Time Stamp Option Pack

nShield® HSM Integration Guide for Microsoft 365

2025-11-24

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Table of Contents

Chapter 1. Introduction

Microsoft 365 (previously called Microsoft Office) is a productivity suite for Microsoft Windows which permits users to digitally sign documents. Entrust nShield Time Stamp Option Pack (TSOP) is a time stamp appliance rooted in FIPS and Common Criteria certified nShield Hardware Security Modules (HSM). This document describes the integration of Microsoft 365 with the Entrust time stamp appliance (TSS).

1.1. Product configuration

Entrust has successfully tested the nShield TSS integration with Office 365 in the following configuration:

1.1.1. TSS server

Product	Version
OS	Windows Server 2025

1.1.2. Client

Product	Version
OS	Windows 11
Microsoft 365	Office Professional Plus 2021

1.2. Supported nShield hardware and software versions

Entrust successfully tested with the following nShield hardware and software versions:

Product	Security World	TSOP	Firmware
nShield Solo XC	13.6.12	8.1.0	12.72.4 (FIPS 140-2 certified)

1.3. Requirements

- Knowledge of your organization Certificate Practices Statement and a Security Policy / Procedure in place covering administration of the HSM.
- Access to the Entrust TrustedCare Portal for downloads and support.
- An Entrust nShield Solo XC HSM.
- A dedicated Windows server.

Familiarize yourself with the nShield Documentation.

- The importance of a correct quorum for the Administrator Card Set (ACS).
- Whether Operator Card Set (OCS) protection or Softcard protection is required.
- If OCS protection is to be used, a 1-of-N quorum must be used.
- Whether your Security World must comply with FIPS 140 Level 3 or Common Criteria standards. If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. For more information see FIPS 140 Level 3 compliance.
- Whether to instantiate the Security World as recoverable or not.

Chapter 2. Deploy the Entrust TSS

All steps below are performed in a dedicated Microsoft server.

2.1. Install the Entrust nShield HSM

Install the nShield Solo XC HSM as described in Install a PCIe HSM.

2.2. Install the Security World software

1. Install the Security World software. For detailed instructions see nShield Security World Software v13.6.11 Installation Guide.
2. Add the Security World utilities path to the system path. This path is typically `C:\Program Files\nCipher\nfast\bin`.
3. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).
4. Open a command window and run the following utility to confirm the Security World installation. Notice the Server and HSM are **operational**.

   For example:

```
>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8D02-02E0-D947
 mode                 operational
 version              13.6.12
 ...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        8D02-02E0-D947
 mode                 operational
 version              12.72.4
 ...
```

2.3. Create a security world

1. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy when creating a Security World. For more information see Create a new Security World.

   The administrator card set (ACS) cards cannot be duplicated after

the Security World is created. You may want to create extras in case of a card failure or a lost card.

In order to use an existing Security World, the Security World will need to have been created with the SEEDebugForAll feature enabled.

For example:

```
>new-world -i -m <module_number> -Q <K/N> --mode=fips-140-2-level-3 --sp80056ar3 p dseeall
```

2. Confirm the Security World is **Usable**:

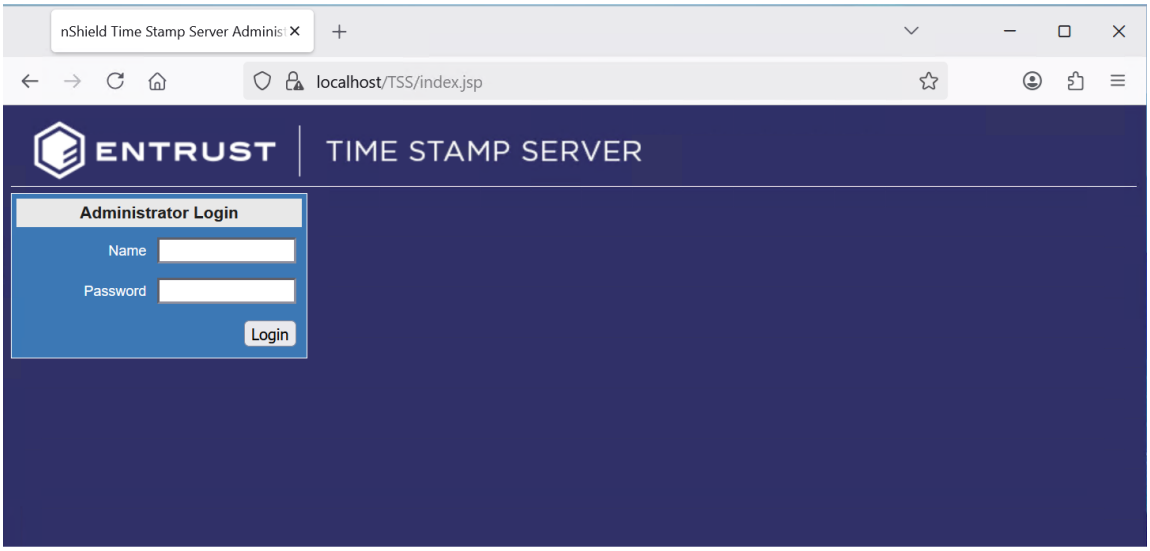
```
>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

2.4. Install the Time Stamp Option Pack software

1. Install Java Runtime Environment (32 bit) Oracle JRE v1.8 or later.

