ApproveIt® Desktop

Network Installation and Deployment Guide

Product Release: 6.5
## CONTENTS

### Chapter 1: Introduction ................................. 1

- Document Conventions ........................................... 1
- Images ................................................................ 1

### Chapter 2: Terminology ................................. 2

### Chapter 3: Windows Installer ............................. 4

- Machine Policies .................................................. 4
- User Policies ....................................................... 5
- ALLUSERS Property ........................................... 6

### Chapter 4: Deployment ................................. 7

- Network Topology ................................................ 7
  - System Requirements ........................................ 8
  - Source Resiliency ............................................. 8
- Deployment Scenario Example ............................... 8
  - Per-Machine Installation .................................... 8
    - Administrator Instructions .............................. 8
    - User Instructions .......................................... 9

### Chapter 5: Setting Preferences ......................... 10

- CD Content ....................................................... 10
- .ini File .................................................................. 10
- ApproveIt Desktop Specific Properties ................. 10
- DAC Engine Repository .................................. 11
- Customizing the Menu in Microsoft Word and Microsoft Excel ........................................ 11
- Configuring ApproveIt Desktop to use an SNTP Server ................................................. 12
- Configuring ApproveIt Desktop to use OCSP ........ 12
- Configuring ApproveIt Desktop to Validate Signer Identity .................................. 12
- Configuring ApproveIt Desktop Certificate Status Display ........................................ 13
- Configuring the Time Format in the ApproveIt Desktop Audit Trail ......................... 13
- Customizing the Signature Block for Adobe Form Client ........................................ 14
  - Customizing Initial Text .................................. 14
  - Customizing Signature Size ............................. 15
- Filtering Certificates ........................................... 15
  - Configuring ApproveIt Desktop to Filter Certificates ............................................. 15
  - Configuring CPS File Certification ........................ 15
- Selecting Cryptographic Service Provider ............. 16
  - Configuring ApproveIt Desktop for Microsoft CryptoAPI ...................................... 16
  - Configuring ApproveIt Desktop for the Certificate Management Library .............. 16
  - Configuring ApproveIt Desktop for Network Security Services ............................ 17
- ApproveIt Signature Manager and Smart Cards .................. 17
- Command Line Options ........................................ 17

### Chapter 6: Network Upgrade ......................... 20

### Appendix A: Acrobat-Specific Issues ................. 21

- Setting Signature Preferences in Acrobat 9 .................. 21
- Setting Signature Preferences in Acrobat 8 .................. 21
- Setting Signature Preferences in Acrobat 7 .................. 21
- Setting Signature Preferences in Acrobat 6 .................. 22

### Appendix B: Post-Installation Procedure for CML Support 23

- Adding Trust Points ........................................... 23
- Caching CA Certificate ....................................... 23
- Listing Trust Points ........................................... 23
CONTENTS

Editing Trust Points ......................................................... 23
Adding/Listing/Editing CRLs ............................................. 23
Getting Help ................................................................. 24
Updating the CML Configuration ....................................... 24
Using CML in Locked Down Environment ............................ 24

Appendix C: Troubleshooting ................................. 25

Installation Starts in Maintenance Mode ......................... 25
'Network resource unavailable’ or Error 1706 ....................... 25
'Insufficient privileges’ or Error 1303 .............................. 26
Version of ApproveIt Desktop Already Installed ................. 27
IE Error ........................................................................... 27
No Host Application Error .................................................. 28
Incorrect Line Parameters ............................................... 28
CHAPTER 1: Introduction

The ApproveIt Desktop Installation Package is based on the Windows Installer technology. Windows Installer (MSI) is a service of the operating system, it introduces many useful security features to protect the network. These same security features may interfere with proper deployment.

This document aims to provide information on the network installation and deployment of ApproveIt Desktop. This document is intended to assist the System Administrator to understand the impact of Windows Installer on ApproveIt Desktop installation and deployments.

This document is not intended to be a tutorial on MSI. Along with relevant technical information, this document includes step-by-step examples of deployment scenarios tested by Silanis, troubleshooting information, references to relevant MSI material and sample login scripts.

To benefit from this document, the reader must be familiar with ApproveIt Desktop, software installation, network management and network security. A short glossary of the technical terms and their definition, as used in this document, is provided.

Document Conventions

This guide uses the following conventions:

**Bold**
Bold text is used for window titles, menus, options, menu options, buttons and tabs.

**Blue**
Blue text is used for Web links and for cross-references to chapters and sections. To access a given selection, click its blue text.

**Italics**
Italicized text is used for important text and for references to other documents.

This icon applies to notes.

This icon applies to important warnings. You should pay close attention to these items.

This icon applies to recommendations.

For optimal viewing of this document, please use the latest version of Adobe Reader. It can be downloaded from [http://www.adobe.com](http://www.adobe.com).

Images

The images in this guide are illustrative only and may differ from what you see when you use a particular version of ApproveIt.
# CHAPTER 2: Terminology

