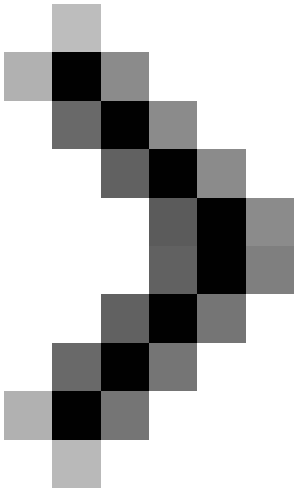
Manage Outlook 2007 through Group Policies - Part 2

In this article, I will show you how to manage some Outlook 2007 features using Group Policy.



Manage Outlook 2007 through Group Policies - Part 1
Anderson Patricio

In this article, I will show you how to manage some Outlook 2007 features using Group Policy.

Introduce

In the previous article of this series, we introduced the process related to downloading and adding templates in both Windows Server 2003 and Windows Server 2008 operating systems to add extensions to the files of Outlook 2007 enters Group Policy. In this second part, we will explore some of the essential features for most administrators, such as PST management, attachment management, and so on.

The PST file

PST can be a nightmare for some Exchange administrators, they can be quite difficult to manage and create a protection strategy in medium and large organizations. PSTs can be completely managed through Group Policy and throughout this section, we will show you how to remove PST from a network or at least change some of the default settings.

There are several storage products that use PST files, such as storage solutions that can search and transfer PST files to an archive. In this scenario, using PST is prohibited for the network.

Note: All PST settings can be found in the following path, in Group Policy: User Configuration / Administrative Templates / Microsoft Office Outlook 2007 / Miscellaneous / PST Settings.

By default, PSTs can be added to Outlook profiles. To prevent the addition of PSTs, we can enable the setting of *Prevent users from adding PSTs to Outlook profiles and users using Sharing-Exclusive PSTs*, then click **Enabled** and select **No PSTs can be added** (See Figure 1).

