



learningcurve

Adobe Acrobat **Digital Signatures** **& Protecting PDFs**



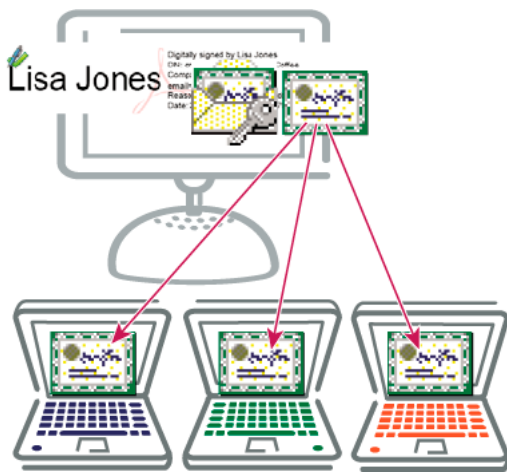
EDUCATION ELITE

Platinum Reseller

What is a digital ID?

A digital ID is like an electronic driver's license or passport that proves your identity. A digital ID usually contains your name and email address, the name of the organization that issued it, a serial number, and an expiration date. Digital IDs are used for certificate security and digital signatures.

Digital IDs contain two keys: the public key locks, or encrypts data; the private key unlocks, or decrypts that data. When you sign PDFs, you use the private key to apply your digital signature. The public key is in a certificate that you distribute to others. For example, you can send the certificate to those who want to validate your signature or identity. Store your digital ID in a safe place, because it contains your private key that others can use to decrypt your information.



Digital IDs include a private key that you safeguard and a public key (certificate) that you share.

Why do I need one?

You don't need a digital ID for most of the work you do in PDFs. For example, you don't need a digital ID to create PDFs, comment on them, and edit them. You need a digital ID to sign a document or encrypt PDFs through a certificate.

What are self-signed digital IDs?

Self-signed digital IDs can be adequate for personal use or small-to-medium businesses. Their use should be limited to parties that have established mutual trust.

What are IDs from certificate authorities?

Most business transactions require a digital ID from a trusted third-party provider, called a certificate authority. Because the certificate authority is responsible for verifying your identity to others, choose one that is trusted by major companies doing business on the Internet. The Adobe website gives the names of Adobe security partners that offer digital IDs and other security solutions. See Adobe Approved Trust List members.

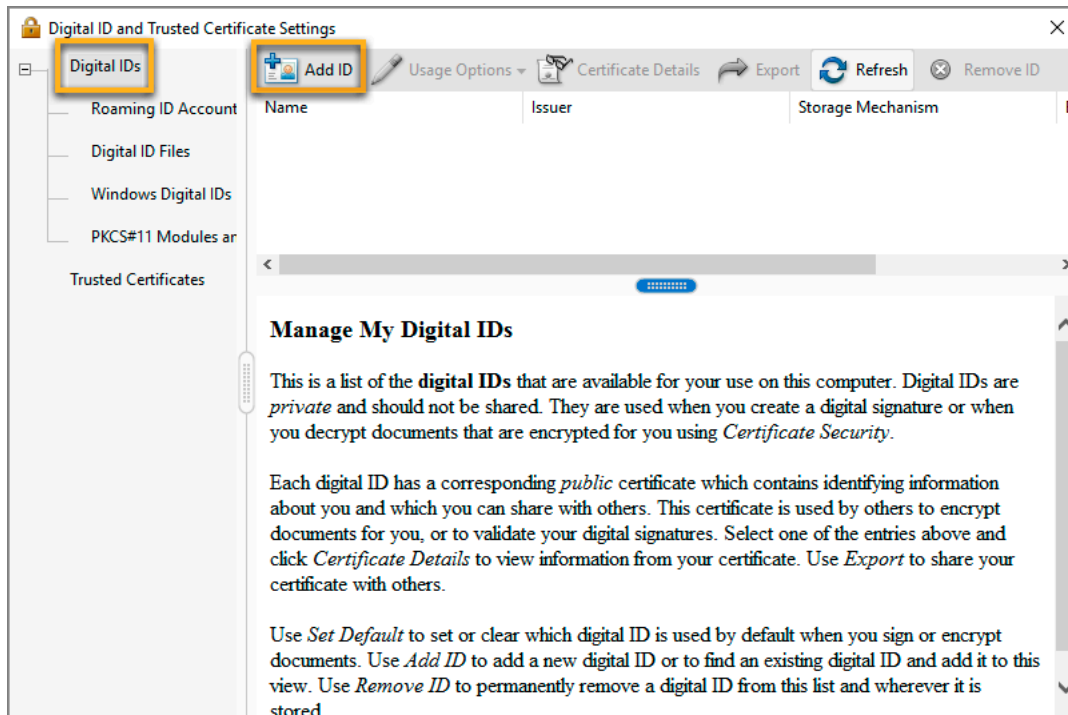
How do I recover or reset my digital ID's password?

Unfortunately, you cannot recover or reset the password if you've forgotten it. If you created the ID yourself, you can create a new one with the same information that you used for the ID. If you got the ID from a certificate authority, contact the authority for help.

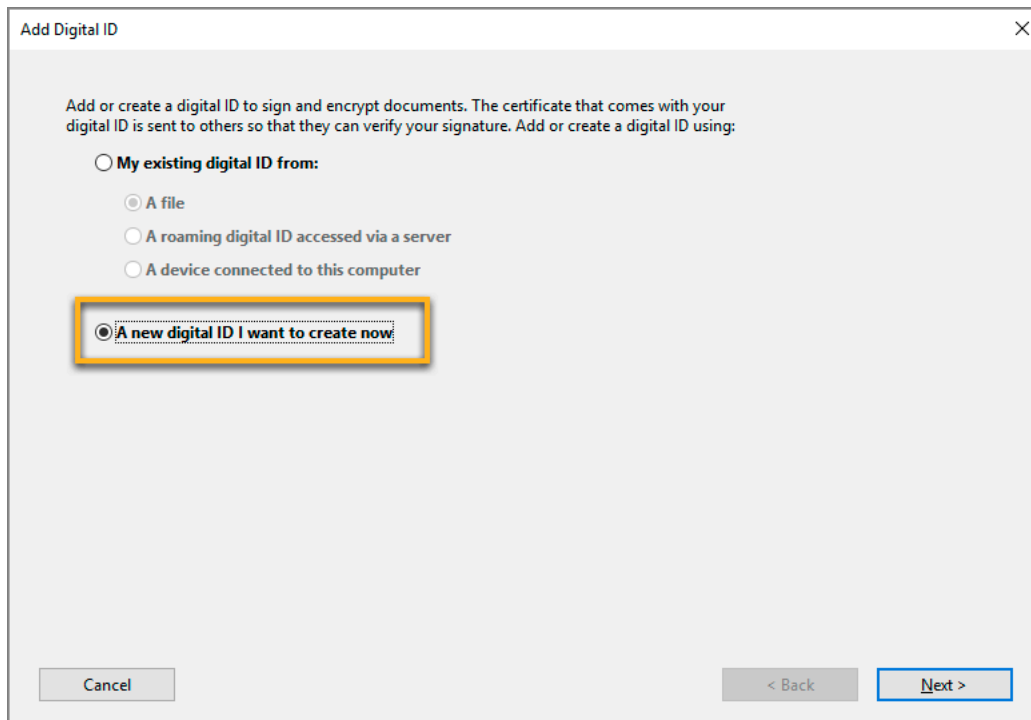
Create a self-signed digital ID

Sensitive transactions between businesses generally require an ID from a certificate authority rather than a self-signed one.

