

ComponentSpace

SAML for ASP.NET Core

ADFS

Relying Party

Integration Guide

Contents

- Introduction..... 1
- Enabling IdP-Initiated SSO..... 1
- Adding a Relying Party 1
- Adding a Claims Rule 7
 - Specifying the Name ID Format 11
- Reviewing Relying Party Configuration 14
- ADFS SAML Metadata..... 25
- Service Provider Configuration 26
- SP-Initiated SSO 26
- IdP-Initiated SSO 30
- SAML Logout..... 34
- ADFS Authentication Methods..... 35
- Windows Integrated Authentication..... 37
 - Browser Support 37
- Default User Name 38
- Troubleshooting ADFS SSO 39

Introduction

This document describes integration of a service provider with Active Directory Federation Services.

The Microsoft terminology for a SAML service provider is a relying party.

Enabling IdP-Initiated SSO

Ensure IdP-initiated SSO is enabled in ADFS using the PowerShell cmdlets Get-AdfsProperties and Set-AdfsProperties.

```
Get-AdfsProperties | Select EnableIdpInitiatedSignonpage
```

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $True
```

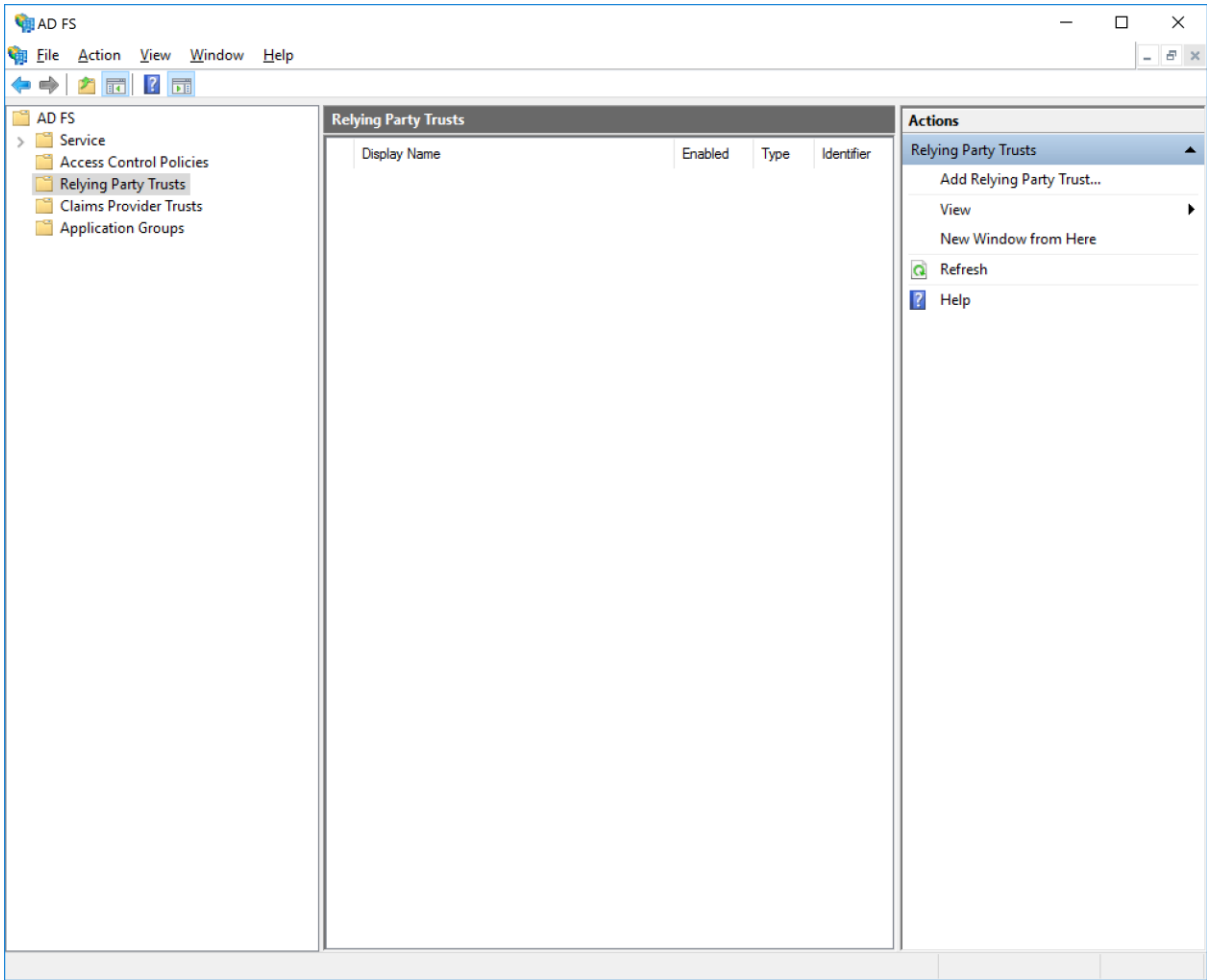
For more information, refer to:

<https://blogs.technet.microsoft.com/rmilne/2017/06/20/how-to-enable-idpinitiatedsignon-page-in-ad-fs-2016/>

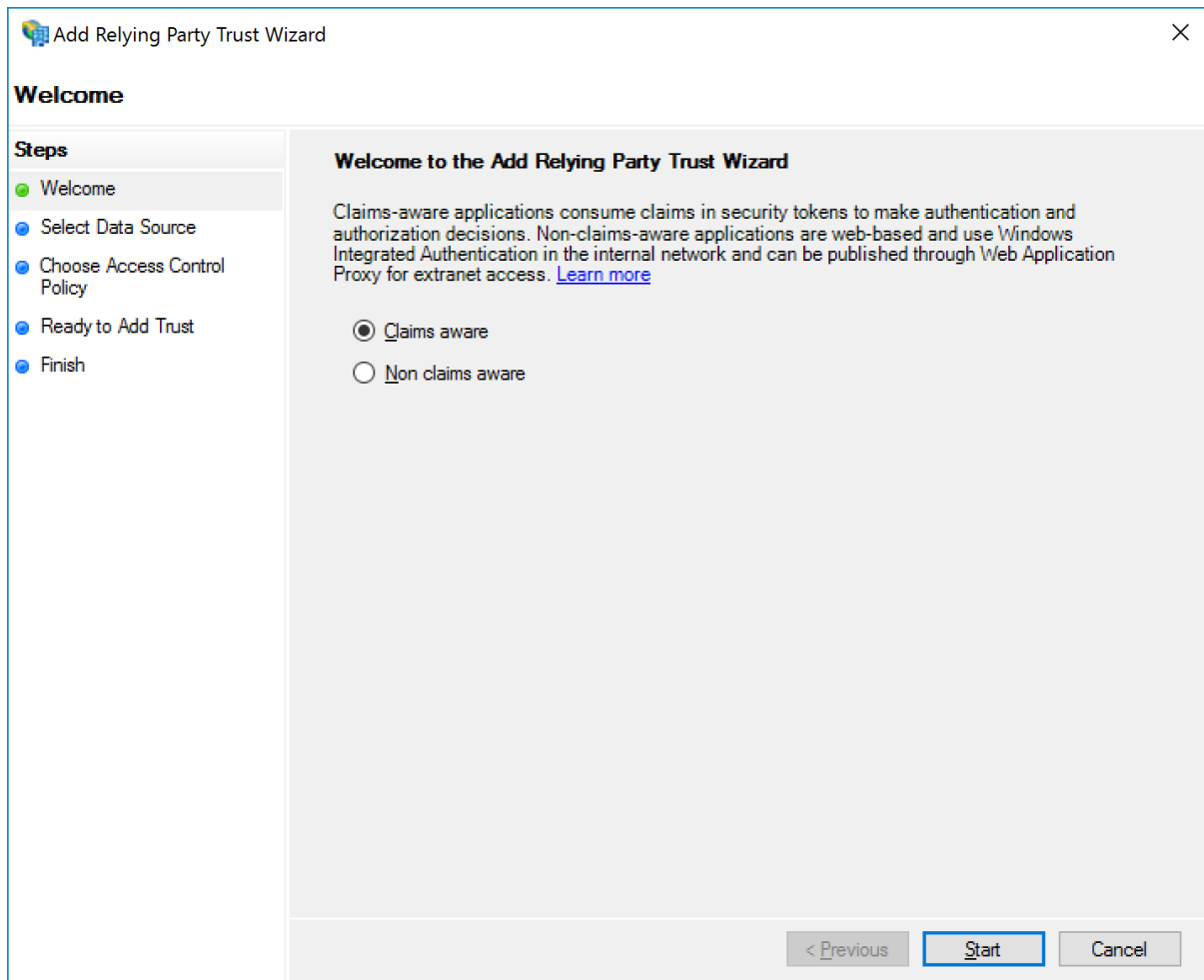
<https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties>

Adding a Relying Party

Open the ADFS console and add a relying party trust.

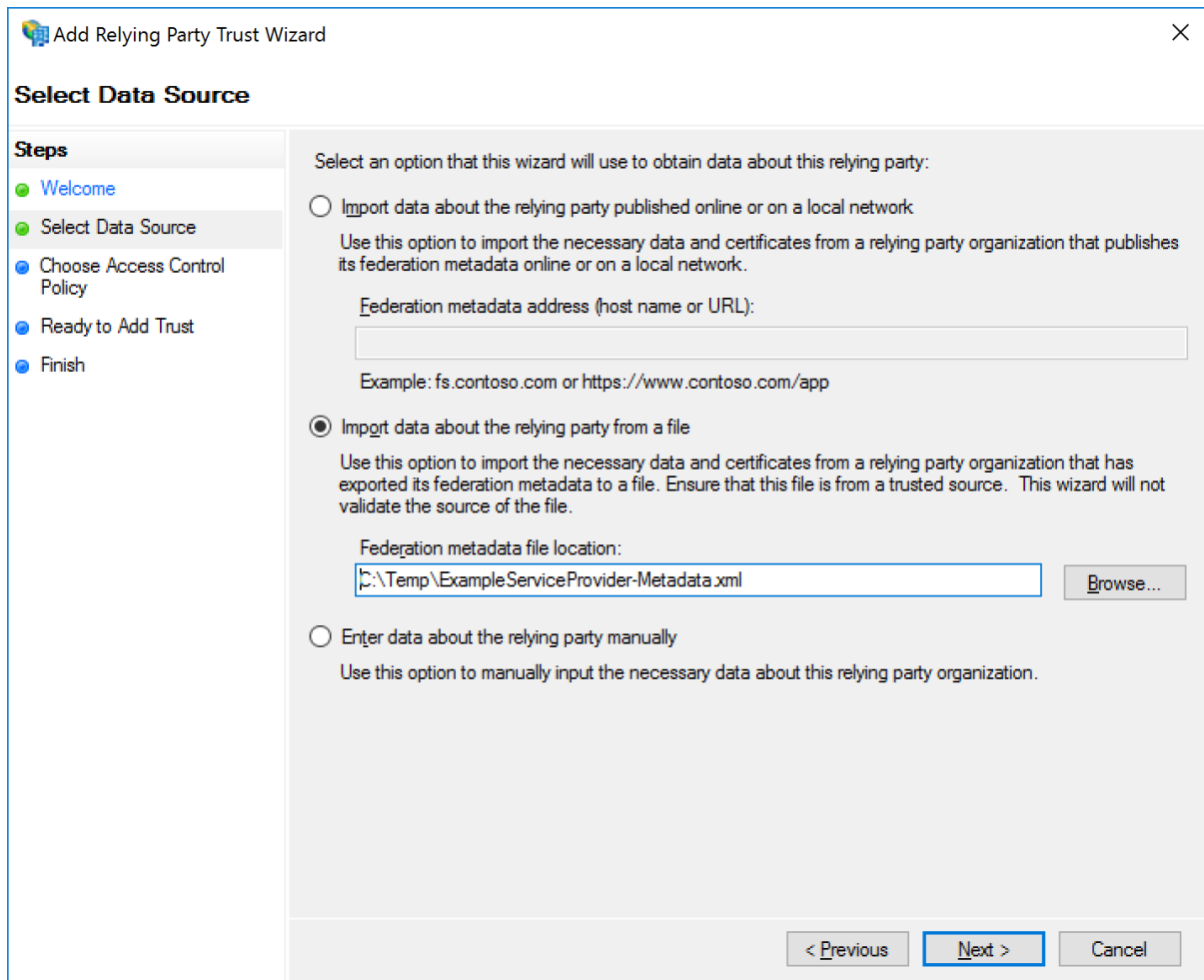


The relying party is claims aware.



The relying party may be configured through SAML metadata or manually.

The included SAML metadata for the ExampleServiceProvider is used.



The image shows a screenshot of the 'Add Relying Party Trust Wizard' window, specifically the 'Select Data Source' step. The window has a title bar with the text 'Add Relying Party Trust Wizard' and a close button. On the left, there is a 'Steps' pane with five steps: 'Welcome', 'Select Data Source' (which is highlighted with a green dot), 'Choose Access Control Policy', 'Ready to Add Trust', and 'Finish'. The main area of the wizard contains three radio button options for selecting data source information. The first option is 'Import data about the relying party published online or on a local network', which is currently unselected. It includes a text box for 'Federation metadata address (host name or URL)' and an example: 'fs.contoso.com or https://www.contoso.com/app'. The second option is 'Import data about the relying party from a file', which is selected with a black dot. It includes a text box for 'Federation metadata file location' containing the path 'C:\Temp\ExampleServiceProvider-Metadata.xml' and a 'Browse...' button. The third option is 'Enter data about the relying party manually', which is unselected. At the bottom right, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- 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:

C:\Temp\ExampleServiceProvider-Metadata.xml

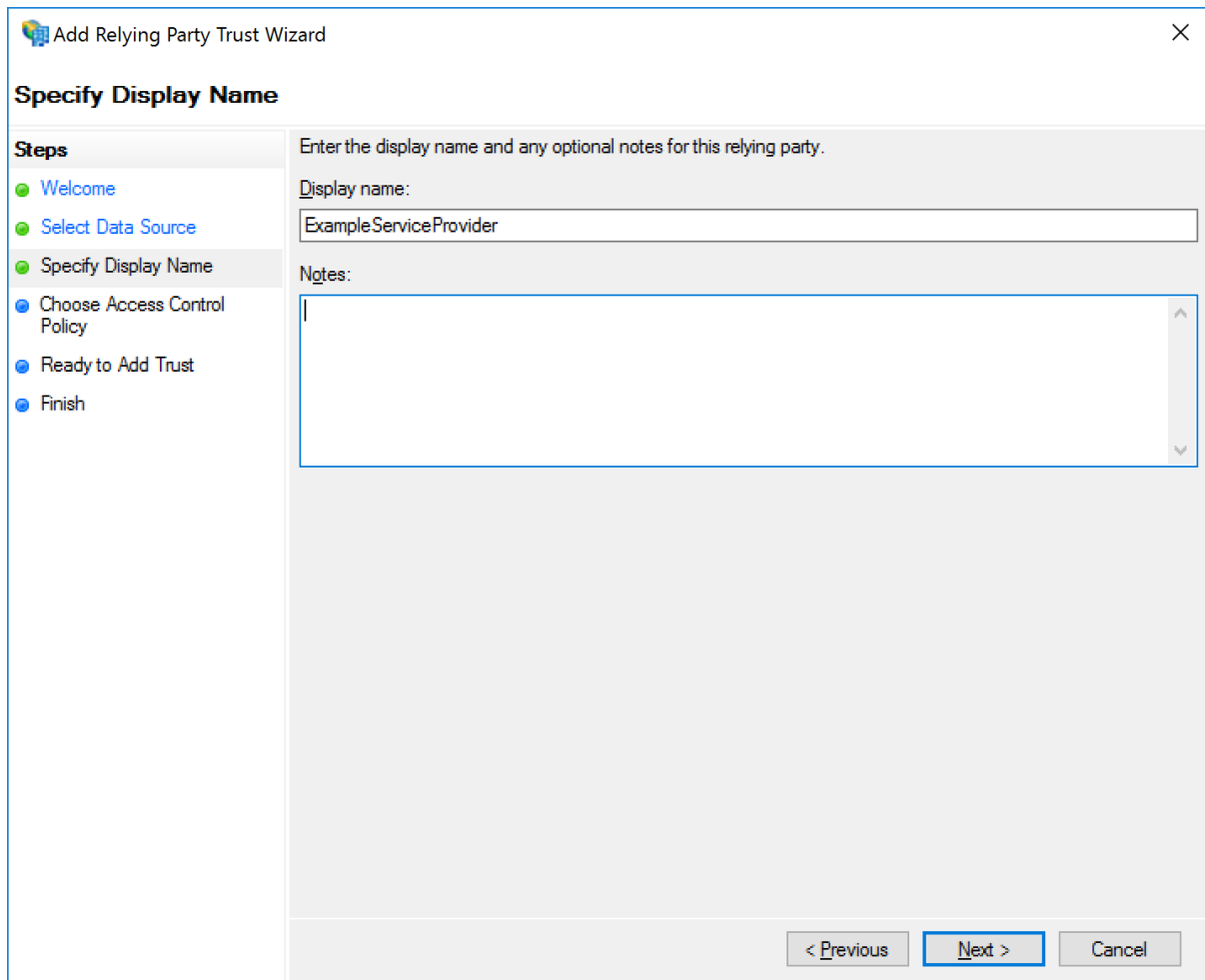
Browse...

☐ Enter data about the relying party manually

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

< Previous Next > Cancel

Provide a name purely for display purpose.



The image shows a screenshot of the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window has a title bar with the text 'Add Relying Party Trust Wizard' and a close button. On the left, there is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source', 'Specify Display Name' (which is highlighted), 'Choose Access Control Policy', 'Ready to Add Trust', and 'Finish'. The main area of the wizard contains the following elements:

- A heading 'Specify Display Name'.
- A sub-heading 'Enter the display name and any optional notes for this relying party.'
- A label 'Display name:' followed by a text input field containing the text 'ExampleServiceProvider'.
- A label 'Notes:' followed by a large, empty text area with a vertical scrollbar on the right.
- At the bottom right, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Specify the access control policy.

Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy**
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more groups.

Policy

Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

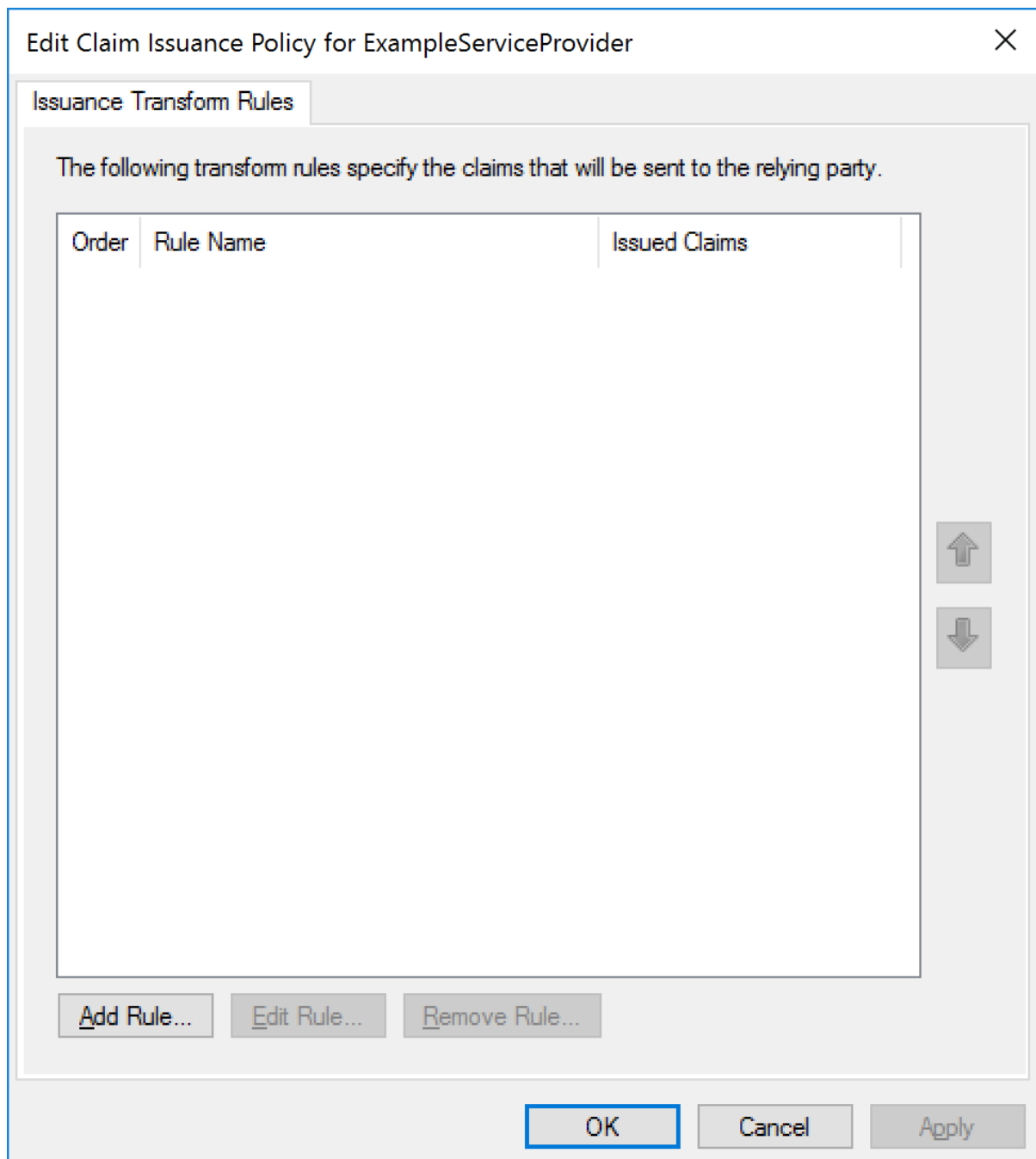
Review the configuration. This can be updated later if required.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Ready to Add Trust'. On the left, a 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name, Choose Access Control Policy, Ready to Add Trust (highlighted), and Finish. The main area contains a message: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with tabs: Monitoring (selected), Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Notes. The 'Monitoring' tab contains the text 'Specify the monitoring settings for this relying party trust.' followed by a text box for 'Relying party's federation metadata URL:'. Below this are two checkboxes: 'Monitor relying party' (unchecked) and 'Automatically update relying party' (unchecked). Further down are two lines of status information: 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

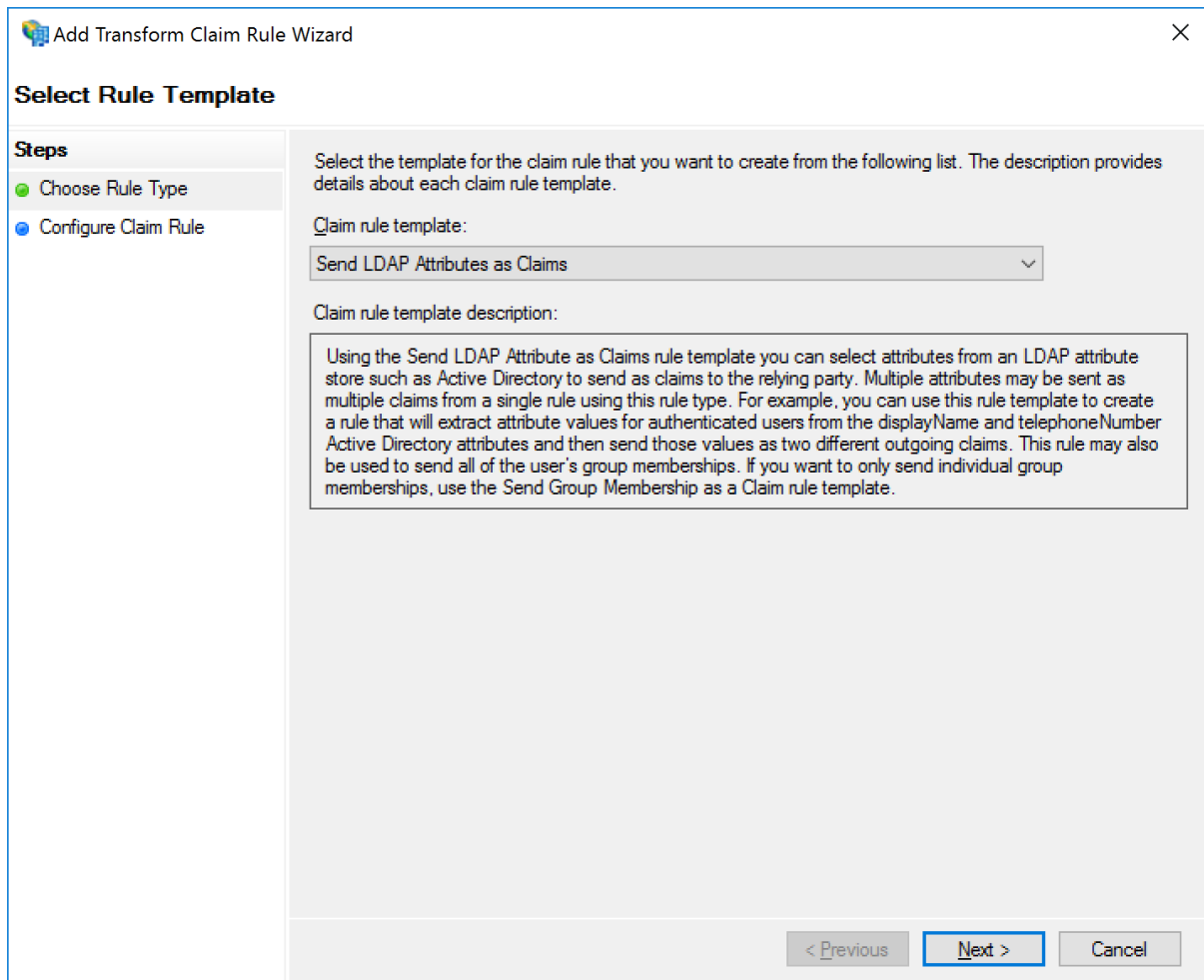
Adding a Claims Rule

