

# PDF Signer Server User Manual

The main function of PDF Signer Server is to sign PDF documents using X.509 digital certificates. Using this product you can quickly sign multiple PDF files (bulk sign) by selecting input and output directory. This is ideal for bulk signing of large number of corporate documents rather than signing each one individually.

**Configurable Signature Appearance** – PDF Signer Server provides a fully configurable appearance for its digital signatures. The positioning of the signature appearance is configurable, plus on which pages of the document it should appear (first page, last page or all pages).

**Interoperability** – Signatures produced with PDF Signer Server can be verified using standard Adobe Reader 7.0+

**PKI Interoperability** – PDF Signer Server is completely PKI neutral and it will work with PKI components from any vendor (this includes CAs, certificates, CRLs, smartcards, etc.).

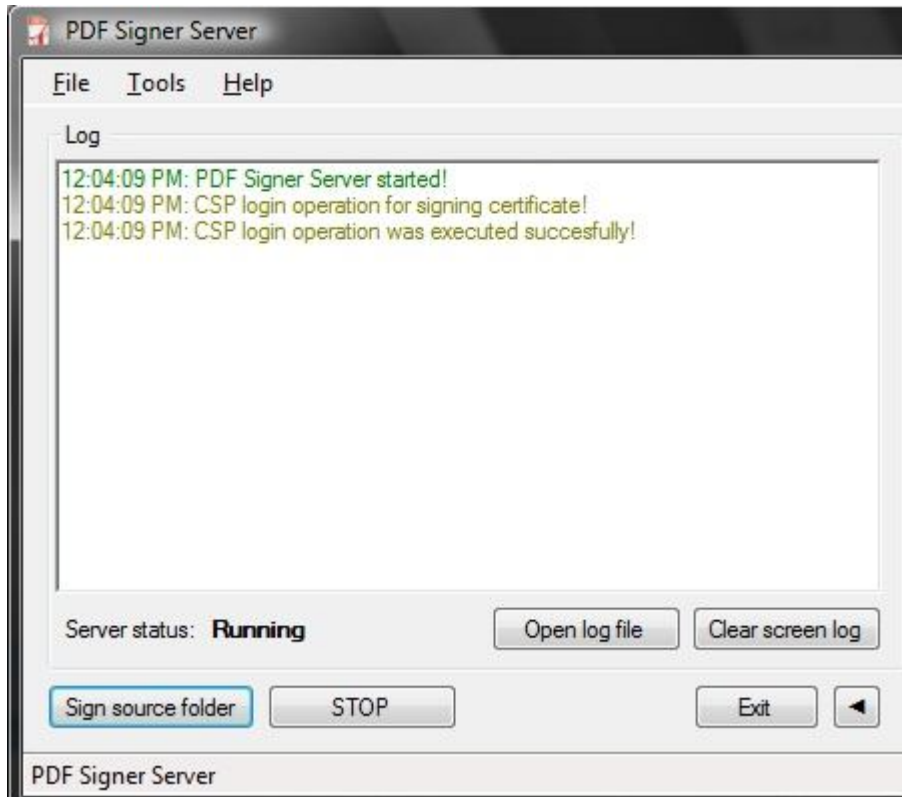
**Timestamping** – Like signatures, timestamps are easier to verify when they're associated with a timestamp authority's trusted certificate. Including a timestamp helps to prove that the document wasn't changed after you had signed it and it reduces the chances of an invalid signature.

**Long-term validation purposes** – Using our software you can sign and timestamp PDF documents for long-term validation purposes. PDF Signer Server supports advanced digital signatures which include embedded RFC 3161 compliant secure timestamps. Such signatures can be verified even after the signer's certificate expires or is revoked.

**SHA-2 hash function** – Our software may sign PDF documents using SHA-256, SHA-512 hash algorithm and RSA 2048 or higher key length according to ETSI TS 102 176-1 V2.0.0 ("ALGO Paper").

**Invoice signing** – PDF Signer Server allows organizations to digitally sign and process large numbers of invoices. EU VAT Directive requires that: "Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed". The only standard and interoperable way of doing this is to use digital signatures and in general EU member states require that a qualified electronic signature is used to confirm the identity of the originator.