1. In Acrobat, click the Edit menu and choose Preferences > Signatures.
2. On the right, click More for Identities & Trusted Certificates.
3. Select Digital IDs on the left, and then click the Add ID button



4. Select the option A New Digital ID I Want To Create Now, and click Next.



5. Specify where to store the digital ID, and click Next.

New PKCS#12 Digital ID File - Stores the digital ID information in a file, which has the extension .pfx in Windows and .p12 in Mac OS. You can use the files interchangeably between operating systems. If you move a file from one operating system to another, Acrobat still

recognizes it.

Windows Certificate Store (Windows only) - Stores the digital ID to a common location from where other Windows applications can also retrieve it.

Add Digital ID

Where would you like to store your self-signed digital ID?

☒ **New PKCS#12 digital ID file**

Creates a new password protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

☐ **Windows Certificate Store**

Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.

Cancel < Back Next >

6. Do the following:

- Type a name, email address, and other personal information for your digital ID. When you certify or sign a document, the name appears in the Signatures panel and in the Signature field.
- Choose an option from the Key Algorithm menu. The 2048-bit RSA option offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible.
- From the Use Digital ID For menu, choose whether you want to use the digital ID for signatures, data encryption, or both.
- Click Next.

Add Digital ID

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith): John Doe

Organizational Unit: Sales

Organization Name: Sales and Marketing Inc.

Email Address: doe@salesandmarketinginc.com

Country/Region: US - UNITED STATES

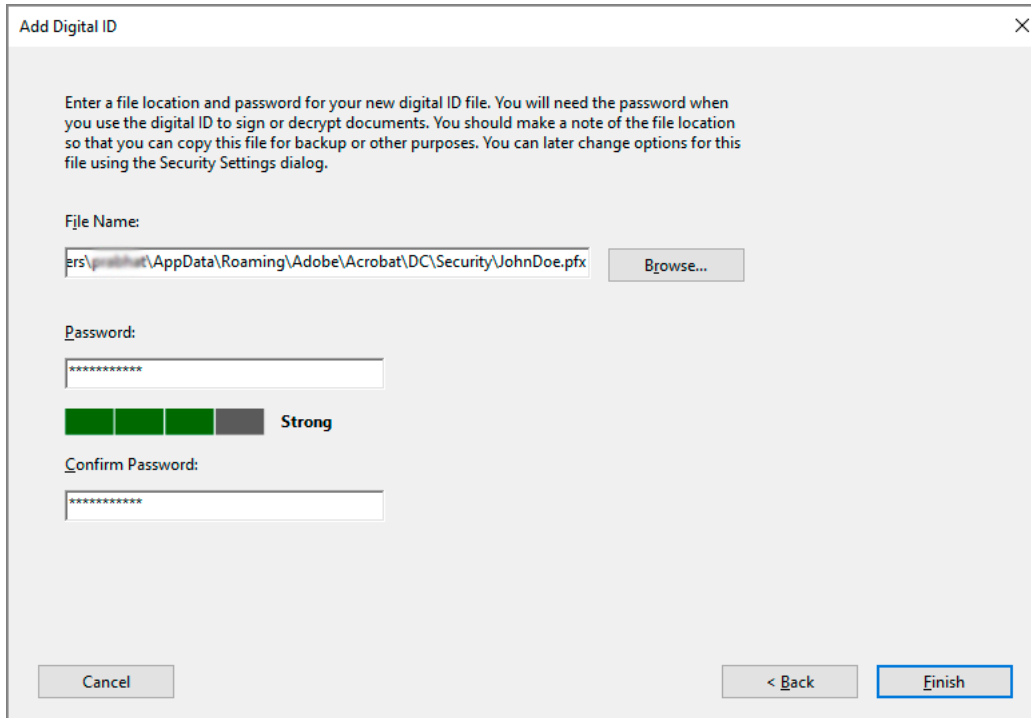
Key Algorithm: 2048-bit RSA

Use digital ID for: Digital Signatures and Data Encryption

Cancel < Back Next >

7. Do the following:

- (a) Type a password for the digital ID file. For each keystroke, the password strength meter evaluates your password and indicates the password strength using colour patterns. Reconfirm your password.
- (b) The digital ID file is stored at the default location as shown in the File Name field. If you want to save it somewhere else, click Browse and choose the location.
- (c) Click Finish.

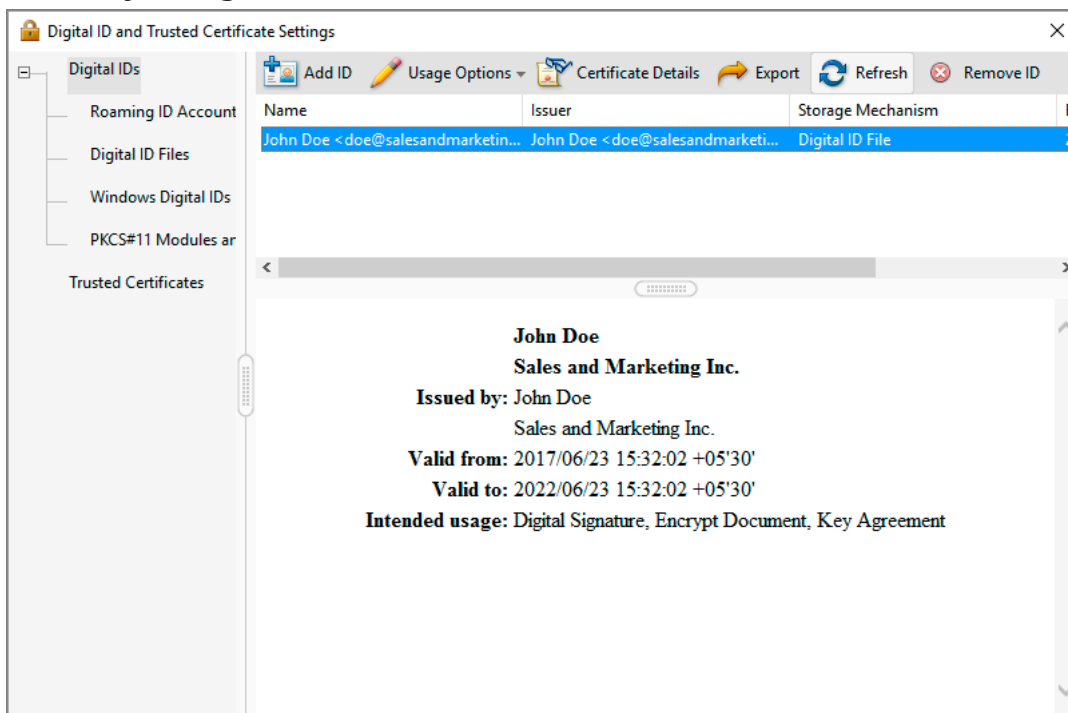


The 'Add Digital ID' dialog box contains the following elements:

- Instructions:** Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.
- File Name:** A text field showing the default path: `ers\...AppData\Roaming\Adobe\Acrobat\DC\Security\JohnDoe.pfx`. A 'Browse...' button is to the right.
- Password:** A text field with masked characters (asterisks).
- Strength Meter:** Four colored bars (green, green, green, grey) followed by the label 'Strong'.
- Confirm Password:** A second masked text field.
- Buttons:** 'Cancel', '< Back', and 'Finish'.

If a digital ID file with the same name exists, you're prompted to replace it. Click OK to replace, or browse and select a different location to store the file.

8. The ID is created. You can export and send your certificate file to contacts who can use it to validate your signature.



