



PDF Creation Date:

August 4, 2008

Document Security User Guide

for Acrobat 9.0 and Adobe Reader 9.0

Acrobat® and Adobe® Reader®

Version 9.0

© 2008 Adobe Systems Incorporated. All rights reserved.

Document Security User Guide for Adobe® Acrobat 9.0 and Adobe® Reader 9.0 on Windows® and Macintosh®.

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names in sample templates are for demonstration purposes only and are not intended to refer to any actual organization.

Adobe, Acrobat, Reader, and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Windows®, Windows NT®, and Windows XP® are registered trademarks of Microsoft® Corporation registered in the United States and/or other countries. Mac® and Macintosh® are registered trademarks of Apple Computer®, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA. Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Contents

1	Getting Started	7
1.1	What's in this Guide?	7
1.2	Who Should Read This Guide?	7
1.3	How Should You Use This Guide?	8
1.4	Roadmap to Security Documentation	8
2	Getting and Using Your Digital ID.....	10
2.1	Digital ID Basics.....	10
2.1.1	What is a Digital ID?	10
2.1.2	Digital ID Storage Mechanisms	11
2.1.3	Registering a Digital ID for Use in Acrobat	12
2.1.4	Digital ID Management and the Security Settings Console.....	13
2.1.5	Setting Identity Information.....	13
2.2	Generic ID Operations	14
2.2.1	Specifying Digital ID Usage.....	14
2.2.2	Sharing (Exporting) a Digital ID Certificate	15
2.2.3	Viewing All of Your Digital IDs	15
2.2.4	Customizing a Digital ID Name	16
2.2.5	Viewing Digital ID Certificates in the Certificate Viewer	16
2.3	Managing PKCS#12 Digital ID Files	17
2.3.1	Logging in to a Digital ID File.....	18
2.3.2	Finding an Existing Digital ID in a PKCS#12 File	18
2.3.3	Adding and Removing Digital ID Files from the File List.....	19
2.3.4	Changing an ID File's Password	19
2.3.5	Changing a PKCS#12 File's Password Timeout.....	20
2.3.6	Logging in to PKCS#12 Files	21
2.3.7	Creating a Self-Signed Digital ID.....	21
2.3.8	Deleting a PKCS#12 Digital ID.....	24
2.4	Managing Windows Digital IDs	25
2.4.1	Finding a Digital ID in a Windows Certificate Store File	25
2.4.2	Deleting a Digital ID from the Windows Certificate Store	25
2.5	Managing Roaming ID Accounts and IDs.....	25
2.5.1	Adding a Roaming ID Account to Get a Roaming ID	26
2.5.2	Logging in to a Roaming ID Account	26
2.6	Managing IDs Accessible via PKCS#11 Devices.....	27
2.6.1	Adding an ID that Resides on External Hardware.....	27
2.6.2	Changing Passwords	28
2.6.3	Logging in to a Device	29
3	Managing Certificate Trust and Trusted Identities	30
3.1	What is a Trusted Identity?	30
3.2	Adding Someone to Your Trusted Identity List.....	32
3.2.1	Adding a Certificate From a Signature	32
3.2.2	Requesting a Digital ID via Email	33
3.2.3	Importing a Certificate From a File.....	33

3.2.4 Searching for Digital ID Certificates	34
3.3 Certificate Trust Settings.....	36
3.3.1 Setting Certificate Trust.....	37
3.3.2 Setting Certificate Policy Restrictions	39
3.3.3 Using Certificates for Certificate Security (Encryption).....	40
3.4 Using Directory Servers to Add Trusted Identities	40
3.4.1 Manually Configuring a Directory Server.....	41
3.4.2 Editing Directory Servers Details	42
3.4.3 Deleting a Directory Server	42
3.4.4 Specifying a Default Directory Server	43
3.4.5 Importing and Exporting Directory Server Settings	43
3.5 Managing Contacts.....	43
3.5.1 Viewing and Editing Contact Details.....	43
3.5.2 Emailing Certificate or Contact Data	44
3.5.3 Saving Certificate or Contact Details to a File	44
3.5.4 Associating a Certificate with a Contact.....	45
3.5.5 Changing a Trusted Identity's Certificate Association	45
3.5.6 Deleting Contacts and Certificates.....	46
4 Document Security Basics.....	48
4.1 Security Method Basics	48
4.1.1 Choosing a Security Method Type	49
4.1.2 Security Policies.....	50
4.1.3 Security Methods and Encryption	50
4.1.3.1 Encryption Workflow	50
4.1.3.2 Choosing What to Encrypt	51
4.1.3.3 Choosing an Algorithm	51
4.1.4 Security Methods and Permissions	52
4.1.4.1 Permissions Workflow.....	53
4.1.4.2 Permissions Options.....	53
4.1.5 Associating Batch Processing with a Security Method	54
4.2 Changing and Viewing Security Settings	55
4.2.1 Viewing Document Encryption and Permission Settings.....	55
4.2.2 Viewing Document Restrictions.....	56
4.2.3 Viewing Security Settings in a Browser	57
4.2.4 Changing the Security Method Type	57
4.2.5 Editing Security Method Settings.....	58
4.2.6 Removing Document Security.....	58
4.3 Security Policies: Reusable Security Settings	59
4.3.1 Creating Security Policies with Policy Manager	60
4.3.2 Applying a Security Policy to a Document.....	60
4.3.3 Viewing a Security Policy	61
4.3.4 Copying a Security Policy	61
4.3.5 Editing a Security Policy.....	61
4.3.6 Making a Security Policy Favorite.....	62
4.3.7 Refreshing the Security Policy List	62
4.3.8 Deleting a Security Policy	62
4.4 Envelopes	63
5 Password Security	65
5.1 Creating Password Security Settings	66

5.1.1	Creating a Reusable Password Security Policy.....	66
5.1.2	Creating Password Security for One-Time Use	69
5.2	Opening a Password-Protected Document	72
5.3	Removing Password Security	72
5.4	Changing Document Collection Passwords.....	72
5.5	Password Recovery.....	73
6	Certificate Security	74
6.1	Setting up the Certificate Security Environment	75
6.1.1	Accessing the Windows Certificate Store	75
6.1.2	Selecting a Certificate to Use for Encryption.....	76
6.2	Working with Groups of Contacts	77
6.2.1	Creating a Group	77
6.2.2	Adding or Removing Group Contacts.....	77
6.2.3	Deleting a Group	78
6.3	Creating Certificate Security Settings.....	78
6.3.1	Creating a Reusable Certificate Security Policy	78
6.3.2	Creating Certificate Security for the Current Document.....	82
6.3.3	Applying a Certificate Security Policy	87
6.3.4	Applying a Certificate Security to a Group.....	87
6.3.5	Opening a Certificate-Protected Document.....	88
7	LiveCycle Rights Management Server Security	90
7.1	Configuring Servers.....	90
7.1.1	Importing ALCRMS Settings from an FDF file	91
7.1.2	Importing ALCRMS Settings with a Security Settings Import	91
7.1.3	Configuring ALCRMS Settings Manually.....	91
7.1.4	Managing your ALCRMS Account	92
7.2	Working with Documents and ALCRMS Policies	92
7.2.1	Creating an ALCRMS Security Policy	92
7.2.2	Applying ALCRMS Security	93
7.2.3	Refreshing the Security Policy List	93
7.2.4	Synchronizing a Document for Offline Use.....	94
7.2.5	Revoking a Document	94
7.2.6	View a Document's Audit History.....	94
8	External Content and Document Security.....	95
8.1	Enhanced Security	95
8.1.1	Enabling Enhanced Security.....	96
8.1.2	Changes in FDF Behavior.....	97
8.1.3	Interaction with Trust Manager.....	98
8.1.4	Make Privileged Folder Locations Recursive	98
8.2	Controlling Multimedia	98
8.2.1	Configuring Multimedia Trust Preferences.....	99
8.2.2	Controlling Multimedia in Certified Documents.....	100
8.3	Setting JavaScript Options.....	101
8.3.1	High Privilege JavaScript Defined	101
8.3.2	Javascript and Certified Documents.....	102
8.4	Adobe Trusted Identity Updates	103
8.5	Working with Attachments	103
8.5.1	Default Behavior: Black and White Lists	103

8.5.2 Adding Files to the Black and White Lists	107
8.5.3 Resetting the Black and White Lists	108
8.5.4 Allowing Attachments to Launch Applications.....	108
8.6 Controlling Access to Referenced Files and XObjects.....	109
8.7 Internet URL Access	109
8.7.1 Turning Internet Access Off and On	110
8.7.2 Allowing and Blocking Specific Web Sites	111
9 Migrating and Sharing Security Settings	112
9.1 Security Setting Import and Export.....	112
9.1.1 Exporting Security Settings to a File.....	112
9.1.2 Importing Security Settings from a File.....	113
9.1.3 Importing Security Settings from a Server	115
9.2 Sharing Settings & Certificates with FDF	115
9.2.1 FDF Files and Security	117
9.2.2 Exporting Application Settings with FDF Files	118
9.2.2.1 Distributing a Trust Anchor or Trust Root.....	118
9.2.2.2 Setting the Certificate Trust Level	121
9.2.2.3 Exporting Your Certificate	121
9.2.2.4 Emailing Your Certificate	122
9.2.2.5 Saving Your Digital ID Certificate to a File	123
9.2.2.6 Requesting a Certificate via Email	124
9.2.2.7 Emailing Server Details.....	125
9.2.2.8 Exporting Server Details.....	126
9.2.3 Importing Application Settings with FDF Files.....	127
9.2.3.1 Responding to an Email Request for a Digital ID	127
9.2.3.2 Importing Someone's Certificate	129
9.2.3.3 Importing Multiple Certificates.....	130
9.2.3.4 Importing Timestamp Server Settings.....	132
9.2.3.5 Importing Directory Server Settings.....	134
9.2.3.6 Importing Adobe LiveCycle Rights Management Server Settings	135
9.2.3.7 Importing Roaming ID Account Settings.....	136
9.2.3.8 Importing a Trust Anchor and Setting Trust	138
10 Glossary of Security Terms	141
11 Index.....	144

1 Getting Started

1.1 What's in this Guide?

This guide describes the document security features of the Acrobat 9.x family of products:

- Working with digital IDs that are used for signing and certificate security workflows:
 - [Chapter 2, "Getting and Using Your Digital ID"](#)
 - [Chapter 3, "Managing Certificate Trust and Trusted Identities"](#)
- Security method and policies:
 - [Chapter 4, "Document Security Basics"](#)
 - [Chapter 5, "Password Security"](#)
 - [Chapter 6, "Certificate Security"](#)
 - [Chapter 7, "LiveCycle Rights Management Server Security"](#)
- Securing the application environment:
 - ["Controlling Multimedia" on page 98](#)
 - ["Setting JavaScript Options" on page 101](#)
 - ["Working with Attachments" on page 103](#)
 - ["Controlling Access to Referenced Files and XObjects" on page 109](#) (only available in 7.0.5 and later)
 - ["Internet URL Access" on page 109](#)
- Sharing certificates and server settings with data exchange files:
 - ["Importing Application Settings with FDF Files" on page 127](#)
 - ["Exporting Application Settings with FDF Files" on page 118](#)

1.2 Who Should Read This Guide?

End users: This document describes how to configure and use the application user interface, register a digital ID for use in Acrobat, and manage other people's public key certificates within your system.

Administrators: This document describes how to configure and use the application user interface. Because system administrators may be responsible for deploying and supporting the Adobe Acrobat family of products (including Adobe Reader) in document security workflows, leverage this guide to help your clients use the product correctly and effectively. This guide should be used in conjunction with the *Acrobat Security Administrator Guide*.

1.3 How Should You Use This Guide?

If you are setting up a document security workflow for the first time, do not have a digital ID, or have not specified which certificates to use for encryption, read [Chapter 2, “Getting and Using Your Digital ID”](#) and [Chapter 3, “Managing Certificate Trust and Trusted Identities”](#). In enterprise settings, the administrator may issue you an ID (or provide instructions on getting one) and may also set up your application to that it can verify (trust) signatures.

If you haven’t used security methods before, don’t know which type to use, and are unfamiliar with why security policies are beneficial, read [Chapter 4, “Document Security Basics”](#).

If you need to learn about a specific type of security method, see one of the following:

- [Chapter 5, “Password Security”](#)
- [Chapter 6, “Certificate Security”](#)
- [Chapter 7, “LiveCycle Rights Management Server Security”](#)

If you are concerned about securing the application environment and controlling document and application access to external content such as the Internet and attachments, see [Chapter 8, “External Content and Document Security”](#).

If you need to share your certificate or server settings with someone, see [Chapter 9, “Security Setting Import and Export”](#).

1.4 Roadmap to Security Documentation

In many enterprise environments, there is no clear distinction between audience types. Some end users are “power users” and don’t shy away from modifying the registry and tweaking applications in admin-like ways. Some system administrators are highly technical and perform developer-like tasks such as PERL programming and JavaScript scripting. For this reason, it is up to the reader to determine what documents listed in [Table 1](#) are pertinent to their tasks. However, this document uses the following definitions:

- **User or end user:** End users usually have their application installed and preconfigured by an administrator. They only interact with the graphical user interface and do not modify the registry. Some end users, such as document authors, may use simple JavaScripts to set seed values on documents.
- **Administrator:** System administrators install and configure end user machines. More often than not, they use the installer wizard to configure the product installer prior to deploying applications across the enterprise. Because the end user experience can be controlled by the registry, administrators must be familiar with both the application’s user interface and capabilities as well as the options for registry configuration.
- **Developer:** Developers typically try to find programmatic ways to generate or process PDF documents. They read specifications and API documents to figure out how to solve real-world enterprise problems without requiring manual human intervention. Communication with servers is often a requirement. Because enterprise solutions often involve understanding application behavior, developers sometimes need to review administration guides to learn how to deploy plugins or handlers and to learn how to configure the application to use those components. Many of the application’s registry settings can be accessed and manipulated via JavaScript.

Note: The most recent document versions may be found online at <http://www.adobe.com/devnet/acrobat/>.

Table 1 Documentation related to Acrobat security

Document	Audience	For information about
<i>Acrobat SDK Documentation Roadmap</i>	Developers	A guide to the documentation in the Adobe Acrobat SDK.
<i>Acrobat and PDF Library API Reference</i>	Developers	A description of the APIs for Acrobat and Adobe Reader® plug-ins, as well as for PDF Library applications.
<i>JavaScript for Acrobat API Reference</i>	Developers	A listing of the Acrobat JavaScript APIs.
<i>Developing Acrobat Applications with JavaScript</i>	Developers	Additional detail about the Acrobat JavaScript APIs.
<i>PDF Reference 1.7</i>	Developers	A detailed description of the PDF language.
<i>FDF Data Exchange Specification</i>	Developers	A object-level FDF file description. The files can be generated programmatically and used to share security-related data.
<i>PDF Signature Build Dictionary Specification</i>	Developers	Build properties for the PDF Reference's signature dictionary which provides interoperability details for 3rd party handlers.
<i>Digital Signature Appearances</i>	Developers & administrators	Guidelines for creating signatures programmatically.
<i>Guidelines for Developing CSPs for Acrobat on Windows</i>	Developers & administrators	Guidelines for developing a Cryptographic Service Provider for use with Acrobat® on the Windows® platform.
<i>Acrobat <version> Security Administration Guide</i>	Administrators	Application deployment and configuration in enterprise settings.
<i>Acrobat <version> Digital Signature User Guide</i>	Administrators & end users	Application usage and configuration via the user interface.
<i>Acrobat <version> Document Security User Guide</i>	Administrators & end users	Application usage and configuration via the user interface.
<i>Acrobat <version> Security FDF User Guide</i>	Administrators & end users	A subset of the user guides that describe how to export and import security settings and certificate data with an FDF file.
<i>Digital Signatures in the PDF Language</i>	Anyone needing an overview	A generic description of how signature work in PDF.
<i>Digital Signatures in Acrobat</i>	Anyone needing an overview	A description of how signatures are implemented in Acrobat.
<i>Enhanced Security in Acrobat 9 and Adobe Reader 9</i>	Anyone needing an overview	A description of new features that can make the application's working environment more secure.

A digital ID is like a driver's license or passport or other "certified by some entity" paper identification. It proves your identity to people and institutions that you communicate with electronically. These IDs are a critical component of digital signatures and certificate security. In signing and certificate security workflows, you will be asked to select a digital ID. Selecting an ID is simply a matter of picking one from a list of your previously installed digital IDs. If you do not have a digital ID, you will be prompted to find or create one.

For more information, refer to the following:

- ["Digital ID Basics" on page 10](#)
- ["Generic ID Operations" on page 14](#)
- ["Managing PKCS#12 Digital ID Files" on page 17](#)
- ["Managing Windows Digital IDs" on page 25](#)
- ["Managing Roaming ID Accounts and IDs" on page 25](#)
- ["Managing IDs Accessible via PKCS#11 Devices" on page 27](#)

2.1 Digital ID Basics

2.1.1 What is a Digital ID?

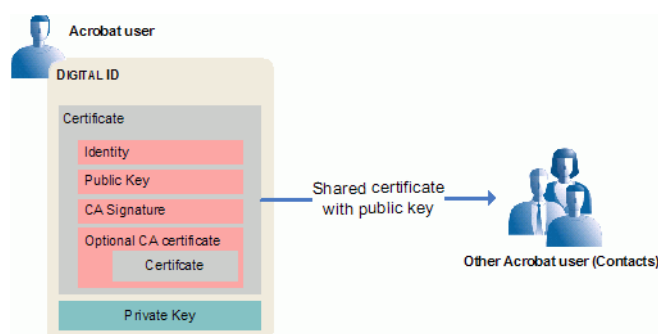
A digital ID consists of two main parts: a certificate and a private key. A certificate consists of your identity information (name, date, serial number, etc.) and a public key that are bound together and signed by a trusted or untrusted certificate authority. The certificate sometimes includes a reference to the certificate issuer's certificate, thereby creating what is known as a "certificate chain."

Digital IDs operate by using a key pair: data encrypted with one key can only be decrypted by the other corresponding key. When you sign PDF documents, you use the private key to apply your digital signature. You distribute the certificate that contains your public key to those who need to validate your signature or encrypt information for you. Only your private key can unlock information that was encrypted using your public key, so be sure to store your digital ID in a safe place.

You must have a digital ID to sign, certify, and apply certificate encryption to PDFs. You can get a digital ID from a third-party provider, or you can create a self-signed digital ID. Self-signed digital IDs may be adequate for many situations. However, to prove your identity in most business transactions, you may need a digital ID from a trusted third-party provider, called a certificate authority. Because the certificate authority is responsible for verifying your identity to others, choose one that is trusted by major companies doing business on the Internet.

You can have multiple digital IDs for different purposes. For example, you may sign documents in different roles or using different certification methods. Digital IDs are usually password protected and can be stored on your computer in password protected file, on a smart card or hardware token, in the Windows certificate store, or on a signing server (for roaming IDs). Acrobat applications include a default signature handler that can access digital IDs from any of these locations.

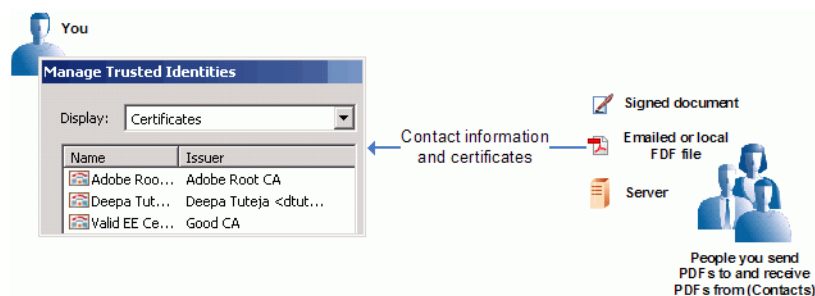
Figure 1 Digital ID: Components



Users exchange their digital ID's certificate so that they can validate signatures and encrypt documents for each other. Shared certificates can be physically sent in a file or made available over a network. The private key is never shared and is used to decrypt documents. There are several ways to share certificates:

- **Physical sharing:** Certificates can be physically shared in a file sent via email or located in a shared directory. They can be imported, exported, and otherwise managed with the Trusted Identity Manager. For details, see [Chapter 3, "Managing Certificate Trust and Trusted Identities"](#).
- **Network sharing:** Certificates can be stored on a central server. The Trusted Identity Manager can be used to search for certificates on LDAP directory servers. Adobe applications provide tools for configuring and managing directory servers. For details, see ["Using Directory Servers to Add Trusted Identities" on page 40](#).

Figure 2 Digital ID: From others



2.1.2 Digital ID Storage Mechanisms

A digital ID's certificate and private key need to be stored in a secure location. There are several file types and file locations where these items could be stored ([Table 2](#)). The digital ID data in these files is provided to the application via digital ID service providers (sometimes called Cryptographic Service Providers or CSPs). A service provider is simply a storage mechanism and code that makes the data available to the application.

In most cases, the digital ID is stored on a local or networked file. Common locations include the Windows Certificate Store which is accessible by Adobe applications and other Windows applications and the Acrobat store which is used only by the Acrobat family of products. Some IDs may exist only on external hardware such as a smart card connected to the computer.

The Acrobat family of products can access a digital ID from the following storage mechanisms:

- **Windows Certificate Store:** A local store (file location) provided by Windows that can import and export various file formats and that can be used by both Windows programs and Acrobat products.

- **PKCS#12 files:** A common file format that contains the entire digital ID and is used on both Windows and Macintosh.
- **PKCS#11 devices:** External devices such as a USB token or smart card that store digital ID data.
- **Roaming ID servers:** The private key is known only to a remote server. The server sends the certificate and its public key to users on demand. Users can import and export the certificate and its public key from Acrobat, but they never have access to the private key.

Table 2 Digital ID-related file types

Type	Description	5.x	6.x	7.x	8.x	9.x
.acrobat security	An XML format encapsulated in a PDF which stores security settings for import and export. Contains: Digital ID (public and private keys)					Export Import
PKCS#12: .pfx (Win), .p12 (Mac)	Personal Information Exchange Syntax Standard: Specifies a portable, password protected, and encrypted format for storing or transporting certificates. Contains: Digital ID (public and private keys)		Export Import	Export Import	Export Import	Export Import
.fdf	An Adobe file data exchange format used for importing and exporting settings and certificates (usually PKCS#12 files).	Export Import	Export Import	Export Import	Export Import	Export Import
PKCS#7: .p7b, .p7c	Certificate Message Syntax (CMS): Files with .p7b and .p7c extensions are registered by the Windows OS. Acrobat products can import and export these files. Contains: Certificate and public key only		Export Import	Export Import	Export Import	Export Import
.cer	Certificate format: A Microsoft format for digital IDs usually stored in the Windows Certificate Store. Contains: Certificate and public key only		Export Import	Export Import	Export Import	Export Import
.apf	Adobe Profile Files (Legacy): Not used after Acrobat 5. Files can be upgraded by double clicking them. Contains: Digital ID (public and private keys)	Import Export	Import	Import	Import	n/a

2.1.3 Registering a Digital ID for Use in Acrobat

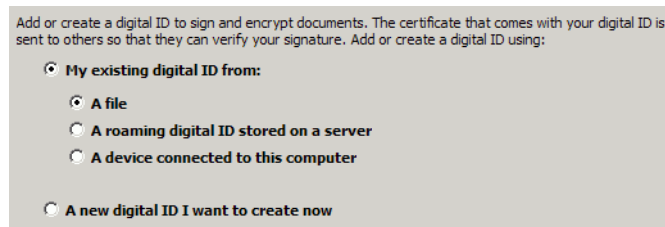
Digital IDs help you sign, certify, and apply certificate security to documents. There are two ways to register a digital ID:

- **In advance:** You can set up the ID ahead of time for later use. To do so, choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**, selecting **Digital IDs** in the left-hand tree, and then choosing **Add ID**.
- **On the fly:** You can find or add IDs in signature and certificate security workflows. For example, when the Sign Document dialog appears, choose **New ID** from the **Sign As** drop down list.

For more information, refer to the following:

- [Finding an Existing Digital ID in a PKCS#12 File](#)
- [Finding a Digital ID in a Windows Certificate Store File](#)
- [Adding an ID that Resides on External Hardware](#)
- [Adding a Roaming ID Account to Get a Roaming ID](#)

Figure 3 Add Digital ID dialog



.apf Digital IDs no longer supported

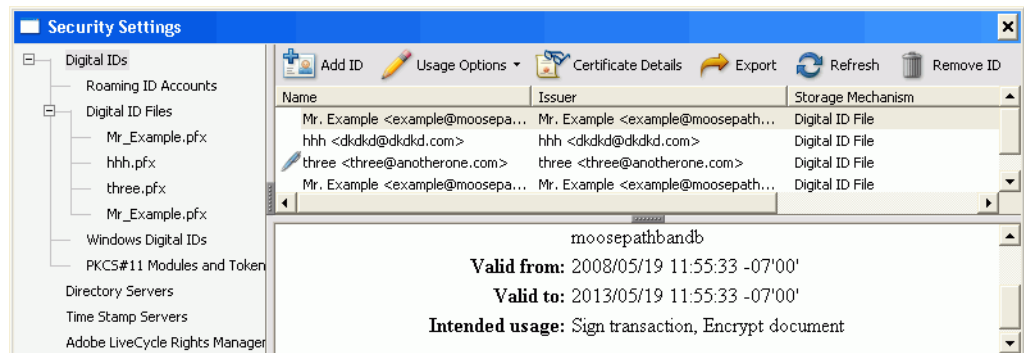
Older application versions use a deprecated digital ID format with an .apf extension. .apf is not supported in 9.0. You must use Acrobat 8.x or earlier to use this type of ID.

2.1.4 Digital ID Management and the Security Settings Console

The Security Settings Console enables users to manage their own digital IDs. Choosing **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings** opens a dialog for adding, removing, and setting the usage preferences for digital IDs stored on .pfx files, PKCS#11 modules and tokens, roaming ID servers, and the Windows Certificate Store.

Tip: You should always back up your private key if you have access to it. Without the key, encrypted documents cannot be decrypted and opened. To protect and back up private keys in an enterprise setting, administrators sometimes escrow private keys. If your digital ID is stored in a file on your local machine, consider copying it to a secure location.

Figure 4 Security settings menu and manager



2.1.5 Setting Identity Information

You can enter default identity (user) information that the application can automatically use as the defaults for workflows such as creating self-signed certificates and emailing certificate and server settings.

To create default user information:

1. Choose one of the following.
 - Acrobat (Windows): Edit > Preferences > **Identity**
 - Acrobat (Macintosh): **Acrobat** > **Preferences** > **Identity**

- Adobe Reader (Windows): **Edit > Preferences > Identity**
 - Adobe Reader (Macintosh): **Adobe Reader > Preferences > Identity**
2. Configure the identity details. These details will appear in your signature appearance when you sign with a self-signed digital ID.
 3. Choose **OK**.

Figure 5 Identity preferences

Identity

Login Name:

Name:

Title:

Organization Name:

Organizational Unit:

Email Address:

Your identity information is used with comments, reviews, and digital signatures. Information entered here is secure and not transmitted beyond this application without your knowledge.

2.2 Generic ID Operations

Once you have one or more digital IDs, you can edit, remove, and otherwise manage them from the Security Settings Console. To simplify workflows that use digital IDs, consider doing the following before using your ID:

- [Specifying Digital ID Usage](#): Set an ID to automatically use each time one is required for signing or certificate encryption.
- [Sharing \(Exporting\) a Digital ID Certificate](#): Since a digital ID's certificate contains the public key required for validating your digital signature and encrypting documents for you, send it to those who participate in these kinds of workflows with you ahead of time.

Other operations also apply to all digital IDs irrespective of their format. For details, see:

- ["Viewing All of Your Digital IDs" on page 15](#)
- ["Customizing a Digital ID Name" on page 16](#)
- ["Viewing Digital ID Certificates in the Certificate Viewer" on page 16](#)

2.2.1 Specifying Digital ID Usage

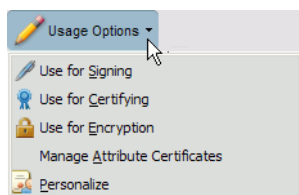
If a digital ID is not specified for a particular task that requires one, a prompt will ask for a digital ID file. To avoid repeated prompts, specify a digital ID for signing and encryption. Different IDs may be used for signing and encryption.

When you specify ID usage, that ID is the first one in the list you'll see when you're asked to select an ID in a signing or encryption workflow. If you select a different ID, your usage option will change to the newly selected ID.

To select a default digital ID file:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 2.2.1).
3. Highlight an ID in the list on the right.
4. Choose **Usage Options**. A drop-down list appears.

Figure 6 Usage options for a digital ID



5. Choose one or more options: signing, certifying, and encrypting. A lock or pen icon (or both) will appear to the left of the digital ID based on this selection.

Caution: Invalid and expired IDs with a yellow caution triangle cannot be used.

2.2.2 Sharing (Exporting) a Digital ID Certificate

Digital ID certificates must be distributed among participants in signing and certificate encryption workflows. Other users must have access to your certificate before:

- They can validate your signature if they are not already trusting a certificate above yours in the certificate chain. Note that a signature always includes the signer's certificate, so validation can occur with the certificate embedded in the signature if it is not already on the validator's machine.
- They can encrypt a document for you using certificate security.

Certificates can be emailed or saved to a file. Acrobat 9.x allows you to export a digital ID to an acrobatsecurity settings file by choosing **Advanced** > **Security** > **Export Security Settings**. You can also use FDF files to export your certificate so that others can import it into their trusted identities list. For details, see ["Exporting Your Certificate" on page 121](#).

Note: To export a certificate displayed in the Certificate Viewer, choose **Export** on the Summary tab.

2.2.3 Viewing All of Your Digital IDs

You can view all of your digital IDs in one list regardless of their type or location.

To view all of your IDs:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 4).

All the IDs you have added appear in the right hand panel. The list includes all of the IDs that you can view separately under:

- Digital ID Files
- Roaming ID Accounts

- Windows Digital IDs
- PKCS#11 Modules and Tokens

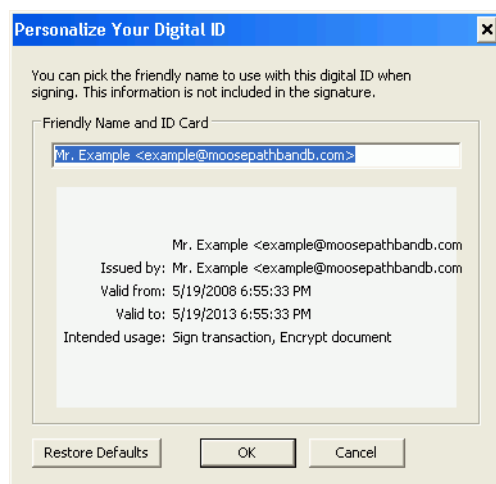
2.2.4 Customizing a Digital ID Name

You can personalize a digital ID by providing a user-friendly name. This name appears in the ID drop-down list in workflows where you are asked to select an ID.

To provide a friendly name:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 4).
3. Highlight an ID in the list on the right.
4. Choose **Personalize**.
5. Enter a name for the ID.

Figure 7 Personalizing an ID name



2.2.5 Viewing Digital ID Certificates in the Certificate Viewer

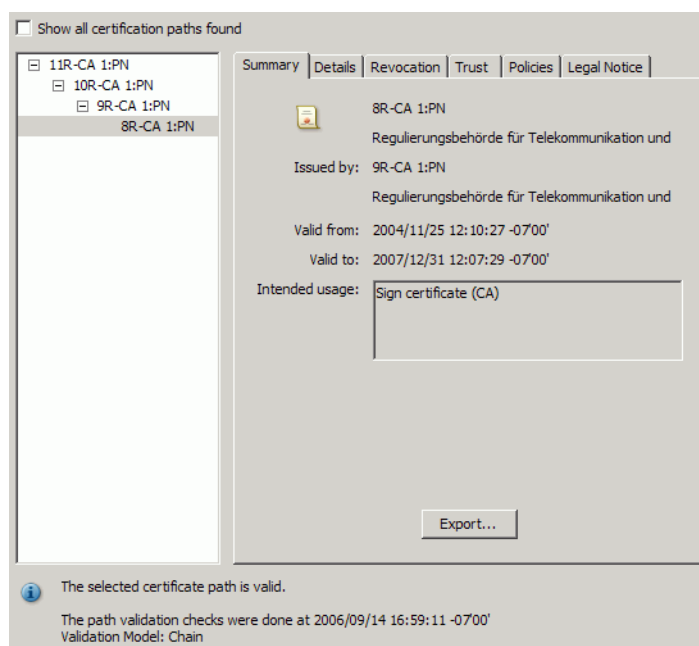
Your digital IDs appear in the Security Settings Console. From there, the Certificate Viewer can be used to display the time for which its certificate is valid and other details such as usage, a unique serial number, public key method, and so on (Figure 8).

To check certificate details:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 2.2.1).
3. Highlight an ID in the list on the right.
4. Choose **Certificate Details**. The Certificate Viewer displays the certificate. (Figure 8). The following details are available:

- **Left hand panel:** The certificate chain.
- **Bottom area:** A description of the certificate, path validity statement, path validation time, and sometimes the type of validation.
- **Summary tab:** Displays the owner, issuer, validity period, and other details. The Intended Usage field tells you whether the certificate can be used for signing, encryption, or both. An **Export** button allow you to export the certificate to a file.
- **Details tab:** Lists all the certificate fields (extensions) and their values.
- **Revocation tab:** Indicates whether a revocation check occurred and the result. Allows users to initiate a manual check and analyze problems.
- **Trust tab:** Displays the certificate's trust level. If it does not already exist in the trusted identities list, the **Add to Trusted Identities** is active.
- **Policies tab:** Displays policy restriction information that must be met for a signature to be valid, if any.
- **Legal Notice tab:** Displays other certificate policies as well as a button which links to that policy, if any.

Figure 8 Digital ID: Certificate viewer

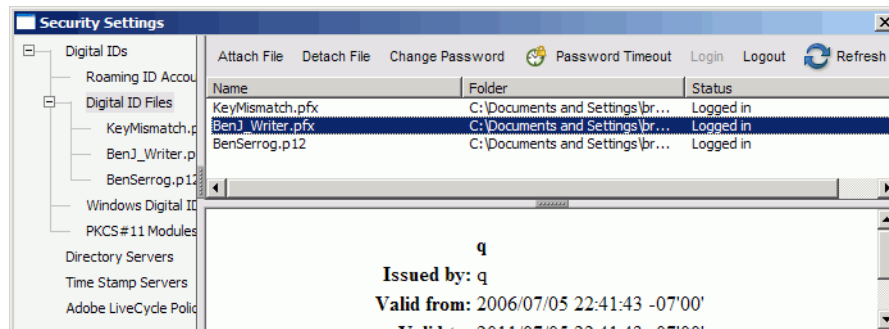


2.3 Managing PKCS#12 Digital ID Files

PKCS#12 digital ID files have several convenient features:

- Multiple IDs can be stored in a single, password-protected file.
- A file can contain both the public and private key.
- Passwords and password time-outs are user customizable.

Figure 9 Digital ID Files menu



2.3.1 Logging in to a Digital ID File

You will not usually need to log in to a digital ID file. Logging in means that Acrobat wants you to prove that you know the password to open the password-protected file containing the digital IDs. Since you likely supplied the password when you created your ID or obtained a new one, then you should be logged in.

However, you may need to log in for the following cases:

- You logged out of the file for some reason.
- You are importing an acrobatsecuritysettings file containing digital IDs.

To log in to a digital ID file:

2.3.2 Finding an Existing Digital ID in a PKCS#12 File

If a required digital ID file does not appear in the digital ID list, search for it and add it. You can browse to PKCS#12 files (with .pfx or .p12 extensions) and Windows Certificate Store compatible files (with .cer and .der extensions).

Note: In enterprise settings, you may be instructed by your administrator to get a digital ID from a specific location or to customize Acrobat or Adobe Reader to work with software supplied by your organization.

To find a digital ID file:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 4).
3. Choose **Add ID**.
4. Select the **My existing digital ID from** and **A file** radio buttons (Figure 3).
5. Choose **Next**.
6. Choose **Browse** and browse to the digital ID file. PKCS#12 files may reside on a network or in some local location. For example, on a Window machine it might be C:\Documents and Settings\<username>\Application Data\Adobe\<application name>\<version>\Security\.

7. Select the ID and choose **Open**.
8. Enter a password if one is required.
9. Review the digital ID list and choose **Finish**.

2.3.3 Adding and Removing Digital ID Files from the File List

Adobe Acrobat and Adobe Reader only allow deletion of user-created self-signed digital IDs created with those applications. A file can have one or more IDs.

To delete or add an ID file:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** > **Digital ID Files** in the left-hand tree (Figure 9).
3. Highlight a digital ID file in the right-hand panel.
4. Do one of the following:
 - Choose **Detach File**. The file is removed from the list but still remains on your file system.
 - Choose **Attach File**. Browse to the file, enter the file password, and choose **OK**.

Note: Detaching a file does not remove it from your system, and it may be reattached later.

2.3.4 Changing an ID File's Password

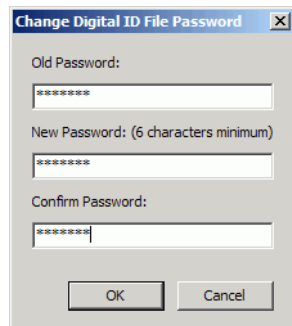
Passwords and password time-outs are unique to PKCS#12 IDs. Since a file can contain multiple IDs, passwords and time-outs are configured at the file level rather than for individual IDs.

