ApproveIt® Desktop

Network Installation and Deployment Guide

Product Release: 6.5

Silanis Technology Inc.
8200 Decarie, 3rd Floor
Montreal, Quebec
H4P 2P5

Phone: 1-888-SILANIS
Fax: (514) 337-5258
Web: www.silanis.com

We make paperless happen®

.

Silanis Technology Inc.
8200 Decarie
3rd Floor
Montreal, Quebec
H4P 2P5
CANADA

Phone: 1-888-SILANIS
Fax: (514) 337-5258
E-mail: CustomerAdvocates@silanis.com

Remember to visit our Web site at: http://www.silanis.com
and our Resource Center at: http://www.silanis.com/resource-center.html

Protected by United States patents 5,606,609; 6,751,632; 6,912,660; 6,931,420; and 7,340,608; Canadian patent 2,340,780; European patents 1,153,352; 1,116,110; and 1,270,179; and Australian patents AU 2,002,215,782; and AU 2,003,204,747. Patents pending in the United States, Canada, Europe, and other countries.

ApproveIt®, One Pen®, We Automate the Business Approval Process®, Process Signature®, Intelligent Signature®, and We Make Paperless Happen® are registered trademarks of Silanis Technology Inc. in the United States and/or other countries. Adobe® and Acrobat Reader® are registered trademarks of Adobe Systems Incorporated. SignatureGem™ is a trademark of Topaz Systems Incorporated. Microsoft®, Windows®, Windows NT®, Office®, Outlook®, Word®, and Excel® are registered trademarks of Microsoft Corporation.

THE CONTENT AND RELATED GRAPHICS PUBLISHED HEREIN COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. SILANIS TECHNOLOGY RESERVES THE RIGHT TO CHANGE ANY AND ALL INFORMATION CONTAINED HEREIN AT ANY TIME WITHOUT NOTICE.

CONTENTS

CONTENTS

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.

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

TERM	DEFINITION
Advertising	A Windows Installer feature with which ApproveIt Desktop automatically installs and configures itself for subsequent users.
Deployment	The process of installing an application across a network on multiple target computers, for multiple users.
Elevated privileges	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.
Installation "Push"	The term "push" 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.
Managed application	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.
Non-administrative user	A user who does not have administrative privileges on the local computer.
Package	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.
Per-machine installation	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.
Per-user installation	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 "All Users" profile.
Source	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.
Subsequent users	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.
System privileges	System privileges are also known as elevated privileges. See "elevated privileges".

Table 1: Terminology

TERM	DEFINITION
Transform	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.
MSI	The Windows Installer technology.
Windows Installer Policies	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.

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.

WINDOWS INSTALLER MACHINE POLICIES		
Registry Location	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer	
AlwaysInstallElevated	REG_DWORD	If you are pushing the ApproveIt Desktop installation to non-administrative users, this policy must be set to “1”. Otherwise, the ApproveIt Desktop installation will fail to add/modify system components and settings. If this value is set to “1” and the corresponding user value is also set, the installer always installs with elevated privileges. Otherwise, the installer uses elevated privileges to install managed applications and uses the current user's privilege level for non-managed applications.
AllowLockdownBrowse	REG_DWORD	If this policy value is set to “1”, non-administrative users can browse for new sources while running an installation at elevated privileges. The default is that only administrators can browse for sources during an elevated installation. Setting this policy also enables non-administrative users to run programs at LocalSystem privileges during an elevated installation.
AllowLockdownMedia	REG_DWORD	If you are deploying ApproveIt Desktop using per-machine installations from a CD, you must set this policy to “1”. Otherwise, the ApproveIt Desktop installation will fail for subsequent non-administrative users. If this policy value is set to “1”, non-administrative users can use media sources, such as a CD-ROM, while running an installation at elevated privileges. The default is that only administrators can use media sources during an elevated installation. Setting this policy also enables non-administrative users to run programs at LocalSystem privileges during an elevated installation.

