
Adobe LiveCycle Rights Management (ALCRM) servers

Adobe LiveCycleRights Management (ALCRM) servers let you define centralized policies to control access to documents. The policies are stored on the ALCRM server. You require server access to use them.

ALCRM servers embed user access information in documents. Therefore, specify document recipients in ALCRM policies. Alternatively, let the ALCRM server retrieve the list of recipients from LDAP directories.

Use ALCRM servers to set permissions for separate document tasks, for example opening, editing, and printing. You can also define document auditing policies on ALCRM servers.

What is a digital signature?

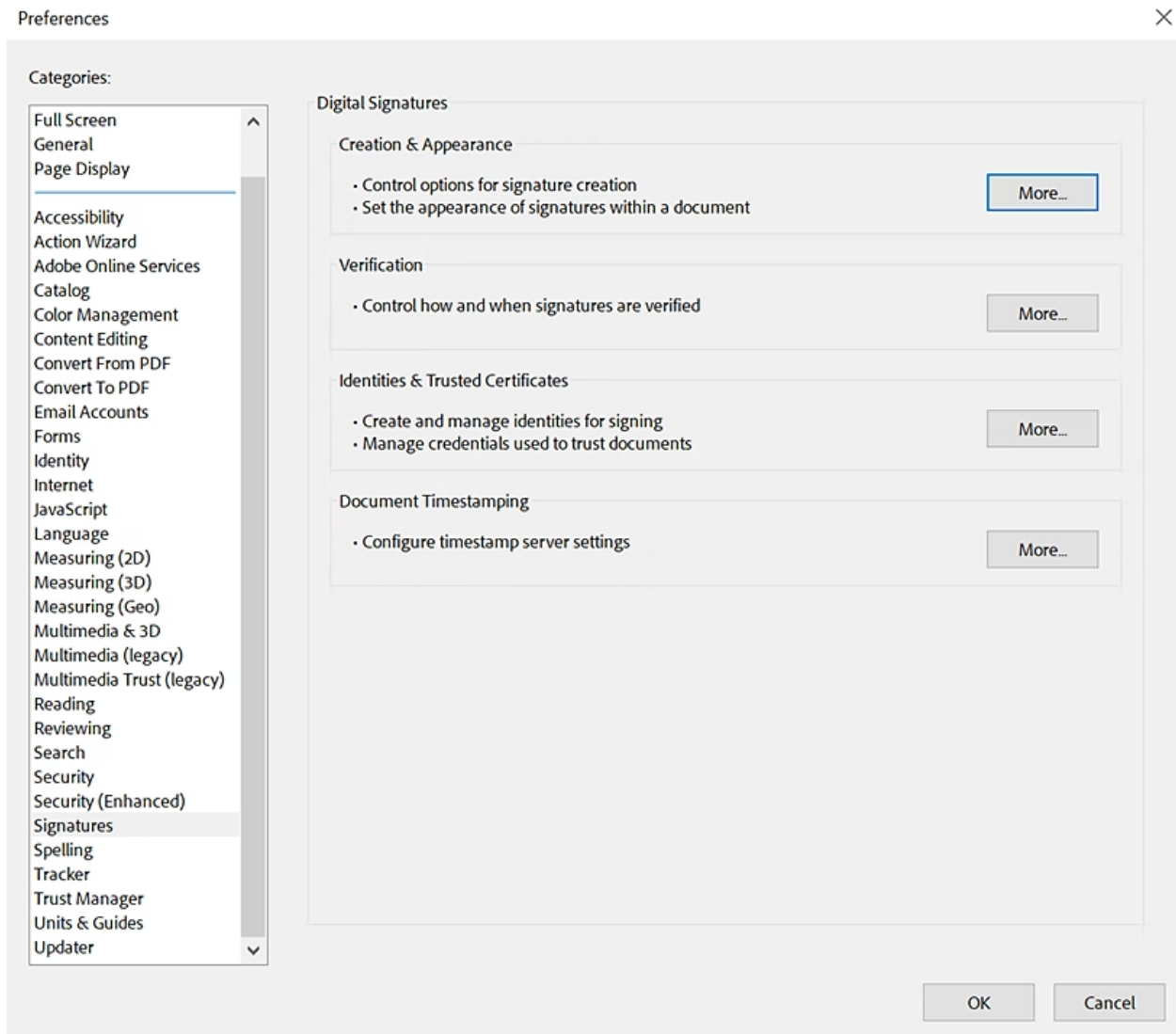
Digital signatures are a secure and efficient way to electronically sign and authenticate documents, ensuring their authenticity and integrity. By using digital signatures, you can sign documents quickly and easily, and be confident that they can't be tampered with or forged.

Why validate a digital signature?

