Microsoft AD Federation Service

nShield® HSM Integration Guide

2024-10-21

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Table of Contents

1. Introduction . . . 1
    1.1. Configuring AD FS using nShield HSMs . . . 2
    1.2. Prerequisites . . . 2
    1.3. Requirements . . . 3
    1.4. Validation matrix . . . 3
    1.5. Supported nShield HSM functionality . . . 5
2. Procedures . . . 7
    2.1. AD DS Domain Controller: Configure the Domain to Support the AD FS Service . . . 7
    2.2. AD CS Server: Install and Configure AD CS Role . . . 8
    2.3. AD FS Server: Create a TLS certificate template for use by AD FS . . . 9
    2.4. Security World client installation . . . 14
    2.5. Configure the nShield HSM . . . 16
    2.6. Create or load a Security World . . . 17
    2.7. Application key tokens . . . 18
    2.8. Install and register the CNG provider . . . 18
    2.9. Install and register the CSP Provider . . . 21
    2.10. AD FS Server: Request an SSL/TLS certificate for use on the AD FS server . . . 21
    2.11. Install the AD FS server role . . . 26
    2.12. Configure the AD FS server . . . 26
    2.13. Prepare the AD FS Keys for rollover . . . 28
    2.14. Check and enable the AD FS install and sign-on page . . . 29
    2.15. Configure AD FS to use the nShield HSM . . . 30
    2.16. Change the Token-Decrypting Certificate from CNG to CAPI . . . 33
    2.17. Add HSM protected certificates to the AD FS server . . . 35
    2.18. Test AD FS . . . 39
3. Troubleshooting . . . 40
    3.1. General AD FS service issues . . . 40
    3.2. Issues with AD FS service startup . . . 40
    3.3. Permissions for the AD FS TLS key . . . 40
4. Additional resources and related products . . . 42
    4.1. nShield Connect . . . 42
    4.2. nShield as a Service . . . 42
    4.3. nShield Edge . . . 42
    4.4. Entrust digital security solutions . . . 42
    4.5. nShield product documentation . . . 42

Chapter 1. Introduction

Active Directory Federation Services (AD FS) is an installable component of the Microsoft Windows Server operating system. Once configured it provides the facility for single sign-on for credential sharing and access control (federation) between trusted business partners and across multiple business boundaries. This process works via a claims-based authorization process that uses standards-based protocols such as https.

The user's native organization has the responsibility for authenticating and providing identity information required by a trusted partner, which in turn allows the user to transparently connect to an application hosted by one of the members within the trust boundaries of the federation.

Microsoft AD FS effectively provides and secures a mutually trusted zone encompassing multiple security domains. Integrating Microsoft AD FS with Entrust nShield Hardware Security Modules (HSMs) provides increased robustness and control between these boundaries by securely managing the high value Transport Layer Security (TLS) and Token Signing/Decrypting keys required by AD FS within a FIPS 140 level 3 approved hardware environment.

The key objects that are used by AD FS, via the Microsoft CNG API, are as follows:

Key Object	Description
SSL/TLS	Secures web services traffic for SSL communication with web clients and with federation server proxies.
Service-Communications	Used for service communication for Windows Communication Foundation (WCF) Message Security.
Token-Signing	Used to digitally sign all security tokens, including signing of published federation metadata and artifact resolution requests. Can have multiple token-signing certificates configured to allow for certificate rollover when one certificate is close to expiring. All the certificates in the list are published, but only the primary token-signing certificate is used by AD FS to sign tokens.

Key Object	Description
Token-Decrypting	Used to decrypt tokens that are received by a federation server. Can have multiple decryption certificates configured to allow for continuous operation after certificate rollover. All certificates can be used for decryption, but only the primary token-decrypting certificate is published in federation metadata.

1.1. Configuring AD FS using nShield HSMs

This document covers the integration using module protection for the AD FS Token keys, with cipher suite **DLf3072s256mAEScSP800131Ar1**.

1.2. Prerequisites

- An existing Active Directory Domain Services (AD DS) system (domain controller) operating the domain at the Windows Server 2016 Functional Level.
- An existing Microsoft Active Directory Certification Service (AD CS) system configured as an Enterprise issuing CA (for access to certificate templates).
- Credentials to update the domain's DNS service to configure a host entry for AD FS.
- A Security World has already been created or loaded on the HSM to be used by AD FS. For details on installing and registering the nShield CNG KSP via the installed CNG wizard, see Install and register the CNG provider.

Throughout this guide, sections are prefaced with **AD FS Server**, **AD DS Server**, or **AD CS Server**; make sure you execute the steps in each section on the intended server.

For details on installing and configuring the Active Directory Certificate Authority using nShield HSMs, see the *Microsoft AD CS and OCSP Integration Guide for Microsoft Windows Server 2022*.

Entrust recommends that you allow only unprivileged

connections unless you are performing administrative tasks.

You must create a DNS Value for the AD FS service, as the AD FS service will have a different name from the AD FS host server.

If you are deploying AD FS across the internet using Web Application Proxy, you will need a certificate issued by a third party whose Root Certificate is installed on all Computers and devices that will be accessing the service. **This guide does not cover deployment using a Web Application Proxy**.

1.3. Requirements

Requirements for deploying the Microsoft Windows Server environment to support the AD FS role:

Component	Minimum Requirement	Recommended Requirement
Memory	512 MB	4 GB
Processor	1.4 GHz 64-bit processor	Quad-core, 2 GHz
Processor Cores	N/A	N/A
Hard Disk	32 GB	100 GB
CD/DVD	Optional	
Network Adapter	1	
USB Controller	Optional (if you want to be able to use nShield Remote Administration)	
Display	Standard configuration	
Operating System	Microsoft Windows Server 2016 (64bit) or later	
nShield Security World Client Software	A validated version of the nShield Security World client software (see the Validation Matrix below)	

1.4. Validation matrix

This *Integration Guide* provides step-by-step instructions to install and configure Microsoft AD FS for use with nShield HSMs. For our testing purposes, Microsoft Windows Server 2022 was used as the platform for all three requires roles (AD DS, AD CS, and AD FS).

Entrust has successfully tested the integration of AD FS and an nShield HSM using the following configurations:

Software	Firmware	Net Image	World Mode	World Cipher Suite	Module	Softcard	OCS
12.60.11	12.50.11 (FIPS 140-2 certified)	12.70.8 vsn31	unrest-ricted	DLf3072s256mAEScSP800131Ar1	YES	NO	YES[1]
12.60.11	12.50.11 (FIPS 140-2 certified)	12.70.8 vsn31	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	NO	YES[1]
12.71	12.50.11 (FIPS 140-2 certified)	12.70.8 vsn31	unrest-ricted	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]
12.71	12.50.11 (FIPS 140-2 certified)	12.70.8 vsn31	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]
12.80.4	12.50.11 (FIPS 140-2 certified)	12.80.4	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]
12.80.4	12.72.1 (FIPS 140-2 certified)	12.80.4	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]

Software	Firmware	Net Image	World Mode	World Cipher Suite	Module	Softcard	OCS
13.2.2	13.2.2	13.2.2	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]
13.6.3	12.72.1 (FIPS 140-2 certified)	13.4.5	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]
13.6.3	13.2.2	13.3.2	FIPS 140 Level 3	DLf3072s256mAEScSP800131Ar1	YES	YES[2]	YES[2]

[1] *In this configuration, the OCS must not have a passphrase.*

[2] *In this configuration, using a Softcard or OCS with passphrase (or with/without passphrase if k>1 requires that you start the AD FS service using the nShield preload tool. For module protected keys or OCS without a passphrase, preload is not necessary. Additionally, In this configuration, only Module Protection is compatible with CAPI Certs.*

The Token-Decrypting Certificate requires a nShield MS CAPI (CSP) provider, for more information see the ADFS and certificate KeySpec property information page: https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-and-keyspec-property

See the following link for more information on nShield cryptographic providers: https://nshielddocs.entrust.com/security-world-docs/v13.6.3/api-cng/intro.html

1.5. Supported nShield HSM functionality

Functionality	Support
Key Generation	YES

Functionality	Support
Key Management	YES
Key Import	Not tested
Key Recovery	Not tested
1-of-N Operator Card Set	YES[1]
K-of-N Operator Card Set	YES[2]
Softcards	YES[3]
Module-only keys	YES
FIPS 140 Level 3 mode support	YES[4]
Common Criteria mode support	Not tested
Load Sharing	YES
Failover	YES

[1] *Requires Security World client software v12.71 or later if OCS has a passphrase*

[2] *Requires Security World client software v12.71 or later both with or without OCS passphrase*

[3] *Requires Security World client software v12.71 or later*

[4] *If using Softcard to protect AD FS keys, an OCS is still required as the preload command requires FIPS-auth to load keys*

Chapter 2. Procedures

2.1. AD DS Domain Controller: Configure the Domain to Support the AD FS Service

Perform the steps in this section on an AD DS (domain controller) system serving the AD FS server.

