
Microsoft Active Directory Federation Services: Integration Guide

THALES LUNA HSM AND DPOD LUNA CLOUD HSM

Document Information

Document Part Number	007-012087-001
Revision	F
Release Date	13 April 2021

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Understanding Active Directory Federation Services	4
Certified platforms	5
Certified platforms for Luna HSM	5
Certified platforms for Luna Cloud HSM	5
Prerequisites	5
Configure Luna HSM	6
Configure Luna Cloud HSM service	7
Set up Microsoft ADFS	10
Configuring Active Directory Certificate Services with Luna HSM	10
Configure SafeNet Key Storage Provider (KSP)	10
Install Microsoft ADCS using SafeNet KSP	11
Configure the CA to issue ADFS Web Server Certificates	12
Register CSP	14
Generate token signing/decrypting certificate using Luna CSP	14
Install ADFS	15
Create and configure a server authentication certificate in IIS	15
Configure the system as a federation server	16
Install the token signing/decrypting certificate generated by Luna CSP	19
Verify that Federation Server is Operational	20
Setting up two instances of ADFS sharing same keys on HSM	22
Microsoft ADFS setup	22
Luna HSM setup	22
Integrating Luna HSM with two instances of Active Directory Federation Services	22
Contacting customer support	27
Customer support portal	27
Telephone support	27
Email support	27

Overview

This document is intended to guide security administrators through the steps for integrating Microsoft Active Directory Federation Services (ADFS) with Thales Luna HSM devices or DPoD Luna Cloud HSM services. This integration provides significant performance improvements by off-loading cryptographic operations from the ADFS Server to the Luna HSM. In addition, Luna HSM provides extra security by protecting and managing the server's high value SSL private key within a FIPS 140-2 certified hardware security module. The benefits of integrating Microsoft ADFS with Luna HSM devices or Luna Cloud HSM services include:

- > Secure generation, storage and protection of the signing private key on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of the keys.
- > Access to the HSM audit trail*.
- > The advantage of cloud services with confidence.

*Luna Cloud HSM services do not have access to the secure audit trail.

Understanding Active Directory Federation Services

Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity. Claims based authentication is the process of authenticating a user based on a set of claims about its identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims based authentication.

In ADFS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

Certified platforms

- > [Certified platforms for Luna HSM](#)
- > [Certified platforms for Luna Cloud HSM](#)

Certified platforms for Luna HSM

This integration is certified for Luna HSM on the following platforms:

HSM Type	Platform Certified
Luna HSM	Windows Server 2019

NOTE: Microsoft ADFS Integration is tested in both HA and FIPS mode.

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

Certified platforms for Luna Cloud HSM

This integration is certified for Luna Cloud HSM on the following platforms:

HSM Type	Platforms Certified
Luna Cloud HSM	Windows Server 2019

Luna Cloud HSM: Luna Cloud HSM services provide on-demand HSM and Key Management services through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective and easy to manage because there is no hardware to buy, deploy and maintain. As an Application Owner, you click and deploy services, generate usage reports, and maintain specific services that you need.

NOTE: For support with earlier versions of Luna HSM and Microsoft ADFS, refer to earlier version of this guide (007-012087-001_Microsoft ADFS_Integration Guide_Rev.

Prerequisites

Before you proceed with the integration, complete the following tasks:

- > [Configure Luna HSM](#)
- > [Configure Luna Cloud HSM service](#)
- > [Set up Microsoft ADFS](#)

Configure Luna HSM

If you are using Luna HSM:

1. Verify the HSM is set up, initialized, provisioned and ready for deployment. Refer to the [Luna HSM documentation](#) for more information.
2. Create a partition that will be later used by MS ADFS.
3. If using a Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize the Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
Available HSMs:
Slot Id ->                0
Label ->                  ADFS
Serial Number ->          1213475834492
Model ->                  LunaSA 7.3.0
Firmware Version ->      7.3.0
Configuration ->         Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description ->       Net Token Slot
```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

NOTE: Refer to the [Luna HSM documentation](#) for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

NOTE: For PED-based Luna HSM, ensure that ProtectedAuthenticationPathFlagStatus is set to '1' in the Misc Section of Chrystoki.conf file.

Set up Luna HSM High-Availability

Refer to the [Luna HSM documentation](#) for HA steps and details regarding configuring and setting up two or more HSM boxes on host systems. You must enable the HAOnly setting in HA for failover to work so that if the primary goes down due to any reason all calls automatically route to the secondary until the primary recovers and starts up.

Set up Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
[Misc]
```

```
RSASKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

NOTE: The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Configure Luna Cloud HSM service

You can configure Luna Cloud HSM Service in the following ways:

- > [Standalone Cloud HSM service using minimum client package](#)
- > [Standalone Cloud HSM service using full Luna client package](#)
- > [Luna HSM and Luna Cloud HSM service in hybrid mode](#)

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

Standalone Cloud HSM service using minimum client package

To configure Luna Cloud HSM service using minimum client package:

1. Transfer the downloaded .zip file to your Client workstation using [pscp](#), scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

[Windows]

```
cvclient-min.zip
```

[Linux]

```
cvclient-min.tar
```

```
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

[Windows]

```
Right-click setenv.cmd and select Run as Administrator.
```

[Linux]

```
Source the setenv script.
```

```
# source ./setenv
```

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

Standalone Cloud HSM service using full Luna client package

To configure Luna Cloud HSM service using full Luna client package:

1. Transfer the downloaded .zip file to your Client workstation using [pscp](#), scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.

3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

[Windows]

cvclient-min.zip

[Linux]

cvclient-min.tar

```
# tar -xvf cvclient-min.tar
```

4. Run the setenv script to create a new configuration file containing information required by the Luna Cloud HSM service.

[Windows]

Right-click setenv.cmd and select Run as Administrator.

[Linux]

Source the setenv script.

```
# source ./setenv
```

5. Copy the server and partition certificates from the Cloud HSM service client directory to Luna client certificates directory:

Cloud HSM Certificates:

server-certificate.pem

partition-ca-certificate.pem

partition-certificate.pem

LunaClient Certificate Directory:

[Windows default location for Luna Client]

C:\Program Files\Safenet\Lunaclient\cert\

[Linux default location for Luna Client]

/usr/safenet/lunaclient/cert/

NOTE: Skip this step for Luna Client v10.2 or higher.

6. Open the configuration file from the Cloud HSM service client directory and copy the XTC and REST section.

[Windows]

crystoki.ini

[Linux]

Chrystoki.conf

7. Edit the Luna Client configuration file and add the XTC and REST sections copied from Cloud HSM service client configuration file.

8. Change server and partition certificates path from step 5 in XTC and REST sections. Do not change any other entries provided in these sections.

[XTC]


```

. . .
PartitionCAPath=<LunaClient_cert_directory>\partition-ca-certificate.pem
PartitionCertPath00=<LunaClient_cert_directory>\partition-certificate.pem
. . .

[REST]
. . .
SSLClientSideVerifyFile=<LunaClient_cert_directory>\server-certificate.pem
. . .

```

NOTE: Skip this step for Luna Client v10.2 or higher.

9. Edit the following entry from the Misc section and update the correct path for the plugins directory:

```

Misc]
PluginModuleDir=<LunaClient_plugins_directory>
[Windows Default]
C:\Program Files\Safenet\Lunaclient\plugins\
[Linux Default]
/usr/safenet/lunaclient/plugins/

```

Save the configuration file. If you wish, you can now safely delete the extracted Cloud HSM service client directory.

10. Reset the ChrystokiConfigurationPath environment variable and point back to the location of the Luna Client configuration file.

Windows

In the Control Panel, search for "environment" and select Edit the system environment variables. Click Environment Variables. In both list boxes for the current user and system variables, edit ChrystokiConfigurationPath and point to the crystoki.ini file in the Luna client install directory.

