Oracle
Textura
DocuSign Help AUS

Version 22
January 2022

Contents

DocuSign Help

In This Section

DocuSign Overview

Documents signed within the Textura Payment Management (TPM) application are signed using DocuSign's secure cloud platform. As the market-leader in digital signature capabilities, DocuSign meets the industry's rigorous security certification standards and operations. DocuSign's comprehensive approach ensures the security, privacy, compliance, and enforceability of your DocuSign transactions.

TPM will notify the Signer when the billing documents are ready for a signature. With DocuSign integration, the signing process does not require the Signer to enter a PIN to at the time of signing due to robust single-sign-on between TPM and the DocuSign platform. DocuSign provides on-screen instructions and visual guides for each step, ensuring an intuitive end-user experience. During the signing process, the Signer signs all documents consecutively. Once the Signer applies a signature to all necessary places, the **Finish** button returns the Signer to TPM.

Each page of a document signed on TPM will now contain a stamp indicating the secure DocuSign Envelope ID that contains that document. The Envelope ID is the permanent reference to the DocuSign signing transaction for that document, and you can use it to access the DocuSign Certificate of Completion described below.

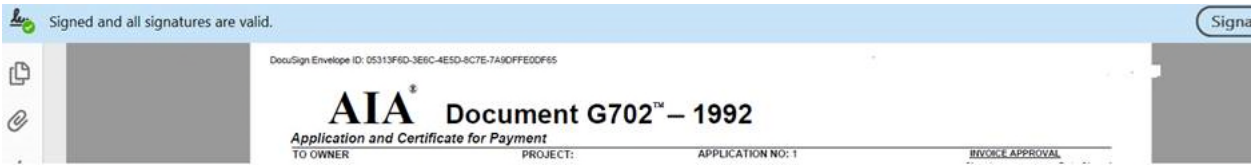
- ***Enforceability and Non-Repudiation of Transactions***
- ***Certificates of Completion.***

Download this DocuSign Overview as a PDF file https://docs.oracle.com/cd/E97083_01/en/docusign/tpm_docusign_guide_aus.pdf.

Enforceability and Non-Repudiation of Transactions

DocuSign takes the security, integrity, and enforceability of the documents signed on their platform very seriously. As noted in their documentation at ***https://www.docusign.com/how-it-works/security*** (see https://www.docusign.com/how-it-works/security - ***https://www.docusign.com/how-it-works/security***), DocuSign employs best-in-class security and privacy standards for and industry-leading technology to ensure the integrity of signatures for documents signed using their platform. As a result, DocuSign is willing to attest to the validity of documents signed with their technology, allowing DocuSign to warrant compliance with the ESIGN Act.

All documents signed on the DocuSign platform utilize a hashing algorithm you can use to verify that the documents have not been modified, and DocuSign's PKI digital certificate technology secures documents and signatures with tamper-evident seals. These seals are visible from most PDF viewers including ***Adobe Reader*** (see Adobe Reader - ***https://support.docusign.com/en/guides/ndse-user-guide-sending-digital-certificates***) and ***BlueBeam*** (see BlueBeam - ***https://support.bluebeam.com/online-help/revu2018/Content/RevuHelp/Tutorials/Digital-Signatures.htm***), as shown below.



Each document signed in TPM using DocuSign will now include the tamper-evident seal. This seal allows confirmation of the following, without returning to TPM to review a vaulted copy of the document:

- The document has not been modified or tampered with since the signature was applied
- The signer's identity is valid
- The time of the signature was recorded properly.

Additionally, DocuSign provides this online utility you can use to verify a document signed on their platform: ***https://validator.docusign.com/*** (see https://validator.docusign.com/ - ***https://validator.docusign.com/***).

> **Note:** Documents downloaded individually from the TPM application will contain the tamper-evident seal. However, documents combined into a single PDF, as from the **Print Period Documents** page, will not contain the DocuSign seal on the resulting PDF.

Certificate of Completion

In addition to the tamper-evident seal that accompanies each document, DocuSign also provides a court-admissible, digitally signed, and tamper-evident ***Certificate of Completion*** (see Certificate of Completion - ***https://support.docusign.com/en/guides/ndse-user-guide-history-coc***) that contains a comprehensive audit trail for each envelope which includes:

- Signing parties' names
- Digital signatures
- Public IP addresses
- Signing location (if provided)
- Chain of custody (sent, viewed, signed, etc.)
- Timestamps.

Unlike the historic documents signed on TPM using Pronto, the documents signed using DocuSign do not contain an embedded link you can use to access the audit trail and vaulted copy of the document.

To facilitate review of the detailed audit trail associated with any DocuSign envelope signed on TPM, TPM will provide several mechanisms to retrieve the DocuSign Certificate of Completion for a specific envelope signed on the platform. First, Certificates of Completion will be available for download from the **Progress Claim Control Log** page in TPM. Second, you can access a new publicly accessible portal at ***https://cpm.texturacorp.com/docusign*** (see https://cpm.texturacorp.com/docusign - ***https://cpm.texturacorp.com/docusign***) to download a tamper-evident Certificate of Completion using the Envelope ID printed on each document.

In an upcoming release, the Certificate of Completion will also be added to the **Print Period Documents** page you can download the document in bulk if required.

> **Note:** To ensure the enforceability of all documents signed on TPM using Pronto, Oracle will continue to support access to the vaulted copy of each document and the signature audit information linked to from documents signed on TPM via Pronto for 10 years from the signing date of the document.

Copyright

Oracle Textura DocuSign Help AUS