



# Single Sign On



# Contents

<b>Chapter 1: Overview</b>	<b>1</b>
Overview of Single Sign-On	2
SSO Workflow	2
<b>Chapter 2: Set up GE Digital APM SSO</b>	<b>3</b>
About Setting Up GE Digital APM SSO	4
Configure Azure Active Directory as the Identity Provider (IDP)	4
Configure Identity Provider (IDP) on Active Directory	9
<b>Chapter 3: Enable SSO</b>	<b>43</b>
About Enabling GE Digital APM SSO	44
About Host Names	44
Enable SSO On Site Authentication Using Active Directory	44
Enable SSO Off-Site Authentication Using GE Digital APM Server Setup	44
<b>Chapter 4: Configure GE Digital APM Server</b>	<b>47</b>
Configure GE Digital APM Server	48

# Copyright GE Digital

© 2020 General Electric Company.

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of and/or its suppliers or vendors. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.



# Chapter 1

---

## Overview

### Topics:

- [Overview of Single Sign-On](#)
- [SSO Workflow](#)

## Overview of Single Sign-On

SSO is a process that allows pre-authenticated users to access GE Digital APM, without having to re-enter their credentials.

The GE Digital APM user logs on initially using a form-based enterprise login screen. SSO is a common procedure in enterprises, where a user logs in once and gains access to different applications without the need to re-enter log-in credentials at each application. SSO authentication facilitates seamless network resource usage. SSO mechanisms vary, depending on application type.

SSO advantages include:

- Eliminates credential re-authentication.
- Streamlines local and remote application and desktop workflow.
- Minimizes phishing.
- Improves compliance through a centralized database.
- Provides detailed user access reporting.

GE Digital APM supports the following types of authentication for SSO:

- **Pass-through authentication**  
Enables the users to enter their Windows credentials in the GE Digital APM login page and GE Digital APM validates the credentials against Active Directory.
- **Security Assertion Markup Language (SAML) authentication**  
Enables the users to navigate to the SSO URL (hosted on the APM Application Server) that redirects the browser to a preconfigured URL (not hosted on the APM Application Server), which is the Identity Provider (IDP). If there are multiple databases, and when the user selects a database, the user account is then authenticated and the IDP provides the web browser a token through a cookie. If the token is valid, the user can access GE Digital APM.

## SSO Workflow

This workflow provides the basic, high-level steps for using this module. The steps and links provided in the workflow do not necessarily reference every possible procedure.

### Procedure

1. [Set up GE Digital APM SSO by configuring an identity provider.](#)
2. [Enable SSO on-site or off-site authentication.](#)
3. [Configure the GE Digital APM server.](#)

# Chapter 2

---

## Set up GE Digital APM SSO

### Topics:

- [About Setting Up GE Digital APM SSO](#)
- [Configure Azure Active Directory as the Identity Provider \(IDP\)](#)
- [Configure Identity Provider \(IDP\) on Active Directory](#)

# About Setting Up GE Digital APM SSO

## About Setting up GE Digital APM SSO

To set up GE Digital APM SSO, perform one of the following tasks:

- [Configure Azure Active Directory as the Identity Provider \(IDP\)](#)
- [Configure IDP on Active Directory](#)

## Configure Azure Active Directory as the Identity Provider (IDP)

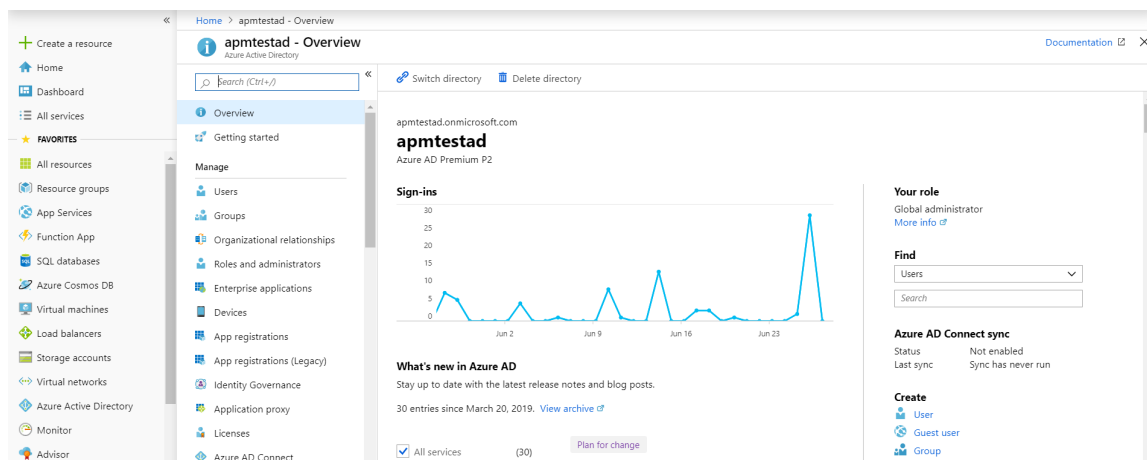
### Configure Azure Active Directory as the Identity Provider (IDP)

#### Before You Begin

You must have an Azure Active Directory (Azure AD) instance.

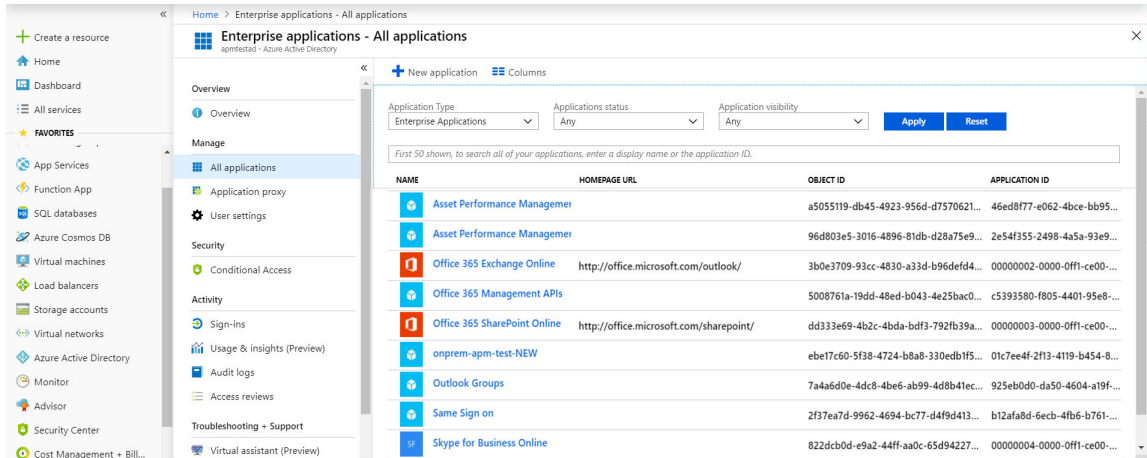
#### Procedure

1. Sign in to the Azure portal.

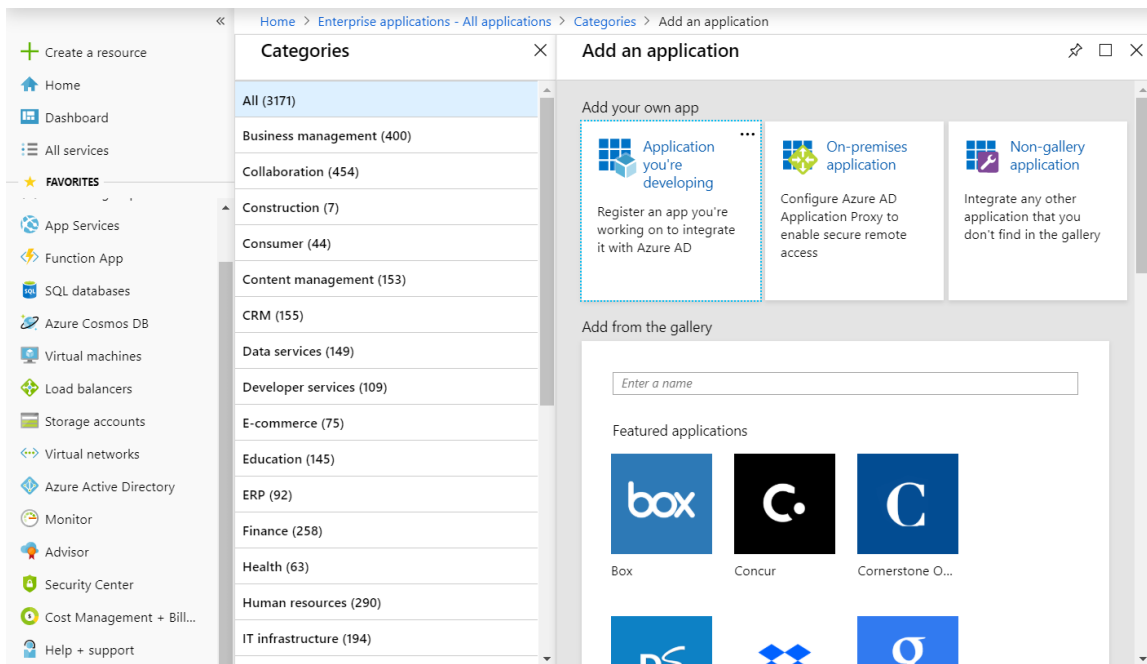


2. In the navigation pane, select **Azure Active Directory**, and then select **Enterprise applications**. The **Enterprise applications - All applications** page appears.

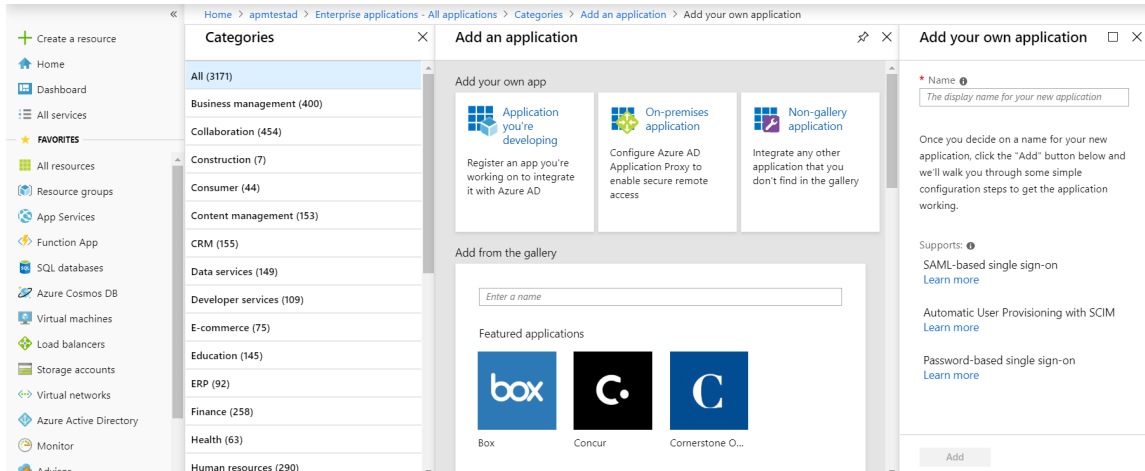




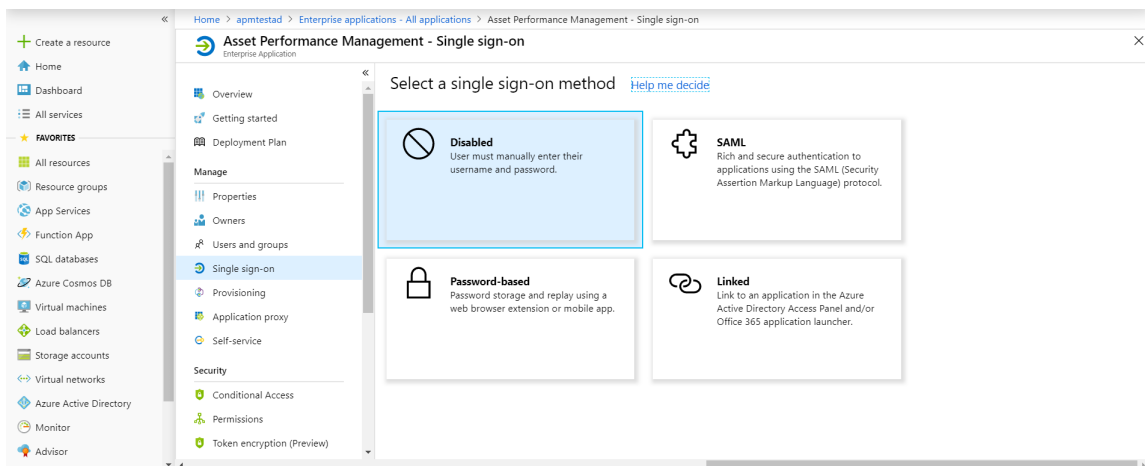
3. Select **New application**.  
The **Add an application** section appears.



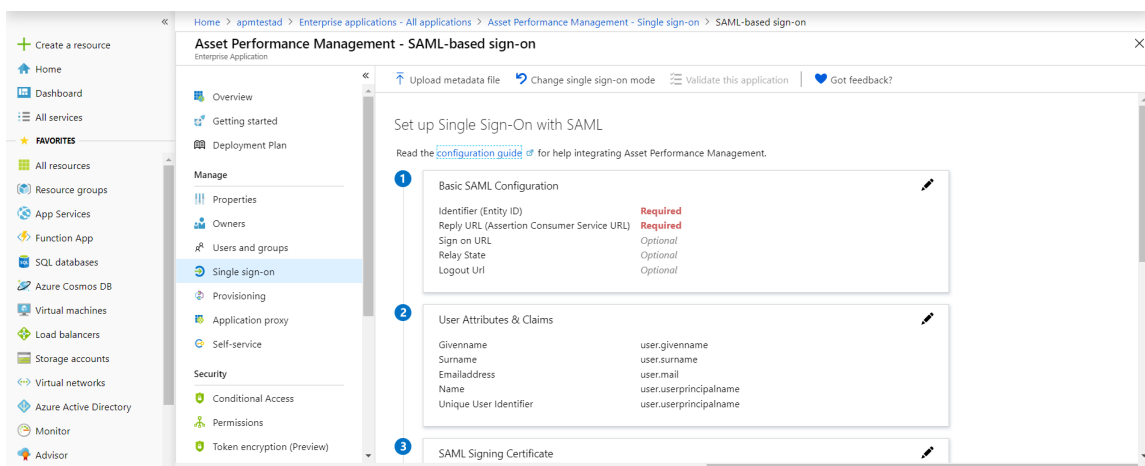
4. Select **Non-gallery application**.  
The **Add your own application** section appears.



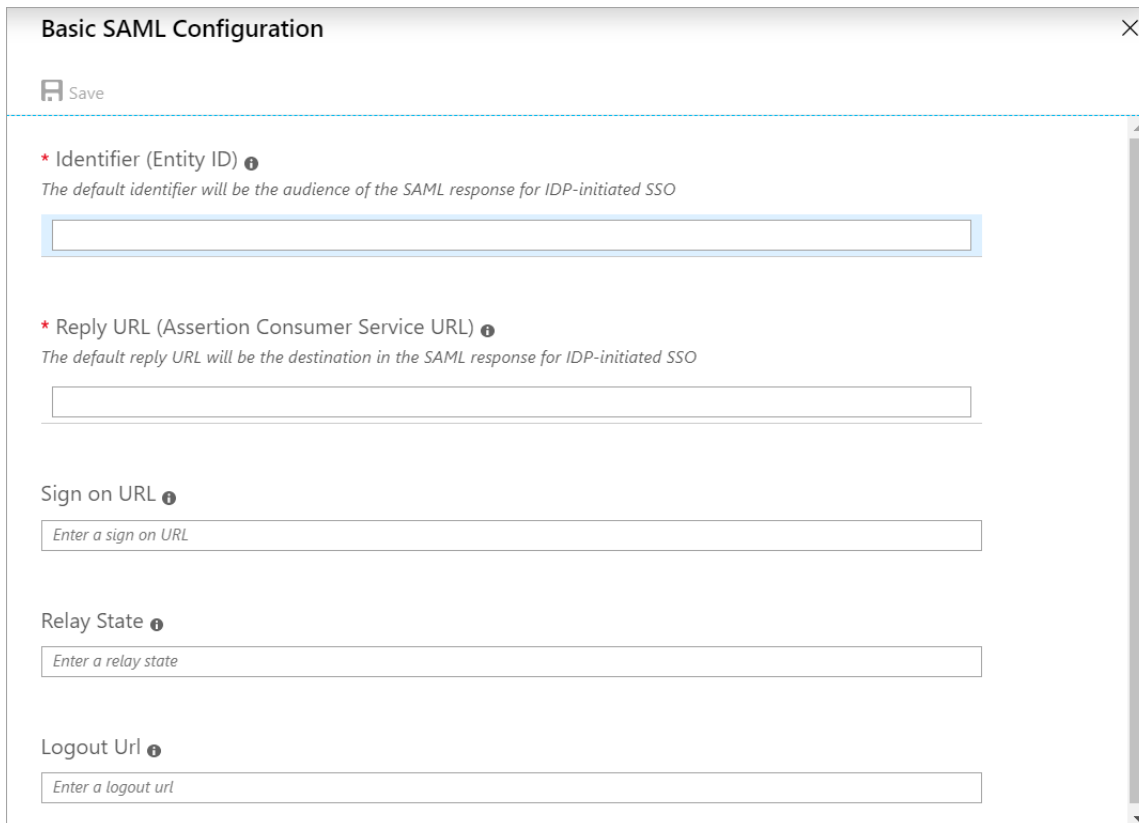
- In the **Name** box, enter a name for the application that you want to configure with Azure AD, and then select **Add**.  
The page of the added application appears.
- In the navigation pane of the application page, select **Single sign-on**.  
The **Select a single sign-on method** section appears.



- Select **SAML**.  
The **Set up Single Sign-On with SAML** section appears.



- In the **Basic SAML Configuration** section, select  .  
The **Basic SAML Configuration** window appears.



- Enter the following details.

<b>Identifier (Entity ID)</b>	Enter a unique ID. <b>Note:</b> This ID will be used in the <code>saml.json</code> file for the service provider name. Therefore, note the ID.
<b>Reply URL (Assertion Consumer Service URL)</b>	The application callback URL where the response will be posted. Enter the URL in the following format: <code>https://&lt;GE Digital APM Server Name&gt;/Meridium/api/core/security/ssologinauth</code> , where <code>&lt;GE Digital APM Server Name&gt;</code> is the name of the GE Digital APM server.
<b>Sign on URL</b>	The application URL, which initiates the same sign-on. Enter the URL in the following format: <code>https://&lt;GE Digital APM Server Name&gt;/meridium/index.html</code> , where <code>&lt;GE Digital APM Server Name&gt;</code> is the name of the GE Digital APM server.

- Select **Save**.
- In the **SAML Signing Certificate** section, select **Download** corresponding to Certificate (Base 64).
- From the **Set up <user name>- sso** section, note the Login URL and Azure AD Identifier.  
**Note:** The Login URL and Azure AD Identifier will be used in the `saml.json` file for `SingleSignOnServiceURL` and `PartnerIdentityProvider` name, respectively.
- In the application server, copy the downloaded Certificate (Base 64) to `C:\Program Files\Meridium\ApplicationServer\api`.