Note: If the file is read only, then the **Change Password** and **Password Timeout** options are disabled.

To change the password:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Highlight **Digital ID Files** in the left-hand tree (Figure 9).
3. Select a file in the right-hand panel (Figure 9).
4. Choose **Change Password**.
5. Enter the old password.
6. Enter a new password and confirm it.
7. Choose **OK**.

Figure 10 Digital ID files: Password configuration



2.3.5 Changing a PKCS#12 File's Password Timeout

Passwords and password time-outs can only be set for PKCS#12 IDs. Since a file can contain multiple IDs, passwords and time-outs are configured at the file level rather than for individual IDs.

Note: If the is read only, then the **Change Password** and **Password Timeout** options are disabled.

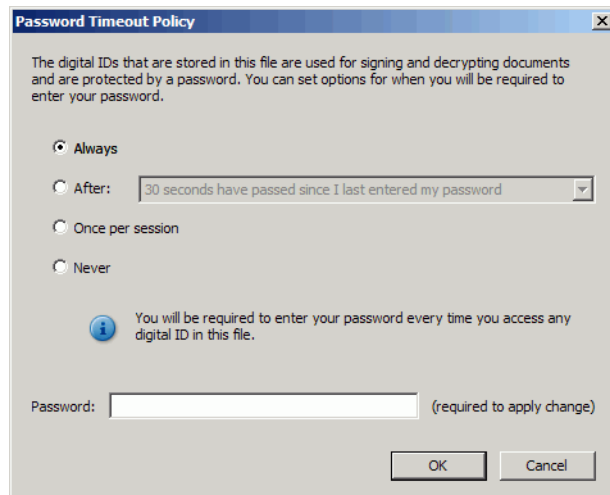
To change the password timeout:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Highlight **Digital ID Files** in the left-hand tree ([Figure 9](#)).
3. Select a file in the right-hand panel ([Figure 9](#)).
4. Choose **Password Timeout**.

Tip: The password timeout feature interacts with the Login/Logout feature as described in ["Logging in to PKCS#12 Files" on page 21](#).

5. Configure the Password Timeout Policy dialog by specifying when a password prompt should appear:
 - **Always:** A password is always required each time the digital ID is used regardless of whether or not you are logged in to a file.
 - **After:** Choose a value from the drop-down list to set a time frame.
 - **Once per session:** A password is asked for only once while the application is open.
 - **Never:** The password is not usually required when using this ID and you are logged into the file.
6. Enter the password.
7. Choose **OK**.

Figure 11 Digital ID files: Timeout settings



2.3.6 Logging in to PKCS#12 Files

The digital ID Login feature provides access to the IDs in a particular file. Login behavior is dependant on the user-specified password timeout feature. If the user has specified a password timeout of **Never**, then the application never asks for a password when an ID is used for some process. For example:

- **Signing:** During signing workflows, you can sign with a digital ID without entering a password if you are logged into a file and the time-out is set to **Never**.
- **Batch processing:** In normal operation, batch sequences that require access to a digital ID invoke the user-interface's authentication dialog. Because the dialog prompts for a password, the batch sequence is effectively stopped until a user intervenes. Logging in to a file provides the ID to the process without stopping it or requiring user input.

To enable sequences to run automatically and bypass normal user interface actions, do the following:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital ID Files** in the left-hand tree (Figure 9).

Tip: Verify the password timeout is set according to your own preferences. For details, see [“Changing a PKCS#12 File’s Password Timeout” on page 20](#).

3. Select a file in the right-hand panel (Figure 9).
4. Do one of the following:
 - **Logout:** Highlight an ID in the list on the right and choose **Logout**.
 - **Login:** Highlight an ID in the list on the right and choose **Login**. Enter a password when prompted and choose **OK**.

2.3.7 Creating a Self-Signed Digital ID

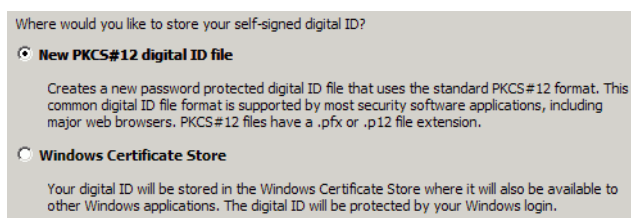
Note: The option to create self-signed digital IDs is unavailable if your administrator has configured your application to prevent this operation.

Users can create a self-signed digital ID if they don't wish to purchase an ID from a 3rd party certificate authority (CA) or are not given a company-provided ID. Self-signed IDs are usually considered less secure because the user has not been verified by a 3rd party CA. For self-signed IDs, you act as your own CA.

To create a self-signed digital ID:

1. Navigate to the Add Digital ID dialog as described in ["Finding an Existing Digital ID in a PKCS#12 File" on page 18](#).
2. Choose **A new digital ID I want to create now** (Figure 3).
3. Choose **Next**.

Figure 12 Digital ID format selection



4. Select a digital ID format and storage location:
 - **New PKCS#12 Digital ID File:** Stores the IDs in a password protected file with a .pfx (Win) or .p12 (Mac) extension. The file is in a PKCS#12 standard format. The files can be copied, moved, and emailed. They are cross-platform, portable, and always password protected. This common format is supported by most security software applications, including web browsers. These files should always be backed up. On Windows XP, the default location is `C:\Documents and Settings\<username>\Application Data\Adobe\<application name>\<version>\Security\`.
 - **Windows Certificate Store:** (Windows only) Stores the ID in the Windows Certificate Store where it is also available to other Windows applications. The ID is protected by your Windows login. These IDs are easy to use and do not have to have file-level password protection. However, they are not portable and could be less secure if a file-level password is not specified.
5. Choose **Next**.

Figure 13 Digital ID: Configuration

Add Digital ID

Enter your Identity information to be used when generating the Self-Signed Certificate.

	ASCII	Unicode
Name (e.g. John Smith):	Neb Studly	
Organizational Unit:	Aardvark	
Organization Name:	AntEater Inc.	
Email Address:	nebrogeros@anteater.com	
Country/Region:	VA - HOLY SEE (VATICAN CITY STATE)	

☒ Enable Unicode Support

Key Algorithm: 1024-bit RSA

Use Digital ID for: Digital Signatures and Data Encryption

Cancel < Back Next >

6. Configure the digital ID. The dialog is prepopulated if the Identity preferences have been previously configured:

Tip: If you use non-Roman characters, choose **Enable Unicode Support** before continuing.

- **Name:** The name that appears in the Signatures tab and in the signature field.
- **Organizational Unit:** Optional. Appears in the signature and certificate.
- **Organizational Name:** Optional. Appears in the signature and certificate.
- **Email Address:** Optional. Appears in the signature and certificate.
- **Country/Region:** Optional. Appears in the signature and certificate.
- **Enable Unicode Support:** Optional. Use Unicode when your information cannot be adequately displayed with Roman characters.

Note: Many applications do not support non-ASCII characters in certificates. Be sure to specify both an ASCII representation of the information as well as the Unicode representation of information you are supplying.

- **Key Algorithm:** 2048-bit RSA offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible. Use the 1024 bit key length if you are unsure.
 - **Use Digital ID for:** Select whether to use the digital ID for digital signatures, data encryption (certificate security), or both.
7. If a Windows digital ID was selected, choose **Finish**; otherwise, for a PKCS#12 ID do the following:
 1. Choose **Next**.
 2. Specify a file name and location for the digital ID file.
 3. Enter a password and confirm it.

Note: Passwords are case-sensitive and must contain at least six characters.

4. Choose **Finish**.

Figure 14 Digital ID: PKCS#12 location and password

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:

Password:

Confirm Password:

2.3.8 Deleting a PKCS#12 Digital ID

Adobe Acrobat and Adobe Reader only allow deletion of user-created, self-signed digital IDs created by them. The methodology for deleting other types of IDs varies with the type of ID.

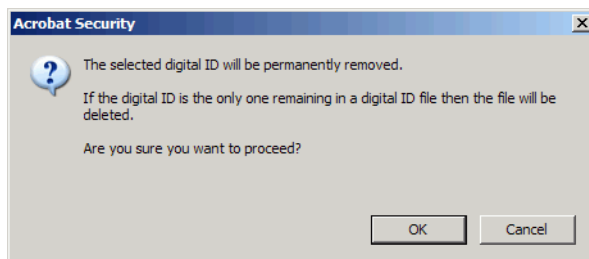
While the ID will be removed from the ID list, other ID's in the container .pfx or p12 file will not be affected. Deleting the last, self-signed PKCS#12 ID in a .pfx or p12 file also deletes the digital ID file.

Caution: Because deleting an ID deletes its private key, operations that require that key will no longer be possible. If the file is used by other programs or you need it to open encrypted documents, do not delete it.

To delete a self-signed ID:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree ([Figure 2.2.1](#)).
3. Highlight a self-signed ID in the list on the right that uses a digital ID file or Windows Certificate Store storage mechanism.
4. Choose **Remove ID**.
5. Choose **OK** when asked to proceed.

Figure 15 Digital ID: Deleting

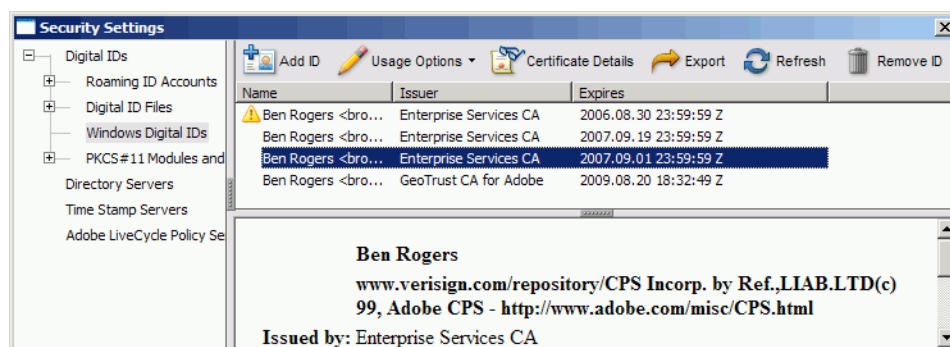


2.4 Managing Windows Digital IDs

For the Acrobat family of products, a “Windows digital ID” is an ID that resides in the Windows certificate store rather than the Acrobat store. Windows supports several formats listed in [Table 2](#). These IDs are protected by your Windows login, are easy to use, and do require file-level password protection. However, they are not portable and are less secure when a file-level password is not specified.

The Windows store makes these IDs available to other Windows applications such as Acrobat and Adobe Reader. When an ID in the Windows store is registered with the application, it appears in the Security Settings Console. IDs in the Windows store are subject to the same operations as described in [“Generic ID Operations” on page 14](#)

Figure 16 Windows digital ID menu



2.4.1 Finding a Digital ID in a Windows Certificate Store File

If a required digital ID file does not appear in the digital ID list, search for it and add it. You can browse to PKCS#12 files (.pfx or .p12) and Windows Certificate Store compatible files (.cer and .p7b).

For details, see [“Finding an Existing Digital ID in a PKCS#12 File” on page 18](#).

2.4.2 Deleting a Digital ID from the Windows Certificate Store

IDs that have been added to the Windows certificate store can only be deleted from the Security Settings Console if they are self-signed IDs created in Acrobat or Reader version 8.0 or later. Other IDs must be removed from the Windows store by using an application such as Internet Explorer. The store's location in Internet Explorer may vary by version, but is typically found under **Tools > Internet Options > Content tab > Certificates button**.

2.5 Managing Roaming ID Accounts and IDs

A roaming ID is a digital ID that is stored on a server. The private key always remains on the server, but the certificate and its public key can be downloaded at the subscriber's request to any location. Roaming IDs require an Internet connection.

Roaming IDs enable remote ID access as well as Web-based user self-registration and ID issuance from a roaming ID server and central ID management. When IDs expire, new ones can be issued and placed on a

server rather than being distributed to each individual. Deployment and management therefore occurs in one location rather than on numerous client machines.

Depending on how the system is configured, users identify themselves (authenticate) to the server either with a username and password, Windows single sign-on, or by some 3rd party method such as ArcotID.

Note: Roaming IDs are only used for signing and cannot be used for certificate encryption. They are subject to the same operations as described in [“Generic ID Operations” on page 14](#)

2.5.1 Adding a Roaming ID Account to Get a Roaming ID

Roaming IDs are only available for those with roaming ID accounts on a roaming ID server. For connection details, contact your system administrator. Once you log in to your account, the IDs associated with that account will be automatically downloaded.

To install the roaming IDs certificate:

1. Verify you have an Internet connection.

Note: If a roaming ID administrator has sent you a file with the account settings preconfigured, see the following sections rather than follow the steps described below:

- **.acrobatsecurity file:** [“Security Setting Import and Export” on page 112](#)
- **FDF file:** [“Importing Roaming ID Account Settings” on page 136](#)

2. Do one of the following:
 - Navigate to the Add Digital ID dialog as described in [“Finding an Existing Digital ID in a PKCS#12 File” on page 18](#).
 - Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**. Then expand the left-hand tree to **Roaming ID Accounts** and choose **Add Account** from the top menu ([Figure 17](#)).
3. Choose **Configure a roaming ID for use on this computer** ([Figure 3](#)).
4. Choose **Next**.
5. In the Add a Roaming ID dialog, enter a server name and URL.
6. Choose **Next**.
7. Enter your user name and password for this roaming ID server account.
8. Enter a server name and URL.
9. Choose **Next**.
10. Your certificate(s) will be automatically downloaded. Review the digital ID list and choose **Finish**.

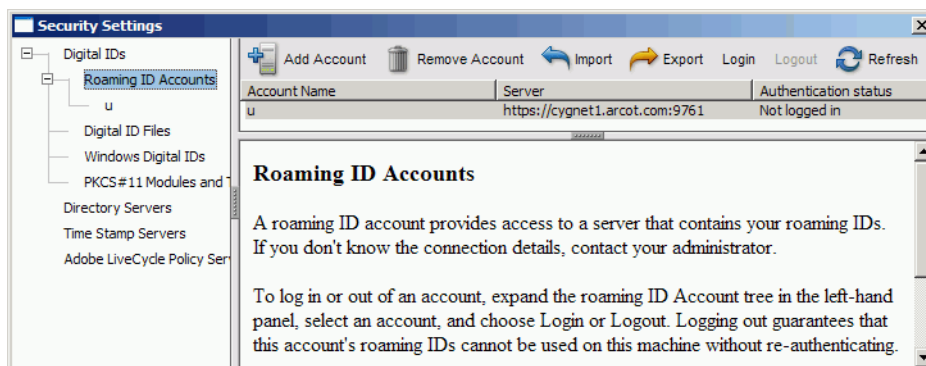
2.5.2 Logging in to a Roaming ID Account

A roaming ID account is a user account on a roaming ID server containing one or more digital IDs. The login feature provides access to the IDs associated with the account. Depending on how the server administrator has set up the server, once you log in you may not be asked to supply a password again when you use that ID to sign.

To log in to a device:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Expand the left-hand tree to **Roaming ID Accounts** (Figure 17).
3. Select an account in the right-hand panel.
4. Choose **Login**.
5. Follow the instructions in the dialogs. The workflow varies by the roaming ID supplier as well as the authentication type.

Figure 17 Roaming ID Security Settings menu items



2.6 Managing IDs Accessible via PKCS#11 Devices

Smart cards, hardware tokens, and other PKCS#11-compliant devices are increasingly being used by businesses and individuals to carry digital IDs. These devices provide enhanced mobility, remote access to intranets and extranets, as well as strong security with public/private key cryptography and PIN access to the digital ID.

The method for registering a digital ID on such a device with the application may vary. The manufacturer or your system administrator should provide detailed instructions. However, the steps below may be used as a general guide. IDs stored on a PKCS#11 device are subject to the same operations as described in ["Generic ID Operations" on page 14](#).

2.6.1 Adding an ID that Resides on External Hardware

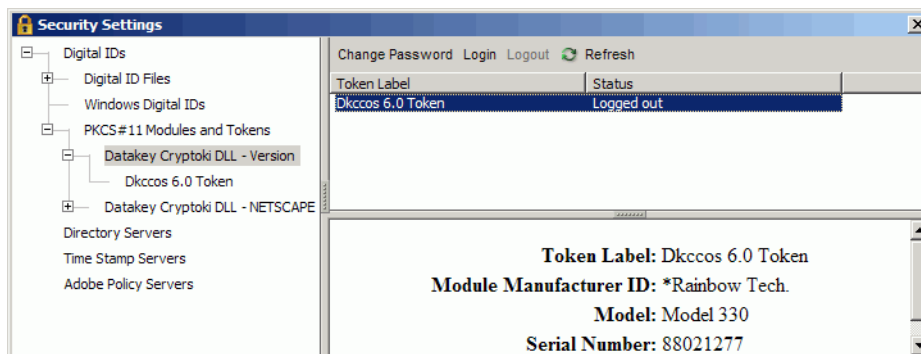
Digital IDs can reside on hardware such as a smart card or token with a USB interface. In these cases, the card is inserted into a smart card reader or the token is inserted directly into a USB port. Adobe products can be configured to look for and use IDs on these devices by adding the device's module (software driver) to the module list. The module's IDs are automatically registered with the application.

To register an ID that resides on external hardware:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Expand **Digital IDs** in the left-hand list (Figure 16).

3. Highlight **PKCS#11 Modules and Tokens**.

Figure 18 PKCS#11 Security Settings menu items



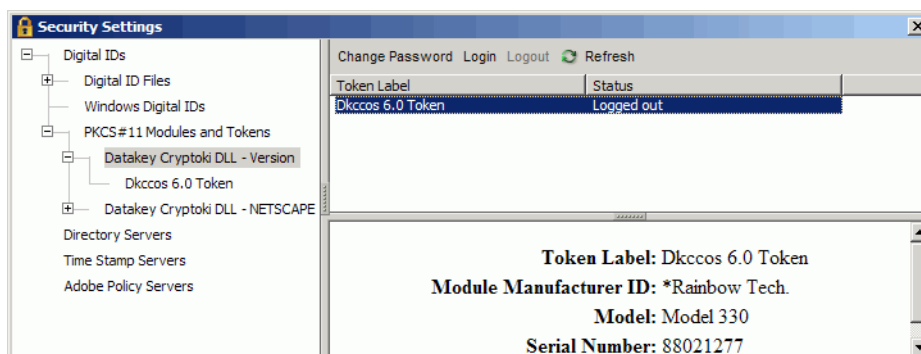
4. Choose **Add Module**.
5. Browse to the device driver. On Windows, this could likely be C:\Windows\system32\<some dll>.dll. The exact path will be supplied by your system administrator or the maker of your device.
6. Choose **Open**.
The module and its IDs are automatically added to the list in the right-hand panel.

2.6.2 Changing Passwords

A card or token may contain multiple IDs. All of the IDs are password protected by a single password. This password is used to log in to a device and to sign.

1. Expand the tree under **PKCS#11 Modules and Tokens**.
2. Highlight any module.

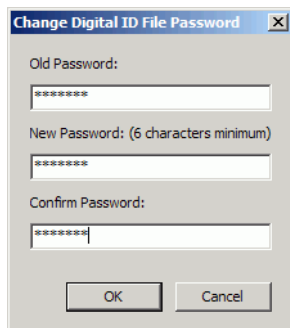
Figure 19 PKCS#11 Security Settings menu items



3. A card or token label should appear in the right-hand panel. If there is more than one, select one.
4. Choose **Change Password**.
5. Enter the old password.

6. Enter a new password and confirm it.
7. Choose **OK**.

Figure 20 Digital ID files: Password configuration



2.6.3 Logging in to a Device

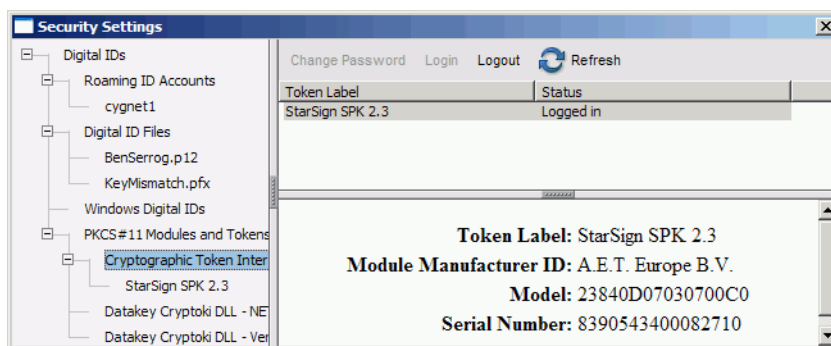
The digital ID login feature provides access to the IDs on a particular device or smart card.

PKCS#11 workflows vary by the device supplier. For example, additional passwords or PINs may or may not be required. The login interface may be provided by the Adobe application or by the device supplier.

To log in to a device:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Expand the tree under **PKCS#11 Modules and Tokens**.
3. Highlight any module.
4. A card or token label should appear in the right-hand panel. If there is more than one, select one.
5. Choose **Login**.
6. Enter a password.
7. Choose **OK**.

Figure 21 PKCS#11 Security Settings menu items



3

Managing Certificate Trust and Trusted Identities

As described in [“What is a Digital ID?” on page 10](#), a digital ID consists of two main parts: a certificate with a public key and a private key. Participants in signing and certificate security workflows need to exchange the public part (the certificate) of their digital ID. Once you obtain someone’s certificate and add it to your trusted identities list, you can encrypt documents for them. If their certificate does not already chain up to a trust anchor that you have specified, you can set the certificate’s trust level so that you can validate the owner’s signature.

Understanding what a trusted identity is and how trust levels are set can help you set up streamlined workflows and troubleshoot problems. For example, you can add trusted identities ahead of time and individually set each certificate’s trust settings. In enterprise settings where certificates are stored on a directory server, you may also be able to search for certificates to expand your list of trusted identities.

For more information, refer to the following:

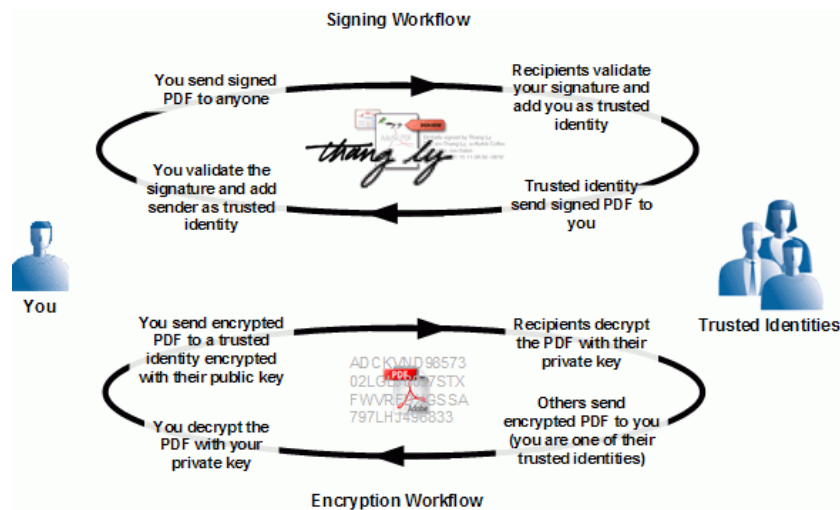
- [“What is a Trusted Identity?” on page 30](#)
- [“Using Directory Servers to Add Trusted Identities” on page 40](#)
- [“Adding Someone to Your Trusted Identity List” on page 32](#)
- [“Managing Contacts” on page 43](#)

3.1 What is a Trusted Identity?

Digital signature and certificate security workflows both rely on certificates. Participants in signing workflows share their certificates ahead of time or embed them in a document. Participants in certificate security workflows must share their certificates ahead of time. Both operations involve importing other people’s certificates into your Trusted Identities list. When a person’s certificate information appears in the Trusted Identity Manager, they become a *trusted identity*.

Groups of people that share documents with certificate security or digital signatures are in essence a community of trusted identities that share their certificates to make those features work. You will add people to your trusted identity list and others will add you to theirs:

- When you sign document, the document recipient can validate your signature by validating the certificate embedded in the document. Conversely, you need access to a document sender’s certificate to validate their signature.
- You encrypt a document with the document recipient’s public key so that they can decrypt it with their corresponding private key. Conversely, others need your certificate to encrypt documents for you.

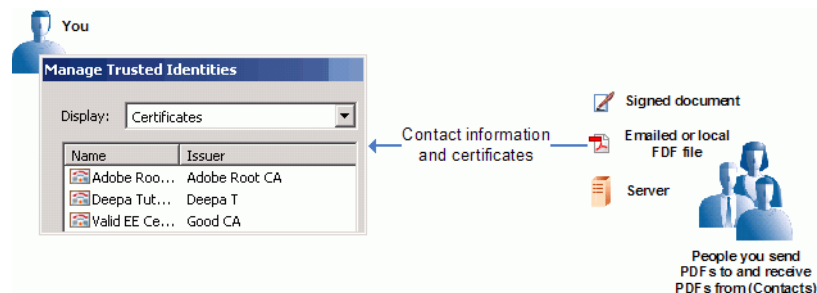


The Acrobat family of products provide tools for selecting and interacting with the certificates of document recipients you trust. For example, Acrobat's user interface prompts authors to select one or more recipients when applying certificate security. Because it is often the case that a document will be sent or received from numerous individuals, it is expedient to create a list of trusted identities ahead of time. In large organizations, an administrator may do this for you; otherwise, you will use Acrobat's Trusted Identity Manager to store your trusted identities' contact information and certificates.

Getting someone's contact information and certificate involves searching for (or having sent to you) the digital ID data in the requisite format. Some common ways of getting the data include the following:

- **Import the data from an .acrobatsecurity file.** Configuration details can be imported from a security settings file as described in ["Migrating and Sharing Security Settings" on page 112](#).
- **Extract the data from an FDF file.** Double-clicking on an FDF file causes Acrobat to automatically import the information.
- **Search a server directory.** Users can add directory servers containing contact information and certificates. Sometimes administrators preconfigure these directories.
- **Use the data embedded in a signed document.** The Certificate Viewer's **Add to Trusted Identities** button adds a certificate to the trusted identities list and allows setting its trust level.

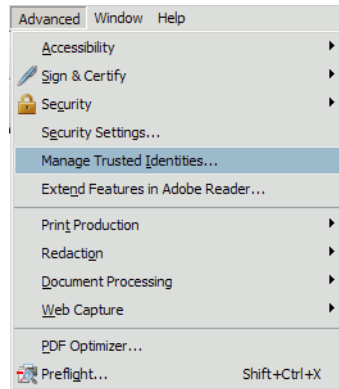
Figure 22 Digital ID: Managing trusted identities



From within the Manage Trusted Identities dialog, users import and manage the certificates and certificate owner data for document recipients they wish to trust. A contact will occasionally be associated with multiple certificates. Therefore, contacts and certificates are in some respects managed independently of

each other. It is also possible to create a group from any number of contacts so that security can be applied to all group members with a single action. Users manage contacts, groups, and certificates by choosing **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities** and opening the Trusted Identities Manager.

Figure 23 Manage Trusted Identities menu item



3.2 Adding Someone to Your Trusted Identity List

As shown in [Figure 22](#), you build a list of trusted identities by getting digital ID certificates from those who will be participating in signing and certificate security workflows. You get this information from a server, a file, or from a signed document. For signing workflows, you can get this information during the signature validation process. For certificate security workflows involving encryption, you must request the information ahead of time so you can encrypt the document with the document recipient's public key.

3.2.1 Adding a Certificate From a Signature

When you receive a signed document from someone whose certificate is not in your trusted identity list AND does not chain up to a trust anchor (another certificate that is trusted), the signing certificate's validity is unknown and a yellow triangle appears in the document message bar. To validate the signature, you will need to trust one of the certificates in the certification chain. You could trust the signer (the end-entity certificate), one of the EE certificate issuer (an intermediate certificate), or the topmost certificate authority (the root).

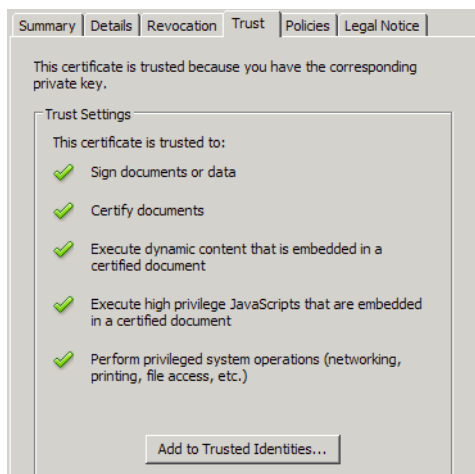
Because revocation checking does not occur for certificates that are directly trusted (a trust anchor), it is best practice to trust a certificate other than the signer's. That is, trust a certificate as high up in the chain as is practical for your signing workflows.

To add a certificate to your trusted identities list directly from a signature:

1. Right click on the signature and choose **Show Signature Properties**.
2. Choose **Show Certificate**.
3. When the Certificate Viewer appears, choose the Trust tab.
4. Choose **Add to Trusted Identities** ([Figure 24](#)).

5. Set the certificate trust settings as described in [“Setting Certificate Trust” on page 37](#).

Figure 24 Certificate Viewer: Trust tab



3.2.2 Requesting a Digital ID via Email

Email requests for digital ID information use .acrobatsecurity or FDF files. For details, see [“Migrating and Sharing Security Settings” on page 112](#).

For details, see [“Requesting a Certificate via Email” on page 124](#).

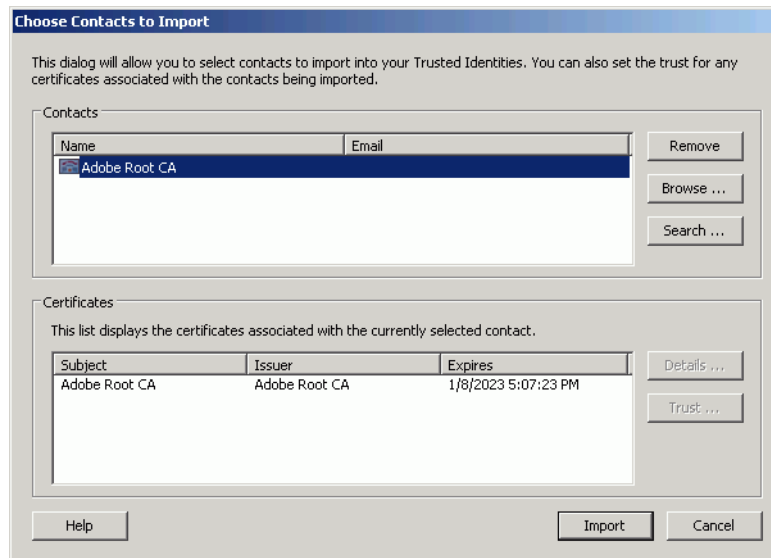
3.2.3 Importing a Certificate From a File

Acrobat and Adobe Reader can export certificates to a file so that they can be shared as needed. To import certificates, follow the instructions described in [“Migrating and Sharing Security Settings” on page 112](#).

However, certificates may also exist in other file types such as .cer, .p7b, and so on. To import certificates from these file types:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose **Add Contacts**.
3. Choose **Browse**.
4. Browse to the contact file location.
5. Select the file.
6. Choose **Open**.

Figure 25 Importing digital ID data



7. Choose **Import**.
8. Choose **OK** when the confirmation dialog appears.

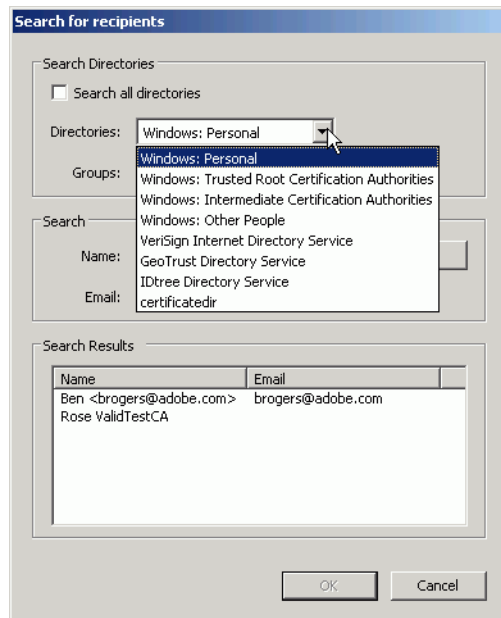
3.2.4 Searching for Digital ID Certificates

The search feature allows you to search a list of directories for certificates. If no directories have been previously specified, the **Search** button will NOT appear. The list of search servers in the Directories drop-down list is populated through three mechanisms:

- The default server settings that ship with Adobe Acrobat and Adobe Reader.
- The Windows Certificate Store if the user has turned on this option.
- User-specified directory servers the user has added in the Security Settings Console. For details, see ["Using Directory Servers to Add Trusted Identities" on page 40](#).

Tip: Home users do not usually need to change the directory server list. Users in enterprise environments typically have the list preconfigured by their system administrator.

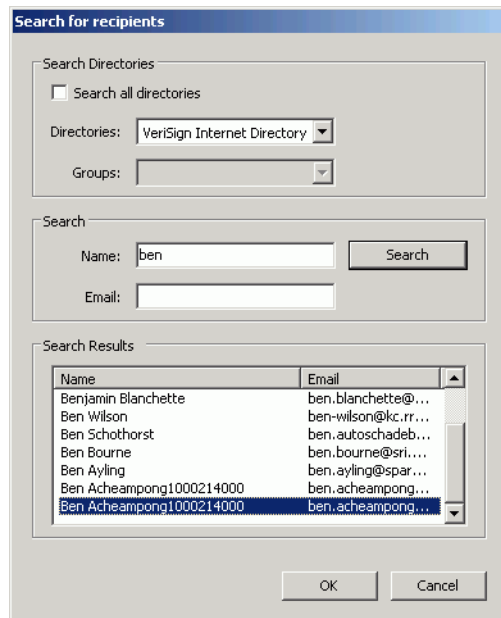
Figure 26 Digital IDs: Searching for certificates



To search for a certificate so that you can add one or more people to your trusted identities list:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose **Add Contacts**.
3. Choose **Search**.
4. Configure the search options:
 - Choose **Search all directories** or select a directory and optional group.
Searching all directories may take some time. In a business environment, it is often expedient to just select the company's LDAP directory.
 - Enter a name and/or email address to search. This is an AND search. Using both fields only returns results that match both criteria.
5. Choose **Search**.
6. Select a name from the search results.
7. Choose **OK**.
8. If the desired entries are found, choose **Import**.
9. Choose **OK** when the confirmation dialog appears.

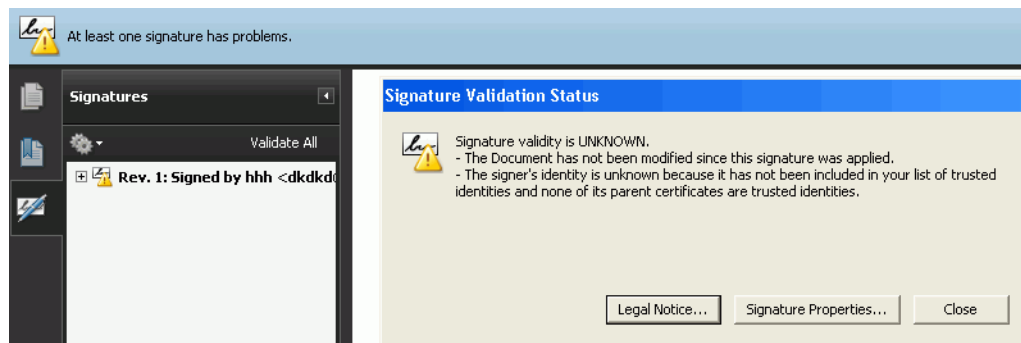
Figure 27 Searching for a document recipients



3.3 Certificate Trust Settings

Contacts in the trusted identities list should be associated with one or more certificates. Those certificate's trust settings may be individually configured. Choosing to not trust a certificate does not prevent a document from displaying, but it will result in signatures having an unknown status. The status is represented by a yellow triangle in the Document Message Bar, Signatures pane, and the Signature Validation Status dialog (Figure 28). For each contact for whom you will encrypt a document with certificate security, one certificate can also be selected as the default for encryption.

Figure 28 Untrusted signature

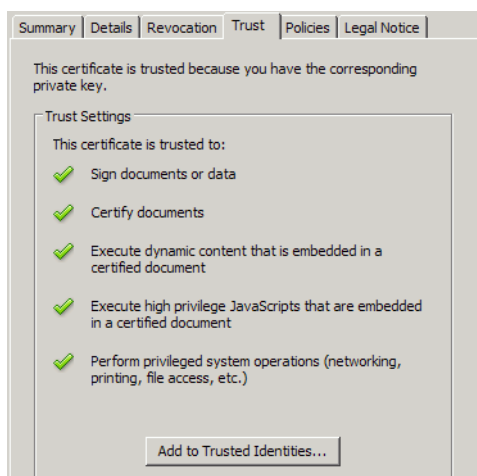


Certificate trust settings have the following features:

- Trust settings are configured in the Trusted Identity Manager ahead of time, at the time of import, or directly from a signature.

- Trust settings can be viewed in the Trusted Identity Manager by choosing **Edit Trust** or by choosing the Trust tab in the Certificate Viewer (Figure 29).
- Certificates can be separately trusted for approval signatures and certification signatures.
- Certificates can be individually configured to trust operations such as signing, certification, and allowing items such as dynamic content and JavaScript in certified documents. These settings interact with application environment settings.