Linux

Either open a new shell session, or export the environment variable for the current session pointing to the location of the Chrystoki.conf file:

```
# export ChrystokiConfigurationPath=/etc/
```

11. Run the LunaCM utility and verify that the Cloud HSM service is listed. In hybrid mode, both Luna and Cloud HSM service will be listed.

NOTE: Follow the [Luna Cloud HSM documentation](#) for detailed steps for creating service, client, and initializing various user roles.

Luna HSM and Luna Cloud HSM service in hybrid mode

To configure Luna HSM and Luna Cloud HSM service in hybrid mode, follow the steps mentioned under the [Standalone Cloud HSM service using full Luna client package](#) section above.

NOTE: Luna Client v10.x or higher is required for configuring Luna HSM device and Luna Cloud HSM service in hybrid mode.

To use Luna Cloud HSM Service in FIPS mode

Cloud HSM service operates in both FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, enable the Allow non-FIPS approved algorithms check box when

configuring your Cloud HSM service. The FIPS mode is enabled by default. Refer to the Mechanism List in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Set up Microsoft ADFS

Install Microsoft ADFS on the target machine using the following setup:

- > Windows Server, which will become a Domain Controller and Certificate Authority.
- > Windows Server, which will become Federation Server and Web Server.
- > Domain Administrator privileges.

The machines utilized in the setup are denoted as follows:

- **ADFSCA**: Domain Controller and CA machine.
- **ADFSWEB**: ADFS and Web Server machine.

Configuring Active Directory Certificate Services with Luna HSM

The key steps involved in integrating Microsoft ADFS with Luna HSM or Luna Cloud HSM are as follows:

- > [Configure the SafeNet Key Storage Provider \(KSP\)](#)
- > [Install ADCS using SafeNet KSP](#)
- > [Configure the CA to issue ADFS Web Server Certificates](#)
- > [Register CSP](#)
- > [Generate Token Signing/Decrypting Certificate using Luna CSP to use with ADFS](#)
- > [Install ADFS](#)
- > [Create and configure a server authentication certificate in IIS](#)
- > [Configure the system as a federation server](#)
- > [Install the token signing/decrypting certificate generated by Luna CSP](#)
- > [Verify that Federation Server is operational](#)

Configure SafeNet Key Storage Provider (KSP)

You must configure SafeNet Key Storage Provider (KSP) to allow the user account and system to access the Luna HSM or Luna Cloud HSM service.

NOTE: If you are integrating a Luna HSM, the KSP package must be installed during the Luna Client software installation.

NOTE: If you are integrating Luna Cloud HSM service, the KSP package is included in the Cloud HSM service client package inside of the /KSP folder.

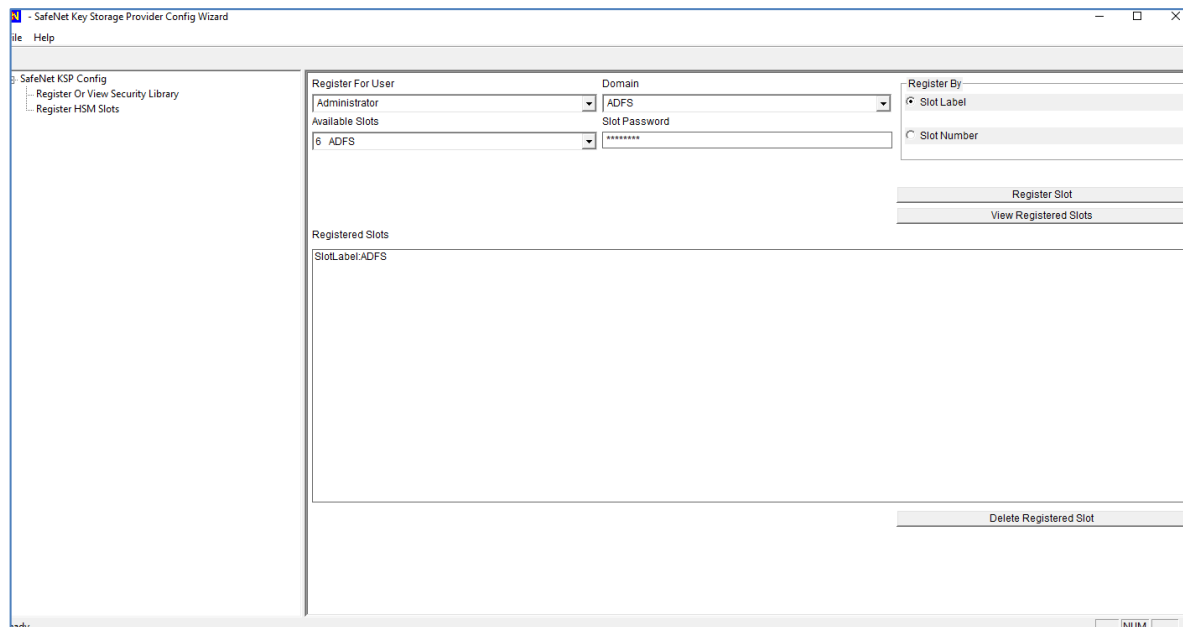
To configure SafeNet KSP:

1. Navigate to the <Luna HSM Client installation Directory>/KSP directory. If you are using Luna Cloud HSM service, the /KSP folder is available in the service client package.
2. Double-click the KspConfig.exe file to launch the KSP configuration wizard.
3. Double-click **Register or View Security Library** on the left side of the pane.
4. Click **Browse**, navigate to the Luna HSM Client installation directory, and select the cryptographic library file named cryptoki.dll. Click **Register**. If you are using Luna Cloud HSM service, the cryptographic libraries are available in the service client package.
5. On successful registration, the following message will appear on screen:

Success registering the security library!

6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the Slot (Partition) password.
8. Click **Register Slot** to register the slot for Domain\User. On successful registration, the following message will appear on screen:

The slot was successfully and securely registered!



9. Register the same slot for **NT_AUTHORITY\SYSTEM**.

Install Microsoft ADCS using SafeNet KSP

To install Microsoft ADCS:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Open Server Manager and click **Add Roles and Features**.
3. The **Add Roles wizard** will appear on your screen.
4. Click **Next**.
5. Select the Role-based or feature-based installation radio button and click Next.

6. Select the **Select a server from the server pool** radio button and select your server from the **Server Pool** menu.
7. Click **Next**. Select the Active Directory Certificate Services check box.
8. A window displays stating Add features that are required for Active Directory Certificate Services? To add a feature, click the Add Features button.
9. Click **Next** to continue.
10. On the Active Directory Certificate Services page click **Next** to continue.
11. Select the **Certification Authority** check box from the **Role services** list and click **Next**.
12. Click **Install**.
13. When installation is complete, click **Configure Active Directory Certificate Services on the destination server** and the AD CS Configuration wizard displays.
14. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.
15. Select the **Certification Authority** check box and click **Next**.
16. Select the **Enterprise CA** radio button and click **Next**.
17. Select the **Root CA radio button** and click **Next**.
18. Setup the Private Key for the CA to generate and issue certificates to clients. Select the **Create a new private key** radio button. Click **Next**.
19. Open the **Select a cryptographic provider:** drop-down menu and select an algorithm using a **SafeNet Key Storage Provider**. Open the **Key length:** drop-down menu and select a key-length.
20. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.
21. Select the Allow administrator interaction when the private key is accessed by the CA check box.
22. Click **Next**.
23. Configure a common name to identify this Certificate Authority. Click **Next**.
24. Proceed to set the **Certificate Validity Period**. Click **Next**. Configure the **Certificate database location**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next**.
25. Click **Configure** to configure the selected roles, role services, or features.
26. Click **Close** to exit the **AD CS Configuration** wizard after viewing the installation results.

A private key for the CA will be generated and stored on the HSM.
27. Open a command prompt and run the following command to verify that service is running:

```
sc query certsvc
```
28. Open a command prompt and run the following command to verify the CA key:

```
certutil -verifykeys
```

The result of the command shows the CA keys have successfully been verified.

