PDFSealer User's Guide

ITEKSOFT Corporation

Table of Contents

Before Installation

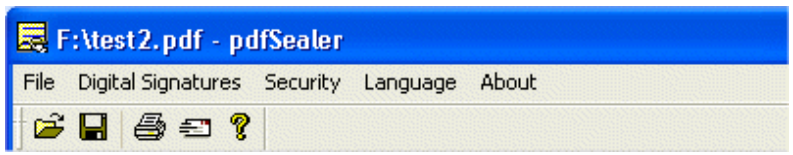
Currently, PDFSealer workstation license supports platforms including Microsoft Windows 2000/XP/Vista/7/8. Server license supports Windows Server 2000/2003/2008/2012 or later versions.

This User's Guide applies to all versions of PDFSealer. Initially the installed package is unregistered. Unregistered version gives users a full function package for evaluation with stamping a trial watermark when digitally signing the PDF document. Registered version has no such restriction. Acrobat reader is required for viewing PDF with or without digital signatures. Reader version above 5.0 is recommended.

User can purchase the proper license online (http://www.iteksoft.com) to obtain a registration key. The user can then enter the userid and registration key to turn the original version into registered version. (Refer section "Registration" for details)

Functions of PDFSealer

The main functions of PDFSealer now include Digitally Signing and Applying Standard Security.

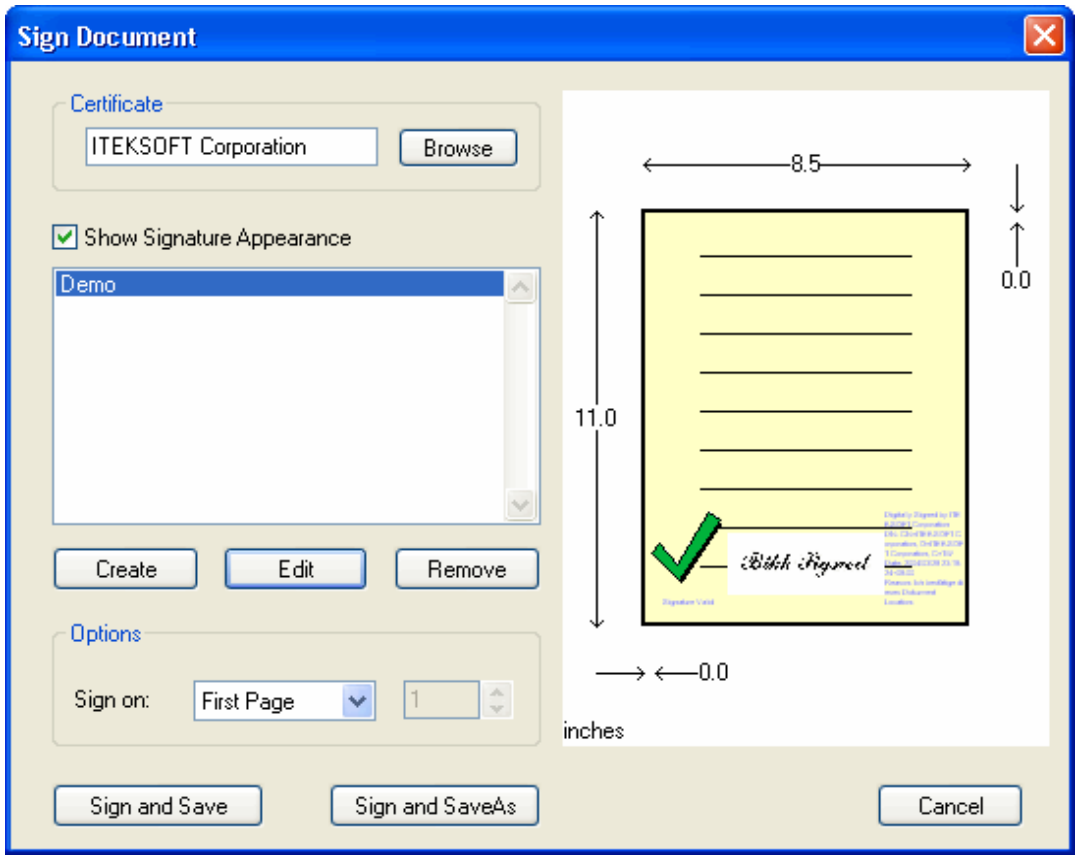


Users can digitally sign the PDF with certificates managed by Windows. The digital signature is compliant with standard PDF signature interchange standard, which can be verified by Acrobat reader or compatible handler directly. Users can apply signing multiple times in workflow for reviewing. Users can also apply or modify the security of the PDF with proper settings. Uses can also click the “Email” toolbar button to launch the default email client with attaching the current PDF for sending.

