Contents

1  Wizard Basics .............................................................................................................................................. 5
   1.1 Getting Started ......................................................................................................................................... 5
      1.1.1 Related enterprise resources ........................................................................................................ 6
   1.2 Installation .............................................................................................................................................. 6
   1.3 Workspace views ..................................................................................................................................... 6
   1.4 Starting a Project .................................................................................................................................... 7
      1.4.1 Loading an installer file .................................................................................................................. 7
      1.4.2 Open a recent project ...................................................................................................................... 7
      1.4.3 Loading a transform file .................................................................................................................. 8
      1.4.4 Saving a project ............................................................................................................................. 8
      1.4.5 Pre deployment file verification .................................................................................................... 8
      1.4.6 Reset installation settings ............................................................................................................ 9
   1.5 Multiple installations ............................................................................................................................. 9

2  Customizing the Installer ............................................................................................................................ 10
   2.1 Configuration panel overview .............................................................................................................. 10
   2.2 Personalization options ......................................................................................................................... 11
   2.3 Installation options ............................................................................................................................... 11
      2.3.1 Default viewer .................................................................................................................................. 11
      2.3.2 Remove installed products .......................................................................................................... 13
      2.3.3 Optimize product performance ...................................................................................................... 13
      2.3.4 Disable caching installer files ........................................................................................................ 14
      2.3.5 Installing interactivity options ...................................................................................................... 14
      2.3.6 Reboot options .............................................................................................................................. 15
      2.3.7 Language selection ......................................................................................................................... 15
   2.4 Features ................................................................................................................................................. 16
   2.5 Files and folders ..................................................................................................................................... 17
      2.5.1 Adding and removing files and folders .......................................................................................... 18
      2.5.2 Viewing a list of changes file and folder changes ......................................................................... 19
      2.5.3 Use case: Deploying digital signature files ................................................................................... 20
   2.6 Registry .................................................................................................................................................... 20
      2.6.1 Registry workflow overview .......................................................................................................... 21
      2.6.2 Adding keys ...................................................................................................................................... 22
      2.6.3 Modifying existing keys ................................................................................................................ 23
      2.6.4 Summary ........................................................................................................................................ 23
   2.7 Shortcuts ............................................................................................................................................... 24
   2.8 Server locations .................................................................................................................................... 25
   2.9 Distiller .................................................................................................................................................. 26
   2.10 Adobe PDF printer ............................................................................................................................... 27
   2.11 Security ............................................................................................................................................... 30
      2.11.1 Directory servers .......................................................................................................................... 30
      2.11.2 Trusted identities .......................................................................................................................... 31
      2.11.3 Enhanced security ....................................................................................................................... 31
         2.11.3.1 Standalone and browser behavior ......................................................................................... 31
         2.11.3.2 Specifying trusted, “privileged” locations ........................................................................... 32
Wizard Basics

**Tip:** The most recent version of this document can always be downloaded from http://kb2.adobe.com/cps/837/cpsid_83709.html.

*Both a PDF and a compiled Help chm file are available.* This guide should be used in conjunction with the resources shown in Table 1. In particular, the Preference Reference provides registry and plist configuration details and the Enterprise Administration Guide provides installation and deployment details.

1.1 Getting Started

Welcome to Adobe Customization Wizard (hereafter, the “Wizard”). This product gives Information Technology (IT) administrators the ability to customize the installation of Acrobat products prior to deploying the applications across their organization.

**Note:** You must use Wizard 8 with version 8.x products, Wizard 9, with version 9.x products, Wizard X with X products, and so on.

The Wizard supports all products in the Acrobat family. Certain UI components are therefore enabled or disabled based on the loaded installer file. For example, when customizing reader, some of the available options which are specific to Acrobat will not be available.

In large organizations that employ site licenses and distribute software to multiple users over networks, or in smaller organizations that require IT assistance for installing, registering, and maintaining software on individual systems, IT administrators can use the Wizard to streamline the installation process. For example, if you have a site license, you do not need to register and personalize each copy of the product that you install. You can customize the installer to not only skip the standard registration questions, but also accept the standard EULA and fill in your organization name automatically. Other options include:

- Leverage existing deployments by copying enterprise files and registry configurations.
- Modify the registry (via the Registry Editor) and installer tables (via the Direct Editor) directly.
- Optimize the behavior of the installer by including silent installation, pre-serialization, reboot, multilingual, and custom setup.
- Remove previous versions of Reader and Acrobat.
- Suppress display EULA, registration prompts, and the Getting Started window.
- Use the Wizard’s UI to perform many other common task such as configuring file and registry-level preferences such as:
  - Adobe Distiller job options files and Adobe PDF file printer settings.
  - All application security settings such as Protected Mode, enhanced security, and JavaScript.
  - And much more!
1.1.1 Related enterprise resources

Tip: This guide should be used in conjunction with the resources shown in Table 1.

Table 1 Related resources

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Administration Guide</td>
<td>Deployment, configuration, and application management details.</td>
</tr>
<tr>
<td>Administrator’s Information Manager (AIM)</td>
<td>Registry configuration: An AIR application containing admin-centric resources such as the Preference Reference for the Acrobat Products</td>
</tr>
<tr>
<td>Enterprise Library</td>
<td>Links to all the documents above as well as other libraries.</td>
</tr>
</tbody>
</table>

1.2 Installation

The Wizard is available as a free download. To use it, do the following:

1. Download the installer.
2. Run CustWiz1000-en_US.exe.
3. At the Welcome screen, choose Next.
4. Accept the license agreement, and choose Next.
5. Verify the install location, and choose Next.
6. Choose Install.
7. Choose Finish.

1.3 Workspace views

The Wizard workspace is made up of five elements:

- The left-hand navigation bar links to configuration panels you use to modify installation settings. Icon links are product sensitive in that they will not display unless that feature is supported by the product. If you do not see a link in the navigation bar, then the setting is not available for installation file you’ve opened.
- The main work area on the right displays the installation settings, with fields where you can specify options.
- The help tip bar below the main work area contains context-sensitive assistance for optimizing your use of the Customization Wizard.
Wizard Basics

Starting a Project

1. The status bar at the bottom of the workspace displays system information.
2. The tool bar at the top of the workspace contains selected Customization Wizard command options.

These elements can be toggled on or off. To adjust the current view:

1. Choose View.
2. Select an element to add to or remove from the workspace.

Note: The title bar, menu bar, and main work area are always available. You cannot remove them from the workspace.

1.4 Starting a Project

1.4.1 Loading an installer file

To get started, open the package in the installation directory.

1. Archive a version of the downloaded MSI or MSP file and back it up. Do not modify this file. Only modify a copy of the file.
2. Open the Customization Wizard.
3. Choose File > Open Package or press CTRL+O.
4. Browse to locate the product installation directory.
5. Select the file to modify.
6. Choose Open.

The package settings are now accessible in the Customization Wizard workspace. Note that the .msi file name appears in the title bar, along with its associated transform file name, as follows:

<project filename> (transformed by <transform filename>) – Adobe Customization Wizard

Tip: You can create a copy of the transform file for use in another package, or you can load a different transform file, if you have created one in a separate directory.

1.4.2 Open a recent project

If you have recently opened a package, you can access it quickly from the shortcut on the File menu.

On the Windows Start menu, point to Programs, and then click Adobe Customization Wizard.

On the File menu, click Open Package, or press CTRL+O, and click the file name from the shortcut list.

The package settings are now accessible in the Customization Wizard workspace. Note that the .msi file name appears in the title bar, along with its associated transform file name, as follows:
You can create a copy of the transform file for use in another package, or you can load a different transform file, if you have created one in a separate directory.

1.4.3 Loading a transform file

To apply a transform file associated with another project to your current project:

1. Choose **Transform > Load Transform**.

2. In the Open dialog box, browse to find the file location, and then select the transform file name.

3. When you are done, click Open. The newly loaded transform file name now appears in the title bar as follows:

   `<project filename> (transformed by <new transform filename>) – Adobe Customization Wizard <version>`

4. To apply the newly loaded installation settings to the open project, click the File menu, and then click Save, or press CTRL+S.

   **Tip:** If the transform file is not located in the same directory as the project file, the Customization Wizard generates a copy of the transform file in the same directory when you save the project (.msi) file.

1.4.4 Saving a project

The Customization Wizard saves your modified installation settings in the associated transform (.mst) file and updates the project (.msi) file and setup.ini file in the same directory.

   **Note:** If the setup.ini file is not located in the same directory as the project file, you will see an error message when you try to save the file. But if the transform file is not located in the same directory as the project file, the Customization Wizard will create a copy in the same directory as the .msi file.

When you are finished making changes to your installation settings, save your customized installation settings in the Installer .msi file.

On the File menu, click Save, or press CTRL+S.

   **Note:** If the setup.ini file is not located in the same directory as the project file, you will see a message indicating that you cannot save the project (.msi) file.

Once the project is saved, the resulting SKU is ready for mass deployment by choosing your desired deployment methodology. For example, you can simply run setup.exe.

1.4.5 Pre deployment file verification

As part of the installation customization process, the Customization Wizard modifies three files which must be located in the same directory:

- Project file (.msi): Enables the executable file (setup.exe) associated with the application you are installing. The .msi file is also referred to as the package.
1.4.6 Reset installation settings

To restore an edited package to its default settings:

1. Choose File > Reset Package to Adobe default.

2. Choose Yes to confirm.

1.5 Multiple installations

If you have multiple installation scenarios in your organization, you can specify multiple sets of installation settings in separate transform files. You do not need to create and store a complete package for each scenario. Instead, you can create a standard package and store multiple transform files in a separate directory. When you are ready to run an installation, open the project file, and load the transform file containing the installation settings you want to use.

- **Transform file (.mst)** Contains your modifications to the installation settings and any files added to the .msi file. The Customization Wizard creates or updates a transform file every time you save an .msi file.

  **Note:** The transform file name appears alongside the project file name in the title bar, as follows: <project filename> (transformed by <new transform filename>) &endash; Adobe Customization Wizard <version>.

- **Setup.ini file:** Contains initialization data for the package. Some Adobe and MSI properties are written to this file. You can manually edit this file to add more properties and features. For details, see the Enterprise Administration Guide.
2 Customizing the Installer

Note: While many registry details are found in the sections below, a more detailed Preference Reference for the Acrobat Family of Products is available as part of the Administrator’s Information Manager (AIM).

2.1 Configuration panel overview

The Wizard displays different set of pages based on the feature support for each product. For example, more panels and options appear for Acrobat than Reader. Every user modification changes the MSI table or Setup.ini file. Modifications can include writing MSI or Adobe properties to the Setup.ini file and/or setting them in the installer tables as well as modifying the EnterpriseRegistries, EnterpriseRegistries, and other installer tables. You can use the Direct editor or a third party tools to inspect your customizations.

