS), workgroup names, IP addresses, computer names, or a generic LDAP query. Only VAMT 2.0 and later versions support Office 2010 in addition to Windows.

VAMT 2.0 enables you to easily transition computers between MAK and KMS activation methods by clicking the target computer and installing the appropriate key.

VAMT 2.0 also enables you to trigger activation on a remote computer. If the target computer has a MAK key installed, that computer sends an activation request to the Microsoft activation servers. If a KMS client key is installed, the target computer sends an activation request to the KMS host.

The tool also supports the collection of activation requests from several computers and then sends them to Microsoft hosted activation servers in bulk. This is called MAK proxy activation through VAMT 2.0, and the target computers must have MAK keys installed. For proxy activation only, VAMT distributes the activation confirmation codes from Microsoft hosted activation servers to the computers that requested activation. Because VAMT also stores these confirmation codes locally, it can reactivate a previously activated computer after it is reimaged without having to contact Microsoft.

Plan a KMS deployment

The KMS service does not require a dedicated server. The KMS service can be co-hosted on a server that also hosts KMS for Windows. Specifically, you can configure a computer that is running Windows Server 2003 with KMS 1.1 or a later version installed, Volume License editions of Windows 7, or

Windows Server 2008 R2 to act as a single KMS host that responds to both Windows and Office 2010 KMS client activation requests. This works as long as the appropriate Office 2010 KMS host licenses are installed and a valid KMS host key is installed, and the key is activated against Microsoft hosted activation servers. You can install Office 2010 KMS host licenses by running the Microsoft Office 2010 KMS Host License Pack (*http://go.microsoft.com/fwlink/?LinkID=169244*).

Important:
KMS hosts that were set up by using the Office 2010 Beta release cannot be used to activate client computers that are running the final released version of Office 2010. To activate these client computers, you can either run the release version of Microsoft Office 2010 KMS Host License Pack (*http://go.microsoft.com/fwlink/?LinkID=169244*) and enter the KMS host key on the same KMS host, or set up a new KMS server only for activating the final release version of Office 2010.

Plan DNS server configuration

The default KMS auto-publishing feature requires SRV RR and dynamic update support. Microsoft DNS or any other DNS server that supports SRV RRs, as documented in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2782, and dynamic updates, as documented in RFC 2136 can support KMS client default behavior and KMS SRV RR publishing. Berkeley Internet Domain Name (BIND) versions 8.x and 9.x support both SRV records and dynamic update, for example.

The KMS host must be configured so that it has the credentials needed to create and update SRV, A (IPv4), and AAAA (IPv6) RRs on the dynamic update servers, or the records must be created manually. The recommended solution for giving the KMS host the needed credentials is to create a security group in AD DS and add all KMS hosts to that group. For Microsoft DNS, ensure that this security group is given full control over the _VLMCS._TCP record on each DNS domain that will contain the KMS SRV RRs.

Activate the KMS host

The KMS host must activate with Microsoft hosted activation servers through the Internet or by telephone. Once the KMS host is activated, it does not communicate any additional information to Microsoft. For more information, see Prepare and configure the KMS host (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section2*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).

Prepare KMS clients

By default, Volume License editions of Office 2010 are preinstalled with the KMS client key. This makes them KMS clients, without additional configuration required. KMS clients can locate a KMS host automatically by querying DNS for SRV RRs that publish the KMS service. If the network environment

does not use SRV RRs, you can manually assign a KMS client to use a specific KMS host by configuring the following registry key:

HKLM\Software\Microsoft\OfficeSoftwareProtectionPlatform

The KMS host name is specified by KeyManagementServiceName (REG_SZ), and the port is specified by KeyManagementServicePort (REG_SZ). These registry keys can also be set through the ospp.vbs script. For more information about ospp.vbs, see Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*).

Activate as a standard user

Office 2010 does not require administrator permissions for KMS activation. However, volume editions require administrator permissions for MAK activation. Administrators can enable users who have non-administrator permissions to activate with MAK by setting the appropriate registry key in the deployments or in the master image:

HKEY_LOCAL_MACHINE\Software\Microsoft\OfficeSoftwareProtectionPlatform\UserOperations = 1

This registry key can also be set through the ospp.vbs script. For more information about ospp.vbs, see Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*).

Plan a MAK activation

MAK is recommended for computers that rarely or never connect to the corporate network and for environments in which the number of physical computers needing activation does not meet the Office 2010 KMS activation threshold (five computers). MAK can be used for individual computers or with an image that can be installed by using Microsoft or third-party deployment solutions. MAK can also be used on a computer that was originally configured to use KMS activation, which is useful for moving a computer off the core network to a disconnected environment.

For more information about how to install a MAK key, see Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).

No authenticated proxy server support

Activation over the Internet will be blocked if the proxy server requires user authentication. In Microsoft Internet Security and Acceleration (ISA) Server, this setting is named basic authentication. Because activation requests do not present the user's credentials to the proxy server, we recommend that you do not use basic authentication with ISA Server or other proxy servers. For more information, see Microsoft Knowledge Base article 921471: Activation fails when you try to activate Windows Vista or Windows Server 2008 over the Internet (*http://go.microsoft.com/fwlink/?LinkId=183044*).

See Also

Volume activation overview for Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*)

Troubleshoot volume activation for Office 2010 (*http://technet.microsoft.com/library/976fc06b-faed-4682-b41f-4a19d8eb3302(Office.14).aspx*)

Plan KMS activation of Office 2010

Plan MAK independent activation of Office 2010

Plan MAK proxy activation of Office 2010

Office 2010 Volume Activation forum (*http://go.microsoft.com/fwlink/?LinkId=180346*)

Office 2010 forums (*http://go.microsoft.com/fwlink/?LinkId=180345*)

Plan MAK independent activation of Office 2010

You are required to activate your deployment of Volume License editions of Microsoft Office 2010. This includes Microsoft Office Professional Plus 2010, Microsoft Project 2010, and Microsoft Visio 2010. Activation reduces the possibility of deploying counterfeit software, which can include malware, viruses, and other security risks.

In this article:

Overview of MAK independent activation

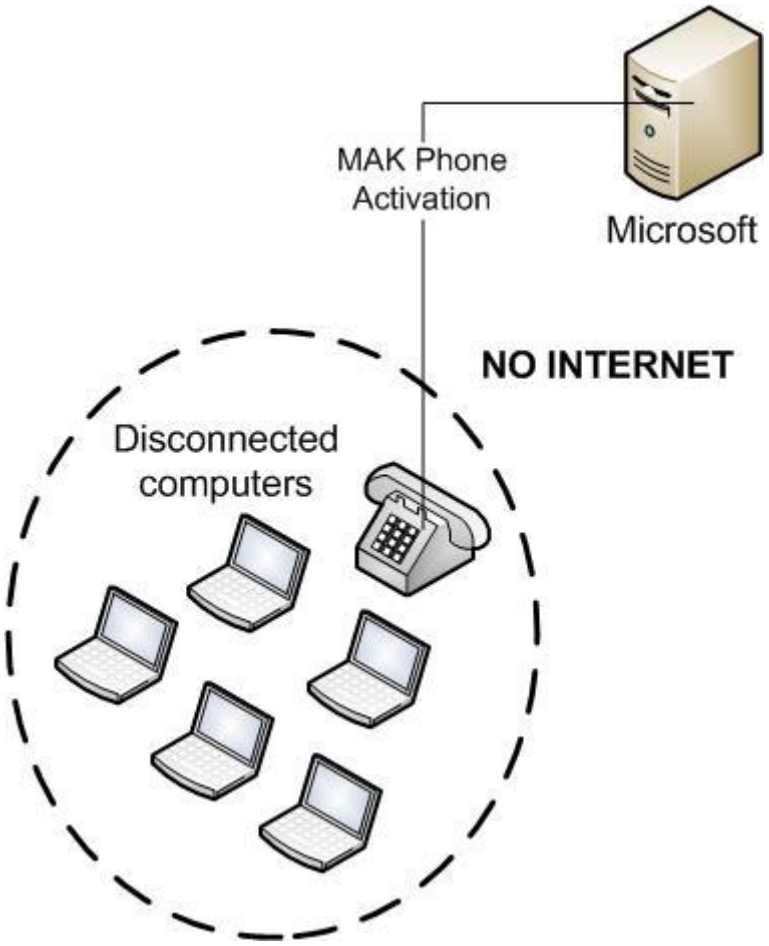
Multiple Activation Key (MAK) activation occurs directly with Microsoft (different from Key Management Service [KMS], in which activation occurs through a local host server). If your organization has five or fewer computers that need to activate Office 2010, we recommend that you use MAK to activate each computer independently. You can also use the Volume Activation Management Tool (VAMT) (*http://go.microsoft.com/fwlink/?LinkId=183042*) to manage all activated computers.