```
C:\Users\Administrator>java -version
java version "1.8.0_471"
Java(TM) SE Runtime Environment (build 1.8.0_471-b09)
Java HotSpot(TM) Client VM (build 25.471-b09, mixed mode, sharing)
```

2. Install the Time Stamp Option Pack software. For detailed instructions see TSOP v8.1.0 Install and User Guide.
3. Open the firewall ports described in section **TCP/IP and UDP port access** of the TSOP v8.1.0 Install and User Guide link above.
4. Enable the features as described in section **Enabling features**.
5. Configure the network as described in section **Configuring the TSS on the network**.
6. Test the connection to the TSS locally, and remotely from the Windows client. The credentials are listed in section **Accessing the TSS web interface**.



2.5. Install NTP

A Network Time Protocol (NTP) distribution or Time Stamp Master Clock (TSMC) is required to calibrate and audit the TSS. See section **TSOP installation prerequisites** of the TSOP v8.1.0 Install and User Guide link above.

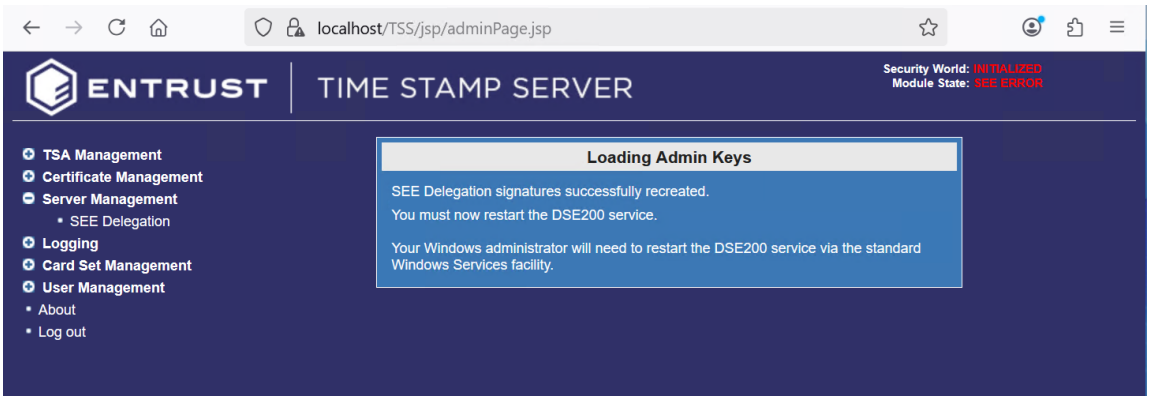
For the purpose on this integration, the Meinberg NTP package was installed.

Chapter 3. Configure the time stamp server

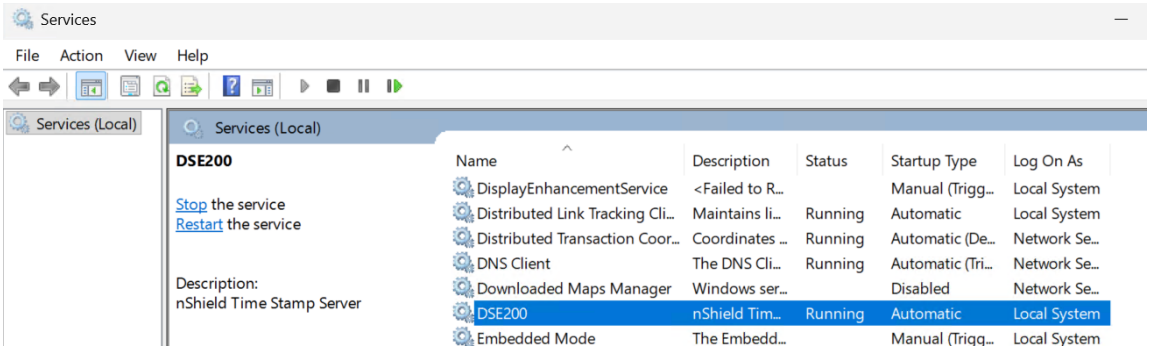
3.1. Activate the SEE delegation

The SEE Delegation gives the TSS SEE machine the permanent ability to set the real-time clock (RTC), to allocate nonvolatile memory (NVRAM), and to originate keys

1. Login to the WEB GUI with the security officer credentials.
2. Select **Server Management** → **SEE Delegation**. Then select **Next**.
3. Present the security world ACS. Then select **Next**.
4. Enter the ACS passphrase. Then select **Next**.



5. Restart the **DSE200** service.

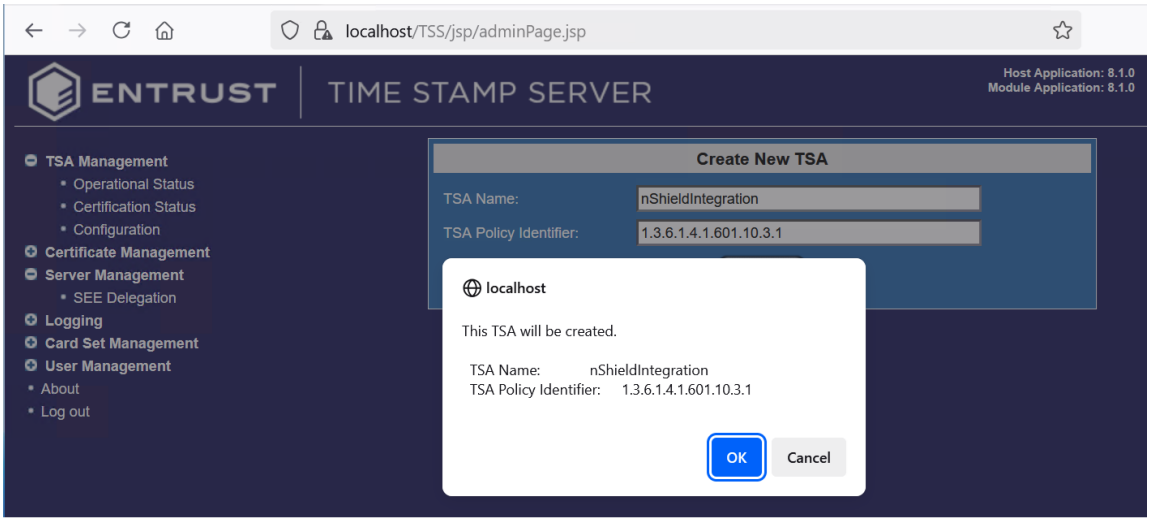


3.2. Create a Time Stamping Authority (TSA)

A TSA key is used for signing time-stamps. You can either create a single TSA and use the same signature key for all time-stamps, or create multiple TSAs depending on your requirements. TSA keys are created by your organization's Security Officer.