Ø Digital Signatures

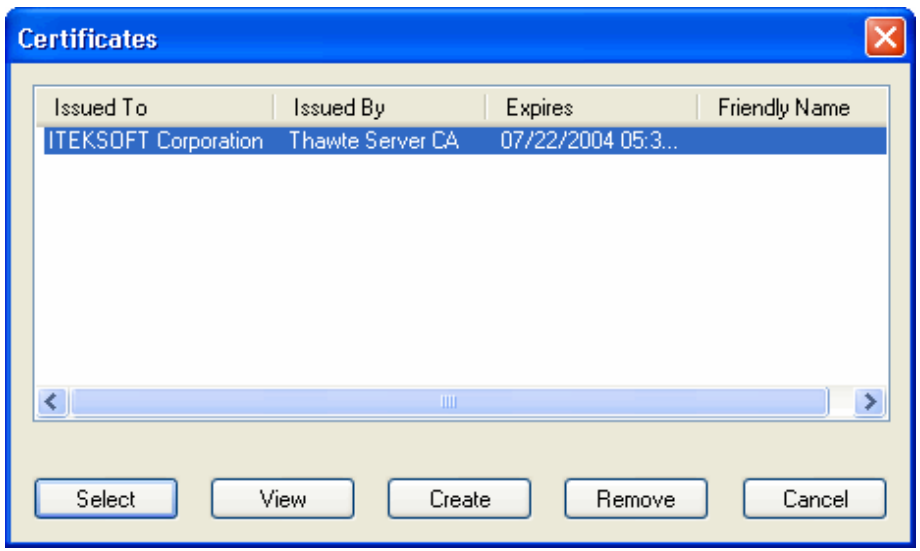
When digital signing PDFs, users need certificates with private key, which can be a self-signed created by PDFSealer directly too.

The main advantage of PDF signature is that it allows a user defined signature appearance added onto the existing PDF. The reader will verify the signature and show the result on the appearance directly. This way gives an intuitive and straightforward way to authenticate and verify the digital signatures. Users can also apply invisible

