Bringing it all together.

A unified Active Directory deployment example.

Overview

Active Directory Group Policies provide a mechanism for System Administrators to customise the deployment of Tracker Software products. Some of these customisations are available during install using command line switches or a transform file and others are applied post install through an Administrative Template that Tracker makes available.

Registry changes – Local Machine or Current User?

The difference between whether an option is available during install or after install depends on whether access to the Current User (HKCU) section of the Windows Registry is needed. Installations performed through Active Directory do not require the user to be logged on and actively run the installation; it is pushed through a Group Policy and happens when the client machine performs a Group Policy Update. Although a client can be configured to check for policy updates periodically, in most cases this happens when a user logs on or off the domain. One impact of how installations work is that the installers run under a different domain account from the end user, one with elevated rights and this elevated user does not have access to HKCU for other accounts. What this means to us is that installers can only write to HKLM (Local Machine) and so cannot make per user registry changes.

Installer Options - Local Machine

Options available to installers (HKLM) are system wide and product specific. They are listed in detail on the Tracker Help Site. The available switches include, amongst other things:

- Setting the application language,
- Applying a license key,
- Installing program features like browser plugins,
- Specifying the default application for PDF files.

Details for each product's available switches can be found here:
PDF-XChange Editor: http://help.tracker-software.com/EUM/default.aspx?pageid=PDFXEdit3:switches_for_msi_installers
PDF-XChange Standard: http://help.tracker-software.com/EUM/default.aspx?pageid=PDFXSTD5:msi_installer_switches
PDF-XChange Pro: http://help.tracker-software.com/EUM/default.aspx?pageid=msi_installation_switches_pro5

This article http://www.tracker-software.com/knowledgebase/373 details how to install Tracker Software Products using the Tracker's .msi installers and a Group Policy under Microsoft's Active Directory. The article deals with applying the switches directly through the command line.

Active Directory does not use command line switches directly, the switches are applied using a transform. Here http://www.tracker-software.com/knowledgebase/462 we describe how to use an .mst (transform) file to apply switches available to the installers during such a software deployment.

Runtime Options - Current User

Some options, not available to installers (HKCU), can be set post install using an Administrative Template and an Active Directory Group Policy. Options available through the Administrative Template include, amongst other things:

- Check if PDF-XChange Editor is the default app
- List of Hidden/Disabled Preferences Pages
- Allow/Disallow copying of the Serial Key
- Open files policy

More detail on using Tracker's Administrative Template can be found here: http://www.tracker-software.com/knowledgebase/494

Precedence – How settings are applied.

The administrative template works independently of install options and its associated registry keys are applied to the user's Current User hive regardless of the state of the Editor's installation. These keys are not in the same section of HKCU as the UI managed keys that are stored in

HKEY_CURRENT_USER\Software\Tracker Software\PDFXEditor\3.0

but in:

HKEY_CURRENT_USER\Software\Policies \Tracker Software\PDFXEditor\3.0\

When the Editor starts it looks first for the presence of any of these policy keys and applies the setting(s) accordingly. Note that these policy applied keys are not changed by user interaction with the Editor's Preferences Pages and are not reflected in the UI screens. In any setting conflict, Domain Policies take precedence.

After checking for Policy settings the Editor then looks to the Tracker Software section of HKCU for user's individual preference settings. This results in the possibility that users could try make changes that conflict with Domain Policy. The conflicting setting will show in the user's Editor Preferences UI but will not be applied.

An example of this might be a Domain Policy for setting PDF-XChange Editor to check if it is the default PDF application and prompt the user with a choice to change it. On launching the Editor this domain policy is silently set, however a user can still access the setting in the preferences (Edit à Preferences à File Associations). This user setting WILL be overridden by the domain policy even though it appears to be set in the user preferences. Domain policy will always override user preferences regardless of what the user preferences UI shows.

Because it can be confusing to users who make changes to their preferences that will not be applied, administrators can change, using the Domain Policy, what users see in the preferences. Entire preferences pages can be explicitly hidden or disabled.

A Real World Example – Deploy the PDF-XChange Editor

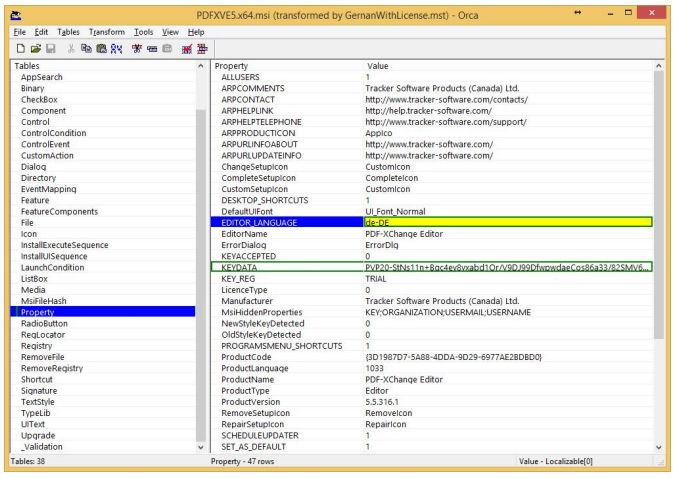
This example will install the PDF-XChange Editor through an Active Directory Group Policy with the following options:

- Use German language for the Editor UI.
- Install a license key.
- Set Domain Policies for:
  - Do not check if PDF-XChange Editor is the default PDF application on start.
  - Do not allow the serial key to be copied from the UI
  - Choose preferences pages to hide or disable
    - Hide "Launch" preferences page
    - Disable "Docs" preferences page
  - Open Embedded Files Policy
    - Always ask when opening attached (embedded) files
  - Open Files Policy – Use File-Extensions Trusted/Untrusted List
    - Deny opening .exe and .com files
    - Allow opening PDF files
    - Always ask when opening MS-Word documents
  - Open Sites Policy
    - Deny opening "mailto" links
    - Allow "https" links
    - Always ask for "http" links