The following are examples of networks that can use MAK independent activation.

Example: Remote sales office that has isolated portable computers

Fabrikam, Inc. has several remote sales offices around the world. Each office has five or fewer portable computers that are isolated from all possible networks or Internet access. The solution is to use MAK activation for the portable computers individually by telephone to Microsoft.

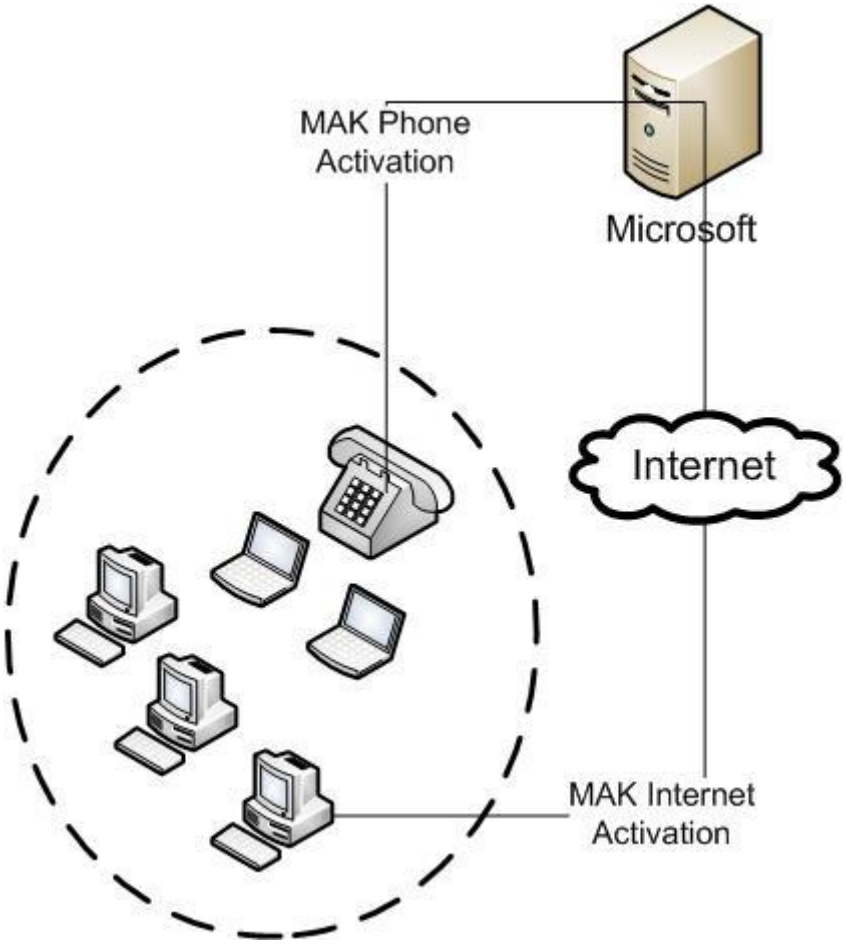
Architecture – Fabrikam sales office example



Example: Small organization that has Internet-connected desktop computers and isolated portable computers

Contoso, Ltd. has three desktop computers that are connected to the Internet and two portable computers that are isolated from the Internet. There are no other networks available. The solution is to manage the MAK activations of the desktop computers through VAMT (http://go.microsoft.com/fwlink/?LinkId=183042), and MAK activate the portable computers by telephone to Microsoft.

Architecture – Contoso small organization example



Plan and assess the Office 2010 environment and configuration

The following articles will help you make sure that your deployment of Office 2010 is properly designed for MAK activation.

- To assess the Office 2010 environment, see Assessing the compatibility of Office 2010 (*http://technet.microsoft.com/library/d0e06c9b-282e-4d83-8f3f-ac0cd7191fbe(Office.14).aspx*).
- To plan the desktop configuration for Office 2010 (if required), see Plan desktop configurations for Office 2010.

- To assess the system requirements for Office 2010, see System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).

Obtain the product keys

To obtain the product keys for Office 2010, register on the Volume Licensing Service Center (VLSC) (*http://go.microsoft.com/fwlink/?LinkId=184280*) Web site. Your license agreement determines the number of MAK activations that you are issued.

MAK independent activation steps

Part of the overall configuration process for Office 2010 is to configure each computer for MAK activation. For more information, see Prepare and configure the Office 2010 client (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section1*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*). Follow the relevant procedure to configure Office 2010 by using the Office Customization Tool (OCT), the Config.xml file, or the Microsoft Office Backstage view.

VAMT management steps

Download and install the VAMT 2.0 tool (*http://go.microsoft.com/fwlink/?LinkId=183042*). Follow the instructions on the download page. For more information about how to use VAMT, click **Help** on the VAMT 2.0 menu bar.

If you increase the number of computers to fewer than 50, we recommend that you use MAK proxy activation for all computers that can connect to a MAK proxy server. For more information, see Plan MAK proxy activation of Office 2010.

If you increase the number of computers to 50 or more, we recommend that you use KMS activation as the activation method for all computers that can connect to a KMS host server. For more information, see Plan KMS activation of Office 2010. Any other computers can activate with MAK by the methods already mentioned.

Note:
For examples of scenarios that require KMS activation combined with MAK activation, see Scenario: Secure network - KMS or MAK activation of Office 2010, Scenario: Roaming or disconnected computers - KMS or MAK activation of Office 2010, and Scenario: Test or development lab - KMS or MAK activation of Office 2010.

See Also

Plan MAK proxy activation of Office 2010

Plan KMS activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Volume Activation Management Tool (*http://go.microsoft.com/fwlink/?LinkId=183042*)

Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*)

Plan MAK proxy activation of Office 2010

You are required to activate your deployment of Volume License editions of Microsoft Office 2010. This includes Microsoft Office Professional Plus 2010, Microsoft Project 2010, and Microsoft Visio 2010. Activation reduces the possibility of deploying counterfeit software, which can include malware, viruses, and other security risks.

In this article:

Overview of MAK proxy activation

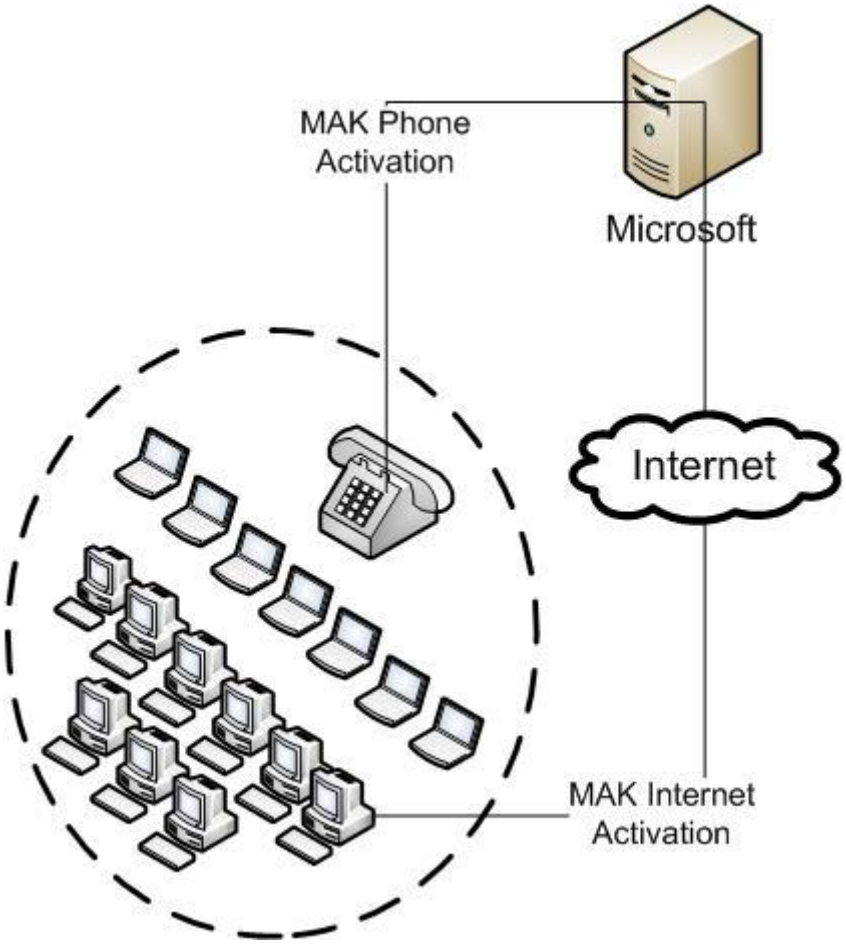
Multiple Activation Key (MAK) activation occurs directly with Microsoft (different from Key Management Service [KMS], in which activation occurs through a local host server). If your organization has 6 to 49 computers that need to active Office 2010, we recommend that you use MAK proxy activations managed through Volume Activation Management Tool (VAMT) (*http://go.microsoft.com/fwlink/?LinkId=183042*) for all computers that can connect to a MAK proxy server. For those computers that are isolated from the corporate network or the Internet, we recommend that you use MAK independent activation through the telephone.

