Adobe Reader 7.X Security Feature Reference
Contents

1 What’s in this Guide? ................................................................. 6

2 Getting and Using Your Digital ID ........................................... 7
   Digital ID Basics ........................................................................ 8
   What is a Digital ID? ................................................................. 8
   How are Digital IDs managed? ............................................... 8
   Digital ID storage formats ..................................................... 9
   Digital ID User Interface ....................................................... 9
   Getting Your Own Digital ID ............................................... 11
   Adding IDs During a Workflow ............................................. 11
   Adding IDs in Advance ......................................................... 12
   Responding to an Emailed Request for a Digital ID .......... 12
   Creating a Self-Signed Digital ID ......................................... 14
   Finding an Existing Digital ID .............................................. 16
   Getting a Third-Party Digital ID ............................................ 17
   Upgrading a Legacy .apf Digital ID ....................................... 17
   Backing up the Private Key ................................................... 17
   Using Your Digital ID ............................................................ 18
   Specifying a Default Digital ID ........................................... 18
   Changing or Clearing the Default Digital ID ...................... 19
   Deleting a Digital ID ............................................................ 19
   Emailing Your Digital ID Certificate .................................. 19
   Saving Your Digital ID Certificate to a File ...................... 21
   Viewing Your Digital ID Certificate Details ..................... 22
   Changing a Digital ID’s Password and Timeout .............. 22
   Login, Logout, and Batch Processing .................................. 24

3 Managing Trusted Identities .................................................. 25
   Creating a Community of Document Authors and Recipients ... 26
   Setting up the Trusted Identity Environment ..................... 28
   Creating Default User Information ................................... 28
   Adding Certificate Servers as Searchable Directories .......... 29
   Using the Windows Certificate Store for Signing and Certificate Security . 29
   Adding Someone to Your Trusted Identity List .................. 32
   Adding a Digital ID from a Signature ................................ 32
   Requesting a Digital ID via Email ...................................... 32
   Browsing for a Trusted Identity .......................................... 34
   Searching for a Digital ID to Trust .................................... 34
   Importing a Single Certificate From an FDF File ............... 36
   Working with Digital IDs and Certificates ......................... 37
   Displaying a Certificate in the Certificate Viewer .............. 37
   Verifying Self-Signed Certificates ..................................... 38
   Checking Certificate Revocation Status ......................... 39
   Trusting Timestamp Authority Certificates ..................... 40
   Certificate Trust Settings .................................................. 41
   Trusting a Certificate for Signing and Certifying .............. 41
4 Digital Signatures for Document Recipients .........................................................55
  Working with Signed Documents ...........................................................................56
  Signature Components: What Makes them Valid? ...............................................56
  Signature Status and Validity Icons .......................................................................57
  Setting up Your Environment for Receiving Documents ........................................59
    Setting Up Automatic Signature Validation ....................................................59
    Setting Digital Signature Validation Preferences .............................................59
    Configuring Document Status Preferences ......................................................61
    Setting Dynamic Content (Multimedia) Security Options ...................................63
    Setting High Privilege JavaScript Security Options ...........................................65
    High Privilege JavaScript Defined ......................................................................65
  Validating Signatures Manually ............................................................................66
    Validating a Single Signature ............................................................................66
    Validating All Signatures Simultaneously .........................................................67
    Validating an Unknown (Untrusted) Signature ...................................................67
    Validating a Signature for an Earlier Document Version ....................................70
  When the Status Icon is Not a Green Check. ........................................................71
    Green Check and Caution Triangle .....................................................................71
    Question Mark and Caution Triangle ..................................................................72
    Question Mark and Person ................................................................................72
    Question Mark and Pen ......................................................................................73
    Red X and Pen ......................................................................................................73
    Running JavaScript and Dynamic Content .......................................................73
  Timestamp Basics for Document Recipients .......................................................74
    Trusting a Timestamp Certificate in a Signature ................................................74
    When Timestamps Can't be Verified. ...................................................................75
  Viewing and Comparing Document Changes and Versions ....................................76
    Viewing a Signed Version of a Document .........................................................76
    Viewing a List of Post-Signing Modifications .....................................................76
Comparing Documents ........................................................................................................ 77
Comparing a Signed Version with the Current Version ............................................... 77
Comparing Documents by Page ...................................................................................... 78
Comparing Documents by Word ...................................................................................... 79

5 Sharing Acrobat Settings and Data with FDF Files ..................................................... 81
Importing Acrobat Data .................................................................................................. 83
Responding to an Emailed Request for a Digital ID ....................................................... 83
Importing a Single Certificate via FDF ........................................................................... 83
Importing Multiple Certificates via FDF ......................................................................... 84
Importing Timestamp Server Settings via FDF ............................................................... 86
Importing Directory Server Settings via FDF ................................................................. 87
Importing APS Server Settings via FDF ......................................................................... 88
Exporting Acrobat Data .................................................................................................. 91
Distributing a Trust Anchor or Trust Root ...................................................................... 91
Setting Certificate Trust Level ....................................................................................... 92
Export the Certificate ...................................................................................................... 93
Provide Instructions to the Trusted Root Recipients ..................................................... 95
Emailing Your Digital ID Certificate .............................................................................. 95
Saving Your Digital ID Certificate to a File ................................................................. 97
Requesting a Digital ID via Email .................................................................................. 97
Emailing Server Details via FDF ................................................................................... 99
Exporting Server Details via FDF ................................................................................ 100

6 External Content and Document Security .................................................................... 102
Setting Attachment Options ....................................................................................... 102
Default Attachment Behavior ...................................................................................... 102
Modifying Attachment Behavior Via the User Interface ............................................... 106
Adding Custom Attachment Extensions ...................................................................... 107
Propagating New Attachment Settings ........................................................................ 107
Allowing Attachments to Open Files or Launch Applications ..................................... 107
External Stream Access ............................................................................................... 108
Internet URL Access ..................................................................................................... 108

7 Index .......................................................................................................................... 111
What’s in this Guide?

This guide describes some of the Adobe Reader 7.X security features. Most features are available in all 7.x series of releases. If a user interface item does not appear, then that feature is not available. The features include the following:

- Working with digital IDs that are used for signing and certificate security workflows:
  - “Getting and Using Your Digital ID” on page 7
  - “Managing Trusted Identities” on page 25
- Sharing digital ID, server settings, and other data with data exchange files:
  - “Exporting Acrobat Data” on page 91
  - “Importing Acrobat Data” on page 83
- Securing the application environment:
  - “Setting Attachment Options” on page 102
  - “External Stream Access” on page 108 (only available in 7.0.5 and later)
  - “Internet URL Access” on page 108
A digital ID is a digital version of a driver license, passport, and other “certified by some entity” paper identification. They are used to electronically prove an identity, thereby granting access and privileges to secure documents. You will need a digital ID to sign with digital signatures and apply certificate security. For participants in signing and certificate security workflows, exchanging the public part the digital ID (the public key and certificate) is a central aspect of sharing signed and secure documents. For more information, refer to the following:

- “Digital ID Basics” on page 8
- “Getting Your Own Digital ID” on page 11
- “Using Your Digital ID” on page 18
Digital ID Basics

What is a Digital ID?

A digital ID is a digital version of a driver license, passport, and other “certified by some entity” paper identification. They are used to electronically prove an identity, thereby granting access and privileges to secure documents. Digital IDs are required for using digital signatures and certificate security.

A digital ID consists of two parts: a certificate and a private key. A certificate consists of an identity 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.” Acrobat users share their certificates and public keys so that documents that are signed or are associated with security methods, policies, and permissions can be securely traverse workflows across the enterprise. Shared certificates can be physically sent in a file, or more commonly, made available over a network. The private key is never shared and is used to decrypt documents.

While most certificates are signed by a third-party, trusted certificate authority, it is also possible to create a self-signed digital ID within Acrobat. In this case, the certificate authority is also the owner of the digital ID. Digital IDs are usually password protected and stored on a user’s computer, flash card, server, smart card, or some other accessible location. Private keys are often backed up or escrowed by IS administrators since the loss of the key means that documents encrypted with that key will no longer be accessible.

How are Digital IDs managed?

Just as your certificate and public key is shared with other Acrobat users so that they can validate your signature and use other security features, so do other users (contacts) share their certificates with you. Sharing a certificate means that it is available to other users, and the physical certificate may or may not be stored on local machines. 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 Trusted Identities".
- **Network sharing**: Certificates are stored on a central server. The Trusted Identity Manager can be used to search for certificates on LDAP directory servers. Acrobat provides tools for configuring and managing as many directory servers as needed. For details, see “Using Directory Servers to Add Trusted Identities” on page 51.
Digital ID storage formats

There are several digital ID storage formats. Common file extensions include .pfx (PKCS#12 on Windows), .p12 (PKCS#12 on Macintosh), .apf (Digital ID files from Acrobat 4 and 5), and .cer (Windows certificates). The most common ID types are as follows:

- **PKCS#12**: A standard password protected and encrypted format that uses a .pfx extension on Windows and .p12 on a Macintosh. These files can be stored anywhere, and Acrobat remembers the file location when the ID is registered.

- **PKCS#11**: An encryption format used on smart cards and other PKCS#11-compatible devices. There is no file associated with these IDs.

- **Windows Personal Certificates**: Windows Certificate digital IDs are stored in the Windows Certificate Store (sometimes called a “credential store”). These IDs can be used by other Windows programs as well as Acrobat. For information about using Windows certificates, see “Using the Windows Certificate Store for Signing and Certificate Security” on page 29.

Digital ID User Interface

The Security Settings dialog enables users to manage their own digital IDs and find the digital IDs for others that will participate in signing and certificate security workflows. Choosing **Advanced > Security Settings** opens a dialog for managing the following:

- **Digital IDs**: The digital ID tree lists your personal digital IDs.
  - **P12 digital IDs**: Users can add, remove, and manage their P12 digital IDs as well as change the password for the .pfx file that may contain one or more IDs.
  - **Windows digital IDs**: Users can add, remove, export, and manage IDs in the Windows Certificate Store.
  - **PKCS#11 modules and tokens**: Users who have smart cards or other PKCS#11 devices can add, remove, and manage their own digital IDs.

- **Servers**: The servers list includes a list of those servers that contain certificates (usually for other people) that are used for signing and certificate security workflows.
  - **Directory servers**: Directory servers are LDAP servers that are capable of returning x.509 public key certificates. These servers are certificate repositories that users search to expand their list of trusted identities. Server administrators often set up a company-specific directory server.

- **Timestamp servers**: Timestamp servers enable users to timestamp signatures with a timestamp that originates from a trusted timestamp authority. Server administrators sometimes set up a company-specific timestamp server or use a third-party service.
- **Adobe Policy Servers**: The Adobe Policy Server is only available to users in companies that have purchase the APS software.

**Figure 3  Security settings menu and manager**
Getting Your Own Digital ID

Digital IDs help you sign, certify, and decrypt documents. There are several ways to get a digital ID:

- **Adding IDs During a Workflow**
- **Adding IDs in Advance**
- **Responding to an Emailed Request for a Digital ID**
- **Creating a Self-Signed Digital ID**
- **Finding an Existing Digital ID**
- **Getting a Third-Party Digital ID**
- **Upgrading a Legacy .apf Digital ID**

Adding IDs During a Workflow

The workflow for adding a digital ID begins with the Add Digital ID dialog (Figure 4). This dialog may be accessed in two ways:

- In workflows where a user attempts to sign, certify, or encrypt a document.
- By setting up the ID ahead of time for later use.

![Add Digital ID dialog](image)

To set up an ID during the course of signing, certifying, or encrypting a document:

1. Start the process that requires a digital ID (Choose **Sign**, **Save as Certified**, or some other menu item.)
2. When the Apply Digital Signature - Digital ID Selection dialog appears, choose **Add Digital ID**.
3. Set up the ID as described by one of the following:
   - **Creating a Self-Signed Digital ID**
   - **Finding an Existing Digital ID**
   - **Getting a Third-Party Digital ID**
**Adding IDs in Advance**

The workflow for adding a digital ID begins with the Add Digital ID dialog (Figure 4). This dialog may be accessed in two ways:

- In workflows where a user attempts to sign, certify, or encrypt a document.
- By setting up the ID ahead of time for later use.

To set up an ID in advance:

1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Choose **Add ID**.
4. Set up the ID as described by one of the following:
   - **Creating a Self-Signed Digital ID**
   - **Finding an Existing Digital ID**
   - **Getting a Third-Party Digital ID**

**Figure 5 Digital ID: Adding a digital ID**

**Responding to an Emailed 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 (apply 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 > Trusted Identities** and then choose **Request Contact**. Acrobat automatically attaches an FDF file with their public digital ID information to an email that requests your digital ID details. 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. Before continuing, get a digital ID as described in “Creating a Self-Signed Digital ID” on page 14 or “Getting a Third-Party Digital ID” on page 17.

To respond to an emailed digital ID request:

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

   **Figure 6** Emailing your certificate

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

   **Tip:** If you do not have a digital ID, an alert appears that says “A certificate was not selected for export.” Exit the workflow and get a digital ID as described in “Creating a Self-Signed Digital ID” on page 14 or “Getting a Third-Party Digital ID” on page 17.

   **Figure 7** Selecting a digital ID

4. Choose **Select**.

5. Review the email details. You can edit the To, Subject, and Body fields.

6. Choose **Email**.

7. Send the email through your mail application.
Creating a Self-Signed Digital ID

Users can use third-party or self-signed digital IDs. Both types store an encrypted private key and a certificate that contains a public key and information such as contact details. Self-signed IDs are usually considered less secure because they are not issued by a third-party certificate authority.

To create a self-signed digital ID:

1. Navigate to the Add Digital ID dialog as described in Adding IDs During a Workflow or Adding IDs in Advance.

2. Choose **Create a Self-Signed Digital ID**.

3. Choose **Next**.

4. Choose **Next**.

5. Select a digital ID format and store:
   - **New PKCS#12 Digital ID File**: Stores the information in a .pfx file. On Windows, the default location is `C:\Documents and Settings\<username>\Application Data\Adobe\Acrobat\7.0\Security\`
   - **Windows Certificate Store**: (Windows only) Stores the private key on disk file where other Windows applications can find it and stores the certificate in the registry.

   **Tip:** Which ID type should you choose? PKCS#12 digital IDs are flexible because they are files that can be copied, moved, and emailed. They are cross-platform, portable, and always password protected. These files should always be backed up.

   Windows Certificate Store digital IDs are easy to use, do not have to be password protected, and can be used by any Windows application. These are not portable and are less secure because a password is not required. Digital IDs in the Windows Certificate Store can be used by other applications.

6. Choose **Next**.

7. Configure the Digital ID:
   - **Name**: The name appears in the Signatures tab and in the signature field.
• **Organizational Unit**: Optional. The company business unit to display in the signature and certificate.

• **Organizational Name**: Optional. The company business unit name to display in the signature and certificate.

• **Email Address**: Optional. The email address to display in the signature and certificate.

• **Country/Region**: Optional. The country or region to display in the signature and certificate.

• **Enable Unicode Support**: Optional: Check the option to use unicode in the form fields.

• **Key Algorithm**: 2048-bit RSA offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible.

