THALES

Microsoft Active Directory Federation Services: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-012087-001
Revision	G
Release Date	16 May 2023

Trademarks, Copyrights, and Third-Party Software

CONTENTS

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 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 Token Signing 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:

- Ensuring secure key generation, storage, and protection through FIPS 140-2 level 3 validated hardware.
- Providing full life cycle management of the keys.
- Maintaining an audit trail through HSM.
- Achieving significant performance enhancements by offloading cryptographic operations from application servers.

> **Note:** The Luna Cloud HSM service does not have access to the secure audit trail.

Understanding Active Directory Federation Services

Active Directory Federation Services (AD FS) is a software 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 AD FS, 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

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 AD FS, refer to previous version of this guide.

Prerequisites

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

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 AD FS.
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. Ignore this if using Luna Client version 10.x.

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]
RSAKeyGenMechRemap=1
```

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

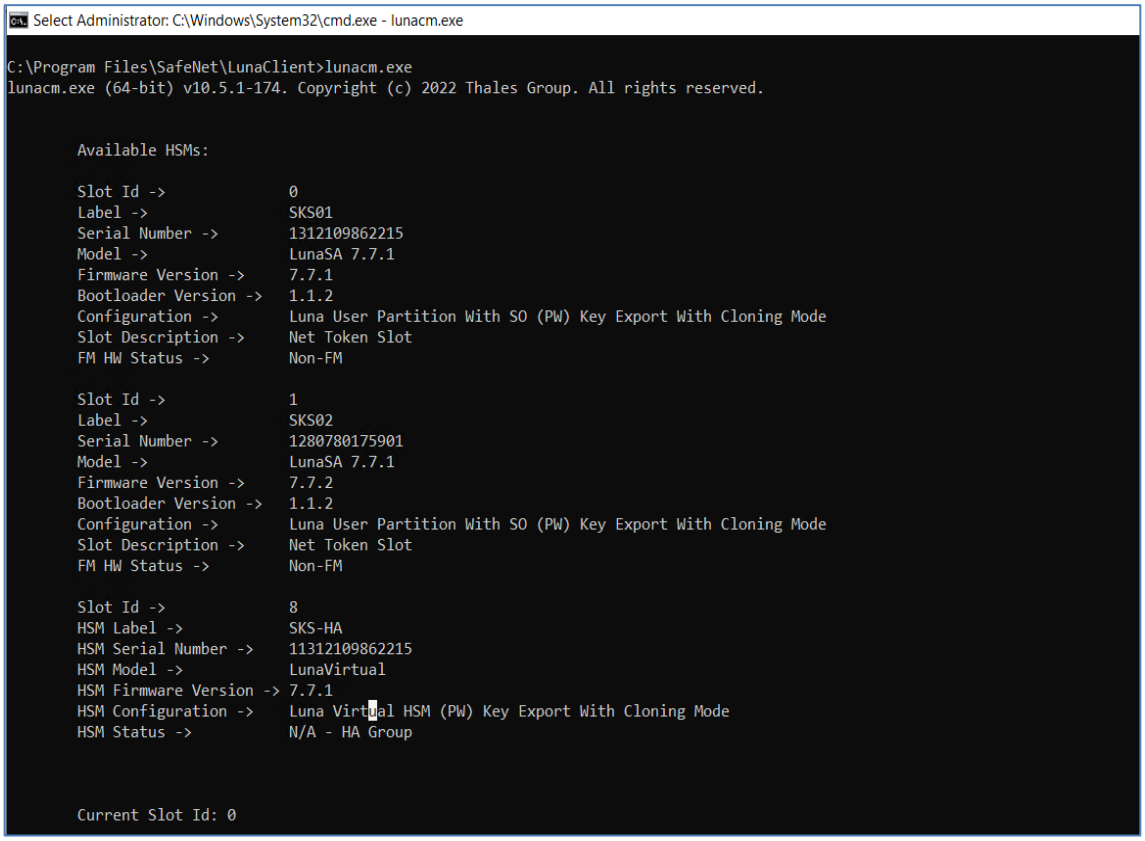
> **NOTE:** The above setting is not required for Universal Client. This setting is applicable only for Luna Client 7.x.

Configure Luna HSM with SKS (Scalable Key Storage)

Complete the following steps to configure SKS:

> **NOTE:** SKS is only supported with Luna Client version 10.4 or above and with Luna Firmware Version 7.7.0 onwards.

1. Make sure that the partitions are assigned to AD FS server and HA is created using the assigned partitions, if required.
2. Open "`C:\Program Files\SafeNet\LunaClient\lunacm.exe`" and note down the **Label**, **Model**, and **Serial Number** of the HSM slot need to be use.



3. Make a directory C:\Temp\simtoken\001\ and create the INF file at that path with the following contents:

   "C:\Temp\simtoken\001\simtoken.inf"