**Certify your documents** - When you certify a PDF, you indicate that you approve of its contents.



*Illustration 1: Main window*

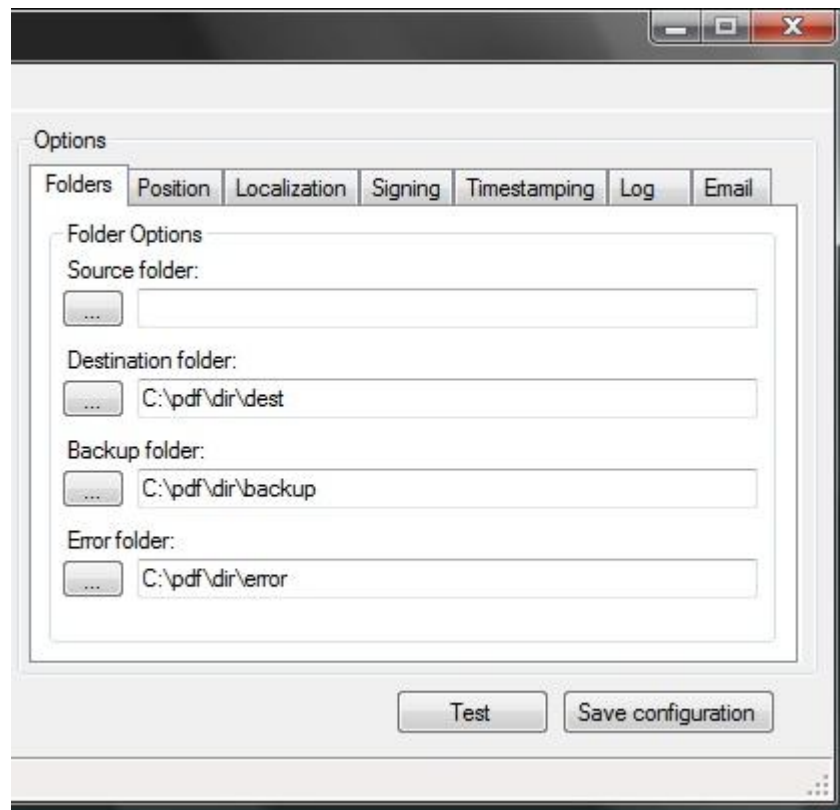
**Log:** All server activity appears on this window.

**Server status:** When the status is **Running**, the files can be signed. When the status is **Not Running**, the server configuration is not OK (folders are not set, signing certificate is not set, etc.).

**Open log file** button: Log file is displayed in the default internet browser.

**Sign source folder** button: Source folder will be scanned and every PDF file will be signed using current configuration.