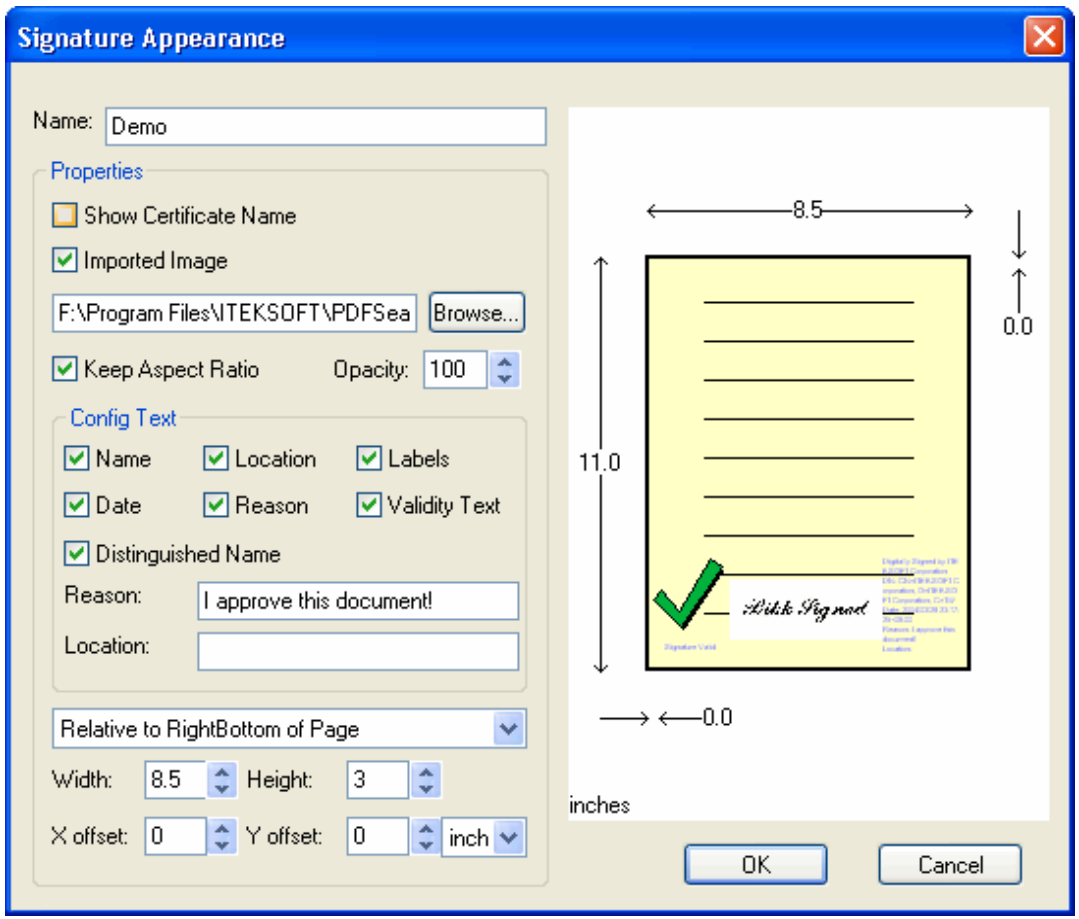


signatures on the PDF by disabling showing signature appearance. Such signatures can also be verified and viewed by the Acrobat Reader signature properties.

PDFSealer uses the same Windows native certificate management for browsing and selection. Users can select any existing Windows certificate with private key to sign the PDF. If users have not any certificate available, users can create a self-signed certificate directly from the dialog "Create" button. Users can view the details of the certificate by double clicking the certificate or click the "View" button. For those certificates without private key will not be shown in the list because such certificates are used for verification and authentication, not for signing.



When editing the signature appearance, users can adjust the width and height and change the relative position by the position attributes on the dialog. Users can also import an image for showing the scanned signature or other related graphics. In the reason and location, users can add the text for annotation to be shown on the PDF signature.



