

Certificates

Signing with pDoc Signer and related applications requires the use of a digital certificate, with the installer providing one by default (either current or expired). **Users are encouraged to use and keep current, a certificate appropriate to their needs (an organization certificate for example).** See user guide for instructions. To update the default certificate, see below.

Updating default pDoc certificate + Previous Version Instructions

Check for a current installed Topaz pDoc application (pDoc Signer V4.3 for example), download the pDoc Cert Updater from the Topaz website, and copy pDocCertUpdater.exe to the desktop.

Right click on pDocCertUpdater.exe and **select Run as administrator** and acknowledge the prompts, including the prompt to update the trusted CA certificate store. If you do not have administrator permission, you will probably need to contact your IT department. The pDoc Signer certificate updater will replace the existing signing certificate in any pDoc applications that are found installed. It also adds the Topaz Systems CA root certificate to the user's trusted CA certificate store. This approach reduces the frequency of update required by the pDoc certificate.

If you are running a version of pDoc signer earlier than 4.3, any installed pDocSigner.pfx files will need to be replaced after running pDocCertUpdater. Replacement files are available from Topaz tech support.

Silent Installation and Update

Running pDocCertupdater.exe /s will suppress the standard messages however the user will still be prompted for administrator permissions and to acknowledge the update to the trusted root certificates.

Running pDocCertUpdater.exe /s /r will replace the pDoc signing certificate silently but will not install the TopazSystemsCA root certificate. To assist those using this approach, the TopazSystemsCA root certificate is provided as a PFX file (for simplified installation a password is not needed).

<https://www.topazsystems.com/ca/TopazSystemsCA.pfx>

Simply download and run, selecting all the default options presented. The root CA certificate will be installed in the local current user's **Trusted Root Certificate Authority** store. Once installed it can be exported as a binary DER or HEX encoded certificate (.CER) file for enterprise redistribution to domain machines using GPOs.

Expired Certificates

Certificates expire as a normal part of the process of using them to assist in the signing process. The certificate needs to be current and not expired for pDoc signer to continue capturing signatures.

If Signature validity is shown as UNKNOWN in Adobe Acrobat after the certificate used for capture has expired, you can set "Verify Signatures Using:" to "Time at which the signature was created", under the Verification Time section listed in Acrobat under:

Go to Edit -> Preferences -> Signatures -> Verification