




# **Learn Acrobat: Request E-signatures**



**Adobe**

# Send a document to get signatures from others

1. Open the PDF form in Acrobat or Acrobat Reader, and then choose **All tools > Request E-signatures**. Alternatively, you can select **Sign** from the top toolbar.
2. The Request Signatures window is displayed. It displays the fields progressively as you enter the details. The left pane provides information on getting signatures from others workflow. In the recipients field, add recipient email addresses in the order you want the document to be signed.

**Get e-signatures *faster* than email**

-  Recipients sign in minutes. No file printing or scanning required.
-  Recipients receive an email link to sign online for free without downloading Acrobat.
-  E-signatures are trusted and secure.

 [See how it works](#) 

**Add recipients to e-sign this document**

[Cancel](#) [Specify where to sign](#)


*Request signatures – Add recipients*

3. The Mail and Message fields are just like the ones you use for sending an email and appear to your recipients in the same way. Change the default text in the Subject & Message area as appropriate.  
Optional: If you want to add more people just for information, use the Add CC button to add their email addresses to the CC list.


Enter the desired information and do one of the following:

- (Optional) To explore advanced options including signer authentication, reminders, and more, click **More Options**.
- To add form fields and specify where to sign, click **Specify where to sign**.


### Get e-signatures *faster* than email





Recipients sign in minutes. No file printing or scanning required.




Recipients receive an email link to sign online for free without downloading Acrobat.



E-signatures are trusted and secure.


[See how it works](#)


### Add recipients to e-sign this document



×
|

[Add Cc](#)

[More Options](#)

Your file will be uploaded as an agreement for e-signing.

Cancel
Specify where to sign

*Request signatures – Add Cc, subject, message, More Options*

- If you don't want to use the **More Options**, skip the next optional step.
- 4. (Optional) Click **More Options**, if you want to specify advanced options, such as signer authentication, reminders, and more.
  - By default, the **Complete in Order** setting is turned on. The numbers by the email addresses reflect the participation order. If you do not want to follow any particular order for signing, toggle the switch to **Complete In Any Order**. (Optional) Click **Add Me**, if you want to be included as a signer of the document.
  - Specify authentication type like **Email, Password, Social Identity, Knowledge-Based Authentication, Phone, or Acrobat Sign**.
  - **Password Protect** the PDF file.
  - Set a **Completion Deadline**.
  - Specify the **Recipient's Language** in the email sent.

More or

#### Advanced Options

5. The Specify Where to Fill & Sign window is displayed showing options based on whether you have added one signer or multiple signers.
  - **Simplified mode for single signer**  
If you've added one signer, the Advanced Editing mode is off, and you see the simplified option as shown below. To place a signature or another field, click at the desired location in the document and then set the field's properties from its context menu.



- You can switch the assignee of any field using the floating toolbar. The assigned colors to the signers make it easy to distinguish the fields for respective signers.

- Advanced mode for multiple signers**

If you've added multiple signers, you see the options as shown below. Click



the button to place the detected form fields in the PDF document. Alternatively, drag fields from the tabs in the right pane and drop the fields where desired in the document.

**Request Signatures**

Field Templates ▾

Close

Add signers Specify where to fill and sign Send and track progress

Field Templates ▾

Relative to Page

Navigate to...

**FORM 30**

[See Rule 55(2) and (3)]

**APPLICATION FOR INTIMATION AND TRANSFER OF OWNERSHIP OF A MOTOR VEHICLE**

(To be made in duplicate if the vehicle is held under an agreement of hire-purchase / lease / hypothecation. The duplicate copy with the endorsement of the Registering Authority to be returned to the Financier simultaneously on making the entry of the transfer of ownership in the Certificate of Registration and Registration Record in Form 24)

To

The Registering Authority.....

**PART I – FOR THE USE OF THE TRANSFEROR**

Name of the transferor.....

Son/Wife/Daughter of.....

Full Address.....

.....

I/We, hereby declare that I/We have on this.....day of the year.....sold my/our motor vehicle bearing Registration mark..... to Shri./Smt ..... Son/Wife/Daughter

**Advanced editing on**

RECIPIENTS

admin@domain.com (Signer)

Signature Fields ▾

Signer Info Fields ▾

Data Fields ▾

More Fields ▾

Transaction Fields ▾

[Reset Fields](#)

☐ Save as template

**Send**

**Note:** You can switch between simplified mode and advanced mode for multiple signers. To switch mode, turn off the **Advanced Editing** switch in the right-pane.

- When you've placed all desired fields in the document, click **Send**. The document is sent for signature to the recipients and a confirmation notice is displayed.



---

## Signer's experience

A signer receives an email with a link to sign the agreement. Also, if the signer uses Acrobat or Acrobat Reader desktop application, the signer sees a notification that an agreement has been shared for signing.

**Note:** Signers are not required to sign up or purchase any Adobe product to sign agreements. They can sign agreements using a web browser, mobile device, or Acrobat / Acrobat Reader desktop application.