A signature will be invalidated if users modify or change the content of the PDF file. Users can append or apply extra signatures to the same PDF by incrementally updating. When PDF is modified by incrementally updating, existing signatures are still valid. Just the validity of those

signatures implies only their corresponding versions of PDF are unchanged. Users can use the function in PDF reader to view the proper version of content signed.

Ø Security

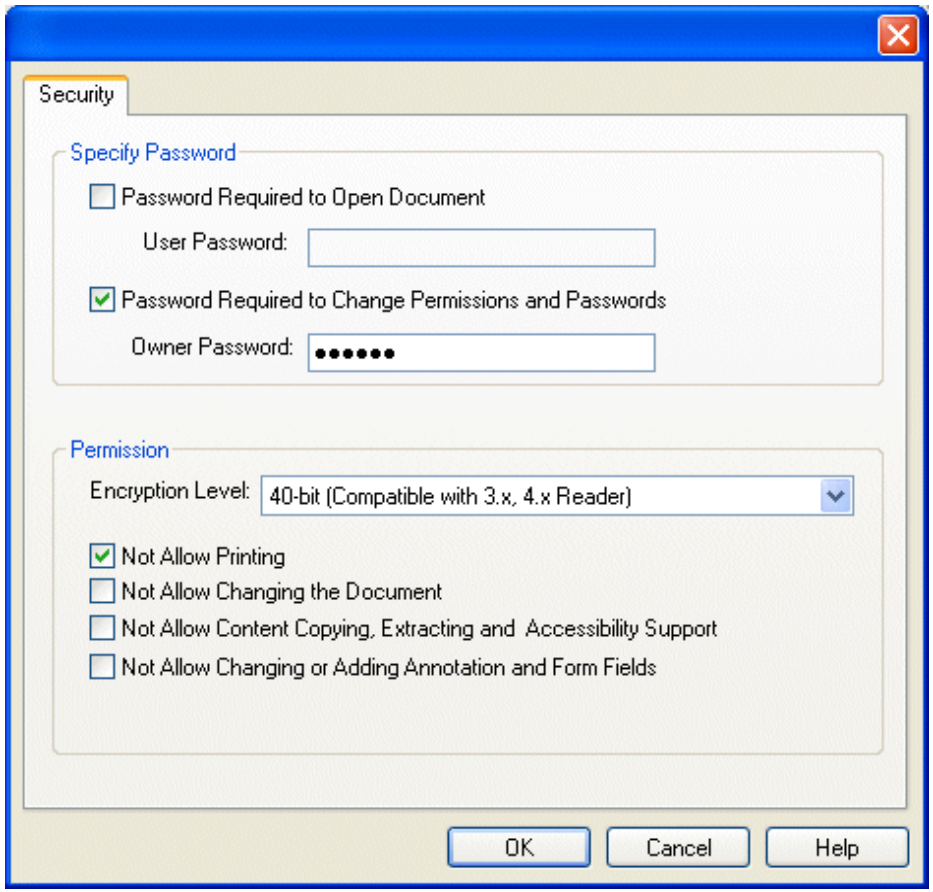
PDFSealer provides standard security setting to protect PDF files generated. Both 40bit and 128bit strong encryption modes are supported. PDF files protected by 128bit mode are supported by Acrobat Reader 5.0 or above. Users have to check ON password to enable encryption and permission control. By giving arbitrary owner password and leave “User Password” to empty will make the PDF with proper permission setting with encryption and the Reader will not ask users to enter password when opening the PDF file.