**STOP** button: If the signing process is started, this action will stop the operation.



*Illustration 2: Folder Option tab*

**Test** button: Sign a single PDF file using current configuration.

**Save configuration** button: Save the current configuration.

**Source folder:** The folder that contains unsigned PDF files.

**Destination folder:** The folder where signed files are stored.

**Backup folder:** All unsigned file that are signed successfully are stored here.

**Error folder:** All unsigned file that are not signed successfully are stored here.

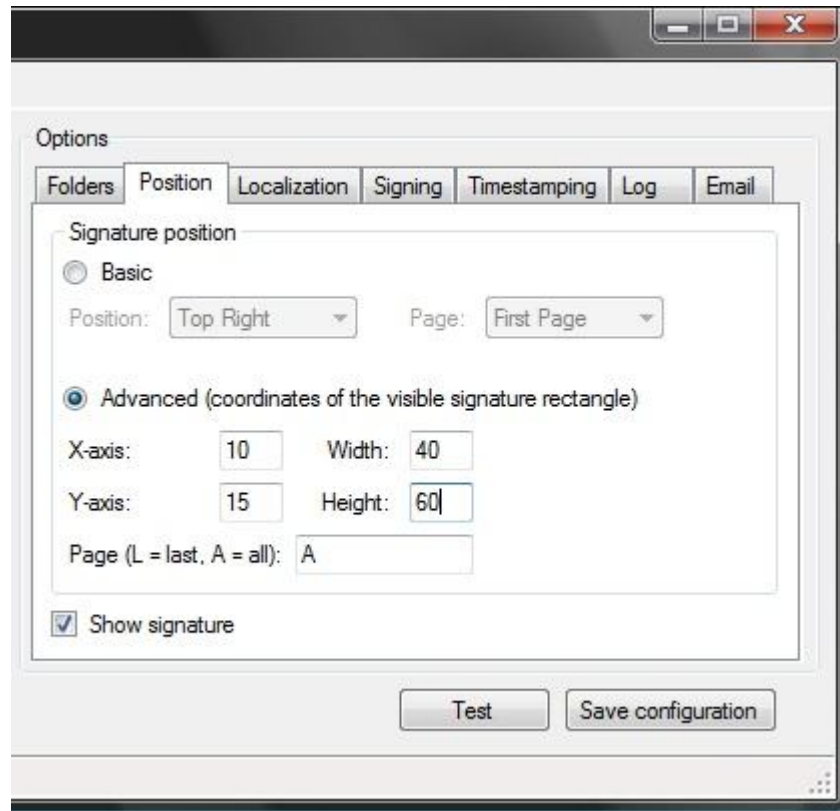


Illustration 3: Position tab

**Basic** position: If *Basic* position is selected, the signature rectangle will be displayed according to *Position* and *Page* options.

**Position:** This may be set to: *Top Right*, *Top Left*, *Bottom Right*, *Bottom Left*.

**Page:** This may be set to: *First Page* or *Last Page*.

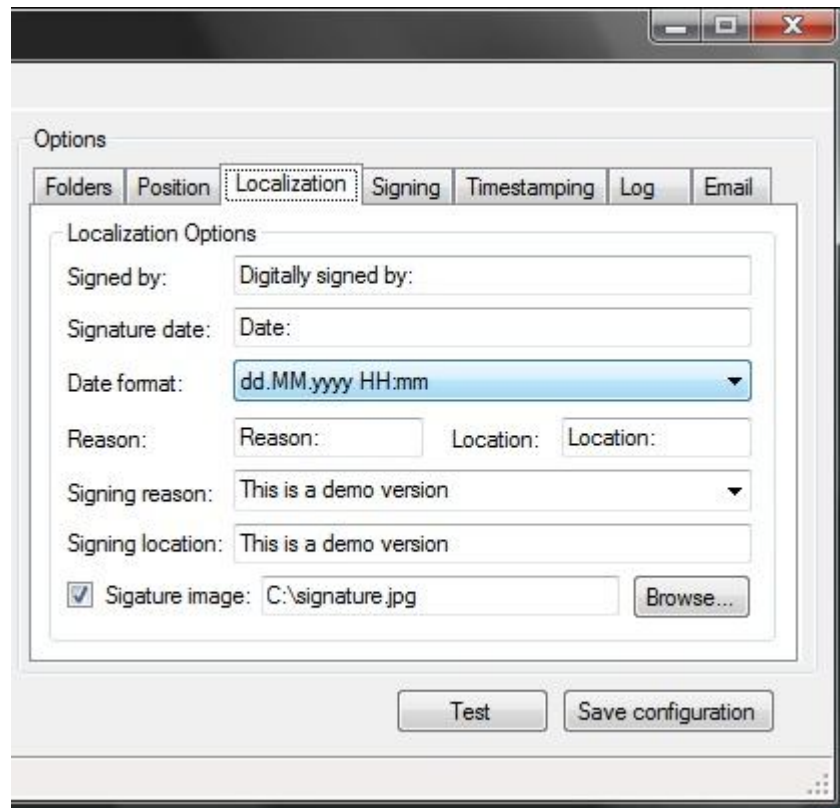
**Advanced** position: If *Advanced* is selected, the signature rectangle will be displayed at position indicated by coordinates.

**X/Y-axis:** Starting point of signature rectangle position. [Note that \(0,0\) means Bottom Left.](#)

**Width/Height:** The signature rectangle width/height.

**Page:** The page where signature will be displayed. It can be a number or L (for the last page) or A for all pages from the document.