Custom registry settings are stored in the EnterpriseRegistries table and custom file settings are stored in the EnterpriseFiles table. Both tables contain an Action field. Field values can have the following meaning:

- 0: Skip Record, do nothing
- 1: Add file or registry value to end-user machine
- 2: Backup original file and add new file to end-user machine. The backup file has extension “aiwbf.”
- 3: Restore backup file
- 4: Remove file or registry value from end-user machine

All controls are initially displayed with the Adobe default values and the corresponding DB records show the Action field with a value of 0 (if the record exists by default). Modifications update the Action field with the requisite value or add a new record if required.

The RootKey field of the EnterpriseRegistries table specifies the OS Registry Root as follows:

- -1: HKEY_CURRENT_USER if per-user installation; HKEY_LOCAL_MACHINE if per-machine installation (Acrobat products supports per-machine installation only)
- 0: HKEY_CLASSES_ROOT
- 1: HKEY_CURRENT_USER
- 2: HKEY_LOCAL_MACHINE
- 3: HKEY_USERS
2.2 Personalization options

Personalization Options settings allow you to specify a standard user name, organization name, product serial number, and default installation path for the installed product. These values appear on the product’s splash screen at startup.

To configure the personalization options:

1. User name. Sets the USERNAME property.
2. Organization name. Sets the COMPANYNAME property.
3. Serial number (if any). The serial number identifies the software for registration and updates. If you have a site license, you can use the same serial number for multiple installations. Sets the ISX_SERIALNUMBER property.

   **Tip:** This field is greyed out if the product (such as Reader) does not require a serial number.

4. Installation path: The installation path specifies the location of the installed product files on the destination system. Sets the INSTALLDIR property. If you’d like to choose a non-default path, do one of the following:
   - Type the path to the product directory.
   - Click **Browse**, navigate to the directory location, and then click **OK**.

2.3 Installation options

2.3.1 Default viewer

When Reader and Acrobat are installed on the same machine, you can choose which viewer is the default for PDF files. In some cases, this choice is critical as Reader has a built in Protected Mode which is more secure. For security details, see the Application Security Guide.

To select a default viewer, choose one of the following:

- **Installer will decide which product will be the default:** The installer decides which application should open PDFs based on the product to install and the values of IW_DEFAULT_VERB and LEAVE_PDFOWNERSHIP. In general, the install leans towards letting the more secure Reader be the default viewer unless a property or user choice overrides that decision.

- **Make Reader the default PDF viewer:** For Reader only. Sets IW_DEFAULT_VERB to **Read**.

- **Make Acrobat the default PDF viewer:** For Acrobat only. Sets IW_DEFAULT_VERB to **Open**.

**Note:** IW_DEFAULT_VERB is written to the MST file and doesn’t exist in the installer tables by default. It can also be used on the command line or Setup.ini. DEFAULT_VERB is deprecated in the X release.
Interaction with LEAVE_PDFOWNERSHIP

IW_DEFAULT_VERB interacts with the Adobe property LEAVE_PDFOWNERSHIP which can be used on the command line. NO allows the new install to own opening PDFs. LEAVE_PDFOWNERSHIP is often used for silent installs where the user should not be asked to select a default PDF viewer.

- YES prevents the new installation from taking over PDF ownership if PDF is already owned. However, if PDF is currently un-owned, take ownership
- If this property unset or not present, the current install assumes ownership

Why is PDF ownership important?

Reader 10 introduces the concept of a Protected Mode, which is a general purpose mitigation against security exploits. This capability does not exist in Acrobat 10. Reader 10 is considered to be far more secure, while Acrobat remains far more capable. Consequently, users will have valid reasons to switch between Acrobat and Reader on a regular basis.

For 9.x products, double clicking a PDF file causes any open instance of the product to load the file regardless of version or product. For example if Reader X is the default PDF handler and Viewer 9 is already open double clicking a PDF would cause the PDF to be displayed by Viewer 9. For security reasons, the user needs control over which application will open a PDF; thus X version products provide users with the capability of selecting which product opens the PDF even if another instance is already running.

Administrators interested in security may want to select **Make Reader the default PDF viewer**. Version X products will be able to switch between any product type and version back to 9.x.

**Locking the feature**

By default, users can select the default handler through the UI. However, administrators can lock the feature via HKLM\SOFTWARE\Policies\Adobe\<product>\<version>\FeatureLockDown\bDisablePDFHandlerSwitching. When bDisablePDFHandlerSwitching is set to 1, the UI (Figure 2) is disabled and end users will not be able to change the default handler.
2.3.2 Remove installed products

The installer can be configured to automatically remove any previously installed version of Acrobat Professional, Standard, or Elements, version 6 or later, and/or Reader during the installation process. Note that these fields are disabled if a previous version is not detected. The two choices are:

- **Remove previous version**: Removes previous versions of Acrobat 6 or later currently installed on the destination system. Sets the REMOVE_PREVIOUS property.

- **Remove previous version of Reader**: Remove previous versions of Adobe Reader 6.0 or later currently installed on the destination system. Sets the REMOVE_PREVIOUS_READER property.

2.3.3 Optimize product performance

The optimization option runs a disk defragmentation utility that will automatically cluster files on a portion of the destination drive during installation, thereby improving launch time and performance. Defragmentation requires available disk space on the destination drive and adds time to the installation process. Adobe recommends that you leave this option selected.
Select **Enable Optimization** to automatically defragment a portion of the destination drive when running the installer. A progress bar will display during the defragmentation process. Sets the ENABLE_OPTIMIZATION property.

**Figure 4 Enable optimization**

- Enable Optimization
  
  Note: This feature allows the installer to run a defragmentation utility on a portion of the target drive during installation, improving launch time and performance. It is recommended you leave this enabled.

- Enable Caching of installer files on local hard drive

### 2.3.4 Disable caching installer files

In addition to the actual product files, there are a number of installer files that may be needed for patching, repair, or uninstall operations. Caching these files during installation allows these operations to fully complete without invoking a dialog with messages that ask the user to provide original installation source. Therefore, Adobe recommends that you enable caching. In cases where a smaller install size is a requirement, you can disable caching.

The files are installed to `<drive>\Program Files\Adobe\<product name and version>\` unless a different location is selected in Personalization Options. By default, all of the other installer files are also cached to the same location. If you change the installation path, then the location of the setup files will change accordingly.

Uncheck **Enable caching of installer files on local hard drive** to disable file caching when running the installer. Sets the ENABLE_CACHE_FILES property.

### 2.3.5 Installing interactivity options

By default, the installation process displays the installation screens to the end user. However, you can control this behavior by choosing one of the following:

- **Interactively (with full interface)**: Displays all installation screens.
- **Unattended (with no user interaction, only a progress bar)**: Suppresses all installation screens and displays only a progress bar when running the installer. It is advisable to choose Reboot without prompt or Suppress reboot in the Reboot section when selecting this option.
  
  The setup.ini command line will be set to /spb.

- **Silently (no interface)**: *This feature is not available for Reader and requires specifying a serial number.* Suppresses all installation screens and runs the installer with no interface. It is advisable to choose Reboot without prompt or Suppress reboot in the Reboot section when selecting this option.
  
  The setup.ini command line will be set to /sALL.
2.3.6 Reboot options

By default, the user is prompted for reboot after installation. Customize this behavior by choosing one of the following:

- **Reboot without prompt**: The setup.ini command line will be set to /rps.
- **Prompt the user for reboot**: Nothing is added to the command line.
- **Suppress reboot**: The setup.ini command line will be set to /rs.

**Tip**: If you select Unattended or Silently in the Run Installation section, then it is advisable to choose **Reboot without prompt** or **Suppress reboot**.

2.3.7 Language selection

For multi-lingual (MUI) installers that provide multiple language options, you can select a language to use during installation and in the installed product or allow the user to select a language to use during the install:

Select one of the following options to specify whether the user can select a language to use:

- **Allow the user to choose the installation language**: Provides the user the user will have the option of selecting an available language to use during installation. Deselecting this box enables the Install Language drop down list.
- **Install Language**: Provides a drop down list of available languages you can preselect for the user. The setup.ini command line will be set to /sl <language ID code>.
2.4 Features

This feature is only available for Acrobat.

The Features settings allow you to enable and disable installation and access for key features, including viewing and creating Adobe PDF files and running Adobe LiveCycle Designer. This feature is similar to what a user would see if they chose Custom Installation during a normal installation and they were given an opportunity to select which components would be installed. Administrators can make those choices here.

To modify any of the available components, do the following:

1. Select a feature from the list in the left pane.
2. Edit the description in the Description box.
3. Configure whether the feature should display on the Custom Installation screen by setting Visible drop down list:
   - Visible and Collapsed
   - Visible and Expanded
   - Not Visible
4. Set with the feature will be installed by setting the Initial State drop down:
   - This Feature will be installed on local hard drive
   - This Feature will not be available

   Tip: If you specify an Interactive installation and the Features setting is Visible, the user will be able to change the initial state.
2.5 Files and folders

The Customization Wizard contains a list of files to be installed by the installer. You can add or remove files from the installation list. Files are stored in the transform (.mst) file associated with the project. Any changes you make are recorded in the EnterpriseFiles table.

Files and Folders settings allow you to open a directory of files and folders on an already configured machine so that existing resources can be copied to the destination system during the install. You can add or remove files from the installation list and modify file records. This feature is particularly useful when migrating to a newer version. For example, you can leverage existing assets such as:

- Company-wide address books
- Custom plugins
- Fonts
Customizing the Installer

Adding and removing files and folders

- JavaScripts
- Templates
- Watermarks and signature logos
- Redaction code sets
- Anything!

**Caution:** As usual, Adobe strongly recommends that you do not make changes to the Files and Folders feature unless you are knowledgeable about editing and troubleshooting Microsoft Windows file lists. Improper use of this feature can result in the corruption of critical system files.

**Note:** Large files will inflate the binary table of the transform and the installer may take a long time to load.

### 2.5.1 Adding and removing files and folders

1. Choose the Modify tab.
   
   The main work area contains four panes. The upper-left pane contains the directory tree for the source computer, which contains the installation files. The lower-left pane contains the directory tree for the installation files to be installed by the installer on the destination system.

2. Navigate to a directory in the upper-left pane to view its contents in the upper-right pane.

3. Verify you can see the files or folders you want to add in the upper-right pane.

4. Select one or more files or folders in the source directory, and drag it to the destination directory.
   
   The added items will appear as red icons (Figure 10) and will be itemized in the Summary tab.

**Removing a default or custom files from the installation list**

Removing a file deletes the data table entry and prevents the item from being installed.