Figure 29 Certificate trust settings



3.3.1 Setting Certificate Trust

Signers use their digital ID certificate to sign documents. In order for you to verify the validity of a signature, you must have explicitly trusted their certificate for signing or that certificate must chain up to another certificate you have trusted (a trusted anchor). You can set trust ahead of time or when you are viewing a signature.

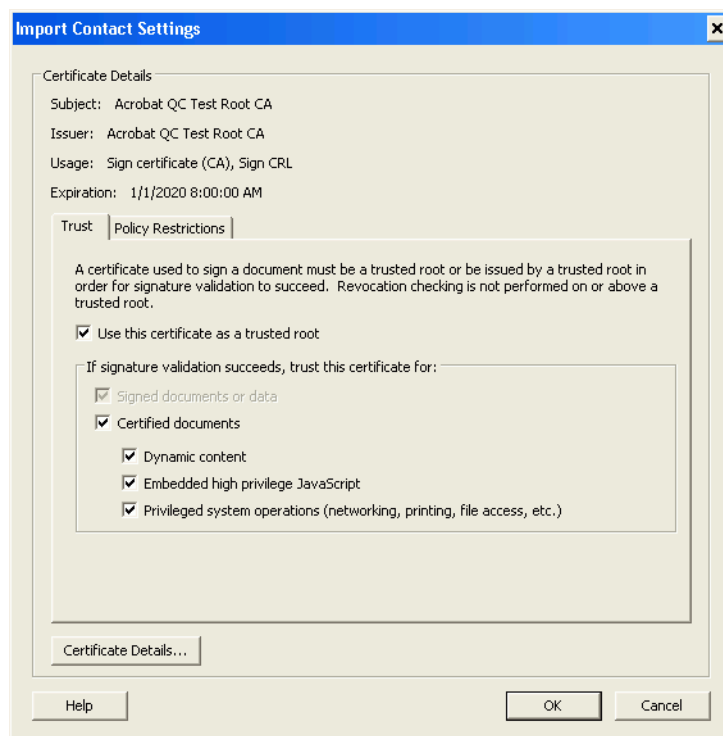
To trust a certificate for signing and certifying:

1. Do one of the following:
 - If you already have the certificate:
 1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities**.
 2. Choose **Certificates** in the **Display** drop down list.
 3. Select the certificate.
 4. Choose **Edit Trust**.
 - If the certificate is in a signature:
 1. Right click and choose **Signature Properties**.
 2. Choose **Show Certificate**.
 3. Select the Trust tab.
 4. Choose **Add to Trusted Identities**.

2. On the Trust tab, select the trust options. In enterprise settings, an administrator should tell you which trust settings to use.

Note: During an import action, recipients of the distributed trust anchor may be able to inherit its trust settings. Once you've verified the sender, you usually want to accept these settings so you can use the certificate they way the sender intended.

Figure 30 Certificate trust settings



- **Use this certificate as a trusted root:** Makes the certificate a trust anchor. The net result is that any certificates which chain up to this one will also be trusted for signing. At least one certificate in the chain (and preferably only one) must be a trusted root (trust anchor) to validate signatures and timestamps.

Tip: There is no need to make end entity certificates trust anchors if they chain up to a trust anchor. It is best practice to trust the topmost certificate that is reasonable to trust because revocation checking occurs on every certificate in a chain until that anchor is reached. For example, in a large organization, it is likely you would want to trust your company's certificate. If that certificate was issued by VeriSign, you would not want to make VeriSign a trusted root unless you wanted to trust every certificate that chains up to VeriSign.

- **Signed documents or data:** Trusts the certificate for approval signatures.
- **Certified documents:** Trusts the certificate for certification signatures.
- **Dynamic content:** Trusts multimedia and other dynamic content in certified documents. Selecting this option automatically adds documents that are certified with this certificate to the Trusted Documents list which is maintained by the Multimedia Trust Manager. For this reason, verify your application environment is configured correctly. For details, "[Controlling Multimedia](#)" on page 98.

- **Embedded high privilege JavaScript:** Trusts embedded scripts. Certificate settings do not override application-level settings, so even if JavaScript is enabled for a particular certificate, it may not execute unless the application's preferences allow it. This option requires that the application environment be configured correctly. For details, see ["Setting JavaScript Options" on page 101](#).
 - **Privileged system operations (networking, printing, file access, etc.):** Some operations represent a security risk more serious than others. Acrobat considers the following operations potential threats to a secure application operating environment: Internet connections, cross domain scripting, silent printing, external-object references, and FDF data injection. If this checkbox is checked, documents that are certified with this certificate will allow these actions.

Tip: This feature interacts with the Enhanced Security preferences which may be set by choosing **Edit > Preferences > Security (Enhanced)**. The application always takes the least restrictive setting when determining what is allowed. For example, if the trust level for this certificate does not allow privileged operations but the certified file resided in a privileged location, then these operations will be permitted.
3. If you need to specify a policy restriction, do so. Most users only need to set policy restrictions at the request of their administrator. ["Setting Certificate Policy Restrictions" on page 39](#).
 4. Choose **OK** twice.
 5. Choose **Close**.

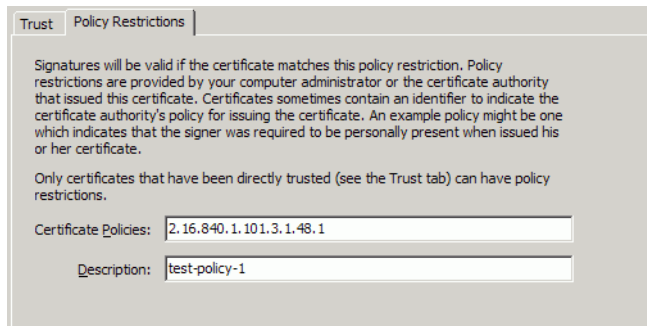
3.3.2 Setting Certificate Policy Restrictions

Policy restrictions are typically used in enterprise settings when configuring trust anchors. A restriction provides criteria the certificate chain must meet before a signing certificate can be used to create a valid signature. For example, a VeriSign certificate may be set as a trusted root, but a company may wish to only trust their own intermediate certificates (ICAs) that chain to VeriSign rather than *all* certificates that chain up to VeriSign. The company can issue an ICA with a certificate policy extension. By including that ICA in the certificate chain between all end entity certificates and VeriSign and requiring the presence of that extension, only company signers will be trusted.

Policies are represented by numbers called *object identifiers* (OIDs). OIDs are usually provided by your system administrator.

1. Select the Policy Restrictions tab if the Edit Certificate Trust dialog is displayed; otherwise, choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose **Certificates from the Display drop-down list**.
3. Highlight a certificate and choose **Edit Trust**.
4. Choose the Policy Restrictions tab and enter the restrictions:
 - **Certificate Policies:** Required. Enter the policy OID.
 - **Description:** Optional. Enter a meaningful description.

Figure 31 Policy restrictions



3.3.3 Using Certificates for Certificate Security (Encryption)

You only need to specify a certificate's encryption usage if you are using certificate security. When more than one certificate is associated with the contact, you can select which one to use as the default encryption certificate. For details, see "Certificate Security" in the *Document Security User Guide*.

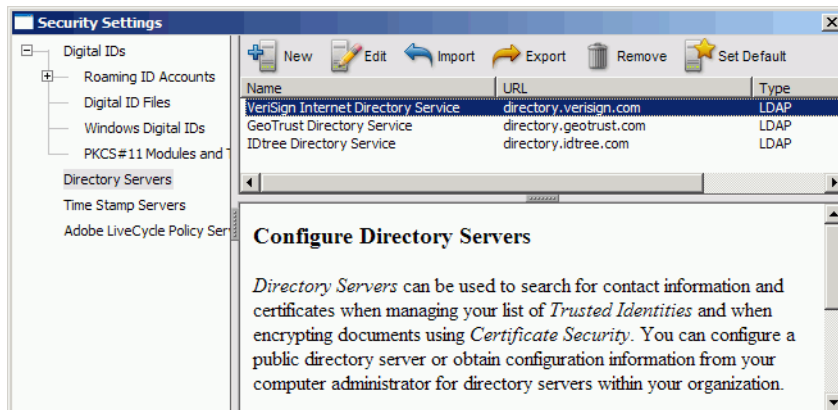
3.4 Using Directory Servers to Add Trusted Identities

Businesses often use a centrally managed certificate repository such as an LDAP directory server. Directory servers are capable of returning X.509 public key certificates. These servers are searchable so that you can easily expand your list of trusted identities. Both Adobe Acrobat and Adobe Reader for Windows ship with default servers:

- Versions 7.x:
 - VeriSign Internet Directory Service
 - GeoTrust Directory Service
 - IDtree Directory Service
- Version 8.x and 9x:
 - VeriSign Internet Directory Service

Home users may never need to use directory servers. In most cases, needed certificates will be sent directly to you or will be embedded in a signature. However, enterprise users will likely use directory servers when their administrator has set up an LDAP server as part of a public key infrastructure. This allows the administrator to make the certificates available to teams and workgroups while managing them from a central location. The administrator usually preconfigures user machines, tells the user how to configure the server manually, or sends the server configuration details in a file as described in ["Migrating and Sharing Security Settings" on page 112](#).

Figure 32 Digital ID Directory servers: Server list



3.4.1 Manually Configuring a Directory Server

Some companies store employee digital ID certificates on a networked LDAP server. To access those certificates, add the server to the list of directories used to locate those IDs.

Tip: In an ideal scenario, the server administrator supplies configuration details in a file as described in [“Migrating and Sharing Security Settings” on page 112](#).

To manually configure an identity directory:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Directory Servers** in the left-hand list ([Figure 32](#)).
3. Choose **New**.
4. Configure the LDAP server settings in the Edit Directory Server dialog:
 - **Directory Name:** An arbitrary directory name.
 - **Access Type:** LDAP is the only type supported.
 - **Server Name:** The server name.
 - **Port:** The server port. 389 is the default port.
 - **Search Base:** A comma-separated list of name-value pairs used in the search. For example, `c=us,cn=Brown Trout,ou=example,dn=Acme Manufacturing` for country, common name, organizational unit, and distinguished name.
 - **This server requires me to log on:** Check this box if the server requires username and password authentication to look up LDAP entries.
 - **User name:** The login username.
 - **Password:** The login password.
 - **Timeout:** The number of seconds to keep trying to connect.
 - **Maximum Number of Records to Receive:** The number of records to return.
5. Choose **OK**.

Figure 33 Digital ID Directory servers: Setting server details

Directory Name:

Server Settings

Access Type:

Server Name: Port:

Search Base:

☒ This server requires me to log on

User name:

Password:

Timeout (in seconds):

Maximum Number of Records to Receive:

3.4.2 Editing Directory Servers Details

Directory server details can be changed at any time.

To edit directory server information:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Directory Servers** in the left-hand list ([Figure 32](#)).
3. Select a directory server from the right-hand panel.
4. Choose **Edit**.
5. Edit the information as described in [“Manually Configuring a Directory Server” on page 41](#).
6. Choose **OK**.

3.4.3 Deleting a Directory Server

Previously configured directory servers can be removed from the server list at any time.

To delete a directory server:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Directory Servers** in the left-hand list ([Figure 32](#)).
3. Select a directory server from the right-hand panel.
4. Choose **Remove**.
5. When a confirmation dialog appears, choose **OK**.

3.4.4 Specifying a Default Directory Server

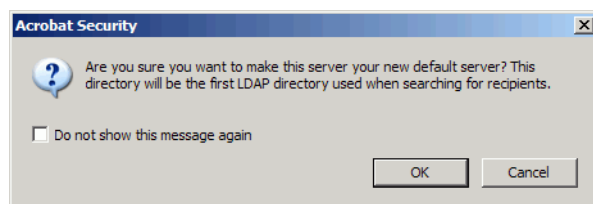
A default server may be specified so that it is always used when searching for digital IDs.

To set default directory server:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security Settings**.
2. Select **Directory Servers** in the left-hand list (Figure 32).
3. Select a directory server from the right-hand panel.
4. Choose **Set Default**.
5. Choose **OK** if a confirmation dialog appears.

A star appears next to the name of the selected server.

Figure 34 Digital ID Directory servers: Setting defaults



3.4.5 Importing and Exporting Directory Server Settings

For details, refer to the following:

- ["Importing Directory Server Settings" on page 134](#)
- ["Emailing Server Details" on page 125](#)
- ["Exporting Server Details" on page 126](#)

3.5 Managing Contacts

Contacts are those people that will send you documents or receive documents from you. Each contact may be associated with one or more certificates. Like certificates, contacts can be added, removed, edited, and so on from the trusted identity list.

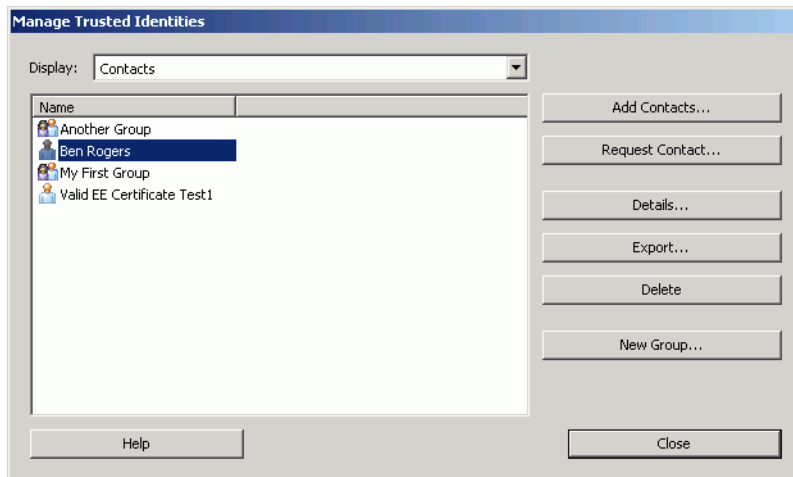
3.5.1 Viewing and Editing Contact Details

When a contact's details change, it is possible to update them in the Trusted Identity Manager.

To change a contact's details:

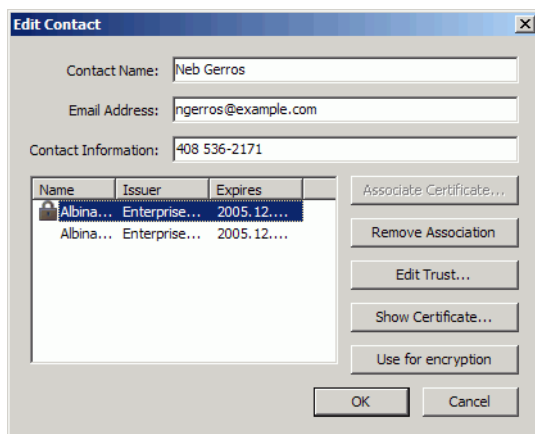
1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose a contact in the left-hand list.

Figure 35 Contacts: Viewing details



3. Choose **Details**.

Figure 36 Edit Contact dialog



4. Edit the details.
5. Choose **OK**.

3.5.2 Emailing Certificate or Contact Data

You can export certificate and contact data via email directly from the Trusted Identity Manager. Doing so allows other users to add that data their trusted identity list, thereby expanding the number of users that can participate in secure document workflows. For details, see [“Emailing Your Certificate” on page 122](#).

3.5.3 Saving Certificate or Contact Details to a File

You can export certificate and contact data and save it to a file from the Trusted Identity Manager. Doing so allows you to email it later or locate it on a shared network directory. Other users can then add that data to their trusted identity list. For details, see [“Saving Your Digital ID Certificate to a File” on page 123](#).

3.5.4 Associating a Certificate with a Contact

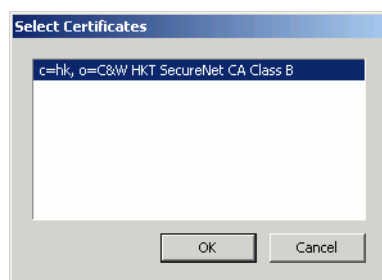
A certificate is usually already associated with a contact. However, in certain cases the two may need to be reassociated:

- Someone has provided you with new contact information.
- An old contact has sent you a certificate to be associated with old contact information.

To associate a certificate with a contact:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose a contact in the left-hand list (Figure 35).
3. Choose **Details**.
4. Choose **Associate Certificate** (Figure 36).

Figure 37 Contacts: Selecting certificates



5. Select a certificate from the list.
6. Choose **OK**.
7. Choose **OK**.

3.5.5 Changing a Trusted Identity's Certificate Association

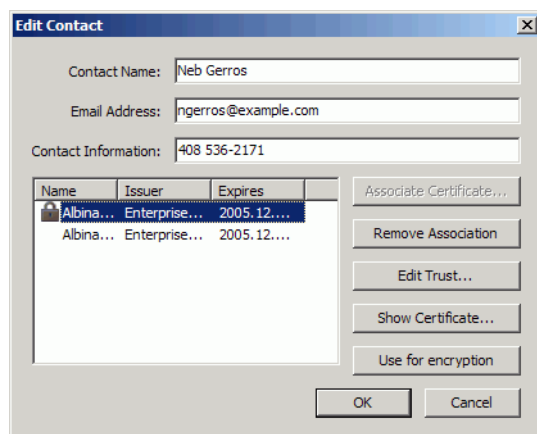
Contacts in the Trusted Identity Manager only have value when they are associated with certificates. Therefore, removing a certificate association only makes sense when it is being replaced by another certificate. For example, someone in your trusted identities list may have replaced a compromised or expired certificate with a new one. In this case, simply replace the old certificate association with a new one.

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose a contact in the left-hand list (Figure 35).
3. Choose **Details**.
4. Choose a certificate from the list.
5. Choose **Remove Association** (Figure 38).
6. Choose a certificate from the list.

Note: The certificate list is populated with the currently associated certificate and any unassociated certificates for the current contact. In other words, the list does not display all of a contact's certificates, it displays only those that have no contact association.

7. Choose **Associate Certificate**.
8. Choose **OK**.

Figure 38 Edit Contact dialog



3.5.6 Deleting Contacts and Certificates

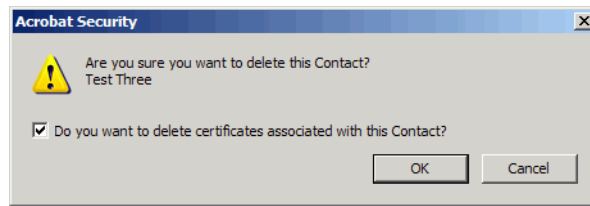
It is possible to delete contact information independently from its certificate. The most common scenarios for deleting trusted identity information include the following:

- You no longer share documents with someone and can delete all of their contact and certificate data.
- The trusted identity's contact information or certificate has changed and new data will be imported.

To delete a contact (and optionally a certificate):

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose Contacts from the **Display** drop-down list.
3. Choose a contact in the left-hand list (Figure 35).
4. Choose **Delete**.
5. Choose whether or not to delete the certificates along with contact. Once a certificate is deleted, it can no longer be used to validate someone's signature or encrypt a document for them.
6. Choose **OK**.

Figure 39 Contacts: Deleting



Deleting a Certificate

To delete a certificate:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Manage Trusted Identities**.
2. Choose Certificates from the **Display** drop-down list.
3. Choose a certificate in the left-hand list ([Figure 36](#)).
4. Choose **Delete**.
5. Choose **OK**.

Security methods provide a mechanism for users to specify document encryption and permission settings. You can encrypt all or part of a document and limit user actions such as only allowing form field fill-in or preventing printing. Each security method offers a different set of benefits, so familiarize yourself with the pros and cons of each type before proceeding (Table 5). Additionally, you can reuse your security settings by saving them as a policy.

To learn about security methods, see the following:

- [“Security Method Basics” on page 48](#): You should understand the options available for specifying the security type, the encryption and permissions options, and whether or not your security settings should be saved as a policy.
- [“Changing and Viewing Security Settings” on page 55](#): Security settings can be changed at any time by the document author.
- [“Security Policies: Reusable Security Settings” on page 59](#): If you would like to reuse your settings, save them as a policy.

For details about security method types, see the following:

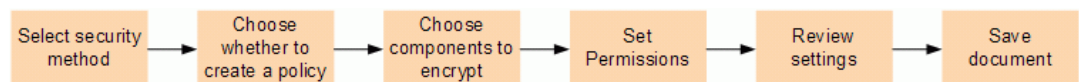
- [Chapter 5, “Password Security”](#): Use password security if document recipients do not have digital IDs or it is too cumbersome to collect their certificates.

Tip: Password security is unavailable if your application is operating in FIPS mode. Trying to save a document with password security applied results in an alert stating that this security method uses a non-FIPS compliant algorithm.
- [Chapter 6, “Certificate Security”](#): Use certificate security if you can share digital ID certificates with workflow participants, need to configure different permissions for different users, or don’t want to rely on shared passwords.
- [Chapter 7, “LiveCycle Rights Management Server Security”](#): If your company uses an Adobe LiveCycle Rights Management Server, use it to control document access and view audit trails.

4.1 Security Method Basics

Security is often added to documents to limit viewing, editing, printing, and other features to only those users that have the required password, a digital ID, or access to an Adobe LiveCycle Rights Management Server. Acrobat’s default security methods not only protect document content from unauthorized access, but also allow users to specify encryption levels and permission settings. At a high level, adding security to a document involves selecting a security type, configuring encryption and permissions, and then saving the document (Figure 40).

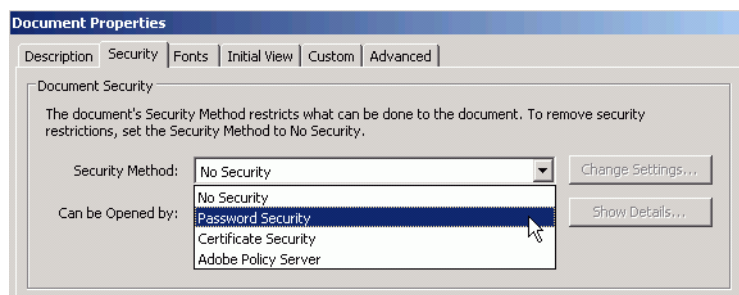
Figure 40 Security method workflow



Unless saved as a policy, security settings are document-specific and do not apply to other documents. Security can be added to a document through two main methods:

- Create new settings that may or may not be saved as a policy: Choose **Advanced > Security > Show Security Properties**, and then select and configure a method (Figure 41). Both certificate and ALCRMS security allows the user to save the settings as a policy.

Figure 41 Security method selection



- Create a new security policy with the Policy Manager: Choose **Advanced > Security > Manage Security Policies**. When the Policy Manager opens, choose **New**, select a policy type, and configure it (Figure 50).

4.1.1 Choosing a Security Method Type

While custom security handlers may be installed, the default security methods provide a wide range of robust options. There are a number of reasons to choose one security type over another, but all methods let the user specify encryption algorithms, what document components to encrypt, and what permissions should be granted to whom. Selecting a security type can involve an analysis of each method's pros and cons (Table 5) or each security method's basic features:

- **Password security:** Password security provides a simple way to share documents among users where sharing passwords is possible or when high levels of backward compatibility is required. Password policies do not require specifying any document recipients.

Tip: Password security is unavailable if your application is operating in FIPS mode. Trying to save a document with password security applied results in an alert stating that this security method uses a non-FIPS compliant algorithm.

- **Public key certificate security:** Certificate security provides a high level of security, eliminates the need for password sharing, and allows assigning different permissions to different users whose identities can be verified and managed. Supported by Acrobat 6.0 and later.
- **Adobe LiveCycle Rights Management Server security:** These policies are stored on a server, and server access is required to use them. User access information is embedded in the document, so creating an ALCRMS policy involves specifying the document recipients from a list on the LiveCycle Server.

Table 5 Security method pros and cons

Method	Pros	Cons
Password	<ul style="list-style-type: none"> Backward-compatible to Acrobat 3.0 for certain encryption levels. Simple and easily understood. Share documents by sharing the password. Supports passwords for document opening. Supports password protecting document permission settings. 	<ul style="list-style-type: none"> Protection depends on password strength. Anyone who knows the password has document access. All users share the same permissions. Won't work when the application is in FIPS mode.
Certificate	<ul style="list-style-type: none"> No password has to be remembered. Key to unlock document is better protected and resides only on the intended recipients machine. Key is not susceptible to brute force discovery. Can encrypt documents for specific people. When the recipient's certificate is in the trusted identities list, passwords are eliminated. Can use certificates issued by a trusted 3rd party certificate authority. Allows specifying different permission settings for users. 	<ul style="list-style-type: none"> Users must have a digital ID. Organizations need to distribute and manage digital IDs. Compatible with Acrobat 5.0, but full support appears first in 6.0.
ALCRMS (server-based)	<ul style="list-style-type: none"> Centralized administration of security policies. Enables document auditing by user. Allows setting permissions for separate tasks such as opening, editing, and so on. Allows specifying different permission settings for users. Can leverage LDAP directories for recipients and group lists. Controls end-user offline access since authors can specify a validity time limit after which the document expires and is locked. 	<ul style="list-style-type: none"> Requires a network connection. Requires an administrator and some infrastructure such as a LiveCycle Server.

4.1.2 Security Policies

Most workflows allow users to save the settings as a policy, thereby creating a reusable library of preconfigured security methods. When a policy author sets an encryption levels and recipient permissions and then saves them, the policy can later be applied to any document by choosing **Advanced > Security > Manage Security Policies** and selecting a policy. Policies save time and ensure a consistently secure workflow. For details, see [“Security Policies: Reusable Security Settings” on page 59](#).

4.1.3 Security Methods and Encryption

Encryption is used whenever a security method is added to a document. Security methods encrypt documents or parts of documents and are always involved in granting or denying permissions, thereby protecting content from unauthorized access and actions.

4.1.3.1 Encryption Workflow

The user workflow varies with the security method type as follows:

- **Password security:** The user is first asked to select a level of Acrobat backward compatibility. The selection automatically determines the encryption algorithm. Different document components can be encrypted based on the user's selection. See [Table 6](#).

Note: Password security is unavailable if your administrator has configured your application to operate in FIPS mode.

- **Certificate security:** The user selects what document components to encrypt and then chooses the encryption algorithm.
- **ALCRMS security:** The user selects what document components to encrypt. The algorithm is automatically applied by the server.

4.1.3.2 Choosing What to Encrypt

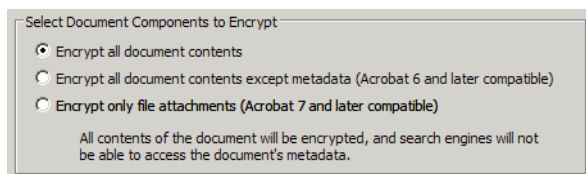
During the security method workflow, select a radio button in the **Select Document Components to Encrypt** panel to set the encryption options. You can encrypt all or part of a document based on your need for a specific security level and support for backward compatibility:

- **All contents:** Encrypts the document and its metadata (Acrobat 3 and later).
- **All contents except metadata:** Allows for document storage/retrieval systems and search engines to have access to the document metadata. A document open or a permissions password will be required to access other document content.

Encrypting everything except the metadata allows continued access to Acrobat's Catalog feature. By leaving the metadata unencrypted, users can catalog and index the metadata of encrypted documents, thereby making that data searchable (compatible with Acrobat 6 and later).

- **Only file attachments:** Allows full access to the document and encrypts only the file attachments. Permissions cannot be set on attachments. Using password security, a document open password is required for attachments (compatible Acrobat 7 and later).

Figure 42 Encryption configuration panel



4.1.3.3 Choosing an Algorithm

Acrobat continues to support more sophisticated encryption algorithms (Table 6). When configuring password security, users also have the opportunity to set the Acrobat compatibility level. Choosing to remain compatible with earlier versions of Acrobat results in the use of older algorithms and limits the document components which may be encrypted. For example, choosing a compatibility level of Acrobat 5.0 or earlier does not enable encrypting document contents but not metadata.

When you apply certificate security you will be asked to select between the 128-bit RC4 or 128 or 256 bit AES algorithms. The selection criteria should include the following:

- **256-bit AES** is only compatible with Acrobat 9.0 and later. It is the most secure algorithm but results in the largest file size.
- **128-bit AES** is only compatible with Acrobat 7.0 and later. It is mandated for some U.S. government documents because it is more secure than RC4. AES has a bigger file size and adds up to 32 bytes per stream.

- **128-bit RC4** is compatible with Acrobat 6.0 and later as well as other non-Adobe and Adobe PDF clients such as Ghostscript® and Apple Preview® that have not implemented AES. RC4 has a smaller file size by about 32 bytes per stream.

Note: RC4 is unavailable if your administrator has configured your application to operate in FIPS mode.

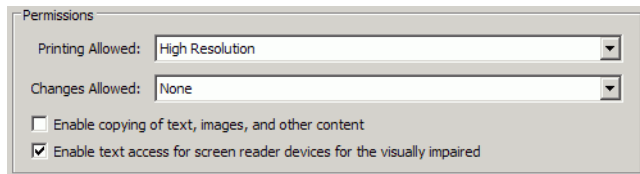
Table 6 Encryption algorithm by security type and product version

V.	Password Security	Certificate Security	LiveCycle Server
9.0	Algorithms: 128-bit RC4, 128 and 256 bit AES Options: All contents, all but metadata, only attachments.	Algorithms: 128-bit RC4, 128 and 256 bit AES Options: All contents, all but metadata, only attachments. Dropped support for .apf files.	Algorithms: 128 and 256 bit AES Options: All contents, all but metadata, only attachments.
8.1	Same as 8.0 except if FIPS mode is turned on, password security is not available.	Same as 8.0 except if FIPS mode is turned on, RC4 is not available.	Same as 8.0
8.0	Algorithms: 128-bit RC4, 128-bit AES Options: All contents, all but metadata, only attachments.	Algorithms: 128-bit RC4, 128-bit AES Options: All contents, all but metadata, only attachments.	Algorithms: 128-bit AES Options: All contents, all but metadata, only attachments.
7.0	Algorithms: 128-bit RC4, 128-bit AES Options: All contents, all but metadata, only attachments.	Algorithms: 128-bit RC4, 128-bit AES Options: All contents, all but metadata, only attachments.	Algorithms: 128-bit AES Options: All contents, all but metadata, only attachments.
6.0	Algorithms: 40 & 128-bit RC4 Options: All contents, all but metadata.	Added support for third-party certificates. Algorithms: 40 & 128-bit RC4 Options: All contents, all but metadata.	N/A
5.0	Algorithms: 40 & 128-bit RC4 Options: All contents.	Self-sign p7b & apf files only. Algorithms: 40 & 128-bit RC4 Options: All contents.	N/A
4.0	Algorithms: 40-bit RC4	N/A	N/A
4.0.5	Algorithms: 40-bit RC4 (64-bit decrypt) Options: All contents.	N/A	N/A
3.0	Algorithms: 40-bit RC4	N/A	N/A
2.0	Algorithms: 40-bit RC4	N/A	N/A

4.1.4 Security Methods and Permissions

Permissions can be set whenever a security method is added to a document. Permission settings enable a document author to limit a document recipient's activities and interaction with a document. For example, restrictions can be placed on editing, copying, and printing. You set permissions by choosing the desired options in the Permissions panel when applying a security method.

Figure 43 Permissions panel



4.1.4.1 Permissions Workflow

The workflow varies slightly with the security method type as follows:

- **Password security:** The permissions panel appears at the beginning of the workflow. Checking **Restrict editing and printing of the document** enables all the other fields. Only the password security method requires a permissions password. If the document has a permission and a document open password, it can be opened with either password. The two passwords cannot be identical.
- **Certificate security:** The permissions panel appears at the end of the workflow. Permissions can be individually specified for different users by highlighting a specific recipient and choosing **Permissions**.
- **ALCRMS security:** The permissions are set ahead of time when the method is configured online. Permissions can be individually specified for different users by highlighting a document recipient and choosing **Permissions**. ALCRMS security provides the option of preventing a document recipient from saving and viewing the document offline, thereby storing a copy of the document on the local machine. This may not be desirable on public computers or when the computer is not secure.

4.1.4.2 Permissions Options

All of the security methods provide the following options:

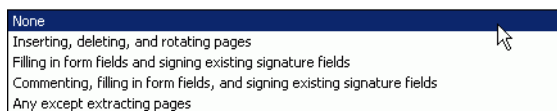
Note: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions. Eryption and therefore document access would likely not be impaired, but Adobe cannot guarantee that individual permissions settings will remain function. Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**

- **None:** Prohibits printing.
- **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
- **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



- **None:** Prevents users from changing the document, including filling in signature and form fields.
 - **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
 - **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
 - **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
 - **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.
3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.

4.1.5 Associating Batch Processing with a Security Method

Acrobat can be configured to associate batch processes with a security method. When a batch process is associated with a security method, the method is invoked whenever a batch process is initiated.

To set the batch process security preference:

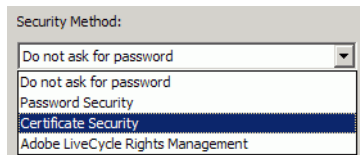
1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select **Batch Processing** in the left-hand tree.
3. Select a security method from the drop-down list.

The security handler does not apply security to files. Instead, it determines how batch processing deals with files that are password-protected.

- If **Don't Ask For Password** is selected, the batch sequence proceeds as if the files are not secure.
- If **Password Security** is selected, batch processing pauses when it encounters secured files and prompts for a password.

4. Choose **OK**.

Figure 44 Security methods for batch processing



4.2 Changing and Viewing Security Settings

While anyone who can open a document can view its security methods, only those with permission can change those methods.

4.2.1 Viewing Document Encryption and Permission Settings

A document's security settings specify an encryption level (algorithm), what components are encrypted, and permissions. The document may be subject to additional restrictions if it is signed or certified. For more information, see ["Viewing Document Restrictions" on page 56](#).

To view a document's encryption settings:

1. Choose **Advanced** (Acrobat) or **Document** (Reader) > **Security** > **Show Security Properties**.

Tip: You can also choose **File** > **Document Properties** or press **Control + D** and view the Security tab.

2. Choose **Show Details**. The settings are displayed in a dialog that varies with the security method type. The dialog does not update until a user saves and closes the document.

Figure 45 Document security settings: Password security



Figure 46 Document security settings: Certificate security

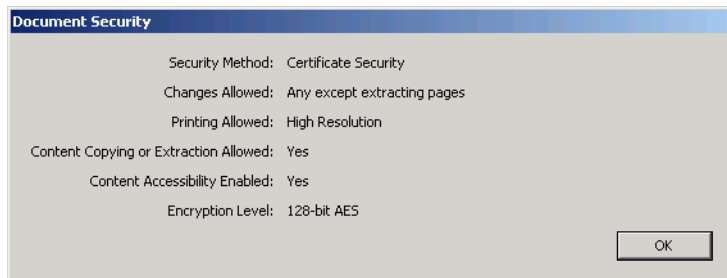
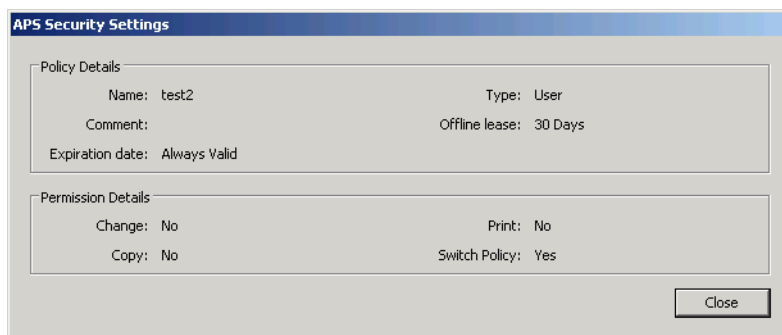


Figure 47 Document security settings: ALCRMS security



4.2.2 Viewing Document Restrictions

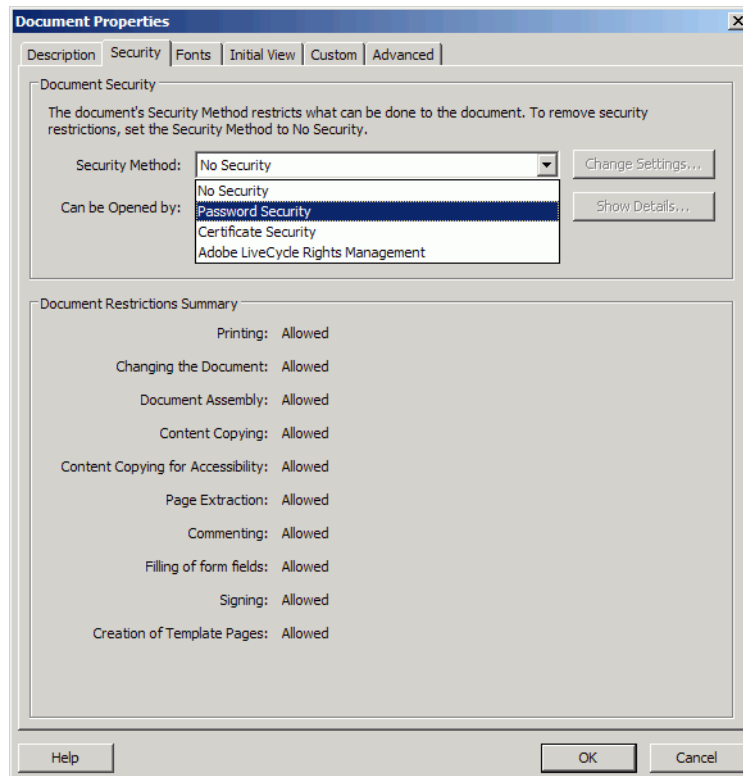
In addition to the encryption and permissions settings enforced by the document's security method, a document may be subject to additional restrictions if it is signed or certified. A summary of all security methods and signature-related restrictions appears in the Document Restrictions Summary panel.