The 'Digital ID and Trusted Certificate Settings' window displays the following information:

- Left Pane:** A tree view showing 'Digital IDs' (with sub-items: Roaming ID Account, Digital ID Files, Windows Digital IDs, PKCS#11 Modules ar) and 'Trusted Certificates'.
- Top Bar:** Icons for 'Add ID', 'Usage Options', 'Certificate Details', 'Export', 'Refresh', and 'Remove ID'.
- Table:** A table with columns 'Name', 'Issuer', and 'Storage Mechanism'. It contains one entry: 'John Doe <doe@salesandmarketin... | John Doe <doe@salesandmarketi... | Digital ID File'.
- Details Panel:** Displays information for the selected ID:
 - Name:** John Doe
 - Issuer:** Sales and Marketing Inc.
 - Issued by:** John Doe
 - Valid from:** 2017/06/23 15:32:02 +05'30'
 - Valid to:** 2022/06/23 15:32:02 +05'30'
 - Intended usage:** Digital Signature, Encrypt Document, Key Agreement

Note: 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 signatures.

Register a digital ID

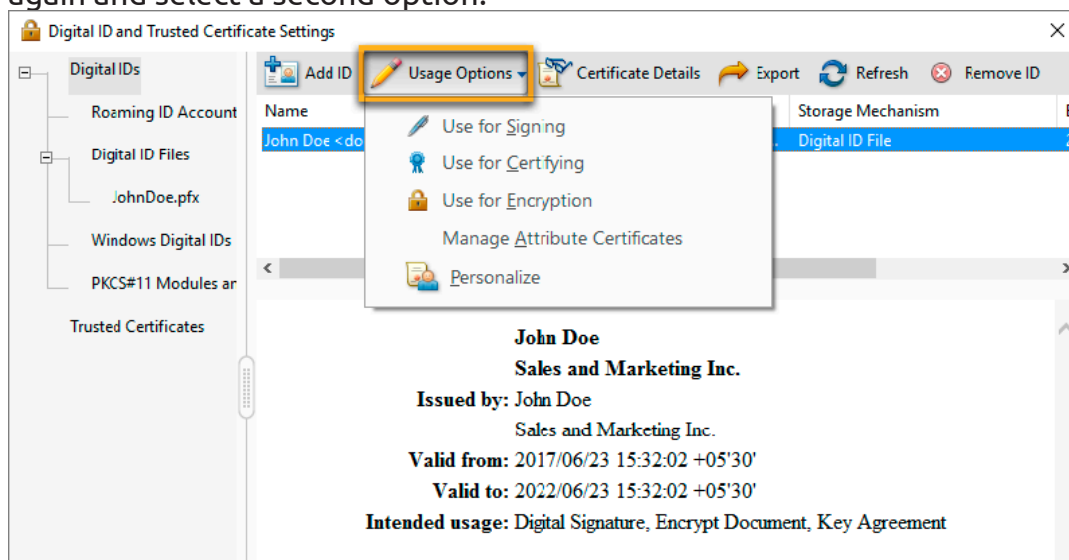
To use your digital ID, register your ID with Acrobat or Reader.

1. In Acrobat, click the Edit menu and choose Preferences > Signatures. In Identities & Trusted Certificates, and click More.
2. Select Digital IDs on the left.
3. Click the Add ID button .
4. Choose one of the following options:
 - A File** - Select this option if you obtained a digital ID as an electronic file. Follow the prompts to select the digital ID file, type your password, and add the digital ID to the list.
 - A Roaming Digital ID Stored On A Server** - Select this option to use a digital ID that's stored on a signing server. When prompted, type the server name and URL where the roaming ID is located.
 - A Device Connected To This Computer** - Select this option if you have a security token or hardware token connected to your computer.
5. Click Next, and follow the onscreen instructions to register your digital ID.

Specify the default digital ID

To avoid being prompted to select a digital ID each time you sign or certify a PDF, you can select a default digital ID.

1. In Acrobat, click the Edit menu and choose Preferences > Signatures. In Identities & Trusted Certificates, and click More.
2. Click Digital IDs on the left, and then select the digital ID you want to use as the default.
3. Click the Usage Options button , and choose a task for which you want the digital ID as the default. To specify the digital ID as the default for two tasks, click the Usage Options button again and select a second option.



A check mark appears before selected options. If you select only the signing option, the Sign icon appears next to the digital ID. If you select only the encryption option, the Lock icon appears. If you select only the certifying option, or if you select the signing and certifying options, the Blue Ribbon icon appears

Change the password and timeout for a digital ID

Passwords and timeouts can be set for PKCS #12 IDs. If the PKCS #12 ID contains multiple IDs, configure the password and timeout at the file level.

Note: *Self-signed digital IDs expire in five years. After the expiration date, you can use the ID to open, but not sign or encrypt, a document.*

1. In Acrobat, click the Edit menu and choose Preferences > Signatures. In Identities & Trusted Certificates, and click More.
2. Expand Digital IDs on the left, select Digital ID Files, and then select a digital ID on the right.
3. Click Change Password. Type the old password and a new password. For each keystroke, the password strength meter evaluates your password and indicates the password strength using colour patterns. Confirm the new password, and then click OK.
4. With the ID still selected, click the Password Timeout button.
5. Specify how often you want to be prompted for a password:
Always - Prompts you each time you use the digital ID.
After - Lets you specify an interval.
Once Per Session - Prompts you once each time you open Acrobat.
Never - You're never prompted for a password.
6. Type the password, and click OK.

Note: *Be sure to back up your password in a secure place. If you lose your password, either create a new self-signed digital ID and delete the old one, or purchase one from a third-party provider.*

Delete your digital ID

When you delete a digital ID in Acrobat, you delete the actual PKCS #12 file that contains both the private key and the certificate. Before you delete your digital ID, ensure that it isn't in use by other programs or required by any documents for decrypting.

Note: *You can delete only self-signed digital IDs that you created in Acrobat. A digital ID obtained from another provider cannot be deleted.*

1. In Acrobat, click the Edit menu and choose Preferences > Signatures. In Identities & Trusted Certificates, and click More.
2. Select Digital IDs on the left, and then select the digital ID to remove.
3. Click Remove ID.
4. Enter the password, and then click OK.

Note: *If you have forgotten the password, you cannot delete the ID from here. When you click Remove ID, the Acrobat Security dialogue box shows the complete location of the digital ID file. Go to the location, delete the file, and then relaunch Acrobat. The ID is removed from the list.*

Protecting digital IDs

By protecting your digital IDs, you can prevent unauthorized use of your private keys for signing or decrypting confidential documents. Ensure that you have a procedure in place in the event your digital ID is lost or stolen.

How to protect your digital IDs

When private keys are stored on hardware tokens, smart cards, and other hardware devices that are password- or PIN-protected, use a strong password or PIN. Never divulge your password to others. If you must write down your password, store it in a secure location. Contact your system administrator for guidelines on choosing a strong password. Keep your password strong by following these rules:

- Use eight or more characters.
- Mix uppercase and lowercase letters with numbers and special characters.
- Choose a password that is difficult to guess or hack, but that you can remember without having to write it down.
- Do not use a correctly spelled word in any language, as they are subject to “dictionary attacks” that can crack these passwords in minutes.
- Change your password on a regular basis.
- Contact your system administrator for guidelines on choosing a strong password.

To protect private keys stored in P12/PFX files, use a strong password and set your password timeout options appropriately. If using a P12 file to store private keys that you use for signing, use the default setting for password timeout option. This setting ensures that your password is always required. If using your P12 file to store private keys that are used to decrypt documents, make a backup copy of your private key or P12 file. You can use the backed up private key of P12 file to open encrypted documents if you lose your keys.

