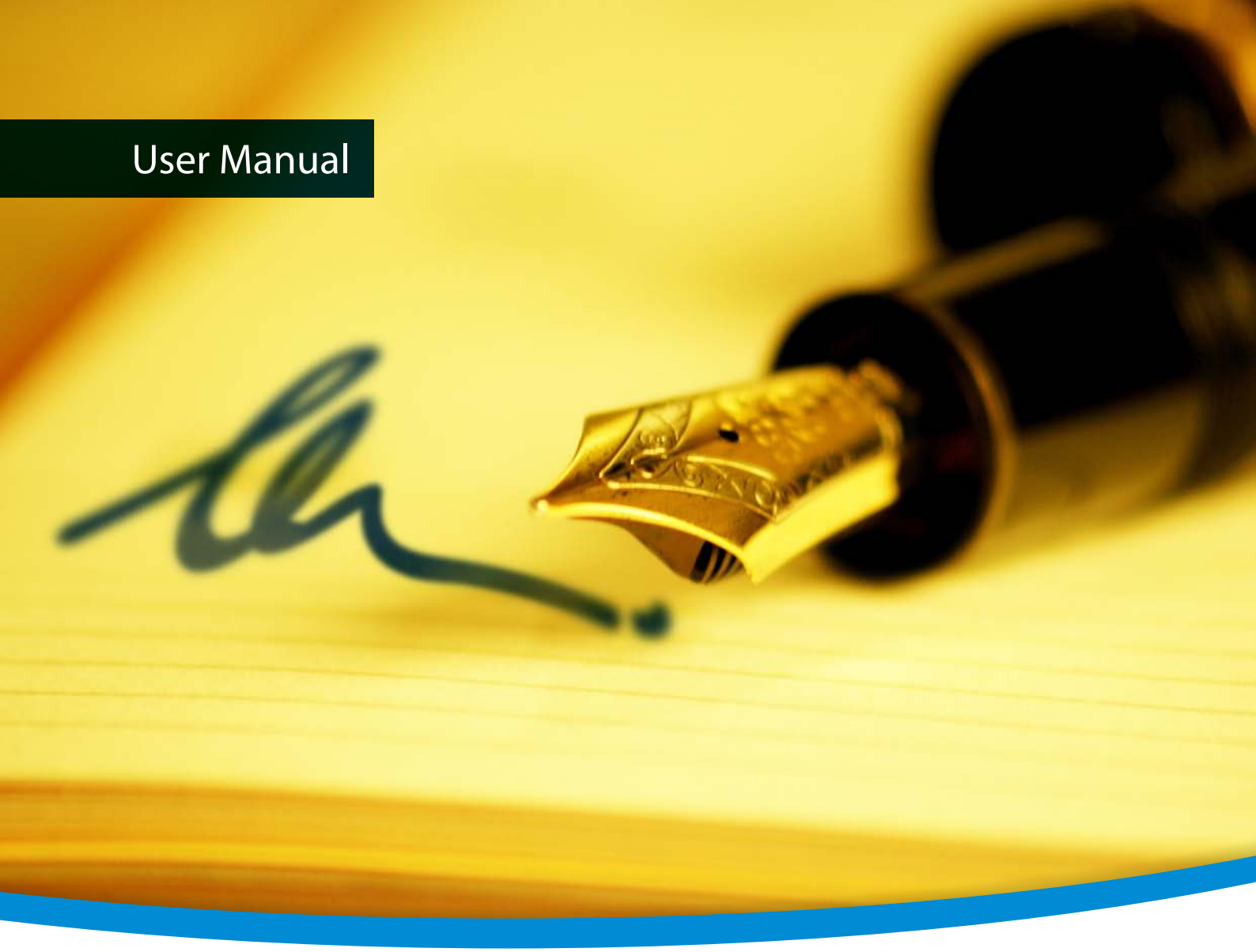
User Manual



3-Heights™ Signature Creation and Verification Service

PDF/A conform

Version 4.12.26.6

PDF-TOOLS.COM
Premium PDF Technology

Contents

1 Introduction

1.1 Description

The 3-Heights™ Signature Creation and Verification Service provides HTTP protocol based remote access to cryptographic providers such as smartcards, USB tokens, and other cryptographic infrastructure such as HSMs. By means of this service the tokens can be hosted centrally and used by any client computer which has access to the service.

The service is configurable to handle multiple tokens and is secured via credentials. While the service is running on a Windows computer, its clients can access it also from other platforms such as UNIX.

PKCS#11 is a widely used standard for providing extensive support in the area of digital signatures, including cryptographic algorithms and storage for certificates and keys. The 3-Heights™ Signature Creation and Verification Service relies on the PKCS#11 infrastructure for creating and verifying digital signatures. It constitutes the preferred infrastructure when dealing with hardware tokens and hardware security modules (HSMs).