1. Open a PowerShell window to execute the commands in this section.
2. Create a Key Distribution Services, (KDS) Root Key so that Domain Controllers (DC) can begin generating gMSA passwords:

```
PS C:\> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))

Guid
-----
bdab22a0-16c1-b0eb-f46c-0638024f7fc9
```

   When the root key has been created, it will take several hours to propagate across to all Domain Controllers on the network.

3. Create the Group Managed Service Account (gMSA) to run the AD FS service:

```
New-ADServiceAccount <Name of AD FS gMSA> -DNSHostName <FQDN of AD FS service>
-ServicePrincipalNames http/<Name of AD FS service>
```

   Example:

```
PS C:\> New-ADServiceAccount FedServgMSA -DNSHostName adfs.example.com -ServicePrincipalNames
http/adfs.example.com
```

4. Configure the AD FS Service Principal Name (SPN):

```
setspn -s http/<name of the AD FS service> <Name of AD FS gMSA>
```

   Example:

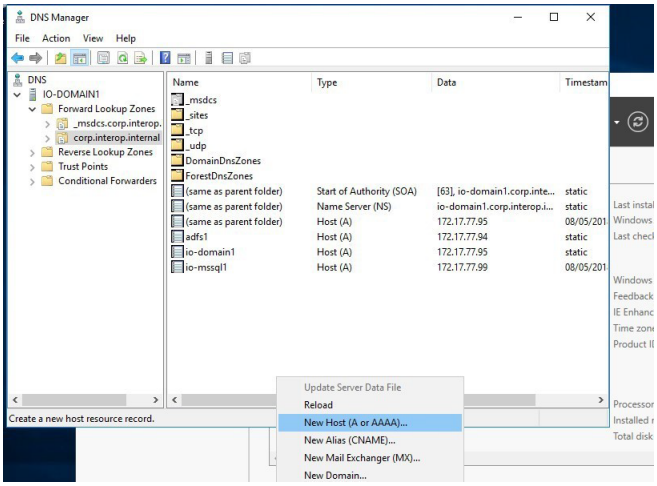
```
PS C:\> setspn -s http/adfs1.example.com example.com\FedServgMSA
```

   This sometimes shows a duplicate SPN, with the following message:

```
Checking domain DC=domain,DC=com
CN=FedServgMSA,CN=Managed Service Accounts,DC=domain,DC=com
   http/adfs.domain.com
```

```
Duplicate SPN found, aborting operation!
```

5. Create a DNS host record for your AD FS service name and its IP address:
   a. Using Server Manager, select **Tools** > **DNS**.
   b. Select the Domain controller and then expand **Forward Lookup Zones**.
   c. Select **<your domain>**.
   d. Right-click either **<your domain>** in the left-hand pane or right-click in the right hand pane and select **New Host (A or AAAA)**.



   e. In **New Host**, enter:

Name	*<AD FS service name>* (the FQDN will auto complete)
IP address	*<IP address of the AD FS host server>*

   f. Select **Add Host** at the bottom of the screen.

Ensure command prompt or PowerShell is launched as Administrator.

2.2. AD CS Server: Install and Configure AD CS Role

Perform the steps in this section on an AD CS(CA) system serving the AD FS server.

This *Integration Guide* relies on the availability of an Enterprise Microsoft AD CS (CA) server within the Active Directory forest. While it may be possible to use another CA product or an external CA for issuing AD FS certificates, the procedures are not in scope of this *Integration Guide*.

Follow the Microsoft installation and configuration procedures to deploy your CA.

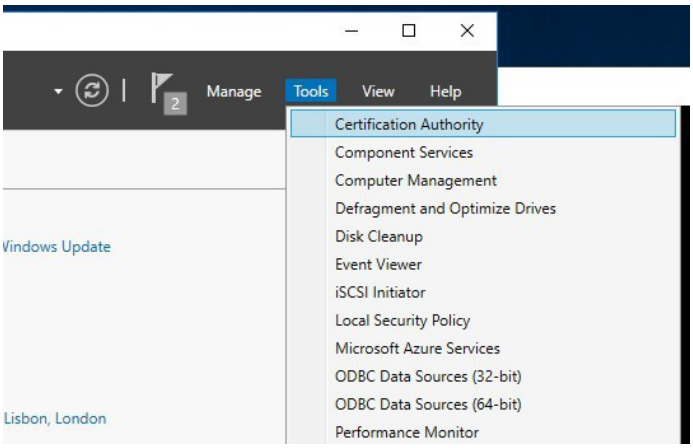
If you wish to deploy your Microsoft AD CS server using an nShield HSM for protection of the CA's private signing key, download the latest *Microsoft AD CS and OCSP Integration Guide for Microsoft Windows Server* from the Entrust nFinity Microsoft partner page.

2.3. AD FS Server: Create a TLS certificate template for use by AD FS

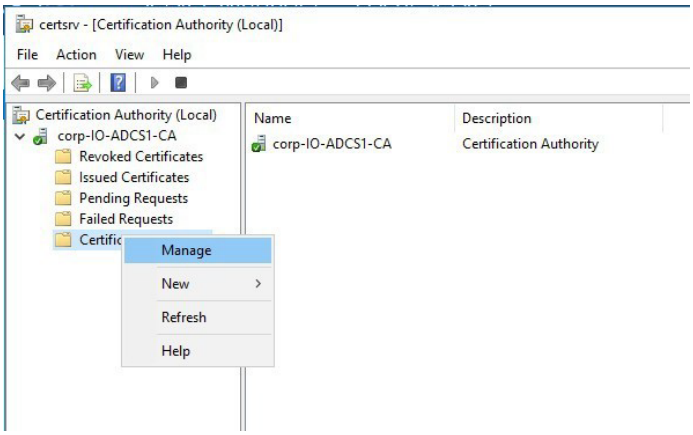
Perform the steps in this section on an AD CS (CA) system serving the AD FS server.

Create a TLS certificate template for use by AD FS as follows:

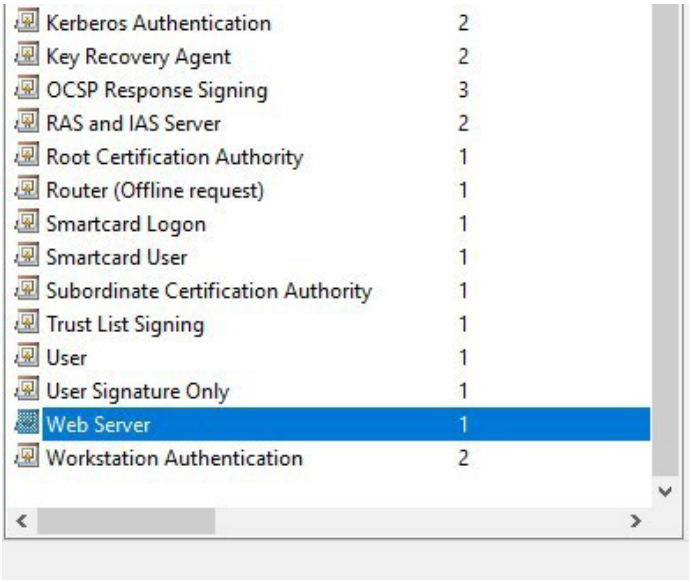
1. On an Issuing CA, open the **Certification Authority** management console.



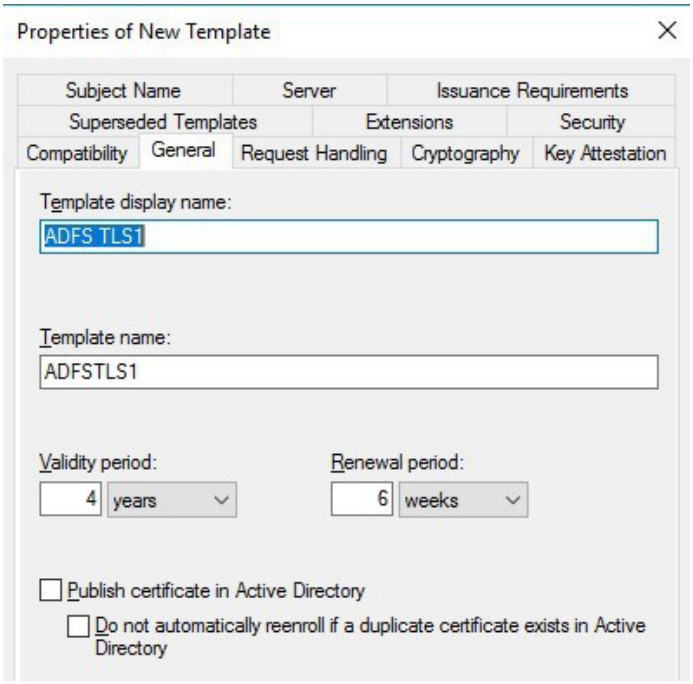
2. Expand the **Certification Authority** node in the left-hand pane, then right-click **Certificate Templates** and select **Manage**.