Prepare needed files

1. Create a Transform

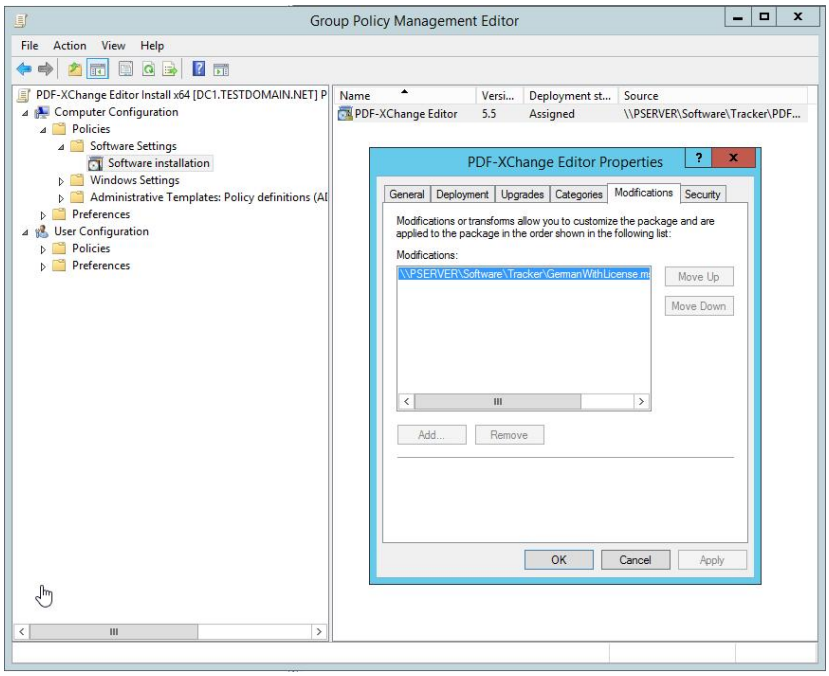
   Create a transform to pass the install options for German language and license key to the installer we use a transform. There are other ways to create a transform; here we use Microsoft's "Orca". See here for details on using Orca with PDF-XChange to create a transform file: http://www.tracker-software.com/knowledgebase/462



2. Create a Software Installation package

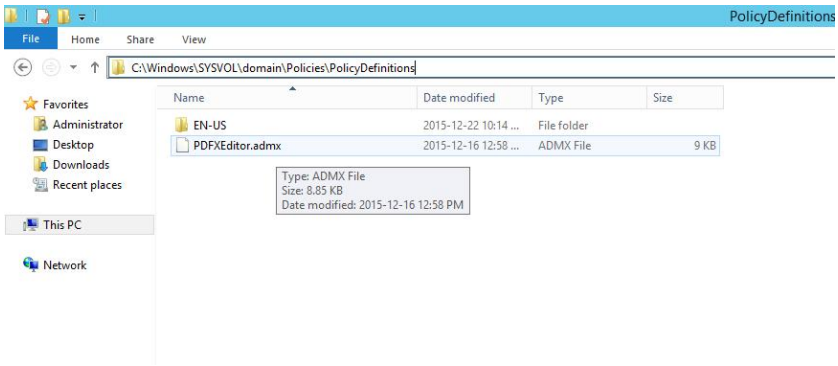
   Create a Software installation package for PDF-XChange on your domain controller and apply changes to it using a transform file. It is important that the transform be applied when creating the installation package as it cannot be added later. See here for details on deploying Tracker Software products through a GPO: http://www.tracker-software.com/knowledgebase/373

3. Apply the transform
   3.1. Make the transform file available to your network on your distribution point.
   3.2. Apply it to the group policy. This is added on the Modifications tab of the installer package properties when the policy is created. If the transform is not added at this point you will not be able to add one later, it must be done now else a new package will need to be defined.



4. Place the Administrative Template

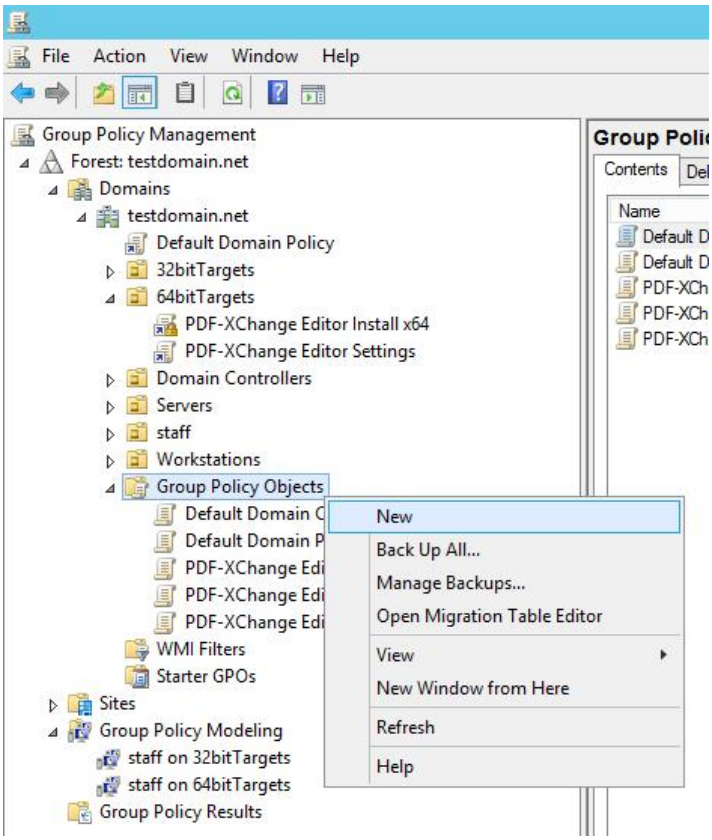
Put the Tracker Administrative Template files in your Domain Controller's Central Store. The default location for this is C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions. You will need a subfolder for the associated language file (.adml) See here for details on features that can be managed by tracker Software's Administrative Template: http://www.tracker-software.com/knowledgebase/494



