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 <u>Tracker Help Site</u>. 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: <u>http://help.tracker-software.com/EUM/default.aspx?pageid=PDFXEdit3:switches_for_msi_installers</u> PDF-XChange Standard: <u>http://help.tracker-software.com/EUM/default.aspx?pageid=PDFXSTD5:msi_installer_switches</u> PDF-XChange Pro: <u>http://help.tracker-software.com/EUM/default.aspx?pageid=msi_installation_switches_pro5</u>

This article <u>http://www.tracker-software.com/knowledgebase/373</u> 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 <u>http://www.tracker-software.com/knowledgebase/462</u> 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: <u>http://www.tracker-software.com/knowledgebase/494</u>

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:
 - o 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
 - o Open Embedded Files Policy
 - § Always ask when opening attached (embedded) files
 - o 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
 - o 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 "<u>Orca</u>". See here for details on using Orca with PDF-XChange to create a transform file: <u>http://www.tracker-software.com/knowledgebase/462</u>

ile <u>E</u> dit T <u>a</u> bles T <u>r</u> ansform <u>T</u> ools <u>V</u> iew <u>H</u> el	2	
🗅 🚅 🖶 🙏 🐿 🏙 👷 🤻 📾 📾 💓 🤅	F	
ables .	Property	Value
AppSearch	ALLUSERS	1
Binary	ARPCOMMENTS	Tracker Software Products (Canada) Ltd.
CheckBox	ARPCONTACT	http://www.tracker-software.com/contacts/
Component	ARPHELPLINK	http://help.tracker-software.com/
Control	ARPHELPTELEPHONE	http://www.tracker-software.com/support/
ControlCondition	ARPPRODUCTICON	Appleo
ControlEvent	ARPURLINEGABOUT	http://www.tracker-software.com/
CustomAction	ARPURLUPDATEINFO	http://www.tracker-software.com/
Dialog	ChangeSetupicon	Customicon
Directory	CompleteSetupicon	Completeicon
EventMapping	CustomSetupicon	Customicon
Feature	DESKTOP SHORTCUTS	1
FeatureComponents	DefaultUlFont	UI Font Normal
File	EDITOR LANGUAGE	de-DE
Icon	EditorName	PDF-XChange Editor
InstallExecuteSequence	ErrorDialog	ErrorDig
InstallUISequence	KEYACCEPTED	0
LaunchCondition	KEYDATA	PVP20-StNs11n+Bgc4ev8vxabd1Or/V9DJ99DfwpwdaeCos86a33/82SMV6.
ListBox	KEY REG	TRIAL
Media	LicenceType	0
MsiFileHash	Manufacturer	Tracker Software Products (Canada) Ltd.
Property	MsiHiddenProperties	KEY:ORGANIZATION:USERMAIL:USERNAME
RadioButton	NewStyleKeyDetected	0
RegLocator	OldStyleKeyDetected	8
Registry	PROGRAMSMENU SHORTCUTS	1
RemoveFile	ProductCode	(3D1987D7-5A88-4DDA-9D29-6977AE28DBD0)
RemoveRegistry	ProductLanguage	1033
Shortcut	ProductName	PDF-XChange Editor
Signature	ProductType	Editor
TextStyle	ProductVersion	5.5.316.1
TypeLib	RemoveSetupicon	Removelcon
UlText	RepairSetupIcon	Repairlcon
Upgrade	SCHEDULEUPDATER	1
Validation		

2. <u>Create a Software Installation package</u>

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: <u>http://www.tracker-software.com/knowledgebase/373</u>

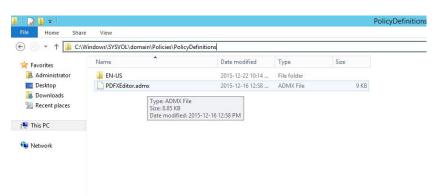
3. Apply the transform

- 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.