14. Modify the `saml.json` file as follows:

- `LocalServiceProviderConfiguration Name` with the value that you entered and noted for the **Identifier (Entity ID)** box.
- `PartnerIdentityProviderConfigurations Name` with the Azure AD Identifier.
- `SingleSignOnServiceUrl` with the Login URL.
- `AssertionConsumerServiceUrl` with the URL that you entered in the **Reply URL (Assertion Consumer Service URL)** box.

```
{
  "SAML": {
    "$schema": "https://www.componentSpace.com/schemas/saml-
config-schema-v1.0.json",
    "Configurations": [
      {
        "LocalServiceProviderConfiguration": {
          "Name": "sdsso",
          "AssertionConsumerServiceUrl": "https://<GE
Digital APM Server Name>/Meridium/api/core/security/ssologinauth",
          "LocalCertificates": [
            {
              "FileName": "sp.pfx",
              "Password": "password"
            }
          ]
        },
        "PartnerIdentityProviderConfigurations": [
          {
            "Name": "https://sts.windows.net/78dd76d6-
f3b7-4b89-9efc-ef8d5483b7ea/",
            "Description": "Azure AD",
            "SignAuthnRequest": true,
            "WantSamlResponseSigned": false,
            "WantAssertionSigned": true,
            "WantAssertionEncrypted": false,
            "UseEmbeddedCertificate": true,
            "SingleSignOnServiceUrl": "https://
login.microsoftonline.com/78dd76d6-f3b7-4b89-9efc-ef8d5483b7ea/
saml2",
            "DigestAlgorithm": "http://www.w3.org/
2001/04/xmlenc#sha256",
            "SignatureAlgorithm": "http://www.w3.org/
2001/04/xmldsig-more#rsa-sha256",
            "PartnerCertificates": [
              {
                "FileName": "sdsso.cer"
              }
            ]
          }
        ]
      }
    ]
  }
}
```

15. Add users to the enterprise application by accessing the **Users and groups** section.

16. Modify the host page with the IDP URL.

## Next Steps

- [Enable SSO](#)

# Configure Identity Provider (IDP) on Active Directory

## About Configuring Identity Provider (IDP) on Active Directory

### About This Task

You must configure IDP on Active Directory using the Active Directory Federation System (AD FS) Management Console.

**Note:** The strings and the URLs in AD FS are case-sensitive.

To configure IDP on Active Directory, you must perform the following tasks:

### Procedure

1. [Add Relying Party Trusts](#) on page 9
2. [Add Claim Rules](#) on page 20
3. [Add Certificates](#) on page 26

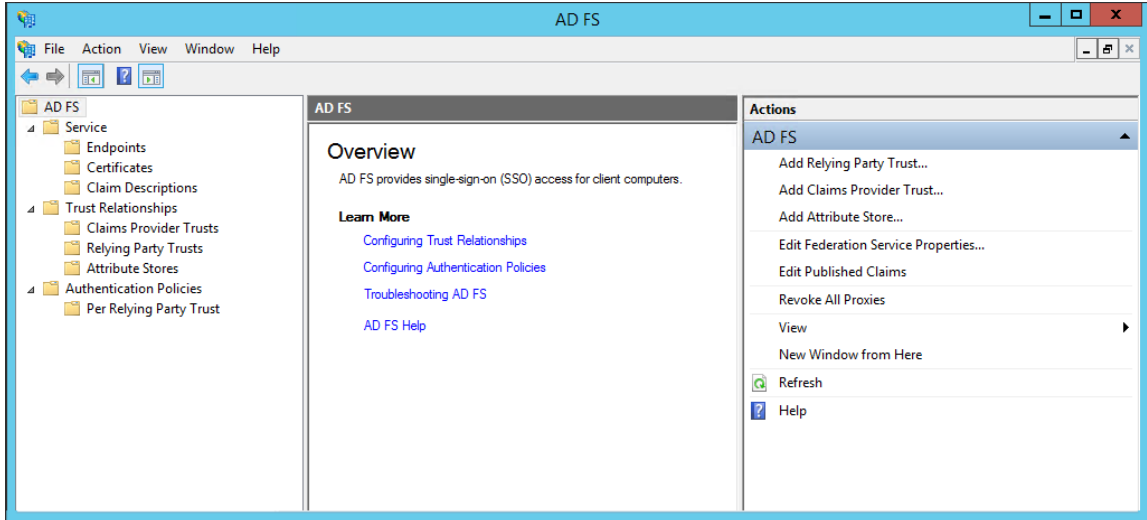
## Add Relying Party Trusts

### Before You Begin

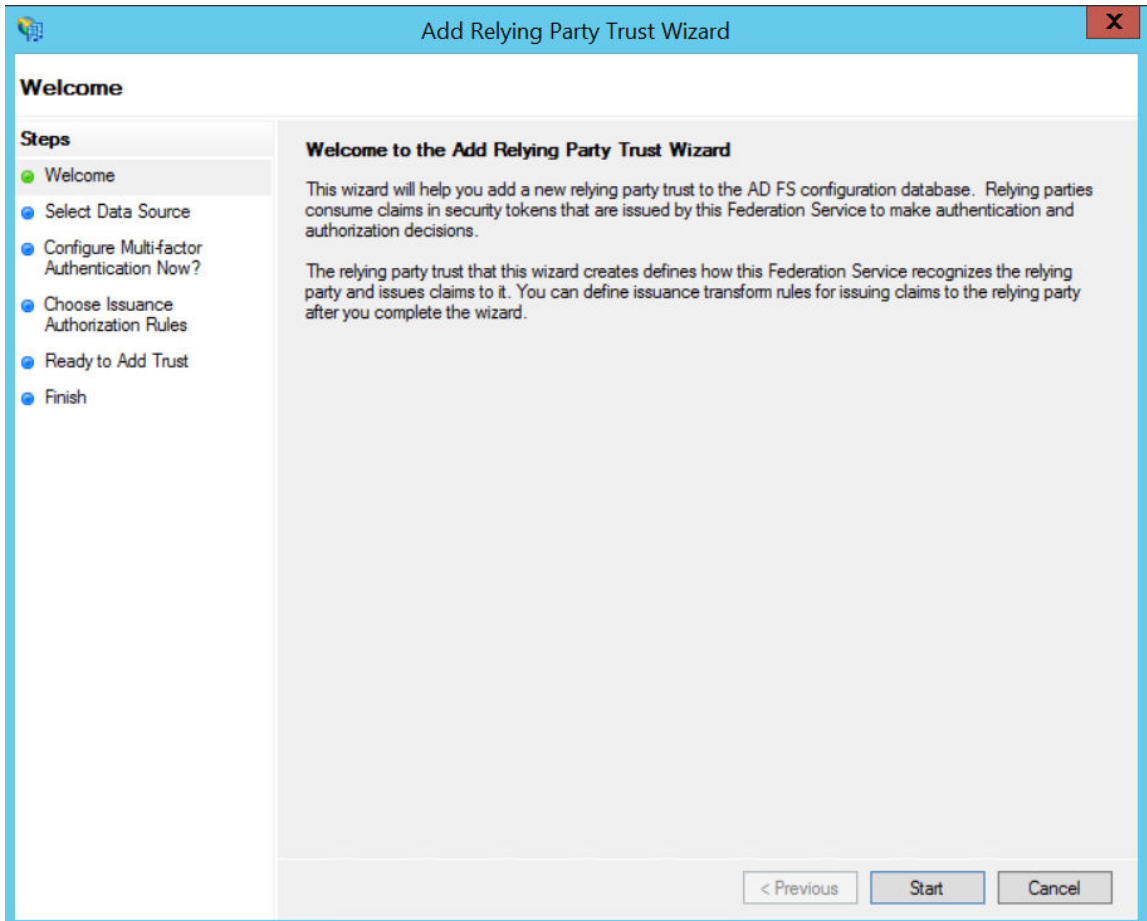
- You must have administrative privileges to configure AD FS.
- Ensure that the /ads/ls endpoint exists for SAML v2.0.  
**Note:** To add ads/ls endpoint, refer to the AD FS documentation.
- Ensure that the token encrypting certificates exist.

### Procedure

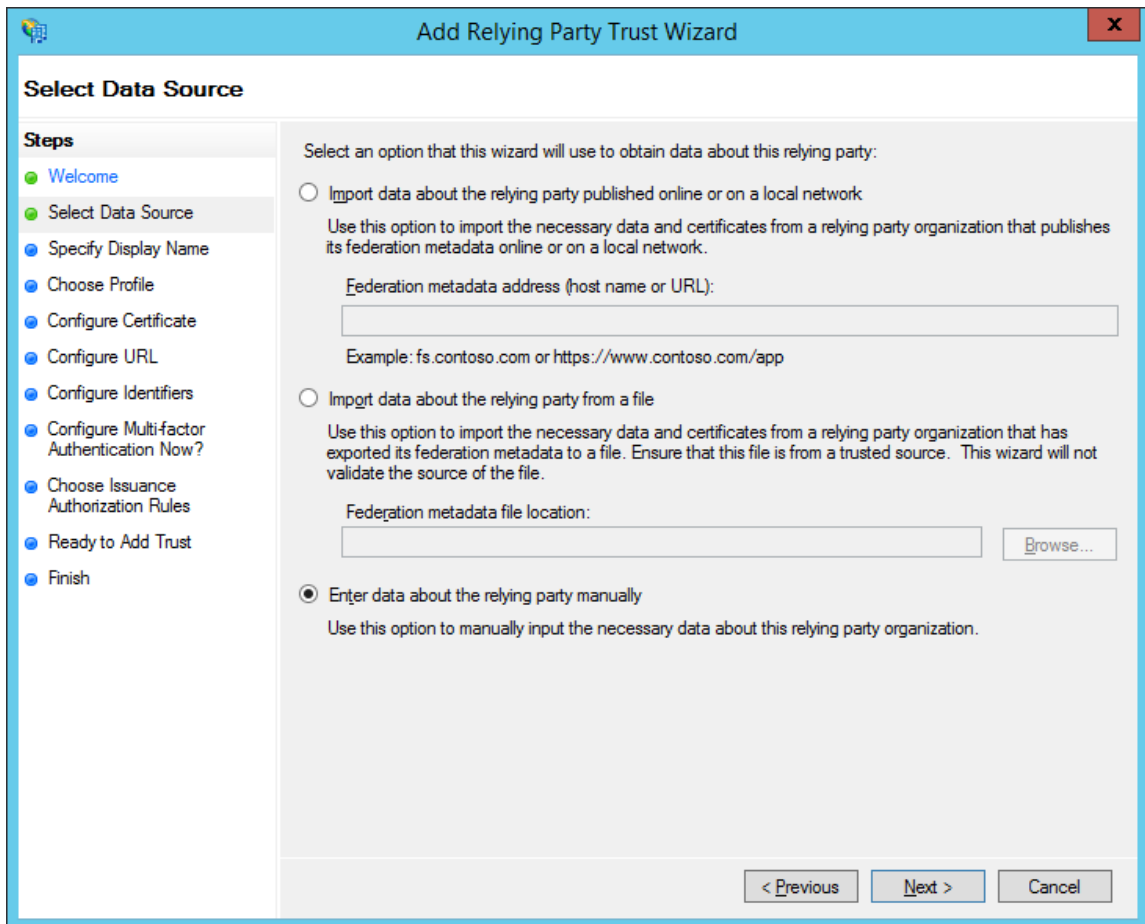
1. Access **Control Panel**, then select **System and Security**, and then select **Administrative Tools**.
2. Select **AD FS Management**.  
The **AD FS** window appears.



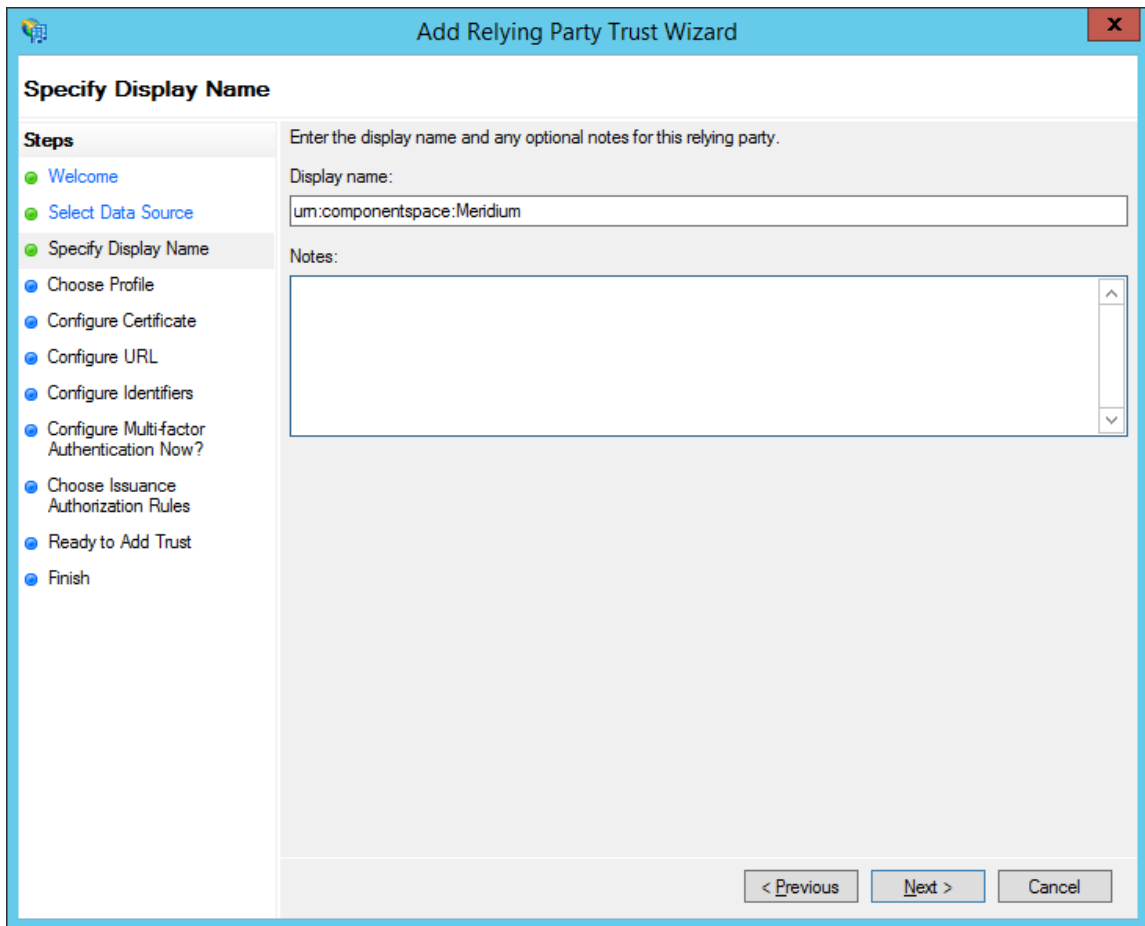
3. In the **Actions** section, select **Add Relying Party Trust**.  
The **Add Relying Party Trust Wizard** appears.



4. Select **Start**.  
The **Select Data Source** page appears.

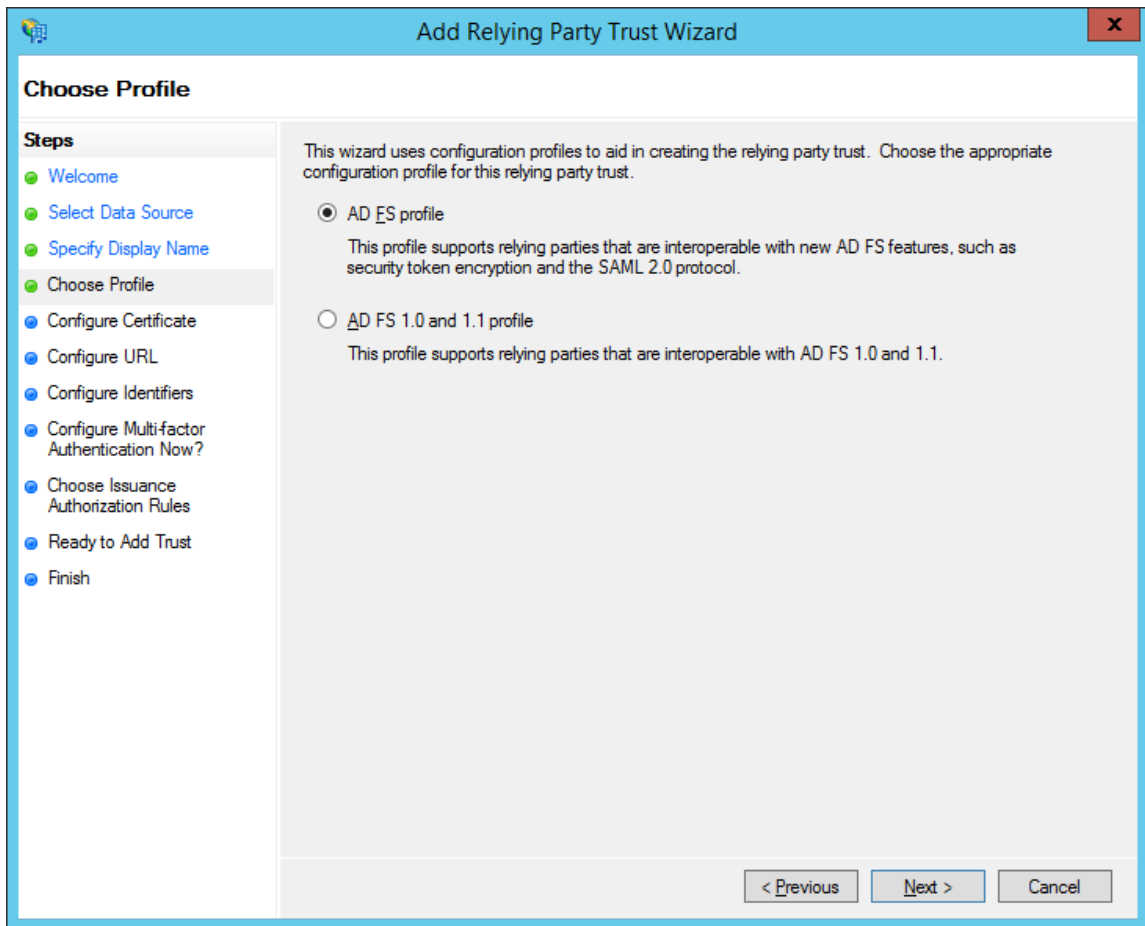


5. Select **Enter data about relying party manually**, and then select **Next**. The **Specify Display Name** page appears.