• **Use Digital ID for**: Select whether to use the digital ID for digital signatures, data encryption, or both.

**Figure 10 Digital ID: Configuration**

8. 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**.
Finding an Existing Digital ID

If a required digital ID file does not appear in the digital ID list, search for it and add it. These files may have the following extensions listed in “Digital ID storage formats” on page 9.

To find a digital ID file:

1. Navigate to the Add Digital ID dialog as described in Adding IDs During a Workflow or Adding IDs in Advance.

2. Choose Find an Existing Digital ID.

3. Choose Next.

4. Choose Browse and browse to the digital ID file. PKCS#12 files can be stored anywhere, but the default location for Windows is C:\Documents and Settings\<username>\Application Data\Adobe\Acrobat\7.0\Security\.

5. Choose Open.

6. Enter the ID password.

7. Choose Next.

Getting a Third-Party Digital ID

In general, third-party digital IDs are used where a high level of trust is required. Vendors such as Entrust provide advanced security features. Third-party providers verify your identity, maintain system integrity, and provide multiple digital IDs for users who sign documents in different roles or certification methods.

To get information on third-party digital IDs:

1. Navigate to the Add Digital ID dialog as described in Adding IDs During a Workflow or Adding IDs in Advance.

2. Choose **Find an Existing Digital ID**.

3. Choose **Next**.

4. When a Web page appears with a list of signature partners, follow the instructions provided.

Upgrading a Legacy .apf Digital ID

Acrobat 4 and 5 use a deprecated digital ID format with an .apf extension. If an .apf digital ID file is selected, users will be prompted to convert the file to a supported file type.

Backing up the Private Key

Users should always back up their private key. Without the key, encrypted document cannot be decrypted and opened. To protect and back up private keys across a business, administrators sometimes escrow private keys for users throughout an organization.
Using Your Digital ID

Once you have one or more digital IDs, you can edit, remove, and otherwise manage them from the Security Settings dialog. To simplify subsequent workflows, it may be expedient to do the following before using your ID:

- **Specifying a Default Digital ID**: Set an ID to automatically use each time one is required for signing or certificate encryption.
- **Emailing Your Digital ID Certificate**: Since a digital ID's certificate contains a public key required for validating digital signatures and encrypting documents, you can send it to eventual document recipients ahead of time. Doing so simplifies their validation process.

**Figure 14 Digital ID management**

Specifying a Default Digital ID

If a default digital ID is not specified, a prompt asks for a digital ID file. To avoid repeated prompts, specify a default digital ID for signing, encrypting, or both. Different IDs may be used for signing and encryption.

To select a default digital ID file:

1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree (Figure 5).
3. Highlight an ID in the list on the right.
4. Choose **Set Default**. A drop down list appears.

**Figure 15 Digital ID: Default ID specification**

5. Choose whether to use the digital ID for signing, encrypting, or both. A lock or pen icon (or both) will appear to the left of the digital ID based on this selection.

**Tip**: Invalid and expired IDs are associated with a yellow caution triangle. These may not be used.
Changing or Clearing the Default Digital ID

Only one default digital ID may be specified at a time.

To change or clear the default digital ID do one the following:
- Specify a new default ID as described in “Specifying a Default Digital ID” on page 18.
- Clear the default specification:
  2. Select Digital IDs in the left-hand tree (Figure 5).
  3. Highlight an ID in the list on the right.
  5. Choose Clear.

Deleting a Digital ID

Caution: Deleting a digital ID has significant consequences that should be understood before proceeding. Because deleting an ID deletes its private key, operations that require that key will no longer be possible. Moreover, deleting a PKCS#12 ID actually deletes the ID rather than Acrobat’s knowledge of the ID. If the file is used by other programs, do not delete it.

To delete a ID from the list of trusted certificates:

2. Select Digital IDs in the left-hand tree (Figure 5).
3. Highlight an ID in the list on the right.
4. Choose Remove ID.
5. Choose OK when asked to proceed.

Emailing Your Digital ID Certificate

A digital ID’s certificate contains a public key required for validating digital signatures and encrypting documents. Therefore:
Before users receiving a document can validate its signature, they must receive the sender's certificate.

Before users can encrypt a document using certificates, they must have access to the certificates of the document recipients.

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

- To export from the certificate list in the Security Settings dialog, display it by choosing Advanced > Security Settings. For details, see below.
- To export any certificate displayed in the Certificate Viewer, choose Export on the General tab.

To email a digital ID certificate:

2. Select Digital IDs in the left-hand tree (Figure 5).
3. Highlight an ID in the list on the right.
5. Choose Email the data to someone (Figure 17).

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

9. Choose Sign if you want to sign the FDF file; otherwise, choose Next.

10. Enter an email address.

11. Choose Next.

12. Review the data and choose Finish.

13. When the email program opens, send the email.

**Saving Your Digital ID Certificate to a File**

A digital ID's certificate contains a public key required for validating digital signatures and encrypting documents. Therefore:

- Before users receiving a document can validate its signature, they must receive the sender's certificate.
- Before users can encrypt a document using certificates, they must have access to the certificates of the document recipients.

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

- Exporting from the certificate list in the Security Settings dialog. Display it by choosing Advanced > Security Settings. For details, see below.
- Exporting any certificate displayed in the Certificate Viewer. Simply choose Export on the General tab.

To save a digital ID certificate to a file:


2. Select Digital IDs in the left-hand tree (Figure 5).

3. Highlight an ID in the list on the right.


5. Choose Save the exported data to a file (Figure 17).

6. Choose a file type:
   - Acrobat FDF Data Exchange: FDF files can only be emailed in 7.0.7
   - Certificate Message Syntax - PKCS#7: Save the file as a PKCS7 file.
   - Certificate File: Saves the file in CER format.

7. Choose Next.

8. Browse to a file location and choose Save.

9. Choose Next.

10. Review the data to export and choose Finish.
Viewing Your Digital ID Certificate Details

A user's personal digital IDs are listed in the Security Settings dialog. The Certificate Viewer displays certificate information, including the time for which the certificate is valid, usage, a unique serial number, public key method, and so on (Figure 19).

To check certificate details:

2. Select Digital IDs in the left-hand tree (Figure 5).
3. Highlight an ID in the list on the right.
4. Choose Certificate Details. The Certificate Viewer displays the certificate (Figure 19).

![Figure 19 Digital ID: Certificate viewer](image)

Changing a Digital ID’s Password and Timeout

Passwords and password time-outs can be set for PKCS#12 IDs and Windows Personal Certificates but not for PKCS#11 IDs. In the case of PKCS#12 IDs where a file can contain multiple IDs, passwords and time-outs are configured at the file level rather than for individual IDs.

**Note:** If a PKCS#12 .pfx file is read only, then change password and timeout options will not be available.

To change the password:

2. Highlight Digital ID Files in the left-hand tree (Figure 20).

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**

To change the password timeout:

1. Choose **Advanced > Security Settings**.

2. Highlight **Digital ID Files** in the left-hand tree (Figure 5).


4. Choose **Password Timeout**.

5. Configure the Password Timeout Policy dialog by specifying when a prompt should appear asking for a password:
   - **Always**: A password is always required each time the digital ID is used.
   - **After**: Choose a value from the drop down list.
   - **Once per session**: A password is asked for only one time while Acrobat is open.
   - **Never**: The password is never asked for.

6. Enter the password.

7. Choose **OK**.
Login, Logout, and Batch Processing

The digital ID Login and Logout feature is used primarily for 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 the user for a password, the batch sequence is effectively stopped until a user intervenes.

The login and logout options are only useful for logging into the default digital ID or when some batch process is set up to only use the digital ID the user is logged into.

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

2. Select Digital IDs in the left-hand tree (Figure 5).
3. 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.
Managing Trusted Identities

A digital ID is a digital version of a driver license or other “certified by some entity” paper identification that electronically proves an identity, thereby granting access and privileges to secure documents. For signing and certificate security workflows, obtaining the public part the digital ID (the public key and certificate) from participants other than yourself is a central aspect of sharing signed and secure documents. Once you obtain their information, they become a “trusted identity” within your application environment.

Understanding what a trusted identity is and how specific trust levels are specified can make secure workflows more efficient. For example, you can add trusted identities ahead of time or as needed. Trusted identity information can be stored locally or on a central server. Moreover, each identity’s certificate trust settings may be individually specified. For more information, refer to the following:

- “Creating a Community of Document Authors and Recipients” on page 26
- “Setting up the Trusted Identity Environment” on page 28
- “Adding Someone to Your Trusted Identity List” on page 32
- “Working with Digital IDs and Certificates” on page 37
- “Certificate Trust Settings” on page 41
- “Managing Contacts” on page 45
- “Working with Groups of Contacts” on page 49
- “Using Directory Servers to Add Trusted Identities” on page 51
Creating a Community of Document Authors and Recipients

Documents by their very nature are created to be shared and distributed, but in enterprise environments, they are also designed to be used. When a document contains a security method, a digital signature, or even a blank signature field, it is often the case that the author intends its distribution to be limited to specific users or document recipients. A document recipient who has a public key certificate and is specifically trusted by you to participate in secure or signature workflows is called a trusted identity. Acrobat lets you to create a list of trusted identities, store their contact and certificate information, and set different trust levels for each identity.

In signature and some secure workflows, a document recipient should be 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.

Both certificate security and digital signatures rely on public key certificates to identify who can participate in document lifecycles involving encrypting/decrypting and signing. Trusted identities are therefore used in several workflows:

- When you sign and send a document, the document recipient can validate your signature by validating the certificate embedded in the document. The recipient can also choose to set the trust level associated with that certificate if it will be reused in the future. Conversely, you need access to a document sender’s certificate to validate their signature.

- When you encrypt a document, you use the public key of the document recipients so that they can decrypt it with their corresponding private key. Conversely, others need your certificate to encrypt documents for you.

Acrobat provides 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 other individuals, it is often desirable to create a list 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 build a list of trusted identities containing your trusted identity’s 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. The three most common ways of getting the data include the following:

- **Extracting the data from an FDF file.** Double-clicking on an emailed file or a file on some accessible directory causes Acrobat to automatically import the information.

- **Searching a server directory.** Users can add directory servers containing contact information and certificates. Sometimes administrator preconfigure these directories or send server details in an FDF file.

- **Using the data embedded in a signed document.** The Certificate Viewer provides options for adding the information to the trusted identities list and setting the trust level.

![Figure 23 Digital ID: Managing trusted identities](image)

From within the Manage Trusted Identities dialog, users import and manage the digital ID information (again, it contains certificate and certificate owner data) for any document recipient that should be trusted. 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 > Trusted Identities** and opening the Trusted Identities Manager.
Setting up the Trusted Identity Environment

In signing and security workflows that use certificates, other users become “trusted” when their digital ID certificates are verified and a specific trust level is set. You can simply validate and trust certificates “on-the-fly” as you receive individual documents, or you can pre-trust certificates and set up product behavior ahead of time to simplify workflows later.

For users making extensive use of certificates in document workflows, it is a good idea to consider doing the following:

- **Creating Default User Information**: Configure your personal information that will be used in subsequent workflows.
- **Adding Certificate Servers as Searchable Directories**: Configure the product to find certificates that are not on your machine.

Creating Default User Information

Users can enter default identity (user) information. Acrobat and Adobe Reader store this information and use it automatically as the defaults for certain workflows such as creating new identities and self-signed certificates, exporting directory server settings, and annotations.

To create default user information:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select **Identity** in the left-hand tree.
3. Configure the identity details as needed.
4. Choose **OK**.

![Figure 24 Identity preferences](image)
Adding Certificate Servers as Searchable Directories

Some security settings enable you to search for digital IDs (public key certificates) that needed to be added to your list of trusted identities because the ID owners will be participating in signing and certificate security workflows. In large organizations, these certificates are often stored on a server. Configuring Acrobat or Adobe Reader with specific server information allows those products to search the servers for the needed certificates.

As described in “Using Directory Servers to Add Trusted Identities” on page 51, choosing Advanced > Security Settings opens a dialog for add the following servers:

- **Directory servers**: Directory servers are LDAP servers that are capable of returning x.509 public key certificates. These servers are certificate repositories that users search in order to expand their list of trusted identities. Server administrators often set up a company-specific directory server.

- **Timestamp servers**: Timestamp servers enable users to timestamp signatures with a timestamp that originates from a trusted timestamp authority. Server administrators sometimes set up a company-specific timestamp server or use a third-party service.

  **Note**: Adobe Policy Servers: The Adobe Policy Server is only available to users in companies that have purchase the APS software. It does not contain certificates.

Using the Windows Certificate Store for Signing and Certificate Security

The Windows Certificate Store is an area in the registry where certificates are stored for use by Windows applications. A certificate store may contain numerous certificates issued by different certification authorities. Moving those certificates is not an option because the Windows Certificate Store is used by programs other Adobe products. For example, when signing outgoing emails in Outlook, the digital ID comes from the “Personal” certificate store in Windows. When validating signed emails from other people in Outlook, the trusted certificates are stored in the Windows “Trusted People” certificate store.

The Windows Certificate Store contains a store called “Trusted Root Certificate Authorities” that contains root certificates. Certificates are “root” certificates simply by virtue of being at the top of the certificate chain hierarchy. These certificates are X.509-compliant certificates that are digitally signed by a certificate authority that Microsoft or a system administrator has determined is trustworthy.

Users often want to use the Windows Certificate Store as well as Adobe's store. Both Acrobat and Reader provide options for adding the Windows Certificate Store to their directory search path in the Trusted Identity Manager so that those certificates can be imported, trusted, and used for validating signatures and encrypting documents.

To use these certificates within Acrobat or Reader, enable import from the Windows Certificate Store. Doing so allows seamless integration between Acrobat and other applications, including encrypting files within Acrobat that are emailed via Outlook. You also might wish to import certificates from here if there are some people you exchange email with via Outlook that you wish to trust for certifying documents, signing JavaScripts, and so on, but you do not wish to trust all of them.

Using Windows Certificate Store Certificates for Validation

The are two common ways a certificate ends up in the Windows Certificate Store root directory:

- The manufacturer of the computer or Microsoft has put them there.
- A company administrator has put them there as part of a larger, company-wide program called a public-key infrastructure (PKI).
For this reason, most home users do not need to trust Windows root certificates by default. Trusting all root certificates for any operation may compromise security because content from companies that have certificates installed in Windows may be automatically trusted. That is, by trusting root certificates, you may be trusting all the content provided by the company that owns that certificate.

Enterprise users, on the other hand, should consult company policy to determine whether or not to trust all Windows root certificates for either validating signature, and/or certifying documents. This information should come from the IS administrator, and Acrobat may already be configured with the correct settings. A common reason to trust Windows roots is so the system administrator can manage from a central location the certificates deployed across a network.

**Tip:** Many root certificates ship with Windows, and they do not always meet the same standards. The decision should be made by an experienced system administrator who knows the implications.

To use these certificates for validation:

1. Choose **Edit > Preferences**.
2. Choose **Security** in the left-hand list.
3. Choose **Advanced Preferences**.
4. Display the Windows Integration tab.