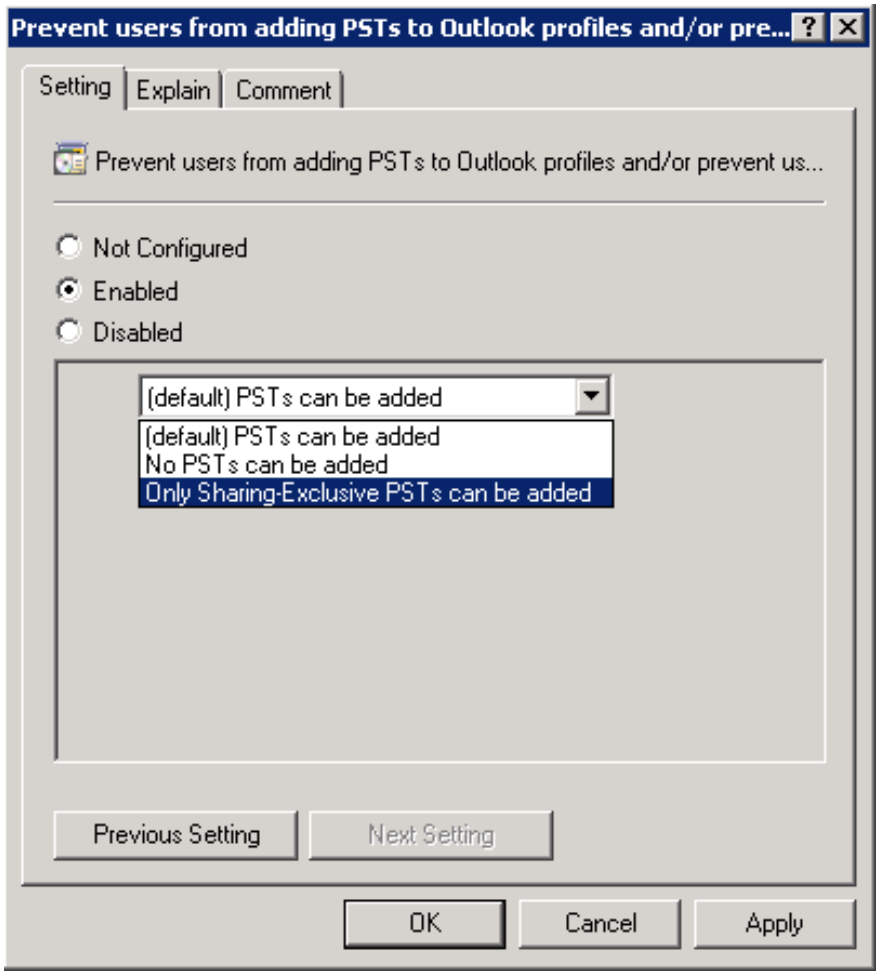


Figure 1

The result will be, the user cannot select any option if that option joins to add a PST, as shown in Figure 2.

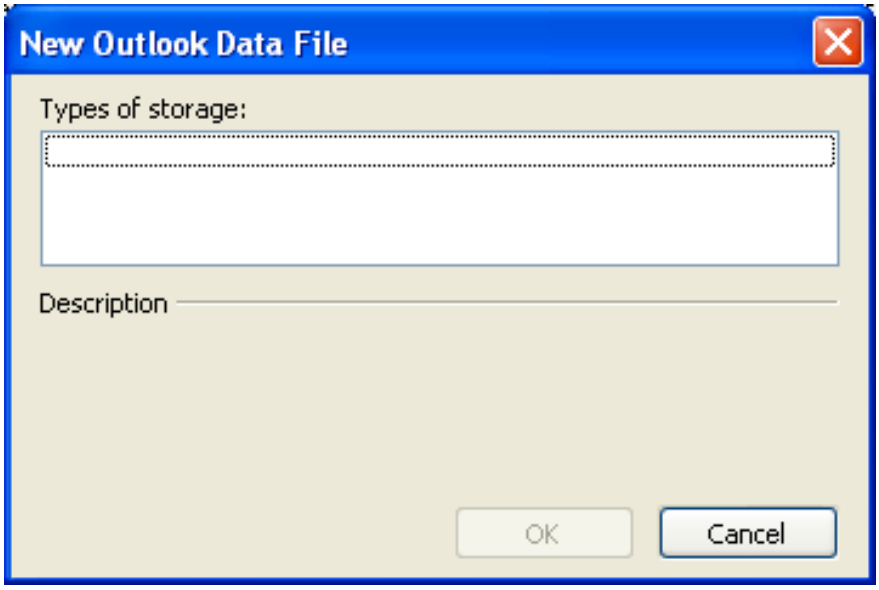


Figure 2

Now that we have blocked the user from adding additional PST files, we can also configure the current PST in a read-only state where users cannot create or delete content within them. . The setting to control the behavior is *Prevent users from adding new content to existent PST files* , as shown in Figure 3.