The following is an example of a network that can use MAK proxy activation.

Example: Medium organization that has Internet-connected desktop computers and isolated portable computers

Contoso, Ltd. has 15 desktop computers and 10 portable computers in their single office. The desktop computers are connected to the Internet, and the portable computers are isolated from all networks. The solution is to use VAMT (*http://go.microsoft.com/fwlink/?LinkId=183042*) to manage the MAK proxy activation of the desktop computers through the Internet, while you independently activate the portable computers through the telephone.

Architecture – Contoso medium organization example



Plan and assess the Office 2010 environment and configuration

The following articles will help you make sure that your deployment of Office 2010 is properly designed for MAK activation.

- To assess the Office 2010 environment, see Assessing the compatibility of Office 2010 (*http://technet.microsoft.com/library/d0e06c9b-282e-4d83-8f3f-ac0cd7191fbe(Office.14).aspx*).
- To plan the desktop configuration for Office 2010 (if required), see Plan desktop configurations for Office 2010.

- To assess the system requirements for Office 2010, see System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).
- To configure each computer for MAK activation, see Customize Office 2010 (*http://technet.microsoft.com/library/a33e64b0-46a5-45e5-b76f-3add595af8de(Office.14).aspx*). Follow the relevant procedure to configure Office 2010 by using the Office Customization Tool (OCT), the Config.xml file, or the Microsoft Office Backstage view.

Obtain the product keys

To obtain the product keys for Office 2010, register on the Volume Licensing Service Center (VLSC) (*http://go.microsoft.com/fwlink/?LinkId=184280*) Web site. Your license agreement determines the number of MAK activations that you are issued.

MAK proxy activation steps

To activate Office 2010 by using MAK proxy through VAMT, follow these steps.

1. In VAMT, under **Product Keys**, enter the MAK key in the **Product Key** field, and then click **Verify**.
2. Right-click the computer on which you want to install the MAK key, select **Install Product Key**, select the **MAK key**, and then click **OK**.
3. To activate Office 2010, right-click the computer name, select **Activate**, and then select **Proxy Activate**.

Important:
You must provide administrator permissions for the selected computer.

Note

- If you have 6 to 49 computers in a department or group that are not connected to the corporate network, we recommend that you follow the MAK activation recommendations in this article.
- If you have five or fewer computers in a department or group that are not connected to the corporate network, we recommend that you use MAK independent activation for each computer. For more information, see Plan MAK independent activation of Office 2010.
- If you increase the number of computers to 50 or more, we recommend that you use KMS activation as the activation method for all computers that can connect to a KMS host server. For more information, see Plan KMS activation of Office 2010. Any other computers can activate with MAK by the methods previously described.

VAMT management steps

Download and install the VAMT 2.0 tool (*http://go.microsoft.com/fwlink/?LinkId=183042*) on the MAK proxy server. Follow the instructions on the download page. For more information about how to use VAMT, click **Help** on the VAMT 2.0 menu bar.

Note:
For examples of scenarios that require KMS activation combined with MAK activation, see Scenario: Secure network - KMS or MAK activation of Office 2010, Scenario: Roaming or disconnected computers - KMS or MAK activation of Office 2010, and Scenario: Test or development lab - KMS or MAK activation of Office 2010.

See Also

Plan MAK independent activation of Office 2010

Plan KMS activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Volume Activation Management Tool (*http://go.microsoft.com/fwlink/?LinkId=183042*)

Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*)

Plan KMS activation of Office 2010

You are required to activate your deployment of Volume License editions of Microsoft Office 2010. This includes Microsoft Office Professional Plus 2010, Microsoft Project 2010, and Microsoft Visio 2010. Activation reduces the possibility of deploying counterfeit software, which can include malware, viruses, and other security risks.

In this article:

Overview of KMS activation

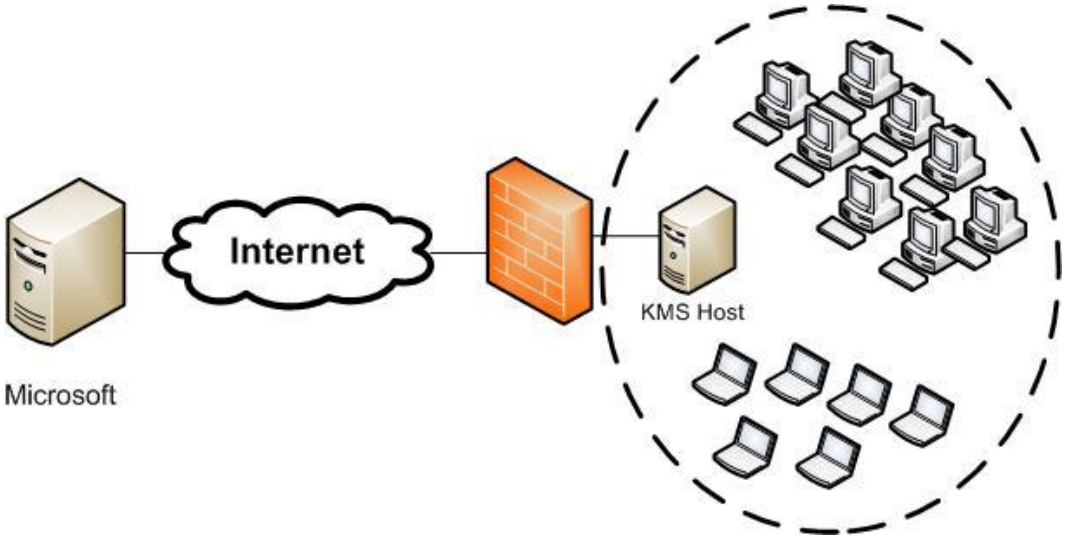
If your organization has 50 or more computers that need to activate Office 2010, we recommend that you use Key Management Service (KMS). KMS activates the computers, or KMS clients, from a KMS host server that contains a KMS host key that is supplied by Microsoft. This method replaces direct activation through Microsoft, and gives the local administrator control of the process. The administrator can easily monitor computers on the network by using the Volume Activation Management Tool (VAMT) (*http://go.microsoft.com/fwlink/?LinkId=183042*).

The following is an example of a network that can use KMS activation.

Example: Medium to large organization that has corporate-connected desktop computers and portable computers

Contoso, Ltd. has 175 desktop computers that are always connected to the corporate network and 50 portable computers that are periodically connected to the corporate network. The solution is to use KMS activation for both the desktop computers and the portable computers, and to make sure that the portable computers are connected for initial activation and at least every 180 days after that for reactivation.

Architecture – Contoso medium to large organization example



Plan and assess the Office 2010 environment and configuration

The following articles will help you make sure that your deployment of Office 2010 is properly designed for Multiple Activation Key (MAK) activation.

- To assess the Office 2010 environment, see Assessing the compatibility of Office 2010 (*http://technet.microsoft.com/library/d0e06c9b-282e-4d83-8f3f-ac0cd7191fbe(Office.14).aspx*).
- To plan the desktop configuration for Office 2010 (if required), see Plan desktop configurations for Office 2010.
- To assess the system requirements for Office 2010, see System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).
- To review the KMS host server requirements, see Prepare and configure the KMS host (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section2*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).
- To configure DNS for the KMS host, see “Understanding KMS” in Customer Hosted Volume Activation Guide (*http://go.microsoft.com/fwlink/?LinkId=187539*).

Note:
At least five computers must request activation from the KMS host before KMS clients can become activated. All KMS clients must connect to the KMS host at least one time every 180 days to reactivate.