**Figure 25 Trusting Windows root certificates**

5. Specify the trust level for all root certificates in the Windows Certificates Store:
   - **Validating signatures**: All root certificates in the Windows Certificates Store will be trusted when validating signatures.
   - **Validating certified documents**: All root certificates in the Windows Certificates Store will be trusted when validating certified documents.
6. Choose **OK**.
7. Choose **OK**.

**Adding Windows Certificate Store Certificates to the Search Path**

Acrobat’s user interface enables users to search directories from the Search for Recipients dialog (**Figure 26**). Adding the Windows store to the search path automatically makes its certificates available for import. This 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**.

By default, the Windows Certificate Store is not added to Acrobat's 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 make Windows Certificate Store directories part of the search path:

1. Choose **Edit > Preferences**.
2. Choose **Security** in the left-hand list.
3. Choose **Advanced Preferences**.
4. Display the Windows Integration tab (Figure 25).
5. Specify whether to enable import of identities from the Windows Certificate Store into the list of trusted identities. Check or uncheck **Enable import and use of identities in the Windows Certificate Store**.

   The Windows Certificate Store appears in the Directory list.

   **Figure 26 Digital IDs: Searching the Windows Certificate Store**

6. Choose **OK**.
7. Choose **OK**.
Adding Someone to Your Trusted Identity List

As shown in Figure 23, you build a list of trusted identities by getting contact and certificate information from others who will be participating in workflows that use public key certificates. 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.

Adding a Digital ID from a Signature

When you receive a signed document from someone whose digital ID is not in your trusted identity list, the certificate validity will be unknown and a question mark will appear in the signature status icon. To validate the signature then, add the signer’s digital ID to your application’s trusted identity list.

To add signer’s ID from their signature:

1. Right click on the signature and choose Properties.
2. Choose the Signer tab.
3. Choose Show Certificate.
4. When the Certificate Viewer appears, choose the Trust tab.
5. Choose Add to Trusted Identities.
6. Choose the certificate trust settings as described in “Trusting a Certificate for Signing and Certifying” on page 41.

Requesting a Digital ID via Email

When you request digital ID information from someone, Acrobat automatically includes in that email an FDF file containing your contact and certificate information.

To request a certificate from another user:

1. Choose Advanced > Trusted Identities.
2. Choose Request Contact.
3. Confirm or enter your identity.

**Tip:** The identity panel is prepopulated if the information has been previously configured in **Edit > Preferences > Identity**. To view or edit identity information, see “Creating Default User Information” on page 28.

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 the digital ID file to export.

8. Choose **Select**.

9. Do one of the following:
   - **Email**: Enter the person’s email address in the Compose Email dialog and choose **Email**. Send the email message when it appears in the default email application with the certificate request attached.
- **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.

**Browsing for a Trusted Identity**

Adding a contact may or may not add a certificate since certificates aren’t necessarily attached to the contact information. However, in most cases you get both. Check the Contacts and Certificates panel to see what was imported.

To browse to the contact file location:

1. Choose **Advanced > Trusted Identities**.
2. Choose **Add Contacts**.
3. Choose **Browse**.
4. Browse to the contact file location.

**Tip**: If the information was exported from Acrobat, it will be in an FDF file. Other file types include .cer, .p7b, and so on.

5. Select the file.
6. Choose **Open**.

**Figure 29 Importing digital ID data**

![Choose Contacts to Import dialog](image)

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

**Searching for a Digital ID to Trust**

The search feature allows you to search a list of preconfigured directories for certificates that you can add to your trusted identity list. When you have access to someone else’s certificate, you can validate their
signature and send them secure documents. 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 list of servers that ship with Adobe Acrobat and Adobe Reader.
- Whether or not the user has configured the application to use the Windows Certificate Store. For details, see “Using the Windows Certificate Store for Signing and Certificate Security” on page 29.
- Whether or not the directory server list is in the Security Settings Manager. For details, see “Using Directory Servers to Add Trusted Identities” on page 51.

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

Adding a contact may or may not add a certificate because certificates aren’t necessarily attached to the contact information. However, since importing only contact information doesn’t let you do anything, in most cases you get both. After finding and importing the data, check the Contacts and Certificates panel to see what was imported.

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

1. Choose **Advanced > 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. Choose **Import**.

9. Choose **OK** when the confirmation dialog appears.

**Importing a Single Certificate From an FDF File**

For details, refer to the following:

- "Importing a Single Certificate via FDF" on page 83
- "Importing Multiple Certificates via FDF" on page 84
Working with Digital IDs and Certificates

In Acrobat, other users become “trusted” when their digital IDs are verified and a specific trust level is set. You can set trust levels ahead of time if you have access to the certificates of those users that will participate in your signing and encryption workflows. If you do not have access to those certificates, simply validate and trust certificates “on-the-fly” as you receive individual documents. As shown in Table 1, the Certificate Viewer provides six tabs with functionality for working with and verifying digital IDs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>What is shows</th>
<th>What you can do</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Signer and Issuer information, validity dates, and intended usage.</td>
<td>Export the certificate to a file</td>
</tr>
<tr>
<td>Details</td>
<td>View certificate data</td>
<td>The data can be used in a variety of ways, one of which is using the digests to verify the certificate's origin.</td>
</tr>
<tr>
<td>Revocation</td>
<td>Show certificate validity status as determined by the revocation check and provides an explanation of that status.</td>
<td>Signer Details: Open the certificate viewer for the selected certificate. The button is only active if the certificate is not a trusted root. Problems encountered: View a description of the problems with the revocation checking. The button is only active if revocation checking occurred but failed. Check revocation: Enables manual revocation checking. The button is only active if no checking occurred.</td>
</tr>
<tr>
<td>Trust</td>
<td>Lists the user-specified certificate trust settings</td>
<td>The certificate can be added to the Trusted Identity list.</td>
</tr>
<tr>
<td>Policies</td>
<td>List policy OIDs associated with this certificate, if any. Describes the policy</td>
<td>View policy details.</td>
</tr>
<tr>
<td>Legal Notice</td>
<td>Displays a generic legal disclaimer, the certificate issuer's policy statement, issuer notice, and link to the policy, if any.</td>
<td>If an issuer policy is used, the policy can be displayed.</td>
</tr>
</tbody>
</table>

Displaying a Certificate in the Certificate Viewer

When a certificate is displayed in the certificate viewer, you can check certificate validity, trust settings, associated policies, and other details that help you establish the owner’s identity. The Certificate Viewer provides six tabs that displays certificate data and allows you to manage that certificate on your system (Table 1).

1. Choose **Advanced > Trusted Identities**.
2. Choose **Certificates** in the **Display** drop down list.

**Note:** In addition 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 32 Certificate Viewer**

Verifying Self-Signed Certificates

Certificates are usually issued by a trusted, third-party certificate authority such as Verisign. However, anyone can set up a certificate authority or create a self-signed certificate purporting to be anyone else. It is even possible to create a certificate authority that claims to be Verisign. It is therefore recommended that users verify a certificate’s origin. After the origin is verified, use the Trusted Identity Manager to specify
certificate trust settings so that it can be used as a trusted root, to certify documents, and so on. For details, see “Certificate Trust Settings” on page 41.

Tip: For self-signed certificates or those issued by unknown or untrusted certificate authorities, it is prudent to verify the certificate owner’s identity before being added to them trusted identity list.

To verify the origin of the certificate:

1. Display the certificate in the Certificate Viewer:
   - If the certificate is embedded in a signature, right click on the signature, choose Properties, display the Summary tab, and choose Show Certificate.
   - If the certificate is in an FDF file attached to an email sent from Acrobat, double-click the attached file, and choose Certificate Details in the Import contact settings dialog.

Tip: Double clicking a file other than an FDF will likely install the certificate in the Windows Certificate Store. If the file is .cer, .p7b, or some other format, save the file locally and import it into the Trusted Identity Manager as described in “Browsing for a Trusted Identity” on page 34

2. Display the Details tab.

3. In the Certificate data panel, scroll to MD5-digest and SHA-1 digest and note the numbers.

4. Contact the certificate’s originator and verify the MD5-digest and SHA-1 numbers are correct.

5. After the certificate is verified, display the Trust tab and add the certificate to the trusted identities list.

Checking Certificate Revocation Status

Only the certificate issuer (a certificate authority) has the right to revoke a certificate, and Acrobat’s check of the revocation status is part of its public key authentication. There are a number reasons why a certificate might be revoked: its security might be compromised, it could be invalid for some reason, or the owner of the ID might have left the company.

To check a certificate’s revocation status:

1. Choose the Revocation tab.

2. Choose Check Revocation. The certificate details appear in the Details panel.
3. Choose **OK**.

![Figure 34 Trusted Identities: Viewing revocation status](image)

**Figure 34 Trusted Identities: Viewing revocation status**

### Trusting Timestamp Authority Certificates

Certificates can be used with a timestamp server and timestamps to associate a particular time and date with a signature. These certificates are typically issued by a third-party timestamp authority. The workflow for importing, validating, and setting trust levels for timestamp certificates is generally the same as those for using certificates with signatures.

For details, see the following:

- “Importing a Single Certificate From an FDF File” on page 36
- “Verifying Self-Signed Certificates” on page 38
- “Timestamp Basics for Authors” on page 91
Certificate Trust Settings

Each contact in the trusted identity list should be associated with one or more certificates. Certificate trust settings may be individually configured as needed. Users can specify whether a certificate received from someone else should be trusted for certain actions. Choosing to not trust a certificate does not prevent a document from displaying, but it can limit what that document can do and whether a signature is valid. Signatures and timestamps associated with valid but untrusted certificate appear with a question mark (Figure 35). One of a contact’s certificates can also be selected as the default for encryption.

Certificate trust settings have the following features:

- Trust settings are configured in the Trusted Identity Manager or at the time of import.
- Trust setting can be viewed in Trusted Identity Manager by choosing Edit Trust (Figure 37) or by choosing the Trust tab in the Certificate Viewer (Figure 36).
- Certificates can be separately trusted for approval signatures and certification signatures.
- Dynamic content and JavaScript can be configured to run on a per-certificate basis, but these settings interact with the application's environment settings.

Trusting a Certificate for Signing and Certifying

To sign or certify a document the signer must have a digital ID with a certificate. In order for ordinary and certification signatures to be valid, the certificate must be valid and it must be explicitly trusted for these operations or chain up to a trusted root which is.

To trust a certificate for signing and certifying:

1. Choose **Advanced > Trusted Identities**.
2. Choose **Certificates** in the **Display** drop down list.
3. Select the certificate.
4. Choose **Edit Trust**.

5. Display the Trust Settings tab.

6. Set the certificate’s trust settings:
   - **Signatures and as a Trusted Root**: Trusts the certificate as a trusted root for approval signatures. The net result is that any other certificates which have this one as a root in the chain will also be trusted for signing. At least one certificate in the chain (and preferably only the root in the chain) must be a trusted root to validate signatures and timestamps certificates.
   
   **Tip**: There is no need to make end entity or intermediate certificates trusted roots if they chain up to trusted root. It is best practice to only trust the topmost certificate as the root because revocation checking occurs on every certificate in a chain until the root is reached. For example, if you have a certificate which chains up to your company’s intermediate certificate which in turn chains up to Verisign, you would only make Verisign a trusted root and NOT your company’s, your own, or any of your coworker’s certificate’s.
   - **Certified Documents**: Trusts the certificate for certification signatures.
   - **Dynamic Content**: Not recommended for certified documents. Trusts movies and other dynamic content. This option requires that the application environment be configured correctly. For more information, see “Trusting Dynamic Content in Certified Documents” on page 42.
   - **Embedded High Privilege JavaScript**: Not recommended for certified documents. Trusts embedded scripts. This option requires that the application environment be configured correctly. For more information, see “Trusting JavaScript in Certified Documents” on page 43.

7. Choose **OK**.

8. Choose **OK**.

**Trusting Dynamic Content in Certified Documents**

Whether dynamic content runs in certified documents depends on whether the document recipient has explicitly trusted the sender’s digital ID for such actions. Recipients can set the application to run JavaScript generally, but they can also control for certified documents JavaScript execution on a per-certificate basis.

It is also possible to trust a root certificate for these actions. Any certificate that chains up to that root will share its trust settings. For example, some enterprises may issue a MyCompany certificate that trusts
dynamic content. If all employee certificates use MyCompany as a root, then they can send and receive certified documents within the company that contain working dynamic content.

**Tip:** Because dynamic content represents a security risk and could potentially change the document’s appearance, it is recommended that participants in certified workflows do not allow multimedia.

To allow dynamic content to execute in certified documents:

1. Configure the application environment to run multimedia as described in “Setting Dynamic Content (Multimedia) Security Options” on page 63.
2. Trust the certificate associated with the certification signature for multimedia as described in “Trusting a Certificate for Signing and Certifying” on page 41.

### Trusting JavaScript in Certified Documents

Whether JavaScript is executed in certified documents depends on whether the document recipient has explicitly trusted the sender’s digital ID for such actions. Recipients can set the application to run JavaScript generally, but they can also control for certified documents JavaScript execution on a per-certificate basis.

It is also possible to trust a root certificate for these actions. Any certificate that chains up to that root will share its trust settings. For example, some enterprises may issue a MyCompany certificate that allows JavaScript. If all employee certificates use MyCompany as a root, then they can send and receive certified documents within the company that contain working JavaScript.

**Tip:** Because scripts represent a security risk and could potentially change the document’s appearance, it is recommended that participants in certified workflows do not allow JavaScript to run.

To allow JavaScript to execute in certified documents:

1. Configure the application environment to run JavaScript as described in “Setting High Privilege JavaScript Security Options” on page 65.
2. Trust the certificate associated with the certification signature for JavaScript as described in “Trusting a Certificate for Signing and Certifying” on page 41.

### Selecting a Certificate to use for Encryption

In order to encrypt a document that can be decrypted by a document recipient, it is necessary to explicitly trust their certificate for encryption. Note that 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:** You can only use certificates for encryption that have encryption usage rights and are valid (not expired). Acrobat displays a warning dialog during the encryption process if the selected certificate cannot be used.

To set a default certificate for encryption:

1. Choose **Advanced > Trusted Identities**.
2. Choose a contact in the left-hand list (**Figure 39**).
3. Choose **Details**.

4. Highlight a certificate in the certificate list. Use the certificate that person tells you to use.

5. Choose **Use for encryption** (Figure 38). The lock icon moves to the selected certificate.

6. Choose **OK**.
Managing Contacts

Contacts are typically 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.

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 > Trusted Identities**.
2. Choose a contact in the left-hand list.

   **Figure 39 Contacts: Viewing details**

3. Choose **Details**.

   **Figure 40 Edit Contact dialog**

4. Edit the details as required.
5. Choose OK.

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 to their trusted identity list, thereby expanding the number of users that can participate in secure document workflows. For details, see “Emailing Your Digital ID Certificate” on page 95.

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, thereby expanding the number of users that can participate in secure document workflows. For details, see “Saving Your Digital ID Certificate to a File” on page 97.

Associating a Certificate with a Contact

A certificate is usually already associated with a contact and contact details. 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 > Trusted Identities.
2. Choose a contact in the left-hand list (Figure 39).
3. Choose Details.
4. Choose Associate Certificate (Figure 40).