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising</td>
<td>A Windows Installer feature with which ApproveIT Desktop automatically installs and configures itself for subsequent users.</td>
</tr>
<tr>
<td>Deployment</td>
<td>The process of installing an application across a network on multiple target computers, for multiple users.</td>
</tr>
<tr>
<td>Elevated privileges</td>
<td>An installation runs with elevated privileges when it is running in system context, with administrative privileges. Deployment to non-administrative users relies on the ApproveIT Desktop installation running with elevated privileges even if it started from the user’s restricted context. Elevated privileges are also known as system privileges.</td>
</tr>
<tr>
<td>Installation “Push”</td>
<td>The term &quot;push&quot; is used when the installation is remotely imposed on a user. For example, using a login script to send a command that will launch the installation of ApproveIT Desktop.</td>
</tr>
<tr>
<td>Managed application</td>
<td>An application is a managed application if elevated privileges are used for installation. An application is managed on a system if it is a “per-machine” installation (see definition below) or if the application is assigned or published using Group Policy.</td>
</tr>
<tr>
<td>Non-administrative user</td>
<td>A user who does not have administrative privileges on the local computer.</td>
</tr>
<tr>
<td>Package</td>
<td>A package consists of an .msi file and any external source files that may be pointed to by this file. Therefore, a package contains all the information that Windows Installer needs to run the user interface and to install or uninstall the application.</td>
</tr>
<tr>
<td>Per-machine installation</td>
<td>A “per-machine” installation of an application means that the application is available for all users of a computer. This also means that shortcuts are installed in the “All Users” profile.</td>
</tr>
<tr>
<td>Per-user installation</td>
<td>A “per-user” installation of an application means that the application is available only for a particular user on that machine. This also means that shortcuts are installed in the &quot;All Users&quot; profile.</td>
</tr>
<tr>
<td>Source</td>
<td>The installation source is the path to the directory that contains the ApproveIT Desktop package used to perform the installation. In the case of “per-machine” installations, the installation source must be available to all the users targeted by the deployment and must stay accessible until the application has been completely deployed. To avoid problems, it is recommended that the installation source remains permanently available.</td>
</tr>
<tr>
<td>Subsequent users</td>
<td>In a “per-machine” installation scenario, subsequent users are those who log in after the initial ApproveIT Desktop installation was completed on the system. When a subsequent user logs in, the ApproveIT Desktop installation is automatically triggered if MSI detects that the ApproveIT Desktop installation/configuration was never performed for this user. Subsequent users do not require administrative privileges because ApproveIT Desktop is a managed application in this case, thus running with elevated privileges.</td>
</tr>
<tr>
<td>System privileges</td>
<td>System privileges are also known as elevated privileges. See “elevated privileges”.</td>
</tr>
</tbody>
</table>

Table 1: Terminology
### Terminology

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transform</td>
<td>A Transform (.mst file) adds or replaces elements in the original installation database (.msi file). A common use for Transforms is the customization of base installation packages for particular groups of users.</td>
</tr>
<tr>
<td>MSI</td>
<td>The Windows Installer technology.</td>
</tr>
<tr>
<td>Windows Installer Policies</td>
<td>Policies are security settings that can be set for machines, users, and user groups. These policies are implemented by registry keys/values and can be managed remotely by a network administrator using the proper tool(s). MSI policies control the behavior of the Windows Installer service on a machine or for a user.</td>
</tr>
</tbody>
</table>

Table 1: Terminology
CHAPTER 3: Windows Installer

Because of the security added by Windows Installer to the software installation process, some deployment scenarios may require changes in machine and user security policies for the ApproveIt Desktop installation to proceed normally. This chapter provides a list of the relevant policies that may be needed to install and deploy ApproveIt Desktop.

Machine Policies

The following table describes the MSI Machine Policies. The Registry location where these policies can be configured is provided at the top of the table. The text in **bold** describes specific impacts of the policies on the installation of ApproveIt Desktop.

<table>
<thead>
<tr>
<th>WINDOWS INSTALLER MACHINE POLICIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Location</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer</td>
</tr>
<tr>
<td>AlwaysInstallElevated</td>
</tr>
<tr>
<td>AllowLockdownBrowse</td>
</tr>
<tr>
<td>AllowLockdownMedia</td>
</tr>
</tbody>
</table>

Table 2: Windows Installer Machine Policies
User Policies

The following table describes the MSI User Policies. The Registry location where these policies can be configured is provided at the top of the table. The text in **bold** describes specific impacts of the policies on the installation of ApproveIt Desktop.

<table>
<thead>
<tr>
<th>User Policies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisableMSI</td>
<td>REG_DWORD</td>
</tr>
<tr>
<td>Logging</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>AlwaysInstallElevated</td>
<td>REG_DWORD</td>
</tr>
</tbody>
</table>

Some of the information in the table above was taken from the Microsoft Windows Installer SDK Help.

Table 2: Windows Installer Machine Policies

Table 3: Windows Installer User Policies
The following table illustrates how the **ALLUSERS** property affects the application's installation when combined with the access privileges of the user and the type of operating system.

<table>
<thead>
<tr>
<th>WINDOWS 2000 / WINDOWS XP</th>
<th>ALLUSERS = NULL</th>
<th>ALLUSERS = 1</th>
<th>ALLUSERS = 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access privileges.</td>
<td>Per-user installation using folders in user's personal profile.</td>
<td>Not valid; returns an error stating the user does not have enough access privileges to install application.</td>
<td>Per-user installation using folders in user's personal profile.</td>
</tr>
<tr>
<td>Administrator access privileges.</td>
<td>Per-user installation using folders in user's personal profile.</td>
<td>Per-machine installation using folders in &quot;All Users&quot; profile.</td>
<td>Per-machine installation using folders in &quot;All Users&quot; profile.</td>
</tr>
</tbody>
</table>

Table 4: ALLUSERS Property

Some of the information in the table above was taken from the Microsoft Windows Installer SDK Help.
CHAPTER 4: Deployment

Network Topology

The diagram below illustrates a typical network topology for deploying ApproveIt Desktop. Although real-life networks can be much more complex than the one represented in this diagram, most of them can be conceptually reduced to a similar representation.

Silanis used this environment to test the various concepts that are described in this document. The physical links constituting the network are irrelevant as long as the network connectivity is available on all computers.

In this diagram, the Network Server is the domain controller and the server that is used to install ApproveIt Desktop on the workstations. The workstations may be used by one of more users but, deployment complexity is reduced if the networked computers have only one user per machine.

Using this network setup, two deployment scenarios will be described in detail in the next section. Here is a brief overview of these scenarios:

1. **Per-Machine Deployment** – In this scenario, a deployment method is used to “push” ApproveIt Desktop to each Client Workstation. This installation will apply to all users of that machine. ApproveIt Desktop is then automatically installed upon login for each subsequent user, regardless of whether or not they have local administrative rights. Note that when using Windows Installer version 1.X, network connectivity to the Network Server must be preserved to insure the source package availability until ApproveIt Desktop has self-configured for all users.