Table 2: Windows Installer Machine Policies

WINDOWS INSTALLER MACHINE POLICIES		
DisableMSI	REG_DWORD	This policy should be absent or set to "0" for the ApproveIt Desktop installation to work. If this value exists and is set to "2", the installer is always disabled for all applications. If this value is set to "1", the installer is disabled for non-managed applications but is still enabled for managed applications. If this value is set to "0", any other number, or is absent, the installer is always enabled.
Logging	REG_SZ	This policy is not required but may be useful in debugging problematic installations. If such problems occur, set this policy to "iwearicmopv". This combination of logging settings produces the most useful log files. This policy is used only if logging has not been enabled by the "/L" command line option or MsiEnableLog. If policy is set in this case, **a log file is created in the temp directory with the random name: MSI*.LOG**. Specify the logging mode by setting the policy value to a string of characters. Use the same characters to specify logging mode policy as used by the '/L' command line option.

Table 2: Windows Installer Machine Policies

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

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.

WINDOWS INSTALLER USER POLICIES		
REGISTRY LOCATION	**HKEY_CURRENT_USER\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\INSTALLER**	
AlwaysInstallElevated	REG_DWORD	If you are pushing the ApproveIt Desktop installation to non-administrative users, this policy must be set to "1". Otherwise, the ApproveIt Desktop installation will fail to add/modify system components and settings. If this value is set to "1" and the corresponding machine value is also set, the installer always installs with elevated privileges. Otherwise, the installer uses elevated privileges to install managed applications and uses the current user's privilege level for non-managed applications.

Table 3: Windows Installer User Policies

WINDOWS INSTALLER USER POLICIES		
DisableMedia	REG_DWORD	If you are distributing ApproveIt Desktop across your network using CR-ROMs, this policy should be absent or set to “0”. If the DisableMedia policy is set to “1”, users and administrators running a maintenance installation of one product are prevented from using the Browse Dialog to browse media sources, such as CD-ROM, for the sources of other products that can be installed. Browsing for other products is prevented regardless of whether the installation is with elevated privileges. It is still possible for the user to reinstall the product from media if the user has a correctly labeled media source.

Table 3: Windows Installer User Policies

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

ALLUSERS Property

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.

WINDOWS 2000 / WINDOWS XP	ALLUSERS = NULL	ALLUSERS = 1	ALLUSERS = 2
User access privileges.	Per-user installation using folders in user's personal profile.	Not valid; returns an error stating the user does not have enough access privileges to install application.	Per-user installation using folders in user's personal profile.
Administrator access privileges.	Per-user installation using folders in user's personal profile.	Per-machine installation using folders in “All Users” profile.	Per-machine installation using folders in “All Users” profile.

Table 4: ALLUSERS Property

The information in the preceding table 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.

