

ComponentSpace

SAML for ASP.NET Core

ADFS

Claims Provider

Integration Guide

Contents

Introduction.....	1
Enabling IdP-Initiated SSO.....	1
Adding a Claims Provider	1
Adding a Claims Rule	6
Reviewing Claims Provider Configuration.....	10
ADFS SAML Metadata.....	20
Identity Provider Configuration	21
SP-Initiated SSO	21
IdP-Initiated SSO	25
SAML Logout.....	28
Troubleshooting ADFS SSO	29

Introduction

This document describes integration of an identity provider with Active Directory Federation Services.

The Microsoft terminology for a SAML identity provider is a claims provider.

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
```

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

```
Get-AdfsProperties | select RelayStateForIdpInitiatedSignOnEnabled  
  
Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $True
```

For more information, refer to:

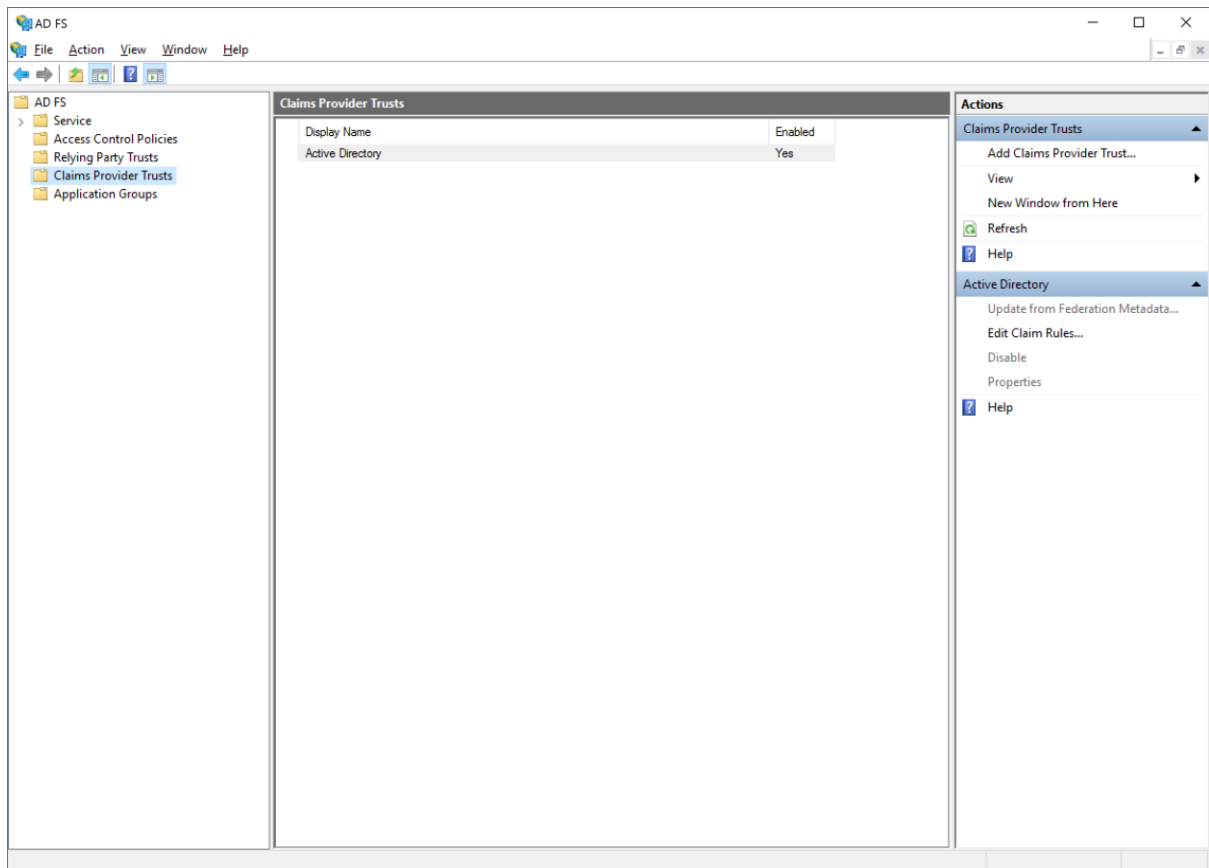
<https://blogs.technet.microsoft.com/rmilne/2017/06/20/how-to-enable-idpinitiatedsignon-page-in-ad-fs-2016/>

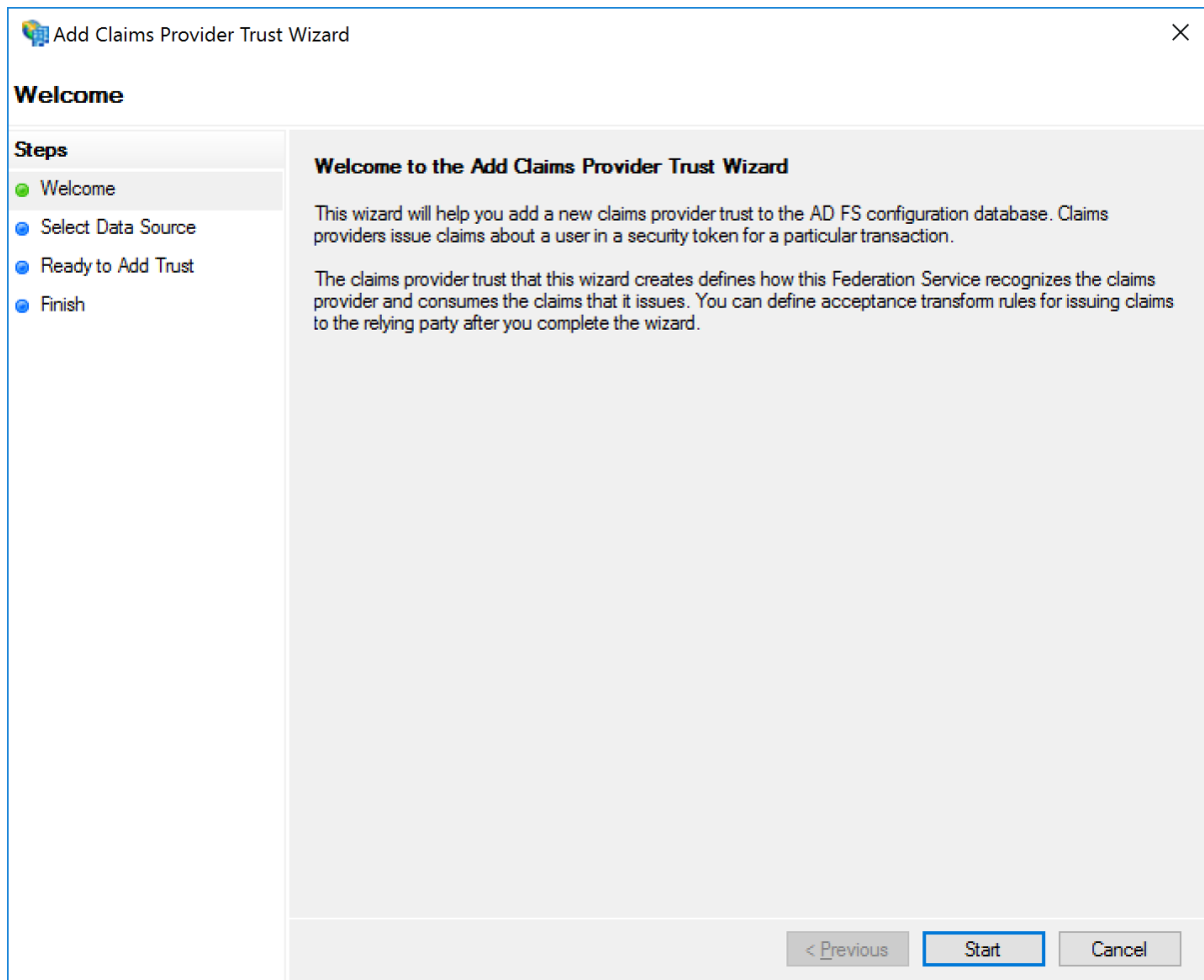
<https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties>

Adding a Claims Provider

Open the ADFS console and add a claims provider trust.

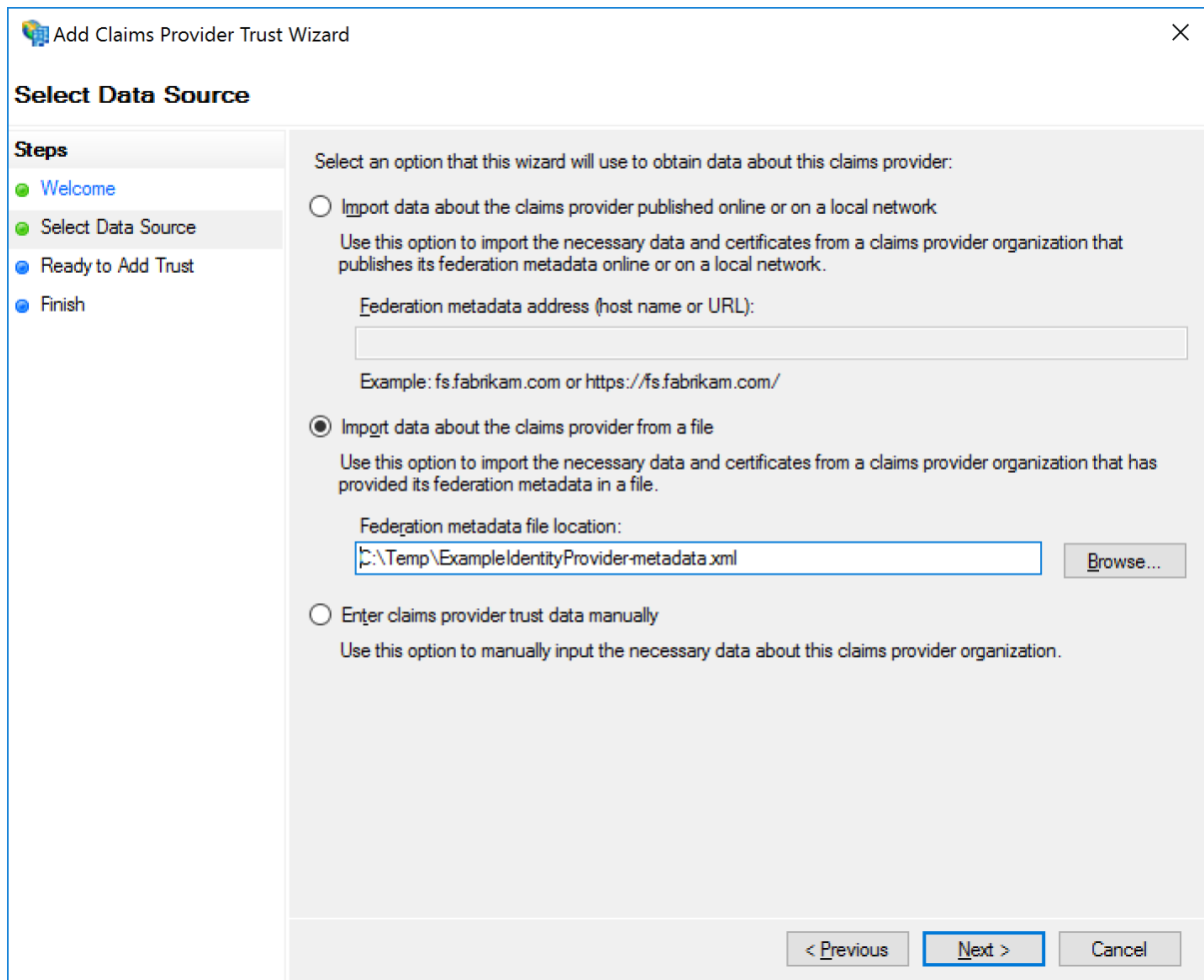
ComponentSpace SAML for ASP.NET Core ADFS Claims Provider Integration Guide





The claims provider may be configured through SAML metadata or manually.

The included SAML metadata for the ExampleIdentityProvider is used.



The image shows a Windows wizard window titled "Add Claims Provider Trust Wizard". The window has a close button (X) in the top right corner. The main title "Select Data Source" is displayed at the top left. On the left side, there is a "Steps" pane with four steps: "Welcome" (green dot), "Select Data Source" (green dot and highlighted), "Ready to Add Trust" (blue dot), and "Finish" (blue dot). The main area of the wizard contains the following content:

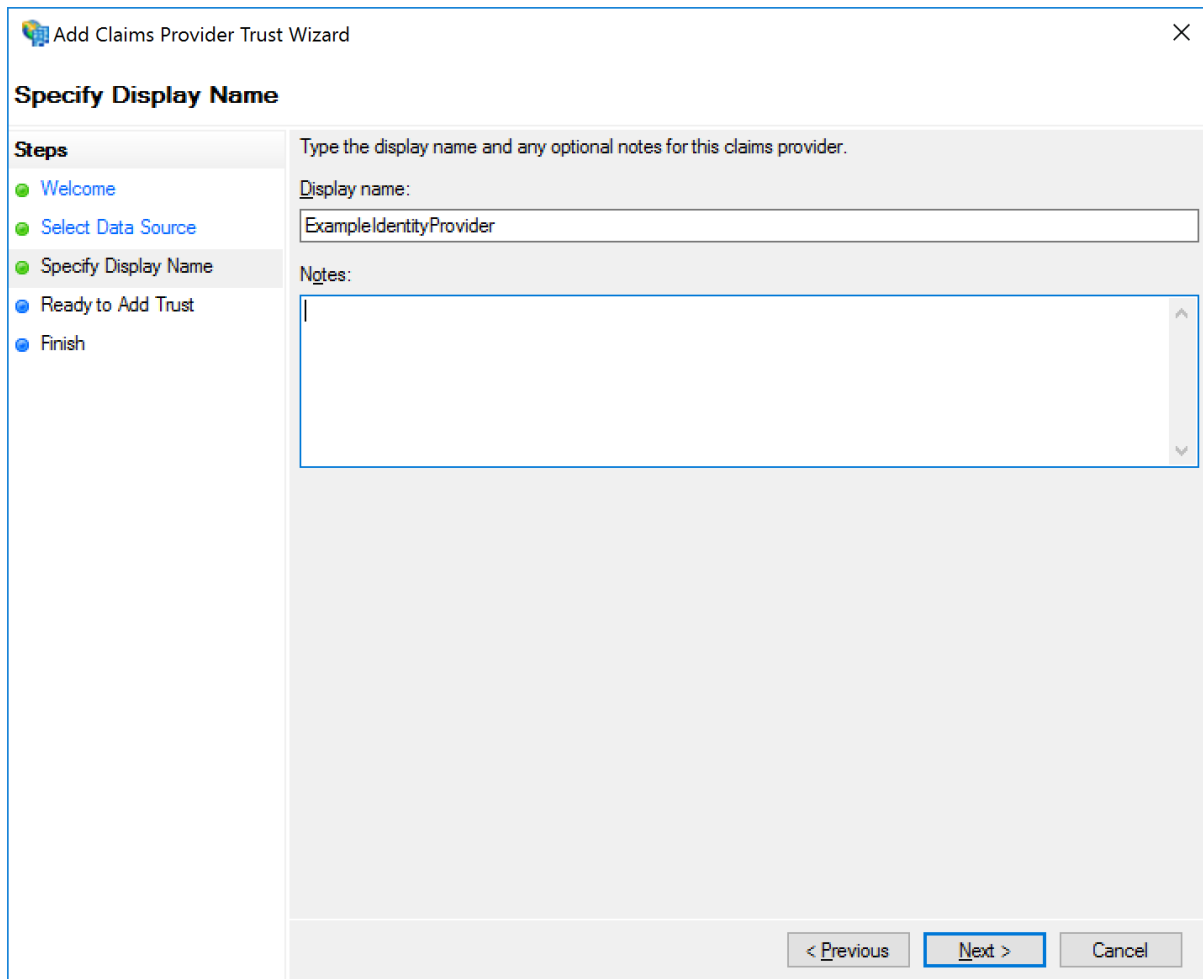
Select an option that this wizard will use to obtain data about this claims provider:

- ☐ Import data about the claims provider published online or on a local network
Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):

Example: fs.fabrikam.com or https://fs.fabrikam.com/
- ☒ Import data about the claims provider from a file
Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.
Federation metadata file location:
- ☐ Enter claims provider trust data manually
Use this option to manually input the necessary data about this claims provider organization.