5. Select a certificate from the list.
6. Choose OK.
7. Choose OK.
Changing a Trusted Identity’s Certificate Association

In Acrobat, contacts in the Trusted Identity Manager only have value when they are associated with certificates that are used in encryption and signing workflows. 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 > Trusted Identities**.
2. Choose a contact in the left-hand list (**Figure 39**).
3. Choose **Details**.
4. Choose a certificate from the list.
5. Choose **Remove Association** (**Figure 42**).
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 42  Edit Contact dialog**

Deleting Contacts and Certificates

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

- You now longer share documents with a trusted identity, and so delete both the contact and certificate.
- The trusted identity’s contact information or certificate has changed and new data will be imported.
- The contact information has changed so only it is deleted. The certificate is associated with a new contact.
To delete a contact (and optionally a certificate):

1. Choose **Advanced > Trusted Identities**.

2. Choose Contacts from the **Display** drop down list.

3. Choose a contact in the left-hand list (**Figure 39**).

4. Choose **Delete**.

5. Choose whether or not to delete the certificate along with contact.

6. Choose **OK**.

**Figure 43 Contacts: Deleting**

**Deleting a Certificate**

To delete a certificate:

1. Choose **Advanced > Trusted Identities**.

2. Choose Certificates from the **Display** drop down list.

3. Choose a certificate in the left-hand list (**Figure 40**).

4. Choose **Delete**.

5. Choose **OK**.
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 or 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.

Creating a Group

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

To create a group:

1. Choose **Advanced > Trusted Identities**.
2. Choose **New Group**.
3. Enter a group name (Figure 44).
4. Add contacts as needed.
5. Choose **OK**.

Adding or Removing Group Contacts

To add or remove group members:

1. Choose **Advanced > 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 44 Contacts: Editing a group*
Deleting a Group

To delete a group:

1. Choose Advanced > Trusted Identities.
2. Choose a group in the left-hand list (Figure 39).
3. Choose Delete.
4. Choose OK.

Using Groups with Security Policies

Certificate and APS security policies can be applied to an entire group. Public key certificate policies applied to groups are typically stored in the author's local Trusted Identity Manager. Adobe Policy Server policies that are applied to groups are stored on the Adobe Policy Server. For details, see “Applying a Security Policy to a Group” on page 173.
Using Directory Servers to Add Trusted Identities

Businesses that use certificates to identify participants in signing and secure workflows often need a single repository for those certificates. Locating in one place that part of a user’s digital ID that is shared across the organization (the public certificate), simplifies management for the administrator and certificate sharing for employees.

Directory servers are LDAP servers that are capable of returning x.509 public key certificates. These servers are certificate repositories that users search to expand their list of trusted identities. Both Adobe Acrobat and Adobe Reader ship with three default servers:

- VeriSign Internet Directory Service
- GeoTrust Directory Service
- IDtree Directory Service

Home users may never need to search or add directory servers. In most cases, needed certificates will be sent directly to you or will be embedded in a signature. However, users in enterprise environments will likely use directory servers when their company administrator has set up an LDAP server as part of their 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, sends the server configuration details in an FDF file so that Acrobat can automatically import them, or tells the user how to configure the server manually.

Figure 46 Digital ID Directory servers: Server list

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.

To configure an identity directory:

2. Select Directory Servers in the left-hand list (Figure 46).
3. Choose New.
4. Configure the LDAP server settings in the Edit Directory Server dialog:

**Tip:** Contact the system administrator for the server details.
- **Directory Name:** The directory to search.
- **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 pair container objects used in the search. For example, `c=us, cn=John West, ou=Engineering, dc=example, dc=com`, representing country, common name, organizational unit, and domain component respectively.
- **This server requires me to log on:** Check if the server requires a username and password.
- **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. Records may include users, users with multiple certificates, and so on.

5. Choose **OK**.

**Figure 47 Digital ID Directory servers: Setting server details**

![Digital ID Directory servers: Setting server details](image)

**Editing Directory Servers Details**

Directory server details can be changed at any time.

To edit directory server information:

1. Choose **Advanced > Security Settings**.
2. Select **Directory Servers** in the left-hand list (Figure 46).
3. Select a directory server from the right-hand panel.
4. Choose **Edit**.
5. Change the information as required. For details, see “Manually Configuring a Directory Server” on page 51.

6. Choose OK.

Deleting a Directory Server

Previously configured directory servers containing digital IDs can be removed at any time.

To delete a directory server:
2. Select Directory Servers in the left-hand list (Figure 46).
3. Select a directory server from the right-hand panel.
4. Choose Remove.
5. When a confirmation dialog appears, choose OK.

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:
2. Select Directory Servers in the left-hand list (Figure 46).
3. Select a directory server from the right-hand panel.
5. Choose OK if a confirmation dialog appears.
   A star appears next to the name of the selected server.
Importing and Exporting Directory Server Settings

For details, refer to the following:

- “Importing Directory Server Settings via FDF” on page 194
- “Emailing Server Details via FDF” on page 206
- “Exporting Server Details via FDF” on page 207
End users that receive signed documents typically need to validate the document signature. Since a signature may not be valid for a number of reasons, it is useful to understand what signature components are involved in determining a signature’s validity. Such knowledge aids troubleshooting and manual validation tasks. Moreover, participants in signing workflows may want to configure their environment to streamline the validation process and control what kinds of content can be run on their machine. For more information, refer to the following:

- “Working with Signed Documents” on page 56
- “Setting up Your Environment for Receiving Documents” on page 59
- “Validating Signatures Manually” on page 66
- “When the Status Icon is Not a Green Check…” on page 71
- “Timestamp Basics for Document Recipients” on page 74
- “Viewing and Comparing Document Changes and Versions” on page 76
Signature Components: What Makes them Valid?

A signed document consists of three main components: the original document, the signature, and the signer’s certificate (Figure 50). In order to participate effectively in signing workflows (or even comprehend the meaning of validated signature icons), users should understand the origin of each component and how that component’s state can affect a signature's validity:

- **The original, unsigned PDF.** The document author creates the PDF. Signing creates a message digest of the current document. Every time a document is signed, a new digest is created. Thus, each signature is only valid for a specific version of the document.

  How does a document current state affect signature validity? If the document changes after signing, its integrity is compromised and the signature may become invalid.

- **The signature.** Acrobat creates a hash (number representation) of the original document. The number is encrypted with a private key and turned into a “signed message digest.” Both the digest and the signature appearance are embedded in the document.

  How determines signature validity? When a document recipient validates a signature, a new message digest is created and compared to the old message digest that was embedded in the document at the time of signing. If the two digests are not identical, the signature may become invalid. Signature validity is also dependant on the validity of the signer’s certificate.

- **The signer’s certificate.** A signer must have a digital ID that includes an X.509 compliant certificate and a private key and a public key that is shared. The private key is used to encrypt the message digest.

  How does certificate status affect signature validity? It must chain up to a trusted certificate authority and at the time of signing must not have been revoked.

Note that signature validity depends on all three of these components. The embedded certificate provides the information needed to verify the signer’s identity. The original document and the embedded message digest are used to verify that the document has not changed since it was signed. Optional components such as embedded revocation information or a timestamp may also reside in a signature. When a signature is invalid, the signer’s identity cannot be verified, or there is some other problem, the signature validator is warned.
Signature Status and Validity Icons

By default, signatures are validated automatically when a document opens. For details, see “Setting Up Automatic Signature Validation” on page 59. A Signature's status is represented by status icons and text both on the document page and the Signatures tab. The state is determined (or verified) by checking the signature's digital ID certificate status (is it valid) and document integrity (has it changed since being signed). A signature's state can be either valid, unknown, or invalid (Table 2):

- **Valid** signatures are associated with a valid certificate and the document has only changed in ways specifically permitted by the author.
- **Unknown** signatures are associated with certificates that cannot be validated or with a document that contains unknown changes or is in an unverified state.
- **Invalid** signatures either have an invalid certificate or the document has changed in ways specifically disallowed by the its author.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Certificate status: Valid. The signature was the first signature in the document. For details, see “Certifying a Document (Certifying Signatures)” on page 65. and Document integrity status: The document has not changed since it was signed or has only changed in ways specifically permitted by the person who certified the document.</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Valid Icon" /></td>
<td>Valid</td>
<td>Certificate status: Valid. The signature was the first signature in the document. For details, see “Certifying a Document (Certifying Signatures)” on page 65. and Document integrity status: The document has not changed since it was signed or has only changed in ways specifically permitted by the person who certified the document.</td>
</tr>
</tbody>
</table>
### Table 2 Digital signature icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Certificate and document status</th>
</tr>
</thead>
</table>
| ![Checkmark] | Valid | **Certificate status:** Valid.  
	**Document integrity status:** The document has not changed since it was signed or only contains changes allowed by a previous signer, if any. |
| ![Exclamation] | Change view | **Certificate status:** Valid. This icon may appear in a certified document, but it is never used for a certification signature. Therefore, it only appears for ordinary (and not the first) document signature.  
	**Document integrity status:** The document has changed since it was signed. The current view of the document is not the same as that which was signed. View the signed version to see what was signed. For details, see “Viewing and Comparing Document Changes and Versions” on page 76 |
| ![Alert] | Unknown | **Certificate status:** Unknown: The certificate has not been trusted (and is not untrusted), the revocation check could not complete, a chain could not be built to trust anchor, and so on.  
	**Document integrity status:** The document has changed since it was signed. The document the user is viewing is not the signed version. |
| ![Alert] | Unknown | **Certificate status:** Unknown: The certificate has not been trusted, the revocation check could not complete, a chain could not be built to trust anchor, and so on.  
	**Document integrity status:** The document has not changed since it was signed. |
| ![Alert] | Unknown | **Certificate status:** Unverified. The certificate validation check has not executed or could not complete.  
	**Document integrity status:** Unverified. The document integrity check has not executed or could not complete. |
| ![X] | Invalid | **Certificate status:** The signer's certificate was invalid.  
	or  
	**Document integrity status:** Illegal changes have been made to the document. |
Setting up Your Environment for Receiving Documents

Document recipients should configure their environment to handle incoming documents in a way that enhances secure and efficient workflows. While Adobe Acrobat and Adobe Reader provide default options, customizing the environment often provides a better user experience. In large, enterprise environments, your environment may be preconfigured by your system administrator. Options include the following:

- **Setting Up Automatic Signature Validation**: If signatures should be validated automatically when a document opens, turn this option on.
- **Setting Digital Signature Validation Preferences**: Configure validation methods such as plugin usage, time display, automatic revocation checking, and so on as needed.
- **Configuring Document Status Preferences**: Participants in secure workflows should turn on (or leave on) the Status dialog in order to view document status information about certificate validity, document integrity, and so on.
- **Setting Dynamic Content (Multimedia) Security Options**: When certified documents may contain multimedia, specify whether or not it is allowed to run in untrusted and untrusted documents.
- **Setting High Privilege JavaScript Security Options**: Certain Adobe JavaScripts are defined as “high privilege.” If certified documents may contain high privilege JavaScript, set your preferences as needed.

### Setting Up Automatic Signature Validation

Advanced digital signature preferences apply to all digital signatures in all documents.

The only reason a user might NOT want to verify a signature is to gain a small increase in application speed when Acrobat document is opened. However, because the difference is negligible, it is advisable to always verify signatures. Verification tells the user two things:

- That the document signed by someone with a valid certificate. (The signer is really who we think it is.)
- The document has not changed in a way that invalidates the signature.

To set advanced digital signature preferences:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Choose **Security** in the left-hand list.
3. Check **Verify signatures when document is opened**.

**Tip**: Verifying a signature is somewhat similar to credit card validation—it is simply the act of verifying that the signature uses a valid certificate.

### Setting Digital Signature Validation Preferences

Verification tab options let you specify how a signature is validated. You can select the validation plugin, default validation methods, whether or not certificate revocation checking is automatic, what time is associated with a validated signature, and whether or not a valid icon will appear if the signature is valid.

To set advanced digital signature preferences:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Choose **Security** in the left-hand list.

3. Choose **Advanced Preferences**.

4. Display the Verification tab.

   Figure 51 Digital Signatures Advanced Preferences: Signature verification

5. Select the signature validation method:
   - **Use the document-specified method, prompt if it is not available.**
   - **Use the document-specified method, use the default method if it is not available.**
   - **Always use the default method (overrides the document-specified method).**

   Signatures are created and validated by plugins. These options specify which plugin is used to verify a signature. Both Acrobat and Adobe Reader provide a default plugin for signing documents and verifying signatures. While the signing and verification plugin are usually the same, this is not always the case, though a signature usually “knows” what plugin is required to verify it. Businesses sometimes create custom plugins that can understand a unique format or extra data. Contact your system administrator for details.


7. Check or uncheck **Require that Certificate revocation checking be done whenever possible when verifying signatures**

   This option checks certificates against a list of revoked certificates during validation, either with the Online Certificate Status Protocol (OCSP) or the Certificate Revocation List (CRL). If this option is not selected, the revocation status for approval signatures is ignored. **Certificates associated with certification signatures will still be verified.**

   **Note:** Signature verification is similar to credit card validation. OCSP checking is like making a phone call to verify the card number. CRL checking is like checking the card numbers against a list.

8. In the Verification Time panel, select a time verification method:
   - **Current time:** The digital signature validation time.
   - **Secure time:** The default timestamp server time specified in the Security Settings dialog.
- **Creation time**: The signature creation time.

9. Check or uncheck **Hide signature field validity icon when the signature is valid**: The icons are useful for rapidly determining signature status (Table 2).
   Icons cannot be hidden for invalid signatures.

10. Choose **OK**.

11. Choose **OK**.

**Configuring Document Status Preferences**

For certain types of documents, Acrobat displays a Document Status dialog when a document is opened. For example, the dialog provides information about the document, certification status, whether or not signatures are valid, and so on.

It is recommended that users turn on (or leave on) the document status dialog when participating in workflows that use signatures and security methods. The dialogs provide details about document security features, signer and certificates (if any), whether or not a signature is valid, and so on. Moreover, for certified documents, the Status dialog links to the legal notice and signature properties dialog.

![Figure 52 Document Status dialog: for Signed and encrypted document](image)
To enable or disable the Document Status dialog on startup:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).

2. Choose **Startup** in the left-hand category list.

---

**Figure 53 Document Status dialog: for certified document**

![Document Status dialog](image)

**Figure 54 Document status preferences**

![Preferences dialog](image)
3. When the Opening Documents panel appears, check or uncheck Display the Document Status dialog checkbox (Figure 54).

4. Check or uncheck Certified documents or Signed documents.
   The dialog may also be permanently turned off in the application for documents signed with an author signature by checking the Do not show this dialog next time when the dialog first appears.

5. If the status dialog is turned off for certified documents, an alert appears. Choose Yes.

Setting Dynamic Content (Multimedia) Security Options

Trust Manager preferences provide multimedia display permissions for both trusted documents and untrusted documents. Permissions are independently set for each document type. As described in “Trusting Dynamic Content in Certified Documents” on page 42, recipients of certified documents can control on a per-certificate basis whether a document uses the trusted or untrusted settings. By definition, a certified document is trusted for dynamic content if the certificate associated with the certification signature is trusted for running dynamic content. The behavior is as follows:

- If the certificate trust settings allow dynamic content, the Trust Manager’s Trusted Document settings are used.
- If the certificate trust settings do not allow dynamic content, the Trust Manager’s Untrusted Document settings are used.

