For IT professionals: Group Policy for Microsoft Office 2010

Microsoft Corporation

Published: January 2011

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

Abstract

This book contains information about how to use Group Policy to deploy and configure an installation 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

I. Overview of Group Policy and 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.

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

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

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 (*http://go.microsoft.com/fwlink/?LinkID=189156*) download page.

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 (*http://go.microsoft.com/fwlink/?LinkID=189156*) download page.

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. 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

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.

Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool

This article contains information about the new and updated Microsoft Office 2010 Group Policy and Office Customization Tool (OCT) settings that are included in the download package for Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*).

In this article:

Overview of new and removed Group Policy and OCT settings

The download package for Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316)* includes an \Admin folder that contains the Office Customization Tool (OCT) and OCT files, and ADMX and ADML versions of the Office 2010 Administrative Template files for Windows Vista and Windows Server 2008 or later versions of Windows.

Also included in the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool download page (*http://go.microsoft.com/fwlink/?LinkId=189316*) is an updated Microsoft Excel 2010 workbook, *Office2010GroupPolicyAndOCTSettings_Reference.xls* which is available in the **Files to download** section of the download page. This workbook provides the latest information about all Office 2010 Group Policy settings and OCT settings, and also includes the new, deleted, and non-versioned specific settings for both Group Policy and OCT.

Group Policy settings location

To obtain information about the policy settings that are currently in effect for the Group Policy object (GPO) linked to the domain or organizational unit that contains a given computer or user, you can use **Group Policy Results** in Group Policy Management Console. To access Group Policy Results data for a user or computer, you must have **Read Group Policy Results data** permission on the domain or organizational unit that contains the user or computer, or you must be a member of the Administrators group on the targeted local computer.

Unless otherwise noted, you will find local Group Policy settings under the **User Configuration/Administrative Templates** node of the Group Policy Object Editor and OCT settings on the **Modify user settings** page of the OCT.

For information about Group Policy Management Console, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010. For more information about how to report by using Group Policy Results, see "Using Group Policy Results to determine Resultant Set of Policy" in Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).

New administrative templates

New administrative templates are available for Microsoft SharePoint Workspace 2010, a new Office 2010 application. The templates available for this application are spw14.adm, spw14.admx, and spw14.adml for Group Policy.

To review the new policy settings, see Group Policy settings reference for Microsoft Office 2010 (*http://go.microsoft.com/fwlink/?LinkId=189156*).

OCT settings and availability

The OCT settings have two new files extensions: *.opax* is the standard file name extension, and *.opal* is the language-specific extension for the OCT settings.

New OCT files are available for SharePoint Workspace 2010, a new Office 2010 application. The OCT files available for this application are spw.opax, and spw.opal for the OCT.

Preventing conflicts with earlier versions of Group Policy settings

Note:
This section applies only to Group Policy, and not the OCT.

Policy setting information for Office 2010 is stored in version-specific locations in the Windows registry, as shown in the following table.

Type of setting	2010 subkey
User-specific policy settings	**HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\14.0**
Computer-specific policy settings	**HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\14.0**

Similarly, policy setting information for the 2007 Office system is stored in version-specific locations in the Windows registry, as shown in the following table.

Type of setting	2007 subkey
User-specific policy settings	**HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0**
Computer-specific policy settings	**HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0**

There are several policy settings for Office 2010 that are not stored in one of the version-specific registry subkeys. For these policy settings, if you had previously configured the 2007 Office system (or earlier) versions, you must set those policy settings to their **Not Configured** state before you remove the previous Office 2010 ADM or ADMX files and load the Office 2010 ADM or ADMX files. This removes the registry key information for the policy setting from the registry. This occurs because if an .adm or .admx file is removed, the settings that correspond to the .adm or .admx file do not appear in Group Policy Object Editor. However, the policy settings that are configured from the .adm or .admx file remain in the Registry.pol file and continue to apply to the appropriate target client or user.

Installing the settings

For information about how to install and load the Group Policy settings, see Enforce settings by using Group Policy in Office 2010.

To update the OCT, replace the /Admin folder in your Office 2010 installation files or installation image with the new /Admin folder that is included in the download package.

Files included in this download

The download package for the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*) contains the following folders and files:

Office2010GroupPolicyAndOCTSettings.xls

Important:
For the latest information about policy settings, please refer to the updated Microsoft Excel 2010 workbook, *Office2010GroupPolicyAndOCTSettings_Reference.xls* which is available in the **Files to download** section of the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool download page (*http://go.microsoft.com/fwlink/?LinkId=189316*). The updated workbook, Office2010GroupPolicyAndOCTSettings_Reference.xls, contains settings changes that were made after the download package was built.

AdminTemplates.exe

\ADMX: The ADMX folder contains XML-based versions (.admx or .adml files) of the Administrative Template files for Windows Vista and Windows Server 2008 or later versions of Windows. Administrative Template files in Windows Server 2008 and Windows Vista or later versions of Windows are divided into ADMX (language-neutral) and ADML (language-specific) files. By default, the %systemroot%\PolicyDefinitions folder on a local computer stores all ADMX files. ADML files are stored in language-specific folders under the %systemroot%\PolicyDefinitions folder. Each language subfolder contains the .adml files for that language; for example, the English language ADML files would be stored in the %systemroot%\PolicyDefinitions\en-us folder. Languages included are Chinese Simplified (People's Republic of China), Chinese (Hong Kong SAR), English, French, German, Italian, Japanese, Korean, and Spanish. The files that are stored in the \ADMX folder are as follows:

access14.admx

excel14.admx

inf14.admx

office14.admx

onent14.admx

outlk14.admx

ppt14.admx

proj14.admx

pub14.admx

spd14.admx

spw14.admx

visio14.admx

word14.admx

\de-de: Contains the German language version of the .adml files.

\en-us: Contains the English language version of the .adml files.

access14.adml

excel14.adml

inf14.adml

office14.adml

onent14.adml

outlk14.adml

ppt14.adml

proj14.adml

pub14.adml

spd14.adml

spw14.adml

visio14.adml

word14.adml

\es-es: Contains the Spanish language version of the .adml files.

\fr-fr: Contains the French language version of the .adml files.

\it-it: Contains the Italian language version of the .adml files.

\ja-jp: Contains the Japanese language version of the .adml files.

\ko-kr: Contains the Korean language version of the .adml files.

\zh-cn: Contains the Chinese Simplified (People's Republic of China) language version of the .adml files.

\zh-tw: Contains the Chinese (Hong Kong SAR) language version of the .adml files.

\ADM: Contains the updated .adm files. Each of the language subfolders contains the .adm files for that language. For example, the en-us subfolder contains the English-US version of the .adm files. Languages included are Chinese Simplified (People's Republic of China), Chinese (Hong Kong SAR), English, French, German, Italian, Japanese, Korean, and Spanish.

\de-de: Contains the German language version of the .adm files.

\en-us

access14.adm

excel14.adm

inf14.adm

office14.adm

onent14.adm

outlk14.adm

ppt14.adm

proj14.adm

pub14.adm

spd14.adm

spw14.adml

visio14.adm

word14.adm

\es-es: Contains the Spanish language version of the .adm files.

\fr-fr: Contains the French language version of the .adm files.

\it-it: Contains the Italian language version of the .adm files.

\ja-jp: Contains the Japanese language version of the .adm files.

\ko-kr: Contains the Korean language version of the .adm files.

\zh-cn: Contains the Chinese Simplified (People's Republic of China) language version of the .adm files.

\zh-tw: Contains the Chinese (Hong Kong SAR) language version of the .adm files.

\Admin: Contains the updated OPAX files, oct.dll, and octca.dll files. These files contain all previous hotfix updates that affected the OCT. Each of the language subfolders contains the .opal files for that language, the Office Customization Help file (OCT.chm), and octres.dll files. For example, the en-us subfolder contains the English-US version of these files. Languages included are Chinese Simplified (People's Republic of China), Chinese (Hong Kong SAR), English, French, German, Italian, Japanese, Korean, and Spanish.

oct.dll

octca.dll

\de-de: Contains the German language version of the files in the \en-us subfolder.

\en-us: Contains the .opal files, oct.chm Help file, and octres.dll files.

access14.opal

excel14.opal

inf14.opal

office14.opal

onent14.opal

outlk14.opal

ppt14.opal

proj14.opal

pub14.opal

spd14.opal

spw14.opal

visio14.opal

word14.opal

oct.chm Help file

octres.dll

\es-es: Contains the Spanish language version of the .opal, oct.chm, and octres.dll files.

\fr-fr: Contains the French language version of the .opal, oct.chm, and octres.dll files.

\it-it: Contains the Italian language version of the .opal, oct.chm, and octres.dll files.

\ja-jp: Contains the Japanese language version of the .opal, oct.chm, and octres.dll files.

\ko-kr: Contains the Korean language version of the .opal, oct.chm, and octres.dll files.

\zh-cn: Contains the Chinese Simplified (People's Republic of China) language version of the .opal, oct.chm, and octres.dll files.

\zh-tw: Contains the Chinese (Hong Kong SAR) language version of the .opal, oct.chm, and octres.dll files.

For information about how to use the ADM files, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

For information about how to use ADMX files for Windows Vista, see Managing Group Policy ADMX Files Step-by-Step Guide (*http://go.microsoft.com/fwlink/?LinkId=75124*).

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

See Also

Group Policy overview for Office 2010

Enforce settings by using Group Policy in Office 2010

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

Planning for Group Policy in Office 2010

II. Plan for customizing Office 2010 by using Group Policy

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.
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.

Setting for PowerPoint 2010	Associated registry key	Description
		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. If disabled or not configured, documents are checked for watermarks and issues found appear

Setting for Word 2010	Associated registry key	Description
		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 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	Allows users to ignore	Spelling checker	Spelling checker	Same as if it is	Microsoft Office	Microsoft Office

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
UPPERCASE	words that are written in UPPERCASE.	ignores words that are written in UPPERCASE.	does not ignore words that are written in UPPERCASE.	enabled, except users can change the setting through the UI.	2010\Tools | Options | Spelling\Proofing Data Collection	2010\Tools | Options | Spelling
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	Spelling checker lets users select words from other sources.	Same as if it is enabled, except users can	Microsoft Office 2010\Tools | Options | Spelling\Proofing Data	Microsoft Office 2010\Tools | Options | Spelling

Name	Description	When enabled	When disabled	When not configured	Group Policy object editor location	OCT location
		only.		change the setting through the UI.	Collection	

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 options for users • No spell checking • Check spelling as you type • Hide spelling errors • Check spelling but hide errors	One or more options can be enabled.	One or more options can be disabled.	Same as enabling the “Check spelling as you type” option, but users can change this through the UI.	Microsoft OneNote 2010\OneNote Options\Spelling	Microsoft OneNote 2010\OneNote 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	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
	spelling before sending • 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 enabled.	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.	Spelling checker does not check for grammar	Same as if it is enabled, except users can change through the UI.	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
			when it checks spelling.			
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

Plan for proofing tools (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanProofingTools*)

Plan for using compatibility mode in Office 2010

Although standardizing on the Microsoft Open XML file format is the best way to minimize compatibility issues, this goal can be difficult to achieve for organizations that plan to deploy Microsoft Office 2010 over a period of months or years. Even after the migration is complete, users might continue to collaborate with partners, customers, and other organizations that use earlier versions of Office. To help users maintain productivity during all phases of an Office 2010 migration, you can let users continue to work in the 97-2003 binary file format (*.doc, *.xls, and *.ppt) and use the compatibility features that are included with Microsoft Excel 2010, Microsoft PowerPoint 2010, and Microsoft Word 2010.

In this article:

Overview of Office document compatibility in Office 2010

When planning a migration to Office 2010, you face the challenge of not only determining which versions of Office documents are being used in your organization, but also assessing how those documents will function when users open and save them by using different versions of Office. Your task can be even more challenging if you are performing this assessment for millions of documents of varying complexity, age, and history.

Nevertheless, in the middle of planning an Office migration, it is easy to forget that converting Office 2003 and earlier binary files to the Open XML format is not a strict requirement of Office 2010 migration. Organizations that do not have a strong business requirement to convert binary files to the Open XML format can skip the bulk conversion process completely. They can let users edit binary files in compatibility mode, which is enabled automatically when a user opens a binary file in Excel 2010, PowerPoint 2010, or Word 2010. Compatibility mode disables certain features that are exclusive to these applications in Office 2010 so that the binary files remain compatible with previous versions of Office.

The disadvantage of using compatibility mode is that Office 2010 users cannot use the full feature set of Office 2010. Users who need full Office 2010 functionality can create new Office documents in Open XML format, or convert existing binary files to Open XML while they edit them. To edit Open XML files after the files are created or converted to the Open XML format, users of Office 2003 or earlier versions of Office must have the Compatibility Pack installed. More details about the Compatibility Pack are provided in Preparing Office 2010 users for using compatibility features, later in this article.

Is using compatibility mode right for your organization?

Reviewing a simple list of document management characteristics can help you decide whether using compatibility features in Office 2010 is sufficient for your organization. For example, if your organization does not use extensive document management policies or systems, you may not have to spend time identifying Office documents to convert and you may not need to perform a conversion. You might also find that business groups in your organization have different requirements, some of which can only be met by conversion, and other requirements that can be satisfied by using the compatibility features.

The following considerations will help you decide whether to pursue compatibility, conversion, or both.

Compatibility is the better strategy if your organization or business group:

- Relies on end-users to troubleshoot issues with their own Office documents.
- Does not have business justification for converting binary files to Open XML format.
- Is not adversely affected by feature differences that occur when compatibility mode is used.

Conversion is the better strategy if your organization or business group:

- Uses document management products and understands the location and kind of Office documents that are managed by those products.
- Manages documents by using retention, compliance, information rights management, or auditing policies.
- Needs conversion to Open XML format as a business justification for migrating to Office 2010.
- Supports Office documents through a Help Desk or IT department.

The instructions in the remainder of this article will help you prepare to work in compatibility mode. However, if your organization chooses conversion as its strategy, you can conduct the assessment and conversion of binary Office files by using the Office 2010 Migration Planning Manager (OMPM), which is available on the Microsoft Download Center. For more information, see Plan for document conversion in Office 2010 (*http://technet.microsoft.com/library/d555e8dc-7a29-46ac-b26f-c9bbf4f3c67e(Office.14).aspx*) and Office Migration Planning Manager (OMPM) overview for Office 2010 (*http://technet.microsoft.com/library/d0373697-31f5-4fc5-8dd1-1b9d7f35842f(Office.14).aspx*)

If you need guidance on assessing the compatibility of Office add-ins and applications, see Application compatibility assessment and remediation guide for Office 2010 (*http://technet.microsoft.com/library/b0d56d5f-f780-483e-8f95-dc7360a05208(Office.14).aspx*).

Preparing Office 2010 users for using compatibility features

As part of your overall Office 2010 training plan, you should provide guidance to users on how to use compatibility mode. Topics to cover include the features that are disabled in compatibility mode, the

visual clues that indicate that compatibility mode is being used, and, if using Open XML is supported by their business group, how to exit compatibility mode by converting files to Open XML format.

The following table provides links to information that you can use to prepare users for working in compatibility mode.

Functionality	Excel 2010	PowerPoint 2010	Word 2010
Enabling compatibility mode	Work in compatibility mode in Excel 2010 (*http://go.microsoft.com/fwlink/?LinkId=196420*)	Features are lost when you open a presentation created in an earlier version of PowerPoint(*http://go.microsoft.com/fwlink/?LinkID=207536&clcid=0x409*)	Use Word 2010 to open documents created in earlier versions of Word (*http://go.microsoft.com/fwlink/?LinkId=196421*) Create a document to be used by previous versions of Word (*http://go.microsoft.com/fwlink/?LinkId=196422*)
Feature differences when compatibility mode is used	Excel 2010 features that are not supported in earlier versions of Excel (*http://go.microsoft.com/fwlink/?LinkId=196436*)	Features are lost when you open a presentation created in an earlier version of PowerPoint (*http://go.microsoft.com/fwlink/?LinkID=207536&clcid=0x409*)	Feature availability in each mode (*http://go.microsoft.com/fwlink/?LinkId=196437*)
Converting files to Office 2010 format (exiting compatibility mode)	Convert a workbook to the Excel 2010 file format (*http://go.microsoft.com/fwlink/?LinkId=196423*)	Convert a PowerPoint presentation from a previous version to PowerPoint 2010 (*http://go.microsoft.com/fwlink/?LinkId=196424*)	Convert a document to the Word 2010 mode (*http://go.microsoft.com/fwlink/?LinkId=196425*)

Office 2010 users who create or edit files in the Open XML format can convert the files to binary format by using the **Save As** command and selecting the appropriate 97-2003 format (.doc, .ppt, or .xls). Compatibility Checker will alert the users to any content in the file that is not supported by earlier versions of the application. If you expect this to be a common scenario, you can also provide guidance on how to use Compatibility Checker. See the articles listed in the following table:

Functionality	Excel 2010	PowerPoint 2010	Word 2010
Running Compatibility checker	Check an Excel 2010 workbook for compatibility with earlier versions of Excel (*http://go.microsoft.com/fwlink/?LinkID=196429*)	Determine whether a PowerPoint 2010 presentation is compatible with PowerPoint 2003 or earlier (*http://go.microsoft.com/fwlink/?LinkId=196430*) Compatibility Checker (*http://go.microsoft.com/fwlink/?LinkId=196431*)	Compatibility changes between versions (http://go.microsoft.com/fwlink/?LinkId=196432)

If your Office 2010 users will be creating new files in the Open XML format, you must deploy the Compatibility Pack to users who will use Microsoft Office 2000, Office XP, or Office 2003 to edit files. The Compatibility Pack is not required for the 2007 Office system with Service Pack 2 (SP2) or later versions. To download the Compatibility Pack, visit the Microsoft Download Center (*http://go.microsoft.com/fwlink/?LinkID=191166*).