When you receive a signed document, you may want to validate its signature to verify the signer and the signed content. Depending on how you've 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.

To verify authenticity, the validator checks if the signer's certificate or its parent certificates are trusted. The validity of the signing certificate is also checked based on the user's Acrobat or Acrobat Reader settings.

To verify document integrity, the validator checks if the signed content was altered after signing. If changes were made, the verification ensures that the signer allowed the changes.



Set preferences for validating digital signatures

You can set verification preferences in advance so digital signatures are valid when you open a PDF and verification details appear with the signature. When Digital Signatures are validated, an icon appears in the document message bar to indicate the signature status.

1. Select the hamburger menu (Windows®), or go to **Acrobat (macOS) > Preferences**.
2. In the Preferences dialog box, from under categories, select **Signatures**.
3. From the *Verification* box in the *Digital Signatures* panel, select **More...**

Signature Verification Preferences ✕

☒ Verify signatures when the document is opened
☐ When document has valid but untrusted signatures, prompt to review and trust signers

Verification Behavior
 When Verifying:

☐ Use the document-specified method; prompt if unavailable
☒ Use the document-specified method; if unavailable, use default method
☐ Always use the default method: Adobe Default Security ▼

☒ Require certificate revocation checking to succeed whenever possible during signature verification
☒ Use expired timestamps
☐ Ignore document validation information

Verification Time
 Verify Signatures Using:

☒ Time at which the signature was created
☐ Secure time (timestamp) embedded in the signature
☐ Current time

Verification Information
 Automatically add verification information when saving signed PDF:

☒ Ask when verification information is too big
☐ Always
☐ Never

Windows Integration
 Trust ALL root certificates in the Windows Certificate Store for:

☐ Validating Signatures
☐ Validating Certified Documents

Selecting either of these options may result in arbitrary material being treated as trusted content.
 Take care before enabling these features.

Help OK Cancel

4. In the 'Signature Verification Preferences' dialog that opens, you can control the following settings:
- **Set automatic validation of signatures:** With the *Verify signatures when the document is opened* check box selected, Acrobat automatically validates all signatures in a PDF when you open the document.
 - **Set verification behavior:** The 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.
 - **Check the revocation status of certificates:** With the *Require certificate revocation checking to succeed...* checkbox selected, Acrobat checks certificates against a list of excluded certificates during validation. If you deselect the check box, the revocation status for Acrobat Approval

signatures is ignored. The revocation status is always checked to certify signatures.

- **Use expired timestamps:** The option is selected by default. It uses the time mentioned in the timestamp or embedded in the signature, even if the signature's certificate has expired. If you deselect the check box, Acrobat discards expired timestamps.
- **Set verification for time:** You can select the appropriate options under 'Verification time' to check the time at which the signature was created, to check the timestamp embedded in the signature, or to check the current time.
- **Add verification information:** Select appropriate options under 'Verification information' to add verification information to the signed PDF or to alert the user when the verification information is too large.
- **Configure to trust the root certificates in the Windows® certificate store:** You can specify whether to trust all root certificates in the Windows® Certificates store for:
 - **Validating signatures:** Certificates are trusted for Acrobat Approval signature validation.
 - **Validating certified documents:** Certificates are trusted for certification signature validation.

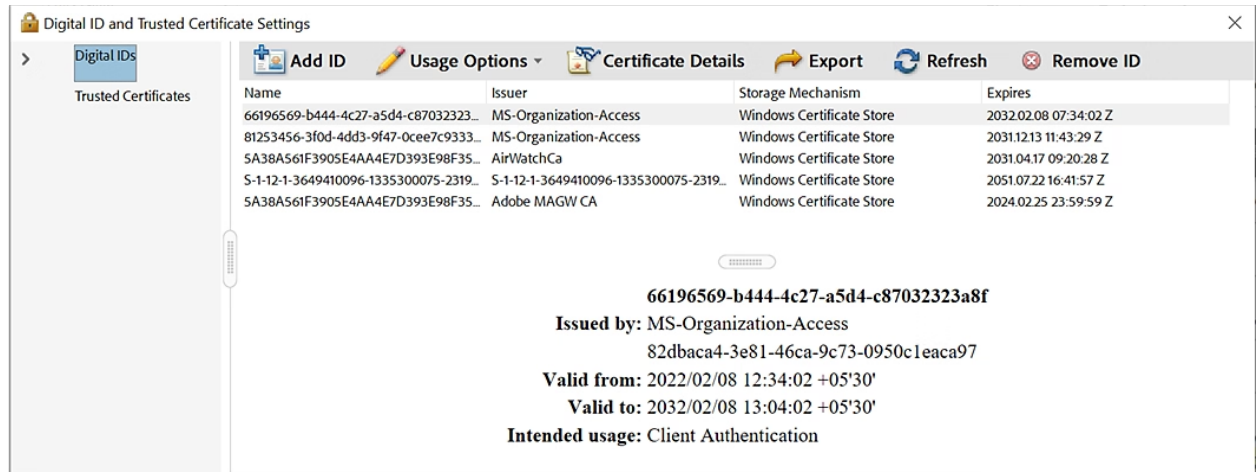
Note: Selecting these options can compromise security.