The mechanisms used to protect private keys stored in the Windows certificate store vary depending on the company that has provided the storage. Contact the provider to determine how to back up and protect these keys from unauthorized access. In general, use the strongest authentication mechanism available and create a strong password or PIN when possible.

What to do if a digital ID is lost or stolen

If your digital ID was issued by a certificate authority, immediately notify the certificate authority and request the revocation of your certificate. In addition, you should not use your private key.

If your digital ID was self-issued, destroy the private key and notify anyone to whom you sent the corresponding public key (certificate).

Securing PDFs with certificates

Note: For a full list of articles about security, see *Overview of security in Acrobat and PDF content*.

Certificate security

Use certificates to encrypt documents and to verify a digital signature. A digital signature assures recipients that the document came from you. Encryption ensures that only the intended recipient can view the contents. A certificate stores the public key component of a digital ID. For more information about digital IDs, see Digital IDs.

When you secure a PDF using a certificate, you specify the recipients and define the file access level for each recipient or group. For example, you can allow one group to sign and fill forms and another to edit text or remove pages. You can choose certificates from your list of trusted identities, files on disk, LDAP server, or the Windows certificate store (Windows only). Always include your certificate in the recipient list so that you can open the document later.

Note: If possible, encrypt documents using certificates from third-party digital IDs. If the certificate is lost or stolen, the issuing authority can replace it. If a self-signed digital ID is deleted, all PDFs that were encrypted using the certificate from that ID are inaccessible forever

Encrypt a PDF or PDF Portfolio with a certificate

To encrypt many PDFs, use Action Wizard in Acrobat Pro (Tools > Action Wizard) to apply a predefined sequence. Alternatively, edit a sequence to add the security features you want. You can also save your certificate settings as a security policy and reuse it to encrypt PDFs.

Note: For PDF Portfolios, Action Wizard applies security to the component PDFs but not to the PDF Portfolio itself. To secure the entire PDF Portfolio, apply security to the portfolio's cover sheet.

1. For a single PDF or a component PDF in a PDF Portfolio, open the PDF. For a PDF Portfolio, open the PDF Portfolio and choose View > Portfolio > Cover Sheet.
2. Choose Tools > Protect > More Options > Encrypt with Certificate. If you don't see the Protection panel, see the instructions for adding panels at Task panes.
3. At the prompt, click Yes.
4. In the Certificate Security Settings dialogue box, select the document components to encrypt.
5. From the Encryption Algorithm menu, choose a rate of encryption, and then click Next. The encryption algorithm and key size are version-specific. Recipients must have the corresponding version (or later) of Acrobat or Reader to decrypt and read the document.
 - If you select 128-bit AES, recipients must have Acrobat 7 or later or Reader 7 or later to open the document.
 - If you select 256-bit AES, Adobe Acrobat 9 or later or Adobe Reader 9 or later is required to open the document.
6. Create a recipient list for the encrypted PDF. Always include your own certificate in the recipient list so that you are able to open the document later.
 - Click Search to locate identities in a directory server or in your list of trusted identities.
 - Click Browse to locate the file that contains certificates of trusted identities.
 - To set printing and editing restrictions for the document, select recipients from the list, and then click Permissions.
7. Click Next to review your settings, and then click Finish.
When a recipient opens the PDF or PDF Portfolio, the security settings you specified for that person are used.

Change encryption settings

1. Do one of the following:
 - For a single PDF or a component PDF in a PDF Portfolio, open the PDF.
 - For a PDF Portfolio, open the PDF Portfolio and choose View > Portfolio > Cover Sheet.
2. Select Tools > Protect > More Options > Security Properties. If you don't see the Protection panel, see the instructions for adding panels at Task panes.
3. Click Change Settings.
4. Do any of the following, and then click Next.
 - To encrypt different document components, select that option.
 - To change the encryption algorithm, choose it from the menu.
5. Do any of the following:
 - To check a trusted identity, select the recipient, and then click Details.
 - To remove recipients, select one or more recipients, and then click Remove. Do not remove your own certificate unless you do not want access to the file using that certificate.

- To change permissions of recipients, select one or more recipients, and then click Permissions.
6. Click Next, and then click Finish. Click OK to close the Document Properties dialogue box, and save the document to apply your changes.

Remove encryption settings

1. Do one of the following:
 - For a single PDF or a component PDF in a PDF Portfolio, open the PDF.
 - For a PDF Portfolio, open the PDF Portfolio and choose View > Portfolio > Cover Sheet.
2. Select Tools > Protect > More Options > Remove Security. If you don't see the Protection panel, see the instructions for adding panels at Task panes.
3. If prompted, type the permissions password. If you don't know the permissions password, contact the author of the PDF.

About certificate signatures in Adobe Acrobat

Adobe Acrobat supports a range of solutions for electronic and digital signatures. These solutions include certificate signatures that let you sign PDF files with a certificate-based digital ID. Certificate signatures are also known as **digital signatures**. Acrobat lets you create your own certificate ID. However, the more common approach is to work with a certificate ID that a trusted third-party certificate authority issued. Additional signing options in Acrobat include integration with Adobe Sign.

Why use certificate signatures?

Many business transactions, including financial, legal, and other regulated transactions, require high assurance when signing documents. When documents are distributed electronically, it is important that recipients can:

- **Verify document authenticity**—confirming the identity of each person who signed the document
- **Verify document integrity**—confirming that the document has not been altered in transit
- **Certificate-based signatures** provide both of these security services. Many businesses and governments have chosen to set up a certificate-based digital signature infrastructure within their organization. They use third-party certificate authorities to provide independent identity validation

What can I do with certificate IDs?

Once certificate-based digital IDs have been provided to end users, they can use Acrobat or Acrobat Reader software to sign PDF files and validate files they receive from others.

1. Sign documents
 - Sign PDF files using certificate IDs
 - Place a signature box anywhere on the page
 - Add multiple signatures to a page
 - Add a time stamp to the document when working with a configured time stamp server
 - Certify a document with a visible or hidden signature so that recipients can verify authenticity with or without seeing a visible signature on the page

- Automatically embed certificate data to support long-term validation
2. Validate documents
- Validate all signatures, confirming the identity of everyone who signed the document
 - Validate document integrity by tracking all previously signed versions of a document to verify changes made during the document's lifecycle
 - Set privileges and permissions for others
 - Certify a document while leaving portions of it available for form filling, signatures, or comments
 - Use Acrobat Pro software to enable users of Reader to sign with certificate IDs
 - Use Acrobat Standard or Pro to encrypt a PDF document with a certificate ID to restrict usage such as printing, editing, or copying


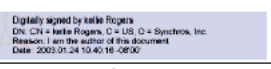
Certificate-based signatures

A certificate-based signature, like a conventional handwritten signature, identifies the person signing a document. Unlike a handwritten signature, a certificate-based signature is difficult to forge because it contains encrypted information that is unique to the signer. It can be easily verified and informs recipients whether the document was modified after the signer initially signed the document.

To sign a document with a certificate-based signature, you must obtain a digital ID or create a self-signed digital ID in Acrobat or Adobe Reader. The digital ID contains a private key and a certificate with a public key and more. The private key is used to create the certificate-based signature. The certificate is a credential that is automatically applied to the signed document. The signature is verified when recipients open the document.

When you apply a certificate-based signature, Acrobat uses a hashing algorithm to generate a message digest, which it encrypts using your private key. Acrobat embeds the encrypted message digest in the PDF, certificate details, signature image, and a version of the document when it was signed.

Credit Card Number ExpDate

Your Signature  

Please keep a copy for your records.