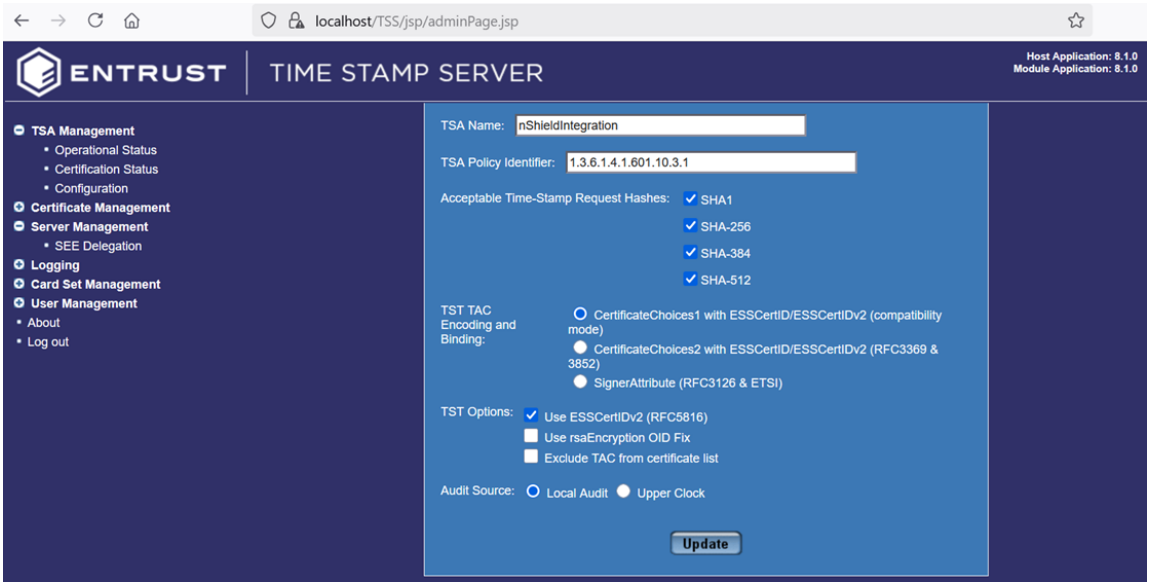
1. Login to the WEB GUI with the security officer credentials.
2. Select **TSA Management** → **Configuration**.

3. In the **TSA Configuration** pop-up window select **Add**.
4. Enter a name and select **Add**, for example **nShieldIntegration**.
5. Select **OK**

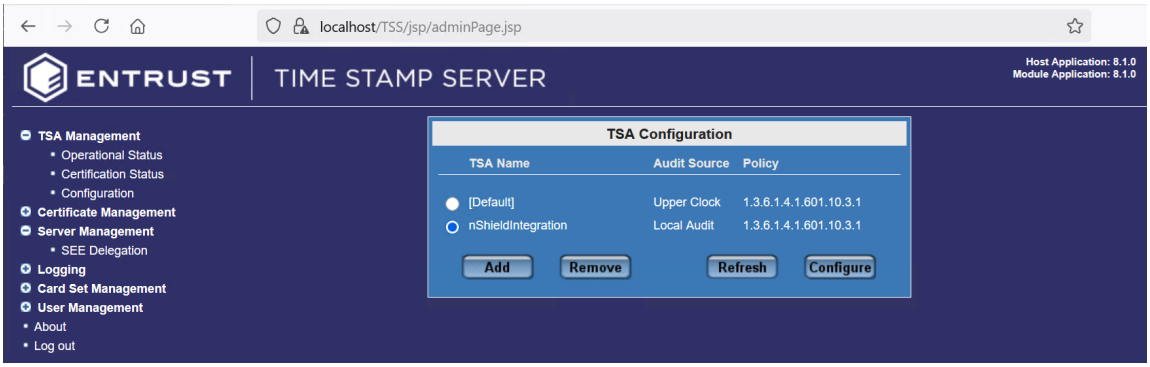


6. Select the options according to you organization security policy. Then select **Update** and **OK**.

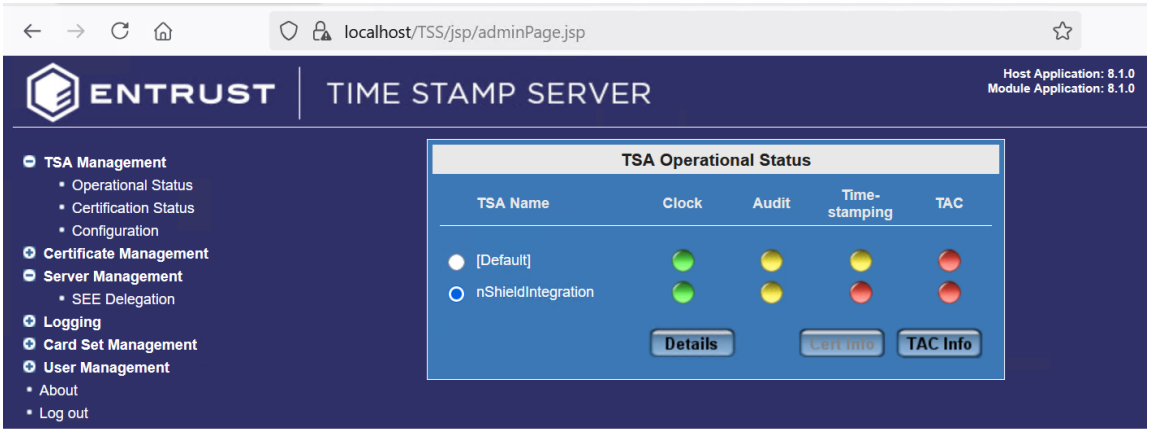
   For example:



7. The newly created TSA appears as follows.



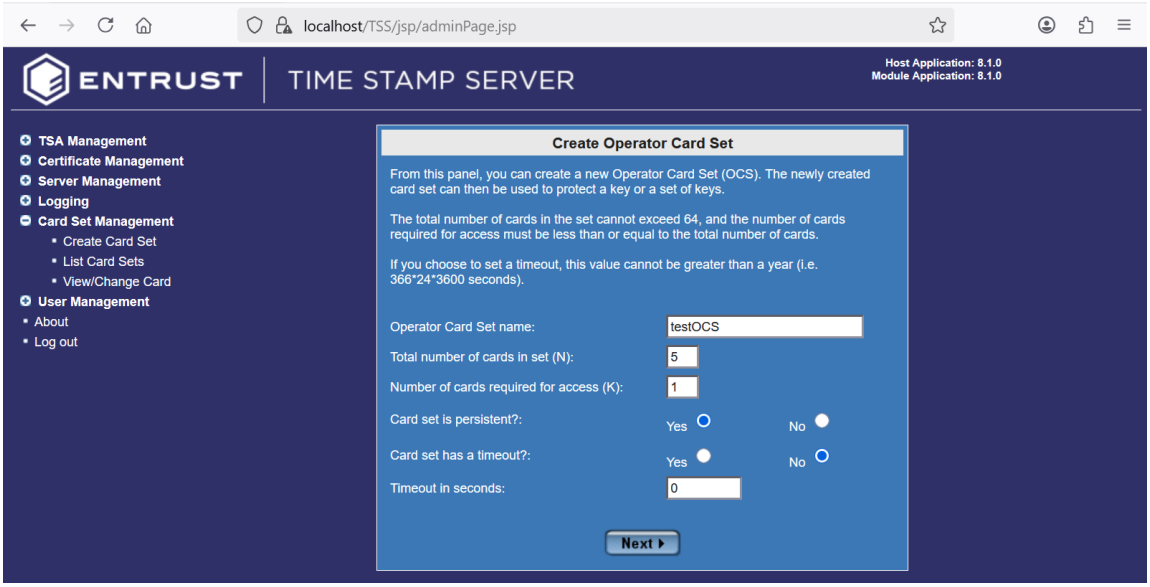
8. Select **TSA Management** → **Operation Status** to view the status of the newly created TSA.



3.3. Create the OCS

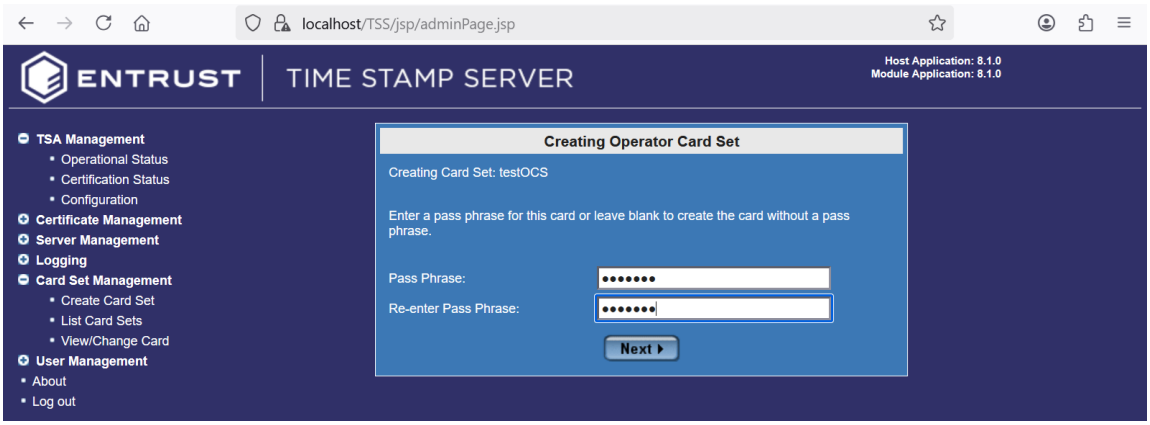
1. Login to the WEB GUI with the security officer credentials.
2. Navigate to **Card Set Management** > **Create Card Set**.
3. In the **Create Operator Card Set** pop-up window enter the information according to your organization security policy. Then select **Next**.

   For example:

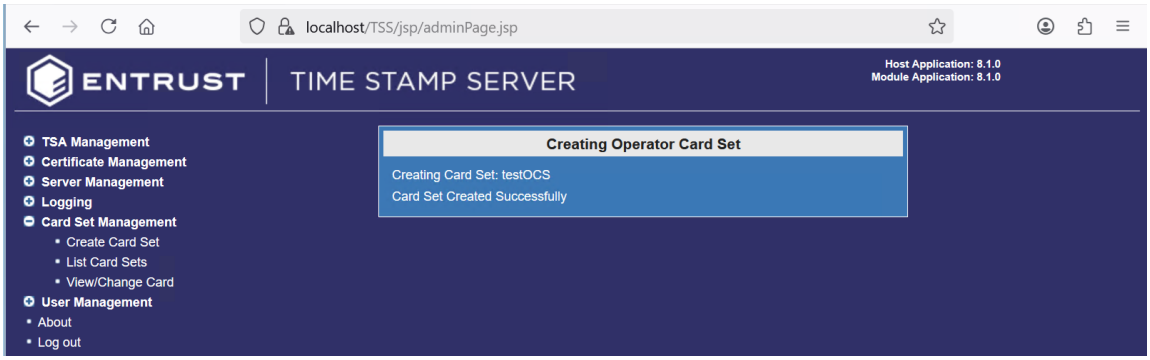


4. Present the ACS to the card reader when prompted.
5. Present each card in the OCS card set as instructed, and enter a passphrase. Then select **Next**.

   For example:



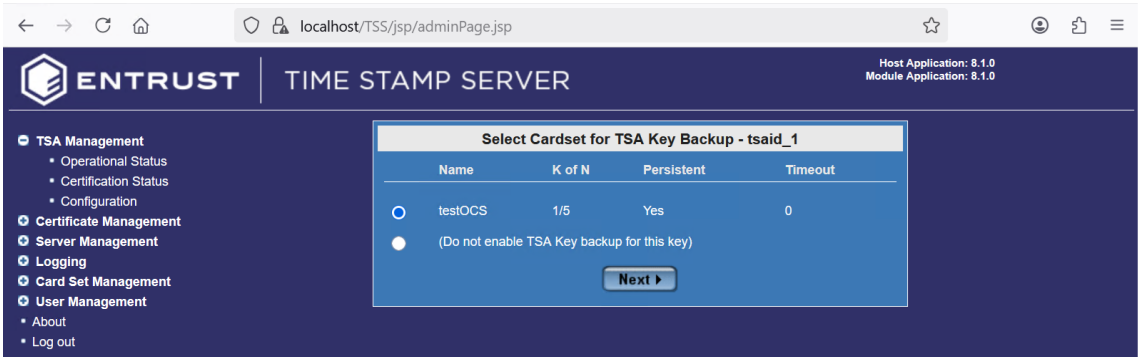
6. Notice a successful completion.



3.4. Create the TSA certificate request

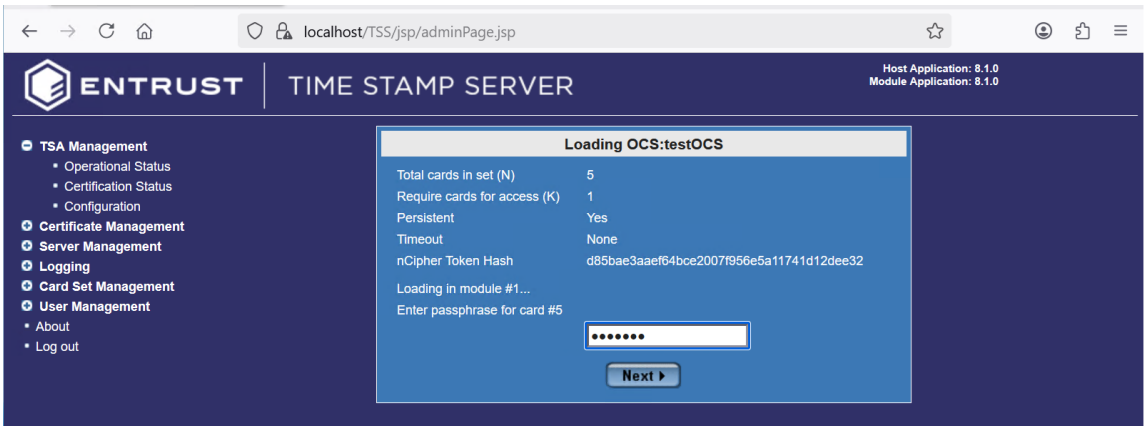
1. Login to the WEB GUI with the security officer credentials.
2. Present the OCS to the card reader, or remotely via the TVD. If using the TVD, do as indicated in Map dynamic slots to slot #0.
3. Navigate to **TSA Management** > **Certification Status**.
4. Select the TSA certificate request that you would like to fulfill. The select **Initiate**.
5. In the **Select Cardset for TSA Key Backup** dialog box, select the OCS. Then select **Next**.

   For example:



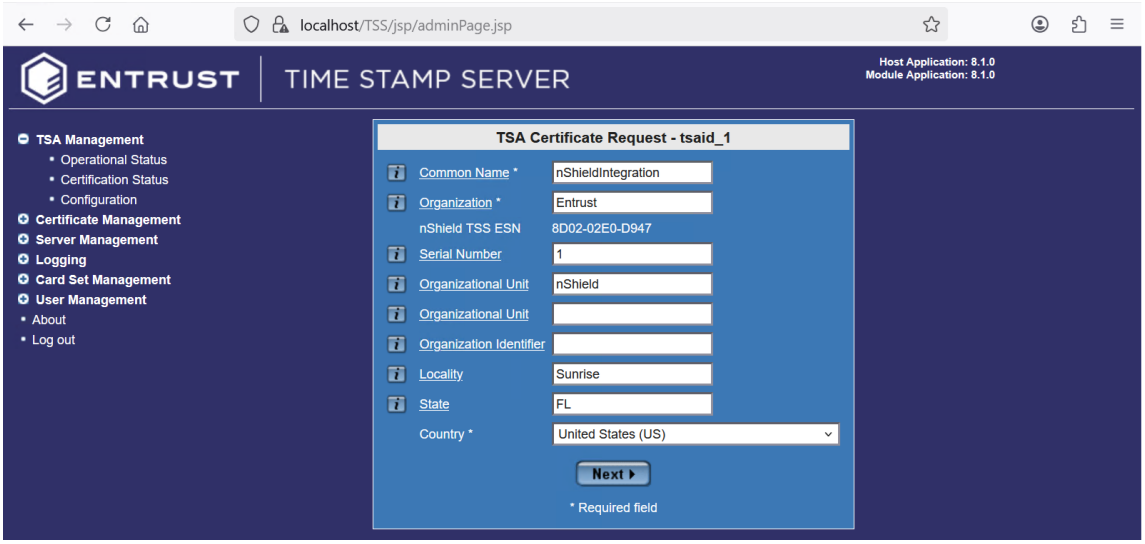