Set the trust level of a certificate

In Acrobat or Acrobat 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. Navigate to the hamburger menu (Windows) or the **Acrobat** menu (macOS) > **Preferences** > **Signatures**.
2. For *Identities & Trusted Certificates*, select **More...**
3. From the left panel, select **Trusted Certificates**.



4. Select a certificate from the list and then select **Edit Trust**.
5. In the *Edit Certificate Trust* dialog that opens, select any of the following items to trust the certificate:

- **Use this certificate as a trusted root:** A root certificate is an 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:** It acknowledges the identity of the signer.
- **Certified documents:** It 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 the 'Certified documents' option is selected, the following options are available:

- **Dynamic content:** It allows movies, sound, and other dynamic elements to play in a certified document.
- **Embedded high privilege JavaScript™:** It allows privileged JavaScript™ embedded in PDF files to run. JavaScript™ files can be used in malicious ways. It's prudent to select this option only when necessary on certificates you trust.
- **Privileged system operations:** It allows Internet connections, cross-domain scripting, silent printing, external-object references, and import/export methodology operations on certified documents.

Note: Allow *Embedded high privilege JavaScript™* and *Privileged system operations* only for sources that you trust and work closely with. For example, use these options for your employer or service provider.

6. Select **OK**.

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.

Sign in preview mode for document integrity

When document integrity is critical for your signature workflow, you can enable 'View documents in Preview mode', and then sign the document. This feature analyzes the document for content that may alter the look and feel of the document and suppresses such content to allow you to view and sign the document in a static and secure state.


By signing in preview mode, you can find if the document contains:

- Any dynamic content or external dependencies.
- Any constructs such as form fields, multimedia, or JavaScript™ that may affect its look and feel.

After reviewing the report, you can contact the author of the document about the problems listed in the report.

Certify a PDF

Certifying a PDF means approving its contents and specifying what changes are allowed for the document to remain certified. For example, a government agency creates a form with signature fields and certifies it, allowing users to only change form fields and sign the document. Removing pages or adding comments will result in losing the certified status.

A certifying signature can only be applied if the PDF has no other signatures. These signatures can be visible or invisible, and a blue ribbon icon  in the Signatures panel confirms a valid certifying signature. Adding a certifying digital signature requires a digital ID.

Timestamp a document

Acrobat allows users to add a document timestamp to a PDF without needing an identity-based signature. To timestamp a PDF, a timestamp server is needed. See how to [configure a timestamp server](#).

A timestamp guarantees the authenticity and existence of a document at a specific time and complies with ETSI 102 778 PDF Advanced Electronic Signatures (PAdES) standard.

Validate a digital signature


If the signature status is unknown or unverified, manually validate it to identify the issue and find a potential solution. In case the signature status is invalid, you must contact the signer to resolve the issue.

Validate all digital signatures

1. Open the PDF for which you want to validate all digital signatures.
2. From the global bar in the upper-left, select **All tools**.
3. From the **All tools** pane, select **Use a certificate > Validate all signature**.
4. Select **OK** in the confirmation dialog box. Once all the signatures are validated. You get a confirmation message.

View previous versions of a digitally signed document

Whenever a certificate is used to sign a document, a signed version of the PDF is created and saved along with the original PDF. The saved versions are in an append-only format, meaning the original PDF can't be modified. The Signatures panel provides access to all digital signatures and their corresponding versions.

To view previous versions, open the Signature panel and then select Options  > **View Signed Version**.

The previous version opens as a new PDF, with the version information and the name of the signer in the title bar. To return to the original document, choose the document name from the Windows® menu.

Compare versions of a signed document

After a document is signed, you can display a list of the changes made to the document after the last version.

To compare the previous versions, open the Signatures panel and then select the signature. Then, select Options  > **Compare Signed Version To Current Version**.

Once you're done, close the temporary document.

Trust a signer's certificate

To trust a certificate, it must be added to the user's trusted identity list in the Trusted Identity Manager. Also, its trust level must be set manually. End users can exchange certificates or add them directly from signed documents and set their trust levels. However, enterprises may require employees to validate signatures without any manual intervention. Acrobat trusts all

certificates that are signed and certified by a trust anchor. Therefore, administrators can preconfigure client installations or allow end users to add a trust anchor.