Certificate-based signature in a PDF form

Setting up certificate-based signatures

You can expedite the signing process and optimize your results by making the following preparations in advance.

Note: Some situations require using particular digital IDs for signing. For example, a corporation or government agency can require individuals to use only digital IDs issued by that agency to sign official documents. Inquire about the digital signature policies of your organization to determine the appropriate source of your digital ID.

- Get a digital ID from your own organization, buy a digital ID (see the Adobe website for security partners), or create a self-signed one. See Create a self-signed digital ID. You can't

apply a certificate-based signature without a digital id.

- Set the default signing method.
- Create an appearance for your certificate-based signature. (See Create the appearance of a certificate-based signature)
- Use the Preview Document mode to suppress any dynamic content that can alter the appearance of the document and mislead you into signing an unsuitable document. For information about using the Preview Document mode, see Sign in Preview Document mode.
- Review all the pages in a document before you sign. Documents can contain signature fields on multiple pages.
- Configure the signing application. Both authors and signers should configure their application environment. (See Set signing preferences)

For details on the full range of configuration options in enterprise settings, see the Digital Signatures Guide.

- Choose a signature type. Learn about approval and certification signatures to determine the type you should choose to sign your document. (See Certifying and signing documents.)

Set signing preferences

Signing workflow preferences control what you can see and do when the signing dialogue box opens. You can allow certain actions, hide and display data fields, and change how content affects the signing process. Setting signing preferences impacts your ability to see what you are signing.

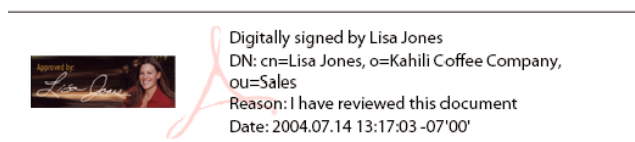
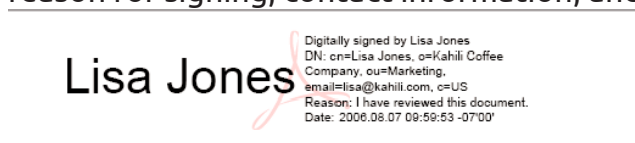
Customizing signature workflows using seed values

Seed values offer additional control to document authors by letting them specify which choices signers can make when signing a document. By applying seed values to signature fields in unsigned PDFs, authors can customize options and automate tasks. They can also specify signature requirements for items such as certificates and timestamp servers. For more information about customizing signatures using seed values, see the Digital Signature Guide (PDF) at www.adobe.com/go/learn_acr_security_en.

Create the appearance of a certificate-based signature

You determine the look of your certificate-based signature by selecting options in the Signatures panel of the Preferences dialogue box. For example, you can include an image of your handwritten signature, a company logo, or a photograph. You can also create different signatures for different purposes. For some, you can provide a greater level of detail.

A signature can also include information that helps others verify your signature, such as the reason for signing, contact information, and more.



Signature formats - A Text signature B Graphic signature

1. (Optional) If you want to include an image of your handwritten signature in the certificate-based signature, scan your signature, and save it as an image file. Place the image in a document by itself, and convert the document to PDF.
2. Right-click the signature field, and select Sign Document or Certify With Visible Signature

Note: You can also create an appearance using the Signature preferences: Edit > Preferences > Signatures (Windows)

3. From the Appearance menu in the Sign dialogue box, select Create New Appearance.
4. In the Configure Signature Appearance dialogue box, type a name for the signature you're creating. When you sign, you select the signature by this name. Therefore, use a short, descriptive title.
5. For Configure Graphic, choose an option:
 - **No Graphic** - Displays only the default icon and other information specified in the Configure Text section.
 - **Imported Graphic** - Displays an image with your certificate-based signature. Select this option to include an image of your handwritten signature. To import the image file, click File, click Browse, and then select the image file.
 - **Name** - Displays only the default signature icon and your name as it appears in your digital ID file.
6. For Configure Text, select the options that you want to appear in the signature. Distinguished Name shows the user attributes defined in your digital ID, including your name, organization, and country.
7. For Text Properties, specify the writing direction and type of digits used, and then click OK. See also Enable right-to-left languages.
8. (Optional) If the dialogue box includes the Additional Signature Information section, specify the reason for signing the document, the location, and your contact information. These options are available only if you set them as your preferences in the Creation and Appearance Preferences dialogue box (Edit > Preferences > Signatures > Creation & Appearance > More).

Add a timestamp to certificate-based signatures

You can include the date and time you signed the document as part of your certificate-based signature. Timestamps are easier to verify when they are associated with a trusted timestamp authority certificate. A timestamp helps to establish when you signed the document and reduces the chances of an invalid signature. You can obtain a timestamp from a third-party timestamp authority or the certificate authority that issued your digital ID.

Timestamps appear in the signature field and in the Signature Properties dialogue box. If a timestamp server is configured, the timestamp appears in the Date/Time tab of the Signature Properties dialogue box. If no timestamp server is configured, the signatures field displays the local time of the computer at the moment of signing.

Note: If you did not embed a timestamp when you signed the document, you can add one later to your signature. (See Establish long-term signature validation.) A timestamp applied after signing a document uses the time provided by the timestamp server.

Configure a timestamp server

To configure a timestamp server, you need the server name and the URL, which you can obtain from an administrator or a security settings file.

If you have a security settings file, install it and don't use the following instructions for configuring a server. Ensure that you obtained the security settings file from a trusted source. Don't install it without checking with your system administration or IT department.

1. Open the Preferences dialogue box.
2. Under Categories, select Signatures.
3. For Document Timestamping, click More.
4. Select Time Stamp Servers on the left.
5. Do one of the following:
 - If you have an import/export methodology file with the timestamp server settings, click the Import button . Select the file, and click Open.
 - If you have a URL for the timestamp server, click the New button . Type a name, and then type the server URL. Specify whether the server requires a username and password, and then click OK.

Set a timestamp server as the default

To be able to use a timestamp server to timestamp signatures, set it as the default server.

1. Open the Preferences dialogue box.
2. Under Categories, select Signatures.
3. For Document Timestamping, click More.
4. Select Time Stamp Servers on the left.
5. Select the timestamp server, and click the Set Default button .
6. Click OK to confirm your selection.

Validating digital signatures

Set your verification preferences in advance. This helps ensure that Digital Signatures are valid when you open a PDF and verification details appear with the signature. See Set signature verification preferences for details.

When Digital Signatures are validated, an icon appears in the document message bar to indicate the signature status. Additional status details appear in the Signatures panel and in the Signature Properties dialogue box.

Setting up digital signature validation

When you receive a signed document, you may want to validate its signature(s) to verify the signer and the signed content. Depending on how you have configured your application, validation may occur automatically. Signature validity is determined by checking the authenticity of the signature's digital ID certificate status and document integrity:

- Authenticity verification confirms that the signer's certificate or its parent certificates exist in the validator's list of trusted identities. It also confirms whether the signing certificate is valid based on the user's Acrobat or Reader configuration.

- Document integrity verification confirms whether the signed content changed after it was signed. If content changes, document integrity verification confirms whether the content changed in a manner permitted by the signer.

Set signature verification preferences

1. Open the Preferences dialogue box.
2. Under Categories, select Signatures.
3. For Verification, click More.
4. To automatically validate all signatures in a PDF when you open the document, select Verify Signatures When The Document Is Opened. This option is selected by default.
5. Select verification options as needed and click OK.

Verification Behaviour

When Verifying - These options specify methods that determine which plug-in to choose when verifying a signature. The appropriate plug-in is often selected automatically. Contact your system administrator about specific plug-in requirements for validating signatures.