6. In the **Loading OCS:<ocs-name>** dialog box, enter the OCS passphrase. Then select **Next** twice.

   For example:



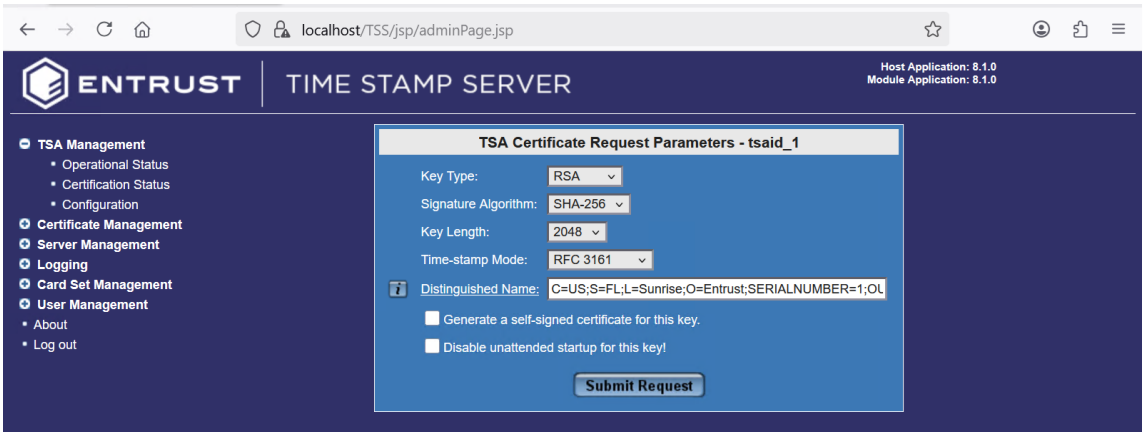
7. In the **TSA Certificate Request - tsaid_1**, enter your organization information. Then select **Next** and **OK**.

   For example:



8. In the **TSA Certificate Request Parameters - tsaid_1**, select the key parameters. Then select **Submit Request**.

   For example:



9. Per your browser, either select **Select All** and copy-paste to a file, or select **Download**.

   For example:

10. Send the TSA certificate request file to your CA for signature. In this example a local root CA was used. Signing was done using the Web Server template.

For additional info see section **Initiating a TSA certificate request** of TSOP v8.1.0 Install and User Guide.

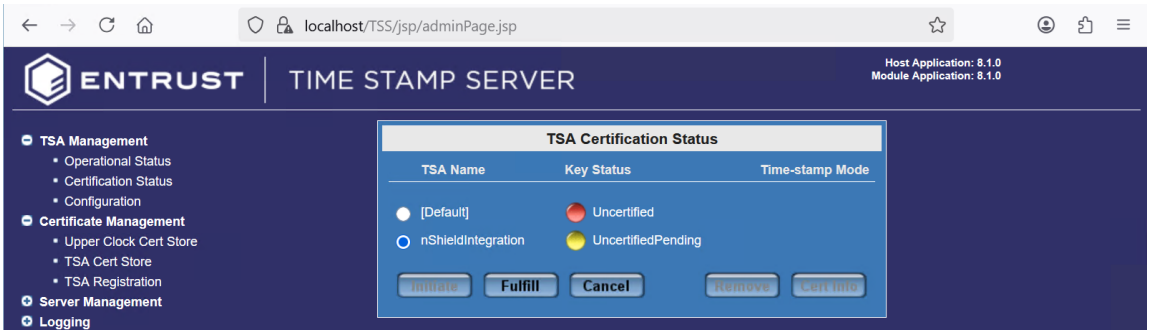
3.5. Import the certificate chain

Import the certificate chain as described in section **Importing the TSA certificate chain** of TSOP v8.1.0 Install and User Guide. Pay special attention to the order: root CA first, follow by the certificates signed by the root CA in the order in which they were signed.

3.6. Fulfill the TSA certificate request

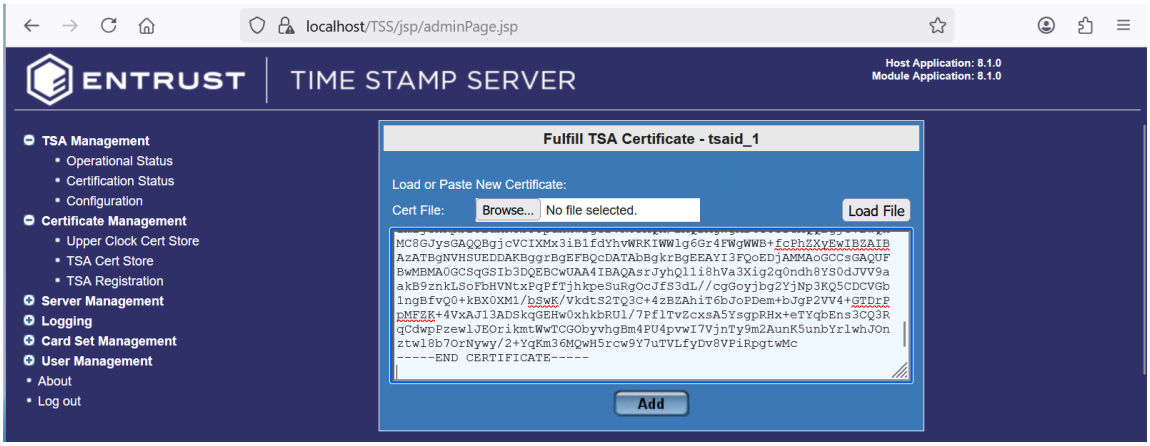
1. Login to the WEB GUI with the security officer credentials.
2. Present the OCS to the card reader, or remotely via the TVD. If using the TVD, do as indicated in Map dynamic slots to slot #0.
3. Navigate to **TSA Management** > **Certification Status**.
4. Select the TSA certificate request that you would like to fulfill. Then select **Fulfill**.

   For example:



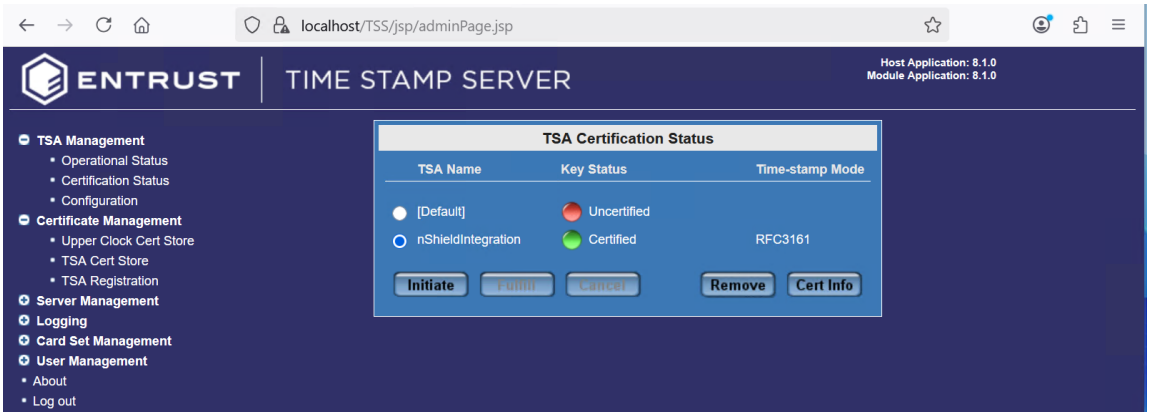
5. Copy-paste the signed certificate from your CA for the certificate request created in Create the TSA certificate request into the text box. Then select **Add**.

   For example:



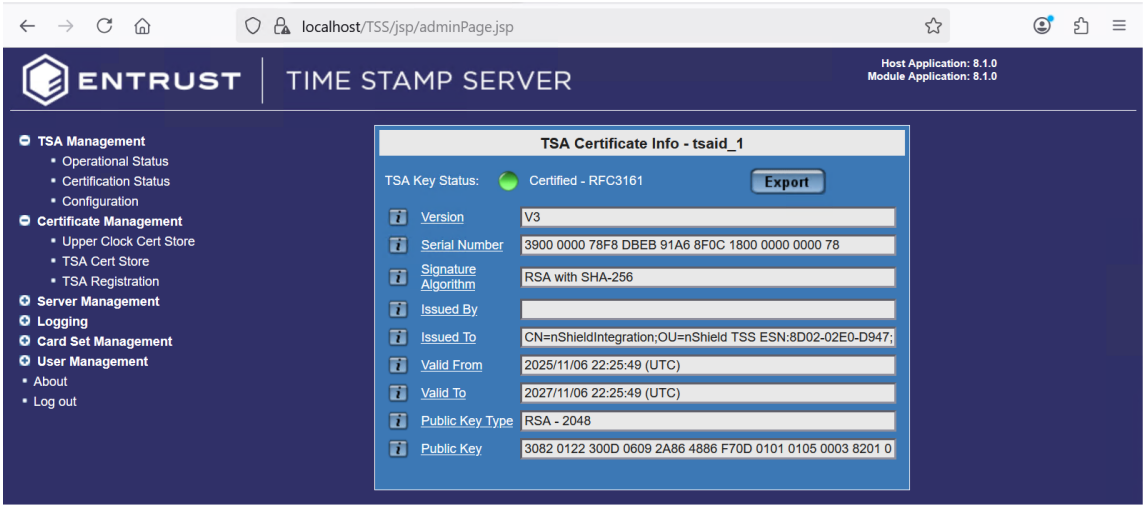
At the time of this integration testing, using the **Browse...** icon and selecting the certificate file was not working as expected.