**Show signature:** If it is checked, the signature rectangle will be displayed on the PDF document. Otherwise, the signature rectangle will be hidden but the signing information will be encapsulated in the document structure.



*Illustration 4: Localization tab*

**Signed by:** Localization text for signer prefix.

**Signature date:** Localization text for date.

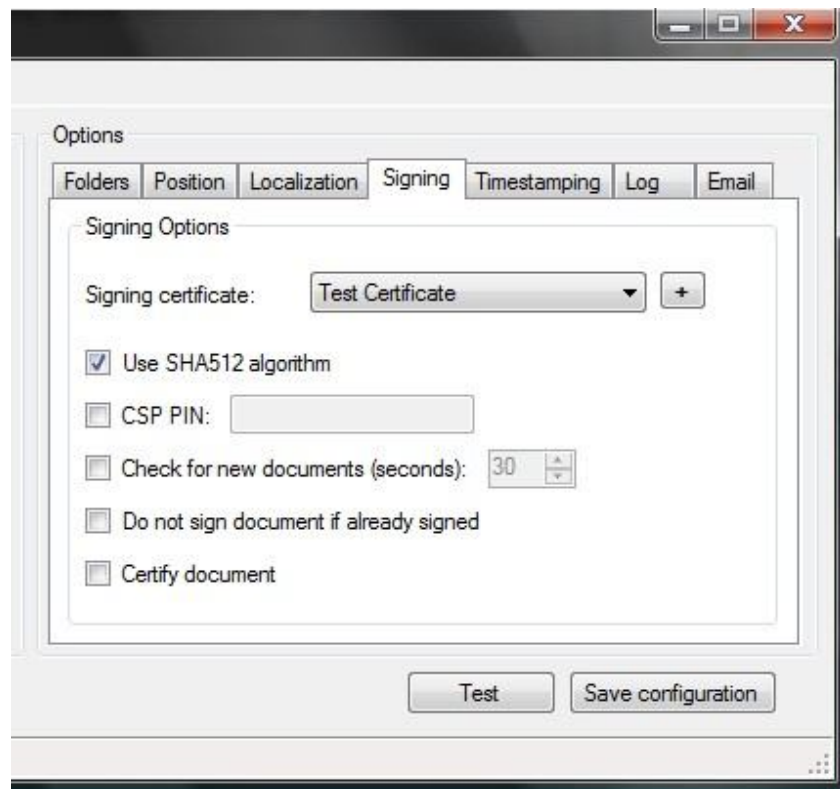
**Date format:** Format of the signature date

**Reason:** Localization text for reason prefix.

**Location:** Localization text for location prefix.

**Signing reason/location:** Reason/location text. It may be empty or changed in the registered version of the product.

**Signature image:** A signature image can be added to the signed document. All other texts will be replaced by this image.



*Illustration 5: Signing tab*

**Signing certificate:** The certificate that will be used for signing operation. The certificates installed on the system may be viewed using: `certmgr.msc` command. If your certificate is a PFX file, it must be installed first on the system.

