We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. Privacy Statement Third-Party Cookies

Accept Reject Manage cookies

Information for administrators about e-mail security settings in Outlook 2007

Article • 01/30/2024 • 4 contributors •

Applies to: Microsoft Office Outlook 2007

Feedback

In this article

Show 4 more

Original KB number: 926512

Introduction

This article contains information for administrators about e-mail security features in Microsoft Office Outlook 2007. This article lists the security settings that you can set when Outlook 2007 is running in a Microsoft Exchange Server environment.

The AdminSecurityMode registry entry and security policy

Outlook 2007 can use either public folder security forms or Group Policy to manage security for attachments and for add-ins. The ability to use Group Policy object (GPO) settings to store security settings is a new feature in Outlook 2007.

If your environment uses public folders, and if you use public folder security forms in earlier versions of Outlook, you can continue to use public folder security forms. You can do this after you make a minor change to the appropriate registry settings.

Outlook 2007 is designed to take advantage of the GPO settings to manage security for attachments and for add-ins. Unlike Office Outlook 2003, Outlook 2007 does not use the `CheckAdminSettings` registry data to determine policy settings or to determine trust levels for add-ins. Instead, Outlook 2007 uses the new `AdminSecurityMode` registry entry to determine the security policy.

The `AdminSecurityMode` registry entry uses the following configuration:

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `AdminSecurityMode`
Values:

- 0: Use the default Outlook security settings

  > **Note**
  >
  > This is the default setting if the `AdminSecurityMode` registry entry is not present.

- 1: Use the security policy from the Outlook Security Settings public folder
- 2: Use the security policy from the Outlook 10 Security Settings public folder
- 3: Use the security policy from the GPO settings

Use the `AdminSecurityMode` registry entry to control the security settings that Outlook 2007 applies. You can configure Outlook 2007 to use the current security settings that are published through the existing Outlook public folder security forms. Alternatively, you can configure Outlook 2007 to use GPO-based security settings.

The AddinTrust registry entry and add-in trust policy

The `AddinTrust` registry entry in Outlook 2007 works exactly as it does in Outlook 2003. Be aware that when you set the value of the `AddinTrust` registry entry to **0** (zero), you configure Outlook 2007 to use the security policy that is determined by the value of the

`AdminSecurityMode` registry entry. The `AddinTrust` registry entry uses the following configuration:

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `AddinTrust`
Values:

- 0: Trust is determined by the value of the AdminSecurityMode registry entry

  > **Note**
  >
  > This is the default setting if the `AddinTrust` registry entry is not present.

- 1: Trust all add-ins
- 2: Trust no add-ins

Outlook 2007 in an Exchange Server environment that uses public folders

If you already use public folder security forms to manage security, the simplest migration route to Outlook 2007 is to continue to use public folder security forms. You can do this regardless of the version of Exchange Server that you are running in your environment.

To make sure that Outlook 2007 uses the security settings that are configured in the public folder security forms, set the `AdminSecurityMode` registry entry to a value of either **1** or **2**. The value that you set depends on whether the published forms are located in the Outlook Security Settings public folder or in the Outlook 10 Security Settings public folder.

The following list describes the `AdminSecurityMode` registry entry values. The list also describes how each value affects Outlook 2007 in an Exchange Server environment that uses public folders, as follows:

- No registry entry present: Outlook 2007 uses the default administrative settings
- 0: Outlook 2007 uses the default administrative settings
- 1: Outlook 2007 uses the custom administrative settings in the Outlook Security Settings public folder
- 2: Outlook 2007 uses the custom administrative settings in the Outlook 10 Security Settings public folder
- 3: Outlook 2007 uses the GPO settings

Outlook 2007 in an Exchange Server environment that does not use public folders

To configure Outlook 2007 to use GPO-based security settings, set the `AdminSecurityMode` registry entry to a value of **3**. Additionally, if it is required, confirm that the `AddinTrust` registry entry is set to a value of **0** (zero).

Attachment security settings

The security settings for attachments in Outlook 2007 are as follows.