6. Notice the successful installation. Then select **Cert Info**.



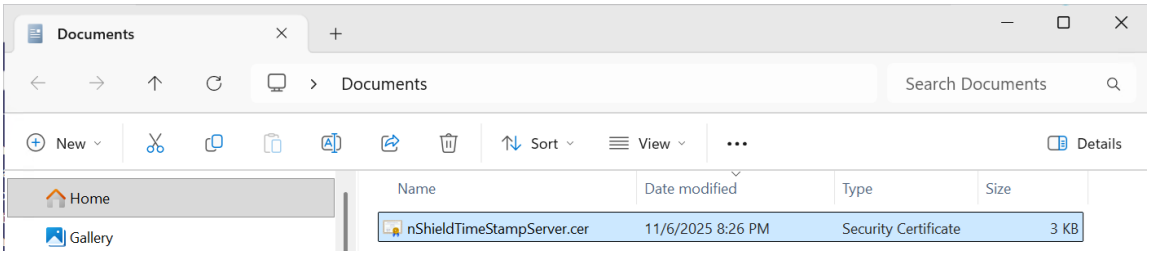
7. In the **TSA certificate info** dialog box, select **Export**.

   For example:



8. In the **Exported Certificate** dialog box, select **Select All** and **Copy**. Open a text editor and paste the certificate. Save this certificate, as it will be imported into each Microsoft 365 host requesting time stamping from this server.

   For example:



Chapter 4. Configure the Office 365 host

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

- Install the TSA certificate
- Edit the registry settings
- Make "Microsoft Office" configuration available in Group Policies

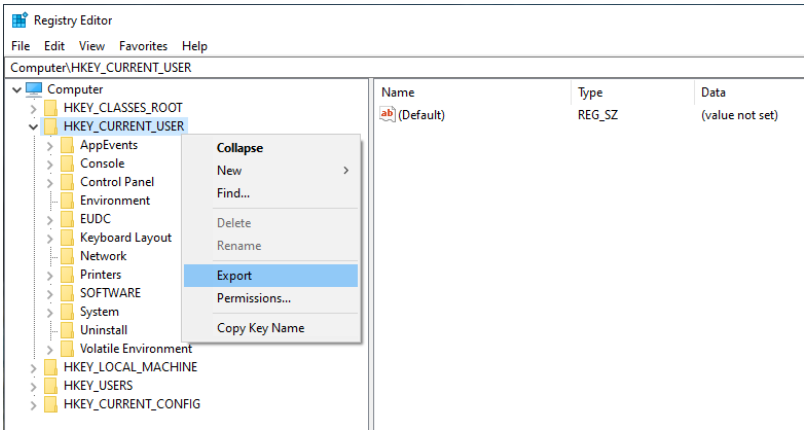
4.1. Install the TSA certificate

1. Log into the Office 365 host.
2. Copy the TSE certificate exported in Fulfill the TSA certificate request to a local folder. If you don't have the certificate, do as follows:
    1. Log into the TSS as the security officer (**superuser**).
    2. In the left pane, navigate to **TSA Management** > **Operational Status**.
    3. Select the **TSA Name**, then select **Cert Info**.
    4. Select the certificate and **Export** it to a `.cer` file.
3. In the Office 365 host, double-select the certificate. In the certificate dialog window select **Install Certificate...**.
4. In the **Certificate Import Wizard** dialog window, select **Local Machine**. Then select **Next**.
5. In the **Certificate Store** dialog window, select **Automatically select the certificate store...** radio button. Then select **Next** and **Finish**.
6. On the **Import was successful** pop-up, select **OK**.

4.2. Edit the registry settings

1. Log into the Office 365 host.
2. Enter **regedit** in the Windows search box and select **Registry Editor**.
3. In the left pane, navigate to **Computer** > **HKEY_CURRENT_USER**.
4. Export the **HKEY_CURRENT_USER** registry settings as a backup before you continue.

    For example:



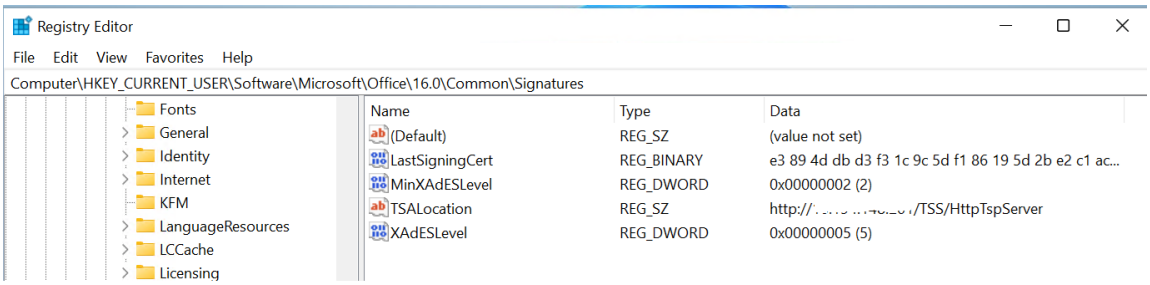
5. Navigate to the following registry path:
   `Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Signatures`.

   If the registry path does not already exist, create it.

6. Add the following entries.

Name	Type	Data
MinXAdESLevel	REG_DWORD (32-bit)	2
TSALocation	String Value	http://<TSS_IP_address>/TSS/HttpTspServer
XAdESLevel	REG_DWORD (32-bit)	5

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

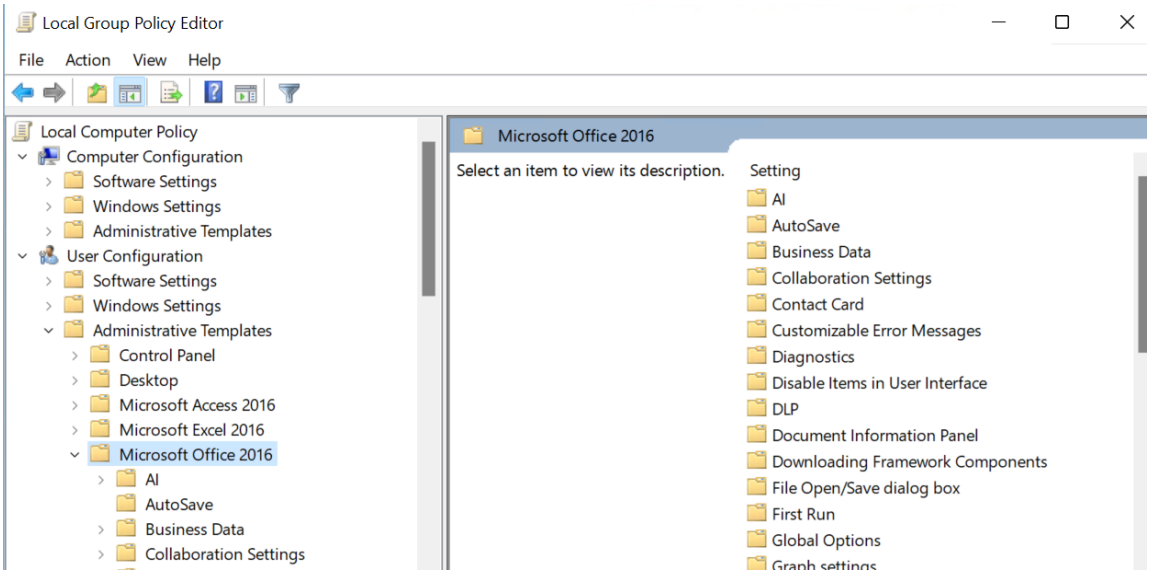


7. Close the registry editor.

4.3. Make "Microsoft Office" configuration available in Group Policies

1. Download the administrative template files (ADMX/ADML) for Microsoft Office. Be sure to select your language. For example, the English version is available at Administrative Template files (ADMX/ADML) for Microsoft Office.
2. Double-select the downloaded file to extract the `admx` and `adml` folders locally.
3. Open the `admx` folder. Copy all the `*.admx` files to `C:\Windows\PolicyDefinitions\.`.
4. In the `admx` folder, select the folder corresponding to your region. For example `en-us`. Copy all the `*.adml` files to `C:\Windows\PolicyDefinitions\<your-region>\.`. For example `C:\Windows\PolicyDefinitions\en-US\.`.
5. Enter **group policy** in the Windows search box and select **Edit group policy**.
6. Navigate to **User Configuration → Administrative Templates → Microsoft Office 2016** The settings for Microsoft Office should now appear.

   For example:



7. Navigate further to **Security Settings → Digital Signatures**. Edit the following policies as shown below.

Name	Value
Specify timestamp server name	http://<TSS_IP_address>/TSS/HttpTspServer
Requested XAdES level for signature generation	XAdES-X-L

Name	Value
Specify Minimum XAdES level for digital signature generation	XAdES-T

8. Close the group policy editor window.
9. Upgrade the group policy.

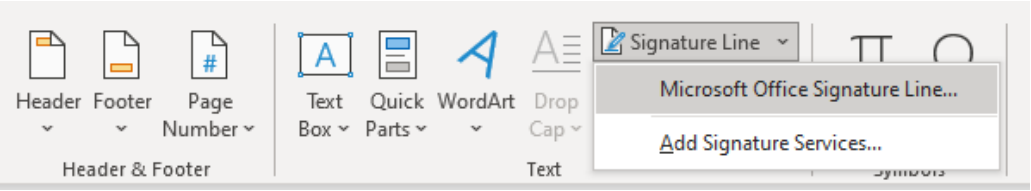
```
>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Chapter 5. Test the integration