J Gro	up Policy Management Editor
File Action View Help	
 PDF-XChange Editor Install x64 (DC1.TESTDOMAIN.NET) P Computer Configuration Policies Software installation Software installation Mindows Settings Administrative Templates: Policy definitions (AI Preferences Policies Policies Preferences 	Name Versi Deployment st Source ■ PDF-XChange Editor 5.5 Assigned \\PSERVER\Software\Tracker\PDF ■ PDF-XChange Editor POF-XChange Editor Properties ? × ■ General Deployment Upgrades Categories Modifications Security ■ Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list: Modifications: Modifications ■ Modifications ■ Modifications ■ Modifications Modifications ■ Voidifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications ■ Modifications: ■ Modifications ■ Move Up ■ Modifications: ■ Move Down ■ Move Down ■ Add Remove ■ Move Down ■ OK © Modifications ■ Apply
<u>ل</u>	

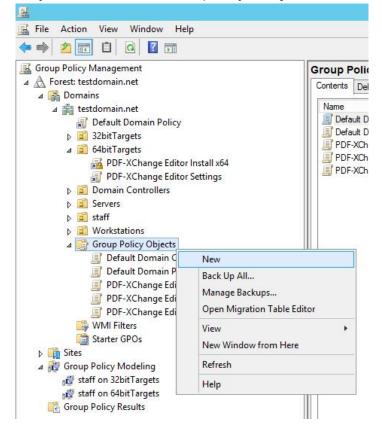
4. Place the Administrative Template

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: <u>http://www.tracker-software.com/knowledgebase/494</u>



5. <u>Use the Template to apply settings</u>

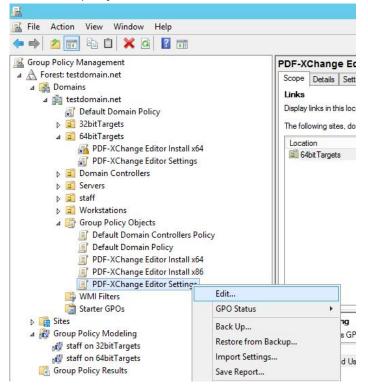
- 5.1. Create a policy based on the template
 - 5.1.1. Use your domain controller's Group Policy Management Console to create a new policy



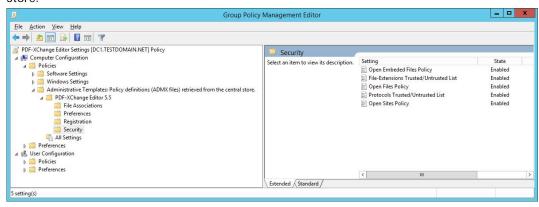
5.1.2. Name it appropriately

New GPO	x
<u>N</u> ame: PDF-XChange Editor Settings	
Source Starter GPO: (none) OK Cancel	~

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.



MANAGING TRACKER SOFTWARE PRODUCTS WITH ACTIVE DIRECTORY

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.

8	Ch	neck if PDF-X0	Change Ed	itor is defau	ult app			×
Check if PDF-XCP	hange Editor is def	ault app		Previous Se	tting	Next Setting		
O Not <u>C</u> onfigured	Comment:							^
• Disabled	Supported on:	PDF-XChange	Editor v5.5.31	4 or later		•		~
Options:			Help:					
			application	i the Editor car a and ask user cy is set to "Dis	the set it	as default if it	is not.	
L] [[OK	Cance	el	Apply

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.

8		Allow Copy Serial Key
Allow Copy Seria	l Key	Previous Setting Next Setting
O Not <u>C</u> onfigured	Comment:	<u>^</u>
O Enabled		
Disabled	Supported on:	PDF-XChange Editor v5.5.312 or later
Options:		Help:
		Specifies if user is allowed to copy serial key(s) to the clipboard on Preferences->Registration page.
		OK Cancel Apply

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.

t: ed on: PDF-XChange	Previous Setting Next Setting ✓ E Editor v5.5.312 or later ✓ Help: List of IDs of pages in "Preferences" dialog with their access modes.
ed on: PDF-XChange	Help: List of IDs of pages in 'Preferences' dialog with their access modes.
	Help: List of IDs of pages in 'Preferences' dialog with their access modes.
Jefining their access	List of IDs of pages in 'Preferences' dialog with their access modes.
defining their access	modes.
	List is a string of elements separated by ' ' character. Each element consists of two parts separated by ' '. First part is an ID of preference page and the second part - is the access mode number. Possible access modes are: 0 - hide; 1 - show (by default); 2 - disable. Examples: Registration: 0 - to hide 'Registration' page. ''x)Docs: 1 - to show only 'Documents' page. The list of standard page IDs: Accessibility, Assoc, ColorMan, Commenting, CustomUI, Defaults, Docs, ExportConverters, Forms, FullScreen, Identity, ImportConverters, JavaScript, Languages, LaunchApp, Mail, Measurement, PageDisplay, PageText, Performance, Plugins, Registration, Rendering, ScannerPresets, SearchProviders, Security, Signatures, Snapshot, Speech, Update.