Configure the CA to issue ADFS Web Server Certificates

Follow the steps below to configure a CA to create a certificate template and issuing properties for ADFS server certificate.

Configuring certificate templates for your test environment

1. Log in to ADFSCA as a domain administrator.
2. From the **Start** menu, select **Run**. The **Run** dialog box will appear on your screen.
3. Type `mmc` and click **OK**.
4. The MMC console displays. In this console, select **File > Add/Remove Snap-in...**
5. In the **Add or Remove Snap-Ins** dialog box, select the **Certificates Templates** snap-in under the Available snap-ins menu.
6. Click **Add**, and then click **OK**.
7. Under Console Root, expand the **Certificate Templates** snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.
8. Scroll down to the **Web Server** template, right-click the same and click **Duplicate Template**.
9. Select **Windows Server 2003 Enterprise** and click **OK**.
10. A pop-up dialog box displays. Click the **General** tab.
11. Enter the **Template Display Name**, such as ADFS.
12. Click the **Request Handling** tab.
13. Click on CSPs and select "Request can use any CSP available on subject's computer" option.
14. Click **OK** to close the window.
15. Click the **Security** tab and click **Add**.
16. Type **NETWORK SERVICE** and click **OK**.
17. Click **NETWORK SERVICE** in the Group or user names area.
18. In the **Permissions** area, ensure that the **Read** and **Enroll** check boxes are selected.
19. Add and provide Read and Enroll permissions to the following members:
 - Domain Computers
 - Domain Controllers
 - NETWORK SERVICE
 - IIS_IUSRS
20. For **Domain Admins** and **Enterprise Admins**, ensure that the **Read**, **Write**, and **Enroll** check boxes are selected.
21. Click **Apply** and then click **OK**.

Configuring the CA to support the ADFS certificate template

1. Log on to ADFSCA as a domain administrator.
2. From the Start menu, select Control Panel > Administrative Tools > Certification Authority.
3. In the console tree, expand the CA (It has a computer icon and a green tick next to it).
4. In console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.

5. In **Enable Certificates Templates**, select the **ADFS** template and any other certificate templates you configured previously, and then click **OK**.
6. Open **Certificate Templates** in the **Certification Authority** and verify that the modified certificate templates appear in the list.

Register CSP

To set up Luna HSM for Active Directory Federation Services:

1. Register CSP on ADFSWEB.
2. Open the command prompt and navigate to <Luna Client installation directory>\CSP.
3. Run the **register.exe** and provide the Luna HSM partition password to register the partition with CSP.
4. Execute the following command:

```
<Luna Client installation directory>\CSP >register.exe /l
```

Generate token signing/decrypting certificate using Luna CSP

1. Log on to ADFSWEB as a domain administrator.
2. From the **Start** menu, select **Run**.
3. In the **Run** dialog box, type **mmc** and click **OK**.
4. The **mmc** console appears on the screen. Select **File > Add/Remove Snap-in...**
5. In the **Add or Remove Snap-Ins** dialog box, select the **Certificates** snap-in (under the Available snap-ins section).
6. Click **Add**, select **Computer Account** and Click **Next**.
7. Select **Local Computer**, and click **Finish**.
8. Click **OK** and expand the **Certificates** under **Console Root**.
9. Right-click the **Personal** folder and select **All Tasks -> Request New Certificate...**
10. Click **Next**, Select **Active Directory Enrollment Policy**, and then click **Next**. The certificate template that you've configured will be displayed.
11. Click on configure settings link.
12. The **Certificate Properties** window appears on the screen. Select the **Subject** tab.
13. Select **Common Name** under **Subject Name** and provide the fully qualified domain name for the computer on which you are installing the certificate in the **Value** field and click **Add**. Repeat the same step for adding more values.
14. Click the **General** tab and provide the **Friendly Name**. For example: ADFS Token Signing.
15. Click the **Private Key** tab, and verify that **Luna enhanced RSA and AES provider for Microsoft Windows** must be selected under the **Cryptographic Service Provider**.
16. Click the **Certificate Authority** tab, and ensure that **Enterprise Root CA** is selected.
17. Click **Apply** and then **OK**.
18. Select ADFS certificate template or the certificate template you have configured, and click **Enroll**.
19. It will take some time to enroll, when enrollment succeeded, click **Finish**.

Setting permission for Private Key of the Certificate

1. Open the certificate snap under the **console root, Certificates** (Local Computer) > **Personal** > **Certificate**.
2. Right-click the certificate generated by Luna CSP and select **All Tasks > Manage Private Keys**.
3. Click **Add** and type the name of the gMSA account you want to use with ADFS in the Enter the object name to select text box.
4. Click **OK**. Ensure that it is added in the **Group or User Name** list.
5. Select the account and select the **Full Permission** check box.
6. Click **Apply** and then **OK** to close the window.

Install ADFS

1. Log in to ADFSWEB as a domain administrator.
2. Open **Server Manager**. In the **Quick Start** tab of the Welcome tile on the Dashboard page, click **Add roles and features**. Alternatively, you can click **Add Roles and Features** on the **Manage** menu.
3. On the **Before you begin** page, click **Next**.
4. On the Select installation type page, click **Role-based or Feature-based installation**, and then click **Next**.
5. On the **Select destination server** page, click Select a server from the server pool, verify that the target computer is selected, and then click **Next**.
6. On the Select server roles page, click **Active Directory Federation Services**, and then click **Next**.
7. On the **Select features** page, click **Next**. The required prerequisites are preselected for you. You do not have to select any other features.
8. On the Active Directory Federation Service (ADFS) page, click **Next**.
9. After you verify the information on the Confirm installation selections page, click **Install**.
10. On the Installation progress page, verify that everything is installed correctly and then click **Close**.

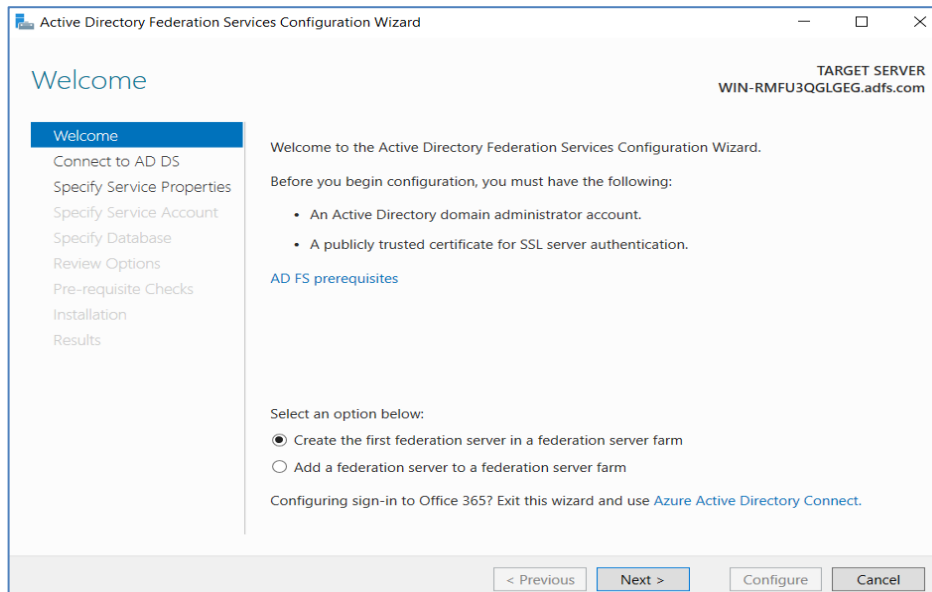
Create and configure a server authentication certificate in IIS

1. Log in to ADFSWEB as a domain administrator.
2. From the Start menu, select **All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
3. In the console tree, click the root node that contains the name of the computer, and then, in the details pane, double-click the icon named **Server Certificates** in the **IIS** grouping.
4. In the Actions pane, click **Create Certificate Request**.
5. Enter the details in the **Create Certificate** window.
6. **Common Name** must be fully qualified domain name.
7. After providing all the details, Click **Next**.
8. Select **Microsoft RSA SChannel Cryptographic Provider** and **2048** as Bit Length.
9. Click **Next**, select the location to save the certificate request as C:\request.txt.