**Tip:** Because dynamic content represents a security risk and could potentially change the document’s appearance or allow security holes in multimedia players to adversely impact your system, it is recommended that participants in certified workflows do not allow multimedia. Consider the source of the document and the security of the workflow before enabling this option.

**Caution:** A document will use the Trusted Document settings if it trusted to allow multimedia at anytime. For example, if you open an unsigned document, are prompted to play the media, and you choose yes, then the document is automatically added to a hidden trusted document list. Documents in that list override certificate trust settings. Therefore, these documents may not always exhibit the expected behavior.

To configure multimedia behavior:

1. Choose Edit > Preferences (Windows) or Acrobat > Preferences (Macintosh).

2. Select Trust Manager in the left-hand tree.
3. From the **Display Permissions for** drop down list, choose **Trusted documents** or **Non-trusted documents**.

4. The Trust Manager displays the select document type’s trust settings (**Figure 55**).

5. Configure the Multimedia Permission Settings 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.
      
   4. Choose **OK**.
Setting High Privilege JavaScript Security Options

This option controls whether high privilege JavaScript can be executed from custom menu items in the Acrobat toolbar. As described in “Trusting JavaScript in Certified Documents” on page 43, document recipients can set whether or not to execute JavaScript on a per-certificate basis. However, 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.

**Tip:** Because scripts could potentially change the document’s appearance or allow attackers access to your system, it is recommended that participants in certified workflows do not allow JavaScript to run. Consider the source of the document and the security of the workflow before enabling this option.

To choose to execute or block execution of all JavaScript from the toolbar:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select **JavaScript** in the left-hand tree.
3. Check or uncheck **Enable menu items JavaScript execution privileges**.
4. Choose **OK**.

**Figure 56 JavaScript Security option**

<table>
<thead>
<tr>
<th>JavaScript Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>○ Enable menu items JavaScript execution privileges</td>
</tr>
</tbody>
</table>

High Privilege JavaScript Defined

High privilege JavaScript are Acrobat methods with security restrictions. These are marked by an S in the third column of the quick bar in the *Acrobat JavaScript Scripting 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 by the document author for 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 *Acrobat JavaScript Scripting Reference*. 
Validating Signatures Manually

Unless the application is configured to do otherwise, signatures are validated automatically when a document opens. If they are not validated or if a signature needs to be revalidated, you can validate one or more signatures manually. Before validating a signature, it is a good idea to understand what a signature is and how signature status is indicated. For details, see the following:

- “Signature Components: What Makes them Valid?” on page 56
- “Signature Status and Validity Icons” on page 57

Validating a signature allows you to verify the signer’s identity and determine whether the displayed document is identical to what was signed (or only allowed changes were made):

- Identity verification confirms the signer’s certificate or one of its parent certificates exists in the list of trusted identities and is not expired or revoked.
- Document integrity verification confirms that the signed content hasn’t changed since signing or that it has only changed in ways specifically permitted by the signer. Signatures can be validated one at a time or all at once.

Ideally, validation results in a green check mark being associated with the signature either on the signature itself or in the Signatures tab (Figure 57).

Figure 57  Valid digital signature

Validating a Single Signature

Signatures can be validated one at a time or all together as described in “Validate all signatures dialog” on page 67. Signature validity can be determined by viewing its associated icon (Table 2). A green checkmark indicates the signature is valid without reservations. Other icons indicate there may be a problem.

There are several ways to verify a signature manually:

- Right click on any signature in the Signatures tab or in the document, and choose Validate Signature.
- Right click on any signature in the Signatures tab or in the document, and choose Properties. When the Signature Properties dialog appears, choose Verify Signature.
- Double click a signature and choose Signature Properties. When the Signature Properties dialog appears, choose Verify Signature.
- Highlight a signature in the Signatures tab, and choose Document > Digital Signatures > Validate Signature.
Validating All Signatures Simultaneously

Multiple signatures may be validated simultaneously. This feature is particularly useful if the auto-validate option has been turned off.

To validate all signatures:

1. Choose **Document > Digital Signatures > Validate All Signatures in Document**. A dialog appears asking if all signatures should be validated.

   **Figure 59 Validate all signatures dialog**

2. Choose **OK**.

3. When a dialog appears confirming all signatures have been validated, choose **OK**.

   **Figure 60 Signature validation confirmation**

Validating an Unknown (Untrusted) Signature

If a signer's digital ID has not been explicitly trusted, the signer is untrusted and the signer's signature validity will be **UNKNOWN**. When a document contains a signature that is associated with an untrusted ID certificate then, it appears with a question mark icon (**Figure 61**).
When a signer has not been trusted ahead of time, you can set their trust level directly from their signature. After their ID (contact information and certificate) is added to your list of trusted identities, the signature can be validated. Acrobat displays the document's content according to the associated certificate's trust settings. For details, see “Certificate Trust Settings” on page 41.

To add an unknown identity to a list of trusted identities:

1. Display the Signature Properties dialog (See “Displaying the Signature Properties Dialog” on page 71).
2. Choose the Summary tab (Figure 61).

   **Tip:** If you are validating a timestamp certificate, choose **Show Certificate** from the Date/Time tab INSTEAD of the Summary tab (Figure 69).

   **Figure 61  Signature Properties: Summary**

   ![Signature Properties Dialog](image)

3. Choose **Show Certificate**.

   Adding an unverified digital ID certificate to the trusted identity list could pose a security threat. This is particularly true for self-signed IDs that are not issued by a third-party certificate authority. For details, see “Verifying Self-Signed Certificates” on page 38.

4. When the Certificate Viewer appears, choose the Trust tab (Figure 62).
5. Choose an item in the left-hand certificate path field. There may be one or more certificates which make up a certificate chain.

   **Tip:** If the bottom-most certificate on the chain is selected, then only that certificate will be trusted. If the top-most certificate is selected, then any certificates having that certificate as a root will be trusted. For example, if the root certificate is from Verisign and it is trusted, then any certificates having Verisign's certificate as the root will also be trusted. It is a best practice to trust the topmost certificate as possible. Revocation checking starts at the bottom of a chain (begins with the end entity), and once it reaches a trusted root revocation checking stops.
6. Choose **Add to Trusted Identities**.

7. When asked if the certificate should be trusted from within the document, choose **OK**.

![Figure 62 Certificate viewer: Trust tab](image1)

8. When the Import Contact Settings dialog appears, configure the Trust Settings and Policy Restrictions. For details, see “Certificate Trust Settings” on page 41.

   The Policy Restrictions tab will not appear if there are no policies associated with this certificate.

9. Choose **OK**.

10. Choose **OK**.

11. Choose **Close**.

12. Right click on the signature and choose **Validate**.

   **Note:** The question mark icon on the signature will not change until the signature is revalidated.
Validating a Signature for an Earlier Document Version

Signed documents contain both a signature and any subsequent versions of that document. In other words, Acrobat and Adobe Reader “remembers” that version A is signed, that changes were made to version B, and so on. When you open a document, the latest version is always displayed. However, it is often necessary to view the signed version in order to see what content was actually signed. When the viewed version is not the signed version, the signature with either be valid with a warning or unknown.

To view the signed version of a document.

1. Display the Signature Properties dialog (See “Displaying the Signature Properties Dialog” on page 71).
2. Choose the Document tab.
4. Revalidate the signature if necessary.
When the Status Icon is Not a Green Check... 

Ideally, signature validation should result in the display of a green check and pen icon for approval signatures or a blue ribbon icon for certification signatures. If it does not, the signatures have not been successfully validated and you should troubleshoot the problem. The type of problem is identified by the icon. For details, see the following:

- “Green Check and Caution Triangle” on page 71
- “Question Mark and Caution Triangle” on page 72
- “Question Mark and Person” on page 72
- “Question Mark and Pen” on page 73
- “Red X and Pen” on page 73

A key tool for troubleshooting signatures is the Signature Properties dialog. The dialog provides five tabs that display signature information and buttons for performing document validation tasks. It also provides a Show Certificate button for invoking the Certificate Viewer. The viewer provides certificate-specific information and buttons for performing certificate validation tasks. Together, the Signature Properties dialog and Certificate Viewer should provide you with enough information to either successfully validate a signature or reject the document as insecure.

**Displaying the Signature Properties Dialog**

There are several ways to invoke the Signature Properties dialog:

- Double click an approval signature and choose Signature Properties.
  - **Note**: Certified signatures that were created in a locked, read-only field do not have access to dialogs invoked by double clicking on a signature. Since certification signature fields are locked by default, use the “right click” method described below.
- Right click on any signature in the document or the Signatures tab and choose Properties.
- Right click on any signature in the Signatures tab and choose Properties.

**Green Check and Caution Triangle**

A green check with a caution triangle means that the signature is valid but that the document has changed since it was signed. The current view of the document is not the same as that which was signed. This icon may appear in a certified document, but it is never used for a certification signature.

To change the icon, simply view the document version that is associated with that particular signature:

1. Right click on a signature and choose View Signed Version. Acrobat opens the signed version of the document.
2. Revalidate the signature if necessary.
Question Mark and Caution Triangle

A question mark with a caution triangle means that the certificate validity is unknown and that the document has changed since it was signed. The question mark means you have not trusted the certificate, the revocation check could not complete, a chain could not be built to trust anchor, and so on. The caution triangle tells you that you are not viewing the signed version of the document.

To change the icon, add the signer to your trusted identity list and view the signed document version:

1. Specify the certificate's trust settings as described in “Trusting a Certificate for Signing and Certifying” on page 41.

2. Verify that a revocation check occurred. Open the Certificate Viewer’s Revocation tab (right click on a Signature, choose Properties and then Show Certificate). Check the following:
   - If revocation checking occurred, Problems encountered is active and you can select the button to view a description of the problems.
   - If revocation checking did not occur at all, Check revocation is active and you can select the button to check revocation manually.

3. Right click on a signature and choose View Signed Version. Acrobat opens the signed version of the document.

4. Revalidate the signature if necessary.

Question Mark and Person

A question mark with a person means that the certificate validity is unknown and that the document has not changed since it was signed. You have not trusted the certificate, the revocation check could not complete, a chain could not be built to trust anchor, and so on. Add the signer to your trusted identities list if needed; otherwise, contact the signer to troubleshoot possible problems with their digital ID.

To change the icon, add the signer to your trusted identity list:

1. Specify the certificate's trust settings as described in “Trusting a Certificate for Signing and Certifying” on page 41.

2. It may be that there was a certificate revocation checking. Open the Certificate Viewer’s Revocation tab (right click on a Signature, choose Properties and then Show Certificate). Check the following:
   - If revocation checking occurred, Problems encountered is active and you can select the button to view a description of the problems.
• If revocation checking did not occur at all, **Check revocation** is active and you can select the button to check revocation manually.

**Question Mark and Pen**

A question mark and a pen means that certificate validity and document integrity status are unverified because both the certificate validation check and the document integrity check did not successfully execute. The certificate could be OK may not be validated for the following reasons:

• If online revocation checking is required it may have failed as a result of no online access or an application problem.

• The **Verify signatures when the document is opened** preference might be turned off in **Edit > Security > Digital Signatures**, and no attempt was made to check certificate validity.

Similarly, the document may be changed in some unknown way. Manually validate the signature, and check document integrity to resolve or identify the problem.

To check certificate validity and document integrity:

1. Revalidate the signature as described in “Validating a Single Signature” on page 66.

2. Open the signed document version as described in “Viewing a Signed Version of a Document” on page 76.

3. Verify whether or not certificate revocation checking occurred. Open the Certificate Viewer’s Revocation tab (right click on a Signature, choose **Properties** and then **Show Certificate**), and check the following:

   • If revocation checking occurred, **Problems encountered** is active, and you can select the button to view a description of the problems.

If revocation checking did not occur at all, **Check revocation** is active, and you can select the button to check revocation manually.

**Red X and Pen**

A red X means that either the signer’s certificate is invalid or that illegal changes have been made to the document. There is no remedy that can occur for this document that would lead to a valid signature status icon. Since the signer’s certificate is embedded in the signature, if it is invalid, the signature will always be invalid. If illegal changes have been made to the document, there is no way to undo those changes without further changing the document illegally.

In both these cases, contact the sender to resolve the problem. The signer may need to get a new digital ID or make the signing workflow more secure so that the document cannot be changed after signing.

**Running JavaScript and Dynamic Content**

High privilege JavaScript and dynamic content in signed documents will only run if you have explicitly trusted the sender’s digital ID certificate for such actions. Because scripts and dynamic content represent a security risk, Acrobat prevents some of those operations by default. For details, see the following:

• “Trusting Dynamic Content in Certified Documents” on page 42

• “Trusting JavaScript in Certified Documents” on page 43.
Timestamp Basics for Document Recipients

All signatures are associated with the signer machine's local time, but they may also be associated with a timestamp provided by a timestamp server. Timestamps tell users that a document and signature existed prior to the indicated timestamp time. Since the timestamp is applied immediately after signing, if the signature is valid, it is likely that the document existed in its present state at the timestamped time and has not changed.

If a timestamp server is not configured, the time is simply taken from the local time on the computer. Because a user can set that time forward or back, this time is usually untrusted. Local times are labelled as such on the Date/Time and Summary tabs of the Signature Property dialog (Figure 66).

Note: If a signature appearance displays the time, that time will always be the local (computer) time. Therefore, if a timestamp server is configured, the time shown in the appearance is likely to be different from the time shown in the Date/Time tab on the Signature Properties dialog.

Figure 66 Timestamps: Local, machine time

Like signatures, timestamps become “trusted” when they are associated with a timestamp authority’s trusted certificate. Therefore, while a timestamp authority certificate could be provided by the user or a company timestamp server administrator, most timestamps are provided by third-party timestamp authorities such as GeoTrust.

In order to validate a timestamped signature, the user should add the timestamp authority’s certificate to the list of trusted identities. When a timestamp server certificate is not trusted, the timestamp is labelled as untrusted in the Signature Properties dialog and the signature verification is stamped with the machine time (Figure 67).

Figure 67 Timestamps: Untrusted stamp

Figure 68 Timestamps: Trusted stamp

Trust a Timestamp Certificate in a Signature

Certificates used by a timestamp authority to timestamp a signature are validated and trusted like any other certificate.

To trust a timestamp certificate:

1. Follow the steps described in "Validating an Unknown (Untrusted) Signature" on page 67.
2. Choose **Show Certificate** from the Date/Time tab INSTEAD of the Summary tab (Figure 69). After the timestamp is validated, the trusted timestamp will display a valid icon (Figure 68).

**Figure 69 Timestamps: Date/Time tab**

---

**When Timestamps Can’t be Verified. . .**

If a signature has a timestamp but it cannot be verified, make sure the following is true:

- A certificate is associated with the timestamp server. Choose **Advanced > Trusted Identities** and verify there is a certificate in the certificate list.