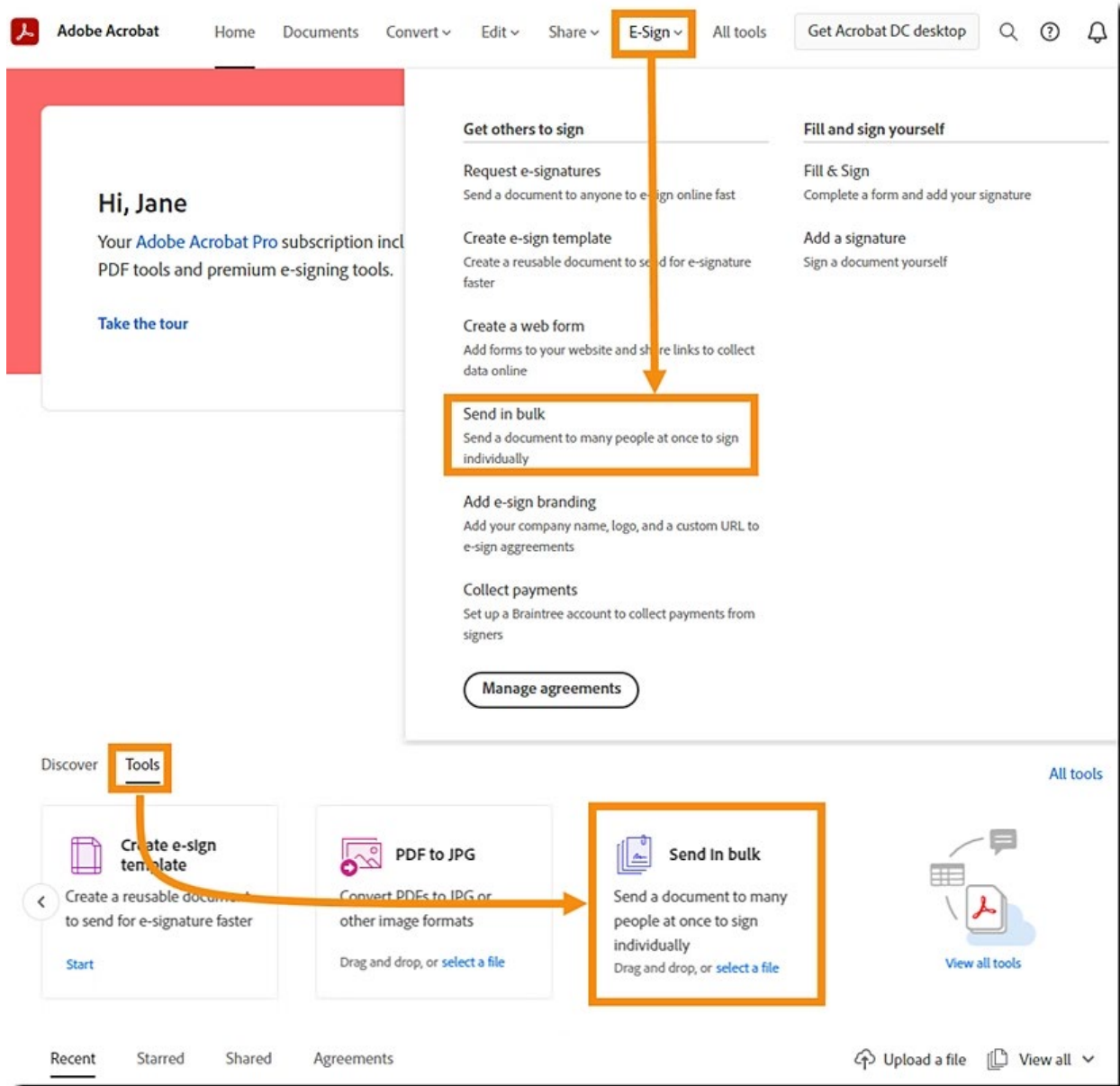
*Send in bulk* allows you to upload a form and use that as a template to create and send many (hundreds!) of unique agreements, each dedicated to one external signer. Each agreement is insulated from the others and contains its own audit report. Each recipient is unaware of all other recipients.

The sender has access to the agreements through their Home or Documents tab or through the *Send in bulk* template, which contains an Agreements report that tracks the overall status of the child agreements created from the template. Additionally, the sender can export the field-level data of all completed agreements in a CSV format using the Download Form Field Data action.

To access the Send in bulk feature, do one of the following:

- In the Acrobat desktop app, go to the **Tools** center, scroll down to the **E-Sign** section, and then select **Send in bulk**.
- Sign in to [Acrobat online](#), select the **E-Sign** menu in the top navigation bar, and then select **Send in bulk**.