For links to additional reference topics about compatibility features, see Document compatibility reference for Excel 2010, PowerPoint 2010, and Word 2010 (*http://technet.microsoft.com/library/2a199cc2-ef18-4ff4-b845-a80fb5877dfe(Office.14).aspx*).

Changing default file formats and other settings for Office 2010 documents

By using the Office Customization Tool (OCT) and Group Policy, you can configure Office to save new Office documents in binary (97-2003) format instead of Open XML, the default file format. Changing the default file format is useful if you have business reasons that require users to continue to create new files in binary format. In addition to settings for default file format, there are also settings to configure how Word 2010 saves Open XML files to make them compatible with Word 2007 and Word 2003.

The following table describes the location of some file format options in the Group Policy Administrative Template files (ADM, ADMX, ADML) and the OCT for Office 2010. You can find a full list of settings related to file formats in Group Policy and Office Customization Tool (OCT) settings that address OpenDocument Format (ODF) and Office Open XML (OOXML) file formats in Office 2010.

Setting	Application	Location in OCT and Group Policy	Default setting	Compatibility setting
Default file format	Excel 2010	Microsoft Excel 2010\Excel Options\Save	Excel Workbook (*.xlsx)	Excel 97-2003 Workbook (*.xls)
	PowerPoint 2010	Microsoft PowerPoint 2010\PowerPoint Options\Save	PowerPoint Presentation (*.pptx)	PowerPoint 97-2003 Presentation (*.ppt)
	Word 2010	Microsoft Word 2010\Word Options\Save	Word Document (*.docx)	Word 97-2003 Document (*.doc)
Set default compatibility mode on file creation	Word 2010	Microsoft Word 2010\Word Options\Save	Full functionality mode	Word 2007 mode or Word 2003 mode
Save As Open XML in compatibility mode	Word 2010	Microsoft Word 2010\Word Options\Save	Disabled; users can decide whether a converted file is compatible with previous versions of Word	Enabled; converted files are always compatible with previous versions of Word

To download the OCT, the Group Policy Administrative Templates, and a workbook that provides information about Office 2010 Group Policy settings and OCT settings, see Office 2010 Administrative Template files (ADM, ADMX/ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkID=189316*).

The following sections provide more details about these settings.

Default file format

Although we recommend leaving the default set to Open XML, you can change the default to binary format if there are business reasons that require users to continue to work in binary files. For example, if you are performing a phased migration of Office 2010 and have not yet deployed the Compatibility

Pack, you will want Office 2010 users to continue to create and work in binary files so that users of Office 2003 or earlier can edit the files. When your deployment is complete, we recommend changing back to the default so that all newly created files use the Open XML format.

Set default compatibility mode on file creation (Word 2010 only)

This policy setting lets you specify the versions of Word (2003, 2007, or 2010) that you want new Word documents in Open XML format to be compatible with. Three configurations options are available for this setting:

- Word 2003: This mode disables features in Word that are incompatible with Word 2003.
- Word 2007: This mode disables features in Word that are incompatible with Word 2007.
- Full functionality mode: This mode ensures that all new features remain enabled. This is the default setting for Word.

Selecting the Word 2003 option configures Word to create new Open XML files that have Word 2007 and Word 2010 features disabled. Doing so ensures that the Open XML files do not contain content that Word 2003 users cannot edit. However, users of Office 2003 and earlier must still have the Compatibility Pack installed before they can edit Word Open XML files that are compatible with Word 2003.

If you select Full functionality mode, there is no effect on the Word 2007 users. Word 2007 can open and edit Word 2010 documents. The only difference is that new features in Word 2010 are not available in Word 2007.

Save As Open XML in compatibility mode (Word 2010 only)

When a user uses the **Save As** command to convert a binary file to the Open XML format, the user has the option of selecting the **Maintain compatibility with previous versions of Word** check box. When users select this check box, the newly converted document is compatible with Word 2007. Features that are exclusive to Word 2010 are disabled. The user then edits the document in Word 2007 compatibility mode.

When you enable this policy, the **Maintain compatibility with previous versions of Word** check box is selected and hidden, and Word 2010 will always save the file so that it is compatible with Word 2007.

Planning security settings for binary files that are opened in Office 2010

Office binary files are susceptible to file format attacks that exploit the integrity of a file. These attacks occur when someone who intends to add malicious code modifies the structure of a file. The malicious code is run remotely and is used to elevate the privilege of restricted accounts on the computer. As a result, attackers 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 to install malware, such as a worm or a key logging program.

Office 2010 includes new features to make viewing and editing binary files safer. Each of these features has settings that you should consider as part of your deployment planning. The following sections provide brief descriptions of these features, their planning considerations, and links to more information.

Office File Validation

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 Word 2010, Excel 2010, or PowerPoint 2010. 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.

Any files that fail validation are opened in Protected View. Users can decide to enable editing for files that fail validation but are opened in Protected View. Users are also prompted to send Office File Validation information to Microsoft. Information is collected only for files that fail validation.

Office 2010 provides several settings that let you configure how the Office File Validation feature behaves. These settings let you do the following:

- Disable Office File Validation.
- Specify Office file behavior when a file fails validation.
- Prevent Office 2010 from sending Office File Validation information to Microsoft.

Although we recommend that you do not change the default settings for Office File Validation, your organization might have to configure Office File Validation settings to suit special security requirements. For more information, see Plan Office File Validation settings for Office 2010 (*http://technet.microsoft.com/library/17f92cf7-75e3-47e1-8383-1ba19ae64e8d(Office.14).aspx*).

Office Protected View

Protected View is a new security feature in Office 2010 that helps mitigate exploits to users' computers by opening files in a restricted environment so they can be examined before they are opened for editing in Word 2010, Excel 2010, and PowerPoint 2010. 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 file. In addition, Protected View prevents users from viewing the details of digital signatures that are used to sign a document, presentation, or workbook.

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.

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. It works with other security features such as Office File Validation and File Block. However, we recognize that your organization might have to

change Protected View settings to suit special security requirements. To that end, Office 2010 provides several settings that let you configure 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.

For more information about how to configure Protected View, see Plan Protected View settings for Office 2010 (*http://technet.microsoft.com/library/dc45ec33-40b0-4dec-a038-c0076115f9c9(Office.14).aspx*).

Group Policy and Office Customization Tool (OCT) settings that address OpenDocument Format (ODF) and Office Open XML (OOXML) file formats in Office 2010

This article lists the Group Policy settings and the Office Customization Tool (OCT) settings that address OpenDocument Format and Open XML Formats in Microsoft Office 2010.

In this article:

Before you can use the settings discussed in this article, you must install the Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*) download package, which contains new and updated Group Policy administrative template files and OCT files.

About the settings

For each setting, the following information is provided:

The application to which the setting applies

The setting name

What the setting does

The default configuration for the setting

Where to find the setting in the Group Policy Object Editor

- Unless otherwise noted, you will find Group Policy settings under the **User Configuration/Administrative Templates** node of the Group Policy Object Editor when you edit a local or domain-based Group Policy object (GPO).

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 and Group Policy overview for Office 2010.

Where to find the setting in the Office Customization Tool (OCT)

- Unless otherwise noted, you will find OCT settings on the **Modify user settings** page of the OCT when you configure a setup customization file.

Note:
If the geographic location of the computer on which you are running the OCT is set to a European location, when you create a new Setup customization .msp file, or open an existing customization .msp file for which file format settings have not been configured for Excel 2010, PowerPoint 2010, or Word 2010, you might be prompted to choose a default file format for users. You can choose to keep the current settings for the Setup customization file, or choose either Office Open XML formats (which support all the features of Office 2010), or OpenDocument formats. For more information about these file formats, click **Learn more** to access OCT help.

Excel 2010 settings

The following table lists the Group Policy settings and the OCT settings that address OpenDocument Format and Open XML Formats for Excel 2010.

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
Default file format	Specifies the default file format for new files that users create in Microsoft Excel. This includes the OpenDocument spreadsheet (.ods) file format.	Files are created in the Excel file format. Users may override this default setting and specify another file format.	Microsoft Excel 2010\Excel Options\Save	Microsoft Excel 2010\Excel Options\Save
Suppress file format compatibility dialog box for	Allows you to enable or disable the file format compatibility	The file format compatibility dialog box appears when users save as an OpenDocument Spreadsheet file in Excel.	Microsoft Excel 2010\Excel Options\Save	Microsoft Excel 2010\Excel Options\Save

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
OpenDocument Spreadsheet format	dialog box from appearing when users save a file as an OpenDocument spreadsheet (*.ods) file in Microsoft Excel.			
OpenDocument Spreadsheet files	Determines whether users can open, view, edit, or save Excel files in OpenDocument Spreadsheet (*.ods) file format.	Users can open, view, edit, or save Excel files in *.ods file format.	Microsoft Excel 2010\Excel Options\Security\Trust Center\File Block Settings	Microsoft Excel 2010\Excel Options\Security\Trust Center\File Block Settings
Microsoft Office Open XML converters for Excel	Determines whether users can open, view, edit, or save Excel files in Open XML file format.	Users can open, view, edit, or save Excel files in Open XML file format.	Microsoft Excel 2010\Excel Options\Security\Trust Center\File Block Settings	Microsoft Excel 2010\Excel Options\Security\Trust Center\File Block Settings
Scan encrypted macros in Excel Open XML	Controls whether encrypted macros in Open XML documents	Encrypted macros are disabled unless antivirus software is installed. Encrypted macros are scanned by your antivirus software when you attempt to open an encrypted workbook that contains macros.	Microsoft Excel 2010\Excel Options\Security	Microsoft Excel 2010\Excel Options\Security

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
workbooks	are required to be scanned by using antivirus software before they are opened. **Note:** The behavior depends on whether the antivirus software uses the Microsoft Antivirus API.	**Note:** If the antivirus software does not use the Microsoft Antivirus API, macros will always be blocked.		
Protect document metadata for rights-managed Office Open XML Files	Determines whether metadata is encrypted in Office Open XML files that are protected by	When Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	Information Rights Management (IRM).			
Protect document metadata for password protected files	Determines whether metadata is encrypted when an Office Open XML file is password protected.	When an Open XML document is protected with a password and saved, any metadata associated with the document is encrypted along with the rest of the document's contents. If this configuration is changed, potentially sensitive information such as the document author and hyperlink references could be exposed to unauthorized people.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings
Encryption type for password protected Office Open XML files	Allows you to specify an encryption type for Office Open XML files.	The default cryptographic service provider (CSP) is used. On computers that run Windows Vista, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit. On computers that run Windows XP, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype), AES-128, 128-bit. Note: This policy setting will not take effect unless the registry key **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\<Office application name>\Security\Crypto\CompatMode** is set to 0. By default, the CompatMode registry key is set to 1.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings
Block opening of pre-release versions of file formats	Controls whether users who have the Microsoft Office Compatibility	Users of the compatibility pack will be unable to open Office Open XML files that were created in pre-release versions of Excel 2010.	Microsoft Office 2010\Office 2010 Converters	Microsoft Office 2010\Office 2010 Converters

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
new to Excel 2010 through the Compatibility Pack for Office 2010 and Excel 2010 Converter	Pack for Word, Excel, and PowerPoint 2010 File Formats installed can open Office Open XML files that were saved with pre-release versions of Excel 2010. Excel Open XML files usually have the following extensions: .xlsx, .xlsm, .xltx, .xltm, .xlam.			
Disable Package Repair	Allows you to disable the option to repair Open XML documents.	When an Office 2010 application detects that an Open XML document is corrupted, the user is given the option of repairing the corrupted document.	This setting cannot be configured by using Group Policy.	Microsoft Office 2010 (Machine)\Security Settings

PowerPoint 2010 settings

The following table lists the Group Policy settings and the OCT settings that address OpenDocument Format and Open XML Formats for PowerPoint 2010.

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
Suppress file format compatibility dialog box for OpenDocument Presentation format	Allows you to enable or disable the file format compatibility dialog box when you save a file as an OpenDocument presentation file in Microsoft PowerPoint.	The file format compatibility dialog box is not displayed when you save as an OpenDocument presentation file in PowerPoint.	Microsoft PowerPoint 2010\PowerPoint Options\Save	Microsoft PowerPoint 2010\PowerPoint Options\Save
OpenDocument Presentation files	Allows you to determine whether users can open, view, edit, or save PowerPoint files with the OpenDocument presentation (*.odp) file format.	OpenDocument presentation files are not blocked.	Microsoft PowerPoint 2010\PowerPoint Options\Security\Trust Center\File Block Settings	Microsoft PowerPoint 2010\PowerPoint Options\Security\Trust Center\File Block Settings
Microsoft Office Open XML	Allows you to determine whether users can	PowerPoint files using Open XML file format converters are not blocked.	Microsoft PowerPoint 2010\PowerPoint	Microsoft PowerPoint 2010\PowerPoint

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
converters for PowerPoint	open, view, edit, or save PowerPoint files using Open XML file format converters.		Options\Security\Trust Center\File Block Settings	Options\Security\Trust Center\File Block Settings
Scan encrypted macros in PowerPoint Open XML presentations	Controls whether encrypted macros in Open XML presentations are required to be scanned by using antivirus software before they are opened.	Encrypted macros are disabled unless antivirus software is installed. If antivirus software is installed, encrypted macros are scanned by users' antivirus software when they attempt to open an encrypted presentation that contains macros. If no vulnerabilities are detected, the macros can run.  **Note:** If the antivirus software does not use the Microsoft Antivirus API, macros will always be blocked.	Microsoft PowerPoint 2010\PowerPoint Options\Security	Microsoft PowerPoint 2010\PowerPoint Options\Security
Turn on an external converter as the default for a file name extension	Allows you to enable an external file format converter as the default for a particular file name extension on a computer. To set this policy, you need to specify the	Microsoft PowerPoint processes files in an application-defined manner.	This setting cannot be configured by using Group Policy.	Microsoft PowerPoint 2010 (Machine)\Converters

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	file name extension (for example, "odp") for Value Name and the external file format converter via the converter's classname (for example, "TestConverter") for Value.			
Protect document metadata for rights-managed Office Open XML Files	Determines whether metadata is encrypted in Office Open XML files that are protected by Information Rights Management (IRM).	When Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings
Protect document metadata for password protected files	Determines whether metadata is encrypted when an Office Open XML file is	When an Open XML document is protected with a password and saved, any metadata associated with the document is encrypted along with the rest of the document's contents. If this configuration is changed, potentially sensitive information such as the document author and	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	password protected.	hyperlink references could be exposed to unauthorized people.		
Encryption type for password protected Office Open XML files	Allows you to specify an encryption type for Office Open XML files.	The default cryptographic service provider (CSP) is used. On computers that run Windows Vista, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit. On computers that run Windows XP, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype), AES-128, 128-bit. Note: This policy setting will not take effect unless the registry key **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\<Office application name>\Security\Crypto\CompatMode** is set to 0. By default, the CompatMode registry key is set to 1.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings
Block opening of pre-release versions of file formats new to PowerPoint 2010 through the Compatibility Pack for Office 2010 and PowerPoint 2010 Converter	Controls whether users who have the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2010 File Formats installed can open Office Open XML files that were saved with pre-	Users of the compatibility pack will be unable to open Office Open XML files that were created in pre-release versions of PowerPoint 2010.	Microsoft Office 2010\Office 2010 Converters	Microsoft Office 2010\Office 2010 Converters

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	release versions of PowerPoint 2010. PowerPoint Open XML files usually have the following extensions: .pptx, .pptm, .potx, .potm, .ppsx, .ppsm, .ppam, .thmx, .xml.			
Disable Package Repair	Allows you to disable the option to repair Open XML documents.	When an Office 2010 application detects that an Open XML document is corrupted, the user is given the option of repairing the corrupted document.	This setting cannot be configured by using Group Policy.	Microsoft Office 2010 (Machine)\Security Settings

Word 2010 settings

The following table lists the Group Policy settings and the OCT settings that address OpenDocument Format and Open XML Formats for Word 2010.