At the bottom right, there are three buttons: "< Previous" (disabled), "Next >" (highlighted with a blue border), and "Cancel" (disabled).

Provide a name purely for display purpose.



The image shows a screenshot of the 'Add Claims Provider Trust Wizard' window, specifically the 'Specify Display Name' step. The window has a title bar with the text 'Add Claims Provider 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 with a blue dot and bold text), 'Ready to Add Trust', and 'Finish'. The main area of the wizard is titled 'Specify Display Name' and contains the instruction 'Type the display name and any optional notes for this claims provider.' Below this instruction, there is a 'Display name:' label followed by a text input field containing the text 'ExampleIdentityProvider'. To the right of the input field is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar. At the bottom right of the wizard, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Add Claims Provider Trust Wizard

Specify Display Name

Type the display name and any optional notes for this claims provider.

Steps

- Welcome
- Select Data Source
- Specify Display Name**
- Ready to Add Trust
- Finish

Display name:

ExampleIdentityProvider

Notes:

< Previous **Next >** Cancel

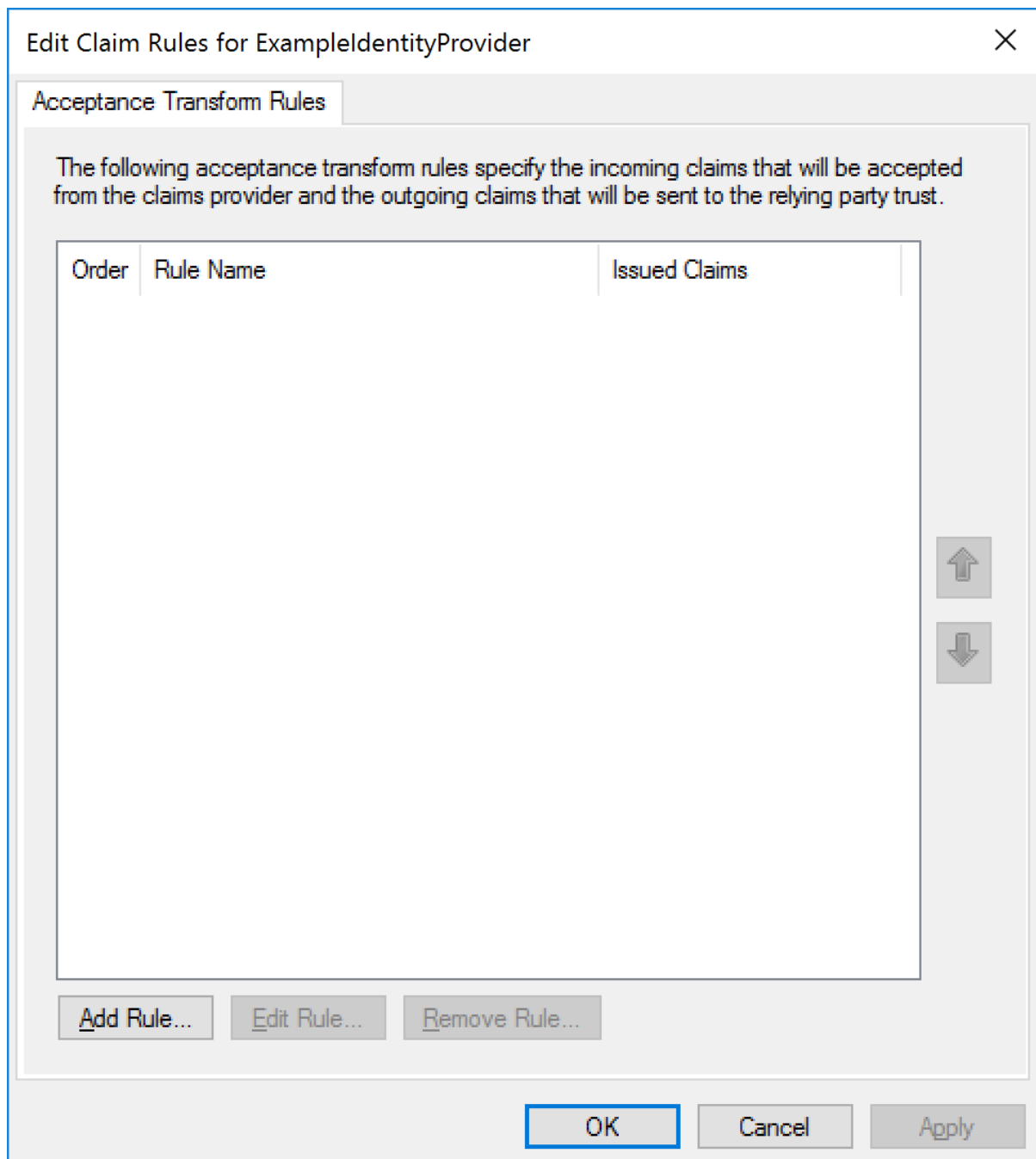
Review the configuration. This can be updated later if required.

The screenshot shows the 'Add Claims Provider Trust Wizard' window. The title bar reads 'Add Claims Provider Trust Wizard'. The window is divided into two main sections. On the left is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source', 'Specify Display Name', 'Ready to Add Trust' (which is highlighted with a blue circle), and 'Finish'. The main area on the right is titled 'Ready to Add Trust' and contains the following text: 'The claims provider trust has been configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configuration database.' Below this text is a tabbed interface with tabs for 'Monitoring', 'Identifiers', 'Certificates', 'Encryption', 'Offered Claims', 'Organization', 'Endpoints', and 'Notes'. The 'Monitoring' tab is selected. Inside the 'Monitoring' tab, there is a section titled 'Specify the trust monitoring settings for this claims provider trust.' which includes a text box for 'Claims provider's federation metadata URL:', a checkbox for 'Monitor claims provider' (which is unchecked), and a sub-checkbox for 'Automatically update claims