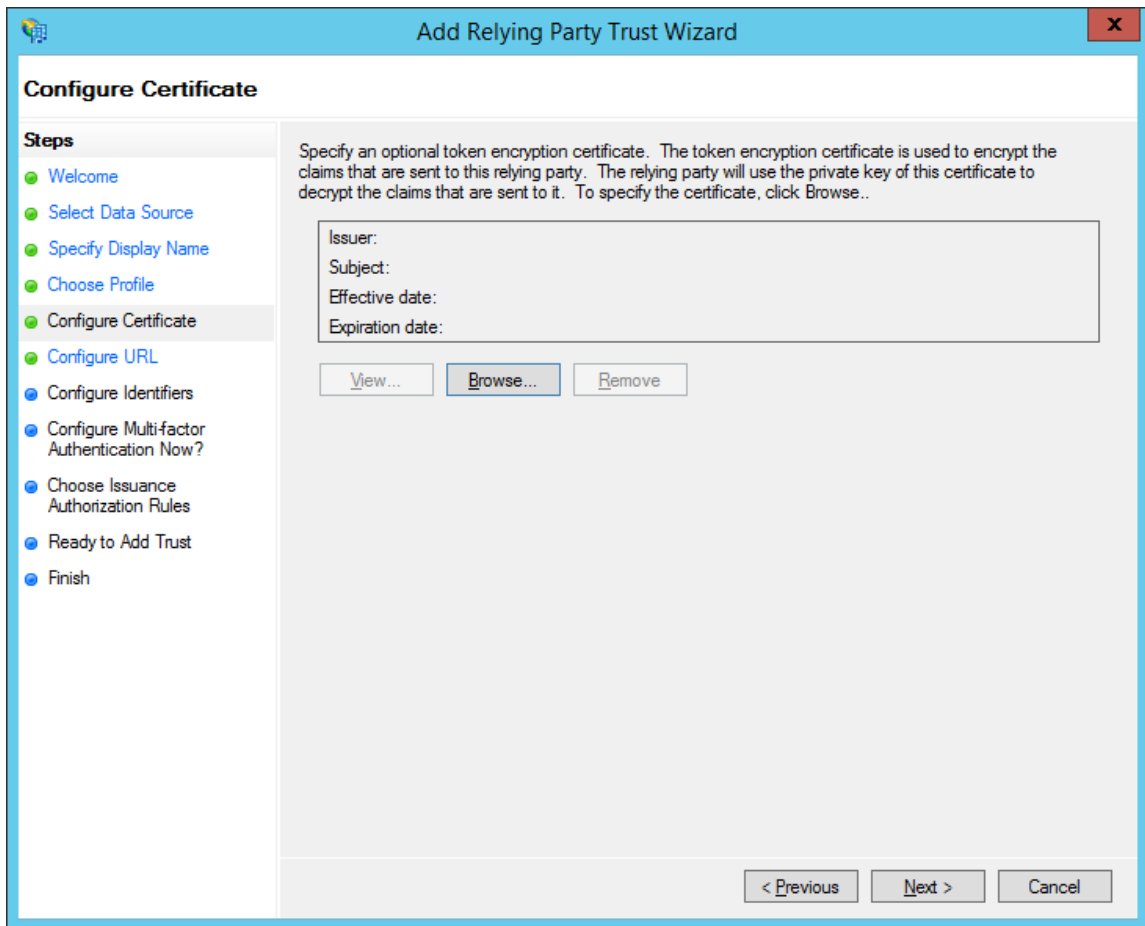


6. In the **Display name** box, enter **urn:componentspace:Meridium**, and then select **Next**. The **Choose Profile** page appears.

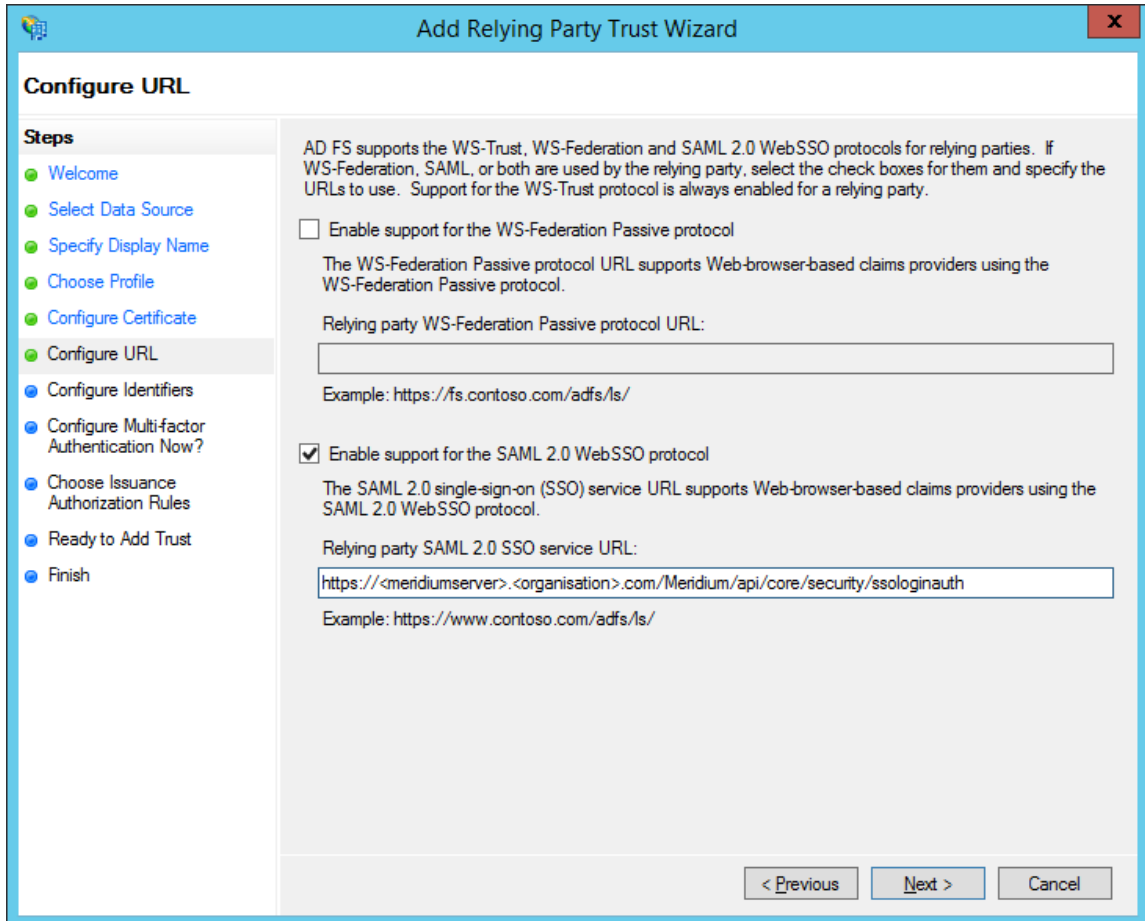




7. Select the **AD FS profile** option, and then select **Next**. The **Configure Certificate** page appears.



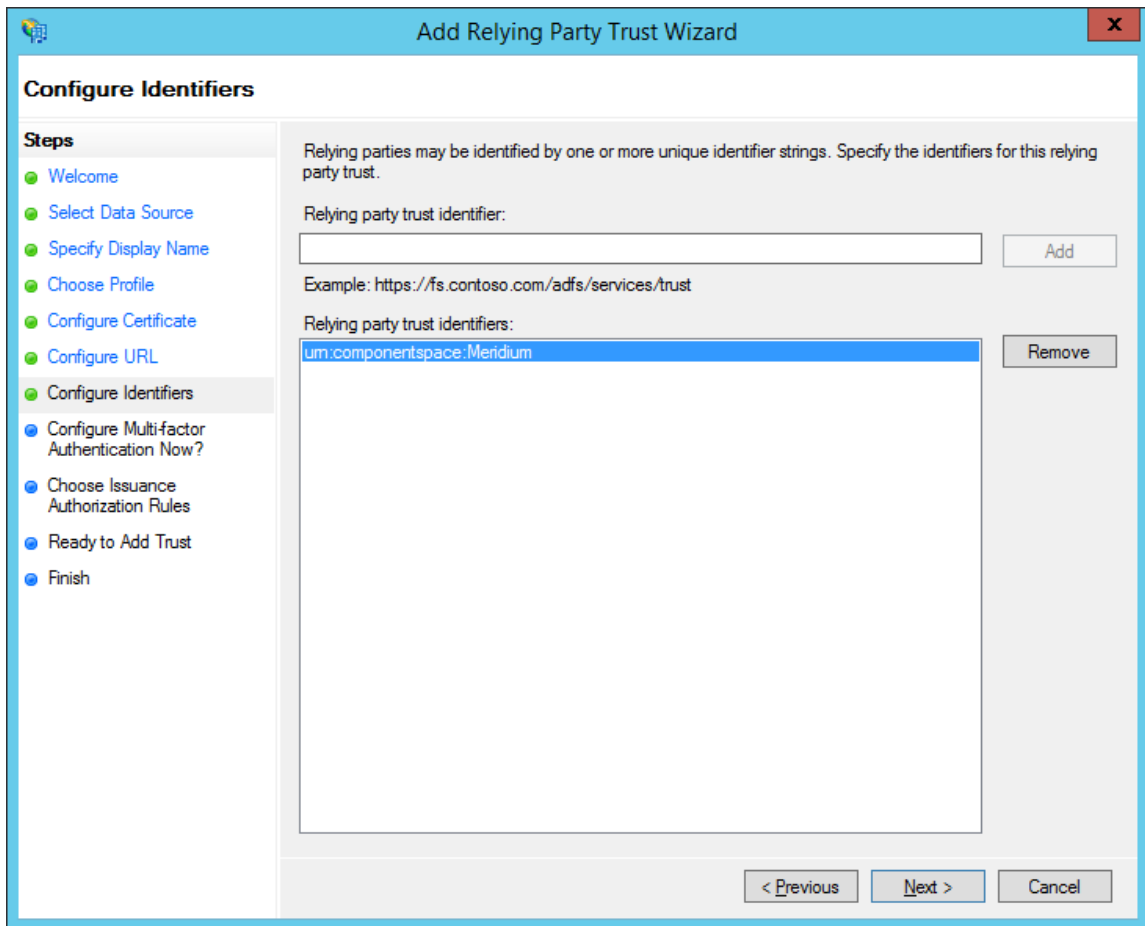
8. Select **Next**.  
The **Configure URL** page appears.



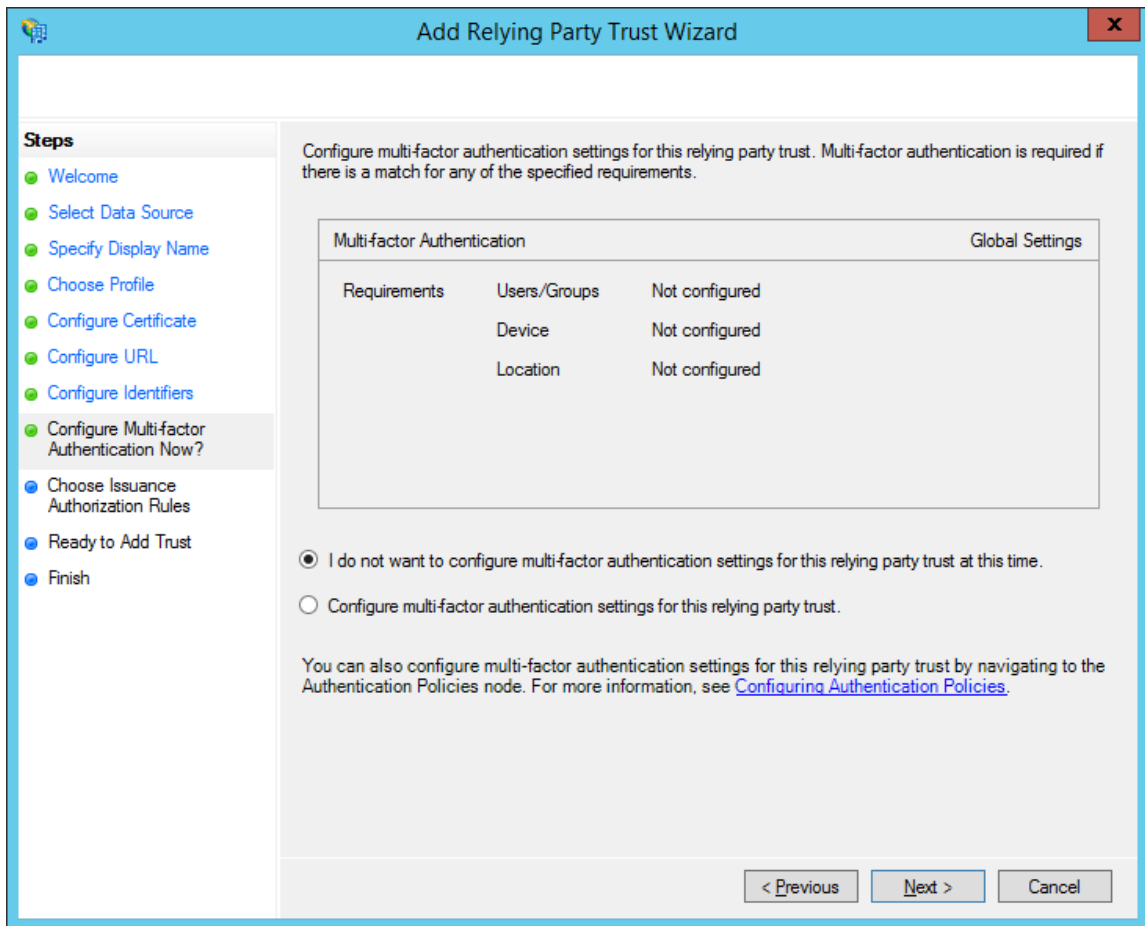
9. Select the **Enable Support for the SAML 2.0 WebSSO protocol** check box.
10. In the **Relying Party SAML 2.0 SSO service URL** box, enter `https://<GE Digital APM Server Name>/Meridium/api/core/security/ssologinauth`, and then select **Next**.

**Note:** The word Meridium is case-sensitive. Therefore, ensure that the first letter of the word is capitalized. Also, the URL must be same as the URL in the `saml.json` file.

The **Configure Identifiers** page appears.

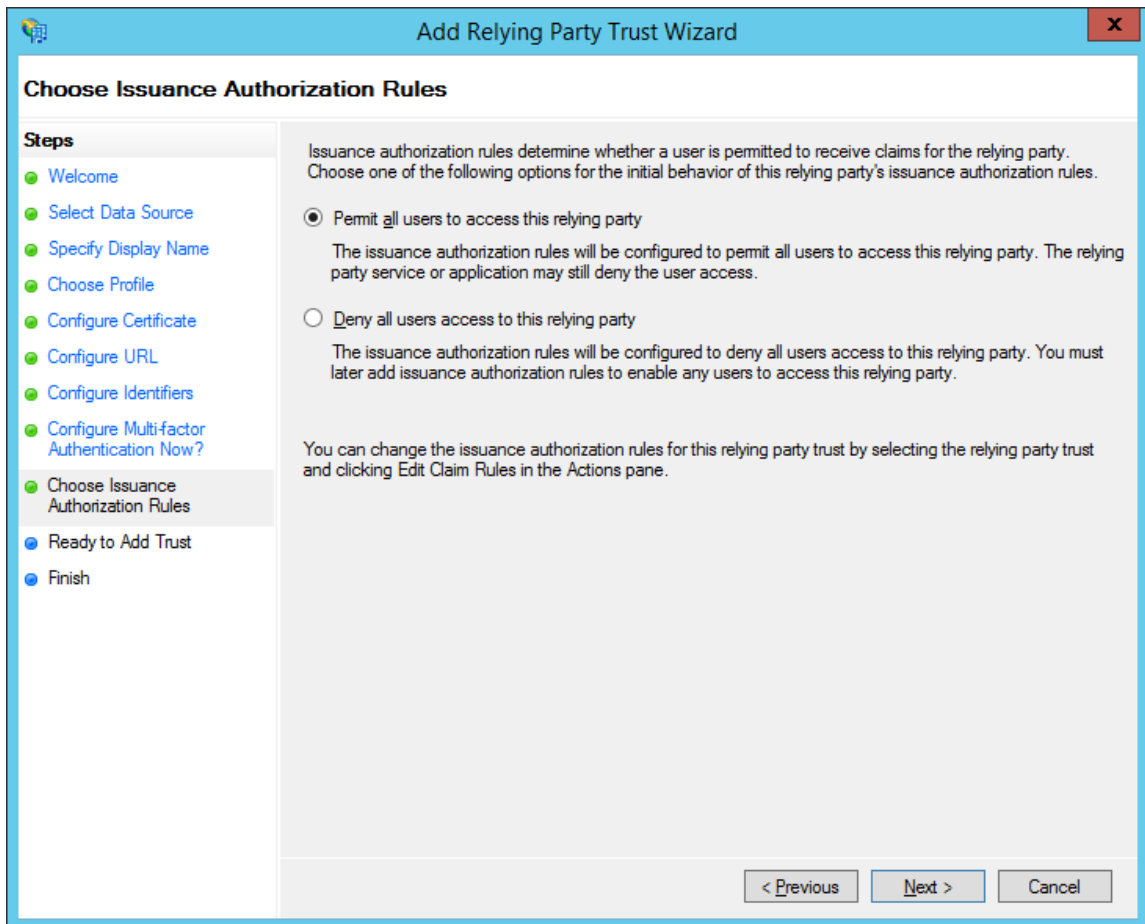


11. In the **Relying party trust identifier** box, enter `urn:componentSpace:Meridium`, then select **Add**, and then select **Next**.  
The **Configure Multi-factor Authentication Now** page appears.

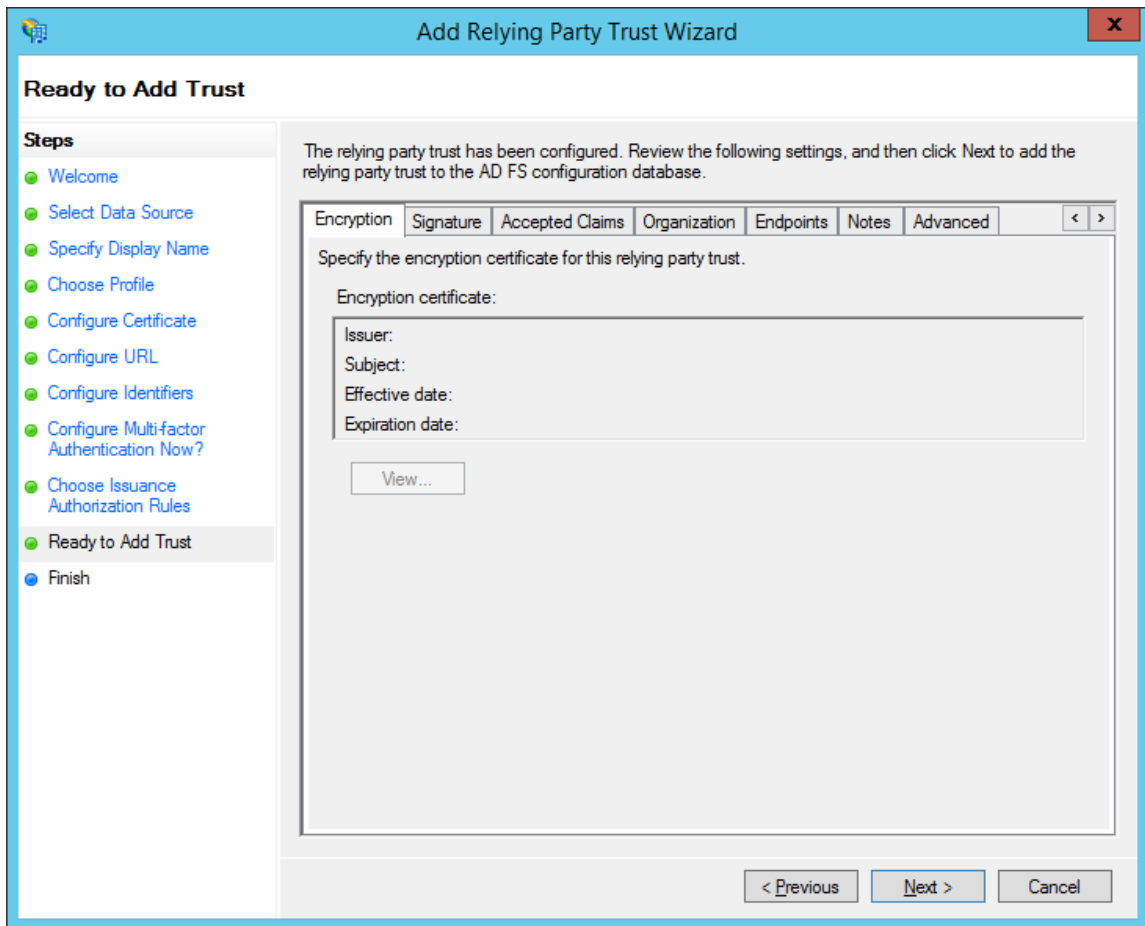


12. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, and then select **Next**.