Users need original owner password if users want to modify the PDF with existing security settings. The modification or security settings will not be applied immediately. When users save the PDF or signing the PDF, these settings will be applied then.

Change security settings of an existing PDF with digital signatures will invalidate the existing signature. This is because changing security will force encrypted content being modified.

User Password	Password required to open the document.	
Owner Password	Password required to change permission and passwords.	
Permission	40bit mode	Printing: Allowed, Not Allowed
		Editing: Allowed, Not Allowed
		Copying: Allowed, Not Allowed
		Annotation: Allowed, Not Allowed
	128bit mode	Accessibility Support: Allowed, Not Allowed
		Copying and Extraction: Allowed, Not Allowed
		Editing: 5 levels control (From diabled to fully allowed)
		Printing: 3 levels control (add Low resolution mode)

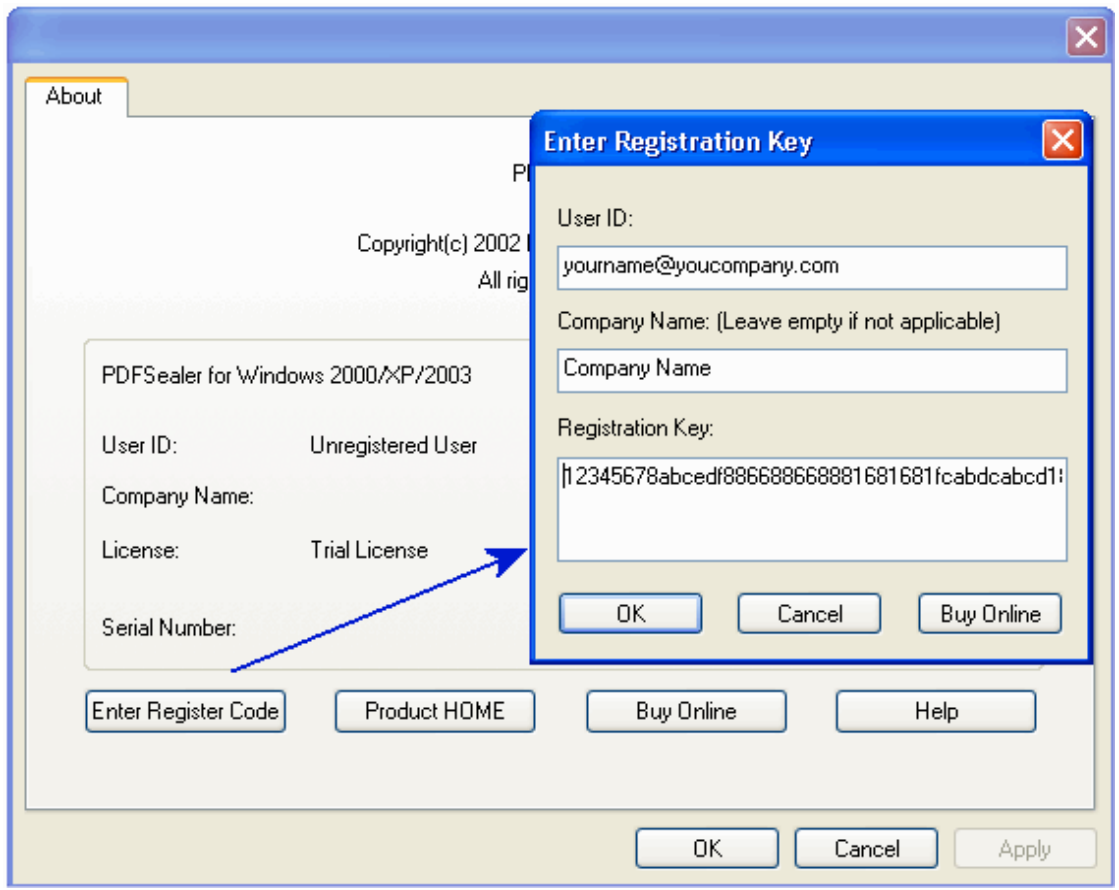
Security Settings Figure



Registration

Unregistered version will stamp a trial watermark when digitally signing the PDF.

All other functions are the same. In other words, unregistered version gives users a full function package for evaluation with stamping with a trial watermark.



Initially the installed package is unregistered. User can purchase online to obtain a registration key. Users then enter the user id (usually the email address) and registration key when clicking the “Enter Register Code” in the [About] page. After purchasing, the registration key and necessary information will be emailed to the customer.

PDFSealer Batch Command-line

PDFSealer batch command-line utility supports users to do digitally signing and encrypting by command-line mode. Users require batch server license or intranet server license for running it. Ordinary workstation or single user license is not applicable for running in command-line mode.

Ø Syntax

C:\>sealbat.exe <options> <filenames>

<filenames> ::= <filename>[<fileoption>] <filenames>
<filename> ::= <ordinary string>
<fileoption> ::= [,[<passwd to open the file>][,[<new user passwd>][,[<new owner passwd>][,[<perm>]]]]]

128bit mode
<perm> ::= (0|1)(0|1)(0|1|2|3|4)(0|1|2)
40bit mode
<perm> ::= (0|1)(0|1)(0|1) (0|1)

<options> ::= [-v][-h][-sd][-sc <certificate name>][-sa <appearance name>][-sh][-sp <pagenum>] [-x][-r <encryption level>][-N <password>][-O <password>][-U <password>][-P <perm>][-o <target path>]

<encryption level> :== (40)|(128)|(-1)
<password> ::= <ordinary string>
<target path> ::= <ordinary string>

128bit mode
<perm> ::= (0|1)(0|1)(0|1|2|3|4)(0|1|2)
40bit mode
<perm> ::= (0|1)(0|1)(0|1) (0|1)

See section **Permission Control Token Representation** for the meaning of these digits used in <perm>.

Ø Options

-sd
This option will disable digitally signing and work as pdfCiphersecurity chang

-sc “Certificate Name”
This option specifies the certificate, which will be applied to sign the PDF. If it is not assigned, it will use the default certificate users choose in the PDFSealer UI.

-sa “Appearance Name”
This option specifies the appearance, which will be applied to sign the PDF. If it is not assigned, it will use the default appearance users create in the PDFSealer UI.

-sh
This option will disable the signature appearance. That is the PDF is digitally signed without appearance.

-sp <page number>
This option will specify the page number on which the signature appearance will appear. Page number starts from 1. –1 means the last page.

-x
This option enables applying or modifying new security and permission assigned.

-N “Default Original Owner Password”
This option specifies the default password, which will be used to open documents without specified open password in the file parameters. This one is similar to the first argument following the file path to be processed. It must be the owner password of the original documents in order to change the security settings. See Notes for explanation.

-U “Default New User Password”
This option specifies the default new owner password, which will be used to apply the new security setting to the documents without specified new owner password in the file parameters. This one is similar to the second argument following the file path to be processed.

-O “Default New Owner Password”
This option specifies the default new owner password, which will be used to apply the new security setting to the documents without specified new owner password in the file parameters. This one is similar to the third argument following the file path to be processed.