Claim rules map user information into the SAML subject name identifier and SAML attributes that are included in the SAML assertion sent to the service provider.

Add a rule.



User properties in Active Directory will be used.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous **Next >** Cancel

Specify the mapping.

In this case the user principal name (UPN) is mapped to the SAML name identifier (Name ID).

The user's given name and surname are mapped to SAML attributes.

Note that to support SAML logout, a claims rule mapping for the SAML name identifier (Name ID) is required.

 Add Transform Claim Rule Wizard X

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	Name ID
	Given-Name	Given Name
	Surname	Surname
»		

Alternatively, the user's email address may be mapped to the SAML name identifier (Name ID).

Edit Rule - Send LDAP Attributes as Claims

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Send LDAP Attributes as Claims

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	Name ID
	Given-Name	Given Name
	Surname	Surname
▶*		

View Rule Language...

OK Cancel

Specifying the Name ID Format

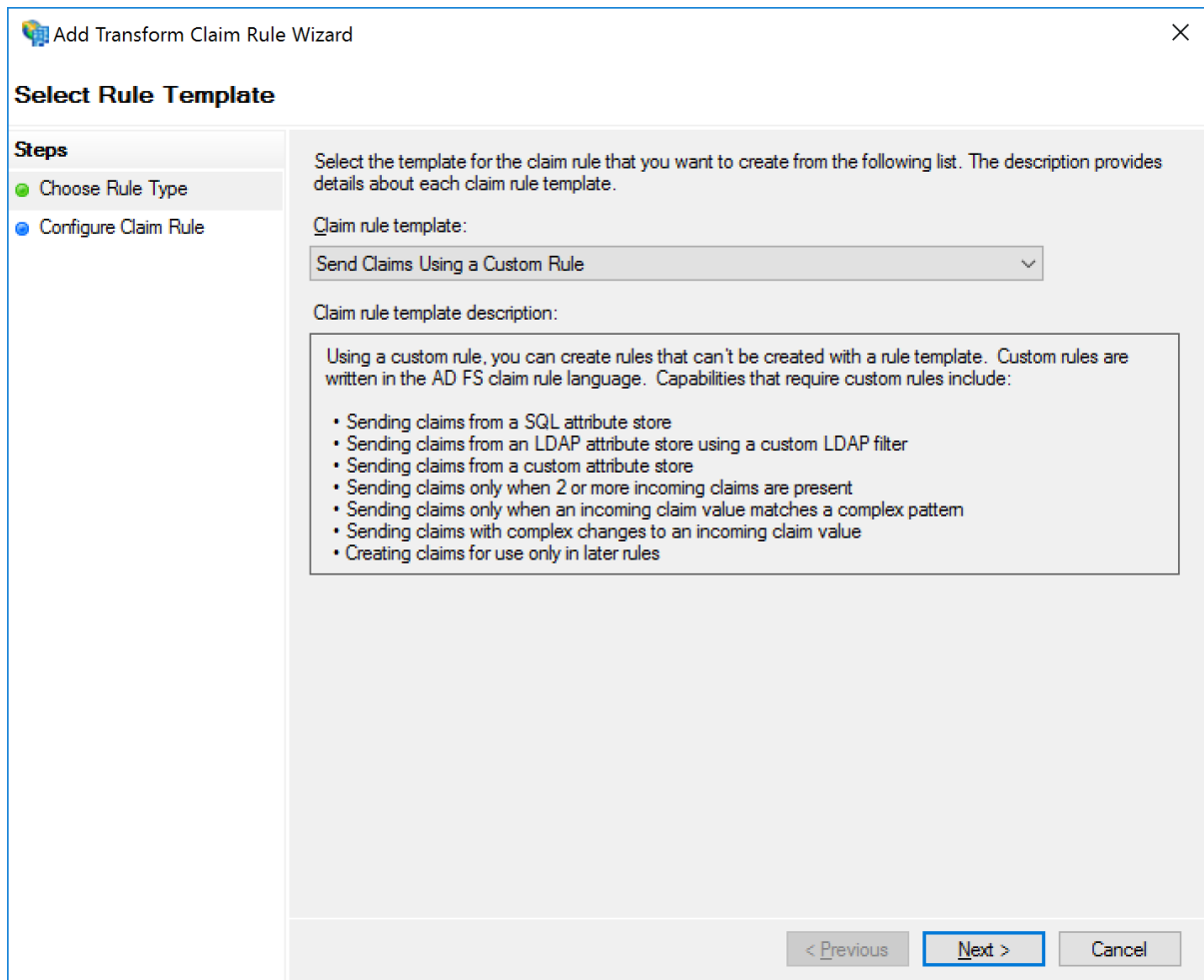
By default, no Name ID format is specified with the Name ID included in the SAML assertion.

A Name ID format may be specified if required by the service provider.

A Name ID format must be specified if the service provider specifies a Name ID policy in the SAML authn request, other than “urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified”.

For example, if the SAML authn request specifies a Name ID policy of “urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress”, the corresponding Name ID format must be returned in the SAML assertion.

To include the Name ID format, add a custom rule.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule**

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

< Previous **Next >** Cancel

The custom rule transforms the <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier> claim to include a <http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format> claim property with the value urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

The rule is:

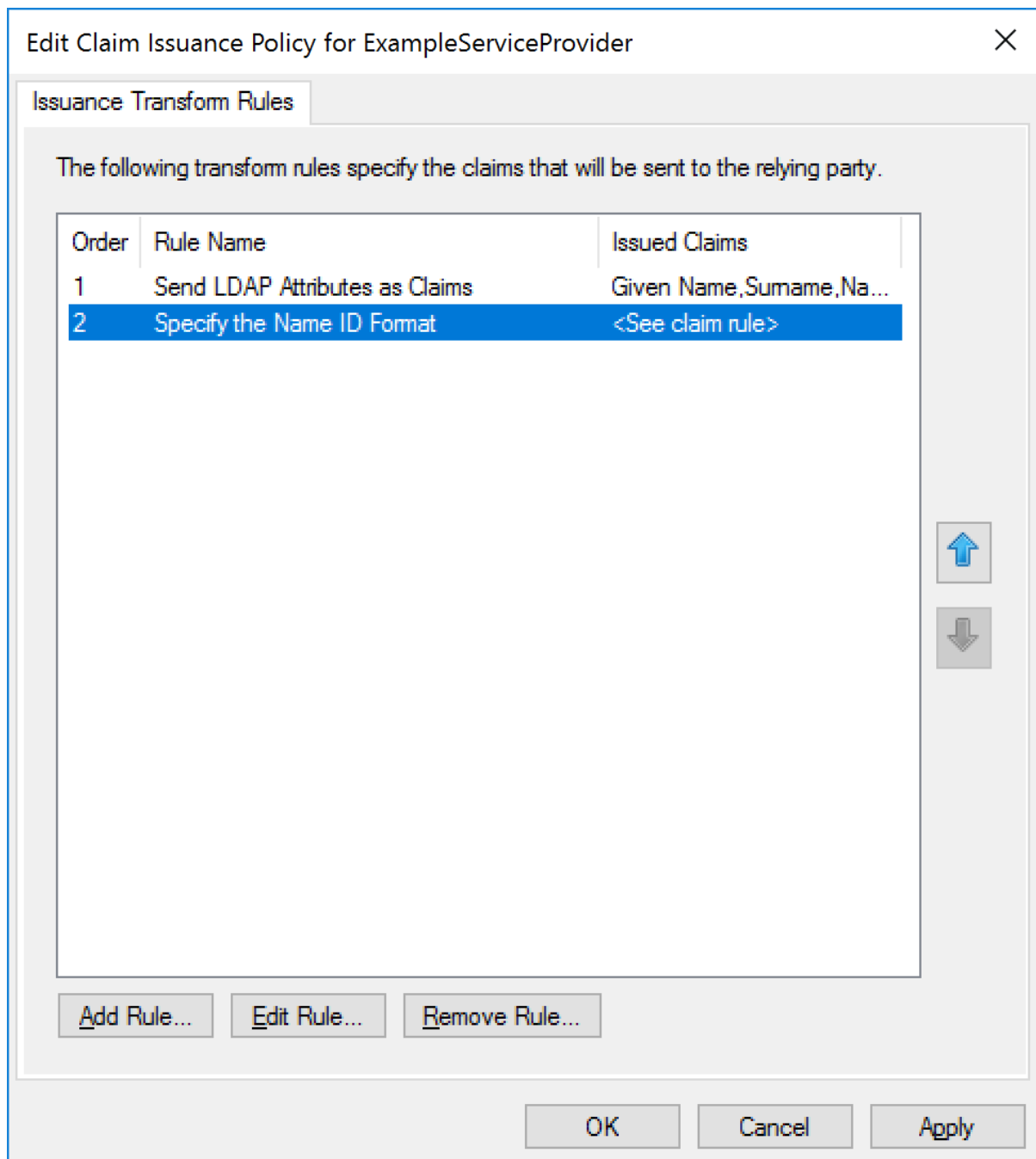
```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The title bar reads 'Add Transform Claim Rule Wizard' with a close button. The 'Steps' pane on the left shows 'Choose Rule Type' and 'Configure Claim Rule', with 'Configure Claim Rule' being the active step. The main area contains instructions: 'You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.' Below this, there is a 'Claim rule name:' label and a text box containing 'Specify the Name ID Format'. The 'Rule template:' is set to 'Send Claims Using a Custom Rule'. The 'Custom rule:' label is followed by a large text area containing the following claim rule code:

```
c:[Type ==  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"]  
=> issue (Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,  
ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

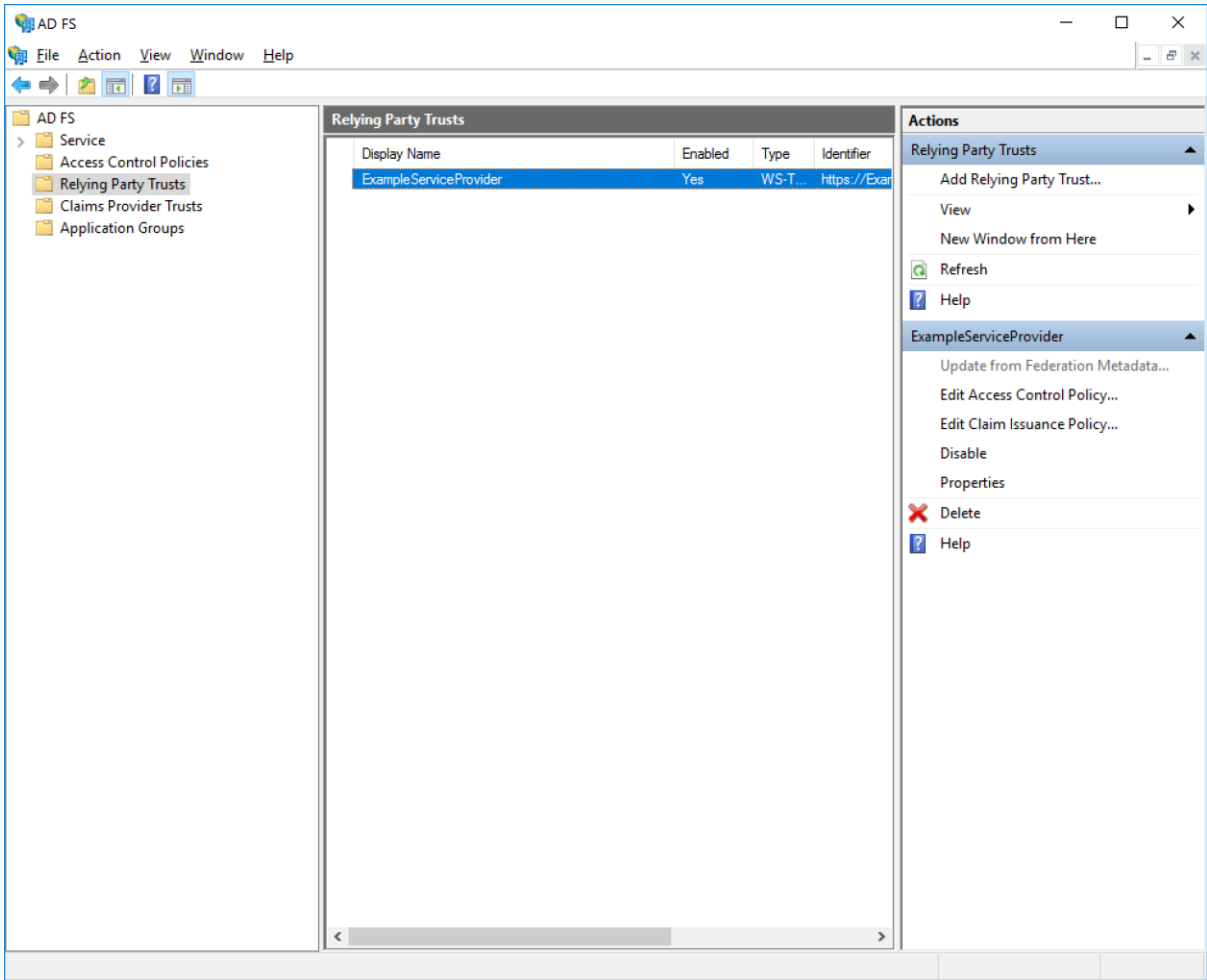
At the bottom right, there are three buttons: '< Previous', 'Finish' (which is highlighted with a blue border), and 'Cancel'.

The rule order is important. The custom rule must be applied after the mapping of the LDAP attributes to outgoing claims.

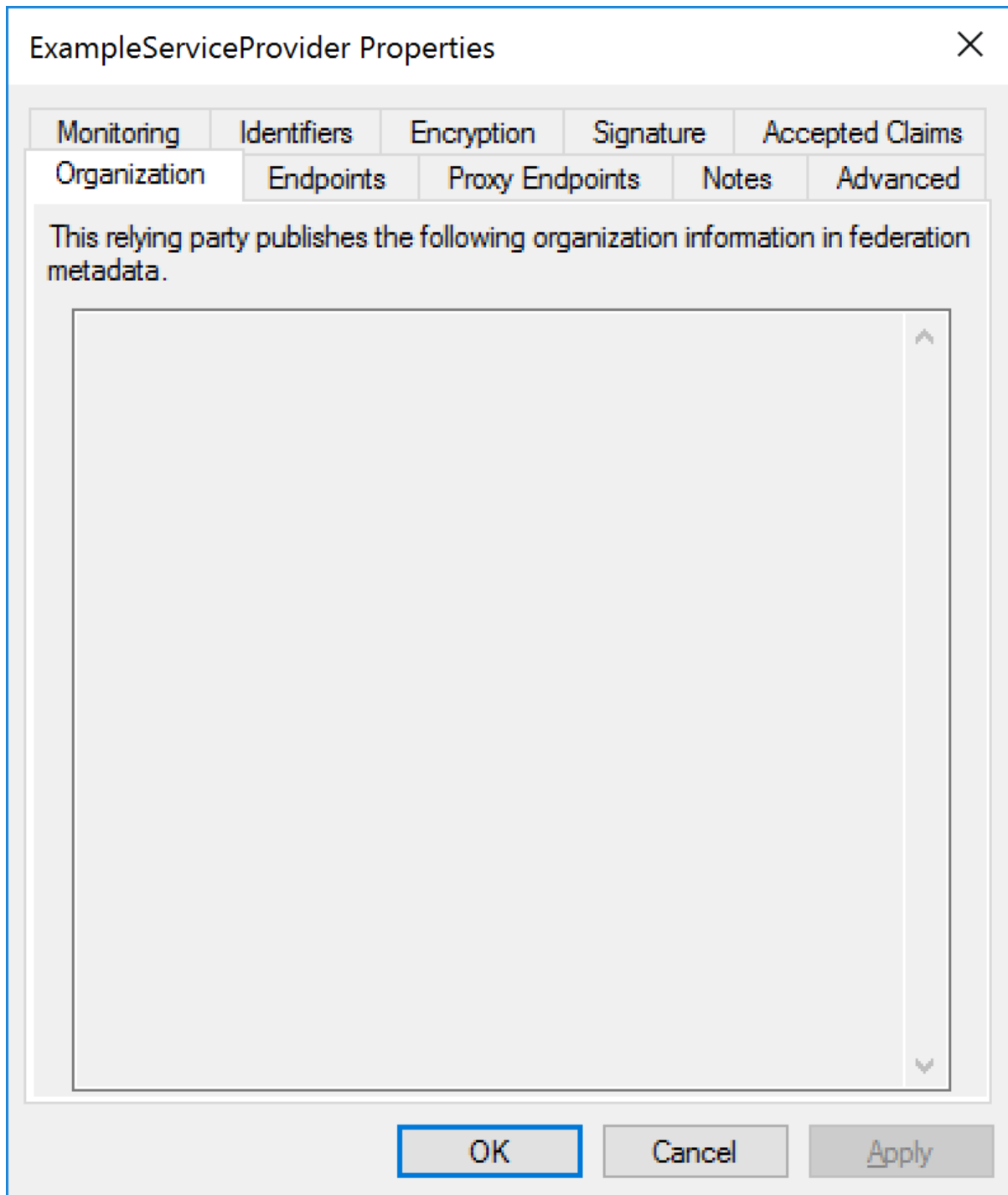


Reviewing Relying Party Configuration

The configuration may be reviewed or modified through the relying party's property tabs.



The organization information from the imported SAML metadata, if any, is displayed.



The endpoints are the URLs and SAML bindings used when communicating with the service provider.

The SAML assertion consumer service receives SAML responses as part of SSO.

The SAML logout service receives logout messages as part of SAML logout.

Note that ADFS treats URLs as being case sensitive.

ExampleServiceProvider Properties

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

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://localhost:44360/SAM...	0	POST	Yes	
SAML Logout Endpoints				
https://localhost:44360/SAM...		Redirect	No	

< >

Add SAML...

Add WS-Federation... Remove Edit...

OK Cancel Apply

Proxied endpoints aren't used in this example.

ExampleServiceProvider Properties

Monitoring

Identifiers

Encryption

Signature

Accepted Claims

Organization

Endpoints

Proxy Endpoints

Notes

Advanced

The following shows the proxied endpoints for this relying party trust.

URL	

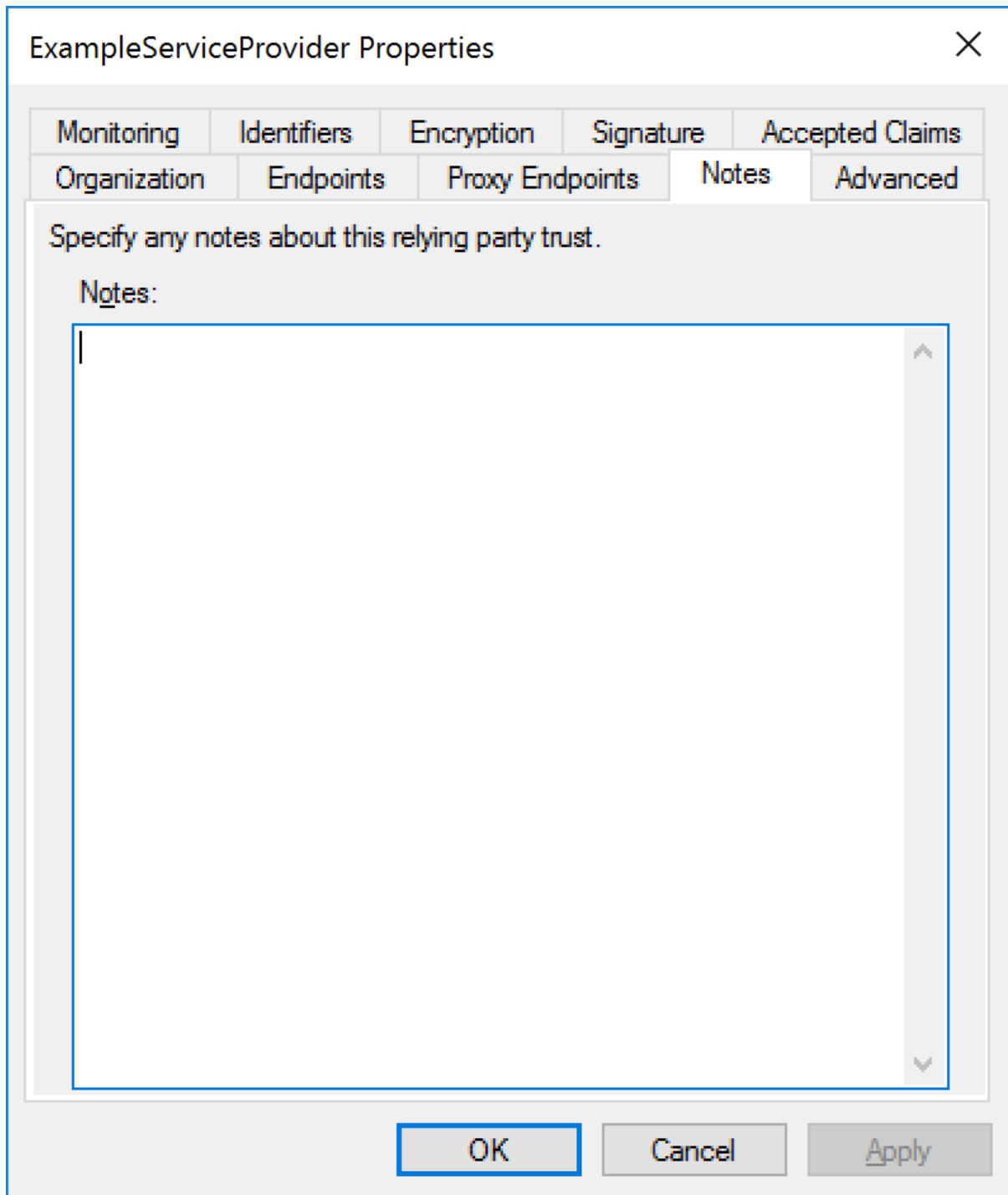
☐ This relying party trust is published through a web application proxy for extranet access.

OK

Cancel

Apply

Notes are internal to ADFS and for documentation purposes only.



The image shows a Windows-style dialog box titled "ExampleServiceProvider Properties". It has a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: "Monitoring", "Identifiers", "Encryption", "Signature", "Accepted Claims", "Organization", "Endpoints", "Proxy Endpoints", "Notes", and "Advanced". The "Notes" tab is currently selected. The main area of the dialog contains the text "Specify any notes about this relying party trust." followed by a label "Notes:" and a large, empty text area with a vertical scrollbar. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