```
[simtoken]
dbtype = sqlite
label = SKS-HA
manufacturerID = Safenet, Inc.
model = LunaVirtual
serialNumber = 11312109862215
```

   NOTE: To ensure that SHIM works properly, enter the correct values for label, model, and serialNumber as noted down in step 2.

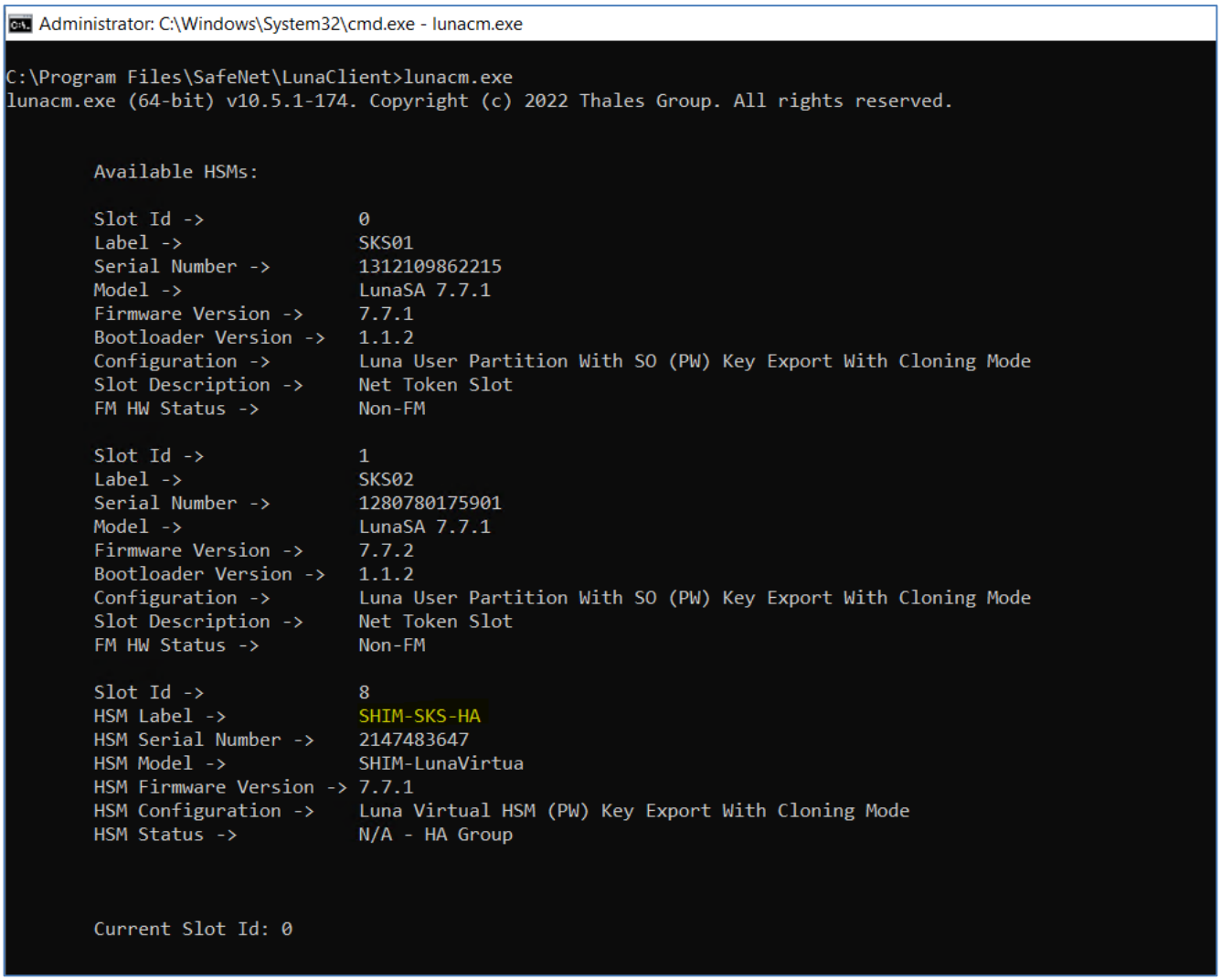
   NOTE: Ensure that the user or service account running AD FS using SKS partition must have read and write permission on C:\Temp\simtoken\001\ directory and files.

4. Open `crystoki.ini` file present in <Luna HSM Client installation Directory> and modify the values, as below:

```
[Chrystoki2]
LibNT=C:\Program Files\SafeNet\LunaClient\shim.dll
. . . . . .

[Shim2]
LibNT=C:\Program Files\SafeNet\LunaClient\cryptoki.dll
. . . . . .

[SimTokenManager]
SimTokenDir=C:\Temp\simtoken\
. . . . . .

[Misc]
ApplicationInstance=SIM_ENGINE
. . . . . .
```

5. Verify that the partition is listed in `C:\Program Files\SafeNet\LunaClient\lunacm.exe` utility with SHIM as prefix.

> **NOTE:** If SHIM is configured correctly for SKS partition, you will see the partition label with **SHIM-** as prefix.



Configure Luna Cloud HSM service

Follow these steps to set up your Luna Cloud HSM:

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 using the following command:

   `tar -xvf cvclient-min.tar`

> **NOTE:** Do not extract to a new subdirectory. Place the files in the client install directory.

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

   ```
   source ./setenv
   ```

   NOTE: To add the configuration to an already installed UC client, use the -addcloudhsm option when running the setenv script.

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

   NOTE: If your organization requires non-FIPS algorithms for your operations, ensure that the Allow non-FIPS approved algorithms check box is checked. For more information, refer to Supported Mechanisms.

Set up Microsoft AD FS

Install Microsoft AD FS 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**: AD FS and Web Server machine.

Configuring Active Directory Federation Services with Luna HSM

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

> Configure the SafeNet Key Storage Provider (KSP)

> Install AD CS using SafeNet KSP

> Configure CA to issue AD FS token signing/decrypting certificates

> Register CSP

> Generate AD FS token signing/decrypting certificate using Luna CSP

> Install AD FS

> Create and configure a server authentication certificate in IIS

> Configure the system as a federation server

> Configure AD FS to use token signing/decrypting certificate generated by Luna CSP

> Verify that federation server is operational

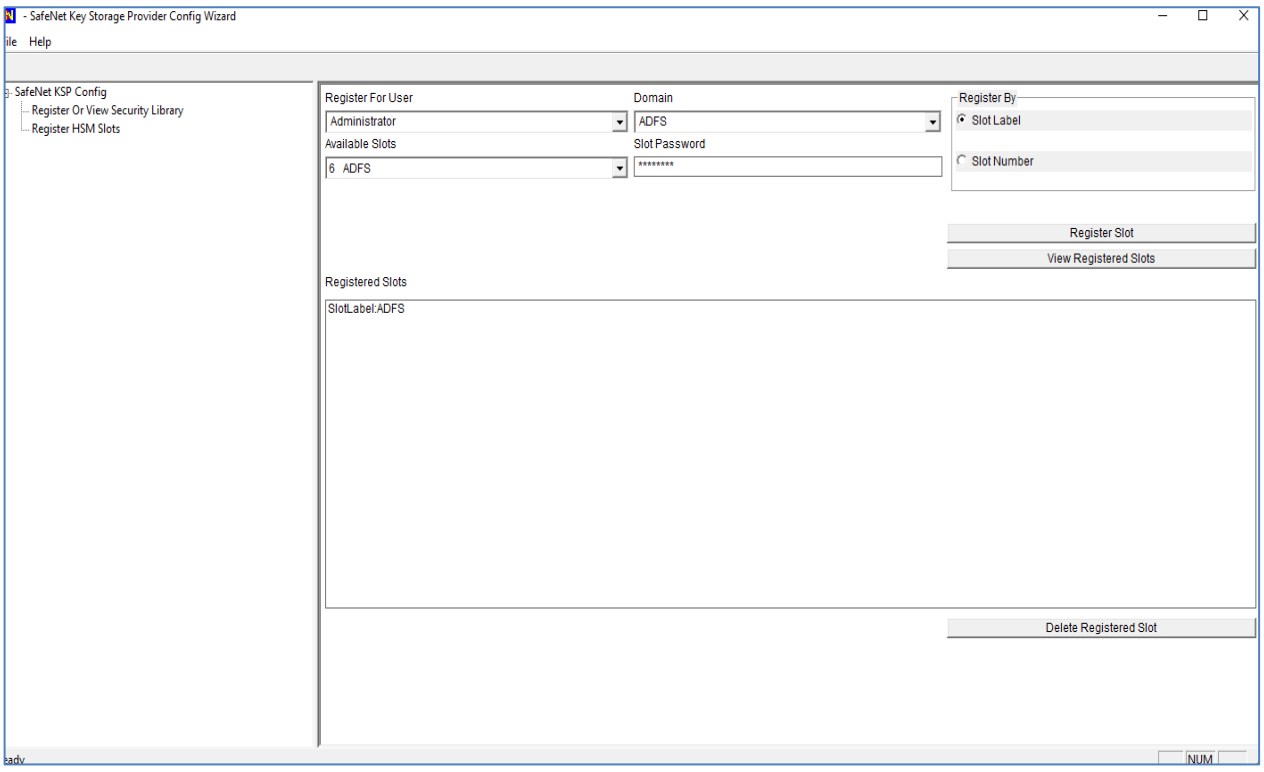
Configure SafeNet Key Storage Provider (KSP)