-P “Default New Permission“

This option specifies the new default permission, which will be used to apply the new security setting to the documents without specified new permission in the file parameters. This one is similar to the 4th argument following the file path to be processed. It must follow the format defined in section **Permission Control Token Representation.**

-o “Output File Path”

This option specifies the output file path of the new PDF document after digitally signing or security setting. By default, pdfSealer supports in place output, i.e., it will overwrite the original PDF file with the one after processing. When specifying this option, the new file will be flushed into the output file path assigned. If the file path exists, it will be replaced. This affects only the first file to be processed, since it supports multiple files in the command line arguments.

-r “Specify the Encryption Level”

This option specifies the encryption level of the security setting, which will be applied. pdfCipher will automatically detect the security setting level contained in the original PDF documents. Now 2 values are allowed, 40 and 128. The default value is 128 when this option is omitted. For example, use “-r 40” to set the new encryption level to 40bit. When “-r –1” is specified, it means to remove the existing security settings in PDF.

-v

It will show current version information.

-?
-h
This option will show the About page of PDFSealer

Ø Permission Control Token Representation

128bit mode – 0000 -> 1142

Content Accessibility Support
0: disable
1: enable
Content Copying and Extraction
0: disable
1: enable
Editing:
0: Not allowed at all
1: Only Document Assembly Allowed
2: Only Form Field Filling or Signing Allowed
3: Annotation Authoring, Form Field Filling or Signing Allowed
4: General Editing (All Functions Allowed)
Printing:
0: Not Allowed
1: Only Low Resolution Allowed (Printing as Image)
2: High Fidelity Allowed

40bit mode – 0000 -> 1111

Content Copying, Extraction, and Accessibility Support:
0: Disable (Disallowed)
1: Enable (Allowed)
Changing or Adding Annotation and Form Fields:
0: Disable (Disallowed)
1: Enable (Allowed)
Changing the Document:
0: Disable (Disallowed)
1: Enable (Allowed)
Printing:
0: Disable (Disallowed)
1: Enable (Allowed)
For Example:

In 128bit mode, 1142 applies no restriction on the PDF document. On the other hand, 1101 means this document is not editable at all and only allowed to print as low-resolution image. In 40bit mode, these 4 bits control the on and off the their corresponding functions. 1001 allows the document to be selectable and printable.

The default value is 0000. That means all disallowed. This applies to both 128bit and 40bit mode.

Ø Examples

1. sealbat –o output.pdf input.pdf
   pdfCipher will generate “output.pdf” by encrypting the “input.pdf” with the new owner password “secret” and all other settings with default values. In this case, “input.pdf” should contain no security setting since open password is not given.
2. sealbat –x c:\temp\example1.pdf,12345,qwert,54321,0000
   This will use “12345” as the original owner password to open example1.pdf and change the security setting with new user password “qwert”, new owner password “54321”, and new permission “0000” (i.e. “all disallowed”, see **Permission Control Token Representation)**. The final result will be written into example1.pdf.
3. sealbat –sc ITEKSOFT –sa Demo src*.pdf
   This example will use certificate “ITEKSOFT” and appearance “Demo” to do digitally signing on all PDF files in wildcard format “src*.pdf” in the current directory.

Ø Notes

1. pdfSealer respects the Security Handler Restrictions defined in the PDF Specification. For example, user cannot remove the security setting unless correct owner password of the original document is given. This also applies to the security password change. User has to enter correct owner password in order to change the document password or permission settings. Users cannot apply digital signature onto those PDFs without permission for signing.
2. Specifying an open password for documents with no security settings has no effects on opening such documents. pdfSealer will treat them as original documents without security settings.
3. Since pdfSealer uses comma ‘,’ as the separator for specifying parameters like passwords for the file option, comma cannot be used in the password.
4. Use double quote to wrap the file path or password if those data contain spaces.
5. The batch command-line supports wildcard file format. Users can use *.pdf to do batch processing for all PDFs under specific directory.
6. Changing security will invalidate the existing digital signatures in the PDFs.

Support

- Report bugs by mailto:bug@iteksoft.com
- Ask technical questions by mailto:support@iteksoft.com
- Visit us at http://www.iteksoft.com/ or http://pdf.iteksoft.com/
- ODM, Reseller, Solution Provider, and etc. Please contact sales@iteksoft.com