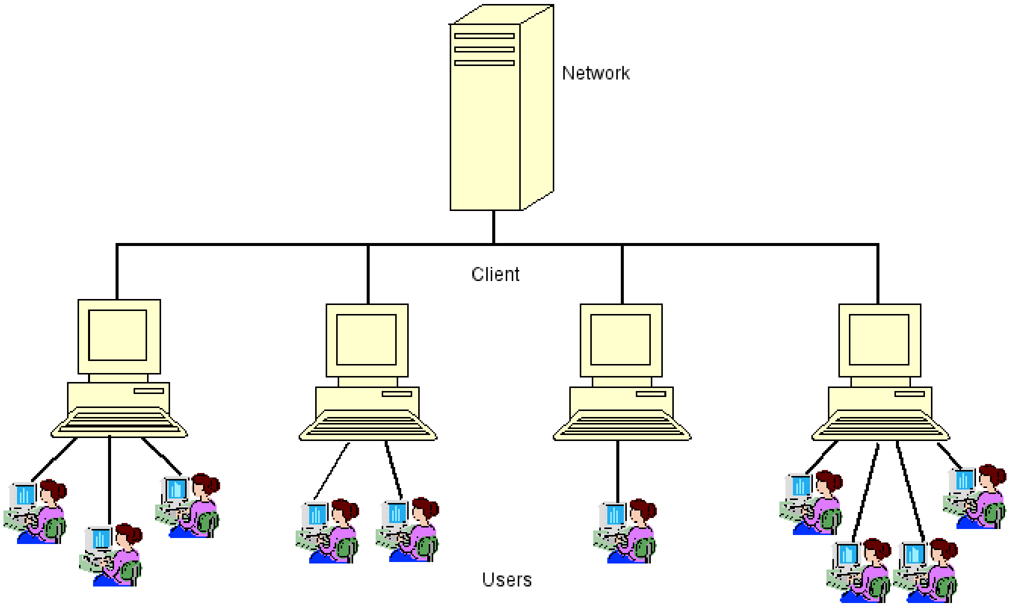


Figure 1: Typical Network Topology for Deploying ApproveIt Desktop

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.

The following deployment scenario is strictly given as tested example and guidelines. Other deployment mechanisms exist, but haven't necessarily been tested by Silanis. If you are using a third party deployment tool (e.g. SMS, Tivoli, Unicenter, Active Directory, etc.), consult with the vendor on how to deploy Windows Installer (MSI) packages. Most of these packages have built-in functionality.

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 **C:\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.

Information for customization using Windows Installer Transforms can be found at: http://msdn.microsoft.com/library.

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.
4. **Instmsiw.exe**, the Windows Installer installation 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= /l*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.

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 **PDFDACEngine.dll** (for Adobe Acrobat). The default URL for ApproveIt Desktop products is **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.

COMMAND	VALUE (HEX)	VALUE (DECIMAL)
Approve	0X0000001	1
Authenticate	0x00000002	2
Secure Print	0x00000004	4
Undo Last	0x00000008	8
Save Unsigned	0x00000010	16
Configuration	0x00000020	32
About ApproveIt	0x00000040	64
Protect Document (Word only)	0x00000080	128
Protect Sheet (Excel only)	0x00000100	256
Protect Workbook (Excel only)	0x00000200	512
Batch Approve	0x00000400	1024
Batch Authenticate	0x00000800	2048
Batch Secure Print	0x00001000	4096
Proponent Prepare	0x00002002	8192
Proponent Prepare Send	0x00004000	16384
Proponent Invite	0x00008000	32768
Batch Approve Folder	0x00010000	65536
Batch Authenticate Folder	0x00020000	131072
Batch Secure Print Folder	0x00040000	262144

Figure 2: Registry Key Values

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).

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]"**.

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

Table 5: Formatting Codes for Time Format

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

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.

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

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**.

- **APRV_SIGNING_DISPLAY_CUSTOMUNAPPROVEDTEXTSIZE** — This is the size of the font used to display the text that appears in the Signature Block before a signature is applied. The default value is **96**.

Customizing Signature Size

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

- **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 **APRV_HKLM_PREFS_CERTPOLICY** to **[CP Identifier]** to list only certificates that may be used under the certificate policy **[CP Identifier]**.
2. Set the property **APRV_HKLM_PREFS_ISSUERSUBSTR** to **[Issuer CA]** to list only certificates with **[issuer CA]** as a substring of the issuer distinguished name.
3. Set the property **APRV_HKLM_PREFS_LISTONLYSIGCERT** to **1** to list only certificates that can be used for signing.
4. Set the property **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 **.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 **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 **APRV_HKLM_PREFS_**

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

HKEY_LOCAL_MACHINE\SOFTWARE\SILANIS\APPROVEIT\PREFS\FAILIFNOMATCHFOUND	
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.
Type	String (REG_SZ)
Default	1

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 following table comes from the “Platform SDK: Windows Installer", which can be found at: http://msdn.microsoft.com/library.

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/). The following table describes the command line options for this program.

OPTION	PARAMETER	DEFINITION
/I	Package|ProductCode	Installs or configures a product.