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

Specify any notes about this relying party trust.

Notes:

OK Cancel Apply

Either SHA-1 or SHA-256 may be specified as the signature algorithm.

SHA-256 is recommended.

The screenshot shows a Windows-style dialog box titled "ExampleServiceProvider Properties" with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: "Monitoring", "Identifiers", "Encryption", "Signature", "Accepted Claims", "Organization", "Endpoints", "Proxy Endpoints", "Notes", and "Advanced". The "Advanced" tab is currently selected. Inside the dialog, there is a text instruction: "Specify the secure hash algorithm to use for this relying party trust." Below this, there is a label "Secure hash algorithm:" followed by a dropdown menu. The dropdown menu is open, showing "SHA-256" as the selected option. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue border.

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

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256

OK Cancel Apply

ADFS supports monitoring a URL for SAML metadata updates.

The screenshot shows a Windows-style dialog box titled 'ExampleServiceProvider Properties' with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: 'Organization', 'Endpoints', 'Proxy Endpoints', 'Notes', 'Advanced', 'Monitoring' (which is selected), 'Identifiers', 'Encryption', 'Signature', and 'Accepted Claims'. The 'Monitoring' tab contains the following elements:

- A text label: 'Specify the monitoring settings for this relying party trust.'
- A text label: 'Relying party's federation metadata URL:'
- A text input field with a cursor inside.
- A button labeled 'Test URL'.
- A checkbox labeled 'Monitor relying party'.
- A sub-checkbox labeled 'Automatically update relying party'.
- A text label: 'This relying party's federation metadata data was last checked on:'
- A text value: '< never >'.
- A text label: 'This relying party was last updated from federation metadata on:'
- A text value: '< never >'.
- At the bottom, there are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Apply'.

Relying party identifiers correspond to SAML metadata entity IDs.

The relying party identifier must match exactly with the service provider's configured name.

The screenshot shows a Windows-style dialog box titled 'ExampleServiceProvider Properties' with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: 'Organization', 'Endpoints', 'Proxy Endpoints', 'Notes', 'Advanced', 'Monitoring', 'Identifiers' (which is the active tab), 'Encryption', 'Signature', and 'Accepted Claims'. The 'Identifiers' tab contains the instruction 'Specify the display name and identifiers for this relying party trust.' Below this, there are three main sections: 1. 'Display name:' with a text box containing 'ExampleServiceProvider'. 2. 'Relying party identifier:' with an empty text box and an 'Add' button to its right. Below the text box is an example: 'Example: https://fs.contoso.com/adfs/services/trust'. 3. 'Relying party identifiers:' with a list box containing 'https://ExampleServiceProvider' and a 'Remove' button to its right. At the bottom of the dialog are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Apply'.

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

Specify the display name and identifiers for this relying party trust.

Display name:

ExampleServiceProvider

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers:

https://ExampleServiceProvider

OK Cancel Apply

The encryption certificate is specified if the SAML assertion is to be encrypted.

If specified, it's the service provider's encryption certificate.

In many scenarios encrypting the SAML assertion isn't required as the privacy provided at the transport layer by HTTPS is sufficient.

The certificate should be removed if the SAML assertion is not to be encrypted.

ExampleServiceProvider Properties

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

Specify the encryption certificate for this relying party trust.

Encryption certificate:

Issuer:	CN=www.sp.com
Subject:	CN=www.sp.com
Effective date:	11/22/2013 6:23:21 PM
Expiration date:	1/1/2050 12:00:00 AM

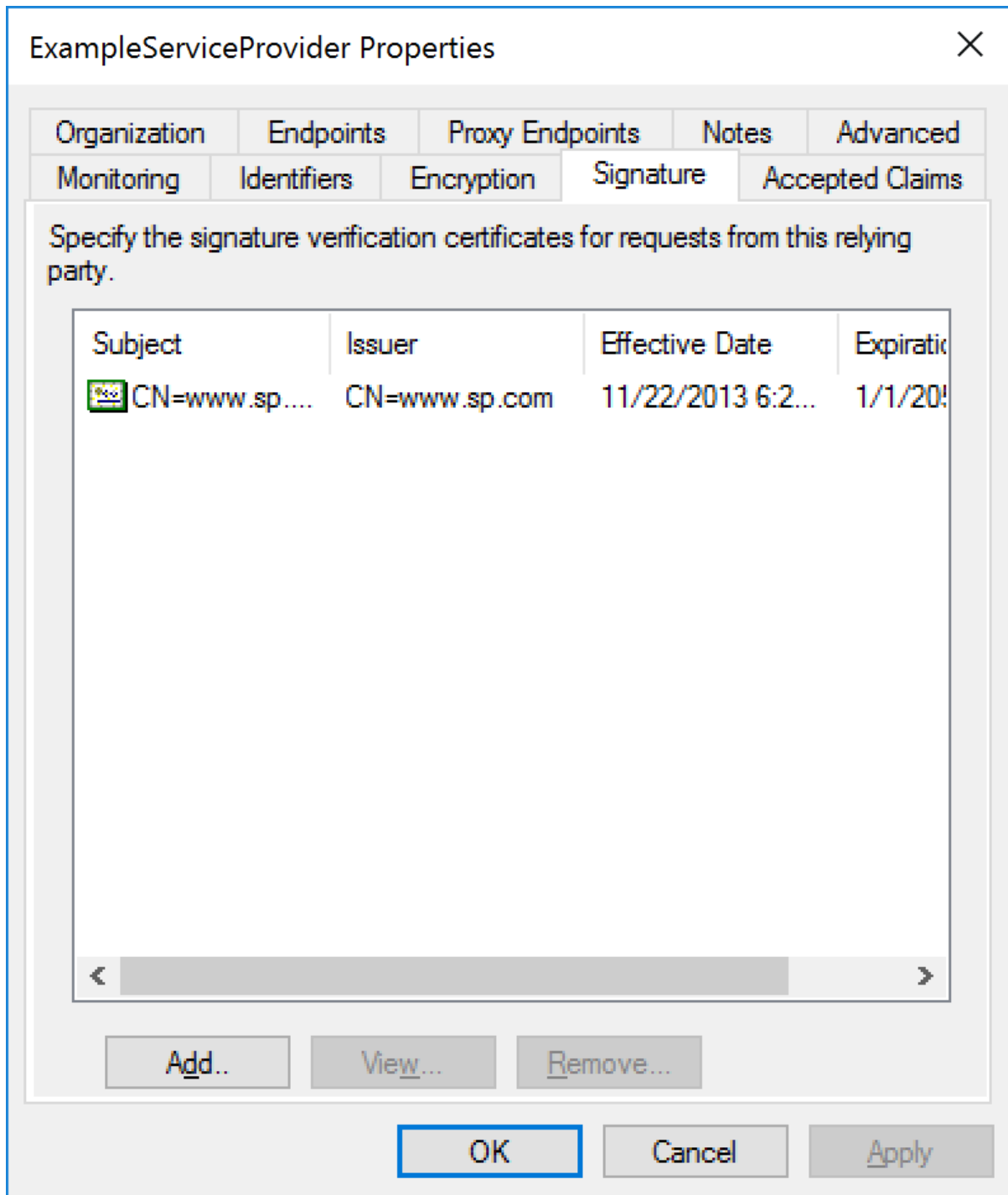
[Browse...](#) [View...](#) [Remove](#)

[OK](#) [Cancel](#) [Apply](#)

The signature certificate is specified if the signatures on SAML messages from the service provider are to be verified.

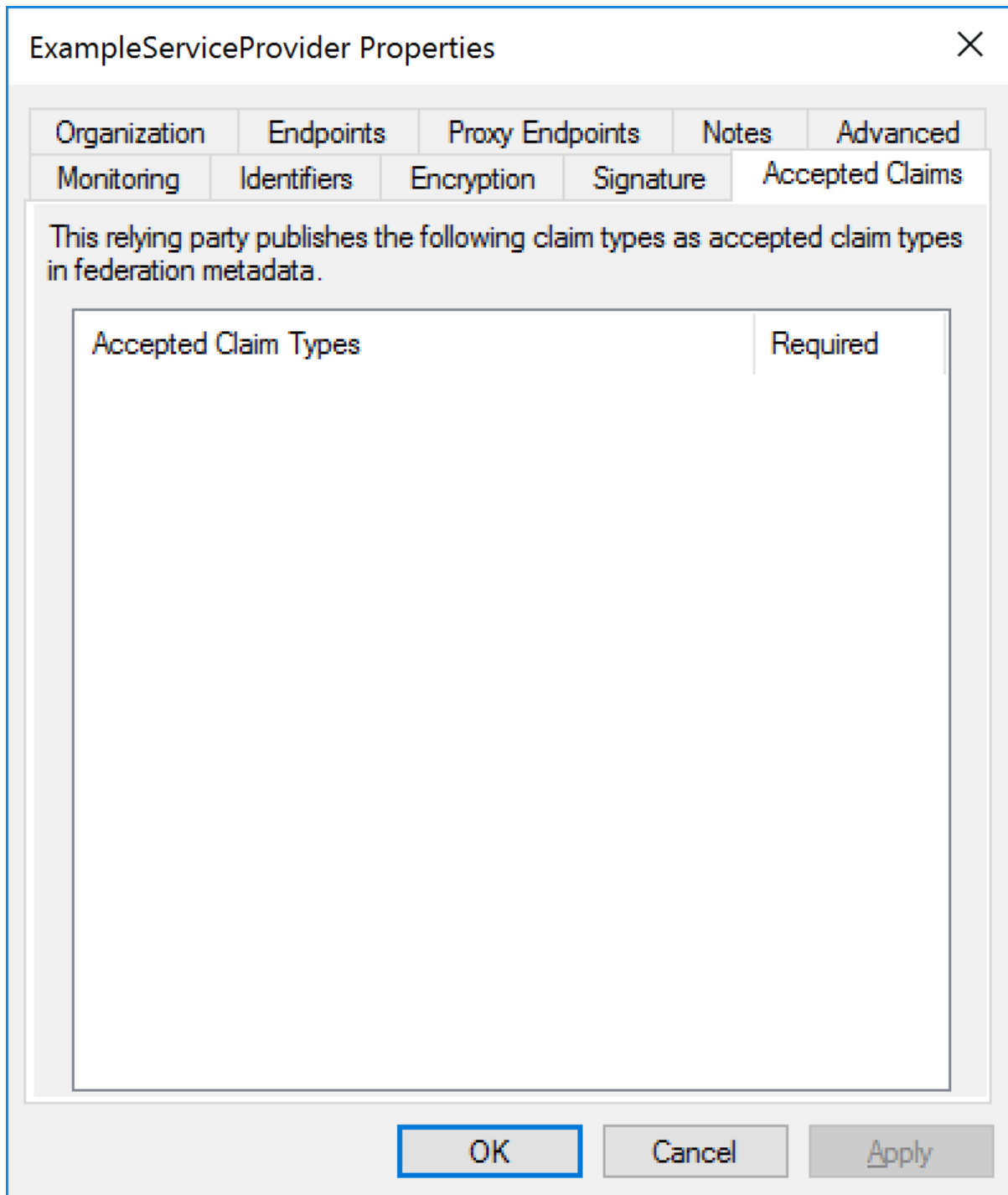
If specified, it's the service provider's signature certificate.

It's recommended that SAML messages from the service provider are signed.



The accepted claims are specified through the service provider's SAML metadata.

These are for documentation purposes and don't affect the claims sent by ADFS.



ADFS SAML Metadata

Metadata may be downloaded from:

<https://<server-name>/FederationMetadata/2007-06/FederationMetadata.xml>

For example:

<https://adfs.componentspace.com/FederationMetadata/2007-06/FederationMetadata.xml>

Service Provider Configuration

The following partner identity provider configuration is included in the example service provider's SAML configuration.

