



ENTRUST

Adobe® Acrobat® DC with Entrust Time Stamp Server™

nShield® HSM Integration Guide

2024-02-12

Table of Contents

| | |
|---|----|
| 1. Introduction | 1 |
| 1.1. Product configurations | 1 |
| 1.2. Requirements | 2 |
| 2. Procedures | 3 |
| 2.1. Check the status of TSS and the Security World | 3 |
| 2.2. Configure Adobe Acrobat DC to use TSS | 4 |
| 2.3. Set up a digital ID | 6 |
| 2.4. Import certificates into Adobe Acrobat DC | 7 |
| 2.5. Configure the certificates | 8 |
| 2.6. Sign and time-stamp a PDF document | 9 |
| 2.7. Check how many time-stamps have been issued | 10 |
| 3. Additional resources and related products | 11 |
| 3.1. nShield Solo | 11 |
| 3.2. Time Stamping Option Pack | 11 |
| 3.3. Entrust digital security solutions | 11 |
| 3.4. nShield product documentation | 11 |

Chapter 1. Introduction

Adobe Acrobat DC enables users to create, control, and secure Portable Document Format (PDF) documents. Users can also collectively review and edit documents, and convert documents from other formats to PDF.

The integration of Adobe Acrobat DC with Entrust nShield Time Stamp Server (TSS) performs signing and time-stamping to provide authenticity, integrity and non-repudiation of the document.

TSS is a time-stamp appliance. It uses the industry-standard IETF RFC 3161 protocol to provide time-stamps. TSS also provides a secure auditable trail of time for the purposes of non-repudiation. Adobe Acrobat DC natively supports the RFC 3161 time-stamp service provided by TSS. Time-stamp a PDF document to validate that document's authenticity at the time it was time-stamped.

nShield Hardware Security Modules (HSMs) integrate with Adobe Acrobat DC to enable a customer the ability to identify the publisher of a document and to verify that no one has altered the contents or any other aspect of the original document after it has been signed. Digital signatures, such as those used to sign for example Adobe PDF documents, rely on proven cryptographic techniques and the use of one or more private keys to sign and time-stamp the published software. It is important to maintain the confidentiality of these keys.

The benefits of using an HSM with Adobe Acrobat DC include:

- Protection for the organizational credentials of the software publisher.
- Secure storage of the private key.
- FIPS 140 Level 3 validated hardware.
- Provision of a trusted time-stamp to RFC 1631.

The benefits of TSS include:

- Centrally managed and secured time-stamp appliance.
- FIPS secure and audited link to a master time source.

1.1. Product configurations

Entrust has successfully tested the integration between TSS and Adobe Acrobat in the following configurations:

| Operating System | Adobe Acrobat DC version | nShield TSS version | Security World | Firmware |
|---------------------|--------------------------|---------------------|----------------|----------|
| Windows Server 2019 | Pro | 8.0 | 12.81.2 | 12.72.1 |



This integration requires that the Default TSA be used for Adobe signing and time-stamping functionality.



Throughout this guide, the term HSM refers to the nShield Solo XC.

Other product configurations might work, but not all possible combinations, but have not been tested by Entrust.

1.2. Requirements

Before setting up the time-stamping functionality, ensure that:

- nShield software and hardware are installed and operational - the server URL of TSS will be needed during the integration process.
- Security World has been created and usable.
- The nShield Time Stamp Option Pack™ (TSOP) has been installed and the Default TSA is usable.
- Required certificates have been imported into the trusted Root CA on the local machine:
 - Signing root certificate.
 - If a third party is used to sign TSA certificates, subordinate certificate(s).
- Adobe Acrobat Pro DC has been installed.
- Appropriate Administrator rights are available to edit Adobe Acrobat settings options.

This document assumes that:

- Familiar with documentation supplied with TSOP and have installed TSS.
- Familiar with Adobe Acrobat DC documentation and have installed Adobe Acrobat DC.