When a document has restricted features, any tools and menu items related to those features are disabled. Users who are restricted from using certain document features they think they need should contact the document author.

To view the document restrictions summary in the Document Properties dialog, choose **Advanced** (Acrobat) or **Document** (Reader) > **Security** > **Show Security Properties**.

Tip: You can also choose **Control + D** and view the Security tab.

Figure 48 Document Property dialog

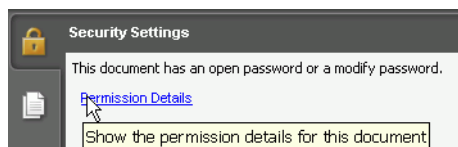


4.2.3 Viewing Security Settings in a Browser

To view document security settings in a Web browser:

1. Click on the lock icon in the left-hand pane.
2. Choose **Permissions Details**.

Figure 49 Security settings icon



4.2.4 Changing the Security Method Type

Security settings cannot be changed on signed documents. Signature fields must first be cleared.

To change a document's security method:

1. Choose **Advanced > Security > Show Security Properties**.
2. Choose a new security method from the drop-down list.

Note: New settings do not appear in the user interface until the document is closed and reopened.

3. If the document is password protected, enter the document password.
4. Choose a security method and configure it. For details, see the following:
 - [Chapter 5, "Password Security"](#)
 - [Chapter 6, "Certificate Security"](#)
 - [Chapter 7, "LiveCycle Rights Management Server Security"](#)
5. Choose **OK**.
6. Save the document. New settings do not appear in the user interface until the document is closed and reopened.

4.2.5 Editing Security Method Settings

To change the security settings for an encrypted document:

1. Choose **Advanced > Security > Show Security Properties**.
2. In the Security panel, choose **Change Settings**. For details, see the following:
 - [Chapter 5, "Password Security"](#)
 - [Chapter 6, "Certificate Security"](#)
 - [Chapter 7, "LiveCycle Rights Management Server Security"](#)

Note: New settings do not appear in the user interface until the document is closed and reopened.

3. Save the document.

4.2.6 Removing Document Security

Security can be removed from an open document by those with permissions to do so. You may be required to enter a password or have the requisite certificate to remove a policy.

To remove security settings from a document:

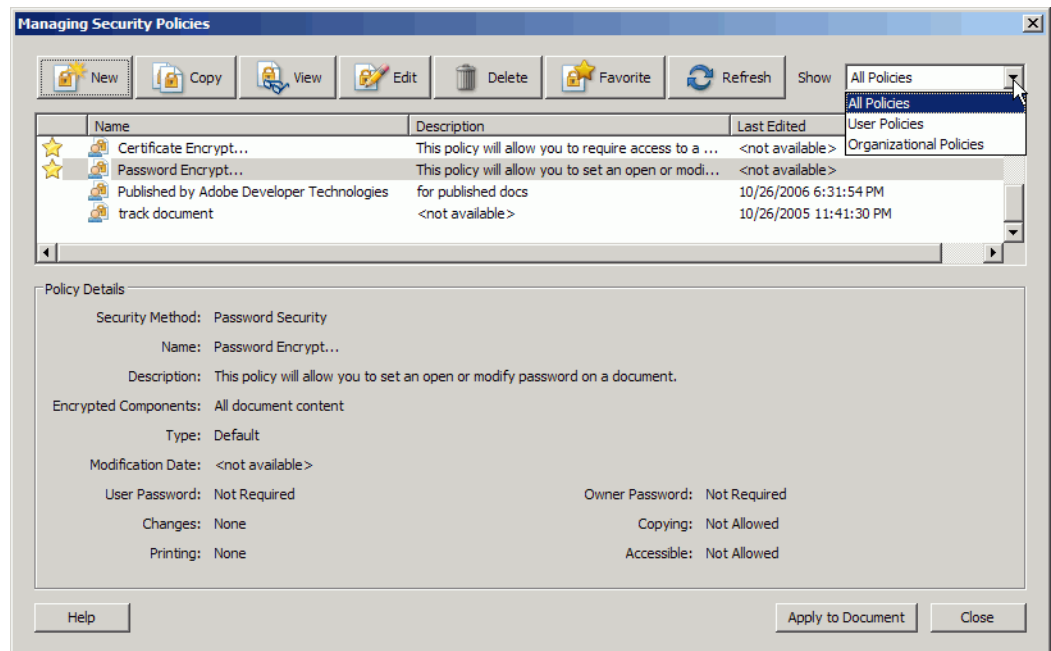
1. From the toolbar, choose **Advanced > Security > Remove Security**.
2. If prompted, type the permissions password.
3. When asked to confirm removal of the security settings, choose **OK**.
4. Choose **OK**.

4.3 Security Policies: Reusable Security Settings

Security policies provide a way to save and reuse security method settings. Saving your configured security method as a policy saves time and effort later. Policies are not embedded in a document. When a document is sent to someone, it contains the specified security settings, but the policy stays with the policy author.

Note: Policies can be applied to documents created with any version of Acrobat. However, specific policy settings may not be supported for documents created with some earlier versions.

Figure 50 Security method selection from Policy Manager



Policy settings include two main kinds of information:

- Encryption type, permission settings, and passwords (if any).
- Information about the individuals or groups that can open a document or change its security settings.

There are two categories of security policy sources. These policies can be displayed together or individually (Figure 50):

- **User policies:** User policies are created and applied by anyone. User password and certificate policies are stored locally while Adobe LiveCycle Rights Management Server policies are stored on the server. Policy authors can edit and delete the policies they create.
- **Organizational policies:** An organizational policy is created by an Adobe LiveCycle Rights Management Server administrator and is stored on a policy server. The server controls access to documents and auditing events as defined by the security policy. Only a policy administrator can edit, and delete organizational policies.

4.3.1 Creating Security Policies with Policy Manager

Policies can be created ahead of time or during the course of creating new security settings. When the Security Settings Console appears, simply choose **Save these settings as a policy** and enter a policy name and optional description (Figure 51).

Figure 51 Security policy: General settings

Provide a name and description for your Password Policy.

☒ Save these settings as a policy
☐ Discard these settings after applying

Policy name: max. 50 Characters

Description: max. 250 Characters

☒ Save passwords with the policy!

To create a security policy ahead of time with Policy Manager:

1. Choose **Advanced > Security > Manage Security Policies** (Figure 50).
2. Choose **New**.
3. Select a security method for the policy and configure in the appropriate section:
 - [Chapter 5, "Password Security"](#)
 - [Chapter 6, "Certificate Security"](#)
 - [Chapter 7, "LiveCycle Rights Management Server Security"](#)

Figure 52 Policy security method selection

How would you like to protect your documents?

Security policies are a collection of reusable security settings.

☒ Use passwords
Require a password when opening a document or restrict document rights, such as the ability to edit or print.

☐ Use public key certificates
You can use someone's public key certificate to encrypt documents so that only they may open the document. Certificates can be found in your trusted identities list, or using a directory search.

☐ Use Adobe LiveCycle Rights Management
If you have access to an Adobe LiveCycle Rights Management Server, you can restrict document access and rights using the user names of people or groups registered with this server.

4.3.2 Applying a Security Policy to a Document

Organization and user policies can be applied to any document by those who have permission to do so.

Tip: If policies are available via a server, Choose **Advanced > Security > Manage Security Policies > Refresh** to ensure that you have access to the most up-to-date server policies.

To apply a security policy to a document:

1. Choose **Advanced > Security > Secure this Document**.
2. Highlight a policy.
3. Choose **Apply to Document**.
4. Save the document.

Tip: If a policy has been designated as a “favorite,” a star appears next to the selected policy. All favorites appear in the security menu ([Figure 53](#)).

4.3.3 Viewing a Security Policy

To view a security policy:

1. Choose **Advanced > Security > Manage Security Policies** ([Figure 50](#)).
2. Choose a security policy.
3. Choose **View**.

The policy opens in read-only mode and cannot be edited.

4.3.4 Copying a Security Policy

Copying a policy is useful when a new policy is needed that is similar to an existing policy. The first policy is simply copied, edited, and saved under a new name.

To copy a security policy:

1. Choose **Advanced > Security > Manage Security Policies** ([Figure 50](#)).
2. Choose a security policy.
3. Choose **Copy**.
4. Change the policy’s settings as described in one of the following sections:
 - [Chapter 5, “Password Security”](#)
 - [Chapter 6, “Certificate Security”](#)
 - [Chapter 7, “LiveCycle Rights Management Server Security”](#)

4.3.5 Editing a Security Policy

Existing policies can be edited. For example, if a document is distributed to a group of users and the owners wants to revoke permission for others to open it, the owner can change the policy.

To edit a security policy:

1. Choose **Advanced > Security > Manage Security Policies** ([Figure 50](#)).
2. Choose a security policy.
3. Choose **Edit**.

4. Change the policy's settings as described in one of the following sections:
 - [Chapter 5, "Password Security"](#)
 - [Chapter 6, "Certificate Security"](#)
 - [Chapter 7, "LiveCycle Rights Management Server Security"](#)

4.3.6 Making a Security Policy Favorite

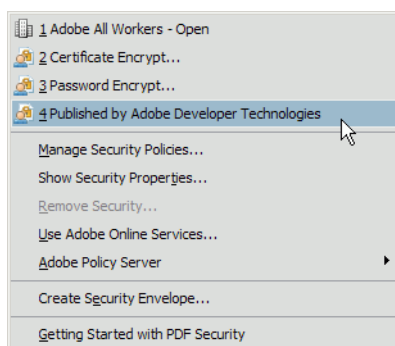
When a policy is selected as a favorite, a star appears next to that policy and the policy is then listed on the security menu. Any new policy you create is automatically made a favorite.

To make a security policy favorite:

1. Choose **Advanced > Security > Manage Security Policies** ([Figure 50](#)).
2. Choose a security policy.
3. Choose **Favorite**.
4. Choose **Close**.

A star appears next to the selected policy. "Favorited" policies appear in the security menu ([Figure 53](#)).

Figure 53 Security policy: Favorites list



4.3.7 Refreshing the Security Policy List

If the policies are available via a server, refresh the security policy list to ensure that you have access to the most up-to-date server policies.

1. Choose **Advanced > Security > Manage Security Policies**.
2. Choose **Refresh**.
3. When the login screen appears, enter a username and password.
4. Choose **OK**.

4.3.8 Deleting a Security Policy

A user can delete any policy that they created. It is not possible to delete organizational policies created by an administrator.

To delete a security policy:

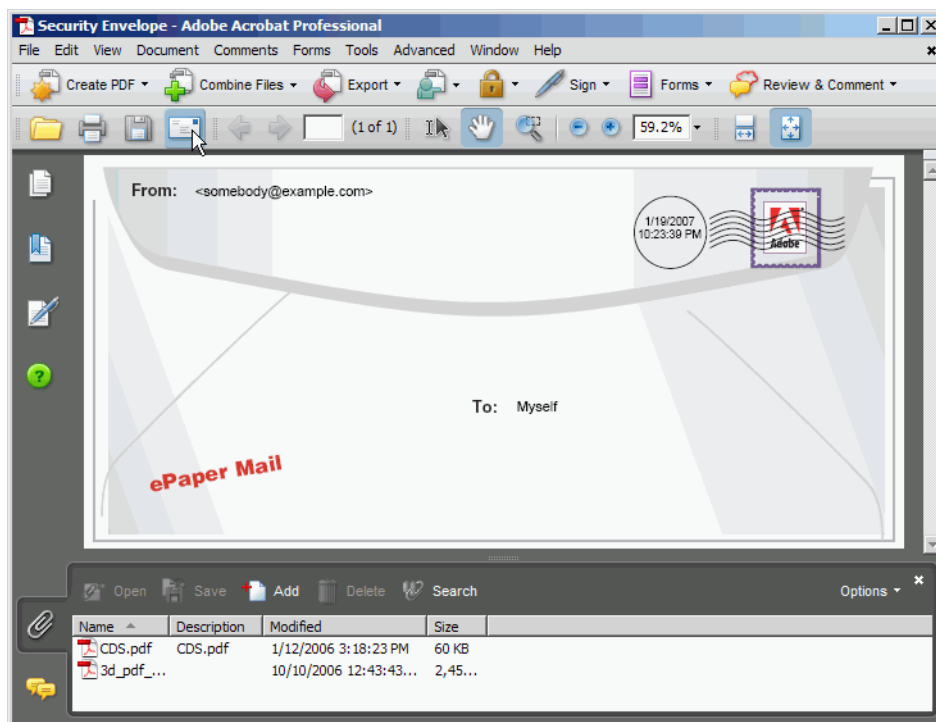
1. Choose **Advanced > Security > Manage Security Policies** (Figure 50).
2. Choose a security policy.
3. Choose **Delete**.
4. Choose **Yes** at the confirmation dialog.
5. Choose **Close**.

4.4 Envelopes

You can add security to one or more documents by embedding them in an encrypted envelope, called a security envelope. Envelopes are simply PDF files with attachments. This method is especially useful if you want to send a secure file attachment without modifying or encrypting the attached files. When someone opens the envelope, they can extract the attachments and save them to disk. The saved files are identical to the original file attachments and are no longer encrypted when saved.

For example, suppose that you want to send several documents, including non-PDF documents, to your accountant, but you don't want anyone else to view the documents. You can embed these documents as file attachments in a security envelope, encrypt the security envelope so that only your accountant can open the attachments, and then email it. Anyone can open the envelope, view its cover page, and even view a list of the contents of that envelope, but only your accountant can view the embedded attachments and extract them to the computer.

Figure 54 Security envelope



Embed file attachments in security envelopes for secure transit.

1. Choose the **Advanced > Security > Create Security Envelope**.
2. Choose **Add File To Send**.
3. Browse to the documents you want to attach and choose **Open**.
Select any PDFs in the list that you don't want to include and choose **Remove Selected Files**.
4. Choose **Next**.
5. Select an envelope template.
6. Choose **Next**.
7. Select whether to deliver the envelope now or later. In most cases, you will want to choose **Send the envelope later** so you can view it and fill out its form fields before sending.

Note: Templates sometimes contain form fields (such as **To** and **From**) that you can fill in before sending. If you choose to send now and a dialog asks if you really want to send before filling in these fields, choose **Yes** or **No** to continue.

8. Choose **Next**.
9. Choose **Next** OR apply a security policy. Security policies are optional.
Select **Show All Policies**, and then select a security policy from the list of available policies (or create a new policy if needed).
Tip: Follow the on-screen instructions to complete the security envelope. If prompted, provide your identity information.
10. Choose **Finish**.
11. Type an email address in the message that appears and choose **Send**, or save the security envelope to send later.

5 Password Security

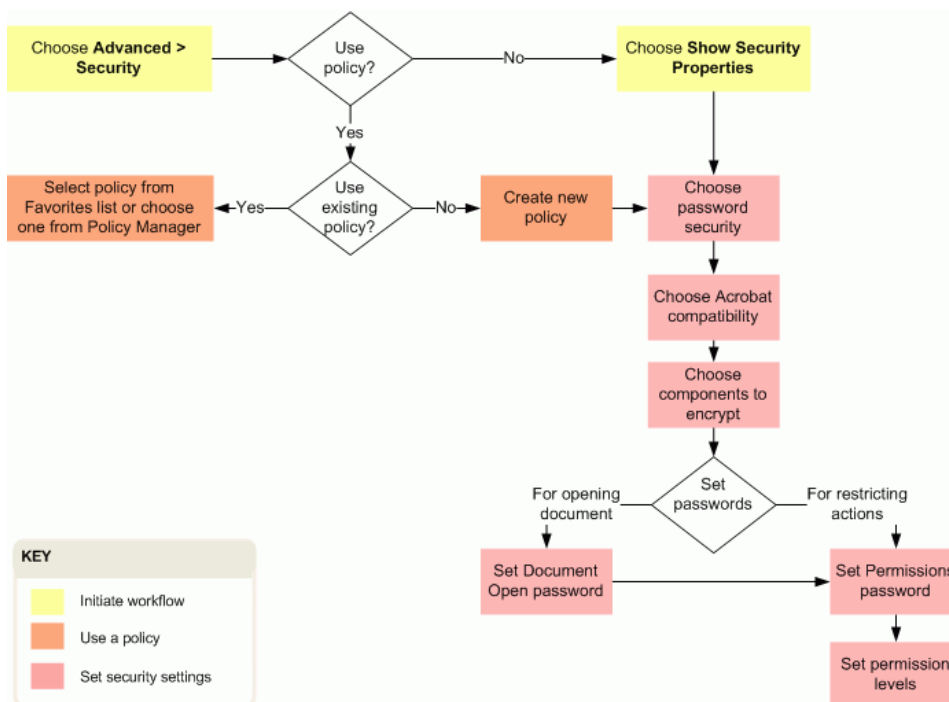
Acrobat users can perform any task in this section. Adobe Reader users can only view encrypted documents and can not encrypt them for others.

Password security provides a simple method for sharing encrypted documents by sharing passwords. Like all security methods, password security can enforce document restrictions on operations such as opening, printing, and editing. Since password security does not provide the ability to specify different permissions for different users, everyone that can open the document will have the same permissions.

Document protection has a dependency on password strength. Acrobat 9.0 now allows full Unicode pass phrases up to 128 characters in length (an actual limit of 128 UTF-8 bytes). Acrobat 8.x and earlier limits passwords to 32 characters maximum and almost entirely to the Latin alphabet (strictly, PDFDocEncoding). Password security encryption levels may also be set to be backward-compatible to Acrobat 3.0.

Note: Password security is unavailable if your administrator has configured your application to operate in FIPS mode.

Figure 55 Password security workflow



Password security also provides separate options for opening the document and setting user permissions; therefore, password security uses two kinds of passwords: a Document Open password and a Permissions password.

- **Document open password:** Required to open a password-protected document.
- **Permissions password:** Required to change permissions such as those for copying and editing.

Tip: If the document has both types of passwords, it can be opened with either password. The document open password and permissions password cannot be identical.

At a high level, adding password security includes specifying encryption settings, creating a Document Open password (if needed), creating a Permissions password (if needed), specifying permissions settings, and saving the document (Figure 55).

5.1 Creating Password Security Settings

Configure and add password security to a document by either creating a policy which can be saved and reused or by creating them once and discarding them. For details, see:

- “Creating a Reusable Password Security Policy” on page 66
- “Creating Password Security for One-Time Use” on page 69

5.1.1 Creating a Reusable Password Security Policy

1. Choose **Advanced > Security > Manage Security Policies** to open the Policy Manager.
2. Choose **New**.
3. Choose **Use passwords**.
4. Choose **Next**.
5. Enter a policy name and optional description.
6. Check or uncheck **Save passwords with the policy**.

Tip: You can save the password with the policy so that it’s automatically used, or you can have Acrobat prompt you for the policy each time you apply it.

Figure 56 Security policy: General settings

Provide a name and description for your Password Policy.

☒ Save these settings as a policy
☐ Discard these settings after applying

Policy name: max. 50 Characters

Description: max. 250 Characters

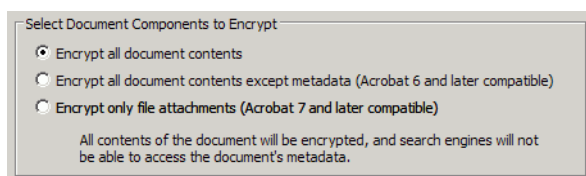
☒ Save passwords with the policy

7. Choose **Next**.
8. Configure the security settings dialog:

1. **Compatibility:** The compatibility options determine what encryption options will be available. Compatibility with earlier versions of Acrobat may mean all document contents will have to be encrypted. Set the Acrobat compatibility level as follows:
 - **Acrobat 3.0 and later:** Encryption uses the 40-bit RC4 encryption algorithm. This setting forces the encryption of strings and streams only and limits other features.
 - **Acrobat 5.0 and later:** Encryption uses the 128-bit RC4 encryption algorithm. This setting allows the accessibility option to be selected independently of the copy option, restricts printing to 150-bit dpi, and expands the set of **Changes Allowed** options.
 - **Acrobat 6.0 and later:** Encryption uses the 128-bit RC4 algorithm. This setting allows the option of leaving the document metadata unencrypted while the remainder of the document is encrypted. All of the options for Acrobat 5.0 and later are also available.
 - **Acrobat 7.0 and later:** Encryption uses the 128-bit AES algorithm. When selected, the option of only encrypting the file attachments is available as well as all of the previous options.
 - **Acrobat 9.0 and later:** Encryption uses the 256-bit AES algorithm. Password length can be up to 64 characters.
2. Configure the **Select Document Components to Encrypt** panel.
 - **All contents:** Encrypts the document and its metadata (Acrobat 3 and later).
 - **All contents except metadata:** Allows for document storage/retrieval systems and search engines to have access to the document metadata. A document open or a permissions password will be required to access other document content.

Encrypting everything except the metadata allows continued access to Acrobat's Catalog feature. By leaving the metadata unencrypted, users can catalog and index the metadata of encrypted documents, thereby making that data searchable (compatible with Acrobat 6 and later).
 - **Only file attachments:** Allows full access to the document and encrypts only the file attachments. Permissions cannot be set on attachments. Using password security, a document open password is required for attachments (compatible Acrobat 7 and later).

Figure 57 Encryption configuration panel



9. If you would like to control who can open the document, provide a Document Open password. You must provide a document open, a permissions password, or both. If you only need to create a permissions password, skip to [Step 8](#).
 - Check **Require a password to open the document**.
 - Enter a password.
10. If you would like to use password-based permissions, check **Use permissions password to restrict editing of security settings**. Otherwise, skip to [Step 12](#).

Document authors can set a permissions password that allows users to change the document's permissions. Only a holder of the permissions password will be able to change the permissions. The Permission password can also be used to open the document even if there is a separate Document Open password.

Tip: Adobe recommends that permission passwords and document open password always be used together. The permissions password is used to change permissions and is NOT needed to gain access to the features the author is permitting. Thus, holders of the permissions password are essentially “owners” of the document and can do anything to it that the author could do.

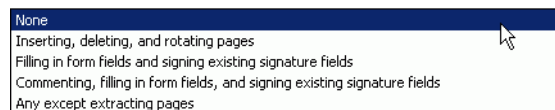
Caution: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions (the encryption would not be violated). Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**

- **None:** Prohibits printing.
- **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
- **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



- **None:** Prevents users from changing the document, including filling in signature and form fields.
 - **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
 - **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
 - **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
 - **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.
3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.

11. Choose **OK**.
12. Reenter the Document Open and/or Permissions passwords (if any) when asked to confirm it and choose **OK**.
13. Choose **Finish**.

5.1.2 Creating Password Security for One-Time Use

Use this method if you:

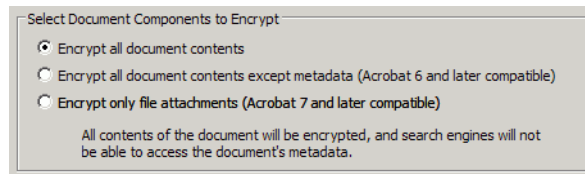
- Need to make the document backward-compatible to Acrobat 3.0.
- Do not need to save the settings as a policy.

To apply password security to the current document:

1. Choose **Advanced > Security > Show Security Properties**.
2. Select **Password Security** from the Security Method menu.
3. Check or uncheck **Save passwords with the policy**.
4. Choose **OK**.
5. Set the compatibility level to control what encryption options will be available. Compatibility with earlier versions of Acrobat may require encrypting all document contents. Compatibility levels include:
 - **Acrobat 3.0 and later:** All document contents are encrypted with the 40-bit RC4 algorithm. This option provides the most limited set of permission setting options.
 - **Acrobat 5.0 and later:** Encryption uses the 128-bit RC4 encryption algorithm. This setting allows the accessibility option to be selected independently of the copy option, restricts printing to 150-bit dpi, and expands the set of **Changes Allowed** options.
 - **Acrobat 6.0 and later:** Encryption uses the 128-bit RC4 algorithm. This setting allows the option of leaving the document metadata unencrypted while the remainder of the document is encrypted. All of the options for Acrobat 5.0 and later are also available.
 - **Acrobat 7.0 and later:** Encryption uses the 128-bit AES algorithm. When selected, the option of only encrypting the file attachments is available as well as all of the previous options.
 - **Acrobat 9.0 and later:** Encryption uses the 256-bit AES algorithm. When selected, the option of only encrypting the file attachments is available as well as all of the previous options.
6. Configure the **Select Document Components to Encrypt** panel:
 - **All contents:** Encrypts the document and its metadata (Acrobat 3 and later).
 - **All contents except metadata:** Allows for document storage/retrieval systems and search engines to have access to the document metadata. A document open or a permissions password will be required to access other document content.

Encrypting everything except the metadata allows continued access to Acrobat's Catalog feature. By leaving the metadata unencrypted, users can catalog and index the metadata of encrypted documents, thereby making that data searchable (compatible with Acrobat 6 and later).
 - **Only file attachments:** Allows full access to the document and encrypts only the file attachments. Permissions cannot be set on attachments. Using password security, a document open password is required for attachments (compatible Acrobat 7 and later).

Figure 58 Encryption configuration panel



7. If you would like to control who can open the document, provide a Document Open password. You must provide a document open, a permissions password, or both. If you only need to create a permissions password, skip to [Step 8](#).

1. Check **Require a password to open the document**.

2. Enter a password.

8. If you would like to use password-based permissions, check **Restrict editing and printing of the document**. Otherwise, skip to [Step 10](#).

Document authors can set a permissions password that allows users to change the document's permissions. Only a holder of the permissions password will be able to change the permissions. Permission password can also open the document even if there is a separate Document Open password.

Tip: Adobe recommends that permission passwords and document open password always be used together. The permissions password is used to change permissions and is NOT needed to gain access to the features the author is permitting. Thus, holders of the permissions password are essentially "owners" of the document and can do anything to it that the author could do.

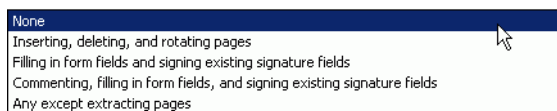
Note: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions. Encryption and therefore document access would likely not be impaired, but Adobe cannot guarantee that individual permissions settings will remain function. Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**

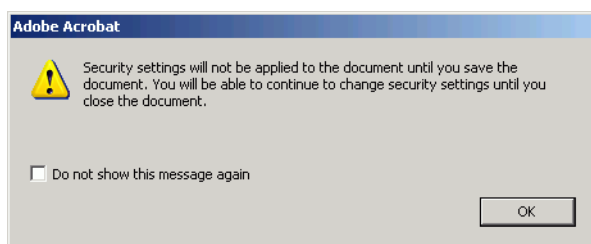
- **None:** Prohibits printing.
- **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
- **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



- **None:** Prevents users from changing the document, including filling in signature and form fields.
 - **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
 - **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
 - **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
 - **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.
3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.
9. Choose **OK**.
10. Reenter the Document Open and/or Permissions passwords (if any) when asked to confirm it and choose **OK**.
11. If an alert appears indicating the changes won't be applied until the document is saved, choose **OK**.

Figure 59 Security settings require "save" alert



12. Save the document. New settings do not appear in the user interface until the document is closed and reopened.

5.2 Opening a Password-Protected Document

You must know the Document Open or Permissions password to open the document.

To open a password protected document:

1. Open the document.
2. Enter the password.
3. Choose **OK**.

Figure 60 Password prompt



5.3 Removing Password Security

To remove password security settings from a document:

1. Open the document and supply the required password.
2. Do one of the following:
 - Choose **Advanced > Security > Remove Security**.
 - Choose **Advanced > Security > Show Security Settings** and select **No Security** from the Security Method menu in the Security tab of the Document Properties dialog box.
3. When asked to confirm that you would like to remove security, choose **OK**.
4. Save the document to have the change take effect.

5.4 Changing Document Collection Passwords

To change security settings for a collection of documents:

1. Choose **Advanced > Batch Processing**.
2. Do one of the following:
 - Select an existing sequence such as **Password** or **Set Security to No Changes**, and then choose **Run Sequence**.
 - To change the security options, define a new batch-processing sequence or edit an existing one.

5.5 Password Recovery

Caution: There is no way to recover a lost password from a document. Keep a backup copy that is not password-protected.

6

Certificate Security

Acrobat users can perform any task in this section. Adobe Reader users can only view encrypted documents and not encrypt them for others.

If you share documents that require high security, you may need certificate security. Businesses use certificate security because a public key infrastructure (PKI) enables central management by an administrator. The administrator can set up an LDAP directory server for providing certificate access, create custom certificates for specialized workflows, and so on. Where secure PDFs do not have to be compatible with Acrobat versions prior to 6.0, certificate security has several advantages:

- **Different users can have different permission settings:** Unlike password-based security which applies permissions equally to everyone, certificate security allows authors to specify permissions for individuals. For example, it is possible to give employees the ability to sign documents and fill in form fields while giving only managers the ability to add comments or delete pages. Permissions are useful for distributing documents to users that need varied document access and usage rights.
- **Superior security attributes:** No password has to be remembered or shared as the public and private keys to encrypt and decrypt documents reside only on the machines of those participating in secure workflows. These keys are less susceptible to brute force discovery than passwords.

Note: Participants in a certificate security workflow must have a digital ID and cannot use Acrobat versions prior to 6.0.

Figure 61 Certificate security workflow



6.1 Setting up the Certificate Security Environment

If you're going to use certificate security, consider doing the following:

- Configuring Acrobat to use certificates in the Windows Certificate store as well as those in the Acrobat store (which is on by default).
- Choosing which certificate to use for encryption for those contacts who have provided you with more than one.
- Setting up a group and a reusable security policy to simplify your workflows.

6.1.1 Accessing the Windows Certificate Store

The Windows Certificate Store contains certificates used by Windows applications. For example, when signing outgoing emails in Outlook, the digital ID comes from the Personal certificate store in Windows. The trusted certificates stored in the Windows Trusted People certificate store are used by Windows applications to validate signed emails from other people.

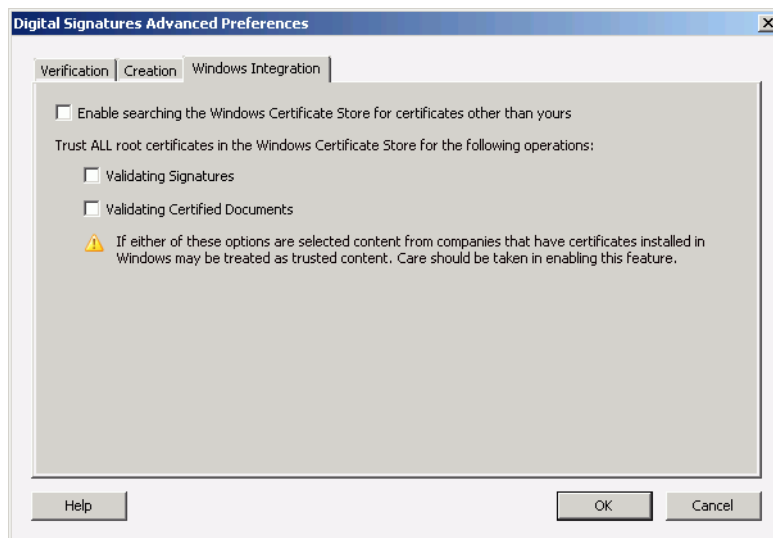
If you want to use certificates in the Windows Certificate Store to encrypt the document for the certificate owner, add the Windows store to the certificate search path. This allows you to search Windows directories when applying certificate security. By default, the Windows Certificate Store is not included in the application search path. Once the option is manually turned on, the Windows store will appear in the Search for recipients dialog **Directories** drop-down list.

To enable searching for certificates in the Windows Certificate Store:

1. Choose **Edit > Preferences**.
2. Choose **Security** in the left-hand panel.
3. Choose **Advanced Preferences**.
4. Display the Windows Integration tab.
5. Check **Enable searching the Windows Certificate Store for certificates other than yours**.
6. Choose **OK**.
7. Choose **OK**.

Tip: The checkboxes related to trust are only used for signature validation.

Figure 62 Windows integration



The Windows Certificate Store will now appear in Search for Recipients dialog's directory list. The dialog can be invoked from two locations:

- From a certificate security workflow: Set the encryption settings, choose **Next**, and then choose **Search**.
- From the Trusted Identity Manager: Choose **Add Contacts**, and then choose **Search**.

6.1.2 Selecting a Certificate to Use for Encryption

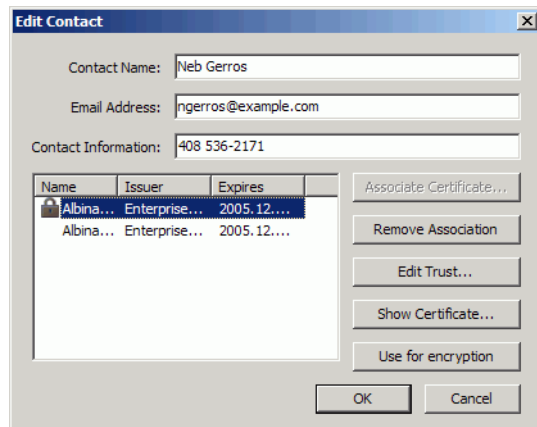
Because you encrypt a document for someone with the public key in their certificate, you must first explicitly choose their certificate for encryption. Each contact in your Trusted Identity list should be associated with at least one certificate. If there is only one certificate, Acrobat automatically selects it as the one to use for encryption. If more than one certificate is associated with the contact, you can select which one to use as the default encryption certificate.

Note: To use a certificate for encryption must have encryption usage rights. A warning dialog appears during the encryption process if the selected certificate cannot be used.

To set a default certificate for encryption:

1. Choose **Advanced > Manage Trusted Identities**.
2. Choose a contact in the left-hand list.
3. Choose **Details**.
4. Highlight a certificate in the certificate list.
5. Choose **Use for encryption** (Figure 63). The lock icon moves to the selected certificate.
6. Choose **OK**.

Figure 63 Choosing a certificate for encryption



6.2 Working with Groups of Contacts

Contacts can be added to a group so that all group members can easily share a predefined set of permissions and restrictions. For example, it is possible to create a certificate-based security policy that applies to an entire group. Administrators and home users can create a group and export the group's details to an FDF file that is then sent to individual users. This feature makes it easy to manage permissions for a large number of people.

Note: Importing a group imports the contacts (all group members), but not the group. If desired, create a new group from those newly imported contacts.

6.2.1 Creating a Group

Individual users and administrators create a group using the same method.

To create a group:

1. Choose **Advanced > Manage Trusted Identities**.
2. Choose **New Group**.
3. Enter a group name (Figure 64).
4. Add contacts .
5. Choose **OK**.

6.2.2 Adding or Removing Group Contacts

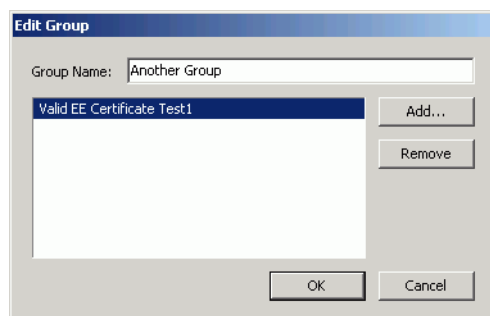
To add or remove group members:

1. Choose **Advanced > Manage Trusted Identities**.
2. Double-click on a group or highlight the group and choose **Details**.

3. Add or remove a contact:

- **Adding a contact:** Choose **Add**, select a contact from the contact list, and choose **OK** twice.
- **Removing a contact:** Select a contact, choose **Remove**, and choose **OK**.

Figure 64 Contacts: Editing a group

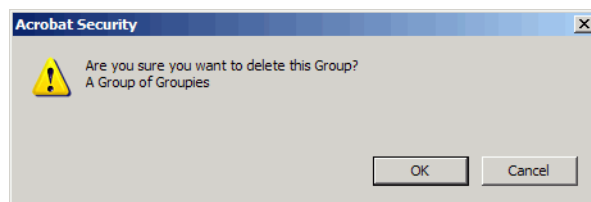


6.2.3 Deleting a Group

To delete a group:

1. Choose **Advanced > Manage Trusted Identities**.
2. Choose a group in the left-hand list.
3. Choose **Delete**.
4. Choose **OK**.

Figure 65 Contacts: Deleting a group



6.3 Creating Certificate Security Settings

When adding security to a document, you either create a policy which can be reused or creating the once and discard them. For details, see:

- ["Creating a Reusable Certificate Security Policy" on page 78](#)
- ["Creating Certificate Security for the Current Document" on page 82](#)

6.3.1 Creating a Reusable Certificate Security Policy

To create a certificate security policy:

1. Choose **Advanced > Security > Manage Security Policies**.
2. Choose **New**.
3. Select **Use public key certificates**.
4. Choose **Next**.
5. Enter a policy name and optional description.

Figure 66 Security policy: General settings

The screenshot shows a dialog box titled "Provide a name and description for your Password Policy." It contains two radio buttons: "Save these settings as a policy" (selected) and "Discard these settings after applying". Below these are two text input fields. The first is labeled "Policy name:" and contains the text "Password Policy", with a "max. 50 Characters" label to its right. The second is labeled "Description:" and contains the text "This password policy will use the secret password that I and only I know.", with a "max. 250 Characters" label to its right. At the bottom, there is a checked checkbox labeled "Save passwords with the policy".

6. Configure the **Select Document Components to Encrypt** panel:
 - **All contents:** Encrypts the document and its metadata (Acrobat 3 and later).
 - **All contents except metadata:** Allows for document storage/retrieval systems and search engines to have access to the document metadata. A document open or a permissions password will be required to access other document content.