provider' (also unchecked). Below these are two lines of status information: 'This claims provider's federation metadata was last checked on: < never >' and 'This claims provider trust was last updated from federation metadata on: < never >'. At the bottom right of the window are three buttons: '< Previous', 'Next >' (which is highlighted with a blue dashed border), and 'Cancel'.


Adding a Claims Rule

Claim rules map the SAML subject name identifier and SAML attributes that are included in the SAML assertion from the identity provider into claims.

Add rules to pass through incoming claims.



Add a rule based off the transform an incoming claim template.

 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:

Transform an Incoming Claim ▾

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous

Next >

Cancel

Pass through the name identifier.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

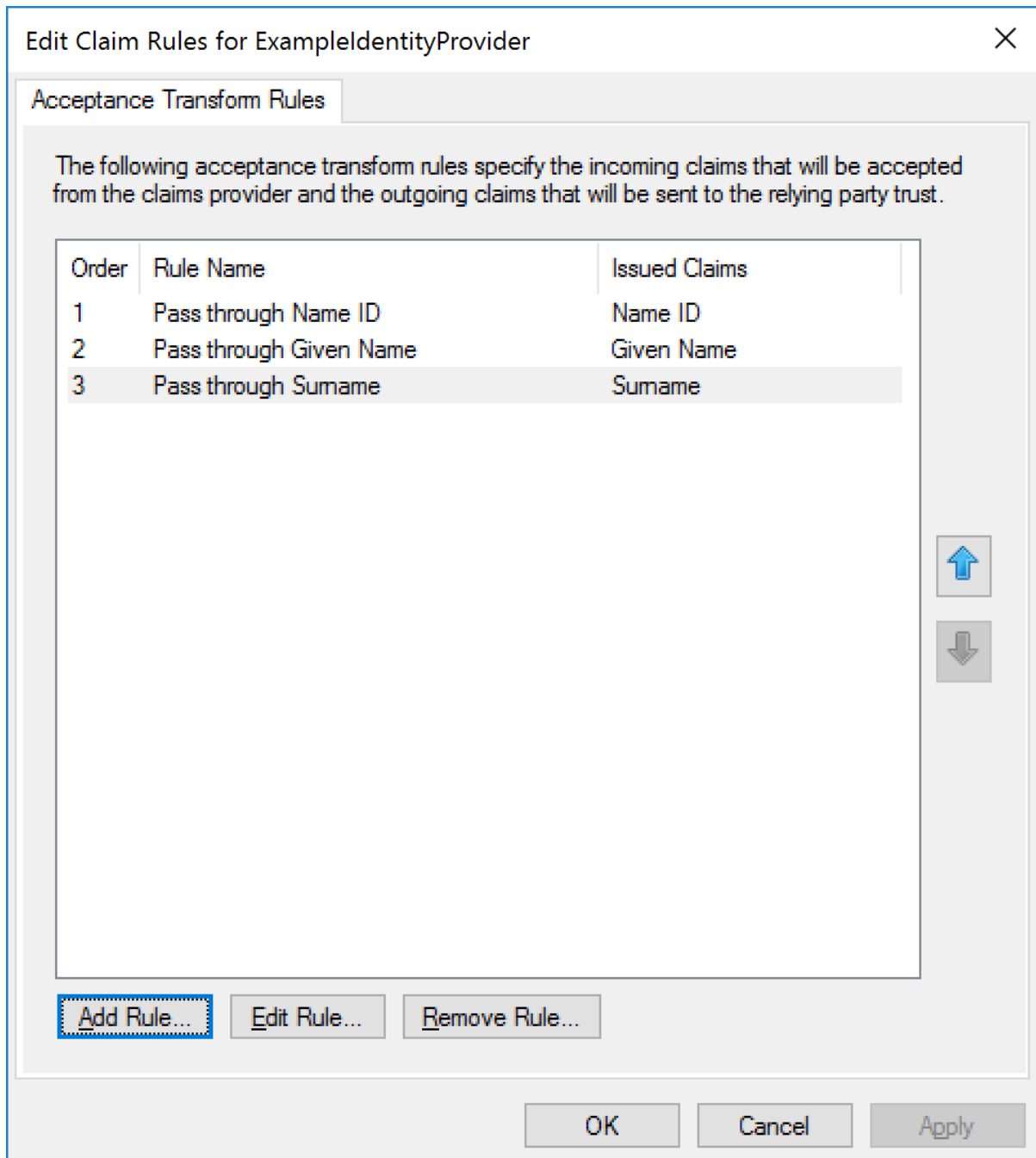
Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values
☐ Replace an incoming claim value with a different outgoing claim value
 Incoming claim value:
 Outgoing claim value:
☐ Replace incoming e-mail suffix claims with a new e-mail suffix
 New e-mail suffix:
 Example: fabrikam.com

ADFS displays a security best practice warning when passing through all claim values. Selecting specific claims for pass through is recommended.

Add similar rules for the given name and surname.

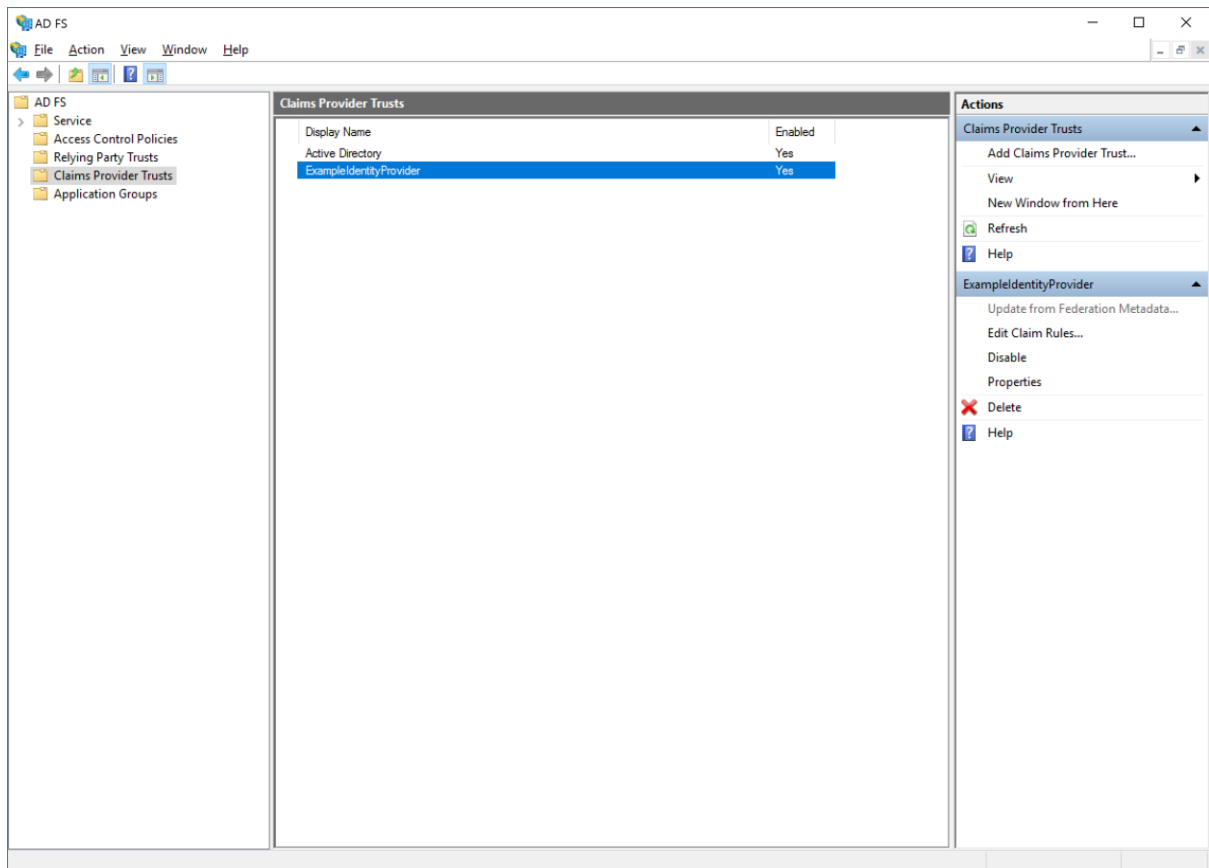


If working with the ExampleServiceProvider relying party, similar rules should be added to the relying party to pass these claims through.

Reviewing Claims Provider Configuration

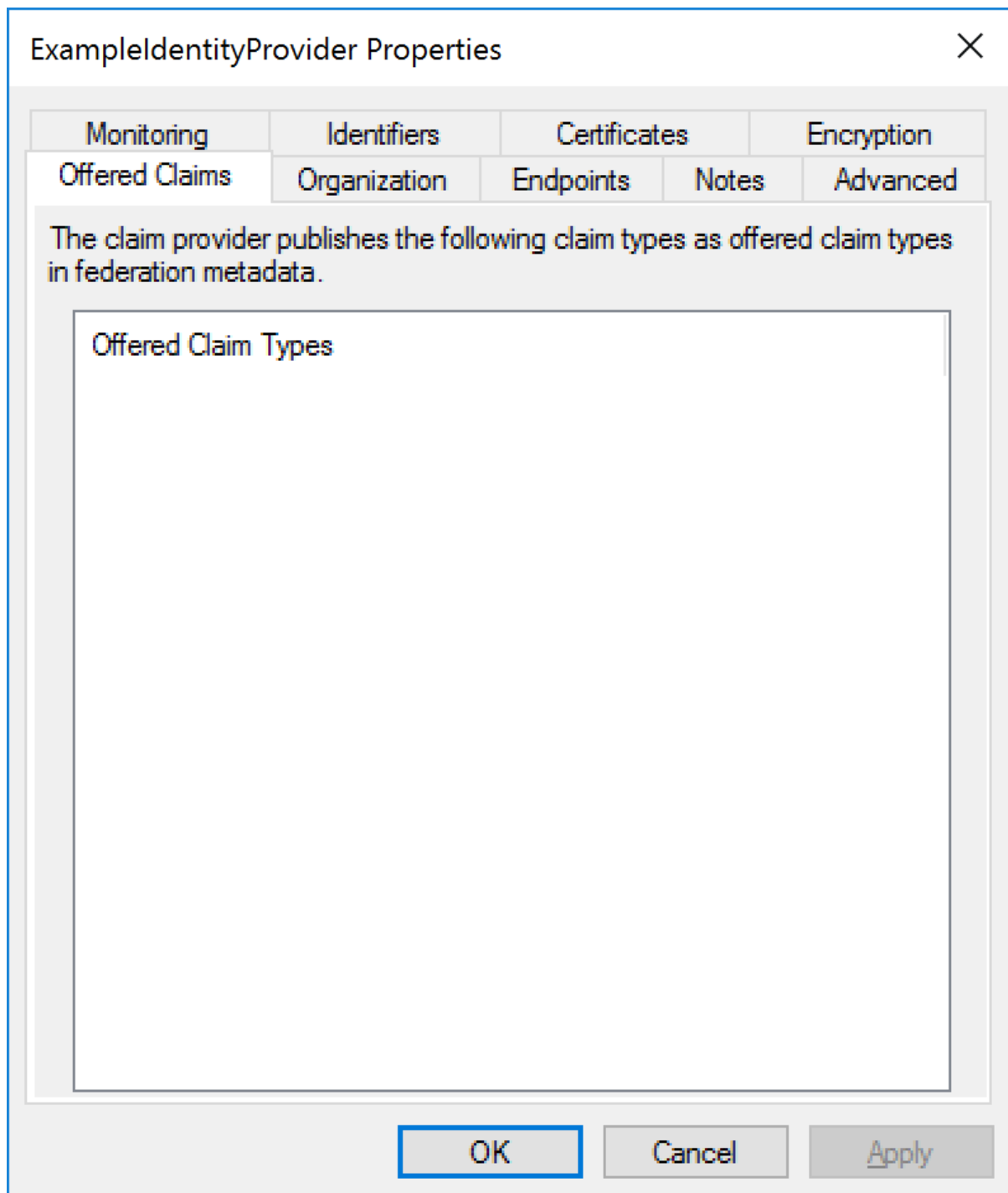
The configuration may be reviewed or modified through the claim provider's property tabs.

ComponentSpace SAML for ASP.NET Core ADFS Claims Provider Integration Guide

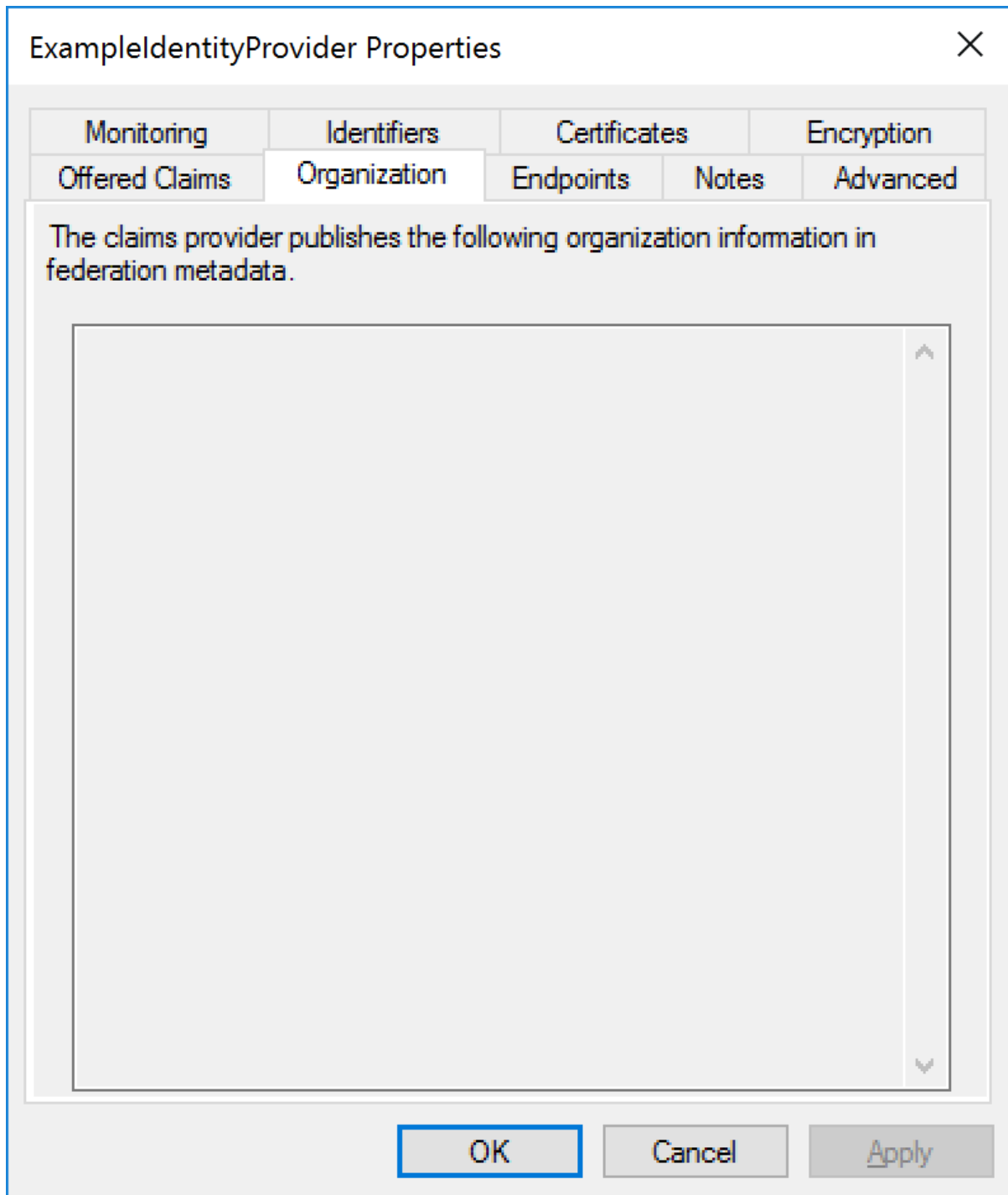


The offered claims are specified through the identity provider's SAML metadata.

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



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 identity provider.

The SAML single sign-on service receives SAML authn requests as part of SSO.

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

ExampleIdentityProvider Properties

Monitoring Identifiers Certificates Encryption
Offered Claims Organization Endpoints Notes Advanced

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

URL	Index	Binding	Default	Re
SAML Single Sign-On Endpoints				