MANAGING TRACKER SOFTWARE PRODUCTS WITH ACTIVE DIRECTORY

- 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.

8 .	Open Embeded Files Policy
Open Embeded Files Policy	Previous Setting
Not <u>C</u> onfigured Comment: Enabled Disabled	
Supported on:	PDF-XChange Editor v5.5.312 or later
Options:	Help:
Value: Always ask 💙	Specifies Editor's behavior on opening embeded files inside PDF. Possible values are: Default (-2): Uses program's default behavior. Always Ak. (-1): Always ask user what to do every time when user wants to open embeded file. Derny (0): Forbids opening all embeded files. Allow (1): Allows to open any embeded files. Allow PDF (3): Always open embeded PDF-files without restrictions. Allow PDF (3): Always open embeded PDF-files without confirmation, for other files use default behavior.
	OK Cancel Apply

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

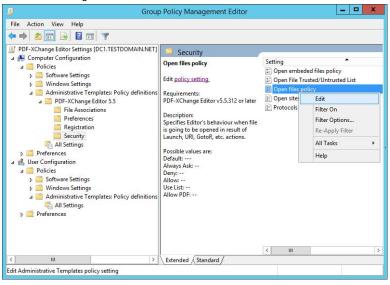
- Deny opening .exe, .com and .bat files
- Allow opening PDF files
- Always ask when opening MS-Word documents

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:

		Op	oen Files Po	olicy			-		x
Open Files Policy				<u>P</u> revious S	Setting	<u>N</u> ext Settin	9		
 Not <u>C</u>onfigured <u>E</u>nabled <u>D</u>isabled 	Comment:								× ×
0 <u>-</u>	Supported on:	PDF-XChange Editor v5.5.312 or later						<	
Options:			Help:						
Value: Use File-Extensions T Default Always ask Deny Allow Use File-Extensions T Allow PDF			Possible va Default (-2 Always Asl user wants Deny (0): F Allow (1): A Use Lists (2 parameter. Allow PDF	unch, URI, G lues are:): Uses progi (-1): Alway: to open loc orbids open Allows to op): Use the 'Fi	GotoR, etc. ram's defa s ask user al file insic ing all files en any file ile-Extensi open PDF-	ult behavior. what to do eve	ery time rictions. Intrusted	when I List'	or v
					ОК	Can	cel	Ар	ply

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:

I Group Policy	Management Editor	_ 🗆 X
File Action View Help ← → 2 □ → 2 □ → 1 □ ▼		
Policies > Policies > Administrative Templete: Policy definitions (ADMX files) retrieved from the central store. > Administrative Templete: Policy definitions (ADMX files) retrieved from the central store. > Policies > File Associations Perferences > Registration > Security > Perferences > Perferences	Security File-Extensions Trusted/Untrusted List Edit golicy setting Requirements: PDF-XChange Editor v5.5.312 or later Description: List of extensions with their permission levels. List is a string of elements separated by ': First part is an extension and the eccond nat', then emmission Vertex of Xtandard	State Enabled Enabled Enabled Enabled Enabled
5 setting(s)		

Enter e	exe:2	com:2	bat:2	pdf:1	doc:0	docx:0	into	the I	ist tex	t box:
---------	-------	-------	-------	-------	-------	--------	------	-------	---------	--------

8	File-Extensio	ns Trusted/Untrusted List
File-Extensions Trusted/Untrust	d List	Previous Setting Next Setting
○ Not <u>C</u> onfigured Comment: ● <u>E</u> nabled		^
 <u>D</u>isabled Supported o 	n: PDF-XChange I	Editor v5.5.312 or later
Options:		Help:
Enter the list of extensions with thei levels. List exc2(com2(bat2)pdfi)(doc:0)		List of extensions with their permission levels. List is a string of elements separated by '' character. Each element consists of two parts separated by ''. 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. Examples: exe:2[com:2][bat:2]pdf:1](doc:0](doc:0 - to prevent some exec:utable formats, allow PDFs, always ask for MS-Word documents. *:2]pdf:1 - to allow opening PDF-documents only.
		OK Cancel Apply