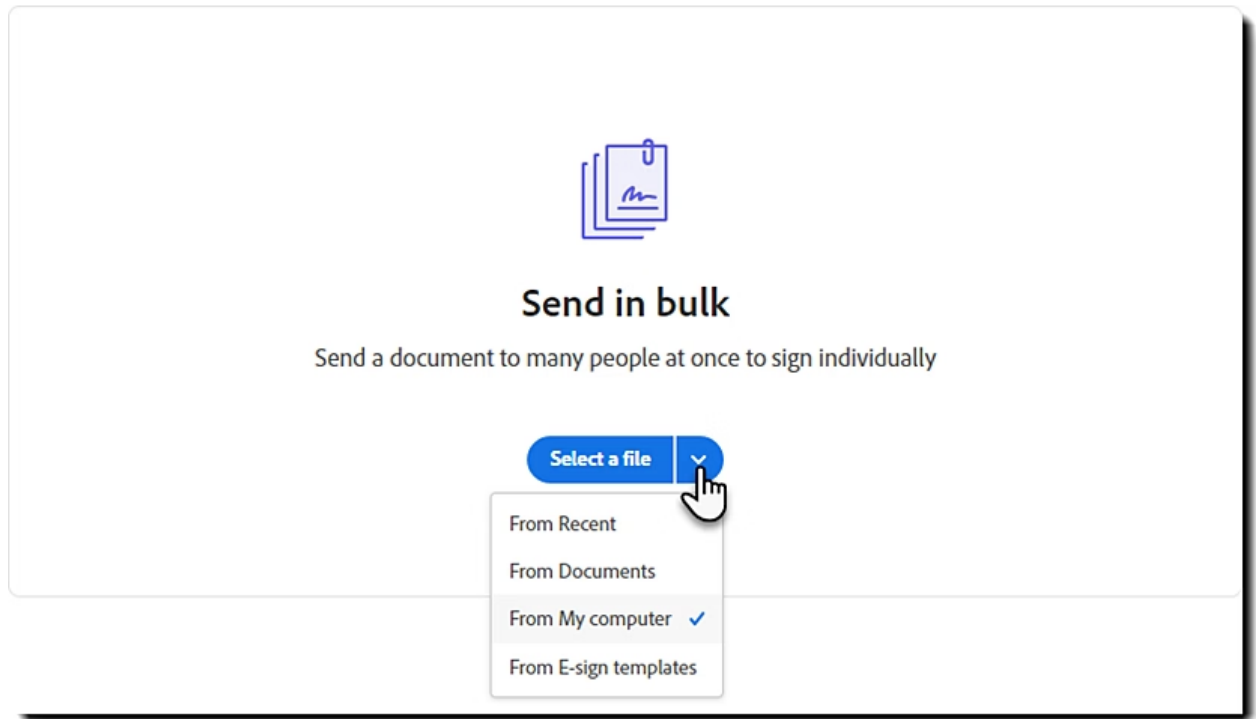
## Steps to send in bulk

1. Select the **Send in Bulk** tool as explained earlier. The Send in bulk file upload page is displayed.

2. **Add a file:**

Upload (by search or drag-and-drop) the primary file that you are using to build your agreement template.

The selector on the right of the *Select a file* button allows you to choose from the source where the file resides. The default is your local system.



Once a file is selected, the configuration page loads.

### 3. Add participants:

#### 1. List the participants required.

- The *Sign* action is assigned by default.
- The *Sign* action allows the participant to enter field data and sign the agreement.
- Up to 50 participants are supported.
- Each participant listed receives their own agreement.

#### 2. Enter recipient email addresses followed by commas, or copy and paste a list of email addresses into the Email field.

#### 3. Configure participant authentication by clicking the key icon to the right of the participant.

- **Email** is the default authentication method for confirming the identity of each participant and is sufficient to obtain a legal signature in most cases.

**Password** authentication can be added to increase security. When configured, the participant must enter the password before they can interact with the agreement.

#### 4. . (Optional) Add yourself and/or CC'd parties

- Click **Add me** to add yourself as a counter signer.

- Click **Add cc** to add people you want to be copied when the agreement is sent and complete.

Send in Bulk
Add
Prepare
Review
Close
Next

## Request signatures in bulk

Sending in bulk saves you time on the repetitive task of sending the same document to multiple people, such as privacy agreements. Each person receives a unique copy, and you can track when each person signs.

### Add recipients \*

Enter up to 50 recipient email addresses. You can also add yourself as a counter signer or add people you want copied on agreement activity.

	Action	Email
1		calliope@jupiter.dom × io@jupiter.dom × gert@jupiter.dom × elmo@jupiter.dom ×
2		casey@caseyjones.dom
	CC	dave@caseyjones.dom ×

### Add files \*

	GlobalCorp Client Services Agreement.pdf
--	--

Drag and drop, or [select files](#)

#### Add participant authentication

Email is the default authentication method for confirming the identity of each participant. You can increase security for a given person by adding a second authentication method before they can interact with the form.

##### Password

Require participants to enter a password, which you must share with them.

Set password	Confirm password
Thingy123	Thingy123

The password must be 6 to 32 characters.

Hide Password





5. (Optional) Add additional files if needed.

The initial file selected to start the agreement template is already attached.

Upload any additional file(s) that you require.

- Multiple files can be uploaded.
- All files uploaded are concatenated into one file for the final agreement.
- The order the files are listed dictates how the final agreement will look.
  - You can click and drag the files to sort them.

### Add files \*

		GlobalCorp Client Services Agreement.pdf	×
		Mutual Confidentiality Agreement.docx	×
Drag and drop, or <a href="#">select files</a>			

### Edit agreement details

- You must share this password with the participants out-of-band.
6. **Add Agreement Details:**
- Name your agreement. All agreements generated from the *Send in bulk* template will have the same agreement name.
  - Change the default text in the *Message* field as appropriate.
7. **Edit the Agreement settings** (Optional):

By default, agreements do not require a password to view the completed agreement, nor do they have reminders set for participants

- Select **Add access password** if you require recipients to enter a password to open and view the signed PDF file.
- Select **Set Reminder** to set the frequency of reminders to be sent until the agreement is completed.