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
Save As Open XML in Compatibility Mode	Allows you to hide the "Maintain compatibil	The "Maintain compatibility with previous versions of Word" check box appears in the Save As dialog when users save a file in an Open XML file format.	Microsoft Word 2010\Word Options\Save	Microsoft Word 2010\Word Options\Save

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	ity with previous versions of Word" check box that appears in the **Save As** dialog when users save a file as an Open XML file format. This check box lets users preserve the fidelity of documents that open in compatibility mode when they save those documents to any of the Open XML file formats. Checking this box			

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	will prevent conversion to the version of Word that is saving the file. Conversion maximizes fidelity with the version of Word that is saving the file, and we recommend it for users who want their Word documents to be compatible with this version of Word. However, conversion might impact the fidelity and compatibility of some			

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	features when the file is opened by an earlier version of Word.			
Do not display file format compatibility dialog box for OpenDocument text format	Allows you to enable or disable the file format compatibility dialog box that appears when users save a file as an OpenDocument text file in Word.	The file format compatibility dialog box appears when users save as an OpenDocument text file in Word.	Microsoft Word 2010\Word Options\Save	Microsoft Word 2010\Word Options\Save
Set default compatibility mode on file creation	Allows you to specify the default compatibility mode for users when they create new files	Full functionality mode is the default compatibility mode for users when they create new files in Word 2010.	Microsoft Word 2010\Word Options\Save	Microsoft Word 2010\Word Options\Save

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	in Word 2010: Word 2003, Word 2007, or full functionality mode (this mode ensures that all new features remain enabled). Note: Open XML file formats such as .docx and .dotx, support all three modes.			
Default file format	Allows you to determine the default file format for saving files in Word. This includes	Word saves new files in the Office Open XML format (*.docx).	Microsoft Word 2010\Word Options\Save	Microsoft Word 2010\Word Options\Save

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	the OpenDocument text (.odt), and Open XML file formats. This policy setting is often set in combination with the "Save As Open XML in Compatibility Mode" policy setting.			
OpenDocument Text files	Allows you to determine whether users can open, view, edit, or save Word files that use the OpenDocument text (*.odt) file format.	Users can open, view, edit, or save *.odt files in Word 2010.	Microsoft Word 2010\Word Options\Security\Trust Center\File Block Settings	Microsoft Word 2010\Word Options\Security\Trust Center\File Block Settings

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
Office Open XML converters for Word	Allows you to determine whether users can open, view, edit, or save Word files that use Open XML file format converters.	Word files that use Open XML file format converters are not blocked.	Microsoft Word 2010\Word Options\Security\Trust Center\File Block Settings	Microsoft Word 2010\Word Options\Security\Trust Center\File Block Settings
Scan encrypted macros in Word Open XML documents	Controls whether encrypted macros in Open XML Word documents are required to be scanned by using antivirus software before they are opened.	Encrypted macros are disabled unless antivirus software is installed. If antivirus software is installed, encrypted macros are scanned by users' antivirus software when they attempt to open an encrypted document that contains macros. If no vulnerabilities are detected, the macros can run. **Note:** If the antivirus software does not use the Microsoft Antivirus API, macros will always be blocked.	Microsoft Word 2010\Word Options\Security\Trust Center	Microsoft Word 2010\Word Options\Security\Trust Center
Protect document metadata for rights-	Determines whether metadata is	When Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
managed Office Open XML Files	encrypted in Office Open XML files that are protected by Information Rights Management (IRM).			
Protect document metadata for password protected files	Determines whether metadata is encrypted when an Office Open XML file is password protected.	When an Open XML document is protected with a password and saved, any metadata associated with the document is encrypted along with the rest of the document's contents. If this configuration is changed, potentially sensitive information such as the document author and hyperlink references could be exposed to unauthorized people.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings
Encryption type for password protected Office Open XML files	Allows you to specify an encryption type for Office Open XML files.	The default cryptographic service provider (CSP) is used. On computers that run Windows Vista, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit. On computers that run Windows XP, the default CSP is Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype), AES-128, 128-bit. Note: This policy setting will not take effect unless the registry key **HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\<Office application name>\Security\Crypto\CompatMode** is set to 0. By default, the CompatMode registry key is set to 1.	Microsoft Office 2010\Security Settings	Microsoft Office 2010\Security Settings

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
Block opening of pre-release versions of file formats new to Word 2010 through the Compatibility Pack for Office 2010 and Word 2010 Open XML/Word 97-2003 Format Converter	Controls whether users who have the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2010 File Formats installed can open Office Open XML files that were saved with pre-release versions of Word 2010. Word Open XML files usually have the following extensions: .docx, .docm, .dotx, .dotm,	Users of the compatibility pack will be unable to open Office Open XML files that were created in pre-release versions of Word 2010.	Microsoft Office 2010\Office 2010 Converters	Microsoft Office 2010\Office 2010 Converters

Setting name	What it does	Default configuration	Group Policy Object Editor location	OCT location
	.xml.			
Disable Package Repair	Allows you to disable the option to repair Open XML documents.	When an Office 2010 application detects that an Open XML document is corrupted, the user is given the option of repairing the corrupted document.	This setting cannot be configured by using Group Policy.	Microsoft Office 2010 (Machine)\Security Settings

See Also

Ecma Office Open XML File Formats overview (*http://go.microsoft.com/fwlink/?LinkId=129465*)

Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool

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

Enforce settings by using Group Policy in Office 2010

Differences between the OpenDocument Spreadsheet (.ods) format and the Excel (.xlsx) format (*http://go.microsoft.com/fwlink/?LinkId=195342*)

Differences between the OpenDocument Presentation (.odp) format and the PowerPoint (.pptx) format (*http://go.microsoft.com/fwlink/?LinkId=195343*)

Differences between the OpenDocument Text (.odt) format and the Word (.docx) format (*http://go.microsoft.com/fwlink/?LinkId=195344*)

III. Plan for security by using Group Policy

Security policies and settings in Office 2010

You can use the Security Compliance Manager as a technical reference for the security settings and privacy options in Microsoft Office 2010, and you can also use it for other purposes. For example, the Microsoft Security Compliance Manager provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility. These features speed up your organization's ability to efficiently manage the security and compliance process for the most widely used Microsoft products. This includes Office 2010.

You can use the Security Compliance Manager and the Office 2010 Security Baseline to determine:

- What a setting does.
- What the default configuration is for a setting.
- What the vulnerability, impact, and countermeasure is for a setting
- Where to find the setting in the Group Policy Management Console (GPMC).

For more information about the Security Compliance Manager and the Office 2010 Security Baseline see Microsoft Security Compliance Manager (*http://go.microsoft.com/fwlink/?LinkID=205635*)

See Also

Group Policy overview for Office 2010

Planning for Group Policy in Office 2010

Microsoft Security Compliance Manager (*http://go.microsoft.com/fwlink/?LinkID=205635&clcid=0x409*)

Microsoft Office 2010 Security Baseline (*http://go.microsoft.com/fwlink/?LinkId=207183*)

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 (*http://technet.microsoft.com/library/83308fb0-db8d-484b-a5ae-0757c162076b(Office.14).aspx*). 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 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 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	*.xlsx *.xltx	• 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
templates		• 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.
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	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.	
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.	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
		• 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 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	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 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.	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 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	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. • 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	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.	
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	• 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	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
	• *.xlb	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 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.	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 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	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 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	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.	
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	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. 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.

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
Other data source files	• *.udl • *.dsn • *.mdb • *.mde • *.accdb • *.accde • *.dbc • *.uxdc	• 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.
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	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. • 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	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
		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 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	• Do not block: The file type is not blocked. • Save blocked: Saving of the file type is blocked.	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
	• *.ppsx • *.ppam • *.thmx • *.xml	• 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.	
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	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. • 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	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 is enabled.	
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	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.	
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.

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 Open XML converters for PowerPoint	• 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.

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 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).
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	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
		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 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	• *.doc • *.dot	• Do not block: The file type is not blocked.	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
documents and templates		• 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.	
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	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. • 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 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	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
		is enabled.	
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 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 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	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.	
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.

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
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** 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 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	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. • 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 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.

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	• *.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 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.
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**	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.	
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**	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.	
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	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.	

See Also

Plan security for Office 2010 (*http://technet.microsoft.com/library/c38e3e75-ce78-450f-96a9-4bf43637c456(Office.14).aspx*)

Group Policy overview for Office 2010

Enforce settings by using Group Policy in Office 2010

Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(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 (*http://technet.microsoft.com/library/67869078-71c6-45f5-aab0-0823c83aed54(Office.14).aspx*)

Configure security for Office 2010

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.
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.

Setting	Description
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.

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 (*http://technet.microsoft.com/library/67869078-71c6-45f5-aab0-0823c83aed54(Office.14).aspx*)

Configure security for 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.

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."
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.

IRM option	Description
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.

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.
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.

Location	IRM option	Description
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.

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

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*)

IV. Plan for Outlook 2010 by using Group Policy

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 (*http://technet.microsoft.com/library/ede86735-65c4-4a03-a5de-82ff4e7100dd(Office.14).aspx*).

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.
- For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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:

- 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.
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.

Option	Description
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**.
HKEY_CURRENT_USER	REG_SZ	Software\Microsoft\Office\14.0\Outlook\Preferences	ModuleOrder	Determines the order in

Root	Data type	Key	Value name	Value data
				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

Root	Data type	Key	Value name	Value data
				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. 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,**.

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.
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.
Do not	Do not download contact photos from Active Directory.

Option	Description
download 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.

Option	Description
Keep search folders offline	Specify the number of days to keep a Search Folder active Outlook is running in offline or cached mode.
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.

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.

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.
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 (*http://technet.microsoft.com/library/ede86735-65c4-4a03-a5de-82ff4e7100dd(Office.14).aspx*)

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

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.

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 in Configure Cached Exchange Mode in Outlook 2010.
- 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 in Configure Cached Exchange Mode in Outlook 2010.
- 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.

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.

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.

- **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.

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 in Configure Cached Exchange Mode in Outlook 2010.

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.

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**.
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	Enable to turn off the **On Slow Connections Download Only**

Option	Description
Only Download Headers	**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.
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 (*http://technet.microsoft.com/library/fcfbec12-7997-4d11-85c3-0ab788837491(Office.14).aspx*).

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. 2. Domain name of e-mail account to be restricted. You can specify the domain of the accounts	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
		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*)

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. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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. • 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.

Scenario	Issue
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.

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.

Option	Description
	• 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. • **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.

Option	Description
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 (*http://technet.microsoft.com/library/83308fb0-db8d-484b-a5ae-0757c162076b(Office.14).aspx*)
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
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 (*http://technet.microsoft.com/library/dc45ec33-40b0-4dec-a038-c0076115f9c9(Office.14).aspx*)

See Also

Plan security for Office 2010 (*http://technet.microsoft.com/library/c38e3e75-ce78-450f-96a9-4bf43637c456(Office.14).aspx*)

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 (*http://technet.microsoft.com/library/dc45ec33-40b0-4dec-a038-c0076115f9c9(Office.14).aspx*).

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. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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 attachments to Level 2	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 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	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.

Option	Description
sending an item	
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 internal senders	When enabled, attachments received from senders within your organization open in Protected View. This setting only applies to 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 (*http://technet.microsoft.com/library/dc45ec33-40b0-4dec-a038-c0076115f9c9(Office.14).aspx*)

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=185585*).
- 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. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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 S/MIME messages	Always use transport neutral encapsulation format (TNEF) for S/MIME messages instead of the format specified by the user.

Cryptography option	Description
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 cannot find the digital ID to	Enter a message to display to users (maximum 255 characters).

Cryptography option	Description
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**.
S/MIME	Specify an option for how S/MIME receipt requests are handled:

<table>
<tr><th>Cryptography option</th><th>Description</th></tr>
<tr><td>receipt requests behavior</td><td>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>
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:
<code>www.microsoft.com/ie/certpage.htm?name=Jeff%20Smith&email=someone@example.com&helplcid=1033</code></td></tr>
</table>

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 • Bad Attribute Sets • No Issuer Certificate Found • No CRL Found • Out of Date CRL • Root Trust Problem • Out of Date CTL
Retrieving CRLs (Certificate	Specify how Outlook behaves when CRL lists are retrieved: • Use system default. Outlook relies on the CRL download schedule that is

Cryptography option	Description
Revocation Lists)	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 (*http://technet.microsoft.com/library/ede86735-65c4-4a03-a5de-82ff4e7100dd(Office.14).aspx*)

Plan security for Office 2010 (*http://technet.microsoft.com/library/c38e3e75-ce78-450f-96a9-4bf43637c456(Office.14).aspx*)

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.

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 e-mail option	Description
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 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.

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.

See Also

Configure junk e-mail settings in Outlook 2010

V. Plan for SharePoint Workspace 2010 by using Group Policy

Group Policy for SharePoint Workspace 2010

When Group Policy settings are applied to an Active Directory organizational unit, you can use them to customize an installation of Microsoft SharePoint Workspace 2010. A collection of Group Policy settings, which is known as a Group Policy object (GPO), is tied to a rules engine that determines which Active Directory group receives related policy settings. SharePoint Workspace–specific Group Policy settings can found in the groove.adm file.

For more information about how to access and use the Group Policy feature, see Group Policy overview (Office system) (*http://go.microsoft.com/fwlink/?LinkID=162307*) and Enforce settings by using Group Policy in the Office system (*http://go.microsoft.com/fwlink/?LinkID=78176*).

For more information about how to customize deployments, see Configure and customize SharePoint Workspace 2010.

The following table describes GPOs that affect SharePoint Workspace 2010 installation.

Group Policy object	Description	Default value or undefined value
Prohibit Groove Workspaces	Prohibits use of Groove workspaces and Shared Folders. Limits SharePoint Workspace use to SharePoint workspaces only.	Disabled
Enable IPv6	Enables IPv6 for SharePoint Workspace.	Disabled
Prefer IPv4	Indicates that IPv4 is preferred over IPv6 if both are supported on client computers.	Disabled
Prevent Indexing Certain Paths	Prevents Windows Search 4.0 from crawling (creating indexes for) SharePoint Workspace content. This policy prevents Windows Search crawling for SharePoint Workspace, removes **Search** from the ribbon in SharePoint Workspace, overrides any user-initiated content crawling, and cleans the Windows Search index of previously indexed SharePoint Workspace content. If this policy is not enabled, Windows Search indexing is enabled by default for the following SharePoint Workspace content: • Metadata for SharePoint workspaces and Groove workspaces for SharePoint Workspace 2010 • Metadata for all Groove workspace tools for SharePoint Workspace 2010	Enabled

Group Policy object	Description	Default value or undefined value
	• The following Groove workspace content is for SharePoint Workspace 2010: Discussions, Documents, Notepad entries, chat transcripts, member messages, and custom lists. If this policy is enabled, Windows Search does not crawl specified paths. The format for specifying a non-searchable path is as follows: `Protocol://site/path/file` and `SharePointWorkspaceSearch` must be entered as the search protocol. For example, the following entry prevents indexing of any SharePoint Workspace content for all users on target SharePoint Workspace computers: `SharePointWorkspaceSearch://{*}/*` For more information about the Prevent Indexing Certain Paths GPO, see Group Policy for Windows Search (*http://go.microsoft.com/fwlink/?LinkID=164564&clcid=0x409*). **Note:** This setting is a Windows Search policy that affects SharePoint Workspace 2010. For more information about Group Policy for Windows Search, see Windows Search Administrators Guides (*http://go.microsoft.com/fwlink/?LinkId=164567*).	
Sync Only On Domain Network	Requires a Secure Socket Layer (SSL) connection for SharePoint Workspace clients trying connect to SharePoint Server 2010 from outside the organization's intranet. **Note:** This setting is a SharePoint Server 2010 custom policy that affects SharePoint Workspace 2010.	Disabled
SharePoint Workspace Account Configuration Code Required	If you use Groove Server 2010 Manager to manage SharePoint Workspace, use this policy to require that a managed account configuration code be entered, manually or automatically, to create a SharePoint Workspace account. This prevents users from creating unmanaged SharePoint Workspace accounts.	Disabled

Group Policy object	Description	Default value or undefined value
	For information about Groove Server 2010 and automatic account configuration, see Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*).	
Groove Server Manager Name	If you use Groove Server 2010 Manager to manage SharePoint Workspace, use this policy to specify the Groove Server 2010 Manager server name to which users are assigned. This attribute supports automatic SharePoint Workspace account configuration or restoration, and migration of unmanaged accounts to managed accounts. For information about how to migrate unmanaged accounts to Groove Server 2010 Manager, see the Migration section of Operations for Groove Server 2010 Manager (*http://technet.microsoft.com/library/32ec0f55-f8c0-444e-a8b8-ac1c900d59f6(Office.14).aspx*).	Disabled
Groove Server Manager Valid Link Security	If you use Groove Server 2010 Manager to manage SharePoint Workspace, use this policy to ensure a trusted SharePoint Workspace-to-Manager communication link. When this requirement is enabled, the presented Groove Server Manager SSL certificate must be valid to enable SharePoint Workspace-to-Manager communication.	Enabled
Maximum Number of Proxy Connection Failures to Groove Server Relay	If you use Groove Server 2010 Manager to manage SharePoint Workspace, use this policy to limit the number of failed proxy connection attempts to a Groove Server Relay by the SharePoint Workspace client. When the limit is reached, additional proxy connection attempts to the Relay server are abandoned.	Enabled
List of Blocked Groove Relay Servers	If you use Groove Server 2010 Manager to manage SharePoint Workspace, use this policy to prevent SharePoint Workspace clients from initiating communications to listed Groove Relay servers that are known to be permanently decommissioned. The format is a comma-separated list of fully qualified domain names of Relay servers. Wildcards in the names are supported. The question mark (?) is for single character substitution and the asterisk (*) is for domain part substitution.	Disabled

See Also

Configure and customize SharePoint Workspace 2010

Office Customization Tool settings for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/43008de2-5eef-4de1-b0e1-19b7ceeb68f6(Office.14).aspx*)

Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*)

Plan for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/e8a433c1-ea1f-4cf7-adc8-50972f58d465(Office.14).aspx*)

VI. Customize Office 2010 by using Group Policy

Customize language setup and settings for Office 2010

This article describes how to manage the distribution of multiple language versions when you deploy Microsoft Office 2010.

In this article:

Overview

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.

For more information, see Plan Setup (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanSetup*) in Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

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. However, you configure language settings by using Group Policy, the Office Customization Tool (OCT), or the Language Settings tool.

For more information, see Plan customizations (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanCustomizations*) in Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

If users will have to edit in a language or a companion proofing language that will not be installed, you can customize and install the Office 2010 Proofing Tools Kit. For more information, see Plan for proofing tools (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanProofingTools*) in Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

Before you begin

To determine which of the following procedures to use for your deployment and which customizations that you might have to make, see Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

Deploy a default language version of Office

If users in your organization work with Office files that are in the same language, or in a language that matches the language of their operating system, you can deploy a default language version of Office.

The following steps are the same as the standard steps for deploying Office 2010 and included for testing. The only difference in the steps is that you must copy the language packs to the same network location as the installation files.

To deploy a default language version of Office to every client computer

1. Create a network installation point for the primary Office 2010 product by copying all the files and folders from the source media to a shared network location.
2. Copy all the files and folders from the source media for each language pack to the same network location, and when you are prompted to overwrite duplicate files, click **No**.
3. Use the Office Customization Tool (OCT) to configure the installation to match your organization's requirements.

   Because most of the customizations apply to the core product, you do not typically have to customize each language separately. Setup applies your customizations during the installation regardless of the language being installed. For information about how to customize language settings, see Customize language settings.

   Language packs that are obtained through a volume license agreement do not require a unique product key; only one volume license key is required for the installation.
4. On the Setup command line, specify the Config.xml file for the primary Office product that you are deploying.