Encrypting everything except the metadata allows continued access to Acrobat's Catalog feature. By leaving the metadata unencrypted, users can catalog and index the metadata of encrypted documents, thereby making that data searchable (compatible with Acrobat 6 and later).
 - **Only file attachments:** Allows full access to the document and encrypts only the file attachments. Permissions cannot be set on attachments. Using password security, a document open password is required for attachments (compatible Acrobat 7 and later).

Figure 67 Encryption configuration panel

The screenshot shows a panel titled "Select Document Components to Encrypt". It contains three radio buttons: "Encrypt all document contents" (selected), "Encrypt all document contents except metadata (Acrobat 6 and later compatible)", and "Encrypt only file attachments (Acrobat 7 and later compatible)". Below the radio buttons is a small text box that reads: "All contents of the document will be encrypted, and search engines will not be able to access the document's metadata."

7. Check or uncheck **Ask for recipients when applying this policy**.
 - If checked, you will not be asked in the next step to select the recipient certificates. Because the policy will not be associated with any recipients you will select them when you apply the policy.
 - If unchecked, you will be asked to select certificates now so that the document recipients will be identified in the policy.
8. Choose the encryption algorithm:

- **128-bit RC4:** Compatible with Acrobat 6.0 and later as well as other non-Adobe and Adobe PDF clients such as Ghostscript and Apple Preview that have not implemented AES. RC4 has a smaller file size by about 32 bytes per stream.
- **128-bit AES:** Compatible with Acrobat 7.0 and later. It is mandated for some U.S. government documents because it is more secure than RC4. AES adds up to 32 bytes per stream.
- **256-bit AES:** Compatible with Acrobat 9.0 and later. Provides the highest level of encryption.

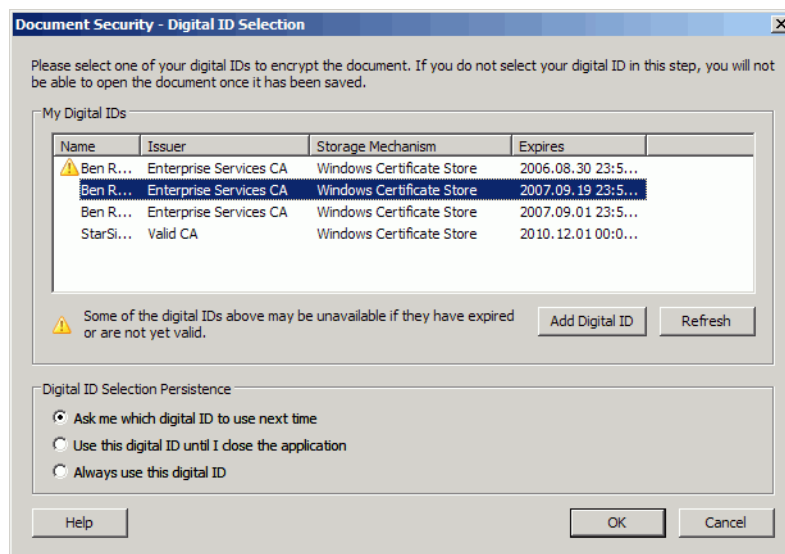
Note: The RC4 encryption algorithm is unavailable if your administrator has configured your application to operate in FIPS mode.

9. Choose **Next**. If you checked **Ask for recipients when applying this policy**, choose **Finish**. Otherwise, go to the next step.
10. *The Digital ID Selection dialog may not appear. If it does not appear, go to the “add document recipients to the recipient list” step:* The digital ID selection dialog only appears if you have no digital IDs suitable for encryption or more than one. If you only have one digital ID suitable for encryption, then this dialog does not appear (for example, one ID is set as the default for encryption in the Security Settings Console). If the dialog does appear, select your digital ID that you will use to access this document in the future.

Tip: While it is possible to apply certificate security without selecting your digital ID, doing so leaves you off of the recipient list and permanently locks you out of the document.

If the required digital ID does not appear in the list, choose **Add Digital ID** and follow the steps described in [“Registering a Digital ID for Use in Acrobat” on page 12](#).

Figure 68 Choosing a digital ID for certificate security



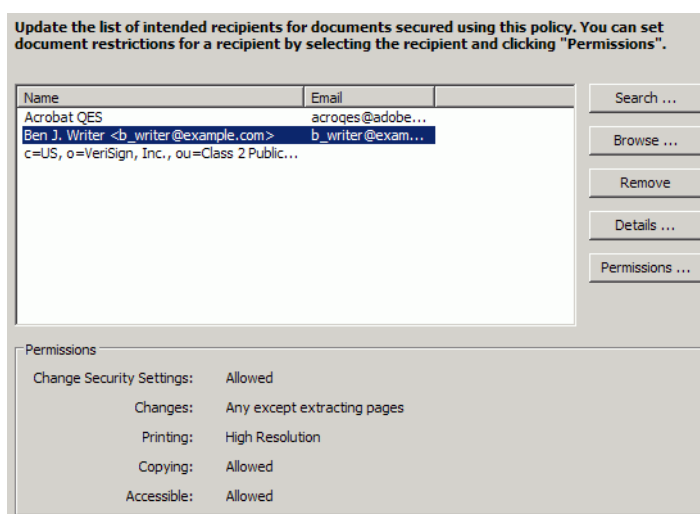
11. If you have more than one digital ID, choose the digital ID persistence level.
 - Ask me which digital ID to use next time
 - Use this digital ID until I close the application
 - Always use this digital ID

Note: This option will not appear for users with only one digital ID.

12. Choose **OK**.
13. Add document recipients to the recipient list. You will be encrypting the document with each recipient's public key so that they can decrypt it. Choose from the following:
 - **Search** lets you search preconfigured directories for certificates on remote servers as well as in your local Trusted Identity list. For details about searching for certificates, see ["Searching for Digital ID Certificates" on page 34](#). Highlight one or more found digital IDs and choose **OK**.
 - **Browse** lets you search your computer for certificate files stored locally. Highlight one or more found digital IDs and choose **OK**.

Tip: Business users may need to search their company LDAP directory server. For details, see ["Using Directory Servers to Add Trusted Identities" on page 40](#).

Figure 69 Adding recipients to a document with certificate security



14. If you want to specify document permissions, do the following. Otherwise, skip to [Step 16](#).
 1. Highlight one or more recipients. Different permissions can be set for different recipients. Select multiple recipients from the list by using the **Control** or **Shift** keys.
 2. Choose **Permissions**.
 3. When an alert appears stating that non-Adobe products may not respect these settings, choose **OK**.
 4. Check **Restrict printing and editing of the document and security settings**.

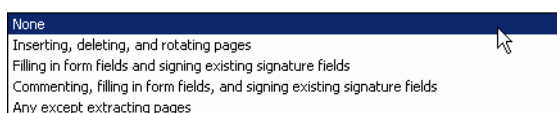
Caution: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions. Encryption and therefore document access would likely not be impaired, but Adobe cannot guarantee that individual permissions settings will remain function. Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**

- **None:** Prohibits printing.
- **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
- **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



- **None:** Prevents users from changing the document, including filling in signature and form fields.
 - **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
 - **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
 - **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
 - **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.
3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.
15. Choose **OK**.
16. Choose **Next**.
17. Choose **Finish**.

6.3.2 Creating Certificate Security for the Current Document

This workflow allows you to save the settings as a policy or discard them after they are applied. Use this method if you:

- Have access to the document recipient's digital IDs.
- Do not need to save the settings as a policy.

To apply certificate security to the current document:

1. Choose **Advanced > Security > Show Security Properties**.
2. Select **Certificate Security** from the **Security Method** drop-down list.
3. Choose one of the following:
 - **Save these settings as a policy:** Choosing to save the settings as a policy activates the **Policy name** and **Description** fields. Once the wizard is completed, the settings are saved as a policy and added to the policy list in the **Advanced > Security** menu and the Policy Manager. If you are creating a policy, enter a policy name and optional description.
 - **Discard these settings after applying:** Choosing to discard the settings deactivates the **Policy name** and **Description** fields and no settings are saved.
4. Configure the **Select Document Components to Encrypt** panel:

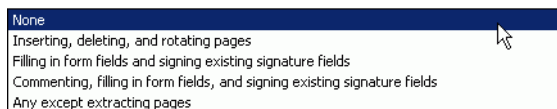
Note: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions. Encryption and therefore document access would likely not be impaired, but Adobe cannot guarantee that individual permissions settings will remain function. Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**

- **None:** Prohibits printing.
- **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
- **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



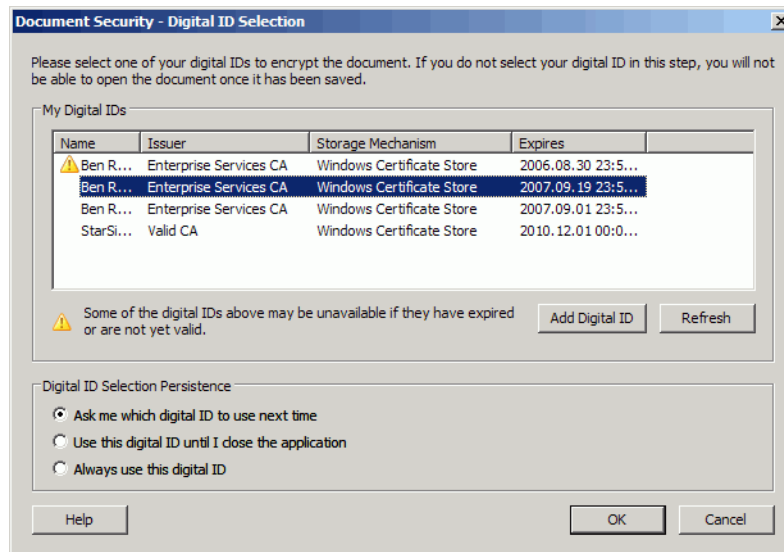
- **None:** Prevents users from changing the document, including filling in signature and form fields.
- **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
- **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
- **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
- **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.

3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.
5. Choose the encryption algorithm:
 - **128-bit RC4:** Compatible with Acrobat 6.0 and later as well as other non-Adobe and Adobe PDF clients such as Ghostscript and Apple Preview that have not implemented AES. RC4 has a smaller file size by about 32 bytes per stream.
 - **128-bit AES:** Compatible with Acrobat 7.0 and later. It is mandated for some U.S. government documents because it is more secure than RC4. AES has a bigger file size and adds up to 32 bytes per stream.
 - **256-bit AES:** Compatible with Acrobat 9.0 and later. Provides the highest level of encryption.
- Note:** The RC4 encryption algorithm is unavailable if your administrator has configured your application to operate in FIPS mode.
6. Choose **Next**.
7. *The Digital ID Selection dialog may not appear. If it does not appear, go to the "add document recipients to the recipient list" step:* The digital ID selection dialog only appears if you have no digital IDs suitable for encryption or more than one. If you only have one digital ID suitable for encryption, then this dialog does not appear (for example, one ID is set as the default for encryption in the Security Settings Console). If the dialog does appear, select your digital ID that you will use to access this document in the future.

Tip: While it is possible to apply certificate security without selecting your digital ID, doing so leaves you off of the recipient list and permanently locks you out of the document.

If the required digital ID does not appear in the list, choose **Add Digital ID** and follow the steps described in ["Registering a Digital ID for Use in Acrobat" on page 12](#).

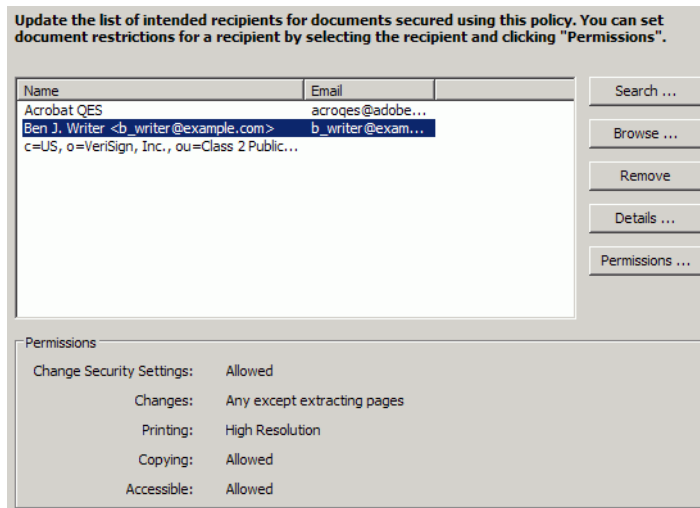
Figure 70 Choosing a digital ID for certificate security



8. If you have more than one digital ID, choose the digital ID persistence level.
 - Ask me which digital ID to use next time
 - Use this digital ID until I close the application
 - Always use this digital ID
- Note:** This option will not appear for users with only one digital ID.
9. Choose **OK**.
10. Add document recipients to the recipient list. You will be encrypting the document with each recipient's public key so that they can decrypt it. Choose from the following:
 - **Search** lets you search preconfigured directories for certificates on remote servers as well as in your local Trusted Identity list. For details about searching for certificates, see ["Searching for Digital ID Certificates" on page 34](#). Highlight one or more found digital IDs and choose **OK**.
 - **Browse** lets you search your computer for certificate files stored locally. Highlight one or more found digital IDs and choose **OK**.

Tip: Business users may need to search their company LDAP directory server. For details, see ["Using Directory Servers to Add Trusted Identities" on page 40](#).

Figure 71 Adding recipients to a document with certificate security



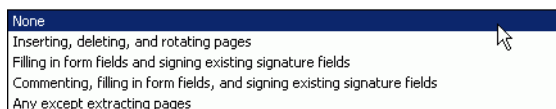
11. If you want to specify document permissions, do the following. Otherwise, skip to [Step 13](#).
 1. Highlight one or more recipients. Different permissions can be set for different recipients. Select multiple recipients from the list by using the **Control** or **Shift** keys.
 2. Choose **Permissions**.
 3. When an alert appears stating that non-Adobe products may not respect these settings, choose **OK**.
 4. Check **Restrict printing and editing of the document and security settings**.

Note: Adobe products enforce permissions restrictions. However, not all third-party products fully support and respect these permissions. Encryption and therefore document access would likely not be impaired, but Adobe cannot guarantee that individual permissions settings will remain function. Recipients using such third-party products might be able to bypass some of your restrictions.

Set the permissions as needed:

1. **Printing Allowed:**
 - **None:** Prohibits printing.
 - **Low Resolution:** Limits printing to 150-dpi resolution. Printing may be slower because each page is printed as a bitmapped image. This option is only available if a high encryption level (Acrobat 5 or Acrobat 6) is selected. Low resolution also inhibits users from printing a high quality document and using optical character recognition software to create a similar document with no security.
 - **High Resolution:** Allows printing at any resolution. For example, you can direct high-quality vector output to PostScript and other printers that support advanced high-quality printing features.

2. **Changes Allowed:** Limits page-level editing, commenting, and form field interaction.



- **None:** Prevents users from changing the document, including filling in signature and form fields.
 - **Inserting, deleting, and rotating pages:** Lets users insert, delete, rotate pages, and create bookmarks and thumbnail pages. This option is only available if a high encryption level is selected.
 - **Filling in form fields and signing existing signature fields:** Lets users fill in forms and add digital signatures. This option doesn't allow users to add comments or create form fields.
 - **Commenting, filling in form fields, and signing existing signature fields:** Lets users fill in forms and add digital signatures and comments.
 - **Any except extracting pages:** Lets users change the document using any method listed in the **Changes Allowed** menu, except remove pages.
3. **Enable copying of text, images, and other content:** Allows file contents (excluding comments) to be copied. It also makes the content available to assistive technology devices such as screen readers. It also lets utilities that need access to the contents of a PDF file, such as Acrobat Catalog, get to those contents. This option is only available if a high encryption level is selected.
 4. **Enable text access for screen reader devices for the visually impaired:** Only available if the option above is NOT checked. Lets visually impaired users read the document with screen readers. This option doesn't allow users to copy or extract the document's contents. This option is only available if a high encryption level is selected.
12. Choose **OK**.
 13. Choose **Next**.
 14. Choose **Finish**.

6.3.3 Applying a Certificate Security Policy

If your certificate security settings already exist in a policy, apply those settings with Policy Manager:

1. Choose **Advanced > Security > Manage Security Policies**.
2. Select a policy that uses certificate security.
3. Choose **Apply to Document**.
4. Save the document. New or changed settings do not appear in the user interface until the document is closed and reopened.

6.3.4 Applying a Certificate Security to a Group

Certificate security may be applied to more than one individual at a time. To apply security for multiple people, use the Search for Recipients dialog:

1. Configure certificate security as described in [“Creating Certificate Security Settings” on page 78](#). When you are prompted to add document recipients to the recipient list, choose **Search**.
2. Select the Search Directories:
 - Check **Search all directories** to search all the directories you have configured in the Security Settings Console.
 - Uncheck **Search all directories** to search a specific directory. If you are just searching for individuals in your Trusted Identities list:
 1. Choose *Trusted Identities* from the **Directories** drop-down list.
 2. Select a group from the **Groups** drop-down list. All members of this group will appear in the **Search Results** field.s.
3. Enter a search name or email address.
4. Highlight one or more of displayed individuals.
5. Choose **OK** and continue configuring the security settings.

Figure 72 Searching for group contacts

Search for recipients

Search Directories

☐ Search all directories

Directories: Trusted Identities

Groups: Group for my security policy

Search

Name:

Email:

Search

Search Results

Name	Email
Joe Smith	
Valid EE Certificate Test1	
nCipher Test v1.8	

OK Cancel

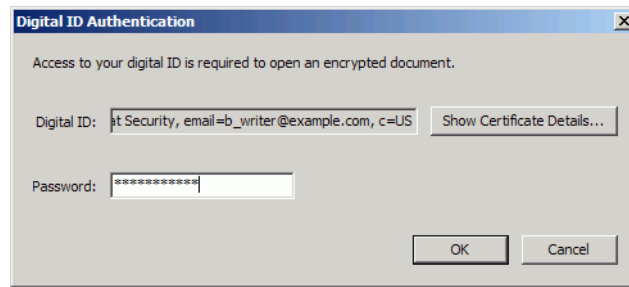
6.3.5 Opening a Certificate-Protected Document

Password protected documents require that a user know the document open password to open it. If a permissions password has been set, that password can also be used to open the document.

To open a password protected document:

1. Open the document.
2. Enter the password associated with the digital ID used to encrypt the document.
3. Choose **OK**.

Figure 73 Opening an encrypted document: With certificate security



Adobe LiveCycle Rights Management Server (ALCRMS) security is only available to users with access to an Adobe LiveCycle Rights Management Server.

Tip: This document provides a cursory overview of the ALCRMS features. For information on configuring your application to use an Adobe LiveCycle Rights Management Server, log in to the server and use the help system.

ALCRMS's server-based security system provides a Web-based user interface for dynamic document control through the use of policies stored on a server. The policies enable centralized document management and event auditing. The documents that use those policies can reside anywhere. ALCRMS policies not only enable reusing security settings, but they also have let the author expire and revoke documents irrespective of how many copies were created or distributed. You can also maintain accountability and audit who opens protected documents.

ALCRMS can be configured to run with LDAP, ADS, and other enterprise systems so that user lists can be leveraged from an organization's existing information.

Using server-based security policies includes the following steps:

1. **Application configuration:** A system administrator configures the machine or the end user can do it manually. Server settings can also be sent via an .acrobatsecurity or an FDF file thereby enabling the end user to automatically import the requisite settings from a secure file. The administrator manages accounts, sets up organizational policies, and maintains the server.
2. **Policy configuration:** Reviewing the list of preconfigured organizational policies or creating a new user policy.
3. **Apply the policy and publish the document:** You apply a policy to the document with Acrobat's Policy Manager which can be accessed via the security main menu or through the Document Properties dialog. The policy server generates a license and an encryption key. Acrobat embeds the license in the document and encrypts it using the encryption key. You distribute the document or tell others where to find it.
4. **Viewing a document that has a policy applied:** When users try to open the document, they must authenticate their identities. The document is decrypted and opens with whatever permissions are specified in the policy.
5. **Auditing events and modifying access:** You audit document and usage history by logging in to the ALCRMS. You can modify access rights and user policies.

7.1 Configuring Servers

In most cases if you have access to an ALRM server then you're administrator will set up the server for you. There are three ways to set up an ALRM server:

- ["Importing ALCRMS Settings from an FDF file" on page 91](#)

- [“Importing ALCRMS Settings from an FDF file” on page 91](#)
- [“Importing ALCRMS Settings from an FDF file” on page 91](#)

7.1.1 Importing ALCRMS Settings from an FDF file

Adobe LiveCycle Rights Management Server settings can be distributed via FDF files. Both users and administrators can import and export server settings in the same way as timestamp and directory server information is imported and exported. For details, see [“Importing Adobe LiveCycle Rights Management Server Settings” on page 135](#).

If you need to configure the server settings manually, refer to [“Configuring ALCRMS Settings Manually” on page 91](#).

7.1.2 Importing ALCRMS Settings with a Security Settings Import

In addition to using FDF files, an administrator may export the requisite security settings and provide you with a file to import. In this case, you will import any settings in the file according to the administrators instructions. For more information, see [“Enhanced Security” on page 95](#).

7.1.3 Configuring ALCRMS Settings Manually

Your server administrators will provide you with server connection details. Once these details are obtained, configure Acrobat to use the server.

To connect to a Adobe LiveCycle Rights Management Server:

1. Choose **Advanced > Security Settings**.
2. Select Adobe LiveCycle Rights Management Servers in the left-hand panel.
3. Choose **New**.
4. Enter the server settings:
 - **Name:** The server name.
 - **Server Name:** The server URL.
 - **Server Port:** The server port.
 - **Username:** The login username if required.
 - **Password:** The login password if required.
5. Choose **Connect to this Server**.
6. Choose **OK**.

Figure 74 ALCRMS Server Configuration

New Adobe LiveCycle Rights Management Server

Name: My company ALRM Server

Server Settings

Server Name: alarm.server.com Port: 443

☒ Remember password on this computer

User name: example

Password: *****

You will never be required to enter your password. Your password will be stored on this computer and protected by your Windows log in.

Connect to this server Cancel

7.1.4 Managing your ALCRMS Account

To manage your ALCRMS Account:

1. Choose **Advanced > Security > Adobe LiveCycle Rights Management > Manage My Account**.
2. If prompted, enter a username and password and choose **OK**.
3. Manage your account as described in the Adobe LiveCycle Rights Management Help documentation.

7.2 Working with Documents and ALCRMS Policies

7.2.1 Creating an ALCRMS Security Policy

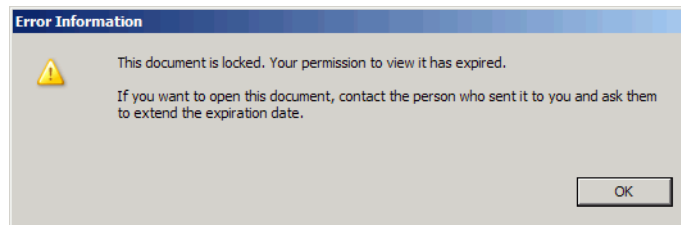
ALCRMS policies are created using the server's web interface. However, it is possible to launch that interface directly from Acrobat. Once the policy is created, return to Acrobat and choose **Finish** to add the policy to the policy list.

To create an ALCRMS user security policy:

1. Choose **Advanced > Security > Manage Security Policies**.
2. Choose **New**.
3. Select **Use Adobe LiveCycle Rights Management**.
4. Log in to the server.
5. Navigate to the Policies page.
6. Enter a policy name and optional description.

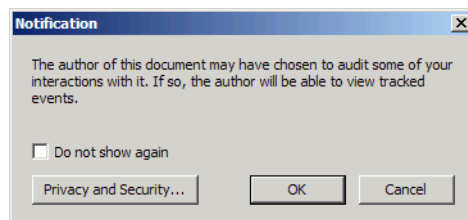
7. Configure the **Validity period** panel. A document's validity period determines how long it will be accessible. When a recipient opens a document with an expired validity period, an alert appears stating that the document is locked (Figure 75).

Figure 75 Validity period expired alert



8. Choose **Yes** or **No** to **Audit Documents**. Auditing tracks events such as printing, modifying, viewing, closing, form filling, and signing documents.

Figure 76 Audit alert for ALCRMS security



9. Set the **Auto-Offline lease period** to specify how long the document can be viewed offline before a user must synchronize with Adobe LiveCycle Rights Management Server.
10. Choose **Save**.
11. Exit the Web console and return to Acrobat.
12. Choose **Finish**.

7.2.2 Applying ALCRMS Security

Your ALCRMS policies will appear in Acrobat policy list.

To apply an ALCRMS policy:

1. Choose **Advanced > Security > Manage Security Policies**.
2. Highlight a policy.
3. Choose **Apply to Document**.

7.2.3 Refreshing the Security Policy List

To refresh the list of available ALCRMS policies:

1. Choose **Advanced > Security > Adobe LiveCycle Rights Management > Refresh Security Policies**.

2. If prompted, enter a username and password and choose **OK**.
An updated list of policies will appear in Policy Manager.

7.2.4 Synchronizing a Document for Offline Use

Synchronizing a document for offline use allows you to get the latest version so that you can access it when you are not connected to the network. To synchronize a document:

1. Choose **Advanced > Security > Adobe LiveCycle Rights Management > Synchronize for Offline**.
2. If prompted, enter a username and password and choose **OK**.

7.2.5 Revoking a Document

To revoke a document so that it cannot be viewed by anyone:

1. Choose **Advanced > Security > Adobe LiveCycle Rights Management > Revoke Document**.
2. If prompted, enter a username and password and choose **OK**.
3. Enter the revocation details as described in the Adobe LiveCycle Rights Management Help documentation.
4. Choose **OK**.

7.2.6 View a Document's Audit History

To view a document's audit history:

1. Open the document you would like to track.
2. Choose **Advanced > Security > Adobe LiveCycle Rights Management > View Audit History**.
3. If prompted, enter a username and password and choose **OK**.
4. View the audited events as described in the Adobe LiveCycle Rights Management Help documentation.

External Content and Document Security

Document access to internal and external content such as the Internet, attachments, and embedded multimedia represents a security risk. Users should configure their application so that it operates at an acceptable risk level. In enterprise settings, administrators should either preconfigure client installations or distribute instructions for setting up the application correctly.

For details about application settings that control how documents interact with elements outside of the document, see the following:

- [“Enhanced Security” on page 95](#)
- [“Controlling Multimedia” on page 98](#)
- [“Setting JavaScript Options” on page 101](#)
- [“Working with Attachments” on page 103](#)
- [“Controlling Access to Referenced Files and XObjects” on page 109](#)
- [“Internet URL Access” on page 109](#)

8.1 Enhanced Security

Like all other file formats, a PDF or an FDF file could contain a malicious script or perform some action that can damage a computer or steal data when it is run. Enhanced Security enables control of potentially risky behavior by allowing users to turn on enhanced security and either prevent dangerous actions altogether or else only permit them based on whether they reside in a privileged location. These behaviors include: silent printing; cross-domain access, external stream access, and internet access; and script and data injection. . For example, if a PDF has an embedded script, but it is from your company, it downloads.

Acrobat and Reader provide two ways to block potentially unsafe PDFs:

- A system administrator can add Internet domain names to the `crossdomain.xml` file on the server. Only files from locations listed in the `crossdomain.xml` file can be downloaded to individual computers.
- Individuals can identify specific files, folders, or URLs (hosts) as privileged locations in the Enhanced Security dialog box. A file that resides in a privileged location is then trusted. Any actions, such as loading data from the Internet or running a script are allowed. For example, Enhanced Security blocks FDFs from loading data from unknown websites. If you add the FDF to your list of privileged locations, Acrobat allows the data to be loaded.

At a high level, Enhanced Security includes the following:

- Preventing silent printing; cross-domain access, external stream access, and internet access; and script and data injection.
- Allowing dangerous behavior for only the specified privileged locations. These locations can be a file, directory, or host server.
- FDF behavior is fundamentally altered when this feature is on. For details, see *Distributing and Migrating Security Settings*.

- Enhanced Security interacts with the Trust Manager so that the least restrictive setting takes precedence. For example, if a document is signed with a certificate that's trusted for an action that Enhanced Security would normally prevent, that action will be allowed.
- External Content panel has been removed from the Preference's Trust Manager panel.

8.1.1 Enabling Enhanced Security

This feature is only available to Acrobat users. To turn on Enhanced Security and specify privileged locations, do the following:

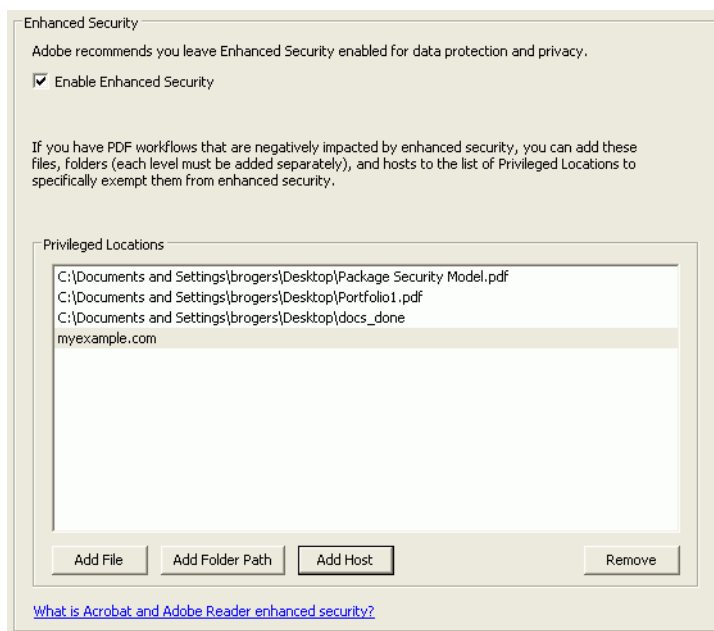
1. Choose **Edit > Preferences > Security (Enhanced)**.
2. Check the Enable Enhanced Security checkbox.
3. (Optional) Set a privileged location by selecting one or more of the following buttons:

Note: Privileged locations bypass Enhanced Security restrictions.

- **Add File:** Select this option if you only have one or two files from a location that you want to add. If you have a large number of files you know you can trust, it can be more practical to place them into one privileged folder.
- **Add Folder Path:** If you have a large number of files that you trust, specify an entire directory.
- **Add Host:** Enter the name of the root URL only. For example, enter www.adobe.com but not www.adobe.com/products. To only allow higher privileges for files accessed from secure connections, select the option for **Secure Connections Only (https:)**.

4. Choose **OK**.

Figure 77 Enhanced security: Configuration dialog



8.1.2 Changes in FDF Behavior

FDF files are data exchange files. Like acrobatsecurity files, they help you move certificate, server, and other data from one machine to another. This data transfer usually involves some mechanism such as data injection into a PDF form field, installing files, executing a script, and so on. These actions represent a potential security risk, and in some environments that risk may be unacceptable. Enhanced Security disables some FDF functionality unless those FDF files originate from a specifically privileged file, folder, or server. [Table 3](#) lists the high level rules defining FDF behavior.

Tip: If you need to configure your environment for enhanced security or need to troubleshoot FDF workflows that may not be working as expected, see [“Enhanced Security” on page 95](#).

Table 3 Rules for opening a PDF via FDF

Action	FDF location	PDF location	8.x behavior	9.x behavior
Opening a target PDF	local	local	PDF opens and no authentication required.	Same.
Opening a target PDF	local	http server	PDF opens	User authorization required unless trusted via enhanced security feature.
Opening a target PDF	https server	http server	PDF opens and no authentication required.	Same.
Opening a target PDF	https server	local	Blocked	Http hosted FDFs cannot open local files.
Data injection	n/a	n/a	Allowed	Allowed if: <ul style="list-style-type: none"> • Data returned via a form submit with url#FDF. • FDF has no /FDF key. • cross-domain policy permits it.
Data injection	server	browser	Allowed	Allowed if: <ul style="list-style-type: none"> • Link to PDF contains #FDF=url. • FDF has no /FDF key. • x-domain policy permits it.
Data injection	server	Application	Allowed	Allowed if: <ul style="list-style-type: none"> • PDF makes EFS POST/GET and FDF sends data in https response to same PDF. • x-domain policy permits it.
Data injection	Varied	Varied	Allowed	Authorization required if enhanced security is on and document is not set as a privileged location.
Script injection	Any	Any	Allowed	Injection is blocked unless if enhanced security is on and FDF is not in a privileged location.

Examples of Prevented Behavior

The following are examples of disallowed actions when Enhanced Security is on:

- If we're in the browser, and the URL to the PDF contains a #FDF=url, then the FDF data specified by that url may be injected into the open PDF if the FDF has no /F key and if the PDF may receive data from the FDF based on the cross domain policy.
- If we're in Acrobat/Reader standalone, and the FDF data comes back in the https response to an EFS POST/GET initiated by the PDF, then the FDF data may be injected into the open PDF if the PDF specified in the FDF is the PDF that made the EFS POST/GET and if the PDF may receive data from the FDF based on the crossdomain policy (i.e. * in crossdomain.xml).

Examples of Allowed Behavior

The following are examples of scenarios where FDF data injection does need a user-authorization dialog when Enhanced Security is on:

- You submit data from a PDF in the browser and the URL has #FDF at the end. The FDF that comes back has an /F key pointing to a different PDF which needs to get loaded (everything is happening in the browser). The FDF data gets injected into the second PDF.
- Same as above, except it all happens in the Acrobat rather than in the browser. In this case, the #FDF at the end of the URL is not needed.
- The "spontaneous FDF" case: In the browser, an unsolicited FDF arrives (via a link from an HTML page before and Acrobat is not running yet), and the FDF has an /F key for a PDF that it needs to open and populate.
- Opening a link of the form <http://A.com/file.pdf#FDF=http://B.com/getFDF>.

8.1.3 Interaction with Trust Manager

Enhanced Security interacts with the Trust Manager so that the least restrictive setting takes precedence. For example, if a document is signed with a certificate that's trusted for an action that Enhanced Security would normally prevent, that action will be allowed.

8.1.4 Make Privileged Folder Locations Recursive

You can extend privileged locations to be recursive by configuring the registry a reg setting. For details, refer to the *Security Administration Guide for Acrobat 9.0 and Adobe Reader 9.0*.

8.2 Controlling Multimedia

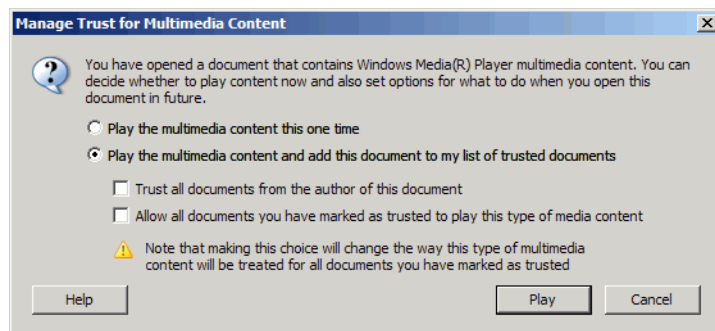
The Acrobat family of products have a notion of *trusted documents* and *other documents* (documents that have not been trusted). For the purposes of multimedia playback, every document will exist in one category or the other. For this reason there are two sets of trust options in the Multimedia Trust panel—one for documents that are trusted and one for documents that are not. In order to understand multimedia behavior then, you need to know whether or not a document is trusted so that you can determine which set of options for multimedia playback will be used.

There are two ways a document can become trusted:

- It can be signed with a valid certification signature, and you have trusted the signer's certificate for dynamic content.

- If your multimedia trust preferences result in a prompt asking whether you want to play multimedia, the Manage Trust for Multimedia Content dialog will offer various options that may allow you to trust the document.

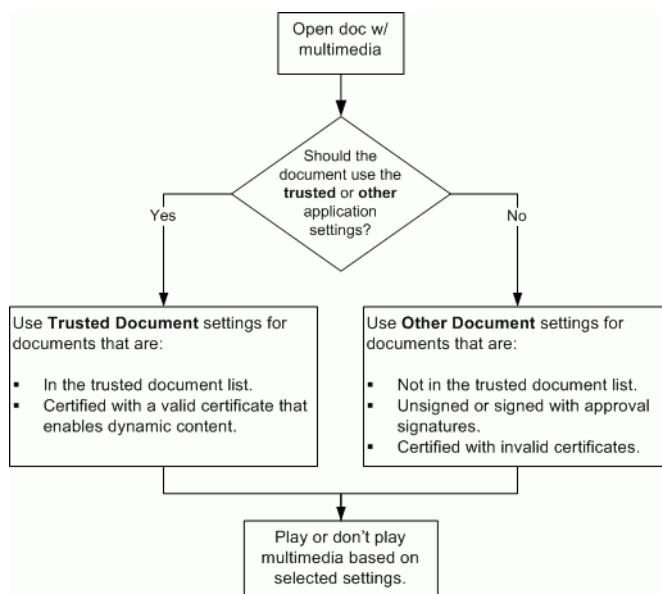
Figure 78 Manage Trust for Multimedia Content dialog



Once a document is trusted, it is added to the Trusted Document list and will always use the preferences set for trusted documents. You can clear this list by selecting **Clear** in the Multimedia Trust panel (Figure 80).

Caution: Membership on the trusted document list is permanent until the list is manually cleared. Therefore, once a document is on that list, changing the certificate trust level to disallow dynamic content will have not effect.