### Edit agreement details

Agreement name \*

GlobalCorp Client Services Agreement

Message

Please review and complete GlobalCorp Client Services Agreement.

#### Agreement settings

- A reminder is not set for recipients
- A password is not required to view

#### Agreement settings

##### ☒ Add a reminder

Set up an email notification to remind recipients to complete the agreement.

- ☐ Every day ☐ Every other day  
☐ Every week ☐ Every third day  
☒ Every business day ☐ Every fifth day

##### ☒ Add an access password

Add a password to restrict access to each completed agreement.


Set password

Confirm password

Stuffs321

Stuffs321

The password must be 6 to 32 characters.



 Hide Password

Cancel

Save

8. Click **Next** in the upper right corner of the window.


The document is now ready to add any fields that you want the signers to fill in or sign.

  Send in Bulk 

Add

Prepare

Review


Close **Next** 


## Request signatures in bulk

Sending in bulk saves you time on the repetitive task of sending the same document to multiple people, such as privacy agreements. Each person receives a unique copy, and you can track when each person signs.

### Add recipients \*

Enter up to 50 recipient email addresses. You can also add yourself as a counter signer or add people you want copied on agreement activity.

Action	Email
	<div>calliope@jupiter.dom x io@jupiter.dom x gert@jupiter.dom x</div> <div>elmo@jupiter.dom x</div>



**Note:** If you have added multiple files, the files are converted into PDFs and combined into a single document. The combined document is opened for you to add fields.

## 9. Prepare the Agreement and Add Fields:

You can now add any necessary fields to the agreement. Remember that a **Signature** field must be placed for each signer (including internal counter-signers).

There are two methods to apply fields:

1. *Simple Authoring* is loaded by default in most instances. Simple authoring:

- Is limited to the most common types of fields:
  - Text input (All Text fields are flagged as Required)
  - Signature
  - Signer's name (Printed)
  - Signer's email
  - Signature date (Read-Only; Supplied by the system)
  - Checkbox
- Places fields anywhere you click on the document.
- Allows resizing of fields by clicking the bottom right corner of the field (blue triangle) and dragging the field to size.

The screenshot shows the 'GlobalCorp Client Services Agreement' document in a web-based editor. The top navigation bar includes a home icon, the document title, and a progress bar with 'Add', 'Prepare', and 'Review' stages. A 'Next' button is visible. The document content is divided into two main sections: 'Client Information' and 'Client Services'. The 'Client Information' section contains a form with fields for Company Name, Address, Phone, Fax, Order Number, Contact, Email, and Website. The 'Client Services' section is a table with two columns: 'Client Services' and 'Investment'. The 'Client Services' column lists various services like 'New client onramp', 'Survey evaluation', etc. The 'Investment' column is currently empty. On the right side of the editor, there is a sidebar with a toggle for 'Advanced editing off' and a 'Specify where to sign' section with instructions on how to place a form field.

Client Information	
Company Name *	
Address *	
Phone	Contact
Fax	Email
Order Number	Website

Client Services	Investment
New Customer Program <ul style="list-style-type: none"><li>• New client onramp</li><li>• Survey evaluation</li><li>• Set up properties and processes</li><li>• Connect to vendor channels</li><li>• Marketing services</li><li>• Staff training</li><li>• Customer service 24/7/365</li></ul>	

2. *Advanced Authoring* can be enabled by selecting the toggle in the upper right corner. Advanced authoring:

- Allows access to [all field types](#) (highlighted in yellow)
- Supports [form field detection](#) (highlighted in green)
- Supports [Prefill fields](#) (highlighted in pink)
- Supports [field assignment](#) (highlighted in purple and pink)
- Supports [field validation](#)

- Supports [calculated fields](#)
- Supports [conditional fields](#)
- Allows [control of the field text font/appearance](#)
- Places fields by dragging them from the menu on the right side of the document.
- Allows resizing of fields by clicking the bottom right corner of the field (blue triangle) and dragging the field to size.

GlobalCorp Client Services Agreement

Add Prepare Review Close Next

Relative to Page Custom Field 1

**globalcorp** CLIENT SERVICES AGREEMENT

Client Information

Company Name		
Address		Contact
Phone		Email
Fax		Website
Order Number		

Client Services

<b>New Customer Program</b>	<ul style="list-style-type: none"> <li>New client onramp</li> <li>Survey evaluation</li> <li>Set up properties and processes</li> <li>Connect to vendor channels</li> <li>Marketing services</li> <li>Staff training</li> <li>Customer service 24/7/365</li> </ul>
-----------------------------	--

Enter Payment Information

PO Number	
-----------	--

**TERMS AND CONDITIONS**

**Terms and Renewal:** The initial term of this Agreement is twelve (12) months, commencing on the date of execution of this Agreement. Thereafter, the Agreement will automatically renew in successive...