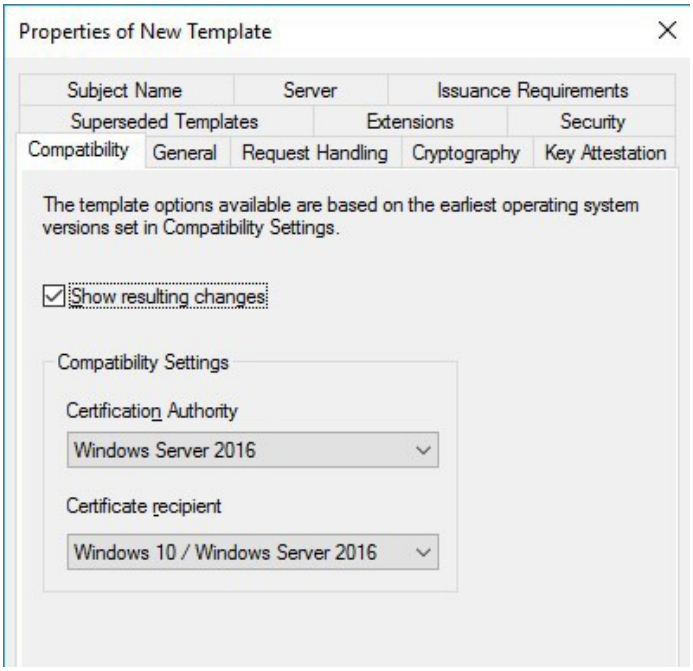
3. In the **Certificate Templates Console**, locate the **Web Server** certificate template, right-click it and from the context menu select **Duplicate Template**.



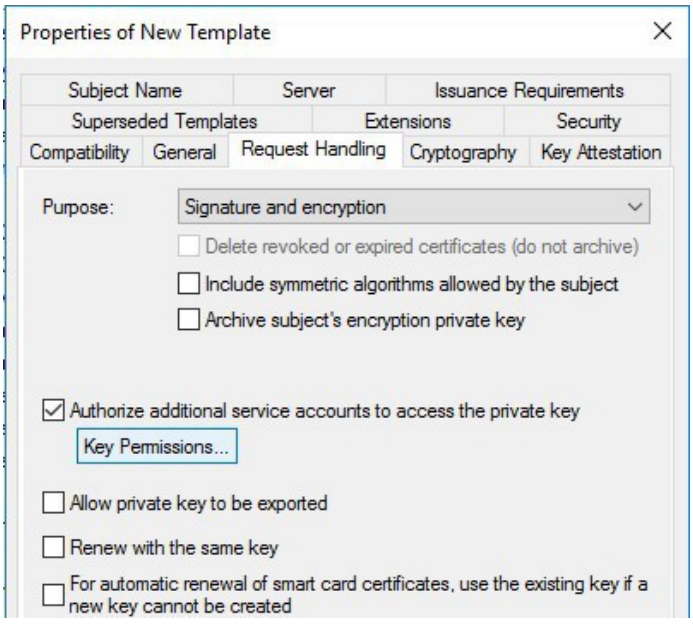
4. In the **Properties of new template** dialog, select the **General** tab.
5. For **Template display name**, name the template, for example "ADFS TLS1".
6. Change the **Validity Period** to whatever value is desired.



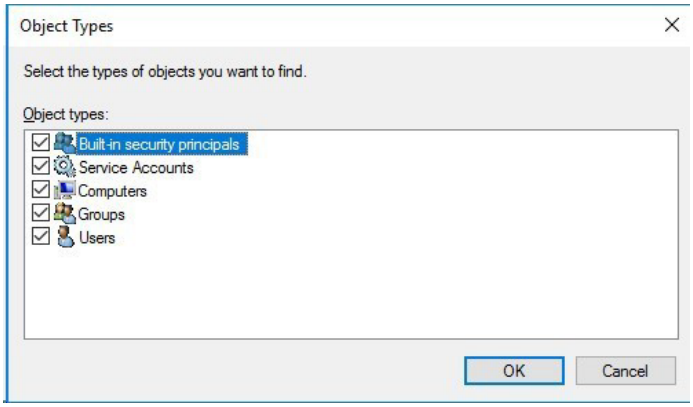
7. Select the **Compatibility** tab and change the **Certification Authority** to **Windows Server 2016** and the **Certificate Recipient** to **Windows 10/Windows Server 2016**.



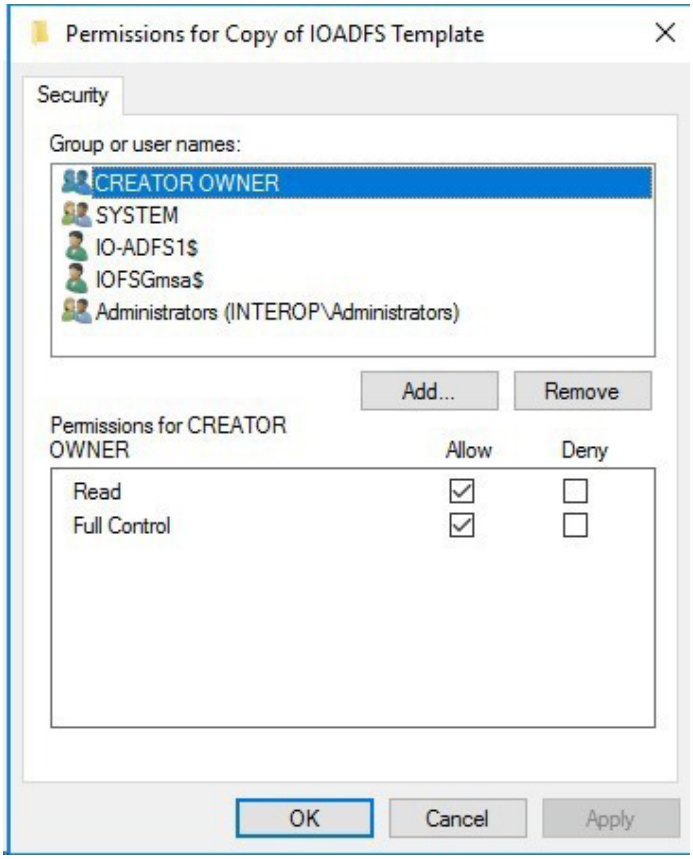
8. Select the **Subject Name** tab and make sure that **Supply in the request** is selected. This is because the AD FS service name will be different from the AD FS Server name and will need to be specified in the request.
9. Select the **Request Handling** tab and under **Purpose** select **Signature and encryption**. Select **Authorize additional service accounts to access the private key**.



10. Select **Key Permissions**.
11. In the **Permissions for** screen, select **Add**.
12. Select **Object Types** and then check the boxes for **Service Accounts** and **Computers** from the listed objects.



13. Select **OK**.
14. For **Enter the object names to select**, type in full/partial names for (separated by semicolons):
    - The Group Managed Service Account you created on your Domain Controller.
    - The AD FS server computer account.
15. Select the **Advanced** tab, select **Find Now** and select the **Group Managed Service Account you created on your Domain Controller**.
16. Select **OK** to add into **Enter the object names**.
17. Select **OK**.
18. Select **Allow Full Control**.
19. Repeat to add the **AD FS server Computer** account, make sure that the **AD FS server Computer** account has **Full Control**.



20. Select **OK** to close the **Permissions for** window.
21. Select the **Cryptography** tab. On this tab:
    a. For **Provider Category**, select **Key Storage Provider**.
    b. For **Algorithm Name**, select **RSA**.
    c. Set the **Minimum Key Size** to at least **2048** for RSA.
    d. Select **Requests can use any provider available on the subject's computer**.
    e. Select **nCipher Security World Key Storage Provider**.
    f. For **Request Hash**, select **SHA256**.
22. Select the **Security** tab. On this tab:
    a. Select **Add**
    b. Select **Object Types** and then check the boxes for **Service Accounts** and **Computers** from the listed objects.
    c. Select **OK**.
    d. For **Enter the object names to select**, type in full/partial names for (separated by semicolons).
    e. The Group Managed Service Account you created on your domain controller. That is, the AD FS server computer account(s) and the Domain Computers group.

f. Select **Check Names** to autocomplete (you may need to select **Advanced** to narrow down your search in large domains).
g. Select **OK**.

23. Back in the **Security** tab, for each account or system that was just added, select the check boxes in the **Allow** column labeled **Read** and **Enroll**. Do not modify the default permissions for any of the existing groups/users:
    - Authenticated Users should only have Read permission.
    - Administrator should have Read/Write permissions.
    - Domain Admins should have Read/Write/Enroll permissions.
    - Enterprise Admins should have Read/Write/Enroll permissions.
24. When all template configuration has been completed, select **Apply and OK** then close the **Certificate Templates** console.
25. Make sure that you are logged into the AD CA as Domain administrator.
26. Issue the new certificate template to the current CA:
    a. Open the **Certificate Authority** console.
    b. On the **Server Manger** Dashboard, go to **Tools > Certificate Authority**.
    c. Under **Certification Authority (local)**, expand the **Domain** (this is presented as a computer with a green tick next to it).