To remove a default file:

1. Navigate to the directory in the lower left hand pane.

2. Right click on the file in the lower right hand pane.

**Figure 10 Viewing files to install**

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>template1.pdf</td>
<td>16 KB</td>
</tr>
<tr>
<td>template2.pdf</td>
<td>29 KB</td>
</tr>
<tr>
<td>template3.pdf</td>
<td>26 KB</td>
</tr>
</tbody>
</table>

Customization Wizard for the Acrobat Family of Products. © 2010 Adobe Systems Inc.
3. Choose **Modify**.

**Figure 11** Modifying and removing default files

![Modify Record dialog box](image)

4. Select **Install file** or **Remove file** from the Action list.

5. In the Binary source field, click the **Browse** button, and then select a binary source file.

   **Tip:** The Binary source field allows you to provide a different source the file in the File name text box.

6. Choose **OK**.

### 2.5.2 Viewing a list of changes file and folder changes

The Summary tab contains a list of files on the source computer that you have added to or removed from the destination directory.

1. Choose the Summary tab. A list of installation files that you have added or removed appears.

2. **Optional:** To change a file record, right-click the file name, and select **Modify**. In the Modify record dialog box, you can rename files and add or remove them from the installation list.

   You can also modify files from this page in the same way as described in **Removing a default or custom files from the installation list**.

**Figure 12** Summary view of file and folder changes

![Summary view of file and folder changes](image)
2.5.3 Use case: Deploying digital signature files

1. Click on Files and Folders to open a directory of files on the source computer that enables copying existing files to the destination system. You can add or remove files from the installation list and modify file records. Copy preconfigured files from an existing installation from the top window to the appropriate folder in the bottom window under Destination Computer.

2. Copy needed files. Paths vary by application, version, and user. For example, on Windows XP, drag and drop all acrodata files from C:\Documents and Settings\<user name>\Application Data\Adobe\Acrobat\<application version>\Security to CommonAppDataFolder\Adobe\<application>\<version>\Replicate\Security. Acrodata files could include:
   - **addressbook.acrodata**: Populates the Trusted Identity Manager with certificate data. This file can be used to distribute a trust anchor for signature validation.
   - **directories.acrodata**: Populates the directory server list in the Security Settings Console. This file can be used to configure connections to an LDAP server used as a certificate repository.
   - **Appearances.acrodata**: Stores signature appearances. Unless there is a shared company appearance, do not use this file.
   - **security-policy.acrodata**: Populates the security policy list in the Security Policy Manager. This file can be used to distribute common document security policies.

3. Copy other needed files to a custom or existing directory. For example, expand the Destination Computer directory ProgramFileFolder\Adobe\Acrobat <application version>\Acrobat\ and create a new folder called Security. Some common files that may be distributed this way include:
   - **SignatureLogo.pdf**: To create a watermark or logo on each employee signature, create the logo and manually copy the file to the Documents and Settings Directory under their username.
   - **PKCS#11 drivers**: If you use smart cards, you can distribute drivers that end users can import via the Security Settings Console.
   - **Custom security handlers**: If you have developed a custom handler for signing or document security, install it in the application’s plugin directory.

   **Note**: The tuned installer will copy these files to the matching location.

2.6 Registry

The Registry feature allows you to leverage existing installations and simplify new ones by simultaneously displaying the registry from the host machine (called the “source”) next to the registry provided by the installer (called the “target”). This powerful feature allows you to copy any setting from an existing installation directly into the new installer. In enterprise settings where the installation may be highly customized, the Registry feature can save time, prevent errors, and assure consistency across installations. Any changes you make are recorded in the EnterpriseRegistries table (Figure 13). The following is supported:
2.6.1 Registry workflow overview

While the Wizard’s user interface (GUI) provides a visual way to configure the registry, it does have limitations. It only provides basic configuration options, its GUI is not identical to the product GUI, and using the Wizard’s GUI to set preferences will result in overwriting existing registry settings that you might drag and drop from your template application. For these reasons, power users—those with extensive experience modifying the registry and who are familiar with the products advanced features—may want to utilize a more manual process. A feature rich deployment workflow involves the following:

1. Install the new application (or use an already configured existing installation).

2. Configure the application via its user interface. In particular, go through the menus under **Edit > Preferences**.

   **Tip:** UI configuration modifies, files, installer properties, and the registry. There are dozens of registry preferences that you can use to control, feature access, workflows, certificate processing, data handling, communications with others servers, and so on. Refer to the Preference Reference in Administrator’s Information Manager (AIM). AIM is an AIR application containing a database of preferences and other resources.

3. Lock down features so that settings can not be changed by end users. See the Preference Reference for available options.

4. Use the Wizard to drag and drop the configured template registry to the installer. You can copy individual keys or entire cabs (directories) of keys. Please note that there are differences in
5. View the Summary tab to inspect a list of your change.
6. Use the Wizard to configure application preferences not already configured manually.

2.6.2 Adding keys

Adding registry keys from an existing registry

1. Choose the Modify tab (Figure 14).
   The main work area contains four panes. The upper-left pane contains the directory tree containing the registry keys on the source computer. The lower-left pane contains the directory tree for the registry hives to be installed by installer on the destination system.
2. Navigate to a directory in the upper-left pane to view its contents in the upper-right pane.
3. Verify you can see the keys you want to add in the upper-right pane.
4. Select one or more keys the source directory, and drag it to the destination directory.

Adding new registry keys

To add a new registry key to the destination directory:
1. Choose the Modify tab.
2. Select a location in the requisite registry hive in the lower left-hand panel.
3. **Optional**: If you’re creating a new folder, right click and choose **New** and enter a name. The added items will appear as red icons and will be itemized in the Summary tab.

4. Highlight the hive in which you will add the new key.

5. In the right pane, right click and choose **New > <data type> Value**.
   - String Value
   - Binary Value
   - DWORD Value
   - Multi-String Value
   - Expandable String Value

   **Tip:** Data types and registry configuration are described in detail in the Enterprise Administration Guide at [http://kb2.adobe.com/cps/837/cpsid_83709/attachments/Acrobat_Enterprise_Administration.pdf](http://kb2.adobe.com/cps/837/cpsid_83709/attachments/Acrobat_Enterprise_Administration.pdf).

6. Create a value with the required name.

7. Right click on the new value.

8. Choose **Modify**.

9. Set **Value Data** as required.

10. Choose **OK**.

   To see a list of changes that you have made, click the Summary tab.

### 2.6.3 Modifying existing keys

The Wizard provides a context menu that’s identical to the Window’s registry. To modify a new or existing registry key:

1. Right-click the key name.

2. In the context menu, select Rename, Delete, or Modify.

3. Make your modifications.

4. Choose **OK**.

   To see a list of changes that you have made, click the Summary tab.

### 2.6.4 Summary

The Summary tab contains a list of registry keys you have added, modified, or removed from the destination directory.

1. Choose the Summary tab. Your list of registry changes appears.
2. **Optional**: To change a key, right-click the key, and select **Modify**. In the Modify record dialog box, you can rename keys and add or remove them from the installation list.

### 2.7 Shortcuts

The Shortcuts settings allow you to open a directory of program shortcuts available from the Windows Start menu and on the desktop. By default, the installer creates shortcuts to installed programs on the Windows Start menu and on the desktop. You can add, remove, or restore shortcuts to installed programs on the destination system.

**Note:** If an option appears dimmed, it is unavailable.

#### Figure 15 Installer table modifications: Shortcuts

<table>
<thead>
<tr>
<th>Tables</th>
<th>Shortcut</th>
<th>Directory</th>
<th>Name</th>
<th>Component</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SC_READER_PFM</td>
<td>ProgramMenu</td>
<td>ADOBER...</td>
<td>Reader_Bin_Acr...</td>
<td>ReaderProgram...</td>
</tr>
<tr>
<td></td>
<td>SC_READER_DT</td>
<td>DesktopFolder</td>
<td>ADOBER...</td>
<td>Reader_Bin_Acr...</td>
<td>[INSTALLDIR]Re...</td>
</tr>
</tbody>
</table>

The following operations are available:

- **Removing a shortcut**: Right-click the shortcut from the Windows Start menu or on the desktop, and then select **Remove**. The shortcut is marked with a red X to indicate that it has been removed.
- **Restoring a shortcut**: that you removed, right-click a shortcut marked with a red X, and then select **Restore**.
- **Adding a folder to the Start menu**: Right-click a folder, and then select **New Folder**. Type a folder name.
- **Creating a shortcut**: Right-click the new folder you added, point to **Add shortcut**, and then select a program name from the list.
- **Deleting a folder**: Right-click a folder you added, and then select **Remove**.
- **Renaming a folder**: Right-click the folder you added, and then select **Rename**.

#### Figure 16 Shortcuts
2.8 Server locations

The Server Locations settings allow you to configure additional server location paths to ensure source resiliency for the Windows installer package. You can add, rearrange, or remove locations. This feature sets the SOURCELIST property which is a semicolon-delimited list of network or URL source paths to the installation package which is appended to each user’s existing source list. The installer uses the first accessible location it finds and only this source is used for the remainder of the installation. Therefore, each item in SOURCELIST must contain:

- A complete source for the application, including all files and cabinets.
- The entire directory tree at each source location must be the same.
- An .msi file with the same file name and product code.

**Note:** The installer only checks the SOURCELIST property if the product has not already been advertised or installed. In all other cases the installer uses the existing source list in the registry.

**Figure 17 Installer table modifications: SOURCELIST property**

<table>
<thead>
<tr>
<th>Tables</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MsiPatchCertificate</td>
<td>ReinstallModeText</td>
<td>omus</td>
</tr>
<tr>
<td>MsiSFCBypass</td>
<td>CloseRestart</td>
<td></td>
</tr>
<tr>
<td>ProgramID</td>
<td>RUNTIMEProperties</td>
<td>CACHE_DIR;ProductName;OriginalDatabase;REMOVE...</td>
</tr>
<tr>
<td>Property</td>
<td>SOURCELIST</td>
<td>(\MyNetworkShare</td>
</tr>
<tr>
<td>RegularButton</td>
<td>SYNCHRONIZER</td>
<td>YES</td>
</tr>
<tr>
<td>Registry</td>
<td>SecureCustomProperty</td>
<td>DEFAULT_VERB;ACTIONPROPERTY;ELEMENTS;RDRM...</td>
</tr>
</tbody>
</table>

**Add a server location**

1. Choose Add Location.

2. Do one of the following:
   - Choose Browse, navigate to the directory, and then click OK.
   - Choose the new line in the Additional Server Location Paths list, and then type a complete path to the server directory.