**Custom Field 1**

Assigned To: Casey Jones (me)

Field Type: Text Input

Value Type: Entered Value

☒ Required ☐ Read Only

☐ Mask field data ☐ Multi-line data entry

Default Value:

Tooltip:

Validation: None

Conditions:

Appearance:

Font: Lato Auto

Alignment: Color:

Tools:

Delete Field Cancel OK

**Advanced editing on**

**RECIPIENTS**

Casey Jones (Prefill)

**Signature Fields**

**Signer Info Fields**

**Data Fields**

Text Input

Drop Down

Check Box

Radio Button

Image

**More Fields**


**Transaction Fields**

**Note:** You can switch between Simple and Advanced mode by selecting the **Advanced editing (on|off)** toggle in the upper-right corner.

10. Select **Next** (in the top-right corner) after all the fields have been placed.

11. **Review and Send**

Review the agreement information and **Send** if everything is correct

 GlobalCorp Client Services Agreement

Add

Prepare

Review

Close

Send

Review and send

From

Casey Jones

To


1 calliope@jupiter.dom + 3 more recipients

2 casey@caseyjones.dom

Cc

dave@caseyjones.dom

Files

 GlobalCorp Client Services Agreement.pdf

Email subject

Your signature requested on GlobalCorp Client Services Agreement

Message

Please review and complete the GlobalCorp Client Services Agreement.

Settings

- A reminder is set for recipients
- A password is required to view the completed agreement

## 12. Confirmation

A confirmation message is shown verifying the agreement has been sent successfully.

There are three options to progress from the post-sending page:

- **Manage agreements** - Opens the *Bulk Sends* page with all your agreements: track status, access audit trails, send reminder
- **Send another document in bulk**- Prepare another document to send to many people
- Click **Close** to return to the Acrobat online Home page





## GlobalCorp Client Services Agreement has been queued for sending to the other parties to sign

Each recipient will receive a PDF copy once the agreement is completed. You can track activity in your [Documents list](#).

Your recipients will be reminded on every business day.

### Recommended actions



#### Send another document in bulk

Prepare another document to send to many at once.



#### Manage agreements

Track agreement status, access audit trails, send reminders, and more.

## Manage your bulk sends

Bulk sends can be managed from your *Documents* tab.

1. Navigate to the **Documents** tab.
2. Select **Bulk Sends** in the list of *Your documents* on the left side of the window.
3. Single-click the Bulk Send you to want to access, opening the context menu on the right side of the window. The context menu on the right side contains five distinct sections:
  - **Metadata** (red square): At the top of the menu is the metadata for the Bulk Send template:
    - Image of the Bulk Sends' first page
    - The title of the Bulk Send
    - The date the Bulk Send was sent to the participants
    - The email value of the userID that created the Bulk Send
    - The current status of the whole Bulk Send
    - The *Message* provided in the initial email

- Any CCd parties (listed by email value)

The screenshot shows the Adobe Acrobat Bulk sends interface. The top navigation bar includes the Adobe Acrobat logo and various menu items like Home, Documents, Sign, Convert, Edit, Share, and All tools. On the left, there's a sidebar with categories like 'Your documents', 'Starred', 'Shared by you', 'Shared by others', 'All agreements', 'In progress (10)', 'Waiting for you (4)', 'Completed', 'Canceled', 'Expired', 'Draft', 'Templates', 'Web forms', and 'Bulk sends'. The main area is titled 'Bulk sends' and contains a table with columns 'TITLE' and 'STATUS'. The table lists several documents, including 'GlobalCorp Client Services Agreement' and 'FieldtripPermission'. A red box highlights the details for the 'GlobalCorp Client Services Agreement' document, showing its creation date, sender, status, and message. A blue box highlights the 'Actions' menu, which includes options like 'Open Bulk Send', 'Reminders (1)', 'Download PDF', 'Download Form Field Data', 'Download Individual Files (1)', 'Hide Bulk Send', 'Share', 'View Activity Report', and 'Add Notes'. A green box highlights the 'Agreements' summary, showing counts for 'All', 'In Progress', 'Canceled', 'Completed', and 'Waiting for You'. An orange box highlights the 'Activity' link at the bottom.

TITLE	STATUS
GlobalCorp Client Services Agreement	Out for signature
GlobalCorp Client Services Agreement	Out for signature
GlobalCorp Client ... ices Agreement - Flat	Draft
GlobalCorp Client Services Agreement	Draft
FieldtripPermission	Draft
GlobalCorp Client Services Agreement	Draft
GlobalCorp Client Services Agreement	Draft
Registration Form	Out for signature
Soccer Registration Form	Out for signature
Pachi Chen-Wong	Out for signature

**GlobalCorp Client Services Agreement**  
Created Sep 07, 2021 7:53 PM  
From: casey@caseyjones.dom  
Status: Out for Signature  
Message: Please review and complete the GlobalCorp Client Services Agreement.  
CC: dave@caseyjones.dom

**Actions**

- Open Bulk Send
- Reminders (1)
- Download PDF
- Download Form Field Data
- Download Individual Files (1)
- Hide Bulk Send
- Share
- View Activity Report
- Add Notes

**Agreements**

- 4 All
- 1 In Progress
- 1 Canceled
- 1 Completed
- 1 Waiting for You

> Activity

- Actions menu** (blue square) - This section contains all of the actions you can take regarding the Bulk Send (parent template). Click the **See More** link at the bottom right of the section to see all values:
- Open Bulk Send** - Opens the Bulk Send template document for viewing only. No fields are available
- Reminders** – Add a reminder for yourself or everyone else who still needs to sign.
- Cancel:** Cancel the Bulk Send.
- Download PDF** - Downloads the whole (blank) PDF.