```
{
  "Name": "http://adfs.componentspace.com/adfs/services/trust",
  "Description": "ADFS",
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "WantLogoutRequestSigned": true,
  "WantLogoutResponseSigned": true,
  "SingleSignOnServiceUrl": "https://adfs.componentspace.com/adfs/ls/",
  "SingleLogoutServiceUrl": "https://adfs.componentspace.com/adfs/ls/",
  "PartnerCertificates": [
    {
      "FileName": "certificates/adfs.cer"
    }
  ]
}
```

Some of this information was extracted from the ADFS SAML metadata.

The partner certificate file corresponds to the signing certificate included in the metadata.

ADFS doesn't require the SAML authn request to be signed although it is recommended.

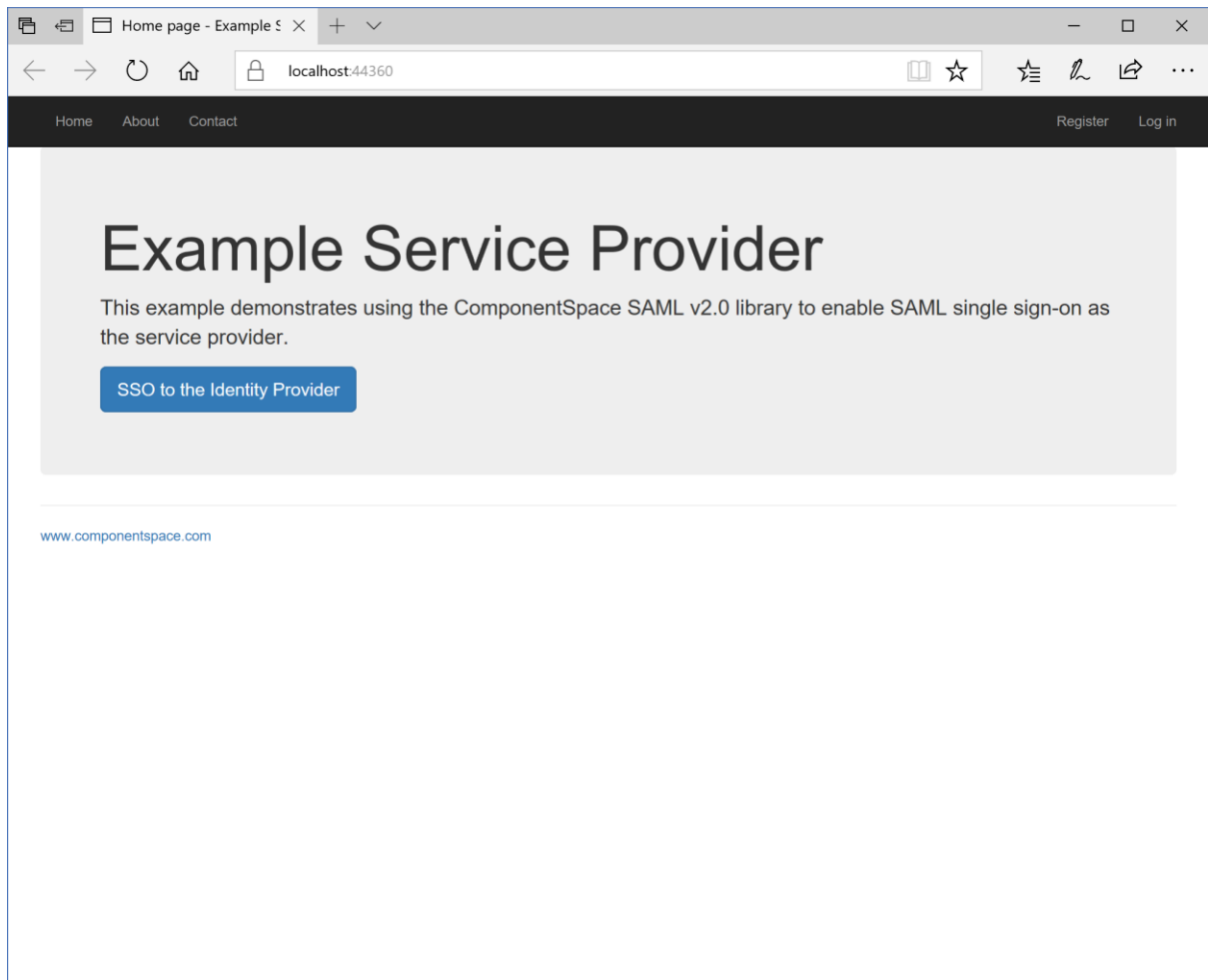
ADFS requires SAML logout messages to signed.

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "http://adfs.componentspace.com/adfs/services/trust"
```