Obtain the product keys

To obtain the KMS host product key for Office 2010, register on the Volume Licensing Service Center (VLSC) (http://go.microsoft.com/fwlink/?LinkId=184280) Web site. For the KMS clients, the product keys are preinstalled.

Install KMS on the host computer

The KMS host service is included as part of Windows 7 and Windows Server 2008 R2. Therefore, these two operating systems can be configured as a KMS host without having to install additional software. To configure an Office 2010 KMS host on Windows Server 2003, see To activate an Office KMS host on Windows Server 2003 in Deploy volume activation of Office 2010.

KMS activation steps

- Although you have six KMS host activations on the KMS host key, we recommend that you activate no more than one or two KMS hosts.

  To activate the KMS host on the Internet, run KeyManagementServiceHost.exe in the Microsoft Office 2010 KMS Host License Pack (*http://go.microsoft.com/fwlink/?LinkID=169244*). This is a free download from Microsoft.

  To activate the KMS host on the telephone or manually, and to configure the KMS host, use the **slmgr.vbs** script. For more information, see Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).
- When the KMS host is activated, existing KMS clients activate automatically. Certain instances require KMS clients to be configured by using the **ospp.vbs** script.

  For more information details, see Tools to configure client computers in Office 2010 (*http://technet.microsoft.com/library/1825df76-7e23-459b-a6c1-224dd6eab81e(Office.14).aspx*).

VAMT management steps

Download and install the VAMT 2.0 tool (*http://go.microsoft.com/fwlink/?LinkId=183042*). Follow the instructions on the download page. For more information about how to use VAMT, click **Help** on the VAMT 2.0 menu bar.

If you have five or fewer computers in a department or group that are not connected to the corporate network, we recommend that you use MAK independent activation for each computer.

For more information, see Plan MAK independent activation of Office 2010.

If you increase the number of computers to fewer than 50, we recommend that you use MAK proxy activation through VAMT for all computers that can connect to a MAK proxy server.

For more information, see Plan MAK proxy activation of Office 2010.

Note:
For an example of a scenario that requires KMS activation, see Scenario: Core network - KMS activation of Office 2010. For examples of scenarios that require KMS activation combined with MAK activation, see Scenario: Secure network - KMS or MAK activation of Office 2010, Scenario: Roaming or disconnected computers - KMS or MAK activation of Office 2010, and Scenario: Test or development lab - KMS or MAK activation of Office 2010.

See Also

Plan MAK independent activation of Office 2010

Plan MAK proxy activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Volume Activation Management Tool (*http://go.microsoft.com/fwlink/?LinkId=183042*)

Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*)

Scenario: Core network - KMS activation of Office 2010

This article contains a more complex volume activation scenario than the examples described in Plan KMS activation of Office 2010, Plan MAK proxy activation of Office 2010, and Plan MAK independent activation of Office 2010. The activation method recommended for this scenario is determined by using one or more of the activation methods — Key Management Service (KMS) and Multiple Activation Key (MAK) — described in these articles.

Core network that has 50 or more computers

If your organization has 50 or more computers that regularly connect to the core network, we recommend that you use KMS to activate Microsoft Office 2010. For more information, see Plan KMS activation of Office 2010. Instead of having to activate each computer individually by connecting directly to Microsoft, you can activate all the computers (known as KMS clients) at the same time through a KMS host server on your main corporate network.

Although a single KMS host can activate thousands of KMS clients, you can physically configure up to six KMS hosts depending on the size and complexity of the network. However, for maximum ease and efficiency, we recommend the configuration guidelines shown in the following table.

Core network setup	Number of KMS hosts (see Considerations)
Medium (50-99 computers)	1
Medium (100 - 249 computers)	1 or 2
Enterprise (250 or more computers)	2 or more

For information about the KMS activation method, see Plan KMS activation of Office 2010.

Considerations

When you use KMS activation of Office 2010 in the core network, consider the following factors:

- The number of KMS hosts should be kept to a minimum. One KMS host key can activate up to six KMS hosts, and each KMS host can activate many KMS clients.
- A KMS host can be activated by telephone or through the Internet.
- Each KMS host operates independently from other KMS hosts.

- Each KMS host must ensure that more than five KMS clients request activation in a 30-day period to maintain the KMS client activation threshold.

See Also

Plan KMS activation of Office 2010

Plan MAK proxy activation of Office 2010

Plan MAK independent activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Scenario: Secure network - KMS or MAK activation of Office 2010

This article contains a more complex volume activation scenario than the examples described in Plan KMS activation of Office 2010, Plan MAK proxy activation of Office 2010, and Plan MAK independent activation of Office 2010. The activation method recommended for this scenario is determined by using one or more of the activation methods — Key Management Service (KMS) and Multiple Activation Key (MAK) — described in these articles.

Secure network

If your organization has a secure network — for example, a branch office network or an extranet behind a firewall — we recommend the guidelines shown in the following table for both KMS and MAK activation of Microsoft Office 2010.

Secure network setup	Recommended activation method
The firewall can be opened to access the core network.	Use Plan KMS activation of Office 2010 through a KMS host within the core network.
Policy prevents the firewall from being opened.	• More than 50 computers: Plan KMS activation of Office 2010 through a local KMS host set up within the secure network. • Fewer than 50 computers: Plan MAK independent activation of Office 2010 or Plan MAK proxy activation of Office 2010.

For information about the KMS activation method, see Plan KMS activation of Office 2010.

For information about the MAK proxy activation method, see Plan MAK proxy activation of Office 2010.

For information about the MAK independent activation method, see Plan MAK independent activation of Office 2010.

Considerations

When you prepare a secure network for volume activation of Office 2010, consider the following factors:

- The firewall should be configured as RPC over TCP and use TCP port 1688.
- The configuration of the client computer firewall can be initiated by the client computer.

See Also

Plan KMS activation of Office 2010

Plan MAK proxy activation of Office 2010

Plan MAK independent activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Scenario: Roaming or disconnected computers - KMS or MAK activation of Office 2010

This article contains a more complex volume activation scenario than the examples described in Plan KMS activation of Office 2010, Plan MAK proxy activation of Office 2010, and Plan MAK independent activation of Office 2010. The activation method recommended for this scenario is determined by using one or more of the activation methods — Key Management Service (KMS) and Multiple Activation Key (MAK) — described in these articles.

Roaming or disconnected networks

Your organization might include any of the following types of network configurations:

- Networks or computers that never connect the Internet or the core network.
- Roaming computers that periodically connect to the core network through either the following ways:
  - A direct connection to the network.
  - A virtual private network (VPN) connection.
- Roaming computers that are connected to the Internet, but that never connect to the core network.

If so, we recommend the guidelines shown in the following table for both KMS and MAK activation of Microsoft Office 2010.

Network setup	Recommended activation method
Computers with Internet access that never connect to the core network.	Plan MAK independent activation of Office 2010 through the Internet.
Computers without Internet access that never connect to the core network.	Plan MAK independent activation of Office 2010 by telephone.

Networks that cannot connect to the core network.	• Five or more computers (the KMS activation threshold) require activation, then use Plan KMS activation of Office 2010 as follows:
	  • Small organization: 1 KMS host
	  • Medium organization: 1 or more KMS hosts.
	  • Large organization (enterprise): 2 or more KMS hosts.

Network setup	Recommended activation method
	• If fewer than five computers require activation, use Plan MAK independent activation of Office 2010 or Plan MAK proxy activation of Office 2010 (through VAMT (*http://go.microsoft.com/fwlink/?LinkId=183042*).
Computers that periodically connect to the core network directly or through a VPN.	Plan KMS activation of Office 2010 through the KMS hosts in the core network.

For information about the KMS activation method, see Plan KMS activation of Office 2010.

For information about the MAK proxy activation method, see Plan MAK proxy activation of Office 2010.

For information about the MAK independent activation method, see Plan MAK independent activation of Office 2010.

Considerations

When you prepare roaming or disconnected networks and computers for volume activation of Office 2010, consider the following factors:

- There might be restricted environments or networks that cannot connect to other networks.
- A KMS host can be activated, and then moved to a disconnected network.
- Both KMS host activation and MAK independent activation can be done by telephone.
- MAK proxy activation is performed through VAMT.