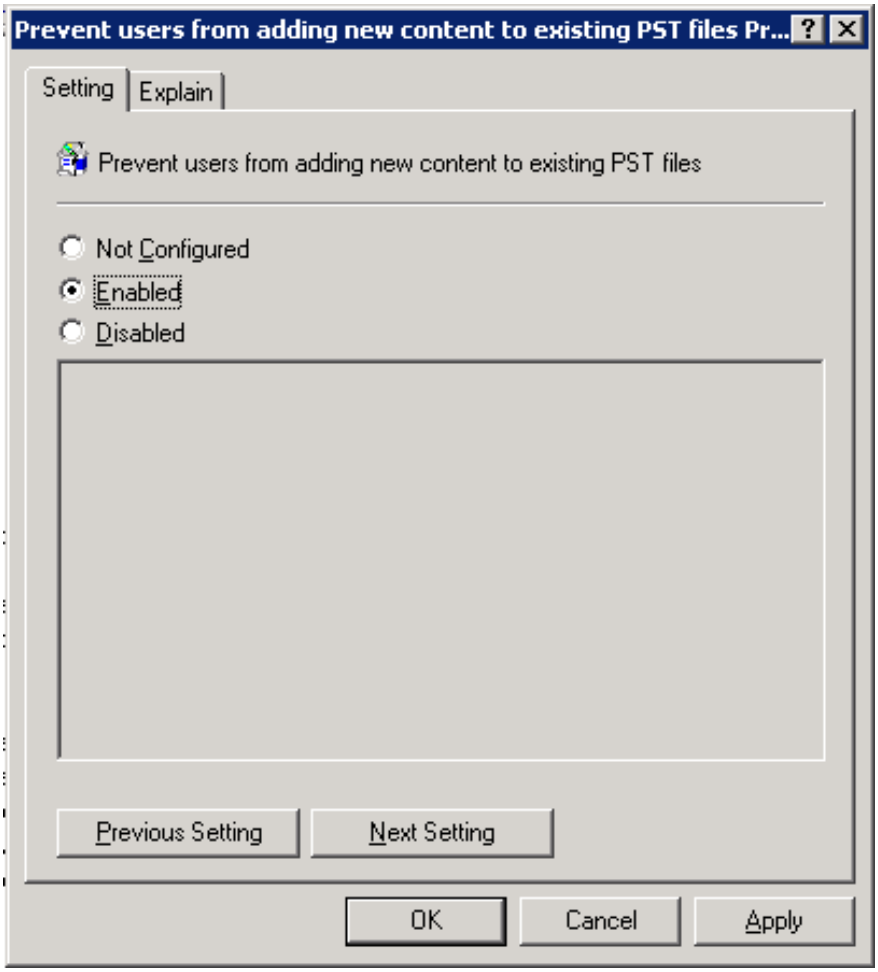


Figure 3

Using the previous settings, the result will appear an error message when the user tries to add new content to an existing PST (see Figure 4).

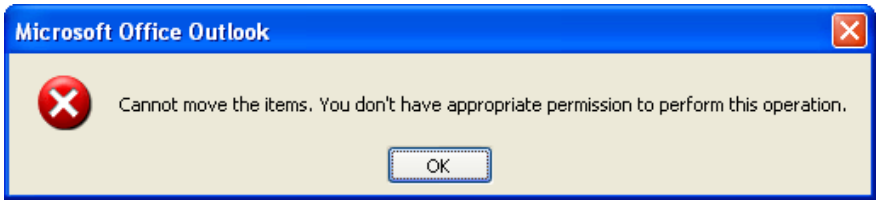


Figure 4

Let's assume that there is an internal policy, with this policy, PST is allowed locally and wants to keep all of them in a standard path to facilitate the protection process when changing the location. Default for PST and also OST files. To configure this setting, double-click *Default location for PST and OST files* and type in the new path (you can use environment variables), as shown in Figure 5.

Note: The new path will be used by all PST or OST created after the policy is applied.