**Note:** If a server is not available or the location is invalid, the installer will ignore the entry.

**Rearrange server locations**

The order of the server locations in the list determines the order in which the installer accesses the servers. If there is more than one server in the list, change the order as follows:

1. Select a server location from the list.

2. Choose the Up and Down arrows on the right to rearrange the server within the list.

**Remove server location**

To remove a server location:

1. Select the server location from the list.
2. Choose **Remove Location**.

### 2.9 Distiller

This feature is not available in Reader.

Distiller settings allow you to specify options for creating a .joboptions file. You can add or remove PDF creation settings and change the default selection. This feature modifies the EnterpriseFiles table as follows:

- The FilePath ALL_USERS_PDFOPTIONS_SETTINGS by default resolves to AllUsersProfileAppData\Adobe\Acrobat\{version}\Distillr\Settings where AllUsersProfileAppData is usually C:\Documents and Settings\All Users\Application Data.

- Action values may be:
  - 2: Add and backup
  - 4: Remove

**Figure 18** Installer tables: Enterprise files for Joboptions

<table>
<thead>
<tr>
<th>Tables</th>
<th>EnterpriseFile</th>
<th>Feature</th>
<th>FileName</th>
<th>FilePath</th>
<th>Ac...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog</td>
<td>834BF06D-D368</td>
<td>AdobePDFfileCS</td>
<td>ADPDF8C5.PPD</td>
<td>[PrinterDriver]\</td>
<td>0</td>
</tr>
<tr>
<td>Directory</td>
<td>8F218F6A-579D</td>
<td>AdobePDFileCT</td>
<td>ADPDF8C1.PPD</td>
<td>[PrinterDriver]\</td>
<td>0</td>
</tr>
<tr>
<td>DrLocator</td>
<td>9F14D355-897E</td>
<td>AdobePDFileJ</td>
<td>ADPDF8J.PPD</td>
<td>[PrinterDriver]\</td>
<td>0</td>
</tr>
<tr>
<td>DuplicateFile</td>
<td>03BB4133-6E7F</td>
<td>AdobePDFileK</td>
<td>ADPDF8K.PPD</td>
<td>[PrinterDriver]\</td>
<td>0</td>
</tr>
<tr>
<td>EnterpriseFile</td>
<td>0363D961-C47D</td>
<td>Setup.INI</td>
<td>Setup.INI</td>
<td>[INSTALLDIR][</td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>4595D854-2D96</td>
<td>Redaction</td>
<td>U.S. F0JA.xml</td>
<td>[REDACTIO...\</td>
<td>0</td>
</tr>
<tr>
<td>EventMapping</td>
<td>087693FE-C1C7</td>
<td>Redaction</td>
<td>U.S. Privacy Act..xml</td>
<td>[REDACTIO...\</td>
<td>0</td>
</tr>
<tr>
<td>Extension</td>
<td>7F19D23E-FAE8</td>
<td>SecLDAPDirectories</td>
<td>directories.acradata</td>
<td>[ALLUSERS...\</td>
<td>0</td>
</tr>
<tr>
<td>Feature</td>
<td>0552E8ED-4C33</td>
<td>joboptions</td>
<td>CustomJobOptions.jobopt...</td>
<td>[ALL_USERS...\</td>
<td>2</td>
</tr>
<tr>
<td>FeatureComponen...</td>
<td>EC0580E2-3EA9</td>
<td>joboptions</td>
<td>POFXa 2001.joboptions</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
<tr>
<td>File</td>
<td>D2E216F4A-15B8</td>
<td>joboptions</td>
<td>Press Quality.joboptions</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
<tr>
<td>Font</td>
<td>D765E1E9-799F</td>
<td>joboptions</td>
<td>POFASb 2005 CMYK.joboptions</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
<tr>
<td>Icon</td>
<td>D636DFS3-0F67</td>
<td>joboptions</td>
<td>Standard.joboptions</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
<tr>
<td>InstallExecuteSe...</td>
<td>78A1820D-1F8E</td>
<td>joboptions</td>
<td>Smallest File Size.joboptions</td>
<td>[ALL_USERS...\</td>
<td>4</td>
</tr>
<tr>
<td>InstallUISequence</td>
<td>863AFE23-5E57</td>
<td>joboptions</td>
<td>MAGAZINE Ad 2006 JPN.j...</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
<tr>
<td>ISCComponentEx...</td>
<td>755F30AD-BBD7</td>
<td>joboptions</td>
<td>POFX3 2002.joboptions</td>
<td>[ALL_USERS...\</td>
<td>0</td>
</tr>
</tbody>
</table>

**Add a job option**

To add PDF creation settings (.joboptions) to the installation:

1. Choose the **Add** button.
2. Navigate to the settings file you want to add.
3. Choose **Open**.

**Note:** The default directory for PDF settings .joboptions files is C:\Documents and Settings\All Users\Application Data\Adobe\Adobe PDF\Settings.
**Set a default joboptions file**

The default PDF creation settings file is highlighted in red. To change the default file:

1. Select a file from the Adobe PDF Settings list.
2. Choose **Set as Default**.

**Note:** The default value is stored in the EnterpriseRegistries table as DistillerDefJobOptions which sets HKCU\SOFTWARE\Adobe\Acrobat Distiller\<version>\JobOptions.

**Remove a joboptions file**

To remove a joboptions file from the installation:

1. Select the file you want to remove.
2. Choose **Remove**.

---

**2.10 Adobe PDF printer**

Adobe PDF Printer settings allow you to display the printer options for Adobe PDF output and PostScript files and specifies the default PostScript Printer Description (PPD) file. These settings modify the EnterpriseRegistries tables and registry as shown in Table 4.

**Note:** The registry root path to these keys is HKLM\SOFTWARE\Adobe\Acrobat Distiller\10.0\.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
<th>Installer table name</th>
<th>Registry path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default PDF Output Folder</td>
<td>C:\My PDF Output</td>
<td>DistillerDefPDFOutput</td>
<td>DefaultPDFOutput</td>
</tr>
<tr>
<td>Adobe PDF Output Folder</td>
<td>&lt;Default&gt;</td>
<td>PDFIniPromptForFileName</td>
<td>AdobePDF.INI\PromptForFileName</td>
</tr>
<tr>
<td>Adobe PDF Security</td>
<td>(Default) Reconfirm Security for each job (1)</td>
<td>PDFIniSecurityOption</td>
<td>AdobePDF.INI\SecurityOption</td>
</tr>
<tr>
<td>TrueType Font Download Option</td>
<td>(Default): Outline (1)</td>
<td>PDFIniTrueTypeFontDL</td>
<td>AdobePDF.INI\True Type Font Download Option</td>
</tr>
<tr>
<td>PostScript Output Options</td>
<td>(Default) Optimize for Portability (1)</td>
<td>PDFIniPSOutputOption</td>
<td>AdobePDF.INI\PostScript Output Option</td>
</tr>
</tbody>
</table>

Customization Wizard for the Acrobat Family of Products. © 2010 Adobe Systems Inc.
Default PDF Output Folder

You can specify a default folder which will appear in the Adobe PDF Output Folder drop down list (below).

To set a default folder, do one of the following:

- Enter a new path in the Default PDF output folder textbox, or
- Choose Browse, navigate to the folder you want to use, and then select Open.

**Note:** The default output folder name must reside on all users' systems.

Adobe PDF Output Folder

Specify a folder for saving newly created PDF files by choosing an option in the Adobe PDF Output Folder drop down list:

- `<Default PDF Output Folder>` (contains the value you’ve set above).
- Prompt for Adobe PDF filename

Adobe PDF Security

Set the security level for PDF documents by choosing an option in the Adobe PDF Security drop down list:

- None
- Reconfirm Security for Each Job
- Use the Last Known Security Settings

**Tip:** Security methods include password, certificate, and Adobe LiveCycle Rights Management Server security. For more information on applying security to documents, see the Rights Management guide in the content security library at http://learn.adobe.com/wiki/display/security/Document+Library.

TrueType Font Download Option

To set TrueType behavior, choose one of the following in the TrueType Font Download Option drop down list:

- Automatic
- Online
Customizing the Installer Adobe PDF printer

- Bitmap
- Native TrueType

After installation, the TrueType setting appears in the printer properties dialog box. To view the settings:

1. Choose Start > Printers and Faxes.
2. Right-click the Adobe PDF printer.
3. Choose Properties > Advanced tab.
5. Choose the Paper/Quality tab.
6. Choose Advanced.
7. Under Document Options expand PostScript Options to view the TrueType Font Download Option.

**Tip:** It’s possible that the method may vary by operating system.

**PostScript Output Option**

To set PostScript output behavior, choose one of the following in the PostScript Output Option drop down list:
- Optimize for Speed
- Optimize for Portability
- Encapsulated Postscript
- Archive Format

1. Choose Start > Printers and Faxes.
2. Right-click the Adobe PDF printer.
3. Choose Properties > Advanced tab.
5. Choose the Paper/Quality tab.
6. Choose Advanced.

**View Adobe PDF results**

Select the check box to open the output file when it is created.

**Ask to replace existing PDF file**

Select the check box to alert the user that a PDF file of the same name exists.
Add document information
Select the check box to record information about the file when it is created.

Rely on system fonts only; do not use document fonts
Select the check box to restrict the use of fonts.

2.11 Security
The configuration options here deal with both content security features such as digital signatures and certificate security as well as application security features such as enhanced security. For complete details and configuration guides, refer to the security library at http://learn.adobe.com/wiki/display/security/Home.

2.11.1 Directory servers
Acrobat products ship with preconfigured directory servers stored in a directories.acrodata file. The servers are used by the Trusted Identity Manager to locate certificates used in digital signature and certificate security workflows. Users can trust these certificates for signing and certifying documents as well as for encrypting documents prior to sending them to the certificate owner. In enterprise settings, certificates are stored on a directory server so thereby providing users with a searchable and already trusted set of trusted identities.

If your company uses a centrally managed certificate repository such as an LDAP directory server you can add preconfigured server information to the installer. To do so:

1. In the Directory Servers field, choose Set.

2. By default, the Wizard opens the Security directory for the currently logged on user. Select the directory server file (directories.acrodata) or navigate to another file.

   [ALL_USERS_PROFILE]\Application Data\Adobe\<product name>\<version>\Replicate\Security.

3. Choose Open.
   The text box displays a message that this feature has been set.
   
   **Note:** If you select a file name other than directories.acrodata, the file will be renamed.

Unsetting directory servers
To unset the directory server, choose Unset. The text box displays the message that this feature is not set.

**Tip:** You can also set these files with the Files and folders feature. Changes modify the EnterpriseFiles table (Figure 18).
2.11.2 Trusted identities

Acrobat products do not ship with trusted identity data. Enterprise IT will typically want to install a preconfigured `addressbook.acrodata` file which captures Lightweight Directory Access Protocol (LDAP) information for contacts and certificates. The certificates can be delivered as already installed trusted identities with specific levels of trust set for any or all certificates used in digital signature and certificate security workflows.

