Acrobat

Signing Adobe PDF documents in Acrobat

A digital signature can be either visible or invisible. A visible signature appears in both the document and the Signatures tab. An invisible signature appears only in the Signatures tab. Adding a signature does not affect the validity of existing signatures in the document.

When you sign a document, your signature and the related information can be stored in a signature field embedded on the page. A signature field is an Acrobat form field.You can add a signature field to a page as you sign, or you can use the Signature tool to create an empty signature field that can be signed later.

Important: Sign a document only after you make final changes. If you make changes to a PDF document after you sign it, the signature may still be valid, but the caution triangle appears in the signature field and in the Signature tab, indicating that changes were made. The author of the PDF document can also lock fields after the document is signed, to prevent additional changes.

To sign a document in Acrobat:

1. Click the unsigned signature field in the PDF document (the field must be a signature form field, not just a blank box), or choose Document > Digital Signatures > Sign This Document.

Signing Adobe PDF documents in a web browser

To sign a PDF document on the web, the document must contain an empty signature field. When you click a signature field, a Sign button appears rather than the Sign And Save and Sign And Save As buttons, which appear when you sign a document directly in Adobe Acrobat. When you sign a document in a browser, only the incremental portion of the file is saved to your hard drive.

To sign a document in a web browser:

1. From the Sign menu on the Tasks toolbar, choose Sign This Document, or click a signature field, and then follow the steps described in Signing Adobe PDF documents in Acrobat.
2. To retain a copy of the signed document, click the Save A Copy button  on the File toolbar.

Creating a digital ID

If you're not using a third-party digital ID, you can create your own self-signed digital ID. When you create a self-signed digital ID, the resulting file stores an encrypted private key used for signing or decrypting documents and a public key contained in a certificate, which is used for validating signatures and encrypting documents.

You can create either a PKCS#12 digital ID, which is a standard encryption format, or a Windows Default Certificate digital ID, which is stored in the Windows Certificate Store. PKCS#12 file name extensions are .pfx in Windows and .p12 in Mac OS.

To create a self-signed digital ID:

1. Choose Advanced > Security Settings.
2. Select Digital IDs on the left, and then click Add ID.
3. Select Create A Self-Signed Digital ID, and then click Next. Click Next again.
4. Select one of the following to specify where to store your digital ID, and then click Next:
   - New PKCS#12 Digital ID File stores the information in a file that you can send to others.
   - Windows Certificate Store (Windows only) stores the file where other Windows applications can also retrieve it.
5. Type a name and other personal information for your digital ID. When you certify or sign a document, the name appears in the Signatures tab and in the signature field.
6. (Optional) To use Unicode values for extended characters, select Enable Unicode Support, and then specify Unicode values for the appropriate fields.
7. Choose a key algorithm from the menu. 2048-bit RSA offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible.
8. From the Use Digital ID menu, choose whether you want to use the digital ID for digital signature, data encryption, or both. (See Encrypting Adobe PDF files using certificates.)
9. Click Next, and specify a file name and location for the digital ID file.
10. Type a password; passwords are case-sensitive, must contain at least six characters, and may not contain double quotation marks or the following characters: ! @ # $ % ^ & * , | \ ; < > _. Type the same password in both the Choose A Password and Confirm Password boxes. Click Next.
11. Click Finish.

You can export and send your certificate file to those who need to validate your signature. (See Managing digital ID certificates.)

Important: Make a backup copy of your digital ID file. If your digital ID file is lost or corrupted, or if you forget your password, you cannot use that profile to add or validate signatures.

Finding and adding existing digital IDs

If you created a digital ID file that does not appear in your list of digital IDs, you can search for the missing digital ID file and add it to your list. One of the common encryption methods that Acrobat uses, PKCS#12, has the .pfx file name extension in Windows and .p12 in Mac OS. Digital ID files from some earlier versions of Acrobat use an .apf extension. If you select an .apf digital ID file, you may be prompted to convert the file to a supported file type.