You may need to restart **Active Directory Certificate Service** to make sure the new template is available.

    d. Right-click **Certificate Templates** (last item from the list in the left-hand section).
    e. Select **New** and then select **Certificate Template to Issue**.
    f. Select the certificate template just created, and then select **OK**. The new template will now appear in the **Certificate templates** list.
27. Close the **Certification Authority** management console.

2.4. Security World client installation

Perform the steps in this section on the AD FS server

Install a compatible and supported version of the nShield Security World software (see the *Validation Matrix* in the introduction for more detail) on the designated AD FS server.

1. Sign in to the Windows workstation as an administrator.

2. Navigate to the location of the Security World software.
3. Install the Security World software:
    a. Double-click on the Security World **setup.msi** to start installation.
    b. At the **Welcome** screen select **Next**.
    c. At the **End-User License Agreement** screen, accept the terms and then select **Yes**.
    d. At the **Product Features** screen, select the appropriate packages for your environment and select **Install**.
    e. The installation will begin installing the selected software components.
    f. At the **Completed** screen, select **Finish**.
4. Add the Security World tools to the system path environment variable:
    a. Navigate to **Start > Windows System > Control Panel**.
    b. Navigate to **System and Security**.
    c. Navigate to **System**.
    d. On the left side of the **System** window, select **Advanced system settings**.
    e. In the **System Properties > Advanced** tab that appears, select **Environment Variables**.
    f. In the popup **Environment Variables** window, in the **System Variables** section, select **Path** and select **Edit**.
    g. In the **Edit environment variable** dialog, select **New**.
    h. In the text field that enables, enter in the additional path of `%NFAST_HOME%\bin` and select **OK**.
    i. Back in the **Environment variables** window, select **OK**.
    j. Back in the **System Properties** window, select **OK**.
5. If using a Softcard or OCS with a passphrase (requires Security World client v12.71 or later — see section *Validation Matrix* for more detail), you will need to use the `preload` command to start the AD FS service, and thus must configure the `NFAST_NFKM_TOKENSFILE` system environment variable.
    a. Navigate to **Start > Windows System > Control Panel**.
    b. Navigate to **System and Security**.
    c. Navigate to **System**.
    d. On the left side of the **System** window, select **Advanced system settings**.
    e. In the **System Properties > Advanced** tab that appears, select **Environment Variables**.
    f. In the popup **Environment Variables** window, in the **System Variables** section, select **New**.

g. For **Variable name**, select `NFAST_NKM_TOKENSFILE`.
h. For **Variable value**, enter `c:\nfast_nfkm_tokensfile` (or another name/location of your choosing).
i. Select **OK**.
j. Back in the **Environment Variables** window, select **OK**.
k. Back in the **System Properties** window, select **OK**.

6. If you are using the nShield Remote Administration cards, you must make sure that the cardlist file, `C:\ProgramData\nCipher\Key Management Data\config\cardlist`, has either the relevant card serial number(s) (recommended) or contains a single line with a wildcard * (not recommended for production environments). See the contents of the default `cardlist` file for more info.
7. Close any open PowerShell or Command Prompt windows (when you open new ones later on, the system environment variables will be known in the new shells)

2.5. Configure the nShield HSM

Refer to the applicable *User Guide* for your nShield HSM for installation and configuration instructions. If using an nShield Connect HSM or nShield-as-a-Service (nSaaS) HSM, be sure to perform the required procedures to enroll the AD FS server with the HSM (with the `nethsmenroll` command).

If you are using an nShield-as-a-Service (nSaaS) fully-managed environment, the nSaaS Operations Team will configure your HSM subscription and assist you with establishing a VPN connection to the HSM datacenter(s).

Once your server is configured to communicate with an HSM, verify the HSM connection with `enquiry` before continuing. The output below should be similar:

```
PS C:\> enquiry -m 1
Module #1:
    enquiry reply flags        UnprivOnly
    enquiry reply level        Six
    serial number              EEEE-SSSS-NNNN
    mode                       operational
    version                    12.50.11
    speed index                15843
    rec. queue                 43..150
    level one flags            Hardware HasTokens SupportsCommandState
    version string             12.50.11-270-fb3b87dd465b6f6e53d9f829fc034f8be2dafd13 2019/05/16 22:02:33
    BST, Bootloader: 1.2.3, Security Processor: 12.50.11 , 12.70.8-0-dca4ca4
    checked in                 000000005cddcfe9 Thu May 16 21:02:33 2019
    level two flags            none
    max. write size            8192
    level three flags          KeyStorage
```

```
    level four flags          OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
    FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasLongJobs
    ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
    ServerHasCreateClient HasInitialiseUnitEx AlwaysUseStrongPrimes Type3Smartcard HasKLF2
    module type code          12
    product name              nC3025E/nC4035E/nC4335N
    device name               Rt3
    EnquirySix version        7
    impath kx groups          DHPrime1024 DHPrime3072 DHPrime3072Ex
    feature ctrl flags        LongTerm
    features enabled          StandardKM EllipticCurve ECCMQV AcceleratedECC HSMHighSpeed
    version serial            37
    connection status         OK
    connection info           esn = EEEE-SSSS-NNNN; addr = INET/10.0.0.253/9004; ku hash =
bf83413225927f7d5c3795d03c645d408be24f24, mech = Any
    image version             12.70.8-358-dca4ca4
    level six flags           none
    max exported modules      1000
    rec. LongJobs queue       42
    SEE machine type          PowerPCELF
    supported KML types       DSAp1024s160 DSAp3072s256
    using impath kx grp       DHPrimeMODP3072
    active modes              UseFIPSApprovedInternalMechanisms AlwaysUseStrongPrimes
    hardware status           OK
```

Ensure to verify the following: HSM serial number, the version, features enabled, version serial, connection info, and image version.

Ensure command prompt or PowerShell is launched as Administrator.

2.6. Create or load a Security World

Refer to the applicable *User Guide* for your nShield HSM for instructions on creating or loading a Security World that fits your organizational security requirements. If you are using an nShield-as-a-Service (nSaaS) fully-managed environment, the Entrust nSaaS Operations Team will create the Security World for you and provide you with the necessary world data files for your AD FS server.

A valid Security World must be loaded in the HSM, and world data must exist in the AD FS server in the `C:\ProgramData\nCipher\Key Management Data\local` folder before continuing to the next section.

Ensure you have properly created a Softcard or Operator Card Set (OCS) if you plan on using either of these to protect your AD FS keys. Refer to the applicable nShield *User Guide* for instructions.

Check the world status using `nfkmcheck` before continuing to the next section.

For a FIPS 140 Level 2 Security World, the output should resemble the following:

```
PS C:\> nfkmcheck

nfkmcheck: information: Module #1 Slot #0 Empty
nfkmcheck: everything seems to be in order
```

For a FIPS 140 Level 3 Security World, the following output should resemble the following:

```
PS C:\> nfkmcheck

nfkmcheck: information: World requires administrator authorization
nfkmcheck: information: Module #1 Slot #0 Empty
nfkmcheck: everything seems to be in order
```

Ensure command prompt or PowerShell is launched as Administrator.

2.7. Application key tokens

Application key tokens are an encrypted form of a Security World generated cryptographic key. These key tokens must not be mistaken for or regarded as being a *Key* in or of itself. The key is at all times obfuscated in this encrypted form and is only available for use as a cryptographic key when copied to the FIPS 140 Level 3 security boundary of a correctly configured nShield HSM.

If you intend to use a web application proxy server, and your HSM must be configured for a FIPS 140 level 3 Security World, you should consider deploying a software-based SSL certificate. In level 3 mode, keys cannot be exported, which is required for configuring a WAP in front of the AD FS server. **This guide does not cover deployment using a Web Application Proxy.**

2.8. Install and register the CNG provider

It is possible to use the CNG wizard to either load (reuse) an existing Security World instance or create a new instance. If you are creating a new Security World, see *Installation Guide* and *User Guide* for your HSM on the information required to define Security World parameters. The HSM must be properly configured before running the CNG installation wizard.

To confirm the HSM is available:

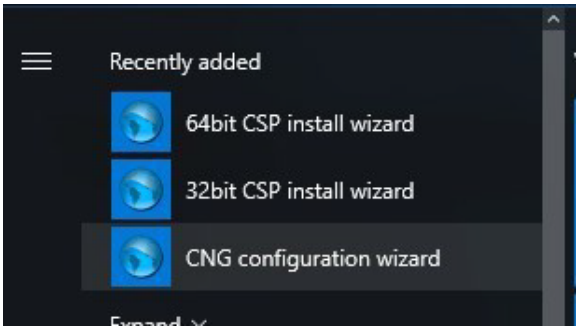
1. Open a CLI as Administrator. You must run **cmd** with elevated privileges. To do this, right-click the **cmd** icon and select **Run as administrator**.
2. Run the command:

```
enquiry
```

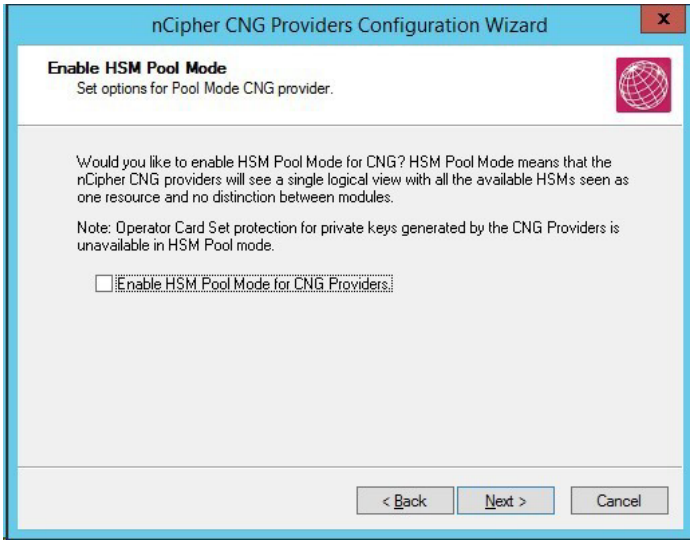
Server: and Module #1: should be reported showing the serial number (in form *eeee-ssss-nnnn*) of the module and hardware status as **OK** (this can be found at the bottom of the section detailing information on the module #).