1. In the Trusted Identities field, choose **Set**.
2. By default, the Wizard opens the Security directory for the currently logged on user. Select the directory server file (`addressbook.acrodata`) or navigate to another file.
   
   `[ALL_USERS_PROFILE]\Application Data\Adobe\<product name>\<version>\Replicate\Security`.
3. Choose **Open**.
   
   The text box displays a message that this feature has been set.

   **Note:** If you select a file name other than `addressbook.acrodata`, the file will be renamed.

   **Tip:** You can also set these files with the Files and folders feature. Changes modify the EnterpriseFiles table (Figure 18).

**Unsetting trusted identities**

To unset the trusted identities, choose **Unset**. The text box displays the message that this feature is not set.

2.11.3 Enhanced security

Enhanced security is part of the security model introduced in version 9.1. Adobe recommends as a best practice that you enable enhanced security to prevent unrestricted cross domain access and other potentially risky behavior. Workflows and content should be designed to operate in the context of enhanced security enabled.

Enhanced security is enabled by default for the 9.3 and 8.2 updates. Its configuration and behavior is nearly identical across platforms and whether or not you are viewing a PDF within a browser or within a standalone application. See the “Enhanced security quick key” for a one page overview. For more detail, see the Application Security Guide in the online Application security library and the Preference Reference in the Administrator’s Information Manager (AIM).

**Tip:** Due the complexity and critical nature of these settings, installations should leverage existing configurations via the Registry feature.

2.11.3.1 Standalone and browser behavior

Depending on how a PDF is opened, the PDF viewer may be a standalone application or may be opened within a browser. Settings may be configured separately for both cases. By default, enhanced security is enabled.

To specify a custom setting, set the Standalone and/or Browser drop down lists to one of the following:

- **Enable:** Enhanced security is on but users can change the setting.
Customizing the Installer

Enhanced security

- **Enable & Lock**: Enhanced security is on but the UI is locked so that users can't change the setting.
- **Disable**: Enhanced security is off but users can change the setting.
- **Disable & Lock**: Enhanced security is off but the UI is locked so that users can't change the setting.

Disabling and enabling enhanced security toggles the keys shown in Example 2.1. Locking the setting sets a key in HKLM that's only available to administrators. For more registry details, see the Application Security Guide in the online Application security library.

Example 2.1: Registry configuration: Enhanced security enabled

```
[HKEY_CURRENT_USER\Software\Adobe\<product>\<version>\TrustManager]
bEnhancedSecurityInBrowser"=dword:00000001
"bEnhancedSecurityStandalone"=dword:00000001
```

Example 2.2: Registry configuration: Locking enhanced security settings

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\(product)\(version)\FeatureLockDown]
bEnhancedSecurityStandalone"=dword:00000001
"bEnhancedSecurityInBrowser"=dword:00000001
```

Tip: You may also want to use the Registry feature to prevent end users from disabling the application from trusting sites trusted by IE. To do so, set:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\(product)\(version)\FeatureLockDown]
bDisableOSTrustedSites"=dword:00000001
```

2.11.3.2 Specifying trusted, “privileged” locations

Enhanced security is specifically designed to let you decide what content to trust and help you selectively bypass its restrictions for trusted files, folders, and hosts. These trusted domains--called privileged locations--are exempt from enhanced security rules.

Figure 19 Privileged locations panel

| Trusted File, Folder or Host | Cross Domain Violations | PDF Script Injection | Data Injection | Elevated Javascript | External Content | Silent Printing | WebLink | Recursive |
|-----------------------------|-------------------------|---------------------|---------------|---------------------|-----------------|----------------|---------|
|                             |                         |                     |               |                     |                 |                |         |           |

Note: Different Trusted objects appear in different colors: Files, Folders and Hosts

- Add File
- Add Folder
- Add Host
- Browse...
- Remove

- Prevent end-user to add trusted Files and Folders.
- Prevent end-user to add trusted Hosts.
To add a trusted location:

1. Choose **Add File**, **Add Folder**, or **Add Host**.
2. Enter a value or browse to the location.
3. Set the trust levels in the columns to the right of an object, double-click a cell and select a value in the list. Note that trust for hosts is recursive by default.

**Tip:** Wizard settings set the values under `[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\(product)\(version)\FeatureLockDown]cTrustedFolder` or `cTrustedSites`.

To remove a trusted object, select the trusted location and choose **Remove**.

**Differences between the application UI and the Wizard**

The Wizard contains some functional differences from what can be done by users via the application UI:

- Privileged location configuration via the application UI sets the keys shown in **Example 2.3**. The Wizard sets all privileged locations in HKLM under `FeatureLockdown\(cTrustedFolders | cTrustedSites)`.
- The Wizard does not provide an option for setting `cAlwaysTrustedForJavaScript` and `cJavaScriptURL` except via the **Registry** feature.
- The Wizard does provide an option for setting `cJavaScript` which is not provided by the application UI.

**Example 2.3: Registry keys set by trusting locations in the product UI**

```
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders]
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cCrossdomain]
  "t3"="(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cAlwaysTrustedForJavaScript]
  "t3"="(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cJavaScriptURL]
  "t3"="(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cDataInjection]
  "t6"="C:\(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cExternalStream]
  "t4"="C:\(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cScriptInjection]
  "t5"="C:\(someFile)"
[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\TrustManager\cTrustedFolders\cSilentPrint]
```
2.11.3.3 Preventing end users from trusting locations

To determine whether end-users can add trusted objects, select or clear the following check boxes:

- **Prevent end-user to add trusted Files and Folders.** This feature locks the user interface by setting:
  
  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\{product}\{version}\FeatureLockDown]
  "bDisableTrustedFolders"=dword:00000001
  ```

- **Prevent end-user to add trusted Hosts.** This feature locks the user interface by setting:
  
  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\{product}\{version}\FeatureLockDown]
  "bDisableTrustedSites"=dword:00000001
  ```

2.11.4 Examine document

This feature is only available in Acrobat.

The Remove Hidden Information dialog box configures the Examine Document feature. This feature identifies hidden document information and allows the user to remove selected items:

To display the Examine document dialog box when closing Acrobat, select the **Examine document when closing document**. The Wizard creates or modifies the following registry key:

**Example 2.4: bAutoLaunchAtDocClose**

```
[HKEY_CURRENT_USER\Software\Adobe\{product}\{version}\Security]
"bAutoLaunchAtDocClose"=dword:00000001
```  

To display the Examine document dialog box when sending e-mail, select **Examine document when sending document by email**. The Wizard creates or modifies the following registry key:

**Example 2.5: bAutoLaunchAtSendMail**

```
[HKEY_CURRENT_USER\Software\Adobe\{product}\{version}\Security]
"bAutoLaunchAtSendMail"=dword:00000001
```  

2.12 Digital signatures

Digital signatures features are only available in Reader for documents that have been rights enabled by a document author that has selected **Extend Features in Adobe Reader** or by a LiveCycle server. Acrobat users can take full advantage of all the available signature capabilities. For more detail about dozens of other available options, see the digital signatures guide in the content security library at [http://learn.adobe.com/wiki/display/security/Document+Library](http://learn.adobe.com/wiki/display/security/Document+Library).
2.12.1 Signature validation

To configure, do the following

1. Set the Default Verification Method to one of the following:
   - Use the document-specified method. Prompt if it is not available.
   - Use the document-specified method. Use the default method if it is not available.
   - Always use the default method (overrides the document-specified method).

   In some enterprise situations administrators may require a method other than Adobe Default Security. For example, non-Adobe plugins may be used in business environments that require support of biometrics, signature escrow, alternative methods of private key access, and so on. In those cases, administrators may specify an alternate plugin or provide user training on how to choose the right one. This setting sets:

   \[
   \text{HKLM\SOFTWARE\Policies\Adobe\product\version\FeatureLockDown\cSecurity\cHandlers}\n   \text{"aPrivKey"="Adobe.PPKLite"}\n   \text{"aVerify"="Adobe.NoHandler"}\n   \text{"bVerifyUseAlways"=dword:00000000}\n   \]

2. Lock Default Verification Method by checking the Disallow user to modify. This setting sets:

   \[
   \text{HKLM\SOFTWARE\Policies\Adobe\product\version\FeatureLockDown\cSecurity\cHandlers\bVerifyUseAlways}\n   \]

3. Set whether you want to automatically Verify signatures when the document is opened. This setting sets:

   \[
   \text{HKCU\Software\Adobe\product name\version\Security\cDigSig\bValidateOnOpen}\n   \]

4. Lock automatic signature verification by choosing Prevent user from modifying this setting. This setting sets:

   \[
   \text{HKLM\SOFTWARE\Policies\Adobe\product\version\FeatureLockdown\Security\cDigSig\bValidateOnOpen}\n   \]

2.12.2 Signing method

To configure, do the following:

1. Set the Default Signature Method to one of the following:
   - Adobe Default Security
   - Ask when I sign
   - Third party

   Sets \text{HKCU\Software\Adobe\product name\version\Security\cHandlers\aPrivKey}

2. Lock Default Signature Method by checking the Disallow user to modify checkbox.

   Sets \text{HKLM\SOFTWARE\Policies\Adobe\product\version\FeatureLockDown\cSecurity\cHandlers\bPrivKey}. 

Tip: Due the complexity and critical nature of these settings, installations should leverage existing configurations via the Registry feature.
3. Check **Show location and contact information when signing** if you would like the **Location** and **Contact Info** fields to appear in the signing dialog during signing. The data is then added to the signature block after signing.

Sets HKCU\Software\Adobe\(product name)\(version)\Security\cPubSec\bAllowOtherInfoWhenSigning.

4. Set **Enable reviewing of document warnings** to allow signers to check document integrity prior to signing. The document can be analyzed to determine if it contains any content that could adversely impact the integrity of the signing process. For example, a document could contain JavaScript that could change a data field before or after a signature is applied.

- Never
- When Certifying only
- Always

Sets HKCU\Software\Adobe\(product name)\(version)\Security\cDigSig\iRequireReviewWarnings.

5. Set **Prevent signing until document warnings are reviewed** to force a review of document warnings.

   **Note:** **Enable Reviewing of Document Warnings** and **Prevent signing until document warnings are reviewed** settings function in tandem and should be set together. Setting both these options to **Always** results in the highest degree of assurance that the signing process is not adversely impacted by malicious content.

Sets HKCU\Software\Adobe\(product name)\(version)\Security\cDigSig\iRequireReviewWarnings.

6. Set **Prevent users from certifying without visible signatures**. Selecting this option prevents the use of invisible certification signatures.