SP-Initiated SSO

Browse to the example service provider.

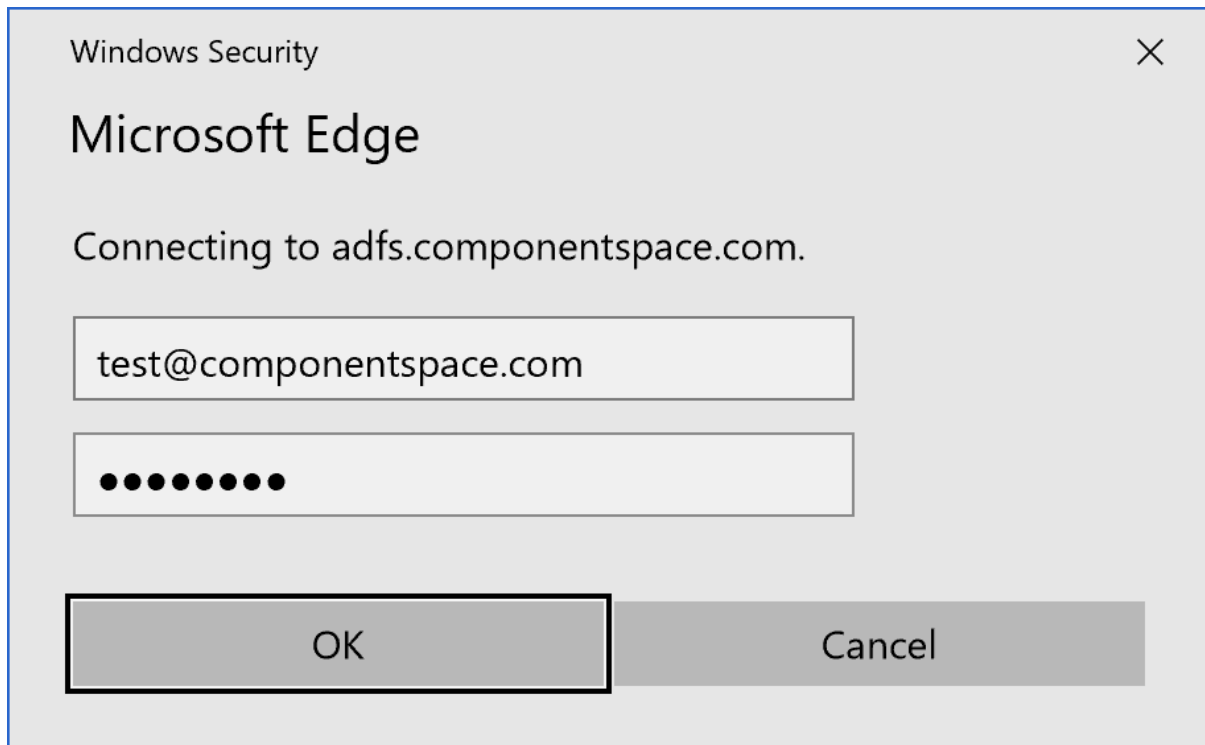


Click the button to SSO to the identity provider.