For example, the following command line installs Microsoft Office Standard 2010 in any language:

\\server\share\Office14\Setup.exe /config \\server\share\Office14\Standard.WW\Config.xml

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

5. Run Setup from the root of the network installation point.

   Setup installs only the language-specific elements that are needed for the Office product that you are installing. Setup does not install the complete language pack unless you deploy the language pack as a separate product.

Specify which languages to install

If users in your organization work with Office files in more than one language, or if they need an Office language that does not match the language of their operating system, you can install all the languages they need at the same time.

The following steps are the same as the standard steps for deploying Office 2010 and included for testing. The only difference in the steps is that you must copy the language packs to the same network location as your installation files and edit the Config.xml file to specify which languages to install.

To specify one or more languages to install on a client computer

1. Create a network installation point for your primary Office 2010 product by copying all the files and folders from source media to a shared network location.
2. Copy all the files and folders from the source media for each language pack to the same network location, and when you are prompted to overwrite duplicate files, click **No**.
3. In the core product folder for the product that you are installing, locate the Config.xml file.

   For example, if you are installing Office Standard 2010, find the Config.xml file in the Standard.WW folder.
4. Open the Config.xml file by using a text editor, such as Notepad.
5. Add the **<AddLanguage>** element.
6. Set the value of the **Id** attribute to the language tag that corresponds to the language that you want to install. You can specify more than one language by including additional **<AddLanguage>** elements and attributes.
7. Specify which language to use for the Shell user interface (Shell UI) by setting the **<ShellTransform>** attribute of the **<AddLanguage>** element.

   For example, to specify that Setup install both English and French, with English as the default installation language, add the following elements:

```
<AddLanguage Id="en-us" ShellTransform="yes"/> <AddLanguage Id="fr-fr" />
```

If you want the default installation language and the Shell UI to match the operating system language, and you also want every user to have Office in both English and French, the code in the Config.xml file looks as follows:

```
<AddLanguage Id="match" ShellTransform="yes"/>

<AddLanguage Id="en-us" />

<AddLanguage Id="fr-fr" />
```

You are required to specify a value for the **ShellTransform** attribute when you add more than one **<AddLanguage>** element. Skipping this step causes the installation to fail.

8. To specify that Setup also match the language of the user's Windows user locale, add another line in the Config.xml file:

   ```
   <AddLanguage Id="match" />
   ```

   In this case, Setup installs all specified languages plus the language that matches the user locale, if that language is different.

9. Save the Config.xml file.

10. Use the Office Customization Tool (OCT) to configure the installation to match your organization's requirements.

    For information about how to customize language settings, see Customize language settings.

11. Run Setup.exe and specify the path of your modified Config.xml file.

    Note that you must use a fully qualified path; for example: **\\server\share\Office14\setup.exe /config\\server\share\Office14\Standard.WW\Config.xml**

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

Deploy different languages to different groups of users

You can give different groups of users different sets of Office languages. For example, a subsidiary based in Tokyo might have to work with Office Standard 2010 documents in English and Japanese, whereas users in the European subsidiary need English, French, and German. In this scenario, you create a unique Config.xml file for each group of users.

The following steps are the same as the standard steps for deploying the Office 2010 and included for testing. The only differences in the steps is that you must copy the language packs to the same network location as the installation files, create and edit the Config.xml file for each group to specify which languages to install, and then deploy the appropriate Config.xml file to the different groups.

To deploy different languages to different groups of users

1. In the core product folder for the product that you are installing, locate the Config.xml file.

   For example, if you are installing Office Standard 2010, find the Config.xml file in the Standard.WW folder.

2. Open the Config.xml file by using a text editor, such as Notepad.
3. Locate the **<AddLanguage>** element and specify the set of languages that you want to install for this user group, as described previously.

   Note:
   You must also set the **<Shell UI>** attribute of the **<AddLanguage>** element, as described previously.
4. Save the Config.xml file by using a unique file name.
5. Repeat these steps for the next user group.
6. Use the OCT to configure the installation to match your organization's requirements.

   For information about how to customize language settings, see Customize language settings.
7. Deploy Office to each group of users separately, and in each case specify the correct Config.xml file on the Setup command line. For example:

   \\server\share\Office14\setup.exe /config\\server\share\Office14\Standard.WW\SubAConfig.xml, or

   \\server\share\Office14\setup.exe /config\\server\share\Office14\Standard.WW\SubBConfig.xml

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

Identify installed languages

You can view a list of languages installed for Office 2010 either during the initial installation or during a separate installation of a language pack at the following registry key, which displays the LCID for each enabled language:

HKCU\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages

You can view the user interface (UI) language and fallback languages at the following registry key:

HKCU\Software\Microsoft\Office\14.0\Common\LanguageResources

Although all applications in the Office 2010 use a shared set of registry data to determine their UI language, they do not necessarily all appear in the same UI language. Applications in the Office 2010 usually appear with the UI language indicated in the **UILanguage** entry of this registry key. But there are circumstances where this might not be the case. For example, some deployments might have Microsoft Word 2010 and Microsoft Excel 2010 installed in French, but another Office application installed in a different language. In this case, the other application will look at the **UIFallback** list in this registry key, and use the first language that works with its installed configuration.

Customize language settings

Use Group Policy to enforce language settings

Policies enforce default language settings. Users in your organization cannot permanently modify settings managed by policy. The settings are reapplied every time that the user logs on.

To use Group Policy to manage language settings

1. Copy the Office 2010 policy template files to your computer.
2. Under **Computer Configuration** or **User Configuration** in the console tree, right-click **Administrative Templates**.
3. Click **Add/Remove Templates**, and then click **Add**.
4. In the **Policy Templates** dialog box, click the template that you want to add, and then click **Open**.
5. After you add the templates that you want, click **Close**.
6. Open the Group Policy object (GPO) for which you want to set policy.
7. Double-click **Computer Configuration** or **User Configuration** and expand the tree under **Administrative Templates**.
8. Locate language-related policies in the **Microsoft Office 2010 system\Language Settings** node.
9. Select the languages that you want to use for each setting.
10. Save the GPO.

Use a Setup customization file to specify default language settings

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 modify the settings after the installation.

To use the OCT to customize language settings

1. Start the OCT by running Setup with the **/admin** command-line option.
2. On the **Modify User Settings** page, expand the tree to **Microsoft Office 2010 system\Language Settings**.
3. Open the folder that you want in the navigation pane. Double-click the setting in the right pane, select **Enable**, and then specify a value.
4. Save the Setup customization file in the Updates folder at the root of the network installation point.

   Setup applies the file automatically when you install Office on users' computers.

For more 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*).

Use the Language Preferences tool to modify language settings

If you are not enforcing language settings by policy, users who work in Office applications can use the Language Preferences tool to change their language preferences.

To change language preferences by using the Language Preferences tool

1. On the **Start** menu, point to **Programs**, point to **Microsoft Office**, and then point to **Microsoft Office 2010 Tools**.
2. Click **Microsoft Office 2010 Language Preferences**.
3. At the bottom of the **Choose Editing Languages** section, in the language list box, select the language that you want to be available for editing, and then click the **Add** button. Repeat this step for each editing language that you want to add.
4. In the **Choose Editing Languages** section, select the language that you most often use for Office applications and documents, and then click **Set as Default**.
5. In the **Choose Display and Help Languages** section, under **Display Language**, select the language that you want to use to view Office application buttons and tabs, and then click **Set as Default**.
6. Under **Help Language**, select the language that you want to use to view Office application Help, and then click **Set as Default**.

   If you do not specify a language for Help, the online Help language uses the display language.

Note:

Users can enable functionality for working in languages that are not installed on the computer. For example, if you select Korean as an editing language, you enable Asian and Korean features in Word even if Korean proofing tools are not installed. You must enable support for that language in the operating system.

Customize and install the Office 2010 Proofing Tools Kit

This section covers how to customize and install Office 2010 Proofing Tools Kit.

Note:

If you only need a few proofing languages, the installation of one or two language packs might provide all the proofing tool languages that you need. Each language version of Office 2010 includes proofing tools for a set of companion languages. For more information, see Plan for proofing tools (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanProofingTools*) in Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

Customize the Office 2010 Proofing Tools Kit

You can specify which proofing tool languages to install by using the Proof.WW Setup file config.xml. For a list of the **OptionState** attributes and IDs to use, see Plan for proofing tools (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a.aspx#BKMK_PlanProofingTools*) in Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*).

To customize Setup for proofing tools

1. In the ProofKit.WW folder, locate the Config.xml file.
2. Open the Config.xml file by using a text editor, such as Notepad.
3. For each set of proofing tools that you do not want to install, in the **OptionState** element, set the **State** attribute to **Absent**. For example, if you do not want Catalan proofing tools installed, use this syntax:

   ```
   <OptionState Id="ProofingTools_1027" State="Absent" Children="force"/>
   ```

4. Set the **State** attribute for each set of proofing tools you want to deploy to **Local** (or **Default** or **Advertise**, if preferred). For example, to deploy Basque proofing tools, you can use this syntax:

   ```
   <OptionState Id="ProofingTools_1069" State="Local" Children="force"/>
   ```

5. Save the Config.xml file.
6. Run Setup.exe, and then specify the path of your modified Config.xml file.

   Note that you must use a fully qualified path; for example:
   \\server\share\Office14\Proof.WW\setup.exe
   /config\\server\share\Office14\Proof.WW\Config.xml

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

Installing the Office Proofing Tools Kit 2010 on a single computer

If you have one or two users who need proofing tools, you can install proofing tools from the Office 2010 Proofing Tools Kit to individual computers.

To install the Office Proofing Tools Kit 2010 on a single computer

1. On the Office 2010 Proofing Tools Kit CD, run Setup.exe.
2. Read and accept the Microsoft Software License Terms, and then click **Continue**.
3. To install the proofing tools for all available languages, click **Install Now**. The installation will begin. Otherwise, to install individual languages, click **Customize**.
4. If you selected **Customize**, click the **File Location** and **User Information** tabs to change the information as needed. On the **Installation Options** tab, click the node (plus (+) sign) for the languages that you want to install, and then use the drop-down arrows to set the appropriate installation states.
5. Click **Install**.

See Also

Plan for multilanguage deployment of Office 2010 (*http://technet.microsoft.com/library/f458a0cb-a3a5-4d4a-9f98-a4a81a17ee3a(Office.14).aspx*)

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

Enforce settings by using Group Policy in Office 2010

This article provides procedural information for using the Group Policy Management Console (GPMC) and the Group Policy Object Editor together with the Microsoft Office 2010 Administrative Templates to configure Office 2010.

In this article:

The Group Policy Management Console and the Group Policy object editor are tools that you use to manage Group Policy. The Group Policy Management Console (GPMC) consists of a Microsoft Management Console (MMC) snap-in and a set of scriptable interfaces for managing Group Policy objects (but not Group Policy settings). Group Policy Object Editor, also a Microsoft Management Console, is used to edit the individual settings contained within each Group Policy object (GPO).

Before you can perform the procedures in this article, you must have already done the following:

1. Set up an Active Directory directory service and Group Policy infrastructure in your organization.
2. Installed GPMC.
3. Downloaded the Office 2010 Administrative Templates.

For more information, see Group Policy overview for Office 2010.

Start GPMC

Depending on the version of Windows that you are running, you will have GPMC on your computer, or you will have to download and install it. For more information, see Group Policy overview for Office 2010.

To start GPMC

- Click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **Group Policy Management**.

For more information about how to set Group Policy, see Step-by-Step Guide to Understanding the Group Policy Feature Set (*http://go.microsoft.com/fwlink/?LinkId=78160*).

Create a GPO

Group Policy settings are contained in GPOs, which are linked to selected Active Directory containers such as sites, domains, or organizational units (OUs) to enforce specific configurations. You can create several GPOs, each with a specific set of configurations. For example, you might want to create a GPO named "Office 2010" that contains only settings for Office 2010 applications, or one named "Outlook 2010" for only Microsoft Outlook 2010 configurations.

To create a GPO

1. Verify that you have the necessary permissions for the GPO:

   By default, only members of the Domain Admins, Enterprise Admins, Group Policy Creator Owners, and SYSTEM groups can create new GPOs. For more information, see "Delegating creation of GPOs" in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. Open GPMC.
3. In the console tree, right-click **Group Policy Objects** in the forest and domain in which you want to create a GPO. For example, navigate to *Forest name*, **Domains**, *Domain name*, **Group Policy Objects**.
4. Click **New**.
5. In the **New GPO** dialog box, specify a name for the new GPO, and then click **OK**.

Load Office 2010 Administrative Templates to a GPO

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 policy settings are contained in several individual .adm, .admx, or .adml template files, depending on the version of Windows that you are running on your computer. Each .adm, .admx, or .adml file contains the policy settings for a single Office application.

For example, outlk14.admx contains the policy settings for Outlook 2010, and Word14.admx contains the templates for Microsoft Word 2010. You can load one or more of these template files into GPOs that you have designated for Office 2010 configurations.

For example, if you have created a GPO named "Office 2010 settings" to hold all of your Office 2010 configurations, load all of the administrative template files into that GPO. Or, if you have created a GPO named "Outlook 2010 settings" for only Outlook 2010 configurations, load only the outlk14.adm or outlk14.admx template file into that GPO.

To load the Office 2010 Administrative Templates (.adm files) to a GPO

1. Verify that you have the necessary permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify**.

For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).

2. In Group Policy Object Editor, right-click **Administrative Templates** in the **Computer Configuration** or **User Configuration** node, and then select **Add/Remove Templates**. A list of the Administrative Template files that are already added to the GPO is displayed.
3. To add another Administrative Template file, click **Add**, and then browse to the location where you have saved the Office 2010 Administrative Template files.
4. Select the file that you want to add, and then click **Open**. Repeat this step for each Administrative Template file that you want to add.
5. When you are finished adding the files to the GPO, click **Close**. You can then edit the added policy settings in the GPO.

If you use .admx and .adml files on computers that run at least Windows Vista or Windows Server 2008, you can store the .admx and .adml files in one of the following locations:

- An Administrative Templates *central store* in the Sysvol folder of the domain controller. The GPMC included with Windows Server 2008 always uses an Administrative Templates central store over the local versions of the Administrative Templates. This provides a replicated central storage location for domain Administrative Templates.

  When you use a central store, the GPMC reads the entire set of Administrative Template files when you edit, model, or report on a GPO. Therefore, the GPMC must read these files from across the network. If you create an Administrative Templates central store, you should always connect the GPMC to the closest domain controller. The central store consists of the following:

  - A root-level folder, which contains all language-neutral .admx files. For example, create the root folder for the central store on your domain controller at this location:

    *%systemroot%***\sysvol\domain\policies\PolicyDefinitions**
  - Subfolders, which contain the language-specific .adml resource files. Create a subfolder of *%systemroot%***\sysvol\domain\policies\PolicyDefinitions** for each language that you will use. For example, create a subfolder for United States English at this location:

    *%systemroot%***\sysvol\domain\policies\PolicyDefinitions\EN-US**

    For more information about how to store and use the Administrative 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*).
- PolicyDefinitions folder in the local computer.
  - .admx files are stored in this location: *%systemroot%***\PolicyDefinitions**
  - .adml files are stored in this location: *%systemroot%***\PolicyDefinitions**<*ll-cc*>

    where *ll-cc* represents the language identifier, such as en-us for English United States

Group Policy Object Editor automatically reads all .admx files stored in the central store of the domain in which the GPO was created.

When there is no central store, Group Policy Object Editor reads the local versions of the .admx files used by the local GPO.

For more information about ADMX files, see Managing Group Policy ADMX Files Step-by-Step Guide (*http://go.microsoft.com/fwlink/?LinkId=75124*).

Edit a GPO

When you edit a GPO, you are opening the GPO and configuring policy settings within it. After editing a GPO, you apply the GPO to the Active Directory site, domain, or OU to enforce the GPO settings for that site, domain, or OU.

Important

The default domain policy and default domain controllers policy are critical to the health of any domain. Do not edit the Default Domain Controller Policy or the Default Domain Policy GPOs, except in the following cases:

- We recommend that you set account policy in the Default Domain Policy.
- If you install applications on domain controllers that require modifications to User Rights or Audit Policies, the modifications must be made in the Default Domain Controllers Policy.

If you want to apply Group Policy settings to the entire domain, create a new GPO, link the GPO to the domain, and then create the settings in that GPO.

To edit the local GPO: open Group Policy Object Editor by clicking **Start**, then click **Run**, type **gpedit.msc**, and then click **OK**. To edit the local GPO on another computer, type the following at the command prompt: **gpedit.msc /gpcomputer: <ComputerName>**.

To edit a GPO

1. Verify that you have the necessary permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify**.

   For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. Open GPMC.
3. In the console tree, double-click **Group Policy Objects** in the forest and domain that contain the GPO that you want to edit. This is located in *Forest name*, **Domains**, *Domain name*, **Group Policy Objects**.
4. Right-click the GPO that you want to modify, and then click **Edit**. This opens Group Policy Object Editor. Edit settings as appropriate in the Group Policy Object Editor console.

Link a GPO

By linking a GPO to an Active Directory site, domain, or OU, you are applying the configurations that you have made in that GPO to it, for all the users or computers it contains.

To link a GPO

1. Verify that you have the necessary permissions:
   - If you want to link an existing GPO to a site, domain, or OU, you must have Link GPOs permission on that site, domain, or OU. By default, only Domain Administrators and Enterprise Administrators have these permissions for domains and OUs, and only Enterprise Administrators and Domain Administrators of the forest root domain have these permissions for sites.
   - If you want to both create and link a GPO, you must have Link GPOs permissions on the domain or OU to which you want to link, and you must have permission to create GPOs in that domain. By default, only Domain Administrators, Enterprise Administrators, and Group Policy Creator owners have permission to create GPOs.
   - If you want to link a GPO to a site, notice that the **Create and Link a GPO Here** option is not available for sites, because it is unclear in which domain to create the GPO. You must first create a GPO in any domain in the forest, and then use the **Link an Existing GPO** option to link the GPO to the site.