- The trust level of the certificate is set. Choose **Advanced > Trusted Identities**, choose a certificate and verify that the trust level is set. The certificate must either chain up to a trusted root (the recommended choice) or it must be specified as a trusted root.
Viewing and Comparing Document Changes and Versions

Document authors and recipients often need to know if a document has changed since it was signed. Acrobat keeps track of a document's version number, stores previous document versions in their entirety, and enables users to compare document versions by work and page. When you open a document, the latest version is always displayed. However, this may not always be the signed version. Document recipients should always remember the following:

- Every time a document is signed, the entire document with all changes are stored in the PDF.
- A signature is only valid for a specific document version. Signature X can be valid for version X, signature Y can be valid for version Y, and so on.

For details, see the following:
- **Document versions**: For details, see “Viewing a Signed Version of a Document” on page 76.
- **Post-signing modifications**: For details, see “Viewing a List of Post-Signing Modifications” on page 76.
- **Visual document changes**: For details, see “Comparing Documents” on page 77.

Viewing a Signed Version of a Document

Signed documents contain both a signature and any subsequent versions of that document. In other words, Acrobat and Adobe Reader “remembers” that version A is signed, that changes were made to version B, and so on. When you open a document, the latest version is always displayed. However, it is often necessary to view the signed version in order to see what content was actually signed. When the viewed version is not the signed version, the signature with either be valid with a warning or unknown.

To view the signed version of a document.

1. Right click on a signature and choose View Signed Version. Acrobat opens the signed version of the document.

2. Revalidate the signature if necessary.

Viewing a List of Post-Signing Modifications

Because it is possible to change a document without changing its appearance, the list of post-signing modifications is often a superset of what is visually displayed when comparing documents using Document Compare. Therefore, for the most thorough analysis of a signed document's integrity, create and view the document modifications list.

To view a list of post-signing modifications:

1. Right click on a signature and choose Properties.
2. Choose the Document tab.

3. Choose **Compute Modifications List**.

![Figure 71 Digital Signature Properties: Modifications panel](image)

**Comparing Documents**

As you revise a document and save it to a different name or location, you can verify that you have the latest version by comparing it against an older version. If you’re revising a document using comments you received during a review, you may need to view a previous version to make sure that you included all the revisions. As a reviewer, you may want to check the updated document against an older version to make sure that the author has incorporated all of your requested changes.

Document Compare finds and displays the differences in two versions of a document. Users can specify the type of differences to look for to verify that the appropriate changes have been made. Document Compare does not compare comments or other annotations in the document.

**Note**: Compare is not available in the Adobe Reader and is only available in the full version of Acrobat.

**Comparing a Signed Version with the Current Version**

To compare two versions of a document:

1. Choose **Document > Compare Documents**.

2. Specify two documents to compare through one of two ways:
   - Select **Choose**, browse to the needed file, and Choose **Open**.
   - If the documents are open, select them from a drop down menu. The drop down lists all OPEN files, NOT a list of recent files.

3. If a file has been signed one or more times, a **Revision** drop down list appears and each document revision will be listed. Select the revision as needed. The timestamp offers the most reliable chronological order of revision.

![Figure 72 Compare: Select file drop down menu](image)
4. Set the options in the Type of Comparison panel:
   - **Page by page visual differences (Compare pages):** Find textual or graphic differences between two documents by comparing each page's bitmap (document A's page one with document B's page one, document A's page two with document B's page two, and so on.) Select the required level of detail. The higher the sensitivity, the slower Compare Pages runs. For details, see “Comparing Documents by Page” on page 78.
   - **Detailed analysis:** High sensitivity compares at 72 dpi.
   - **Normal analysis:** Normal sensitivity compares at 36 dpi.
   - **Coarse analysis:** Low sensitivity compares at 18 dpi.
   - **Textual differences (Compare words):** to show which text has been inserted, deleted, or moved. Select Include Font Information to compare any formatting differences. For details, see “Comparing Documents by Word” on page 79.
   - Set the **Markup color** as desired.

   ![Compare: Type of comparison](image)

5. Set the options in the Choose Compare Report Type panel:
   - **Side by Side Report:** Creates a new document that displays the two documents in Continuous-Facing mode.
   - **Consolidated Report:** Adds markup where the differences occur in the current document. Placing the pointer over a markup in a consolidated report using the Hand tool displays the differences.
   - To compare text-based documents, select **Textual Differences** to appear in Side By Side Report format.

   ![Compare: Choose compare report type](image)

### Comparing Documents by Page

Compare completes by opening a temporary document that summarizes the differences. The first two pages summarize the changed, added, deleted, or moved pages, taking document A as the original and document B as the modified version (Figure 75).

The differences are displayed as follows:
   - Even numbered pages (the pages on the left on the two page document view) are pages from document A.
Odd numbered pages (the pages on the right on the two page document view) are pages from document B.

Pages that were moved are not shown in the report.

Any added page, which only exists in document B, is paired with a blank page in the report. Naturally, the added page will be on the right and the blank page will be on the left in the two-page view.

Any deleted page, which only exists in document B, is paired with a blank page in the report. Naturally, the deleted page will be on the left and the blank page will be on the right in the two-page view.

Pages that were in both documents but were modified are paired with each other in the report. There will be purple hexagons around regions in the two documents that were modified.

Pages that were not modified will not be in the report.

**Figure 75** Compare: By page summary report

**Figure 76** Compare: By page

---

**Comparing Documents by Word**

Acrobat can compare the document text rather than its visual appearance, including words that are deleted, added, and moved. For example, if a word in document A, say *Acrobat*, is changed to *Acrobatic*, Acrobat interprets this change as if the word *Acrobat* was replaced by *Acrobatic*. 
This reliance on a word level of granularity affects the way Acrobat detects moved blocks of text. Compare Words can only reliably detect moved strings of contiguous words at least four words long since this scheme breaks down when working with common words such as the or this. On the other hand, Compare Words can detect text blocks that were moved and changed as long as 92% of the text block stays the same.

Compare Words presents results using a temporary document with roughly the same layout as Compare Pages; that is, a two-page summary, followed by actual pages from both documents that differ, and so on. However, there are a few differences:

- The summary page displays the number of added, deleted, or moved words instead of the number of changed pages.
- In the actual document pages that differ, words that were deleted from document A are struck out; words that were added to document B are underlined.
- When a word’s position within the document has been moved, it will be highlighted in a user-specified color. Click on any text block of highlighted text on one document to see the two page view that shows the corresponding text block in the other document.

**Figure 77** Compare: Displaying changed text
Acrobat and Adobe Reader use FDF files to exchange data between the Acrobat family of client and server products. With FDF files, users can exchange digital ID data and Adobe Policy Server, directory server, and timestamp server settings. FDF files can be created on a server or by any Acrobat user. They can be shared in networked directories or sent as email attachments.

**Note:** FDF files use a .fdf extension, and like .pdf, it is registered by Adobe so that files with these extensions are opened by the required application when opened in a browser or file explorer.

Contact information and certificates associated with digital IDs can be easily shared with FDF files. Digital ID information can be exported and imported using workflows that rely on email or files on networked directories. Individual users can send and request digital ID data, and administrators can distribute FDF files with data for any number of users (groups) across an organization.

FDF files enable administrators (and any other user) to help end others configure their Acrobat installations by exporting directory and timestamp server settings to FDF files. 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:

- **Importing Acrobat Data**
  - “Responding to an Emailed Request for a Digital ID” on page 83
  - “Importing a Single Certificate via FDF” on page 83
  - “Importing Multiple Certificates via FDF” on page 84
  - “Importing Timestamp Server Settings via FDF” on page 86
• “Importing Directory Server Settings via FDF” on page 87
• “Importing APS Server Settings via FDF” on page 88

Exporting Acrobat Data
• “Distributing a Trust Anchor or Trust Root” on page 91
• “Emailing Your Digital ID Certificate” on page 95
• “Saving Your Digital ID Certificate to a File” on page 97
• “Requesting a Digital ID via Email” on page 97
• “Emailing Server Details via FDF” on page 99
• “Exporting Server Details via FDF” on page 100
Importing Acrobat Data

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

- By choosing **File > Open**.
- Double clicking on an FDF file (.fdf)
- For digital ID information, importing it into the Trusted Identity Manager.
- For server settings, importing it with the Security Settings dialog.

**Figure 78 Certificates: Email attachment**

![Image of a certificate email attachment]

Responding to an Emailed Request for a Digital ID

For details, see “Responding to an Emailed Request for a Digital ID” on page 12.

Importing a Single Certificate via FDF

Contact information and certificates may be exported from Acrobat, stored on local and networked directories, or sent as attachments in an email. Administrators often export certificate details to an FDF file that can be shared throughout a company. Individual users can also use FDF files to share certificates. Sharing this information ahead of time enables users to configure their trusted identities list all at once, on an as needed basis, or before receiving a signed document.

To add a contact and the contact’s certificate to the list of trusted identities:

1. Click on the FDF file or select the file and choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment (Figure 78) or may reside in a networked directory.

2. Review the contact information when the Import Contact dialog appears.

   **Note:** If the file is signed, then Import Contact dialog will also have a Signature panel as shown in Figure 80.
3. Choose **Set Contact Trust**.

4. When the Import Contact Settings dialog appears, configure the Trust Settings and Policy Restrictions. For details, see the user documentation.

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**.

### Importing Multiple Certificates via FDF

Contact information and certificates may be exported from Acrobat, stored on local and networked directories, or sent as attachments in an email. Administrators often export certificate details for multiple users to an FDF file that can be shared throughout a company. Sharing this information ahead of time enables users to configure their trusted identities list all at once, on an as-needed basis, or before receiving a signed document.

To add more than one certificate to the list of trusted identities all at once:

1. Click on the FDF file or select the file and choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment (**Figure 78**) or may reside in a networked directory.
2. Check or uncheck **Accept the level of Trust specified by the signer for all Contacts in this file.**

   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.

   **Note:** This step assumes a trust level has been specified by the sender.

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.
In most cases, timestamp servers do not have to be manually configured. Timestamp server administrators often place the server information to an FDF file. This file can be emailed or made available on a network.

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, or
   - Import it through the Security Settings dialog: Choose **Advanced > Security Settings**:
     1. Select **Time Stamp Servers** in the left-hand list.
     2. Choose **Import**.
     4. Choose **Open**.
     5. Review the sender’s details. Verify the signature properties if needed (**Figure 82**).

   **Note:** The FDF may be signed. If it is not, it will have no signature properties.
6. Review the timestamp server list. To avoid importing all servers, highlight those that should not be imported and Select Remove.

7. Choose Import.
   Default server information may have been exported with the FDF file. If one of the servers has been selected as a default, a dialog appears asking if the specified server should be used as the default.

8. Choose Yes or No.
   If No is selected, a default timestamp server must be selected before timestamps can be used.

9. After the import completes, choose OK.

Importing Directory Server Settings via FDF

Administrators and other users can export directory server settings to an FDF file. This file can be emailed or placed in a local or network directory. Users can import (add) directory server information through the Security Settings user interface 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, or
   - Import it through the Security Settings dialog: Choose Advanced > Security Settings:
     1. Select Directory Servers in the left-hand list.
     2. Choose Import.
     4. Choose Open.

5. Review the sender’s details. Verify the signature properties if needed (Figure 84).
   
   **Note:** The FDF may be signed. If it is not, it will have no signature properties.


7. If a confirmation dialog appears, choose OK.
   This dialog will not appear if Do not show this message again was previously selected.

8. Choose Close.
   The server settings are automatically imported and the new server should now appear in the directory server list.

**Importing APS Server Settings via FDF**

Administrators and other users can export APS server settings to an FDF file. This file can be emailed or placed in a local or network directory. Users can import (add) server information through the Security Settings user interface or simply by double clicking on the FDF file containing the data.
To add a server 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, or
   - Import it through the Security Settings dialog: Choose **Advanced > Security Settings**:

   1. Select **Adobe Policy Servers** in the left-hand list.
   2. Choose **Import**.
   4. Choose **Open**.

5. Review the sender’s details. Verify the signature properties if needed (**Figure 84**).

   **Note:** The FDF should be signed. If it is not, it will have no signature properties.

   **Figure 85 Importing APS settings**

6. Choose **Log In**.

   **Figure 86 Logging in to an Adobe Policy Server**

7. Choose **OK**.

8. Choose **Import**.
9. When a dialog appears asking whether or not you want to make this your default server, choose **Yes** or **No**.

10. Choose **OK**.

The server settings are automatically imported and the new server should now appear in the directory server list.
Exporting Acrobat Data

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 easily trust the file and its contents.

**Note:** Recipients won’t be able to validate your signature unless you have previously sent them your digital ID certificate.

**Figure 87 Signing an FDF file**

---

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 issued by a trusted Certificate Authority (CA). Certificates in between the end entity and root certificates are sometimes called “intermediate certificates” (ICAs). 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 higher up in the chain. For example, if the root certificate is trusted, then any certificates chaining up to the that root will also be trusted. Some organizations issue their own CA or ICA certificates and make them trust anchors for their employees.

It is a common practice to trust certificates as high up in the chain as possible. Since revocation checking starts at the chain bottom and continues until it reaches a trusted root, trusting the top-most certificate enables revocation checking for each certificate in the chain. It also allows users to trust other certificates that chain up to the same root. However, if the root is issued by 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.
Administrators may need to distribute and install ICA or CA trust anchors to users and individuals may need to distribute EE certificate for the same reasons:

- To distribute certified or signed documents to partners and customers.
- To enable public key encryption (certificate security) to restrict documents access to a known audience outside the enterprise.
- To help document recipients validate the signatures of document authors.

At a high level, the process for distributing a trusted anchor, CA, ICA, or EE certificate is always the same:

1. Setting the certificate's trust level for actions such as validating signatures, certifying documents, executing JavaScript, or enabling multimedia.

2. Exporting the desired certificate. When Acrobat exports a certificate, it automatically exports the other certificates in that certificate's chain and includes them in the FDF file.

3. Providing the certificate recipient with instructions for importing the certificate.

**Setting Certificate Trust Level**

Before distributing a trusted root, set the certificate trust level:

1. Choose **Advanced > Trusted Identities**.

2. Choose **Certificates** in the **Display** drop down list.

![Figure 88 Trusted Identities: Viewing](image)

3. Highlight the needed certificate.

4. Choose **Edit Trust**.

5. Display the Trust Settings tab.
6. Set the certificate’s trust settings:

- **Signatures and as a Trusted Root**: Trusts the certificate as a trusted root for approval signatures. The net result is that any other certificates which have this one as a root in the chain will also be trusted for signing. At least one certificate in the chain (and preferably only the root in the chain) must be a trusted root to validate signatures and timestamps certificates.

  **Tip**: There is no need to make end entity or intermediate certificates trusted roots if they chain up to trusted root. It is best practice to only trust the topmost certificate as the root because revocation checking occurs on every certificate in a chain until the root is reached. For example, if you have a certificate which chains up to your company’s intermediate certificate which in turn chains up to VeriSign, you would only make VeriSign a trusted root and NOT your company’s, your own, or any of your coworker’s certificate’s.

- **Certified Documents**: Trusts the certificate for certification signatures.

- **Dynamic Content**: Not recommended for certified documents. Trusts movies and other dynamic content. This option requires that the application environment be configured correctly. For more information, see “Trusting Dynamic Content in Certified Documents” on page 42.