See Also

Plan KMS activation of Office 2010

Plan MAK proxy activation of Office 2010

Plan MAK independent activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

Scenario: Test or development lab - KMS or MAK activation of Office 2010

This article contains a more complex volume activation scenario than the examples described in Plan KMS activation of Office 2010, Plan MAK proxy activation of Office 2010, and Plan MAK independent activation of Office 2010. The activation method recommended for this scenario is determined by using one or more of the activation methods — Key Management Service (KMS) and Multiple Activation Key (MAK) — described in these articles.

Test or development lab network

If your organization has a network that is used as a short-term test or development lab, which re-images its client computers after testing or development is complete, we recommend the guidelines shown in the following table for both KMS and MAK activation of Microsoft Office 2010.

Network setup	Recommended activation method
Five or more computers that require activation (the KMS activation threshold).	Plan KMS activation of Office 2010 through a single KMS host. **Note:** You can set up a KMS host for each network that has five or more computers to activate.
Fewer than five computers that require activation.	1. If computers are re-imaged within 90 days, no activation is necessary. Simply reset the 25-day grace period as required. See Rearm the Office 2010 installation (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section4*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*). 2. Otherwise, activate with Plan MAK proxy activation of Office 2010 by using the saved confirmation ID (CID). For more information, see MAK architecture in Plan volume activation of Office 2010.

For information about the KMS activation method, see Plan KMS activation of Office 2010.

For information about the MAK proxy activation method, see Plan MAK proxy activation of Office 2010.

For information about the MAK independent activation method, see Plan MAK independent activation of Office 2010.

Considerations

When you prepare a test or development lab network for volume activation of Office 2010, consider the following factors:

- There are generally fewer computers in a lab network than there are in the production network.
- A lab network configuration can vary from setup to setup, and the activation method (KMS, MAK proxy, MAK independent) can also vary.
- If you have more than one lab network, each lab network requires its own activation method.

See Also

Plan KMS activation of Office 2010

Plan MAK proxy activation of Office 2010

Plan MAK independent activation of Office 2010

Plan volume activation of Office 2010

Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*)

FAQ: Volume activation of Office 2010

The following frequently asked questions (FAQ) provide information about various aspects of volume activation of Microsoft Office 2010.

In this article:

Volume Activation FAQ overview

Volume activation is a product activation technology that was introduced with the Microsoft Windows Vista operating system and Windows Server 2008. The technology enables Volume Licensing customers to automate the activation process in a way that is transparent to end users. Volume activation is used strictly to activate systems that are covered under a Volume Licensing program and is not tied to license invoicing or billing. There are two volume activation methods:

- Key Management Service (KMS)
- Multiple Activation Key (MAK)

Customers can use either or both methods within their environment.

- KMS enables organizations to activate Windows systems and Microsoft Office 2010 within their own network. There is one KMS client key for all Office 2010 products, Microsoft Project 2010, and Microsoft Visio 2010.
- MAK activates Windows systems or Office 2010 on a one time basis by contacting the Microsoft hosted activation services either through the Internet or by telephone. There is a unique MAK client key for each volume licensed product.

As part of the installation, it is important to plan and manage deployment of any product that uses volume activation (for example, Windows 7, Windows Server 2008 and Windows Vista). Read the documents and review the videos before you start deployment in your organization. You can find all Office 2010, Project 2010, and Visio 2010 resources at the Volume Activation for Office 2010 Resource Center (*http://go.microsoft.com/fwlink/?LinkId=189005*).

How are volume activation for Office 2010 and volume activation for Windows associated?

Office 2010 has adopted the Software Protection Platform (SPP) introduced with Windows Vista and Windows Server 2008, and the SPP is also used with Windows 7 and Windows Server 2008 R2. Office 2010 client products must be activated either by KMS or MAK.

How does volume activation help Microsoft customers?

Volume activation is useful to customers for the following reasons:

- **Reliability** Studies have shown that the process of downloading counterfeit software often results in the introduction of other malicious code, such as keystroke loggers and Trojan horses, which can put the security of the user and the ecosystem at risk. Volume activation helps reduce that risk and provides better reliability and stability.
- **Supportability** Software versions that are validated as Office genuine and activated receive the full range of support offered by Microsoft.
- **License compliance** Volume activation tools help determine which software is installed and activated, which reduces the risk of software being out of compliance.

Is volume activation connected to licensing?

Activation is connected to licensing. However, activation is not license enforcement. There is no change to existing Volume Licensing agreements or programs. Keys and corresponding activation limits (MAK only) depend on the specific Volume Licensing agreement that the user has. Microsoft uses the information collected during activation to confirm that the user has a licensed copy of the software, and the information is aggregated for statistical analysis. Microsoft does not use the information to identify or contact customers.

Can an Office activated installation be rearmed?

No. An Microsoft Office-activated installation cannot be rearmed at present.

Are there any changes specific to volume activation regarding Office 2010, Project 2010, and Visio 2010?

Volume activation changes are available in the following areas:

- Only one Office 2010 KMS client key is required to be installed and used for activation. The Office 2010 KMS client key activates any version of Office 2010 suites, Office 2010 applications, Project 2010, and Visio 2010.
- Office 2010 has a specific MAK for each product version; for example: Office 2010 Standard MAK, Word 2010 MAK, Visio 2010 MAK, and so on.

For more information, see the Volume Activation for Office 2010 Resource Center (*http://go.microsoft.com/fwlink/?LinkId=189005*).

Are there any changes specific to volume activation regarding Windows 7 and Windows Server 2008 R2?

Volume activation is applicable to the following areas:

- Activation of virtual computers.
- Using a Windows Server 2008 R2 KMS key and Windows 7 KMS key for earlier versions of the products.
- Deployment improvements and improvements in performance, product key management, and reporting.

- Inclusion of Office 2010, Project 2010, and Visio 2010 on the same activation platform as Windows Vista, Windows Server 2003, and Windows Server 2008.

For more information, see Windows Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=184668*).

Which activation method should be used for virtual computers?

Either MAK or KMS can be used to activate virtual computers. However, KMS is the preferred method, because each time that a computer is activated by using a MAK, the number of activations is decremented. This applies to both physical and virtual computers.

- Windows Vista with SP1, Windows Server 2008, Windows Server 2003 v1.1, and Windows 7 support hosting KMS on a virtual server.
- For Windows Vista with SP2, Windows Server 2008 with SP2, Windows 7, Windows Server 2008 R2, and Office 2010, virtual computers count toward the activation threshold for KMS. For more information, see Windows Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=184668*).
- Each KMS host key can be used to set up six physical or virtual KMS hosts.
- When using KMS, customers must have at least five clients requesting activation. This non-configurable threshold helps ensure that the activation service is used only in an enterprise environment and that it serves as a piracy protection mechanism. Servers can be physical or virtual, so it does not take a large deployment to meet the required minimums.
- A dedicated server is not needed to run KMS for Office 2010. A KMS host is a lightweight service, and you can co-host an Office 2010 and Windows KMS host. However, only Windows Server 2003, volume editions of Windows 7, and Windows Server 2008 R2 are supported as Office 2010 KMS hosts.

Can an Office 2010 KMS host run on a virtual computer?

Yes. An Office 2010 KMS host can run on a virtual computer that has Windows Server 2003, volume editions of Windows 7, and Windows Server 2008 R2.

Must the language version of Office 2010 KMS host for Windows Server 2003 match the language version installed on the server?

Yes, the language version of the Office 2010 KMS host for Windows Server 2003 must match the language version that is installed on the server. This requirement applies only to KMS for Windows Server 2003.

Must the language version of Office 2010 clients that are to be activated by an Office 2010 KMS host for Windows Server 2003 match the language version that is installed on the server?

No. The language versions of Office 2010 clients do not have to match the language version of the Office 2010 KMS host for Windows Server 2003 and the server. This requirement applies only to KMS for Windows Server 2003.

I purchased new client computers preinstalled with Windows 7 Professional and plan to downgrade to an earlier version of Windows. What key can I use?

Choose a key based on the following:

- A KMS host activated with a Windows 7 KMS key activates Windows Vista and Windows 7 KMS clients.
- A KMS host activated with a Windows Vista KMS key activates Windows Vista KMS clients.
- Windows Vista can also use MAK.

If you want to downgrade to Windows XP, you must use only the Windows XP Professional key.

If a "child" company (owned by a "parent" company) has an individual agreement, can the parent company use the same key (such as a Windows Server 2008 Standard/Enterprise R2 KMS key) to deploy Windows 7 and Windows Server 2008 R2 across both companies?

