Time Stamp Option Pack

nShield® HSM Integration Guide for Microsoft 365

25 Nov 2022

Contents

1. Introduction

Microsoft 365 (previously called Microsoft Office) is a productivity suite for Microsoft Windows. The Microsoft 365 applications include Microsoft Word, Microsoft Excel, and Microsoft PowerPoint. Microsoft 365 also permits users to create, control, and digitally sign documents.

You can integrate Microsoft 365 with a Entrust Time Stamp Option Pack to permit the use of time stamping to seal documents. The Entrust Time Stamp Option Pack is referred to in this guide as Time Stamp Server (TSS). TSS is a time stamp appliance, which 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 nonrepudiation. In this way, you can time stamp an Microsoft document to validate that document's authenticity at the time it was time stamped.

1.1. Requirements

Entrust has successfully tested the integration between TSS and Microsoft 365 in the following configurations:

| Operating System	Microsoft 365 version	TSS version	HSM	Security World Version	Firmware
Microsoft Windows Server 2019 (x64)	Microsoft 365 2022	8.0	Solo XC	12.80.5	12.80.5

2. Setup

To enable Microsoft 365 to use a specified TSS appliance for its default time stamp service, you must:

- Install the root certificate of TSS on the client machine.
- Edit the registry settings.

2.1. Install the root certificate of TSS on the client machine

To install the root certificate of TSS on the client machine:

1. Log into the TSS as the security officer (**superuser**).

2. In the left pane, navigate to **TSA Management** > **Operational Status**. For example:
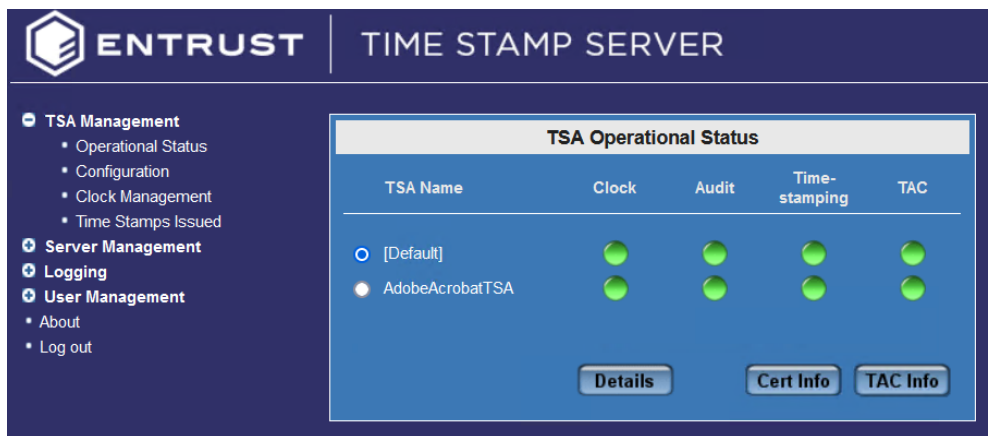
3. Select the **TSA Name**, then select **Cert Info**.

4. Select the certificate and **Export** it to a `.cer` file. For example:
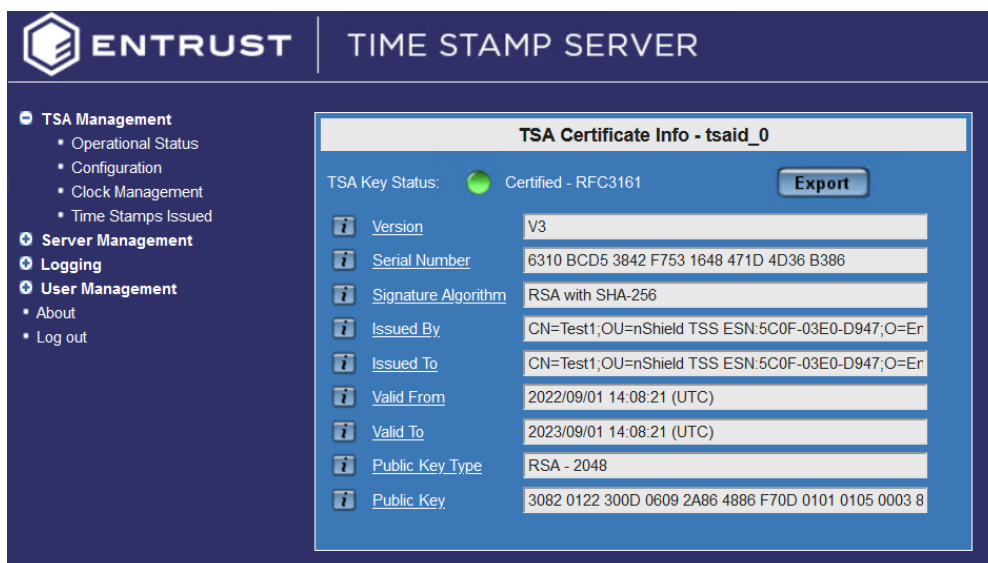
5. On the client machine, enter **certmgr** on the Windows **Start** menu to start the

Microsoft Certificate Manager.