https://localhost:44313/SAM...		Redirect	No	
SAML Logout Endpoints				
https://localhost:44313/SAM...		Redirect	No	

< >

Add SAML...

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

OK Cancel Apply

Notes are internal to ADFS and for documentation purposes only.

The screenshot shows a Windows-style dialog box titled "ExampleIdentityProvider Properties" with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: "Monitoring", "Identifiers", "Certificates", "Encryption", "Offered Claims", "Organization", "Endpoints", "Notes" (which is the active tab), and "Advanced". The "Notes" tab contains the text "Specify any notes about this claims provider 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".

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

SHA-256 is recommended.

The screenshot shows a dialog box titled 'ExampleIdentityProvider Properties' with a close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: 'Monitoring', 'Identifiers', 'Certificates', 'Encryption', 'Offered Claims', 'Organization', 'Endpoints', 'Notes', and 'Advanced'. The 'Advanced' tab is currently selected. Inside the 'Advanced' tab, there is a text label 'Specify the secure hash algorithm to use for this claims provider trust.' followed by a dropdown menu labeled 'Secure hash algorithm:' with 'SHA-256' selected. At the bottom of the dialog, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Monitoring	Identifiers	Certificates	Encryption
Offered Claims	Organization	Endpoints	Notes
Advanced			

Specify the secure hash algorithm to use for this claims provider 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 "ExampleIdentityProvider Properties" with a close button (X) in the top right corner. The dialog has a tabbed interface with five tabs: "Offered Claims", "Organization", "Endpoints", "Notes", and "Advanced". The "Monitoring" tab is currently selected. Below the tabs, the text "Specify the trust monitoring settings for this claims provider trust." is displayed. There is a label "Claims provider's federation metadata URL:" followed by a text input field and a "Test URL" button. Below this, there are two checkboxes: "Monitor claims provider" (which is unchecked) and "Automatically update claims provider" (also unchecked). Under the "Monitor claims provider" checkbox, there are two lines of text: "This claims provider's federation metadata was last checked on:" followed by "< never >", and "This claims provider trust was last updated from federation metadata on:" followed by "< never >". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