Figure 79 Multimedia behavior workflow



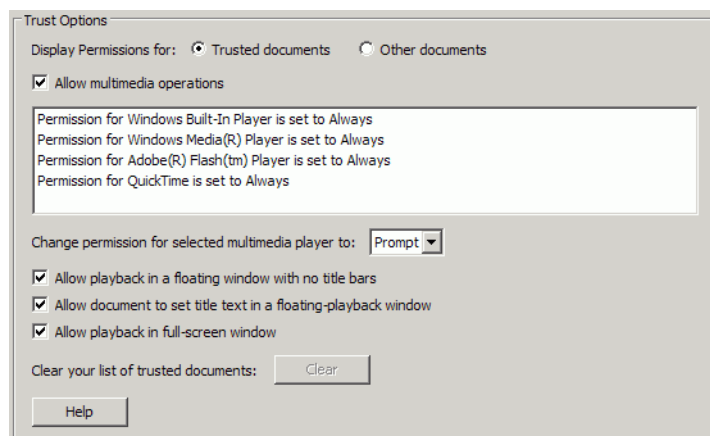
8.2.1 Configuring Multimedia Trust Preferences

Controlling multimedia behavior in documents begins with specifying preferences for *trusted documents* and *other documents*.

To configure multimedia preferences:

1. Open the Multimedia Trust Manager:
 - Acrobat and Adobe Reader (Windows): **Edit > Preferences > Multimedia Trust**
 - Acrobat and Adobe Reader (Macintosh): **(Application) > Preferences > Multimedia Trust**

Figure 80 Multimedia Trust (legacy)



2. From the **Display Permissions for** radio buttons, choose **Trusted documents** or **Non-trusted documents**. The Trust Manager displays the selected trust preferences (Figure 80).
 3. Configure the Trust Options panel:
 1. Check or uncheck **Allow multimedia operations**.
 2. Set multimedia player permissions as follows: Select the player in the list and select an option from the **Change permission for selected multimedia player to** drop-down list:
 - **Always**: The player is used without prompting.
 - **Never**: Prevents the player from being used.
 - **Prompt**: Prompts the user to enable the player when a media clip tries to use that player.
 3. Select one or more of the playback options:
 - **Allow playback in floating window with no title bars**: Opens the media in a separate window without a title bar.
 - **Allow document to set title text in a floating-playback window**: Opens the media in a separate window with a title bar.
 - **Allow playback in full-screen window**: Opens the media in full-screen mode.
- Note:** Membership on the trusted document list is permanent until the list is manually cleared. Choose **Clear** to remove all documents from that list.
4. Choose **OK**.

8.2.2 Controlling Multimedia in Certified Documents

Note: Multimedia and other dynamic content poses a security risk because it could potentially change the document's appearance or allow security holes in multimedia players to adversely impact

your system. Participants in certification workflows should consider the source of the document and the security of the workflow before enabling dynamic content.

Whether dynamic content executes in certified documents based on the Trusted Document or Other Document settings depends on two items under your control:

- You can configure a certified document to use the trusted document settings on a per-certificate basis or by using trust anchors. If a signer's certificate chains up to another certificate (a trust anchor) that allows multimedia, then multimedia will run in that certified document. For example, some enterprises may issue a MyCompany certificate that allows dynamic content. If all employee certificates use MyCompany as a trust anchor, then they can send and receive certified documents within the company that could contain working multimedia.
 - If the certificate trust settings allow dynamic content, the Multimedia Trust Manager's **Trusted documents** settings are used.
 - If the certificate trust settings do not allow dynamic content, the Trust Manager's **Other Documents** settings are used, UNLESS the document has already been added to the trusted documents list.
- You can configure a certified document to always use the trusted document settings regardless of certificate trust levels by adding it to the Trusted Documents list.

For details about setting certificate trust, see [“Setting Certificate Trust” on page 37](#).

Preventing Multimedia Playback in Certified Documents

To prevent dynamic content from playing in any certified document do one of the following:

- Never allow multimedia: Uncheck **Allow multimedia operations** in the Trust Options panel for both trusted and untrusted documents as described in [“Configuring Multimedia Trust Preferences” on page 99](#).
- Never allow multimedia for untrusted documents: Never trust any certificate for dynamic content and clear your trusted document list. Then configure your Other Document multimedia settings to **Never** or **Prompt**.

Note: There is no way to guarantee that multimedia won't play based on the trusted document list and certificate trust level alone. Application preferences always override these features.

8.3 Setting JavaScript Options

8.3.1 High Privilege JavaScript Defined

High privilege JavaScripts are Acrobat methods with security restrictions. These are marked by an “S” in the third column of the quick bar in the *JavaScript for Acrobat API Reference*. These methods can be executed only in a privileged context, which includes the console, batch, menu, and application initialization events. All other events (for example, page open and mouse-up events) are considered non-privileged.

The description of each security-restricted method indicates the events during which the method can be executed. Beginning with Acrobat 6.0, security-restricted methods can execute in a non-privileged context if the document is certified and the certifier's certificate is trusted for executing embedded JavaScript.

In Acrobat versions earlier than 7.0, menu events were considered privileged contexts. Beginning with Acrobat 7.0, execution of JavaScript through a menu event is no longer privileged. You can execute security-restricted methods through menu events in one of the following ways:

- By checking the item named **Enable menu items JavaScript execution privileges**.
- By executing a specific method through a trusted function (introduced in Acrobat 7.0). Trusted functions allow privileged code—code that normally requires a privileged context to execute—to execute in a non-privileged context. For details and examples, see `app.trustedFunction` in the *JavaScript for Acrobat API Reference*.

8.3.2 Javascript and Certified Documents

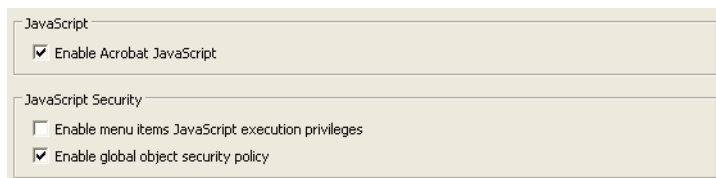
Whether JavaScript runs in certified documents depends on whether you have explicitly trusted the sender's digital ID certificate for that action. You can control script behavior on a per-certificate basis or by using trust anchors. If a signer's certificate chains up to another certificate (a trust anchor) that allows multimedia, then JavaScript will run in that document. For example, some enterprises may issue a MyCompany certificate that allows JavaScript. If all employee certificates use MyCompany as a trust anchor, then they can send and receive certified documents within the company that contain working JavaScript.

Tip: Because scripts could potentially change the document's appearance or allow attackers access to your system, participants in certified workflows should consider the source of the document and the security of the workflow before enabling this option.

To block or allow execution of all JavaScript from the tool bar:

1. Choose one of the following:
 - Acrobat and Adobe Reader (Windows): **Edit > Preferences > JavaScript**
 - Acrobat and Adobe Reader (Macintosh): **(Application) > Preferences > JavaScript**
2. Check or uncheck **Enable menu items JavaScript execution privileges**.
3. Check or uncheck **Enable global object security policy**.
4. Choose **OK**.
5. If you need to enable JavaScript in certified documents, set certificate trust for the certifying certificate as described in [“Setting Certificate Trust” on page 37](#).

Figure 81 JavaScript Security option



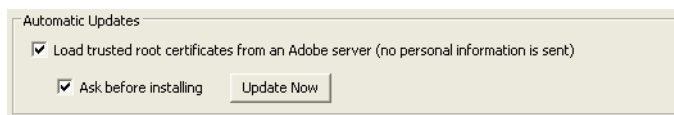
8.4 Adobe Trusted Identity Updates

In order to facilitate workflows that use certificates, Adobe occasionally sends new certificates configured as trust anchors to application users. These certificates allow you to validate signatures that are signed with certificates that chain up to those trusted certificates. In other words, you can validate those signatures without the extra steps of trusting each signer's certificate or manually configuring another trust anchor.

The application default is to check for updates and then ask if you would like to install them. However, you can modify this behavior as follows:

1. Choose one of the following:
 - Acrobat and Adobe Reader (Windows): **Edit > Preferences > Trust Manager**
 - Acrobat and Adobe Reader (Macintosh): **(Application) > Preferences > Trust Manager**
2. Configure the options as needed:
 - Turn the update off or on.
 - Turn **Ask before installing** option off or on.
 - Choose **Update Now** to get the latest certificates.
3. Choose **OK**.

Figure 82 Automatic updates



8.5 Working with Attachments

Before attempting to modify the application's default behavior, you should understand the default behavior. For details, see the following:

- ["Default Behavior: Black and White Lists" on page 103](#)
- ["Adding Files to the Black and White Lists" on page 107](#)
- ["Resetting the Black and White Lists" on page 108](#)
- ["Allowing Attachments to Launch Applications" on page 108](#)

Note: You cannot attach anything to a document in Adobe Reader.

8.5.1 Default Behavior: Black and White Lists

Exercise caution when attaching files to a PDF since some content may adversely impact document integrity or even the document's operating environment. To mitigate the risk inherent in attachments:

- Know what the content is and from where it originated.

- Be aware of dangerous file types and how the application manages those types. Adobe applications maintain [Black Lists and White Lists](#) which control application behavior.
- Prevent attachments from opening other files and launching applications. This is the default behavior. For details about changing this behavior, see [“Allowing Attachments to Launch Applications” on page 108](#).

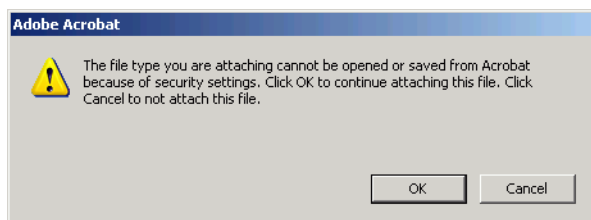
Black Lists and White Lists

The Acrobat family of products always allow you to open and save PDF and FDF file attachments. However, attachments represent a potential security risk because they can contain malicious content, open other dangerous files, or launch applications. Certainly file types such as .bin, .exe, .bat, and so on will be recognized as threats by most users.

The applications store a list of some of these good (white) and bad (black) file types in the registry ([Table 4](#)). Application behavior is controlled by the file type's membership in a list:

- **File types on the white list:** These can be attached and may be opened or saved if the file extension is associated with the requisite program.
- **File types on the black list:** These can be attached, but a warning dialog appears stating that they cannot be saved or opened from the application. No actions are available for these files.
- **File types not on any list:** These can be attached without a warning dialog. Trying to open or save them invokes a dialog which allows the user to perform the action just once or to add them to the good type (white) list or bad type (black) list.

Figure 83 Attachment: Dangerous type warning



Why Attach a File that's on the Black List?

You can attach file types that are on the black list because a document recipient may have a less restrictive black list than you (the sender). While recipient may be able to open the file, the attacker will not be able to execute or open it from within the application. Attempting to open a prohibited file type results in a warning that the action is not allowed ([Figure 84](#)).

Figure 84 Attachment: Cannot open warning

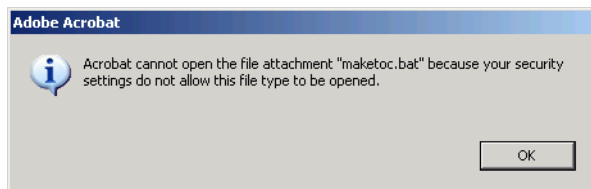


Table 4 Default prohibited file types

Extension	Description
.ade	Access Project Extension (Microsoft)
.adp	Access Project (Microsoft)
.app	Executable Application
.asp	Active Server Page
.bas	BASIC Source Code
.bat	Batch Processing
.bz	Bzip UNIX Compressed file
.bz2	Bzip 2 UNIX Compressed file (replaces BZ)
.cer	Internet Security Certificate file (MIME x-x509-ca-cert)
.chm	Compiled HTML Help
.class	Java Class file
.cmd	DOS CP/M Command file, Command file for Windows NT
.com	Command
.command	Mac OS Command Line executable
.cpl	Windows Control Panel Extension (Microsoft)
.crt	Certificate file
.csh	UNIX csh shell script
.exe	Executable file
.fxp	FoxPro Compiled Source (Microsoft)
.gz	Gzip Compressed Archive
.hex	Macintosh BinHex 2.0 file
.hlp	Windows Help file
.hqx	Macintosh BinHex 4 Compressed Archive
.hta	Hypertext Application
.inf	Information or Setup file
.ini	Initialization/Configuration file
.ins	IIS Internet Communications Settings (Microsoft)
.isp	IIS Internet Service Provider Settings (Microsoft)
.its	Internet Document Set, International Translation
.jar	Java Archive
.job	Windows Task Scheduler Task Object
.js	JavaScript Source Code
.jse	JScript Encoded Script file
.ksh	UNIX ksh shell script
.lnk	Windows Shortcut file
.lzh	Compressed archive (LH ARC)

Table 4 Default prohibited file types

Extension	Description
.mad	Access Module Shortcut (Microsoft)
.maf	Access (Microsoft)
.mag	Access Diagram Shortcut (Microsoft)
.mam	Access Macro Shortcut (Microsoft)
.maq	Access Query Shortcut (Microsoft)
.mar	Access Report Shortcut (Microsoft)
.mas	Access Stored Procedures (Microsoft)
.mat	Access Table Shortcut (Microsoft)
.mau	Media Attachment Unit
.mav	Access View Shortcut (Microsoft)
.maw	Access Data Access Page (Microsoft)
.mda	Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)
.mde	Access MDE Database file (Microsoft)
.mdt	Access Add-in Data (Microsoft)
.mdw	Access Workgroup Information (Microsoft)
.mdz	Access Wizard Template (Microsoft)
.msc	Microsoft Management Console Snap-in Control file (Microsoft)
.msi	Windows Installer file (Microsoft)
.msp	Windows Installer Patch
.mst	Windows SDK Setup Transform Script
.ocx	Microsoft Object Linking and Embedding (OLE) Control Extension
.ops	Office Profile Settings file
.pcd	Visual Test (Microsoft)
.pkg	Mac OS X Installer Package
.pif	Windows Program Information file (Microsoft)
.prf	Windows System file
.prg	Program file
.pst	MS Exchange Address Book file, Outlook Personal Folder file (Microsoft)
.rar	WinRAR Compressed Archive
.reg	Registration Information/Key for Windows 95/98, Registry Data file
.scf	Windows Explorer Command
.scr	Windows Screen Saver
.sct	Windows Script Component, Foxpro Screen (Microsoft)
.sea	Self-expanding archive (used by Stuffit for Mac files and possibly by others)
.shb	Windows Shortcut into a Document
.shs	Shell Scrap Object file

Table 4 Default prohibited file types

Extension	Description
.sit	Compressed archive of Mac files (Stuffit)
.tar	Tape Archive file
.tgz	UNIX Tar file Gzipped
.tmp	Temporary file or Folder
.url	Internet Location
.vb	VBScript file or Any VisualBasic Source
.vbe	VBScript Encoded Script file
.vbs	VBScript Script file, Visual Basic for Applications Script
.vsmacros	Visual Studio .NET Binary-based Macro Project (Microsoft)
.vss	Visio Stencil (Microsoft)
.vst	Visio Template (Microsoft)
.vsw	Visio Workspace file (Microsoft)
.webloc	Mac OS Finder Internet Location
.ws	Windows Script file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file
.zip	Compressed Archive file
.zlo	ZoneLabs ZoneAlarm Mailsafe Renamed .PIF file
.zoo	An early compressed file format

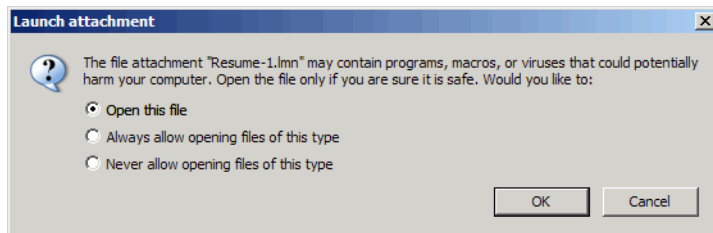
8.5.2 Adding Files to the Black and White Lists

Users can indirectly manage the registry list of which file types can be opened and saved. In other words, the list in [Table 4](#) can be extended one at a time as each attached file is opened. Administrators can modify the registry directly (refer to the *Acrobat Security Administration Guide*).

To add a file to a black or white list, attach the *new* file type to a document and then try to open it:

1. Choose **Document > Attach a File** and attach a file type not on the black or white list (e.g. `myfile.xyz`).
2. Open the file by highlighting it in the Attachments pane and choosing **Open**.
3. When the Launch Attachment dialog appears, choose one of the following ([Figure 85](#)):
 - **Open this file:** Opens the files without changing the registry list.
 - **Always allow opening files of this type:** Adds the file type to the white list and prevents future warnings.
 - **Never allow opening files of this type:** Adds the file type to the black list and does not open it.
4. Choose **OK**.

Figure 85 Launch Attachment dialog



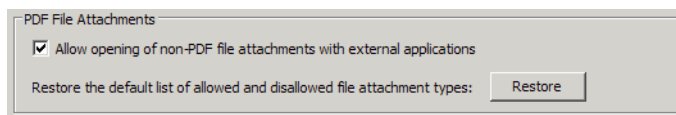
8.5.3 Resetting the Black and White Lists

Because the registry list could grow over time and users do not have direct access to the lists through the user interface, resetting the list to its original state may result in the highest level of security.

To reset the black and white lists:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Trust Manager in the Categories panel.
3. Choose **Restore** (Figure 86).

Figure 86 Attachment panel in Trust Manager



8.5.4 Allowing Attachments to Launch Applications

The Trust Manager enables users to control whether or not non-PDF attachments can open with other applications. By default, this option is enabled so that common file types such as .doc (not on the application's black list) can be easily opened in the appropriate application.

To set attachment preferences:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Trust Manager in the Categories panel.
3. Configure **Allow opening of non-PDF file attachments with external applications** (Figure 86):
 - **Checked:** Default. The application uses its stored black list to determine whether Acrobat should let the attachment invoke the launch an application action so the attachment can be opened.
 - **Unchecked:** Clicking or opening an attachment will never result in launching it's associated viewing application. Use this option if a higher level of security is needed.

8.6 Controlling Access to Referenced Files and XObjects

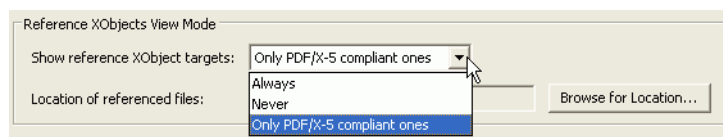
Your application can inform you when a PDF file is attempting to access external content identified as a stream object by flags as specified in the *PDF Reference*. For example, a URL might point to an image external to the document. Only PDF developers create PDF files with streams, so you may not need to enable access to external content.

Silently transmitting data represents a security risk since malicious content can be transferred whenever the application communicates with an external source. Therefore, you may want to disable this feature.

To configure external content access:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Page Display in the Categories panel.
3. Configure the Reference XObjects View Mode panel:
 - Set **Show reference XObject targets** to:
 - Always:
 - Never:
 - Only PDF/X-5 compliant ones:
4. Set the location of referenced files (if any).
5. Choose **OK**.

Figure 87 Resource access



8.7 Internet URL Access

Your application can inform you when a PDF file is attempting to connect to an Internet site. Opening a Web page represents a security risk because malicious content can be transferred whenever the application communicates with the Internet. In addition to visible links in a PDF document, form fields can contain hidden JavaScript calls that open a page in a browser or silently requests data from the Internet.

Tip: This feature interacts with the new Security (Enhanced) preference feature. URLs that are set as privileged locations will bypass enhanced security restrictions if enhanced security is on.

You can control Internet access via the Manage Internet Access dialog (Figure 89). Controls are provided for the following:

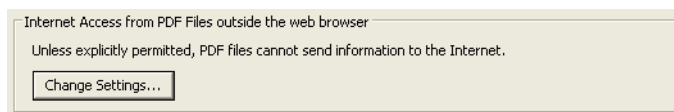
- [“Turning Internet Access Off and On” on page 110](#)
- [“Allowing and Blocking Specific Web Sites” on page 111](#)

8.7.1 Turning Internet Access Off and On

To block or allow all Web sites:

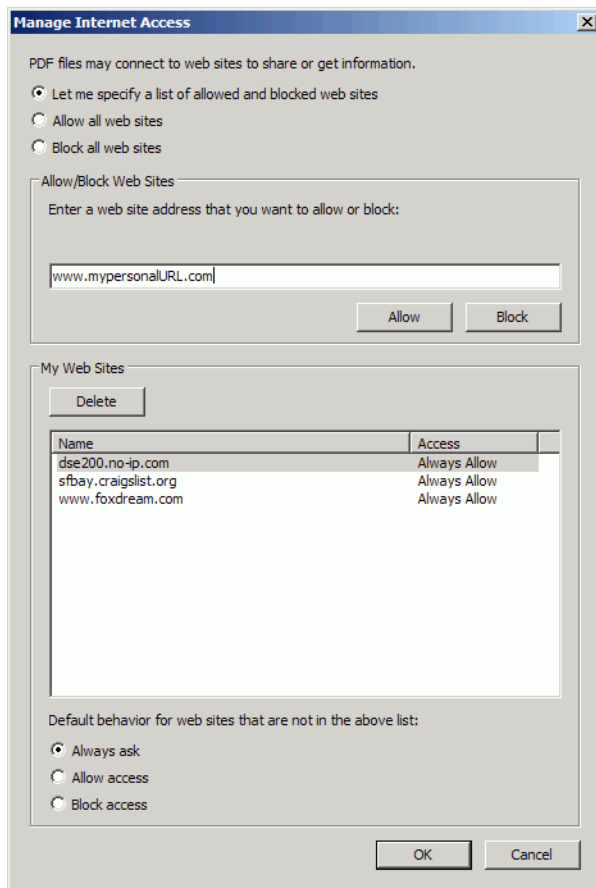
1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Trust Manager in the Categories panel.
3. Choose **Change Settings** in the **Internet Access...** panel.

Figure 88 Internet access panel



4. Choose **Allow all web sites** or **Block all web sites** (Figure 89).
5. Choose **OK**.

Figure 89 Manage Internet Access dialog



8.7.2 Allowing and Blocking Specific Web Sites

The Acrobat family of products maintain a white and black list of URLs called the *Trust List*. Users can specify whether or not URL access is allowed on a global or per-URL basis. For URLs that aren't explicitly trusted or blocked (they are not on the white or black list), a warning appears whenever a document tries to access the Internet (Figure 91). When you check **Remember my action for this site**, the site is added to your URL white or black list.

Figure 90 Blocked URL alert

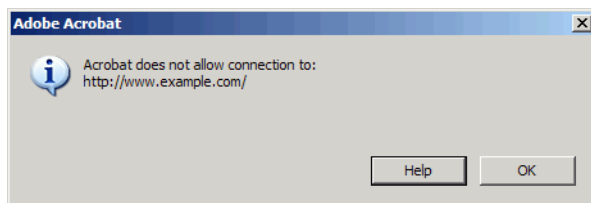
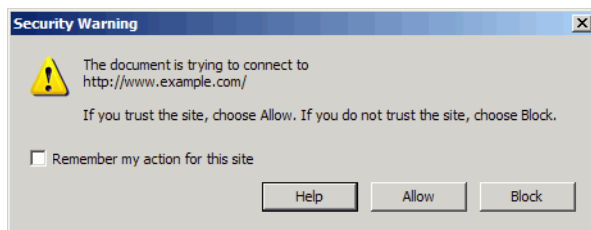


Figure 91 External connection warning



To configure Internet resource access on a per-URL basis, add specific Web sites to the black and white lists:

1. Choose **Edit > Preferences** (Windows) or **Acrobat (or Adobe Reader) > Preferences** (Macintosh).
2. Select Trust Manager in the Categories panel.
3. Choose **Change Settings** in the **Internet Access...** panel.
4. Choose **Let me specify a list of allowed and blocked web sites**.
5. Configure the black and white lists:
 - Add a URL to the URL fields and choose **Allow** or **Block**.
 - Choose a URL already in My Web Sites panel and choose **Delete**.
6. Select an option from the **Default behavior for web sites that are not in the above list**:
 - **Always ask**: You will be prompted to allow or block access for URLs not in the Trust List.
 - **Allow access**: URLs not in the Trust List will always be accessible.
 - **Block access**: URLs not in the Trust List will never be accessible.
7. Choose **OK**.

Note: This document was formerly an FDF user guide.

Security settings can be complex, and more importantly, they are often critical components of digital signature and document security workflows. For this reason, it's often necessary to migrate and even share settings across one or more machines. There are two methods available:

- **Security Setting Import and Export:** One of Acrobat 9.0's major new security features includes the ability to import and export security settings via .acrobatsecuritysettings files, thereby enabling easier version upgrades as well as configuration of multiple machines. The security settings import/export features offers several advantages over FDF files:
 - All settings can be encapsulated in an .acrobatsecuritysettings file whereas FDF could only transport one setting type and a time and could not encapsulate registry settings at all.
 - One file can be used instead of many files.
 - Trust can be assigned to imported on the fly, thereby simplifying workflows.
- **Sharing Settings & Certificates with FDF:** FDF files are useful for importing and exporting a specific type of setting such as trust anchors, timestamps, directory servers, and so on.

9.1 Security Setting Import and Export

Acrobat 9.0 introduces a new feature that helps users and organizations migrate existing security settings through version upgrades and across multiple machines. Unlike FDF files, the new .acrobatsecurity settings file supports the import and export of all settings including digital ID data, trust, server details, signing preferences, and so on. Settings can only be exported from Acrobat but settings can be imported by both Acrobat and Adobe Reader.

9.1.1 Exporting Security Settings to a File

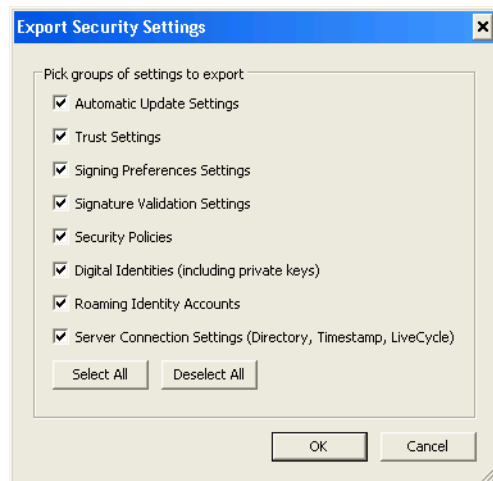
Settings can only be exported from Acrobat.

1. Choose **Advanced > Security > Export Security Settings**.
2. Check or uncheck the settings you would like to export.

Note: Whether you export or import settings via an FDF file or an .acrobatsecurity setting file, the actual settings are the same. Details about each individual setting are found in the FDF section as well as elsewhere in this document.

Choose **OK**.

Figure 92 Security settings: Export dialog



3. When the detailed Export Security Settings dialog appears, review the settings again.
4. If you would like to include or exclude any settings, highlight the setting and choose the **Include/Exclude Setting** button.
5. Choose **Export**.
6. Choose an encryption method. Encrypting the file ensures that the settings can't be viewed by anyone other than the intended recipients.

Figure 93 Security settings: Encryption method



7. Follow the dialog instructions which will vary with your choice of the document security method (password security or certificate security).
8. Choose **OK**.
9. You will be required to certify the file by signing it with a certification signature. When the certification workflow begins, choose **OK**.
10. Sign and save the file. If you don't know how to certify a file, refer to the *Digital Signatures User Guide*.

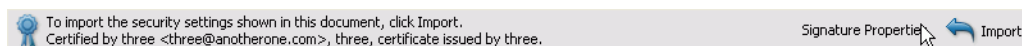
9.1.2 Importing Security Settings from a File

Settings can be imported by both Acrobat and Adobe Reader.

To import security settings:

1. Choose **Advanced > Security > Import Security Settings**.
2. Browse to an .acrobatsecuritysettings file.
3. Choose **Open**.
4. .acrobatsecuritysettings files must be certified and are therefore signed. You can verify the signer's identity by choosing the **Signature Properties** in the Document Message Bar and reviewing the signer's details.

Figure 94 Security settings: Document message bar

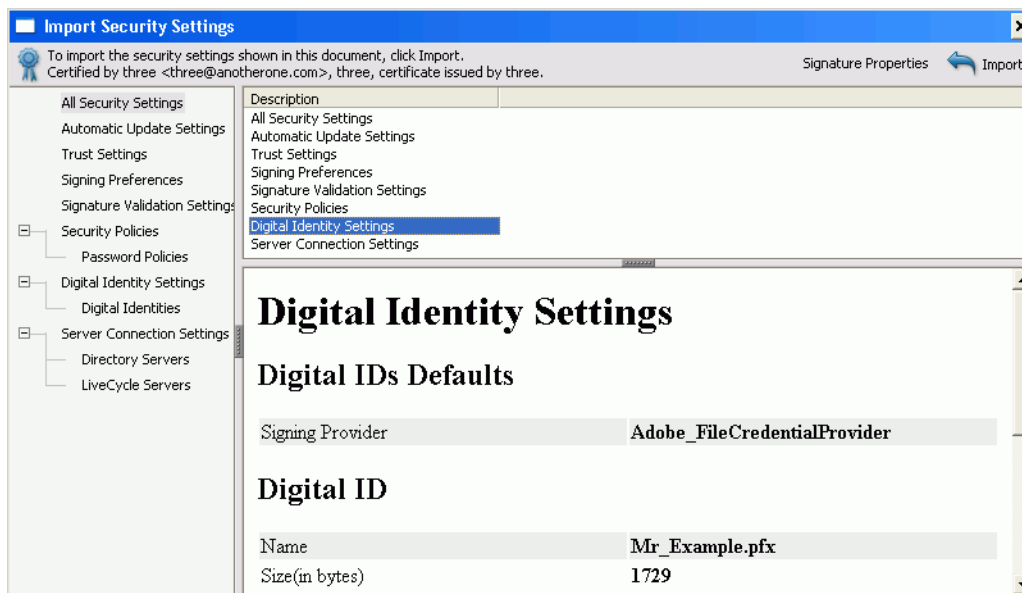


5. Review the settings carefully.

Note: Whether you export or import settings via an FDF file or an .acrobatsecurity setting file, the actual settings are the same. Details about each individual setting are found in the FDF section as well as elsewhere in this document.

Caution: The settings in the imported file will overwrite your current settings. Be sure to verify you're getting the correct settings and that they are coming from a trusted source.

Figure 95 Security settings: Import from a file panel



6. Choose **Import**.
7. After successfully importing the settings, a dialog appears asking if you'd like to open the Security Settings Console and log in to the digital IDs you just imported. Choose **Yes** or **No**.

Note: For security reasons, .acrobatsecuritysettings files do not care the digital ID passwords. Before you can use any of the digital IDs you just imported, you must log in to each ID. You can do it now or later.

Figure 96 Security setting import: Success dialog

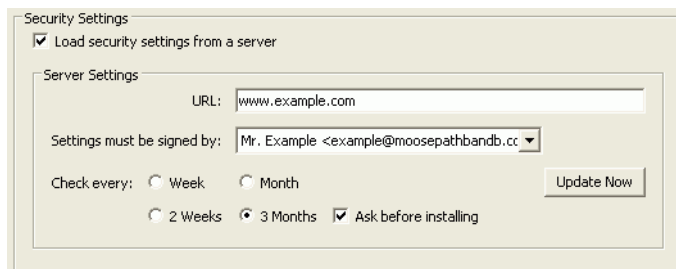


9.1.3 Importing Security Settings from a Server

If your organization distributes security settings periodically, you can set up Acrobat to regularly check for updates to these policies. Server-based security is set up by an administrator who provides the URL from which to get security updates. Once the application is configured, Acrobat will periodically poll the server (the default time is every three months) via http or https.

1. Choose **Edit > Preferences > Security**.
2. Check **Load security settings from a server**.
3. Enter the server address in the URL field.
4. Select a signing certificate if any. The .acrobatsecurity file will be signed with a certified signature. In order to install the file, you will need validate the signature.
5. Specify how often you want to check for security updates.
6. Select **Ask Before Installing** to be notified prior to installing new settings.
7. When the acrobatsecurity file opens, follow the instructions as described in [“Importing Security Settings from a File” on page 113](#).

Figure 97 Security setting preferences for server import



9.2 Sharing Settings & Certificates with FDF

Acrobat and Adobe Reader support the use of FDF files to exchange data between the Acrobat family of client and server products. FDF files use a .fdf extension, and like .pdf, it is registered by Adobe so that the

required application is used to open these files via a browser or file explorer. Acrobat provides the following FDF features:

- Import and export of digital ID certificates.
- Import and export of server settings for an Adobe LiveCycle Rights Management Server, LDAP directory servers, roaming credential servers, and timestamp servers.
- Creation by a user (through the application) or by a server programmatically.
- Sharing via networked directories or as email attachments.

Whether the file is located on a network or emailed, FDF file recipients simply double click on a FDF file to import its data automatically via the FDF import wizard, thereby eliminating the need for error prone, manual configuration.

FDF files provide individuals and businesses with many opportunities for streamlining workflows. For example:

- Alice wants to email her certificate to Bob and wants Bob to reply with his certificate. Alice chooses **Request Contact** in the Trusted Identity Manager. The workflow generates and emails an FDF file that can contain her certificate, a request for Bob's certificate, and Alice's return email address.
- Alice needs to encrypt documents for a number of people in her organization. An administrator sends her an FDF file that contains a large group of contacts. When Alice opens the FDF file, she is walked through the FDF Data Exchange UI wizard so that she can import these contacts into her Trusted Identities list.
- A server wants a copy of Bob's certificate so that the server can encrypt documents for Bob. The server generates an FDF file that contains a certificate request and a return URL address. When Bob downloads the FDF file from the server, he is walked through the FDF Data Exchange UI wizard where he can respond by allowing his certificate to be returned.
- A company needs to distribute its trusted certificate to customers so that they can verify that the company's documents are authentic. A server or administrator creates an FDF file that contains the trusted certificate and posts it on a Web server that hosts a Web page with a link to the file. When customers download the file, they are asked whether they wish to add this certificate to the Trusted Identity list and are given the ability to set the certificate's trust level.

For more information, refer to the following:

- [FDF Files and Security](#)
- [Importing Application Settings with FDF Files](#)
 - ["Responding to an Email Request for a Digital ID" on page 127](#)
 - ["Importing Someone's Certificate" on page 129](#)
 - ["Importing Multiple Certificates" on page 130](#)
 - ["Importing Timestamp Server Settings" on page 132](#)
 - ["Importing Directory Server Settings" on page 134](#)
 - ["Importing Adobe LiveCycle Rights Management Server Settings" on page 135](#)
 - ["Importing Roaming ID Account Settings" on page 136](#)
 - ["Importing a Trust Anchor and Setting Trust" on page 138](#)
- [Exporting Application Settings with FDF Files](#)
 - ["Distributing a Trust Anchor or Trust Root" on page 118](#)
 - ["Setting the Certificate Trust Level" on page 121](#)

- [“Exporting Your Certificate” on page 121](#)
- [“Emailing Your Certificate” on page 122](#)
- [“Saving Your Digital ID Certificate to a File” on page 123](#)
- [“Requesting a Certificate via Email” on page 124](#)
- [“Emailing Server Details” on page 125](#)
- [“Exporting Server Details” on page 126](#)

9.2.1 FDF Files and Security

FDF files are data exchange files. Like acrobatsecurity files, they help you move certificate, server, and other data from one machine to another. This data transfer usually involves some mechanism such as data injection into a PDF form field, installing files, executing a script, and so on. These actions represent a potential security risk, and in some environments that risk may be unacceptable. Acrobat therefore provides a new security feature that, when turned on, disables some FDF functionality unless those FDF files originate from a specifically privileged file, folder, or server.

The new feature is called Enhanced Security and may be enabled or disabled by choosing **Edit > Preferences > Security (Enhanced)**. [Table 5](#) lists the high level rules defining FDF behavior.

Tip: If you need to configure your environment for enhanced security or need to troubleshoot FDF workflows that may not be working as expected, see [“Enhanced Security” on page 95](#).

Table 5 Rules for opening a PDF via FDF

Action	FDF location	PDF location	8.x behavior	9.x behavior
Opening a target PDF	local	local	PDF opens and no authentication required.	Same.
Opening a target PDF	local	http server	PDF opens	User authorization required unless trusted via enhanced security feature.
Opening a target PDF	https server	http server	PDF opens and no authentication required.	Same.
Opening a target PDF	https server	local	Blocked	Http hosted FDFs cannot open local files.
Data injection	n/a	n/a	Allowed	Allowed if: <ul style="list-style-type: none"> • Data returned via a form submit with url#FDF. • FDF has no /FDF key. • cross-domain policy permits it.
Data injection	server	browser	Allowed	Allowed if: <ul style="list-style-type: none"> • Link to PDF contains #FDF=url. • FDF has no /FDF key. • x-domain policy permits it.

Table 5 Rules for opening a PDF via FDF

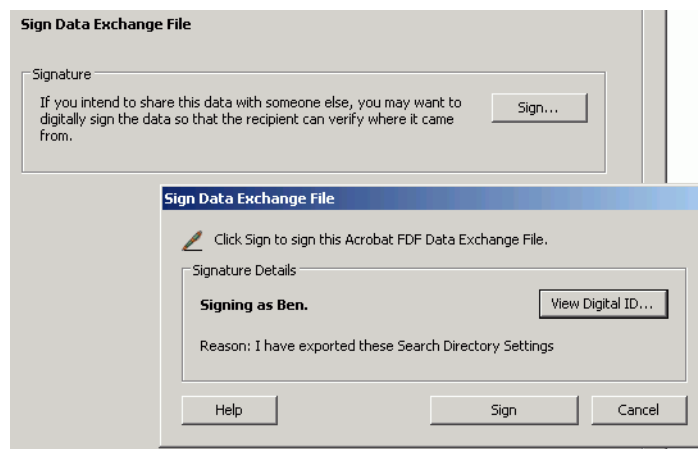
Action	FDF location	PDF location	8.x behavior	9.x behavior
Data injection	server	Application	Allowed	Allowed if: <ul style="list-style-type: none"> PDF makes EFS POST/GET and FDF sends data in https response to same PDF. x-domain policy permits it.
Data injection	Varied	Varied	Allowed	Authorization required if enhanced security is on and document is not set as a privileged location.
Script injection	Any	Any	Allowed	Injection is blocked unless if enhanced security is on and FDF is not in a privileged location.