If you are using an existing Security World, you can check to make sure it is available by running the command `nfkminfo`. Look at the state line of the output it should be reported as **initialized** and **usable**. There should be no **!** prefix.

3. When the Security World software is operational, you must run the CNG install wizard to install and register the nShield Key Storage Provider (KSP). This can be performed via the CNG install wizard that can be found in the **Start** menu of the desktop > **nCipher** > **CNG Configuration Wizard**.
4. Select **Start** and look for the recently added nShield utilities, double-click the **CNG configuration wizard**. If the User **Access Control** prompt appears, select **YES** to continue.



5. The **Enable HSM Pool Mode** screen prompts you to **Enable HSM Pool Mode for CNG Providers**. Leave the default value, make sure that the check box is clear, and select **Next**.



6. At the **Initial Setup** screen, your security world should have already been created or loaded in the section **Create or Load a Security World**. Choose **Use the existing security world** and select **Next**.
7. Make sure that the **Set Module States** screen, ensure module 1 shows both `operational` and `usable` then select **Next**.
8. At the **Key Protection Setup** screen choose **Allow any protection method to be selected in the GUI when generating** and select **Next**.
9. At the **Software Installation** screen, select **Next**.
10. At the **Finish registering the nCipher Providers** screen, select **Finish**.
11. The nShield CNG providers will now be installed and the KSP will be registered. To confirm that the KSP has been successfully registered open

either a CLI or PowerShell (right-click and **Run as Administrator**) and run the following command:

```
>cnglist.exe --list-providers

PS C:\WINDOWS\system32> cnglist.exe --list-providers
Microsoft Key Protection Provider
Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider
Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Microsoft SSL Protocol Provider
Windows Client Key Protection Provider
nCipher Primitive Provider
nCipher Security World Key Storage Provider

PS C:\WINDOWS\system32>
```

You should see the **nCipher Security World key Storage Provider** listed.

2.9. Install and register the CSP Provider

Run 64bit CSP install wizard through Start menu under Entrust nShield Security World.

1. On the start menu select **Next**.
2. Select **Next** on the Enable HSM Pool Mode Screen.
3. Select **Next** on the Initial Set Up Screen.
4. Select **Next** on the Set Module States Screen.
5. Select **Module Protection**.
6. Select **Next** on the Software Installation Screen.
7. Select **Finish**.

Ensure command prompt or PowerShell is launched as Administrator.

8. Reboot the server.

2.10. AD FS Server: Request an SSL/TLS certificate for use on the AD FS server

The instructions in this section assume that all certificates for AD FS will be issued from an Enterprise Microsoft AD CS (CA) server within the Active Directory forest

The certificate template to be used was previously configured in section AD FS Server: Create a TLS certificate template for use by AD FS. Configuring AD FS for use with a different CA product or an external PKI is not in scope of this integration guide.

Four keys/certificates will be created for use by AD FS. You can create all four of these keys/certificates before installing the AD FS role, so they will be ready for use in later sections. The critical parameters for these objects are as follows (tailor these for your environment), which will be referenced in the steps to follow:

AD FS Token-Decrypting cert will later be modified to use CAPI. Module protection must be used for this specific certificate during this integration.

Protection	Crypto Provider	Common Name	Alternative Name(s)	Friendly Name
Software	RSA,Microsoft Software Key Storage Provider	adfs.domain.com	adfs.domain.com, certauth.adfs.domain.com	AD FS TLS Software Key
HSM	RSA,nCipher Security World Key Storage Provider	adfs.domain.com	adfs.domain.com, certauth.adfs.domain.com	AD FS TLS HSM Key
HSM	RSA,nCipher Security World Key Storage Provider	AD FS Token-Signing Key	N/A	AD FS Token-Signing HSM Key
HSM	RSA,nCipher Security World Key Storage Provider	AD FS Token-Decrypting Key	N/A	AD FS Token-Decrypting HSM Key

Make sure the new certificate template is visible within the domain, run `gpupdate` to refresh the Group Policy before proceeding Open a command prompt opened as Administrator and run `gpupdate`:

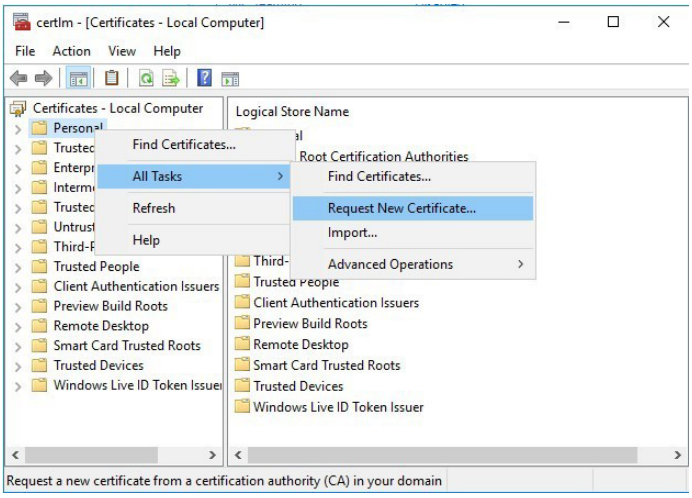
```
gpupdate /force
```

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

If using Security World 13.2.2 with softcard protection, run the following command before continuing. Otherwise, certificate enrollment fails.

```
preload --reload-everything --softcard-name=<Softcard Name> pause
```

1. On the AD FS server, open `certlm.msc` using the `Run` command or an administrator level command prompt.
2. From the left-hand panel beneath **Certificates-Local Computer**, right-click the **Personal** folder, select **All Tasks > Request New Certificate**.



3. The **Certificate Enrollment** wizard will start, select **Next**.
4. On the **Select Certificate Enrollment Policy** screen, select **Next**.
5. The **Request Certificates** window should display the recently created certificate template, select the link **More information is required to enroll for this certificate. Click here to configure settings** to continue.

6. On the **Certificate Properties** window, in the **Subject** tab:
   a. Under **Subject Name**, in **Type** choose **Common Name**.
   b. In **Value**, enter the value from the **Common Name** field in the table at the beginning of this section.
   c. Select **Add**.
   d. Under **Alternative name**, in **Type** choose **DNS**.

e. In **Value**, enter the value from the **Alternative Name** field in the table at the beginning of this section. If there is no alternative name required as shown in the table, this step can be skipped. Select **Add**.

Repeat this process if more than one alternative name is required.

7. On the **General** tab, specify a sensible and recognizable name for the certificate.
8. Select the **Private Key** tab and expand the **Cryptographic Service Provider** and select the appropriate provider defined in the table at the beginning of the section. Make sure that only one provider is checked. Uncheck all of them except the one you need.
   - For a software-based key, choose **RSA,Microsoft Software Key Storage Provider**.
   - For an HSM-based key, choose **RSA,nCipher Security World Key Storage Provider**.
9. Select **OK** to close the **Certificate Properties** window.
10. On the **Certificate Enrollment**, **Request Certificates** window, check the box for the certificate just requested, and then select **Enroll**.
11. For HSM-based keys, the **nCipher Key Storage Provider - Create Key** wizard will appear.
    a. At the **Create new key** screen, select **Next**.
    b. At the **Select a method to protect new key** screen, select the desired key protection mechanism to use. For module, select **Module protection** and select **Finish**. For Softcard select **Softcard protection** and select **Next**.
    c. At the **Select token to protect key with** screen select the appropriate Softcard from the list and select **Finish**.
    d. When prompted for the passphrase (if required) enter it and select **Finish**.
12. For OCS select **Operator Card Set protection** and select **Next**.
13. At the **Select token to protect key with** screen select the appropriate OCS from the list and select **Finish**.
14. At the **Loading "<OCS name>"** screen, insert a card from the selected OCS.
15. When the OCS card has been read, if it has a passphrase, enter it now and select **Next**.
16. If using a k/n OCS with k>1, repeat to load other OCS cards until quorum is made.

17. After loading the required card(s), at the **Card reading complete** screen, select **Finish**.
18. The **Certificate Installation Results** window should show **STATUS: Succeeded**, select **Finish**.