To find and add digital ID files:

1. Choose Advanced > Security Settings.
2. Select Digital IDs on the left, and then click Add ID.
3. Select Find An Existing Digital ID, and then click Next.
4. Click Browse, select a Digital ID and click Open.
5. Type the ID password, and then click Next.
6. Click Finish.

Getting digital ID information from other users

You can keep a copy of other users' digital ID certificates in a list of trusted identities. Your list of trusted identities is like an address book that stores digital ID certificates. The list lets you validate the signatures of these users on any documents you receive. You can also use the list of trusted identities to encrypt files. (See Encrypting Adobe PDF files using certificates.)

The preferred method of adding another user's certificate to your list of trusted identities is by importing the certificate from an FDF file that the user sends to you. You can also add a certificate directly from the PDF document signed by someone who used a self-signed digital ID, although this method may not be trustworthy.

To request a certificate from another user:

1. Choose Advanced > Trusted Identities.
2. Click Request Contact.
3. Type your name, email address, and contact information.
4. To allow other users to add your certificate to their list of trusted identities, select Include My Certificates.
5. Select whether you want to email the request or save it as a file so that you can email it later, and then click Next.
6. Select the digital ID file to use, and then click Select.
7. Do one of the following:

- If the Compose Email dialog box appears, type the email address of the person you are requesting a certificate from, and type a subject. Click Email. A new email message appears in your default email application with the certificate request attached. Send this message in your email application.
- If the Export Data As dialog box appears, choose a location for the certificate file in the Save In box, type a file name, click Save, and then click OK.

To add a certificate from email to your list of trusted identities:

1. After a user sends you certificate information, open the email attachment in Acrobat, and then click Set Contact Trust in the dialog box that appears.
2. Select trust options, and then click OK. Click OK again, and then click Close.

To add a certificate from a file to your list of trusted identities:

1. If you're using the Certificates feature in Windows to organize certificates, select the Enable Import And Use Of Identities From The Windows Certificate Store option in the Security preferences. Click the Windows Integration tab in the Digital Signatures Advanced Preferences, select the desired options, click OK, and then click OK again. (See Setting Digital Signature preferences.)
2. Choose Advanced > Trusted Identities.
3. Click Add Contacts.
4. Do any of the following:

- If Windows Certificate digital IDs are allowed, select the appropriate directory and group.
- If you configured an identity search directory, select the appropriate directory and group. You can then click Search to locate specific digital ID certificates. (See Configuring identity search directories.)
- Click Browse, locate the certificate file, and then click Open.

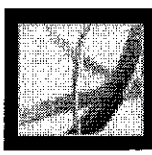
5. Select the added certificate, and then click Details.
6. In the Certificate Attributes dialog box, note the MD5 Fingerprint and the SHA-1 Fingerprint numbers. Confirm with the certificate's originator that the information is correct. If the information isn't correct, the certificate shouldn't be trusted. Click OK.
7. After you verify that the information is correct, click Trust, specify trust options, and then click OK.

To add a certificate using a signature in a PDF document:

1. Open the PDF document containing the user's self-signed signature.
2. Click the signature in the document to check whether it's valid.
3. Click Signature Properties, and then click Show Certificate.
4. In the Certificate Attributes dialog box, note the MD5 Fingerprint and the SHA-1 Fingerprint numbers. Confirm with the certificate's originator that the information is correct. After you verify that the certificate information is correct, click Close, click Trust Identity, click OK, specify trust options, and then click Import.

To delete a certificate from the list of trusted certificates:

1. Choose Advanced > Security Settings.
2. Select the certificate, and click Remove ID.



Managing digital ID certificates

A digital ID certificate contains a public key that is used to validate digital signatures and to encrypt documents.

- Validating signatures. Before other users can validate your signature on documents they receive, they must have access to your certificate, which you can share with them. Likewise, other users can share their certificates with you so that you can build a list of trusted user certificates, called *trusted identities*, for validating signatures. (See Validating signatures.)
- Encrypting documents. If you're encrypting a document using certificates, you need access to the certificates of the people for whom you're encrypting the document. You can use a directory search to locate these trusted identities, or you can store the users' certificates in your list of trusted identities. Acrobat keeps track of the trusted identities that you build.