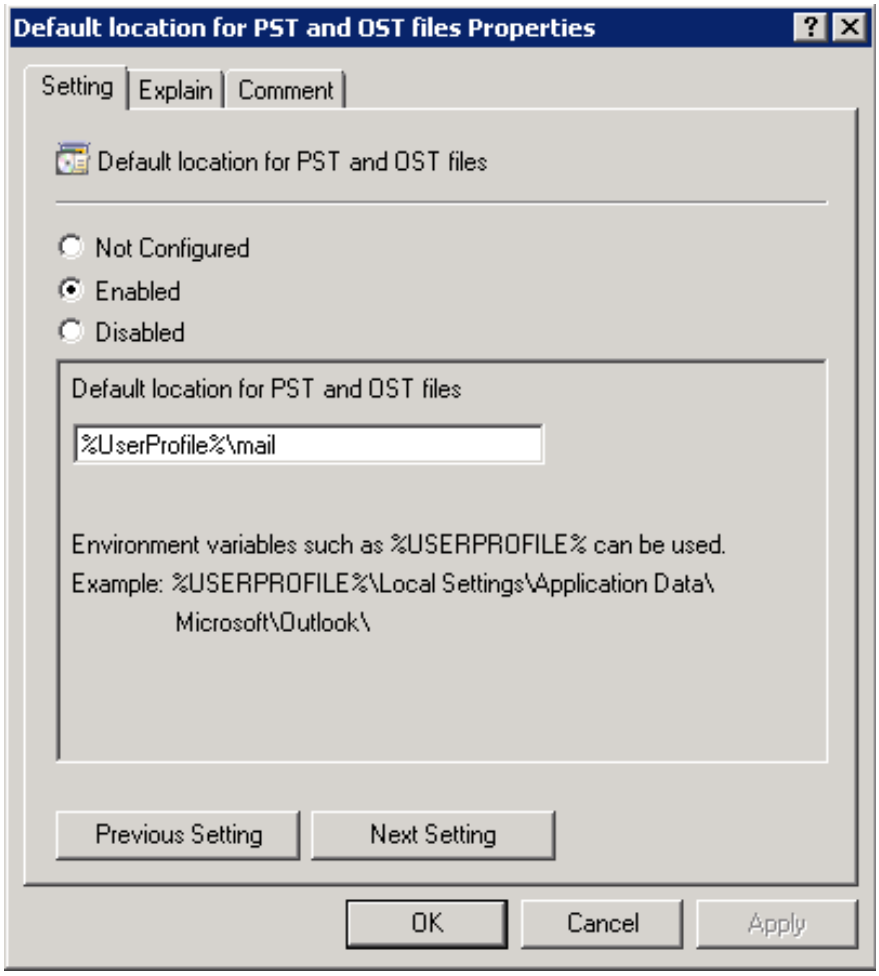


Figure 5

Besides the configuration we have seen, we can also change the settings related to PST, such as the largest PST size, file format and, .

Manage attachments

Outlook 2007 manages attachments with security levels. Outlook uses three different groups: Level 1 (unsafe attachments), Level 2 (they must be saved on disk before opening) and other attachments where users can open directly from Outlook.

We can use Group Policy to add and remove extensions from level 1 and level 2 groups. There are many default extensions available in Level 1 of Outlook 2007: .ade, .adp,. app, .asp, .bas, .bat, .cer, .chm, .cmd, .com, .cpl, .crt, .csh, .der, .exe, .fxp, .gadget, .hlp, .hta , .inf, .ins, .isp, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat,. mau, .mav, .maw, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .msc, .msh, .msh1, .msh2, .mshxml, .msh1xml, .msh2xml, .msi, .msp, .mst, .ops, .pcd, .pif, .plg, .prf, .prg, .pst, .reg, .scf, .scr, .sct, .shb, .shs, .ps1, .ps1xml , .ps2, .ps2xml, .psc1, .psc2, .tmp, .url, .vb, .vbe, .vbs, .vsmacros, .vsw, .ws, .wsc, .wsf, .wsh, .xnk.

If you have never seen a similar image of attachments, we can see in Figure 6 below, where the .xxx extension is attached to Level 1. If you look at the image, You will find that there is no way for users to manipulate that file

and Outlook displays **Outlook block access to the following unsafe attachments:.**