ExampleIdentityProvider Properties

Offered Claims Organization Endpoints Notes Advanced

Monitoring Identifiers Certificates Encryption

Specify the trust monitoring settings for this claims provider trust.

Claims provider's federation metadata URL:

 Test URL

☐ Monitor claims provider

☐ Automatically update claims provider

This claims provider's federation metadata was last checked on:
< never >

This claims provider trust was last updated from federation metadata on:
< never >

OK Cancel Apply

Claims provider identifiers correspond to SAML metadata entity IDs.

The claims provider identifier must match exactly with the identity provider's configured name.

The screenshot shows a Windows-style dialog box titled 'ExampleIdentityProvider Properties' with a close button (X) in the top right corner. The dialog has a tabbed interface with five tabs: 'Offered Claims', 'Organization', 'Endpoints', 'Notes', and 'Advanced'. The 'Organization' tab is selected, and within it, the 'Identifiers' sub-tab is active. The main content area contains the instruction 'Specify the display name and identifier for this claims provider trust.' followed by two text input fields. The first field, labeled 'Display name:', contains the text 'ExampleIdentityProvider'. The second field, labeled 'Claims provider identifier:', contains the text 'https://ExampleIdentityProvider'. Below these fields is an example URL: 'Example: https://fs.fabrikam.com/adfs/services/trust'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Offered Claims	Organization	Endpoints	Notes	Advanced
Monitoring	Identifiers	Certificates		Encryption

Specify the display name and identifier for this claims provider trust.

Display name:

Claims provider identifier:

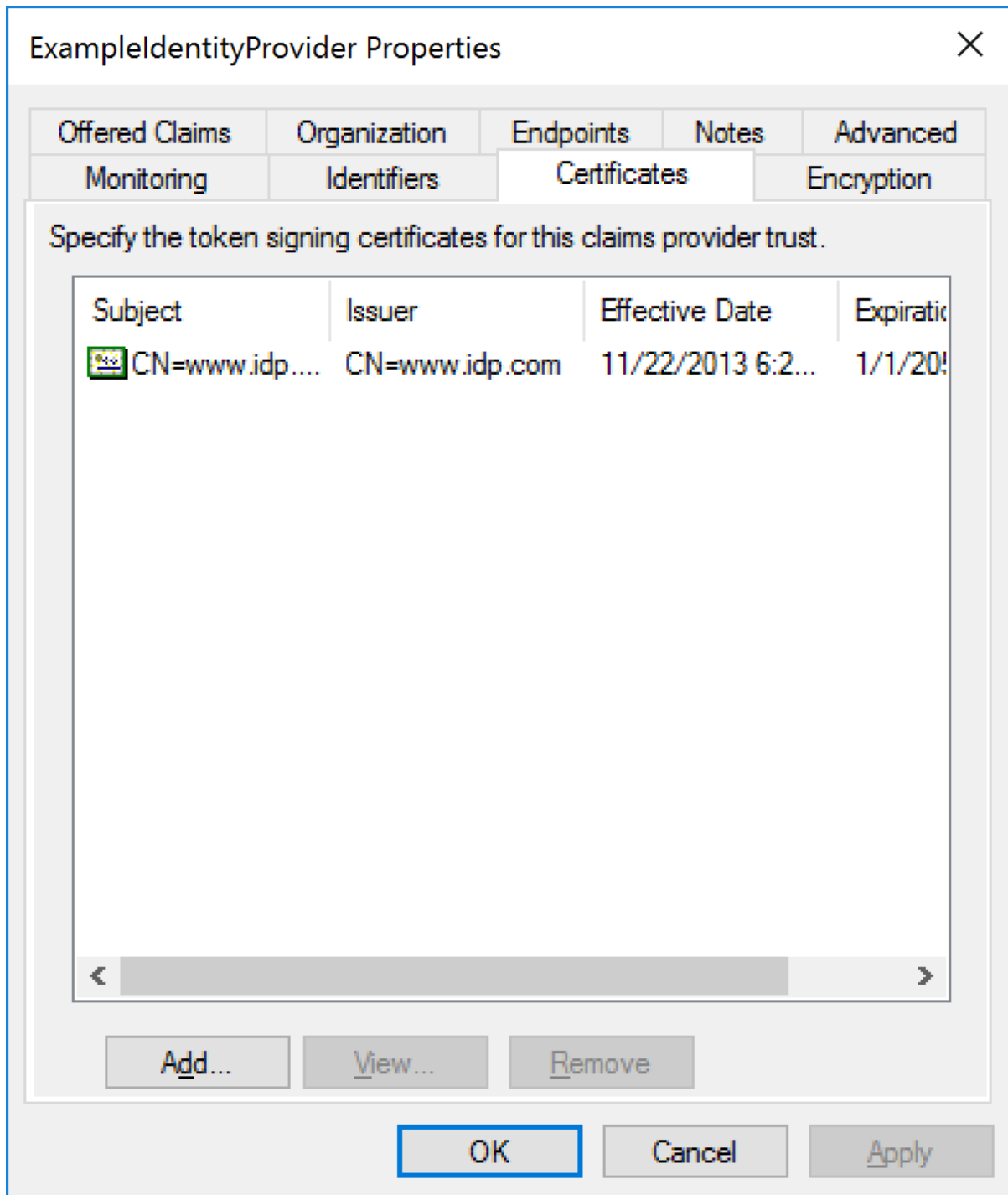
Example: https://fs.fabrikam.com/adfs/services/trust

OK Cancel Apply

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

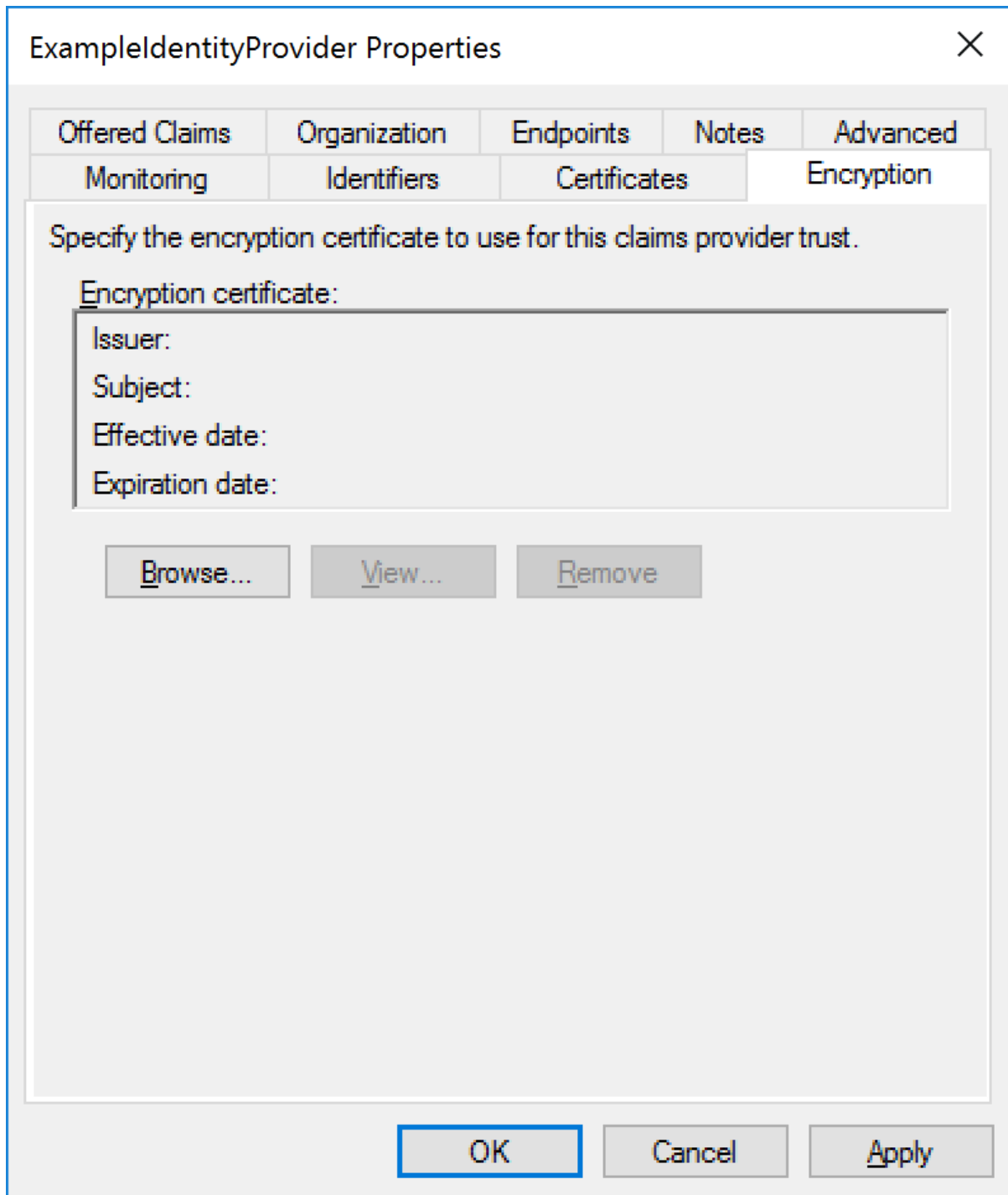
If specified, it's the identity provider's signature certificate.

It's recommended that SAML messages or assertions from the identity provider are signed.



The encryption certificate is not used and either may be ignored or removed.

If a SAML assertion is to be encrypted this is done using the service provider's certificate.



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>

Identity Provider Configuration

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