    Repeat these steps until all four certificates have been generated.

19. Verify the new HSM keys:
    a. Open a **cmd** window as Administrator and run `nfkminfo.exe` similar to the example below This will print the CNG key created via the Certificate template. The key will have been generated using the nShield Key Storage Provider. It is possible to use the key's `AppName` and its `Ident` to show further details.

    Example:

```
PS C:\> nfkminfo -l

OUTPUT:
key_caping_machine--c4ce33928f457a19dd5a536a9038b55f02a2eaf1 `te-ADFSTLS-3ec97a8c-791a-4139-a0e6-
ecbf1e185bd8`

PS C:\> nfkminfo -k caping machine--c4ce33928f457a19dd5a536a9038b55f02a2eaf1

OUTPUT:
Key AppName caping Ident machine--c4ce33928f457a19dd5a536a9038b55f02a2eaf1
BlobKA length        1052
name                 "te-ADFSTLS-3ec97a8c-791a-4139-a0e6-ecbf1e185bd8"
hash                 42b4875c0a2fc7af57fa8a904939c4a361c30ff9
recovery             Enabled
protection           Module
other flags          PublicKey !SEEAppKey !NVMemBlob +0x0
gentime              2021-09-10 19:49:17
SEE integrity key    NONE

PS C:\> certutil -silent -store MY tq-ADFSKeys-9ad0688f-4686-4368-9586-95dc5a89c672

OUTPUT:
Serial Number: 610000000d4ee2b718a2dd02ef00000000000d
Issuer: CN=DOMAIN ENTERPRISE ROOT CA, DC=domain, DC=com
NotBefore: 9/17/2021 10:07 PM
NotAfter: 9/17/2023 10:17 PM
Subject: CN=ADFS Token-Decrypting Key
Non-root Certificate
Template: ADFSKeys, ADFS Keys
Cert Hash(sha1): dc36ce9322cc6be72acf6c073861105074d036cb
Key Container = tq-ADFSKeys-9ad0688f-4686-4368-9586-95dc5a89c672
Provider = nCipher Security World Key Storage Provider
Encryption test FAILED
```

    b. In the first output, copy the key hash for the next command, then verify the `Protection` field for the proper protection type. `Module` for module protection, `PassPhrase` for Sard protection, and `CardSet` for OCS protection.

The hash may not match the ones generated for your system.

c. Save the name of the output of the second command for the last command.

d. Verify the `Provider` field to ensure the proper Key Storage Provider has been used.

Ensure command prompt or PowerShell is launched as Administrator.

2.11. Install the AD FS server role

Perform the steps in this section on the AD FS server.

This can be done manually in the Server Manager.

1. Open **Server Manager**.
2. In **Server Manager**, navigate to **Manage > Add Roles and Features**.
3. On the **Before you begin** page (if it appears), select **Next**.
4. On the **Select installation** type page, select **Role-based or feature-based installation**, and then select **Next**.
5. On the **Select destination server** page, select **Select a server from the server pool**, verify that the target computer is selected, and then select **Next**.
6. On the **Select server roles** page, check the box for **Active Directory Federation Services** and select **Next**.
7. On the **Select features** page, select **Next**.
8. On the **Active Directory Federation Service (AD FS)** page, select **Next**.
9. Verify the information on the **Confirm installation selections** page then select **Install**.

Do not select the **Restart the destination server automatically if required** check box.

10. On the **Installation progress** page, wait for everything to install correctly.
11. Once the installation has completed, select **Close**.

2.12. Configure the AD FS server

This step can be completed manually in the Server Manager.

1. In **Server Manager**, initiate post-deployment configuration for the AD FS role.
2. At the **Welcome** screen, select **Create the first federation server in a federation server farm**, select **Next**.
3. In the **Connect to Active Directory Domain Services** page, select the account you want to use to perform the configuration (the currently logged-on account if you have admin rights, which you will need to configure the role) then select **Next**.
4. On the **Specify Service Properties** window:
    a. Select the appropriate **SSL Certificate** from the list. Choose the software-based TLS key previously generated, which should be first in the list. This will be replaced later with an HSM-based key. If you need to, select the **View** link to verify the certificate serial number (since both the software and HSM based credentials will be the FQDN of the AD FS service.
    b. In **Federation Service Name**, ensure the same FQDN is shown (the first Alternative Name, the one that matches the certificate common name.
    c. For **Federation Service Display Name**, enter a meaningful name for the AD FS service.
    d. Select **Next**.
5. On the **Specify Service Account** page:
    a. Select **Use an existing domain user account or group Managed Service Account**.
    b. Select **Select**.
    c. Enter the name of the gMSA account that was created on the domain controller.
    d. Select **Check Names**, the account should be found.
    e. Select **OK**.
    f. Select **Next**.
6. On the **Specify Configuration Database** page, select **Create a database on this server using Windows Internal Database**, and then select **Next**.
7. On the **Review Options** page, verify your configuration selections then select **Next**.
8. On the **Prerequisite Checks** page, verify that all prerequisite checks completed successfully then select **Configure**.
9. On the **Results** page you should see a green tick against **This server was successfully configured**.

10. You may be informed that a machine restart is required.
11. Select **Close** to exit the configuration.
12. In **Services**, make sure to configure **Active Directory Federation Services** to start **manually**. If you are using OCS or Softcard protection for your AD FS integration with the HSM, some sort of manual interaction will be required to start the service.

At this point, the AD FS server should be restarted. Once it has rebooted, sign in as `Administrator`.

2.13. Prepare the AD FS Keys for rollover

1. Ensure the AD FS service is stopped.

```
net stop adfssrv
```

2. Ensure any existing preload cache is reset.

```
preload exit
```

3. Remove the `NFAST_NFKM_TOKENSFILE` cache (if it exists) by deleting the file `c:\nfast_nfkm_tokensfile`.

```
del c:\nfast_nfkm_tokensfile
```

4. Preload the keys into the HSM if necessary:
   a. For module protected keys, go to the next step.
   b. For Softcard protected keys:

```
preload --reload-everything --softcard-name=<Softcard Name> pause
```

   c. For OCS protected keys:

```
preload --reload-everything --cardset-name=<OCS Name> pause
```

   This preload command will intentionally pause until cancelled. You will cancel this in a later step.

5. In a separate PowerShell window, start the AD FS service.

```
net start adfssrv
```

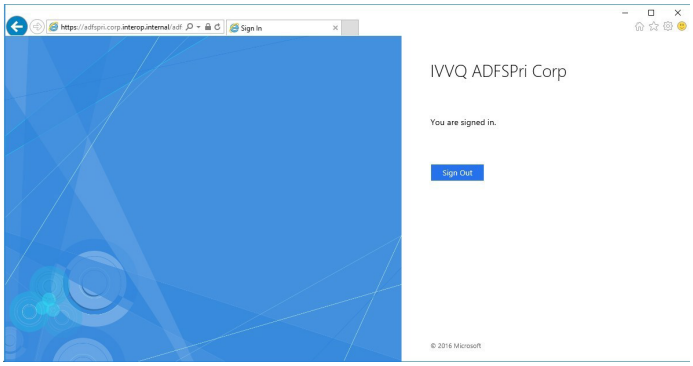
Ensure command prompt or PowerShell is launched as Administrator.

2.14. Check and enable the AD FS install and sign-on page

The AD FS sign-on page is not enabled by default in Windows 2016 and later. To enable and allow verification of a successful installation, open a PowerShell CLI as Administrator and run the following command:

```
PS C:\Users\Administrator.DOMAIN> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
```

1. Open Internet Explorer.
2. Add the AD FS server FQDN to the local intranet zone.
3. Add the web page to Trusted Sites:
    a. Navigate to **Internet Options > Security > Trusted Sites**.
    b. Select **Sites**.
    c. In **Add this website to the zone**, the web site should be populated automatically. Select **Add**.
    d. Select **Close**.
    e. Select **OK** to close the **Internet Options** window.
4. Navigate to https://adfs.domain.com/adfs/ls/idpinitiatedsignon.aspx (substitute your correct FQDN of the AD FS service).
5. You should see the AD FS sign in screen, enter your credentials to sign in AD FS.
6. You should also successfully be able to pull the AD FS configuration XML from https://adfs.domain.com/federationmetadata/2007-06/federationmetadata.xml.



Ensure command prompt or PowerShell is launched as Administrator.

2.15. Configure AD FS to use the nShield HSM

Perform the steps in this section on the AD FS server.

When using AD FS certificates that have keys protected by an HSM, they cannot automatically rollover when nearing expiration. As such, AD FS will not allow you to manually rollover certificates (in this case, from software-based keys to HSM-based keys) without first disabling the AutoCertificateRollover property.

1. On the AD FS server, open a Powershell command prompt as Administrator.
2. Run the following command:

```
> Set-AdfsProperties -AutoCertificateRollover $false
```

The Token-decryption and Token-signing certificates initially created by the AD FS role configuration are software-based and self-signed, and the initial TLS key was generated in software. This steps in this section will add new keys for Token-decryption, Token-signing, and TLS communication created earlier. Which improves the security of the solution.