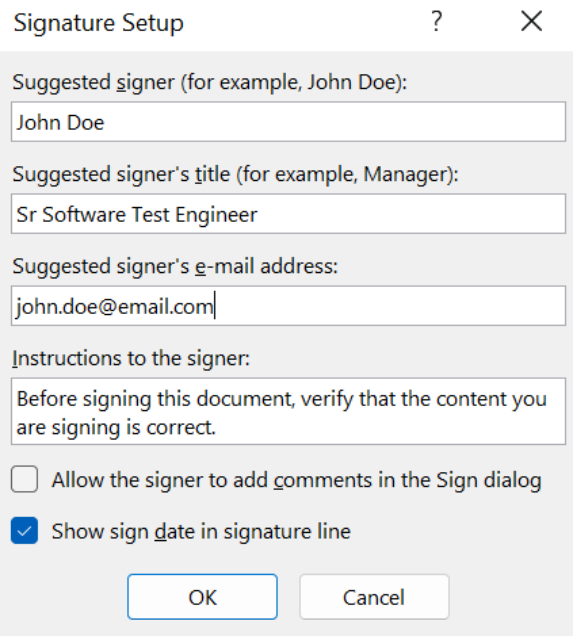
5.1. Add a signature line to a document

1. Open a Microsoft 365 Word document or create one.
2. Select 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. Select the arrow next to **Signature Line**, and then select **Microsoft Office Signature Line**. For example:



5. The **Signature Setup** dialog appears. Enter your information.

   For example:



6. Select **OK**.

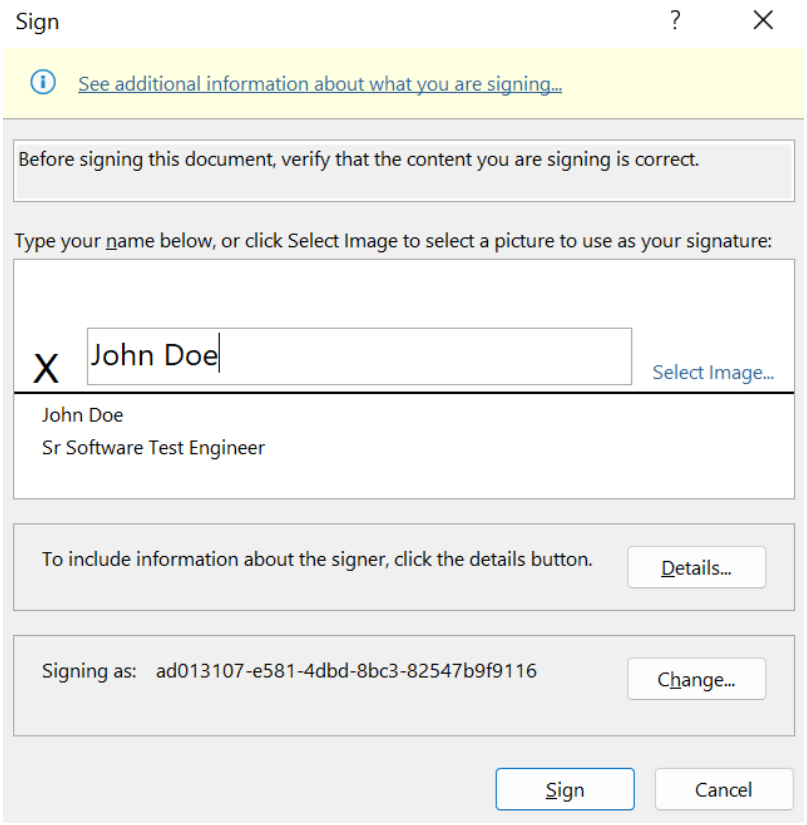
5.2. Sign the signature line

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

time stamp information.

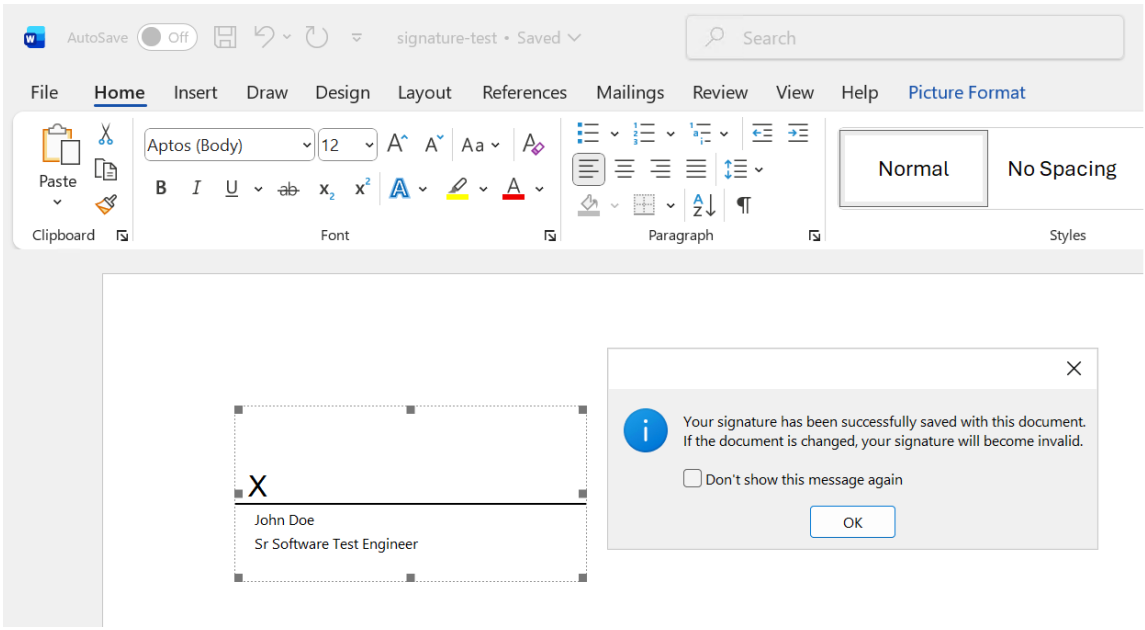
1. Open the document above.
2. Double-select the signature line where a signature is requested.
3. In the **Sign** dialog window, add the required information. Then select **Sign**.