   For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208).*
2. Open GPMC.
3. In the console tree, locate the site, domain, or OU to which you want to link a GPO. These are located under *Forest name*, **Domains** or *Sites*, or *Site name*, *Domain name*, or *organizational unit name*.
4. To link an existing GPO, right-click the domain or organizational unit within the domain, and then click **Link an Existing GPO**. In the **Select GPO** dialog box, click the GPO that you want to link, and then click **OK**.

   -or-

   To link a new GPO, right-click the domain or OU in a domain, and then click **Create and Link a GPO Here**. In the **Name** box, type a name for the new GPO, and then click **OK**.

See Also

Group Policy overview for Office 2010

Planning for Group Policy in Office 2010

Disable user interface items and shortcut keys in Office 2010

Disable user interface items and shortcut keys in Office 2010

You can use Group Policy to disable user interface (UI) items and keyboard shortcuts in Microsoft Office 2010. The background and procedural information in this article will assist you with that process.

In this article:

Before performing any of the procedures in this article, make sure that you have installed the Office 2010 Administrative Templates. For more information about how to download and install the Administrative Templates, see Load Office 2010 Administrative Templates to a GPO in Enforce settings by using Group Policy in Office 2010.

Using Group Policy to disable UI items and keyboard shortcuts

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**.

The **Custom | Disable commands** and **Disable shortcut keys** policy settings are available for the following Office 2010 applications:

- Microsoft Access 2010
- Microsoft Excel 2010
- Microsoft Outlook 2010
- Microsoft PowerPoint 2010
- Microsoft Visio 2010
- Microsoft Word 2010

The **Custom | Disable commands** policy settings are also available for the following Office 2010 applications:

- Microsoft InfoPath 2010

- Microsoft Publisher 2010
- Microsoft SharePoint Designer 2010

Policy settings for the Office 2010 applications are accessed under the **User Configuration\Administrative Templates** node in Group Policy Object Editor. To disable user interface items and shortcut keys, administrators can enable one of the following policy settings under the **Disable items in User Interface\Custom** node for an Office 2010 application:

- **Disable commands** Allows you to specify the control ID for the command that you want to disable. If you disable a TCID, that TCID is disabled everywhere the toolbar control is used. To disable a tab, you can disable the controls on the tab. For more information, see Disabling commands by using control IDs later in this article.
- **Disable shortcut keys** Allows you to specify the virtual key code and modifier (as *key,modifier*) for the keyboard shortcut you want to disable. Key is the value of a key (for example, **K**) in Windows, and modifier is the value of either a modifier key (such as **ALT**) or a combination of modifier keys in Windows. For more information, see Disabling shortcut keys by using virtual key codes later in this article.

Policy settings are also available for disabling *predefined* user interface items and shortcut keys for the Office 2010 applications. For more information, see Disabling predefined user interface items and shortcut keys later in this article.

Disabling commands by using control IDs

You must first obtain the control IDs for the Office 2010 application controls that you want to disable by using the custom **Disable commands** policy setting. For information about how to download files that list the control IDs for built-in controls in all applications that use the Office 2010 Office Fluent UI, see Office 2010 Help Files: Office Fluent User Interface Control Identifiers (*http://go.microsoft.com/fwlink/?LinkId=181052*).

For information about how to use Group Policy Object Editor from the Group Policy Management Console Microsoft Management Console (MMC) snap-in, see Group Policy management tools in Group Policy overview for Office 2010.

To disable commands by using control IDs

1. Verify that you have the necessary security permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify security**. For more information about permissions that are needed to manage Group Policy, see “Delegating administration of Group Policy” in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. In the Group Policy Object Editor console, expand **User Configuration**, expand **Administrative Templates**, and then expand the application for which you want to disable commands (for example, double-click **Microsoft Excel 2010**).
3. Click **Disable items in User Interface**, click **Custom**, double-click **Disable commands**, and then click **Enabled**.

4. Click **Show**. In the **Show Contents** dialog box, click **Add**, enter the control ID for the command that you want to disable in the **Add Item** dialog box, and then click **OK**.

   For example, to disable the **Check for Updates** button in Excel (assuming you had previously added this command to the Excel Quick Access Toolbar), you would enter **9340** (the control ID for the **CheckForUpdates** control).

5. Click **OK**. In the **Disable commands** policy **Properties** page, click **OK**.

Disabling shortcut keys by using virtual key codes

The **Disable shortcut keys** policy setting under the **Disable items in user interface\Predefined** node includes several built-in shortcut keys that are listed by name. For example, you can disable **CTRL+K**, the shortcut for the **Hyperlink** command (**Insert** tab, **Links** group). For more information, see Disabling predefined user interface items and shortcut keys later in this article.

To disable other shortcut keys, you set the **Disable shortcut keys** policy setting under the **Disable items in User Interface\Custom** node and add the virtual key code and modifier for the user interface item that you want to disable. Key is the numeric value for a key (such as **V**) in Windows. Modifier is the value of either a modifier key such as **CONTROL**, or a combination of modifier keys in Windows.

The following resources provide information about Office 2010 combination shortcut keys, function keys, and other common shortcut keys, together with descriptions of their functionality. You need the shortcut key information to use the **Custom |Disable shortcut keys** policy settings.

- Keyboard shortcuts for Access (*http://go.microsoft.com/fwlink/?LinkId=182281*)
- Excel shortcut and function keys (*http://go.microsoft.com/fwlink/?LinkId=182282*)
- Keyboard shortcuts for Outlook (*http://go.microsoft.com/fwlink/?LinkId=182283*)
- Keyboard shortcuts for PowerPoint (*http://go.microsoft.com/fwlink/?LinkId=182284*)
- Keyboard shortcuts for Word (*http://go.microsoft.com/fwlink/?LinkId=182285*)
- Keyboard shortcuts for Visio (*http://go.microsoft.com/fwlink/?LinkId=182286*)

The following table provides information about keys and modifiers.

Key or modifier	Value (decimal)
ALT	16
CONTROL	8
SHIFT	4
A	65
B	66
C	67

Key or modifier	Value (decimal)
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

The following table lists the values for the function keys used by the system.

Function key	Value (decimal)
F1	112
F2	113
F3	114
F4	115
F5	116
F6	117
F7	118
F8	119
F9	120
F10	121
F11	122
F12	123

For a more comprehensive list of symbolic constant names, hexadecimal values, and mouse or keyboard equivalents for the virtual-key codes used by the system, see Virtual-Key Codes (*http://go.microsoft.com/fwlink/?LinkId=182271*).

To disable shortcut keys (Custom)

1. Verify that you have the necessary security permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify security**. For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. In the Group Policy Object Editor console, expand **User Configuration**, expand **Administrative Templates**, and then expand the application for which you want to disable commands (for example, double-click **Microsoft Excel 2010**).
3. Click **Disable items in User Interface**, click **Custom**, click **Disable shortcut keys**, and then click **Enabled**.
4. Click **Show**. In the **Show Contents** dialog box, click **Add**. In the **Add Item** dialog box, enter the values for the keyboard shortcut you want to disable as *key,modifier*, and then click **OK**.

For example, to disable the shortcut keys **ALT+F11** in Excel (which opens the **Microsoft Visual Basic Editor**, where you can create a macro), enter **122,16** in the **Add Item** dialog box (where **F11** key = 122 and modifier = 16).

Note:
If there are multiple modifier keys for the keyboard shortcut, add the values of the modifier keys together to determine the modifier value to enter in Group Policy Object Editor console. For example, for the **ALT+SHIFT** combination, you would use the sum of their assigned values, 16+4 = 20.

5. Click **OK**. In the **Disable shortcut keys** policy **Properties** page, click **OK**

Disabling predefined user interface items and shortcut keys

Policy settings are also available to disable predefined user interface items and shortcut keys for the Office 2010 applications. These predefined policy settings for the Office 2010 applications are available in **User Configuration\Administrative Templates\<*application name*>**, under the **Disable items in user interface\Predefined** node of Group Policy Object Editor.

Policy settings for disabling user interface items are available for the following applications:

- Access 2010
- Excel 2010
- PowerPoint 2010
- Word 2010
- SharePoint Designer 2010
- Publisher 2010
- Visio 2010

To disable predefined commands

1. Verify that you have the necessary security permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify security**. For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. In Group Policy Object Editor console, expand **User Configuration**, expand **Administrative Templates**, and then expand the application for which you want to disable commands (for example, double-click **Microsoft Excel 2010**).
3. Click **Disable items in User Interface**, click **Predefined**, double-click **Disable commands**, click **Enabled**, select the commands that you want to disable, and then click **OK**.

To disable predefined shortcut keys

1. Verify that you have the necessary security permissions for the GPO: either **Edit settings** or **Edit settings, delete, and modify security**. For more information about permissions that are needed to manage Group Policy, see "Delegating administration of Group Policy" in the Group Policy Planning and Deployment Guide (*http://go.microsoft.com/fwlink/?LinkId=182208*).
2. In Group Policy Object Editor console, expand **User Configuration**, expand **Administrative Templates**, and then expand the application for which you want to disable commands (for example, double-click **Microsoft Excel 2010**).
3. Click **Disable items in User Interface**, click **Predefined**, double-click **Disable shortcut keys**, click **Enabled**, select the shortcut keys that you want to disable, and then click **OK**.

See Also

Group Policy overview for Office 2010

Planning for Group Policy in Office 2010

Enforce settings by using Group Policy in Office 2010

VII. Customize security by using Group Policy

Configure security for Office 2010

This article provides required information and procedures to configure security settings in Microsoft Office 2010 by using the Office Customization Tool (OCT) and Group Policy.

In this article:

Process overview

You can configure security settings by using the Office Customization Tool (OCT), and by using the Office 2010 Administrative Templates (.adm or admx files) with Group Policy. You can also configure some security settings in the Trust Center, which can be accessed through the user interface of every Office 2010 application. However, from an administration and deployment standpoint, Trust Center settings are useful only for troubleshooting installation and configuration problems on individual computers. The Trust Center cannot be used to deploy or centrally manage security settings.

When you use the OCT to configure security settings, the settings are not permanent. The OCT establishes the initial value for the setting. After Office 2010 is installed, users can use the Trust Center to modify some, but not all, security settings. If you must enforce and prevent users from changing security settings, use Group Policy.

Before you begin

Before you configure security settings, review the following information about planning, permissions, and tool requirements.

Plan security settings

You must complete the following steps in the security planning process before you configure security settings:

- Read Security overview for Office 2010 (*http://technet.microsoft.com/library/67869078-71c6-45f5-aab0-0823c83aed54(Office.14).aspx*). This article describes the new security architecture in Office 2010 and explains how the new security features work together to help provide a layered defense. We recommend that you do not change any security settings until you understand how all of the security features work.
- Read Understand security threats and countermeasures for Office 2010 (*http://technet.microsoft.com/library/1d80acb0-5ca3-4c32-b2f4-e3e013c85cfc(Office.14).aspx*). This

article describes which security risks and threats are relevant to Office 2010. This article also helps you determine which of those security risks and threats pose a risk to the business assets or processes of your organization.

- Read the planning articles in Plan security for Office 2010 (*http://technet.microsoft.com/library/c38e3e75-ce78-450f-96a9-4bf43637c456(Office.14).aspx*). These articles describe the various security settings that you can use to customize Office 2010 security features.

Review required permissions

The following table lists the administrative credentials that are required to configure security settings by using various deployment and management tools.

To perform these actions	You must be a member of this group or groups
Run the OCT.	Administrators group on the local computer
Configure local Group Policy settings by using the Group Policy Object Editor.	Administrators group on the local computer
Configure domain-based Group Policy settings by using the Group Policy Management Console.	Domain Admins, Enterprise Admins, or Group Policy Creator Owners group

Tool prerequisites

You can use several different tools to configure security settings. Before you use these tools, make sure that you:

- Understand how to use the OCT to customize Office 2010. 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*) and Customization overview for Office 2010 (*http://technet.microsoft.com/library/72a93ebf-389a-491a-94c8-d7da02642139(Office.14).aspx*).
- Have created a network installation point from which you can run the OCT. For more information about network installation points, see Create a network installation point for Office 2010 (*http://technet.microsoft.com/library/72c9ae03-1342-4524-8242-1524fbd068a5(Office.14).aspx*).
- Understand what Administrative Templates are (.adm or .admx files). For more information about Administrative Templates, see Group Policy overview for Office 2010.
- Have loaded the Office 2010 Administrative Templates into the Group Policy Object Editor or installed them onto a domain controller.

The OCT is available only with volume licensed versions of Office 2010 and the 2007 Microsoft Office system. To determine whether an 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. If the Admin folder does not exist, the disk is a retail edition.

Configure security settings by using the OCT

The following procedure shows how to use the OCT to configure security settings.

To use the OCT to configure security settings

1. Open a command prompt window and navigate to the root of the network installation point that contains the Office 2010 source files.
2. At the command prompt, type setup.exe /admin, and then press ENTER.
3. In the left pane of the OCT, click **Office security settings**.
4. Change the security settings that you want to configure in the right pane.

Configure security settings by using Group Policy

The following procedure shows how to use Group Policy to configure security settings.

To use Group Policy to configure security settings

1. If you want to change local Group Policy settings, open the Group Policy Object Editor.

   To do this, at the **Run** command, type gpedit.msc, and then press ENTER.
2. Or, open the Group Policy Management Editor on a domain controller if you want to change domain-based Group Policy settings.

   To do this, open the Group Policy Management snap-in, right-click the Group Policy object (GPO) that you want to modify, and then click **Edit**.
3. In the Group Policy Object Editor tree or the Group Policy Management Editor tree, find the security setting that you want to change in one of the following locations:
   - User Configuration/Policies/Administrative Templates/Microsoft Access 2010/Application Settings/Security
   - User Configuration/Policies/Administrative Templates/Microsoft Excel 2010/Excel Options/Security
   - User Configuration/Policies/Administrative Templates/Microsoft InfoPath 2010/Security
   - User Configuration/Policies/Administrative Templates/Microsoft Office 2010/Security Settings
   - User Configuration/Policies/Administrative Templates/Microsoft OneNote 2010/OneNote Options/Security
   - User Configuration/Policies/Administrative Templates/Microsoft Outlook 2010/Security
   - User Configuration/Policies/Administrative Templates/Microsoft PowerPoint 2010/PowerPoint Options/Security
   - User Configuration/Policies/Administrative Templates/Microsoft Project 2010/Security

- User Configuration/Policies/Administrative Templates/Microsoft Publisher 2010/Security
- User Configuration/Policies/Administrative Templates/Microsoft Visio 2010/Visio Options/Security
- User Configuration/Policies/Administrative Templates/Microsoft Word 2010/Word Options/Security

4. Double-click the security setting and make the changes that you want to make.

Tip:

If you cannot find the security setting that you want to change, try searching in the previously listed locations within the Computer Configuration/Policies/Administrative Templates node.

See Also

Security overview for Office 2010 (*http://technet.microsoft.com/library/67869078-71c6-45f5-aab0-0823c83aed54(Office.14).aspx*)

Configure Information Rights Management in Office 2010

Users can restrict permission to content documents and e-mail messages in Microsoft Office 2010 by using Information Rights Management (IRM). You can configure IRM options in your organization to encrypt document properties for IRM content by using Group Policy or the Office Customization Tool (OCT).

In this article:

Overview

You can lock down many settings to customize IRM by using the Office Group Policy template (Office14.adm) and Outlook Group Policy template (Outlk14.adm). You can also use the Office Customization Tool (OCT) to configure default settings, which enables users to change the settings. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT. In addition, there are IRM configuration options that can only be configured by using registry key settings. For a list of IRM settings, see Plan for Information Rights Management in Office 2010.

In Microsoft 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 Outlook administrator, you can configure several options for IRM e-mail, such as disabling IRM or configuring local license caching. You can also design custom IRM permissions for users, in addition to the default **Do Not Forward** permissions group. For more information, see Setting up IRM for Office 2010 in Plan for Information Rights Management in Office 2010.

Before you begin

Before you start deployment, review Plan for Information Rights Management in Office 2010 to determine which settings that you might have to configure for IRM.

The Office 2010 and Outlook 2010 templates and other ADM files can be downloaded from the Microsoft Download Center. For more 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*).

Turn off Information Rights Management

You can turn off IRM for all Microsoft Office applications. To turn off IRM in Outlook 2010, you must turn off IRM for all Microsoft Office applications. There is no separate option to turn off IRM only in Microsoft Outlook.

To turn off IRM in Office 2010 by using Group Policy

1. In Group Policy, load the Office 2010 template (Office14.adm) and go to **User Configuration\Administrative Templates\Microsoft Office 2010\Manage Restricted Permissions**.
2. Double-click **Turn Off Information Rights Management User Interface**.
3. Click **Enabled**.
4. Click **OK**.

Configure automatic license caching for Outlook

By default, Outlook 2010 automatically downloads the IRM license for rights-managed e-mail when Outlook synchronizes with Exchange Server. You can configure Outlook 2010 to prevent license information from being cached locally so that users must connect to the network to retrieve license information to open rights-managed e-mail messages.

To disable automatic license caching for IRM by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm) and go to **User Configuration\Administrative Templates\Microsoft Outlook 2010\Miscellaneous**.
2. Double-click **Do not download rights permission license information for IRM e-mail during Exchange folder sync**.
3. Click **Enabled**.
4. Click **OK**.

Enforce e-mail expiration

You can also use IRM to help enforce an e-mail expiration period that you configure for Outlook 2010. When a user specifies the number of days before a message expires with IRM enabled, the message cannot be accessed after the expiration period.

As an administrator, you can specify an expiration period for all Outlook e-mail messages in your organization. The expiration period is enforced only when users send rights-managed e-mail.