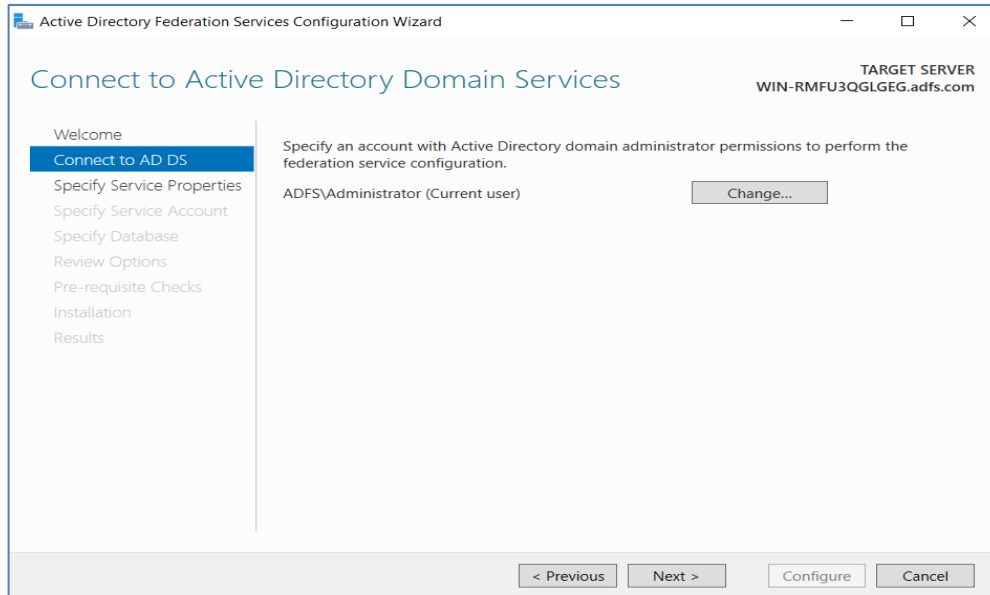
10. Click **Finish**, it will generate the certificate request. Submit certificate request to CA and save the signed certificate.
11. In the IIS Action pane, click **Complete Certificate Request**.
12. Browse and select the CA signed certificate and enter the **Friendly Name** as ADFS Server Certificate.
13. Click **OK** to complete the certificate request and close the window.
14. In the console tree, click the root node that contains the name of the computer and then click **Default website**.
15. In the **Actions** pane, click **Bindings**.
16. In the **Site Bindings** dialog box, click **Add**.
17. In the **Add Site Binding** dialog box, select **https** in the **Type** drop-down list and the certificate that you have generated through IIS in the SSL certificate drop-down list.
18. Click **OK**, and then click **Close**.
19. Close the Internet Information Services (IIS) Manager console.

Configure the system as a federation server

1. Log on to ADFSWEB as a domain administrator.
2. Open the Server Manager.
3. On the Dashboard page, click the Notifications flag, and then click **Configure the federation service on the server**.
4. The Active Directory Federation Service Configuration Wizard opens.
5. On the Welcome page, click **Create a new Federation Service**, and then click **Next**.

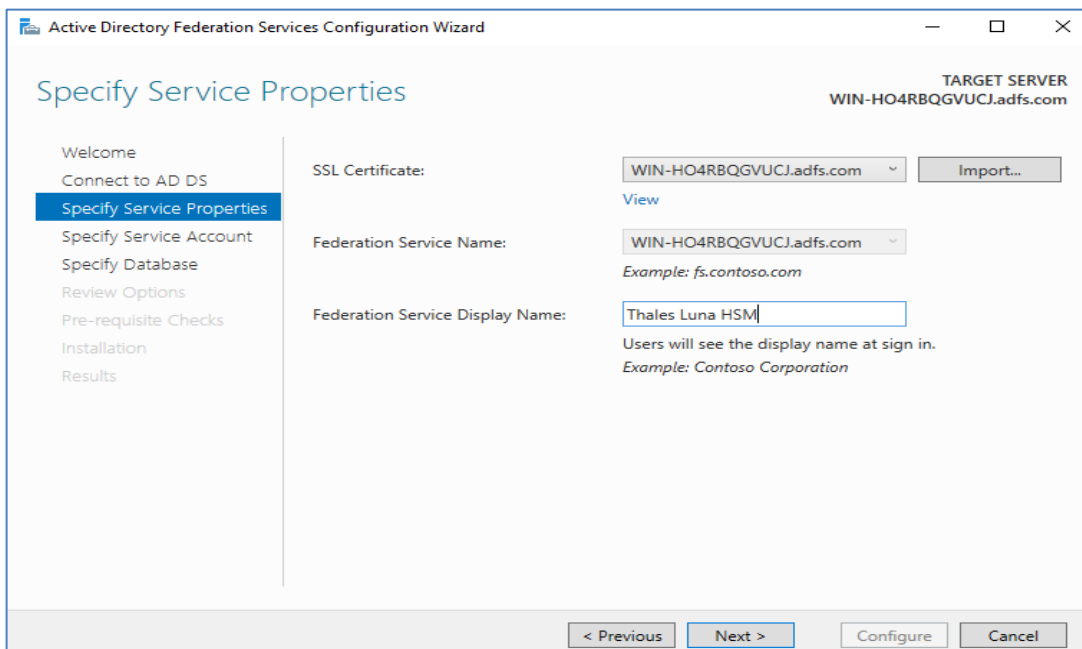


6. On the **Connect to AD DS** page, specify an account by using domain administrator permissions for the Active Directory (AD) domain to which this computer is joined, and then click **Next**.