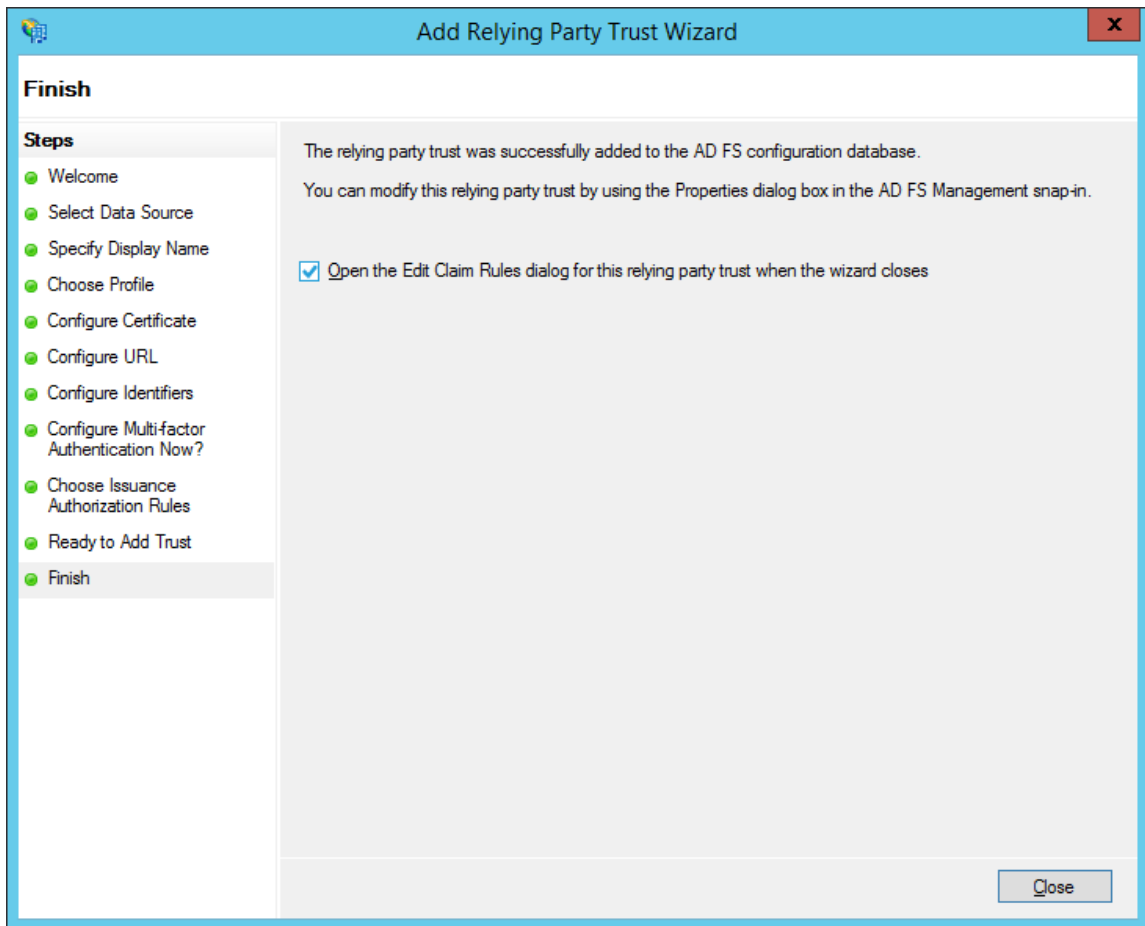
The **Choose Issuance Authorization Rules** page appears.



13. Select **Permit all users to access this relying party**, and then select **Next**. The **Ready to Add Trust** page appears.



14. Select **Next**.  
The **Finish** page appears.



15. Clear the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box, and then select **Close**.

### Next Steps

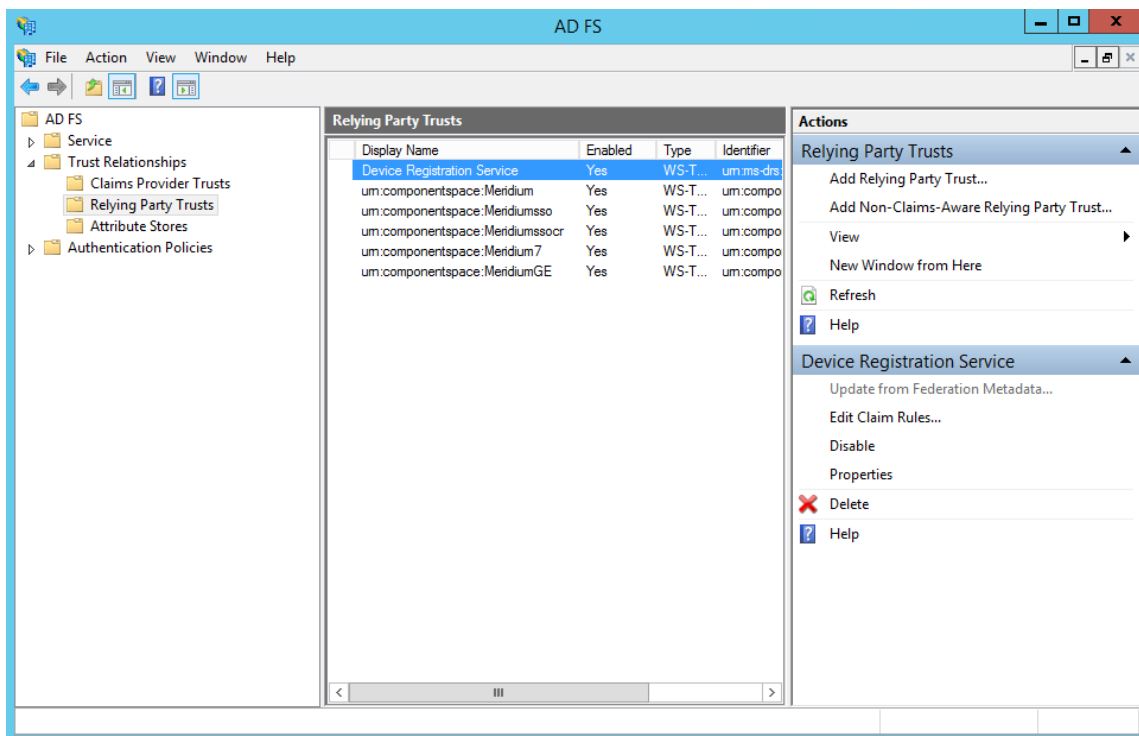
- [Add Claim Rules](#) on page 20

## Add Claim Rules

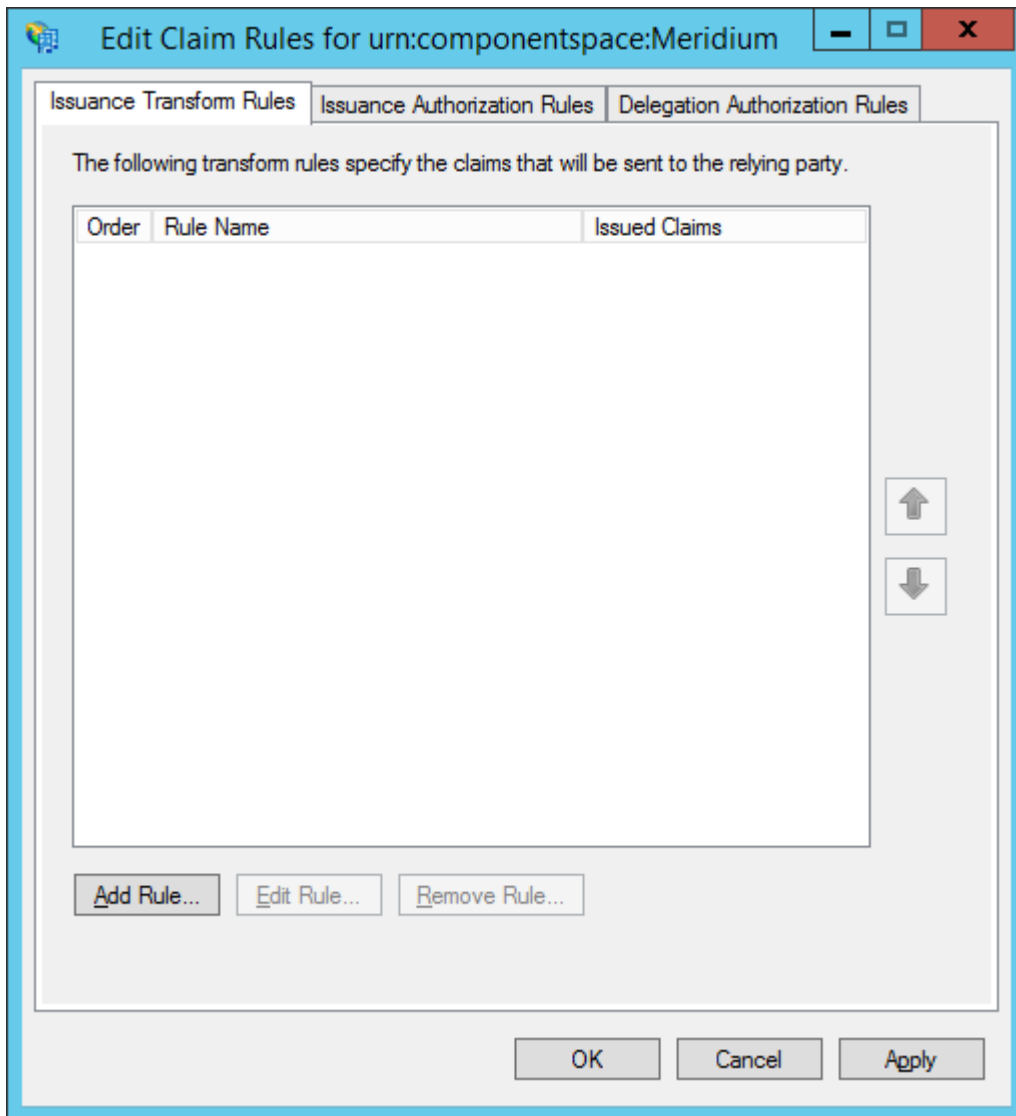
### Procedure

1. In the **AD FS** window, expand the **Trust Relationships** folder, and then select **Relying Party Trusts**. The **Relying Party Trusts** page appears.

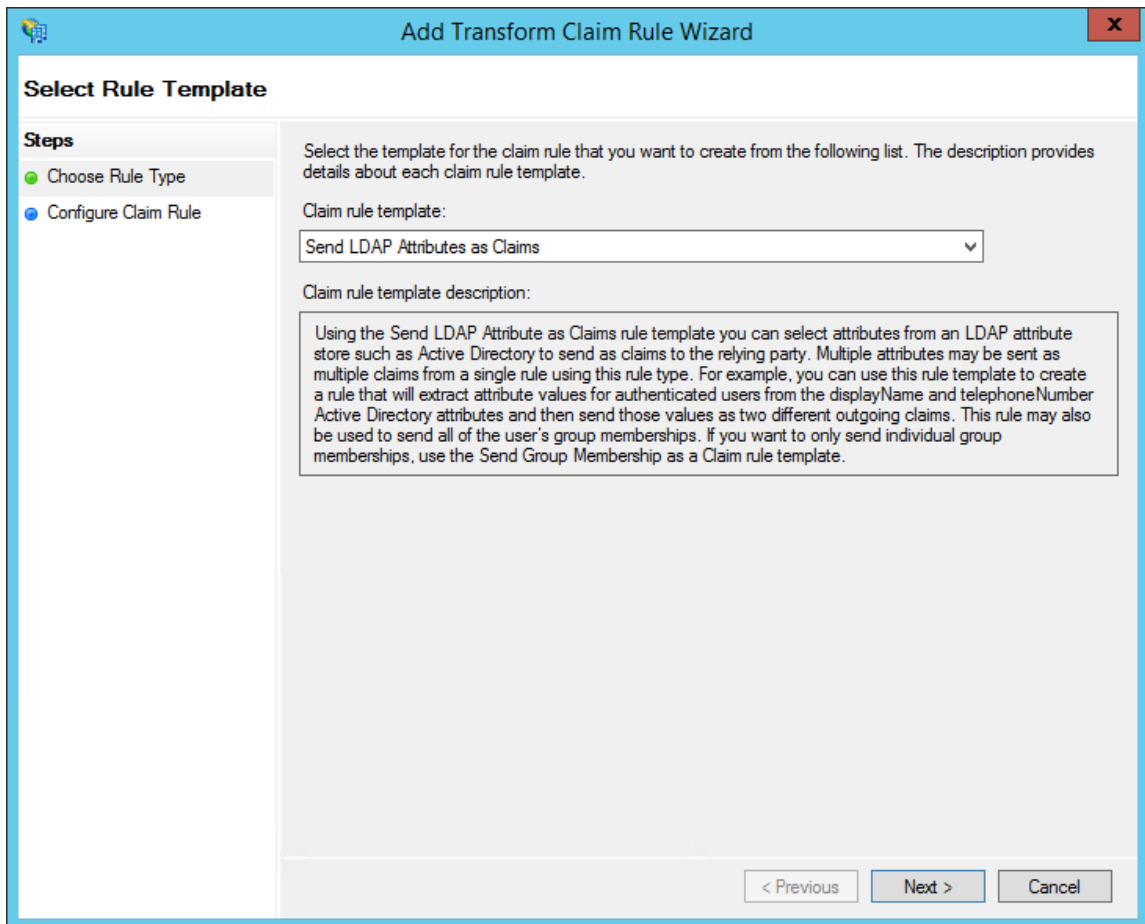




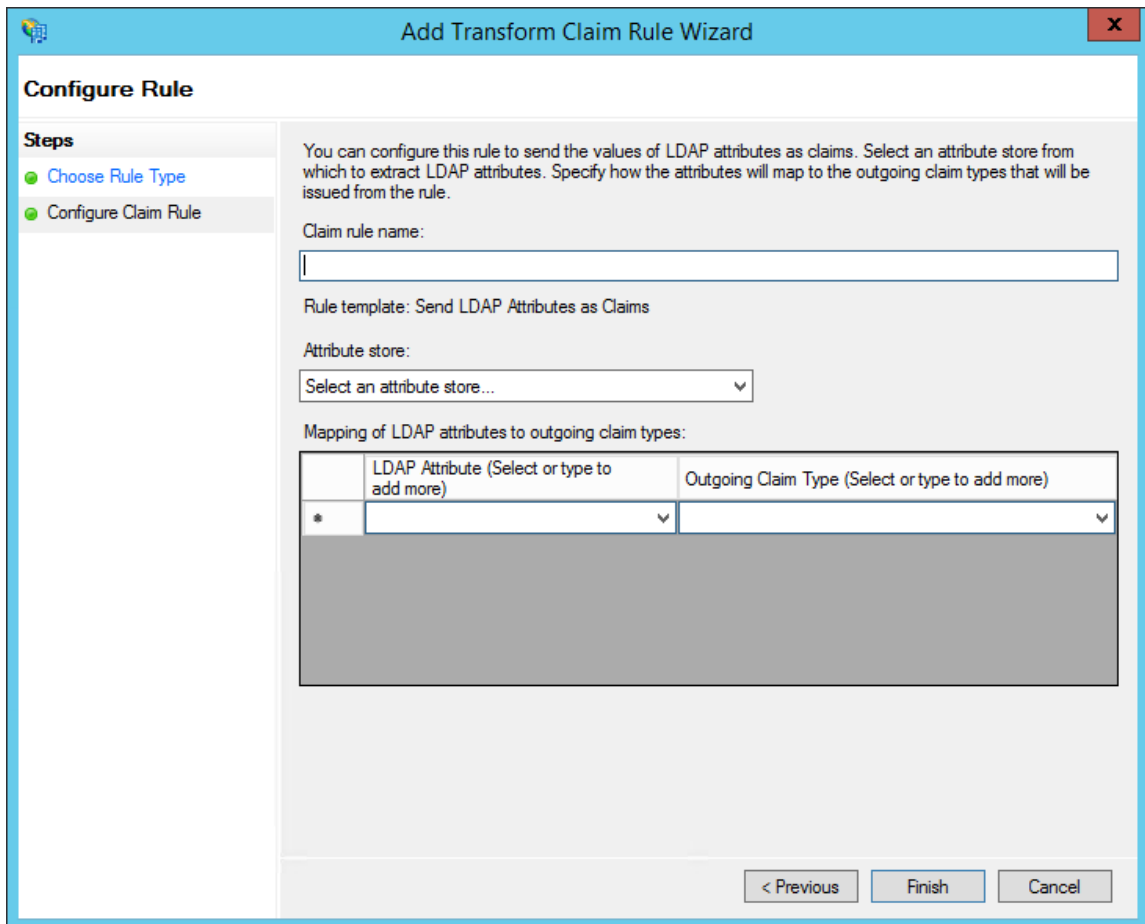
2. Select **urn:componentspace:Meridium**, and then, in the **Actions** section, select **Edit Claim Rules**. The **Edit Claim Rules for urn:componentspace:Meridium** window appears.