To configure an expiration period for e-mail messages by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm) and go to **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Preferences\E-mail Options\Advanced E-mail Options**.
2. Double-click **When sending a message**.
3. Click **Enabled**.
4. In the **Messages expire after (days)** box, enter a number of days.
5. Click **OK**.

Deploy rights policy templates

The IRM policy settings that are available in the Office Group Policy template (Office14.adm) can be configured to point to the location where the rights policy templates are stored (either locally or on an available server share).

To configure the IRM rights policy templates location in Group Policy

1. In Group Policy, load the Office 2010 template (Office14.adm) and go to **User Configuration\Administrative Templates\Microsoft Office 2010\Manage Restricted Permissions**.
2. Double-click **Specify Permission Policy Path**.
3. Click **Enabled**.
4. In the **Enter path to policy templates for content permission** box, type the full path to the IRM permission policy templates.
5. Click **OK**.

See Also

Plan for Information Rights Management in Office 2010

VIII. Customize Outlook 2010 by using Group Policy

Enable SharePoint Server 2010 Colleague in Outlook 2010

This article describes how to configure the Microsoft Office 2010 client to enable the Microsoft SharePoint Server 2010 Colleague add-in in Microsoft Outlook 2010.

In this article:

Overview

The SharePoint Server Colleague add-in in Microsoft 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 by the **Add Colleagues** page on a user's SharePoint My Site Web site where they can choose the colleagues they want to add to their My Site. The user can approve or reject contact names and keywords before they are added to the **Ask Me About** Web Part.

By default, the Colleagues scan is turned on. You can disable this feature by using Group Policy.

You can lock down the settings to customize the Colleagues scan by using the Office Group Policy Administrative template (Office14.adm). Or, you can configure default settings by using the Office Customization Tool (OCT), in which case users can change the setting from the configuration you deploy.

Before you begin

Before you start deployment, review Planning for Group Policy in Office 2010, Planning overview for Outlook 2010 (*http://technet.microsoft.com/library/9eabd5ec-3f76-4048-b98b-f11aa85cc544(Office.14).aspx*), and Plan user profiles (SharePoint Server 2010) (*http://go.microsoft.com/fwlink/?LinkId=182364*).

Configure Colleagues for My Site

Use the following procedures to configure Colleagues settings. The first two procedures are for administrators to configure Colleagues by using Group Policy or the OCT. The third procedure describes how to deploy the My Site registry keys for users by using the OCT. You must deploy the My Site URL registry data for the Colleagues scan to work. The last procedure provides steps for users to turn off this feature in Outlook 2010.

To configure Colleagues by using Group Policy

1. In Group Policy, load the Office 2010 template (Office14.adm). Steps vary according to the version of Windows that you are running.
2. Open the Group Policy Management Console (GPMC). In the tree view, expand **Domains**, and then expand **Group Policy Objects**.
3. Right-click the policy object that you want, and then click **Edit**. The Group Policy Management Editor window opens.
4. In the tree view, expand **User Configuration** | **Policies** | **Administrative Templates \ Classic Administrative Templates (ADM)** \ **Microsoft Office 2010 \ Server Settings \ SharePoint Server**.
5. Double-click **Enable Colleague Import Outlook Add-In to work with Microsoft SharePoint Server**.
6. Select **Enabled** to enable the policy setting. Or, select **Disabled** to disable the policy.
7. Click **OK**.
8. If you enable the policy, you can also set other policies in this folder, such as **Maximum number of recipients in an Outlook item to scan to determine the user's colleagues for recommendation** and **Minimum time before starting Colleague recommendation scan**.
9. Save the Group Policy.

To configure Colleagues by using the Office Customization Tool

1. Start the OCT by running Setup with the **/admin** command-line option.
2. On the **Modify User Settings** page, expand the tree to **Microsoft Office 2010 system \Server Settings \ SharePoint Server**.
3. Double-click **Enable Colleague Import Outlook Add-In to work with Microsoft SharePoint Server**.
4. Select **Enabled** to enable the policy setting. Or, select **Disabled** to disable the policy by default.
5. If you enable the policy, you can also set other policies in this folder, such as **Maximum number of recipients in an Outlook item to scan to determine the user's colleagues for recommendation** and **Minimum time before starting Colleague recommendation scan**.
6. Complete other Office 2010 configurations. On the **File** menu, click **Save** to create the customization file that you can deploy to users.

To set the My Site URL by using the OCT

1. Start the OCT by running Setup with the **/admin** command-line option.
2. In the **Additional content** area, click **Add registry entries**.

3. Click **Add** to add the registry entries shown 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*.
HKEY_CURRENT_USER	REG_SZ	Software\Policies\Microsoft\Office\14.0\common\Portal\Link Providers\MySiteHost	Display Name	The name to display to the user – for example, *MySite*.

4. Complete other Office 2010 configurations. On the **File** menu, click **Save** to create the customization file that you can deploy to users.

To manually turn off Colleagues in Outlook 2010

1. In Outlook 2010, on the **File** tab, click **Options**.
2. In the **Outlook Options** dialog box, select **Advanced**.
3. In the **Other** section, clear the check box **Allow analysis of sent e-mails to identify people you commonly e-mail and subjects you commonly discuss, and upload this information to the default SharePoint Server**.
4. Click **OK**.

See Also

Planning for Group Policy in Office 2010

Planning overview for Outlook 2010 (*http://technet.microsoft.com/library/9eabd5ec-3f76-4048-b98b-f11aa85cc544(Office.14).aspx*)

Plan user profiles (SharePoint Server 2010) (*http://technet.microsoft.com/library/3e61c238-cc09-4369-b8d3-f1150c1ae89b(Office.14).aspx*)

Configure Outlook Anywhere in Outlook 2010

You can configure user accounts in Microsoft Outlook 2010 to connect to Microsoft Exchange Server 2003 or a later version over the Internet without using virtual private network (VPN) connections. This feature, which permits connection to an Exchange Server account by using Outlook Anywhere, enables Outlook users to access their Exchange Server accounts from the Internet when they travel or work outside the organization's firewall.

This article describes the requirements and options for you to configure a group of Outlook user accounts to use Outlook Anywhere. If you want to configure this feature on a single computer, see Use Outlook Anywhere to connect to your Exchange server without VPN (*http://go.microsoft.com/fwlink/?LinkId=160586*).

In this article:

Overview

To configure Outlook 2010 with Outlook Anywhere as part of an Outlook deployment, you enable the option in the Office Customization Tool (OCT) and (optionally) specify additional settings, such as security-level requirements, to communicate with the Exchange Server computer. After you specify these options, you save the settings with other configurations in the Setup customization file (.msp file) that you use to deploy Outlook to users. 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 also lock down some Outlook Anywhere settings by using Group Policy. For more information about Outlook Anywhere Group Policy settings, see Use Group Policy to lock down Outlook Anywhere settings later in this article. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

If your messaging server is Microsoft Exchange Server 2007 or Microsoft Exchange Server 2010, you can use the Outlook 2010 Autodiscover feature to automatically configure Outlook Anywhere. For more information about automatic account configuration, see Outlook Automatic Account Configuration (*http://go.microsoft.com/fwlink/?LinkID=79065*).

Outlook Anywhere was known as RPC over HTTP in earlier versions of Outlook.

Before you begin

- Before you start deployment, review Planning overview for Outlook 2010 (*http://technet.microsoft.com/library/9eabd5ec-3f76-4048-b98b-f11aa85cc544(Office.14).aspx*) to determine the settings that you might have to configure for Outlook Anywhere.
- We recommend that the user accounts that you configure for Outlook Anywhere use Cached Exchange Mode. For more information about Cached Exchange Mode in Outlook, see Plan an Exchange deployment in Outlook 2010.
- Download the Group Policy Administrative template (.adm or .admx) for Outlook 2010. To download the template files, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*).
- Before you configure Outlook Anywhere for Outlook 2010 in an Exchange environment without the Autodiscover service, obtain the URL for the Exchange proxy server that is configured for Outlook Anywhere. This URL is available from the organization's Exchange administrator.

Use the OCT to configure Outlook Anywhere

Use this procedure to use the OCT to configure Outlook Anywhere.

To configure Outlook Anywhere by using the OCT

1. In the OCT, in the tree view, locate **Outlook**, and then click **Add accounts**. Click the Exchange account that you want to configure and then click **Modify**.
2. If you are defining a new Exchange Server computer for users, enter a value or replaceable parameter in **User Name**.

   For example, you might specify *=%UserName%* to use the exact logon name for each user. This helps prevent user prompts when Outlook asks users to decide among several variations.
3. If you are defining a new Exchange Server computer, in the **Exchange Server** text box enter the name of the Exchange Server computer.

   Skip steps 2 and 3 if you are configuring Outlook Anywhere for existing Exchange users who are not moving to a new Exchange Server computer.
4. Click **More Settings**.
5. In the **Exchange Settings** dialog box, select the **Configure Outlook Anywhere** check box and then select the **Connect to Exchange Mailbox using HTTP** check box.
6. In the text box that follows these check boxes, type the server name for the Outlook Anywhere proxy server.

   Do not enter **http://** or **https://** as part of the name.
7. Decide whether you want users to connect through Secured Sockets Layer (SSL) only. If you want to support both server authentication and client authentication, select **Mutually authenticate the session when the system connects with SSL** and enter the principal name

of the proxy server.

8. Select whether or not to reverse the default way in which Outlook decides which connection type to try first, LAN (TCP/IP) or Outlook Anywhere (HTTP). The default is LAN (TCP/IP) first, then Outlook Anywhere (HTTP). If you expect users to connect when they are outside the corporate network more frequently than when they are inside the corporate network, we recommend that you configure Outlook to try Outlook Anywhere (HTTP) first.
9. Select an authentication method from the drop-down list.

   The default method is Password Authentication (NTLM).
10. Click **OK** to return to the **Exchange Settings** dialog box, and then click **Finish**.
11. Complete other Outlook or Microsoft Office configurations, and on the **File** menu, click **Save** to create the customization file that you can deploy to users.

Use Group Policy to lock down Outlook Anywhere settings

Use this procedure to use Group Policy to lock down Outlook Anywhere.

To lock down Outlook Anywhere settings in the user interface by using Group Policy

1. In the Group Policy Object Editor, load the Outlook 2010 Administrative template (Outlk14.adm).
2. To customize Cached Exchange Mode options, open the Group Policy Management Console (GPMC) and in the tree view expand **Domains** and then expand **Group Policy Objects**.
3. Right-click the policy object you want and click **Edit**. The Group Policy Management Editor window opens.
4. In the tree view, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Classic Administrative Templates (ADM)**, expand **Microsoft Outlook 2010**, expand **Account Settings**, and then click **Exchange**.
5. In the reading pane, in the **Setting** column, double-click the policy that you want to set. For example, double-click **Configure Outlook Anywhere user interface options**.
6. Select **Enabled**.
7. Click an option in the **Choose UI State when OS can support feature** drop-down list.
8. Click **OK**.

Verification

After you have finished your configurations, apply the configurations in a test environment. In the test environment, open Outlook and verify that the configurations are applied as expected.

See Also

Exchange Server 2003 RPC over HTTP Deployment Scenarios (*http://go.microsoft.com/fwlink/?LinkId=124051*)

Deploying Outlook Anywhere (*http://go.microsoft.com/fwlink/?LinkId=124053*)

Configure Cached Exchange Mode in Outlook 2010

This article describes how to configure Cached Exchange Mode for Microsoft Exchange Server e-mail accounts in Microsoft 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 Exchange mailbox stored in an Offline Folder (.ost file) on the user's computer, and with the Offline Address Book (OAB). The cached mailbox and OAB are updated periodically from the Exchange Server computer.

Cached Exchange Mode can be configured for Exchange Server e-mail accounts only. Cached Exchange Mode is supported by all versions of Exchange Server with which Outlook 2010 can connect; that is, by Exchange Server 2003 or later versions.

If you do not configure Cached Exchange Mode options, the current state of Cached Exchange Mode does not change for existing profiles when Microsoft Outlook is upgraded to a new version. For example, if a user account was configured to use Cached Exchange Mode in Office Outlook 2003 or Microsoft Office Outlook 2007, Cached Exchange Mode remains enabled when the user upgrades the software to Outlook 2010. The location for new .ost or OAB files is the default location: For Windows XP, the location is %userprofile%\Local Settings\Application Data\Microsoft\Outlook; for Windows Vista and Windows 7, the location is %userprofile%\AppData\Local\Microsoft\Outlook.

You can configure several options for Cached Exchange Mode. These include the default .ost file location for users in your organization who do not already have .ost files for Cached Exchange Mode. If you do not specify a different .ost file location, Outlook creates an .ost file in the default location when users start Outlook in 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.

Before you begin

Before you start deployment, review Plan an Exchange deployment in Outlook 2010 and Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*) to determine which settings you might have to configure for Cached Exchange Mode.

To download the Outlook 2010 administrative templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool (*http://go.microsoft.com/fwlink/?LinkId=189316*). For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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*).

If you migrate from an earlier version of Outlook with Cached Exchange Mode enabled, determine which format your users' .ost files are in (ANSI or Unicode). 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*).

Configure Cached Exchange Mode

Use the following procedures to configure Cached Exchange Mode settings.

To configure Cached Exchange Mode settings by using the Office Customization Tool

1. In the Office Customization Tool, in the tree view, locate **Outlook**, click **Add Accounts**. In the **Account Name** column of the reading pane list, click the account that you want to configure, and then click **Modify**. The **Exchange Settings** dialog box appears.

   Note that in the tree view of the OCT you must click **Outlook Profile** and then select **Modify Profile** or **New Profile** to add an Exchange account and configure Exchange Server settings.
2. To specify a new location for users' Outlook data files (.ost), in the **Exchange Settings** dialog box click **More Settings**, and then select **Enable offline use**. Enter a folder path and file name for the .ost file location. You can also enter a path in the **Directory path to store the Offline Address Book files** text box
3. To enable or disable Cached Exchange Mode, or to specify default download behavior when Cached Exchange Mode is enabled, click the **Cached Mode** tab.
4. Select **Configure Cached Exchange Mode** and then select the **Use Cached Exchange Mode** check box to enable Cached Exchange Mode for users. By default, Cached Exchange Mode is disabled if you do not select the **Use Cached Exchange Mode** check box.
5. If you enabled Cached Exchange Mode in step 4, select a default download option on the **Cached Mode** tab:
   - **Download only headers** Users see header information and the beginning of the message or item body (a 256-KB plain-text buffer of information). Full items can be

downloaded later in several ways; for example, by double-clicking to open the message or by clicking **Download the rest of this message now** in the reading pane.

- **Download headers followed by the full item** All headers are downloaded first, and then full items are downloaded. The download order might not be chronological. Outlook downloads headers followed by full items in the folder that the user is currently accessing, and then downloads headers followed by full items in folders that the user has recently viewed.
- **Download full items** Full items are downloaded. We recommend this option unless you have a slow network connection. The download order might not be chronological. Outlook downloads full items in the folder that the user is currently accessing, and then downloads full items in folders that the user has recently viewed.

6. To turn off Headers Only mode, select the **Download full items** option button and clear the **On slow connections, download only headers** check box. Downloading only headers is the default behavior when users have slow connections. There are scenarios in which Outlook perceives that users have slow connections when users' data throughput is fast, or vice versa. In these situations, you might want to set or clear this option.
7. Disable the downloading of shared non-mail folders as part of Cached Exchange Mode synchronizations to users' .ost files. By default, shared non-mail folders are downloaded. Downloading shared non-mail folders increases the size of users' .ost files.
8. Download Public Folder Favorites as part of Cached Exchange Mode synchronizations to users' .ost files. By default, Public Folder Favorites are not downloaded. As with shared non-mail folders, downloading Public Folder Favorites increases the size of users' .ost files. Also, synchronizing Public Folder Favorites causes additional network traffic that might be unwelcome for users who have slow connections.
9. If you have to enable shared mail folders that use Cached Exchange Mode, follow these steps:
   a. In OCT, in the tree view, locate **Additional Content** and then click **Add registry entries**.
   b. In the reading pane, click **Add**.
   c. Enter the following information:

Root	Data type	Key	Value name	Value data
HKEY_Current_User	REG_SZ	Software\Microsoft\Office\14.0\Outlook\CachedMode	CacheOthersMail	1

   d. Click **OK**.

To configure Cached Exchange Mode settings by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm).
2. To customize Cached Exchange Mode options, open the Group Policy Management Console (GPMC) and in the tree view expand **Domains** and then expand **Group Policy Objects**.
3. Right-click the policy object that you want and then click **Edit**. The Group Policy Management Editor window opens.
4. In the tree view, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Classic Administrative Templates (ADM)**, expand **Microsoft Outlook 2010**, expand **Account Settings**, and then click **Exchange**. You can also expand **Exchange** and then click **Cached Exchange Mode**.
5. In the reading pane, in the **Setting** column, double-click the policy that you want to set. For example, in the **Exchange** reading pane, double-click **Use Cached Exchange Mode for new and existing Outlook profiles**.
6. Select **Enabled** and select an option (if appropriate).
7. Click **OK**.

To configure a default .ost location by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm).
2. To configure a default .ost location, open the Group Policy Management Console (GPMC) and in the tree view expand **Domains** and then expand **Group Policy Objects**.
3. Right-click the policy object that you want and then click **Edit**. The Group Policy Management Editor window opens.
4. In the tree view, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Classic Administrative Templates (ADM)**, expand **Microsoft Outlook 2010**, expand **Miscellaneous**, and then click **PST Settings**.
5. Double-click **Default location for OST files**.
6. Select **Enabled** to enable the policy setting.
7. In the **Default location for OST files** text box, enter the default location for .ost files. For example:

   %userprofile%\Local Settings\Application Data\Microsoft*newfolder*.
8. Click **OK**.

   You can define a new default location for both Personal Outlook data files (.pst) and .ost files. After you click **PST Settings** in the tree view, click the **Default location for PST and OST files** setting in the reading pane.

