



Digital IDs FAQ

- > What is a digital ID?
- > Why do I need one?
- > What are self-signed digital IDs?
- > What are IDs from certificate authorities?
- > How do I recover or reset my digital ID's password?

ON THIS PAGE


[Digital IDs FAQ](#)[Create a self-signed digital ID](#)[Register a digital ID](#)[Specify the default digital ID](#)[Change the password and timeout for a digital ID](#)[Delete your digital ID](#)[Protecting digital IDs](#)[Smart cards and hardware tokens](#)

Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC

Last Published: June 2, 2020

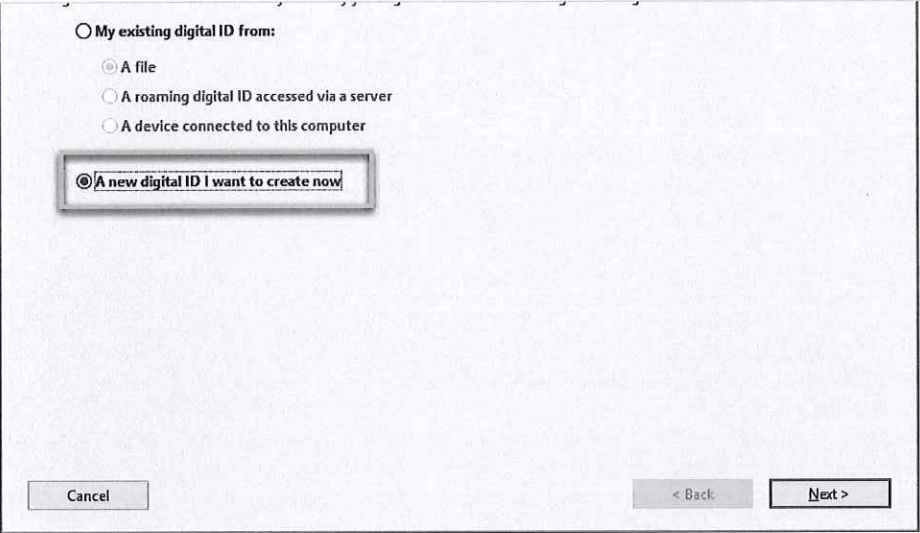
Create a self-signed digital ID

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**.



ON THIS PAGE

[Digital IDs FAQ](#)

[Create a self-signed digital ID](#)

[Register a digital ID](#)

[Specify the default digital ID](#)

[Change the password and timeout for a digital ID](#)

[Delete your digital ID](#)

[Protecting digital IDs](#)

[Smart cards and hardware tokens](#)

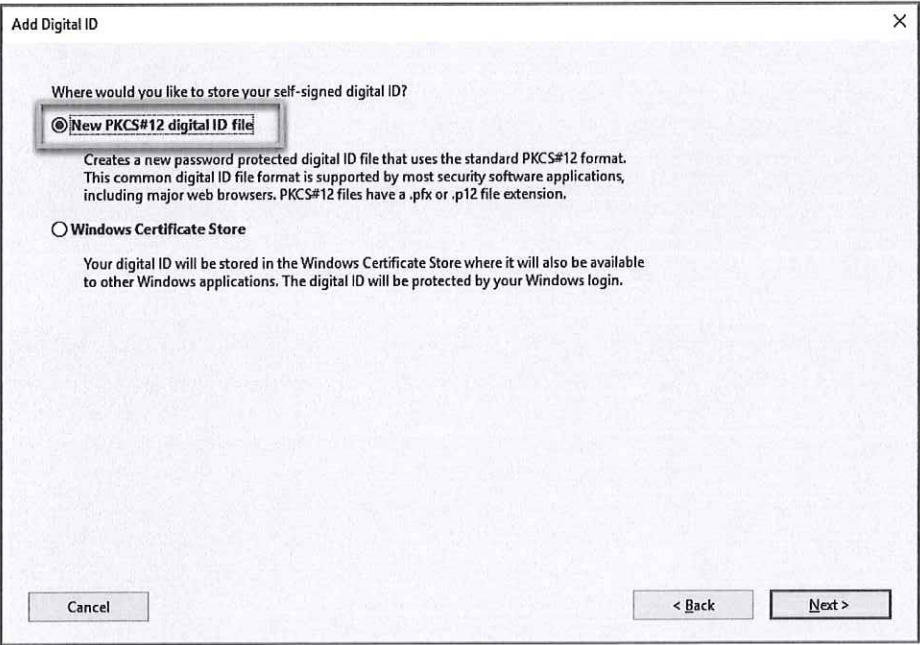
[Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC](#)

[Last Published: June 2, 2020](#)

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.



- 6 Do the following:
- a. 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.
 - b. 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.
 - c. From the **Use Digital ID For** menu, choose whether you want to use the digital ID for signatures, data encryption, or both.