Sets HKCU\Software\Adobe\(product name)\(version)\Security\cDigSig\bAllowInvisibleSig.

7. Set **Show reasons when signing**. Enabling this option results in a **Reasons** field appearing in the signing dialog. The signer can then choose a default reason such as “I have reviewed this document” or create a new one.

Sets HKCU\Software\Adobe\(product name)\(version)\Security\cPubSec\bAllowReasonWhenSigning.

8. Lock **Show reasons when signing** by choosing **Prevent user from modifying this setting**.

Sets HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockdown\cSecurity\cPubSec\bReasons.

---

### 2.13 Rights management servers

To specify the Adobe LifeCycle Rights Management Servers (ALCRM) used by the installed application, do one or more of the following:

**Add an ALCRM Server**

To add a rights management server:
1. Enter the server name.
   Sets HKCU\Software\Adobe\(product name)\(version)\Security\cEDC\cKnownServers\tName.

2. Enter the server URL.
   Sets HKCU\Software\Adobe\(product name)\(version)\Security\cEDC\cKnownServers\tURL.

3. Choose Add.

**Remove an ALCRM Server**

1. Select the server in the list.

2. Choose Remove.

**Set a default ALCRM Server**

To set a default server:

1. Select the server in the list.

2. Choose Set as default.

   The default server is highlighted in Red and its details are stored in:

   \[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\Security\cEDC\]
   "tServerURL"="SomeURL"
   "tServerName"="SomeName"

**Lock ALCRM Server settings**

To suppress user configuration of a rights management server in Acrobat, check Prevent Rights Management Server from being configured via Acrobat.

Sets HKLM\SOFTWARE\Policies\Adobe\(product)\(version)\FeatureLockDown\cSecurity\cEDC\bAllowAPSCOnfig.

### 2.14 3D support

This feature is only available in Acrobat 3D and Acrobat Extended.

To disable support for the PRC or U3D 3D file formats in the installed application, do one or more of the following:

- **PRC format support**: Select the Disable all PRC support check box. This options sets:
  \[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\comAdobeAcromanImport3D]\bdisable_u3d_all

- **U3D format support**: Select the Disable all U3D support check box.
  \[HKEY_CURRENT_USER\Software\Adobe\(product)\(version)\comAdobeAcromanImport3D]\bdisable_prc_all

To disable PRC and U3D format support for specific file types:
1. Select a file extension in the list.

2. Select the Disable PRC support, Disable U3D support, or both check boxes.
   This feature sets one or more of the following keys for each selected file type:

   \[HKEY_CURRENT_USER\Software\Adobe\{product\}\{version\}\comAdobeAcromanImport3D]\bdisable_prc_com_adobe_acroman_<file extensions>

   or

   \[HKEY_CURRENT_USER\Software\Adobe\{product\}\{version\}\comAdobeAcromanImport3D]\bdisable_u3d_com_adobe_acroman_<file extensions>

### 2.15 EULA

You can suppress the display of the EULA and automatically accept the agreement on behalf of your company for every installation that references the current .msi file.

This feature sets the EULA_ACCEPT property.

To accept the EULA and suppress its display to end users:

1. Choose **Display EULA**. The EULA opens in a new window.

2. After reading the EULA, choose the **Close** button in the upper-right corner to return to the Customization Wizard.

3. Check **Suppress display of End User License Agreement (EULA)**.

   **Caution:** By choosing this option, you accept the terms of the EULA on behalf of your organization.

### 2.16 Online and Acrobat.com features

#### 2.16.1 Online feature integration

To disable online features, such as automatic updates and registration of software, select one or more check boxes in the Online Features list. To retain a feature clear the check box.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable all updates</td>
<td>The Check for updates command on the Help menu is unavailable.</td>
</tr>
<tr>
<td></td>
<td>Sets [HKLM\SOFTWARE\Policies\Adobe{product name}{version}\FeatureLockDown]\bUpdater=dword:00000000</td>
</tr>
</tbody>
</table>
To disable access points to Acrobat.com services, such as initiation of live collaboration and shared reviews, select one or more check boxes in the Acrobat.com list. To retain a service, clear the check box.
Table 6 Controls for Acrobat.com integration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable all Acrobat.com access, including initiation and participation</td>
<td>Disables all access points to Acrobat.com services. Sets the Action field for all the keys below to 4.</td>
</tr>
<tr>
<td>Disable only initiation of shared review and forms</td>
<td>(Acrobat only) Commands to initiate shared reviews and forms are unavailable. Sets HKCU\Software\Adobe(product)\10.0\Workflows\bEnableDocCtrInit</td>
</tr>
<tr>
<td>Disable initiation of live collaboration and screen sharing</td>
<td>Commands to initiate live collaboration and screen sharing are unavailable. Sets HKCU\Software\Adobe\Acrobat Reader\10.0\Workflows\bEnableRTCAuth</td>
</tr>
<tr>
<td>Disable only Upload and Share documents to Acrobat.com</td>
<td>The end-user cannot use Acrobat.com to upload and share documents. Sets HKCU\Software\Adobe(product)\10.0\Workflows\bEnableShareFile</td>
</tr>
</tbody>
</table>

2.17 Comments and forms

The Comments and Forms settings allow you to specify the options for forms auto-complete and shared reviews servers:

2.17.1 Forms auto-complete

You can select the options for forms auto-complete and prevent the end-user from modifying these settings.

To choose the forms auto-complete options:

1. Select one of the following options from the Auto-Complete list:
   - Off
   - Basic: Sets HKCU\Software\Adobe\Acrobat Reader\10.0\FormsPrefs these keys:
     - bInlineAutoComplete
     - bRecordsNewEntries
     - bShowDropDown
     - bUserAskedToEnableAutoComplete
   - Advanced: Sets HKCU\Software\Adobe\Acrobat Reader\10.0\FormsPrefs these keys:
     - bInlineAutoComplete
     - bRecordsNewEntries
     - bShowDropDown
2.17.2 Shared reviews servers

This feature is not available in Reader.

The Shared Reviews feature offers enhanced document-sharing functionality across network servers. The Shared Reviews Servers Settings list contains the names, types, and addresses of the currently configured shared reviews servers. You can control shared reviews, add a server to the list, and remove a shared reviews server from the list. The executable file for Shared Reviews Servers is synchronizer.exe.

To control user access to shared reviews:

1. Check or uncheck **Disable Shared Reviews and Reviews/Forms workflows**. When this setting is checked, synchronizer.exe will not run. This control sets the following key:

   HKCU\Software\Adobe\<product name>\<version>\Workflows\"bNeedSynchronizer"=dword:00000000

2. Add a shared reviews server to the Shared Reviews Servers Settings list:
   1. In the Add Shared Review Server area, type a server name in the Server Name box. Sets:
      HKCU\Software\Adobe\(product)\10.0\Collab\cReviewServers\c\UI
   2. Select one of the following server types from the Server Type list:
      - Network Folder: This option allows you to specify the server path by choosing **Browse**, navigating to the network folder, and then choosing **OK**.
      - WebDAV
      - SharePoint

      Sets HKCU\Software\Adobe\(product)\10.0\Collab\cReviewServers\c\cSetting
   3. Enter the server address in the Server Path or URL box. Sets:
      HKCU\Software\Adobe\(product)\10.0\Collab\cReviewServers\c\tURL

3. Select a **Distribution Method**:
   - Upload to server and send email with link
   - Send email with attachment
   - Save to local disk and send later manually

Tip: If you select either Basic or Advanced, you can specify whether the form will remember numerical data:

2. Check or uncheck **Remember numerical data** (e.g., telephone numbers) to enable forms to auto-complete numerical data. Sets:

   HKCU\Software\Adobe\Acrobat Reader\10.0\FormsPrefs\bStoreNumericEntries

3. To lock these controls so that end users can't change the setting, select the **Prevent user from modifying this setting in Edit > Preferences > Forms** check box. This feature sets:

   HKLM\Software\Policies\Adobe\Acrobat Reader\10.0\FeatureLockdown\bAutoFill
2.18 File attachments

The Acrobat family of products always allow you to open and save PDF and FDF file attachments. However, attachments represent a potential security risk because they can contain malicious content, open other dangerous files, or launch applications. Certainly file types such as .bin, .exe, .bat, and so on will be recognized as threats by most users and are not allowed as attachments.

For a complete guide to attachment configuration, see the Application Security Guide.

To mitigate the risk inherent in attachments:

- Know what the content is and from where it originated.
- Be aware of dangerous file types and how the application manages those types. Adobe applications maintain Black lists and white lists which control application behavior, and application behavior is controlled by the file type's membership in a list:
  - **File types on the white list**: These can be attached and may be opened or saved if the file extension is associated with the requisite program.
  - **File types on the black list**: These can be attached, but a warning dialog appears stating that they cannot be saved or opened from the application. No actions are available for these files.
  - **File types not on any list**: These can be attached without a warning dialog. Trying to open or save them invokes a dialog which allows the user to perform the action just once or to add them to the good type (white) list or bad type (black) list.
- Prevent attachments from opening other files and launching applications. This is the default behavior.

**Preventing documents from opening other files and applications**

To prevent users from opening or launching any file type other than PDF and FDF from a document opened in the application, check the Prevent document from opening other files and launching other applications check box. This disables the ability of the application to open attachments or launch other applications that will open those attachments.