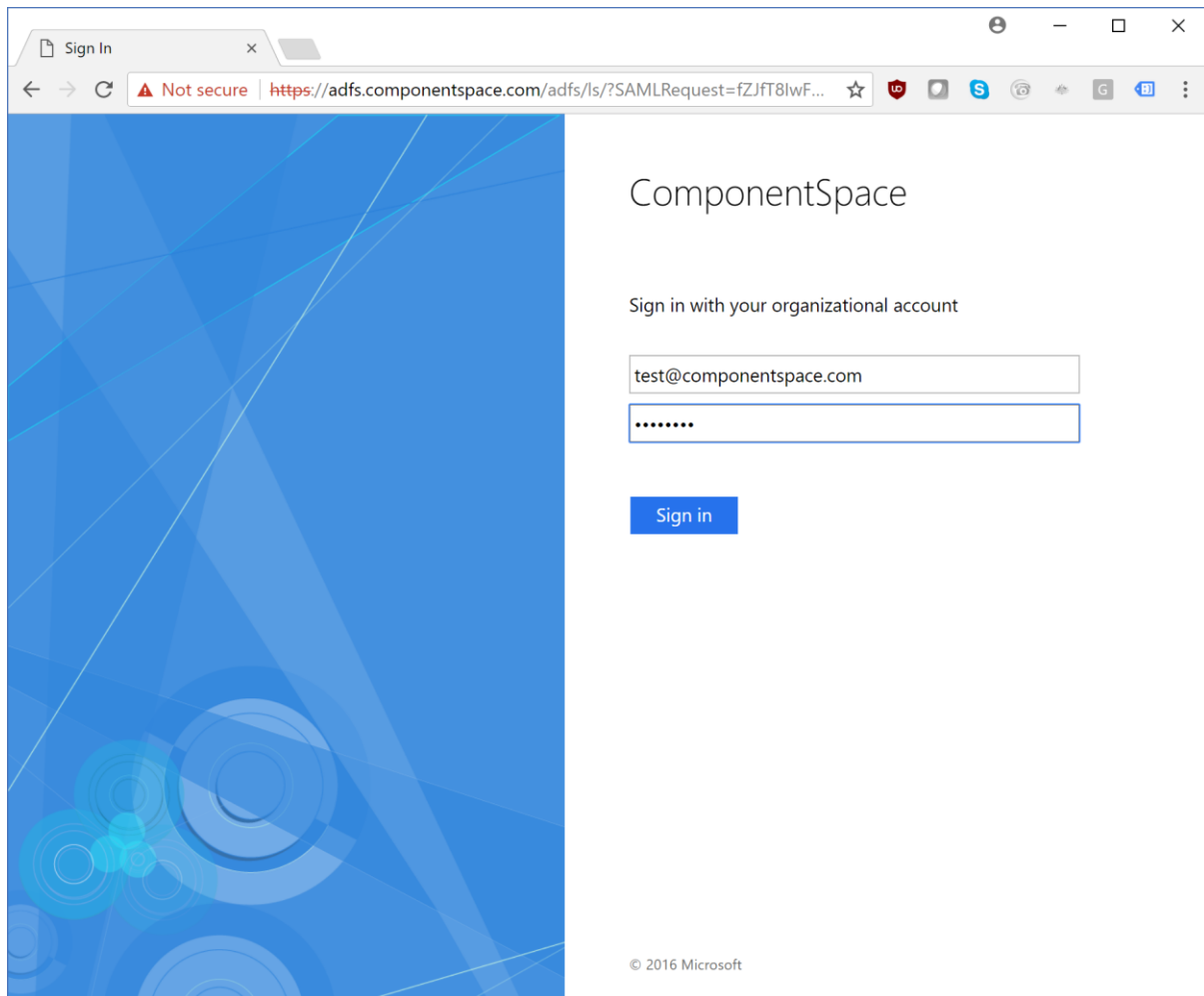
Log into ADFS.

The login method (e.g. forms authentication, Windows authentication) will be dependent on the authentication methods configured in ADFS and the browser type.

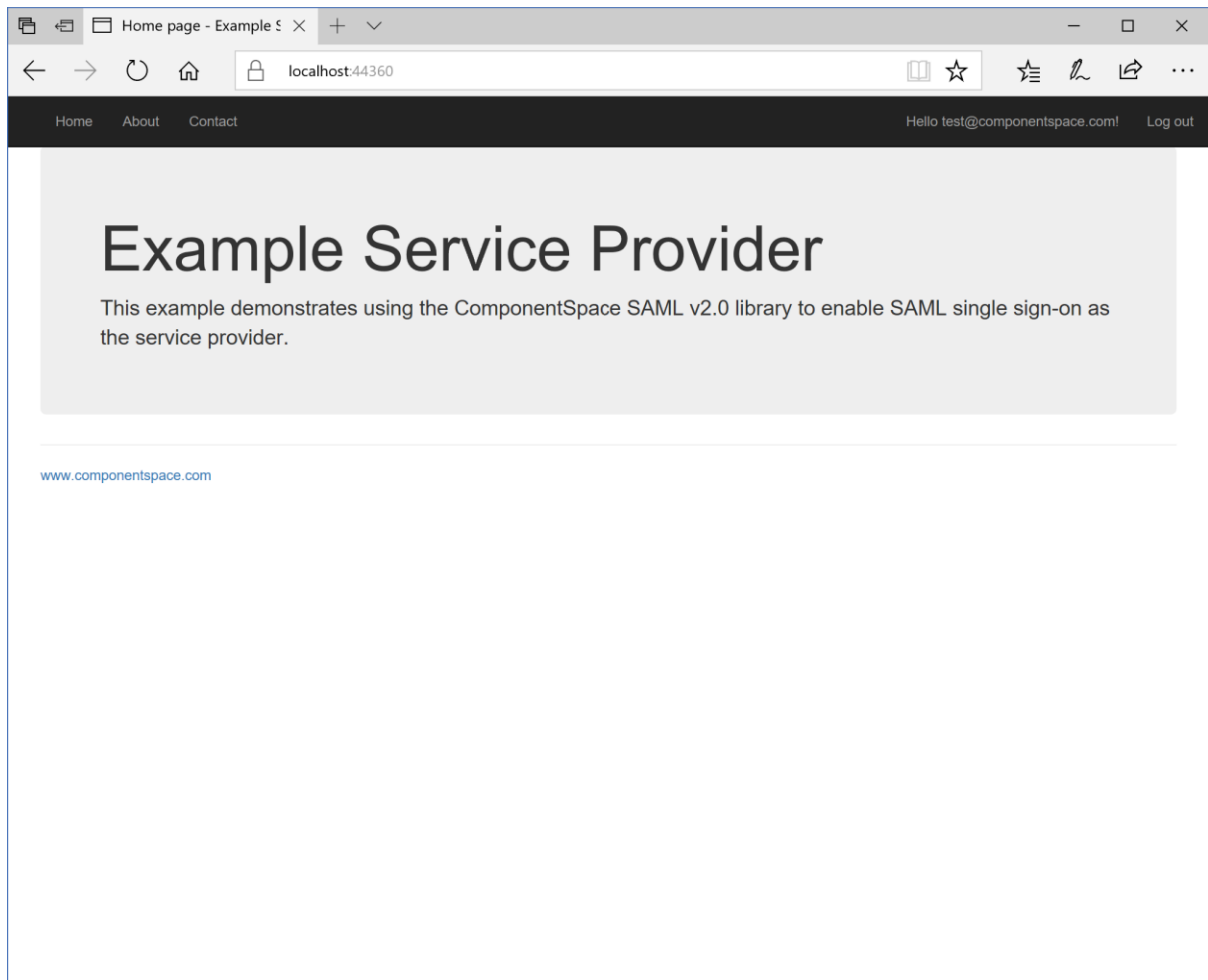
The following is the authentication prompt displayed by Microsoft Edge when Windows integrated authentication is enabled but the user is not logged into the domain.



The following is the forms authentication prompt displayed by Google Chrome.



The user is automatically logged in at the service provider.



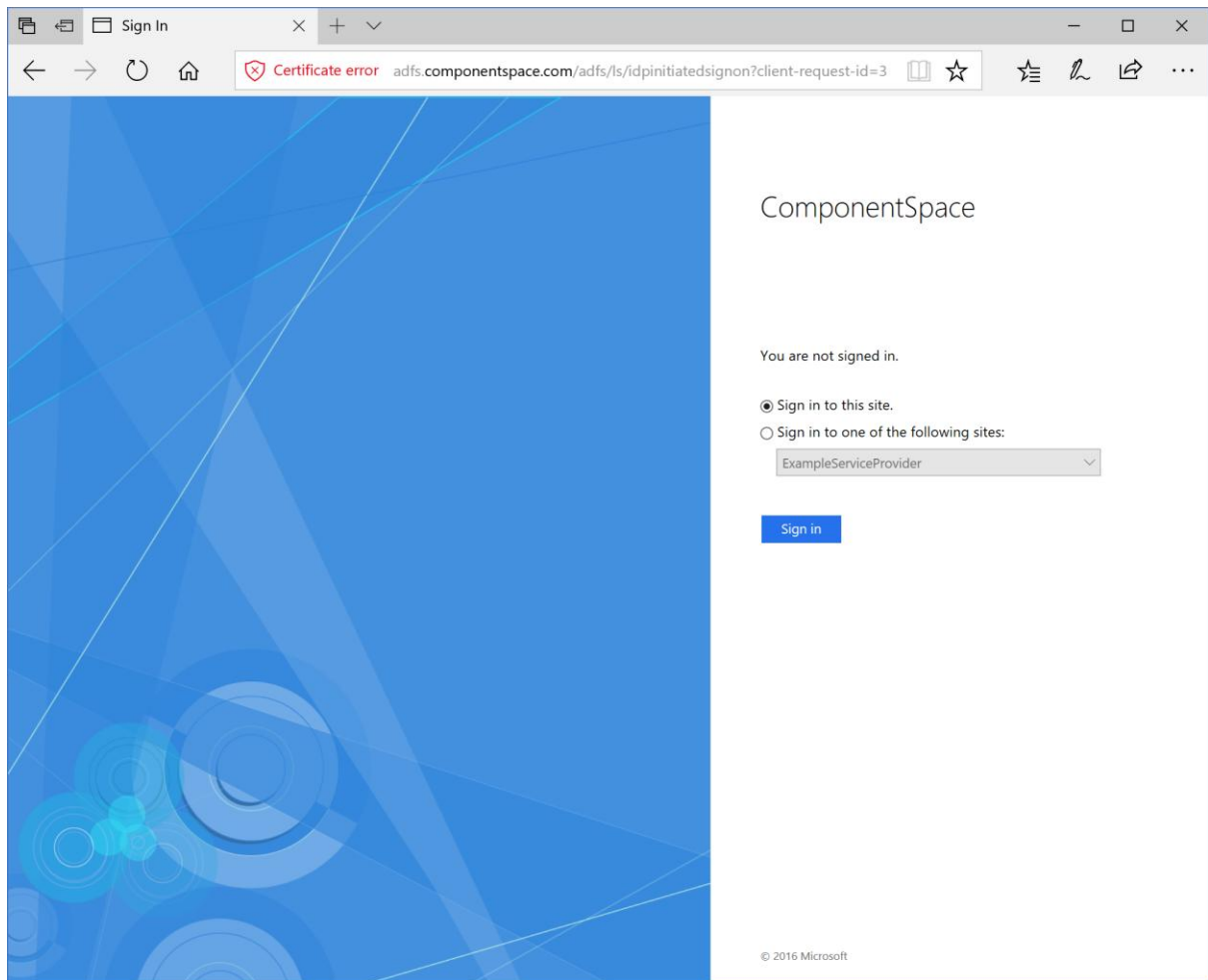
IdP-Initiated SSO

Browse to:

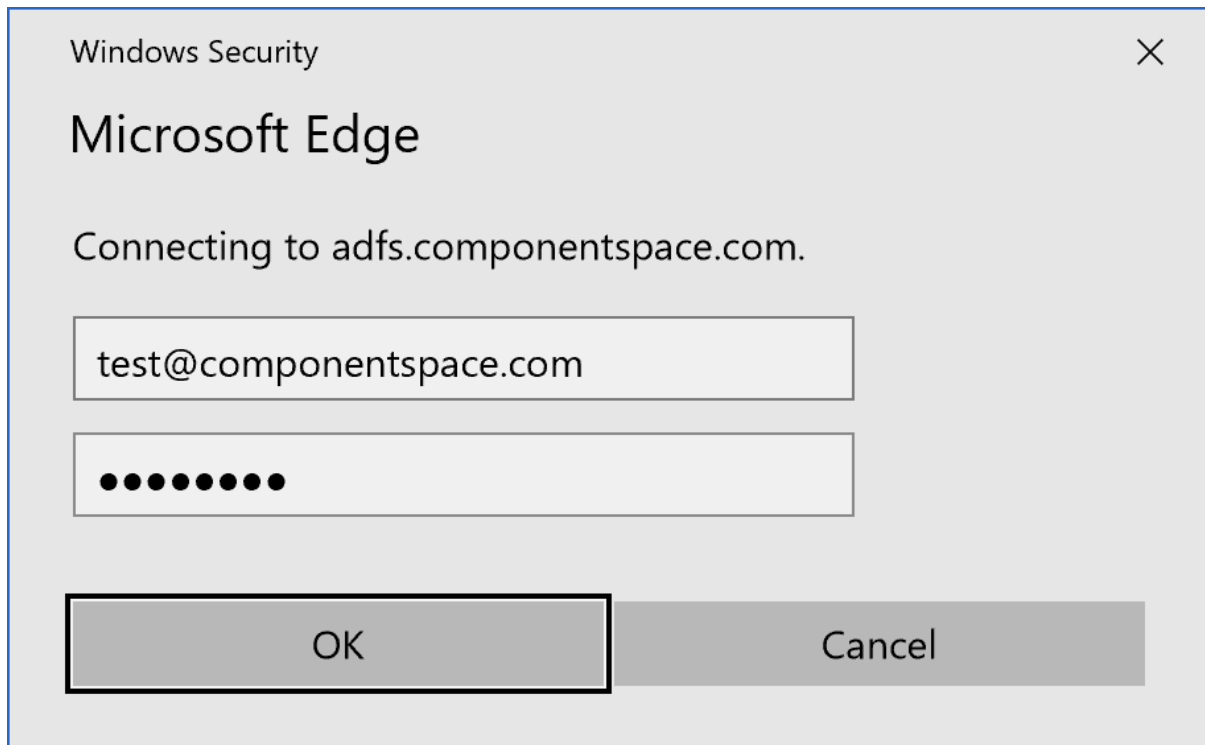
`https://<server-name>/adfs/ls/IdpInitiatedSignon`

For example:

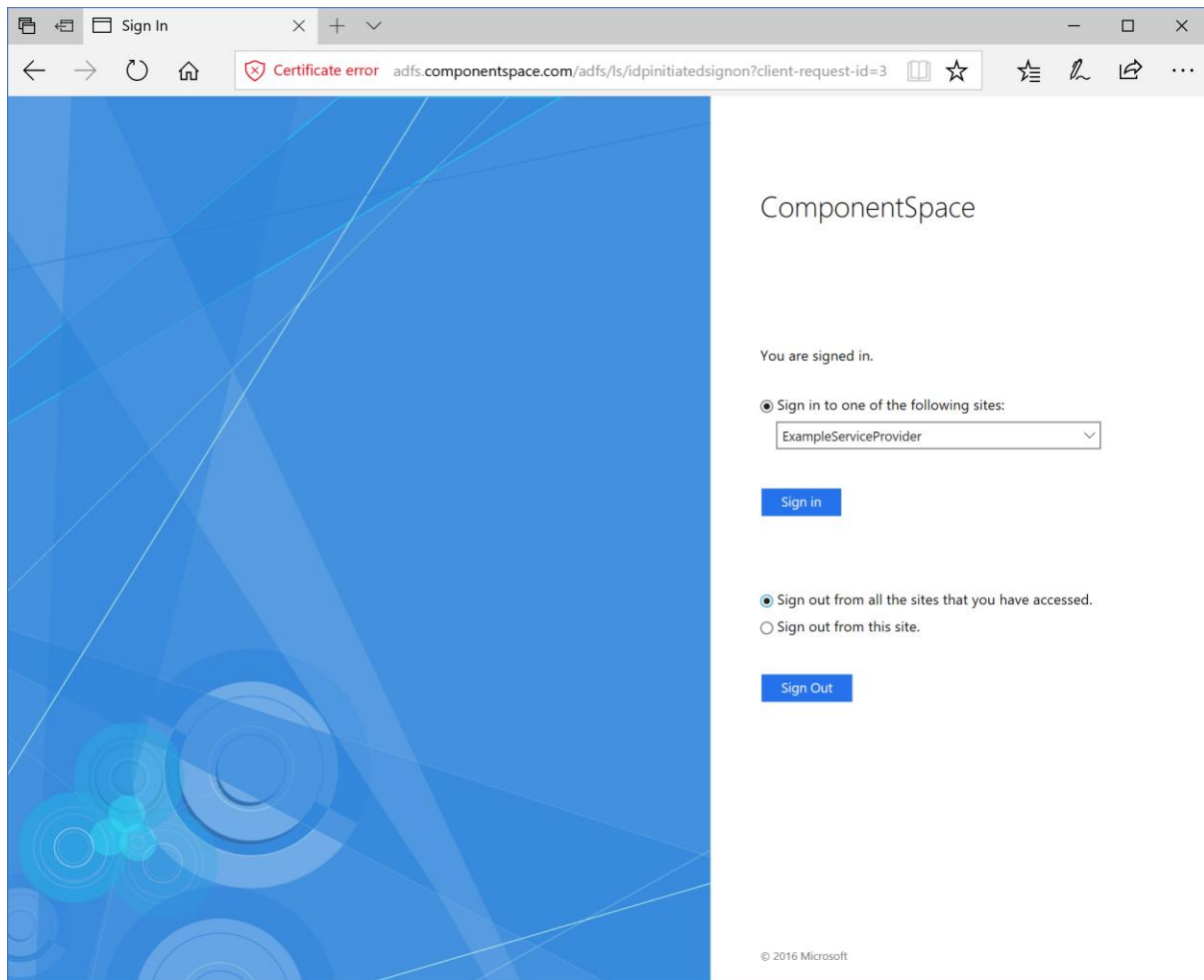
<https://adfs.componentspace.com/adfs/ls/IdpInitiatedSignon>



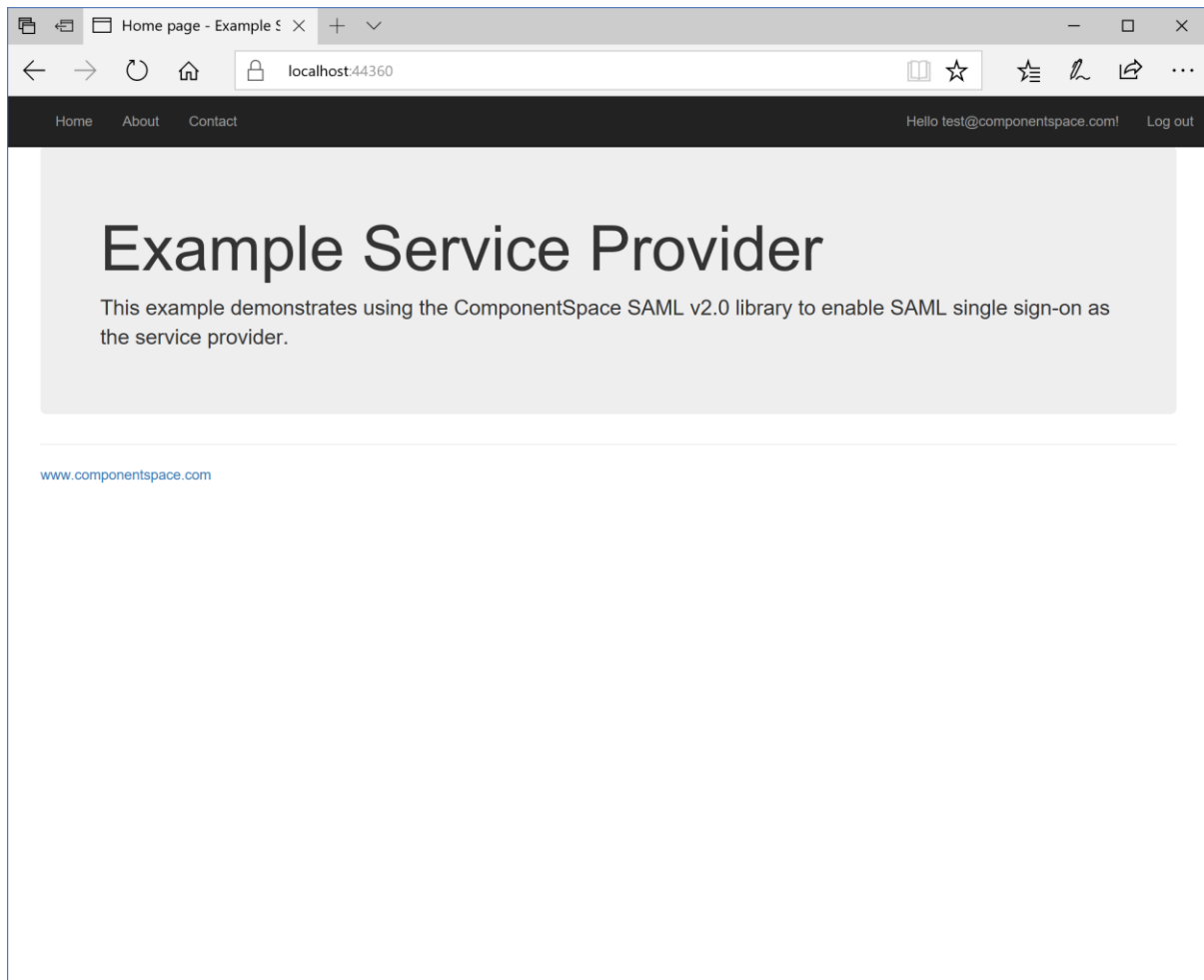
Log into ADFS.



Select the service provider and sign in.



The user is automatically logged in at the service provider.



SAML Logout

Both SP-initiated and IdP-initiated SLO are supported.

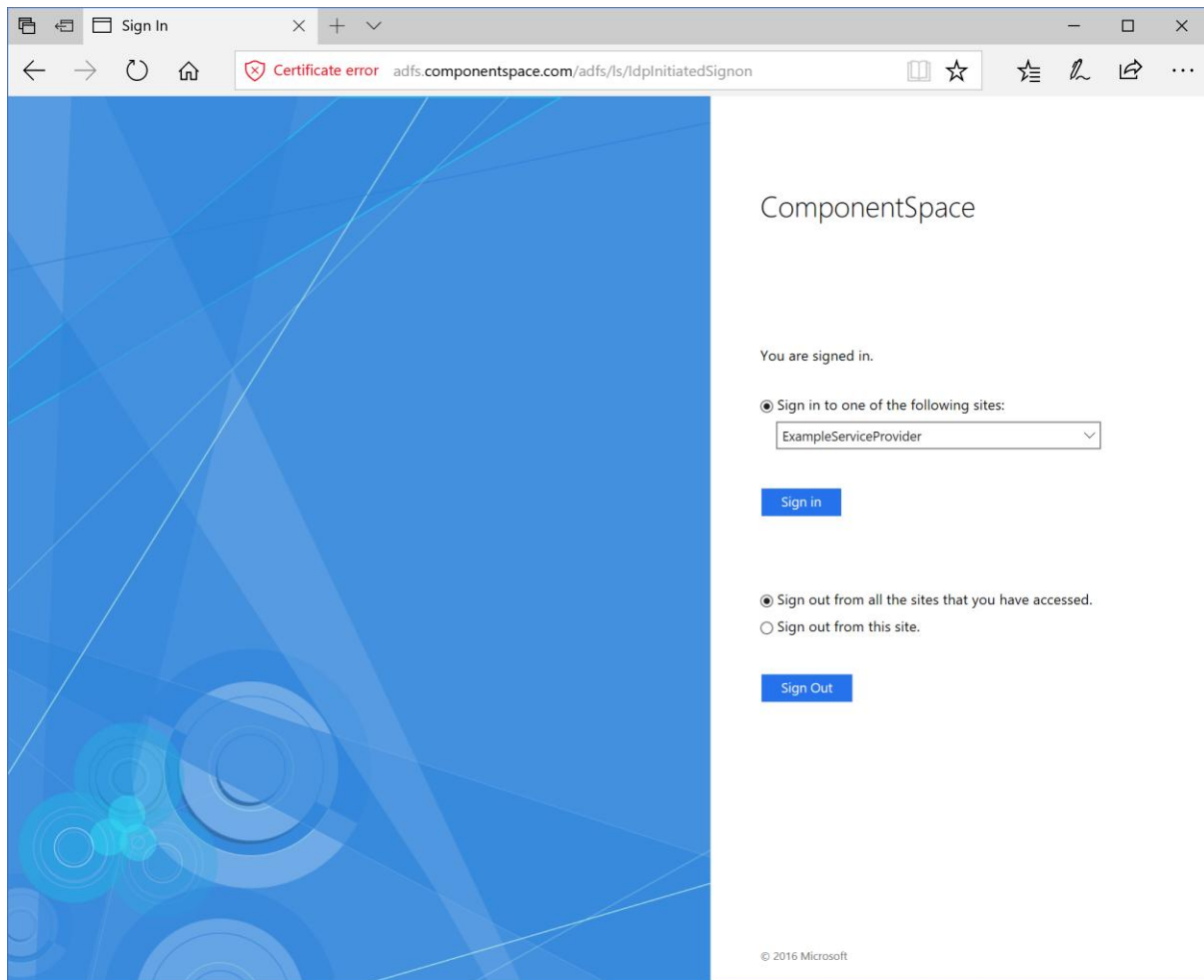
IdP-initiated SLO may be invoked from:

<https://<server-name>/adfs/ls/IdpInitiatedSignon>

For example:

<https://adfs.componentspace.com/adfs/ls/IdpInitiatedSignon>

Select to sign out from all sites.



Depending on the authentication method and the browser used, although ADFS reports logout as successful, the user may not be logged out from ADFS.

For example, with forms authentication and using Chrome, the user is logged out from ADFS.

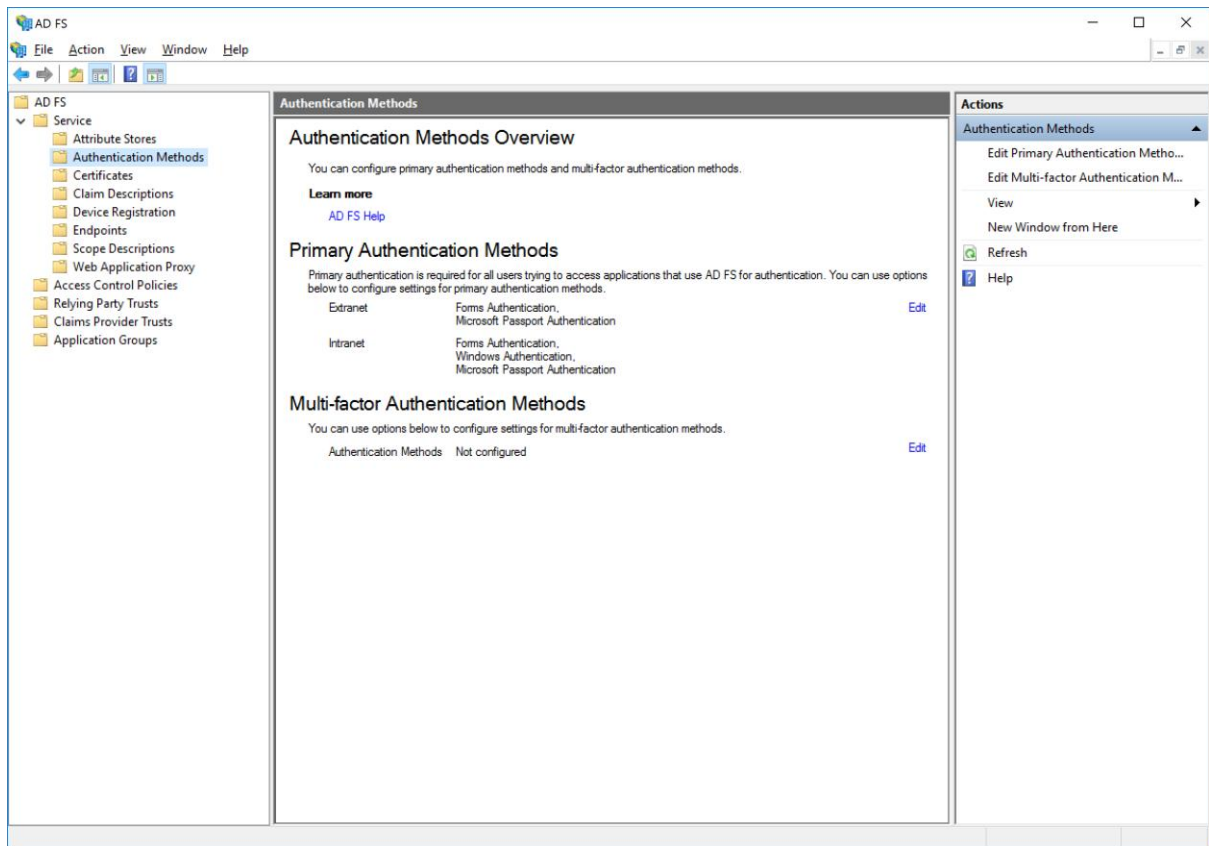
When using Microsoft Edge, no error occurs but the user is still logged into ADFS.