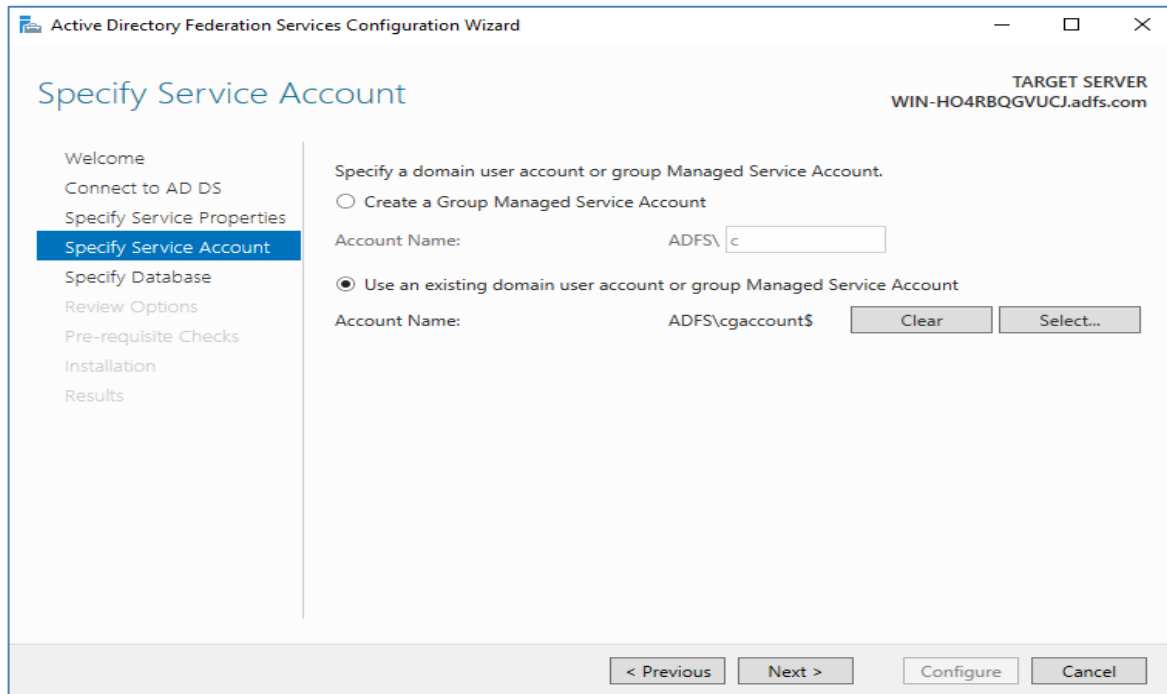


7. On the **Specify Service Properties** page:

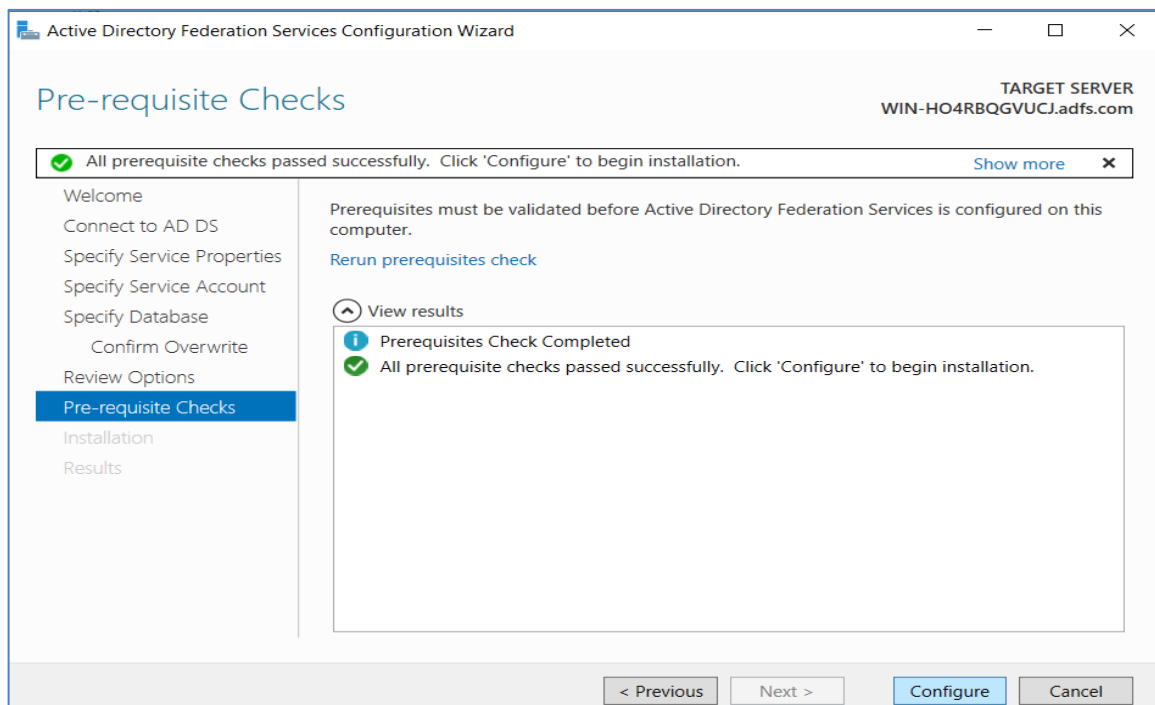
- i. Select the certificate that you have configured and bind in the IIS.
- ii. Provide a name for your federation service. For example, fsweb.contoso.com. This name must match one of the subject or subject alternative names in the certificate.
- iii. Provide a display name for your federation service. Users will see this name on the Active Directory Federation Services (AD FS) sign-in page.
- iv. Click **Next**.



- On the **Specify Service Account** page, select the option to use an existing gMSA or domain account.



- On the **Specify Configuration Database** page, specify an ADFS configuration database, and then click **Next**. You can select **create a database on this computer by using Windows Internal Database (WID)**, or you can specify the location and the instance name of Microsoft SQL Server.
- On the **Review Options** page, verify your configuration selections, and then click **Next**.
- On the **Pre-requisite Checks** page, verify that all prerequisite checks are successfully completed and then click **Configure**.



12. On the **Results** page, check whether the configuration has been completed successfully, and then click **Next** steps required for completing your federation service deployment. Click **Close** to close the configuration wizard.

Configure Corporate DNS for the Federation Service and DRS

1. On your domain controller, log in as domain administrator.
2. In **Server Manager**, on the **Tools** menu, click **DNS** to open the DNS snap-in.
3. In the console tree, expand the `domain_controller_name` node, expand **Forward Lookup Zones**, right-click `domain_name`, and then click **New Host (A or AAAA)**.
4. In the **Name** box, type the name to use for your ADFS farm. i.e. ADFSWEB
5. In the **IP address** box, type the IP address of your federation server. Click **Add Host**.
6. Right-click the `domain_name` node, and then click **New Alias (CNAME)**.
7. In the **New Resource Record** dialog box, type enterprise registration in the Alias name box.
8. In the fully qualified domain name (FQDN) of the target host box, type `federation_service_farm_name.domain_name.com`, i.e. ADFSWEB.contoso.com and then click **OK**.
9. Open the command prompt and then run `ipconfig /flushdns` on domain controller and also the ADFS server.

Install the token signing/decrypting certificate generated by Luna CSP

1. From the Start menu, select All Programs > Administrative Tools > Windows PowerShell Modules.

2. Run the command

```
Set-ADFSProperties -AutoCertificateRollover $False
```

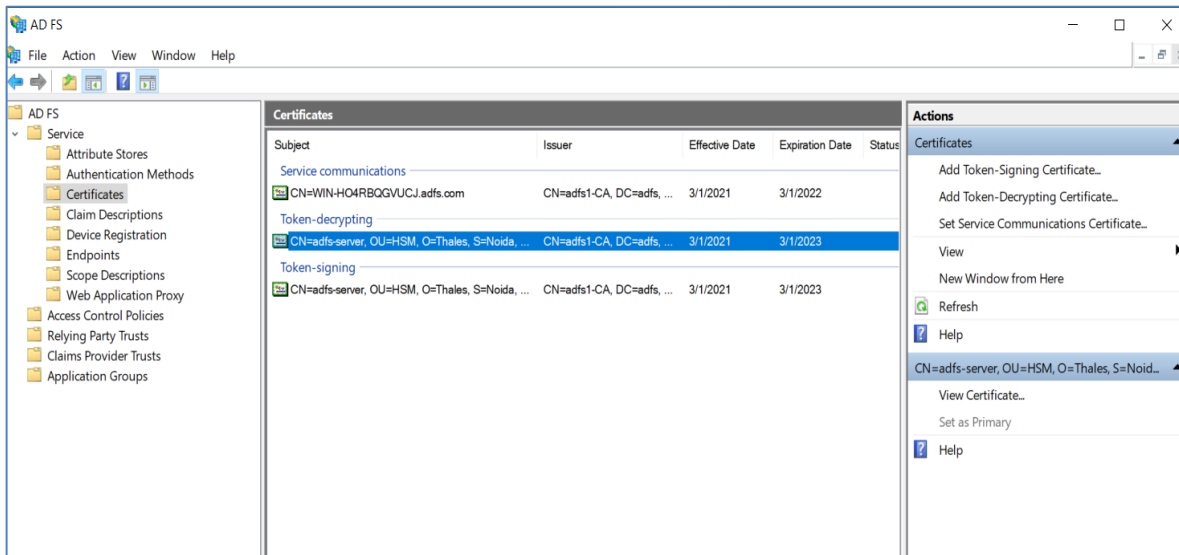
3. Run the command

```
get-ADFSProperties
```

Verify that **AutoCertificateRollover** is set to be **False**.