Although they can choose to do so, customers do not have to use keys provided under a specific Licensing ID (agreement, enrollment, affiliate, or license) with the licenses specified under that Licensing ID. Customers have this flexibility so that they can centrally manage their deployment/image. They can choose to use keys specific to agreements/licenses or one set of keys for all.

What if we do not activate our computers?

Activation is designed to provide a transparent activation experience for users. If within the grace period provided (usually 30 days), activation does not occur, Windows or Office 2010 transitions into notification mode. During notification mode for Windows, the user sees activation reminders during logon. In Windows 7, for example, the user sees a notification in the Action Center (*http://go.microsoft.com/fwlink/?LinkId=189038*), and the desktop background is set to black.

What is the difference between Reduced Functionality Mode and Notification mode?

Under *Reduced Functionality Mode* (applies to retail only), the application can only be accessed under a restrictive mode with constrained capabilities when it is not properly activated within the grace period of 30 days. It is important to note that all volume customers have no reduced functionality and only experience regular notifications beyond the grace period. *Notification mode* (applies to all volume systems running Office 2010) is a licensing state in which the user receives clear, recurring reminders about activation if activation is not completed within the grace period.

What if customers are a victim of counterfeit software or license non-compliance?

Microsoft provides various licensing options known as Get Genuine legalization offers.

Can I use my Volume License Keys to exercise my reimaging rights?

Yes. Reimaging rights are granted to all Microsoft Volume Licensing customers. Under these rights, customers can reimage original equipment manufacturer (OEM), or full packaged product (FPP) licensed copies by using media provided under their Volume Licensing agreement, as long as copies made from the Volume Licensing media are identical to the originally licensed product.

As a Volume Licensing customer, the Volume License keys that you need can be found on the Product Key page. You can also request your keys through the Activation Call Centers. For a list of call centers, see Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*). If you are an Open License customer, you must purchase at least one unit of the product that you want to reimage to obtain access to the product media and receive a key.

For more information, see “Re-imaging Rights” in About Licensing (*http://go.microsoft.com/fwlink/?LinkId=154939*).

With a VPN connection, how long do I have to activate?

The reminder is every two hours. Once activated, the reminder changes to every seven days. These are default settings that can be customized through ospp.vbs. Mobile users on the VPN can activate manually either by launching an Office 2010 application to send the activation request or by running **ospp.vbs /act**.

On a remote computer, how do I remove the red bar in the application?

Connect through the VPN, and then activate as described in the previous answer.

Can I set Group Policy for Windows Management Instrumentation (WMI)?

Yes. Through Group Policy, you can open up the firewall to allow WMI.

Can activation information be pulled through System Center Configuration Manager (SCCM)?

Yes.

Does sysprep automatically rearm Office 2010?

No. At present, sysprep does not have this capability.

What if I do not rearm before imaging?

Imaged computers are then recognized as the same computer. The request counter does not increment, and the computers do not activate.

What about Token Activation?

Token activation can be used with Office 2010 for specific highly secure customers.

Key Management Service (KMS) FAQ

KMS is a lightweight service that does not require a dedicated system and can easily be co-hosted on a system that provides other services. By using KMS, you can complete activations on your local network. This eliminates the need for individual computers to connect to Microsoft for product activation.

KMS requires a minimum number of physical or virtual computers in a network environment. You must have at least five computers to activate computers running Windows Server 2008 or Windows Server 2008 R2, at least 25 computers to activate computers running Windows Vista or Windows 7, and at least 5 computers running Office 2010, Project 2010, and Visio 2010. These minimums, known as *activation thresholds*, are set so that they can easily be met by enterprise customers.

For more information about activation thresholds, see Windows Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=184668*). For Office 2010, Project 2010, and Visio 2010, see Volume activation quick start guide for Office 2010 (*http://technet.microsoft.com/library/dbff777c-3a2d-4d8e-a7be-6c45900c73c2(Office.14).aspx)* and Volume activation overview for Office 2010.

A KMS key is used to activate only the KMS host with a Microsoft activation server. A KMS key can activate up to six KMS hosts with 10 activations per host. Each host can activate an unlimited number of computers. If you need to activate more than six KMS hosts, contact your Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*), and state why you must increase the activation limit.

Warning:
For more details about product activation, see Windows Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=184668*) and Volume Activation for Office 2010 Resource Center (*http://go.microsoft.com/fwlink/?LinkId=189005*).

I have installed part of the Office 2010 suite that requires KMS. What is the impact on functionality?

There is no impact as long as the installation follows all the outlined steps.

Can the Office 2010 KMS license and key install on Windows 7 and Windows Server 2008 R2?

Yes.

Are there separate KMS host keys for Office 2010?

One KMS Host key can activate all Office 2010 client products.

My organization's KMS host computer was activated by using a Windows Server 2008 KMS key. Can I use that same computer as a host to deploy Windows Server 2008 R2?

Existing KMS hosts installed on Windows Server 2003, Windows Server 2008, or Windows Vista must be updated to support activation of Windows 7 and Windows Server 2008 R2 in addition to Office 2010, Project 2010, and Visio 2010. This update is available through Windows Server Update Services (WSUS) (*http://go.microsoft.com/fwlink/?LinkId=151433*), the Microsoft Download Center (*http://go.microsoft.com/fwlink/?LinkId=189018*), and Windows Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=184668*). After installing the update, you can install the Windows Server 2008 R2 KMS key on the host and activate.

Can you use these activation tools to true-up?

Activation itself is not intended to assist customers in correcting licensing.

- Activation is not linked to true-up. There is no automated way to do true-up by using KMS host or Volume Activation Management Tool (VAMT) (*http://go.microsoft.com/fwlink/?LinkId=183042*).
- KMS host or VAMT are not intended as reporting tools. However, a user who uses Microsoft System Center can use it to keep a count of activations.

Can I run the slmgr.vbs script in Safe Mode?

No. Activation information is unavailable in Safe Mode.

What if a computer is in a test lab or is disconnected?

- If a test lab has enough physical and virtual computers to meet the KMS threshold, the system administrator can deploy KMS to activate Microsoft Office 2010 client installations in the lab. The KMS host can be activated by telephone.

- If a computer has occasional connectivity to the Internet, the Office client installation can activate with Microsoft directly by using MAK through the Internet or by telephone.
- If the computer has no network connectivity, it can be activated by telephone, or through MAK Proxy activation by using VAMT.

Why is the Office 2010 KMS host supported only on Windows Server 2003, Windows 7, and Windows Server 2008 R2?

Microsoft made the decision based on the release cycle of Office 2010. Office 2010 ships after Windows 7 ships. Microsoft anticipates that most customers will upgrade from Windows Server 2003 to Windows Server 2008 R2. Microsoft believes Windows Server 2008 R2 will replace Windows Server 2008 in the channel after release, so it will be the most recent version that customers receive.

For the Office 2010 KMS host, why is Windows Server 2008 not supported?

Windows Server 2003 originally did not have a KMS service, so it was easy to add the KMS service to it. Windows Server 2008 has a code base that is different from Windows 7 and Windows Server 2008 R2. Supporting Windows Server 2008 for the Office 2010 KMS host requires a complete overhaul of the code, which is not cost-effective.

Why can Windows Server 2008 R2 and Windows 7 be activated simply by patching Windows Server 2008?

This patch contains license files that recognize the new KMS host key to activate Windows Server 2008 R2 and Windows 7. No change to the KMS service is required.

What if my configuration won't allow me to upgrade my Windows Server 2008 computer? Is there any other alternative for setting up an Office 2010 KMS host?

You can set up a Windows Server 2003, Windows 7, or Windows Server 2008 R2 virtual machine on the Windows Server 2008 computer, and then set up the Office 2010 KMS host on the virtual machine.

What does the error, “The KMS host cannot be activated,” mean?

It means that the KMS host key threshold is surpassed. There are several possible sources for this error:

- KMS host for Office 2010 can be set up only on one of the following servers: Windows Server 2003, Windows Server 2008 R2 and Windows 7. Using another operating system causes this error to appear.
- For Windows Server 2003, install KMS host version 1.2 (version 1.1 does not count virtual computers into the threshold). Follow the instructions specified in Microsoft Knowledge Base article 968915: An update is available that installs Key Management Service (KMS) 1.2 for Windows Server 2003 Service Pack 2 (SP2) and for later versions of Windows Server 2003 (*http://go.microsoft.com/fwlink/?LinkId=183046*).
- Not enough computers to reach the threshold for the KMS host to activate.
- The KMS client configuration is incorrect.