- **Download Form Field Data** - Downloads a CSV file of the field-level content for all child agreements spawned from this parent Bulk Send that have been completed.
- **Download Individual Files** - Provides the option to download the individual PDF files if multiple files were used to create the web form.
- **Hide/Unhide Bulk Send**- Hide/Unhiding the Bulk Send simply removes (or adds) the Bulk Send from your normal Manage page view.
- **Share** - Shares the Bulk Send along with its status with the user email you provide. Shared web forms can be viewed on the Manage page, but do not allow editing.
- A PDF copy of the Bulk Send parent document (without added fields) is emailed to the sharee.
- **View Activity Report**
- View the current status of all child agreements created by the Bulk Send parent template.
- **Add Notes** - Allows the user to make personal notes for the Bulk Send.
- **Agreements summary/filter** (green square) - The *Agreements* section shows up to five values that reflect the number of child agreements in each status. If no child agreements are in a given status, the status is not exposed, so you may see fewer than five line items. Clicking any one status will produce a filter list of those child agreements:
- **All** - Shows all (child) agreements that have spawned from the Bulk Send (parent template).
- **In Progress** - Indicates that the child agreement is waiting for the participant to complete their signature.
- **Canceled** - Indicates that either the sender explicitly canceled the child agreement, or the participant declined to sign.
- **Completed** - Completed agreements have successfully obtained all signatures from all participants on the agreement.
- **Waiting for You** - Indicates that the agreement is waiting for the sender to countersign the agreement.
- **Activity** for the Bulk Send parent template (orange square) - The **Activity** > link at the bottom of the context panel opens a chronological list of the enablement actions taken against the (parent) Bulk Send template (eg: *Creation, Completed* events).

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 certificate ID. However, the common approach is to work with a certificate ID from a trusted third-party certificate authority. Additional signing options in Acrobat include integration with [Adobe Acrobat 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's 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. Examples include:

For instance, companies in the European Union who need to comply with advanced or qualified electronic signature requirements in [eIDAS e-signature regulation](#) or the [ETSI PAdES standard](#) (PDF Advanced Electronic Signatures).

## 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.

### 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 timestamp 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

### 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 9 or later 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

## What if my organization isn't prepared to set up certificate-based signatures?

Consider signing up for [Adobe Acrobat Sign](#) online, the leader in [e-signatures](#) and web contracting. With Acrobat Sign, you can get PDF, Microsoft Word, and other documents sent, signed, and filed instantly. And best of all, Adobe hosts it securely, so your IT department doesn't have to do the work of setting up a signature infrastructure.

## Resources

[Adobe Approved Trust List \(AATL\)](#): The Adobe Approved Trust List is a program that allows millions of users worldwide to create digital signatures that are trusted whenever the signed document is opened in Acrobat or Reader software. Check out the [current members](#).

[Adobe Security and Privacy Portal](#): A good first stop for all things security and privacy at Adobe.

[Certified Document Services](#): Certified Document Services (CDS) was the predecessor to the AATL.

[Content Security Library](#): Extensive documentation on Adobe certificate signature administration.


[Managing Digital IDs](#): Help pages for digital ID management.

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 it.

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 **Acrobat 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 document version when signed.

Credit Card	<input type="text"/>	Number	<input type="text"/>	ExpDate	<input type="text"/>
Your Signature	 Digitally signed by John Smith Date: 2023.03.09 08:53:30 +05'30'				
Please keep a copy for your records.					

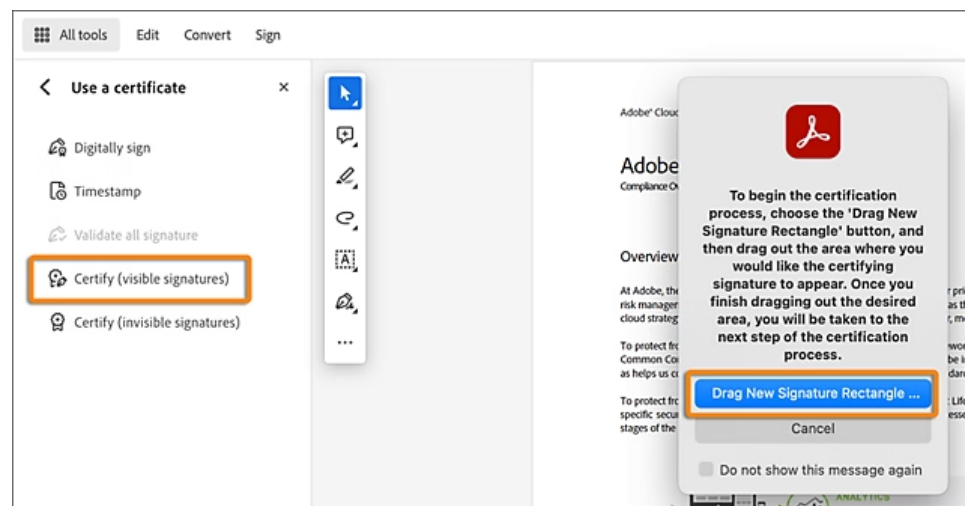
*Certificate-based signature in a PDF form*