9.2.2 Exporting Application Settings with FDF Files

FDF files can be created by administrators, end users, and even a server. It is a good idea to sign FDF files so that recipients of the file can establish a level of trust for the contents of the FDF file. For example, when an FDF file is signed, the **Accept the level of trust specified by the signer for all contacts in this file** checkbox becomes enabled, thereby allowing the importer to accept the level of trust you have specified.

Note: Recipients won't be able to validate your signature unless you have previously sent them your digital ID certificate or your certificate was issued by someone they already trust.

Figure 98 Signing an FDF file



9.2.2.1 Distributing a Trust Anchor or Trust Root

Distributing a trusted certificate from Acrobat involves wrapping one or more certificates in an FDF file and making it available to other users via email, a network directory, or a Web site. Recipients simply click on the file or a link to the file to open the Acrobat wizard which downloads and/or installs the certificate.

Certificate Chains and Trust Anchors /Roots

Certificates usually exist as part of a hierarchy or “chain” of certificates, and part or all of the chain can be wrapped in an FDF file. The bottom-most and end user certificate (yours) is called an “end entity” (EE) certificate. The top-most certificate, (the root) is typically belongs to a trusted Certificate Authority (CA).

Certificates in between the end entity and root certificates are sometimes called “intermediate certificates” (ICAs) and are issued by the CA or ICAs underneath the CA. Acrobat enables users to specify one or more of the certificates in a chain as trusted for specific operations. Thus, an EE certificate could have one or more trust anchors (trusted ICAs) that chain up to a the top-most CA certificate which is the primary trust anchor or “trusted root.”

A typical chain might include your certificate, your company’s ICA, and a root CA. Certificates inherit trust from certificates on the root end of the chain. For example, if the root certificate is trusted, then any certificates chaining to the that root will also be trusted. Some organizations have their own root CA or use an ICA certificate that is issued by an external CA and make these the trust anchors for their employees.

It is a common practice to trust certificates as high up in the chain as is reasonable since revocation checking starts at the chain bottom and continues until it reaches a trust anchor. Revocation checking occurs until reaching a certificate that is absolutely trusted by you or your organization. It also allows users to trust other certificates that chain up to the same root. The trust anchor is often an ICA for example, since if the root is issued by a company such as VeriSign, it might not be wise to make it a trust anchor as that tells Acrobat to trust the millions of certificates that chain up to VeriSign.

Distributing and installing ICA or CA trust anchors to a user or group of users allows them to:

- Distribute certified or signed documents to partners and customers.
- Help document recipients validate the signatures of document authors.

Exporting a Trust Anchor

When Acrobat exports a certificate, it automatically exports other selected certificates in that certificate’s chain and includes them in the FDF file.

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities**.
2. Choose **Certificates** in the **Display** drop-down list.

In addition to this method, you can also display the certificate from any signature or certificate security method workflow where a **Show Certificate** or **Certificate Details** button appears, such as the Signature Properties dialog.

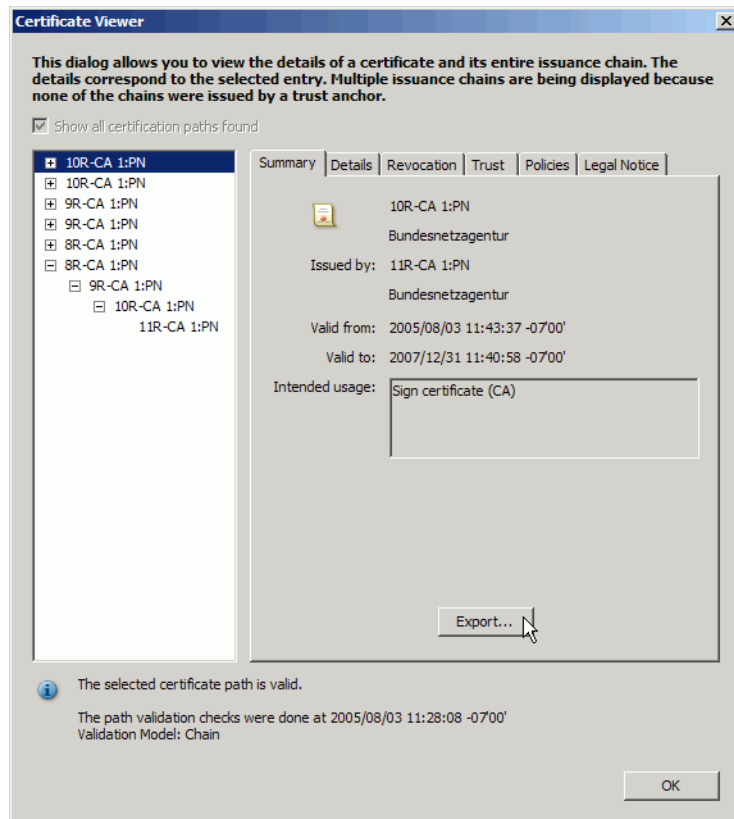
3. Select the certificate ([Figure 100](#)).

Note: In the unlikely event that you can sign the FDF file with a signature the recipient can validate (they will use a different certificate than the one you are exporting), set the certificate’s trust level before exporting it. For details, see [“Setting the Certificate Trust Level” on page 121](#)

Tip: You could just choose **Export** and bypass the following two steps. However, exporting the certificate from the Certificate Viewer allows you to see the entire certificate chain where you can select all or part of it.

4. Choose **Show Certificate**. The Certificate Viewer displays the certificate.
5. Select a certificate in the chain that appears in the left-hand window.

Figure 99 Selecting a certificate chain for export



6. Choose **Export**.
7. Choose one of the following:
 - **Email the data to someone:** Emailing the data automatically creates an FDF file that other Adobe product users can easily import.
 - **Save the exported data to a file:** Acrobat FDF Data Exchange. FDF is a format recognized by the Acrobat family of products.
8. Choose **Next**.
9. (Optional) If the Identity Information dialog appears, enter the your email address and any other information. If you have already configured your identity details, this screen may not appear. For details, see [“Setting Identity Information” on page 13](#).
10. **Do not sign** if the certificate you use to sign uses the same trust anchor or you are distributing. Since recipients do not have this certificate yet, they will not be able to validate your signature.

Note: Signing the FDF will only be useful if you have a digital ID that the recipient has already trusted (uses a trust anchor OTHER than the one you are currently distributing). The FDF file recipients must also already have that digital IDs certificate so that they can validate your signature without relying on the certificate you are currently sending. This workflow is uncommon, but it does allow recipients to automatically inherit your predefined trust settings for the certificate embedded in the file.
11. Choose **Next**.

12. Continue with the workflow until the trusted root is emailed or placed in a directory where your intended recipients can find it.

Providing Instructions to the Trusted Root Recipients

For details, see [“Importing a Trust Anchor and Setting Trust” on page 138](#).

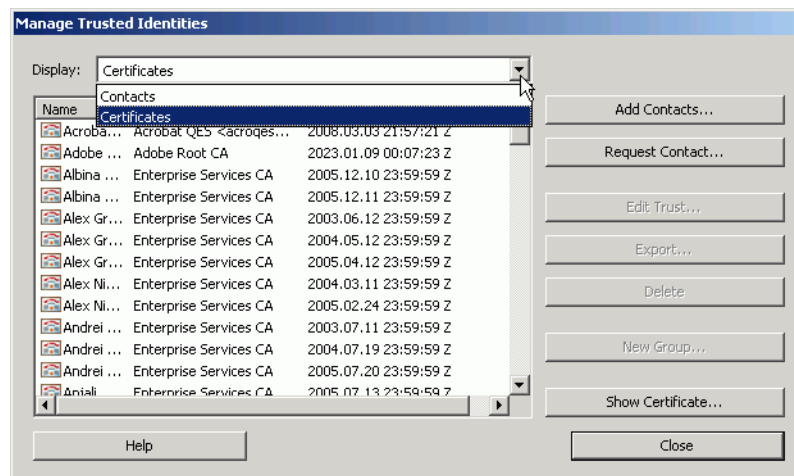
9.2.2.2 Setting the Certificate Trust Level

Note: This section is only relevant for trust anchor’s in FDF files that are signed with a trusted signature. This is an unlikely scenario, since the trust anchor distributor is probably using the same trust anchor that is being distributed and the recipient doesn’t have it yet. Most users will likely need to manually set the imported certificate’s trust level.

When distributing a trusted root in a signed file that the FDF recipient can validate, set the certificate trust level:

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities**.
2. Choose **Certificates** in the **Display** drop-down list.

Figure 100 Certificates in the Trusted Identities list



3. Highlight the needed certificate.
4. Choose **Edit Trust**.
5. Display the Trust tab.
6. Set the trust level as described in [“Importing a Trust Anchor and Setting Trust” on page 138](#).

9.2.2.3 Exporting Your Certificate

You can use FDF files to export your certificate so that others can import it into their list of trusted identities. This enables them to encrypt documents for you and validate your signature for documents that you digitally sign.

- Before users receiving your signed document can validate your signature, they must receive the your certificate or one above it in the trust chain.

- Before users can encrypt a document for you with certificate encryption, they must have access your certificate.

Certificates can be emailed or saved to a file for later use. There are two ways to export a certificate:

- To export a certificate from the list in the Security Settings Console, refer the following:
 - [“Emailing Your Certificate” on page 122](#)
 - [“Saving Your Digital ID Certificate to a File” on page 123](#)
- To export any certificate displayed in the Certificate Viewer, choose **Export** on the Summary tab.

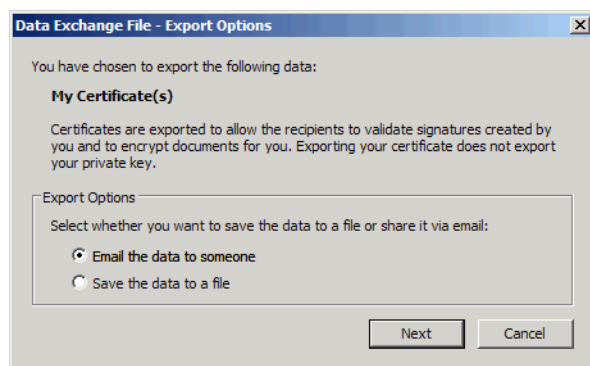
9.2.2.4 Emailing Your Certificate

If you do not have an email program on your machine, save the data to a file as described in [“Saving Your Digital ID Certificate to a File” on page 123](#) and then send the file as an attachment using your web-based email program.

To email a digital ID certificate:

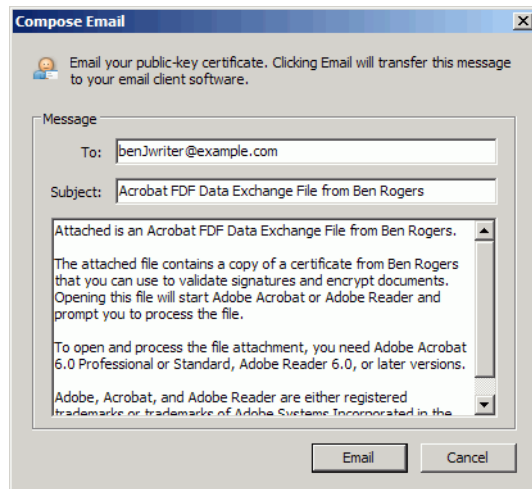
1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right. If you have more than one, choose the one that is appropriate for the usage context. For example, send your company-issued ID to those you do business with.
4. Choose **Export**.
5. Choose **Email the data to someone** ([Figure 101](#)).

Figure 101 Digital ID: ID export options



6. Choose **Next**.
7. Enter the recipient's email address and any other optional information.

Figure 102 Emailing your certificate



8. Choose **Email**.
9. When the email program opens, send the email.

9.2.2.5 Saving Your Digital ID Certificate to a File

To save a digital ID certificate to a file:

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right.
4. Choose **Export**.
5. Choose **Save the exported data to a file** (Figure 101).
6. Choose a file type:
 - **Acrobat FDF Data Exchange**: FDF files enable the easy exchange of data between any Acrobat family of products.
 - **Certificate Message Syntax - PKCS#7**: Save the file as a PKCS7 file. Use this format when the data will be imported into a non-Adobe store such as the Macintosh key store or Windows Certificate Store.
7. Choose **Next**.
8. Browse to a file location and choose **Save**.
9. Choose **Next**.
10. Review the data to export and choose **Finish**.

9.2.2.6 Requesting a Certificate via Email

When you request digital ID information from someone, the application automatically attaches to the email an FDF file containing your contact information and certificate.

To request a certificate from someone:

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities**.
2. Choose **Request Contact**.

Figure 103 Emailing a certificate request

3. Confirm or enter your identity so that the recipient can identify you. The identity panel is prepopulated if the information has been previously as described in [“Setting Identity Information” on page 13](#).
4. Choose **Include My Certificates** to allow other users to add your certificate to their list of trusted identities.
5. Choose whether to email the request or save it as a file.
6. Choose **Next**.
7. Select one or more digital IDs to export. Highlight contiguous IDs by holding down the Shift key. Highlight non-contiguous IDs by holding down the Control key.

Figure 104 Certificates: Selecting a digital ID for export

Name	Issuer	Expires
Ben	Ben	2010.08.10 23:08:02 Z
Fred Smith	Fred Smith	2004.12.08 11:20:18 Z
Joe Smith	Joe Smith	2005.11.12 18:36:23 Z
Johnny Rotten	Johnny Rotten	2005.02.08 20:36:56 Z
Rose ValidTestCA	CDS QE CA	2009.01.26 08:00:00 Z

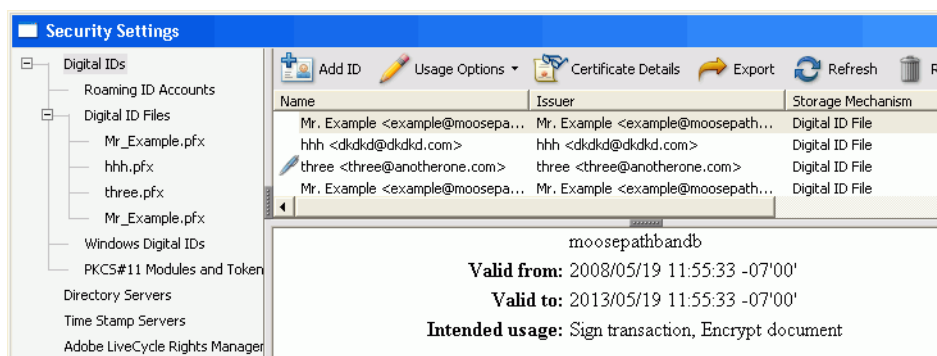
8. Choose **Select**.
9. The next step varies depending on whether you chose to email the ID:
 - **If you chose Email:** Enter the person's email address in the Compose Email dialog and choose **Email**. Send the email message when it appears in the launched email application with the certificate request attached.
 - **If you chose Save as file:** Choose a location for the certificate file Export Data As dialog. Choose **Save**, and then choose **OK**. Tell the intended recipient(s) where to find the file.

9.2.2.7 Emailing Server Details

Adobe LiveCycle Rights Management Server, directory server, roaming credential server, and timestamp server details can be exported to an FDF file for distribution to one or more people. Server information sent via an email resides in an attached FDF file. To send directory server details in an email:

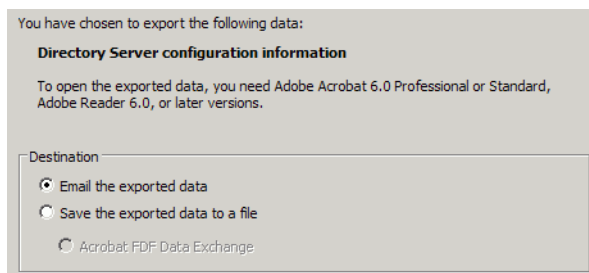
1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**.
2. Select a server category from the left-hand list.
3. Select a server from the right-hand panel.
4. Choose **Export**.

Figure 105 Security Settings menu items



5. Choose **Email the exported data** to email the FDF file.

Figure 106 Digital ID Directory servers: Export destination



6. Choose **Next**.

The Identity panel (Figure 107) will not appear if the information has been previously configured. For details, see “Setting Identity Information” on page 13.

Figure 107 Digital ID Directory servers: Sender’s identify

Your identity information is used with comments, reviews, and digital signatures. Information entered here is secure and not transmitted beyond this application without your knowledge. To modify this information in the future, simply go to the Identity panel in the preferences.

Identity

Login Name: brogers

Name: Neb Whifflesnit

Title: Senior Technical Writer

Organization Name: Acrobat

Organization Unit: CCC

Email Address: neb.whifflesnit@adobe.com

☒ Do not show again

7. Choose **Sign** and complete the signing workflow (Figure 117). Sign FDF files so that recipients of the file can easily trust the file and its contents.
8. Choose **Next**.
9. Enter the email information.

Figure 108 Digital ID Directory servers: Email details

You can specify the contents of the email message to which you will attach the exported data. This information will be sent to your email program.

Message

To: frontallabotomy@bottleinfrontofme.com

Subject: Acrobat FDF Data Exchange File from Neb Whifflesnit

Attached is an Acrobat FDF Data Exchange File from Neb Whifflesnit.

The attached file contains search directory configuration information that can be used to access search identity directories.

Opening this file will start Adobe Acrobat or Adobe Reader and prompt you to process the file.

To open and process the file attachment, you need Adobe Acrobat 6.0 Professional or Standard, Adobe Reader 6.0, or later versions.

10. Choose **Next**.
11. Review the export details.
12. Choose **Finish**.

9.2.2.8 Exporting Server Details

Adobe LiveCycle Rights Management Server, directory server, roaming ID, and timestamp server details can be exported to an FDF file for distribution to one or more people. Server information can be written to a file and saved to any location.

To save server details to a file:

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**.
2. Select a server category from the left-hand list.

Note: For roaming ID server settings, choose an account under **Roaming ID Accounts**.
3. Select a server from the right-hand panel.
4. Choose **Export**.
5. Choose **Save the exported data to a file** to save the data in an FDF file that can be shared (Figure 106).
6. Choose **Next**.
The Identity panel (Figure 107) will not appear if the information has been previously configured. For details, see “Setting Identity Information” on page 13.
7. Choose **Sign** and complete the signing workflow (Figure 117). Sign FDF files so that recipients of the file can easily trust the file and its contents.
8. Choose **Next**.
9. Browse to a location in which to save the file.
10. Choose a file name and choose **Save**.
11. Choose **Next**.
12. Review the export details.
13. Choose **Finish**.

9.2.3 Importing Application Settings with FDF Files

There are several ways to import Acrobat and Adobe Reader data from an FDF file:

- By choosing **File > Open**.
- Double clicking on an FDF file (.fdf)

Tip: The first two options above automatically invoke the simplest workflow.

- For digital ID information, importing it into the Trusted Identity Manager.
- For server settings, importing it with the Security Settings Console.

9.2.3.1 Responding to an Email Request for a Digital ID

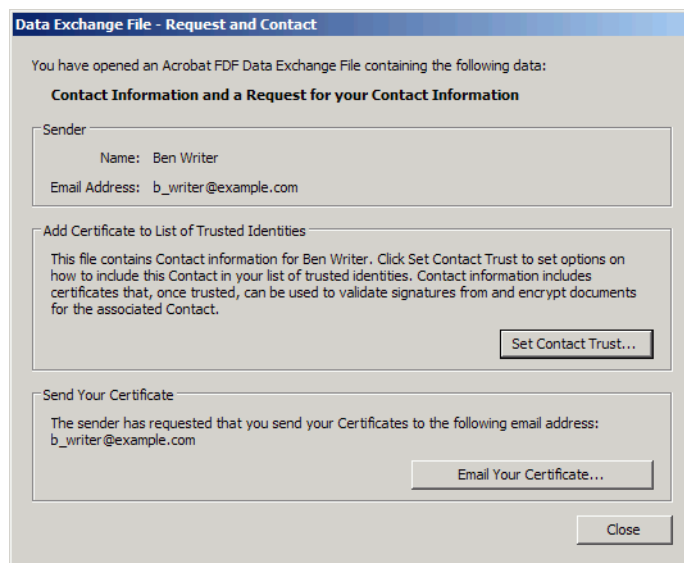
There may be times when someone else needs your digital ID to verify your signature or encrypt a file for you to decrypt (for example, when applying certificate security). To do either, they need access to the public part of your digital ID so that it can be added to their trusted identities list. One way someone can get your ID is to request it in an email.

To request your certificate, a user will simply choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities** and then choose **Request Contact**. Acrobat automatically attaches an FDF file with their public certificate to an email that requests your digital ID. The workflow is essentially a digital ID “trade” that allows two users to exchange digital IDs. You must have a digital ID before responding to the request.

To respond to an email digital ID request:

1. Double click the attached FDF file.
2. Choose **Email your Certificate**.

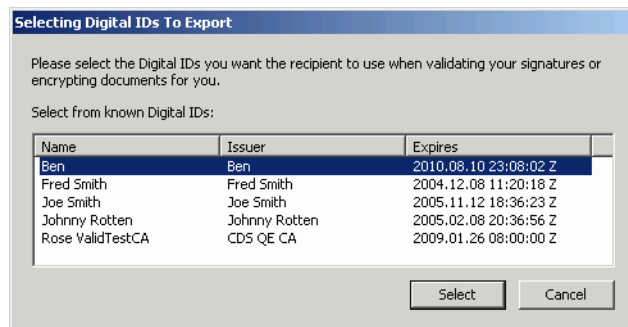
Figure 109 Emailing your certificate



3. Choose a digital ID from the list of existing digital IDs.

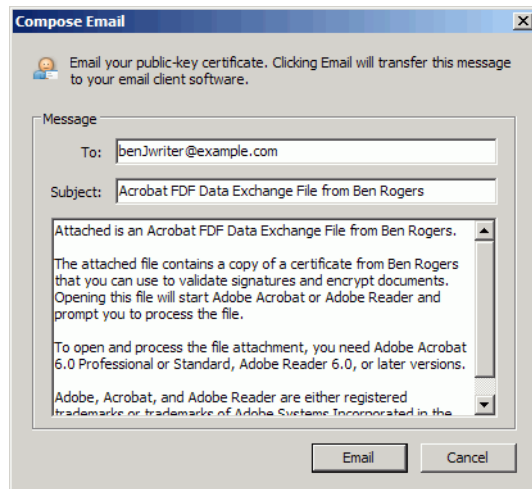
Note: If you do not have a digital ID or choose **Cancel**, an alert appears that says "A certificate was not selected for export." Exit the workflow and get a digital ID.

Figure 110 Selecting a digital ID



4. Choose **Select**.
5. Review the email details. You can edit the To, Subject, and Body fields (Figure 111).
6. Choose **Email**.
7. Send the email through your mail application.

Figure 111 Emailing your certificate



9.2.3.2 Importing Someone's Certificate

You can use an FDF file to import someone's certificate into your list of trusted identities. This enables you to validate their signature and encrypt documents with their public key so only that intended recipient can open it.

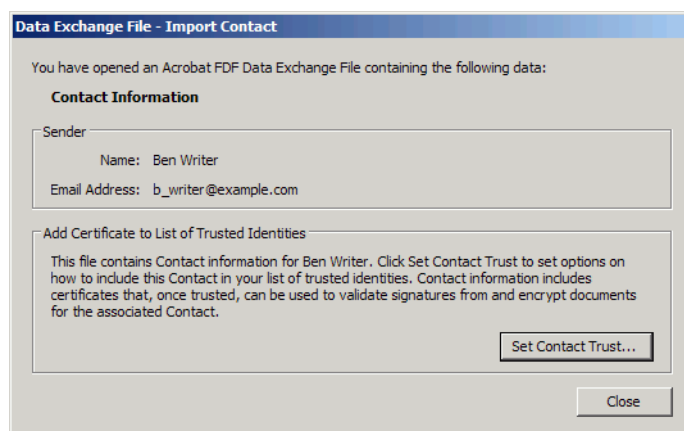
Tip: Importing this information ahead of time enables you to configure your trusted identities list before needing to validate a signature or encrypt a document for someone.

To add someone's certificate to your list of trusted identities:

1. Click on the FDF file or from Acrobat or Adobe Reader choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment or may reside in a networked directory.
2. Review the sender's information when the Import Contact dialog appears.

Note: If the file is signed, then the Import Contact dialog will also have a Signature panel as shown in [Figure 113](#).

Figure 112 Certificates: Contact Information



3. Choose **Set Contact Trust**.
4. When the Import Contact Settings dialog appears, configure the Trust and Policy Restrictions. For details, see [“Importing a Trust Anchor and Setting Trust” on page 138](#).
5. Choose **Certificate Details**.
6. Choose the Details tab.
7. In the Certificate data panel, scroll to MD5-digest and SHA-1 digest and note the fingerprint numbers.
8. Contact the certificate's originator and verify the fingerprints are correct.
9. Choose **OK**.
10. Choose **OK**.
11. Choose **Close**.

9.2.3.3 Importing Multiple Certificates

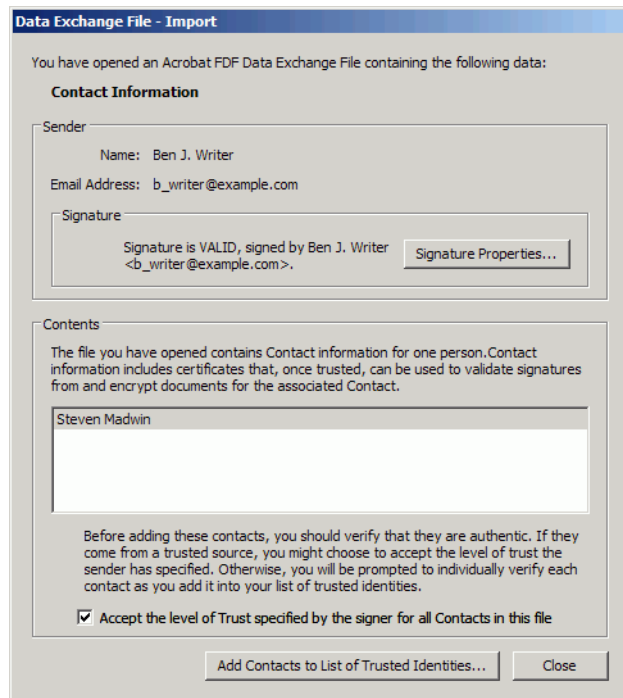
You can use an FDF file to import multiple certificates or a company-wide address book into your list of trusted identities. This enables you to encrypt a document using the public key of the intended recipient so that only they can open it.

Tip: Importing this information ahead of time enables you to configure your trusted identities list before needing to validate signature or encrypt a document to those identities. Administrators can create a company-wide address book and can export it to an FDF file for distribution throughout a company via a network or email.

To add multiple certificate to the trusted identities list all at once:

1. Click on the FDF file or from Acrobat or Adobe Reader choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment or may reside in a networked directory.

Figure 113 Importing multiple certificates

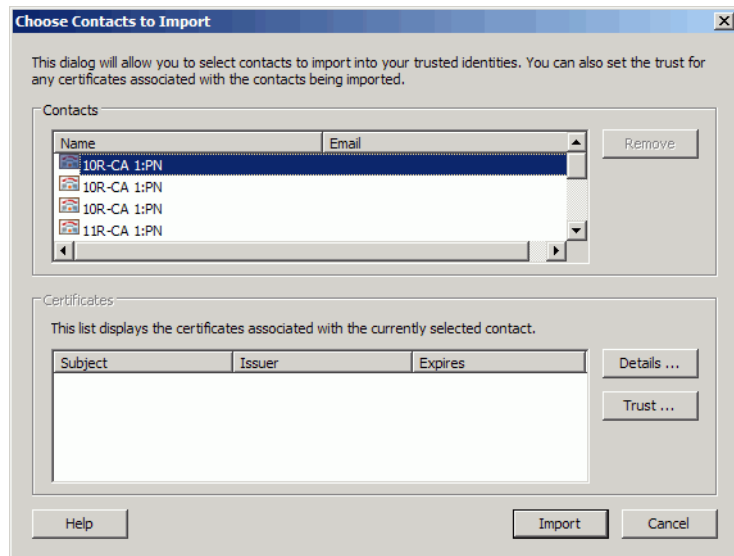


2. If the FDF file is signed, the signature can be validated, AND a trust level has been specified by the sender, check or uncheck **Accept the level of Trust specified by the signer for all Contacts in this file**.

Note: The box is disabled if both the above conditions are not met. If the FDF is signed by someone you trust but their signature has a status of UNKNOWN, you may be able to simply add the sender to your list of trusted identities. To do so, choose **Signature Properties > Show Certificate > select the Trust tab > and choose Add to Trusted Identities**.

- If the checkbox is selected, all contacts associated with this certificate will accept the level of trust that was set by the user that signed the FDF file.
 - If the checkbox is not selected, no trust level will be set for these certificates. The certificate cannot be used for many actions (such as providing a valid timestamp or encrypting) until a trust level is set as described in the user documentation.
3. Choose **Add Contacts to List of Trusted Identities**.
 4. If there are multiple contacts in the file, the Choose Contacts to Import dialog appears. Remove those that are not wanted and highlight the rest.
 5. Choose **Import**.
 6. Choose **OK** in the confirmation dialog.

Figure 114 Making a contact a trusted identity



9.2.3.4 Importing Timestamp Server Settings

In enterprise settings, servers do not usually have to be manually configured. Timestamp server administrators often export the server information to an FDF file which is emailed or made available on a network. Users can import (add) directory server settings through the Security Settings user interface or simply by double clicking on the FDF file containing the data.

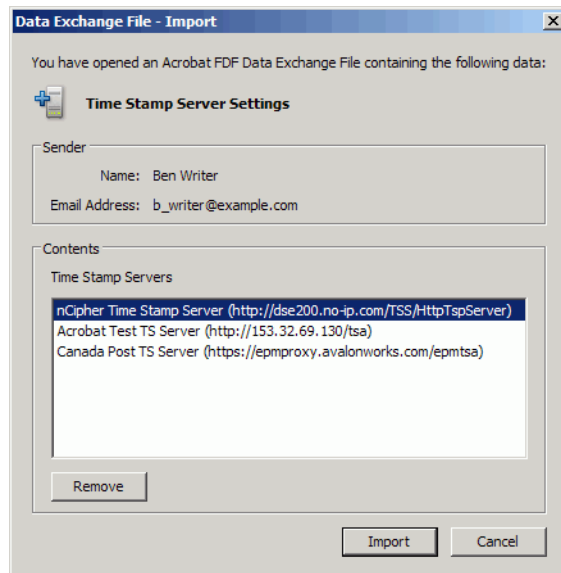
To import the server settings:

1. Locate the FDF file: find the file in an email or on the local file system and double click on it.

The FDF can also be imported through the Security Settings Console by choosing **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**, selecting **Time Stamp Servers** in the left-hand list, and choosing **Import**.

2. Review the sender's details. Note the following:
 - If the FDF is unsigned, no Signature panel appears in the import dialog.
 - If the FDF is signed, you can use the **Signature Properties** button to find out more information about the sender and the validity of the signature.

Figure 115 Timestamps: Importing server details from an FDF file



3. Review the timestamp server list. Note the following behavior:

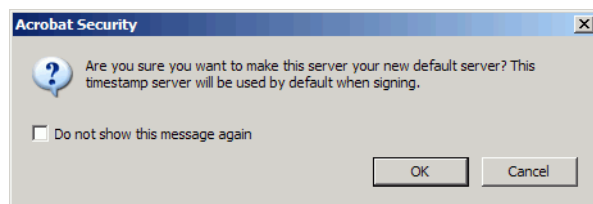
- If there is more than one server listed, all of the servers will be imported even though only one is highlighted.
- At import time, you will be asked if you want to make the highlighted server the default server.

Note: If there is more than one server and you do not want to import all of them, highlight those that should not be imported and select **Remove**.

4. Choose **Import**.

A dialog appears asking if the first (or only) server in the server list should be used as the default.

Figure 116 Timestamps: Importing a server



5. Choose **Yes** or **No**.

If **No** is selected, a default timestamp server must be set before timestamps can be used. To set a default timestamp server, Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings** > **Time Stamp Servers**, select a server, and choose **Set Default**.

6. After the import completes, choose **OK**.

The settings are automatically imported and should now appear in your list of Time Stamp Servers.

9.2.3.5 Importing Directory Server Settings

In enterprise environments, administrators often set up user machines or export the configuration details to an FDF file which is emailed or made available on a network. In the latter case, you can import the server settings through the Security Settings Console or simply by double clicking on the FDF file containing the data.

To add server settings from a file:

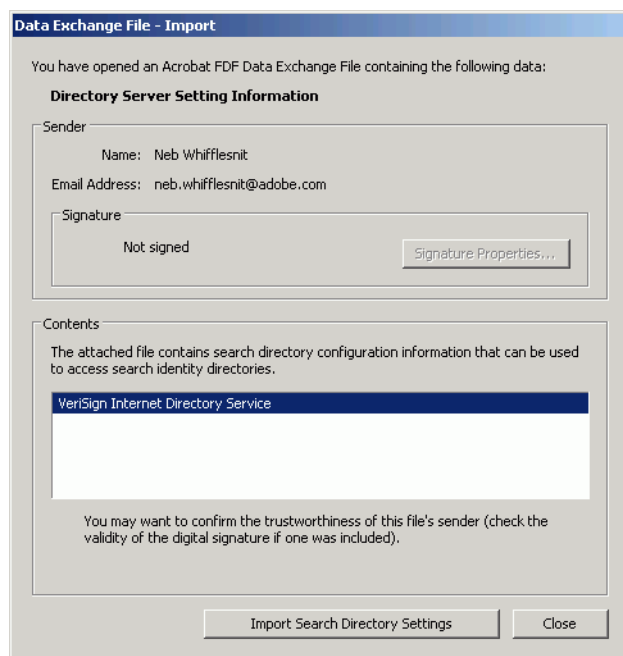
1. Locate the FDF file: find the file in an email or on the local file system and double click on it.

The FDF can also be imported through the Security Settings Console by choosing **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**, selecting **Directory Servers** in the left-hand list, and choosing **Import**.

2. Review the sender's details. Verify the signature properties if needed (Figure 117).

Note: If the FDF is unsigned, the Signature panel will display *Not signed* and the **Signature Properties** button will be disabled.

Figure 117 Digital ID Directory servers: Importing



3. Choose **Import Search Directory Settings**.

4. If a confirmation dialog appears, choose **OK**.

This dialog will not appear if **Do not show this message again** was previously selected.

5. Choose **Close**.

The settings are automatically imported and should now appear in the Directory Servers list in the Security Settings Console.

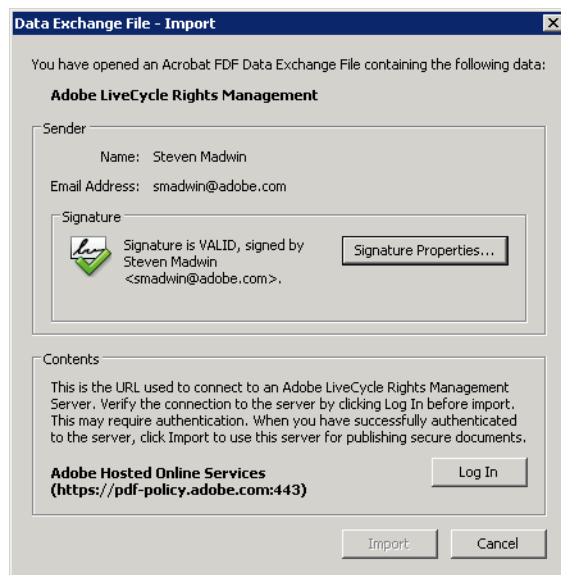
9.2.3.6 Importing Adobe LiveCycle Rights Management Server Settings

In enterprise settings, administrators often set up user machines or export the configuration details to an FDF file which is emailed or made available on a network. In the latter case, you can import the server settings through the Security Settings Console or simply by double clicking on the FDF file containing the data.

To import the server settings:

1. Locate the FDF file: find the file in an email or on the local file system and double click on it.
The FDF can also be imported through the Security Settings Console by choosing **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**, selecting **Adobe LiveCycle Rights Management Servers** in the left-hand list, and choosing **Import**.
2. Review the sender's details. Note the following:
 - If the FDF is unsigned, no Signature panel appears in the import dialog.
 - If the FDF is signed, you can use the **Signature Properties** button to find out more information about the sender and the validity of the signature.

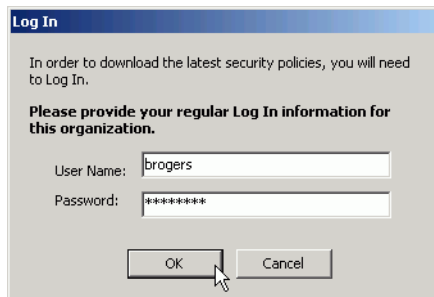
Figure 118 Importing Adobe LiveCycle Server settings



3. Choose **Log In**.

Tip: You must identify yourself to the server before you will be allowed to import these settings. The Import button does is disabled until you log in.