3. Select **Add Rule**.  
The **Add Transform Claim Rule Wizard** window appears.

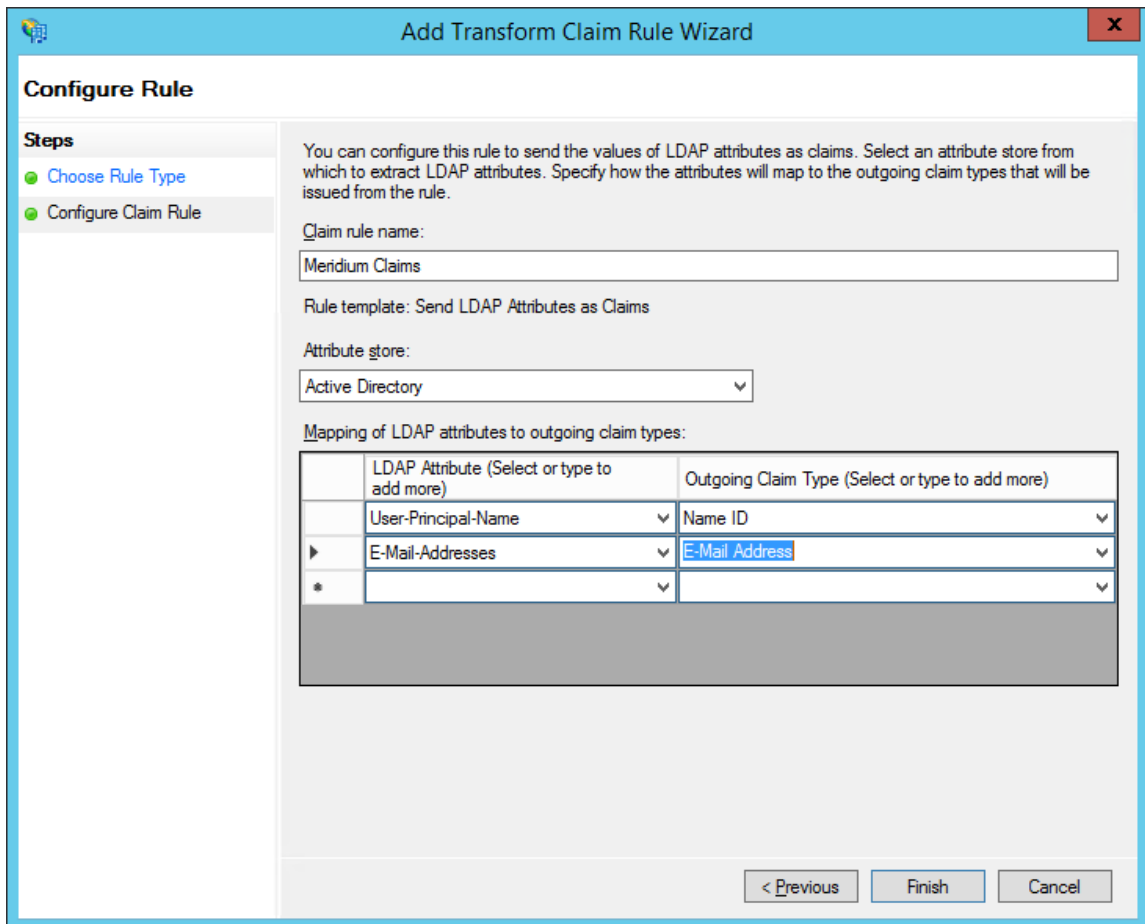


4. In the **Claim rule template** drop-down list box, select **Send LDAP Attributes as Claims**, and then select **Next**.  
The **Configure Rule** page appears.

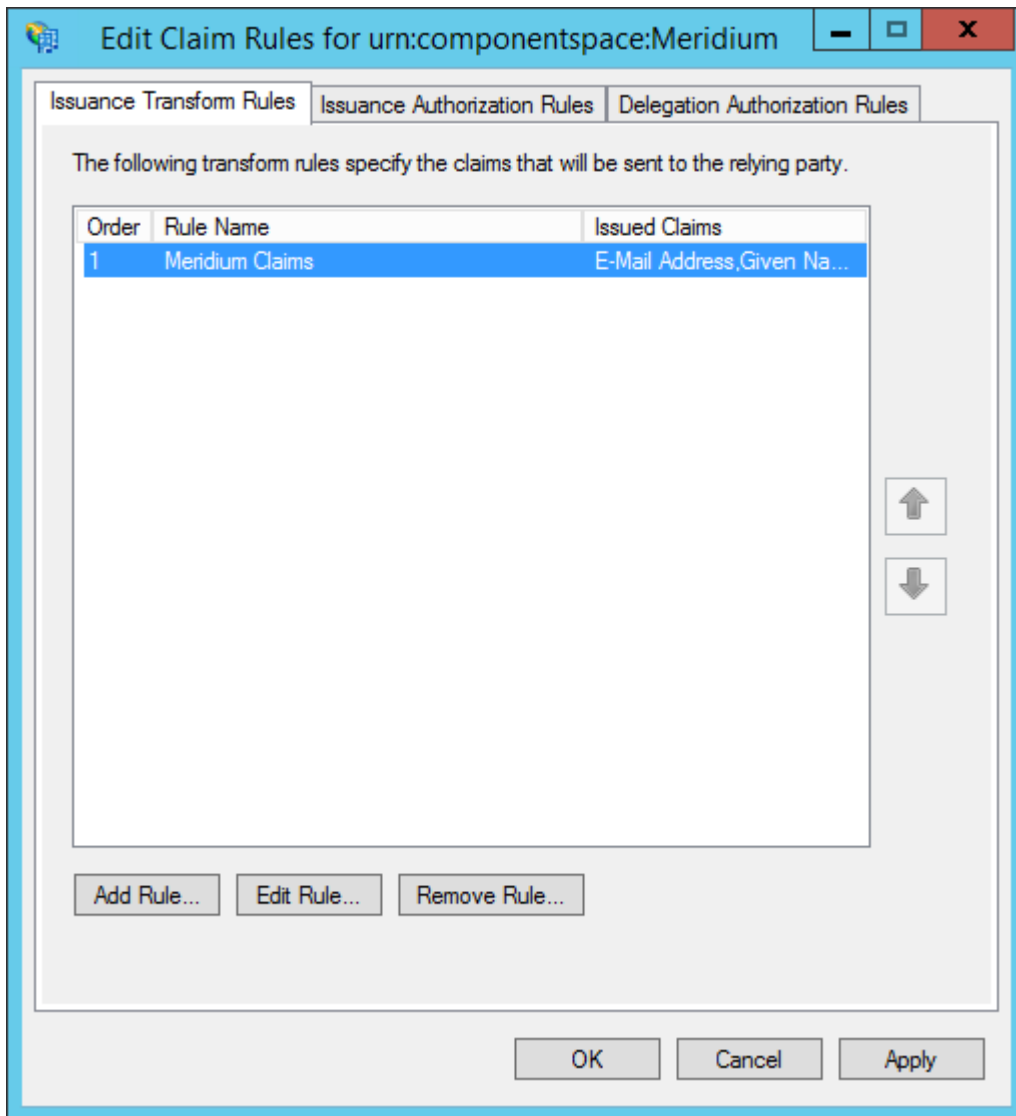


5. In the **Claim rule name** box, enter **Meridium Claims**, and then, in the **Attribute store** drop-down list box, select **Active Directory**.
6. Perform the following steps:
  - In the first drop-down list box in the **LDAP Attribute** column, select **User-Principal-Name**, and then, in the corresponding **Outgoing Claim Type** drop-down list box, select **Name ID**.
  - In the second drop-down list box in the **LDAP Attribute** column, select **E-mail-Addresses**, and then, in the corresponding **Outgoing Claim Type** drop-down list box, select **E-Mail Address**.

The **Configure Rule** page is populated with the selected values.



7. Select **Finish**.  
The **Edit Claim Rules for urn:componentSpace:Meridium** window appears.



8. Select **OK**.  
The claim rule is added to the **Edit Claim Rules for urn:componentspace:Meridium** window.

### Next Steps

- [Add Certificates](#) on page 26

## Add Certificates

### About This Task

To add certificates, you must perform the following tasks:

### Procedure

1. [Install the Public Key Certificate File \(sp.pfx\)](#) on page 27
2. [Export the Certificate](#) on page 31
3. [Copy the Certificate to Active Directory](#) on page 38

4. [Install the Token Signing idp.cer Certificate on the Application Server](#) on page 40

### Install the Public Key Certificate File (sp.pfx)

#### Procedure

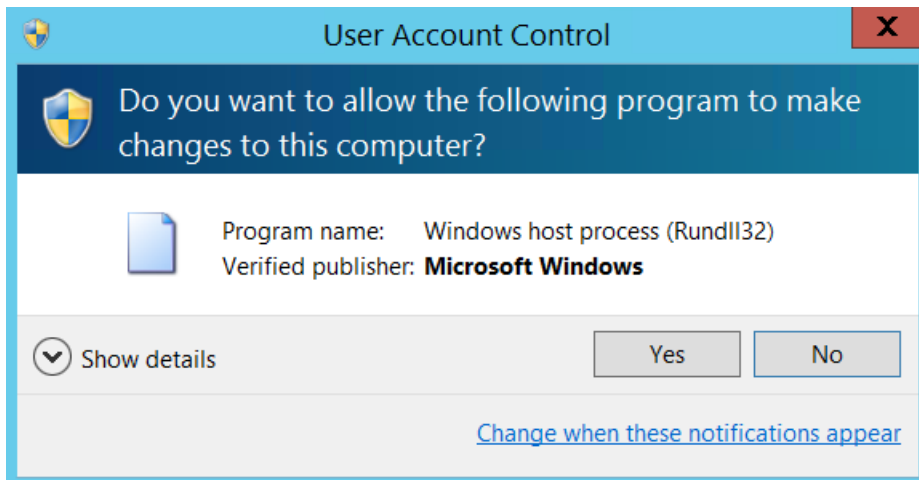
1. Navigate to C:\Program Files\Meridium\ApplicationServer\api, where the public key certificate file (sp.pfx) is located.

**Note:** GE Digital provides the public key certificate file (sp.pfx). pfx is personal information exchange.

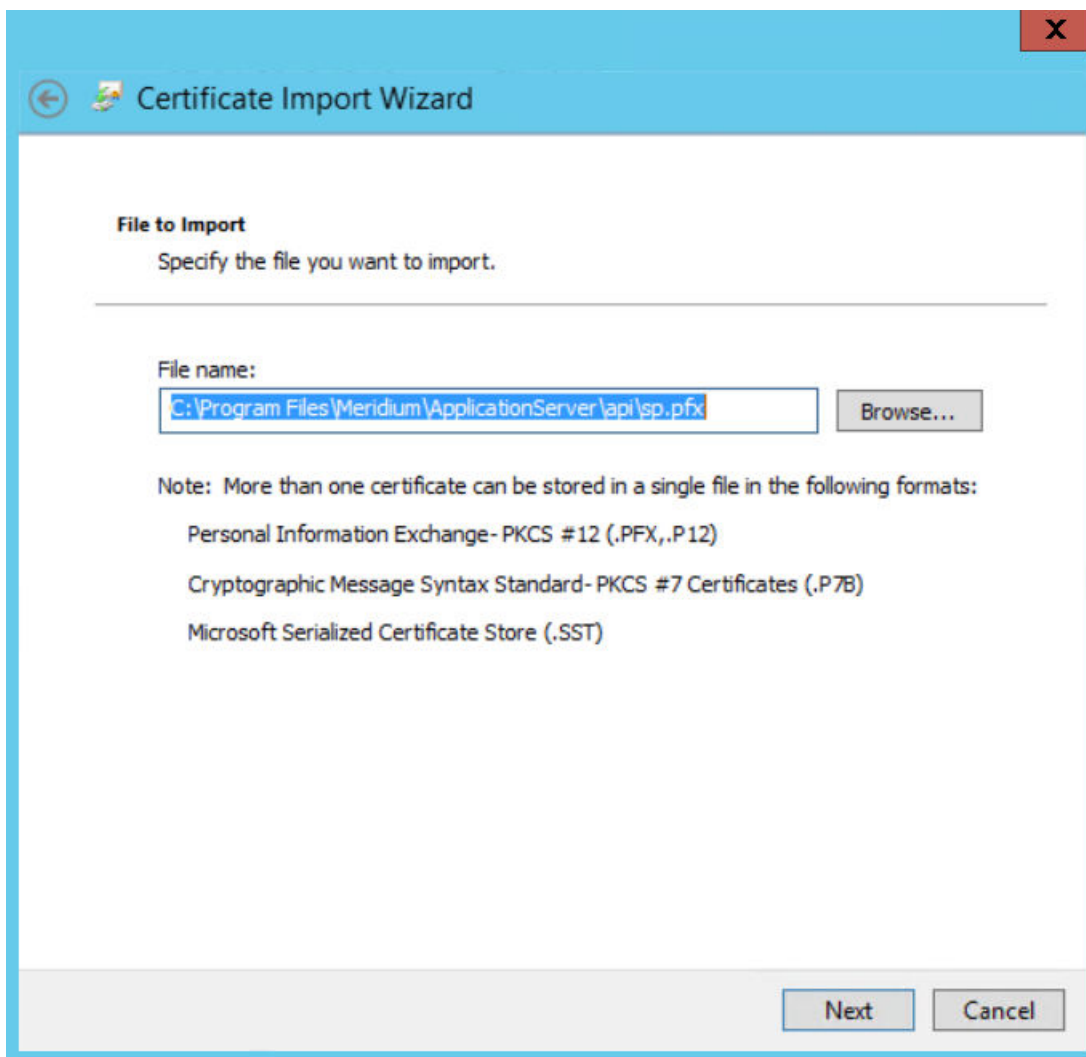
2. Right-click **sp**, and then select **Install PFX**.  
The **Certificate Import Wizard** appears.



3. Select **Local Machine**, and then select **Next**.  
The **User Account Control** window appears.

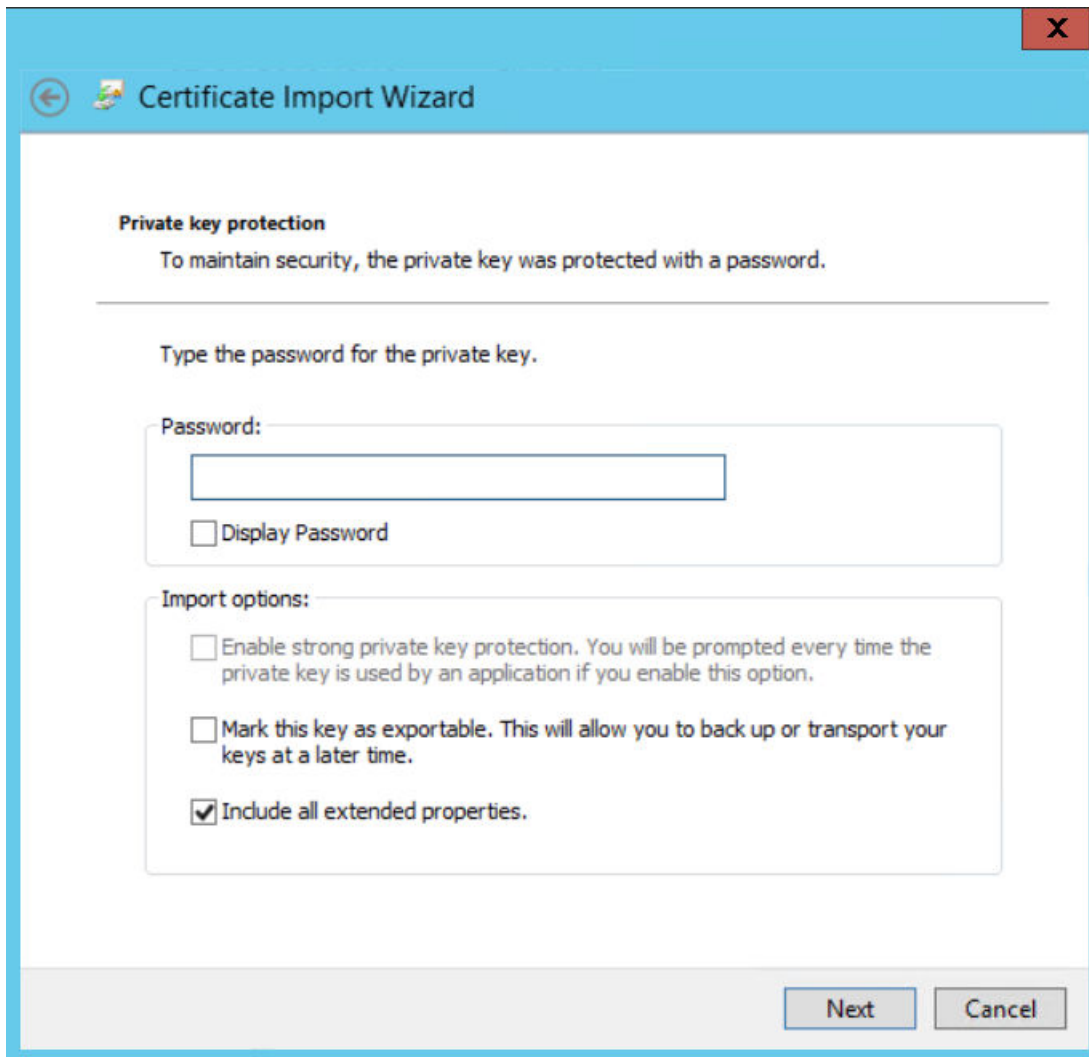


4. Select **Yes**.  
The **Certificate Import Wizard** appears, and the **File Name** box displays the file path where the certificate is located.