2. **Per-User Deployment** – In this scenario, a deployment method is used to “push” ApproveIt Desktop to each user of a Client Workstation. The ApproveIt Desktop installation for each of these users on that machine occurs independently of the other users but requires users have elevated privileges. Note that connectivity to the Network Server is required for each ApproveIt Desktop user install.

All users on the Client Work stations must have, at least, restricted network domain access to the installation source folder.
System Requirements

- The Client Workstations are running Windows 2000, Windows XP, or Windows Vista.
- The host applications (e.g. Office 2000, etc.) are properly installed and configured on each Client Workstation and for every user on a given Client Workstation if multiple users will be sharing the same machine.

Source Resiliency

Applications that rely on network resources for installation-on-demand are susceptible to source failures if the source location should change for any reason or become damaged. Windows Installer provides source resiliency for features that are installed on-demand by using a source list. The source list contains the locations searched by the installer for installation packages. The entries in this list can be network locations, Uniform Resource Locators (URLs), or compact discs. If one of these sources fails, the installer can quickly and seamlessly try the next.

Deployment Scenario Example

ApproveIt Desktop installations and deployments can be grouped in two categories: per-machine installations and per-user installations. The next section illustrates a per-machine installation, which is the preferred deployment method.

Per-Machine Installation

In this scenario, ApproveIt Desktop is installed once for each target machine using startup scripts. These scripts run in the service-account context of the target machine and hence install ApproveIt Desktop as a managed application. ApproveIt Desktop will self-configure automatically upon user login, completing the ApproveIt Desktop installation for that user.

It is recommended that the installation source stay available beyond the deployment period. Removing the original installation source would break Windows Installer’s self-repair mechanism as well as cause problems for new users.

Administrator Instructions

1. Create a shared folder on the network to which all targeted users have access (e.g., ApproveItInstall).
2. Copy the entire contents of the ApproveIt Desktop CD to this folder.
3. If you need to change the install’s default behavior, you can modify the ‘setup.ini’ file. For example, you could make the installation “silent”, without any user intervention, by adding the following line:

   `CmdLine=/qb! ALLUSERS=1 APRV_SERIALNUMBER=azz000-111111 /i`

   For a list of ApproveIt-Desktop-specific variables that can be set in the .ini file, see ApproveIt Desktop Specific Properties on page 10.

You should apply a transform if you require more complex customizations. For more information on the MSI command line options, see http://msdn.microsoft.com/library.
4. Create a startup script, and ensure that the installation command is executed only once per machine.

User Instructions

As part of the login process, Windows Installer will automatically self-configure the ApproveIt Desktop application. The installation will start and complete rapidly without any user intervention. If the self-configuration is cancelled for any reason before completing, it will restart at the next login.

If you intend to use ApproveIt for FormFlow Designer and Filler, we recommend changing the default installation folder from \Program Files\ApproveIt to a folder with a path respecting the old 8.3 naming standard. Because Adobe Accelio Classic FormFlow Starter Kit and Filler is an older 16-bit application, it may have some problems locating the ApproveIt Desktop plug-in if the path contains long file names.
CHAPTER 5: Setting Preferences

The typical installation procedure is described in the User Guide included in this package. The purpose of this chapter is to describe how to set ApproveIt Desktop preferences using Windows Installer command-line options. This is widely used to build silent or partially silent installs, to log installation information, and to redefine default installation properties.

Network installation and deployment will be described in following chapters.

CD Content

All installation CDs contain the following files:

1. **Setup.msi**: the ApproveIt Desktop installation file.
2. **Setup.exe**, the file that determines whether or not the Windows Installer resides on the target machine and installs the Windows Installer if necessary. It also passes any information contained in the .ini file to the .msi file.
3. **Setup.ini**, the file that tells setup.exe the name of your .msi file to install. It also contains any command line options to be passed to the .msi file.

.ini File

The setup.ini file can be used to pass command line options to the installation. These command line options are passed to the .msi file by adding them to the .ini file and running the .exe file. For example, to ensure a pre-machine deployment and provide the ApproveIt Desktop serial number, add the following line to the .ini file.

```
CmdLine= ALLUSERS="1" APRV_SERIALNUMBER=azz000-111111 /i
```

To log all installation information in the file C:\install.log, add the following line to the .ini file:

```
CmdLine= /I*V "c:\install.log" ALLUSERS="1" APRV_SERIALNUMBER=azz000-111111 /i
```

The list of command-line options is provided in the section Command Line Options on page 17. It can also be found at [http://msdn.microsoft.com/library](http://msdn.microsoft.com/library).

ApproveIt Desktop Specific Properties

Following are the ApproveIt Desktop specific properties that can be customized:

- **APRV_SERIALNUMBER**: <The serial number>. No default value is set.
- **ALLUSERS**: Takes value "" (Single user) or "1" (All users). The default is 1.
- **APRV_ENABLEDACENGINEUPGRADE**: 0 or 1. Default is 1.
- **APRV_ENFORCEDEFaulTPHRASE**: 0 or 1. Default is 0.
- **APRV_HKCU_DIR_CAPTUREDSIGPATH**: Default directory containing the .cps files. Default is [INSTALLDIR]\Capture.
• **APRV_HKLM_CONFIG_COMMANDS**: This key enables you to customize the ApproveIt menu and toolbar in Microsoft Word and Microsoft Excel, see Customizing the Menu in Microsoft Word and Microsoft Excel on page 11.

**DAC Engine Repository**

The DAC engine repository is where the current versions of the DAC engine for Microsoft Office and Adobe Acrobat are located. In this repository are the files DACengine.dll (for Microsoft Office) and PDFAEngine.dll (for Adobe Acrobat). The default URL for ApproveIt Desktop products is [http://dac.silanis.com/latestdacs/](http://dac.silanis.com/latestdacs/).

For more information about the DAC engine repository, please contact our Customer Support Centre by phone at 1-888-silanis (choose option 3) or by e-mail at support@silanis.com.

**Customizing the Menu in Microsoft Word and Microsoft Excel**

It is possible to remove menu items from the ApproveIt menu and icons from the ApproveIt toolbar in Microsoft Word and Microsoft Excel. The menu is customized at installation using the ApproveIt Desktop property **APRV_HKLM_CONFIG_COMMANDS**.

Please note that menu items and corresponding toolbar icons cannot be removed separately. For example, the Approve menu item cannot be removed from the ApproveIt menu while leaving the Approve toolbar icon from the ApproveIt toolbar. Moreover, preset ApproveIt configurations have precedence over customization. In short, customization allows the removal of menu items and toolbar icons that are already available in the base ApproveIt version.

Each item menu corresponds to a decimal value (given in the table below). The value of the property **APRV_HKLM_CONFIG_COMMANDS** should be the sum of the decimal values corresponding to the items you wish to be listed in the ApproveIt menu and toolbar. For example, to get only the Approve, Secure Print and About items, the value should be 1+4+64=69.
Configuring ApproveIt Desktop to use an SNTP Server

ApproveIt Desktop can be configured to use a Simple Network Time Protocol (SNTP) server. To do so, you must define the following properties:

- **APRV_SNTP_ENABLED**: Takes value 0 (not enabled) and 1. Default value is 0.
- **APRV_SNTP_SERVER1**: URL of the SNTP server. No default value.
- **APRV_SNTP_SERVER1_PORT**: Port to use to connect to SNTP server. Default value is 123.

ApproveIt Desktop can also be configured to enforce the connection to the SNTP server. This configuration prevents users to sign when the SNTP server cannot be contacted. To do so, you must define the following property:

- **APRV_SNTP_ENFORCED**: Takes value 0 (not enforced) and 1. Default value is 0.

### Configuring ApproveIt Desktop to use OCSP

ApproveIt Desktop can be configured to use an OCSP responder.

To use an OCSP responder, you must define the following property:

- **APRV_OCSP_RESPONDER1**: URL of the OCSP responder (should start with "http://"). No default value.

### Configuring ApproveIt Desktop to Validate Signer Identity

ApproveIt for PureEdge ICS and ApproveIt for XHTML can be configured to validate the signer identity in specially designed forms. (See the appropriate designer guide for more instructions).

---

**Figure 2: Registry Key Values**

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>VALUE (HEX)</th>
<th>VALUE (DECIMAL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve</td>
<td>0x00000001</td>
<td>1</td>
</tr>
<tr>
<td>Authenticate</td>
<td>0x00000002</td>
<td>2</td>
</tr>
<tr>
<td>Secure Print</td>
<td>0x00000004</td>
<td>4</td>
</tr>
<tr>
<td>Undo Last</td>
<td>0x00000008</td>
<td>8</td>
</tr>
<tr>
<td>Save Unsigned</td>
<td>0x00000010</td>
<td>16</td>
</tr>
<tr>
<td>Configuration</td>
<td>0x00000020</td>
<td>32</td>
</tr>
<tr>
<td>About ApproveIt</td>
<td>0x00000040</td>
<td>64</td>
</tr>
<tr>
<td>Protect Document (Word only)</td>
<td>0x00000080</td>
<td>128</td>
</tr>
<tr>
<td>Protect Sheet (Excel only)</td>
<td>0x00000100</td>
<td>256</td>
</tr>
<tr>
<td>Protect Workbook (Excel only)</td>
<td>0x00000200</td>
<td>512</td>
</tr>
<tr>
<td>Batch Approve</td>
<td>0x00000400</td>
<td>1024</td>
</tr>
<tr>
<td>Batch Authenticate</td>
<td>0x00000800</td>
<td>2048</td>
</tr>
<tr>
<td>Batch Secure Print</td>
<td>0x00001000</td>
<td>4096</td>
</tr>
<tr>
<td>Proponent Prepare</td>
<td>0x00002002</td>
<td>8192</td>
</tr>
<tr>
<td>Proponent Prepare Send</td>
<td>0x00004000</td>
<td>16384</td>
</tr>
<tr>
<td>Proponent Invite</td>
<td>0x00008000</td>
<td>32768</td>
</tr>
<tr>
<td>Batch Approve Folder</td>
<td>0x00010000</td>
<td>65536</td>
</tr>
<tr>
<td>Batch Authenticate Folder</td>
<td>0x00020000</td>
<td>131072</td>
</tr>
<tr>
<td>Batch Secure Print Folder</td>
<td>0x00040000</td>
<td>262144</td>
</tr>
</tbody>
</table>
To validate the signer identity, you must define the following property:

- **APRV_ENFORCEIDMATCH**: When set to 1, it requires that the associated form filed data is a substring of the certificate common name (CN). When set to 2, it requires that the associated form filed data matches exactly the certificate common name (CN). When set to 0, no validation is performed. Default is 0.

**Configuring ApproveIt Desktop Certificate Status Display**

ApproveIt Desktop can be configured to display certificate validation information for the current date as well as validation for when the document was signed.

To enable this feature, you must define the following property:

- **APRV_CERTDISPLAY**: Takes value NEVER (at signing time information only), AUTO (automatic) and ALWAYS. Default value is NEVER.

**Configuring the Time Format in the ApproveIt Desktop Audit Trail**

The format of the time information presented in the ApproveIt Trail can be configured. The time format can be set at installation time using the property **APRV_AT_DTF**.

This property should be formatted as follows:

- **APRV_AT_DTF=“G|L[format]”**: Where G indicates that format will represent the GMT time, and L indicates that format represents a local time. The format string is an arbitrary string with the formatting codes which are listed in the table below.

The default audit trail time format is:

**APRV_AT_DTF= “G[%Y %m %d %H:%M]”**.

<table>
<thead>
<tr>
<th>FORMATTING CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>Abbreviated weekday name</td>
</tr>
<tr>
<td>%A</td>
<td>Full weekday name</td>
</tr>
<tr>
<td>%b</td>
<td>Abbreviated month name</td>
</tr>
<tr>
<td>%B</td>
<td>Full month name</td>
</tr>
<tr>
<td>%c</td>
<td>Date and time representation appropriate for locale</td>
</tr>
<tr>
<td>%d</td>
<td>Day of month as decimal number (01 - 31)</td>
</tr>
<tr>
<td>%H</td>
<td>Hour in 24-hour format (00 - 23)</td>
</tr>
<tr>
<td>%I</td>
<td>Hour in 12-hour format (01 - 12)</td>
</tr>
<tr>
<td>%J</td>
<td>Day of year as decimal number (001 - 366)</td>
</tr>
<tr>
<td>%m</td>
<td>Month as decimal number (01 - 12)</td>
</tr>
<tr>
<td>%M</td>
<td>Minute as decimal number (00 - 59)</td>
</tr>
</tbody>
</table>

Table 5: Formatting Codes for Time Format
The # flag may prefix any formatting code. In that case, the meaning of the format code is changed as described in the table below.

<table>
<thead>
<tr>
<th>FORMATTING CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%p</td>
<td>Current locale’s A.M./P.M. indicator for 12-hour clock</td>
</tr>
<tr>
<td>%S</td>
<td>Second as decimal number (00 - 59)</td>
</tr>
<tr>
<td>%U</td>
<td>Week of year as decimal number, with Sunday as first day of week (00 - 53)</td>
</tr>
<tr>
<td>%W</td>
<td>Weekday as decimal number (0 - 6; Sunday is 0)</td>
</tr>
<tr>
<td>%x</td>
<td>Date representation for current locale</td>
</tr>
<tr>
<td>%X</td>
<td>Time representation for current locale</td>
</tr>
<tr>
<td>%y</td>
<td>Year without century, as decimal number (00 - 99)</td>
</tr>
<tr>
<td>%Y</td>
<td>Year with century, as decimal number</td>
</tr>
<tr>
<td>%z, %Z</td>
<td>Either the time-zone name or time zone abbreviation, depending on registry settings; no characters if time zone is unknown</td>
</tr>
<tr>
<td>%%</td>
<td>Percent sign</td>
</tr>
</tbody>
</table>

Table 5: Formatting Codes for Time Format

<table>
<thead>
<tr>
<th>FORMATTING CODE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%#a, %#A, %#b, %#B, %#p, %#X, %#z, %#Z, %%%</td>
<td># flag is ignored.</td>
</tr>
<tr>
<td>%#c</td>
<td>Long date and time representation, appropriate for current locale. For example: &quot;Tuesday, March 14, 1995, 12:41:29&quot;.</td>
</tr>
<tr>
<td>%#x</td>
<td>Long date representation, appropriate to current locale. For example: &quot;Tuesday, March 14, 1995&quot;.</td>
</tr>
<tr>
<td>%#d, %#H, %#I, %#j, %#m, %#M, %#S, %#U, %#w, %#W, %y, %Y</td>
<td>Removes leading zeros (if any).</td>
</tr>
</tbody>
</table>

Table 6: Additional Formatting Codes for Time Format

**Customizing the Signature Block for Adobe Form Client**

This section tells you how to customize the ApproveIt Signature Block of a document that is viewed using Adobe Form Client.

**Customizing Initial Text**

To customize the text that initially appears in the Signature Block, use the following three parameters in the `setup.ini` file:

- **APRV_SIGNING_DISPLAY_CUSTOMUNAPPROVEDTEXT**
  - This is the character string that appears in the Signature Block before a signature is applied. The default value is Click to Approve.
- **APRV_SIGNING_DISPLAY_CUSTOMUNAPPROVEDTEXTFONT**
  - This is the font used to display the text that appears in the Signature Block before a signature is applied. The default value is Verdana.
Customizing Signature Size

To determine if an applied signature will be stretched to fit its Signature Block, use the following parameter in the \texttt{setup.ini} file:

- **\texttt{APRV\_SIGNING\_PLUGINOPTIONS\_FF99\_STRETCHSIGNATURE}**
  - The default value is 1 (the signature will be stretched). The alternate value is 0 (the signature will not be stretched).

Filtering Certificates

External third-party certificates may be used in ApproveIt Desktop for signing documents and creating ePersona files. When signing using certificates, the default ApproveIt Desktop configuration is to display a certificate selection dialog that lists all valid certificates available on the system.

Configuring ApproveIt Desktop to Filter Certificates

ApproveIt Desktop can be configured to filter certificates in the Certificate Selection dialog. The filtering criteria presently supported are:

- certificate policy
- certificate validity
- issuing CA
- key usage restrictions

These criteria can be enabled independently during the installation using the following properties:

1. Set the property **\texttt{APRV\_HKLM\_PREFS\_CERTPOLICY}** to \texttt{[CP Identifier]} to list only certificates that may be used under the certificate policy \texttt{[CP Identifier]}.
2. Set the property **\texttt{APRV\_HKLM\_PREFS\_ISSUERSUBSTR}** to \texttt{[Issuer CA]} to list only certificates with \texttt{[issuer CA]} as a substring of the issuer distinguished name.
3. Set the property **\texttt{APRV\_HKLM\_PREFS\_LISTONLYSIGCERT}** to 1 to list only certificates that can be used for signing.
4. Set the property **\texttt{APRV\_HKLM\_PREFS\_LISTONLYVALIDCERT}** to 1 to list only valid certificates.

For example, to list only valid certificates issued by a CA identified as Dummy CA which can be used for signing under the CP identified as 1.23.43.23.2324.1.0, add the following line (with no line breaks) to the \texttt{.ini} file:

```
CmdLine= APRV_HKLM_PREFS_LISTONLYVALIDCERT=1
APRV_HKLM_PREFS_ISSUERSUBSTR ="Dummy CA"
APRV_HKLM_PREFS_LISTONLYSIGCERT =1
APRV_HKLM_PREFS_CERTPOLICY="1.23.43.23.2324.1.0" /i
```

The ApproveIt Desktop dialogs listing certificates (CPS File Certification Dialog and Certificate Selection) can be configured to be displayed only when more than one certificate is found on the system that matches the filtering conditions (if any). This behavior can be enabled during installation using the property **\texttt{APRV\_HKLM\_PREFS\_USE3RDPARTYCERTIFUNIQUE}** by setting it to 1.

Configuring CPS File Certification

The default behavior of the CPS File Certification dialog is to enable users to export the certificate and the private key in the CPS file. This can be configured during installation using the following properties:

1. Set the property **\texttt{APRV\_HKLM\_PREFS\_}**
Selecting Cryptographic Service Provider

1. Set the property COPYPRIVATEKEYDEFAULT to 1 to check the Key Export checkbox.
2. Set the property APRV_HKLM_PREFS_COPYPRIVATEKEYENABLE to 0 to disable the Key Export checkbox.

Selecting Cryptographic Service Provider

<table>
<thead>
<tr>
<th>HKEY_LOCAL_MACHINE\SOFTWARE\SILANIS\APPROVEIT\PREFS\FAILIFNOMATCHFOUND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description Is only enabled if Use3rdPartyCertIfUnique is set to 1. If set to 1 and no certificate matches the search criteria, an error appears (to prevent users from creating or upgrading an ePersona with the wrong certificate); if set to 0, the certification appears with an empty certificate list.</td>
</tr>
<tr>
<td>Type String (REG_SZ)</td>
</tr>
<tr>
<td>Default 1</td>
</tr>
</tbody>
</table>

Table 7: Configuring CPS File Certification

ApproveIt Desktop integrates to several cryptographic libraries and public key infrastructures. The choice of a cryptographic library is determined by the location of the certificates to use in ApproveIt Desktop. The selection of the cryptographic libraries is done at installation using the following property: APRV_HKLM_PROVIDER_DEFAULTPROVIDER.

Configuring ApproveIt Desktop for Microsoft CryptoAPI

The default ApproveIt Desktop configuration supports Microsoft CryptoAPI (CAPI), which enables the use of certificates from Microsoft certificate stores. No modification to the installation is required in this case.

Configuring ApproveIt Desktop for the Certificate Management Library

ApproveIt Desktop can be configured to support the Certificate Management Library (CML) which offers remote directory retrieval options using the Lightweight Directory Access Protocol (LDAP).

To enable CML support during installation (and disable the CAPI support), you must define the following properties:

• APRV_HKLM_PROVIDER_DEFAULTVERPROVIDER: - Verification provider. This can be either Microsoft CAPI, Certificate Management Library or Network Security Services. To enable CML support, this value must be set to Certificate Management Library.
• APRV_CML_USELDAP: This can be either TRUE (use an LDAP server to update the CML CRL database) or FALSE (use local CML CRL database). The default value is set to FALSE. If you set it to TRUE you should also set the APRV_CML_LDAPSERVER and APRV_CML_LDAPPORT properties (see below).
• APRV_CML_LDAPSERVER: The LDAP server’s URL. No default value is set.
• APRV_CML_LDAPPORT: Port to use to connect to the LDAP server. No default value is set.

Please note that to fully configure CML support, some post-installation steps must be performed. For more information, please see Post-Installation Procedure for CML Support on page 23.
Configuring ApproveIt Desktop for Network Security Services

ApproveIt Desktop can be configured to support Network Security Services (NSS), which enables the use of certificates from personal Netscape certificate stores.

To set the NSS support you need to provide the absolute path to the Netscape profile of the user. Typically, the path takes the following form:

For Netscape version 4.X: `%ProgramFiles%\Netscape\Users\%UserName%`

For later versions of Netscape: `%AppData%\Mozilla\Profiles\%UserName%\*.slt`

where * is a string of 8 characters.

To enable NSS support during installation (and disable the CAPI support), add the following line to the .ini file:

```
CmdLine= APRV_HKLM_PROVIDER_DEFAULTPROVIDER="Network Security Services" APRV_HKLM_PROVIDER_NSS_CONFIGDIR=[PATH] /I, where [PATH] is the absolute path to the user’s Netscape profile.
```

ApproveIt Signature Manager and Smart Cards

ApproveIt Signature Manager can be configured to generate smart card based ePersona files. To do so, you must define the following property:

- **APRV_HKLM_PREFS_CREATEV7CPSFILE:**
  - Takes value 0 (No smart card support) and 1.
  - Default value is 0.

With this configuration, no password is required upon creation of the ePersona file as the private key access is enforced by the smart card itself. When used to sign, only the smart card pin is requested.

Command Line Options

The executable program which interprets packages and installs products is **Msiexec.exe**. Note that **Msiexec.exe** also sets an error level on return that corresponds to system error codes (for more information on system error codes, please go to [http://msdn.microsoft.com/library](http://msdn.microsoft.com/library)). The following table describes the command line options for this program.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>/I</td>
<td>Package</td>
<td>ProductCode</td>
</tr>
</tbody>
</table>

The following table comes from the "Platform SDK: Windows Installer", which can be found at: [http://msdn.microsoft.com/library](http://msdn.microsoft.com/library).
<table>
<thead>
<tr>
<th>OPTION</th>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
</table>
| /f     | [p|o|e|d|c|a|u|m|s|v] Package|ProductCode | Repairs a product. This option ignores any property values entered on the command line. The default argument list for this option is 'pecms'. This option shares the same argument list as the REINSTALL MODE property.  
  p - Reinstall only if file is missing  
  o - Reinstall if file is missing or if an older version is installed.  
  e - Reinstall if file is missing or an equal or older version is installed.  
  d - Reinstall if file is missing or a different version is installed.  
  c - Reinstall if file is missing or the stored checksum doesn't match the calculated value. Only repairs files that have msidbFileAttributesChecksum in the Attributes column of the File table.  
  a - Force all files to be reinstalled.  
  u - Rewrite all required user specific registry entries.  
  m - Rewrite all required computer-specific registry entries.  
  s - Overwrite all existing shortcuts.  
  v - Run from source and re-cache the local package. Do not use the v reinstall option for the first installation of an application or feature. |
| /a     | Package  | Administrative installation option. Installs a product on the network. |
| /x     | Package|ProductCode | Uninstalls a product. |
| /j     | [u|m]Package or [u|m]Package /t Transform List or [u|m]Package /g LanguageID | Advertises a product. This option ignores any property values entered on the command line.  
  • u - Advertise to the current user.  
  • m - Advertise to all users of machine.  
  • g - Language ID  
  • t - Applies transform to advertised package. |
| /L     | [i|w|e|a|r|u|c|m|o|p|v|+!]+!Logfile | Specifies path to log file and the flags indicate which information to log.  
  • i - Status messages  
  • w - Non-fatal warnings  
  • e - All error messages  
  • a - Start up of actions  
  • r - Action-specific records  
  • u - User requests  
  • c - Initial UI parameters  
  • m - Out-of-memory or fatal exit information  
  • o - Out-of-disk-space messages  
  • p - Terminal properties  
  • v - Verbose output  
  • + - Append to existing file  
  • ! - Flush each line to the log  
  • "**" - Wildcard, log all information except for the v option. To include the v option, specify "/!v". |

Table 8: Command Line Options
The options /i, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, /p, /y and /z should not be used together. The one exception to this rule is that patching an administrative installation requires using both /p and /a. The options /t and /g should only be used with /j. The options /i and /q can be used with /l, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, and /p.
CHAPTER 6: Network Upgrade

Upgrading from previous ApproveIt versions can be performed by running the new installation package. All old files will be upgraded automatically. The process to upgrade is the same as for the initial deployment already described in the previous sections of this document. You may not change the installation folder, the username nor the company name when doing an upgrade of ApproveIt Desktop.

Please note that during the upgrade, the ePersona (.cps) files, the reports and the log files created by previous ApproveIt versions are neither deleted nor replaced. However, for added security, you may want to save all current ePersona files before performing an upgrade.
APPENDIX A: Acrobat-Specific Issues

Setting Signature Preferences in Acrobat 9

In Acrobat 9.1, users can sign documents using Acrobat's DigSig method or ApproveIt Desktop. To ensure that ApproveIt Desktop is the preferred default for your users:

1. Open the Registry.
2. Create `Software\Adobe\Adobe Acrobat\9.1\Security\cHandlers` (if not already present). The key is in the HKEY_CURRENT_USER registry hive.
3. Set the following key name `aPrivKey` with `Silanis.ApproveIt`.

![Edit String](image)

Setting Signature Preferences in Acrobat 8

In Acrobat 8.0, users can sign documents using Acrobat's DigSig method or ApproveIt Desktop. To ensure that ApproveIt Desktop is the preferred default for your users:

1. Open the Registry.
2. Create `Software\Adobe\Adobe Acrobat\8.0\Security\cHandlers` (if not already present). The key is in the HKEY_CURRENT_USER registry hive.
3. Set the following key name `aPrivKey` with `Silanis.ApproveIt`.

![Edit String](image)

Setting Signature Preferences in Acrobat 7

In Acrobat 7.0, users can sign documents using the Acrobat's DigSig method or ApproveIt Desktop. To ensure that ApproveIt Desktop is the preferred default for your users:

1. Open the Registry.
2. Create `Software\Adobe\Adobe Acrobat\7.0\Security\cHandlers` (if not already present). The key is in the HKEY_CURRENT_USER registry hive.
3. Set the following key name `aPrivKey` with `Silanis.ApproveIt` (binary value of `53696C616E69732E417070726F7665497400`).
In Acrobat 6.0, users can sign documents using the Acrobat DigSig method or ApproveIt Desktop. To ensure that ApproveIt Desktop is the preferred default for your users:

1. Open the Registry.
2. Create `Software\Adobe\Adobe Acrobat\6.0\Security\cHandlers` (if not already present). The key is in the `HKEY_CURRENT_USER` registry hive.
3. Set the following key name `aPrivKey` with `Silanis.ApproveIt` (binary value of `53696C616E69732E417070726F7665497400`).
APPENDIX B: Post-Installation Procedure for CML Support

The command-line utility trustpts.exe, located in the Support folder (e.g. C:/Programs Files/ApproveIt/Support), is used to manage the CML trust points (i.e. root certificates that are trusted by ApproveIt Desktop) and Certificate Revocation Lists (CRLs). The trust points and CRLs will be stored in the CML databases certs.db and crl.db respectively, both located in the Support folder.

Adding Trust Points

In order for your personal certificate to be validated by ApproveIt Desktop, your PKI root certificate must be installed as a trust point. To add a trusted root certificate, execute the following instruction on the Command Prompt: trustpts -add file, where file is a path to an ASN.1 encoded certificate file (extension .crt or .cer).

Caching CA Certificate

Intermediate CA certificate needed to build certificate path will be automatically downloaded from the LDAP server. It is however possible to pre-install the intermediate certificates in the certificate database using the following command: trustpts -cache file, where file is a path to an ASN.1 encoded certificate file (extension .crt or .cer).

Listing Trust Points

To list trust points installed execute the following instruction on the Command Prompt: trustpts -list. The DN of each trust points in the database will be displayed on the screen. The -listall option can be used instead, to list both the trust points and the cached certificates.

Editing Trust Points

To edit trust points, you must execute the following instruction on the Command Prompt: trustpts -edit. The DN of each trust points in the database will be displayed on the screen. To delete a specific trust point, enter its index and hit the Enter key. To quit, press Q followed by the Enter key. The -editall option can be used instead to edit both the trust points and the cached certificates.

Adding/Listing/Editing CRLs

Usually, the required CRLs are downloaded by ApproveIt Desktop when validating a certificate. However, a user may want to import a CRL into the CML database to avoid a longer download time. Adding, editing or listing CRLs can be done using the -CRL option with the associated commands, as described earlier. For example, to add a CRL to the database, simply enter: trustpts -CRL -add file where file is the path to an ASN.1 encoded CRL file (extension crl).