For keys protected by Softcard or OCS, there should still be a preload session.

Roll the AD FS Certificates from Default Objects to HSM Objects, this can be done manually on the AD FS Management Console.

1. Update the **SSL Certificate** object to use the new HSM-backed certificate/key in a PowerShell window running as Administrator:

For customers that installed the desired end-state SSL certificate during AD FS role configuration, there is no need to roll the SSL cert at this time. Skip to the next step (Service-Communications certificate).

If you intend to use a Web Application Proxy (which is not covered in this guide), you may want to keep the SSL/TLS certificate as a software-protected key. Refer to Microsoft guidance for requirements to configure a Web Application Proxy.

   a. Get the current state of the certificate configuration:

```
Get-AdfsSslCertificate

HostName                  PortNumber     CertificateHash
--------                  ----------     ---------------
adfs.domain.com               443        92E09233FF55F16A661AB417845C04FF3EC8F68E
localhost                     443        92E09233FF55F16A661AB417845C04FF3EC8F68E
certauth.adfs.domain.com      443        92E09233FF55F16A661AB417845C04FF3EC8F68E
```

   b. Locate the certificate thumbprint of the new HSM-backed SSL key (locate the object with the **nCipher Security World Key Storage Provider** and capture its `Cert Hash(sha1)` field for later use:

```
certutil -silent -store my "adfs.domain.com"

Serial Number: 610000000b29ee27dd2a24900c00000000000b
Issuer: CN=DOMAIN ENTERPRISE ROOT CA, DC=domain, DC=com
NotBefore: 9/17/2021 10:06 PM
NotAfter: 9/17/2023 10:16 PM
Subject: CN=adfs.domain.com
Non-root Certificate
Template: ADFSKeys, ADFS Keys
Cert Hash(sha1): 6c4d3d71556303f42d5813d87836757a4a07f2ac
Key Container = tq-ADFSKeys-8ca805b2-5e51-495f-a223-59d6fcf3c4db
Provider = nCipher Security World Key Storage Provider
Encryption test FAILED
```

   c. Set the certificate object to point to the new HSM-backed certificate:

```
Set-AdfsSslCertificate -Thumbprint 6c4d3d71556303f42d5813d87836757a4a07f2ac

WARNING: PS0344: ADFS is configured to use Alternate TLS client binding. This command will not modify
Alternate TLS client binding. If you want to modify Alternate TLS client binding too, please use the
cmdlet 'Set-AdfsAlternateTlsClientBinding'.
```

d. Get the updated state of the certificate configuration - notice how the `certauth` object did not change, and there is a new object at port `49443`:

```
Get-AdfsSslCertificate

HostName                    PortNumber      CertificateHash
--------                    ----------      ---------------
certauth.adfs.domain.com        443         92E09233FF55F16A661AB417845C04FF3EC8F68E
localhost                       443         6C4D3D71556303F42D5813D87836757A4A07F2AC
adfs.domain.com                 443         6C4D3D71556303F42D5813D87836757A4A07F2AC
adfs.domain.com                49443        6C4D3D71556303F42D5813D87836757A4A07F2AC
```

e. To correct the certauth object, update the alternate TLS client binding (ignore the warning):

```
Set-AdfsAlternateTlsClientBinding -Force $true -Member "certauth.adfs.domain.com" -Thumbprint
"6c4d3d71556303f42d5813d87836757a4a07f2ac"

Set-AdfsAlternateTlsClientBinding : PS0317: One or more of AD FS servers returned errors during
execution of command 'Set-AdfsAlternateTlsClientBinding'. Error information: PS0316: AD FS Server:
'certauth.adfs.domain.com', Error: 'Connecting to remote server certauth.adfs.domain.com failed with
the following error message : WinRM cannot process the request. The following error occurred while
using Kerberos authentication: Cannot find the computer certauth.adfs.domain.com. Verify that the
computer exists on the network and that the name provided is spelled correctly.
For more information, see the about_Remote_Troubleshooting Help topic.'.
At line:1 char:1
+ Set-AdfsAlternateTlsClientBinding -force $true -member "certauth.adfs ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     + CategoryInfo          : NotSpecified: (:) [Set-AdfsAlternateTlsClientBinding], RemoteException
     + FullyQualifiedErrorId :
RuntimeException,Microsoft.IdentityServer.Management.Commands.SetAlternateTlsClientBinding
```

f. Get the updated state of the certificate configuration (all the certificate hashes should match now):

```
Get-AdfsSslCertificate

HostName                    PortNumber      CertificateHash
--------                    ----------      ---------------
certauth.adfs.domain.com        443         6C4D3D71556303F42D5813D87836757A4A07F2AC
localhost                       443         6C4D3D71556303F42D5813D87836757A4A07F2AC
adfs.domain.com                 443         6C4D3D71556303F42D5813D87836757A4A07F2AC
adfs.domain.com                49443        6C4D3D71556303F42D5813D87836757A4A07F2AC
```

g. Remove the new addition on port `49443`:

```
netsh http delete sslcert hostnameport=adfs.domain.com:49443
SSL Certificate successfully deleted
```

h. Get the updated state of the certificate configuration (everything should look good now):

```
Get-AdfsSslCertificate
```

```
HostName                    PortNumber      CertificateHash
--------                    ----------      ---------------
certauth.adfs.domain.com         443        6C4D3D71556303F42D5813D87836757A4A07F2AC
localhost                        443        6C4D3D71556303F42D5813D87836757A4A07F2AC
adfs.domain.com                  443        6C4D3D71556303F42D5813D87836757A4A07F2AC
```

2.16. Change the Token-Decrypting Certificate from CNG to CAPI

CAPI certs are only supported with Module Protection during this integration.

Microsoft only supports CAPI for the Token-Decrypt certificate, therefore we must edit it from using CNG to use CAPI:

1. Open a PowerShell as administrator, create a container for the ms capi (ncipher CSP) key:

```
cd "c:\program files\ncipher\nfast\bin"
```

```
keytst -c -m adfstokendecrypt

CSP being used: nCipher Enhanced Cryptographic Provider

Container 'adfstokendecrypt' created
```

2. List all of the containers:

```
csputils -U ALL -m

File ID    Container name       Container owner      DLL name   S X
=========  ===================  ===================  =========  = =
cb551513e  adfstokendecrypt     MACHINE              ncsp

1 container and 0 keys found.
```

3. Find the container you just created by name and go to the left hand column and get the **FILEID** of that container.
4. To find your ADFS Token-Decrypting Key **IDENT** value, for example, key_caping-machine-**IDENT**, run:

```
nfkminfo -l

Keys with module protection:
 key_caping_machine--0e29b54e36c1a2006981a7a8ca6234fd6cf15bed `te-ADFSTLS-dc716c04-87e1-417e-9ec6-
5fb9928de1fc'
 key_caping_machine--2c21df63f288ed189ef4f1e6af9b781ae2c6c031 `te-ADFSTLS-1d0559b1-2759-4645-991c-
```

```
8d7838097e6a'
 key_caping_machine--5d9f162dec839f3e4250af803fb0a81415359ed1 `te-ADFSTLS-9b36d23f-397a-48a2-adc4-
f03888c145d9'
```

The **IDENT** can additionally be located in the generated certificate file name located at C:\ProgramData\nCipher\Key Management Data\local.

5. Now run the following command and type yes if prompted, see the next line for an example:

```
cspimport -i -k machine--IDENT -a caping FILEID exchange
```

6. Now we have the key imported into the CSP container as a machine and exchange key.
7. Move the original ADFS Token-Decrypting Key key-caping-machine out of C:\ProgramData\nCipher\Key Management Data\local or else it will continue to use CNG. The new CAPI container and cloned key should remain in local.
8. Run the following command:

```
 certutil -store my

================ Certificate 3 ================
Serial Number: 18000000047adbec8d4cc951f5000000000004
Issuer: CN=ADFSWIN2022-3, DC=interop, DC=local
 NotBefore: 7/30/2024 8:26 AM
 NotAfter: 7/30/2026 8:26 AM
Subject: CN=ADFS Token-Decrypting Key
Non-root Certificate
Template: ADFSTLS, ADFS TLS
Cert Hash(sha1): 03a19f17154193a70231c19dcdf64f91c496cf8e
  Key Container = te-ADFSTLS-d223bf5d-ab52-4753-a401-06f82de95711
  Provider = nCipher Security World Key Storage Provider
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
CertUtil: -store command completed successfully.
```