Require Certificate Revocation Checking To Succeed Whenever Possible ...

Checks certificates against a list of excluded certificates during validation. This option is selected by default. If you deselect this option, the revocation status for approval signatures is ignored. The revocation status is always checked for certifying signatures.

Verification Time

Verify Signatures Using - Select an option to specify how to check the digital signature for validity. By default, you can check the time based on when the signature was created. Alternatively, check based on the current time or the time set by a timestamp server when the document was signed.

Use Expired Timestamps - Uses the secure time provided by the timestamp or embedded in the signature, even if the signature's certificate has expired. This option is selected by default. Deselecting this option allows discarding of expired timestamps.

Verification Information - Specifies whether to add verification information to the signed PDF. Default is to alert user when verification information is too large.

Windows Integration - specify whether to trust all root certificates in the Windows Certificates feature when validating signatures and certified documents. Selecting these options can compromise security.

Note: *It is not recommended to trust all root certificates in the Windows Certificate feature. Many certificates that are distributed with Windows are designed for purposes other than establishing trusted identities.*

Set the trust level of a certificate

In Acrobat or Reader, the signature of a certified or signed document is valid if you and the signer have a trust relationship. The trust level of the certificate indicates the actions for which you trust the signer.

You can change the trust settings of certificates to allow specific actions. For example, you can change the settings to enable the dynamic content and embedded JavaScript within the certified document.

1. Open the Preferences dialogue box.
2. Under Categories, select Signatures.
3. For Identities & Trusted Certificates, click More.
4. Select Trusted Certificates on the left.
5. Select a certificate from the list, and click Edit Trust.
6. In the Trust tab, select any of the following items to trust this certificate:

Use This Certificate As A Trusted Root - A root certificate is the originating authority in a chain of certificate authorities that issued the certificate. By trusting the root certificate, you trust all certificates issued by that certificate authority.

Signed Documents Or Data - Acknowledges the identity of the signer.

Certified Documents - Trusts documents in which the author has certified the document with a signature. You trust the signer for certifying documents, and you accept actions that the certified document takes.

When this option is selected, the following options are available:

Dynamic content - Allows movies, sound, and other dynamic elements to play in a certified document.

Embedded High Privilege JavaScript - Allows privileged JavaScript embedded in PDF files to run. JavaScript files can be used in malicious ways. It is prudent to select this option only when necessary on certificates you trust.

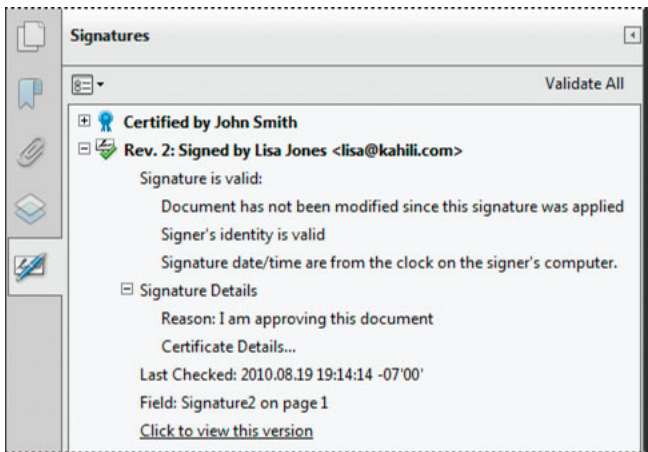
Privileged System Operations - Allows Internet connections, cross domain scripting, silent printing, external-object references, and import/export methodology operations on certified documents.

Note: *Only allow Embedded High Privilege JavaScript and Privileged System Operations for sources you trust and work with closely. For example, use these options for your employer or service provider.*

7. Click OK, close the Digital ID and Trusted Certificate Settings dialogue box, and then click OK in the Preferences dialogue box.

Signatures panel for digital signatures

The Signatures panel displays information about each digital signature in the current document and the change history of the document since the first digital signature. Each digital signature has an icon identifying its verification status. Verification details are listed beneath each signature and can be viewed by expanding the signature. The Signatures panel also provides information about the time the document was signed, and trust and signer details.



Verify signatures in the Signatures panel

Choose View > Show/Hide > Navigation Panes > Signatures, or click the Signature Panel button in the document message bar.

Note: You can right-click a signature field in the Signatures panel to do most signature-related tasks, including adding, clearing, and validating signatures. In some cases, however, the signature field becomes locked after you sign it.

Certify a PDF

When you certify a PDF, you indicate that you approve of its contents. You also specify the types of changes that are permitted for the document to remain certified. For example, suppose that a government agency creates a form with signature fields. When the form is complete, the agency certifies the document, allowing users to change only form fields and sign the document. Users can fill the form and sign the document. However, if they remove pages or add comments, the document doesn't retain its certified status.

You can apply a certifying signature only if the PDF doesn't already contain any other signatures. Certifying signatures can be visible or invisible. A blue ribbon icon in the Signatures panel indicates a valid certifying signature. A digital ID is required to add the certifying digital signature.

1. Remove content that may compromise document security, such as JavaScripts, actions, or embedded media.
2. Choose Tools > Certificates to open the panel.
3. Click one of the following options:
 - **Certify (Visible Signature)** - Places a certified signature in either an existing digital signature field (if available) or in the location you designate
 - **Certify (Invisible Signature)** - Certifies the document, but your signature appears only in the Signatures panel.
4. Follow the onscreen instructions to place the signature (if applicable), specify a digital ID, and set an option for Permitted Actions After Certifying.

Note: If you enabled the *When Signing: View Documents In Preview Mode* in the Signature preferences, click *Sign Document* in the document message bar.

5. Save the PDF using a different filename than the original file, and then close the document without making additional changes. It is a good idea to save it as a different file so that you can retain the original unsigned document.

Timestamp a document

Acrobat provides users with the capability to add a document timestamp to a PDF without also requiring an identity-based signature. A timestamp server is required to timestamp a PDF. (See [Configure a timestamp server](#).) A timestamp assures the authenticity and existence of a document at a particular time. These timestamps are compliant with the timestamp and revocation features described in Part 4 of ETSI 102 778 PDF Advanced Electronic Signatures (PAdES) standard. Users of Reader X (and later) can also timestamp a document if the document includes appropriate Reader Enabling features.

For more information on PAdES, see blogs.adobe.com/security/2009/09/eliminating_the_penone_step_at.html

1. Open the document to which you want to add a timestamp.
2. Choose Tools > Certificates > Time Stamp.
3. In the Choose Default Timestamp Server dialogue box, select a default timestamp server from the list, or add a new default timestamp server.
4. Click Next, and then save the document with the timestamp.

Validate a digital signature

If the signature status is unknown or unverified, validate the signature manually to determine the problem and possible solution. If the signature status is invalid, contact the signer about the problem.

For more information about signature warnings and valid and invalid signatures, see the Digital Signature Guide at www.adobe.com/go/acrodigsig.

You assess the validity of a Digital Signature and Timestamp by checking the Signature Properties.