Figure 119 Logging in to an Adobe LiveCycle Rights Management Server



4. Choose **OK**.
5. Choose **Import**.
6. If you do not already have a default Adobe LiveCycle Rights Management Server, a dialog appears asking whether or not you want to make this your default server, choose **Yes** or **No**.
7. Choose **OK**.

The settings are automatically imported and should now appear in the Adobe LiveCycle Rights Management Servers list in the Security Settings Console.

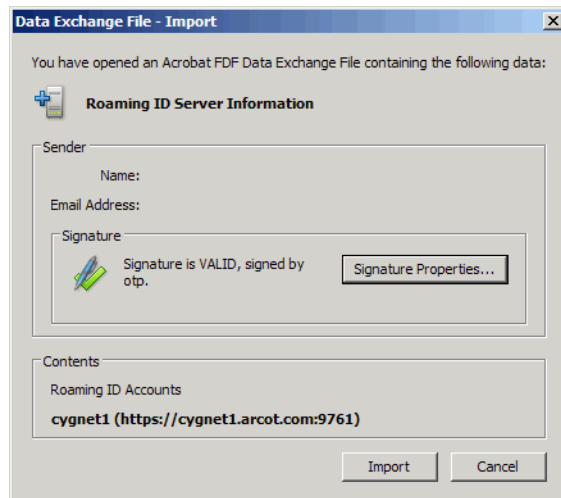
9.2.3.7 Importing Roaming ID Account Settings

In enterprise settings, administrators often set up user machines or export the configuration details to an FDF file which is emailed or made available on a network. In the latter case, you can import the server settings through the Security Settings Console or simply by double clicking on the FDF file containing the data.

To import the server settings:

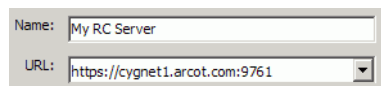
1. Locate the FDF file: find the file in an email or on the local file system and double click on it.
The FDF can also be imported through the Security Settings Console by choosing **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Security Settings**, selecting **Roaming ID Accounts** in the left-hand list, and choosing **Import**.
2. Review the sender's details. Note the following:
 - If the FDF is unsigned, no Signature panel appears in the import dialog.
 - If the FDF is signed, you can use the **Signature Properties** button to find out more information about the sender and the validity of the signature.

Figure 120 Importing roaming ID server settings



3. Choose **Import**.
4. Verify the roaming ID account name and server URL.

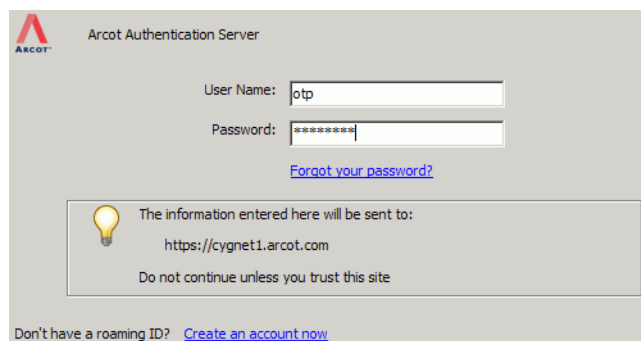
Figure 121 Roaming ID server name and URL



5. Choose **Next**.
6. Enter a user name and password.

Tip: The topmost portion of this dialog is customizable and server-dependant. The fields will remain the same, but the branding will vary.

Figure 122 Logging in to a roaming ID server



7. Choose **Next**.
8. After the confirmation that you have downloaded the roaming ID(s) appears, choose **Finish**.
The server settings and associated certificates are automatically imported and will now appear in the Roaming ID Accounts list in the Security Settings Console.

Figure 123 Downloaded roaming ID certificates

You have downloaded the following roaming ID(s):

Name	Issuer	Expires
otp	arcot	2007.08.25 23:17:33 Z

9.2.3.8 Importing a Trust Anchor and Setting Trust

Users occasionally need to import a trust anchor so that certificates that chain up to that anchor will also be trusted. This is particularly true in large organizations, and system administrators often distribute a trust anchor so that everyone within that organization can trust everyone else at the same level for signature workflows. For more information about trust anchors, see [“Distributing a Trust Anchor or Trust Root” on page 118](#).

To import a certificate that will be used as a trust anchor:

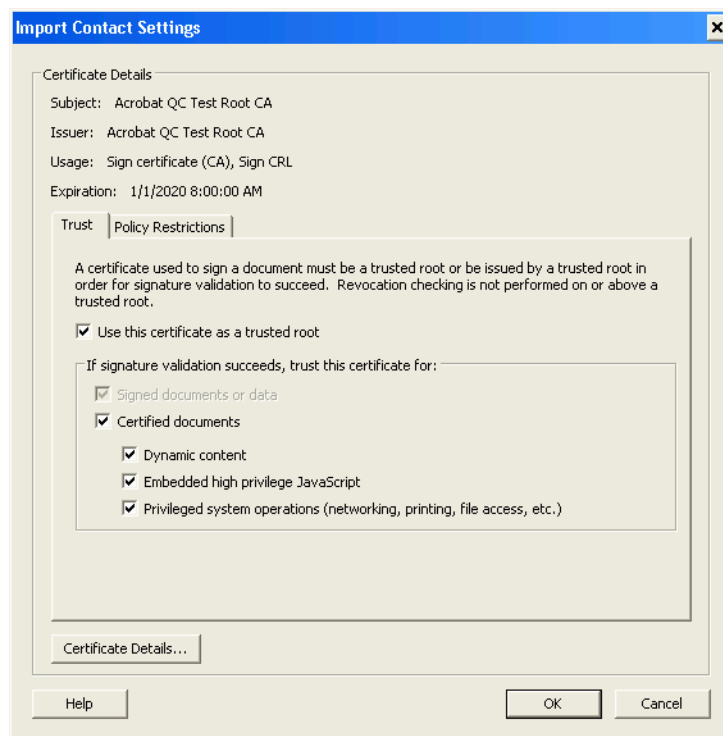
1. Open the FDF with one of the following methods:
 - Click on the FDF file. It may be an email attachment or a file on a network or your local system.
 - In Acrobat or Adobe Reader choose **File > Open**, browse to the FDF file, and choose **Open**.

Note: It is unlikely that you will receive a signed FDF file containing a trusted root. However, if you do, simply check **Accept the level of trust specified by the signer for all contacts in this file** and then choose **Close**. Skip the rest of the steps.

2. For unsigned FDF files containing a trusted root (the most likely case), choose **Set Contact Trust**.
 1. Do one of the following:
 - If you already have the certificate:
 1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) > **Manage Trusted Identities**.
 2. Choose **Certificates** in the **Display** drop down list.
 3. Select the certificate.
 4. Choose **Edit Trust**.
 - If the certificate is in a signature:
 1. Right click and choose **Signature Properties**.
 2. Choose **Show Certificate**.
 3. Select the Trust tab.
 4. Choose **Add to Trusted Identities**.
 - 2. On the Trust tab, select the trust options. In enterprise settings, an administrator should tell you which trust settings to use.

Note: During an import action, recipients of the distributed trust anchor may be able to inherit its trust settings. Once you've verified the sender, you usually want to accept these settings so you can use the certificate they way the sender intended.

Figure 124 Certificate trust settings



- **Use this certificate as a trusted root:** Makes the certificate a trust anchor. The net result is that any certificates which chain up to this one will also be trusted for signing. At least one certificate in the chain (and preferably only one) must be a trusted root (trust anchor) to validate signatures and timestamps.

Tip: There is no need to make end entity certificates trust anchors if they chain up to a trust anchor. It is best practice to trust the topmost certificate that is reasonable to trust because revocation checking occurs on every certificate in a chain until that anchor is reached. For example, in a large organization, it is likely you would want to trust your company's certificate. If that certificate was issued by VeriSign, you would not want to make VeriSign a trusted root unless you wanted to trust every certificate that chains up to VeriSign.

- **Signed documents or data:** Trusts the certificate for approval signatures.
- **Certified documents:** Trusts the certificate for certification signatures.
 - **Dynamic content:** Trusts multimedia and other dynamic content in certified documents. Selecting this option automatically adds documents that are certified with this certificate to the Trusted Documents list which is maintained by the Multimedia Trust Manager. For this reason, verify your application environment is configured correctly. For details, ["Controlling Multimedia" on page 98](#).
 - **Embedded high privilege JavaScript:** Trusts embedded scripts. Certificate settings do not override application-level settings, so even if JavaScript is enabled for a particular certificate, it may not execute unless the application's preferences allow it. This option requires that the

application environment be configured correctly. For details, see [“Setting JavaScript Options” on page 101](#).

- **Privileged system operations (networking, printing, file access, etc.):** Some operations represent a security risk more serious than others. Acrobat considers the following operations potential threats to a secure application operating environment: Internet connections, cross domain scripting, silent printing, external-object references, and FDF data injection. If this checkbox is checked, documents that are certified with this certificate will allow these actions.

Tip: This feature interacts with the Enhanced Security preferences which may be set by choosing **Edit > Preferences > Security (Enhanced)**. The application always takes the least restrictive setting when determining what is allowed. For example, if the trust level for this certificate does not allow privileged operations but the certified file resided in a privileged location, then these operations will be permitted.

3. If you need to specify a policy restriction, do so. Most users only need to set policy restrictions at the request of their administrator. [“Setting Certificate Policy Restrictions” on page 39](#).
4. Choose **OK** twice.
5. Choose **Close**.

10 Glossary of Security Terms

Table 5 Security Terms

.apf	See Adobe Profile Files.
.cer	Certificate format: A Microsoft format for digital IDs often stored in the Windows Certificate Store. These IDs can be used by Windows programs as well as the Acrobat product family.
.p12	See PKCS#12.
.p7b	See PKCS#7.
.p7c	See PKCS#7.
.pfx	See PKCS#12.
Adobe Profile Files	Adobe's legacy certificate format not used after Acrobat 5. The certificates are stored in .apf files. This format is not supported as of version 9.0.
ALCRMS	Adobe LiveCycle Rights Management Server.
approval signature	A signature used to indicate approval of, or consent on, the document terms.
CA	See certificate authority.
CDS	See Certified Document Services.
CDS digital ID	A digital ID issued by a certified document services provider.
CDS digital ID certificate	See CDS digital ID.
certificate authority (CA)	An entity that issues trusted roots.
certificates	That part of a digital ID that contains the public key. Certificates are shared among participants of signature and certificate security workflows in order to verify participant identities.
certification signature	A digital signature applied using an individual digital ID or organizational digital ID for the purpose of establishing the authenticity of a document and the integrity of a document's content, including its appearance and business logic.
certified document	A document to which a certification signature has been applied.
Certified Document Services (CDS)	A joint solution offered by Adobe and its security partners that can help recipients trust a PDF document. CDS can help provide assurance of the author's identity while also showing that the PDF document has not been modified. CDS is the only security solution that provides automatic validation of these attributes in Adobe Reader or Acrobat without also requiring additional software or configuration changes by the recipients.
certify or certifying	The act of applying a certification signature to a document using the Acrobat "Certify" feature. Certifying helps establish document authenticity as well as the integrity of its content, including its appearance and business logic.
CRL	See Certificate Revocation List.
Certificate Revocation List (CRL)	CRL is a method that public key infrastructures use to maintain access to cached or networked lists of unexpired but revoked certificates. The list specifies revoked certificates, the reasons for revocation (optional), and the certificate issue date and issuing entities. Each list contains a proposed date for the next release. Acrobat's CRL revocation checker adheres to RFC 3280 and NIST PKITS except for delta CRLs.
CSP	See Cryptographic Service Provider

Table 5 Security Terms

Cryptographic Service Provider	Application software that allows it to use MSCAPI to communicate with cryptographic module APIs such as PKCS#11 modules, PFX files, and so on
digital ID	An electronic representation of data based on the ITU-T X.509 v3 standard, associated with a person or entity. It is often stored in a password-protected file on a computer or network, a USB token, a smart card, or other security hardware device. It can be used for digital signatures and certificate security. "Digital ID" is sometimes used interchangeably with "certificate"; however, a certificate is only one part of a digital ID which also contains a private key and other data.
digital signature	An electronic signature that can be used to verify the identity of the signer through the use of public key infrastructure (PKI) technology. Signers need a digital ID and an application capable of creating a signature.
digitally sign	To apply a digital signature using a digital ID.
EE	See end entity certificate.
electronic signatures	A digital signature.
embedded JavaScript	JavaScript that exists within a document rather than that which is executed from the JavaScript Console or through a batch process.
embedded validation response	Information from the digital ID issuer that was used to apply the digital signature and that indicates if the digital ID was valid when the signature was applied. If the digital ID was valid and no one has tampered with the document, the signature will have a status of VALID. Once the digital ID expires or is cancelled (revoked), it won't be possible to determine if the signature was valid at the time it was applied unless there is an embedded revocation response.
end entity certificate (EE)	The bottom-most and end user certificate in a certificate chain is called an "end entity" (EE) certificate. It is the certificate that the holder uses for signing and others use for certificate encryption.
GeoTrust	An Adobe security partner that has joined the Adobe CDS program to provide CDS digital IDs to end users and organizations. As of Acrobat 6, Adobe Reader and Acrobat trust CDS digital IDs and are able to validate signatures that use GeoTrust digital IDs, without requiring any special application configuration.
ICA	See intermediate certificate authority.
individual digital ID	A digital ID issued to an individual to digitally sign as them self (e.g. John Smith) as opposed to an organization or other non-human entity.
intermediate certificate authority (ICA)	Certificates in between the end entity and root certificates are sometimes called "intermediate certificates" (ICAs) and are issued by the CA or ICAs underneath the CA.
MSCAPI	Windows Microsoft Crypto API (MSCAPI) is the API that the application uses to access cryptographic service providers such as PFX files and PKCS#11 files. MSCAPI is also used by the application anytime it uses a Windows security feature.
OCSP	See Online Certificate Status Protocol.
Online Certificate Status Protocol (OCSP)	OCSP defines a protocol for determining the revocation status of a digital certificate without requiring a CRL. Unlike CRL, OCSP obviates the need to frequently download updates to keep certification status lists current. Acrobat's OCSP revocation checker adheres to RFC 2560.
organization digital ID, desktop	A digital ID issued to an organization or non-human entity (for example, the Adobe Public Relations Department). It can be used by an authorized employee to perform signing operations, at the desktop, on behalf of the company.
organization digital ID, server	A digital ID issued on behalf of an organization or non-human entity (e.g. Adobe Public Relations Department, Cisco Corporation, etc.) for performing server-based, automated signing operations.
PKCS#11 device	External hardware such as a smart card reader or token. It is driven by a module (a software driver such as a .dll file on Windows).
PKCS#11 digital ID	An ID on a PKCS# device. A device may contain one or more IDs.
PKCS#11 format	Cryptographic Token Interface Standard: An encryption format used by smart cards, tokens, and other PKCS#11-compatible devices. The ID is stored on the device rather than on the user's computer.

Table 5 Security Terms

PKCS#11 module	The software module that drives a PKCS#11 device.
PKCS#11 token	See PKCS#11 device.
PKCS#12	Personal Information Exchange Syntax Standard: Specifies a portable, password protected, and encrypted format for storing or transporting certificates. The certificates are stored in .pfx (Windows) and .p12 (Macintosh) files. Unlike other formats, the file may contain private keys.
PKCS#7	Certificate Message Syntax (CMS): Files with .p7b and .p7c extensions are registered by the Windows OS. If you double click on a .p7c file it will be viewed by a Windows application.
Policy Server	As of Acrobat 9, Adobe Policy Server is renamed to Adobe LiveCycle Rights Management Server
privileged context	A context in which you have the right to do something that's normally restricted. Such a right (or privilege) could be granted by executing a method in a specific way (through the console or batch process), by some PDF property, or because the document was signed by someone you trust. For example, trusting a document certifier's certificate for executing JavaScript creates a privileged context which enables the JavaScript to run where it otherwise would not.
qualified certificates	A qualified certificate that conforms to the RFC 3739 specification. It contains a qc statement that simply states that it is a qualified certificate. These types of certificates meet the requirements of the German digital signature law, and most qualified certificates currently originate from German trust centers.
qualified electronic signatures	Electronic signatures that use a qualified certificate valid at the time of their creation and that have been produced with a secure signature-creation device.
roaming ID	A roaming ID is a digital ID that is stored on a server. The private key always remains on the server, but the certificate and its public key can be downloaded at the subscriber's request to any location. Roaming IDs require an Internet connection.
root certificate	The top-most certificate in a certificate chain. It is sometimes used as a trust anchor.
secure signature-creation devices	(SSCD) Software or hardware products used to store and apply signature code and that are designed for qualified electronic signatures
security restricted property or method	A property or method whose availability is restricted to certain events such as batch processing, console execution, or application startup. For example, in Acrobat 7.0, a security-restricted method (S) can only be executed through a menu event if one of the following is true: The JavaScript user preferences item "Enable menu items JavaScript execution privileges" is checked or the method is executed through a trusted function. The <i>JavaScript for Acrobat API Reference</i> identifies the items that have restrictions.
SSCD	See Secure signature-creation devices
timestamp	The date and time that a digital signature was applied. The time stamp data is embedded in the digital signature using a trusted time server (instead of the time clock of the computer that is used to apply the digital signature).
trust anchor	A certificate in a certificate chain that is trusted for selected operations. It could be an ICA rather than a trusted root; that is, it does not have to be the topmost certificate in the chain. Certificates that chain up to this certificate will also be trusted for the same operations. It is usually issued by a 3rd party CA.

Index

-
- .ade 105
- .adp 105
- .apf 141
- .apf Digital IDs no longer supported 13
- .app 105
- .asp 105
- .bas 105
- .bat 105
- .bz 105
- .bz2 105
- .cer 105, 141
- .chm 105
- .class 105
- .cmd 105
- .com 105
- .command 105
- .cpl 105
- .crt 105
- .csh 105
- .exe 105
- .fxp 105
- .gz 105
- .hex 105
- .hlp 105
- .hqx 105
- .hta 105
- .inf 105
- .ini 105
- .ins 105
- .isp 105
- .its 105
- .jar 105
- .job 105
- .js 105
- .jse 105
- .ksh 105
- .lnk 105
- .lzh 105
- .mad 106
- .maf 106
- .mag 106
- .mam 106
- .maq 106
- .mar 106
- .mas 106
- .mat 106
- .mau 106
- .mav 106
- .maw 106
- .mda 106
- .mde 106
- .mdt 106

- .mdw 106
- .mdz 106
- .msc 106
- .msi 106
- .msp 106
- .mst 106
- .ocx 106
- .ops 106
- .p12 141
- .p7b 141
- .p7c 141
- .pcd 106
- .pfx 141
- .pif 106
- .pkg 106
- .prf 106
- .prg 106
- .pst 106
- .rar 106
- .reg 106
- .scf 106
- .scr 106
- .sct 106
- .sea 106
- .shb 106
- .shs 106
- .sit 107
- .tar 107
- .tgz 107
- .tmp 107
- .url 107
- .vb 107
- .vbe 107
- .vbs 107
- .vsmacros 107
- .vss 107
- .vst 107
- .vsw 107
- .webloc 107
- .ws 107
- .wsc 107
- .wsf 107
- .wsh 107
- .zip 107
- .zlo 107
- .zoo 107

A

- Access (Microsoft) 106
- Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft) 106
- Access Add-in Data (Microsoft) 106
- Access Data Access Page (Microsoft) 106

- Access Diagram Shortcut (Microsoft) 106
- Access Macro Shortcut (Microsoft) 106
- Access MDE Database file (Microsoft) 106
- Access Module Shortcut (Microsoft) 106
- Access Project (Microsoft) 105
- Access Project Extension (Microsoft) 105
- Access Query Shortcut (Microsoft) 106
- Access Report Shortcut (Microsoft) 106
- Access Stored Procedures (Microsoft) 106
- Access Table Shortcut (Microsoft) 106
- Access Type 41
- Access View Shortcut (Microsoft) 106
- Access Wizard Template (Microsoft) 106
- Access Workgroup Information (Microsoft) 106
- Accessing the Windows Certificate Store 75
- Acrobat Digital Signature User Guide 9
- Acrobat Document Security User Guide 9
- Acrobat Security Administration Guide 9
- Acrobat Security FDF User Guide 9
- Acrobat 3.0 and later 67, 69
- Acrobat 5.0 and later 67, 69
- Acrobat 6.0 and later 67, 69
- Acrobat 7.0 and later 67, 69
- Acrobat 9.0 and later 67, 69
- Acrobat and PDF Library API Reference 9
- Acrobat SDK Documentation Roadmap 9
- Active Server Page 105
- Add Digital ID dialog 13
- Adding a Certificate From a Signature 32
- Adding a contact 78
- Adding a Roaming ID Account to Get a Roaming ID 26
- Adding an ID that Resides on External Hardware 27
- Adding and Removing Digital ID Files from the File List 19
- Adding Files to the Black and White Lists 107
- Adding or Removing Group Contacts 77
- Adding recipients to a document with certificate security 81, 86
- Adding Someone to Your Trusted Identity List 32
- Adobe LiveCycle Rights Management Server security 49
- Adobe Profile Files 141
- Adobe Trusted Identity Updates 103
- ALCRMS 141
- ALCRMS Server Configuration 92
- All contents 51, 67, 69, 79
- All contents except metadata 51, 67, 69, 79
- Allowing and Blocking Specific Web Sites 111
- Allowing Attachments to Launch Applications 108
- Always use this digital ID 80, 85
- An early compressed file format 107
- Applying a Certificate Security Policy 87
- Applying a Certificate Security to a Group 87
- Applying a Security Policy to a Document 60
- Applying ALCRMS Security 93
- approval signature 141
- Ask me which digital ID to use next time 80, 85
- Associating a Certificate with a Contact 45
- Attachment
 - Cannot open warning 104
 - Dangerous type warning 104
 - Attachment panel in Trust Manager 108
- Audit alert for ALCRMS security 93
- Automatic updates 103
- B**
 - BASIC Source Code 105
 - Batch Processing 105
 - Black Lists and White Lists 104
 - Blocked URL alert 111
 - Bzip 2 UNIX Compressed file (replaces BZ) 105
 - Bzip UNIX Compressed file 105
- C**
 - CA 141
 - CDS 141
 - CDS digital ID 141
 - CDS digital ID certificate 141
 - certificate authority (CA) 141
 - Certificate Chains and Trust Anchors /Roots 118
 - Certificate file 105
 - Certificate Revocation List (CRL) 141
 - Certificate Revocation List. 141
 - Certificate Security 74
 - Certificate security workflow 74
 - Certificate Trust Settings 36
 - Certificate trust settings 37, 38, 139
 - Certificate Viewer
 - Trust tab 33
 - Certificates
 - Contact Information 129
 - Selecting a digital ID for export 124
 - certificates 141
 - Certificates in the Trusted Identities list 121
 - certification signature 141
 - certified document 141
 - Certified Document Services (CDS) 141
 - Certified Document Services. 141
 - certify or certifying 141
 - Changes Allowed 54, 68, 71, 82, 83, 87
 - Changes in FDF Behavior 97
 - Changing a PKCS#12 File's Password Timeout 20
 - Changing a Trusted Identity's Certificate Association 45
 - Changing an ID File's Password 19
 - Changing and Viewing Security Settings 55
 - Changing Document Collection Passwords 72
 - Changing Passwords 28
 - Changing the Security Method Type 57
 - Choosing a certificate for encryption 77
 - Choosing a digital ID for certificate security 80, 85
 - Choosing a Security Method Type 49
 - Choosing What to Encrypt 51
 - Command 105
 - Compatibility 67
 - Compiled HTML Help 105
 - Compressed archive (LH ARC) 105
 - Compressed Archive file 107
 - Compressed archive of Mac files (Stuffit) 107
 - Configure the Select Document Components to Encrypt 67,

- 69, 79, 83
- Configuring ALCRMS Settings Manually 91
- Configuring Multimedia Trust Preferences 99
- Configuring Servers 90
- Contacts
 - Deleting 47
 - Deleting a group 78
 - Editing a group 78
 - Selecting certificates 45
 - Viewing details 44
- Controlling Access to Referenced Files and XObjects 109
- Controlling Multimedia 98
- Controlling Multimedia in Certified Documents 100
- Copying a Security Policy 61
- Creating a Group 77
- Creating a Reusable Certificate Security Policy 78
- Creating a Reusable Password Security Policy 66
- Creating a Self-Signed Digital ID 21
- Creating an ALCRMS Security Policy 92
- Creating Certificate Security for the Current Document 82
- Creating Certificate Security Settings 78
- Creating Password Security for One-Time Use 69
- Creating Password Security Settings 66
- Creating Security Policies with Policy Manager 60
- CRL 141
- Customizing a Digital ID Name 16

D

- Default Behavior
 - Black and White Lists 103
- Default prohibited file types 105
- Deleting a Certificate 47
- Deleting a Digital ID from the Windows Certificate Store 25
- Deleting a Directory Server 42
- Deleting a Group 78
- Deleting a PKCS#12 Digital ID 24
- Deleting a Security Policy 62
- Deleting Contacts and Certificates 46
- Developing Acrobat Applications with JavaScript 9
- Digital ID
 - Certificate viewer 17
 - Components 11
 - Configuration 23
 - Deleting 24
 - From others 11
 - ID export options 122
 - Managing trusted identities 31
 - PKCS#12 location and password 24
- digital ID 142
- Digital ID Basics 10
- Digital ID Directory servers
 - Email details 126
 - Export destination 125
 - Importing 134
 - Sender's identify 126
 - Server list 41
 - Setting defaults 43
 - Setting server details 42
- Digital ID files

- Password configuration 20, 29
- Timeout settings 21
- Digital ID Files menu 18
- Digital ID format selection 22
- Digital ID Management and the Security Settings Console 13
- Digital ID Storage Mechanisms 11
- Digital ID-related file types 12
- Digital IDs
 - Searching for certificates 35
- digital signature 142
- Digital Signature Appearances 9
- Digital Signatures in Acrobat 9
- Digital Signatures in the PDF Language 9
- digitally sign 142
- Directory Name 41
- Distributing a Trust Anchor or Trust Root 118
- Document open password 65
- Document Property dialog 57
- Document Security Basics 48
- Document security settings
 - ALCRMS security 56
 - Certificate security 56
 - Password security 55
- Documentation related to Acrobat security 9
- DOS CP/M Command file, Command file for Windows NT 105
- Downloaded roaming ID certificates 138

E

- Edit Contact dialog 44, 46
- Editing a Security Policy 61
- Editing Directory Servers Details 42
- Editing Security Method Settings 58
- EE 142
- electronic signatures 142
- Emailing a certificate request 124
- Emailing Certificate or Contact Data 44
- Emailing Server Details 125
- Emailing Your Certificate 122
- Emailing your certificate 123, 128, 129
- embedded JavaScript 142
- embedded validation response 142
- Enable text access for screen reader devices for the visually impaired 54, 68, 71, 82, 84, 87
- Enabling Enhanced Security 96
- Encryption algorithm by security type and product version 52
- Encryption configuration panel 51, 67, 70, 79
- Encryption Workflow 50
- end entity certificate (EE) 142
- end entity certificate. 142
- Enhanced Security 95
- Enhanced security
 - Configuration dialog 96
- Enhanced Security in Acrobat 9 and Adobe Reader 9 9
- Envelopes 63
- Examples of Allowed Behavior 98
- Examples of Prevented Behavior 97

- Executable Application 105
- Executable file 105
- Exporting a Trust Anchor 119
- Exporting Application Settings with FDF Files 118
- Exporting Security Settings to a File 112
- Exporting Server Details 126
- Exporting Your Certificate 121
- External connection warning 111
- External Content and Document Security 95

F

- FDF Data Exchange Specification 9
- FDF Files and Security 117
- Finding a Digital ID in a Windows Certificate Store File 25
- Finding an Existing Digital ID in a PKCS#12 File 18
- FoxPro Compiled Source (Microsoft) 105

G

- Generic ID Operations 14
- GeoTrust 142
- Getting and Using Your Digital ID 10
- Getting Started 7
- Glossary of Security Terms 141
- Guidelines for Developing CSPs for Acrobat on Windows 9
- Gzip Compressed Archive 105

H

- High Privilege JavaScript Defined 101
- How Should You Use This Guide? 8
- Hypertext Application 105

I

- Identity preferences 14
- IIS Internet Communications Settings (Microsoft) 105
- IIS Internet Service Provider Settings (Microsoft) 105
- Importing a Certificate From a File 33
- Importing a Trust Anchor and Setting Trust 138
- Importing Adobe LiveCycle Rights Management Server Settings 135
- Importing Adobe LiveCycle Server settings 135
- Importing ALCRMS Settings from an FDF file 91
- Importing ALCRMS Settings with a Security Settings Import 91
- Importing and Exporting Directory Server Settings 43
- Importing Application Settings with FDF Files 127
- Importing digital ID data 34
- Importing Directory Server Settings 134
- Importing Multiple Certificates 130
- Importing multiple certificates 131
- Importing Roaming ID Account Settings 136
- Importing roaming ID server settings 137
- Importing Security Settings from a File 113
- Importing Security Settings from a Server 115
- Importing Someone's Certificate 129
- Importing Timestamp Server Settings 132
- individual digital ID 142
- Information or Setup file 105
- Initialization/Configuration file 105

- Interaction with Trust Manager 98
- intermediate certificate authority (ICA) 142
- Internet access panel 110
- Internet Document Set, International Translation 105
- Internet Location 107
- Internet Security Certificate file (MIME x-x509-ca-cert) 105
- Internet URL Access 109

J

- Java Archive 105
- Java Class file 105
- Javascript and Certified Documents 102
- JavaScript for Acrobat API Reference 9
- JavaScript Security option 102
- JavaScript Source Code 105
- JScript Encoded Script file 105

L

- Launch Attachment dialog 108
- LiveCycle Rights Management Server Security 90
- Logging in to a Device 29
- Logging in to a Digital ID File 18
- Logging in to a Roaming ID Account 26
- Logging in to a roaming ID server 137
- Logging in to an Adobe LiveCycle Rights Management Server 136
- Logging in to PKCS#12 Files 21

M

- Mac OS Command Line executable 105
- Mac OS Finder Internet Location 107
- Mac OS X Installer Package 106
- Macintosh BinHex 2.0 file 105
- Macintosh BinHex 4 Compressed Archive 105
- Make Privileged Folder Locations Recursive 98
- Making a contact a trusted identity 132
- Making a Security Policy Favorite 62
- Manage Internet Access dialog 110
- Manage Trust for Multimedia Content dialog 99
- Manage Trusted Identities menu item 32
- Managing Certificate Trust and Trusted Identities 30
- Managing Contacts 43
- Managing IDs Accessible via PKCS#11 Devices 27
- Managing PKCS#12 Digital ID Files 17
- Managing Roaming ID Accounts and IDs 25
- Managing Windows Digital IDs 25
- Managing your ALCRMS Account 92
- Manually Configuring a Directory Server 41
- Maximum Number of Records to Receive 41
- Media Attachment Unit 106
- Microsoft Management Console Snap-in Control file (Microsoft) 106
- Microsoft Object Linking and Embedding (OLE) Control Extension 106
- Migrating and Sharing Security Settings 112
- MS Exchange Address Book file, Outlook Personal Folder file (Microsoft) 106
- Multimedia behavior workflow 99

Multimedia Trust (legacy) 100

O

OCSP 142
Office Profile Settings file 106
Online Certificate Status Protocol (OCSP) 142
Only file attachments
 51, 67, 69, 79
Opening a Certificate-Protected Document 88
Opening a Password-Protected Document 72
Opening an encrypted document
 With certificate security 89
organization digital ID, desktop 142
organization digital ID, server 142
Organizational policies 59

P

Password 41
Password prompt 72
Password Recovery 73
Password Security 65
Password security 49
Password security workflow 65
PDF Reference 1.7 9
PDF Signature Build Dictionary Specification 9
PDF/X-5 109
Permissions Options 53
Permissions panel 53
Permissions password 65
Permissions Workflow 53
Personalizing an ID name 16
PKCS#11 device 142
PKCS#11 digital ID 142
PKCS#11 format 142
PKCS#11 module 143
PKCS#11 Security Settings menu items 28, 29
PKCS#11 token 143
PKCS#12 143
PKCS#7 143
Policy restrictions 40
Policy security method selection 60
Policy Server 143
Port 41
Preventing Multimedia Playback in Certified Documents 101
Printing Allowed 53, 68, 70, 82, 83, 86
privileged context 143
Program file 106
Providing Instructions to the Trusted Root Recipients 121
Public key certificate security 49

Q

qualified certificates 143
qualified electronic signatures 143

R

Refreshing the Security Policy List 62, 93
Registering a Digital ID for Use in Acrobat 12

Registration Information/Key for Windows 95/98, Registry Data file 106
Removing a contact 78
Removing Document Security 58
Removing Password Security 72
Requesting a Certificate via Email 124
Requesting a Digital ID via Email 33
Resetting the Black and White Lists 108
Resource access 109
Responding to an Email Request for a Digital ID 127
Revoking a Document 94
Roadmap to Security Documentation 8
roaming ID 143
Roaming ID Security Settings menu items 27
Roaming ID server name and URL 137
root certificate 143
Rules for opening a PDF via FDF 97, 117

S

Saving Certificate or Contact Details to a File 44
Saving Your Digital ID Certificate to a File 123
Search Base 41
Searching for a document recipients 36
Searching for Digital ID Certificates 34
Searching for group contacts 88
secure signature-creation devices 143
Security envelope 63
Security Method Basics 48
Security method pros and cons 50
Security method selection 49
Security method selection from Policy Manager 59
Security method workflow 48
Security Methods and Encryption 50
Security Methods and Permissions 52
Security methods for batch processing 55
Security Policies 50
 Reusable Security Settings 59
Security policy
 Favorites list 62
 General settings 60, 66, 79
security restricted property or method 143
Security setting import
 Success dialog 115
Security Setting Import and Export 112
Security setting preferences for server import 115
Security settings
 Document message bar 114
 Encryption method 113
 Export dialog 113
 Import from a file panel 114
Security Settings Console 13
Security settings icon 57
Security settings menu and manager 13
Security Settings menu items 125
Security settings require “save” alert 71
Security Terms 141
Select Document Components to Encrypt panel 51
Selecting a certificate chain for export 120
Selecting a Certificate to Use for Encryption 76

- Selecting a digital ID 128
- Self-expanding archive (used by Stuffit for Mac files and possibly by others) 106
- Server Name 41
- Set the compatibility level 69
- Setting Certificate Trust 37
- Setting Identity Information 13
- Setting JavaScript Options 101
- Setting the Certificate Trust Level 121
- Setting up the Certificate Security Environment 75
- Sharing (Exporting) a Digital ID Certificate 15
- Sharing Settings & Certificates with FDF 115
- Shell Scrap Object file 106
- Signing an FDF file 118
- Specifying a Default Directory Server 43
- Specifying Digital ID Usage 14
- SSCD 143
- Synchronizing a Document for Offline Use 94

T

- Tape Archive file 107
- Temporary file or Folder 107
- This server requires me to log on 41
- Timeout 41
- timestamp 143
- Timestamps
 - Importing a server 133
 - Importing server details from an FDF file 133
- trust anchor 143
- Turning Internet Access Off and On 110

U

- UNIX csh shell script 105
- UNIX ksh shell script 105
- UNIX Tar file Gzipped 107
- Untrusted signature 36
- Usage options for a digital ID 15
- Use this digital ID until I close the application 80, 85
- User name 41
- User policies 59
- Using Certificates for Certificate Security (Encryption) 40
- Using Directory Servers to Add Trusted Identities 40

V

- Validity period expired alert 93
- VBScript Encoded Script file 107
- VBScript file or Any VisualBasic Source 107

- VBScript Script file, Visual Basic for Applications Script 107
- View a Document's Audit History 94
- Viewing a Security Policy 61
- Viewing All of Your Digital IDs 15
- Viewing and Editing Contact Details 43
- Viewing Digital ID Certificates in the Certificate Viewer 16
- Viewing Document Encryption and Permission Settings 55
- Viewing Document Restrictions 56
- Viewing Security Settings in a Browser 57
- Visio Stencil (Microsoft) 107
- Visio Template (Microsoft) 107
- Visio Workspace file (Microsoft) 107
- Visual Studio .NET Binary-based Macro Project (Microsoft) 107
- Visual Test (Microsoft) 106

W

- What is a Digital ID? 10
- What is a Trusted Identity? 30
- What's in this Guide? 7
- Who Should Read This Guide? 7
- Why Attach a File that's on the Black List? 104
- Windows Control Panel Extension (Microsoft) 105
- Windows digital ID menu 25
- Windows Explorer Command 106
- Windows Help file 105
- Windows Installer file (Microsoft) 106
- Windows Installer Patch 106
- Windows integration 76
- Windows Program Information file (Microsoft) 106
- Windows Screen Saver 106
- Windows Script Component 107
- Windows Script Component, Foxpro Screen (Microsoft) 106
- Windows Script file 107
- Windows Script Host Settings file 107
- Windows SDK Setup Transform Script 106
- Windows Shortcut file 105
- Windows Shortcut into a Document 106
- Windows System file 106
- Windows Task Scheduler Task Object 105
- WinRAR Compressed Archive 106
- Working with Attachments 103
- Working with Documents and ALCRMS Policies 92
- Working with Groups of Contacts 77

Z

- ZoneLabs ZoneAlarm Mailsafe Renamed .PIF file 107