Show Level 1 attachments

Typically, Level 1 attachments are blocked. If you enable this policy, users can see Level 1 attachments in Outlook 2007.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`

DWORD value: `ShowLevel1Attach`
Values:

- 1: Enabled
- 0: Disabled

Let users demote attachments to Level 2

If you enable this policy, users can demote the security level of attachments from Level 1 security to Level 2 security. By doing this, users can access Level 1 attachments in Outlook 2007. If you disable this policy, users cannot demote the security level of attachments.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `AllowUsersToLowerAttachments`
Values:

- 1: Enabled
- 0: Disabled

Disable the prompt about Level 1 attachments when users send an item

By default, Outlook 2007 prompts users when an item that has a Level 1 attachment is sent. If you enable this policy, you disable the prompt.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `DontPromptLevel1AttachSend`
Values:

- 1: Enabled
- 0: Disabled

Disable the prompt about Level 1 attachments when users close an item

By default, Outlook 2007 prompts users when an item that has a Level attachment is closed. If you enable this policy, you disable the prompt.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `DontPromptLevel1AttachClose`
Values:

- 1: Enabled
- 0: Disabled

Enable in-place activation of embedded OLE objects

Outlook 2007 can enable in-place activation of embedded OLE objects. This condition may potentially enable users to run malicious code that is disguised as another document. If you enable this policy, Outlook 2007 enables users to make OLE objects in place become active. If you disable this policy, Outlook 2007 cannot enable users to make embedded OLE objects in place become active.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `AllowInPlaceOLEActivation`
Values:

- 1: Enabled
- 0: Disabled

Show OLE package objects

Outlook 2007 can display OLE package objects. OLE package objects can disguise malicious code as another document. If you enable this policy, Outlook 2007 shows OLE package objects. If you disable this policy, Outlook 2007 cannot show OLE package objects.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `ShowOLEPackageObj`
Values:

- 1: Enabled
- 0: Disabled

Add file name extensions that are blocked as Level 1 security items

This policy lists the file name extensions that are promoted to Level 1 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
String: FileExtensionsAddLevel1
Values: List of file name extensions that are separated by a semicolon

Remove file name extensions that are blocked as Level 1 security items

This policy lists the file name extensions that are demoted to Level 2 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`

String: `FileExtensionsRemoveLevel1`

Values: List of file name extensions that are separated by a semicolon

Add file name extensions that are blocked as Level 2 security items

This policy lists the file name extensions that are added to Level 2 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`

String: FileExtensionsAddLevel2

Values: List of file name extensions that are separated by a semicolon

Remove file name extensions that are blocked as Level 2 security items

This policy lists the file name extensions that are removed from Level 2 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`

String: `FileExtensionsRemoveLevel2`

Values: List of file name extensions that are separated by a semicolon

Custom form security settings

The security settings for custom forms in Outlook 2007 are as follows.

Enable scripts in one-off Outlook 2007 forms

When you enable this policy, scripts can run in a one-off Outlook 2007 form.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `EnableOneOffFormScripts`
Values:

- 1: Enabled
- 0: Disabled

Configure a prompt for Outlook object model custom actions

When you enable this policy, certain actions can occur when a custom action is performed by using the Outlook object model. You can configure Outlook 2007 to automatically allow the action, to automatically deny the action, or to prompt the user.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMCustomAction`
Values:

- 0: Automatically deny
- 1: Prompt user

  > **Note**
  >
  > This is the default setting.

- 2: Automatically approve

Configure a prompt for the ItemProperty property of a control

This policy controls how the access process works for the ItemProperty property of a control on a custom form. You can configure Outlook 2007 to automatically allow the action, to automatically deny the action, or to prompt the user.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMItemPropertyAccess`
Values:

- 0: Automatically deny
- 1: Prompt user

  > **Note**
  >
  > This is the default setting.

- 2: Automatically approve

Programmatic security settings

Programmatic security settings are listed as follows.

Configure a prompt when a program sends items by using the Outlook object model

This policy determines the behavior that occurs when a program sends items by using the Outlook object model.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMSend`
Values:

- 0: Automatically deny
- 1: Prompt user

> **Note**
>
> This is the default setting.

- 2: Automatically approve

Configure a prompt when a program accesses an address book by using the Outlook object model

This policy determines the behavior that occurs when a program accesses an address book by using the Outlook object model.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMAddressBookAccess`
Values:

- 0: Automatically deny
- 1: Prompt user

> **Note**

This is the default setting.