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:

S		Ор	en Sites Policy	x
Dp Op	en Sites Policy		Previous Setting	
 ○ Not ● Enal ○ Disa 				^
O <u>D</u> isa	Supported on:	PDF-XChange E	Editor v5.5.312 or later	^ ~
Options			Help:	
Value:	Use Protocols Trusted/Untrus Default Always ask Deny Allow Use Protocols Trusted/Untrus		Specifies Editor's behaviur on opening sites inside PDF. 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 URL. Deny (0): Forbids all URLs Allow (1): Allows all URLs USE Lists(2): Use the 'Protocols Trusted/Untrusted List' parameter.	<
			OK Cancel A	pply

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:

<u>14</u>			Group Policy Management		- 0 ×
File Action	n View Window Help				_ 8 ×
💠 🔿 🙍	T fa 🖬 🗙 @ 🛛 🖬				
if it Action if it Action	Corput Configuration Configuration CorputConfiguration Corput Configuration	Volicy Management Editor	Setting Set		
					~
				ENC.	G 10:19 AM
	, 🛛 📋 🛃 🛩 🐇			* 🏳 🛱 🕼 US	

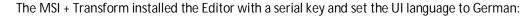
mailto:2|https:1|http:0 will Deny mailto: Allow https: and always ask for http:

	Protocols Trusted/Untrusted List
Protocols Trusted/Untrusted List	Previous Setting Next Setting
Not <u>Configured</u> Comment: Enabled Disabled Supported on:	Previous Setting Next Setting ured Comment: Supported on: PDF-XChange Editor v5.5.312 or later Help: f protocols with their permission Help: Itist of URI protocols with their permission levels. List is a string of elements separated by '' character. Each element consists of two parts separated by '' character. Each element
Options: Enter the list of protocols with their per levels. List mailto:2(https://https://	List of URI protocols with their permission levels. List is a string of elements separated by ' ' character. Each element consists of two parts separated by '' First part is a protocol, and the second part - permission level. Possible permissions level are: 0 - always ask user; 1 - always allow; 2 - always deny the protocol. Examples:
	OK Cancel Apply

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.





Kategorien	lizenzinformationen	
	Installierte Lizenzschlüssel:	
Seitentext Seitentext Vollbild Leistung Farbverwaltung Sprachen Dialoge Dateizuordnungen Lesbarkeit In PDF umwandeln Aus PDF konvertieren Messen Identität	PDF-XChange Editor Lizenz: Single User License Tage Softwarewartung Lizenz: Single User License Chlüsseldaten: PVP20-StNs11n+Bgc4FalNeelQQ9M= Ablaufdatum: Monday, April 25, 2016 (Noch 75 Tage Wartung) Schlüsselstatus: GÜLTIG	(x
Sicherheit	Löschen Binzufügen	
Bildschirmfotos	Alle unlizenzierten Funktionen in Menüs und Symbolleisten verbergen	
	OK Übernehmen Abbreche	n



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.

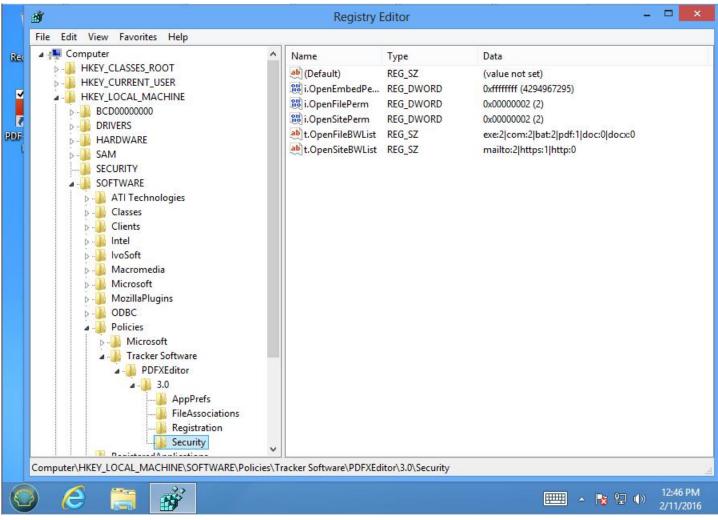
PDF-XChange Editor



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