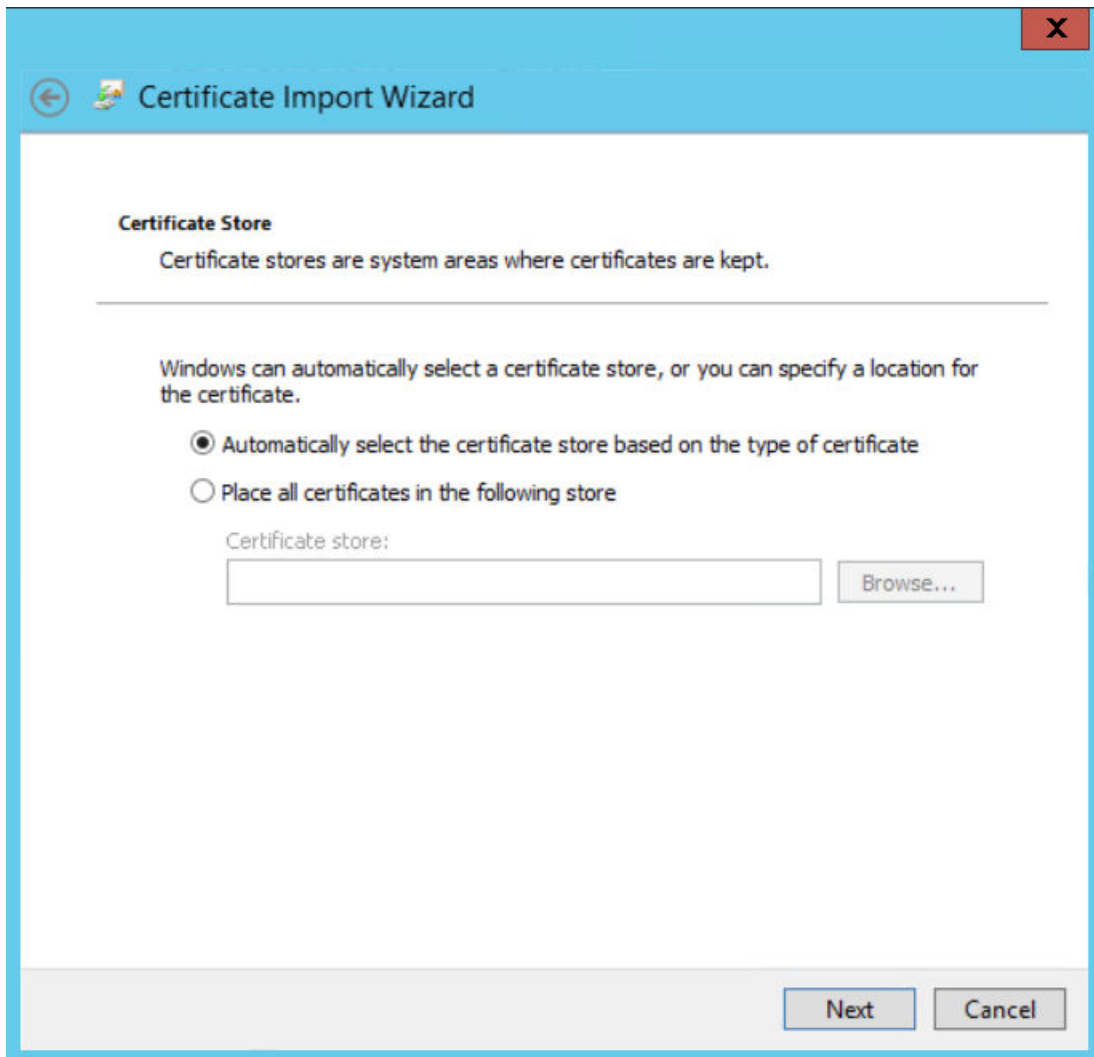


5. Select **Next**.

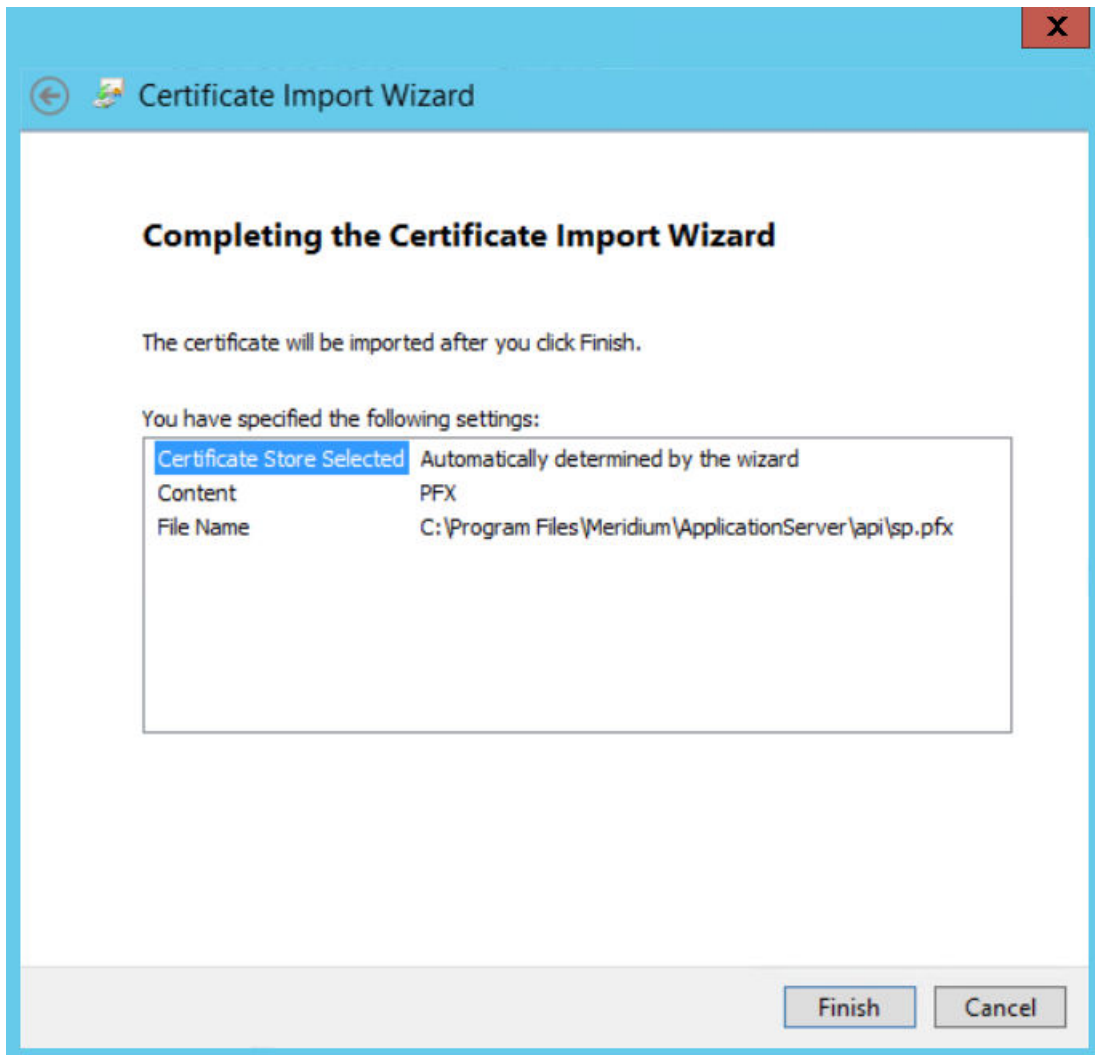




6. Enter a password, and then select **Next**.



7. Select **Automatically select the certificate store based on the type of certificate**. The **Completing the Certificate Import Wizard** appears.



8. Select **Finish**.

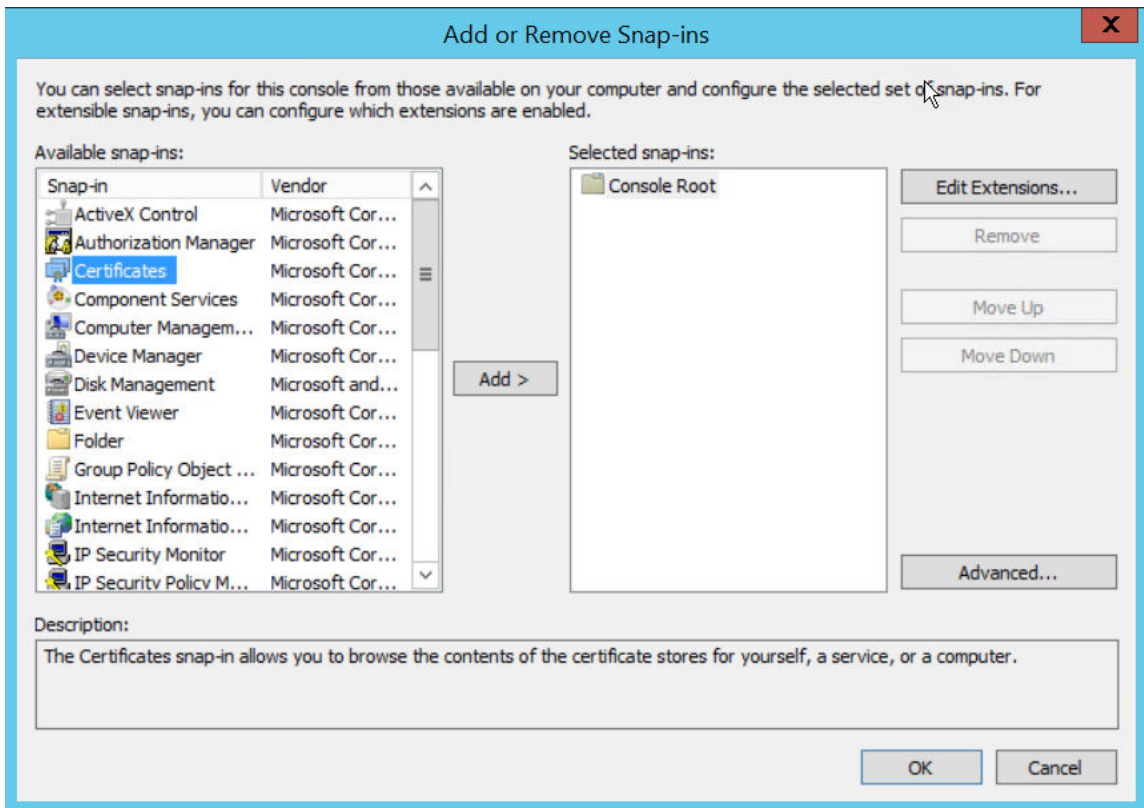
### Next Steps

- [Export the Certificate](#) on page 31

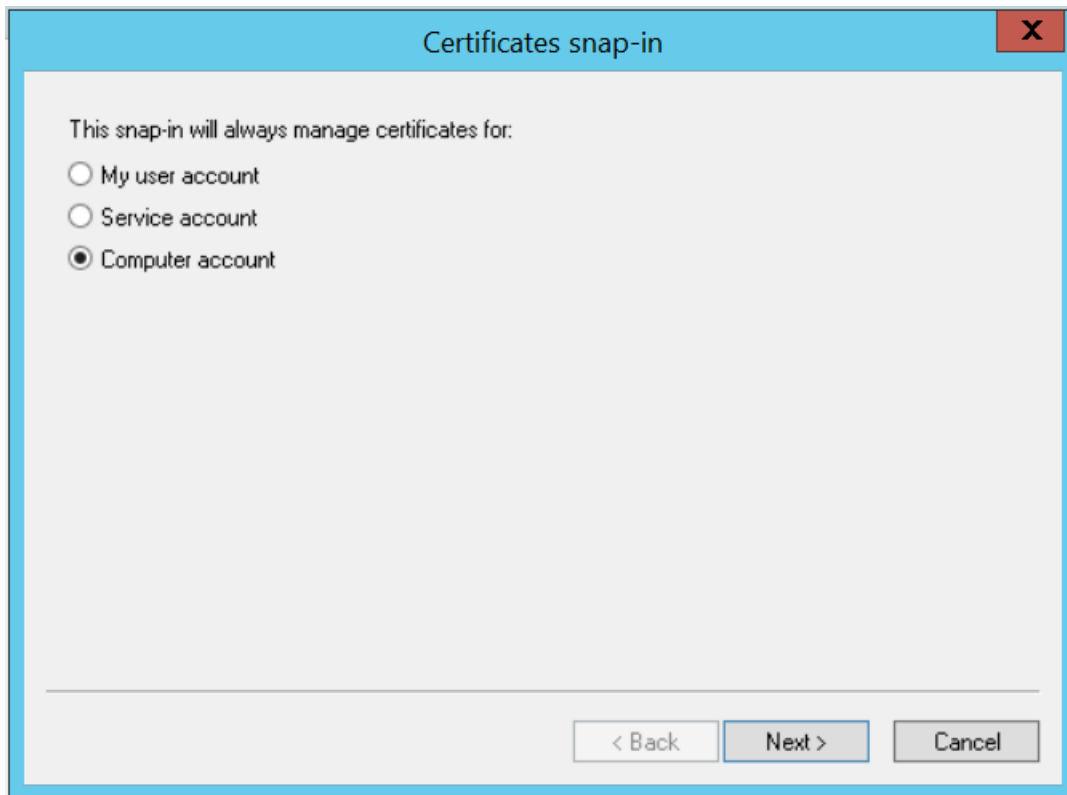
### Export the Certificate

#### Procedure

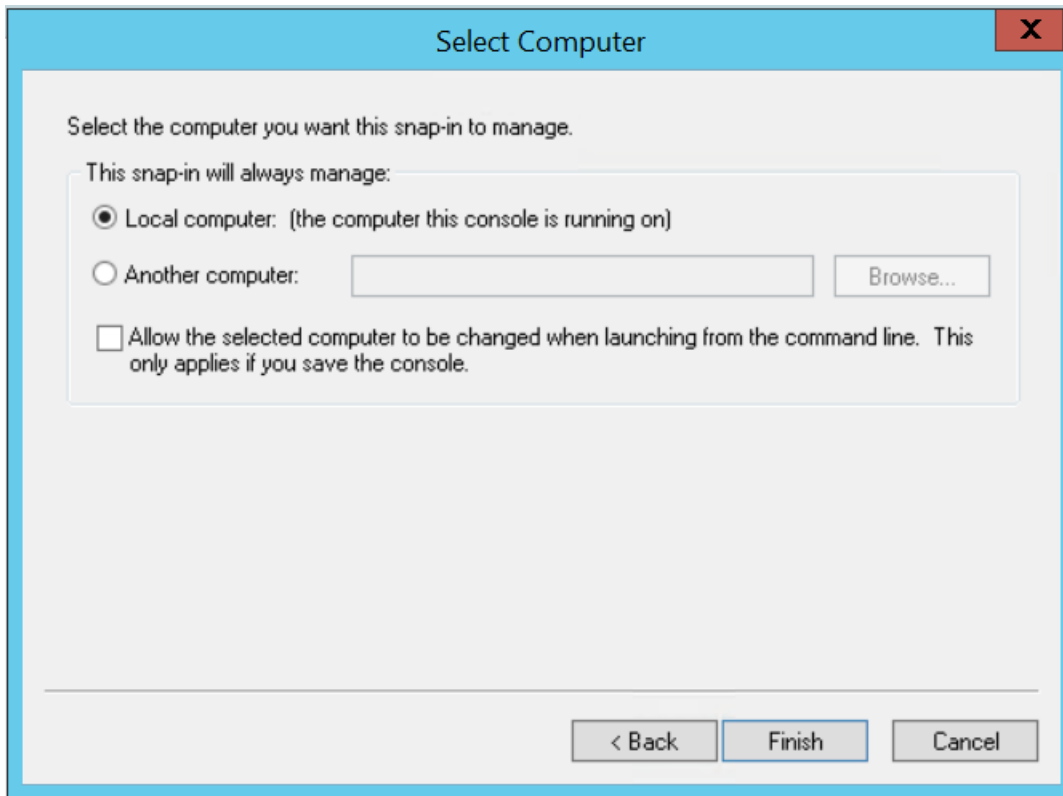
1. Access **Microsoft Management Console**.
2. In the main navigation bar, select **File**, then select **Add/Remove Snap-in**, and then select **Certificates**.  
The **Add or Remove Snap-ins** window appears.



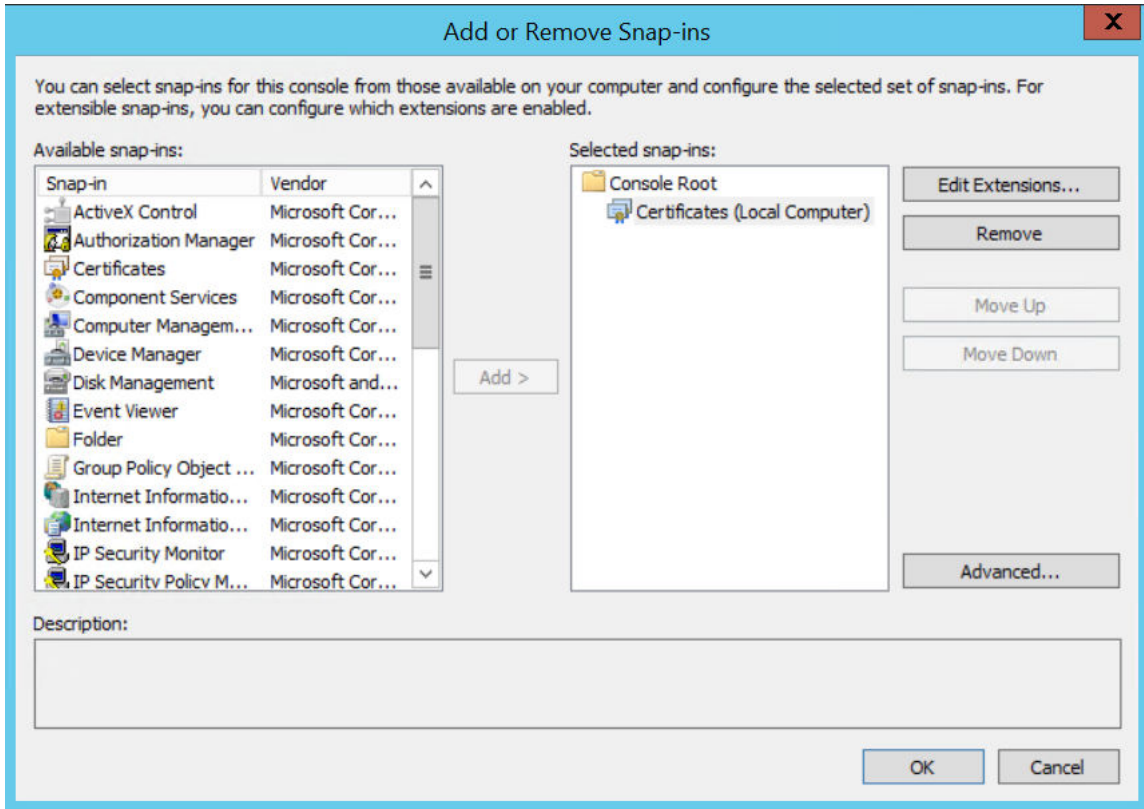
3. Select **Add**.  
The **Certificates snap-in** window appears.



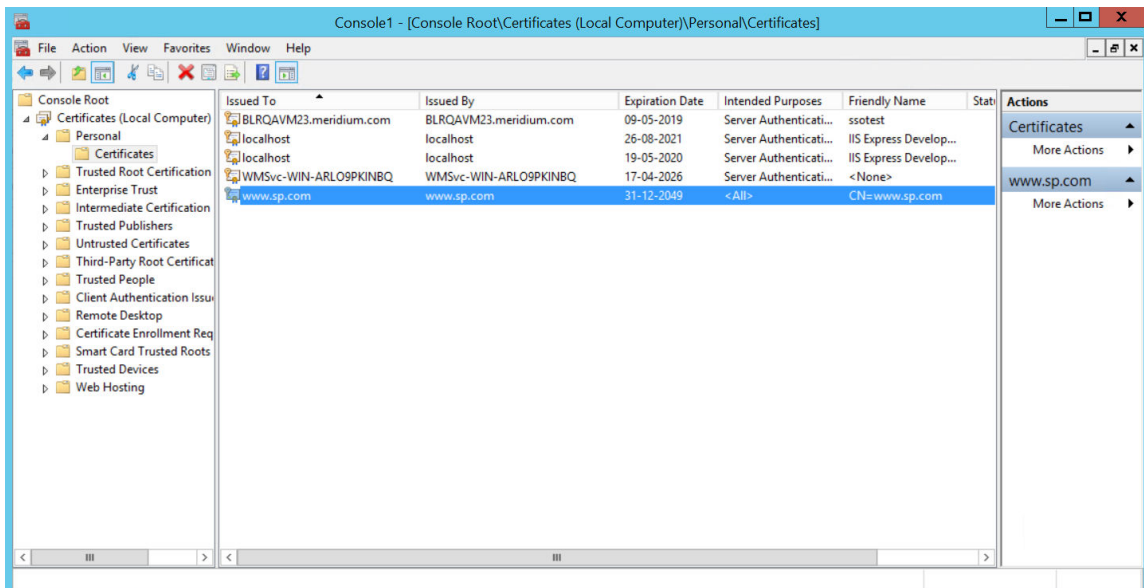
4. Select the **Computer account** option, and then select **Next**. The **Select Computer** window appears.