- 2: Automatically approve

Configure a prompt when a program reads address information by using the Outlook object model

This policy determines the behavior that occurs when a program reads address information by using the Outlook object model.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMAddressInformationAccess`
Values:

- 0: Automatically deny
- 1: Prompt user

> **Note**
>
> This is the default setting.

- 2: Automatically approve

Configure a prompt when a program responds to meeting requests and task requests by using the Outlook object model

This policy determines the behavior that occurs when a program responds to meeting requests and task requests by using the Outlook

object model.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMMeetingTaskRequestResponse`
Values:

- 0: Automatically deny
- 1: Prompt user

  > **Note**
  >
  > This is the default setting.

- 2: Automatically approve

Configure a prompt when a program uses the Outlook object model to access the Save As command to save an item

This policy determines the behavior that occurs when a program uses the Outlook object model to access the Save As command to save an item.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMSaveAs`
Values:

- 0: Automatically deny
- 1: Prompt user

> **Note**
>
> This is the default setting.

- 2: Automatically approve

Configure a prompt when users access the Formula property of a UserProperty object

This policy determines the behavior that occurs when users access the `Formula` property of a `UserProperty` object.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMFormulaAccess`
Values:

- 0: Automatically deny
- 1: Prompt user

> **Note**
>
> This is the default setting.

- 2: Automatically approve

Configure a prompt when a program accesses address information by using the UserProperties.Find method

This policy determines the behavior that occurs when a program accesses address information by using the `UserProperties.Find`

method.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `PromptOOMAddressUserPropertyFind`
Values:

- 0: Automatically deny
- 1: Prompt user

  > **Note**
  >
  > This is the default setting.

- 2: Automatically approve

About the settings for Simple MAPI operations

Originally, there were plans to include settings for the following Simple MAPI operations:

- A program sends items by using Simple MAPI
- A program resolves addresses by using Simple MAPI
- A program opens a message by using Simple MAPI

However, these settings were not added to the product in the release version of Outlook 2007. We are researching the ability to add this functionality to the GPO settings. These settings may be included in a future release.

Trusted add-ins

The security settings for trusted add-ins are as follows.

List of trusted add-ins

This policy lists the file names and the hash values that are always trusted by Outlook 2007.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security\TrustedAddins`
String: The file name of the add-in
Value: A hash of the file that is generated by the Secure Hash Algorithm (SHA-1). The hash is stored in the same format that is used in the security form.

> **Note**
>
> Each trusted add-in has a string value and a corresponding hash value in the `TrustedAddins` subkey.

Registry settings that were used in earlier versions of Outlook

Certain registry settings that were used in earlier versions of Outlook also apply to Outlook 2007. You can use these registry settings together with public folder security forms, or you can use them as independent settings. These registry settings are not considered part of the Outlook 2007 Group Policy object approach to attachment and add-in security.

The DisallowAttachmentCustomization registry entry

When you enable this policy, Outlook 2007 disables the `Level1Remove` registry entry. However, the `Level1Add` registry entry continues to work.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
DWORD value: `DisallowAttachmentCustomization`
Values: Any value

> ⓘ **Note**
>
> This policy controls whether you can customize the attachment security settings by using non-policy registry keys.

The Level1Remove registry entry

This policy lists the file name extensions that are demoted to Level 2 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security`
String: `Level1Remove`
Values: List of file name extensions that are separated by a semicolon

> ⓘ **Note**
>
> If the DisallowAttachmentCustomization registry entry is present, Outlook 2007 ignores the `Level1Remove` registry entry.

The Level1Add registry entry

This policy lists the file name extensions that are promoted to Level 1 security.

Key: `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Out`

`look\Security`

DWORD value: `Level1Add`

Values: List of file name extensions that are separated by a semicolon

> **Note**
>
> The file name extensions on this list are blocked by Outlook 2007.

For more information about Outlook 2007 security settings, see Customize programmatic settings in Outlook 2007.

Feedback

Was this page helpful? Yes No

English (United States) Your Privacy Choices Theme

Manage cookies Previous Versions Blog Contribute Privacy Terms of Use Trademarks

© Microsoft 2024