You must configure SafeNet Key Storage Provider (KSP) to enable user accounts and system access to the Luna HSM or Luna Cloud HSM service. To configure SafeNet KSP:

1. Log in to ADFSCA as a domain administrator.
2. 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.
3. Double-click the `KspConfig.exe` file to launch the KSP configuration wizard.
4. Double-click **Register or View Security Library** on the left side of the pane.
5. 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.
6. On successful registration, the following message will appear on screen:

   Success registering the security library!
7. Double-click **Register HSM Slots** on the left side of the pane.
8. Enter the **Slot Password**.
9. 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!



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

Install Microsoft AD CS using SafeNet KSP

To install Microsoft AD CS:

1. Log in to ADFSCA 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 will appear asking if you want to add the required features for Active Directory Certificate Services. To add a feature, click the **Add Features** button.
9. Click **Next** to continue.
10. On the **Features** page click **Next** to continue.
11. On the **AD CS** page click **Next** to continue.
12. Select the **Certification Authority** check box from the **Role services** list and click **Next**.
13. Click **Install**.
14. When installation is completed, click **Configure Active Directory Certificate Services on the destination server** to open the AD CS Configuration wizard.
15. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.
16. Select the **Certification Authority** check box on **Role Services** and click **Next**.
17. Select the **Enterprise CA** radio button and click **Next**.
18. Select the **Root CA** radio button and click **Next**.
19. Select the **Create a new private key** radio button. Click **Next**.
20. Click the **Select a cryptographic provider** drop-down menu and select **RSA#SafeNet Key Storage Provider**. Select the **Key length** for example: **2048**.
21. Choose the hash algorithm that will be used for signing certificates issued by this Certificate Authority. For instance, select SHA256 as the desired hash algorithm.
22. Click **Next**.
23. Enter a common name to identify this Certificate Authority. Click **Next**.
24. Set the **Certificate Validity Period**, and then click **Next**. Configure the location of the **Certificate database**, which stores all certificate requests, issued certificates, and records of revoked or expired certificates. Click **Next** to proceed.
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
```

```
C:\Users\Administrator>sc query certsvc

SERVICE_NAME: certsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

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.