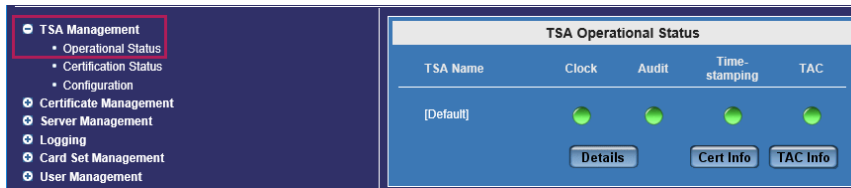
Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Procedures

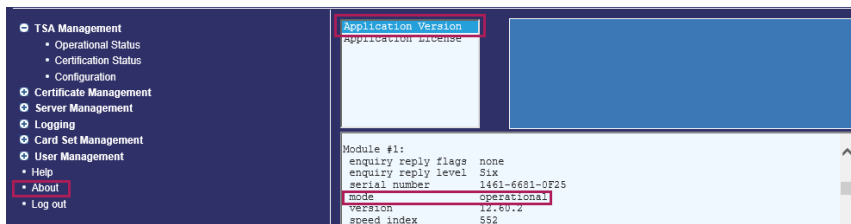
2.1. Check the status of TSS and the Security World

To check the status of TSS and the Security World:

1. Ensure that your TSA is healthy and operational. To do, this, access the **TSA Operational Status** page, and check that the TSA shows all green lights. If you do not have all green lights after creating a new certificate, then try restarting the DSE200 service.



2. Ensure that the Security World is operational and healthy:



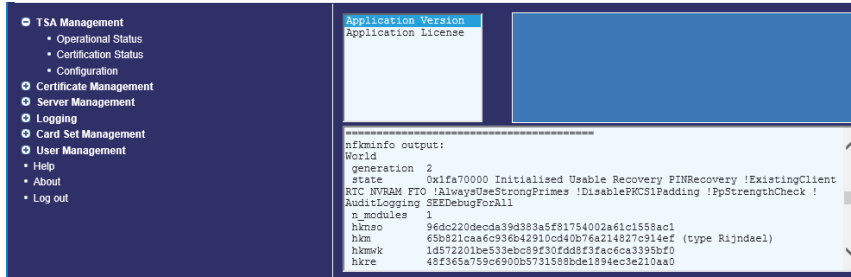
- a. On the left, select **About**.
- b. Select **Application Version**.
- c. Scroll down to show **Module 1#**.

The **mode** should show as **operational**.

3. Continue to scroll down to **nfkminfo output: World**.

The **state** should show as **Initialised** and **Usable**. There should be no exclamation marks (!).

If either properties are preceded by an **!**, ensure that the Security World is available and operational.