4. Open the ADFS Management.
5. Expand the **Service** and click **Certificates**.
6. In the Actions pane, click **Add Token-Signing Certificate**.
7. Select the ADFS Token Signing certificate that you have generated using Luna CSP.
8. Click **OK**. It will add the certificate in the Certificate pane.
9. Right-click the certificate and select **Set as Primary**.
10. A confirmation message will pop up. Click **Yes**.
11. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.
12. In the Actions pane, click on **Add Token-Decrypting Certificate**.
13. Select the ADFS Token Signing certificate that you have generated using Luna CSP.
14. Click **OK** to add the certificate in the Certificate pane.
15. Right-click on the certificate and select **Set as Primary**.
16. A confirmation message will pop up. Click **Yes**.

17. Delete the other certificate, i.e., ADFS Signing Secondary Certificate.



18. Open the command prompt and run the following commands to stop and start the ADFS service:

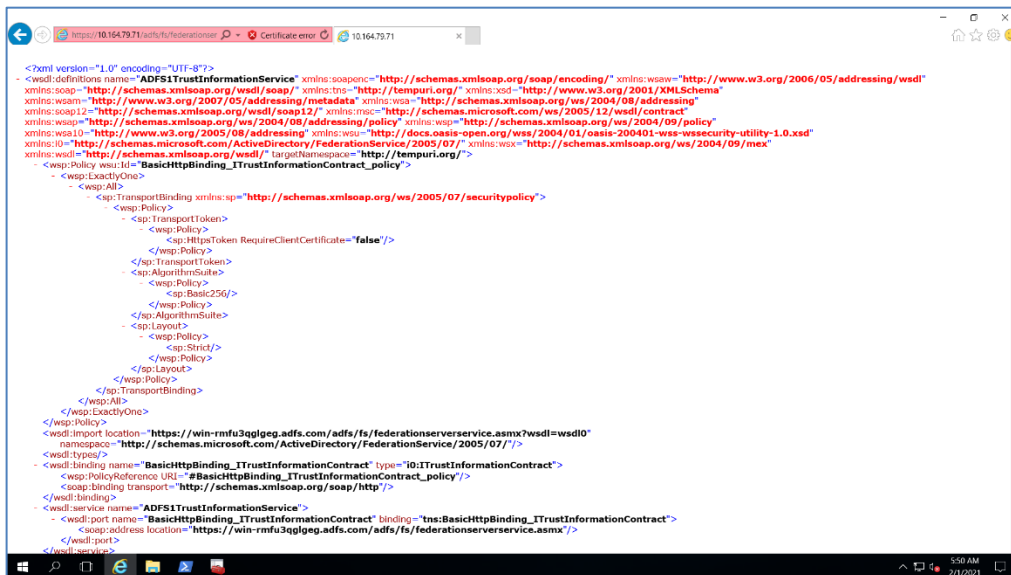
```
Net stop adfssrv
Net start adfssrv
```

19. Verify that the ADFS Service successfully started.

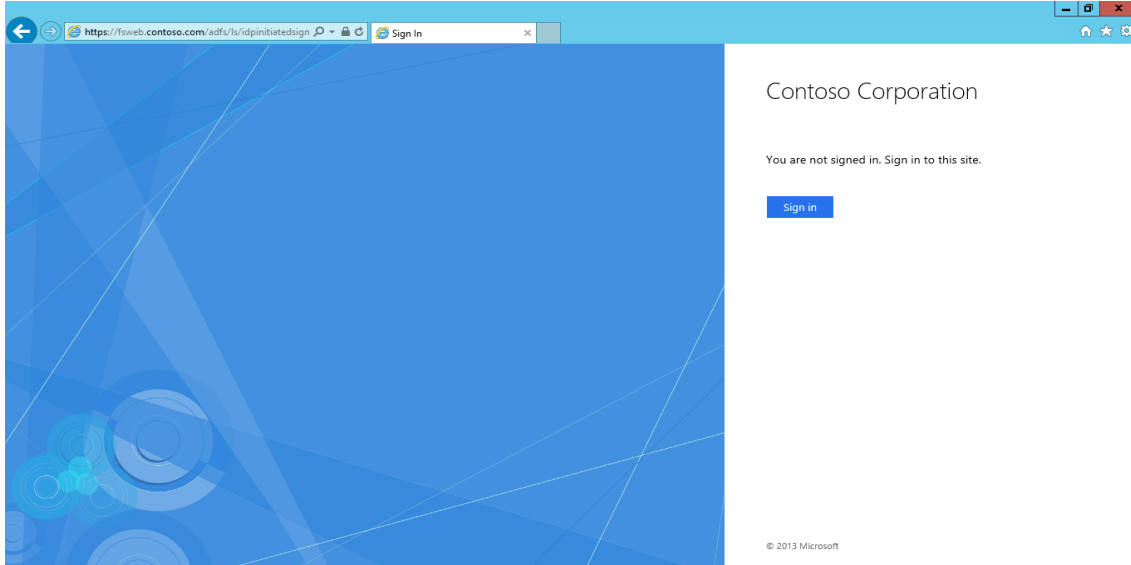
Verify that Federation Server is Operational

1. Open a browser window and in the address bar, type the federation server name, and then append it with federationmetadata/2007-06/federationmetadata.xml to browse to the federation service metadata endpoint. For example, <https://adfsweb.contoso.com/federationmetadata/2007-06/federationmetadata.xml>.

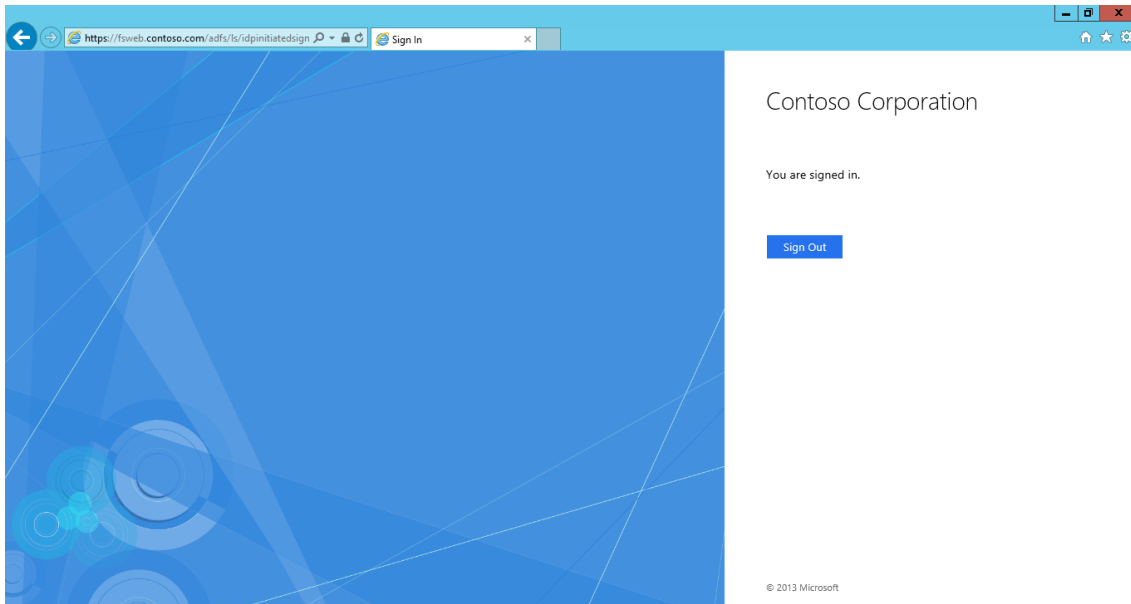
In your browser window, if you can see the federation server metadata without any Secure Socket Layer (SSL) errors or warnings, your federation server is operational.