1. Set your signature verification preferences. For more information, see [Set signature verification preferences](#).
2. Open the PDF containing the signature, then click the signature. The Signature Validation Status dialogue box describes the validity of the signature.
3. For more information about the Signature and Timestamp, click Signature Properties.
4. Review the Validity Summary in the Signature Properties dialogue box. The summary might display one of the following messages:
 - Signature date/time are from the clock on the signer's computer - The time is based on the local time on the signer's computer.
 - Signature is timestamped - The signer used a Timestamp Server and your settings indicate that you have a trust relationship with that timestamp server.
 - Signature is timestamped but the timestamp could not be verified - Timestamp verification requires obtaining the timestamp server's certificate to your list of trusted identities. Check with your system administrator.
 - Signature is timestamped but the timestamp has expired - Acrobat and Reader validate a timestamp based on the current time. This message is displayed if the timestamp signer's

certificate expires before the current time. To let Acrobat or Reader accept an expired timestamp, select Use Expired Timestamps in the Signature Verification Preferences dialogue box (Preferences > Signatures > Verification: More). Acrobat and Reader display an alert message when validating signatures with expired timestamp.

5. For details about the signer's certificate, such as trust settings or legal restrictions of the signature, click Show Signer's Certificate in the Signature Properties dialogue box.

If the document was modified after it was signed, check the signed version of the document and compare it to the current version.

Remove a digital signature

You cannot remove a digital signature unless you are the one who placed it and you have the digital ID for signing it installed.

Do one of the following:

- To remove a digital signature, right-click the signature field and choose Clear Signature.
- To remove all digital signatures in a PDF, choose Clear All Signature Fields from the options menu in the Signatures panel. (To open the Signatures panel, choose View > Show/Hide > Navigation Panes > Signatures.)

Securing PDFs with passwords

Password security basics

You can limit access to a PDF by setting passwords and by restricting certain features, such as printing and editing. However, you cannot prevent saving copies of a PDF. The copies have the same restrictions as the original PDF. Two types of passwords are available:

Document open password - A Document Open password (also known as a user password) requires a user to type a password to open the PDF.

Permissions password - A permissions password (also known as a master password) requires a password to change permission settings. Using a permissions password, you can restrict printing, editing, and copying content in the PDF. Recipients don't need a password to open the document in Reader or Acrobat. They do need a password to change the restrictions you've set.

If the PDF is secured with both types of passwords, it can be opened with either password. However, only the permissions password allows the user to change the restricted features.

Because of the added security, setting both types of passwords is often beneficial.

Note: *You cannot add passwords to a signed or certified document.*

Add a password to a PDF

One-click option to protect a PDF with a password


1. Open the PDF in Acrobat DC.
2. Choose File > Protect Using Password. Alternatively, you can choose Tools > Protect > Protect Using Password.
3. Select if you want to set the password for Viewing or Editing the PDF.

Protect Using Password

Requires user to enter a password for:

☒ Viewing
☐ Editing

Type Password

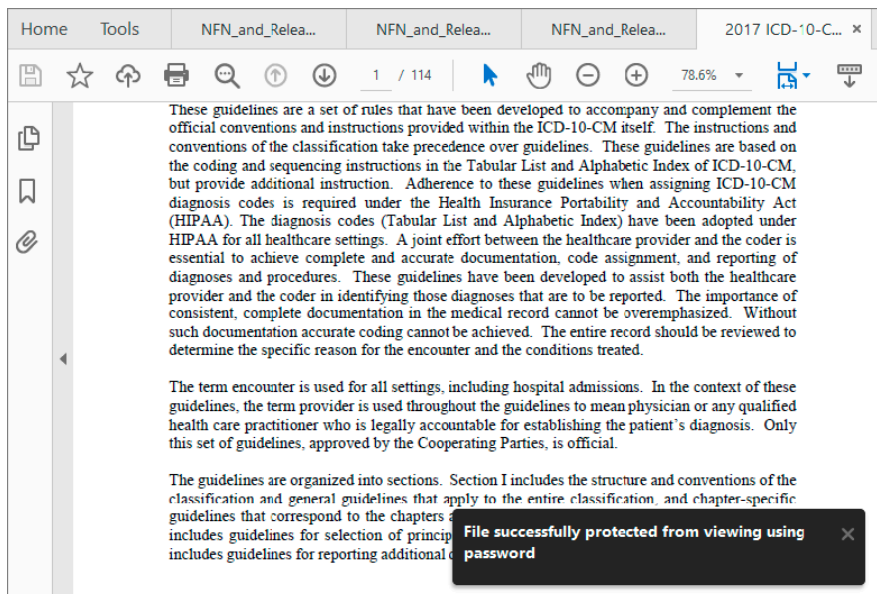
.....  Strong Password

Re-type Password

.....

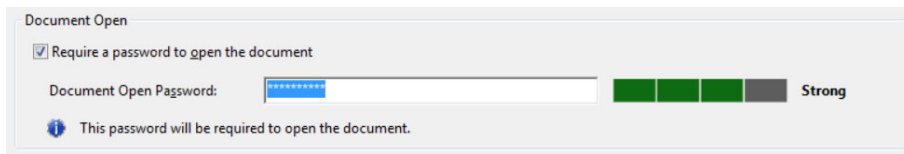
More Options ▾ Cancel Apply

4. Type and retype your password. The password strength is displayed next to your password to indicate whether the chosen password is weak, medium, strong, or best.
5. Click Apply. Acrobat displays a confirmation message that the file was successfully protected using password.



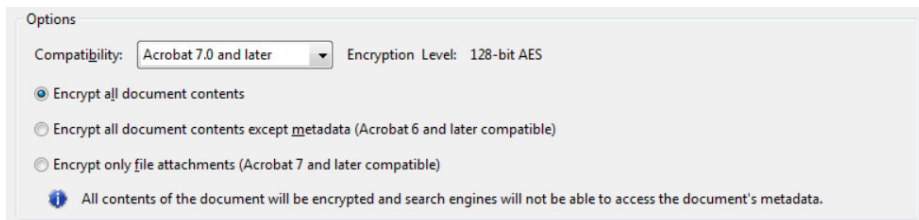
Advanced password protection

1. Open the PDF in Acrobat DC, and do one of the following:
 - Choose Tools > Protect > More Options > Encrypt with Password.
 - Choose File > Protect Using Password, and then choose Advanced Password Protection from More Options.
2. If you receive a prompt, click Yes to change the security.
3. Select Require A Password To Open The Document, then type the password in the corresponding field. For each keystroke, the password strength meter evaluates your password and indicates the password strength



Password Security - Settings let you set a password to open a PDF

4. Select an Acrobat version from the Compatibility drop-down menu. Choose a version equal to or lower than the recipients' version of Acrobat or Reader.



Options control compatibility with previous versions and type of encryption

5. Select an encryption option:
Encrypt All Document Contents - Encrypts the document and the document metadata. If this option is selected, search engines cannot access the document metadata.

Encrypt All Document Contents Except Metadata - Encrypts the contents of a document but still allows search engines access to the document metadata.

Note: The iFilter and the Find or Advance Search commands of Acrobat do not look into the PDF's metadata even when you select the Encrypt All Document Contents Except Metadata option. You can use a search tool that takes advantage of XMP metadata.

Encrypt Only File Attachments - Requires a password to open file attachments. Users can open the document without a password. Use this option to create security envelopes.

6. Click OK. At the prompt to confirm the password, retype the appropriate password in the box and click OK.

Restrict editing of a PDF

You can prevent users from changing PDFs. The restrict editing option prohibits users from editing text, moving objects, or adding form fields. Users can still fill in form fields, sign, or add comments.

1. Open the PDF in Acrobat DC, and do one of the following:
 - Choose File > Protect Using Password.
 - Choose Tools > Protect > Protect Using Password.
2. If you receive a prompt, click Yes to change the security.
3. Choose Editing, and then type and retype your password. The password strength is displayed next to your password to indicate whether the chosen password is weak, medium, or strong.