- **Embedded High Privilege JavaScript**: Not recommended for certified documents. Trusts embedded scripts. This option requires that the application environment be configured correctly. For more information, see “Trusting JavaScript in Certified Documents” on page 43.

  **Note**: Recipients of the distributed root will be able to inherit these trust settings as well as any other trust settings of certificates higher up in the chain during import.

7. Choose OK.

8. Choose OK.

**Export the Certificate**

After setting the certificate trust level, export it to a file:

**Tip**: If the Trusted Identity Manager is open after setting the trust levels, skip to step 3.

1. Choose Advanced > 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 88).

   **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 and select all or part of it.


5. Select a certificate in the chain that appears in the left-hand window.

   ![Figure 90 Selecting a certificate chain for export](image)

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** and **Acrobat FDF Data Exchange**: FDF is a format that other Adobe product users can easily import. It is only recognized by Adobe products.

8. Choose **Next**.

9. **Optional**: If the Identity Information dialog appears, enter your email address and any other information. If you have already configured your identity details, this screen may not appear. To view your current settings, choose **Edit > Preferences > Identity**.
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:** You can sign the FDF if you have a digital ID that 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.

**Provide Instructions to the Trusted Root Recipients**

1. Open the FDF attachment 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.
   - Choose **File > Open**, browse to the FDF file, and choose **Open**.

2. The instructions for installing a trusted root depend on whether or not the FDF file is signed or unsigned:
   - If you receive an unsigned FDF containing a trusted root:
     1. Choose **Set Contact Trust**.
     2. On the Trust Settings tab, select the requisite trust options.
   
   **Note:** The sender should tell the recipient which settings are appropriate.

     3. Choose **OK**.
     4. Choose **OK**.

   - If you receive a signed FDF containing a trusted root:
     1. Check **Accept the level of trust specified by the signer for all contacts in this file**.
     2. Choose **Close**.

**Emailing Your Digital ID Certificate**

A digital ID’s certificate contains a public key required for validating digital signatures and encrypting documents. Therefore:

- Before users receiving a document can validate its signature, they must receive the sender’s certificate.

- Before users can encrypt a document using certificates, they must have access to the certificates of the document recipients.

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

- To export from the certificate list in the Security Settings dialog, display it by choosing **Advanced > Security Settings**. For details, see below.
To export any certificate displayed in the Certificate Viewer, choose **Export** on the General tab.

To email a digital ID certificate:

1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right.
4. Choose **Export Certificate**.
5. Choose **Email the data to someone** (Figure 91).

**Figure 91 Digital ID: ID export options**

6. Choose **Next**.

7. Enter the recipient's email address and any other optional information.

**Figure 92 Emailing a digital ID**

8. Choose **Next**.

9. Choose Sign if you want to sign the FDF file; otherwise, choose **Next**.

10. Enter an email address.

11. Choose **Next**.

12. Review the data and choose **Finish**.
13. When the email program opens, send the email.

**Saving Your Digital ID Certificate to a File**

A digital ID's certificate contains a public key required for validating digital signatures and encrypting documents. Therefore:

- Before users receiving a document can validate its signature, they must receive the sender's certificate.
- Before users can encrypt a document using certificates, they must have access to the certificates of the document recipients.

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

- Exporting from the certificate list in the Security Settings dialog. Display it by choosing **Advanced > Security Settings**. For details, see below.
- Exporting any certificate displayed in the Certificate Viewer. Simply choose **Export** on the General tab.

To save a digital ID certificate to a file:

1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right.
4. Choose **Export Certificate**.
5. Choose **Save the exported data to a file** (Figure 91).
6. Choose a file type:
   - **Acrobat FDF Data Exchange**: FDF files can only be emailed in 7.0.7
   - **Certificate Message Syntax - PKCS#7**: Save the file as a PKCS7 file.
   - **Certificate File**: Saves the file in CER format.
7. Choose **Next**.
8. Browse to a file location and choose **Save**.
9. Choose **Next**.
10. Review the data to export and choose **Finish**.

**Requesting a Digital ID via Email**

When you request digital ID information from someone, Acrobat automatically includes in that email an FDF file containing your contact and certificate information.

To request a certificate from another user:

1. Choose **Advanced > Trusted Identities**.
2. Choose **Request Contact**.
3. Confirm or enter your identity.

**Tip:** The identity panel is prepopulated if the information has been previously configured in **Edit > Preferences > Identity**.

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 the digital ID file to export.

8. Choose **Select**.

9. Do one of the following:
   - **Email:** Enter the person's email address in the Compose Email dialog and choose **Email**. Send the email message when it appears in the default email application with the certificate request attached.
• **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.

**Emailing Server Details via FDF**

Adobe Policy Server, directory 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 > Security Settings**.
2. Select **Directory Servers**, **Timestamp Servers**, or **Adobe Policy Servers** from the left-hand list.
3. Select a server from the right-hand panel.
4. Choose **Export**.
5. Choose **Email the exported data** to email the FDF file.

![Figure 95 Digital ID Directory servers: Export destination](image)

6. Choose **Next**.
7. Configure the identity information if it is not already specified under **Edit > Preferences > Identity** (Figure 96).

**Tip:** The Identity panel will not appear if the information has been previously configured. The identity panel is prepopulated if the information has been previously configured in **Edit > Preferences > Identity**.
8. Choose **Next**.

9. Enter the email information.

**Figure 97 Digital ID Directory servers: Email details**

- **Message**: (Enter the email message to attach the exported data)
- **To**: [Enter email addresses]
- **Subject**: [Enter subject]
- **Attached file**: Adobe FDF Data Exchange File
- **Description**: The attaches file contains search directory configuration information that can be used to access search identity directories.
- **Opening this file will prompt**: Adobe Acrobat or Adobe Reader to open the file.
- **To open and process the file, 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**.

**Exporting Server Details via FDF**

Adobe Policy Server, directory server, 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 save to any location. To save server details to a file:

1. Choose **Advanced > Security Settings**.

2. Select **Directory Servers, Timestamp Servers**, or **Adobe Policy Servers** from the left-hand list.

3. Select a server from the right-hand panel. Choose **Export**.

4. Choose **Save the exported data to a file** to save the data in an FDF file that can be shared (Figure 95).

5. Choose **Next**.
6. Configure the identity information if it is not already specified under Edit > Preferences > Identity (Figure 96).

**Tip:** The Identity panel will not appear if the information has been previously configured.

7. Choose **Next**.

8. Choose **Sign**. When the signing dialog appears, choose **Sign** again (Figure 84). Sign FDF files so that recipients of the file can easily trust the file and its contents.

9. Choose **Next**.

10. Browse to a location in which to save the file.

11. Choose a file name and choose **Save**.

12. Choose **Next**.

13. Review the export details.

14. Choose **Finish**.
External Content and Document Security

This document describes how to use Trust Manager control how documents interact with elements outside of the document.

- Setting Attachment Options
- External Stream Access
- Internet URL Access

For information about multimedia permission settings, refer to “Setting Dynamic Content (Multimedia) Security Options” on page 63.

Setting Attachment Options

Before working with attachments, you should understand both the default behavior as well as how to modify that behavior. For details, see the following:

- “Default Attachment Behavior” on page 102
- “Modifying Attachment Behavior Via the User Interface” on page 106

Modifiable attachment options include the following:

- “Adding Custom Attachment Extensions” on page 107
- “Propagating New Attachment Settings” on page 107
- “Allowing Attachments to Open Files or Launch Applications” on page 107

Default Attachment Behavior

You should exercise caution when attaching files to a PDF since the content may adversely affect a document 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 Acrobat manages those types. Acrobat maintains a Black Lists and White Lists which controls application behavior:
  - **File types not on the black list**: These can be attached without a warning dialog. Trying to open or save them from within Acrobat 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.
  - **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 save or opened from Acrobat. No actions are available for these files.

For details about changing this list, see “Modifying Attachment Behavior Via the User Interface” on page 106.

- Prevent attachments from opening other files and launching applications. This is Acrobat’s default behavior. For details about changing this behavior, see “Allowing Attachments to Open Files or Launch Applications” on page 107.
Black Lists and White Lists

Acrobat 7.0 products (Professional, Standard, and Adobe Reader) 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.

Adobe Acrobat and Adobe Reader store some of these good and bad (white and black) file types in a list in the registry (Table 3). This list contains the file types that can and cannot be opened or saved. Acrobat recognizes these file types. If a bad file type is recognized during the attachment process, a warning appears (Figure 98).

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

Acrobat will let you attach files types that are on the black list because a document recipient may have a less restrictive black list than the sender. While the recipient may be able to open the file, the attacher 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 99).

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ade</td>
<td>Access Project Extension (Microsoft)</td>
</tr>
<tr>
<td>.adp</td>
<td>Access Project (Microsoft)</td>
</tr>
<tr>
<td>.app</td>
<td>Executable Application</td>
</tr>
<tr>
<td>.asp</td>
<td>Active Server Page</td>
</tr>
<tr>
<td>.bas</td>
<td>BASIC Source Code</td>
</tr>
<tr>
<td>.bat</td>
<td>Batch Processing</td>
</tr>
<tr>
<td>.bz</td>
<td>Bzip UNIX Compressed file</td>
</tr>
<tr>
<td>.bz2</td>
<td>Bzip 2 UNIX Compressed file (replaces BZ)</td>
</tr>
<tr>
<td>Extension</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>.cer</td>
<td>Internet Security Certificate file (MIME x-x509-ca-cert)</td>
</tr>
<tr>
<td>.chm</td>
<td>Compiled HTML Help</td>
</tr>
<tr>
<td>.class</td>
<td>Java Class file</td>
</tr>
<tr>
<td>.cmd</td>
<td>DOS CP/M Command file, Command file for Windows NT</td>
</tr>
<tr>
<td>.com</td>
<td>Command</td>
</tr>
<tr>
<td>.command</td>
<td>Mac OS Command Line executable</td>
</tr>
<tr>
<td>.cpl</td>
<td>Windows Control Panel Extension (Microsoft)</td>
</tr>
<tr>
<td>.crt</td>
<td>Certificate file</td>
</tr>
<tr>
<td>.csh</td>
<td>UNIX csh shell script</td>
</tr>
<tr>
<td>.exe</td>
<td>Executable file</td>
</tr>
<tr>
<td>.fpx</td>
<td>FoxPro Compiled Source (Microsoft)</td>
</tr>
<tr>
<td>.gz</td>
<td>Gzip Compressed Archive</td>
</tr>
<tr>
<td>.hex</td>
<td>Macintosh BinHex 2.0 file</td>
</tr>
<tr>
<td>.hlp</td>
<td>Windows Help file</td>
</tr>
<tr>
<td>.hqx</td>
<td>Macintosh BinHex 4 Compressed Archive</td>
</tr>
<tr>
<td>.hta</td>
<td>Hypertext Application</td>
</tr>
<tr>
<td>.inf</td>
<td>Information or Setup file</td>
</tr>
<tr>
<td>.ini</td>
<td>Initialization/Configuration file</td>
</tr>
<tr>
<td>.ins</td>
<td>IIS Internet Communications Settings (Microsoft)</td>
</tr>
<tr>
<td>.isp</td>
<td>IIS Internet Service Provider Settings (Microsoft)</td>
</tr>
<tr>
<td>.its</td>
<td>Internet Document Set, International Translation</td>
</tr>
<tr>
<td>.job</td>
<td>Windows Task Scheduler Task Object</td>
</tr>
<tr>
<td>.js</td>
<td>JavaScript Source Code</td>
</tr>
<tr>
<td>.jse</td>
<td>JScript Encoded Script file</td>
</tr>
<tr>
<td>.ksh</td>
<td>UNIX ksh shell script</td>
</tr>
<tr>
<td>.lnk</td>
<td>Windows Shortcut file</td>
</tr>
<tr>
<td>.lzh</td>
<td>Compressed archive (LH ARC)</td>
</tr>
<tr>
<td>.mad</td>
<td>Access Module Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.maf</td>
<td>Access (Microsoft)</td>
</tr>
<tr>
<td>.mag</td>
<td>Access Diagram Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.mam</td>
<td>Access Macro Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.maq</td>
<td>Access Query Shortcut (Microsoft)</td>
</tr>
</tbody>
</table>
Table 3 Default prohibited file types

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.mar</td>
<td>Access Report Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.mas</td>
<td>Access Stored Procedures (Microsoft)</td>
</tr>
<tr>
<td>.mat</td>
<td>Access Table Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.mau</td>
<td>Media Attachment Unit</td>
</tr>
<tr>
<td>.mav</td>
<td>Access View Shortcut (Microsoft)</td>
</tr>
<tr>
<td>.maw</td>
<td>Access Data Access Page (Microsoft)</td>
</tr>
<tr>
<td>.mda</td>
<td>Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)</td>
</tr>
<tr>
<td>.mde</td>
<td>Access MDE Database file (Microsoft)</td>
</tr>
<tr>
<td>.mdt</td>
<td>Access Add-in Data (Microsoft)</td>
</tr>
<tr>
<td>.mdw</td>
<td>Access Workgroup Information (Microsoft)</td>
</tr>
<tr>
<td>.mdz</td>
<td>Access Wizard Template (Microsoft)</td>
</tr>
<tr>
<td>.msc</td>
<td>Microsoft Management Console Snap-in Control file (Microsoft)</td>
</tr>
<tr>
<td>.msi</td>
<td>Windows Installer file (Microsoft)</td>
</tr>
<tr>
<td>.msp</td>
<td>Windows Installer Patch</td>
</tr>
<tr>
<td>.mst</td>
<td>Windows SDK Setup Transform Script</td>
</tr>
<tr>
<td>.ocx</td>
<td>Microsoft Object Linking and Embedding (OLE) Control Extension</td>
</tr>
<tr>
<td>.ops</td>
<td>Office Profile Settings file</td>
</tr>
<tr>
<td>.pcd</td>
<td>Visual Test (Microsoft)</td>
</tr>
<tr>
<td>.pif</td>
<td>Windows Program Information file (Microsoft)</td>
</tr>
<tr>
<td>.prf</td>
<td>Windows System file</td>
</tr>
<tr>
<td>.prg</td>
<td>Program file</td>
</tr>
<tr>
<td>.pst</td>
<td>MS Exchange Address Book file, Outlook Personal Folder file (Microsoft)</td>
</tr>
<tr>
<td>.rar</td>
<td>WinRAR Compressed Archive</td>
</tr>
<tr>
<td>.reg</td>
<td>Registration Information/Key for Windows 95/98, Registry Data file</td>
</tr>
<tr>
<td>.scf</td>
<td>Windows Explorer Command</td>
</tr>
<tr>
<td>.scr</td>
<td>Windows Screen Saver</td>
</tr>
<tr>
<td>.sct</td>
<td>Windows Script Component, Foxpro Screen (Microsoft)</td>
</tr>
<tr>
<td>.sea</td>
<td>Self-expanding archive (used by Stuffit for Mac files and possibly by others)</td>
</tr>
<tr>
<td>.shb</td>
<td>Windows Shortcut into a Document</td>
</tr>
<tr>
<td>.shs</td>
<td>Shell Scrap Object file</td>
</tr>
<tr>
<td>.sit</td>
<td>Compressed archive of Mac files (Stuffit)</td>
</tr>
<tr>
<td>.tar</td>
<td>Tape Archive file</td>
</tr>
</tbody>
</table>
Table 3 Default prohibited file types

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

Modifying Attachment Behavior Via the User Interface

Users can indirectly manage the registry list of which file types can be opened and saved. In other words, the list in Table 3 can be extended one at a time as each attached file is opened.

To add a file to the registry’s attachment list:

1. Attach a file type not in the registry list. For example, myfile.xyz.
2. In Acrobat, try to open the files.
3. When the Launch Attachment dialog appears, choose one of the following (Figure 100):
   - **Open this file**: Opens the files without changing the registry list.
   - **Always allow opening files of this type**: Adds the file type to the registry list and warnings are bypassed in the future.
   - **Never allow opening files of this type**: Does not open the file or add it to the registry list.
4. Choose OK.

*Note:* Because the registry list could grow over time and users do not have direct access to the list (it can’t be easily viewed), resetting the list to its original state results in the highest level of security.
Choosing **Reset list of allowed / disallowed file attachment types** in the Trust Manager removes all custom, user-specified entries in the registry list.

**Figure 100 Launch Attachment dialog**

![Launch Attachment dialog](image)

**Adding Custom Attachment Extensions**

To add custom extensions, add your own file extension entries to the very end of the list. The method is the same on both Windows and Macintosh. Use the following format for each custom extension:

```
|.FILEEXTENSION:PERMVALUE
```

For example, to add the extension .ext with a value of **Always Allowed**, you would add:

```
|.ext:2
```

**Propagating New Attachment Settings**

If the Acrobat 7.x product is already installed various user machines and InstallShield Tuner 7 for Acrobat was not used to customize user installations, it is still possible to propagate the change across multiple users.

To do so:

1. Finish editing the FeatureLockDown Windows registry key.

2. Select the `bBuiltInPermList` key.

3. Choose **File > Export** to save the REG key.

4. Invoke this REG key using whatever method you normally use to deploy this change in your organization. For example, use a BAT file that runs during a user’s logon script to invoke the REG key.

**Allowing Attachments to Open Files or Launch Applications**

The Trust Manager enables users to control whether or not attachments can open files or launch applications. By default, Acrobat does not allow attachments to open files or launch applications.

To set attachment preferences:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).

2. Select Trust Manager in the left-hand tree.

3. Check or uncheck **Allow documents to open other files an launch other applications**. Leave this option unchecked if a high level of security is needed.
**Note:** When the option is unchecked, documents will never open other files or launch applications. When the option is checked, the application uses a stored black list to determine what that file can do. Any file on the black list will not be allowed to open a file or launch an application. Acrobat and Adobe Reader both ship with a default black list.

4. Choose **OK**.

### External Stream Access

Both Adobe Acrobat and Adobe Reader can inform the user when a PDF file is attempting to send or receive stream data. In the PDF world, a stream is an URL or some file specification identified as a stream object by flags as specified in the *PDF 1.6 Reference*. Only PDF developers create PDF files with streams, so the average user usually does not need to enable access to external streams.

Silently transmitting data represents a security risk since malicious content can be transferred whenever the application communicates with an external source. Therefore, only users that are advised to do so by a system administrator should enable this feature.

To configure external stream access:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Trust Manager in the left-hand tree.
3. Check or uncheck **Enable External Streams** in the Resource Access panel.
4. The default (and most secure) behavior does not enable external streams. When external streams are enabled, PDF files that contain an embedded switch defining a host address can silently transmit data to and from the remote host. Do not enable this option unless you want access to remote data.
5. Choose **OK**.

[Figure 101 Resource Access](#)

### Internet URL Access

Both Adobe Acrobat and Adobe Reader can inform the user 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 obvious, visible links in a PDF document, form fields can contain JavaScript calls that open a page in a browser or try to get data silently from the Internet.

Adobe Acrobat and Adobe Reader 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, a warning should appear whenever a PDF document tries to access the Internet (Figure 102).
To configure Internet resource access:

1. Choose **Edit > Preferences** (Windows) or **Acrobat > Preferences** (Macintosh).
2. Select Trust Manager in the left-hand tree.
3. Choose **Change Site Settings**.
4. Select an option from the **Default behavior for URL access** drop down list (Figure 103):
   - **Use Trust List**: The default. When the URL is not in the list, the application behaves as specified by the **Default behavior for other sites** field.
   - **Always Allow**: The application makes the connection to any URL without prompting the user.
   - **Always Deny**: The application never makes the connection to any URL and does not advise the user why the connection was not established.
5. If **Use Trust List** is selected, add a URL in the text field and choose **Allow** or **Block**. Repeat as necessary.
6. Configure the behavior for sites not in the trust list by selecting an option from **Default behavior for other sites**. Choose **Always Deny**, **Always Allow**, or **Always Prompt**.
7. Choose **OK**.
8. Choose **OK**.

---

**Figure 102 External connection warning**

![Security Warning]

The document is trying to connect to the site: http://www.kts.gov
If you trust the site click "Allow", otherwise click "Block".

[Click] [Allow]
Figure 103 Managed Sites dialog
Index

.A 103
.adp 103
.app 103
.asp 103
.bas 103
.bat 103
.bz 103
.bz2 103
.cer 104
.chm 104
.class 104
.cmd 104
.command 104
.cpl 104
.crt 104
.csh 104
.exe 104
.fxp 104
.gz 104
.hex 104
.hlp 104
.hqx 104
.hta 104
.inf 104
.ini 104
.ins 104
.jsp 104
.its 104
.job 104
.js 104
.jse 104
.ksh 104
.lnk 104
.lzh 104
.mad 104
.maf 104
.mag 104
.mam 104
.maq 104
.maw 104
.mar 105
.mas 105
.mat 105
.mau 105
.mav 105
.maw 105
.mda 105
.mde 105
.mdw 105
.mdz 105
.msc 105
.msi 105
.msp 105
.mst 105
.oce 105
.ops 105
.pcd 105
.pif 105
.prf 105
.prg 105
.pst 105
.rar 105
.reg 105
.scf 105
.scr 105
.sct 105
.sea 105
.shb 105
.shs 105
.sit 105
.tar 105
.tgz 106
.tmp 106
.url 106
.vb 106
.vbe 106
.vbs 106
.vsmacos 106
.vss 106
.vst 106
.vsw 106
.webloc 106
.ws 106
.wsc 106
.wsf 106
.wsh 106
.zip 106
.zlo 106
.zoo 106

A
Access Type 52
Add Digital ID dialog 11
Adding a contact 49
Adding a Digital ID from a Signature 32
Adding Certificate Servers as Searchable Directories 29
Adding Custom Attachment Extensions 107
Adding IDs During a Workflow 11
Adding IDs in Advance 12
Adding or Removing Group Contacts 49
Adding Someone to Your Trusted Identity List 32
Adding Windows Certificate Store Certificates to the Search Path 30
Allowing Attachments to Open Files or Launch Applications 107
Associating a Certificate with a Contact 46
Attachment
   Cannot open warning 103
   Dangerous type warning 103

B
Backing up the Private Key 17
Black Lists and White Lists 103
Browsing for a Trusted Identity 34

C
Certificate Chains and Trust Anchors /Roots 91
Certificate Trust Settings 41
Certificate trust settings 41, 42, 93
Certificate Viewer 38
Certificate viewer
  Trust tab 69
Certificate Viewer information 37
Certificates
  Contact Information 84
  Email attachment 83
  Selecting a digital ID for export 33, 98
  Verifying originator 39
Changing a Digital ID’s Password and Timeout 22
Changing a Trusted Identity’s Certificate Association 47
Changing or Clearing the Default Digital ID 19
Check revocation 37
Checking Certificate Revocation Status 39
Compare
  By page 79
  By page summary report 79
  Choose compare report type 78
  Displaying changed text 80
  Select file drop down menu 77
  Type of comparison 78
Comparing a Signed Version with the Current Version 77
Comparing Documents 77
Comparing Documents by Page 78
Comparing Documents by Word 79
Configuring Document Status Preferences 61
Contacts
  Deleting 48
  Deleting a group 50
  Editing a group 49
  Selecting certificates 46
  Viewing details 45
Creating a Community of Document Authors and Recipients 26
Creating a Group 49
Creating a Self-Signed Digital ID 14
Creating Default User Information 28
Creation time 61
Current time 60

D
Default Attachment Behavior 102
Default prohibited file types 103
Deleting a Certificate 48
Deleting a Digital ID 19
Deleting a Directory Server 53
Deleting a Group 50
Deleting Contacts and Certificates 47
Details 37
Digital ID
  Adding a digital ID 12
  Certificate viewer 22
  Components 8
  Configuration 15
  Creating a self-signed ID 14
  Default ID specification 18
  Deleting 19
  Finding an existing ID 16
  From others 9
  Getting a third-party ID 17
  ID export options 20, 96
  Managing trusted identities 27
  PKCS#12 location and password 16
Digital ID Basics 8
Digital ID Directory servers
  Email details 100
  Export destination 99
  Importing 88
  Sender’s identity 100
  Server list 51
  Setting defaults 53
  Setting server details 52
Digital ID files
  Login and Logout 24
  Password configuration 23
  Timeout settings 24
Digital ID management 18
Digital ID storage formats 9
Digital ID User Interface 9
Digital IDs
  Searching the Windows Certificate Store 31
Digital signature 56
Digital signature icons 57
Digital Signature Properties
  Document Versioning panel 70, 76
  Modifications panel 77
Digital Signatures Advanced Preferences
  Signature verification 60
Digital Signatures for Document Recipients 55
Directory Name 52
Displaying a Certificate in the Certificate Viewer 37
Displaying the Signature Properties Dialog 71
Distributing a Trust Anchor or Trust Root 91
Document Status dialog
  for certified document 62
  for Signed and encrypted document 61
Document status preferences 62
Document Versioning panel 72
Document versions 76

E
Edit Contact dialog 45, 47
Editing Directory Servers Details 52
Emailing a certificate request 33, 98
Emailing a digital ID 20, 96
Emailing Certificate or Contact Data 46
Emailing Server Details via FDF 99
Emailing your certificate 13
Emailing Your Digital ID Certificate 19, 95
Export the Certificate 93
Exporting Acrobat Data 91
Exporting Acrobat Data via FDF 100
External connection warning 109
External Content and Document Security 102
External Stream Access 108

F
Finding an Existing Digital ID 16

G
General 37
Getting a Third-Party Digital ID 17
Getting and Using Your Digital ID 7
Getting Your Own Digital ID 11
Green Check and Caution Triangle 71

H
High Privilege JavaScript Defined 65
How are Digital IDs managed? 8

I
Identity preferences 28
Importing a Single Certificate From an FDF File 36
Importing a Single Certificate via FDF 83
Importing Acrobat Data 83
Importing and Exporting Directory Server Settings 54
Importing APS Server Settings via FDF 88
Importing APS settings 89
Importing certificate from FDF 85
Importing digital ID data 34
Importing Directory Server Settings via FDF 87
Importing Multiple Certificates via FDF 84
Importing Timestamp Server Settings via FDF 86
Internet URL Access 108

J
JavaScript Security option 65

L
Launch Attachment dialog 107
Legal Notice 37
Logging in to an Adobe Policy Server 89
Login, Logout, and Batch Processing 24

M
Making a contact a trusted identity 86
Managed Sites dialog 110
Managing Contacts 45
Managing Trusted Identities 25
Manually Configuring a Directory Server 51
Maximum Number of Records to Receive 52
Modifying Attachment Behavior Via the User Interface 106

P
Password 52
Policies 37
Port 52
Post-signing modifications 76

Problems encountered 37
Propagating New Attachment Settings 107
Provide Instructions to the Trusted Root Recipients 95

Q
Question Mark and Caution Triangle 72
Question Mark and Pen 73
Question Mark and Person 72

R
Red X and Pen 73
Removing a contact 49
Requesting a Digital ID via Email 32, 97
Resource Access 108
Responding to an Emailed Request for a Digital ID 12, 83
Revalidate signatures warning 69
Revocation 37
Running JavaScript and Dynamic Content 73

S
Saving Certificate or Contact Details to a File 46
Saving Your Digital ID Certificate to a File 21, 97
Search Base 52
Searching for a Digital ID to Trust 34
Searching for a document recipients 36
Secure time 60
Security settings menu and manager 10
Selecting a certificate chain for export 94
Selecting a Certificate to use for Encryption 43
Selecting a digital ID 13
Self-signed ID alert 14
Server Name 52
Setting Attachment Options 102
Setting Certificate Trust Level 92
Setting Digital Signature Validation Preferences 59
Setting Dynamic Content (Multimedia) Security Options 63
Setting High Privilege JavaScript Security Options 65
Setting Up Automatic Signature Validation 59
Setting up the Trusted Identity Environment 28
Setting up Your Environment for Receiving Documents 59
Sharing Acrobat Settings and Data with FDF Files 81
Signature Components
  What Makes them Valid? 56
Signature components 57
Signature Properties
  Summary 68
Signature Status and Validity Icons 57
Signature validation confirmation 67
Signatures tab
  Validate signature 67
Signer Details 37
Signing an FDF file 91
Specifying a Default Digital ID 18
Specifying a Default Directory Server 53

T
This server requires me to log on 52
Timeout 52
Timestamp Basics for Document Recipients  74
Timestamps
  Date/Time tab  75
  Importing a default server  87
  Importing server details from an FDF file  87
  Local, machine time  74
  Trusted stamp  74
  Untrusted stamp  74
Trust  37
Trust Manager  64
Trusted Identities
  Viewing  38, 92
  Viewing revocation status  40
Trusting a certificate for encryption  44
Trusting a Certificate for Signing and Certifying  41
Trusting a Timestamp Certificate in a Signature  74
Trusting Dynamic Content in Certified Documents  42
Trusting JavaScript in Certified Documents  43
Trusting Timestamp Authority Certificates  40
Trusting Windows root certificates  30

U
Untrusted signature  41
Upgrading a Legacy .apf Digital ID  17
User name  52
Using Directory Servers to Add Trusted Identities  51
Using Groups with Security Policies  50
Using the Windows Certificate Store for Signing and Certificate Security  29
Using Windows Certificate Store Certificates for Validation
  29
Using Your Digital ID  18

V
Valid digital signature  66
Validate all signatures dialog  67
Validating a Signature for an Earlier Document Version  70
Validating a Single Signature  66
Validating All Signatures Simultaneously  67
Validating an Unknown (Untrusted) Signature  67
Validating Signatures Manually  66
Verifying Self-Signed Certificates  38
Viewing a List of Post-Signing Modifications  76
Viewing a Signed Version of a Document  76
Viewing and Comparing Document Changes and Versions  76
Viewing and Editing Contact Details  45
Viewing Your Digital ID Certificate Details  22
Visual document changes  76

W
What is a Digital ID?  8
What’s in this Guide?  6
When the Status Icon is Not a Green Check . . .  71
When Timestamps Can’t be Verified . . .  75
Why Attach a File that’s on the Black List?  103
Working with Digital IDs and Certificates  37
Working with Groups of Contacts  49
Working with Signed Documents  56