To force upgrade of non-Unicode ANSI format .ost files to Unicode

1. For users who have existing non-Unicode ANSI format .ost files, the following procedure does

not upgrade ANSI .ost files to Unicode .ost files. The procedure merely creates a new Unicode .ost file for the user's profile, leaving the original ANSI .ost files alone.

2. To determine which format your users' .ost files are in (ANSI or Unicode), 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*).
3. In Group Policy, load the Outlook 2010 template (Outlk14.adm).
4. Open the Group Policy Management Console (GPMC) and in the tree view expand **Domains** and then expand **Group Policy Objects**.
5. Right-click the policy object that you want and then click **Edit**. The Group Policy Management Editor window opens.
6. In the tree view, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Classic Administrative Templates (ADM)**, expand **Microsoft Outlook 2010**, expand **Account Settings**, and then expand **Exchange**.
7. Double-click **Exchange Unicode Mode — Ignore OST Format**.
8. Select **Enabled** to enable the policy configuration.
9. In the **Choose whether existing OST format determines mailbox mode** drop-down list, click **Create new OST if format doesn't match mode**.
10. Click **OK**.
11. Double-click **Exchange Unicode Mode — Silent OST format change**.
12. Select **Enabled** to enable the policy configuration, and then click **OK**.
13. Double-click **Exchange Unicode Mode — Turn off ANSI mode**.
14. Select **Enabled** to enable the policy configuration, and then click **OK**.
15. In the tree view, expand **Miscellaneous**, click **PST Settings**, and in the reading pane double-click **Preferred PST Mode (Unicode/ANSI)**.
16. Select **Enabled**, in the **Choose a default format for new PSTs** drop-down list click **Enforce Unicode PST**, and then click **OK**.

See Also

Plan an Exchange deployment in Outlook 2010

Manage trusted add-ins for Outlook 2010

If you use default Microsoft Outlook 2010 security settings, all Component Object Model (COM) add-ins 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 Microsoft Outlook object model blocks.

In this article:

Overview

To trust a COM add-in, you include the file name for the add-in in a Group Policy setting that uses a calculated hash value for the file. Before you can specify an add-in as trusted by Outlook, you must install the Microsoft Office Outlook 2007 Security Hash Generator Tool to calculate the hash value.

The Office Outlook 2007 Security Hash Generator Tool runs on 32-bit Windows systems and can be used to calculate the hash value for Outlook 2010 add-ins. You cannot run the Office Outlook 2007 Security Hash Generator Tool on 64-bit Windows systems.

Before you begin

For more information about how to download the Outlook 2010 administrative template, and about other Office 2010 administrative template files, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

For information about how to work with Outlook 2010 COM add-ins and how to customize other security settings, see Choose security and protection settings for Outlook 2010.

For more information about how to use the Office Outlook 2007 Security Hash Generator Tool, see Tips for using the Outlook 2007 Security Hash Generator Tool (*http://go.microsoft.com/fwlink/?LinkId=185017*).

Get the hash value for a trusted add-in

To add a trusted add-in by using Group Policy, you must install and run the hash calculation program to calculate the hash value for the Group Policy setting, **Configure trusted add-ins**.

To get the hash value for a trusted add-in

1. From the Microsoft Download Center, download the Outlook 2007 Tool: Security Hash Generator (*http://go.microsoft.com/fwlink/?LinkId=75742*).
2. Extract the contents to a local folder (such as C:\Hashtool).
3. Run the command prompt for your computer: Click **Start**, **All Programs**, **Accessories**, **Command Prompt**.

   Windows Vista requires an additional step: Right-click **Command Prompt**, and then select **Run as administrator**.
4. Change directories to the folder where you extracted the hash tool files.
5. Type the following command, and then press ENTER:

   createhash.bat /register

   (This step needs to be completed only once.)
6. Type the following command, and then press ENTER:

   createhash.bat <filename>

   Where <*filename*> is the full path and file name of the add-in file that you are creating the hash number for. There should be no spaces in the file path or file name. If there is, make a copy of the add-in DLL and put it in a folder that has no spaces in the file path or use the short file name and path (8.3 path). The hash is based on the registered DLL and not the location of the DLL.
7. Press ENTER.
8. Copy and save the value that is displayed on the screen to the clipboard. This is the value that you will add to the Group Policy setting (see the following procedure).

Specify the trusted add-in by using Group Policy

Once you have generated the hash value for the add-in, you must specify the add-in as trusted by entering in Group Policy the value generated by the program, paired with the add-in file name.

To specify the trusted add-in by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm) and go to **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security\Security Form Settings\Programmatic Security\Trusted Add-ins**.
2. Double-click **Configure trusted add-ins**, and then click **Enabled**.
3. Click **Show**.
4. In the **Show contents** dialog box, click **Add**.

5. In the **Add item** dialog box, in the **Enter the name of the item to be added** field, type the file name of the COM add-in.
6. In the **Enter the value to be added** field, paste the hash value of the COM add-in that you saved when you ran the hash value calculation program.
7. Click **OK** three times.

The COM add-in can now run without prompts for Outlook 2010 users who use this security setting.

To remove a file from the list of trusted add-ins, update the Group Policy setting by deleting the entry for the add-in.

Remove the Security Hash Generator Tool

You can remove the Office Outlook 2007 Security Hash Generator Tool by unregistering the CreateHash.bat file and deleting the extracted files.

To remove the Security Hash Generator Tool

1. Run the command prompt for your computer: Click **Start**, **All Programs**, **Accessories**, **Command Prompt**.

   Windows Vista requires an additional step: Right-click **Command Prompt**, and then select **Run as administrator**.
2. Change directories to the folder where you extracted the hash tool files.
3. Type the following command, and then press ENTER:

   createhash.bat /unregister
4. Delete the extracted files from the folder.

See Also

Choose security and protection settings for Outlook 2010

Tips for using the Outlook 2007 Security Hash Generator Tool
(*http://go.microsoft.com/fwlink/?LinkId=185017*)

Configure junk e-mail settings in Outlook 2010

This article describes how to create Junk E-mail Filter lists in Microsoft Outlook 2010, and how to configure the Junk E-mail Filter and automatic picture download by using Group Policy or the Office Customization Tool (OCT).

This article is for Outlook administrators. To learn more about how to configure junk e-mail settings in Outlook on your desktop, see Change the level of protection in the Junk E-Mail Filter (*http://go.microsoft.com/fwlink/?LinkId=81273*).

In this article:

Overview

Microsoft Outlook 2010 provides features that can help users avoid receiving and reading junk e-mail messages that include the Junk E-mail Filter and the ability to disable automatic content download from external servers.

Junk e-mail filtering in Outlook 2010 includes Junk E-mail Filter lists and technology built into the software that helps determine whether an e-mail message should be treated as junk e-mail. You can create the following initial Junk E-mail Filter lists to deploy to users: lists for Safe Senders, Safe Recipients, and Blocked Senders.

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. If you deploy the lists by using the OCT, users can customize and keep their customized lists as they use Outlook, to fine-tune the filters to work best for their messaging needs.

You can use Group Policy or the Office Customization Tool (OCT) to customize settings for the Junk E-mail Filter, and to disable automatic content download to meet the needs of your organization. For example, you can configure the Junk E-mail Filter to be more aggressive. However, that might also catch more legitimate messages. Rules that are not part of the junk e-mail management built into the software are not affected.

Before you begin

Review Plan for limiting junk e-mail in Outlook 2010 to determine what settings to configure for the Junk E-mail Filter and automatic content download.

For information about how to download the Outlook 2010 administrative template, and about other Office 2010 templates, see Office 2010 Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool. For more information about Group Policy, see Group Policy overview for Office 2010 and Enforce settings by using Group Policy in Office 2010.

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*).

Create and deploy Junk E-mail Filter lists

To deploy Junk E-mail Filter lists, first create the lists on a test computer and then distribute the lists to users. You can distribute the lists by putting the lists on a network share. 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.

To create default Junk E-mail Filter lists

1. Install Outlook 2010 on a test computer.
2. Start Outlook 2010.
3. In Outlook 2010, on the **Home** tab, in the **Delete** group, click **Junk** and **Junk E-mail Options**.
4. On the **Safe Senders** tab, click **Add**.
5. Enter an e-mail address or domain name. For example:

   someone@exchange.example.com
6. Click **OK**.
7. To add more e-mail addresses or domain names, repeat steps 3 through 6.
8. Click **Export to file**.
9. Enter a unique file name for the Safe Senders list, and then click **OK**.
10. Repeat steps 3 through 9 with the Safe Recipients tab and the Blocked Senders tab to create Safe Recipients and Blocked Senders lists. Be sure to specify a unique file name for each of the three lists.

Deploy Junk E-mail Filter lists for users by using the Office Customization Tool

1. Copy the three Junk E-mail Filter files that you created in the previous procedure to a network file share.
2. If you have remote users not connected to the domain, follow these steps.
   a. In the OCT, click **Add Files** and then click **Add**.
   b. In the **Add Files to** dialog box, select the three Junk E-mail Filter files that you created in

the previous procedure.

Hold down the CONTROL or SHIFT key to select multiple files.

c. Click **Add**.

d. In the **Destination path on the user's computer** dialog box, enter the folder where you want to install the file on users' computers, and then click **OK**.

e. Click **OK** again.

1. On the **Modify User Settings** page, under **Microsoft Outlook 2010\Outlook Options\Preferences**, click **Junk Mail**.
2. Double-click **Junk Mail Import List**, click **Enabled** and **OK** so that the setting is applied and Junk E-mail Filter lists are imported for users.
3. To overwrite existing Junk E-mail Filter lists with new lists, double-click **Overwrite or Append Junk Mail Import List**, click **Enabled** and then click **OK**.
4. To specify a path of each Junk E-mail Filter list, double-click the settings that correspond to each list (for example, **Specify path to Safe Senders**), click **Enabled** and enter a path and file name in the box (for example, in the **Specify path to Safe Senders** list).
5. Click **OK** or click **Next setting** to specify the path for another Junk E-mail Filter list.
6. Complete other Outlook 2010 or Office 2010 configurations, and on the **File** menu, click **Save** to create the customization file that you can deploy to users.

You can later change an existing Outlook 2010 installation to update the Junk E-mail Filter lists by following the procedure and including more recent Junk E-mail Filter files.

For more information about how to use the Office Customization Tool for configuring an Office installation to deploy files, see Office Customization Tool in Office 2010 (*http://technet.microsoft.com/library/8faae8a0-a12c-4f7b-839c-24a66a531bb5(Office.14).aspx*).

Configure the Junk E-mail Filter

You can lock down the settings to customize Junk E-mail Filter options by using the Outlook 2010 Group Policy template (Outlk14.adm). Or you can configure default settings by using the OCT. If this is the case, users can change the settings. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

If you decide to configure Junk E-mail Filter settings in the OCT, see the procedure *To configure Outlook Junk E-mail Filter settings in the Office Customization Tool* later in this article for an additional setting that must be configured.

Use the following procedure to configure Junk E-mail Filter options in Outlook. For the Junk E-mail Filter options that you can configure, see Plan for limiting junk e-mail in Outlook 2010.

To configure Outlook Junk E-mail Filter settings in Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm) and open **User Configuration\Administrative Templates\Microsoft Outlook 2010\Outlook Options\Preferences\Junk E-mail**.
2. Double-click the option that you want to configure. For example, double-click **Junk E-mail protection level**.
3. Click **Enabled**.
4. If appropriate, select a radio button for the option that you want to set, or select an option from a drop-down list.
5. Click **OK**.
6. To activate the Junk E-mail settings, you must set the Junk E-Mail Import list setting. You can do this by using the OCT.
    f. In the OCT, on the **Modify user settings** page, under **Microsoft Outlook 2010\Outlook Options\Preferences\Junk E-mail**, double-click **Junk Mail Import list**.
    g. Click **Enabled**.
    h. Click **OK**.
    i. Complete other Outlook 2010 or Microsoft Office 2010 configurations in the OCT, and on the **File** menu, click **Save** to create the customization file that you can deploy to users.

To configure Outlook Junk E-mail Filter settings in the Office Customization Tool

1. In the OCT, on the **Modify user settings** page, under **Microsoft Outlook 2010\Outlook Options\Preferences\Junk E-mail**, double-click **Junk Mail Import list**.
2. Click **Enabled**.
3. Click **OK**.
4. Double-click and set any other Junk E-mail options that you want to configure.
5. Complete other Outlook 2010 or Microsoft Office 2010 configurations, and on the **File** menu, click **Save** to create the customization file that you can deploy to users.

Configure automatic picture download

To help protect users' privacy and to combat Web beacons—functionality embedded within items to detect when recipients have viewed an item—Outlook 2010 is configured by default to not automatically download pictures or other content from external servers on the Internet.

You can lock down the settings to customize automatic picture download by using the Outlook 2010 Group Policy template (Outlk14.adm). Or you can configure default settings by using the OCT. If this is

the case, users can change the settings. The OCT settings are in corresponding locations on the **Modify user settings** page of the OCT.

To configure options for automatic picture download behavior in Outlook by using Group Policy

1. In Group Policy, load the Outlook 2010 template (Outlk14.adm).
2. Under **User Configuration\Administrative Templates\Microsoft Outlook 2010\Security**, click **Automatic Picture Download Settings**.
3. Double-click the option that you want to configure. For example, double-click **Do not permit download of content from safe zones**.
4. Click **Enabled**.
5. If appropriate, select a radio button for the option that you want to set, or select an option from a drop-down list.
6. Click **OK**.

To configure options for automatic picture download behavior in Outlook by using the Office Customization Tool

1. In the OCT, on the **Modify user settings** page, under **Microsoft Outlook 2010\Security\Automatic Picture Download Settings**, double-click the option that you want to configure. For example, double-click **Include Intranet in Safe Zones for Automatic Picture Download**.
2. Select a radio button for the option that you want to set.
3. Click **OK**.
4. Complete other Outlook 2010 or Office 2010 configurations, and on the **File** menu, click **Save** to create the customization file that you can deploy to users.

See Also

Plan for limiting junk e-mail in Outlook 2010

IX. Customize SharePoint Workspace 2010 by using Group Policy

Configure SharePoint Workspace 2010

This section provides information and procedures for installing, configuring, and testing Microsoft SharePoint Workspace 2010, a client to Microsoft SharePoint Server 2010 and Microsoft SharePoint Foundation 2010.

In this section:

Article	Description
Configure and customize SharePoint Workspace 2010	Provides information and procedures for installing and configuring SharePoint Workspace 2010, a client to SharePoint Server 2010 and SharePoint Foundation 2010.
Test SharePoint Workspace connections	Provides information and procedures for testing SharePoint Workspace 2010 connections to and synchronization with SharePoint Server 2010 and client peers.

Configure and customize SharePoint Workspace 2010

Deploying Microsoft SharePoint Workspace 2010 gives people in your organization anytime interactive access to document libraries and lists at designated SharePoint sites. SharePoint Workspace 2010 also provides options for creating Groove peer workspaces and Shared Folder workspaces, but you can customize the installation to prohibit peer activity or to deploy other configuration settings.

SharePoint Workspace 2010 is a client to Microsoft SharePoint Server 2010 and Microsoft SharePoint Foundation 2010. It is included with Microsoft Office Professional Plus 2010.

For an overview of SharePoint Workspace 2010, see SharePoint Workspace 2010 overview (*http://technet.microsoft.com/library/650cb781-4dbd-45ac-b8d3-2ce9b3a16600(Office.14).aspx*).

In this article:

Before you begin

Before you start deployment, address the following prerequisites:

- Confirm that your setup meets required hardware and software requirements, which are specified in System requirements for Office 2010 (*http://technet.microsoft.com/library/399026a3-007c-405a-a377-da7b0f7bf9de(Office.14).aspx*).
- Address the planning steps in Plan for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/e8a433c1-ea1f-4cf7-adc8-50972f58d465(Office.14).aspx*).
- Confirm that Internet Explorer, version 6, version 7, or version 8 is installed on client computers that have a 32-bit browser.
- Confirm that SharePoint Workspace port settings comply with the specifications in Plan for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/e8a433c1-ea1f-4cf7-adc8-50972f58d465(Office.14).aspx*). SharePoint Workspace 2010 is installed with Windows Firewall turned on and exceptions enabled to support SharePoint Workspace server and client communications. To review or change these settings, open Control Panel, click **System and Security**, click **Windows Firewall**, click **Change notification settings**, and then change or review the settings.
- If you use Active Directory Domain Services (AD DS) and want to customize SharePoint Workspace deployment for Active Directory system group members, make sure that you have

appropriate administrative permissions on the Active Directory system and identify the group to which you want to deploy SharePoint Workspace policies.

- Review customization options in Review customization options for SharePoint Workspace 2010, later in this article.
- If you are integrating SharePoint Workspace with SharePoint Server 2010 sites, prepare SharePoint Server 2010 as follows:
  - Open incoming port 80 to support client/server communications.
  - Consider configuring Secure Socket Layer (SSL) protection for the SharePoint Server-SharePoint Workspace communications port. This configuration is strongly recommended, because no default encryption security is in place.
  - Install Remote Differential Compression (RDC) on SharePoint Server. RDC supports offline synchronization protocols, and optimizes performance during document transfer between SharePoint Workspace and SharePoint Server. To verify RDC status, open Windows Server Manager on the SharePoint Server system and then click **Add Features**. In the **Add Features Wizard** dialog box, make sure that the **Remote Differential Compression** check box is selected. Click **Next**, and then follow the Wizard instructions to install RDC. Or, you can install RDC from a Command Prompt window by typing the following: **servermanagercmd -install rdc**. For more information about RDC, see About Remote Differential Compression (*http://go.microsoft.com/fwlink/?LinkId=162305*).
  - Ensure that offline availability of content is enabled for SharePoint sites (the default condition). SharePoint site administrators can configure this setting by clicking **Site Actions**, **Site Settings**, **Site Administration**, **Search and offline availability**, and finally, in the **Offline Client Availability** section, selecting **Yes**. This allows SharePoint content to be taken offline for offsite work.
  - Configure access control settings for designated SharePoint sites to enable access by SharePoint Workspace users and groups. Note that users must have at least Read permission in order to synchronize SharePoint content with a SharePoint workspace. For more information about how to configure access to SharePoint sites, see Managing Site Groups and Permissions (*http://go.microsoft.com/fwlink/?LinkID=162300*).
  - If your organization uses Line of Business Interoperability (LOBi) lists (for connections to external databases instead of to the server database) and if users have to take these lists offline, ensure that **Offline Synchronization of External Lists** is enabled on the SharePoint server. You can configure this setting from the Central Admin interface by clicking **System Settings** and looking under **Manage farm features**. This setting can also be configured at the site level under **Site Actions** > **Site Settings** > **Site Actions** > **Manage site features**.