Protect Using Password

Requires user to enter a password for:

☐ Viewing


☒ **Editing**

Type Password

.....  Strong Password

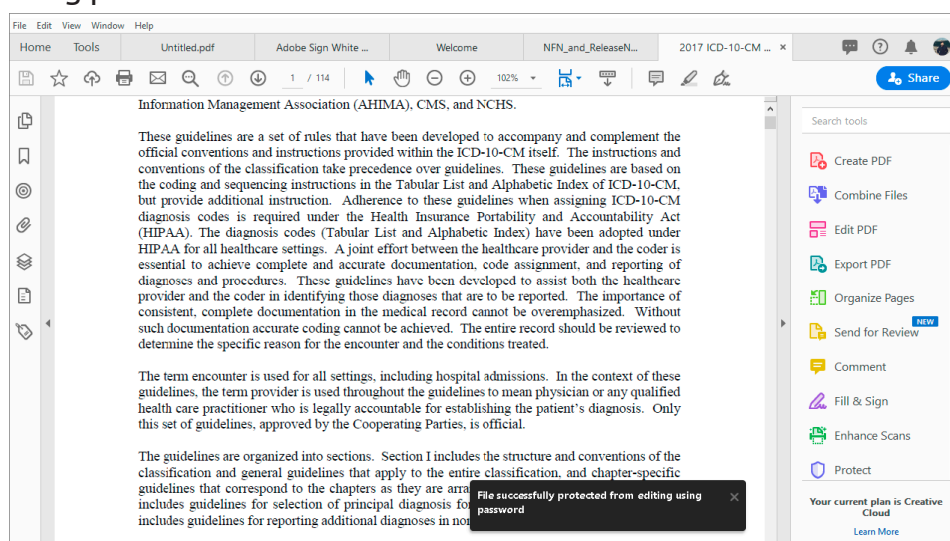
Re-type Password

.....

[More Options](#) 

[Cancel](#) [Apply](#)

- Click Apply. Acrobat displays a confirmation message that the file was successfully protected using password.



Restrict printing, editing, and copying

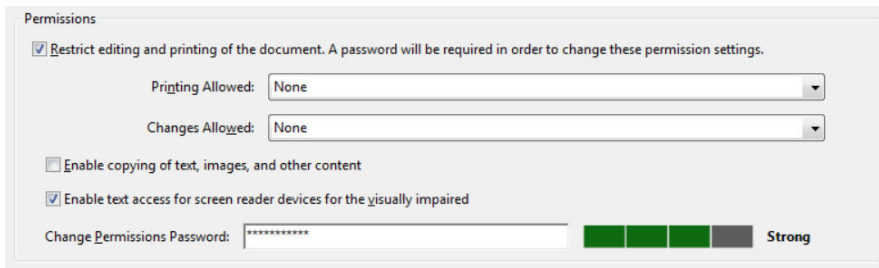
You can prevent users from printing, editing, or copying content in a PDF. You can set the restrictions you want to apply to the PDF. Users cannot change these restrictions unless you give them password.

Note: *you forget a password, you cannot recover it from the PDF. Consider keeping a backup copy of the PDF that isn't password-protected.*

- Open the PDF in Acrobat DC, and do one of the following:
 - Choose Tools > Protect > More Options > Encrypt with Password.
 - Choose File > Protect Using Password, and then choose Advanced Password Protection from More Options.
- If you receive a prompt, click Yes to change the security.
- Select Restrict Editing And Printing Of The Document.

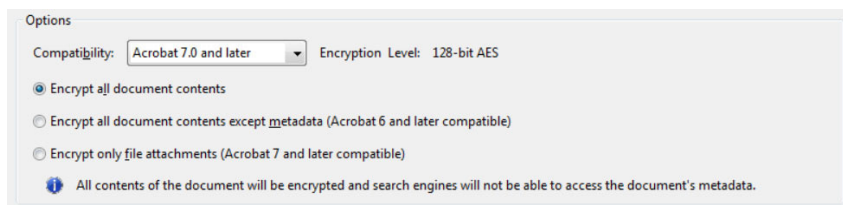
All Adobe products enforce the restrictions set by the permissions password. However, if third-party products do not support these settings, document recipients are able to bypass some or all of the restrictions you set.

4. Type the password in the corresponding field. For each keystroke, the password strength meter evaluates your password and indicates the password strength.



Password Security - Settings let you restrict printing, editing, and copying

5. Select what the user can print from the Printing Allowed menu:
 - None** - Prevents users from printing the document.
 - Low Resolution (150 dpi)** - Lets users print at no higher than 150-dpi resolution. Printing may be slower because each page is printed as a bitmap image. This option is available only if the Compatibility option is set to Acrobat 5 (PDF 1.4) or later.
 - High Resolution** - Lets users print at any resolution, directing high-quality vector output to PostScript and other printers that support advanced high-quality printing features.
6. Select what the user can change from the Changes Allowed menu:
 - None** - Prevents users from making any changes to the document that are listed in the Changes Allowed menu, such as filling in form fields and adding comments.
 - Inserting, Deleting, And Rotating Pages** - Lets users insert, delete, and rotate pages, and create bookmarks and thumbnails. This option is only available for high (128-bit RC4 or AES) encryption.
 - Filling In Form Fields And Signing Existing Signature Fields** - Lets users fill in forms and add digital signatures. This option doesn't allow them to add comments or create form fields. This option is only available for high (128-bit RC4 or AES) encryption.
 - Commenting, Filling In Form Fields, And Signing Existing Signature Fields** - Lets users add comments and digital signatures, and fill in forms. This option doesn't allow users to move page objects or create form fields.
 - Any Except Extracting Pages** - Lets users edit the document, create and fill in form fields, and add comments and digital signatures.
7. Choose any of the following options:
 - Enable Copying Of Text, Images, And Other Content** - Lets users select and copy the contents of a PDF.
 - Enable Text Access For Screen Reader Devices For The Visually Impaired** - Lets visually impaired users read the document with screen readers, but doesn't allow users to copy or extract the document's contents. This option is available only for high (128-bit RC4 or AES) encryption.
8. Select an Acrobat version from the Compatibility menu. Choose a version equal to or lower than the recipients' version of Acrobat or Reader. The Compatibility option you choose determines the type of encryption used. It is important to choose a version compatible with the recipient's version of Acrobat or Reader. For example, Acrobat 7 cannot open a PDF encrypted for Acrobat X and later.



- Acrobat 6.0 And Later (PDF 1.5) encrypts the document using 128-bit RC4.
 - Acrobat 7.0 And Later (PDF 1.6) encrypts the document using the AES encryption algorithm with a 128-bit key size.
 - Acrobat X And Later (PDF 1.7) encrypts the document using 256-bit AES. To apply 256-bit AES encryption to documents created in Acrobat 8 and 9, select Acrobat X And Later.
9. Select what you want to encrypt:
- Encrypt All Document Contents** - Encrypts the document and the document metadata. If this option is selected, search engines cannot access the document metadata.
- Encrypt All Document Contents Except Metadata** - Encrypts the contents of a document but still allows search engines access to the document metadata.
- Encrypt Only File Attachments** - Requires a password to open file attachments. Users can open the document without a password. Use this option to create security envelopes.
10. Click OK. At the prompt to confirm the password, retype the appropriate password in the box and click OK.

Remove password security

You can remove security from an open PDF if you have the permissions to do so. If the PDF is secured with a server-based security policy, only the policy author or a server administrator can change it.

1. Open the PDF, then select Tools > Protect > More Options > Remove Security.
2. Your options vary depending on the type of password security attached to the document:
 - If the document had only a Document Open password, click OK to remove it from the document.
 - If the document had a permissions password, type it in the Enter Password box, and then click OK. Click OK again to confirm the action.