How do I enable the firewall for KMS host activation?

Make sure that the TCP communications port number is set to the default of **1688**.

If I suspect that my KMS host key is leaked, can it be blocked from further activations?

Yes, you can work with Microsoft to block a KMS host key. For more information contact your Activation Call Center. For a list of call centers, see Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*).

What does a count of -1 mean?

A count of -1 means that no clients have contacted the KMS host.

Can I expose my KMS host to the Internet so my outside users can activate against it?

You are responsible for both the use of keys assigned to you and the activation of Office 2010 clients through your KMS hosts. You should not disclose keys to non-Microsoft parties, and you must not provide unsecured access to your KMS over an uncontrolled network such as the Internet.

What provisions are available for KMS host failover?

Multiple KMS hosts can be registered in DNS SRV resource records. If one KMS host is down, the KMS client computer will choose another from the list. If direct registration is used on the KMS Office client, you can use round-robin DNS or network load-balancing mechanisms (software or hardware) to increase KMS host availability.

Do I have to back up the KMS service data?

You do not have to back up KMS service data. However, if you want a record of KMS activations, you could keep the Key Management Service log on the Applications and Services Logs folder to preserve activation history.

If a KMS host fails, how do I restore a backup KMS host?

You merely replace the failed KMS host with a new KMS host that uses the same configuration and ensure that the SRV resource record of the new KMS host is added to DNS if you are using DNS auto-discovery. The old SRV record is eventually deleted if record scavenging is implemented for DNS, or you can delete it manually. The new KMS host then starts to collect renewal requests, and KMS clients begin to activate as soon as the KMS activation threshold is met.

When routine cleanup of event logs is performed, is there a risk of losing the activation history stored in the event log?

Yes. If you use a cleanup tool, consider exporting data from the **Key Management Service**. Log on the **Applications and Services Logs** folder to archive activation history. You do not have to do this if you use the Operations Manager KMS Management Pack updated for Office. This Management Pack collects event log data and stores it in the Operations Data Warehouse for reporting.

Many organizations block all ActiveX as a security measure. Does volume activation use ActiveX in the same manner as Genuine Validation does?

Volume activation does not use ActiveX. It uses WMI properties and methods. These are described in Appendix 1 of the Volume Activation 2.0 Operations Guide, which you can download on the Volume Activation 2.0 Technical Guidance (*http://go.microsoft.com/fwlink/?LinkId=190472*) page.

How do I respond to, "Activation server determined that Specific Product key could not be used, when activating the KMS host with the KMS key"?

This message can be caused by any of the following:

- KMS host key has more than six activations (the maximum is six activations).
- Commands were not run correctly during activation of the KMS host.
- KMS host key was leaked and the activations are used up (see first bullet).

I have deployed Microsoft Office 2010 clients but the KMS host did not receive activation requests. Where do I go to check my current status of activation requests on the client-side?

On the client computer, go to the Microsoft Office Backstage view for any Office 2010 application. Click the application name, and the status is displayed in the upper-right corner.

Where do I go to check my current status of activation requests on the server side?

On the server side, use slmgr.vbd to check activation requests. For more information, see Configure the Office 2010 KMS host (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060.aspx#section6*) in Deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/b418501a-eb83-4991-8ea9-b18e7309e060(Office.14).aspx*).

We have to see servers by either name or IP. Is there a command or a way to see which servers are activated using the KMS?

- The following command shows you a list of KMS that are registered in DNS and available to provide activation to clients: **Nslookup –type=srv _vlmcs._tcp**.
- On the client side, **slmgr/dlv** provides all the information.
- On the KMS host, you can monitor the KMS events or you can use Microsoft System Center Operations Manager.

Multiple Activation Key (MAK) FAQ

A MAK requires computers to connect one time to a Microsoft activation server. Once computers are activated, no further communication with Microsoft is required.

What are the activation methods for MAK?

There are two activation types for MAK: MAK independent activation and MAK proxy activation.

Note:
Each MAK has a predetermined number of allowed activations, based on your Volume Licensing agreement. To increase your MAK activation limit, contact the Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*).

- **MAK independent activation** Each computer individually connects to Microsoft through the Internet or telephone to complete activation.
- **MAK proxy activation** MAK proxy activation uses VAMT (*http://go.microsoft.com/fwlink/?LinkId=183042*), which is part of the Windows Automated Installation Kit (*http://go.microsoft.com/fwlink/?LinkId=180604*) for Windows 7. One centralized activation request is made on behalf of multiple computers by using one connection to Microsoft

online or by telephone. This method enables IT professionals to automate and centrally manage the MAK volume activation process.

Can I use both MAK and KMS keys for deployment across my organization?

Yes. KMS, MAK, or both can be used to activate volume licensed Windows and Office 2010 computers.

My organization plans to use our MAKs to activate most of our computers. The amount of activations provided by our MAKs does not match the number of licenses that we have purchased. Why don't the activations match our licenses purchase, and what do I need to do to request more activations?

There are many benefits to using KMS as the preferred activation method, and most customers choose to do so. Using KMS as the primary method of activation is one reason that we do not match the number of licenses and activations on a MAK, because the MAK might not be used. Microsoft looked at many factors to determine the number of activations associated with each MAK. These include licenses purchased, the customer purchase pricing level, and the Volume Licensing program.

For Open License customers, we look at the number of licenses they have and usually give them more than what might be needed to ensure activations are available for scenarios such as reactivations and virtual machine (VM) licensing rights. For example, if a customer purchases between 1-25 licenses, they can get 50 activations on their MAK. For Select, Enterprise Agreement, Campus Agreement, School Agreement, and SPLA, we look at the pricing levels (A, B, C, D) and give a specific amount of activations for each level based on the general amount of licenses purchased for each level. We also consider that KMS is the most common activation method to use.

To increase your MAK activation limit, contact the Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*).

I want to reimage Windows 7 Professional by using MAK activation rather than KMS. What if I don't have enough MAK activations to do so?

First, check how many activations are associated with the Windows 7 MAK by going to the product key page, or by using VAMT (*http://go.microsoft.com/fwlink/?LinkId=183042*), which is part of the Windows Automated Installation Kit (*http://go.microsoft.com/fwlink/?LinkId=180604*) for Windows 7.

To increase your MAK activation limit, contact the Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*).

How do customers get a MAK activation limit revised?

Customers can check their MAK allocation limit, check remaining activations on the keys, and request to increase the activation limit by contacting the Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*).

Why is a key with a 250-activation limit not given to someone with a Volume Licensing agreement that contains 49 licenses? Will they not activate more than their license allows for?

- MAK limits on keys are specific to the programs - Open and Select, as shown in the following table. For example, Open_MAK_50 means that key has 50 activations.

Open	Select
Open_MAK_50	Select_MAK_500
Open_MAK_100	Select_MAK_1000
Open_MAK_250	Select_MAK_2500
Open_MAK_500	Select_MAK_5000
Open_MAK_750	
Open_MAK_1000	

- Therefore, a customer who has up to 35 licenses could have an Open_MAK_50 key, for example, which enables them to install and activate 35 computers. However, if one hard disk fails and it is replaced, that computer must be reactivated.

What happens when a customer receives a MAK key and creates a single installation image? How is the upper limit of the MAK key accounted for?

For example, if a customer is using an Open_MAK_50 key, the system administrator creates an image, and users can install the image on a large number of computers. During this phase, the piracy solution has not yet triggered, and the MAK upper limit has not been reached. The MAK upper limit is reached when these computers try to activate by using Microsoft Activation services. Computers 1 through 50 successfully activate, but with computer 51, activation fails and the remaining computers receive Unlicensed Notifications.

Is there a time limit on how long a MAK activation remains activated?

No. the MAK activation is permanent.

Will MAK-activated clients ever be required to activate through KMS?

No, but if you want to reactivate the MAK-activated clients through KMS after setting up a KMS host, you simply change the client product key.

What do I do if I use up all of my MAK activations?

Contact Microsoft and explain the situation. You will be provided additional activations (under reasonable circumstances).

During setup, what if I want to transition from MAK to KMS?

You can do either of the following:

- Wait to activate when the number of Office 2010 clients is above the KMS activation threshold.
- Activate the first few Office 2010 clients by using MAK, and then change the client product keys to KMS when the number of clients is above the KMS activation threshold.

Volume Activation Management Tool (VAMT) FAQ

The Volume Activation Management Tool (VAMT) enables IT professionals to automate and centrally manage the volume activation process.