This functionality is controlled by ADFS.

ADFS Authentication Methods

ADFS supports a number of authentication methods that may be configured based on whether the user is in the intranet or not.

ComponentSpace SAML for ASP.NET Core ADFS Relying Party Integration Guide



The default configuration is to use Windows authentication for intranet users using a browser supporting Windows integrated authentication. Otherwise, forms authentication is used.

Edit Authentication Methods [X]

Primary **Multi-factor**

Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.

If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.

[Learn more](#) about Azure MFA (Multi-Factor Authentication).

Extranet

- ☒ Forms Authentication
- ☐ Certificate Authentication
- ☐ Device Authentication
- ☒ Microsoft Passport Authentication

Intranet

- ☒ Forms Authentication
- ☒ Windows Authentication
- ☐ Certificate Authentication
- ☐ Device Authentication
- ☒ Microsoft Passport Authentication

i Azure MFA authentication methods will not be available until an Azure Active Directory tenant is configured. [Learn More](#)

i To use device authentication as a primary authentication method, you need to configure device registration.

OK Cancel Apply

Windows Integrated Authentication

For a user logged into the domain, Windows integrated authentication, means the user is not prompted to login again. The Windows user principal name is used instead.

If Windows integrated authentication is enabled but the user is not logged into the domain, ADFS returns a 401, unauthorized, error to the browser which will prompt the user for their credentials and send an authorization header along with the SAML authentication request to ADFS.

Note SAML logout will be successful but the user will remain logged into ADFS.

Browser Support

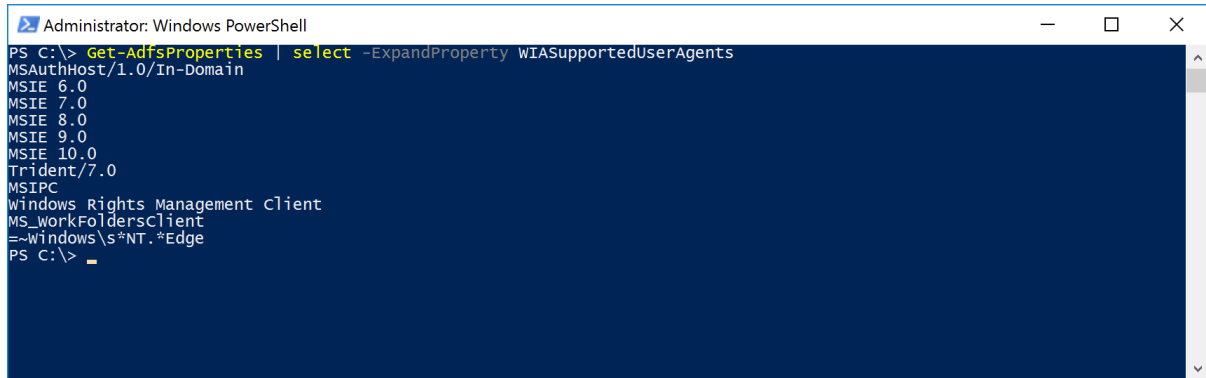
Microsoft Edge and Internet Explorer support Windows integrated authentication by default.

Support for other browsers may be enabled using the `WIASupportedUserAgent` setting.

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-browser-wia>

The default settings support Internet Explorer and Microsoft Edge.

The “=~” syntax indicates a regular expression when matching the user agent.



```

Administrator: Windows PowerShell
PS C:\> Get-AdfsProperties | select -ExpandProperty WIASupportedUserAgents
MSAuthHost/1.0/In-Domain
MSIE 6.0
MSIE 7.0
MSIE 8.0
MSIE 9.0
MSIE 10.0
Trident/7.0
MSIPC
Windows Rights Management client
MS_workFoldersClient
=~Windows\s*NT.*Edge
PS C:\>

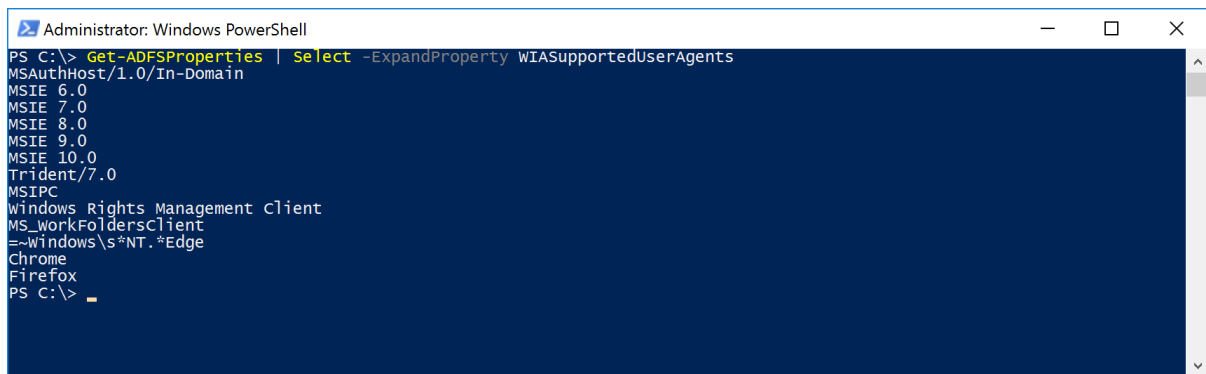
```

The following PowerShell command includes Chrome as a supported user agent.

Set-AdfsProperties -WIASupportedUserAgents ((Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents) + “Chrome”)

The following command includes Firefox as a supported user agent.

Set-AdfsProperties -WIASupportedUserAgents ((Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents) + “Firefox”)



```

Administrator: Windows PowerShell
PS C:\> Get-AdfsProperties | select -ExpandProperty WIASupportedUserAgents
MSAuthHost/1.0/In-Domain
MSIE 6.0
MSIE 7.0
MSIE 8.0
MSIE 9.0
MSIE 10.0
Trident/7.0
MSIPC
Windows Rights Management client
MS_workFoldersClient
=~Windows\s*NT.*Edge
Chrome
Firefox
PS C:\>

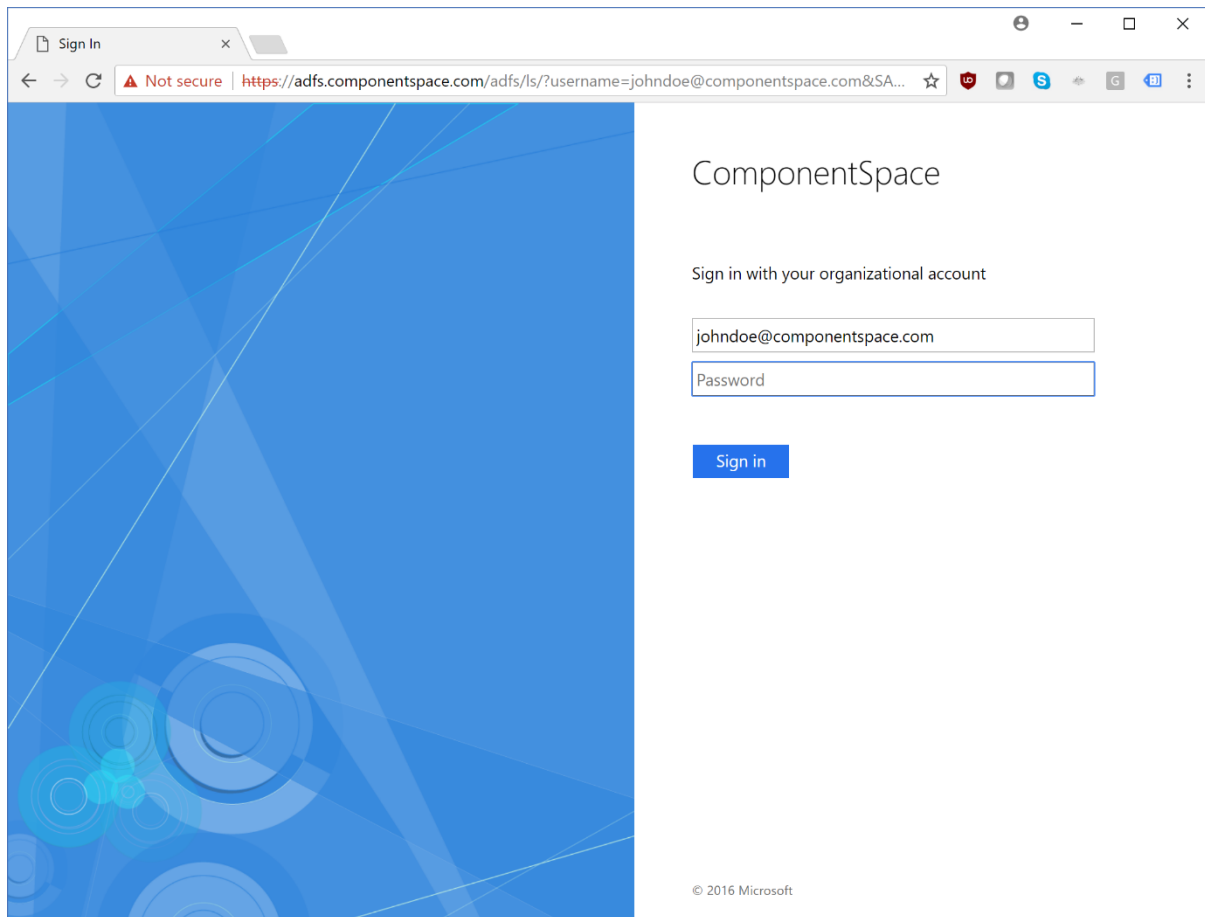
```

The following command removes Chrome and Firefox from the list of supported user agents.

Set-AdfsProperties -WIASupportedUserAgents (Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents | Where-Object { \$_ -ne "Chrome" -and \$_ -ne "Firefox" })

Default User Name

ADFS accepts a username query string parameter that specifies the user name to include in the login form.



The syntax is:

`https://<server-name>/adfs/ls/?username=<user-name>`

For example:

<https://adfs.componentspace.com/adfs/ls/?username=johndoe@componentspace.com>

This is useful if for some reason the user has already entered their user name at the service provider.

For security reasons, ADFS does not support passwords being included as a query string parameter.

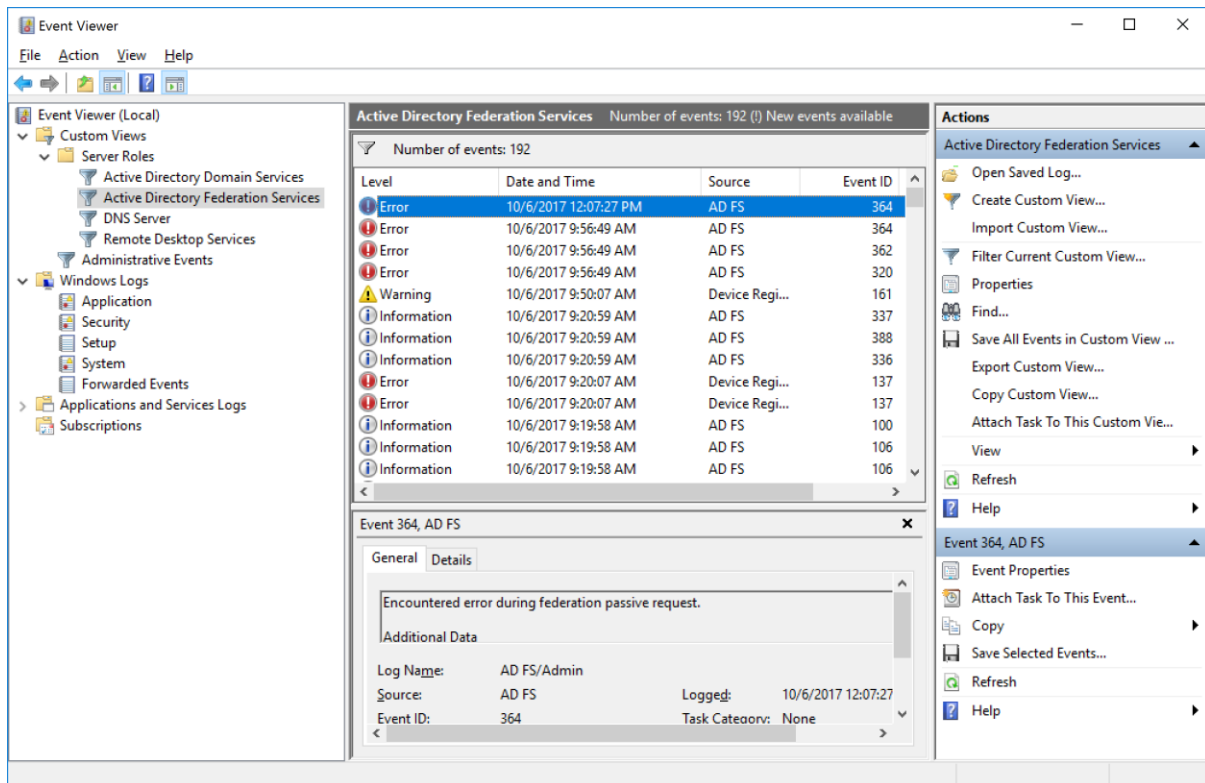
The OnResolveUrl delegate may be used to update the SSO service URL with the query string parameter. Refer to the Developer Guide for details.

Troubleshooting ADFS SSO

If an error occurs, ADFS will display a generic error message in the browser or return a generic Requester/Responder error to the service provider.

To troubleshoot configuration and other problems, refer to the ADFS event log.

ComponentSpace SAML for ASP.NET Core ADFS Relying Party Integration Guide



For more information on troubleshooting ADFS, refer to:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-overview>

To enable ADFS trace logging, refer to:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging>