GE VERNOVA

Asset Performance Management
On-Premises APM
V5.2.2.0.0

Single Sign On

Contents

Copyright Digital, part of GE Vernova

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 APM, without having to re-enter their credentials.

The 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.

APM supports the following types of authentication for SSO:

- Pass-through authentication
  Enables the users to enter their Windows credentials in the APM login page and 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 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 APM SSO by configuring an identity provider.
2. Enable SSO on-site or off-site authentication.
3. Configure the APM server.

Chapter
2

Set up APM SSO

Topics:

About Setting Up APM SSO

About Setting up APM SSO

To set up 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 and select **Azure Active Directory**.
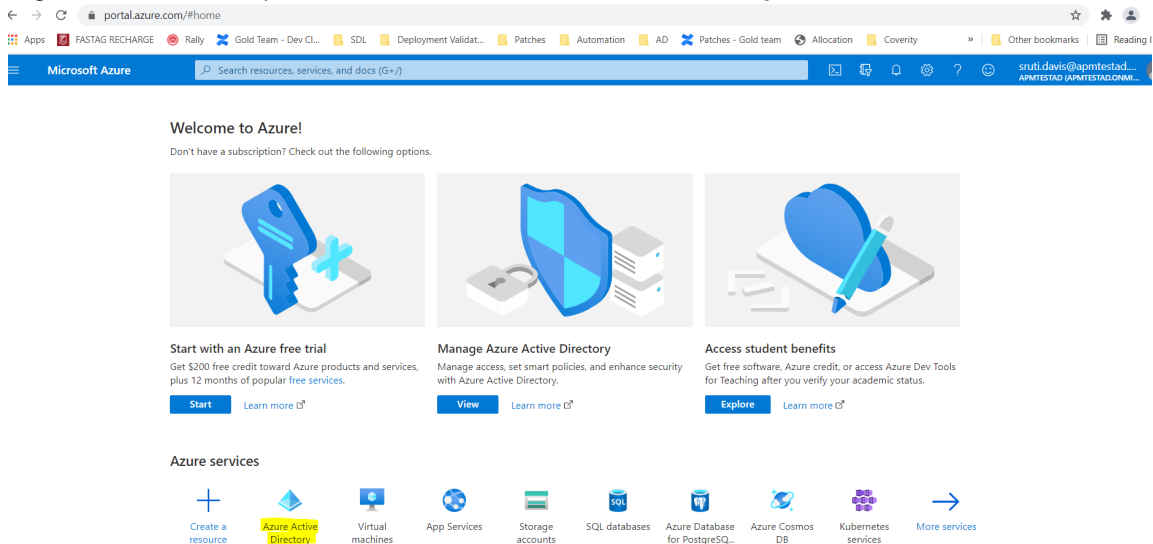
2. In the navigation pane, select **Enterprise applications**.
   The **Enterprise applications – All applications** page appears.
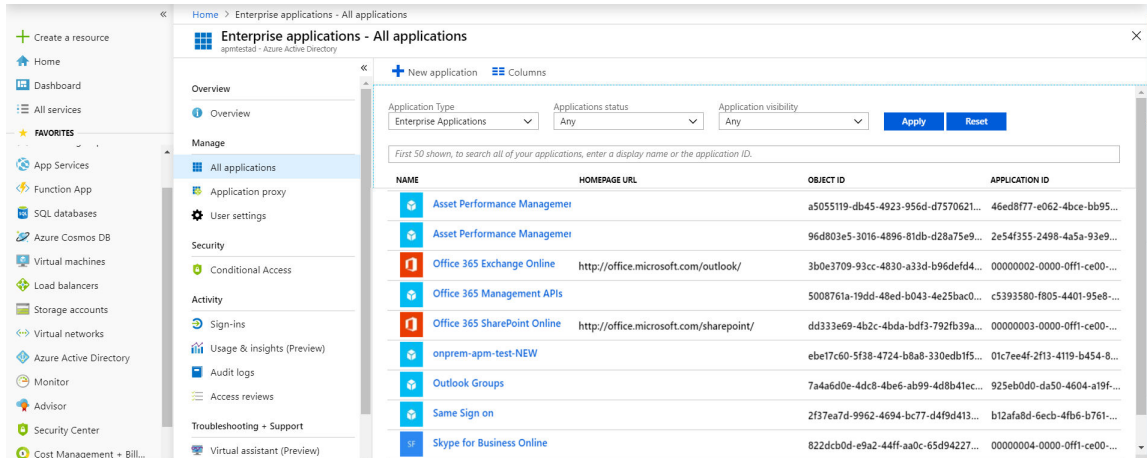
3. Select **New application**.
   The **Add an application** section appears.
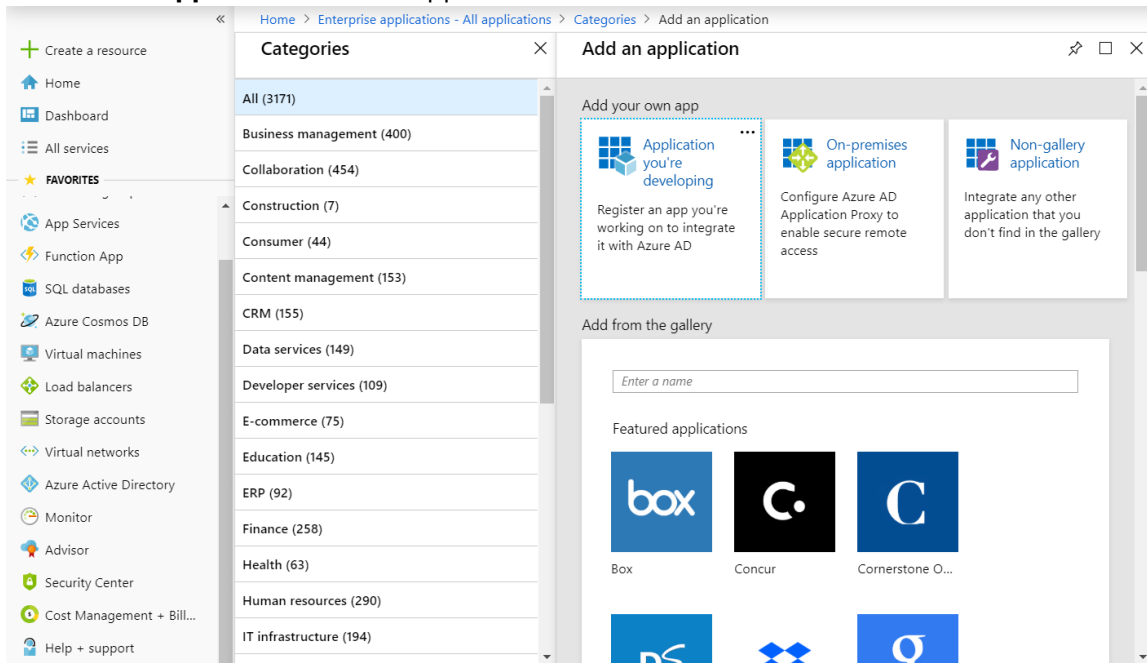
4. Select **Non-gallery application**.
   The **Add your own application** section appears.
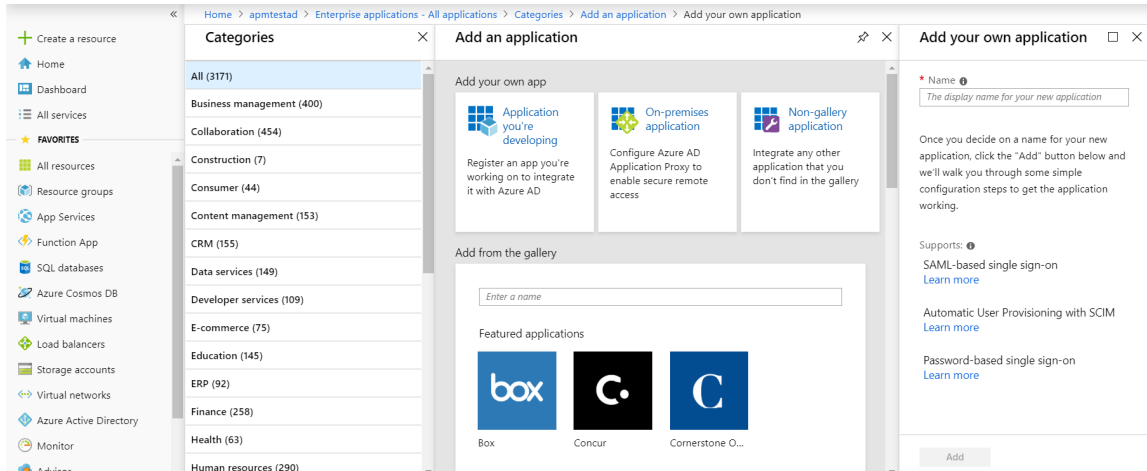
5. In the **Name** box, enter a name for the application that you want to configure with Azure AD, and then select **Add**.
   The page of the added application appears.

6. In the navigation pane of the application page, select **Single sign-on**.
   The **Select a single sign-on method** section appears.
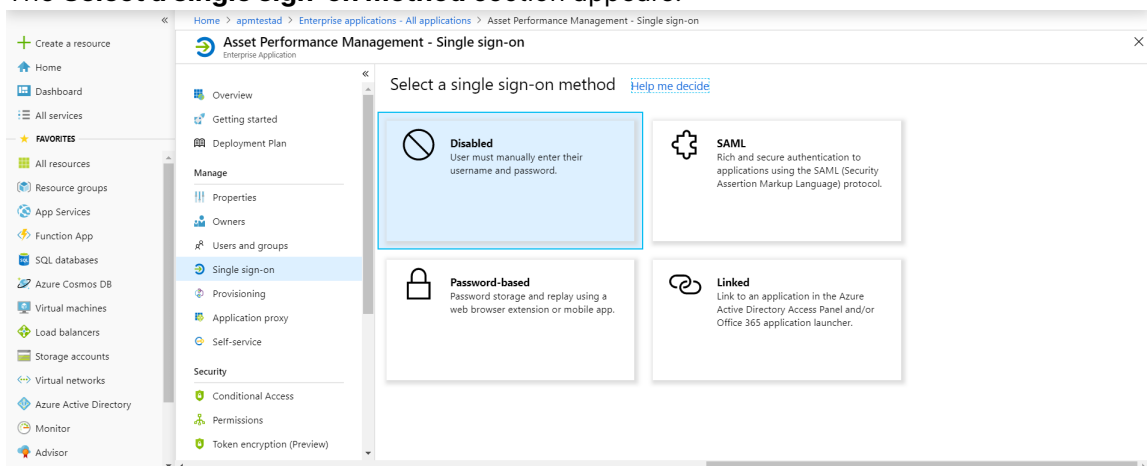
7. Select **SAML**.
   The **Set up Single Sign-On with SAML** section appears.
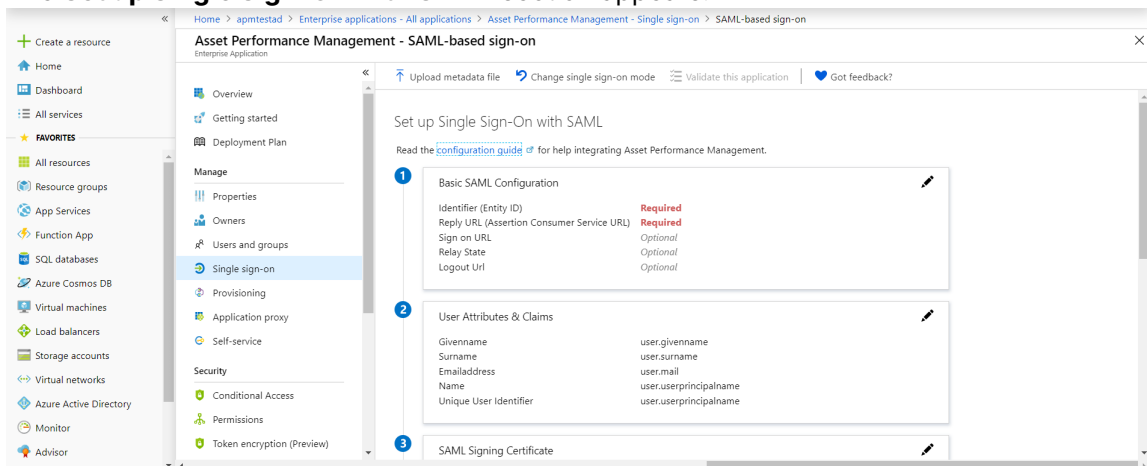
8. In the **Basic SAML Configuration** section, select ✏.

6

The **Basic SAML Configuration** window appears.

Basic SAML Configuration   ✕

💾 Save

* Identifier (Entity ID) ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

[   ]

* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

[   ]

Sign on URL ⓘ
[*Enter a sign on URL*   ]

Relay State ⓘ
[*Enter a relay state*   ]

Logout Url ⓘ
[*Enter a logout url*   ]

9. Enter the following details.

Identifier (Entity ID)	Enter a unique ID. **Note:** This ID will be used in the `saml.json` file for the service provider name. Therefore, note the ID.
Reply URL (Assertion Consumer Service URL)	The application callback URL where the response will be posted. Enter the URL in the following format: `https://<APM Server Name>/Meridium/api/v1/core/security/ssologinauth`, where *<APM Server Name>* is the name of the APM server.
Sign on URL	The application URL, which initiates the same sign-on. Enter the URL in the following format: `https://<APM Server Name>/meridium/index.html`, where <APM *Server Name>* is the name of the APM server.

10. Select **Save**.
11. In the **SAML Signing Certificate** section, select **Download** corresponding to `Certificate (Base 64)`.
12. From the **Set up <Identifier>,** section copy the Login URL and Azure AD Identifier.

Set up sdsso

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/78dd76d6-f3b7...
Azure AD Identifier	https://sts.windows.net/78dd76d6-f3b7-4b89-9ef...
Logout URL	https://login.microsoftonline.com/78dd76d6-f3b7...

Note: The Login URL and Azure AD Identifier will be used in the `saml.json` file for SingleSignOnServiceURL and PartnerIdentityProviderConfigurations Name, respectively.

13. In the application server, copy the downloaded `Certificate (Base 64)` to `C:\Program Files\Meridium\ApplicationServer\api` and install it. Please refer to section Install the Token Signing idp.cer Certificate on the Application Server on page 42 , steps 5 - 8 for installing the certificate.

14. Modify the `saml.json` file found in `C:\Program Files\Meridium\ApplicationServer\api` 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.
- `PartnerCertificates FileName` with the downloaded certificate name.

```
{
"SAML":
{
    "$schema": "https://www.componentspace.com/schemas/saml-config-
schema-v1.0.json",
    "Configurations":
    [
    {
        "LocalServiceProviderConfiguration":
        {
            "Name": "sdsso",
            "AssertionConsumerServiceUrl": "https://<APM Server
Name>/Meridium/api/v1/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": false,
                "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.

    a) Select Users and groups section in the left navigation pane.

    b) Click on Add user/group button to add a new user to this enterprise application. Search for the user in the Users list and then click on Assign.

    Users are added to the enterprise application.

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 10
2. Add Claim Rules on page 21
3. Add Certificates on page 27
4. Federation Service Identifier from ADFS on page 44

Add Relying Party Trusts

Before You Begin

- You must have administrative privileges to configure AD FS.
- Ensure that the /adfs/ls endpoint exists for SAML v2.0.

  Note: To add adfs/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.
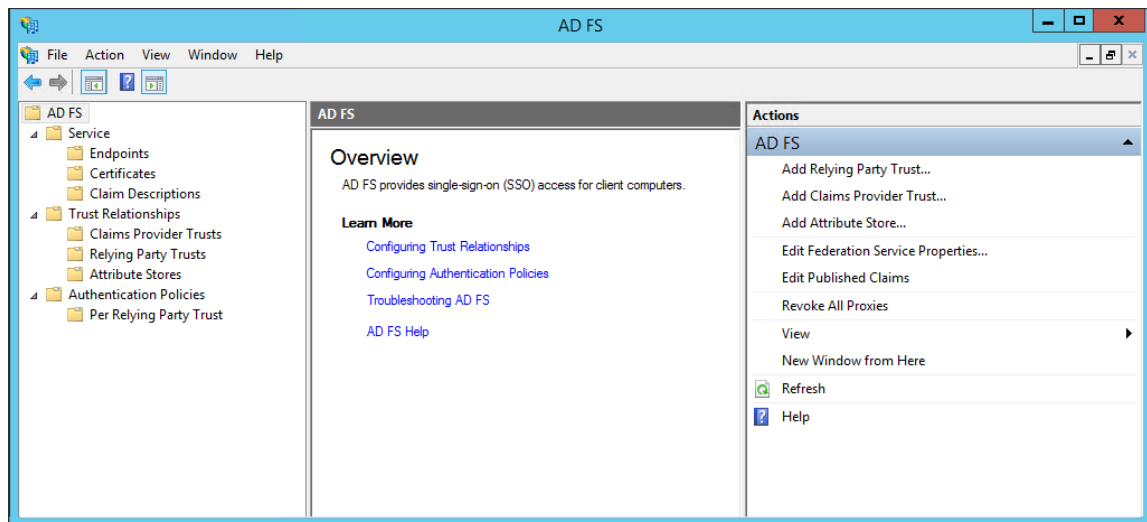
3. In the **Actions** section, select **Add Relying Party Trust**.
   The **Add Relying Party Trust Wizard** appears.
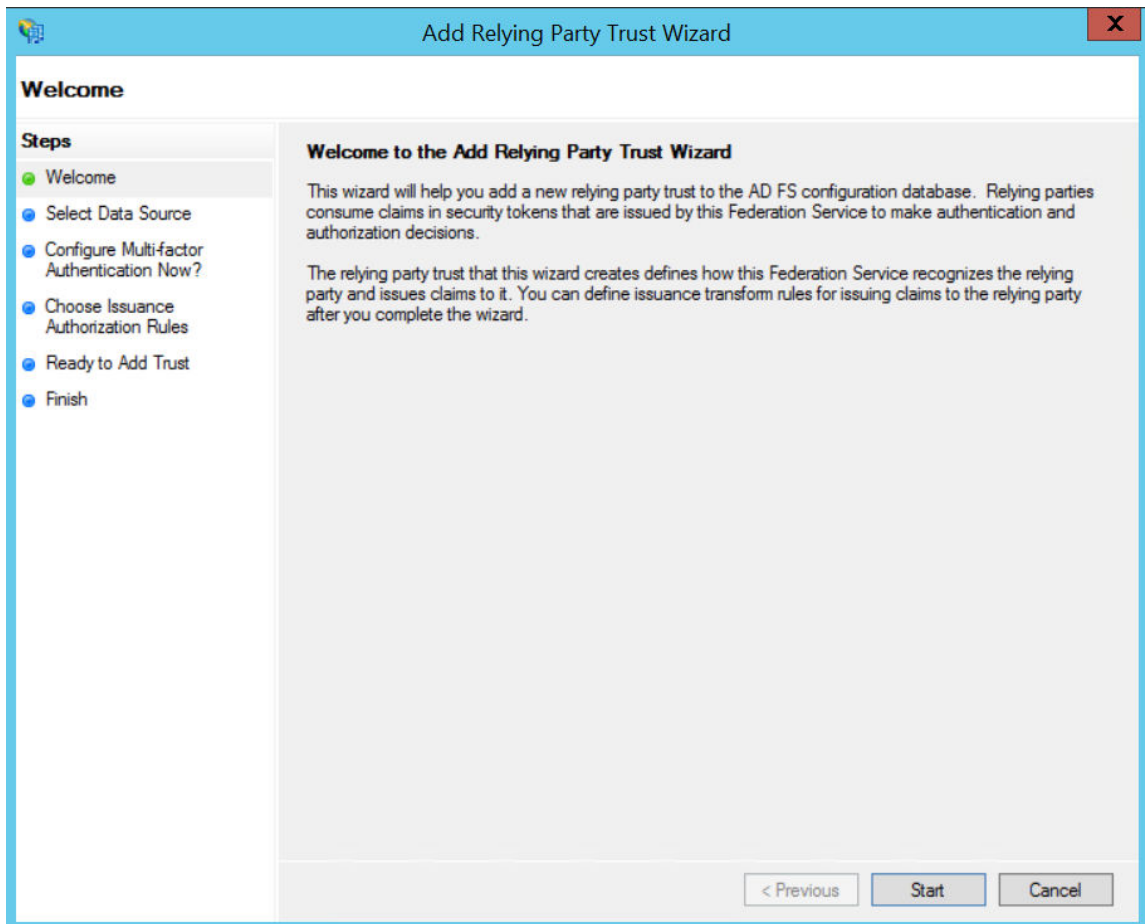
4. Select **Start**.
   The **Select Data Source** page appears.

Add Relying Party Trust Wizard

Select Data Source

Steps

- ● Welcome
- ● Select Data Source
- ● Specify Display Name
- ● Choose Profile
- ● Configure Certificate
- ● Configure URL
- ● Configure Identifiers
- ● Configure Multi-factor Authentication Now?
- ● Choose Issuance Authorization Rules
- ● Ready to Add Trust
- ● Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):
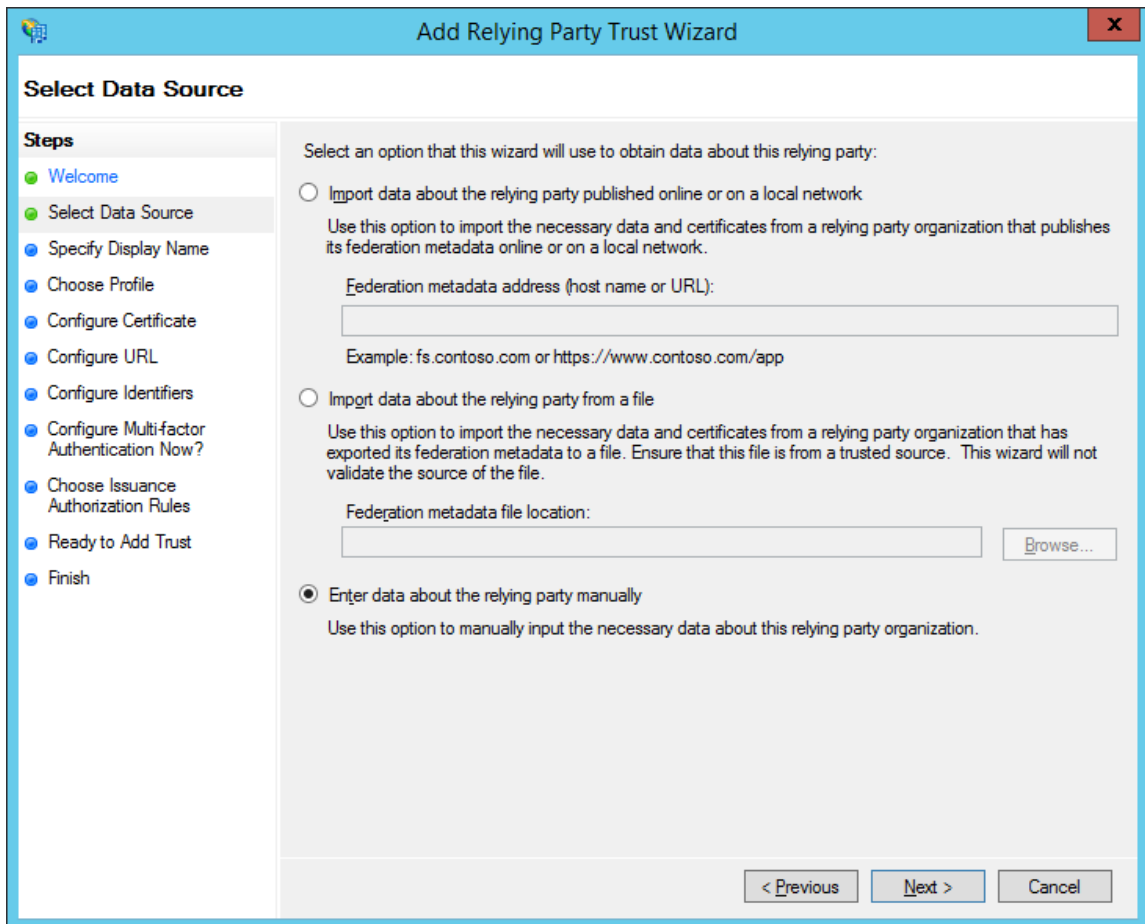
[   ]

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

[   ] [Browse...]

◉ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

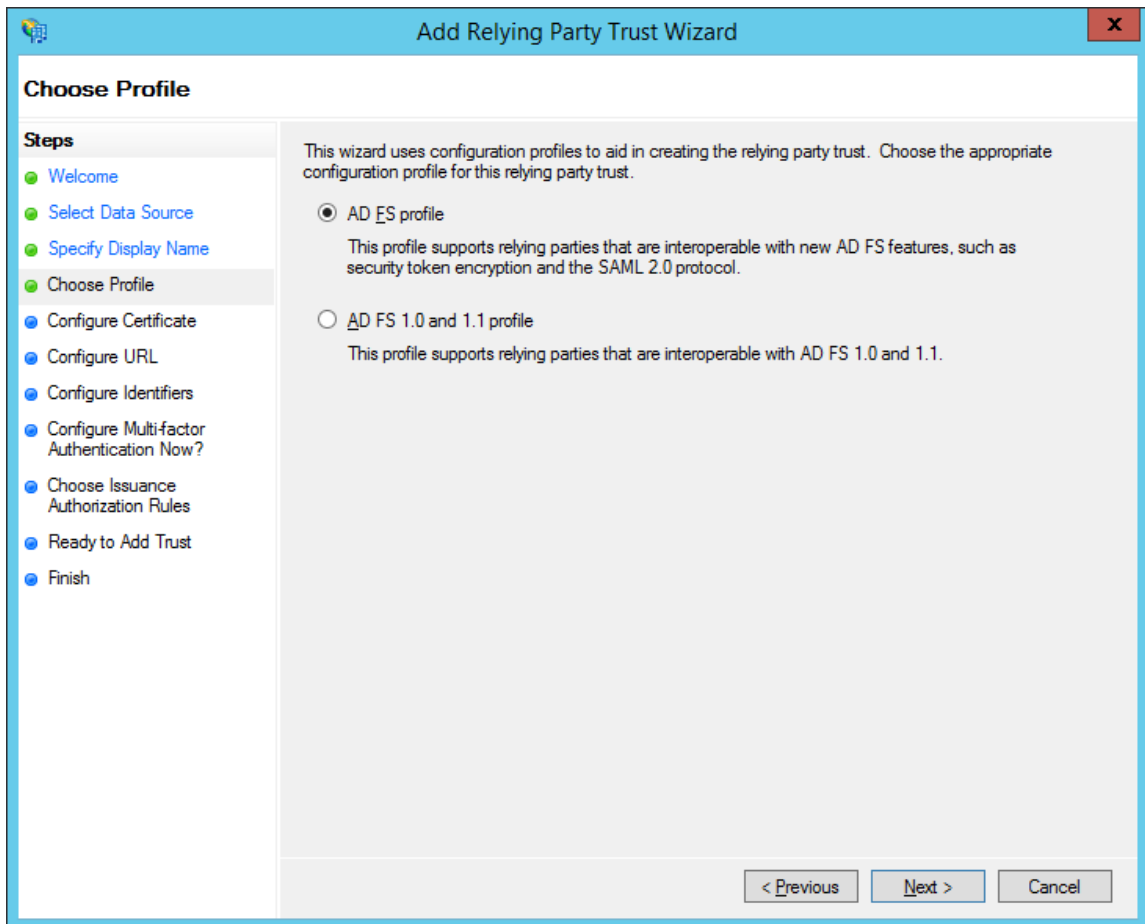[< Previous] [Next >] [Cancel]

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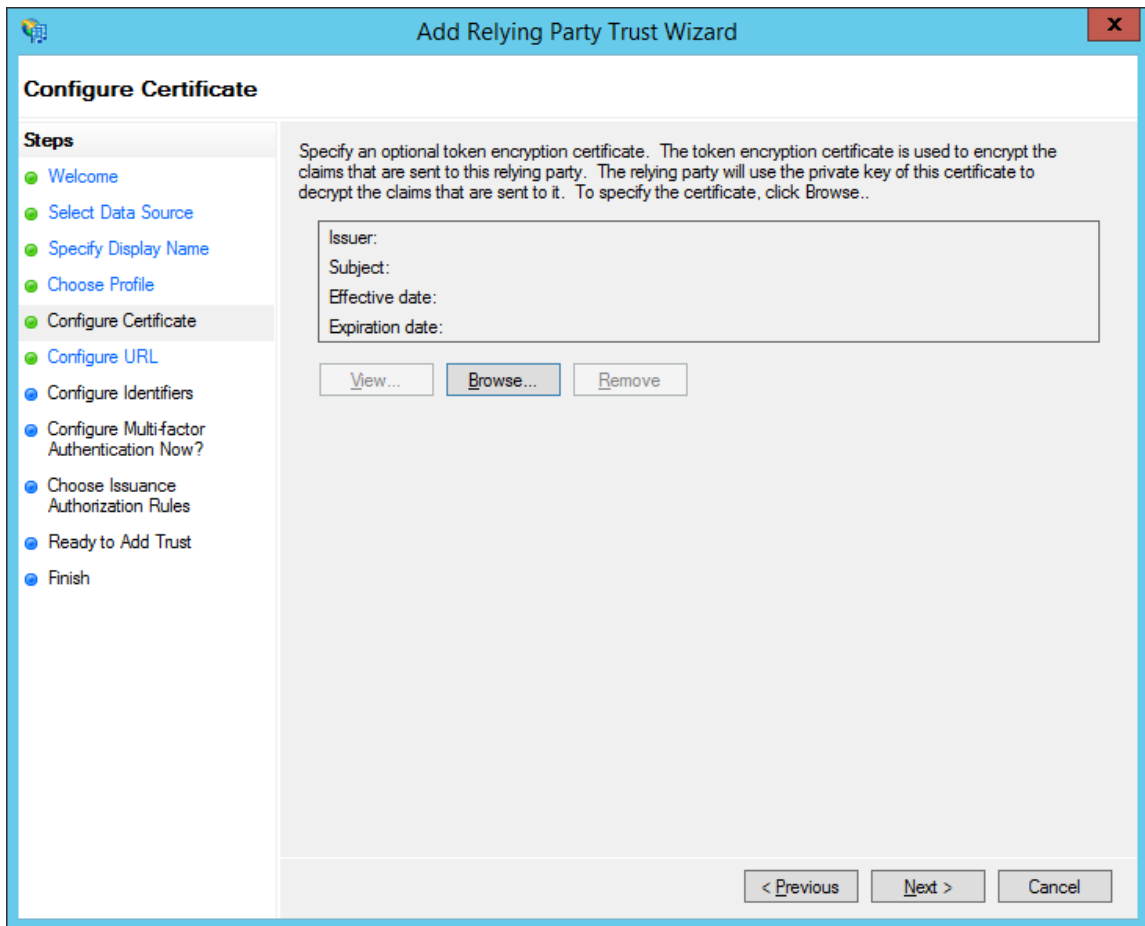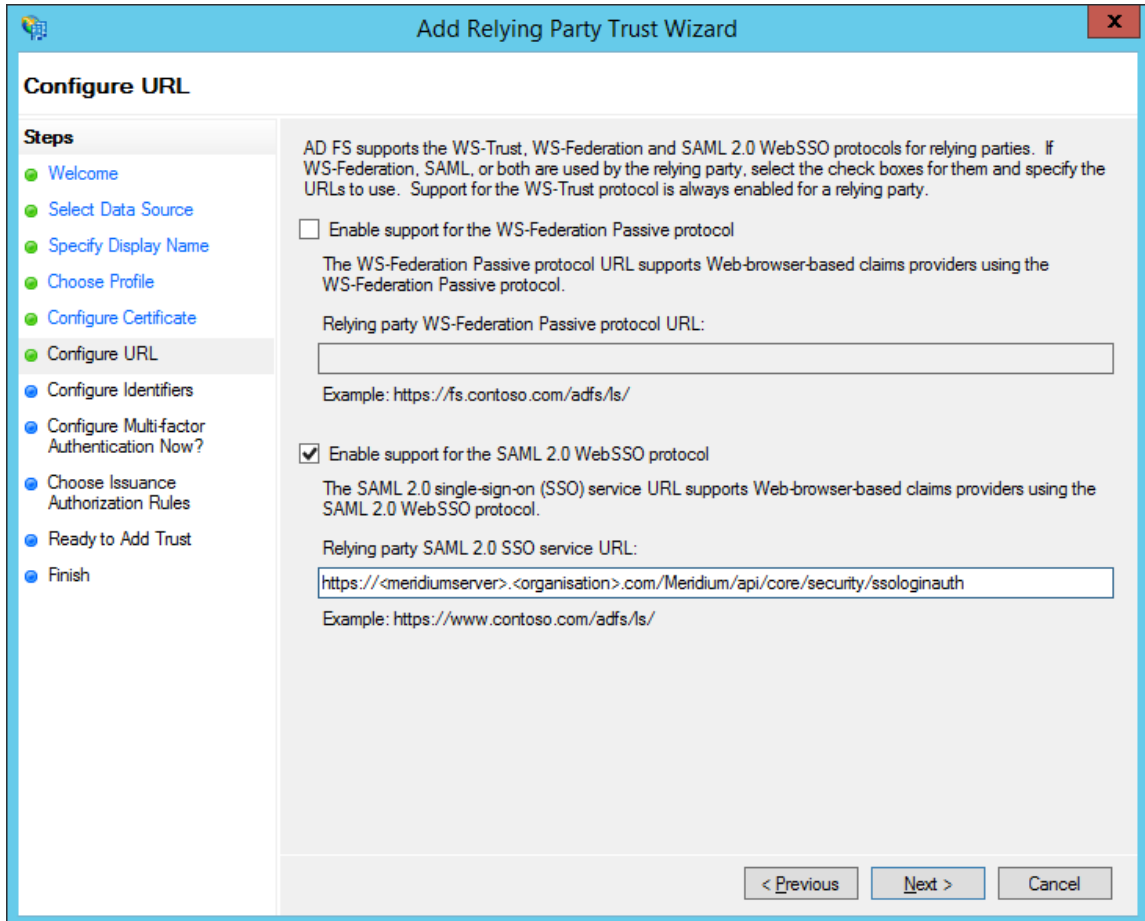   The **Specify Display Name** page appears.

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.

Add Relying Party Trust Wizard

Configure Certificate

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

[View...] [Browse...] [Remove]

[< Previous] [Next >] [Cancel]

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

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://<meridiumserver>.<organisation>.com/Meridium/api/core/security/ssologinauth

Example: https://www.contoso.com/adfs/ls/

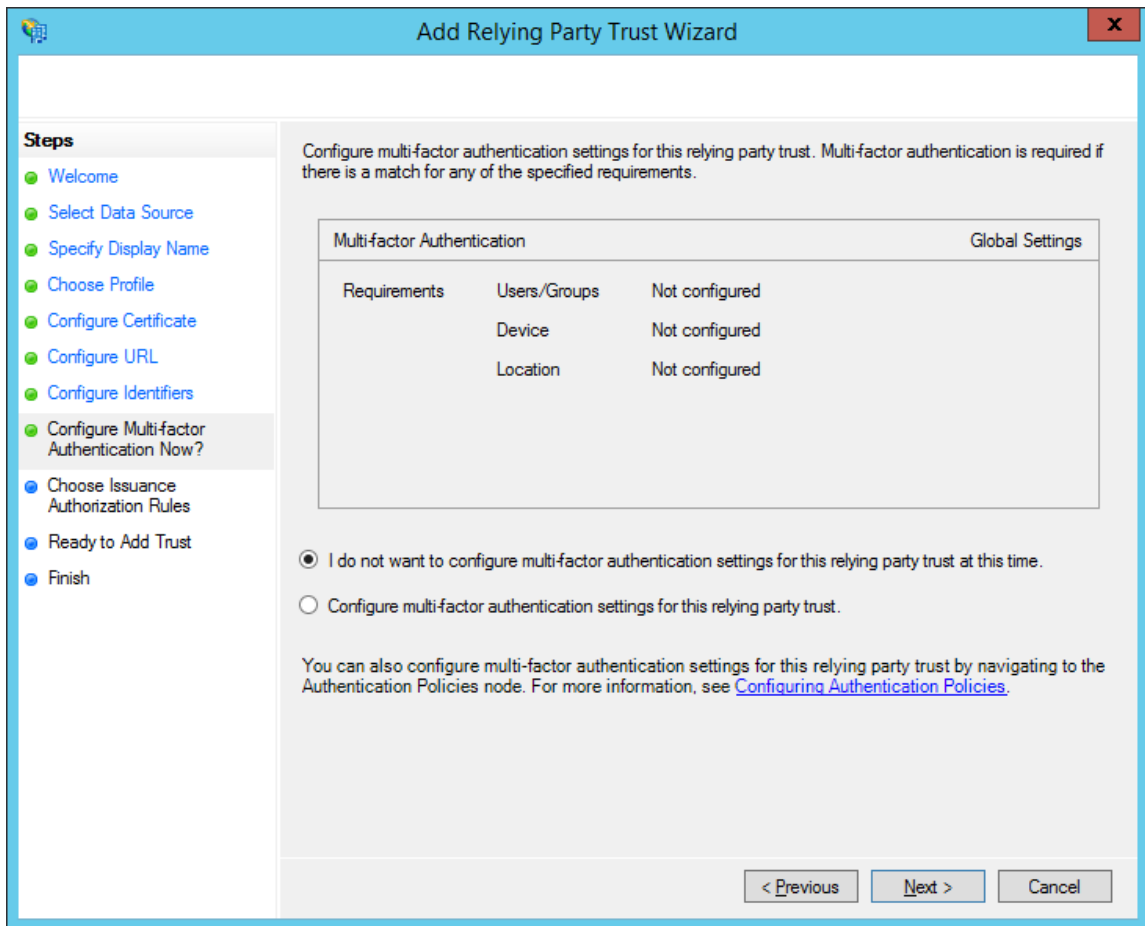< Previous   Next >   Cancel

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://<APM Server Name>/Meridium/api/v1/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 AssertionConsumerServiceUrl in the `saml.json` file.
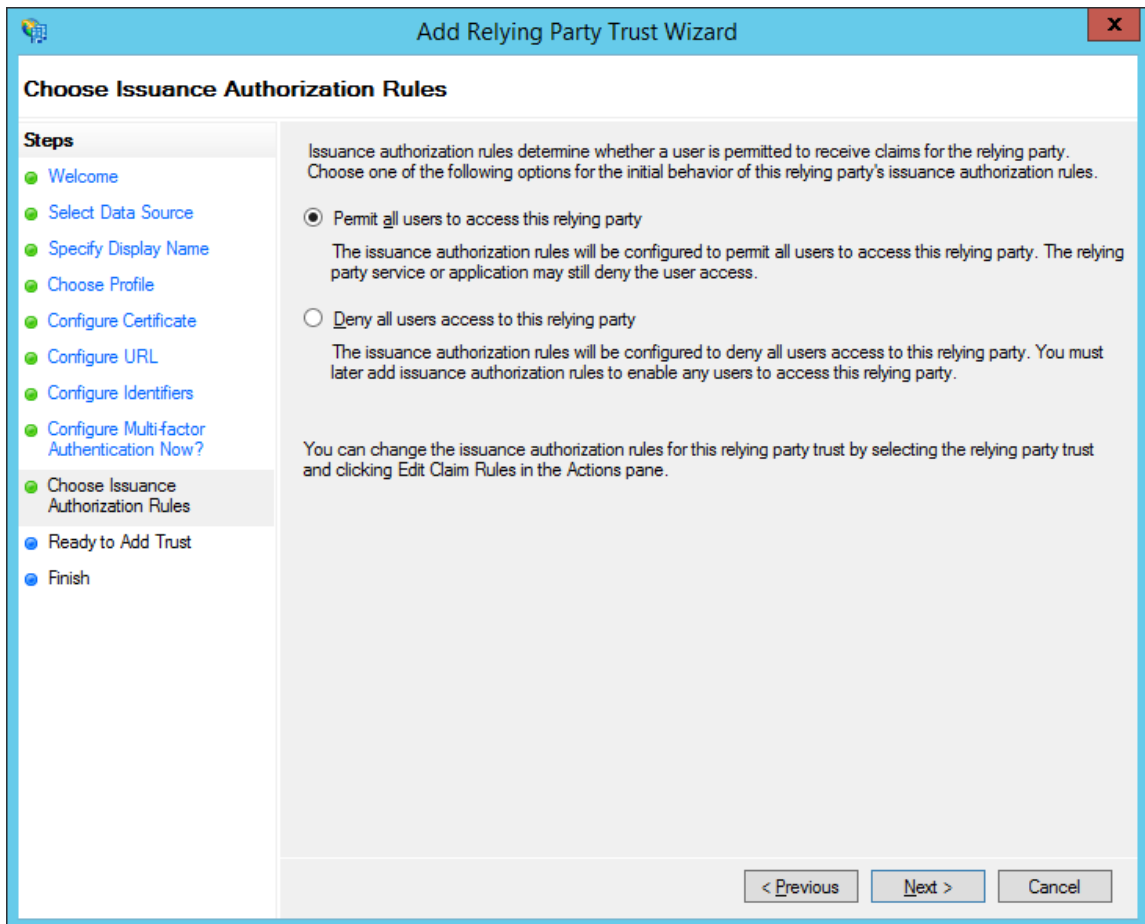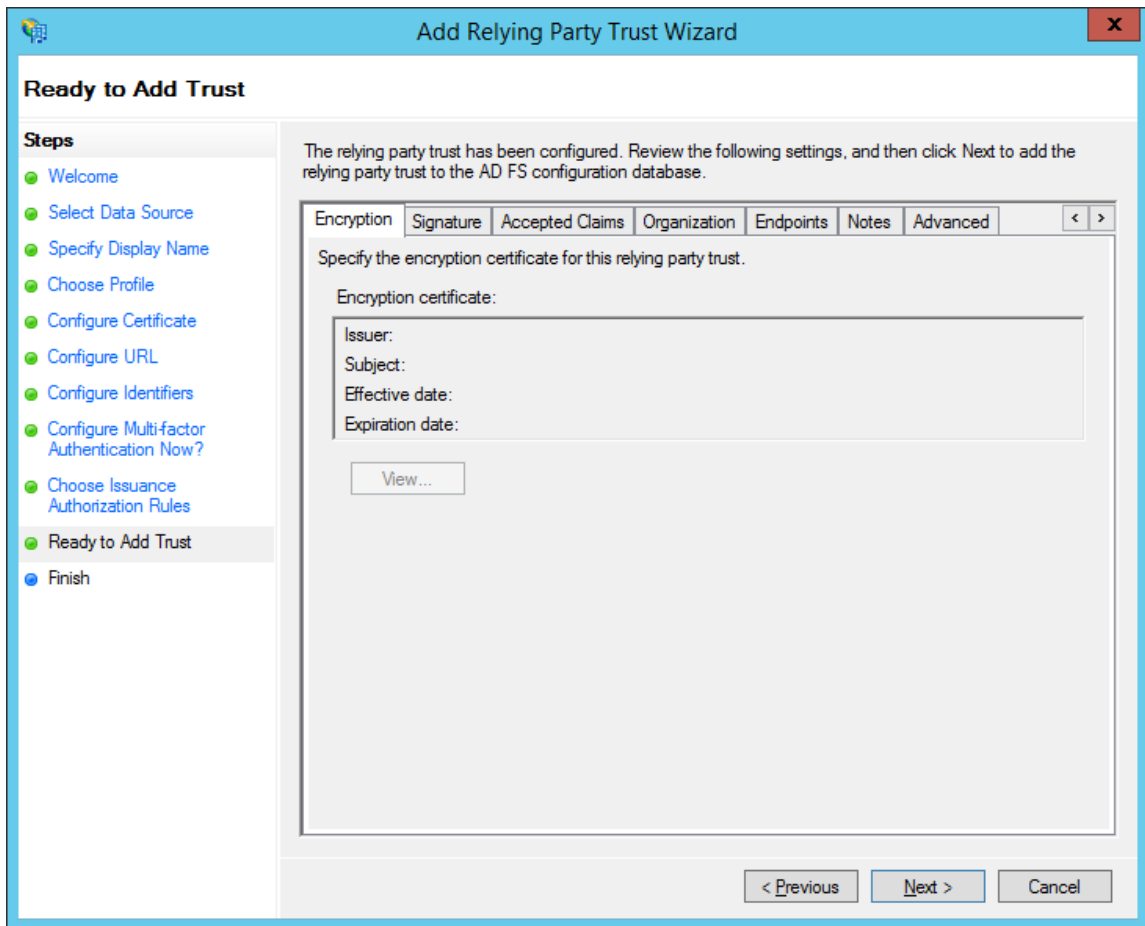
The **Configure Identifiers** page appears.

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.

Add Relying Party Trust Wizard		x

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication			Global Settings
Requirements	Users/Groups	Not configured	
	Device	Not configured	
	Location	Not configured	

⦿ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

< Previous   Next >   Cancel

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.

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

◉ Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous   Next >   Cancel

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

19

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

Procedure