Review customization options for SharePoint Workspace 2010

Customizing the SharePoint Workspace installation enables you to decide how SharePoint Workspace will be deployed and used. The following sections describe settings that you can configure to customize SharePoint Workspace 2010 installation.

Control use of Groove workspaces

This setting lets you prevent Groove workspaces and Shared Folders from being used in SharePoint Workspace, therefore limiting SharePoint Workspace usage to SharePoint workspaces exclusively. You can configure this setting by using the Office Customization Tool (OCT) or by deploying a Group Policy object (GPO), as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

Enable IPv6

This setting lets you enable IPv6 for SharePoint Workspace installation. You can configure this setting by using the OCT or by deploying a GPO, as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

Prefer IPv4

This setting lets you specify that IPv4 is preferred over IPv6 for SharePoint Workspace 2010 on client computers. You can configure this setting by using the OCT or by deploying a GPO, as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

Remove legacy files and registry settings

This setting removes previous installations of SharePoint Workspace (Microsoft Office Groove 2007). You can also use this option if you have special requirements that can only be configured through the Windows Registry (such as removing a Office Groove 2007 device management registry setting). You can configure this setting by using the OCT, as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

Prevent Windows Search crawling for SharePoint Workspace

This setting prevents crawling of SharePoint Workspace paths by Windows Search. By default, crawling (creation of indexes) for Windows Search 4.0 is enabled for the following SharePoint Workspace content:

- Metadata for SharePoint workspaces and Groove workspaces for SharePoint Workspace 2010
- Metadata for all Groove workspace tools for SharePoint Workspace 2010

- The following Groove workspace content for SharePoint Workspace 2010: discussions, documents, Notepad entries, chat transcripts, member messages, and custom lists.

Users can start Windows Search 4.0 from SharePoint Workspace by clicking **Search** on the **Home** tab of the ribbon, unless prevented from doing this by administrative policy. Setting this policy prevents Windows Search from crawling and searching SharePoint Workspace content, overrides any user search settings, removes **Search** from the ribbon in SharePoint Workspace, and cleans the Windows Search index of any previously crawled SharePoint Workspace data.

To configure this setting, use a Search GPO, as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

For more information about Windows Search, see Windows Search Administrator Guide (*http://go.microsoft.com/fwlink/?LinkID=164567*) and Windows Search IT Guides (*http://go.microsoft.com/fwlink/?LinkId=163450*).

Require Secure Socket Layer protection for external client connections

This setting blocks SharePoint Server connections from SharePoint Workspace clients that are outside an organization's intranet, unless the connections are over a Secure Socket Layer (SSL)-protected port. To configure this setting, use a SharePoint Server GPO, as described in Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool .

Customize SharePoint Workspace in a managed environment

If you use Microsoft Groove Server 2010 to manage SharePoint Workspace, you can further customize installation to make administrative tasks easier. For example, you can use Group Policy to configure policy settings, such as a Microsoft Groove Server 2010 assignment, that apply to an organizational unit in Active Directory. Or, you can configure an Office Resource Kit setting to require SharePoint Workspace users to automatically configure SharePoint Workspace user accounts for management in an environment that does not include Active Directory. For more information about how to deploy SharePoint Workspace in a Groove Server-managed environment, see Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*).

Customize SharePoint Workspace 2010 by using Active Directory Group Policy objects or the Office Customization Tool

You can customize SharePoint Workspace installations by deploying Active Directory Group Policy objects (GPOs) or by including an Office Customization Tool (OCT) .msp file together with the SharePoint Workspace installation kit. The method that you choose depends on the following deployment conditions:

- If intended SharePoint Workspace clients are members of an in-house Active Directory group and are connected to the Windows domain, you can configure Active Directory GPOs to customize client installations, as described in To customize SharePoint Workspace installation through Active Directory Group Policy objects.
- If your organization does not use an Active Directory server or if intended SharePoint Workspace clients are outside your Windows domain, use OCT settings to customize installation as described in To customize SharePoint Workspace installation through Office Customization Tool settings.

Note:
Decide on one customization approach to help ensure a smooth deployment. Do not use both GPOs and OCT settings. For more information about these customization options, see Group Policy overview (Office system) (*http://go.microsoft.com/fwlink/?LinkID=162307*) and Office Customization Tool in the Office system (*http://go.microsoft.com/fwlink/?LinkID=162306*).

If you use Groove Server 2010 Manager to manage SharePoint Workspace clients, you can use a combination of Groove Server 2010 Manager policies and GPOs or OCT settings to customize SharePoint Workspace installations. For information about Groove Server 2010 Manager policies, see Deploying policies to SharePoint Workspace users (*http://technet.microsoft.com/library/5edf15f7-0233-4cf3-a855-3a41d1a59e57(Office.14).aspx*). For information about how to customize SharePoint Workspace in a Groove Server 2010-managed environment, see Deploy SharePoint Workspace 2010 (*http://technet.microsoft.com/library/24ec9cec-361b-4862-b5c3-d7ad5650c425(Office.14).aspx*).

To customize SharePoint Workspace installation through Active Directory Group Policy objects

1. Address the requirements in Before you begin.
2. Determine which Group Policy object (GPO) that you need to customize SharePoint Workspace for the management environment, based on the information in Review customization options for SharePoint Workspace 2010.
3. From the Active Directory server, access the required policies by downloading the AdminTemplates.exe file for Office 2010, available at the Microsoft Download Center (*http://go.microsoft.com/fwlink/?LinkID=162268*).
4. Double-click the AdminTemplates.exe file to extract the Administrative template files that enable you to configure Group Policy settings that apply to an Active Directory unit. The spw14.admx file (or .adml file for language-specific versions) contains SharePoint Workspace-specific policies.
5. If you are using a Windows Server 2008 computer, copy the ADMX\ADML files to folders as follows:
    a. Copy the ADMX files (.admx) to your computer's Policy Definitions folder (for example, <systemroot>\PolicyDefinitions).
    b. Copy the ADML language-specific resource files (.adml) to the appropriate language folder, such as en-us; for example, <systemroot>\PolicyDefinitions\[MUIculture].

For more information about Group Policy object editing requirements and steps, see Requirements for Editing Group Policy Objects Using ADMX Files (*http://go.microsoft.com/fwlink/?LinkId=164568*) and Managing Group Policy ADMX Files Step-by-Step Guide (*http://go.microsoft.com/fwlink/?LinkId=164569*).

6. From the Active Directory server, use the Group Policy Management Console (GPMC), which you can access from gpedit.msc in the Microsoft Management Console, to change the policy settings that are contained in the .adm files.
7. In the tree view, locate **Group Policy Objects**, click the policy that you want to configure, and then in the details pane fill in the required fields to enable or change the policy. See Group Policy for SharePoint Workspace 2010 for more guidance.
8. When you are finished editing the GPO in the GPMC, save the policy settings. The policy settings are saved in the registry.pol file, which the Group Policy program uses to store registry-based policy settings made by using the Administrative template extension.

For more information about Group Policy technology and use, see Group Policy overview (Office system) (*http://go.microsoft.com/fwlink/?LinkId=162307*) and Enforce settings by using Group Policy in the Office system (*http://go.microsoft.com/fwlink/?LinkID=78176&clcid*).

To customize SharePoint Workspace installation through Office Customization Tool settings

1. Address the requirements in Before you begin.
2. Determine how you want to customize SharePoint Workspace, based on the information in Review customization options for SharePoint Workspace 2010.
3. You can run the Office Customization Tool (OCT) from the **Start** menu. Click **Run**, and then type **cmd**. At the command prompt, go to the Office 2010 installation directory, and then type **setup/admin**. This opens the OCT.

   Or, you can download the OCT from the Office 2010 installation media.
4. In the OCT tree view, locate **Features**, and then click **Modify user settings**. In the navigation pane, click SharePoint Workspace, SharePoint Server, or Search Server, depending on the kind of setting that you want to configure.
5. In the list pane, double-click the setting that you need, and change its properties as needed. See Office Customization Tool settings for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/43008de2-5eef-4de1-b0e1-19b7ceeb68f6(Office.14).aspx*) for more guidance.
6. When you are finished, click the **File** drop-down menu and then click **Save** to save your updated settings in a Microsoft setup customization file (.msp). For example, enter **spw.msp** as a file name.
7. Include the .msp file in the SharePoint Workspace deployment.

For more information about how to use the OCT, see Office Customization Tool in the Office system (*http://go.microsoft.com/fwlink/?LinkId=162306*).

Verify installation

Test SharePoint Workspace connections and synchronization as described in Test SharePoint Workspace connections.

See Also

SharePoint Workspace 2010 overview (*http://technet.microsoft.com/library/650cb781-4dbd-45ac-b8d3-2ce9b3a16600(Office.14).aspx*)

Plan for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/e8a433c1-ea1f-4cf7-adc8-50972f58d465(Office.14).aspx*)

Deployment for Groove Server 2010 (*http://technet.microsoft.com/library/8d7d33c2-3954-489b-ac82-49f7da119489(Office.14).aspx*)

Group Policy for SharePoint Workspace 2010

Office Customization Tool settings for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/43008de2-5eef-4de1-b0e1-19b7ceeb68f6(Office.14).aspx*)

Deployment checklist for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/3a1dc784-a7c1-467d-b21b-f1e3cd18ed20(Office.14).aspx*)

Test SharePoint Workspace connections

This article provides information and procedures for testing SharePoint Workspace 2010 connections to and synchronization with SharePoint Server 2010 and client peers.

In this article:

Before you begin

Before you start testing, address the following prerequisites:

- Choose a SharePoint Workspace 2010 deployment topology and plan accordingly, as described in Plan for SharePoint Workspace 2010 (*http://technet.microsoft.com/library/e8a433c1-ea1f-4cf7-adc8-50972f58d465(Office.14).aspx*).
- For a SharePoint Server 2010-based topology, prepare SharePoint Server 2010, as described in Configure and customize SharePoint Workspace 2010.
- Customize SharePoint Server 2010 deployment, as described in Configure and customize SharePoint Workspace 2010.
- Follow the organization's standard client software deployment processes to install Office 2010 or SharePoint Workspace 2010 on target user desktops.
- Identify two SharePoint Server 2010 sites to synchronize with a test SharePoint Workspace 2010 client. Make sure that you are a member of these sites to that you can create and edit site content.
- Identify test SharePoint Workspace 2010 clients inside and outside the local firewalls.

Test SharePoint Workspace synchronization with SharePoint Server

The following procedure provides guidance for validating connections and content synchronization between SharePoint Workspace 2010 and SharePoint Server 2010, in support of SharePoint workspaces.

To test SharePoint Workspace connections and synchronization

1. Create a SharePoint workspace from a SharePoint site as follows:
   a. Start SharePoint Workspace 2010 on a test client.
   b. Browse to a SharePoint Server 2010 Central Administration Web site from a test

SharePoint Workspace 2010 client.

c. From the SharePoint Server site, click the **Site Actions** drop-down menu and then click **Sync to SharePoint Workspace**.

d. To download all the Document libraries and List content on the site to the local test client, click **OK** from the **Sync to Computer** dialog box that appears. To download selected content, click **Configure** in the dialog box, select the document libraries and lists that you want to download, and then click **OK**. Within a few moments, a new SharePoint workspace will be downloaded to your computer. The new workspace contains a copy of the requested SharePoint lists and libraries which you can edit while your online or offline.

e. Experiment with editing a document or list from the SharePoint workspace while you are online, and then save your changes. These edits and updates will be synchronized automatically with the document and list content on the SharePoint site.

f. Disconnect from the Internet and experiment with update the content from an offline state, and then save your changes. When you return online, these edits and updates will be synchronized automatically with the document and list content on the SharePoint site.

2. Verify that the client updates are visible on the SharePoint site as follows:

   a. Reconnect to the Internet and browse to the SharePoint site. Or, for quick browsing from the SharePoint workspace that contains the SharePoint site content, open the SharePoint workspace and then click the site link next to the **Contents** pane in the SharePoint workspace.

   b. Select **View all content** from the **Site Actions** drop-down menu and navigate to the document or list that you changed from the SharePoint workspace.

   c. Wait several moments or refresh the screen to see the updates that you made from the client.

3. To verify that SharePoint site updates are visible in the SharePoint workspace, follow these steps:

   a. Browse to the SharePoint site and update a document or list that you have synchronized with content in the test SharePoint workspace.

   b. Open the SharePoint workspace that you created on the test client.

   c. Wait a few moments for the site content to appear in the workspace. Or, click the **Sync** tab in the ribbon, click the **Sync** drop-down menu, and then select either, **Sync Tool** to synchronize with the current document library or list, or **Sync Workspace** to synchronize with all the documents and libraries on the site.

4. You can test a similar procedure, initiated from a SharePoint Workspace test client, as follows:

   a. Start SharePoint Workspace 2010 on a test client.

   b. From the SharePoint Workspace Launchbar, on the **Home** tab, click the **New** drop-down menu, and then select **SharePoint Workspace**.

   c. Enter the URL to a SharePoint site in the **Location** text box.

d. Click **Configure** to access the site and select the content that you want to download, and then click **OK**. Within a few moments, a new SharePoint workspace will be downloaded to your computer. The new workspace contains a copy of the requested SharePoint lists and libraries which you can edit while your online or offline.

e. Experiment with editing document or lists as described previously in this procedure.

For more information about how to create SharePoint workspaces and how to use SharePoint Workspace 2010, see the SharePoint Workspace 2010 product information at Microsoft Office Online (*http://go.microsoft.com/fwlink/?LinkID=162269*).

5. If a test step fails, see Troubleshoot SharePoint Workspace 2010 (*http://technet.microsoft.com/library/ff6ae209-ceab-4dcb-b5f5-a9c582f92a40(Office.14).aspx*), resolve the problem, and run the test again.

Test Groove workspace synchronization among peer clients

SharePoint Workspace supports peer connections for Groove workspace and Shared Folder workspace types. The following procedures explain how to validate Groove workspace and Shared Folder workspace connections and peer synchronization.

To test Groove workspace synchronization

1. From SharePoint Workspace client 1, start SharePoint Workspace 2010, then create a Groove workspace in SharePoint Workspace by clicking the **New** drop-down menu on the **Home** tab on the Launch bar and then clicking **Groove workspace**. Accept the default tools and configuration. Then invite SharePoint Workspace client 2 to the workspace.

   For more information about how to use SharePoint Workspace 2010 and how to create Groove workspaces, see the product information at Microsoft Office Online (*http://go.microsoft.com/fwlink/?LinkID=162269*).

2. From SharePoint Workspace client 2, accept the invitation. When the accepted invitation download is complete, open the new Groove workspace, click the **New Documents** option on the **Home** tab, and then add a document that contains some test content.
3. From client 1, click the **Documents** item in the **Contents** pane, check for the new content that you added in the previous step, and then edit the document. Client 2 appears in the workspace Members list.
4. From client 2, look for the client 1 update in the test document.
5. Repeat these steps to test connections and synchronization between clients inside and outside the corporate LAN and for clients who have made offline contributions.
6. If a test step fails, see Troubleshoot SharePoint Workspace 2010 (*http://technet.microsoft.com/library/ff6ae209-ceab-4dcb-b5f5-a9c582f92a40(Office.14).aspx*), resolve this problem, and run the test again.

To test Shared Folder synchronization

1. From SharePoint Workspace client 1, start SharePoint Workspace 2010, and then create a test folder in the Windows file system. Then create a shared folder in SharePoint Workspace by clicking the **New** drop-down menu on the **Home** tab on the Launch bar, clicking **Shared Folder**, and specifying the test folder. Now invite SharePoint Workspace client 2 to the workspace.

   For more information about how to create shared folders and how to use SharePoint Workspace 2010, see the SharePoint Workspace 2010 product information at Microsoft Office Online (*http://go.microsoft.com/fwlink/?LinkID=162269*).
2. From SharePoint Workspace client 2, accept the invitation. When the folder download is complete, you will see the new folder in the Windows file system on client 2 and client 2 will appear in the workspace Members list. Now add a document that contains some test content to the folder.
3. From client 1, check for new content in the folder and client 2 in the workspace Members list. Then edit the document.
4. From client 2, look for the client 1 update in the test document.
5. Repeat these steps to test connections and synchronization between clients inside and outside the corporate LAN and for clients who have made offline contributions.
6. If a test step fails, see Troubleshoot SharePoint Workspace 2010 (*http://technet.microsoft.com/library/ff6ae209-ceab-4dcb-b5f5-a9c582f92a40(Office.14).aspx*), resolve this problem, and run the test again.

SharePoint Workspace peer connections are often supported in a managed environment where Microsoft Groove Server is deployed onsite. For more information about how to deploy these workspace types in a managed environment, see Deploy SharePoint Workspace 2010 (*http://technet.microsoft.com/library/24ec9cec-361b-4862-b5c3-d7ad5650c425(Office.14).aspx*).

See Also

Deploy SharePoint Workspace 2010 (*http://technet.microsoft.com/library/24ec9cec-361b-4862-b5c3-d7ad5650c425(Office.14).aspx*)