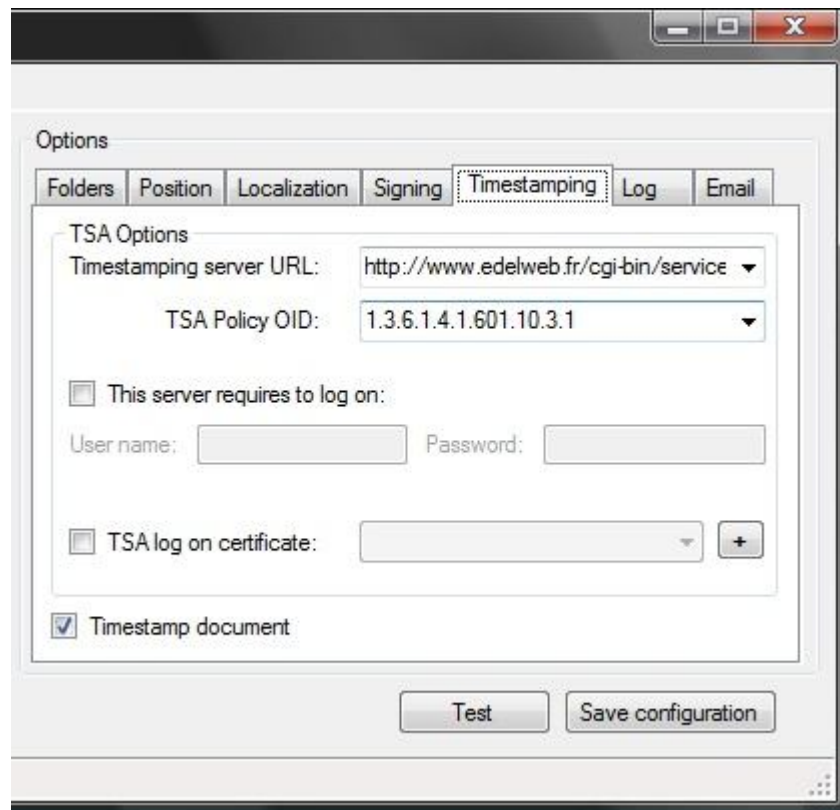
**Use SHA512 algorithm:** SHA-512 hash algorithm will be used for signing operations. This option is not available for Windows XP and for some cryptographic smart cards.

**CSP PIN:** If the certificate is issued on a cryptographic token (like Aladdin or SafeNet iKey), the token PIN may be entered here to override the PIN dialog.

**Check for new documents:** The signing engine may sign automatically the files from source folder from time to time.

**Do not sign document if already signed:** if the source document is already signed, the application will not sign that document.

**Certify document:** When a PDF is certified, it indicates that the signer approve its contents (more details [here](#)).



*Illustration 6: Timestamping tab*

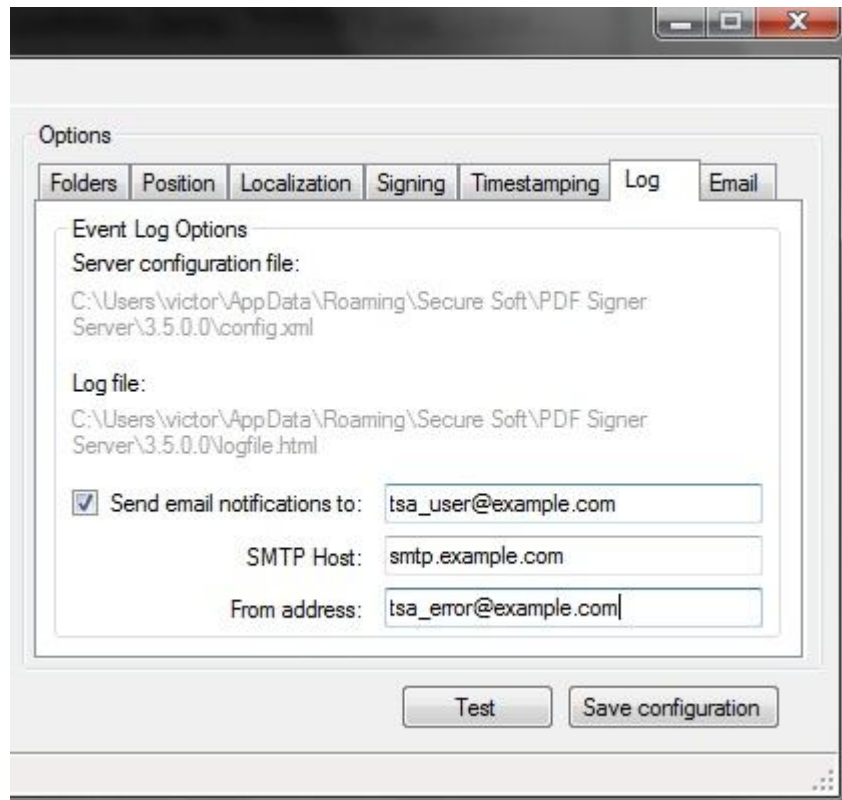
**Timestamping server URL:** TSA server URL (must be compliant with RFC 3161).