Table 8: Command Line Options

OPTION	PARAMETER	DEFINITION
/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 “/l*v”.

Table 8: Command Line Options

OPTION	PARAMETER	DEFINITION
/m	filename	Generates an SMS status .mif file. Must be used with either the install (-i), remove (-x), administrative installation (-a), or reinstall (-f) options. The ISMIF32.DLL is installed as part of SMS and must be on the path. The fields of the status mif file are filled with the following information: •Manufacturer - Author •Product - Revision Number •Version - Subject •Locale - Template •Serial Number - not set •Installation - set by ISMIF32.DLL to “DateTime” InstallStatus - “Success” or “Failed” Description - Error messages in the following order: 1) Error messages generated by installer. 2) Resource from Msi.dll if install could not commence or user exit. 3) System error message file. 4) Formatted message: “Installer error %i”, where %i is error returned from Msi.dll
/p	PatchPackage	Applies a patch. To apply a patch to an installed administrative image you must combine options as follows: /p *<PatchPackage>* /a *<Package>*
/q	n|b|r|f	Sets user interface level. q, qn - No UI qb - Basic UI. Use qb! to hide the Cancel button. qr - Reduced UI with no modal dialog box displayed at the end of the installation. qf - Full UI and any authored FatalError, User Exit or Exit modal dialog boxes at the end. qn+ - No UI except for a modal dialog box displayed at the end. qb+ - Basic UI with a modal dialog box displayed at the end. The modal box is not displayed if the user cancels the installation. Use qb+! or qb!+ to hide the Cancel button. qb- - Basic UI with no modal dialog boxes. Please note that /qb+- is not a supported UI level. Use qb-! or qb!- to hide the Cancel button. Note that the ! option is available with Windows Installer version 2.0 and works only with basic UI. It is not valid with full UI.
/? or /h		Displays copyright information for the Windows Installer.
/y	module	Calls the system API Dll-RegisterServer to self-register modules passed in on the command line. For example, msiexec /y my_file.dll. This option is used only for registry information that cannot be added using the registry tables of the .msi file.
/z	module	Calls the system API DllUn-RegisterServer to unregister modules passed in on the command line. For example, msiexec /z my_file.dll. This option is used only for registry information that cannot be removed using the registry tables of the .msi file.

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 /l and /q can be used with /i, /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 4of ApproveIt Desktop.

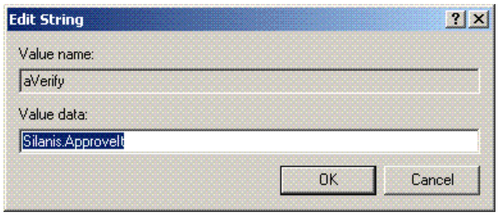
Please note that during the upgrade, the ePersona (.cps) files, the reports and the log files created by previous ApproveIt versions are neither deleted nor replaced. However, for added security, you may want to save all current ePersona files before performing an upgrade.

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**.



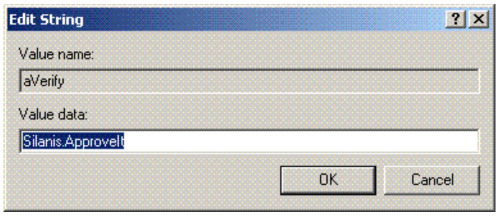
Value name: aVerify

Value data: Silanis.ApproveIt

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**.



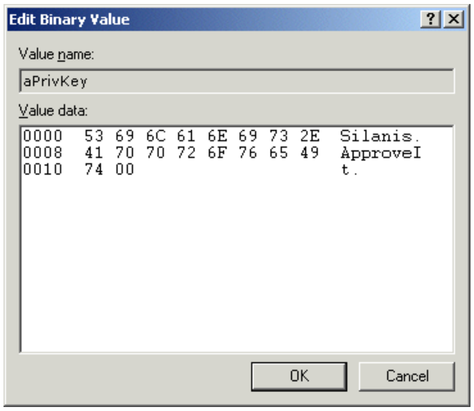
Value name: aVerify

Value data: Silanis.ApproveIt

Setting Signature Preferences in Acrobat 7

In Acrobat 7.0, users can sign documents using the Acrobats 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**).