1. In the **AD FS** window, expand the **Trust Relationships** folder, and then select **Relying Party Trusts**.
   The **Relying Party Trusts** page appears.
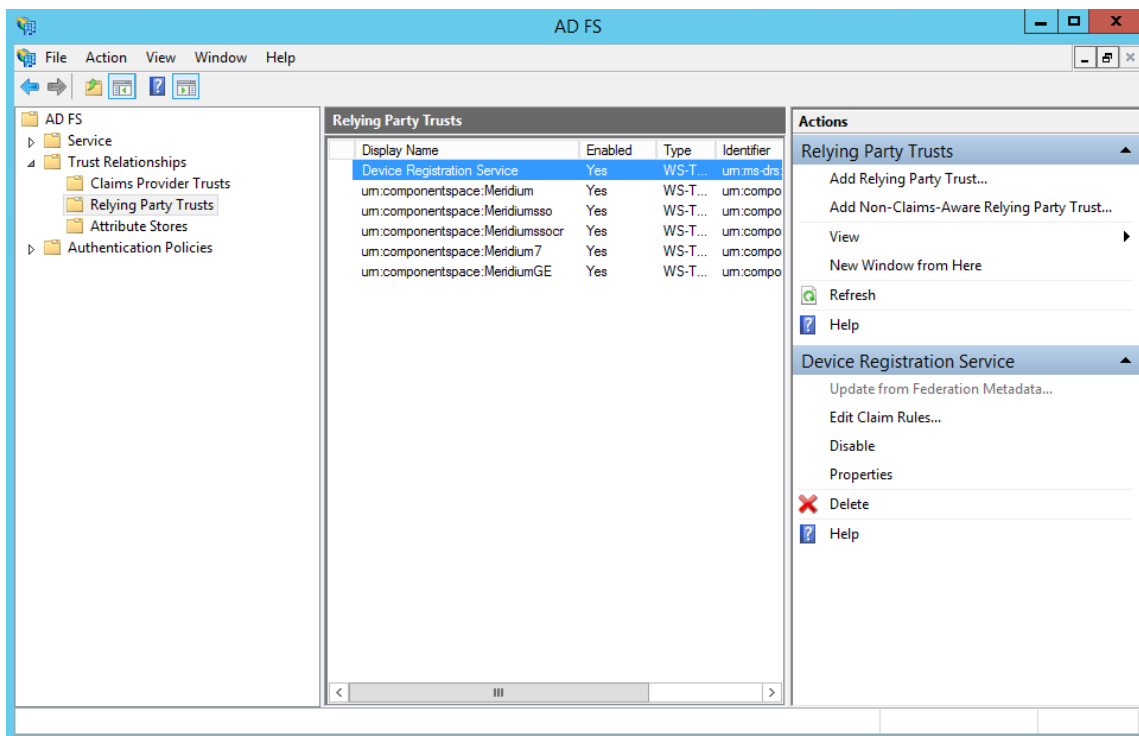
2. Select **urn:componentspace:Meridium**, and then, in the **Actions** section, select **Edit Claim Rules**.
   The **Edit Claim Rules for urn:componentspace:Meridium** window appears. Select **Issuance Transform Rules** tab.
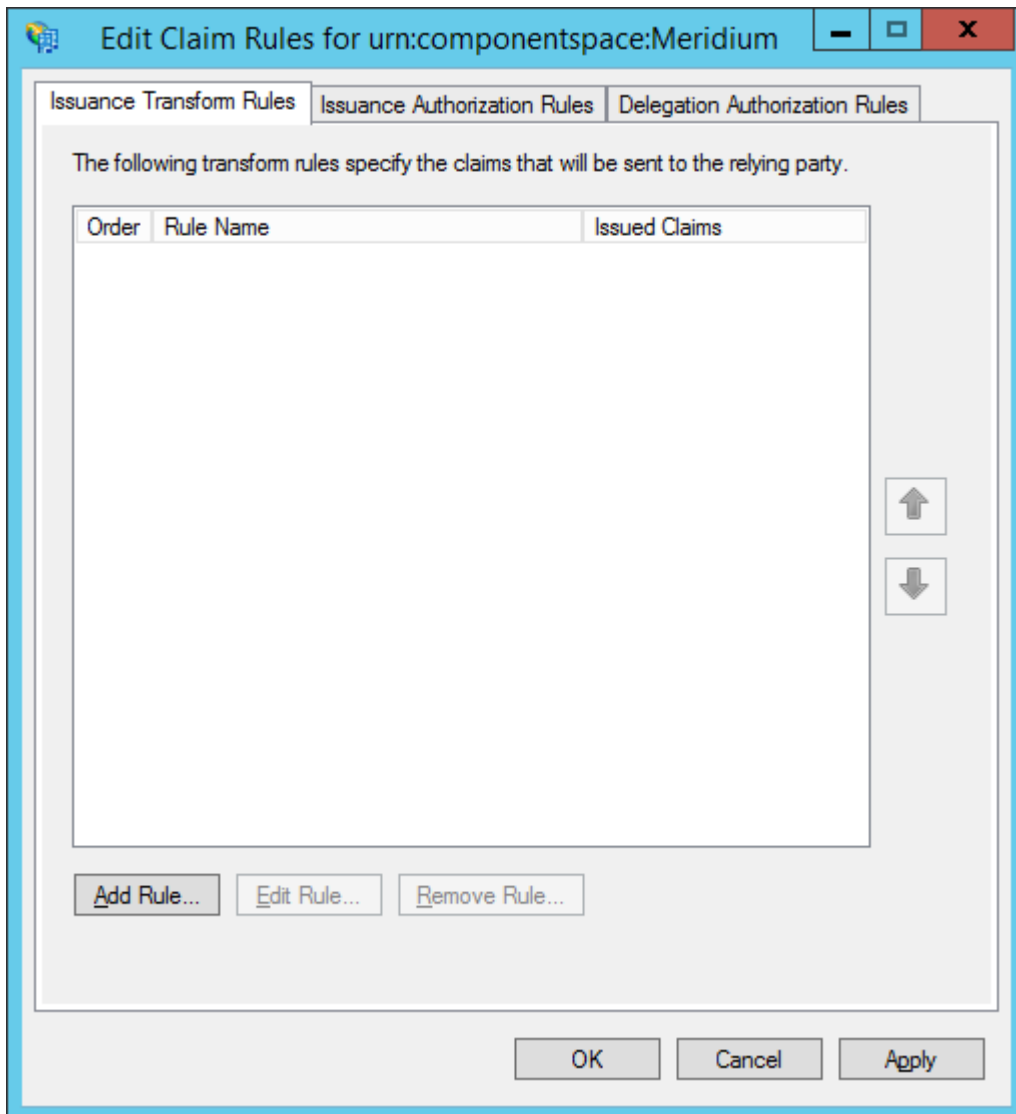
3. Select **Add Rule**.
   The **Add Transform Claim Rule Wizard** window appears.
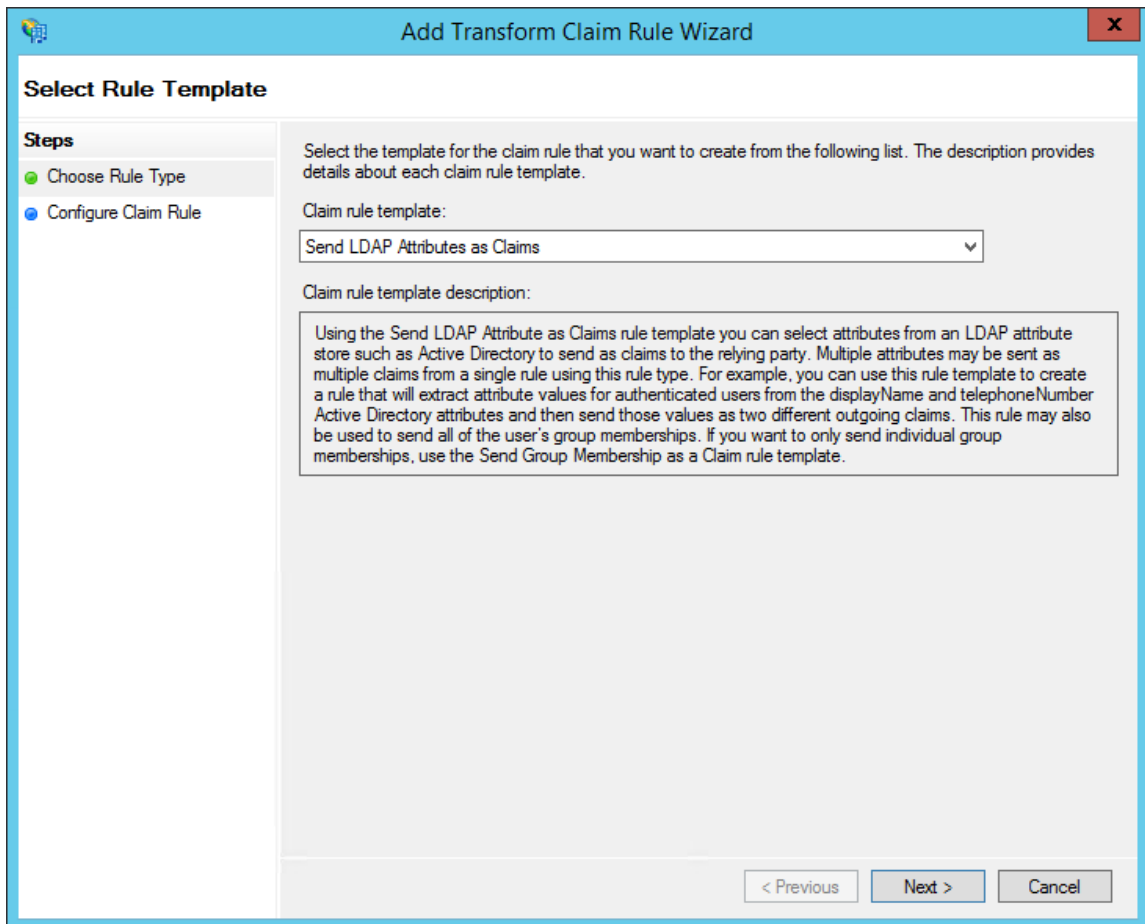
4. In the **Claim rule template** drop-down list box, select **Send LDAP Attributes as Claims**, and then select **Next**.
   The **Configure Rule** page appears.
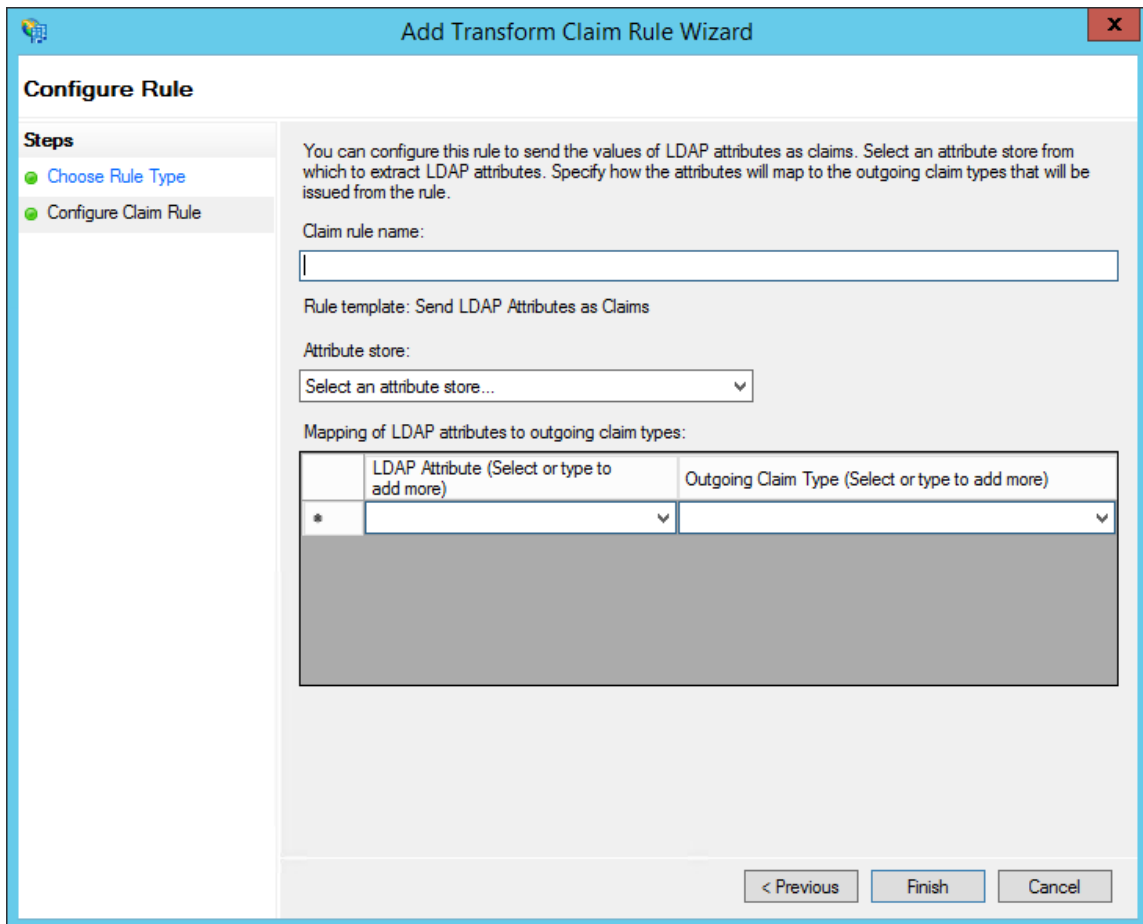
5. In the **Claim rule name** box, enter **Meridium Claims**, and then, in the **Attribute store** drop-down list box, select **Active Directory**.

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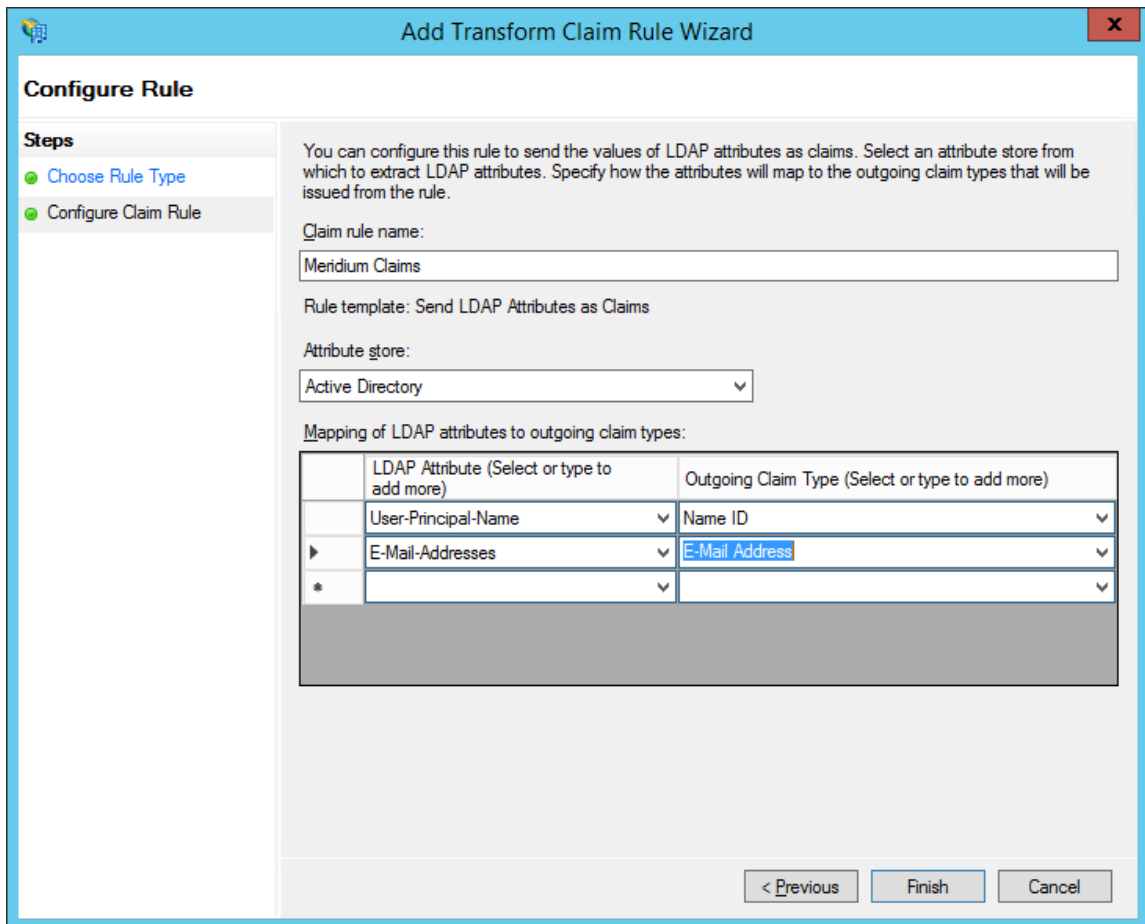
7. Select **Finish**.
   The **Edit Claim Rules for urn:componentspace:Meridium** window appears.
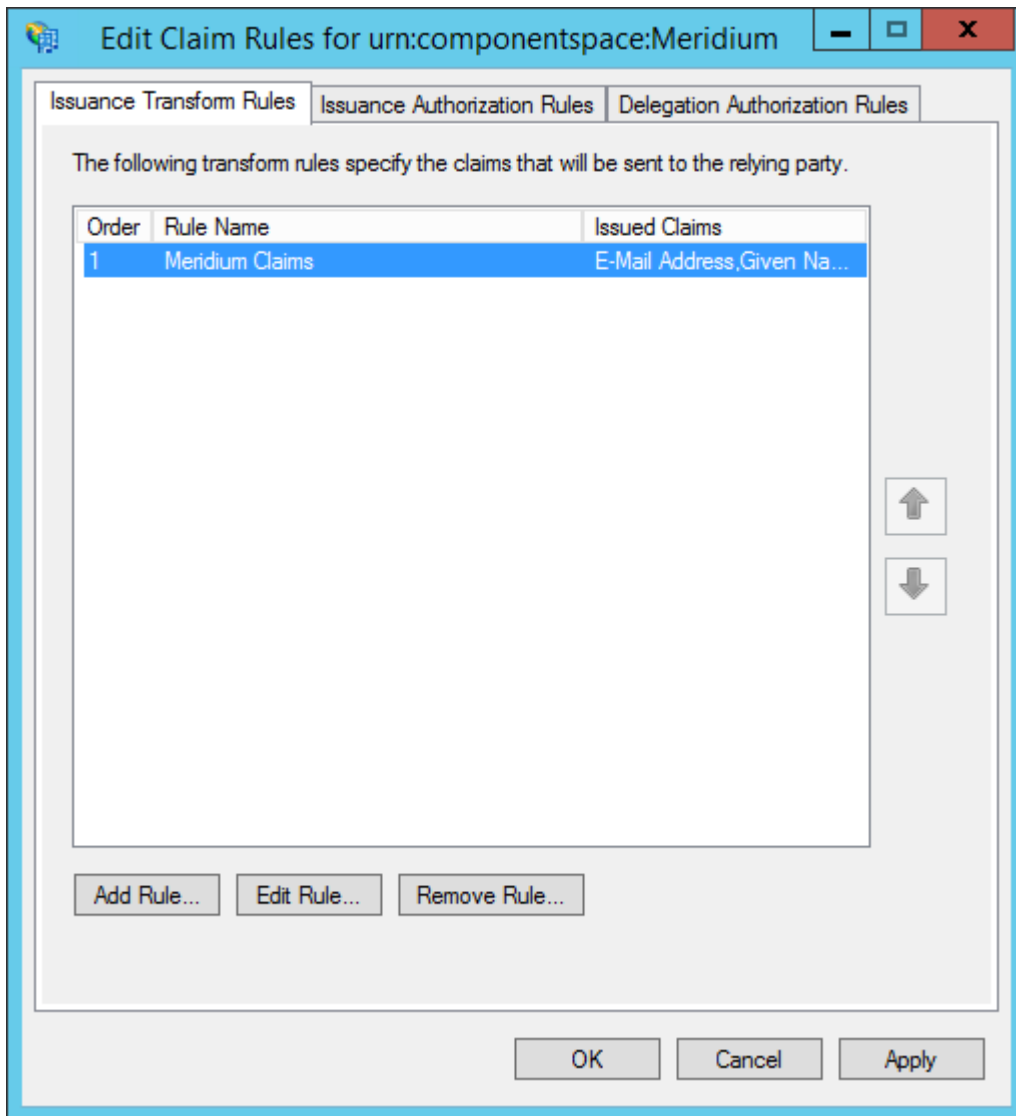
8. Select **OK**.
   The claim rule is added to the **Edit Claim Rules for urn:componentspace:Meridium** window.

Next Steps

- Add Certificates on page 27

Add Certificates

About This Task

To add certificates, you must perform the following tasks:

Procedure

1. Install the Service Provider certificate (sp.pfx) on page 28
2. Export the Public Key Certificate on page 32

Install the Service Provider certificate (sp.pfx)

Procedure

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

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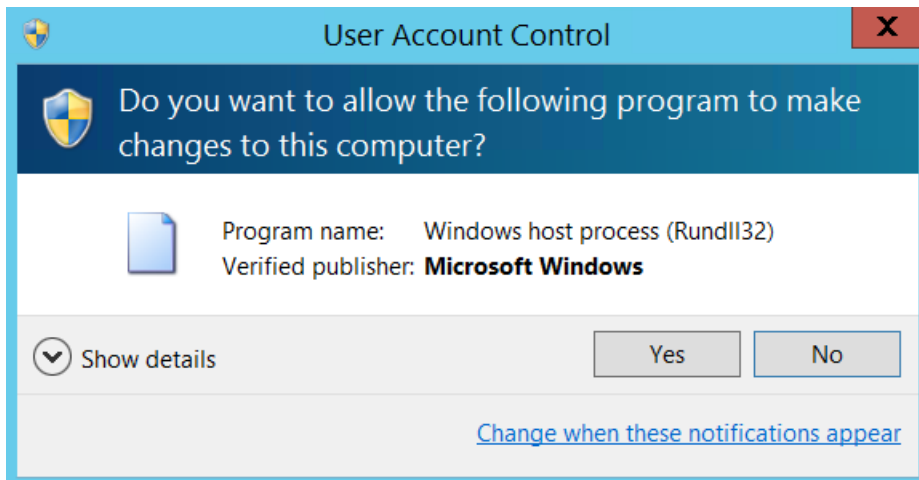
4. Select **Yes**.
The **Certificate Import Wizard** appears, and the **File Name** box displays the file path where the certificate is located.

5. Select **Next**.

×

← 🪪 Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

[password]

☑ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

[Next]   [Cancel]

6. Enter a password `password`, and then select **Next**.
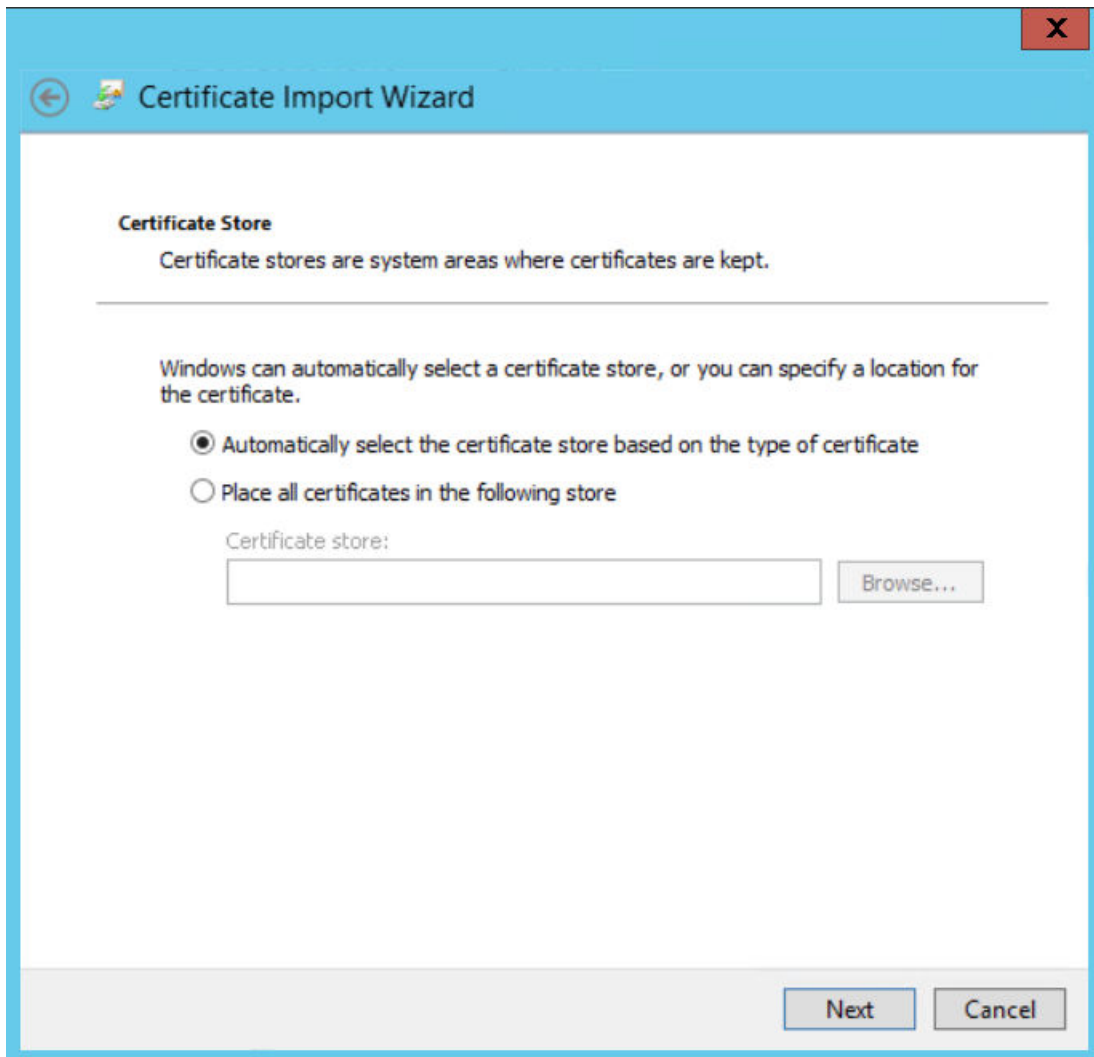
7. Select **Automatically select the certificate store based on the type of certificate**.
    The **Completing the Certificate Import Wizard** appears.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\Program Files\Meridium\ApplicationServer\api\sp.pfx
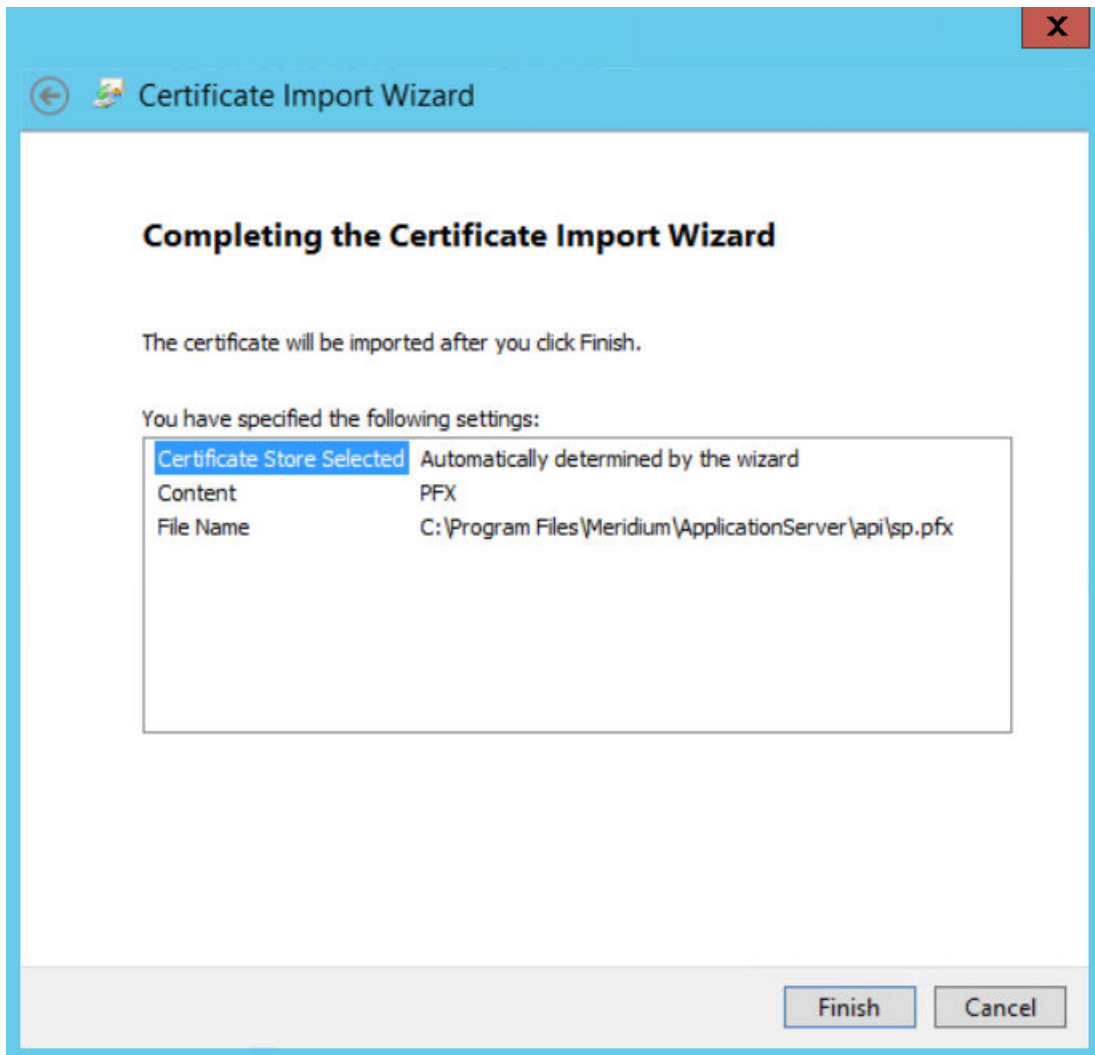
8. Select **Finish**.

Next Steps

-

Export the Public Key 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.
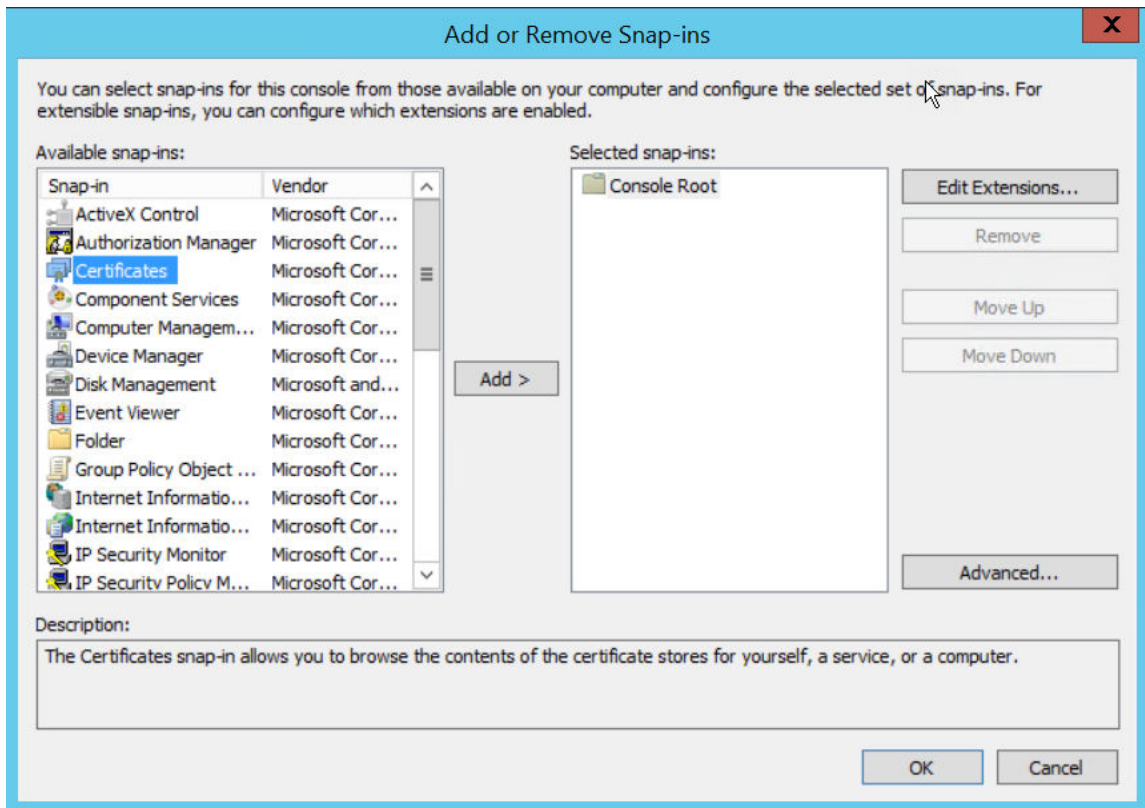
3. Select **Add**.
   The **Certificates snap-in** window appears.
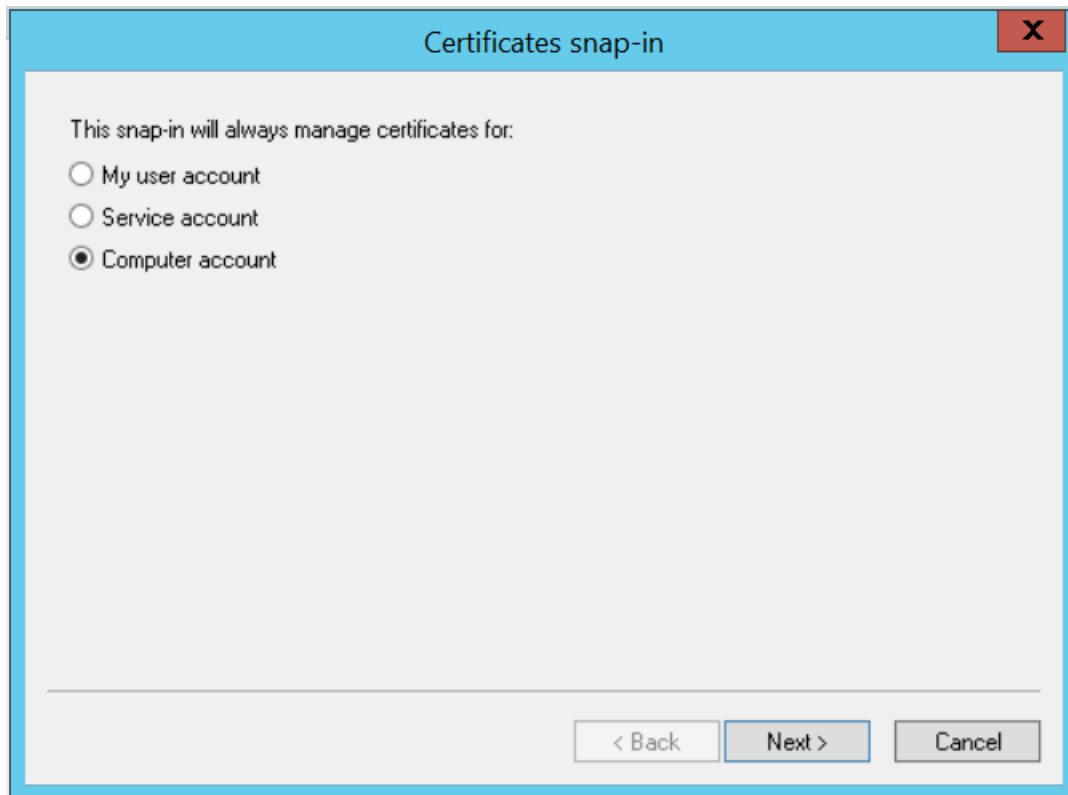
4. Select the **Computer account** option, and then select **Next**.
The **Select Computer** window appears.
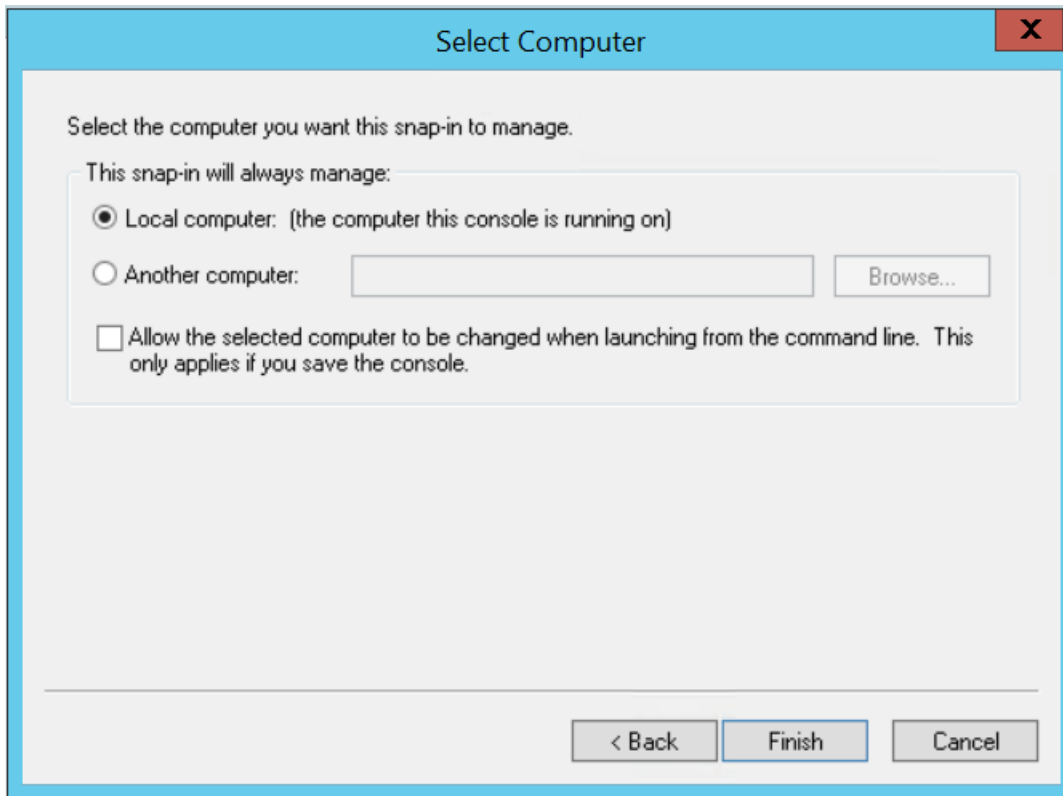
5. Select the **Local computer** option, and then select **Finish**.
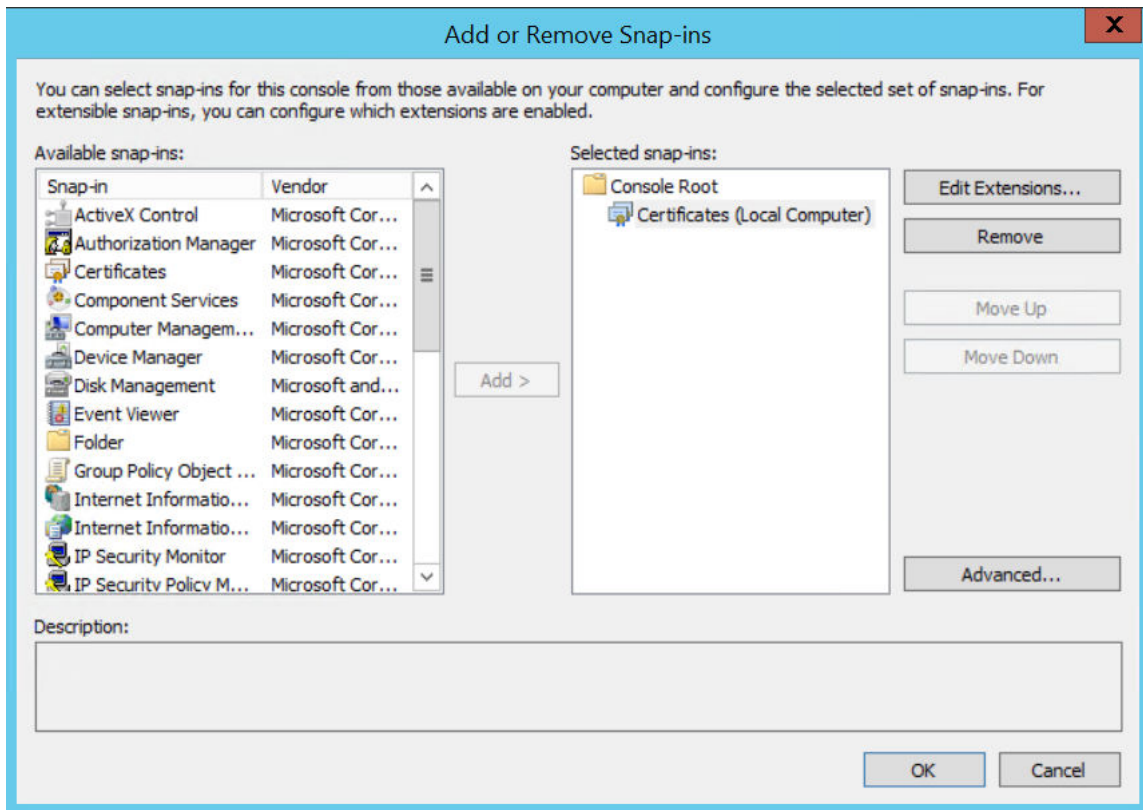
6. In the **Add or Remove Snap-ins** window, select **OK**.
   The certificate appears in the **Personal** > **Certificates** folder of the **Certificates (Local Computer)** folder.
7. Select **Certificates (Local Computer)**, then select **Personal**, and then select **Certificates**.
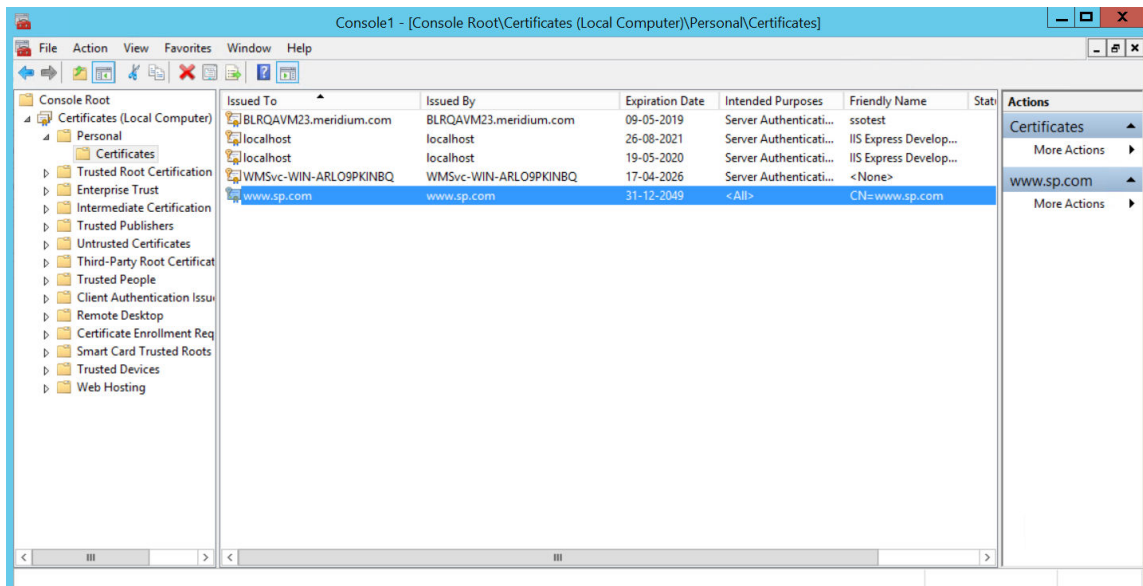
8. Right-click the certificate that you have installed, select **All Tasks**, and then select **Export**.
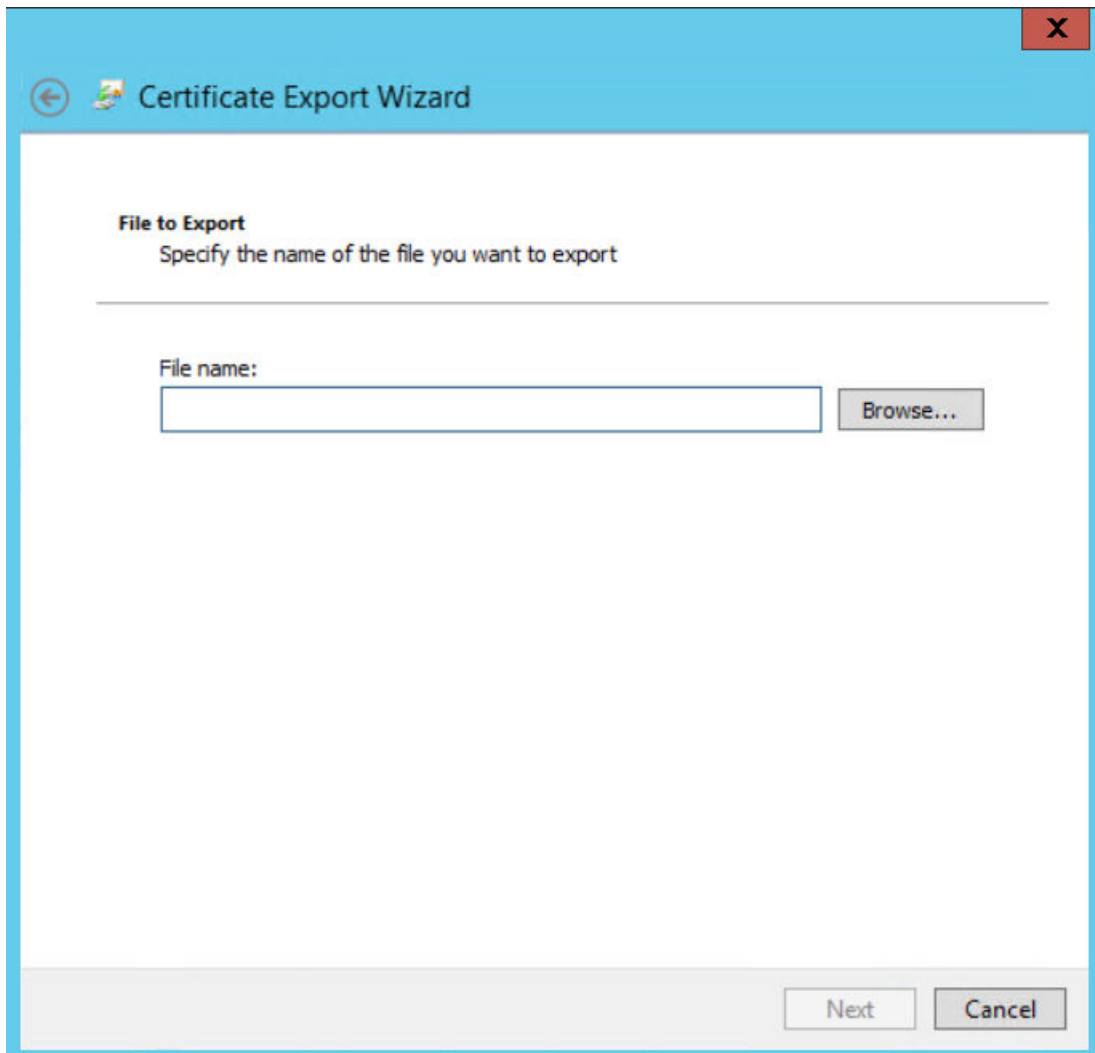   The **Certificate Export Wizard** appears.
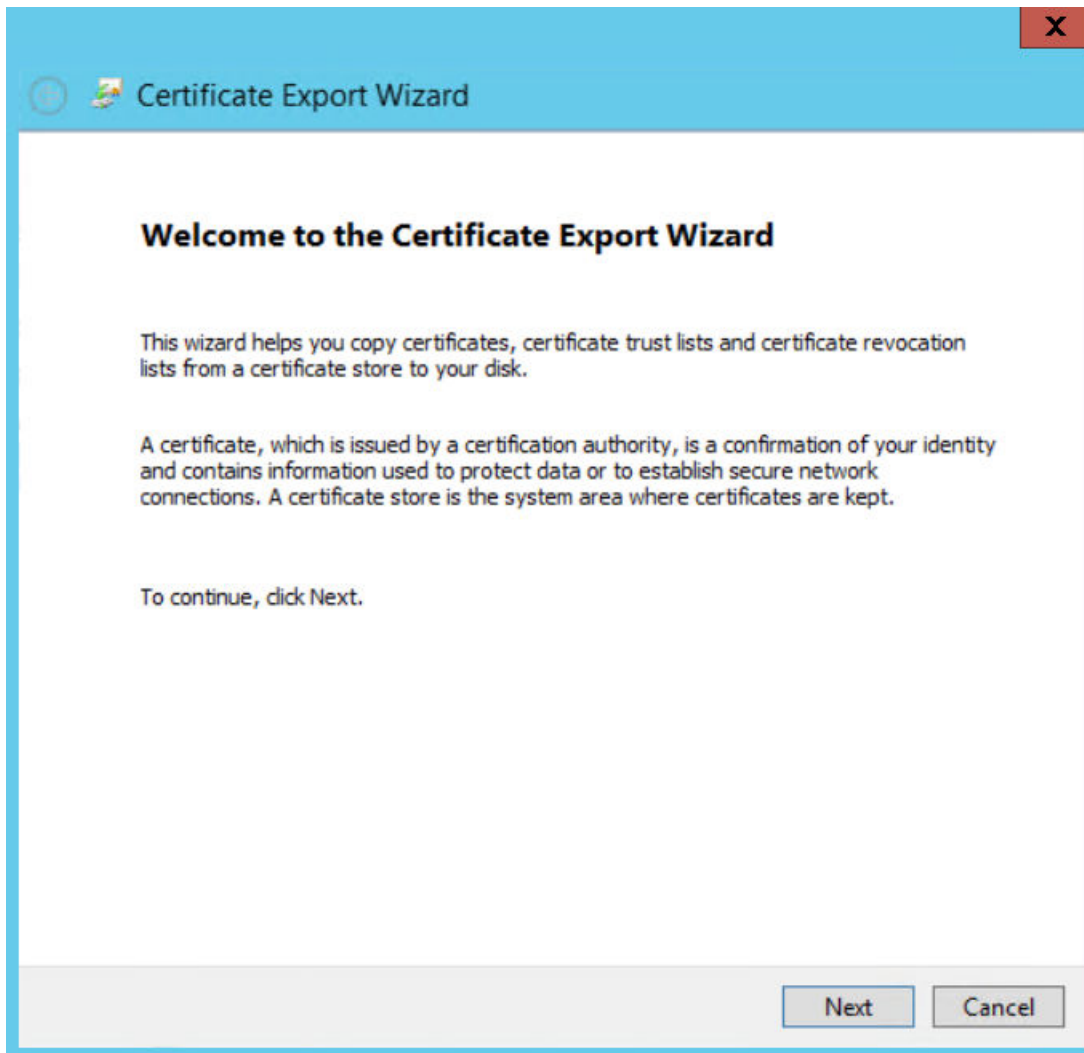
9. Select **Next**.
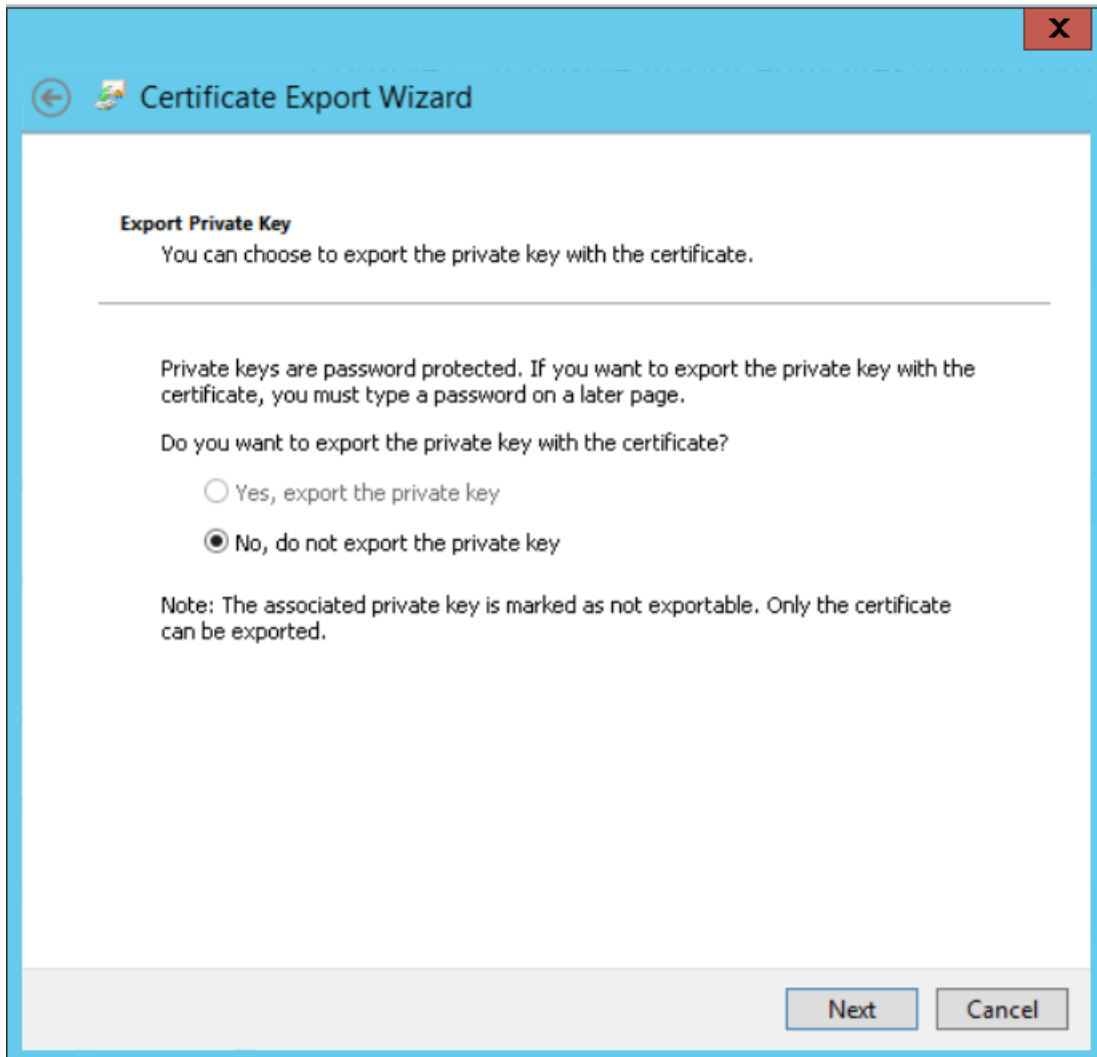
10.Select the **No, do not export the private key** option, and then select **Next**.
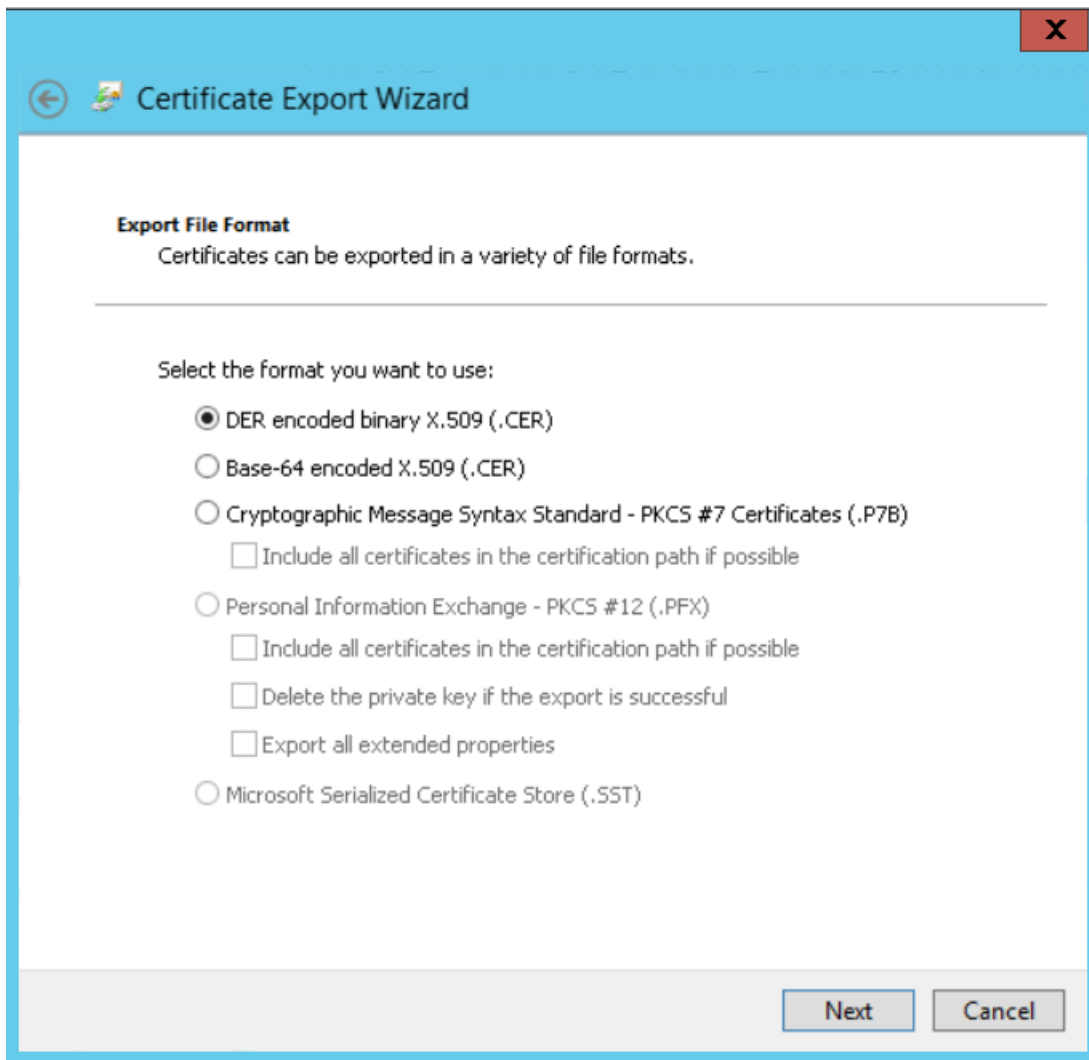
11. Select **DER encoded binary X.509 (.CER)**, and then select **Next**.

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**.
15. Copy the exported certificate to Active Directory and install it. Please refer to section for detailed process of installing the certificate.

Next Steps
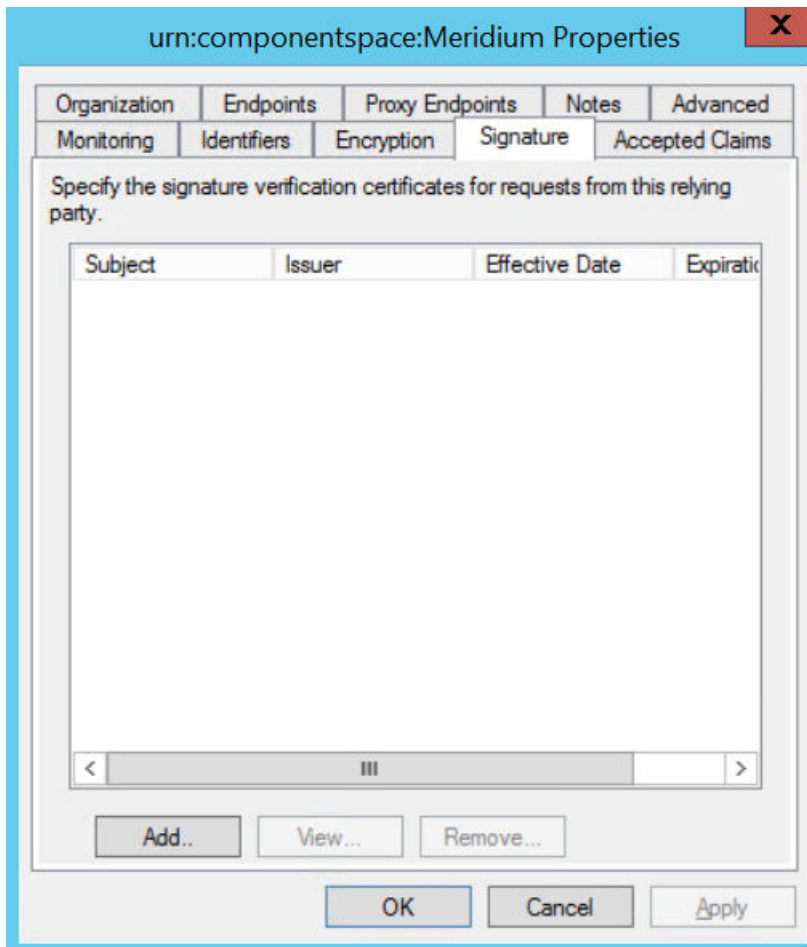
-

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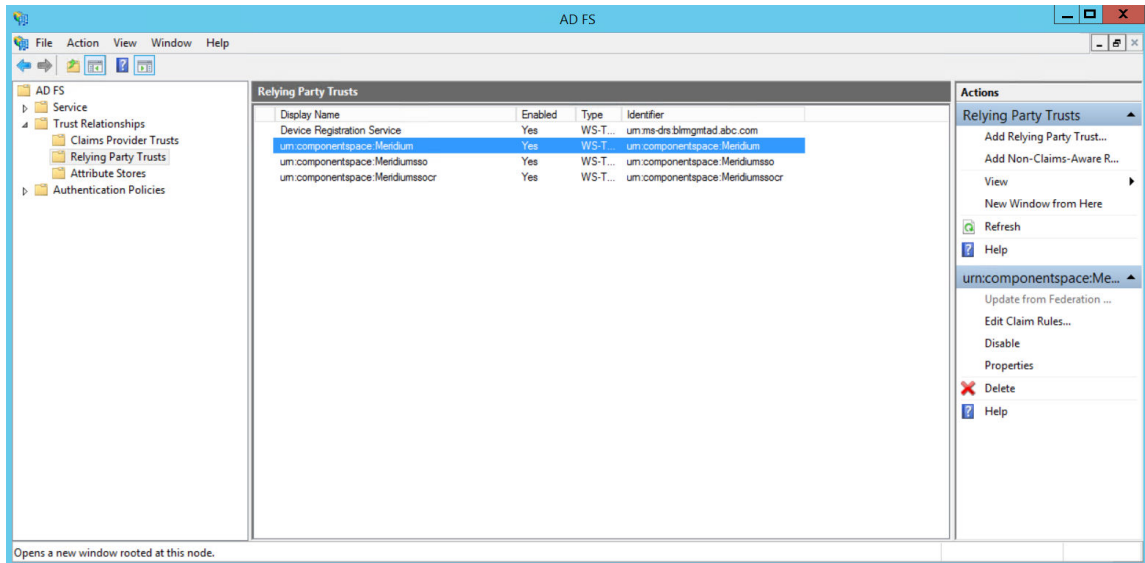
3. Expand **Trust Relationships**, and then select **Relying Party Trusts**.
4. Select **urn:componentspace:Meridium**, and then, in the **Actions** section, select
    Properties.
    The **urn:componentspace:Meridium Properties** window appears.

urn:componentspace:Meridium Properties

| Organization | Endpoints | Proxy Endpoints | Notes | Advanced |
| Monitoring | Identifiers | Encryption | Signature | Accepted Claims |

Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiratic

Add.. | View... | Remove...

OK | Cancel | Apply

5. Select the **Signature** tab, and then select **Add**.
6. 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**.
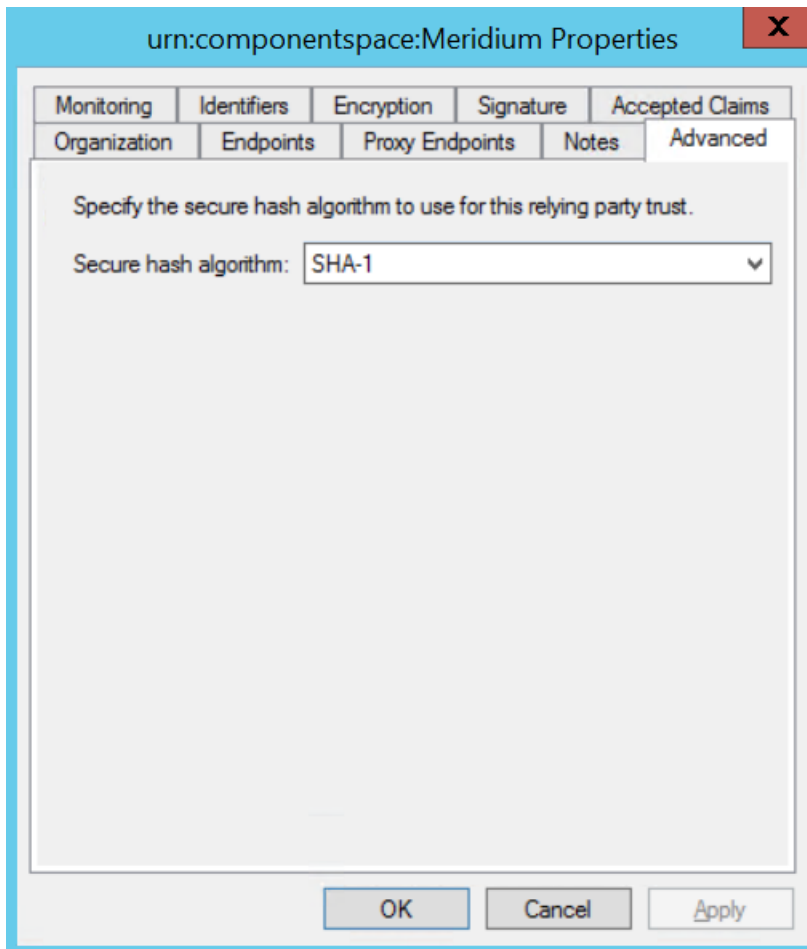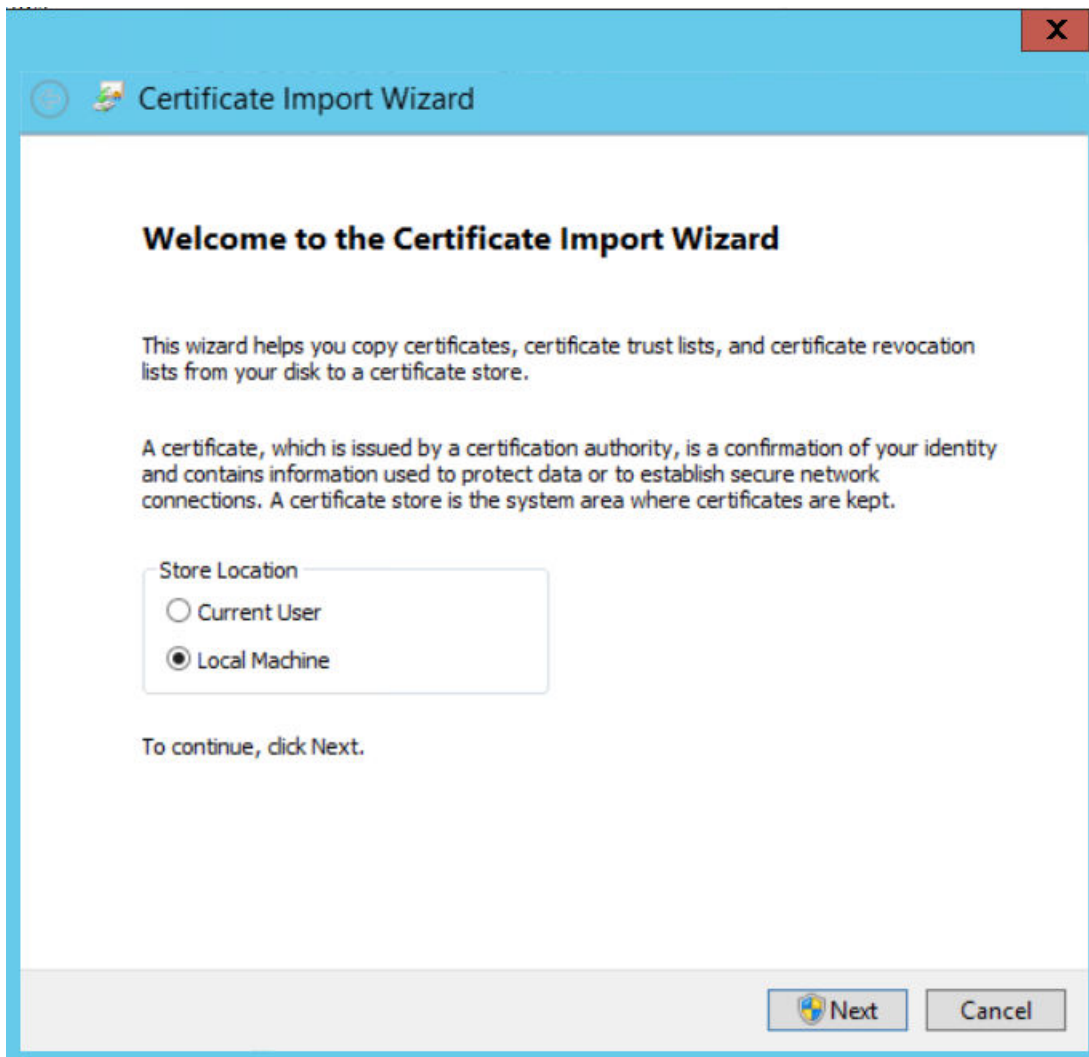
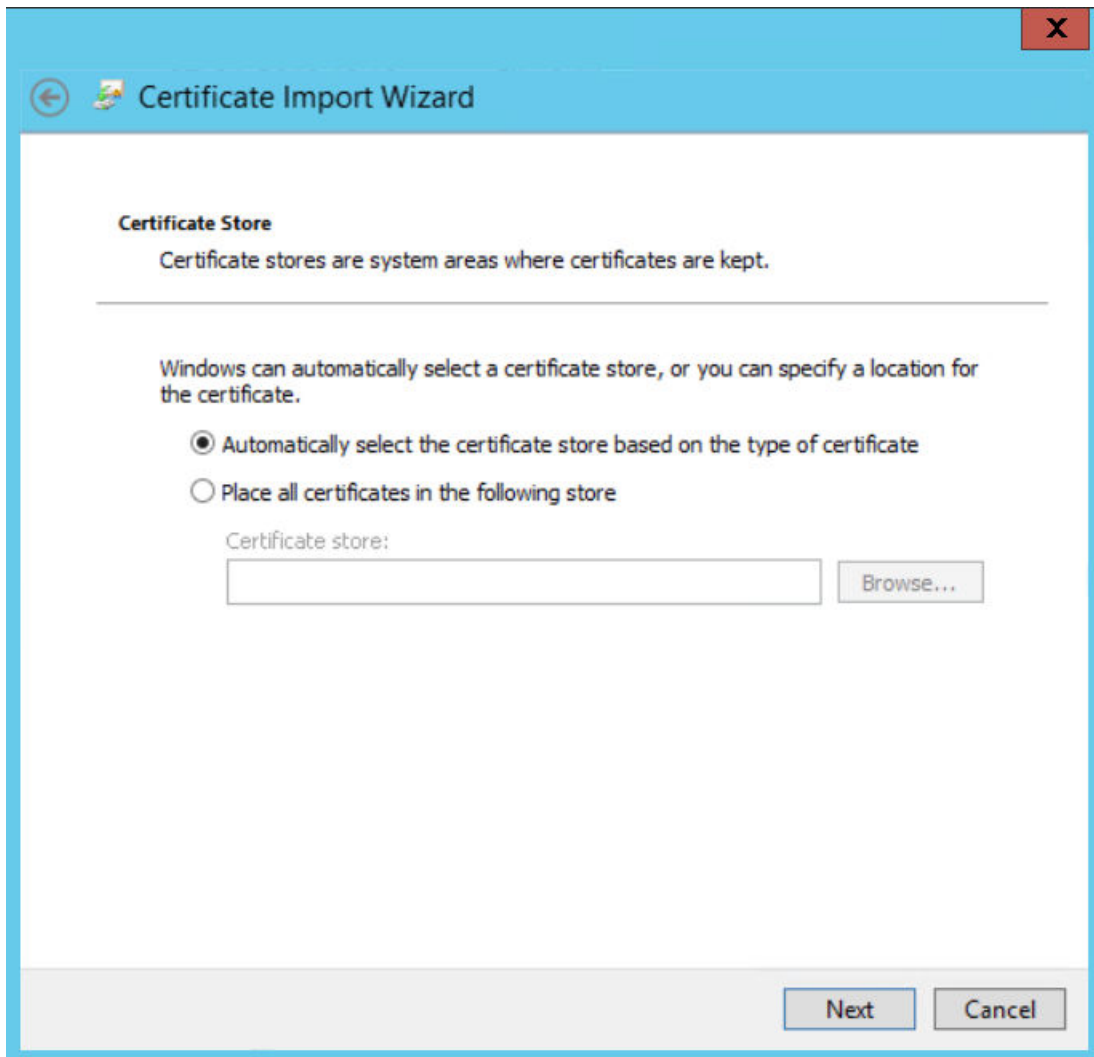10. Select **Apply**, and then select **OK**.

Next Steps

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

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 47

Federation Service Identifier from ADFS

To get Federation Service Identifier from ADFS.

Procedure

1. Open AD FS management console.
2. Select AD FS from left navigation and select 'Edit Federation Service Properties' from Actions pane on the right.
3. On the **Federation Service Properties** dialog window, you can find the Federation Service identifier value.

4. Navigate to `C:\Program Files\Meridium\ApplicationServer\api` folder and open saml.json file in a text editor. Update the `PartnerIdentityProviderConfigurations` **Name** value with the Federation Service Identifier.

Next Steps

- About Enabling APM SSO

Chapter
3

Enable SSO

Topics:

About Enabling APM SSO

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

- Enable SSO On Site Authentication Using Active Directory on page 47