  You can also configure Windows Certificate Security to trust identities in the common Windows Certificate Store. (See Setting Digital Signature preferences.) Third-party providers may validate identities using other methods, or these validation methods may be integrated with Acrobat.

Related Subtopics:

Sharing your digital ID certificate
Getting digital ID information from other users
Checking information on certificates
Determining the trust level of a certificate
Configuring identity search directories

Validating signatures

When you validate a signature, you verify the signer's identity and assess any changes made after the document was signed. For an identity to be valid, the signer's certificate, or one of its parent certificates that was used to issue the signer's certificate, must be in your list of trusted identities, and it must not have expired or been revoked. (See Getting digital ID information from other users.)

When you open a document, its signatures are validated automatically, unless you turn off a preference setting. The verification status appears on the document page and in the Signatures tab. If the signer's certificate isn't recognized in the list of trusted identities, the signature validity is unknown. Third-party signature handlers may verify identities using other methods. You can specify whether document-specific settings or default settings are used for verifying documents, check to see if the signature has been revoked, add time stamps to signatures, and change other validation settings. (See Setting Digital Signature preferences.)

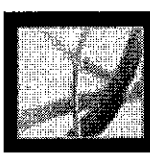
To validate a signature:

1. Open the PDF document containing the signature.
2. In the signature field or in the Signatures tab, check whether the Warning Sign icon  appears next to the signature. If this icon appears, the document may have been modified after it was signed.
3. Select the signature in the Signatures tab, and then choose Validate Signature from the Options menu. The Signature Validation Status describes the signature status.
4. Click Legal Notice to learn more about the legal restrictions of this signature, and then click OK.
5. If the status is unknown, click Signature Properties, click the Signer tab, and then click Show Certificate to view the details of the certificate. If you're working with self-signed digital IDs, confirm that the certificate details are valid. (See Checking information on certificates.)

If the document was modified after it was signed, you can view a previous version, or you can compare the versions to see which changes have been made. (See Viewing previous versions of a signed document or Comparing versions of a signed document.)

Related Subtopics:

Viewing previous versions of a signed document



Acrobat 7.0 Professional

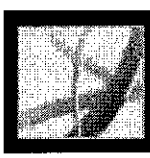
Setting Digital Signature preferences

You can use the Security panel of the Preferences dialog box to change your signature appearances, specify a default security method, change validation settings, and specify other advanced preferences. (See also Changing signature appearance.)

To set advanced digital signature preferences:

1. In the Preferences dialog box, select Security on the left, and then click Advanced Preferences.
2. To require certificates to be checked against a list of excluded certificates during validation, select Require That Certificate Revocation Checking Be Done Whenever Possible When Verifying Signatures. The Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) are common schemes that maintain security of a network server, containing lists of revoked but unexpired certificates. If this option is not selected, the revocation status for nonauthor signatures is ignored.
3. Under Verification Time, select an option to determine whether the time that appears in the digital signature reflects the time the signature was validated (Current Time), the time set by the default Time Stamp Server specified in the Security Settings, or the time the signature was created.
4. Click the Windows Integration tab, and do the following:

- Specify whether you can import identities from the Windows Certificates feature into the list of trusted identities. (See Getting digital ID information from other users.)
- Specify whether to trust all root certificates in the Windows Certificates feature when validating signatures and when validating certified documents. Be aware that selecting these options might compromise security.



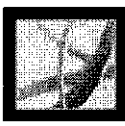
Configuring identity search directories

Identity search directories help you locate specific digital ID certificates from network servers, including LDAP (Lightweight Directory Access Protocol) servers. By developing a trusted digital ID certificate storage area, you or a member of your workgroup can facilitate the use of encryption in your workgroup. After you locate a digital ID certificate, you can add it to your list of trusted identities so that you don't have to look it up again.