Sign component PDFs and PDF Portfolios

You can sign component PDFs within a PDF Portfolio, or sign the PDF Portfolio as a whole. Signing a component PDF locks the PDF for editing and secures its content. After signing all the component PDFs, you can sign the entire PDF Portfolio to finalize it. Alternatively, you can sign the PDF Portfolio as a whole to lock the content of all component PDFs simultaneously.

- To sign a component PDF, see [Signing PDFs](#). The signed PDF is automatically saved to the PDF Portfolio.
- To sign a PDF Portfolio as a whole, sign the cover sheet (View > Portfolio > Cover Sheet). Once you sign the PDF Portfolio as a whole, you can't add signatures to the component documents. However, you can add more signatures to the cover sheet.

Digitally sign on attachments to component PDFs

You can add signatures to attachments before signing the cover sheet. To do so:

1. Open the PDF in a separate window.
2. Right-click the attachment and select **Open file**.
3. To view signatures on the PDF Portfolio, navigate to the cover sheet to view the document message bar and signatures pane.

View signed and certified PDF Portfolios

A properly signed or certified PDF Portfolio has one or more signatures that approve or certify the PDF Portfolio. The most significant signature appears in a Signature badge in the toolbar. Details of all signatures appear on the cover sheet.

- To view the name of the organization or person that signed the PDF Portfolio, hover the pointer over the Signature Badge.
- To view details about the signature that appears on the Signature Badge, click the Signature Badge. The cover sheet and the Signatures pane on the left are open with details.

If the PDF Portfolio approval or certification is invalid or has a problem, the Signature Badge shows a warning icon. To view an explanation of the problem, hover the pointer over a Signature Badge with a warning icon. Different warning icons appear for different situations.

For a list and explanation of each warning, see the [DigSig Admin Guide](#).

XML data signatures

Acrobat and Acrobat Reader support XML data signatures that are used to sign data in XML Forms Architectures (XFA) forms. The form author provides XML signing, validating, or clearing instructions for form events, such as button click, file save, or submit.

XML data signatures conform to the W3C XML-Signature standard. Like PDF digital signatures, XML digital signatures ensure integrity, authentication, and non-repudiation in documents.

However, PDF signatures have multiple data verification states. Some states are called when a user alters the PDF-signed content. In contrast, XML signatures only have two data verification states, valid and invalid. The invalid state is called when a user alters the XML-signed content.

Establish long-term signature validation

Long-term signature validation allows you to verify the signature's validity long after the document was signed. To achieve this, all the necessary elements for signature validation must be embedded in the signed PDF. These elements can be embedded during the document signing process or added afterward.

If certain information is not included in the PDF, the signature can only be validated for a limited time because certificates related to the signature eventually expire or are revoked. When a certificate expires, the issuing authority is no longer responsible for providing revocation status, rendering the signature unverifiable.

The necessary elements for signature validity include the signing certificate chain, certificate revocation status, and possibly a timestamp. If these elements are embedded during signing, the signature can be validated without requiring external resources.

Acrobat and Acrobat Reader can embed the necessary elements if available, and the PDF creator must enable usage rights for Acrobat Reader users by going to the hamburger menu (Windows) or the **Acrobat** menu (macOS) > **Save as other** > **Acrobat Reader extended PDF**.

Note: Embedding timestamp information requires an appropriately configured timestamp server. In addition, the signature validation time must be set to Secure Time by navigating to **Preferences** > **Security** > **Advanced Preferences** > **Verification** tab.

CDS certificates can add verification information, such as revocation and timestamp into the document without requiring any configuration from the signer. However, the signer must be online to fetch the appropriate information.

Add verification information at signing

To add verification information while signing:

1. Ensure that your computer can connect to the appropriate network resources.
2. Go to **Preferences > Signatures > Creation & Appearances: More** and make sure that the **Include signature's revocation status** option is selected.
3. Sign the PDF.

If all the elements of the certificate chain are available, the information is added to the PDF automatically. If a timestamp server has been configured, the timestamp is also added.

Add verification information after signing

In certain workflows, signature validation information may be unavailable during the signing but can be obtained later. For instance, a company official may sign a contract on a laptop while traveling without internet access. When internet access is later available, anyone validating the signature can add timestamping and revocation information to the PDF. Subsequent signature validations can also make use of this information.

To add verification information after signing:

1. Ensure that your computer can connect to the appropriate network resources, and then right-click the signature in the PDF.
2. Select **Add Verification Information**.

Information and methods used to include this long-term validation (LTV) information in the PDF comply with Part 4 of the ETSI 102 778 PDF Advanced Electronic Signatures (PADES) standard.

The command is unavailable if the signature is invalid, or is signed with a self-signed certificate. The command is also unavailable in case the verification time equals the current time.