2. You can also browse to the ADFS sign-in page where your federation service name is appended with `adfs/ls/idpinitiatedsignon.htm`, for example, `https://adfsweb.contoso.com/adfs/ls/idpinitiatedsignon.htm`.



This entry displays the ADFS sign-in page where you can sign in by using domain administrator credentials.



NOTE: Ensure to configure your browser settings to trust the federation server role by adding your federation service name, for example, `https://adfsweb.contoso.com`, to the browser's local intranet zone.

Setting up two instances of ADFS sharing same keys on HSM

This section describes how to set up small test lab for multiple ADFS instances that will use the same keys on the HSM for encryption\decryption of tokens issued by ADFS.

Microsoft ADFS setup

Microsoft ADFS must be installed on the target machines to carry on with the integration process.

The following setup is required:

- > ADFS1: Windows Server machine for first instance.
- > ADFS2: Windows Server machine for second instance.
- > TESTDC: Windows Server machine, which will become a Domain Controller.
- > Domain Administrator privileges

It is assumed that you have joined the ADFS1 and ADFS2 computer to the CONTOSO domain.

Luna HSM setup

Luna Client should be installed on the target machines to carry out the integration. Refer the [Prerequisite section](#) of this guide to install the Luna HSM Client and establishing the NTLS connection with the registered partition on the Luna HSM.

To use the same key pair on Luna HSM, you have to register the same Luna HSM partition on both ADFS1 and ADFS2 computers. Run the **'vtl verify'** command to ensure that you have registered the same partition with both instances.

Integrating Luna HSM with two instances of Active Directory Federation Services

To set up Luna HSM with two instances of Active Directory Federation Services, perform the following steps:

- > [Register CSP](#)
- > [Generate token signing/decrypting certificate to use with ADFS1](#)
- > [Export the existing Token Signing/Decrypting certificate from ADFS1](#)
- > [Import the ADFS1 Token Signing/Decrypting certificate to ADFS2](#)

Register CSP

CSP must be registered on the Federation Servers (ADFS1 and ADFS2).

Generate token signing/decrypting certificate to use with ADFS1

1. Log in to ADFS1 as domain administrator.
2. From the **Start** menu, select **Run**.
3. In the **Run** dialog box, type **mmc**, and click **OK**.

4. The **mmc** console displays. Select **File > Add/Remove Snap-in...**
5. In the **Add or Remove Snap-Ins** dialog box, find the **Certificates** snap-in under the Available snap-ins section, and select it.
6. Click **Add**, select **Computer Account**, and Click **Next**.
7. Select **Local Computer** and click **Finish**.
8. Click **OK** and expand the **Certificates** under **Console Root**.
9. Right-click on the Personal folder and select All Tasks > Advanced Operations > Create Custom Request...
10. Click **Next**, select **Proceed** without enrollment policy, and then click **Next**.
11. On **Custom request** page, select **(No template) Legacy Key** from the drop-down list and select **Request format** as **PKCS #10**. Click **Next**.
12. Click **Details** and then click **Properties**.
13. The **Certificate Properties** window displays. Select the **Subject** tab.
14. Select **Common Name** under **Subject Name** and enter the “**ADFSTokenSigning**” in **Value** field and click **Add**. Repeat the same step for adding more values.
15. Click the **General** tab and provide the **Friendly Name**. For example ADFS Token.
16. Click the **Private Key** tab, and verify that **Luna enhanced RSA and AES provider for Microsoft Windows** must be selected under the **Cryptographic Service Provider**.
17. Click **Key** and select **Key size** as **2048** from the drop-down list.
18. Click **Key type** and select **Exchange**.
19. Click Key permissions and select Use custom permissions check box.
20. Click **Set permissions...** and then **Add**.
21. Type **NETWORK SERVICE** in the text box and click **OK**. It will add the **NETWORK SERVICE** in the **Group or user name** area. Provide read permissions by selecting **Read** check box under the **Permission** area.
22. Click **Add** again and add the Domain Administrator (CONTOSO\Administrator) and provide **Full Control** and **Read** permissions to the Administrator by clicking respective check boxes and click **OK**.
23. Click **Next** and then Browse to save the certificate request.
24. Select **Base 64 File** format, and click **Finish**.
25. Check the Luna HSM registered partition to see the container and keys generated. The snapshot given below shows the keys and container generated on the Luna HSM partition.

```
-----  
lunacm :> partition contents
```

```
Object Label: X-1e-aa48606f-252d-4753-9e7c-26cbcb11baa9  
Object Type: Public Key
```

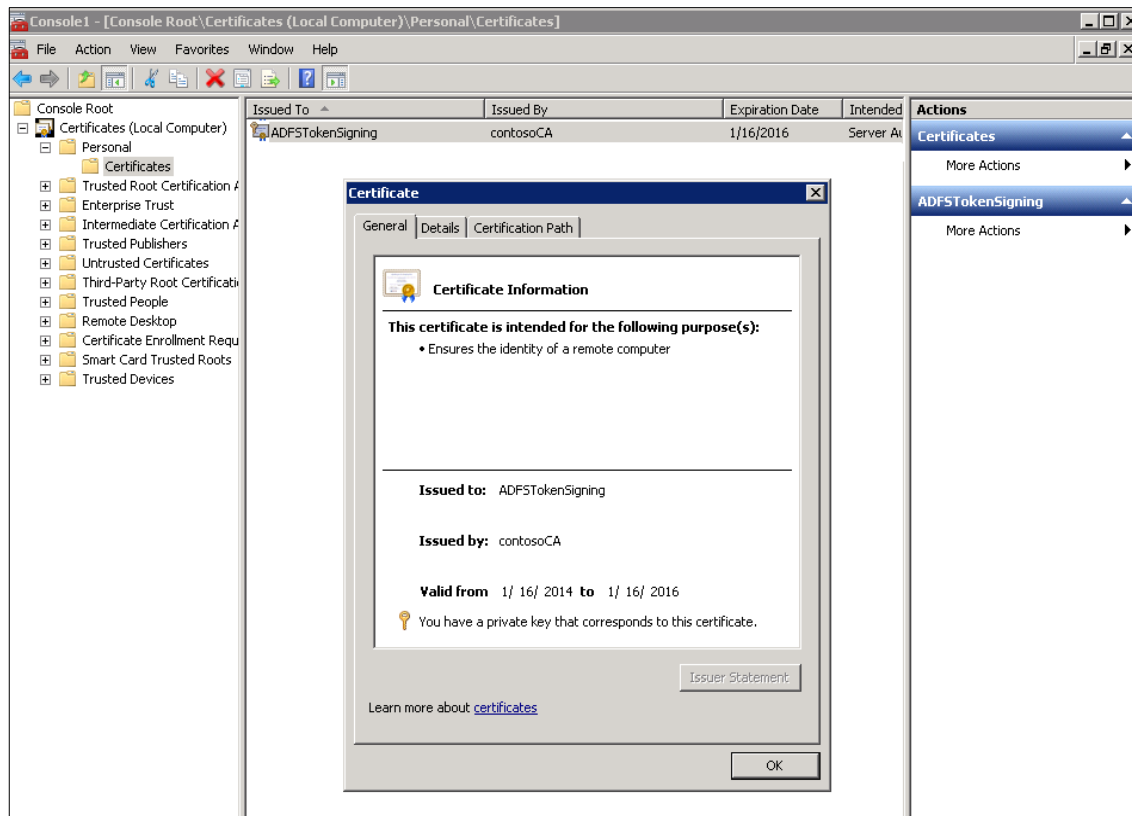
```
Object Label: X-1e-aa48606f-252d-4753-9e7c-26cbcb11baa9  
Object Type: Private Key
```

```
Object Label: 1e-aa48606f-252d-4753-9e7c-26cbcb11baa9  
Object Type: Data
```

Command Result: 0 (Success)

NOTE: The Object Type: Data is the key container for the ADFS keys; copy the Object Label of the container i.e. "le-aa48606f-252d-4753-9e7c-26cbcb11baa9". This container will be used to associate the certificate with the same key pair on ADFS2.