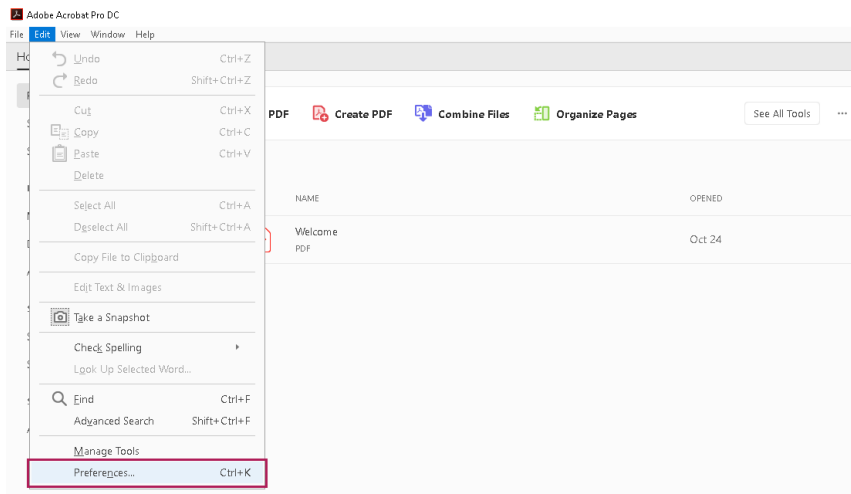


4. Continue to scroll down to **hardware status** and ensure that it is reported as **OK**.

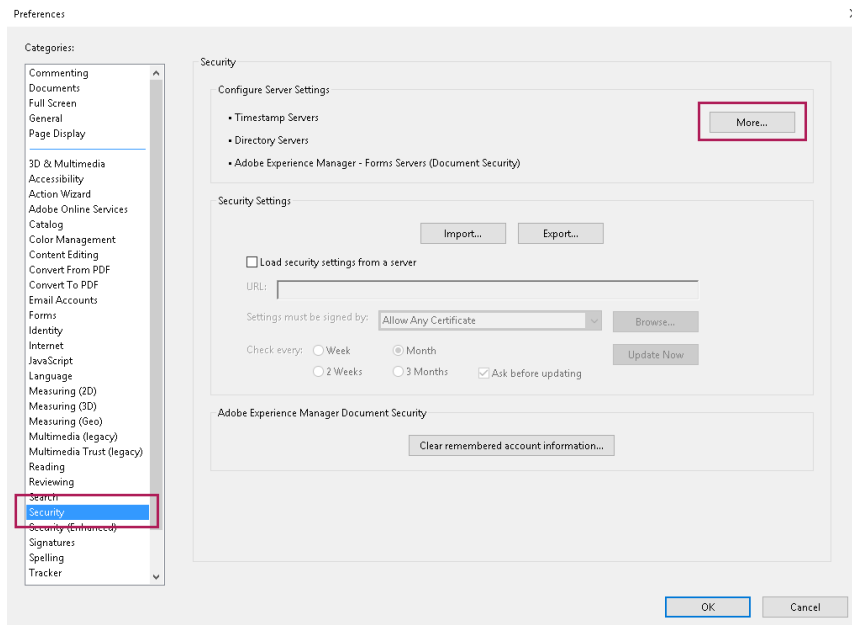
2.2. Configure Adobe Acrobat DC to use TSS

To configure Adobe Acrobat DC to use TSS:

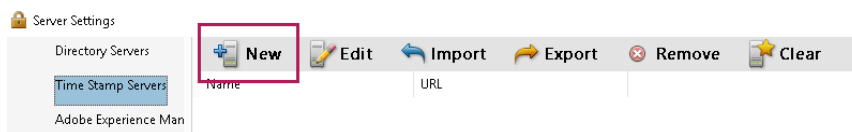
1. In the Windows Start menu, select **Adobe Acrobat DC**.
2. In the **Edit** menu of Adobe Acrobat, select **Preferences**.



3. From the list of categories, select **Security**.



4. In the **Configure Server Settings** pane, select **More**.
5. In the **Server Settings** dialog, from the list of options, select **Time Stamp Servers**.



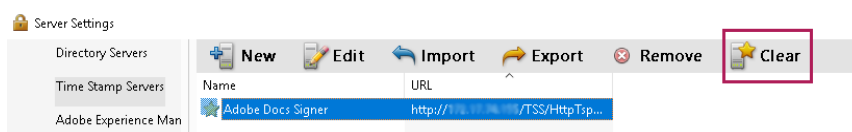
6. In the top ribbon, select **New**.
7. In the **New Time Stamp Server** dialog, enter a name and the server URL of TSS, then select **OK**.

The server is now added.



8. Select the TSS, and in the top ribbon select **Set Default**.
9. When prompted **Are you sure you want to make this your new default server?**, select **OK**.

If the default is successfully set, **Set Default** is replaced by **Clear**.