To configure an identity search directory:

1. Choose Advanced > Security Settings.
2. Select Directory Servers on the left.
3. Click New, specify a directory name, and type server settings, and then click OK.

For more information on server settings, contact your system administrator.



Acrobat® 7.0 Professional

Setting Trust Manager preferences

Use the Trust Manager panel of the Preferences dialog box to change multimedia security settings for trusted and nontrusted documents. For example, you can allow multimedia files to be played in trusted documents but not in nontrusted documents.

A document is trusted if it's added to the list of trusted documents and authors. If a document is not trusted, you are prompted to add the document to this list when you try to play a media clip in which the permission is set to Prompt. If you decide to add a certified document to the list, both the document and the author's certificate are added to the list. All documents certified by this author are trusted.

To set Trust Manager preferences:

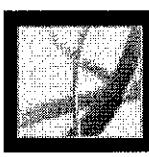
1. Choose Edit > Preferences (Windows) or Acrobat > Preferences (Mac OS), and then select Trust Manager on the left.
2. From the Display Permissions For menu, choose whether you want to display security permissions for trusted documents or nontrusted documents.
3. Select whether the trusted documents (or nontrusted documents) can open other files or launch applications.
4. Under Multimedia Permission Settings, select Allow Multimedia Operations to allow media clips to be played.
5. To change the permission settings for a particular multimedia player, select the player in the list, and choose one of the following options from the Change Permission For Select Multimedia Player To menu:

- Always to allow the player to be used without prompting.
- Never to prevent the player from being used.
- Prompt to ask whether the player can be used. This option lets you decide whether to add a nontrusted document to the list of trusted documents when you try to play the media clip using the selected player.

6. To set the media playback options, select any of the following options:

- Allow Playback In A Floating Window With No Title Bars.
- Allow Document To Set Title Text In A Floating-playback Window.
- Allow Playback In Full-screen window.

For information on setting general multimedia preferences, see Setting Multimedia preferences.



Acrobat 7.0 Professional

Using digital IDs and certification methods

A *digital ID* lets you create a digital signature or decrypt a PDF document that has been encrypted. A digital ID is sometimes referred to as a *private key*, a *credential*, or a *profile*. When you sign or decrypt a document, you select which digital ID to use. A digital ID is usually password protected and can be stored on your computer as a PKCS#12 file, on a smart card, or in the Windows Credential Store. You can get a digital ID from a third-party provider, or you can create a self-signed digital ID and share your signature information with others using a public key certificate. A *certificate* is a confirmation of your digital ID and contains information used to protect data. (See Managing digital ID certificates.)

When a digital signature is applied, a unique fingerprint with encrypted numbers is embedded in the document. The recipient needs the signer's certificate to validate that the digital signature and certificate match the signer's digital ID. Adobe Acrobat 7.0 includes one handler that has access to trusted certificates in a number of different locations. The locations include Microsoft's cryptographic store used for Windows security, PKCS#12 encryption, which is a standard encryption format, and PKCS#11 encryption, which is used on smart cards.

Related Subtopics:

Obtaining a digital ID from a third party
Creating a digital ID
Finding and adding existing digital IDs
Selecting digital IDs
Using third-party digital IDs

About document security

When creating Adobe PDF documents, authors can use the following methods to enhance document security:

- Password security. You can add passwords and set security options to restrict opening, editing, and printing PDF documents. (See Adding passwords and setting security options
- Certification security. Encrypt a document so that only a specified set of users have access to it. (See Encrypting Adobe PDF files using certificates.)
- Adobe Policy Server. Apply server-based security policies to PDF documents. Server-based security policies are especially useful if you want others to have access to PDF documents only for a limited time. (See Encrypting Adobe PDF files using security policies.)
- Document certification. When an author digital signature is added, editing changes are restricted and detected. (See Certifying documents.)

If you often use the same security settings for a set of PDF documents, consider creating a security policy to simplify your workflow. (See Creating user security policies.)

Related Subtopics:

Opening Adobe PDF documents with security restrictions

Viewing document properties

When you view a PDF document, you can get information about it, such as the title, the fonts used, and security settings. Some of this information is set by the person who created the document, and some is generated by Acrobat. You can change any information that can be set by the document creator, unless the file has been saved with security settings that prevent changes.

To get information about the current document:

1. Choose File > Document Properties, or choose Document Properties from the document pane menu.
2. Click a tab in the Document Properties dialog box:

Description

The Description tab shows basic information about the document. The title, author, subject, and keywords may have been set by the person who created the document in the source application, such as Microsoft Word or Adobe InDesign, or by the person who created the PDF document. You can add to or edit this information if the security options allow such changes. You can search for these description items in Acrobat to find particular documents. The Keywords section can be particularly useful for narrowing searches.

Note that many search engines use the title to describe the document in their search results list. If a PDF file does not have a title, the file name appears in the results list instead. A file's title is not necessarily the same as its file name.

The Advanced group box shows which PDF version the document is created in, the page size, number of pages, and whether the document is tagged. This information is generated automatically and cannot be modified.

Security

The Security tab describes what activities, if any, are not allowed. (See About document security.)

Fonts

The Fonts tab lists the fonts and the font types used in the original document, and the fonts, font types, and encoding used to display the original fonts.

If substitute fonts are used and you aren't satisfied with their appearance, you may want to install the original fonts on your system or ask the document creator to re-create the document with the original fonts embedded in it. (See Accessing and embedding fonts.)

Initial View

The Initial View tab describes how the PDF document appears when it's opened. This includes the initial window size, the opening page number and magnification level, and whether bookmarks, thumbnails, the toolbar, and the menu bar are displayed. You can change any of these settings to control how the document appears the next time it is opened. (See Initial View options for document properties.)

Custom

The Custom tab lets you add document properties to your document. (See Creating document properties.)

Advanced

The Advanced tab shows PDF settings and reading options.

Base URL displays the base Uniform Resource Locator (URL) set for web links in the document. Specifying a base URL makes it easy for you to manage web links to other websites. If the URL to the other site changes, you can simply edit the base URL and not have to edit each individual web link that refers to that site. The base URL is not used if a link contains a complete URL address.

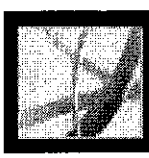
Search Index associates a catalog index file (PDX) with the PDF file. When the PDF file is searched with the Search PDF window, all of the PDF files that are indexed by the specified PDX file are also searched. (See Searching across multiple Adobe PDF documents.)

The Trapped menu indicates whether trapping is applied to the file. Prepress software uses this information to determine whether to apply trapping at print time.

Print Scaling determines whether the Page Scaling value in the Print dialog box is set to None or the last value that was used.

Binding affects how the pages are arranged side by side when you view them using the Continuous - Facing page layout. (See Setting the page layout and orientation.) This is for matching the reading direction (left to right or right to left) of text in the document. Right Edge binding is useful for viewing Arabic or Hebrew text or vertical Japanese text. You can change this setting.

Language specifies the language for the screen reader. You can change this setting. (See Using a screen reader.)

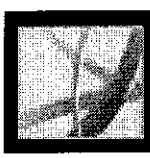


Acrobat 7.0 Professional

Reviewing documents with additional usage rights

By including additional usage rights in a PDF document, you can invite Adobe Reader 7.0 users--in addition to Acrobat users--to participate in document reviews. (Adobe Reader 7.0 is a free download, available from the Adobe website.) Additional usage rights, such as commenting rights, are document-specific. Acrobat 7.0 Professional adds commenting rights to the review PDF document when you use the wizard to initiate an email-based review. You can also add commenting rights to a PDF document by choosing Comment > Enable For Commenting In Adobe Reader. To enable commenting for browser-based reviews, you must use an Adobe server product in addition, such as Adobe Document Server or Adobe Reader Extensions Server. (For more information about Adobe server products, visit the Adobe website.) When a PDF document with commenting rights opens in Adobe Reader, it includes a Document Message Bar that provides instructions, and the appropriate toolbar opens. (See Additional usage rights.)