```
{
  "Name": "http://ads.componentspace.com/ads/services/trust",
  "Description": "ADFS",
  "SignAssertion": true,
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "WantLogoutRequestSigned": true,
  "WantLogoutResponseSigned": true,
  "AssertionConsumerServiceUrl": "https://ads.componentspace.com/ads/ls/",
  "SingleLogoutServiceUrl": "https://ads.componentspace.com/ads/ls/",
  "PartnerCertificates": [
    {
      "FileName": "certificates/ads.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 requires SAML logout messages to signed.

Ensure the PartnerName specifies the correct partner service provider.

The RPID specifies a relying party by its identifier.

If not specified, ADFS prompts to select a relying party.

```
"PartnerName": "http://ads.componentspace.com/ads/services/trust",
"RelayState": "RPID=https://ExampleServiceProvider"
```

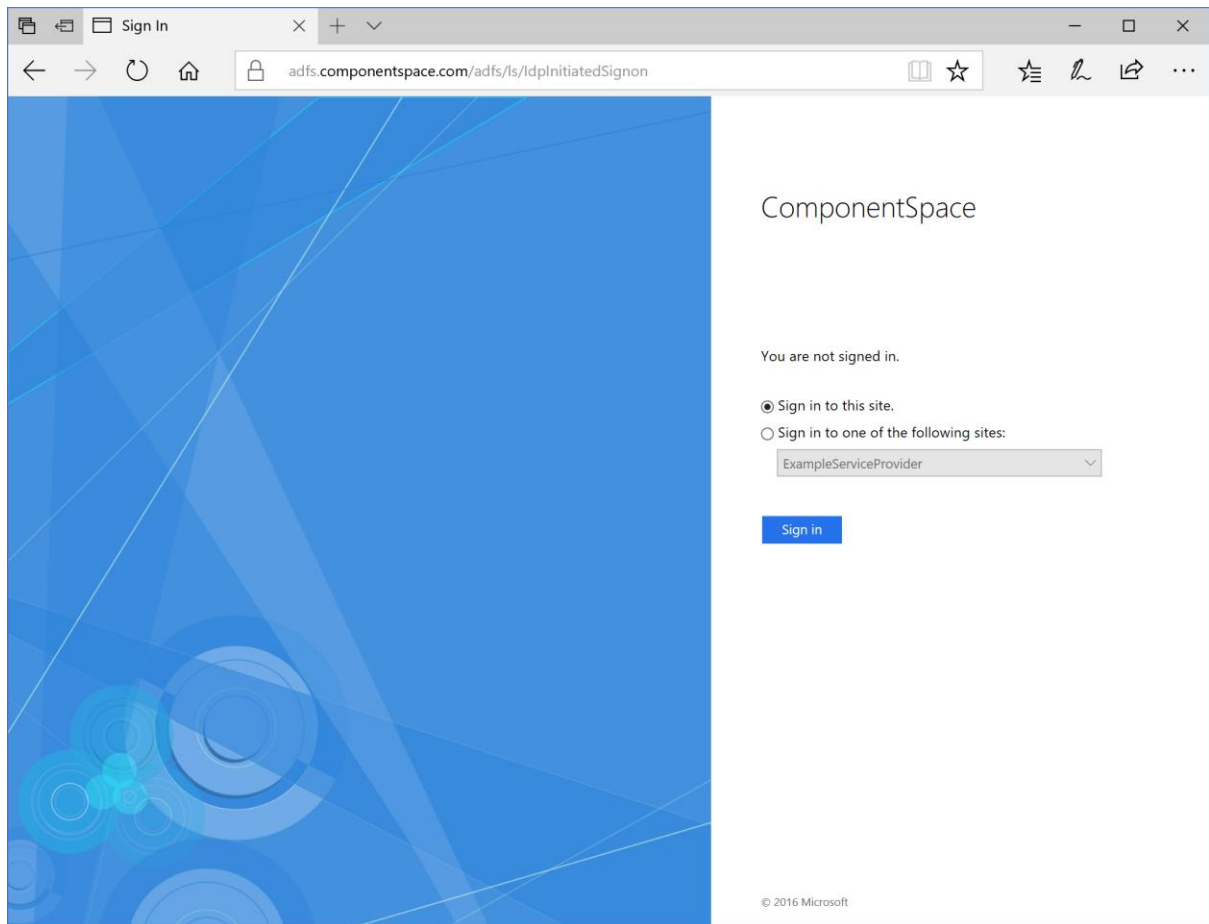
SP-Initiated SSO

Browse to:

<https://<server-name>/ads/ls/ldpInitiatedSignon>

For example:

<https://ads.componentspace.com/ads/ls/ldpInitiatedSignon>



Click the button to sign into this site.

Log in at the Identity Pr

localhost:44313/Account/Login?ReturnUrl=%2FSAML%2FSingleSignOnServiceCompleti

Home About Contact Register Log in

Log in at the Identity Provider

Use a local account to log in.

Use another service to log in.

Email

Password

☐ Remember me?

Log in

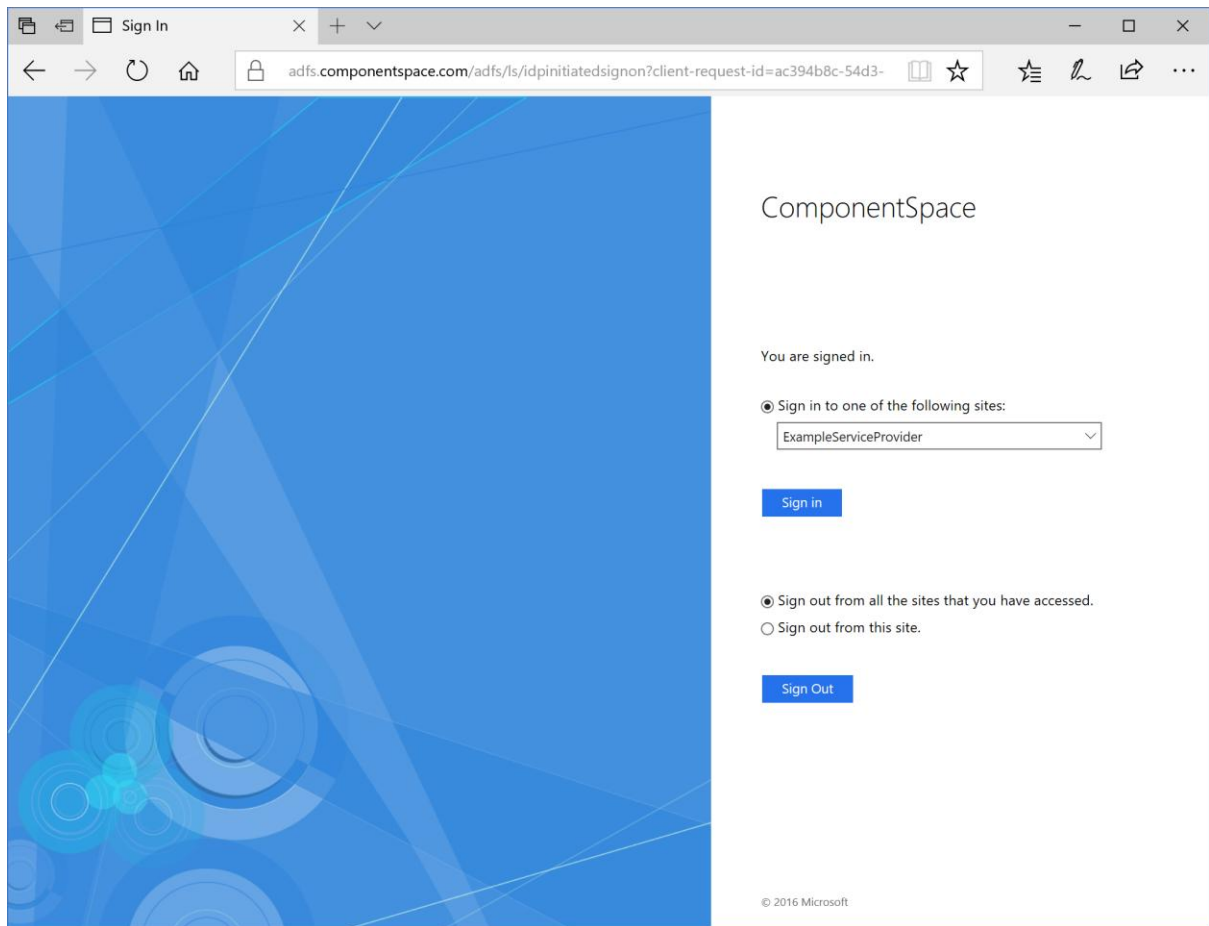
[Forgot your password?](#)

[Register as a new user](#)

There are no external authentication services configured. See [this article](#) for details on setting up this ASP.NET application to support logging in via external services.