Value name:

aPrivKey

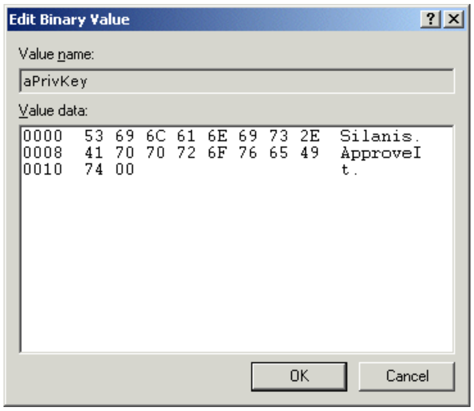
Value data:

```
0000   53 69 6C 61 6E 69 73 2E   Silanis.
0008   41 70 70 72 6F 76 65 49   ApproveI
0010   74 00                     t.
```

Setting Signature Preferences in Acrobat 6

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**).



Value name:

aPrivKey

Value data:

```
0000   53 69 6C 61 6E 69 73 2E   Silanis.
0008   41 70 70 72 6F 76 65 49   ApproveI
0010   74 00                     t.
```

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**).

The administrator may want to pre-install the root certificate and all the required intermediate CAs from the PKI using the **add** and **cache** options. The resulting **certs.db** can then be distributed to the users (in the Support folder). This will minimize the number of future LDAP connections.

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:

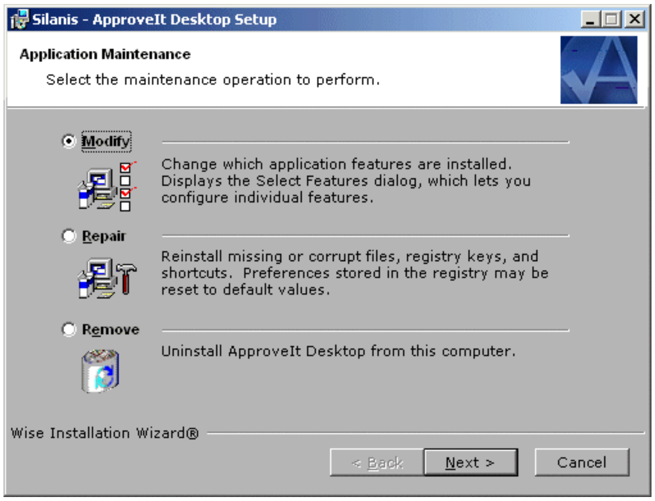
1. Move both databases in an unrestricted location, for example **C:/ApproveItDatabases**.
2. Open the file **srl.cfg**, which can be found under **C:/Program Files/ApproveIt/Support** and modify the PATH entry so that it points to a location where ApproveIt users have write access.

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.



Application Maintenance

Select the maintenance operation to perform.

● Modify

Change which application features are installed. Displays the Select Features dialog, which lets you configure individual features.

○ Repair

Reinstall missing or corrupt files, registry keys, and shortcuts. Preferences stored in the registry may be reset to default values.

○ Remove

Uninstall ApproveIt Desktop from this computer.

Wise Installation Wizard®

Figure 1: Application Maintenance

Explanation

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

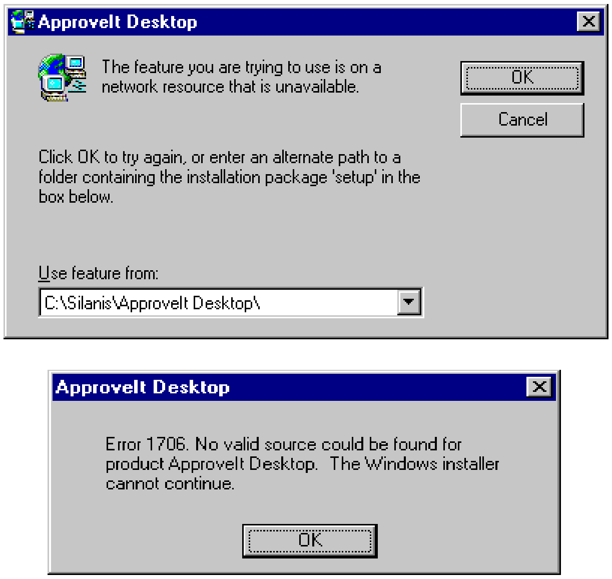
Solution

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.



The feature you are trying to use is on a network resource that is unavailable.

Click OK to try again, or enter an alternate path to a folder containing the installation package 'setup' in the box below.

C:\Silanis\ApproveIt Desktop\

Error 1706. No valid source could be found for product ApproveIt Desktop. The Windows installer cannot continue.

Figure 2: Network Resource Unavailable and Error 1706

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**.

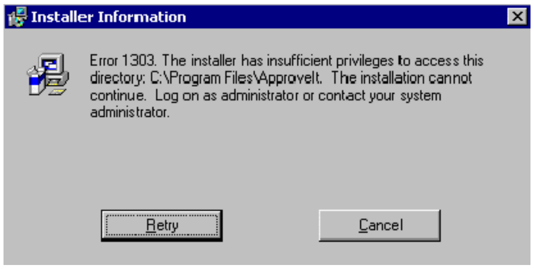
Solution

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:



Error 1303. The installer has insufficient privileges to access this directory: C:\Program Files\ApproveIt. The installation cannot continue. Log on as administrator or contact your system administrator.

Figure 3: Installer Information - Error 1303

Explanation

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

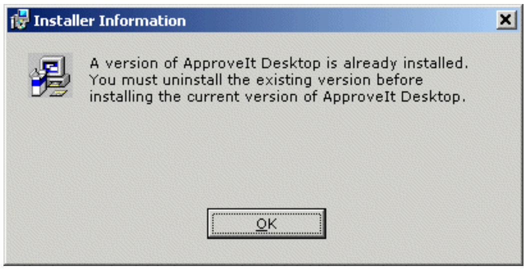
Solution

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:



A version of ApproveIt Desktop is already installed. You must uninstall the existing version before installing the current version of ApproveIt Desktop.

Figure 4: Installer Information

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.

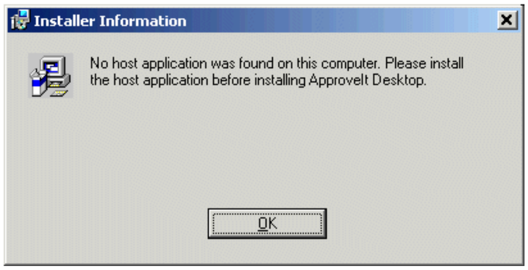
Solution

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.**



Installer Information

No host application was found on this computer. Please install the host application before installing ApproveIt Desktop.

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.

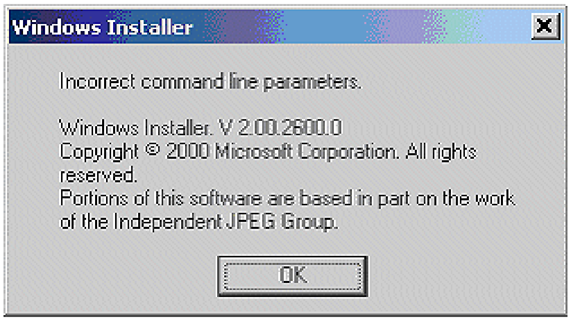
Solution

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

Incorrect command line parameters.

Windows Installer. V 2.00.2600.0
Copyright © 2000 Microsoft Corporation. All rights reserved.
Portions of this software are based in part on the work of the Independent JPEG Group.

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.