## Steps to add a certificate-based signature to a PDF

1. Open a PDF in Acrobat and choose **All Tools > more > Use a certificate** in the global bar.

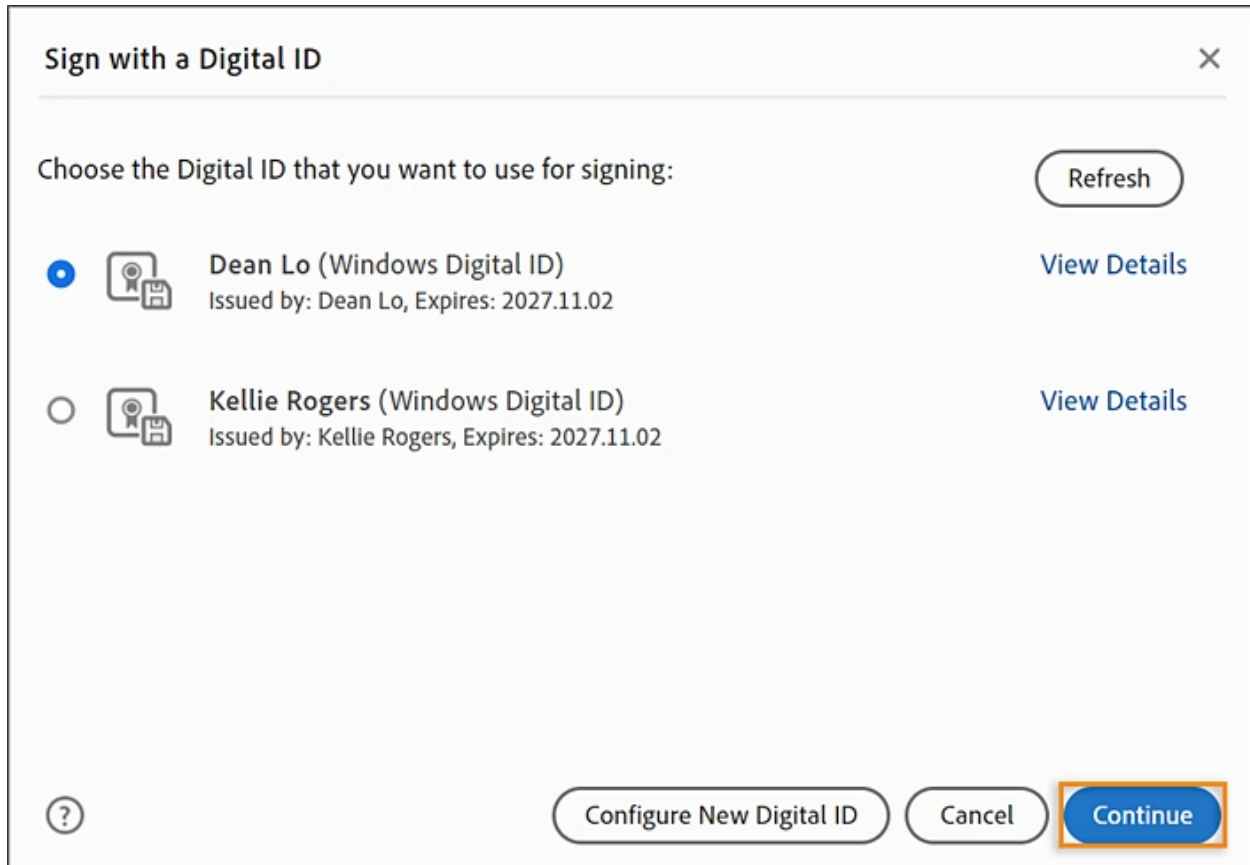
Alternatively, from Acrobat Home, select **See all tools**. In the Protect section, select **Use a certificate**, and then **select a file** you want to certify.

2. The **Use a certificate** tool is open on the left pane.
  - Select **Certify (visible signatures)** to certify with a visible digital signature, and then select **Drag New Signature Rectangle** in the dialog box that appears.
  - Select **Certify (invisible signatures)** if you want to certify the document without a visible signature.



3. Select **OK** in the Save as Certified Document dialog box.

4. If you've selected, Certify (visible signatures) in step 2, use the mouse to drag and draw a rectangle area where you want your signature to appear.
5. In the Sign with a Digital ID dialog box, choose the Digital ID you want to use for certifying the document and select **Continue**, or select **Configure New Digital ID** to create a new ID.



6. Select **Review** to review the document content before signing, then select **Sign**. Save the PDF when prompted. Your document is now certified.

## Certifying and signing documents

The **Use a certificate** tool lets you apply two types of certificate-based signatures. You can **Certify** a document, attest to its content or approve a document with the **Digitally sign** option.

### Digitally sign

When you **Digitally sign** with a certificate, the signature is considered an approval signature.