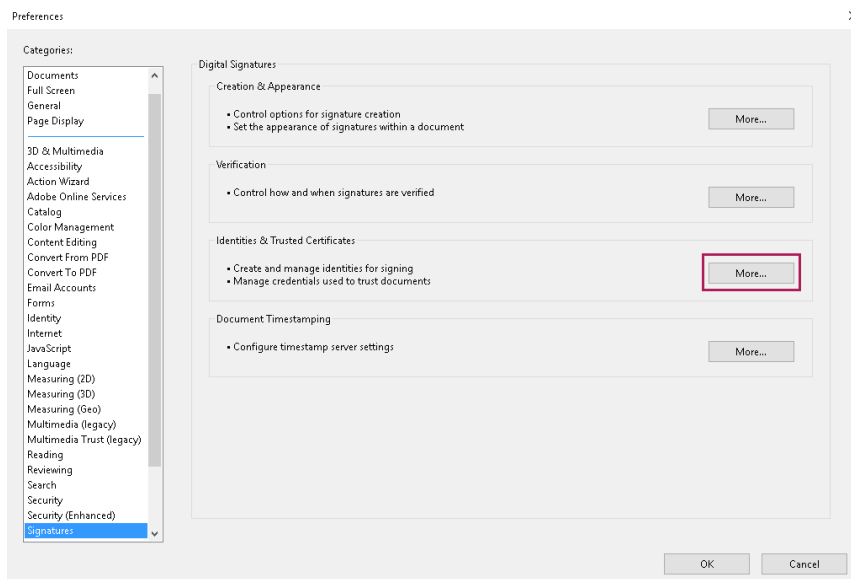


10. Close the **Server Settings** dialog.

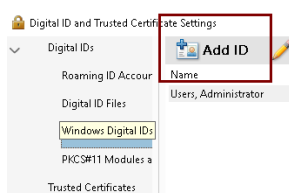
2.3. Set up a digital ID

To set up a digital ID:

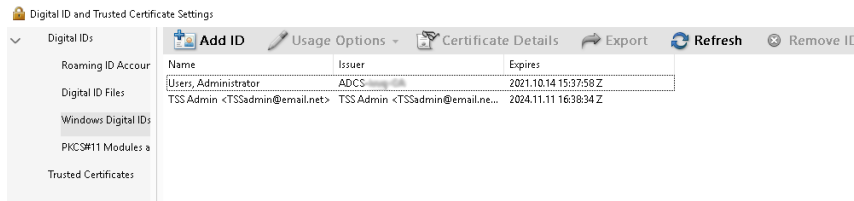
1. Stay in the **Preferences** dialog of Adobe Acrobat DC, and from the list of categories, select **Signatures**.



2. In the **Identities & trusted Certificates** box select **More**.
3. In the **Digital ID and Trusted Certificate Settings** dialog, select **Digital IDs > Windows Digital ID Files**, then select **Add ID**.



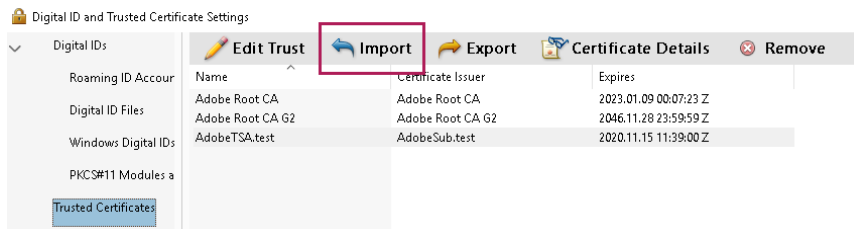
4. Select **Add a new self-signed digital ID**, then select **Next**.
5. Fill in the information fields (name, organizational unit, and so on), use the drop-down lists to select the key algorithm and the digital ID usage, then select **Finish**.
6. Confirm that the new ID appears in the list.



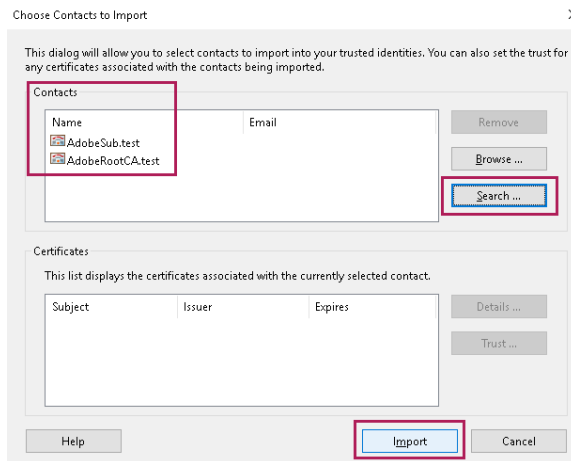
2.4. Import certificates into Adobe Acrobat DC

To import certificates into Adobe Acrobat DC:

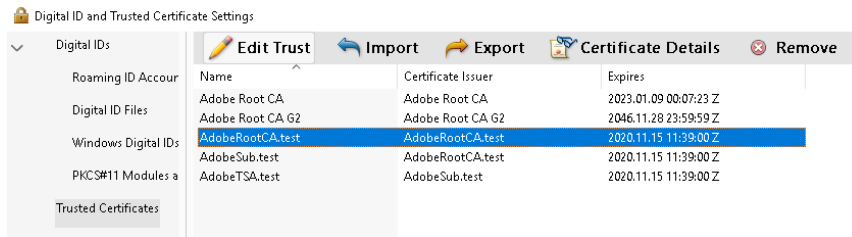
1. Still in the **Digital ID and Trusted Certificate Settings** dialog, select **Digital IDs > Trusted Certificates**.
2. On the **Trusted Certificates** tab, select **Import**.



3. In the **Choose Contacts to Import** dialog, use **Browse** or **Search** to locate the Root Certificate and any Subordinate Certificates.
4. Double-click the certificates to select. They will appear in the **Contacts**.



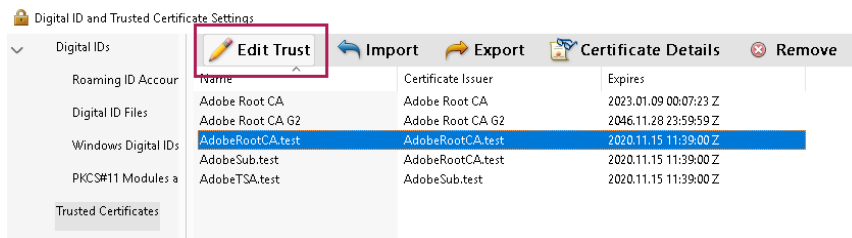
5. To add the certificates, select **Import**, then select **OK** to close the confirmation dialog about the import.
6. Confirm that the imported certificates appear in the list.



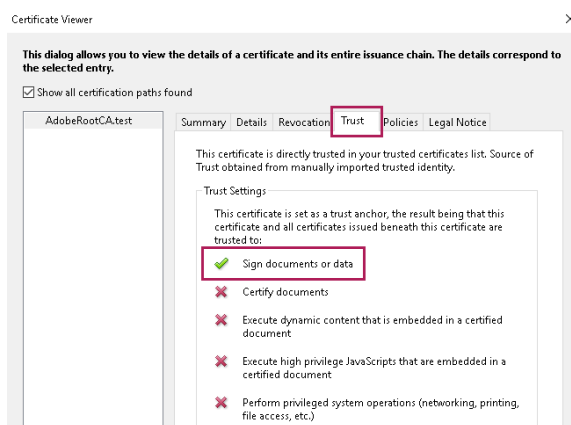
2.5. Configure the certificates

To configure the certificates:

1. Still in the **Digital ID and Trusted Certificate Settings** dialog, select the imported Root CA, then in the ribbon at the top of the window select **Edit Trust**.



2. Select **Use this certificate as a trusted root**, then select **OK**.
3. In the ribbon at the top of the window select **Certificate Details**.
4. In the **Certificate Viewer** dialog, switch to the **Trust** tab.

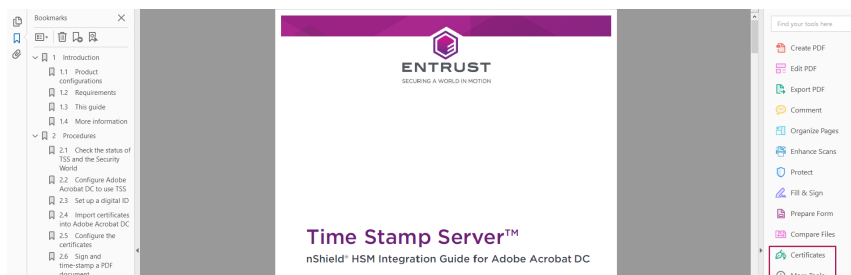


5. Ensure that there is a green check mark next to **Sign documents or data**, then select **OK**.
6. Close the **Digital ID and Trusted Certificates Settings** dialog.
7. To exit the Adobe **Preferences** configuration settings, select **OK**.