1.2 Advantages

Using the 3-Heights™ Signature Creation and Verification Service has several advantages over the direct use of client software:

1.2.1 Hosted Tokens

By means of the 3-Heights™ Signature Creation and Verification Service personal tokens of employees may be hosted in a secure location and can be used remotely from any client computer which has access to the service by using individual credentials. The tokens may also be stored in a hardware security module (HSM).

1.2.2 Platform support

The 3-Heights™ Signature Creation and Verification Service uses a HTTP interface. This enables signature support for platforms that are otherwise not supported by the cryptographic infrastructure.

1.2.3 Restricted Intranet Access

The creation of a digital signature requires access to the servers of the certificate authority (CA) to be able to query the status of a certificate (OCSP or CRL) and optionally access to the servers of a time stamp authority (TS) to create trusted time stamps (TSP). With the 3-Heights™ Signature Creation and Verification Service these functions are centralized on a server and are not performed by the client any more. Thus, internet access is not required by the client computers and may be restricted to a dedicated server.

1.2.4 Robustness

The fact that the signature creation and verification is done in a separate process greatly increases the robustness of the client application.

If the cryptographic middleware produces a crash, only the respective worker process is terminated. The 3-Heights™ Signature Creation and Verification Service and the client application remain untouched.

2 Installation

2.1 Requirements

2.1.1 Operating Systems

The 3-Heights™ Signature Creation and Verification Service is available for the following operating systems:

- Windows 7, 8, 8.1, 10 – 32 and 64 bit
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016 – 32 and 64 bit

2.1.2 PKCS#11 Cryptography Provider

The middleware of the cryptographic infrastructure (USB Token, HSM) must be installed on the same computer as where the 3-Heights™ Signature Creation and Verification Service runs. The middleware also installs a DLL for the PKCS#11 interface. The name of the library, e.g. `cryptoki.dll` and the path on the file system must be known for the configuration of the signature software.

The following providers have been tested for interoperability with the 3-Heights™ Signature Creation and Verification Service:

- SafeNet Protect Server (`cryptoki.dll`)
- SafeNet Luna (`cryptoki.dll`)
- SafeNet Authentication Client (`eTPKCS11.dll`)
- CryptoVision (`cvp11.dll`)
- Siemens CardOS
- IBM OpenCrypTokI (`opencryptoki.dll`)

2.1.3 Client Software

The 3-Heights™ Signature Creation and Verification Service can be used by any signature-aware 3-Heights™ client software in particular with the following client software:

- 3-Heights™ Security Tool
- 3-Heights™ PDF to PDF/A Converter
- 3-Heights™ Document Converter

2.2 Windows

The 3-Heights™ Signature Creation and Verification Service comes as an MSI installer.

The installation of the software requires the following steps.

1. You need administrator rights to install this software.
2. Log in to your download account at `http://www.pdf-tools.com`. Select the product “Signature Creation and Verification Service”. If you have no active downloads available or cannot log in, please contact `pdf-sales@pdf-tools.com` for assistance.
   You will find different versions of the product available. We suggest to download the version, which is selected by default. If another is required, it can be selected using the combo box.
   The product comes as an MSI (Microsoft Installer) that provides an installation routine that installs and uninstalls the product for you.
   The package installs the 64-bit version, which runs on 64-bit platforms only.

3. Start the MSI and follow the steps in the installation routine.
4. Ensure the cache directory exists as described in chapter Special Directories.

2.3 Uninstall

If you have used the MSI for the installation, go to Start → 3-Heights™ Signature Creation and Verification Service... → Uninstall ...

2.4 Service Configuration

2.4.1 Configuration files

The service configuration of the 3-Heights™ Signature Creation and Verification Service is done by editing the configuration files `TokenConfig.xml` and `SignatureService.exe.config`. The files must reside in the same directory as the executable `SignatureService.exe`. The first file is used to configure the cryptographic tokens and the latter to configure the properties of the service itself.

XML structure of `TokenConfig.xml`:

- `<configuration>`
  - `ID`: The unique identifier of the cryptographic provider.
  - `ProviderString`[1]: A string to identify and access a cryptographic token. The attributes in the provider string are separated by a semicolon. The attributes for PKCS#11 providers are:
    - location of the PKCS#11 interface DLL[2]
    - slot number
    - user PIN
  - `Password`: The password which must be used by the client software to access the token.
  - All additional attributes are added to the provider session properties. E.g. for the Windows Cryptographic Provider the `StoreLocation` can be set to either `Current User` (default) or `Local Machine`.