9. Get the signing cert Serial Number from the above command and use it in the next command.

```
certutil -f -repairstore -csp "nCipher Enhanced Cryptographic Provider" my
"18000000047adbec8d4cc951f5000000000004"

. my "Personal"
================ Certificate 3 ================
Serial Number: 18000000047adbec8d4cc951f5000000000004
Issuer: CN=ADFSWIN2022-3, DC=interop, DC=local
 NotBefore: 7/30/2024 8:26 AM
 NotAfter: 7/30/2026 8:26 AM
Subject: CN=ADFS Token-Decrypting Key
Non-root Certificate
Template: ADFSTLS, ADFS TLS
```

```
Cert Hash(sha1): 03a19f17154193a70231c19dcdf64f91c496cf8e
cbData: 14 ==> 40
  Key Container = adfstokensign
  Provider = nCipher Enhanced Cryptographic Provider
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
nCipher Enhanced Cryptographic Provider: KeySpec=1
AES256+RSAES_OAEP(RSA:AT_KEYEXCHANGE) test passed
================ Begin force NCrypt ================
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
nCipher Security World Key Storage Provider: KeySpec=0
AES256+RSAES_OAEP(RSA:CNG) test passed
----------------  End force NCrypt  ----------------
CertUtil: -repairstore command completed successfully.
```

10. Now the ADFS Decrypting Certificate is linked to the key in the MS CAPI nCipher provider.
11. For the Decryption Certificate you should see **"Provider = nCipher Enhanced Cryptographic Provider"** when you run the below command:

```
certutil -store my
```

2.17. Add HSM protected certificates to the AD FS server

1. Navigate to **Start > Windows Administrative Tools > AD FS Management**.
2. Expand the **ADFS** folder and navigate to **Service > Certificates**.
3. Update the **Service-Communications** object to use the new HSM-backed certificate/key:
    a. Right-click on **Certificates** and select **Set Service Communication Certificate**.
    b. In the **Select a service communication certificate** screen, select **More Choices** and select the newly created HSM-based TLS certificate. You may have named it as **AD FS TLS HSM Key**.
    c. A dialog appears if the AD FS cannot determine the keyspec of the key. Select **OK**.
    d. A warning will pop up advising you to make sure the private key is accessible for each AD FS server, select **OK**.

All AD FS services in the cluster must contain the same keys/certificates, so you will need to copy the HSM key(s) to other AD FS systems in the cluster, restore their CNG linkage, and configure AD FS with those

key(s). The procedures for performing this are not in scope of this *Integration Guide*.

e. The new certificate should be visible in the middle pane; you can double-click on the certificate to view its properties.

4. Update the **Token-Decrypting** object to use the new HSM-backed certificate/key:
   a. Right-click on **Certificates** and select **Add Token-Decrypting Certificate**.
   b. In the **Select a token-decrypting certificate** screen, select **More Choices** and select the newly created HSM-based token-decrypting certificate and select **OK** You may have named it as **AD FS Token-Decrypting HSM Key**.
   c. A dialog appears if the AD FS cannot determine the keyspec of the key. Select **OK**.
   d. A warning will pop up advising you to make sure the private key is accessible for each AD FS server, select **OK**.

All AD FS services in the cluster must contain the same keys/certificates, so you will need to copy the HSM key(s) to other AD FS systems in the cluster, restore their CNG linkage, and configure AD FS with those key(s). The procedures for performing this are not in scope of this *Integration Guide*.

   e. The new certificate should be visible in the middle pane; you can double-click on the certificate to view its properties.
   f. In the middle pane, right-click on the new HSM token-decrypting certificate and select **Set as Primary**.
   g. Do NOT delete the original certificate (yet), which should now be marked as Secondary.

5. Update the **Token-Signing** object to use the new HSM-backed certificate/key:
   a. Right-click on **Certificates** and select **Add Token-Signing Certificate**.
   b. In the **Select a token-signing certificate** screen, select **More Choices** and select the newly created HSM-based token-signing certificate and select **OK**. You may have named this as **AD FS Token-Signing HSM Key**.
   c. A dialog appears if the AD FS cannot determine the keyspec of the key. Select **OK**.
   d. A warning will pop up advising you to make sure the private key is accessible for each AD FS server, select **OK**.

All AD FS services in the cluster must contain the same keys/certificates, so you will need to copy the HSM key(s) to other AD FS systems in the cluster, restore their CNG linkage, and configure AD FS with those key(s). The procedures for performing this are not in scope of this *Integration Guide*.

e. The new certificate should be visible in the middle pane; you can double-click on the certificate to view its properties.

f. In the middle pane, right-click on the new HSM token-signing certificate and select **Set as Primary**.

g. When warned about setting this certificate as primary, select **Yes**.

Setting a new token-signing certificate as primary could break trust relationships with relying parties that do not yet have the certificate. If this is an existing AD FS infrastructure, make sure you coordinate this activity prior to performing this step.

h. Do NOT delete the original certificate (yet), which should now be marked as Secondary.

6. Close the AD FS Management Console.

At this point, restart the AD FS Service:

1. Stop the AD FS service:

```
net stop adfssrv
```

2. If `preload` is still running in `pause` mode in another window, go back to that window and use `[CTRL]-[C]` to break the pause and return to the command prompt.
3. Clear the preload state:

```
preload exit
```

4. Remove the `NFAST_NFKM_TOKENSFILE` cache:

```
del c:\nfast_nfkm_tokensfile
```

5. Verify the preload cache is clear:

```
nfkminfo -p

<...snip all but last line...>

No Pre-Loaded Objects
```

To restart AD FS, refer to the chosen HSM Key protection mechanism below for instructions:

1. For module protected HSM Keys:
   a. Stop the AD FS service via the command prompt as follows:

   ```
   net stop adfssrv
   ```

   b. Start the AD FS service via the command prompt as follows:

   ```
   net start adfssrv
   ```

2. For Softcard protected HSM Keys:
   a. Stop the AD FS service via command prompt as follows:

   ```
   net stop adfssrv

   preload exit

   del c:\nfast_nfkm_tokensfile
   ```

   b. Start the AD FS service via command prompt as follows:

   ```
   preload --reload-everything --softcard-name=<Softcard name> net start adfssrv
   ```

3. For OCS protected HSM Keys:
   a. Stop the AD FS service via the command prompt as follows:

   ```
   net stop adfssrv

   preload exit

   del c:\nfast_nfkm_tokensfile
   ```

   b. Start the AD FS service via command prompt as follows:

   ```
   preload --reload-everything --cardset-name=<OCS Name> net start adfssrv
   ```

Ensure command prompt or PowerShell is launched as

> Administrator.

2.18. Test AD FS

Sign in to the AD FS web page (in the integration steps we used https://adfs.domain.com/adfs/ls/idpinitiatedsignon.aspx to ensure the service is working properly. The sign-in process should be successful.

Chapter 3. Troubleshooting

3.1. General AD FS service issues

1. Open a PowerShell window and execute the following command(s):

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -force
Install-Module -Name ADFSToolbox -force
Import-Module ADFSToolbox -force
Export-AdfsDiagnosticsFile -ServerNames @("adfs.domain.com")
```

2. Navigate to https://adfshelp.microsoft.com/diagnosticsanalyzer/Analyze.
3. Upload the resulting JSON from the `Export-AdfsDiagnosticsFile` command and analyze the results.

3.2. Issues with AD FS service startup

- If you are using `preload` to start AD FS, the `NFAST_NFKM_TOKENSFILE` system environment variable must have been previously configured or AD FS will not start/work properly.
- If you receive the following error when performing any HSM operation (including AD FS service start), then the `NFAST_NFKM_TOKENSFILE` (`c:\nfast_nfkm_tokensfile`) has gone stale from not cleaning up properly:

```
HH:MM:SS WARNING: NFastApp_Connect failed: ClientUnknown
error setting application: ClientUnknown
```

  Make sure any services that were using preload have been stopped, delete the file referenced in `NFAST_NFKM_TOKENSFILE` and try running the HSM command again.

  To avoid seeing this error, make sure you run `preload exit` after stopping the service using the preloaded HSM keys.

3.3. Permissions for the AD FS TLS key

1. Stop the AD FS service.
2. Run the preload command from the previous section for your particular HSM configuration but use preload with `pause` instead of `net start adfssrv`.

3. Navigate to **Start > Run**, enter `certlm.msc`, then select **OK**.
4. Expand **Certificates - Local Computer > Personal > Certificates**.
5. Right-click on the AD FS TLS key generated on the HSM and navigate to **All Tasks > Manage Private Keys**.
6. In the **Permissions** for screen, select **Add**.
7. Select **Object Types** and then check the boxes for **Service Accounts** and **Computers** from the listed objects.
8. Select **OK**.
9. For **Enter the object names to select**, type in full/partial names for (separated by semicolons). That is, the Group Managed Service Account you created on your domain controller, and the AD FS server computer account(s).
10. Select **Check Names** to auto-complete (you may need to select **Advanced** to narrow down your search in large domains).
11. Select **OK**.
12. Back in the **Permissions for** window, for each added account/computer ensure that **Full control** and **Read** are both checked in the **Allow** column.
13. Select **OK** to close the **Permissions for** window.
14. Close the **Certificates - Local Computer** window.
15. Cancel the preload window with `[CTRL]+[C]`.
16. Delete the `c:\nfast_nfkm_tokensfile`.
17. Resume whatever you were doing before.

Chapter 4. Additional resources and related products

4.1. nShield Connect

4.2. nShield as a Service

4.3. nShield Edge

4.4. Entrust digital security solutions

4.5. nShield product documentation