Note: Participants must have email capabilities to review PDF documents that include additional usage rights.



Additional usage rights

You can assign special rights to a PDF document, making more tools and features available to users of Adobe Reader and letting them save the data that they type in a PDF form, sign documents, participate in online document reviews, and attach files to a PDF document. If a user opens a document that has these additional usage rights, a yellow Document Message Bar displays the additional tools required to work with the document, and Adobe Reader provides instructions.

You can add commenting capabilities for email-based reviews directly from Acrobat Professional. You add other additional usage rights by using a server extension. For more information, see the Adobe website at www.adobe.com/products/server/readerextensions/main.html (English only).

Adobe Help Resource Center

Browse

Go

Search

Search

Contents | Index

Acrobat

About Adobe PDF forms

An Adobe PDF form is an electronic-based document that can collect data from a user and then send that data via email or the web. A PDF form can contain static or interactive form fields; interactive form fields let the user fill in the form using his or her computer, while static form fields must be printed and filled in by hand. Users who fill in a PDF form that contains interactive form fields using Adobe Acrobat Professional or Adobe Acrobat Standard can save their form data along with the PDF form; Adobe Reader users can save only a blank copy of the PDF form, unless the form author added special usage rights to the PDF form.

It's easy to create electronic PDF forms using Adobe Designer or Adobe Acrobat Professional. You can design and create an entirely new form, or you can quickly convert your existing paper and electronic forms to PDF and then add PDF form fields.

There are three types of Adobe PDF forms:

- Fill-and-print PDF forms are typically digital presentations of paper forms. Fill-and-print forms may contain interactive form fields or static form fields; either way, the user must manually deliver the form, such as via postal mail or fax machine.
- Submit-by-email PDF forms contain a button that either extracts the form data from the PDF form and attaches that data to an email message or attaches the filled-in PDF form to an email message.
- Submit on-line PDF forms contain a button that sends the form data to an online repository, such as a database.

Related Subtopics:

Elements of an Adobe Acrobat PDF form

Changing signature appearance

You can specify how your signature appears in the signature field. For example, you can include an image of your company logo. When you use an SVG image in a signature, only the image is used, not the white space around it. The image is cropped and scaled to fit in the signature field.

Note: To use a signature appearance that you've created, you choose it during the last step of signing the document. (See Signing Adobe PDF documents in Acrobat.)

To create a new signature appearance:

1. If you want to include an image (such as a scanned signature or logo) in your signature, create or import an image from any authoring application, place the image on a page by itself, and convert the file to PDF.
2. Choose Edit > Preferences (Windows) or Acrobat (Mac OS) > Preferences, and select Security on the left.
3. Click New.
4. In the Configure Signature Appearance dialog box, type a title for the signature appearance. When you sign a document, you select the signature by its title, so use a short title that accurately describes the signature.
5. Select one of the following in the Configure Graphic section to define the signature's appearance:

- No Graphic displays only the default digital signature icon and other information specified by the Configure Text options.
- Imported Graphic displays a graphic signature that you specify. Click the File button, click the Browse button, choose the graphic file type from the Files Of Type menu, select a graphic, click Select and then click OK (Windows) or Select (Mac OS).

Note: The Palm Organizer button is unavailable unless Palm OS® appearance files are detected. (See Setting up Palm OS appearance files.)

- Name displays only the default digital signature icon and your name as it appears in your digital ID file.

6. In the Configure Text section, select any text items you want to appear in the signature. Distinguished Name shows the user attributes defined in your Digital ID, including your name, organization, and country.

To edit or delete a signature appearance:

1. In the Preferences dialog box, select Security on the left.
2. Do one of the following:

- To edit a signature appearance, select its title in the Appearance box, and then click Edit.
- To delete a signature appearance, select its title in the Appearance box, and then click Delete.