This feature locks the setting so that it cannot be changed by end users by setting the following key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\(product)\(version)\FeatureLockDown]
"iFileAttachmentPerms"=dword:00000001
```
Modifying attachment black and white lists

To modify the level of user access to file types:

1. In the Add and Modify File Types (Extensions) list, scroll to the file type you want to modify.
2. Set the user access level when opening or launching the file type to one of the following:
   - Unspecified: Behavior is determined by the values selected for Specifying behavior for file types not on black and white lists.
   - Allowed: The tBuiltInPermList Value is set to 2.
   - Prohibited: The tBuiltInPermList Value is set to 3.

This feature modifies the following registry key:

```
HKLM\SOFTWARE\Policies\Adobe\<product name>\<version>\FeatureLockDown\cDefaultLaunchAttachmentPerms\tBuiltInPermList
```

PDF (documents) and FDF file extensions are always allowed. You cannot prohibit them or mark them as Unspecified.

Restoring default behaviors

To restore all of the changes you have made to the Add and Modify File Types (Extensions) list:

1. Choose Restore Defaults.
2. Choose Yes to confirm.

This feature modifies the following registry key:

```
HKLM\SOFTWARE\Policies\Adobe\<product name>\<version>\FeatureLockDown\cDefaultLaunchAttachmentPerms\tBuiltInPermList
```

Tip: The level of access for all default file types (except PDF and FDF) is set to Prohibited; any new file types that you added to the list are removed.

Specifying behavior for file types not on black and white lists

You can control user access to file types marked Unspecified or are not listed in the Add and Modify File Types (Extensions) list.

To specify user access to unspecified file types, select one of the following options:

- Prompt user without the ability to set the file type as Allowed
- Prompt user with the ability to set the file type as Allowed
- Never launch files of unspecified types

After installation, if the Prevent document from opening other files and launching other applications check box is selected, users do not have access to any other file types. Go to Preferences > Edit > Trust Manager and verify the PDF File Attachments options are unavailable.

This feature modifies the following registry key:

```
HKLM\SOFTWARE\Policies\Adobe\<product name>\<version>\FeatureLockDown\cDefaultLaunchAttachmentPerms\tBuiltInPermList
```
2.19 Launch other applications

Launch Other Applications allows you to specify additional applications to be installed along with the Acrobat product. You can specify both executable files or batch files that will run applications on the destination system(s) after the install product installation completes.

The feature modifies the EnterpriseLaunches table and writes to the Setup.ini file.

To add an application to the installation:

1. Choose **Add Application**.

2. Enter a complete path to the application in **Application Path** or choose **Browse** and navigate to the application.

   **Note:** If an executable file or batch file is not available or the location is invalid, the installer will ignore the entry.

3. Add any needed command line parameters to the application path by double-clicking the **Command Line** field and entering the parameter.

4. To specify whether the installation process waits before proceeding with the application, double-click the **Wait** field, and then select **Yes** or **No**.

**Rearrange application installation order**

The order of the applications in the list determines the order in which the installer runs the executable files and batch files. The order is customizable:

1. Select an application from the list.

2. Choose the **Up** and **Down** arrows on the right to rearrange the application within the list.

   **Note:** Each application executes according to its location on the list, so verify there is no conflict among the files in the list.

**Remove application from the installation list**

To remove an application:

1. Select the application from the list.

2. **Remove Application**.

2.20 Header and footer, watermark & background

This feature is not available in Reader.

Acrobat users can specify one or more files to use as headers, footers, watermarks, and backgrounds. This feature modifies the EnterpriseFiles installer table.
Files for these features are stored by default at C:\Program Files\Adobe\<product & version>\<product>\DocSettings\ You can also use the Files and folders feature to add these files.

The Header/Footer, Watermark, & Background settings allow you to specify additional header/footer, watermark, and background settings:

Header/Footer
You can add or remove header and footer settings from the installed application.

To specify a header and footer settings file:
1. Go to the Header/Footer Saved Settings panel.
2. Choose Add.
3. Navigate to the XML file containing the settings you want to add.
4. Choose Open.

The settings file appears in the Header/Footer Saved Settings list. To remove a header and footer settings file from the Header/Footer Saved Settings list, select the header/footer XML file you want to remove and choose Remove.

Watermark
You can add or remove watermark settings from the installed application.

To specify a watermark settings file:
1. Go to the Watermark Saved Settings panel
2. Choose Add.
3. Navigate to the XML file containing the settings you want to add.
4. Choose Open.

The settings file appears in the Watermark Saved Settings list. To remove a watermark settings file from the Watermark Saved Settings list, select the watermark XML file you want to remove and choose Remove.

Background
You can add or remove background settings from the installed application.

To specify a background settings file:
1. Go to the Background Saved Settings panel.
2. Choose Add.
3. Navigate to the XML file containing the settings you want to add.
4. Choose Open.
NOTE: The default XML file location is <drive>:\Program Files\Adobe\Acrobat(version)\Acrobat\DocSettings\Background.

The settings file appears in the Background Saved Settings list. To remove a background settings file from the Background Saved Settings list, select the background XML file you want to remove and choose **Remove**.

## 2.21 Redaction

This feature is not available in Reader.

Acrobat users can set predefined redaction codes, similar to custom text, to appear over your redaction areas. These codes often indicate why the material was redacted. Code sets and entries are provided from the U.S. FOIA (Freedom Of Information Act) and the U.S. Privacy Act. Redaction codes can be saved, imported, and exported. This feature modifies the EnterpriseFiles installer table.

**Tip:** Redaction code set files are stored by default at C:\Program Files\Adobe\<product & version>\<product>\DocSettings\Redaction\<language>. You can also use the Files and folders feature to add these files.

The Redaction settings allow you to specify the pre-defined code sets for use as replacement text when the end-user redacts page content with the Redaction tool.

To add a new code set file:

1. In the **Select Language** list, choose the language of the file you want to add.
2. Click **Add**.
3. Navigate to the file.
4. Choose **Open**.

To remove a code set file:

1. Select the file in the list.
2. Choose **Remove**.

Codes don’t save the current attributes for overlay text as part of the code definition, such as colors, font characteristics, and repetition or size of text. Codes only make the overlay text itself reusable in future sessions and by other users with whom you share code sets. You set other attributes for the code in the Redaction Tool Properties dialog box.
2.22 Portfolio navigators

This feature is not available in Reader.

Portfolio Navigators settings allow you to specify custom Portfolio navigator templates to be installed with Acrobat. This feature modifies the EnterpriseFiles installer table.
Customizing the Installer

Customization Wizard for the Acrobat Family of Products. © 2010 Adobe Systems Inc.

Tip: Files for these features are stored by default at C:\Program Files\Adobe\<product & version>\<product>\Navigators\. You can also use the Files and folders feature to add these files.

To add a navigator template:

1. In the Select Language list, choose the language of the file you want to add.
2. Choose Add.
3. Navigate to the portfolio .nav file.
4. Choose Open.

To remove a navigator template select the file in the list, and then choose Remove.

2.23 Direct editor

The Direct Editor allows advanced users to modify the installer tables directly rather than using the Wizard’s UI or MSI and Adobe properties on the command line.

Caution: Adobe strongly recommends that you do not use the Direct Editor feature unless you are knowledgeable about editing and troubleshooting installer tables. Improper use of this feature can result in the corruption of critical system files.

To modify a setting in an installer table:

1. In the Tables list, choose the table that contains the installation setting you want to change.
2. In the selected table, locate the item you want to change in the right hand panel.
   Tip: All of the columns in the Direct Editor are sortable alphabetically. Simply click the column heading.
3. Modify the entry as follows
   • Editing a value: Double-click to select a text string and enter a new value.
   • Editing rows: Right click on the row to see the context menu that allows you to cut, copy, paste, add, and drop rows.
3 Deploying Customized Installers

Once the project is saved, the resulting SKU is ready for mass deployment by choosing your desired deployment methodology. For example, you can simply run setup.exe. In addition to the SMS method below, X products support AIP-GPO and bootstrapper installations as well as deployment via SCCM and SCUP catalogs. For details, refer to the Enterprise Administration Guide.

3.1 Generate a transform file

A transform (.mst) file contains your modifications and any files added to the project (.msi) file. The Wizard updates the associated transform file every time you save a project. You can generate a copy of an open transform file and then apply it to another project.

To create a Transform file:

1. Choose Transform > Generate Transform.
2. In the Save dialog, browse to the desired location.
3. Enter the transform file name in the File name box.
4. Choose Save.

In order to apply the new transform file to another project, you must open the new project and load the transform file.

3.2 Generating SMS-compliant packages

Note: While SMS workflows are likely to work, Adobe has focused software distribution testing on System Center Configuration Manager (SCCM) 2007 and patch distribution through SCUP for the Acrobat X family of products. Since SMS is a legacy product for Microsoft, it is expected that most organizations have migrated or will migrate to SCCM or System Center Essentials (SCE).

In order to distribute your modified installation files (.msi, .mst, and Setup.ini) using Microsoft Systems Management Server (SMS), you must create an .sms file and, optionally, specify a Management Information Format (.mif) file in the same directory as the project (.msi) file.

To do so:

1. Choose SMS > Create SMS file at save.

   A check mark appears next to the command name when it is selected. This option creates an .sms file in the same directory as the project file the next time the project is saved. A Microsoft Systems Management Server (.sms) file is a text file containing product information and installation settings.
2. Choose **SMS > Specify MIF file name.**
   
   A check mark appears next to the command name when it is selected. A Management Information Format (.mif) file describes the installed application and is preset in the Windows directory on the destination system.

3. Enter a name in the MIF Filename box.

4. Choose **OK.**

### 3.3 Administrative install point installation

You can use your customized MST in AIP workflows. Simply add the TRANSFORMS property to your command line call to msiexec.

**Example 3.6: MST usage: In an AIP**

```plaintext
msiexec /a PRODUCTSOURCE\<ProductName>.msi /p PRODUCTAIP\AdbeRdr910_en_US.msp
msiexec /a PRODUCTSOURCE\<ProductName>.msi /p PRODUCTAIP\AdbeRdr912_en_US.msp
msiexec /p AIPPath\<ProductName>.msi TRANSFORMS=PRODUCTSOURCE\<ProductName>.mst
```

### 3.4 Binary bootstrapper installation

You can use your customized MST in bootstrapper workflows. The bootstrapper Setup.exe file uses Setup.ini as it’s configuration file. The Wizard modifies this file as you use it to configure your installation. Before deployment, open the file and verify it contains all the properties you need.

**Example 3.7: MST usage: In Setup.ini**

```ini
[Startup]
CmdLine=/sAll /s1 “1031”
RequireOS=Windows 2000

[Product]
CmdLine=TRANSFORMS=“AcroPro.mst”
msi=AcroPro.msi
Languages=1033;1031;1036
1033=English (United States)
1031=German (Germany)
1036=French (France)