   For example:



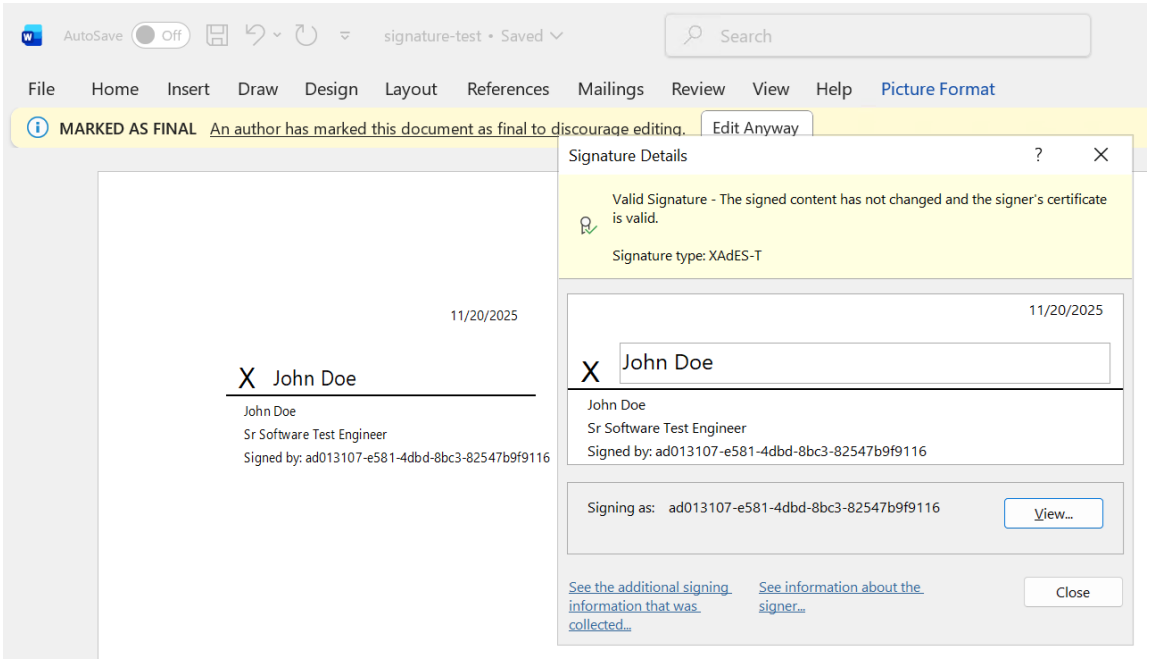
4. The document is signed.

   For example:



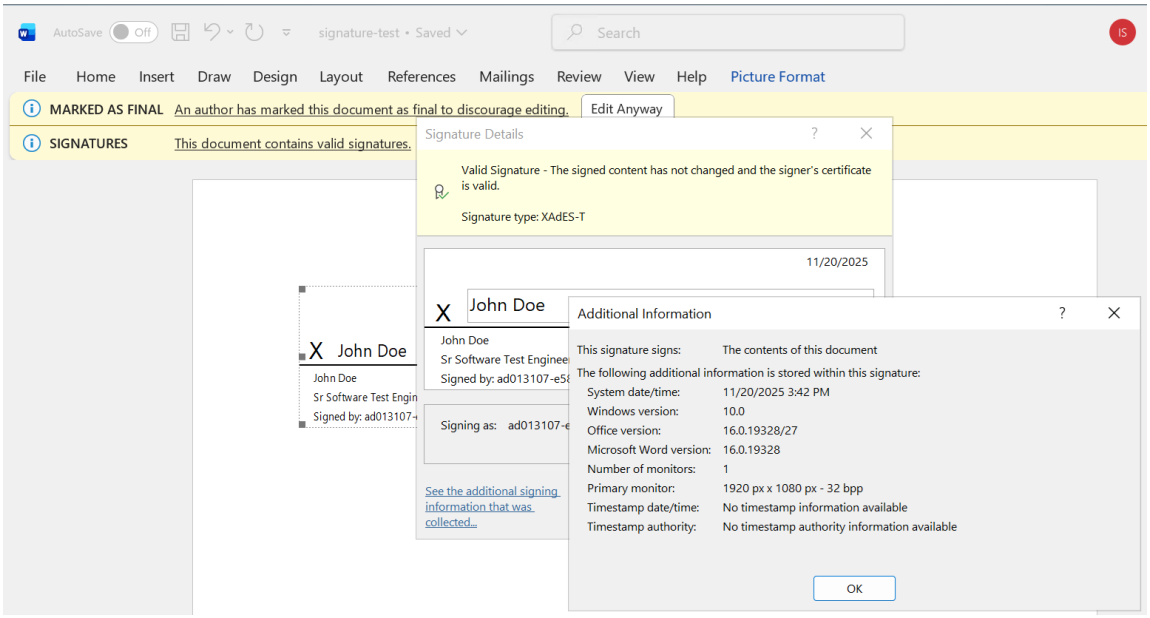
5. Select the signature in the document to confirm it is valid. The signature type should be **XAdES-T**.

   For example:



6. Select **See additional signing information that was collected...** to view the time stamp information.

   For example:


AutoSave
Off
signature-test • Saved
Search
File
Home
Insert
Draw
Design
Layout
References
Mailings
Review
View
Help
Picture Format
MARKED AS FINAL
An author has marked this document as final to discourage editing.
Edit Anyway
SIGNATURES
This document contains valid signatures.
Signature Details
Valid Signature - The signed content has not changed and the signer's certificate is valid.
Signature type: XAdES-T
11/20/2025
X John Doe
John Doe
Sr Software Test Engine
Signed by: ad013107-e5
Signing as: ad013107-
See the additional signing information that was collected...
Additional Information
This signature signs: The contents of this document
The following additional information is stored within this signature:
System date/time: 11/20/2025 3:42 PM
Windows version: 10.0
Office version: 16.0.19328/27
Microsoft Word version: 16.0.19328
Number of monitors: 1
Primary monitor: 1920 px x 1080 px - 32 bpp
Timestamp date/time: No timestamp information available
Timestamp authority: No timestamp authority information available
OK

Chapter 6. Troubleshooting

The following table provides troubleshooting guidelines.

Problem	Cause	Resolution
When attempting to sign a document, the following error appears: The **Get a Digital ID** dialog appears instead of the **Sign** window. or "Signing cannot be completed due to problems applying the required timestamp. Check your network connection".	Registry or group policy settings not set correctly.	Set these and attempt to re-sign the document.

Chapter 7. Additional resources and related products

7.1. nShield Connect

7.2. nShield as a Service

7.3. Entrust products

7.4. nShield product documentation