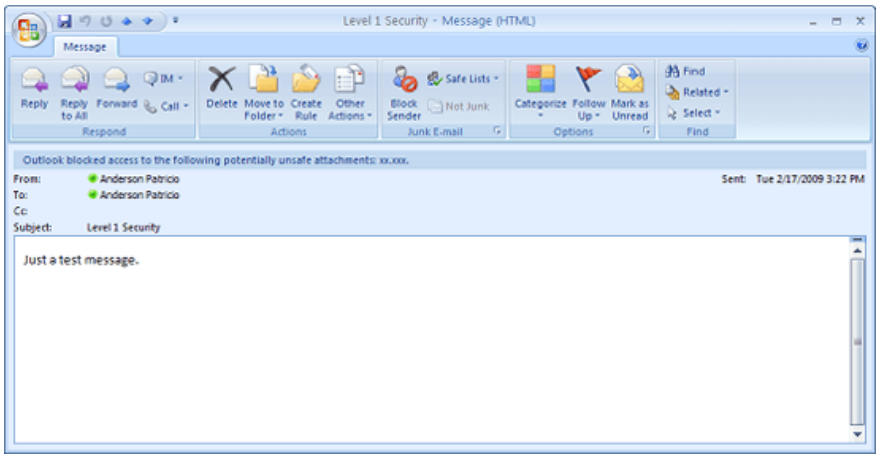


Figure 6

However, if we have a similar .xxx extension configured with Level 2, then the user can see the file on the message (Figure 7), but the message in Figure 8 will be displayed, This display will require users to save the file on disk and not allow it to run directly from Outlook 2007.

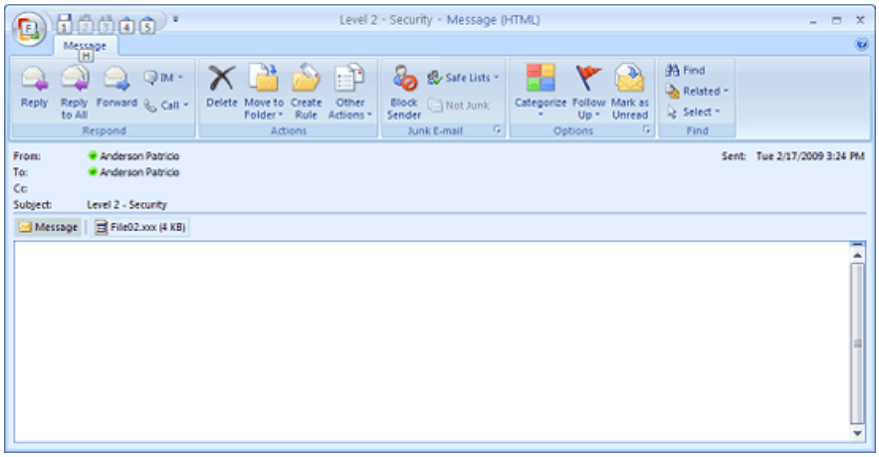


Figure 7

Figure 8

To manage file extensions for Level 1 and Level 2 groups, we need to change the **Outlook Security Mode setting.** Open **Security** , click **Security Forms Settings.** Then select **Enabled** and select **Use Outlook Security Group Policy** , click **OK** , see Figure 9.