6. In the left pane, navigate to **Certificates** > **Trusted Root Certificate Authorities** > **Certificates**.

7. Import the exported `.cer` file. For example:
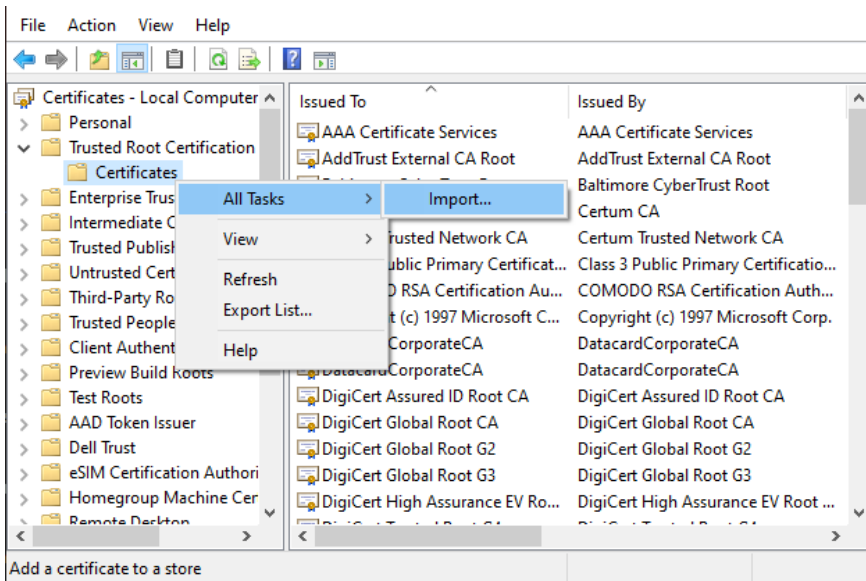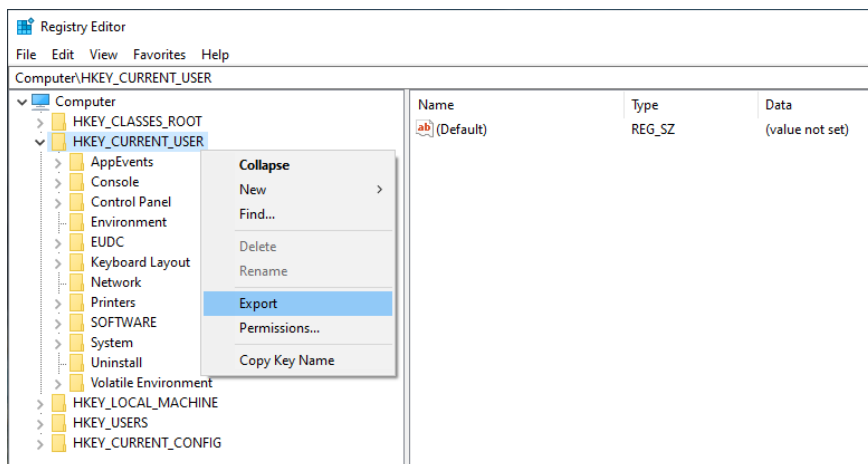

The certificate is added.

2.2. Edit the registry settings

To edit the registry settings:

1. On the Microsoft 365 computer, enter **regedit** on the Windows **Start** menu to start the Registry Editor.

2. In the left pane, navigate to **Computer** > **HKEY_CURRENT_USER**.

3. Export the **HKEY_CURRENT_USER** registry settings as a backup before you continue. For example:

4. Navigate to the following registry path:
   `Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Signatures`.

   > **i** | If the registry path does not already exist, you must create it.

5. Add the following variables to the registry path:

Name	Type	Data
MinXAdESLevel	REG_DWORD	2
Timestamp Required	REG_DWORD	1
TSALocation	REG-SZ	http://<TSS_IP_address>/TSS/HttpTspServer
XAdESLevel	REG_DWORD	5

In this table, `<TSS_IP_address>` is the IP address of the TSS appliance. You may use a host name instead of an IP address.