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 >

ON THIS PAGE

[Digital IDs FAQ](#)[Create a self-signed digital ID](#)[Register a digital ID](#)[Specify the default digital ID](#)[Change the password and timeout for a digital ID](#)[Delete your digital ID](#)[Protecting digital IDs](#)[Smart cards and hardware tokens](#)

Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC

Last Published: June 2, 2020

7 Do the following:

- Type a password for the digital ID file. For each keystroke, the password strength meter evaluates your password and indicates the password strength using color patterns. Reconfirm your password.
- 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.
- Click **Finish**.

Add Digital ID

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: C:\Users\JohnDoe\AppData\Roaming\Adobe\Acrobat\DC\Security\JohnDoe.pfx Browse...

Password: [password field] Strong

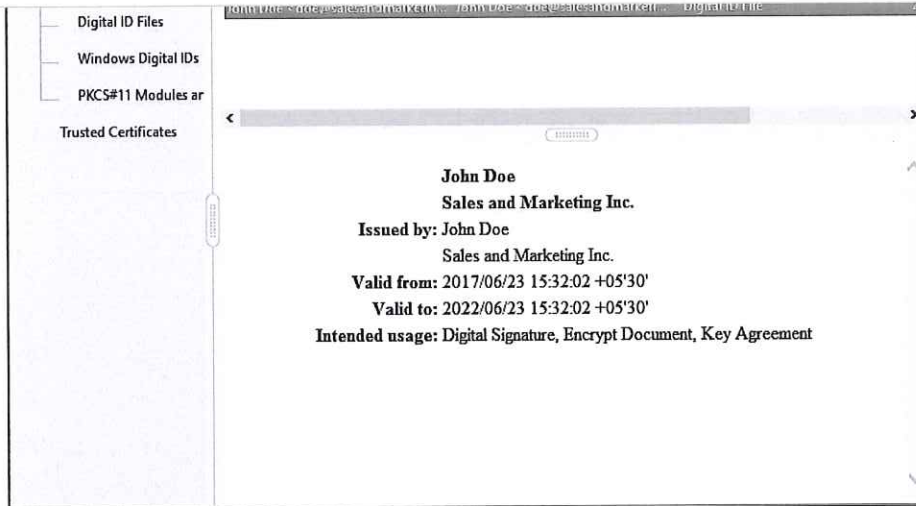
Confirm Password: [password field]

Cancel < Back 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.





ON THIS PAGE

[Digital IDs FAQ](#)[Create a self-signed digital ID](#)[Register a digital ID](#)[Specify the default digital ID](#)[Change the password and timeout for a digital ID](#)[Delete your digital ID](#)[Protecting digital IDs](#)[Smart cards and hardware tokens](#)

Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC


Last Published: June 2, 2020

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.

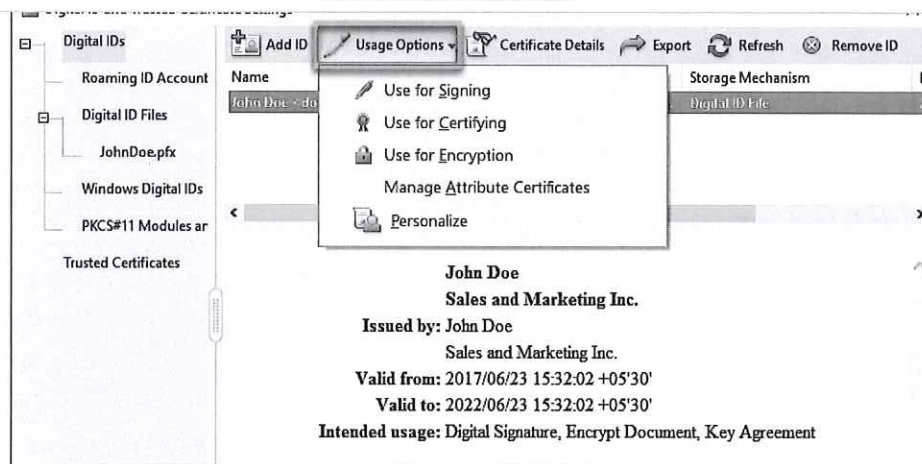
- 5 Click **Next**, and follow the onscreen instructions to register your digital ID.

Specify the default digital ID

To avoid being prompted to select a digital ID each time your 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








ON THIS PAGE

[Digital IDs FAQ](#)[Create a self-signed digital ID](#)[Register a digital ID](#)[Specify the default digital ID](#)[Change the password and timeout for a digital ID](#)[Delete your digital ID](#)[Protecting digital IDs](#)[Smart cards and hardware tokens](#)

Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC

Last Published: June 2, 2020

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.

Note:

To clear a default digital ID, repeat these steps, and deselect the usage options you selected.

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 color 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**.





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 dialog 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.

ON THIS PAGE[Digital IDs FAQ](#)[Create a self-signed digital ID](#)[Register a digital ID](#)[Specify the default digital ID](#)[Change the password and timeout for a digital ID](#)[Delete your digital ID](#)[Protecting digital IDs](#)[Smart cards and hardware tokens](#)

Applies to: Adobe Acrobat 2017, Adobe Acrobat 2020, Adobe Acrobat DC

Last Published: June 2, 2020

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.