```
C:\Users\Administrator>certutil -verifykeys
Key "contoso-CA" verifies as the public key for Certificate "contoso-CA"
  V0.0
  Signature test passed

CertUtil: -verifykeys command completed successfully.
```

Configure CA to issue AD FS token signing/decrypting 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**. Type **certtmpl.msc** and hit **Enter**. **Certificate Templates Console** dialog box will appear on your screen.
3. Under Console Root, expand the **Certificate Templates** snap-in. Listed in the middle section will be all available certificate templates. Update the template that your CA will issue.
4. Locate the Web Server template by scrolling down.
5. Right-click on the Web Server template. From the options that appear, select **Duplicate Template**.
6. In **Compatibility** tab, select **Windows Server 2003 Enterprise** and **Windows XP / Server 2003**.
7. Click the **General** tab.
8. Enter the **Template Display Name**, such as AD FS.
9. Select **Publish certificate in Active Directory**.
10. Click the **Cryptographic** tab.
11. Select the "**Request can use any CSP available on subject's computer**" option.
12. Click the **Security** tab and click **Add**.

13. Type **NETWORK SERVICE** and click **OK**.
14. Click **NETWORK SERVICE** in the Group or user names area.
15. In the **Permissions** area, ensure that the **Read** and **Enroll** check boxes are selected.
16. Add and provide **Read** and **Enroll** permissions to the following members:
    - Domain Computers
    - Domain Controllers
    - NETWORK SERVICE
    - IIS_IUSRS
17. For **Domain Admins** and **Enterprise Admins**, ensure that the **Read**, **Write**, and **Enroll** check boxes are selected.
18. Click **Apply** and then click **OK**.

Configuring the CA to support the AD FS certificate template

1. Log on to ADFSCA as a domain administrator.
2. From the Start menu, select **Control Panel** > **Administrative Tools** > **Certification Authority**.
3. Expand the CA in the console tree. Look for the computer icon with a green tick next to it.
4. In the Certification Authority snap-in's console tree, right-click **Certificate Templates**, and then select **New Certificate Templates to Issue**.
5. In the **Enable Certificates Templates** window, choose the AD FS or any other certificate templates you have configured. Click **OK** to confirm your selection.
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. Log in to ADFSWEB as a domain administrator.
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.

> **Note:** If you are using HA use “register.exe /h” command to register CSP with HA Partition.

4. Execute the following command to list the CSP libraries:

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

Generate AD FS 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 **Details** and then **Properties**.
12. The **Certificate Properties** window appears on the screen. Select the **Subject** tab.