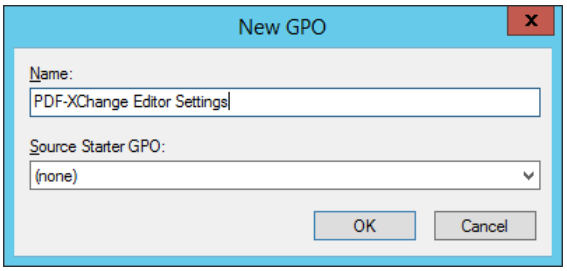
5. Use the Template to apply settings

5.1. Create a policy based on the template

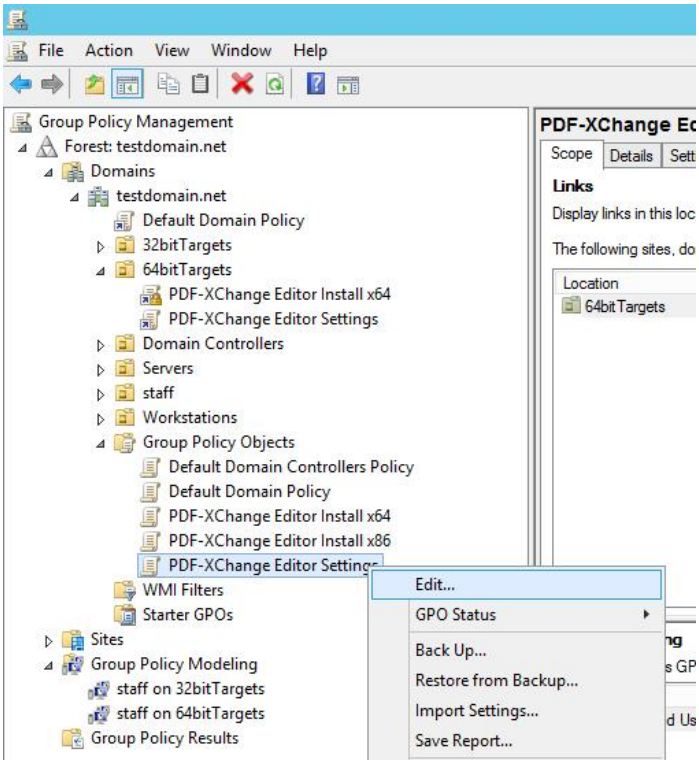
5.1.1. Use your domain controller's Group Policy Management Console to create a new policy



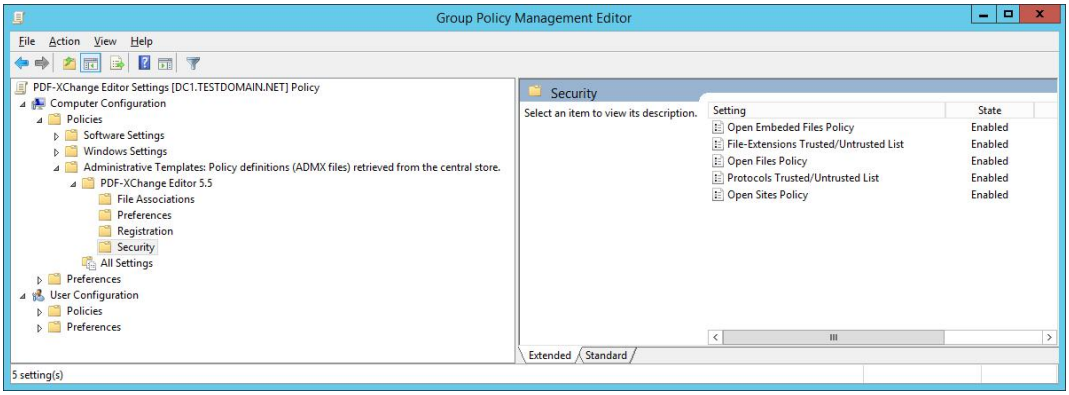
5.1.2. Name it appropriately



5.1.3. Edit the new policy



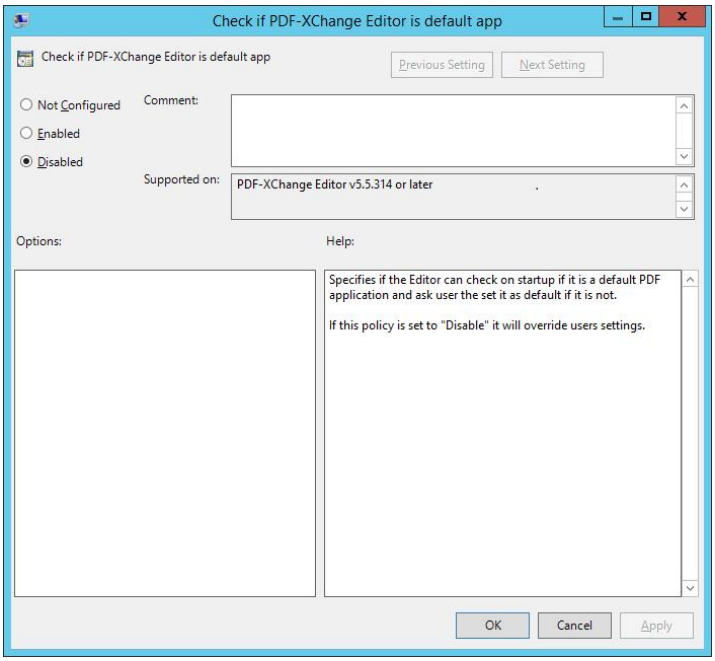
5.1.4. The PDF-XChange Editor 5.5 Administrative Template will automatically be available, pulled for you from the Central Store.