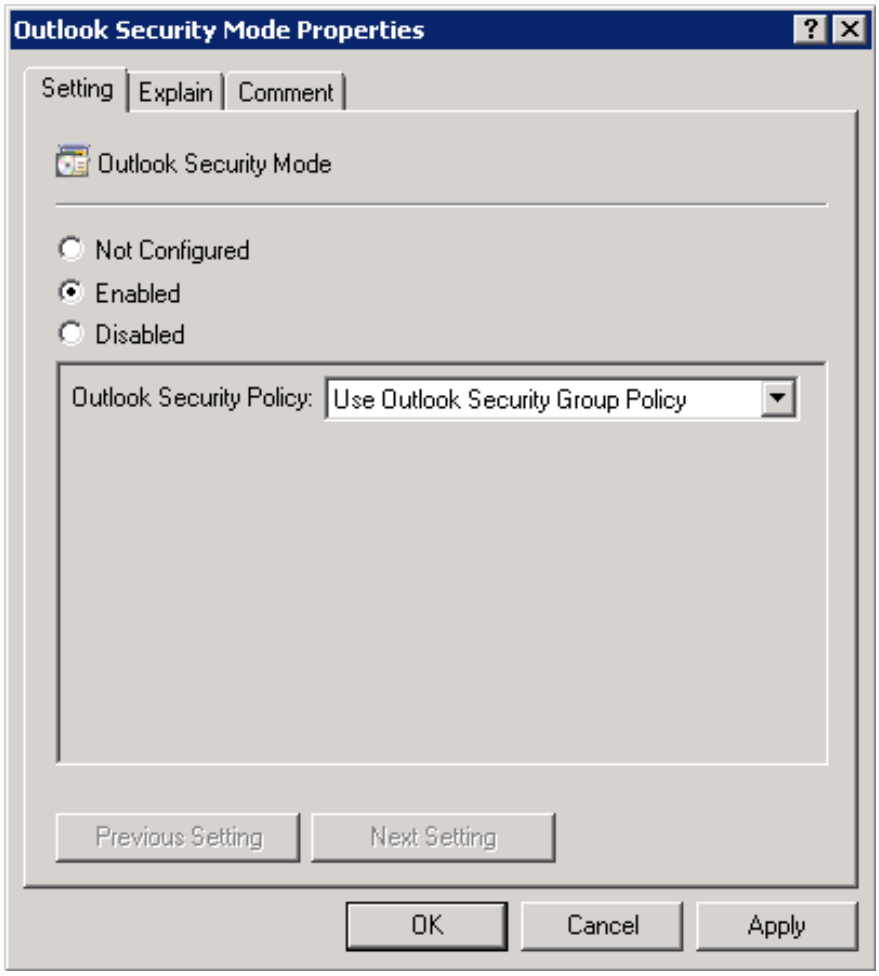


Figure 9

At this point, we have defined Outlook Security Mode in the previous step and can open **Attachment Security** , on this location we can Add, Remove as well as Disable Level 1 and Level 2. In Figure 10 below, we are Adding an extension of XXX and level 1, or immediately the client will receive the definitions of Group Policy and Outlook restarted, XXX will be considered level 1, the level does not allow users to perform a Number to manipulate files.

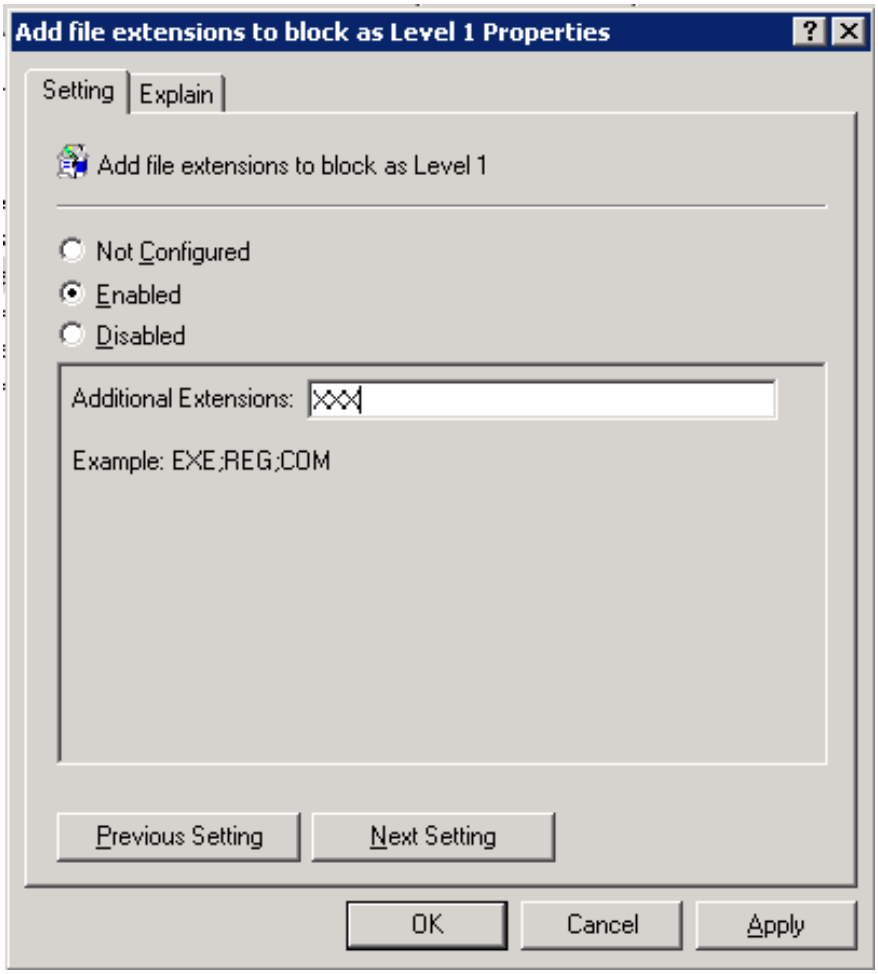


Figure 10

We can also add / remove Level 1 and Level 2 extensions, allowing Level 1 to display in Outlook, .