2.6. Sign and time-stamp a PDF document

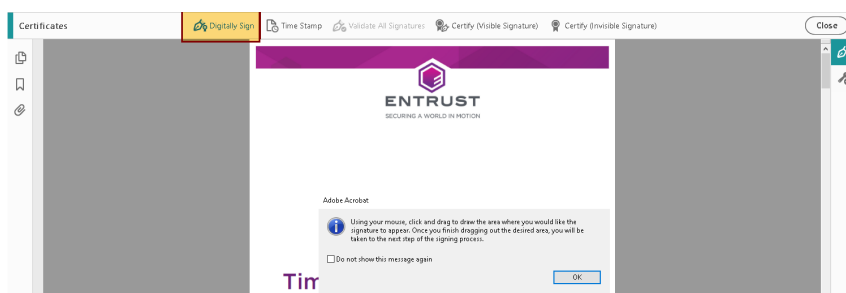
To sign and time-stamp a PDF document:

1. In Adobe Acrobat DC, open the document to sign and time-stamp it digitally.
2. From the ribbon on the right-hand side, select **Certificates**.



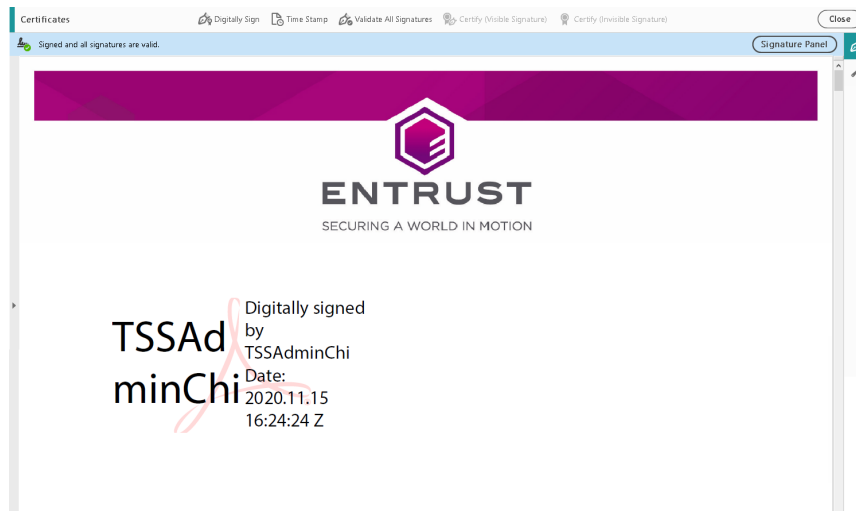
If the **Certificates** option is not visible:

- a. In the ribbon on the right-hand side, select **More tools**.
 - b. Under **Forms & Signatures**, select **Add** for the **Certificates** tool.
3. In the **Certificates** toolbar, select **Digitally Sign**.



4. Follow the information in the dialog box to select an area for signature, then select **OK**.
5. Select the Digital ID with which to sign, and select **Continue**.
6. Confirm all details and select **Sign**.
7. Choose a location to save the newly signed document.

To avoid overwriting the original file, use a different file name for the signed document.

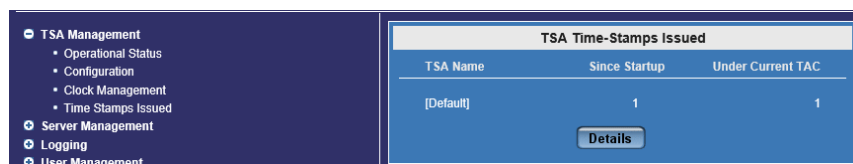


- To inspect the signature properties, right-click the signature on the PDF page and select **Show Signature Properties**.

2.7. Check how many time-stamps have been issued

To check how many time-stamps have been issued:

- Log in to TSS as Admin.
- Under **TSA Management**, select **Time Stamps Issued**.
- Check for the number of issued time-stamps under the current TAC since TSS was started up.



Chapter 3. Additional resources and related products

[3.1. nShield Solo](#)

[3.2. Time Stamping Option Pack](#)

[3.3. Entrust digital security solutions](#)

[3.4. nShield product documentation](#)