5.2. Use the Group Policy Management Editor to customise settings

5.2.1. Do not check if PDF-XChange Editor is the default PDF application on start.

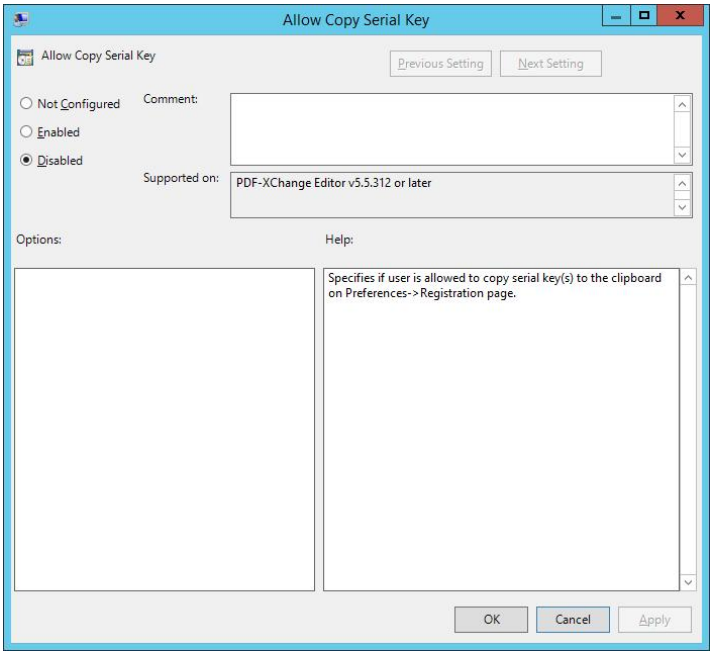
In the File Associations folder, double click “Check if PDF-XChange Editor is default app” and it will open a window where you can change the options.



Set this to “Disabled” to prevent the Editor from checking if it is the default PDF application when it is started.

5.2.2. Do not allow the serial key to be copied from the UI

This policy is in the Registration folder. Set to Disabled to prevent users copying the key.

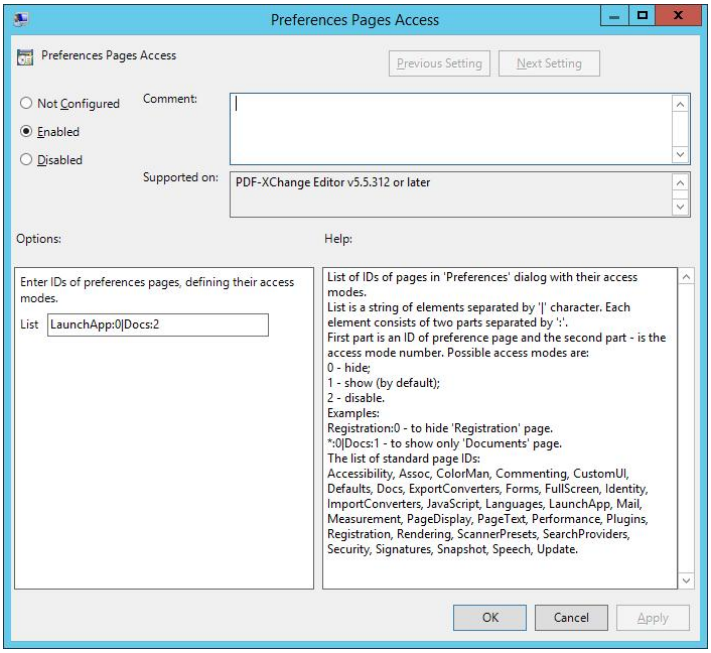


5.2.3. Hide or Disable Preferences Pages

Found in the Preferences folder, this policy when enabled supports a list of preference pages defined with IDs to be: set to

0 – hide,
1 - show (default)
2 - disable.

Page IDs are listed in the Help section of the policy's edit window. The list is a series of *key:value* statements separated by the | (pipe) character. To hide the Launch Applications preference page and disable (controls are greyed out) the Documents preferences page you would enter LaunchApp:0|Docs:2 in the Options dialogue pane List text box.



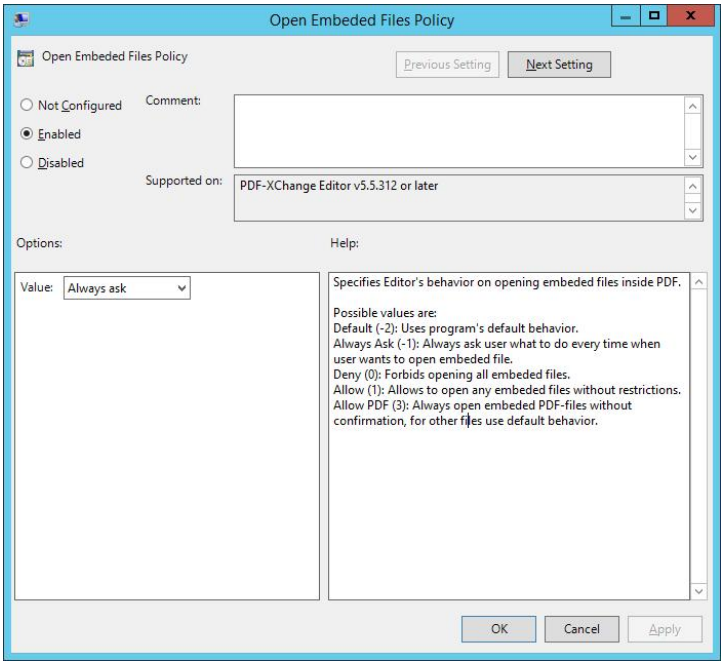
5.2.4. Always ask when opening attached (embedded) files.

Found in the “Security” folder, the Open Embedded Files Policy has the following options:

- Default (-2): Uses program's default behaviour.
- Always Ask (-1): Always ask user what to do every time a user wants to open an embedded file.
- Deny (0): Forbids opening all embedded files.
- Allow (1): Allows opening any embedded files without restrictions.
- Allow PDF (3): Always open embedded PDF-files without confirmation.

Enable the Policy and set to “Always Ask”.

Note that embedded and attached files are in this context the same thing.