Lock account types

Outlook 2007 supports a variety of account types, which can be configured through the Outlook profile creation process. Using Group Policies we can control the protocols that will be available to users during the profile creation process. We can prevent these protocols from being configured: HTTP, Exchange, POP3, IMAP4 and any other type.

To block certain protocols, the option to *Prevent users from adding e-mail account types* must be configured for it. Click **Enable** and check all the services you want to block for end users (Figure 11).

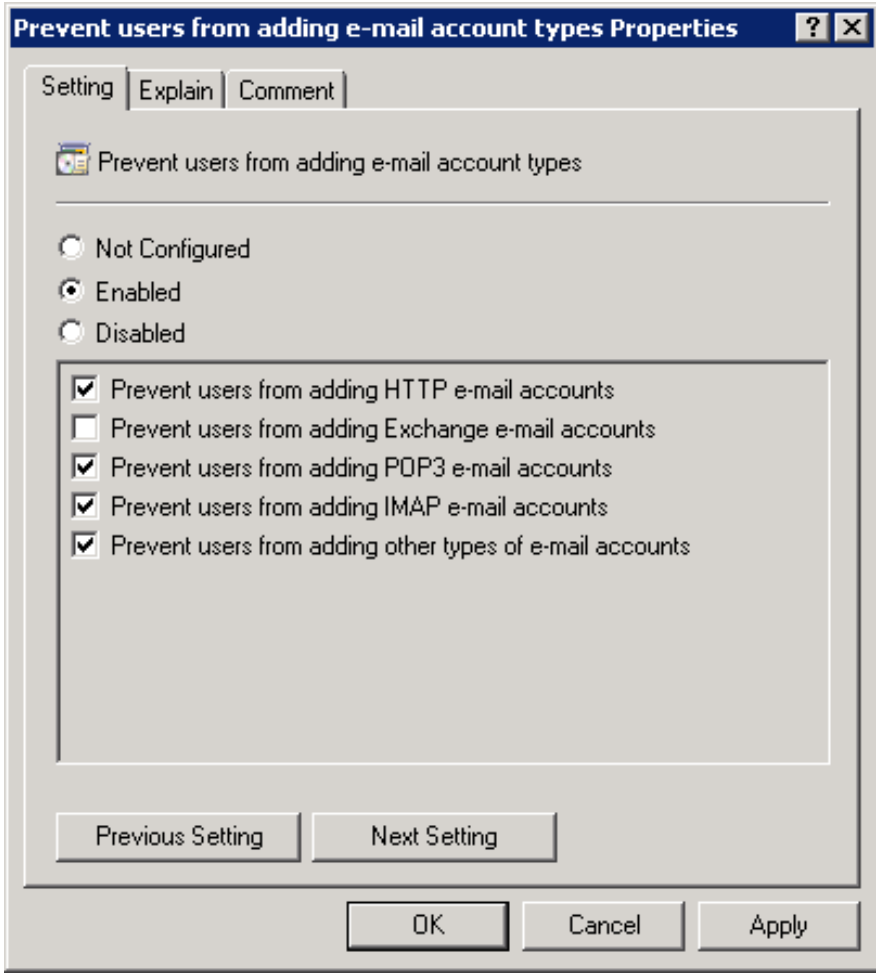


Figure 11

As a result of previous configurations, the configured service in Group Policy will not display during profile creation.

Conclude

In this article, I have discussed the process of configuring some Outlook 2007 settings using Group Policy. You can use this series as a basis for creating your policies for your company's needs.

You finished reading the article "**Manage Outlook 2007 through Group Policies - Part 2**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.