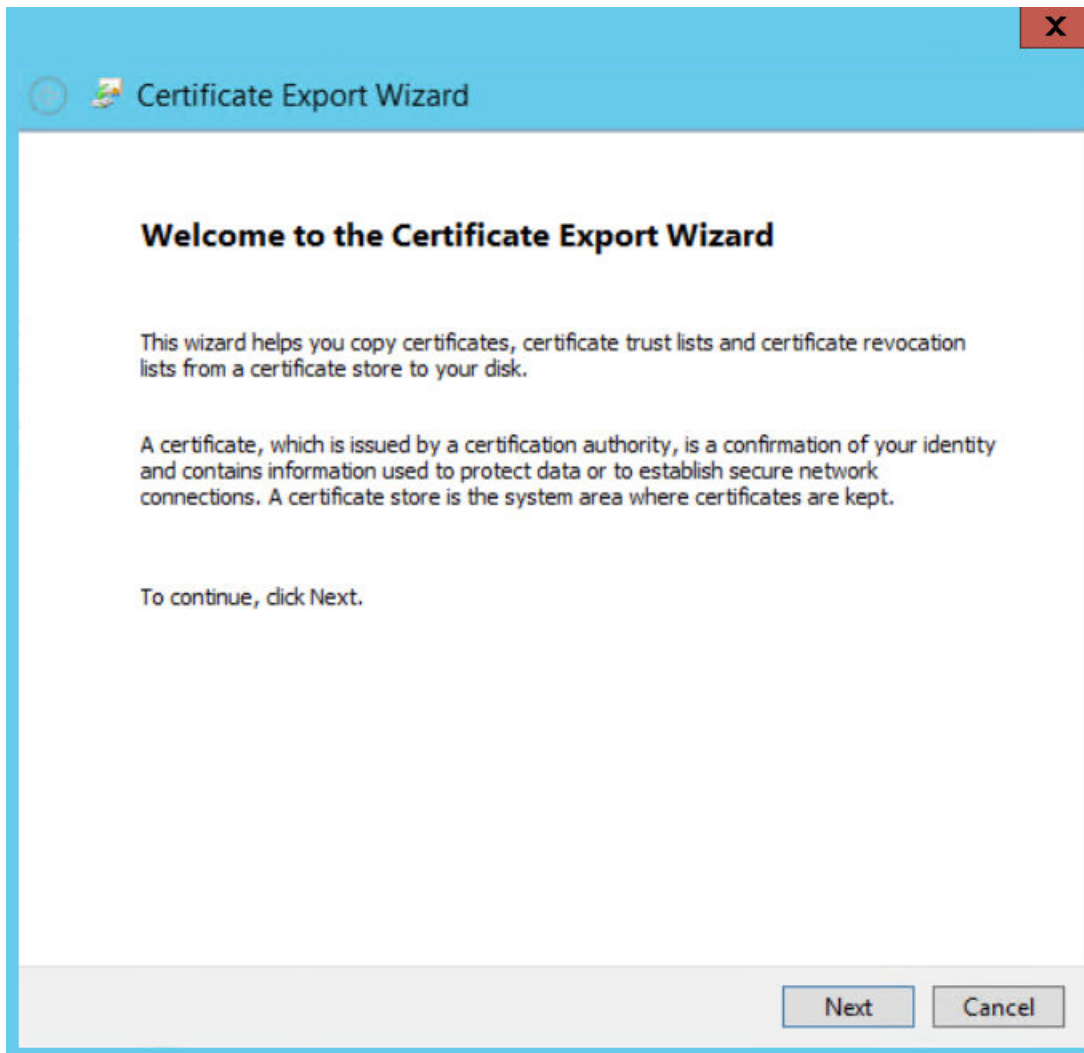
5. Select the **Local computer** option, and then select **Finish**.



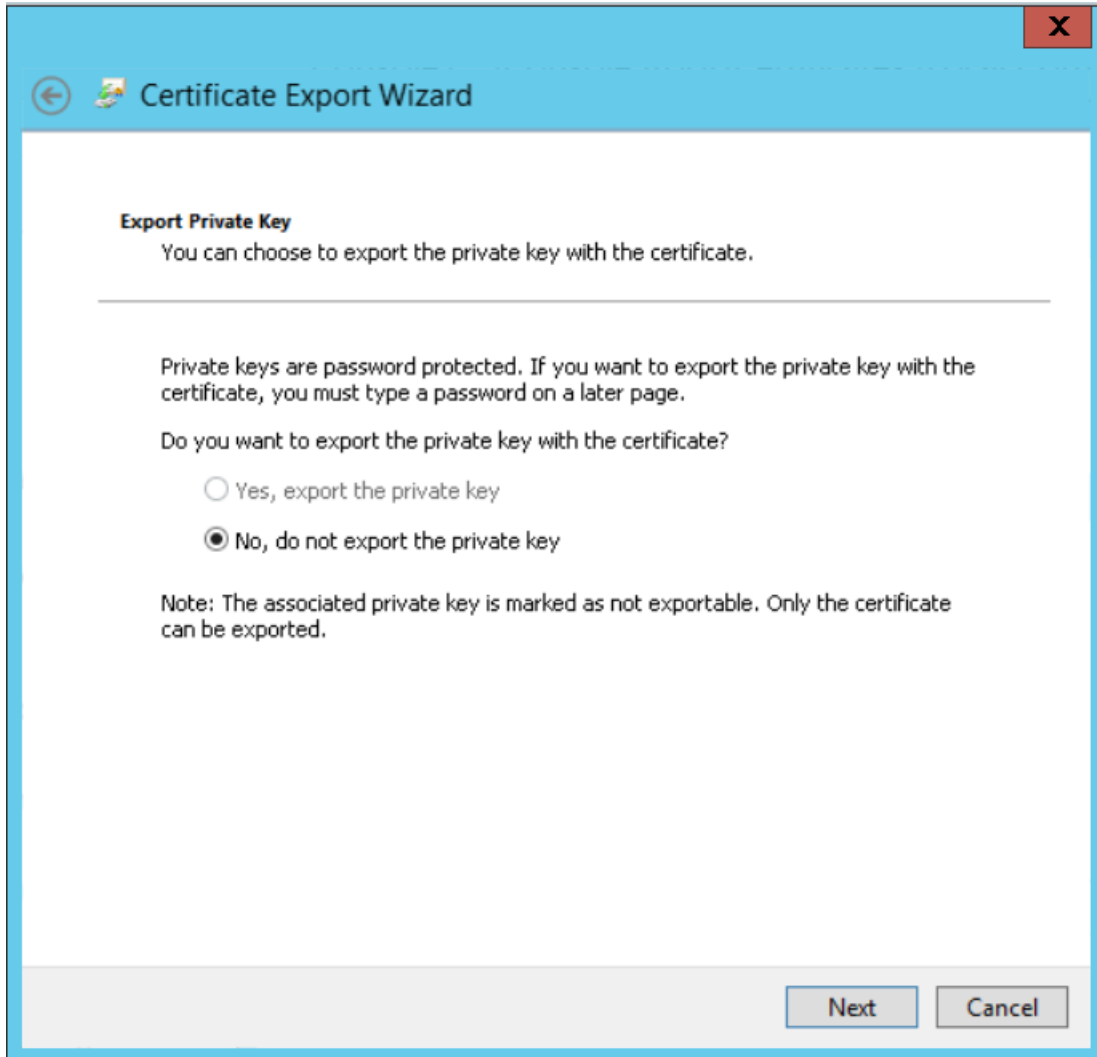
6. In the **Add or Remove Snap-ins** window, select **OK**.  
The certificate appears in the **Personal > Certificates** folder of the **Certificates (Local Computer)** folder.
7. Select **Certificates (Local Computer)**, then select **Personal**, and then select **Certificates**.



8. Right-click the certificate that you have installed, select **All Tasks**, and then select **Export**.  
The **Certificate Export Wizard** appears.

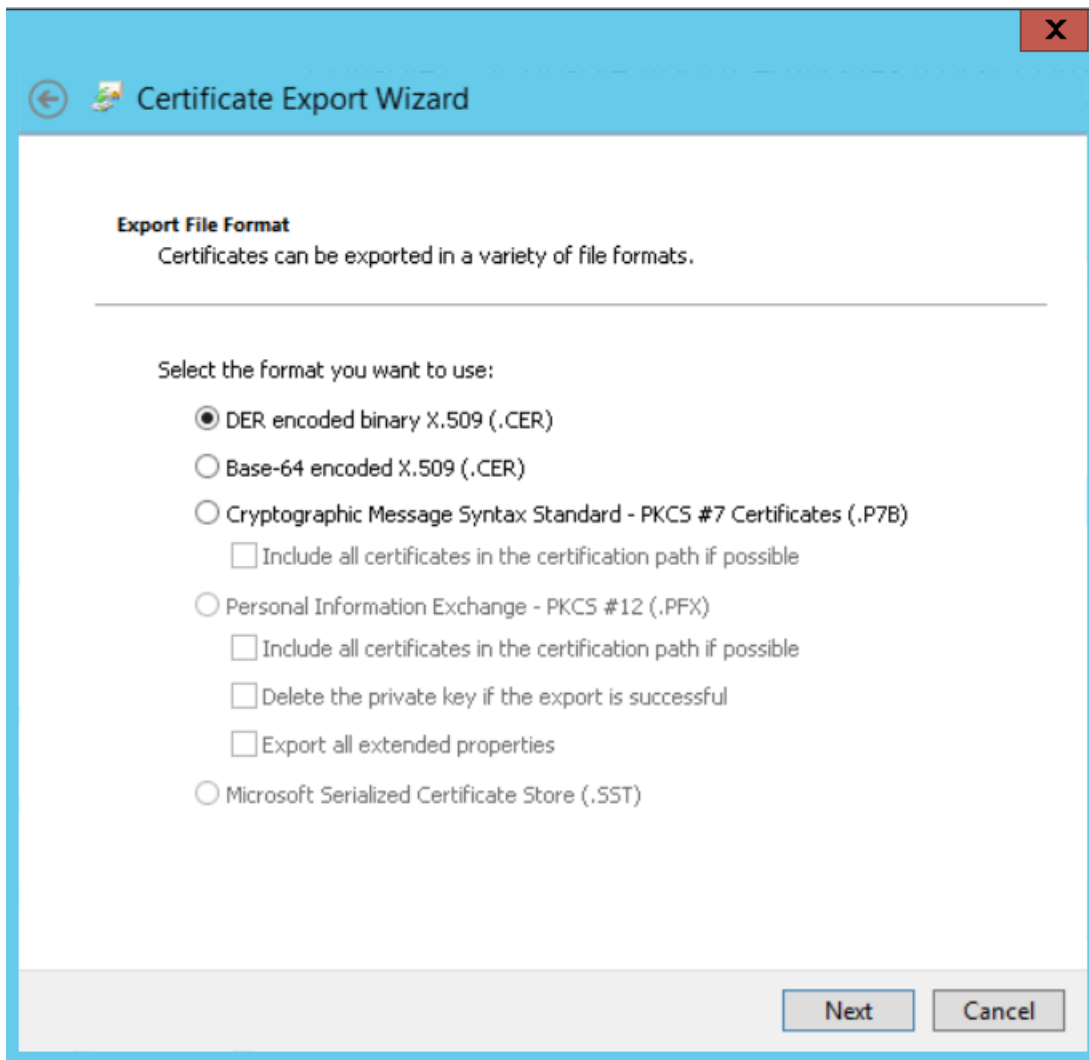


9. Select **Next**.

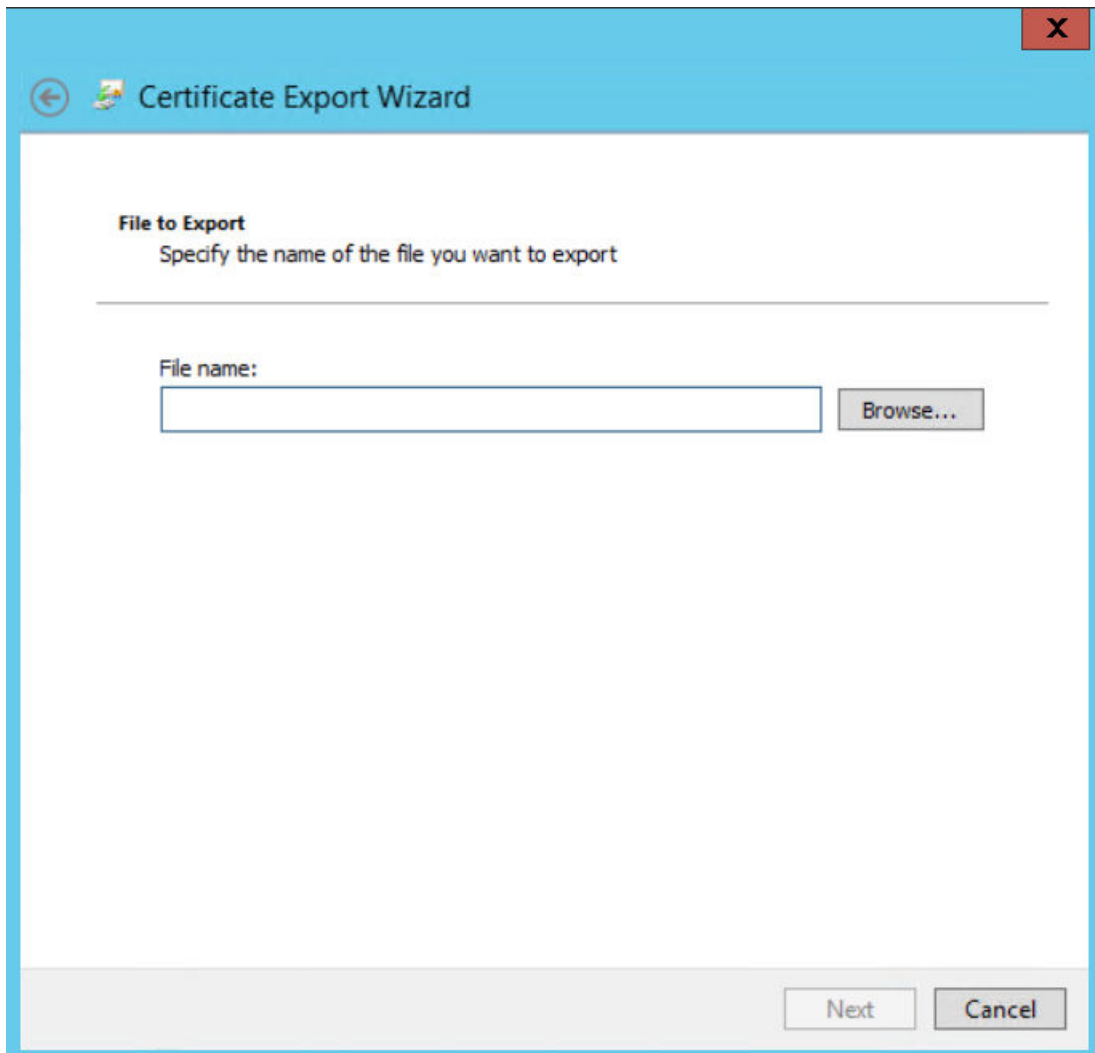


10. Select the **No, do not export the private key** option, and then select **Next**.





11. Select **DER encoded binary X.509 (.CER)**, and then select **Next**.



12. Select **Browse**, and then navigate to the location to which you want to export the certificate.
13. In the **File name** box, enter the same name that was mentioned while installing the certificate, and then, in the **Save as type** drop-down list box, select **DER Encoded Binary X.509 (.cer)**.
14. Select **Next**, and then select **Finish**.

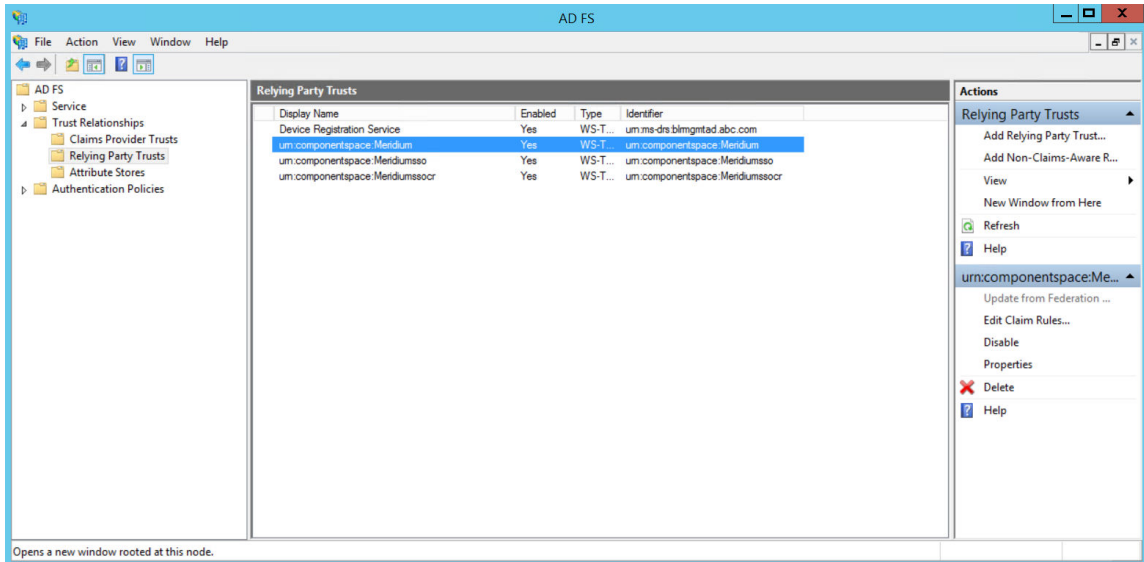
### Next Steps

- [Copy the Certificate to Active Directory](#) on page 38

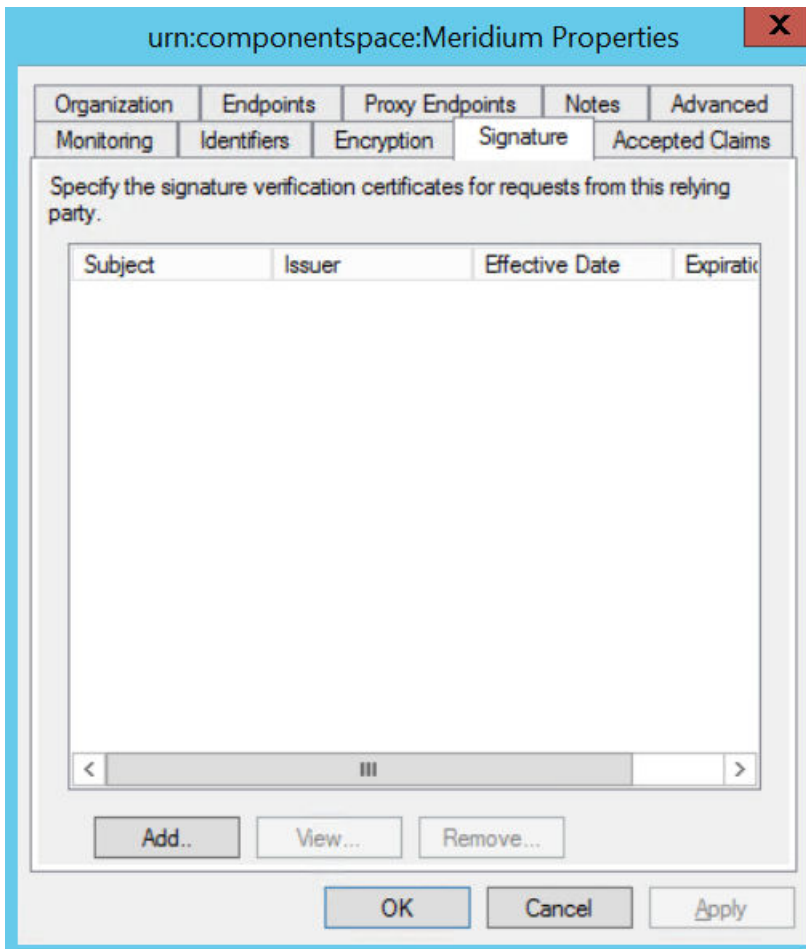
### Copy the Certificate to Active Directory

#### Procedure

1. Access **Control Panel**, then select **System and Security**, and then select **Administrative Tools**.
2. Select **AD FS Management**.  
The **AD FS** window appears.