Will VAMT install on any Windows operating system?

Yes.

Will VAMT install on any computer, not necessarily on a KMS host?

Yes. VAMT is primarily used for MAK activation, but can be used to monitor KMS activations.

If I want to MAK activate a certain number of computers through VAMT, can I configure the computers to detect the VAMT automatically?

Computers cannot detect VAMT. VAMT is simply a tool that allows you to manage the MAK activation of one or more computers. For more information, see Plan volume activation of Office 2010.

The Error Code Lookup tool does not show the content of an error returned by VAMT on Windows XP or Windows Server 2003.

Volume Activation 2.0 errors are native to Microsoft Windows Vista operating system and Windows Server 2008 operating systems. VAMT relies on the operating system to provide descriptive text for some error codes. This text is not available for Windows XP or Windows Server 2003 systems. To look up the text associated with such error codes, install VAMT on a computer that is running Microsoft Windows Vista operating system, or run **SLUI 0x2A <error_code>** at a command prompt on a computer that is running Microsoft Windows Vista operating system.

Does VAMT require Internet access to function?

Certain operations available in VAMT require Internet access. These include retrieving the remaining MAK activations count, and the retrieve confirmation ID (CID) step in MAK Proxy activation. However, most VAMT operations do not require Internet access.

Is the CID saved for image activation?

Yes.

When changing out a hard drive or re-imaging, can I use the MAK CID?

Yes, through VAMT. Hardware changes are not an issue with KMS. Be aware that changing out the hard drive most likely can cause hardware drift and a need for reactivation.

Does VAMT need to be activated?

No.

Can I run VAMT on a virtual computer?

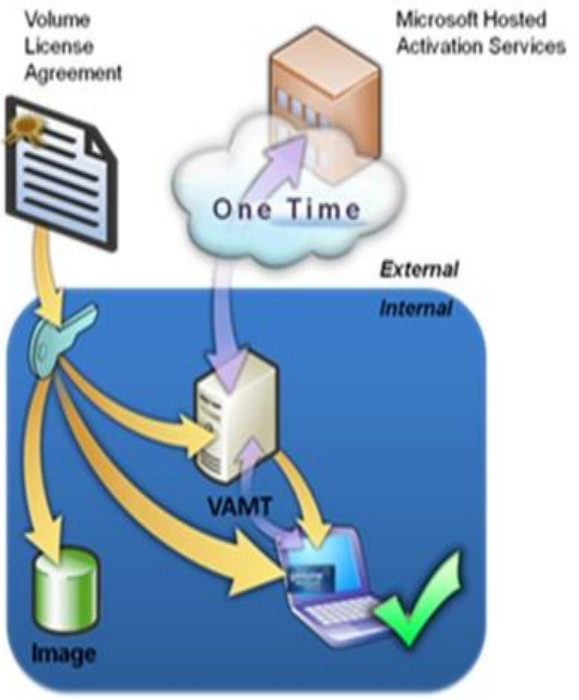
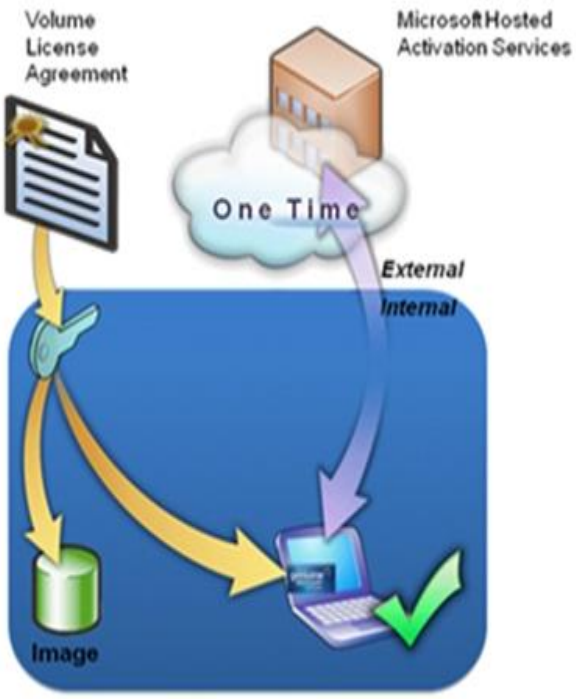
Yes.

What customer problem are we solving with the Volume Activation Management Tool in a MAK scenario? Is this not similar to KMS, if we have an activation with a customer hosted VAMT in a MAK scenario?

- MAK activation occurs directly with Microsoft Hosted Activation Services in which a user enters the key in the Office 2010 user interface. The rationale for using VAMT is that it provides convenience

to the system administrator so that the MAK can be applied to multiple computers at the same time, instead of having to apply the MAK on each computer one at a time.

- Perform proxy activation for Office 2010 installations that do not have Internet connectivity.
- The difference with KMS is that without a KMS host, KMS clients cannot be activated. VAMT is not comparable to KMS and is a way to deploy MAKs to individual Office 2010 clients. KMS manages activations on the customer's network without administrative overhead beyond the initial setup.

Option 1: With VAMT	Option 2: Without VAMT
	

Product Keys FAQ

Product keys enable use of the software products that you have licensed under a specific Volume Licensing program. The product keys on this site should be used only with Volume License products and are intended for use only by your organization.

What is a Setup key?

Setup keys are used for each product/version combination to "unlock" the product and will bypass activation. There are three ways to obtain setup keys:

- **Physical fulfillment** For products obtained through physical fulfillment, the setup key is printed on the media sleeve.

- **Download fulfillment** For products obtained by download, the setup key is provided with the download.
- For products that are available for download from the Volume Licensing Service Center (*http://go.microsoft.com/fwlink/?LinkId=184280*), the setup key is provided on the download screen and might be accompanied by the following text: "Some products available for download require setup keys. Please take note of this setup key as it will be needed during product installation."
- Call the appropriate Microsoft Activation Centers Worldwide Telephone Numbers (*http://go.microsoft.com/fwlink/?LinkId=182952*) to obtain the setup keys that you need. You will be asked to provide Volume Licensing agreement information and proof of purchase.

Are product keys required for all Volume Licensing products?

No, not all products require a product key. To view the list of products that require a Volume License product key, see Product Activation and Key Information (*http://go.microsoft.com/fwlink/?LinkId=110471*).

How do I respond to "Invalid Volume License Key" or "Use a different type of key" or "Invalid key for activation"?

These messages can be caused by either of the following:

- The administrator tries to install a KMS Host key on a KMS client.
- Mismatch between SKU and key.

How does Microsoft determine which product keys are associated with my agreement?

Volume License product keys are provided for each Licensing ID listed in the Microsoft Relationship Summary. You can have several Licensing IDs. For more information about the Licensing ID and the Relationship Summary, see Frequently Asked Questions Overview (*http://go.microsoft.com/fwlink/?LinkId=189254*).

- Enterprise Agreement (EA) customers receive all applicable Volume License keys for available products.
- Select Agreement customers receive keys per product pool (systems, servers, applications) based on their purchasing forecasts.
- Select Plus Agreement customers receive all applicable Volume License key for available products.
- Open License and Open Value customers receive applicable keys based on their license purchase.

For more information about reimaging and downgrade, see "Re-imaging Rights" in About Licensing (*http://go.microsoft.com/fwlink/?LinkId=154939*). EA, Select, and Select Plus customers are also provided with evaluation rights and limited software copies for training and backup.

How do I know which key should be used?

For Windows products, see the video, Fundamentals of Volume Activation (*http://go.microsoft.com/fwlink/?LinkId=150087*). For Office 2010, Visio 2010, and Project 2010, see the video, "Volume Activation for Office 2010 Products" at the Volume activation for Office 2010 Resource Center (*http://go.microsoft.com/fwlink/?LinkId=189005*).

How do I respond to, “Activation server determined that Specific Product key could not be used, when activating the KMS host with the KMS key”?

This message can be caused by any of the following:

- KMS host key has more than six activations (the maximum is six activations).
- Commands were not run correctly during activation of the KMS host.
- KMS host key was leaked and the activations are used up (see first bullet).

See Also

Plan for volume activation of Office 2010

Configure and deploy volume activation of Office 2010 (*http://technet.microsoft.com/library/0327f69a-b908-4a72-bbc2-9be13e359115(Office.14).aspx*)

Office 2010 Volume Activation forum (*http://go.microsoft.com/fwlink/?LinkId=180346*)