Example: `TokenConfig.xml`

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <add ID="0001" ProviderString="c:/Program Files (x86)/SafeNet/Protect
    Toolkit C SDK/bin/sw/cryptoki.dll;0;123456" Password="pass01"
    LOCKING_OK="true"/>
  <add ID="0002" ProviderString="cvp11.dll;1;123456" Password="pass02"/>
  <add ID="0003" ProviderString="" Password="pass03"
    StoreLocation="Local Machine" />
</configuration>
```

XML structure of `SignatureService.exe.config`:

- `<configuration>`
  - `<appSettings>`
    - `add`: Add a `key`/`value` pair to the property bag. The following keys are supported.

[1] A more detailed description of the `ProviderString` can be found in the manual of the 3-Heights™ PDF Security API in the description of the property Provider of the interface PdfSignature.

[2] The 3-Heights™ Signature Creation and Verification Service and this dll must use the same platform, i.e. both must be either 32-bit or 64-bit.

- `Port`: The IP port number on which the service is listening.
- `TokenConfigFile`: The path to the XML configuration file. If empty, the server looks for a file named `TokenConfig.xml` in the installation directory.
- `LicenseKey`: The license key.

- `<system.serviceModel>`
  The 3-Heights™ Signature Creation and Verification Service is a Windows Communication Foundation (WCF) service. So this element can be used to configure service model properties.
- `<system.diagnostics>`
  Configure logging properties. By default the service creates a log file called `SignatureService.log`.

Example: `SignatureService.exe.config`

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <add key="Port" value="8080"/>
    <add key="TokenConfigFile" value="" />
    <add key="LicenseKey" value="X-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX" />
  </appSettings>
  ...
</configuration>
```

2.5 Client Configuration

Once you have the service configured and running, it can be accessed from any signature-capable 3-Heights™ product by specifying a provider string of the form:

```
"http://server.mydomain.com:8080/0001;pass01"
```

`server.mydomain.com` is the network name of the computer hosting the service.

`8080` designates the TCP/IP port that is configured the `SignatureService.exe.config` file.

`0001` designates the "ID" entry in the `TokenConfig.xml` file for the selected token.

`pass01` stands for the password that is configured for the selected token.

2.6 Service Execution

The 3-Heights™ Signature Creation and Verification Service is registered as a Windows service during installation. However, there is no obligation to actually execute the service as a Windows service. It can also be run in a command line window. Either way has its advantages and disadvantages:

Interactive Use Some cryptographic hardware (e.g. USB tokens and smart cards) are usable from within interactive sessions only (due to the Windows smartcard redirection). Also, the activities of the service can be monitored more easily.

Service The service will automatically start up when the computer is started, without the need to perform an interactive login.

For interactive use, change the startup mode of the Windows service to “manual” or “disabled”. Then, a Command Prompt window must be opened in the installation directory of the 3-Heights™ Signature Creation and Verification Service, where `SignatureService.exe` can be started:

```
C:\Program Files\PDF Tools AG\Signature Service> SignatureService.exe
```

2.7 Special Directories

2.7.1 Directory for temporary files

This directory for temporary files is used for data specific to one instance of a program. The data is not shared between different invocations and deleted after termination of the program.

The directory is determined as follows. The product checks for the existence of environment variables in the following order and uses the first path found:

Windows

1. The path specified by the `%TMP%` environment variable.
2. The path specified by the `%TEMP%` environment variable.
3. The path specified by the `%USERPROFILE%` environment variable.
4. The Windows directory.

2.7.2 Cache Directory

The cache directory is used for data that is persisted and shared between different invocations of a program. The actual caches are created in subdirectories. The content of this directory can safely be deleted to clean all caches.

This directory should be writable by the application, otherwise caches cannot be created or updated and performance will degrade significantly.

Windows

- If the user has a profile:
  `%LOCAL_APPDATA%\PDF Tools AG\Caches`
- If the user has no profile:
  `<TempDirectory>\PDF Tools AG\Caches`

where `<TempDirectory>` refers to the Directory for temporary files.

3 License Management

The 3-Heights™ Signature Creation and Verification Service requires a valid license in order to run correctly. If no license key is set or the license is not valid, then an error message will be printed to the service log.

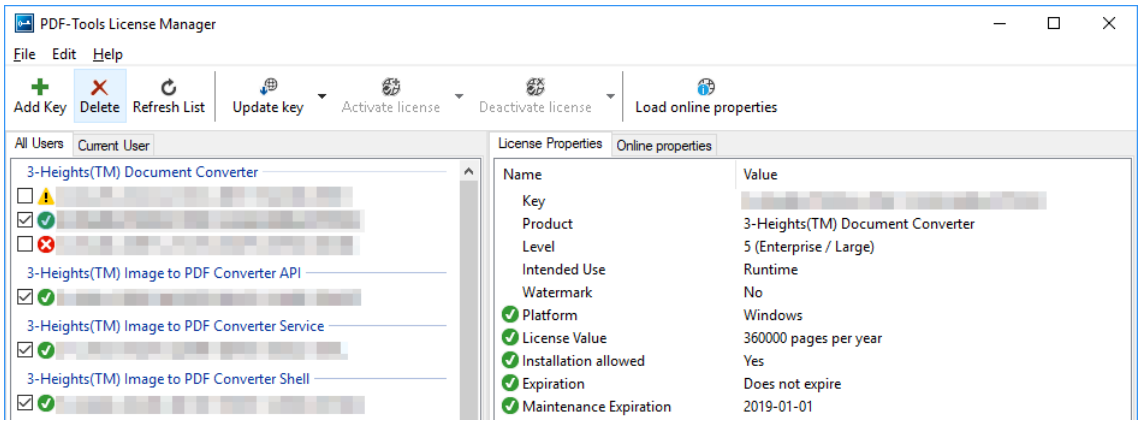
3.1 License Installation and Management

There are two possibilities to pass the license key to the application:

1. The license key is installed using the GUI tool (graphical user interface). This is the easiest way if the licenses are managed manually. It is only available on Windows.
2. The license key is installed using the shell tool. This is the preferred solution for for automated license management.