5.2.5. Open Files Policy – Use File-Extensions Trusted/Untrusted List

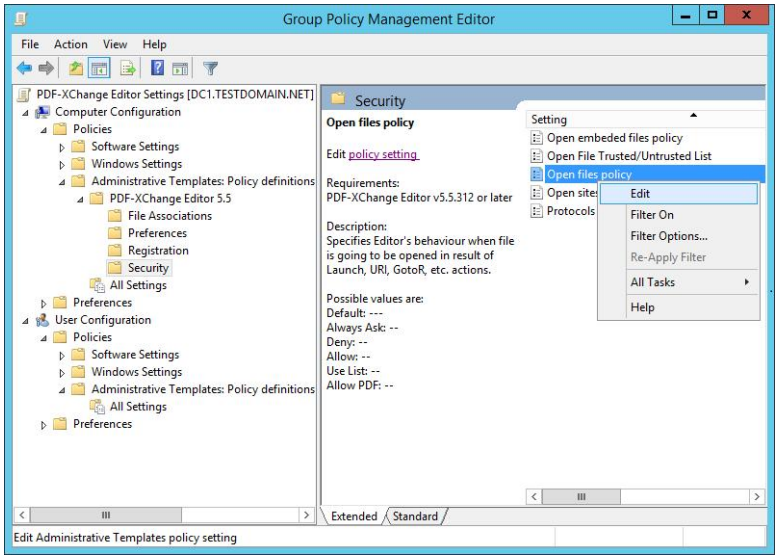
- Deny opening .exe, .com and .bat files
- Allow opening PDF files
- Always ask when opening MS-Word documents

Possible values are:

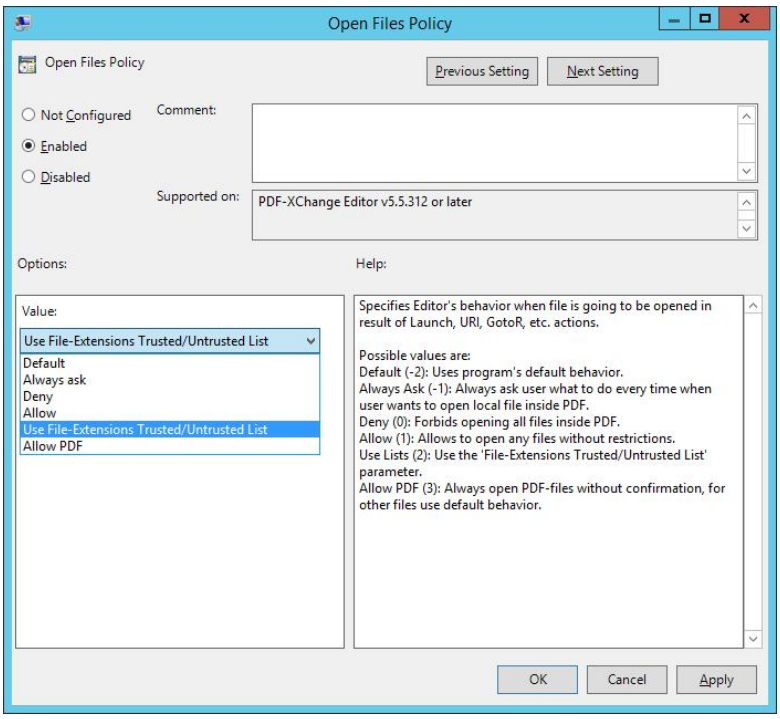
- Default (-2): Uses program's default behavior.
- Always Ask (-1): Always ask user what to do every time when user wants to open local file inside PDF.
- Deny (0): Forbids opening all files inside PDF.
- Allow (1): Allows to open any files without restrictions.
- Use Lists (2): Use the 'File-Extensions Trusted/Untrusted List' parameter.
- Allow PDF (3): Always open PDF-files without confirmation, for other files use default behavior.

For our example we wish to specify behaviour based on file extension so we set the “Open Files Policy” to “Use File-Extension Trusted/Untrusted List”:

Using the Group Policy Management Editor, select the “Open Files Policy” in the “Security” folder of the template and “Edit” with a right click:



In the “Open Files Policy” dialogue select the “Enabled” radio button and choose the “Use File-Extension Trusted/Untrusted List” value from the drop down list:



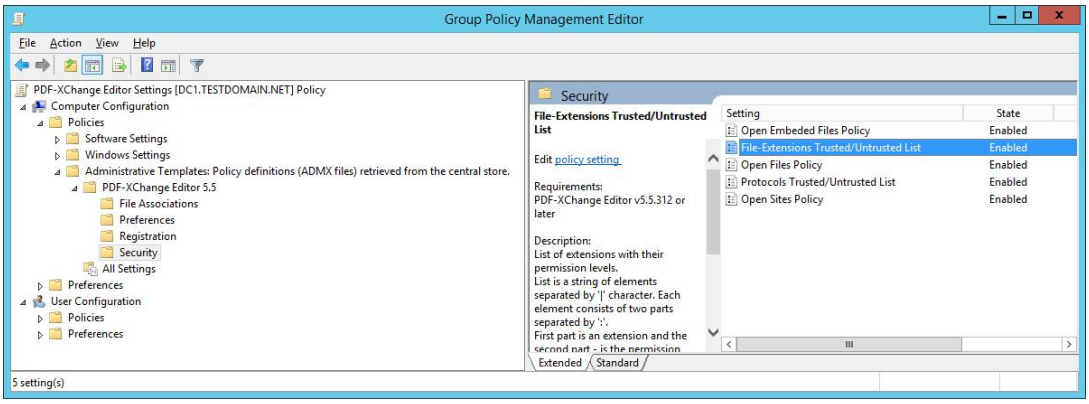
Use the “File-Extensions Trusted/Untrusted List” to specify the behaviour by file extension:
The list is a string of elements separated by the '|' (pipe) character. Each element consists of two parts separated by a ':' (colon).