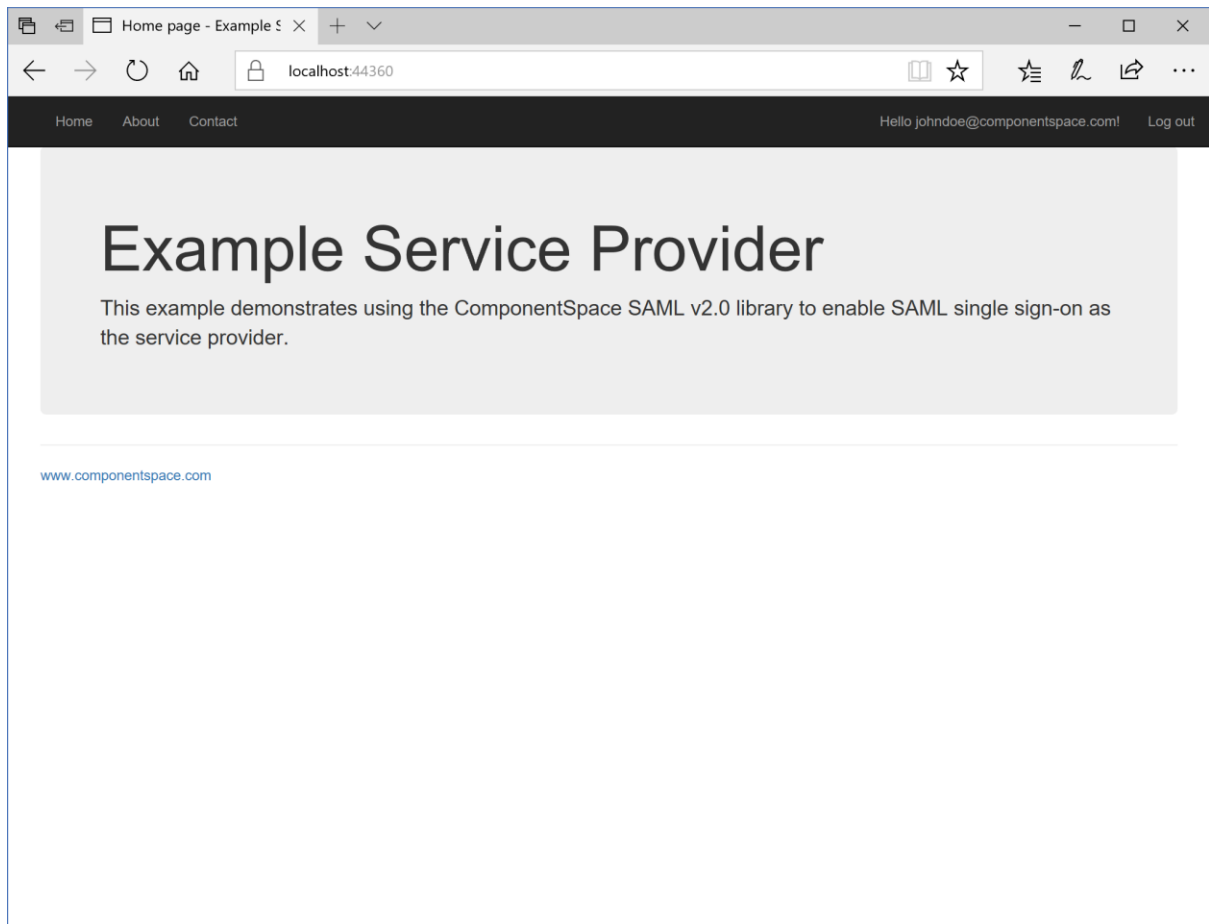
www.componentspace.com

Login at the example identity provider.



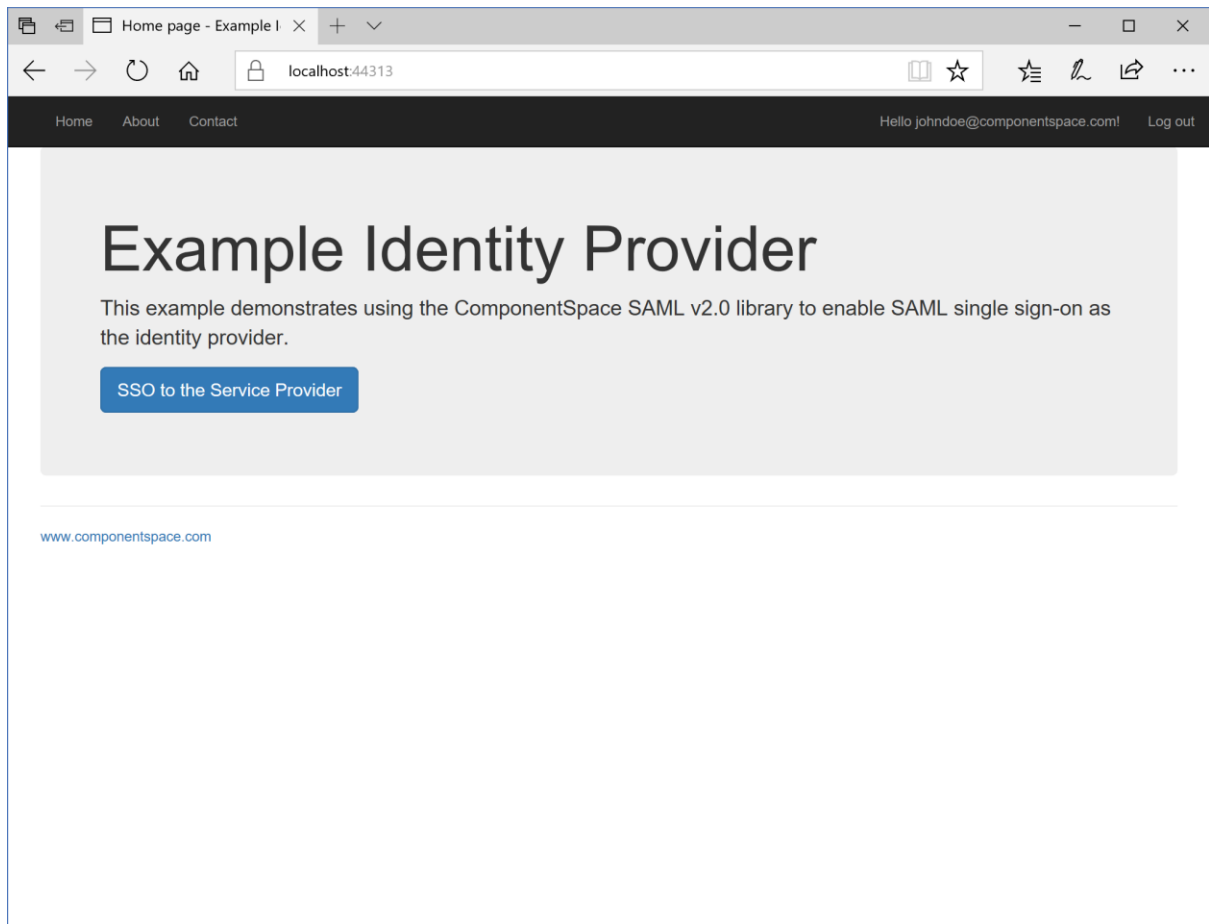
Select the relying party and click the Sign in button.

The user is automatically logged in at the service provider.

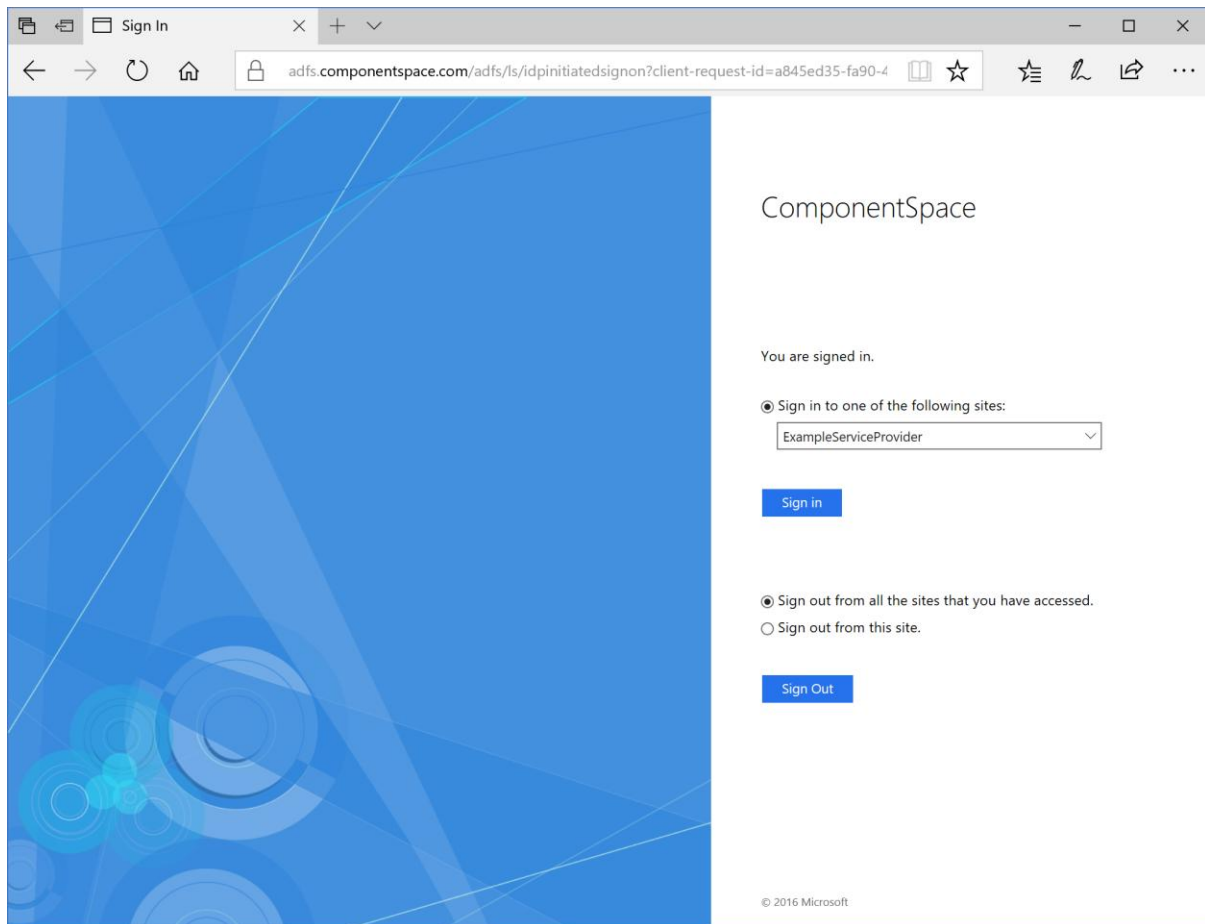


IdP-Initiated SSO

Browse to the example identity provider and login.