3.1.1 Graphical License Manager Tool

The GUI tool `LicenseManager.exe` is located in the `bin` directory of the product kit (Windows only).



List all installed license keys

The license manager always shows a list of all installed license keys in the left pane of the window. This includes licenses of other PDF Tools products. The user can choose between:

- Licenses available for all users. Administrator rights are needed for modifications.
- Licenses available for the current user only.

Add and delete license keys

License keys can be added or deleted with the “Add Key” and “Delete” buttons in the toolbar.

- The “Add key” button installs the license key into the currently selected list.

> **Note:** Services run by default under the LOCAL SERVICE user, not under the current user.

- The “Delete” button deletes the currently selected license keys.

Display the properties of a license

If a license is selected in the license list, its properties are displayed in the right pane of the window.

3.1.2 Command Line License Manager Tool

The command line license manager tool `licmgr` is available in the `bin\x86` and `bin\x64` directory.

> **Note:** The command line tool licmgr is not included in Windows platform kits, as the GUI tool is the recommended tool for managing Licenses. A Windows licmgr shelltool is available on request.

A complete description of all commands and options can be obtained by running the program without parameters:

```
licmgr
```

List all installed license keys

```
licmgr list
```

The currently active license for a specific product is marked with a * on the left side.

Example:

```
>licmgr list
Local machine:
  Product Name:
      1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
      1-YYYYY-YYYYY-YYYYY-YYYYY-YYYYY-YYYYY-YYYYY
    * 1-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ
Current user:
```

Add and delete license keys

Install new license key:

```
licmgr store 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Delete old license key:

```
licmgr delete 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Both commands have the optional argument `-s` that defines the scope of the action:

g For all users

u Current user

Display the properties of a license

```
licmgr info 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Properties that invalidate the license are marked with an X, properties that require attention are marked with an !. In that case an additional line with a comment is displayed.

Example:

```
>licmgr info 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
 - Key:          1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
 - Product:      Product Name
 - Features:     Feature1,Feature2
 - Intended use: Development
 - Watermark:    No
 - Platform:     Windows
 - Installation: Yes
 ! Activation:   2018-05-07
                  (The license has not yet been activated.)
 - Expiration:   Does not expire
 - Maintenance:  2019-04-27
```

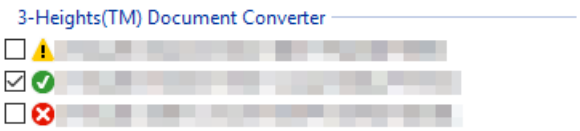
3.2 License Selection and Precedence

3.2.1 Selection

If multiple keys for the same product are installed in the same scope, only one of them can be active at the same time.

Installed keys that are not selected are not considered by the software!

In the Graphical User Interface use the check box on the left side of the license key to mark a license as selected.



With the Command Line Interface use the `select` subcommand:

```
licmgr select 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.2.2 Precedence

License keys are considered in the following order:

1. License key passed at runtime.
2. License selected for the current user

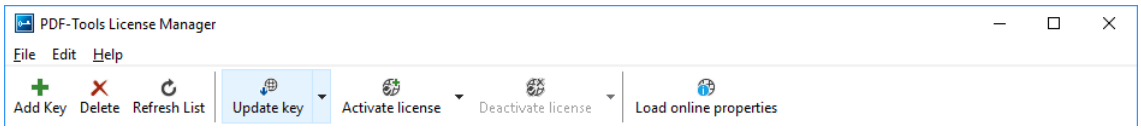
3. License selected for the current user (legacy key format)
4. License selected for all users
5. License selected for all users (legacy key format)

The first matching license is used, regardless whether it is valid or not.

3.3 Key Update

If a license property like the maintenance expiration date changes, the key can be update directly in the license manager.