13. In the **Subject Name** section, choose **Common Name** and enter the fully qualified domain name of the computer where you are installing the certificate in the Value field. Click **Add** to include the value. You can repeat this step to add additional values, if needed.
14. Click the **General** tab and provide the **Friendly Name**. For example: `ADFS Token Signing`.
15. Click the **Private Key** tab, and ensure 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 AD FS 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` that you want to use with ADFS in the Enter the object name to select text box.

   Note: Ensure that you are using the same gMSA account that you will use for ADFS service. To know more about gMSA account, refer to Microsoft Documentation.

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 AD FS

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 (AD FS) 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**.

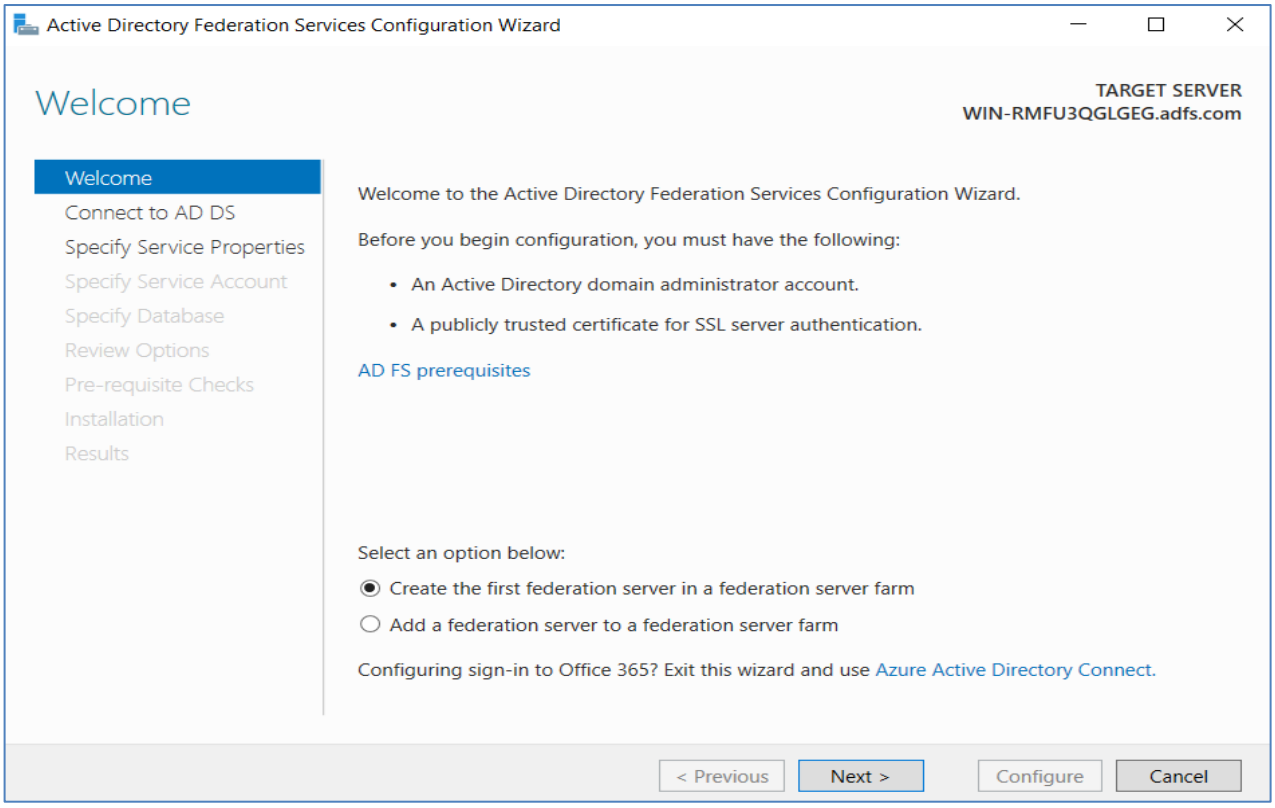
Create and configure a server authentication certificate in IIS

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 the **Finish** button to generate the certificate request. Afterward, submit the certificate request to the Certificate Authority (CA) and save the resulting 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 Web Server`.
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.

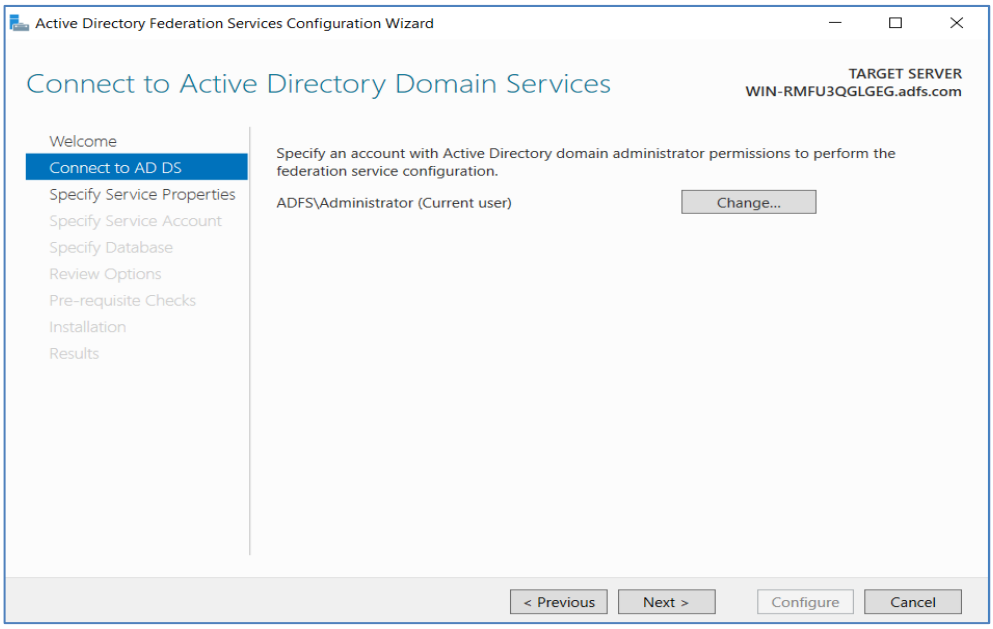
18. Click **OK**, and then click **Close**.
19. Close the Internet Information Services (IIS) Manager console.

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**.



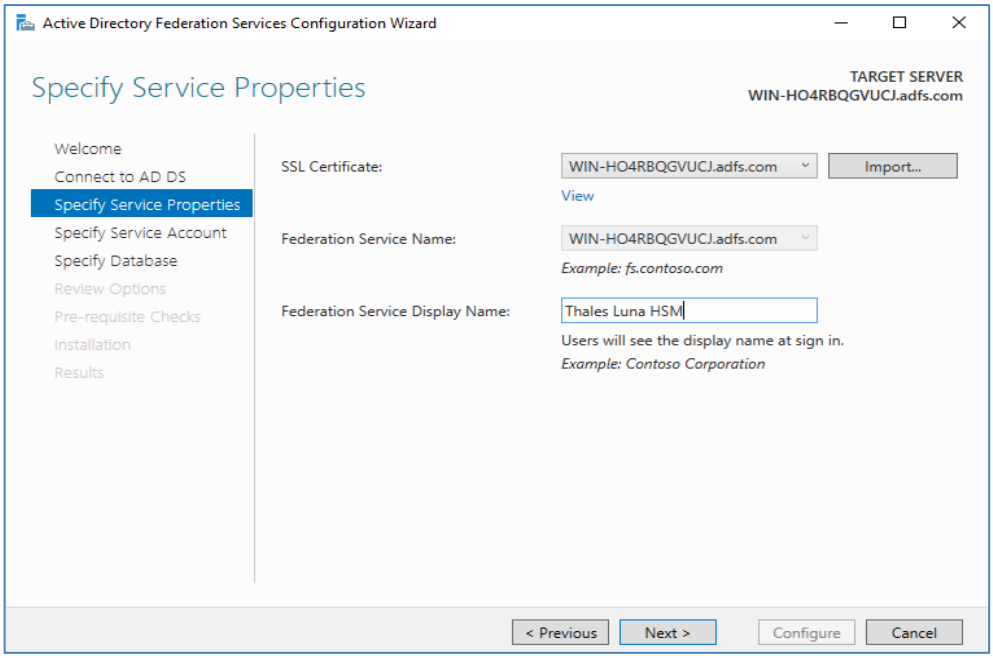
7. On the **Specify Service Properties** page:

   i. Select the certificate that you have configured and bind in the IIS.

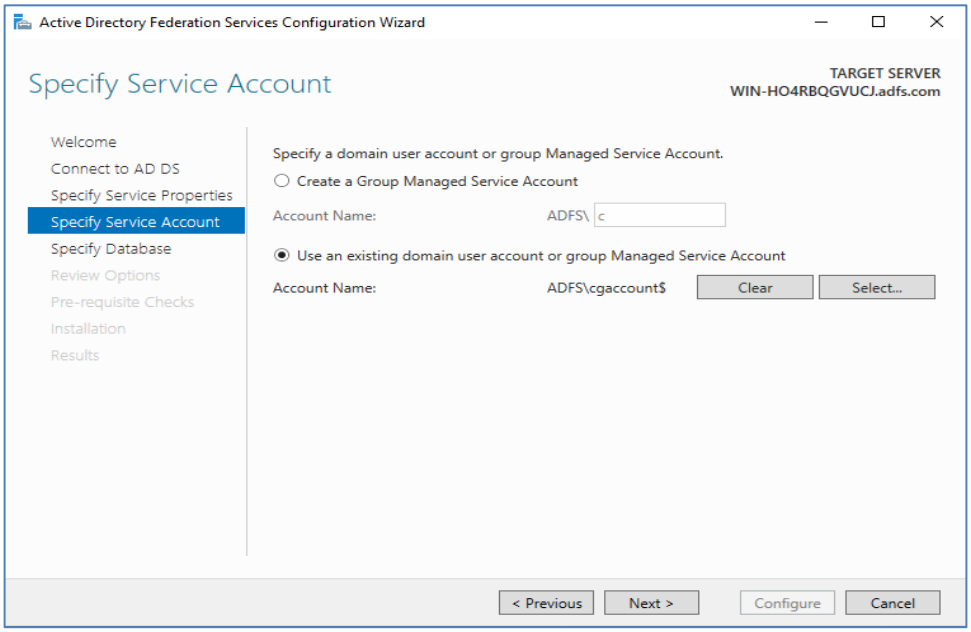
   ii. Provide a name for your federation service. For example, `adfsweb.contoso.com`. This name must match one of the subject or subject alternative names in the certificate.

   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.

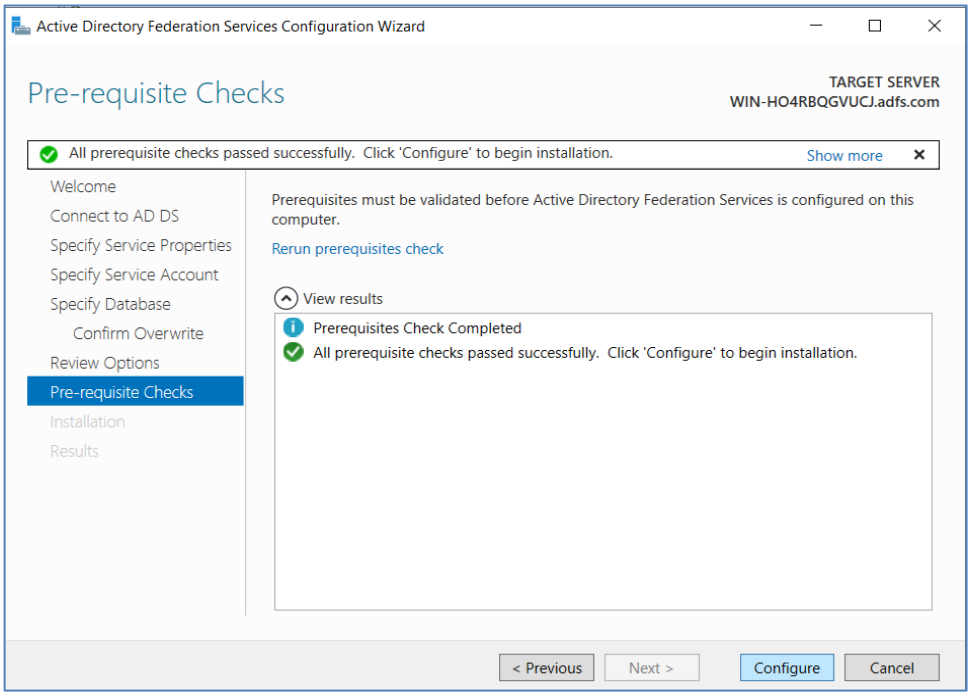
   iv. Click **Next**.



8. On the **Specify Service Account** page, select the option to use an existing gMSA or domain account and provide the gMSA account which have the permission to use the keys created on Luna HSM.



9. 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.
10. On the **Review Options** page, verify your configuration selections, and then click **Next**.
11. On the **Pre-requisite Checks** page, verify that all the 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. Enter a name of your choice to designate your ADFS farm, such as ADFSWEB, in the **Name** box.
5. Enter the IP address of your federation server in the **IP address** box, and then click on the **Add Host** button.
6. Right-click the **domain_name** node, and then click **New Alias (CNAME)**.