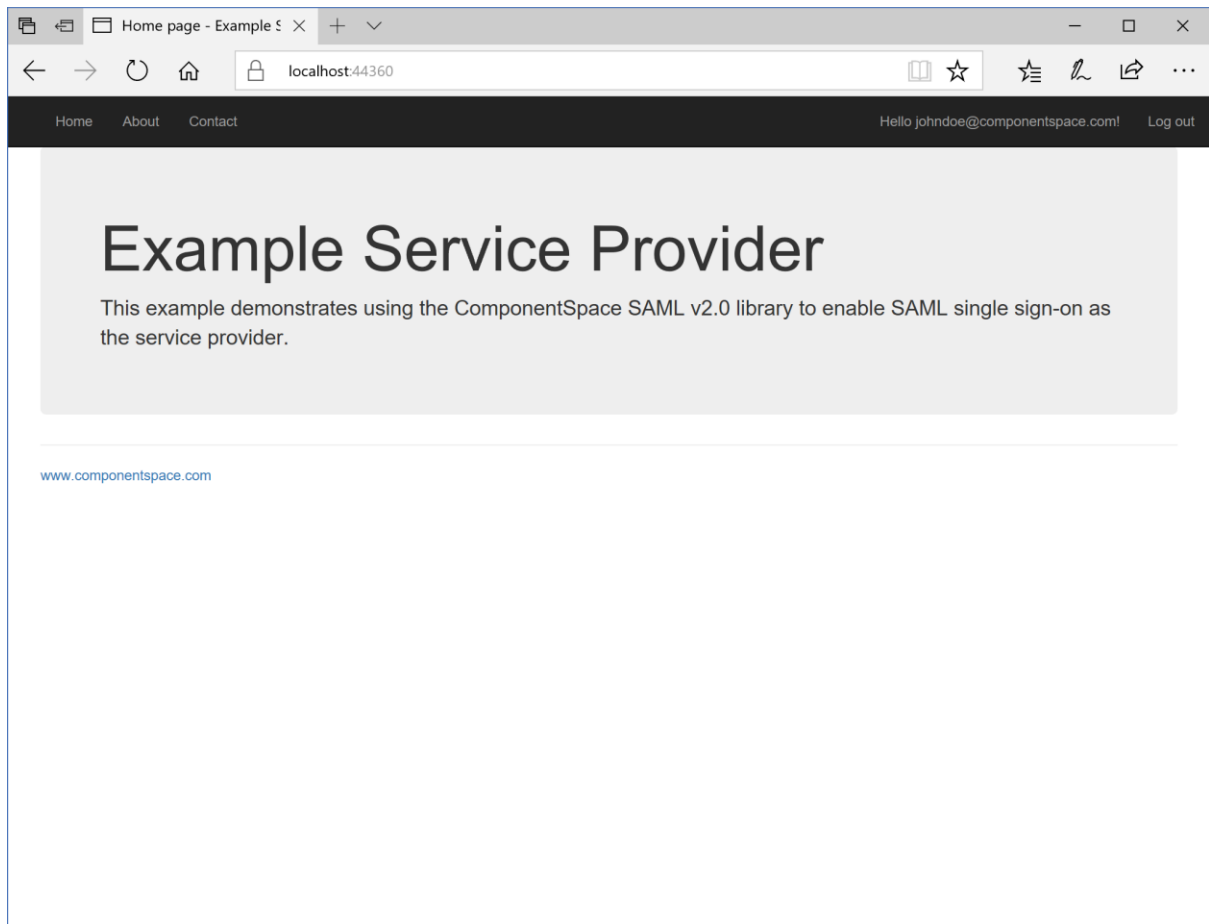
Click the button to browse to the service provider.



Select the relying party and click the Sign in button.

This step is only required if the relying party wasn't specified using the RPID relay state parameter.

The user is automatically logged in at the service provider.



SAML Logout

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

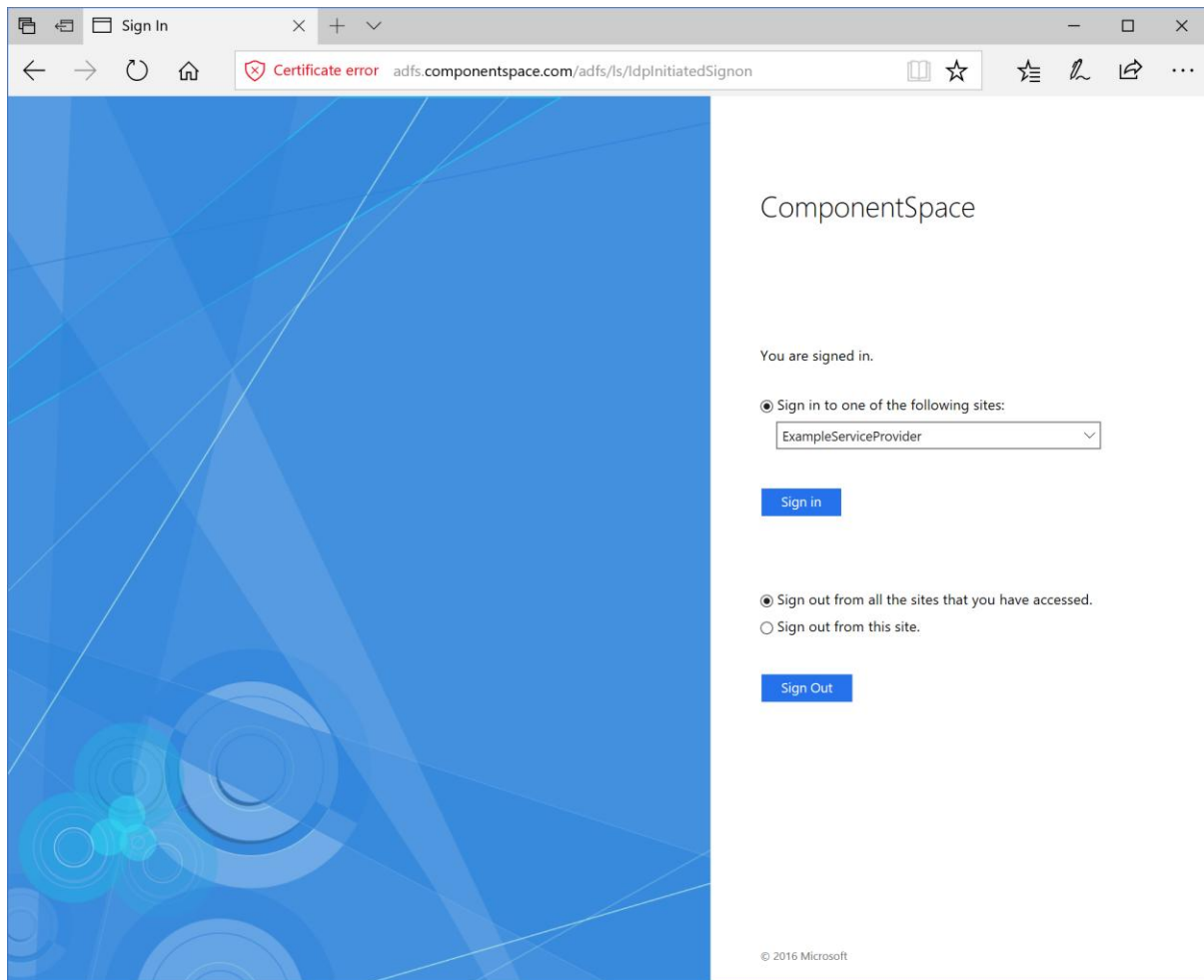
IdP-initiated SLO may be invoked from:

<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.

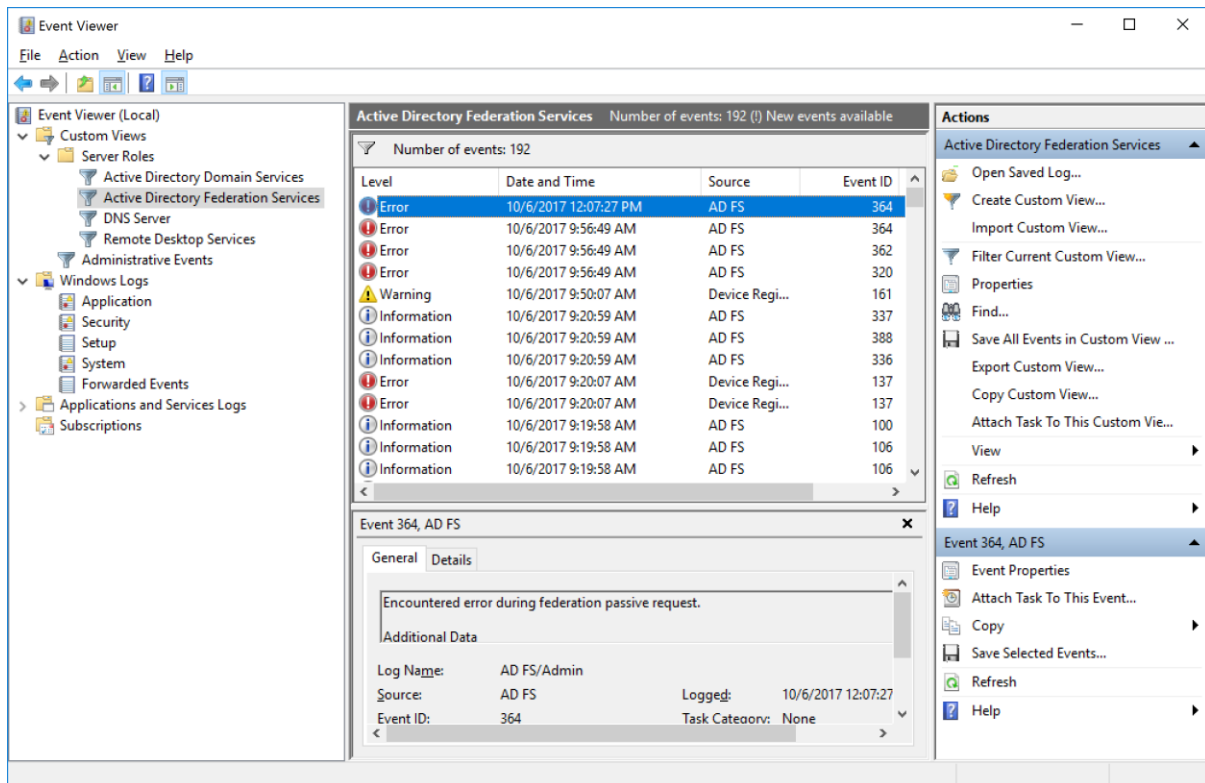
When using Microsoft Edge, no error occurs but the user is still logged into ADFS.

This functionality is controlled by ADFS.

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.



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>