The first part is an extension and the second part - is the permission level. Possible permissions levels are:

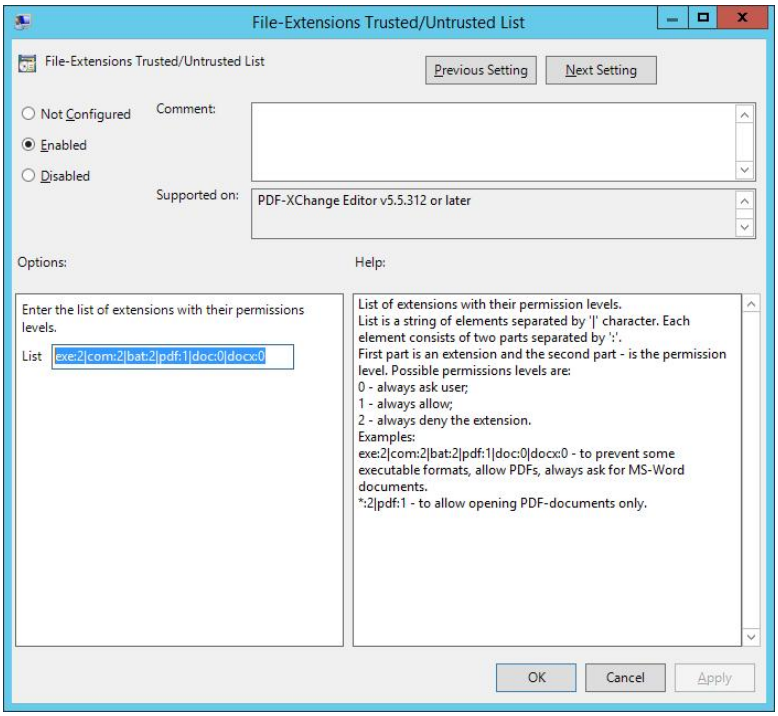
- 0 - always ask user;
- 1 - always allow;
- 2 - always deny the extension;

For our example use: **`exe:2|com:2|bat:2|pdf:1|doc:0|docx:0`** - to prevent some executable formats, allow PDFs and to always ask for MS-Word documents.

Open the File-Extensions Trusted/Untrusted List from the Security folder in the Administrative Template in the Group Policy Management Editor:



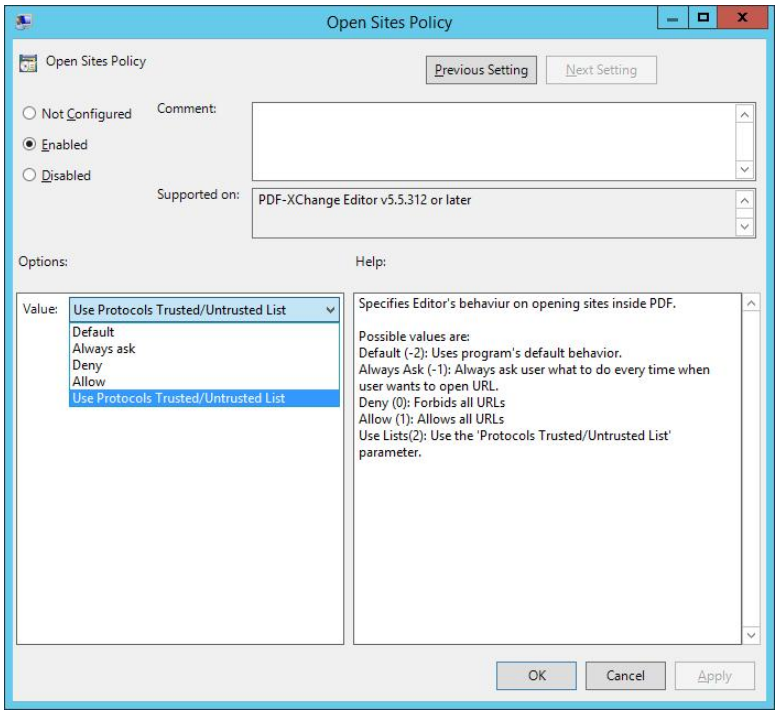
Enter **`exe:2|com:2|bat:2|pdf:1|doc:0|docx:0`** into the list text box:



5.2.6. Open Sites Policy (by protocol)

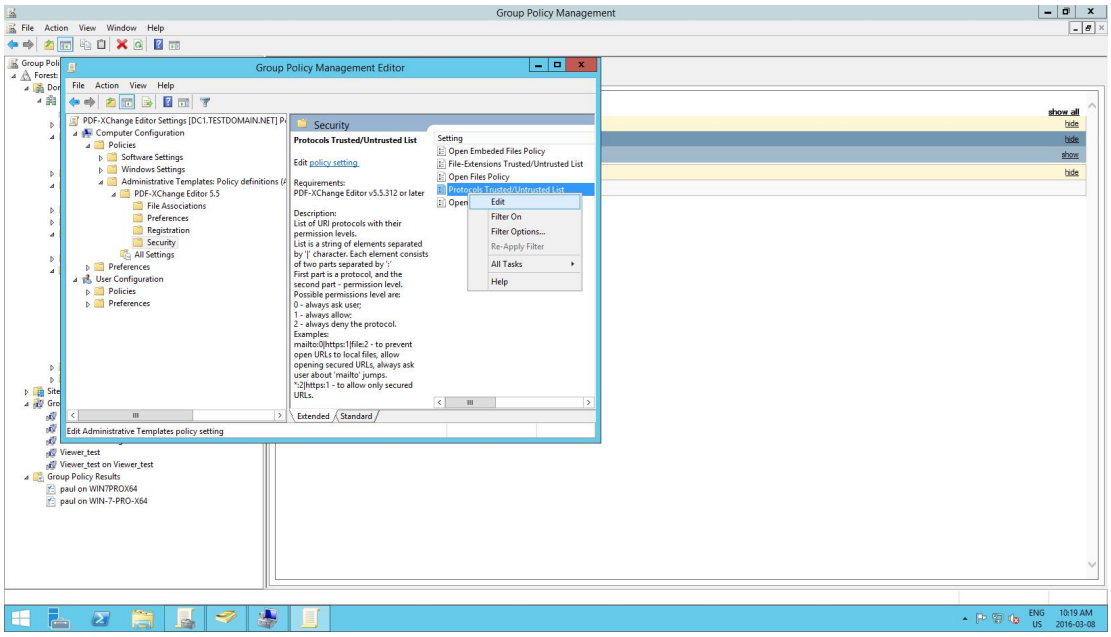
- Deny opening “mailto” links
- Allow opening “https” links
- Always ask when opening “http” links