7. In the **New Resource Record** dialog box, type `enterpriseregistration` in the **Alias name** box.
8. Type the fully qualified domain name (FQDN) for the target host in the provided box. For example, enter ADFSWEB.contoso.com as the FQDN for the federation service farm, and then click the **OK** button.
9. Open the command prompt and then run `ipconfig /flushdns` on domain controller and also the ADFS server.

Configure AD FS to use 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

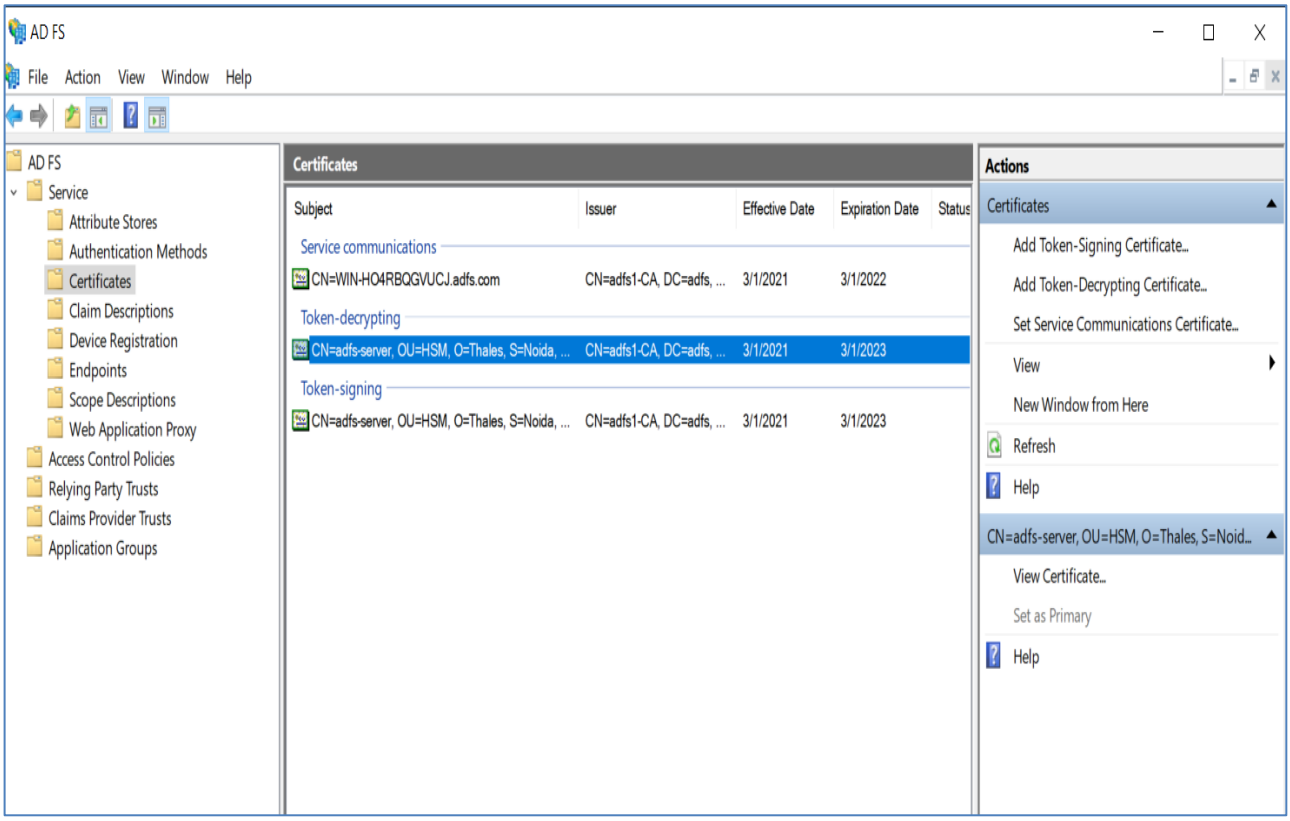
   ```
   Set-ADFSProperties -AutoCertificateRollover $False
   ```

3. Run the command

   ```
   get-ADFSProperties
   ```

   Verify that **AutoCertificateRollover** is set to be **False**.
4. Open the ADFS Management console.
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** to add the certificate to 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, that is, AD FS Token-Signing Secondary Certificate.
12. In the Actions pane, click on **Add Token-Decrypting Certificate**.
13. Select the AD FS 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, that is, AD FS Token-Decrypting Secondary Certificate.



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

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

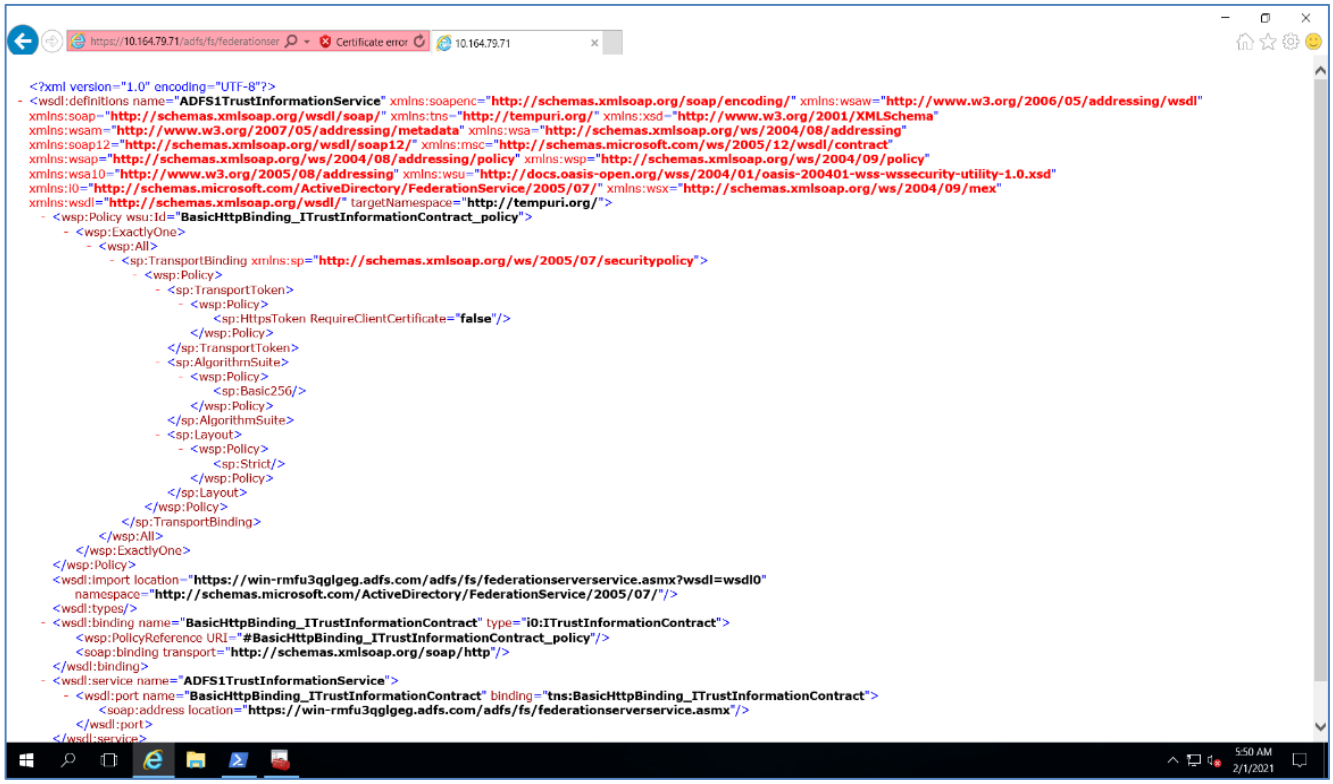
19. Verify that the AD FS Service successfully started.

Verify that federation server is operational

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.



> **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.

This completes the AD FS integration with Luna HSM by securing the AD FS Token signing/decrypting keys on Luna HSM.

Setting up two instances of AD FS sharing same keys on HSM

This section describes how to set up small test lab for multiple AD FS instances that will use the same keys on the HSM for tokens issued by AD FS.

Microsoft AD FS setup

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

The following setup is required:

- **ADFSWEB**: Windows Server machine for first instance.
- **ADFSDR**: Windows Server machine for second instance.
- **ADFSCA**: Windows Server machine, which will become a Domain Controller and CA.
- Domain Administrator privileges

It is assumed that you have joined the ADFSWEB and ADFSDR computer to the CONTOSO domain.

Luna HSM setup

Luna Client should be installed on the target machines to carry out the integration. Refer the Prerequisites 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 ADFSWEB and ADFSDR instances.

Run the **'vtl verify'** command to ensure that you have registered the same partition on both instances.

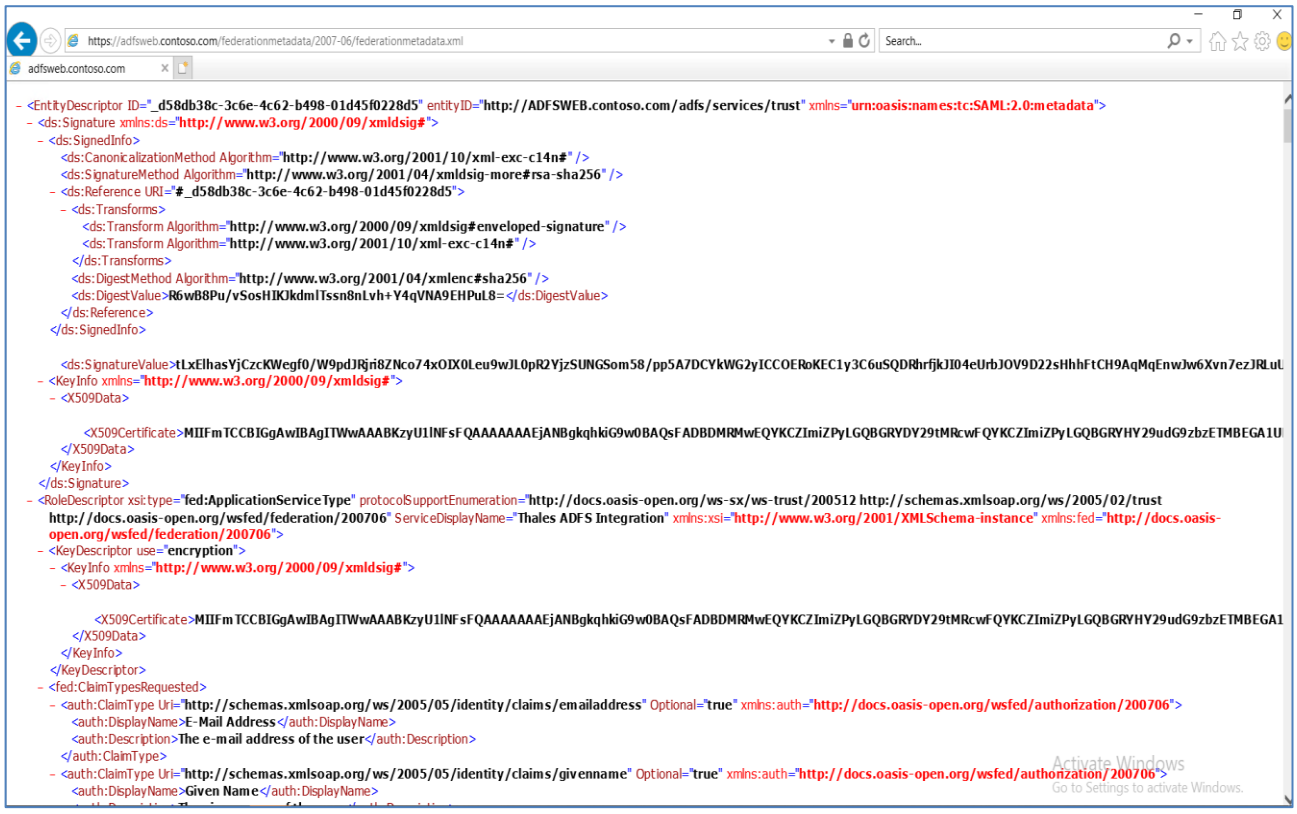
> **Note:** If using SKS partition ensure that SKS partition is registered as per the instructions provided in the Configure Luna HSM with SKS (Scalable Key Storage) section and both instances are registered with the same SKS partition.

Integrating Luna HSM with ADFSWEB (First Instance)