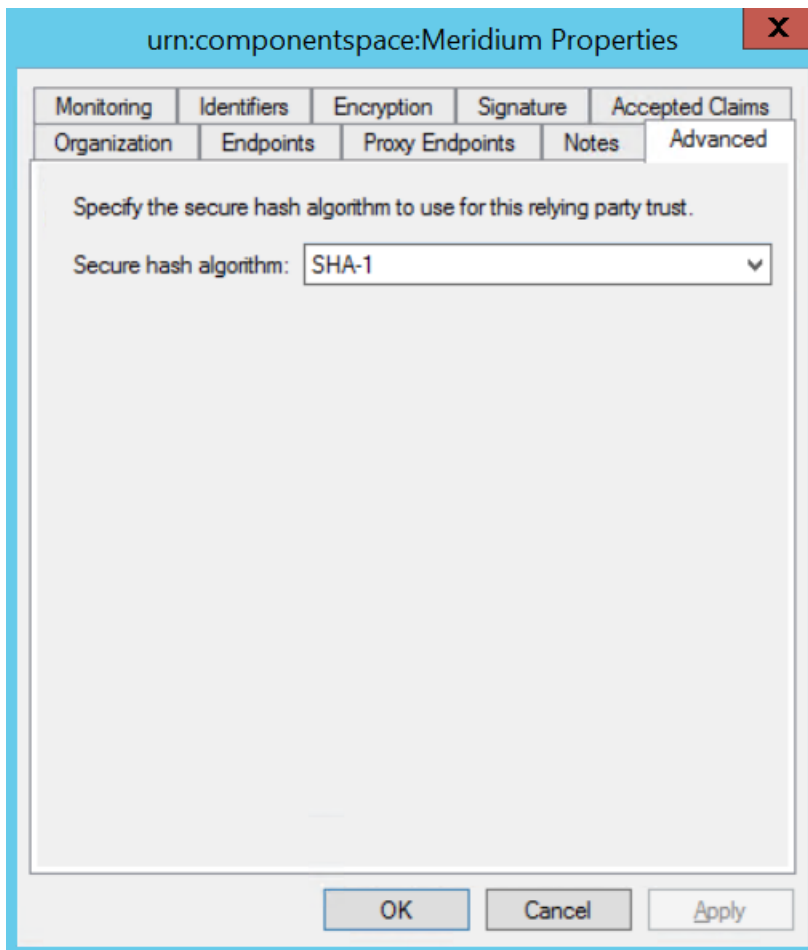


- Expand **Trust Relationships**, and then select **Relying Party Trusts**.
- Select **urn:componentspace:Meridium**, and then, in the **Actions** section, select **Properties**. The **urn:componentspace:Meridium Properties** window appears.



- Select the **Signature** tab, and then select **Add**.
- Navigate to the location in which you have saved the certificate, and then select the file.

7. Select **Yes** to ignore the warning about certificate key length.
8. Select the **Advanced** tab.
9. In the **Secure hash algorithm** drop-down list box, based on the policy of your organization, select **SHA-1** or **SHA-256**.



10. Select **Apply**, and then select **OK**.

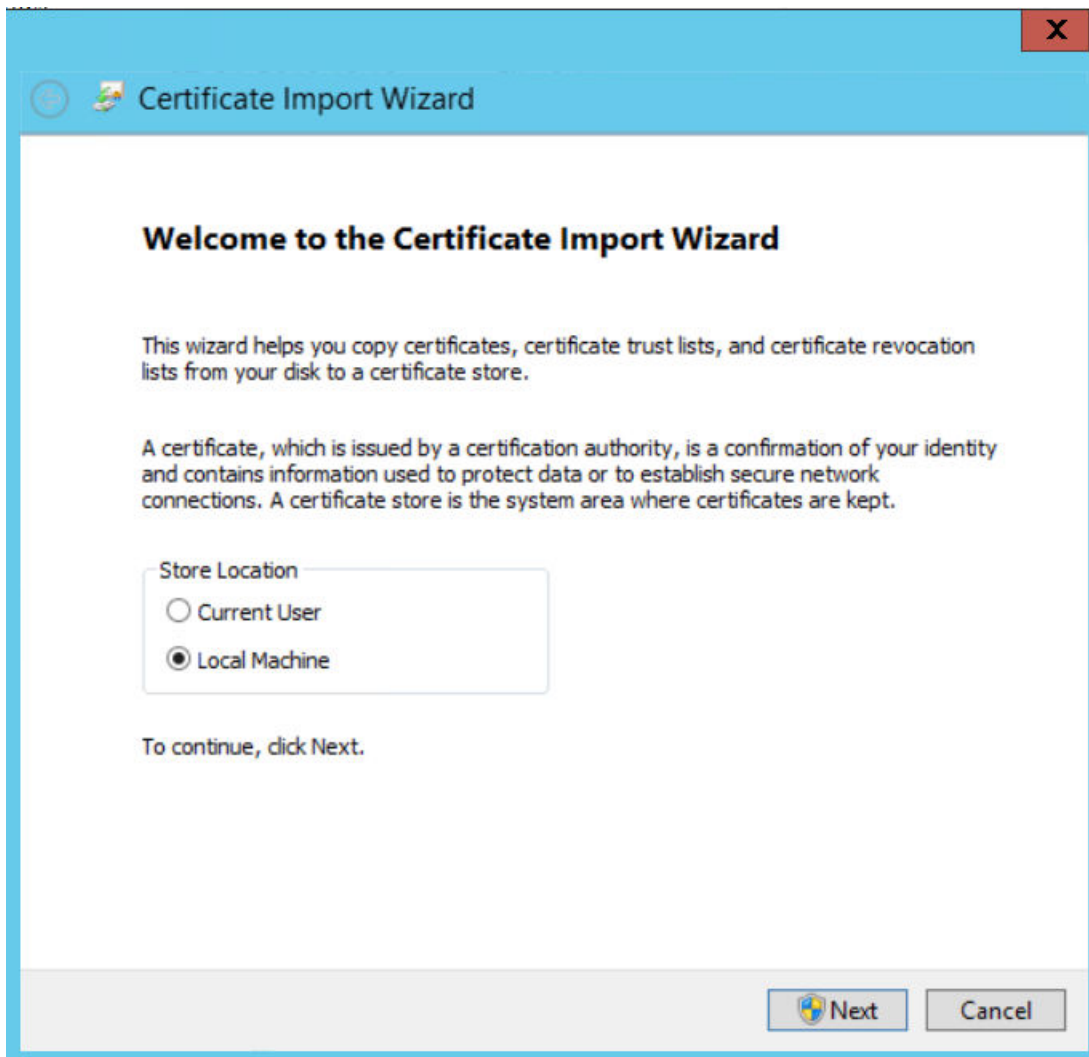
### Next Steps

- [Install the Token Signing idp.cer Certificate on the Application Server](#) on page 40

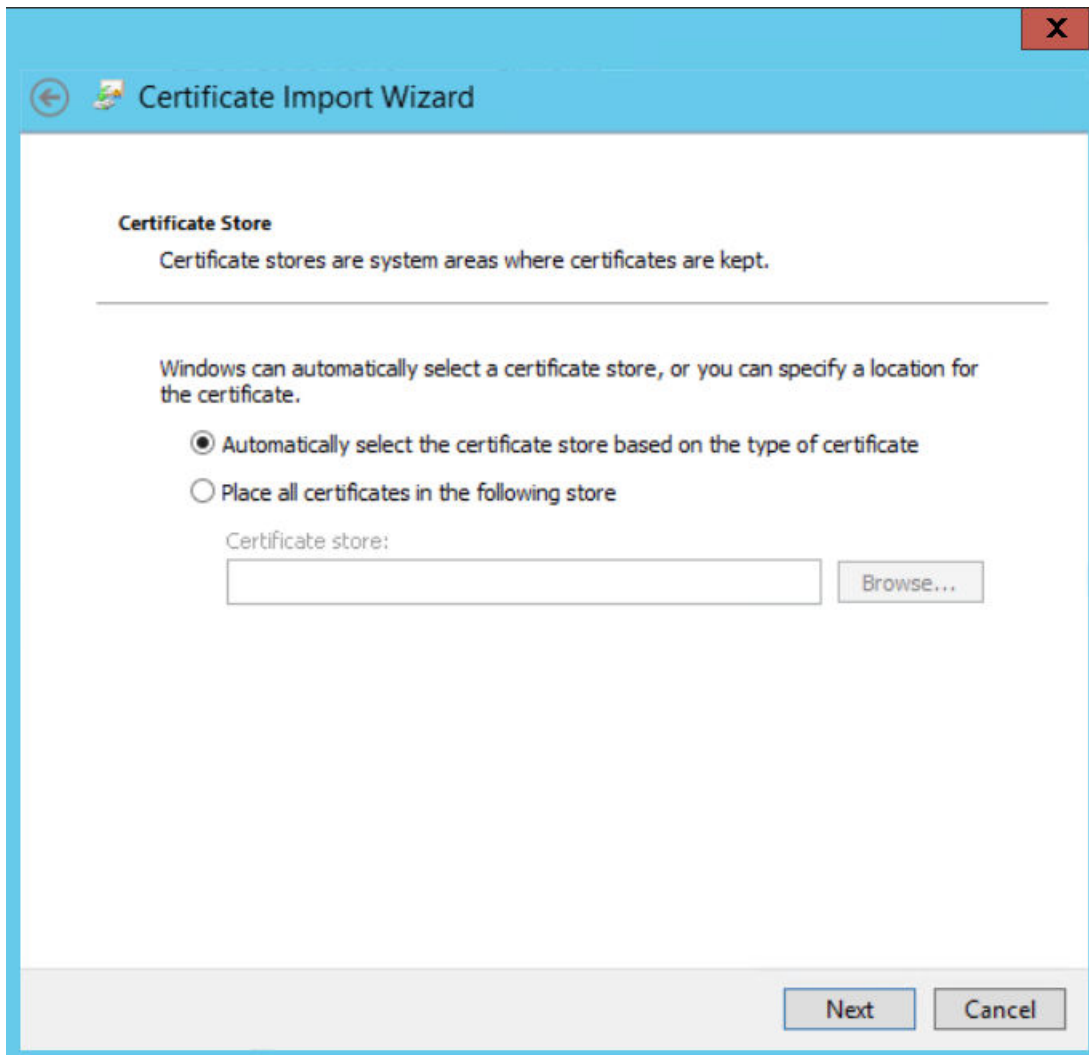
### Install the Token Signing idp.cer Certificate on the Application Server

#### Procedure

1. Access the Active Directory.
2. Export the token signing certificate and save the certificate.
3. Select **Finish**.
4. Copy the certificate to the api folder of the application server.
5. Right-click the file, and then select **Install Certificate**.  
The **Certificate Import wizard** appears.



6. Select **Local Machine**, and then select **Next**.



7. Select **Automatically select the certificate store based on the type of certificate.**
8. Select **Next**, and then select **Finish**.

#### **Next Steps**

- [Enable SSO On Site Authentication Using Active Directory](#) on page 44

# Chapter 3

---

## Enable SSO

### Topics:

- [About Enabling GE Digital APM SSO](#)
- [About Host Names](#)
- [Enable SSO On Site Authentication Using Active Directory](#)
- [Enable SSO Off-Site Authentication Using GE Digital APM Server Setup](#)

## About Enabling GE Digital APM SSO

To enable GE Digital APM SSO, perform one of the following tasks:

- [Enable SSO On Site Authentication Using Active Directory](#) on page 44
- [Enable SSO Off-Site Authentication Using GE Digital APM Server Setup](#) on page 44

## About Host Names

Using the Host Names feature, you can:

- [Enable Single Sign-On \(SSO\) off-site authentication](#) and [SSO on-site authentication](#).
- Filter Data Sources to access the related GE Digital APM database.
- Create a unique URL to access GE Digital APM.

When you use a URL to access GE Digital APM, you can access the data sources that are mapped to the host name. For example, if two data sources (data\_source1 and data\_source2) are associated with a GE Digital APM server, you can create two different URLs ([https://data\\_source1/meridium/index.html](https://data_source1/meridium/index.html) and [https://data\\_source2/meridium/index.html](https://data_source2/meridium/index.html)) using the host names that are mapped to the data sources. If you log in to GE Digital APM with [https://data\\_source1/meridium/index.html](https://data_source1/meridium/index.html) or [https://data\\_source2/meridium/index.html](https://data_source2/meridium/index.html), you can access data\_source1 or data\_source2, respectively.

In the **Host Names** page, you can add multiple host names. However, only the host name of the URL with which you have logged in to GE Digital APM is listed.

## Enable SSO On Site Authentication Using Active Directory

### Procedure

1. Run the LDAP Synchronization Process Manually or Schedule a LDAP Synchronization Process .
2. Log out of GE Digital APM.
3. Log in to GE Digital APM with the Windows user name and password.  
You are logged in.

### Results

- SSO On-Site Authentication is enabled.

### Next Steps

- [Configure GE Digital APM Server](#) on page 48

## Enable SSO Off-Site Authentication Using GE Digital APM Server Setup

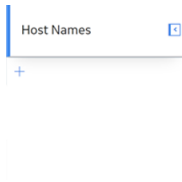
### About This Task

**Note:** The settings shown below may vary depending on your system.

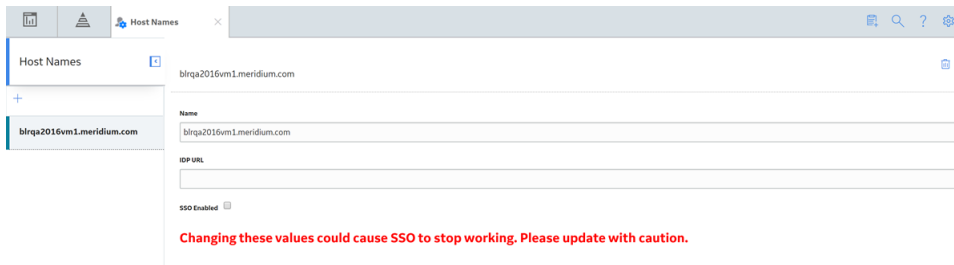


## Procedure

1. In the module navigation menu, select **Admin > Operations Manager > Host Names**.  
The **Host Names** page appears.



2. In the left pane, select **+**.  
The workspace for a new host name appears, displaying default values.



3. In the **Name** box, replace the default text with the GE Digital APM Server's fully qualified hostname.
4. In the **IDP URL** box, replace the default text with the SAML Issuer ID that is specified on the IDP.
5. Select the **SSO Enabled** check box.

6. Select .

The host name is saved.

7. Log out of GE Digital APM.
8. On the GE Digital APM Server, in the GE Digital APM program files, navigate to the folder `.. \ApplicationServer\api`.

**Note:** If you installed the software in the default location, the folder location will be `C:\Program Files\Meridium\ApplicationServer\api`.

9. Replace the text `urn:componentSpace:MvcExampleIdentityProvider` with the SAML Issuer ID that is specified on the IDP.

**Note:** The settings in `saml.json` must be configured to match the environment to which you are connecting. For example, the URL listed in `SingleSignOnServiceUrl` should point to the URL where you want to authorize the users.

10. Modify the assertion and response signing settings to match the signing settings that are specified on the IDP, and then save and close the file.

11. In your system's IDP, specify **urn:componentSpace:Meridium** as the Audience Restriction.

**Note:** If the IDP is doing assertion and/or response signing, then the IDP signature algorithm must be **SHA1**.

12. Place the `idp.cer` file in the following location `C:\Program Files\Meridium \ApplicationServer\api`.

**Note:** The `idp.cer` file should be obtained from the team responsible for setting up the SAML Identity Provider (IDP).

13. Reset IIS.  
IIS is reset.

14. Access GE Digital APM via a web browser.

The user is logged in, and SSO off-site authentication is enabled.

**Next Steps**

- [Configure GE Digital APM Server](#) on page 48

# Chapter 4

---

## Configure GE Digital APM Server

### Topics:

- [Configure GE Digital APM Server](#)

# Configure GE Digital APM Server

## Before You Begin

- Ensure that the GE Digital APM Server is installed and the server is configured to use SSL.
- Ensure that you can access the GE Digital APM application in a web browser using HTTPS protocol.
- Ensure that the GE Digital data source is configured and you can log in with administrative privileges.

## Procedure

1. Using a web browser, log in to GE Digital APM as an Administrator.
2. In the module navigation menu, select **Admin**, then select **Operations Manager**, and then select **Data Sources**.  
The **Data Sources** page appears.

V4030100\_BASE\_QA\_LAST

Data Source ID	Database Server
V4030100_BASE_QA_LAST	BLRDEVDB01/SQL2012
Data Source Description	Database Name
V4030100_BASE_QA_LAST	V4030100_BASE_QA_LAST
Data Source Host	Database Alias
*	
Database Type	Oracle Host
SQL Server	
Database User Name	Oracle Port
V4030100_BASE_QA_LAST	
Password	Oracle Service
.....	
<input type="checkbox"/> Preload Cache	
<input type="checkbox"/> Datasource Offline	

3. In the **Data Source Host** box, enter the name of the GE Digital APM server, and then select **Save**.
4. Enable LDAP Integration, configure Domain Record, and then schedule and run LDAP synchronization.

**Note:** For more information on how to enable LDAP Integration, configure a Domain Record, and schedule LDAP synchronization, refer to the Lightweight Directory Access Protocol documentation.

The users from Active Directory are now imported to GE Digital APM and are assigned the appropriate Security Roles and Groups.

5. Stop IIS, the Redis service, and all Meridium Windows services.
6. Navigate to `C:\Program Files\Meridium\ApplicationServer\api`
7. Using a json or text editor, access the file `saml.json`.
8. Add a new configuration to `<PartnerIdentityProviderConfigurations>` json array or update the existing configuration by setting the following attributes:

- Name: urn:componentspace:Meridium  
**Note:** The value for the Name element is same as the IDP name.
- WantSAMLResponseSigned: false
- WantAssertionSigned: true
- WantAssertionEncrypted: false
- UseEmbeddedCertificate: false

- SingleSignOnServiceUrl: {https version of Federation Service identifier} + "/adfs/ls". For example, https://myadfsserver/adfs/ls

**Note:**

For SHA-256, you must add the following two attributes to the `saml.json` file:

- DigestMethod="http://www.w3.org/2001/04/xmlenc#sha256"
- SignatureMethod="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"

The following example shows the configured `saml.json` file:

```
{
  "SAML": {
    "$schema": "https://www.componentSpace.com/schemas/saml-
config-schema-v1.0.json",
    "Configurations": [
      {
        "LocalServiceProviderConfiguration": {
          "Name": "urn:componentSpace:Meridium",
          "AssertionConsumerServiceUrl": "~/core/security/
ssologinauth",
          "LocalCertificates": [
            {
              "FileName": "sp.pfx",
              "Password": "password"
            }
          ]
        },
        "PartnerIdentityProviderConfigurations": [
          {
            "Name": "http://fs.xyz.com/adfs/services/
trust",
            "Description": "ADFS",
            "SignAuthnRequest": true,
            "WantSamlResponseSigned": false,
            "UseEmbeddedCertificate": true,
            "WantAssertionEncrypted": false,
            "WantAssertionSigned": true,
            "SingleSignOnServiceUrl": "https://
fs.xyz.com/adfs/ls/idpinitiatedsignon.aspx",
            "PartnerCertificates": [
              {
                "FileName": "idp.cer"
              }
            ]
          }
        ]
      }
    ]
  }
}
```

9. Save and close the file `saml.json`.

10. Start IIS, the Redis service, and all Meridium Windows Services.