3. Procedures

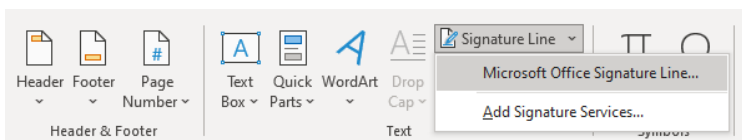To test and use the time stamping functionality:

- Add a signature line to a document.
- Sign the signature line in a document.

These procedures are described in the following sections.

3.1. Add a signature line to a document

To add a signature line to a document:

1. Open the document in Microsoft Word.
2. Click the location in the document where you want to add the signature line.
3. On the ribbon, select the **Insert** tab and locate the **Text** group.
4. Click the arrow next to **Signature Line**, and then select **Microsoft Office Signature Line**. For example:

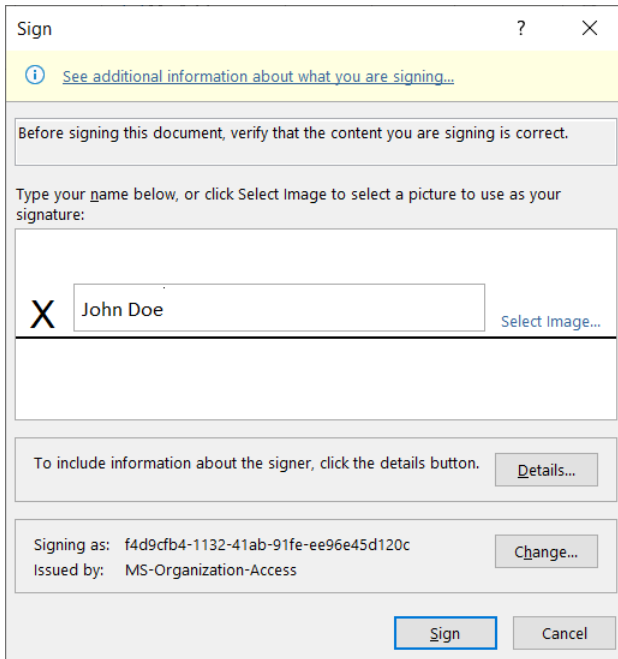5. The **Signature Setup** dialog appears. For example:

6. Click **OK**.

3.2. Sign the signature line in a document

When you sign the signature line in an Microsoft 365 document, you add both a visible representation of your signature and a digital signature.

To sign the signature line in a document:

1. Open the document in Microsoft Word.

2. In the document, double-click the signature line where your signature is requested.

3. In the **Sign dialog**, add the required information. For example:
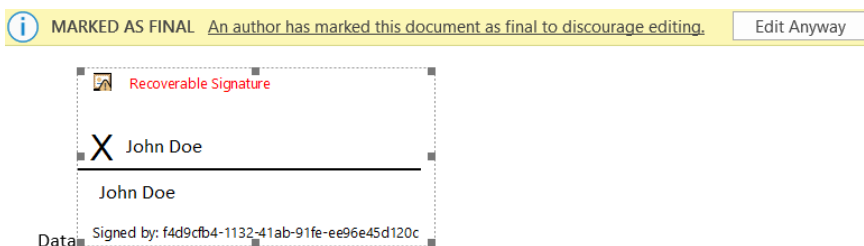

> ℹ️ Ensure the signer you choose is in the Trusted Certificates.

4. Click **Sign**.

   A message about the certificate selected not being verified may appear. In this case, you can click **OK** to continue.

   The document is signed. For example:

5. Click on the signed section of the document to confirm that the signature is valid. The signature type should be **XAdES-T**. For example:

Signature Details   ?   ✕

Recoverable Signature - The signer's certificate can't be verified, please try again later or check your network connection.

Signature type: XAdES-T

X   John Doe

John Doe

Signed by: f4d9cfb4-1132-41ab-91fe-ee96e45d120c

Commitment Type:

Purpose for signing this document:

Signing as: f4d9cfb4-1132-41ab-91fe-ee96e45d120c

Issued by: MS-Organization-Access

View...

See the additional signing information that was collected...

See information about the signer...

Close

4. Troubleshooting

The following table provides troubleshooting guidelines.

Problem	Cause	Resolution
When attempting to sign a document, the Get a Digital ID dialog appears instead of the Sign dialog.	The Microsoft Office registry entries have not been changed correctly.	Follow setup steps again.
When attempting to sign a document, the following error appears: Signing cannot be completed due to problems applying the required timestamp. Check your network connection.	Network issue.	Attempt to re-sign the document.