To set up Luna HSM on first instance of Active Directory Federation Services, perform the same steps as mentioned in the Configuring Active Directory Federation Services with Luna HSM section.

Ensure that first instance is up and running using Luna HSM generated Token Signing/Decrypting certificate.

https://adfsweb.contoso.com/federationmetadata/2007-06/federationmetadata.xml



Integrating Luna HSM with ADFSDR (Second Instance)

To use the same Token Signing/Decrypting keys from Luna HSM on the second instance of AD FS use the following:

> Install AD FS

> Configure AD FS

> Register CSP

> Export the existing Token Signing/Decrypting certificate from ADFSWEB

> Import the ADFSWEB Token Signing/Decrypting certificate to ADFSDR

> Configure ADFSDR to use Token signing/decrypting certificate generated by Luna CSP

Install AD FS

Follow the instructions provided in the Install AD FS section.

Configure AD FS

Follow the same instructions provided in section Configure the system as a federation server section.

Register CSP

CSP must be registered on the Federation Servers (ADFSWEB and ADFSDR) using the same partition. Follow the instructions provided in the Register CSP section.

> **Note:** If using same SKS partition, ensure that the `simtoken.db` and `simtoken.inf` files are copied from ADFSWEB (first instance) to ADFSDR (second instance) before registering the CSP with SKS partition.

Export the existing Token Signing/Decrypting certificate from ADFSWEB

1. Log on to the ADFSWEB (first instance) 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. Choose **Computer Account** and proceed by clicking **Next**.
5. Select **Local computer** and click on **Finish**.
6. Click **OK** to confirm and then expand the **Personal** section, and select **Certificates**.
7. Right-click the AD FS Token Signing 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 ADFSDR (second instance) server.

> **Note:** If using SKS partition, ensure that the directory "`C:\Temp\simtoken\001`" and files (`simtoken.db` and `simtoken.inf`) must be copied on all AD FS instances.

Import the ADFSWEB Token Signing/Decrypting certificate to ADFSDR

1. Log on to the ADFSDR (second instance) server with the administrator account.
2. Click **Start**->**Run**->type **MMC** and press Enter.
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 **Certificate**, point to **All Tasks**, and then click **Import**.
8. On the Welcome to the **Certificate Import Wizard** page, click **Next**.
9. On the **File to Import** page, click **Browse** and select the certificate you have copied from ADFSWEB.
10. Click Next. On the **Completing the Certificate Import Wizard** page, click **Finish**.
11. Right-click the certificate and click **Open**.
12. 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 of the certificate.
13. Create a file `repaircsp.inf` with the following contents:

```
[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 of the already generated keys on your Luna HSM.

14. Launch the command prompt and execute the following command:

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

15. After executing the command, right-click on the certificate and select **Properties**.
16. In the **General** tab, type `ADFS Token Signing` in the **Friendly name** text box.
17. Click **OK** to close the **Properties** window.
18. Right-click on the certificate and select the "Open" option. You will see the certificate displays the text "**You have a private key that corresponds to this certificate**".
19. Click **OK** to close the certificate window.

20. Open the command prompt, type `certutil –verifystore My "Thumbprint"` and press the **Enter** key.

    Note: Ensure that the command result states that the Certificate is Valid and shows `Encryption test passed`. Certificate is now ready to use as a Token Signing Certificate for ADFSDR.

```
C:\>certutil -verifystore My 200faa6a7dc078e5d3284423db7d8fd1ac913e24
My "Personal"
================ Certificate 2 ================
Serial Number: 5b00000012b3c94d65345b0540000000000012
Issuer: CN=contoso-CA, DC=contoso, DC=com
 NotBefore: 5/4/2023 5:45 PM
 NotAfter: 5/3/2025 5:45 PM
Subject: CN=ADFSWEB.contoso.com, OU=ADFS INTG, O=Thales, L=Noida, S=Uttar Pradesh, C=IN
Non-root Certificate
Template: ADFS
Cert Hash(sha1): 200faa6a7dc078e5d3284423db7d8fd1ac913e24
  Key Container = te-ADFS-52aafdfc-fff6-453c-9ec0-c3ffeb5cec81
  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.
```

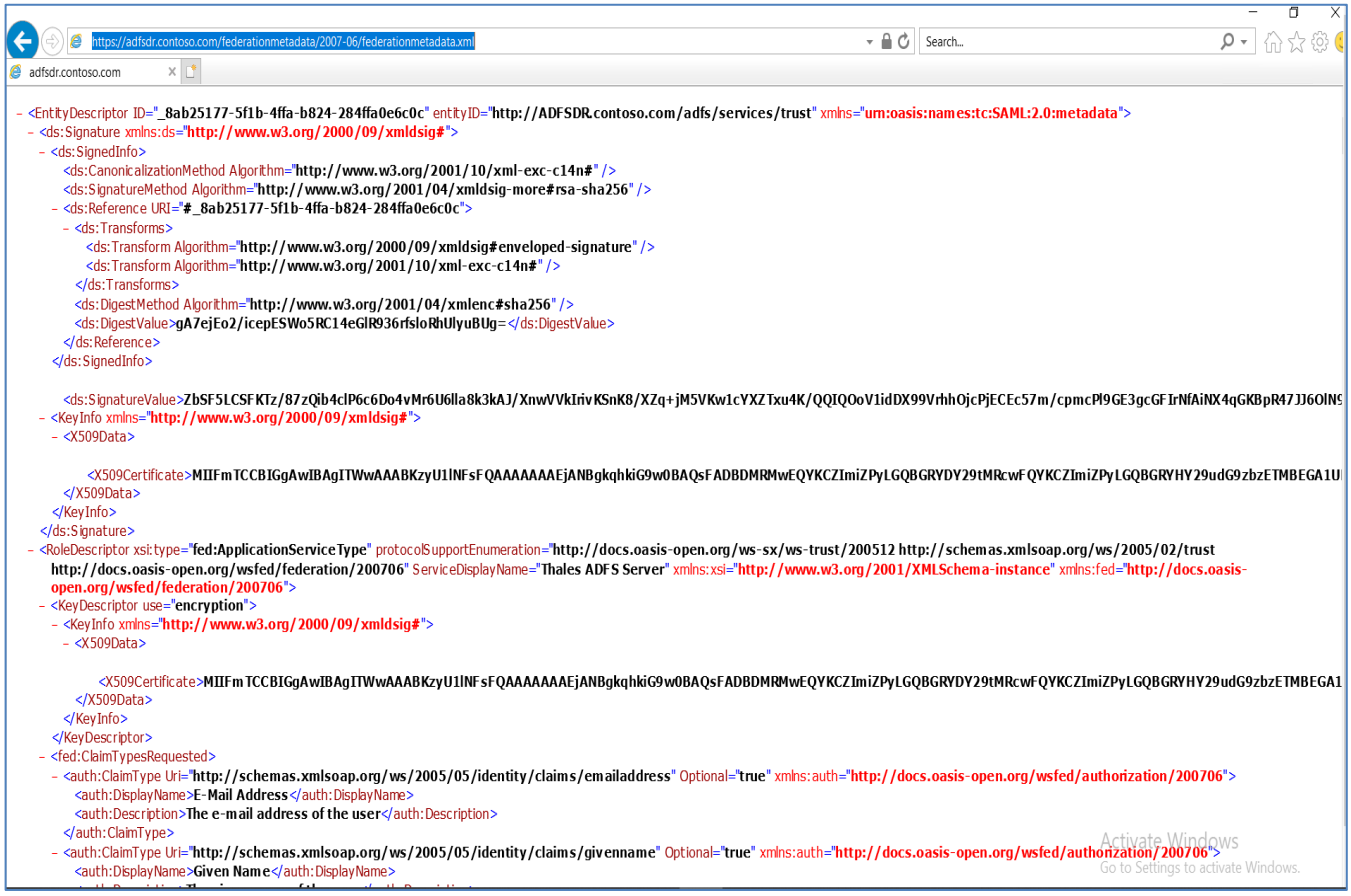
21. Close the **Command Prompt** window.
22. Close all the open windows and restart the server.

Configure ADFSDR to use Token signing/decrypting certificate generated by Luna CSP

Log on to the ADFSDR as administrator and follow the steps provided in the Configure ADFS to use Token signing/decrypting certificate generated by Luna CSP section to complete the AD FS integration on ADFSDR (second instance).

Verify that AD FS server is now operational on ADFSWDR (second instance) using the same certificate and keys generated on Luna HSM using ADFSWEB (first instance).

https://adfsdr.contoso.com/federationmetadata/2007-06/federationmetadata.xml



Note: Ensure that you follow the same steps on all AD FS instances in the case of multiple AD FS servers utilizing the same key for token signing and decrypting. This key should be generated and securely stored on Luna HSM. Consistency across all instances will help maintain a seamless and secure token signing and decrypting process.

Congratulations! You have successfully completed the integration of two AD FS instances with Luna HSM, utilizing the same key for AD FS token signing and decrypting. By following the same steps as you did for the ADFSDR (second instance), you can integrate multiple instances of AD FS, ensuring consistent token signing and decrypting using a shared key. Take a moment to appreciate your accomplishment and the enhanced efficiency this integration brings to your AD FS environment.

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.