- Enable SSO Off-Site Authentication Using APM Server Setup on page 47

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 APM.
3. Log in to APM with the Windows user name and password.
   You are logged in.

Results

- SSO On-Site Authentication is enabled.

Next Steps

- Configure APM Server on page 50

Enable SSO Off-Site Authentication Using APM Server Setup

About This Task

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

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **SSO Configuration**.
   The **SSO Configuration** page appears.
2. In the **IDP URL** box, enter the `PartnerIdentityProviderConfigurations` *Name* value configured in the `C:\Program Files\Meridium\ApplicationServer\api \saml. json` file.
3. Select the **SSO Enabled** check box.
4. Select 🖫.
   The SSO configuration is saved.
5. Log out of APM.
6. On the APM Server, in the 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`.
- The settings in the `saml.json` file must 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.
7. 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.
8. Reset IIS.
9. Access APM via a web browser.
SSO off-site authentication is enabled.

Next Steps

Enable OAuth for APM using SSO Off-Site

About This Task

For specific workflows, you can authenticate with APM using a JSON Web Token (JWT) provided by an IDP using the OAuth protocol. To enable this authentication, you must provide the following configuration.

Note: This form of authentication can be used by external applications that require access to APM APIs, such as mobile applications.

Procedure

1. On the APM server, navigate to `C:\ProgramData\Meridium`.
2. Open the `appsettings.Global.json` file using a text editor.
3. Add the following values:

   - `msEntraIDOAuthURL`: URL represents the location for the public signing key for JWT tokens issued by your IDP. For Microsoft Entra, this URL is `https://login.microsoftonline.com/<tenantId>`.