[Windows 2000]
PlatformID=2
MajorVersion=5
ServicePackMajor=2
```
Administrators should also look for installation and deployment details in the Enterprise Administration Guide.

### 4.1 Multilanguage (MUI) package creation

After downloading and expanding the compressed installer, do the following to create a multilanguage Reader package:

1. Download the non-English Installers you need and expand them.
2. Install one localized version in a virtual machine (VM).
3. Search the Program folder for the language files (e.g. for German the file extension is DEU). Backup the language files and make sure to keep the directory structure.
4. Reset your VM and repeat the step above for each localized setup.
5. Open the AcroRead.msi of the US Version in the Customization Wizard.
6. Go to the **Files and Folders** and import the language files to the appropriate folders.
7. To set Reader automatically to the OS Language go to the **Registry** and add the following key:
   ```
   HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\<version>\Language\UseMui
   ```
8. Create a dummy value inside that Key so that the Wizard will recognize your change.

You now have a multilanguage package which automatically follows the OS language (or OS MUI language) if the appropriate language files are installed.

### 4.2 Error: Cannot modify MSI package

Why do I get the error "The Wizard cannot modify this MSI package..."?

Double check the following:

- Verify you are opening a product MSI that is supported. The Wizard checks a signature based on a GUID in the property table: the target product should have the requisite signature property as well as the expected major version value in the GUID.
- Verify you are not using Acrobat Elements which is not supported by the Wizard.
- Verify the Acrobat product and Wizard versions are identical. For example, the Wizard 9 can only be used with 9.x products.
4.3 Silent install isn’t silent

Why doesn’t my install respect the “silent install” settings I specified with the Wizard?

If your command line is something like:

    MSIEXEC /I <path to msi>\AcroPro.msi TRANSFORMS="<path to mst>\AcroPro.mst"

Then you are not using Setup.ini your workflow. The Wizard rewrites Setup.ini when you specify a silent install to include this option. The silent install switch is not saved in the MST. Either run Setup.ini or change your command line to include the /qn switch. For example:

    MSIEXEC /I <path to msi>\AcroPro.msi TRANSFORMS="<path to mst>\AcroPro.mst" /qn
Index

A
Acrobat.com services integration 39
AcroPro7 EFG – Tuned for silent, transformed, German destination 50
Add a job option 26
Add a server location 25
Add an ALCRM Server 36
Add and Modify File Types (Extensions) 43
Add document information 28, 30
Add Location 25
Add shortcut 24
Adding a folder to the Start menu 24
Adding and removing files and folders 18
Adding keys 22
Adding new registry keys 22
Adding registry keys from an existing registry 22
addressbook.acrodata 31
Administrative install point installation 50
Adobe PDF Output Folder 27, 28
Adobe PDF printer 27
Adobe PDF Security 27, 28
AdobePDF.INIbAddDocInfo 28
AdobePDF.INIbAskToReplacePDF 28
AdobePDF.INIbDonotSendFont 28
AdobePDF.INIbViewPrintOutput 28
AdobePDF.INIbPostScript Output Option 27
AdobePDF.INIPromptForFileName 27
AdobePDF.INISecurityOption 27
AdobePDF.INITrue Type Font Download Option 27
ALL_USERS_PDFOPTIONS_SETTINGS 26
Allow the user to choose the installation language 15
AllUsersProfileAppData 26
Application Path 44
aPrivKey 35
Ask to replace existing PDF file 28, 29
aVerify 35

B
Background 45
bAllowAPSConfig 37
bAllowInvisibleSig 36
bAllowOtherInfoWhenSigning 36
bAllowReasonWhenSigning 36
bAutoCompleteOnTab 41
bAutoFill 41
bAutoLaunchAtDocClose 34
bAutoLaunchAtSendMail 34
bBrowserIntegration 39
bCommercialPDF 39
bdisable_prc.all 37
bdisable_prc_com_adobe_acroman_ 38
bdisable_u3d_all 37
bdisable_u3d_com_adobe_acroman_ 38
bDisablePDFHandlerSwitching 12
bDisableTrustedFolders 32, 34
bDisableTrustedSites 32, 34
bEnableDocCtrInit 40
bEnableRTC Auth 40
bEnableShareFile 40
bEnhancedSecurityInBrowser 32
bEnhancedSecurityStandalone 32
Binary bootstrapper installation 50
blnlineAutoComplete 40
bNeedSynchronizer 41
bPrivKey 35
bPurchaseAcro 39
bReasons 36
bRecordsNewEntries 40
bShowDropDown 40
bShowEbookMenu 39
bStoreNumericEntries 41
bUpdater 38
bUsageMeasurement 39
bUserAskedToEnableAutoComplete 41
bValidateOnOpen 35
bVerifyUseAlways 35

C
cCrossdomain 33
cDataInjection 33
cExternalStream 33
Comments and forms 40
COMPANYNAME 11
Configuration panel overview 10
Configure once-deploy many 5
Controls for Acrobat.com integration 40
Controls for online features 38
Creating a shortcut 24
cScriptInjection 33
cSilentPrint 33
Index

cTrustedFolders 33
Customizing the Installer 10
cWeblink 34

D
Default PDF Handler selection 13
Default PDF Output Folder 27, 28
Default Signature Method 35
Default Verification Method 35
Default viewer 11
DefaultPDFOutput 27
Deleting a folder 24
Deploying Customized Installers 49
Digital signatures 34
Direct editor 48
directories.acrodata 30
Directory servers 30
Disable all Acrobat.com access, including initiation and participation 40
Disable all updates 38
Disable caching installer files 14
Disable Help > Digital Editions 39
Disable only initiation of live collaboration 40
Disable only initiation of shared review and forms 40
Disable only Upload and Share documents to Acrobat.com 40
Disable Product Improvement Program 39
Disable registration 39
Disable Viewing of PDF with Ads for Adobe PDF 39
Disallow user to modify 35
Disallow user to modify. . 35
Display PDF in browser 39
Distiller 26
DistillerDefJobOptions which sets HKCUSOFTWAREAdobeAcrobat
   Distiller<version>JobOptions. 27
DistillerDefPDFOutput 27
do not use document fonts 30
document fonts 30

E
Enable caching of installer files on local hard drive 14
Enable Optimization 14
Enable optimization 14
Enable reviewing of document warnings 36
ENABLE_CACHE_FILES 14
ENABLE_OPTIMIZATION 14
Enhanced security 31
EnterpriseFiles 17
EnterpriseLaunches 44
EnterpriseRegistries 10, 20, 27
Error
   Cannot modify MSI package 51
EULA 38
EULA_ACCEPT 38
Examine document 34
Examine document when closing document 34
Examine document when sending document by email 34
Extend Features in Adobe Reader 34

F
Features 16
Features to install 17
File attachments 42
Files and folders 17
fonts. 30
Forms auto-complete 40
Frequently Asked Questions 51

G
Generate a transform file 49
Generating SMS-Compliant Packages 49
Generating SMS-compliant packages 49

H
Header and footer, watermark & background 44
Header/Footer 45

I
In Adobe Reader, disable Help > Purchase Adobe Acrobat 39
Install Language 15
Install language 16
Installation 6
Installation options 11
Installation path 11
INSTALLDIR 11
Installer table modifications
   Enterprise Files 17
   Enterprise Registry 21
   Shortcuts 24
   SOURCELIST property 25
Installer tables
   Enterprise files for Joboptions 26
Installing interactivity options 14
Interactively (with full interface) 14
iRequireReviewWarnings 36
ISX_SERIALNUMBER 11
IW_DEFAULT_VERB and LEAVE_PDFOWNERSHIP. In general, the install leans towards letting the more secure Reader be the default viewer unless a property or user choice overrides that decision. 11
IW_DEFAULT_VERB interacts with the Adobe property
   LEAVE_PDFOWNERSHIP which can be used on the command line. 12
IW_DEFAULT_VERB is written to the MST file and doesn’t exist in the installer tables by default. It can also be used on the command line or Setup.ini. DEFAULT_VERB 11
IW_DEFAULT_VERB to 11

J
joboptions 26
Index

L
Language selection 15
Launch other applications 44
LiveCycle 34
Load trusted root certificates from Adobe 39
Loading a transform file 8
Loading an installer file 7
Lock ALCRM Server settings 37
Locking the feature 12

M
Management Information Format 49
Microsoft Systems Management Server 49
Modifying and removing default files 19
Modifying attachment black and white lists 43
Modifying existing keys 23
msiexec 50
MST usage
In an AIP 50
In Setup.ini 50
Multilanguage (MUI) package creation 51
Multiple installations 9

N
Navigators 47

O
Online and Acrobat.com features 38
Online feature integration 38
Open a recent project 7
Optimize product performance 13
Organization name 11

P
PDFIniAddDocInfo 28
PDFIniAskToReplaceFile 28
PDFIniDonoSendFonts 28
PDFIniPrompForFileName 27
PDFIniPSOutputOption 27
PDFIniSecurityOption 27
PDFIniTrueTypeFontDL 27
PDFIniViewPDFResults 28
Personalization options 11
Portfolio navigators 47
PostScript Output Option 29
PostScript Output Options 27
PostScript Printer Description 27
PRC format support 37
Prevent end-user to add trusted Files and Folders 34
Prevent end-user to add trusted Hosts 34
Preventing documents from opening other files and applications 42
Preventing end users from trusting locations 34
printer options 27
Prompt the user for reboot 15

R
Rearrange application installation order 44
Rearrange server locations 25
Reboot options 15
Reboot without prompt 15
Rebooting configuration 15
Redaction 46
Redaction tool properties 47
REGISTRATION_SURPRESS 39
Registry 20
Registry configuration
Enhanced security enabled 32
Locking enhanced security settings 32
Registry keys set by trusting locations 33
Registry workflow overview 21
Related resources 6
Rely on system fonts only 28, 30
Remember numerical data 41
Remove a joboptions file 27
Remove an ALCRM Server 37
Remove application from the installation list 44
Remove installed products 13
Remove previous version 13
Remove previous version of Reader 13
Remove server location 25
REMOVE_PREVIOUS 13
REMOVE_PREVIOUS_READER 13
Removing a default or custom files from the installation list 18
Removing a shared review server 42
Removing a shortcut 24
Renaming a folder 24
Reset installation settings 9
Restoring a shortcut 24
Restoring default behaviors 43
Rights management servers 36
RootKey 10
Run installation 15

S
Saving a project 8
Security 30
Serial number 11
Server locations 25
Set a default ALCRM Server 37
Set a default joboptions file 27
Shared reviews servers 41
Shortcuts 24
Show location and contact information when signing 36
Signature validation 35
Signing method 35
Silent install isn't silent 52
Silently (no interface) 14
SMS 49
SOURCELIST 25
Specifying behavior for file types not on black and white lists 43
Specifying trusted, "privileged" locations 32
Index

Standalone and browser behavior 31
Starting a Project 7
Summary 23
Summary view of file and folder changes 19
Suppress reboot 15
system fonts 30

T

TBuiltInPermList 43
tName 37
TRANSFORMS 50
TrueType Font Download Option 27, 28
Trusted identities 31
tServerName 37
tServerURL 37
tUI 41
tURL 37

U

U3D format support 37
Unattended (with no user interaction, only a progress bar) 14
Uninstalling older product versions at install time 13
Unsetting directory servers 30
Unsetting trusted identities 31
Use case
  Deploying digital signature files 20
User name 11
USERNAME 11

V

Verify signatures when the document is opened 35
View Adobe PDF results 28, 29
Viewer defaults 12
Viewing a list of changes file and folder changes 19
Viewing files to install 18

W

Wait 44
Watermark 45
When launching PDF in Internet Explorer, prompt user with
  Open/Save dialog 39
Why do I get the error "The Wizard cannot modify this MSI
  package..."? 51
Why doesn’t my install respect the “silent install” settings I
  specified with the Wizard? 52
Why is PDF ownership important? 12
Wizard Basics 5, 49
Workspace views 6