### Certify (visible or invisible signatures)

**Certify** options provide a higher level of document control than **Digitally sign**. For documents that require certification, you must certify the documents before others sign them. If a document has already been signed, the Certify options are disabled. When you certify a document, you can control the types of changes other people can make. You can certify with or without displaying a signature.

Signatures made with the **Certify** or **Digitally sign** options comply with data protection standards specified by the **European Telecommunications Standards Institute** (ETSI). In addition, both signature types comply with the PDF Advanced Electronic Signature (PAdES) standard. Acrobat and Acrobat Reader provide an option to change the default signing format to a CAdES format. This option is compliant with Part 3 of the PAdES standard. The timestamp capability and native support for long-term validation of signatures (introduced in Acrobat 9.1) is in compliance with Part 4 of the PAdES standard. The default signing format, when set up accordingly, is compliant with Part 2 of the PAdES standard. You can change the default signing method or format, in the Signatures panel of the Preferences dialog box. Under Creation & Appearance, click More.

## 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 signature appearance](#).)
- 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 [Signature types](#).)

## Set signing preferences

Signing workflow preferences control what you can see and do when the signing dialog 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. For information on the available signing preferences, see "**Signing Workflow Preferences**" in the [Digital Signature Guide](#).

## 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](#).

## 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 dialog 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.

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:  
Hamburger menu  > Preferences > Signatures (Windows) or Acrobat > Preferences > Signatures (macOS).

3. From the Appearance menu in the Sign dialog box, select **Create New Appearance**.
4. In the Configure Signature Appearance dialog 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, select File, select 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 dialog 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 dialog box (Preferences > Signatures > Creation & Appearance > More).

## **Set up a roaming ID account**

A *roaming ID* is a digital ID that is stored on a server and can be accessed by the subscriber. You must have an Internet connection to access a roaming ID and an account from an organization that supplies roaming digital IDs.

1. Open the Preferences dialog box.

2. Under **Categories**, select **Signatures**.
3. For **Identities & Trusted Certificates**, select **More**.
4. Expand **Digital IDs** on the left, select **Roaming ID Accounts**, and select **Add Account**.
5. Type the name and URL for the roaming ID server, and select **Next**.
6. Type your user name and password, or follow the directions to create an account. Select **Next**, and then select **Finish**.

Once the roaming ID is added, it can be used for signing or encryption. When you perform a task that uses your roaming ID, you're automatically logged in to the roaming ID server if your authentication assertion hasn't expired.

## PKCS#12 modules and tokens

You can have multiple digital IDs that you use for different purposes, particularly if you sign documents in different roles or using different certification methods. **Digital IDs** are usually password protected. They can be stored on your computer in PKCS #12 file format. **Digital IDs** can also be stored on a smart card, hardware token, or in the Windows certificate store. Roaming IDs can be stored on a server. Acrobat includes a default signature handler that can access digital IDs from various locations. Register the digital ID in Acrobat for it to be available for use.

## Store certificates on directory servers

Directory servers are commonly used as centralized repositories of identities within an organization. The server acts as an ideal location to store user certificates in enterprises that use certificate encryption. Directory servers let you locate certificates from network servers, including **Lightweight Directory Access Protocol** (LDAP) servers. After you locate a certificate, you can add it to your list of trusted identities so that you don't have to look it up again. By developing a storage area for trusted certificates, you or a member of your workgroup can facilitate the use of encryption in the workgroup.

For more information about directory servers, see the [Digital Signature Guide](#).

## Import directory server settings (Windows only)

You import directory server settings using security import/export methodology or a security settings file. Before, you import settings in a file using import/export methodology, ensure that you trust the file provider before opening it.

1. Open the **Preferences** dialog box.
2. Under **Categories**, select **Signatures**.
3. For **Document Timestamping**, select **More**.
4. Select **Directory Servers** on the left, and then select **Import**.
5. Select the import/export methodology file and select **Open**.
6. Select the Signature Properties button to check the current signature status if the file is signed.
7. Select **Import Search Directory Settings**.
8. Select **OK**, if prompted to confirm your choice.

The directory server appears in the **Security Settings** dialog box.

## Export directory server settings (Windows only)

Although it is preferable to export security settings, you can export directory settings as an import/export methodology file. Use the file to configure the directory server on another computer.

1. Open the **Preferences** dialog box.
2. Under **Categories**, select **Identity**.
3. Enter your name, organization, and email address to create your profile.
4. Under **Categories**, select **Signatures**.
5. For **Document Timestamping**, select **More**.
6. Select **Directory Servers** on the left, and then select one or more servers on the right.
7. Select **Export**, select a destination, and then select **Next**.
8. To prove that the file came from you, select **Sign**, add your signature, and then select **Next**.
9. Do one of the following:
  - To save the file, specify its name and location, and select **Save**.
  - To send the file as an attachment, type an email address in the To box, select **Next**, and then select **Finish**.

**Note:** See also [Export security settings](#).

## 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** dialog box. If a timestamp server is configured, the timestamp appears in the Date/Time tab of the **Signature Properties** dialog 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** dialog 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 select **Open**.

- If you've a URL for the timestamp server, select the **New** button . Type a name, and then type the server URL. Specify whether the server requires a username and password, then select **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** dialog 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. Select **OK** to confirm your selection.
-