To edit CRLs, you must execute the following instruction on the Command Prompt: trustpts -CRL -edit. To delete a specific CRL, enter its index and hit the Enter key. To quit, press Q followed by the Enter key.
Getting Help

To get the description of all available commands from the trustpts.exe program, simply execute the following instruction on the Command Prompt: trustpts - help. The most important functions are described next.

Updating the CML Configuration

The CML configuration is set in the srl.cfg, which can be found under C:/Program Files/ApproveIt/Support. This configuration file contains the following variables:

- **PATH**: Path to the location of the CML databases (certs.db and crl.db). Default value is current directory (\).
- **CERT_FILE**: Filename of the CML certificate database. Default value is certs.db.
- **CRL_FILE**: Filename of the CML CRL database. Default value is crl.db.
- **USE_LDAP**: Online verification (use an LDAP server to update the CML CRL database) or Offline verification (use local CML CRL database). This can be either TRUE or FALSE. The default value is set to FALSE.
- **LDAP_DLL_NAME**: Library to use. Should be set to nsldapssl32v40.dll.
- **LDAP_SERVER**: The LDAP server's URL to be used to obtain the CRL files. No default value is set.
- **LDAP_PORT**: Port to use to connect to the LDAP server. No default value is set.

Note that some of these variables may be set during installation. See Configuring ApproveIt Desktop for the Certificate Management Library on page 16

Using CML in Locked Down Environment

When ApproveIt is configured for CML Support, ApproveIt users must have write access to both CML databases (certs.db and crl.db).

In environments where ApproveIt users do not have write access to the ApproveIt support folder, the system administrator must perform the following installation manually:

1. Move both databases in an unrestricted location, for example C:/ApproveItDatabases.
2. Open the file srl.cfg, which can be found under C:/Program Files/ApproveIt/Support and modify the PATH entry so that it points to a location where ApproveIt users have write access.
APPENDIX C: Troubleshooting

Installation Starts in Maintenance Mode

Symptom

When launching the ApproveIt Desktop installation manually or through a deployment push, the Application Maintenance dialog appears, giving the user the choice to Modify, Repair or Remove the application.

![Figure 1: Application Maintenance](image)

Explanation

This is the normal MSI behavior when launching an installation package for a product that is already installed.

Solution

Make sure the ApproveIt Desktop installation is only called once per machine or once per user, depending on the deployment method used. If this dialog does come up, press Cancel; the current version of ApproveIt Desktop is already installed.

'Network resource unavailable' or Error 1706

Symptom

When a subsequent user logs in after a "per-machine" installation has been done, the following dialog will appear. Canceling the first dialog will bring up the 'Error 1706' error message.
**Explanation**

All subsequent users of a per-machine installation must have access to the original installation source if MSI version is 1.X. Because the default is MSI policy, non-administrative users cannot change nor browse to a different location.

By default, the MSI policy does not allow non administrators to access the installation package. See See Windows Installer on page 4.

**Solution**

1. Upgrade to MSI version 2.0 or later.
2. Make sure that all users involved in the ApproveIt Desktop deployment have access to the installation source if MSI version is 1.X.
3. Do not use mapped drive letters unless the drive mapping is identical for all users.
4. The installation package should be always available, even after the deployment is complete.
5. For CD-ROM deployments, make sure the AllowLockdownMedia policy is set on the computers involved in the ApproveIt Desktop deployment.

**‘Insufficient privileges’ or Error 1303**

**Symptom**

When attempting to push a “per-user” deployment to non-administrative users, you may get the following error message:
**Explanation**

This error appears when the targeted users do not have administrator privileges and the AlwaysInstallElevated policies are not set.

**Solution**

Ensure that the MSI AlwaysInstallElevated policies (for both machine and user) are set before deploying ApproveIt Desktop. See See Windows Installer on page 4.

---

**Version of ApproveIt Desktop Already Installed**

**Symptom**

When the ApproveIt Desktop installation is launched, the following message appears:

![Installer Information](image)

**Explanation**

This behavior is the normal ApproveIt Desktop installation behavior when MSI detects that a Silanis product is already installed and it can not be upgraded.

**Solution**

Ensure that the ApproveIt Desktop installation is called only when upgradable versions of ApproveIt Desktop are installed; this can be done by verifying the registry. To verify the registry:

1. Go to Start>Settings>Control Panel.
2. Double-click Add/Remove Programs.
3. Click ApproveIt Desktop.
4. Click support information.

---

**IE Error**

**Symptom**

When the installation is launched, the following message appears:

"[ProductName] requires that you have Microsoft Internet Explorer 5.01 or higher installed on your system."

**Explanation**

ApproveIt Desktop requires a version of MS Internet Explorer greater or equal to 5.01.

**Solution**

Upgrade IE (go to http://www.microsoft.com/windows/IE).
No Host Application Error

Symptom

When the installation is launched, the following message appears: **No host application was found on this computer. Please install the host application before installing ApproveIt Desktop.**

![No Host Application Found](image)

Figure 5: No Host Application Found

Explanation

ApproveIt Desktop requires at least one of the following host application be installed: Microsoft Word, Microsoft Excel, Adobe Acrobat, Adobe Reader, Adobe Form Designer and Client, Adobe FormFlow Form Designer with Filler, PureEdge ICS Designer and Viewer, Lotus Forms Designer and Viewer, and Microsoft InfoPath.

Solution

Text: Install one or use the APRV_SKIPCONDITION_HOSTAPP property described in See Setting Preferences on page 10.

Incorrect Line Parameters

Symptom

When the installation is launched, the following message appears: “Incorrect command line parameters.”

![Windows Installer](image)

Figure 6: Windows Installer

Explanation

This error appears when inadmissible parameters are passed to MSI on the command line. This happens when the ApproveIt Desktop install is launched from the command line or when a line is added to the .ini file. See Setting Preferences on page 10 for admissible property names.

Solution

Make sure the command line parameters you are passing to MSI are correct.