   - `msEntraIDAppID`: Application ID represents the application you have configured within your IDP.
4. Reset IIS.
5. Access APM APIs, providing the JWT token in the header of an HTTP request as a Bearer token.

Results

OAuth authentication for APM using SSO Off-Site is enabled.

Note: In the Azure App Proxy settings, add `com.ge.mobileinspection://auth` to the Redirect URIs configuration for Mobile and Desktop Applications. To access the proxy settings, navigate to **App Registrations** > **Enterprise App Name** > **Authentication**.

Chapter
4

Configure the APM Server

Topics:

* Configure APM Server

Configure APM Server

Before You Begin

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

Procedure

1. Using a web browser, log in to APM as an Administrator.
2. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Data Sources**. The **Data Sources** page appears.
3. In the **Data Source Host** box, enter the name of the 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 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: As described in sections Configure Azure Active Directory as the Identity Provider (IDP) on page 4 and About Configuring Identity Provider (IDP) on Active Directory on page 9.
   - WantSAMLResponseSigned: false
   - WantAssertionSigned: true
   - WantAssertionEncrypted: false
   - UseEmbeddedCertificate: false
   - SingleSignOnServiceUrl: {https version of Federation Service identifier} + "/adfs/ls". For example, https://myadfsserver/adfs/ls. This information must be obtained from the ADFS team. In the case of Azure AD, please refer to section Configure Azure Active Directory as the Identity Provider (IDP) on page 4

   Note:

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

   - "DigestAlgorithm":"http://www.w3.org/2001/04/xmlenc#sha256"
   - "SignatureAlgorithm":"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": "https://<APM Server
Name>/Meridium/api/v1/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.