In the Graphical User Interface select the license and press the button "Update Key" in the toolbar:



With the Command Line Interface use the `update` subcommand:

```
licmgr update 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.4 License activation

New licenses keys have to be activated (except for OEM licenses).

> **Note:** Licenses that need activation have to be installed in the license manager and must not be passed to the component at runtime.

The license activation is tied to a specific computer. If the license is installed at user scope, the activation is also tied to that specific user. The same license key can be activated multiple times, if the license quantity is larger than 1.

Every license key includes a date, after which the license has to be activated, which is typically 10 days after the issuing date of the key. Prior to this date, the key can be used without activation and without any restrictions.

3.4.1 Activation

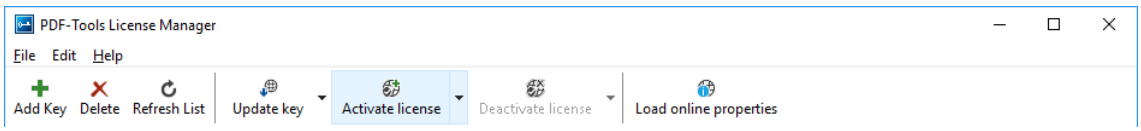
The License can be activated directly within the license manager. Every activation increases the activation count of the license by 1.

It is recommended to add a comment to the activation request which helps keeping track of all activations for a specific license key. In case of problems it also helps us providing support.

The comment is stored in the activation database as long as the license key remains activated. Upon deactivation it is deleted from the database immediately.

All activations and the corresponding comments can be examined using the **Load online properties** function of the license manager. The information is accessible to anyone with access to the license key.

In the Graphical User Interface select the license and press the button "Activate license" in the toolbar:



It is recommended to add a comment to the activation request by using the subsequent dialog box.

With the Command Line Interface use the `activate` subcommand:

```
licmgr activate 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Note that the key has to be installed first.

It is recommended to add a comment to the activation request by using the `-c` or `-cd` option:

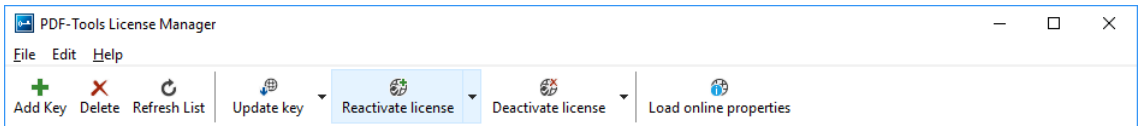
```
licmgr activate -cd 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
licmgr activate -c "custom comment" 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.4.2 Reactivation

The activation is tied to specific properties of the computer like the MAC address or host name. If one of these properties changes, the activation becomes invalid and the license has to be reactivated. A reactivation does **not** increase the activation count on the license.

The process for reactivation is the same as for the activation.

In the Graphical User Interface the button "Activate license" changes to "Reactivate license":



With the Command Line Interface the subcommand `activate` is used again:

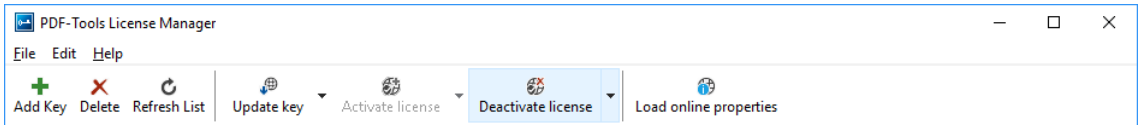
```
licmgr activate 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.4.3 Deactivation

To move a license to a different computer, it has to be deactivated first. Deactivation decreases the activation count of the license by 1.

The process for deactivation is similar to the activation process.

In the Graphical User Interface select the license and press the button "Deactivate license" in the toolbar:



With the Command Line Interface use the `deactivate` subcommand:

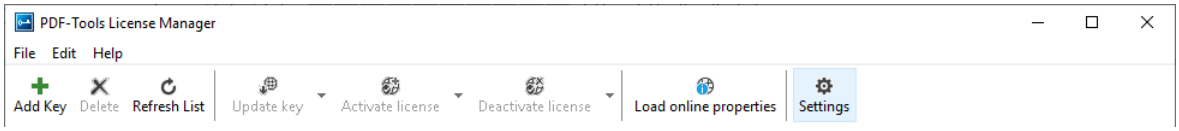
```
licmgr deactivate 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.5 Proxy Setting

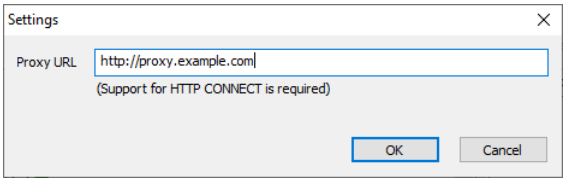
A proxy URL can be configured for computers that cannot access the internet without a web proxy.

> **Note:** The proxy must allow connections via HTTP CONNECT to the server www.pdf-tools.com:443.

In the Graphical User Interface press the button "Settings" in the toolbar:



and enter the proxy URL in the respective field:



3.6 Offline Usage

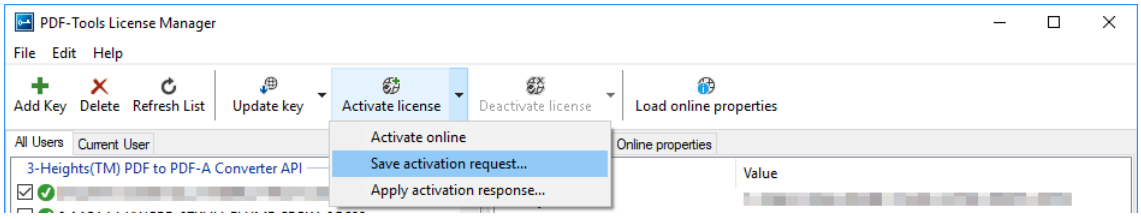
The following actions in the license manager need access to the internet:

- License Activation
- License Reactivation
- License Deactivation
- Key Update

On systems without internet access, a three step process can be used instead, using a form on the PDF Tools website.

3.6.1 First Step: Create a Request File

In the Graphical User Interface select the license and use the dropdown menu on the right side of the button in the toolbar:



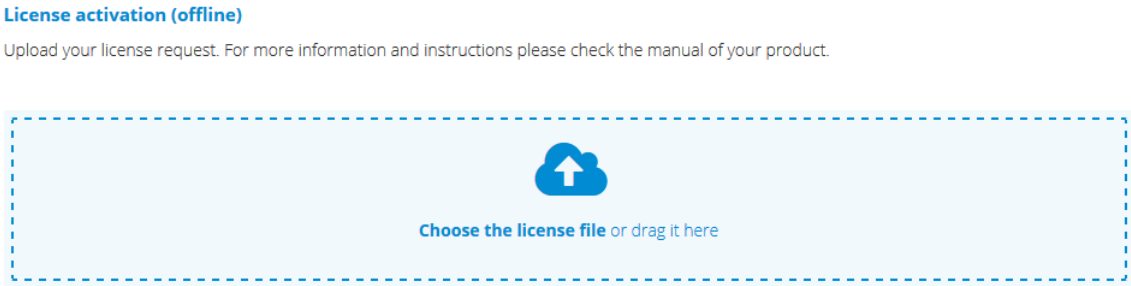
With the Command Line Interface use the `-fs` option to specify the destination path of the request file:

```
licmgr activate -fs activation_request.bin 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

License Deactivation: When saving the deactivation request file, the license is **deactivated immediately** and cannot be used any further. It can however only be activated again after completing the deactivation on the website.

3.6.2 Second Step: Use Form on Website

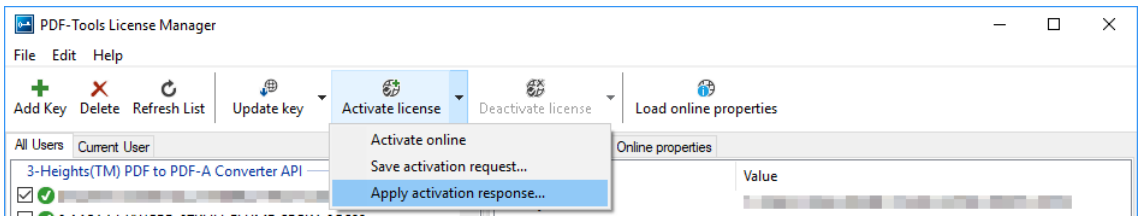
Open the following website in a web browser: http://www.pdf-tools.com/pdf20/en/mypdftools/licenses-kits/license-activation/ Upload the request by dragging it onto the marked area:



Upon success, the response will be downloaded automatically if necessary.

3.6.3 Third Step: Apply the Response File

In the Graphical User Interface select the license and use the dropdown menu on right side of the button in the toolbar:



With the Command Line Interface use the `-fl` option to specify the source path of the response file:

```
licmgr activate -fl activation_response.bin 1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

3.7 License Key Versions

As of 2018 all new keys will have the format `1-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`. Legacy keys with the old format `0-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` are still accepted for a limited time period.

For compatibility reasons, old and new version keys can be installed side by side and one key of each version can be selected at the same time. In that case, the software always uses the new version.

3.8 License Key Storage

Depending on the platform the license management system uses different stores for the license keys.

3.8.1 Windows

The license keys are stored in the registry:

- "HKLM\Software\PDF Tools AG" (for all users)
- "HKCU\Software\PDF Tools AG" (for the current user)

3.9 Troubleshooting

3.9.1 License key cannot be installed

The license key cannot be installed in the license manager application. The error message is: `"Invalid license format."`

Possible causes:

- The license manager application is an older version that only supports the legacy key format.

Solution

Use a current version of the license manager application or use a license key in the legacy key format if available.

3.9.2 License is not visible in license manager

The license key was successfully installed previously but is not visible in the license manager anymore. The software is still working correctly.

Possible causes:

- The license manager application is an older version that only supports the legacy key format.

Solution

Use a current version of the license manager application.

3.9.3 License is not found at runtime

The license is not found at runtime by the software. The error message is: `"No license key was set."`

Possible causes:

- The license key is actually missing (not installed).
- The license key is installed but not selected in the license manager.
- The application is an older version that only supports the legacy key format, while the license key has the new license format.

Solution

Install and select a valid license key that is compatible with the installed version of the software or use a newer version of the software. The new license key format is supported starting with version 4.10.26.1

For compatibility reasons, one license key of each format can be selected at the same time.

3.9.4 Eval watermark is displayed where it should not

The software prints an evaluation watermark onto the output document, even if the installed license is a productive one.

Possible causes:

- There is an evaluation license key selected for the **current user**, that takes precedence over the key for **all users**.

  > **Note:** The software might be run under a different user than the license manager application.

- An evaluation license key that is passed at runtime takes precedence over those selected in the license manager.
- There is an evaluation license key selected with a newer license format that takes precedence over the key in the older format.
- The software was not restarted after changing the license key from an evaluation key to a productive one.

Solution

Disable or remove all evaluation license in all scopes, check that no evaluation key is passed at runtime and restart the software.

3.9.5 Activation is not recognized

The license is installed and activated in the license manager, but the software does not recognize it as activated.

The error message is: `"The license has not been activated."`

Possible causes:

- There is an unregistered license key selected for the **current user**, that takes precedence over the key for **all users**. This leads to an error even if the same license is registered for all users.

  > **Note:** The software might be run under a different user than the license manager application.

- A license key that is passed at runtime takes precedence over those selected in the license manager. This leads to an error even if the same license is registered in the license manager.

  > **Note:** Licenses that need activation have to be installed in the license manager and must not be passed to the component at runtime.

- The software was not restarted after activating the license.

Solution

Disable, remove or activate all unregistered licenses in all scopes, check that no key is passed at runtime and restart the software.

3.9.6 Activation is invalidated too often

The license activation is invalidated regularly, for no obvious reason.

Possible causes:

- The MAC address used for computing the machine fingerprint is not static. This may happen e.g. for virtual network adapters with dynamic MAC address (VPN, Juniper, ...).

Solution

Update to a newer version (>= 4.12) of the PDF Tools product, deactivate the license key using the new license manager and activate it again. After that, an imporved fingerprinting algorithm is used.

Deactivation and activation have to be **executed separately**, a reactivation of the license in one step does not change the fingerprinting algorithm and thus does not solve the problem.

> **Note:** After this procedure, older products might not recognize the activation as valid anymore. Reactivating the license using an old license manager will revert the activation to the old fingerprinting algorithm.

As an alternative, remove any virtual network adapter with a dynamic MAC address.

3.9.7 Connection to the licensing service fails

The license activation/deactivation/update fails because the license manager cannot reach the licensing server.

The error message depends on the platform and the exact error condition.

Possible causes:

- The computer is not connected to the internet.
- The connection is blocked by a corporate firewall.

Solution

Make sure that the computer is connected to the internet and that the host `www.pdf-tools.com` is reachable on port 443 (HTTPS).

If this is not possible, try Offline Usage instead.

3.9.8 Offline usage fails due to a request/response mismatch

The offline license activation/deactivation/update fails because the response file does not match the request file.

The error message is: `"Mismatch between request and response."`

Possible causes:

- The response file is applied to a different machine than the request file was created.
- The response file as applied to a different user than the request file was created.
- The response file was applied to a specific user while the request was created for all users, or vice versa.
- The response file is applied to the wrong license key.
- Another request file has been created between creating the request file and applying the response file.
- The license key was updated between creating the request file and applying the response file.
- The license key was removed and re-added between creating the request file and applying the response file.

Solution

Delete any old request and response files to make sure they are not used by accident.

Retry the entire process as outlined in chapter 3.6 and refrain from making any other license-related actions between creating the request file and applying the response file.

Make sure that the response file is applied to exactly the same license key in exactly the same location (machine, all users or specific user) where the request file was created.

4 Glossary

4.1 Technical Terms

Signature	Cryptographic procedure to ensure the integrity and/or authenticity of a document. The signature may be embedded in the PDF document in the form of a cryptographic message (CMS/PKCS#7).
Certificate	A certificate is an electronic confirmation of the identity of a natural or legal person.
Public Key	The certificate contains a public key for the verification of the signature. The public key must match a private key, which is used for the creation of the signature.
Private Key	The private key is used to create the digital signature. It is contained on a cryptographic token and is protected against unauthorized access.
Token	A "container" (part of HSM, USB stick, smart card, etc.) that contains cryptographic objects such as certificates and private keys which are protected against unauthorized access.
Slot	A logical address of a USB-Token or a "plug-in position" inside the HSM that holds a token. The Token must not be physically present instead it may be part of the HSM.
PIN	A secret number, which is required to access the token. There are User PINs and Administrator PINs. The first allows for creating digital signatures and the latter for managing the cryptographic objects in the token.

4.2 Abbreviations

CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKCS	Public Key Cryptography Standard
QES	Qualified Electronic Signature
TSA	Time Stamp Authority
TSP	Time Stamp Protocol
PIN	Personal Identification Number

5 Troubleshooting

5.1 Additional Documentation

Additional information on PKCS11 including software and hardware stores for certificates can be found in the Technical Note on PKCS#11:

http://www.pdf-tools.com/public/downloads/manuals/TechNotePKCS11.pdf

5.2 HTTP Access, Proxy Server, Firewall

5.2.1 HTTP Access

For the application of a time stamp or an online verification of certificates, the signature software requires access to the server of the issuer (e.g. `http://ocsp.quovadisglobal.com` or `http://platinum-qualified-g2.ocsp.swisssign.net/`) via HTTP. The URL for verification is stored in the certificate; the URL for time stamp services is provided by the issuer. In case these functions are not configured, no access is required.

5.2.2 Proxy Server

In organizations where a web proxy is in used, it must be ensured that the required MIME types are supported. These are:

```
application/ocsp-request
application/ocsp-response
application/timestamp-query
application/timestamp-reply
```

The proxy server must be configured for all tokens using the provider session property `Proxy`.

5.2.3 Firewall

In case no web proxy server is used, it must be ensured the HTTP requests and responses can pass the firewall.

5.3 Usage of certificates from the Windows Certificate Store

Soft certificates and other certificates stored in the Windows Certificate Store can be used with the 3-Heights™ Signature Creation and Verification Service as well. For this, a token can be used with a ProviderString configuration of the Microsoft Cryptographic Provider. The default for which is the empty string `ProviderString=""`.

Unless the token supports CNG, clients using token must set the provider session property MessageDigestAlgorithm to SHA-1. Special care must be taken that the 3-Heights™ Signature Creation and Verification Service runs in a session and under a user that has access to the signing certificate (see chapter Service Execution)

5.4 Error Codes and Possible Reasons

5.4.1 SIG_E_SESSION (0x8A130001)

- PKCS#11 library (e.g. DLL) not found
- The library does not have a PKCS#11 interface

- Initialization of the library failed due to too many applications and / or threads access the library concurrently
- The slot number is invalid
- The PIN is incorrect

5.4.2 SIG_E_STORE (0x8A130002)

- This error does not occur in combination with PKCS#11

5.4.3 SIG_E_CERT (0x8A130003)

- Certificate not found in the defined slot number

5.4.4 SIG_E_OCSP (0x8A130004), SIG_E_TSP (0x8A130005)

- Failed to establish an HTTP connection (see requirements)
- The server of the issuer is not available

5.4.5 SIG_E_PRIVKEY (0x8A130006)

- The private key is not installed in the slot number or does not match the certificate
- The PIN is incorrect
- The signature algorithm in the certificate is unknown
- The message digest algorithm sent by the client is not supported by the token

5.4.6 PDF_E_SIGVAL (0x85410002)

- The provider name is invalid when starting the session

6 Version History

6.1 Patches in Version 4.12

Note that the version number of the initial “final release” is 4.12.26.3.

Patch 4.12.26.4

- **Improved** error messages for failed HTTP connections in various situations (including license manager).
- **Added** missing documentation and release note for the proxy setting in the GUI license manager.
- **Improved** license reactivation behavior of the commandline license manager (licmgr): The server is now only contacted if necessary.
- **Improved** behavior of license manager when dealing with licenses of unreleased products.

6.2 Changes in Version 4.12

- **New** HTTP proxy setting in the GUI license manager.

6.3 Changes in Version 4.11

No functional changes.

6.4 Changes in Version 4.10

- **Improved** robustness against corrupt input PDF documents.
- **New** support for the European PAdES Standard (ETSI EN 319 142), for which a new protocol version has been introduced. So for new clients, a new version of the service must be used. The new service can handle both clients using the old and the new version of the protocol.

6.5 Changes in Version 4.9

- **Improved** support for and robustness against corrupt input PDF documents.
- **Improved** repair of embedded font programs that are corrupt.
- **New** support for OpenType font collections in installed font collection.
- **Improved** metadata generation for standard PDF properties.
- **New** implementation as Windows Communication Foundation (WCF) service.
  - Improved configuration. Note that during upgrade configuration files must be merged manually as described in the user manual.
  - Support multi-threaded operation.
  - Improved performance due to provider session caching.
  - More detailed logging and powerful logging configuration.
  - Upon request, the service is also available as IIS web application, e.g. to support HTTPS or advanced user authenticaion.
- **New** support for provider session properties, e.g. `Proxy` or `LOCKING_OK`.

- **New** application configuration entry `LicenseKey`.
- **New** support for local machine store of Windows Cryptographic Provider.

6.6 Changes in Version 4.8

- **Improved** creation of annotation appearances to use less memory and processing time.
- **Added** repair functionality for TrueType font programs whose glyphs are not ordered correctly.

7 Licensing, Copyright, and Contact

PDF Tools AG is a world leader in PDF (Portable Document Format) software, delivering reliable PDF products to international customers in all market segments.

PDF Tools AG provides server-based software products designed specifically for developers, integrators, consultants, customizing specialists and IT-departments. Thousands of companies worldwide use our products directly and hundreds of thousands of users benefit from the technology indirectly via a global network of OEM partners. The tools can be easily embedded into application programs and are available for a multitude of operating system platforms.

Licensing and Copyright

Contact

PDF Tools AG
Kasernenstrasse 1
8184 Bachenbülach
Switzerland
http://www.pdf-tools.com
pdfsales@pdf-tools.com