As in the previous example we need to set the Policy to use a Trusted/Untrusted list:

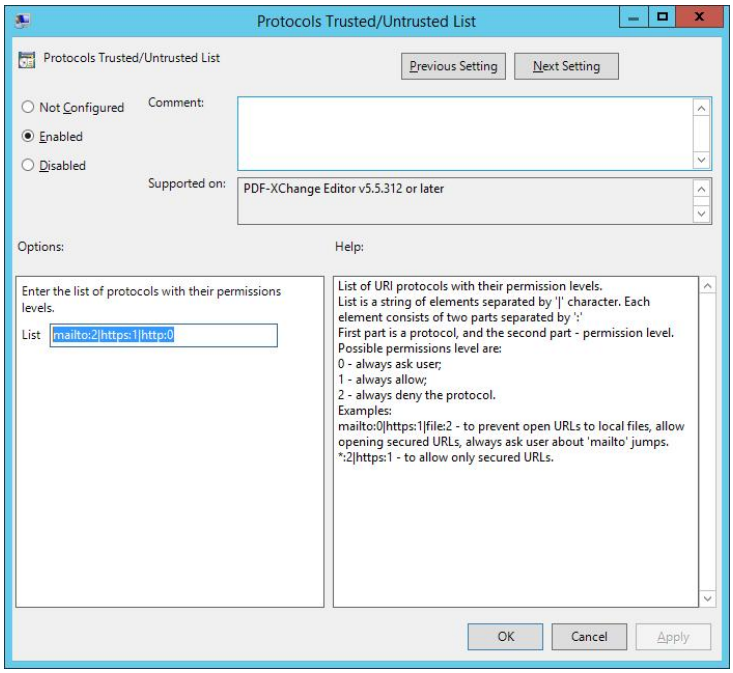


Then apply a list in the Protocols Trusted/Untrusted List:

Use the Group Policy Management Editor to edit the “Protocols Trusted/Untrusted List” found in the “Security” folder of the Administrative Template:

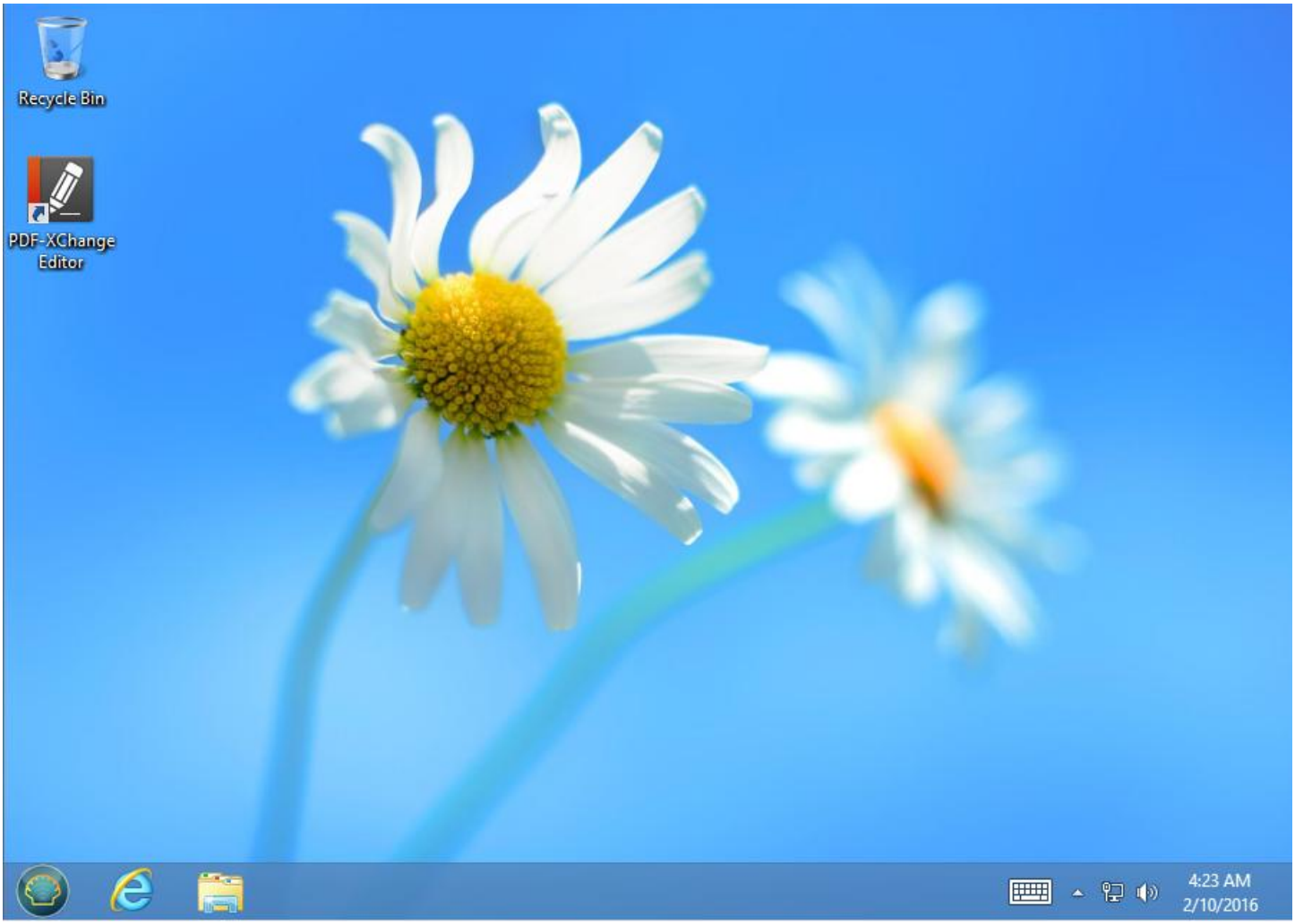


`mailto:2|https:1|http:0` will Deny mailto: Allow https: and always ask for http:

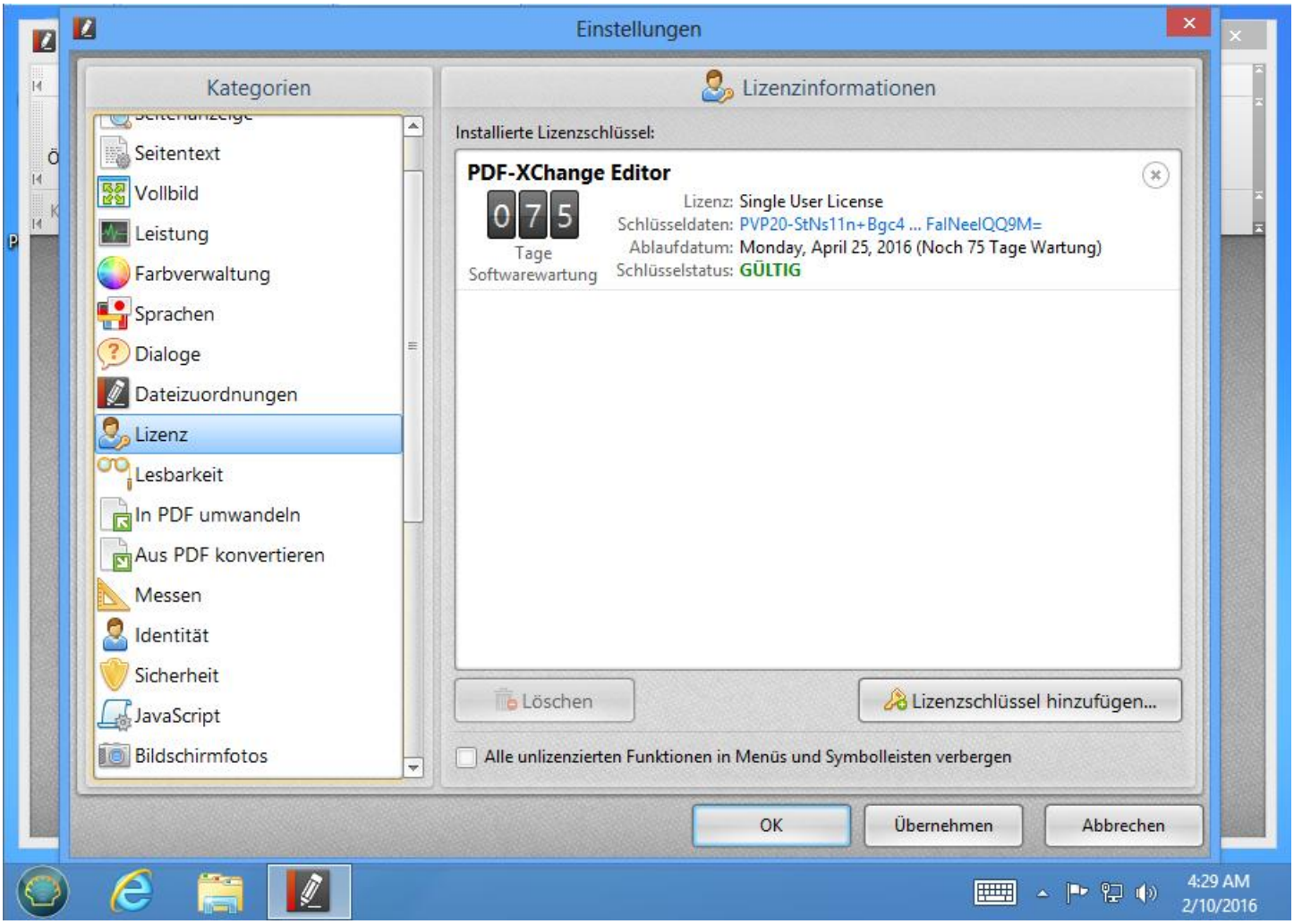


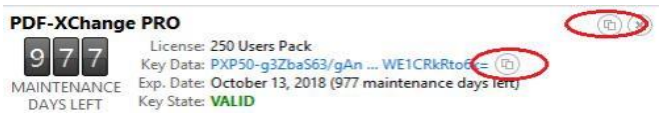
6. Applying the Policy

Your Active Directory Group Policy for installation will determine how the software is presented to your users. This example shows assigning the software to specific machines. This means that after a Group Policy Update, typically a computer restart, the install options used mean the Editor will be installed and a shortcut made available on the desktop.

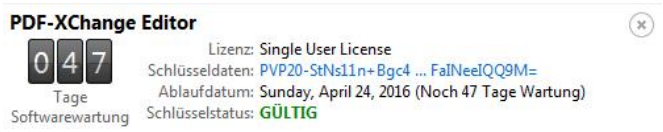


The MSI + Transform installed the Editor with a serial key and set the UI language to German:





Note that in the above screen shot there are no “Copy” capabilities displayed. By default, (see left), there is an icon to copy the long (256 characters) serial key into the Windows clipboard.



This has been silently disabled by our Group Policy “Do not allow the serial key to be copied from the UI”.

The other policies are also in place; the Editor does not check if it is the default PDF application even though the user's preferences show it is set to notify him if it's not the default. Restrictions are in place on opening both linked and embedded files as well as by protocol.

The policies from the Administrative Template can be found in
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Tracker Software\PDFXEditor\3.0`