26. Submit the certificate request and obtain signed certificate from the Certificate Authority such as VeriSign, GlobalSign, etc. You can also use local CA to sign the certificate request.
27. In the **Certificate** Console, right-click on the **Personal** folder and select **All Tasks > Import** and follow the instruction to import the Token Signing Certificate signed by CA. You will get the following message: **Certificate imported successfully**
28. Double-click the certificate and verify that **"You have a private key that corresponds to this certificate."**



Now follow the steps in section [“Configure ADFS to use Luna HSM”](#) to complete the integration on ADFS1.

Export the existing Token Signing/Decrypting certificate from ADFS1

1. Log on to the ADFS1 server with the administrator account.
2. Click **Start > Run >** type **MMC** and press the Enter key.
3. In the console click **File > Add/Remove Snap-in...> Certificates > Add**.
4. Select **Computer Account** and click **Next**.

5. Select **Local computer** and click **Finish**.
6. Click **OK** and expand **Personal**, and then click **Certificates**.
7. Right-click the *ADFSTokenSigning* certificate, point to **All Tasks**, and then click **Export**.
8. On the **Welcome to the Certificate Export Wizard** page, click **Next**.
9. On the **Export Private Key** page, click **No**, do not export the private key, and then click **Next**.
10. On the **Export File Format** page, click **DER encoded binary X.509**, and then click **Next**.
11. On the **File to Export** page, in the **File Name** box, type **C:\export.cer**, and then click **Next**.
12. On the **Completing the Certificate Export Wizard** page, click **Finish**.
13. In the **Certificate Export Wizard** message box, click **OK**.
14. Close the certificate management console.
15. Copy and paste the exported certificate on the ADFS2 server.

Import the ADFS1 Token Signing/Decrypting certificate to ADFS2

1. Log on to the ADFS2 server with the administrator account.
2. Register Luna CSP with same partition on ADFS2.
3. Click Start->Run->type **MMC** and press Enter.
4. In the console click **File-> Add/Remove Snap-in...-> Certificates-> Add**.
5. Select **Computer Account** and click **Next**.
6. Select **Local computer** and click **Finish**.
7. Click **OK** and expand **Personal**, and then click **Certificates**.
8. Right-click **Certificate**, point to **All Tasks**, and then click **Import**.
9. On the Welcome to the **Certificate Import Wizard** page, click **Next**.
10. On the **File to Import** page, click **Browse** and select the certificate you have copied from ADFS1.
11. Click Next. On the Completing the **Certificate Import Wizard** page, click **Finish**.
12. Right-click the certificate and click **Open**.
13. In the **Certificate** dialog box, on the **Details** tab, select the **Thumbprint** attribute then press the **Control-C** on the keyboard to copy the Thumbprint to the Windows clipboard.
14. Open the command prompt and type:

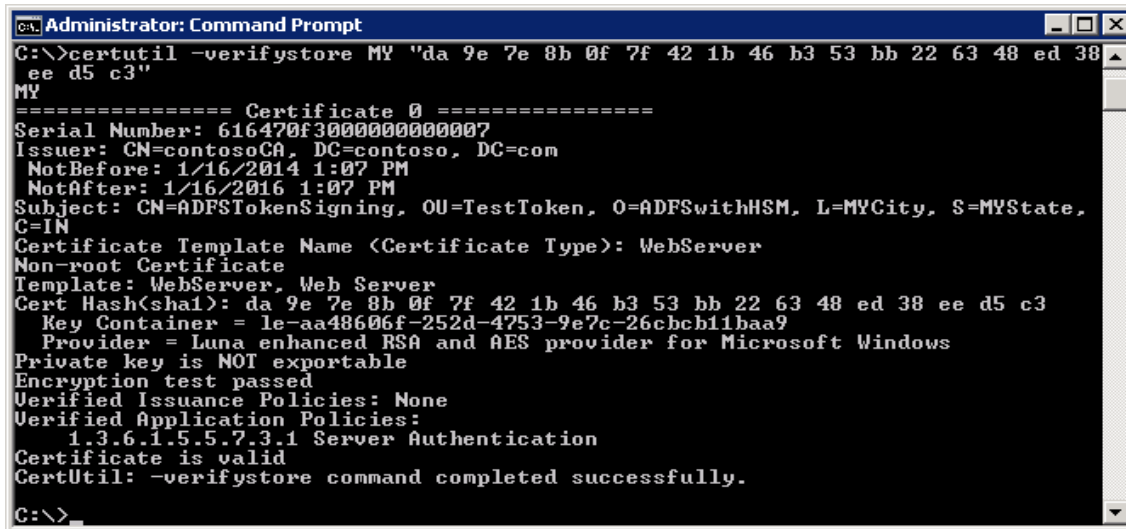
```
certutil -repairstore -v -csp "Luna enhanced RSA and AES provider for Microsoft Windows" My "Thumbprint" repaircsp.inf
```

where sample "repaircsp.inf" looks like:

```
[Properties]
11 = ""; Add friendly name property
2 = "{text}"; Add Key Provider Information property
  _continue_="Container=le-aa48606f-252d-4753-9e7c-26cbcb11baa9&"
  _continue_="Provider=Luna enhanced RSA and AES provider for Microsoft Windows&"
  _continue_="ProviderType=24&"
  _continue_="Flags=32&"
  _continue_="KeySpec=1"
```

NOTE: Replace the container “le-aa48606f-252d-4753-9e7c-26cbcb11baa9” with Object label that is generated on your Luna HSM partition when you generated the keys on ADFS1.

15. After completing the command, right-click the certificate in console and click **Properties**.
16. In the **General** tab, type **ADFS Token** in the **Friendly name** text box. Click **OK** to close the **Properties** window.
17. Right-click the certificate and click **Open**.
18. Ensure that the certificate displays the text “You have a private key that corresponds to this certificate”.
19. Click **OK** to close the certificate window.
20. At the command prompt, type `certutil -verifystore My "Thumbprint"` and press the **Enter** key.



```

C:\>certutil -verifystore MY "da 9e 7e 8b 0f 7f 42 1b 46 b3 53 bb 22 63 48 ed 38 ee d5 c3"
MY
===== Certificate 0 =====
Serial Number: 616470f3000000000007
Issuer: CN=contosoCA, DC=contoso, DC=com
NotBefore: 1/16/2014 1:07 PM
NotAfter: 1/16/2016 1:07 PM
Subject: CN=ADFS token signing, OU=TestToken, O=ADFSwithHSM, L=MYCity, S=MYState, C=IN
Certificate Template Name (Certificate Type): WebServer
Non-root Certificate
Template: WebServer, Web Server
Cert Hash(sha1): da 9e 7e 8b 0f 7f 42 1b 46 b3 53 bb 22 63 48 ed 38 ee d5 c3
Key Container = le-aa48606f-252d-4753-9e7c-26cbcb11baa9
Provider = Luna enhanced RSA and AES provider for Microsoft Windows
Private key is NOT exportable
Encryption test passed
Verified Issuance Policies: None
Verified Application Policies:
1.3.6.1.5.5.7.3.1 Server Authentication
Certificate is valid
CertUtil: -verifystore command completed successfully.
C:\>

```

21. Ensure that the command result states that the Certificate is Valid and shows Encryption test passed. Now the certificate is ready to use as a Token Signing Certificate for ADFS2.
22. Close the **Command Prompt** window.
23. Close all the open windows and restart the server.

After successful restart, log on to the ADFS2 server as a domain administrator and follow the steps of Chapter two from section [Install the token signing/decrypting certificate generated by Luna CSP](#) to complete the integration on ADFS2. You can configure more ADFS instances like ADFS2 node to use the same key pair on HSM using the steps provided above.

Contacting customer support

If you encounter a problem during this integration, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer support portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.