**TSA Policy OID:** the OID for TSA request.

**This server requires to log on:** If the TSA authority provides a set of credentials, they must be entered here to gain access to the TSA.

**TSA log on certificate:** If the TSA authority provides a digital certificate to access the service, it must be selected here to gain access to the TSA.

**Timestamp document:** If it is checked, the document will be time stamped using current TSA configuration.

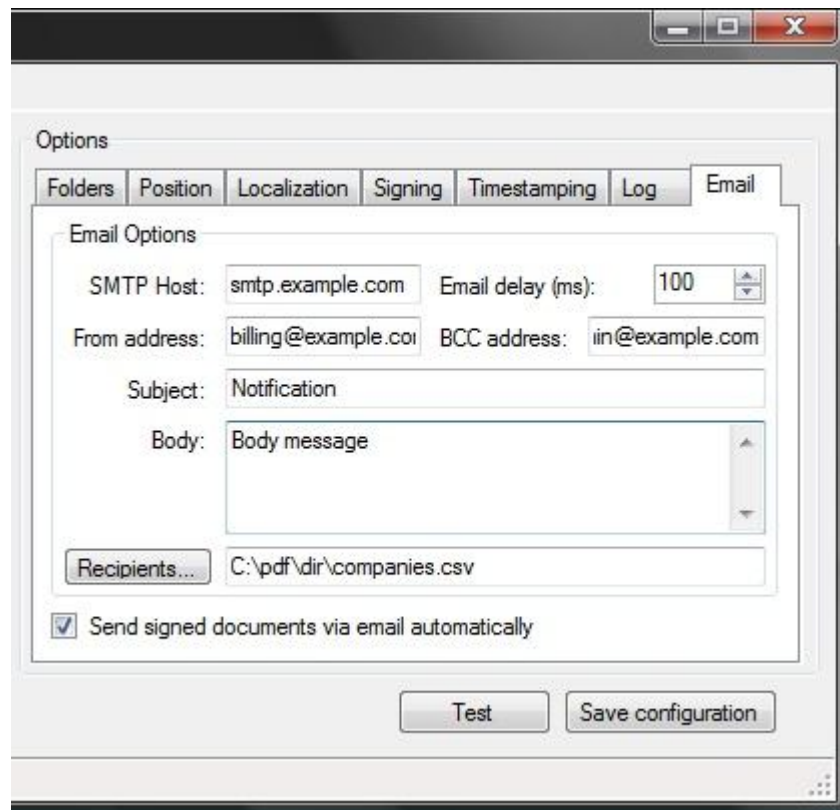


*Illustration 7: Log tab*

**Server configuration file:** The location of the server configuration.

**Log file:** The log file location.

**Send email notifications to:** If it is selected, all errors will be sent via email.



*Illustration 8: Email tab*

After the file is signed, the application may send that file via email to the corresponding user. The users and file prefixes must be saved in a CSV file to be interpreted by the application.

When a signed file name started with a prefix defined in CSV file, the file is sent automatically to the email address specified in the CSV file.

Example:

CSV file:

Prefix,Email

Company 1, email@company1.com

Company 2, email@company2.com

Company 3, email@company3.com

Company 4, email@company4.com

Output folder:

**Company 1** bill.pdf – will be send to email@company1.com (prefix matched)

**Company 2** invoice.pdf – will be send to email@company2.com (prefix matched)

**Company 3**.pdf – will be send to email@company3.com (prefix matched)

**Company**.pdf – this file will not be sent to anybody (no prefix defined in CSV file)

Other company.pdf - this file will not be sent to anybody (no prefix defined in CSV file)

Ltd **Company1**.pdf - this file will not be sent to anybody (no prefix defined in CSV file even if Company1 appears in the file name)

Other **Company 4** invoice.pdf - this file will not be sent to anybody (no prefix defined in CSV file even if Company1 appears in the file name)

### **Other application options**

PDF Signer has some command line options described below:

PDF Signer Server.exe [/onepass] [/config <config\_file>]. If the config file does not exist, the default configuration file will be loaded.

/onepass mode is useful when you want to sign a folder without user intervention.

/config <config\_file> is useful when you want to apply different signing configuration for different input folders.