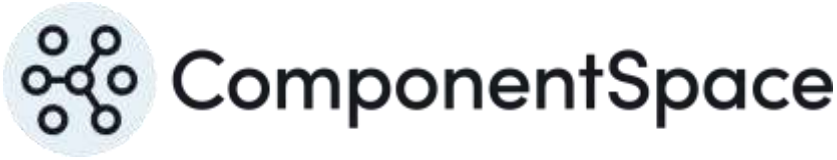


ComponentSpace
SAML for ASP.NET Core
ADFS
Claims Provider
Integration Guide

www.componentspace.com

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
```

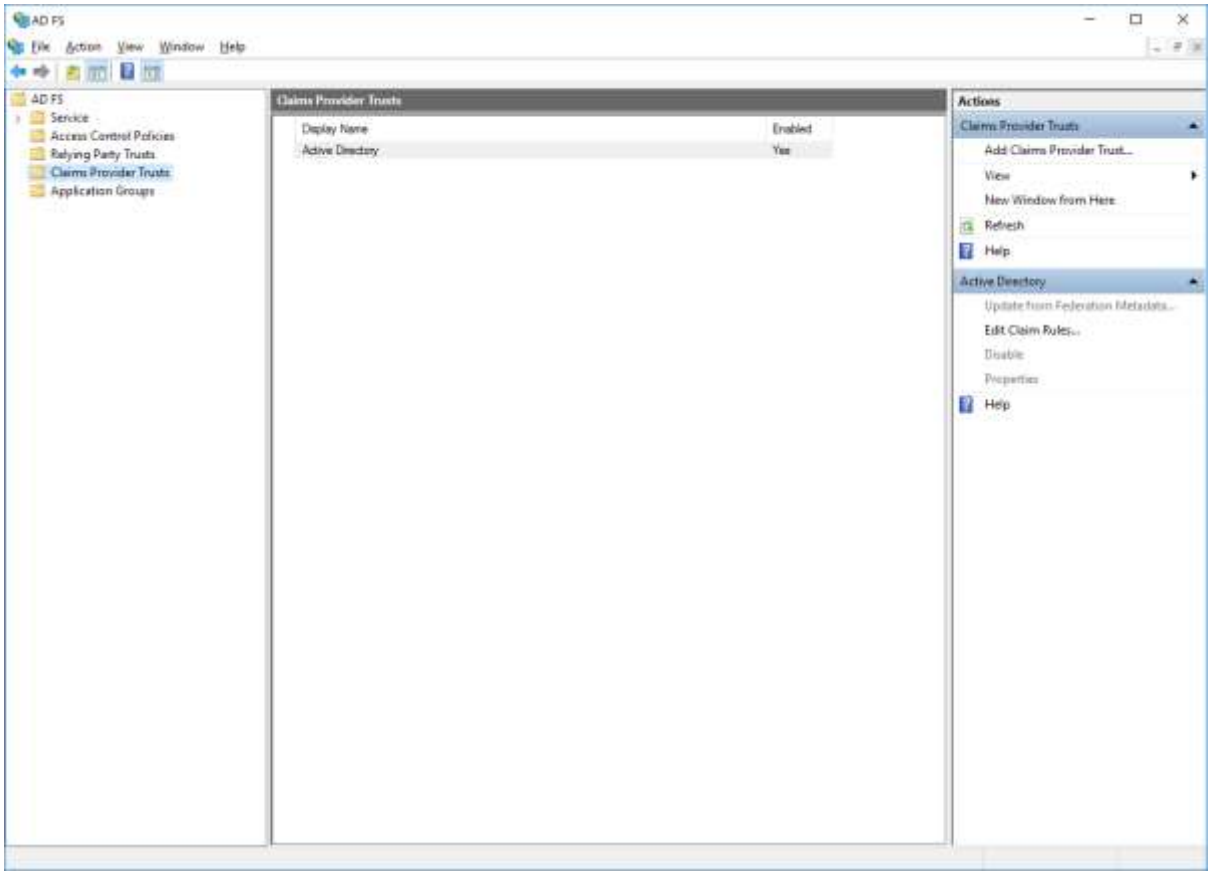
For more information, refer to:

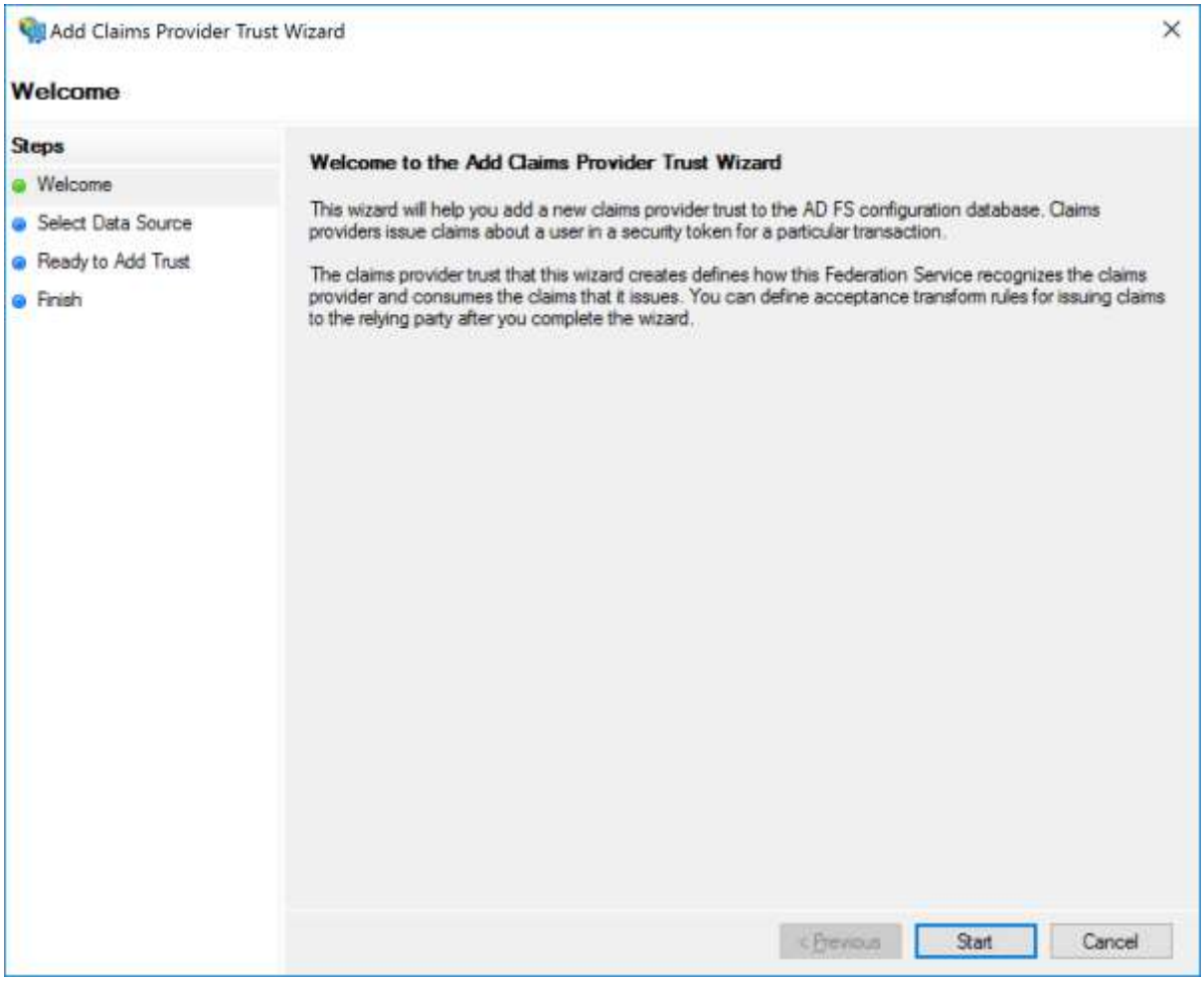
https://blogs.technet.microsoft.com/rmilne/2017/06/20/how-to-enable-idpinitiatedsignon-page-in-ad-fs-2016/

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

Adding a Claims Provider

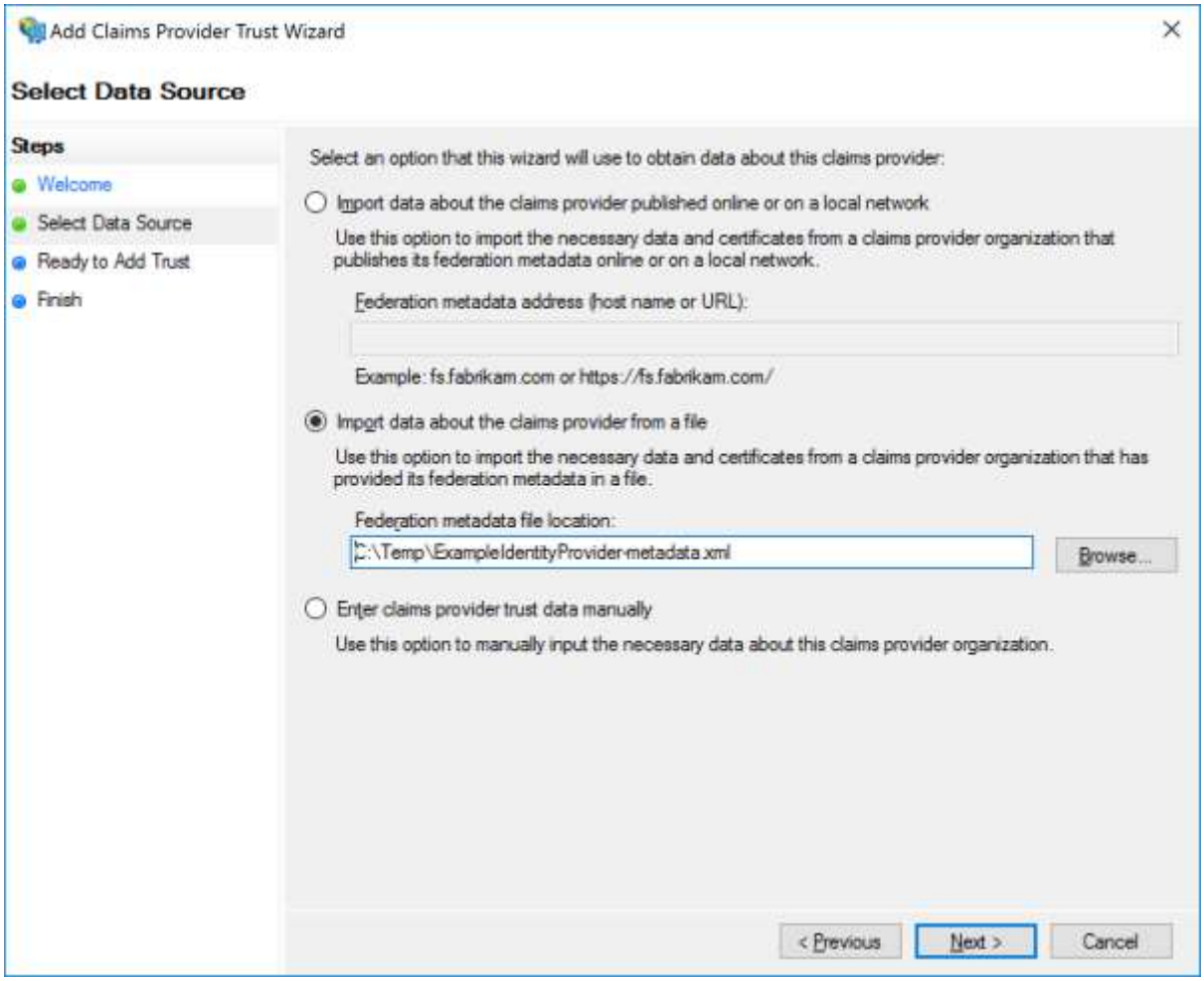
Open the ADFS console and add a claims provider trust.


AD FS
File Action View Window Help
AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Claims Provider Trusts
Display Name
Enabled
Active Directory
Yes
Actions
Claims Provider Trusts
Add Claims Provider Trust...
View
New Window from Here
Refresh
Help
Active Directory
Update from Federation Metadata...
Edit Claim Rules...
Disable
Properties
Help

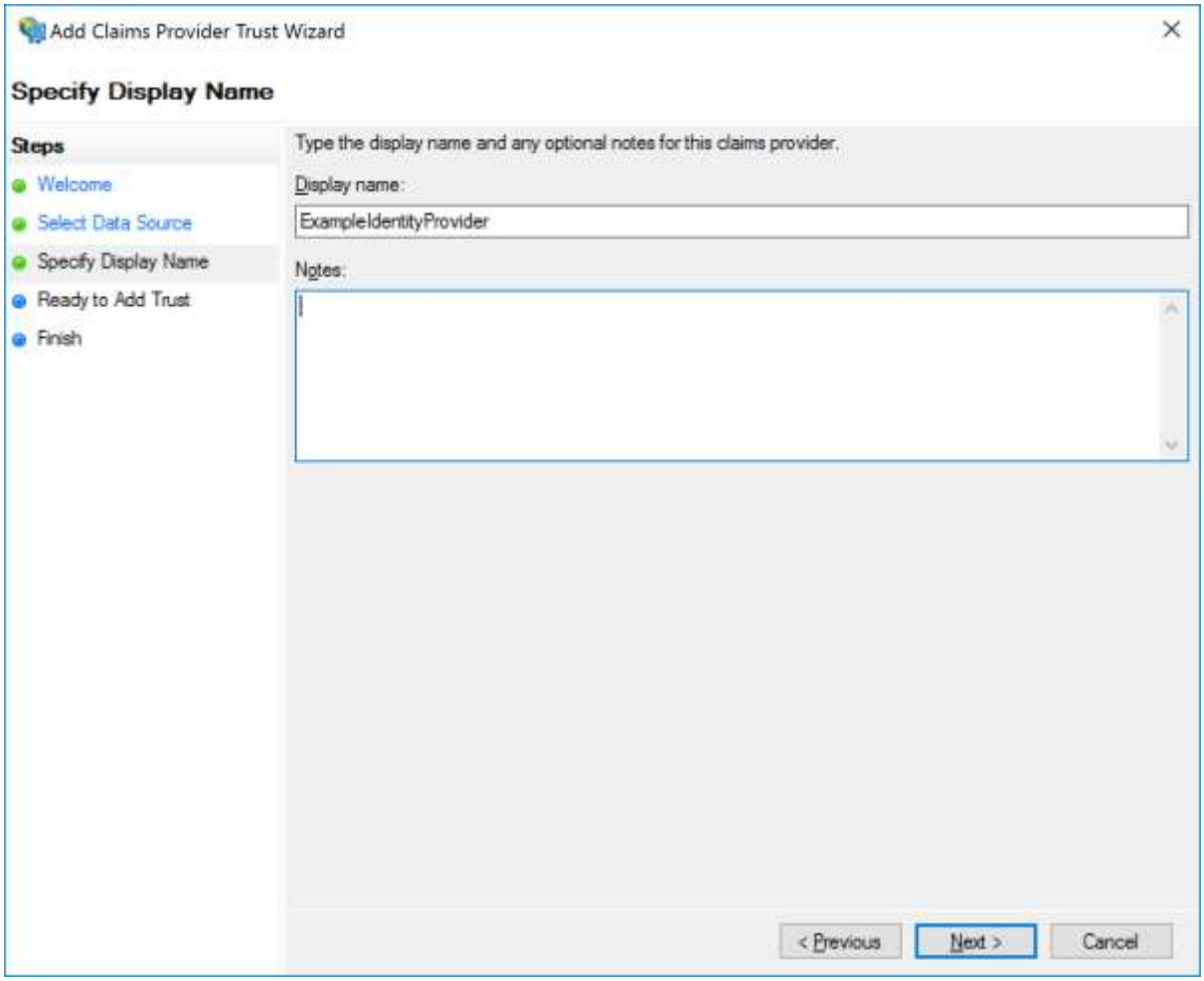


The claims provider may be configured through SAML metadata or manually.

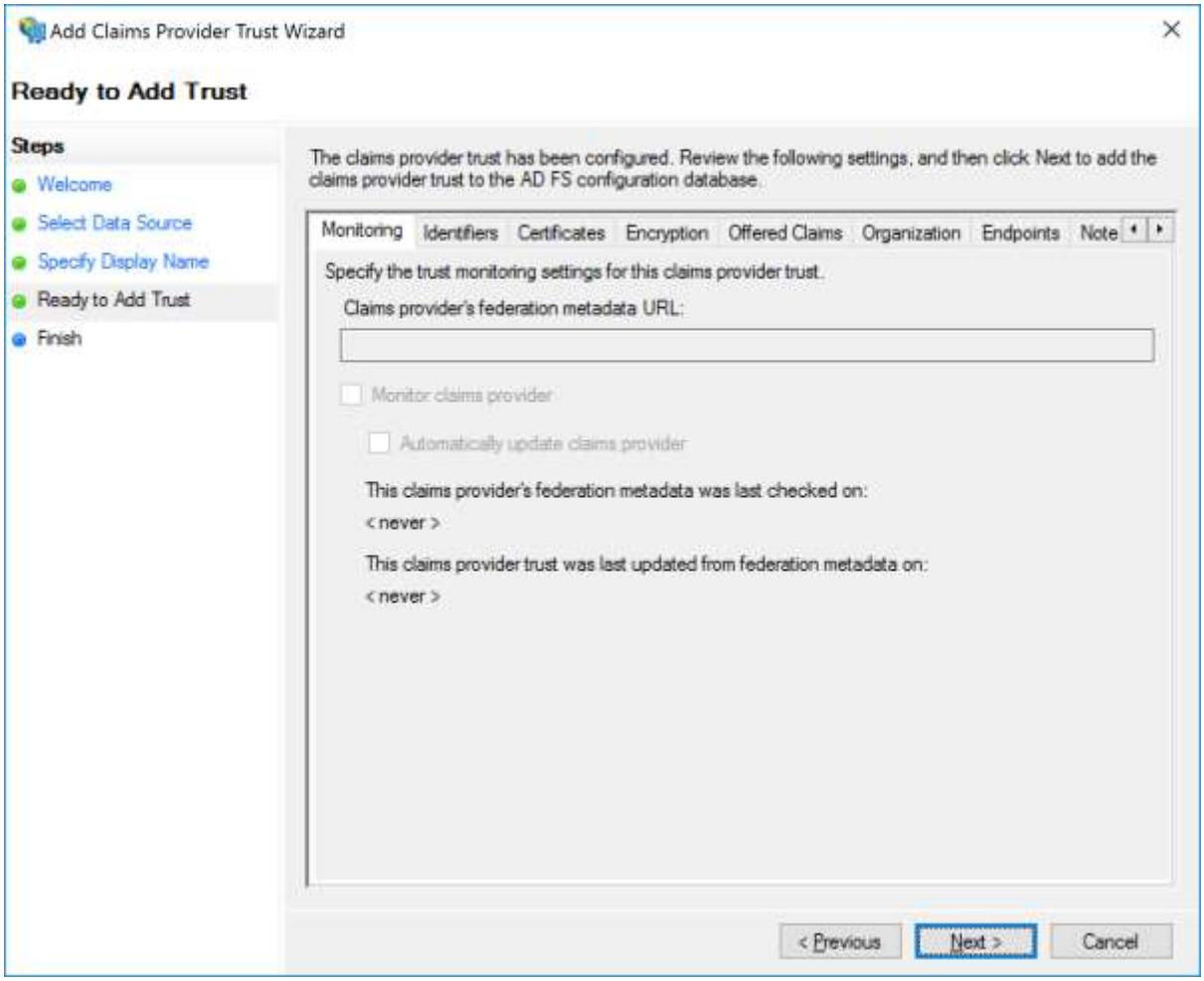
The included SAML metadata for the ExampleIdentityProvider is used.



Provide a name purely for display purpose.



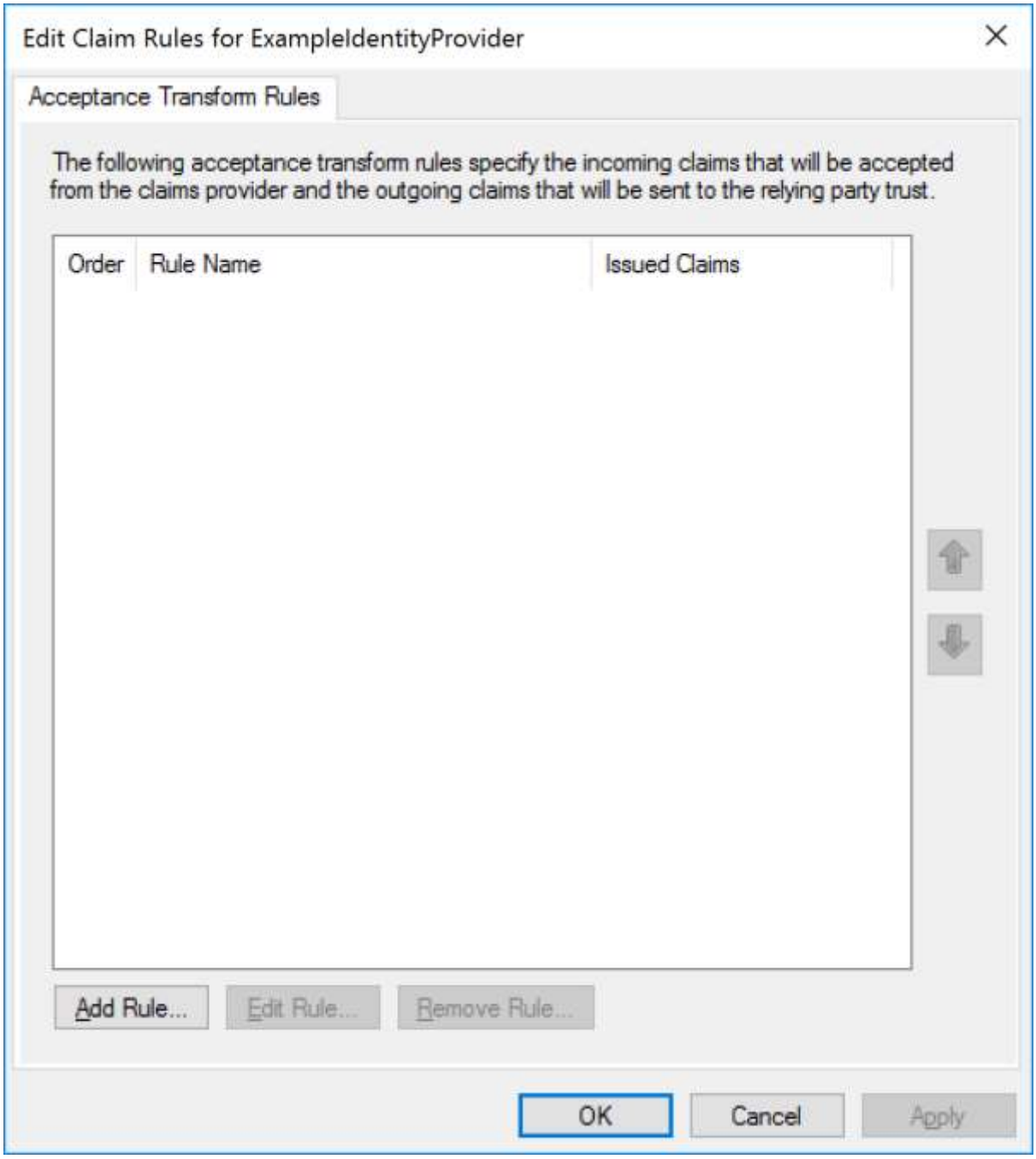
Review the configuration. This can be updated later if required.



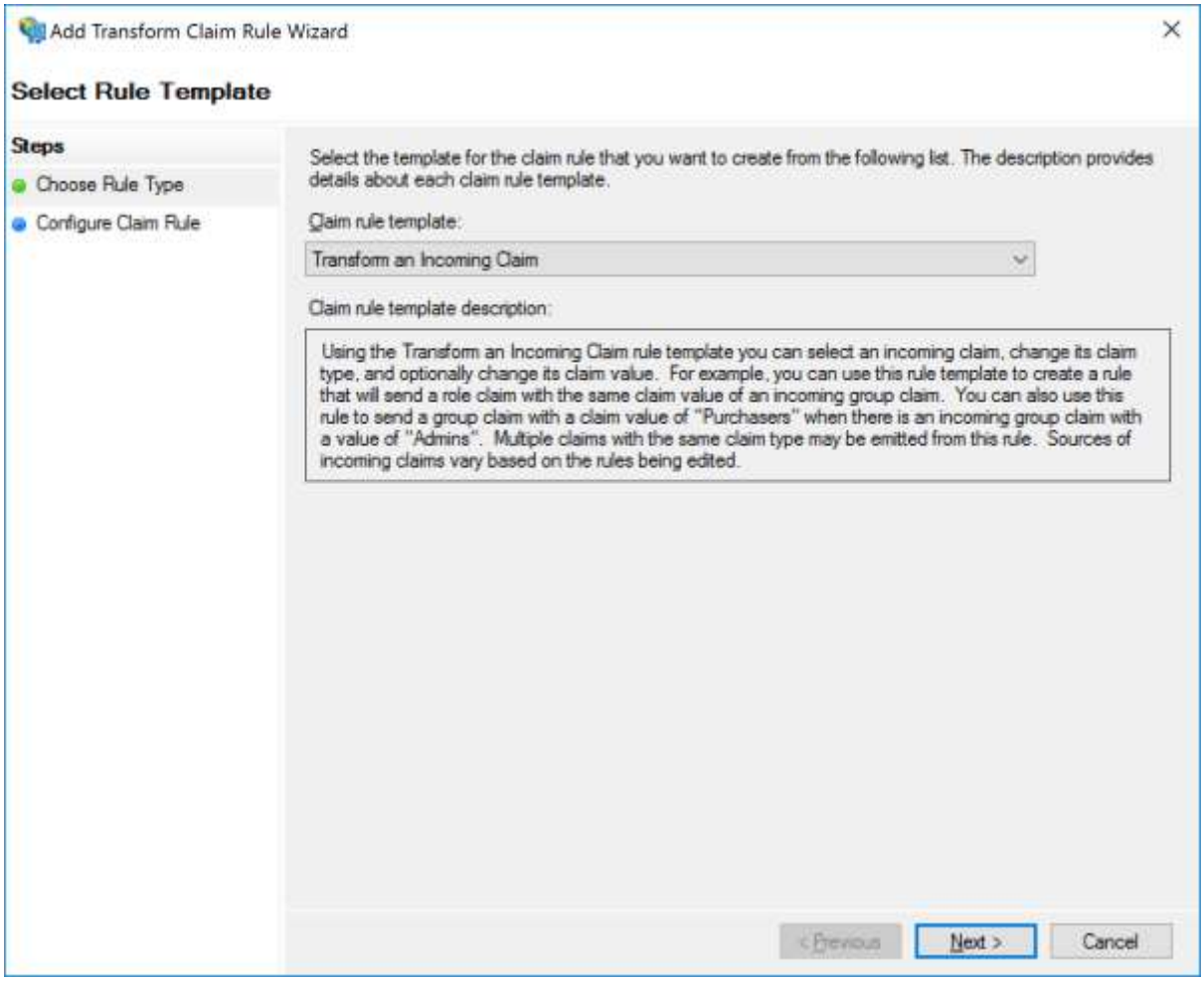
Adding a Claims Rule

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

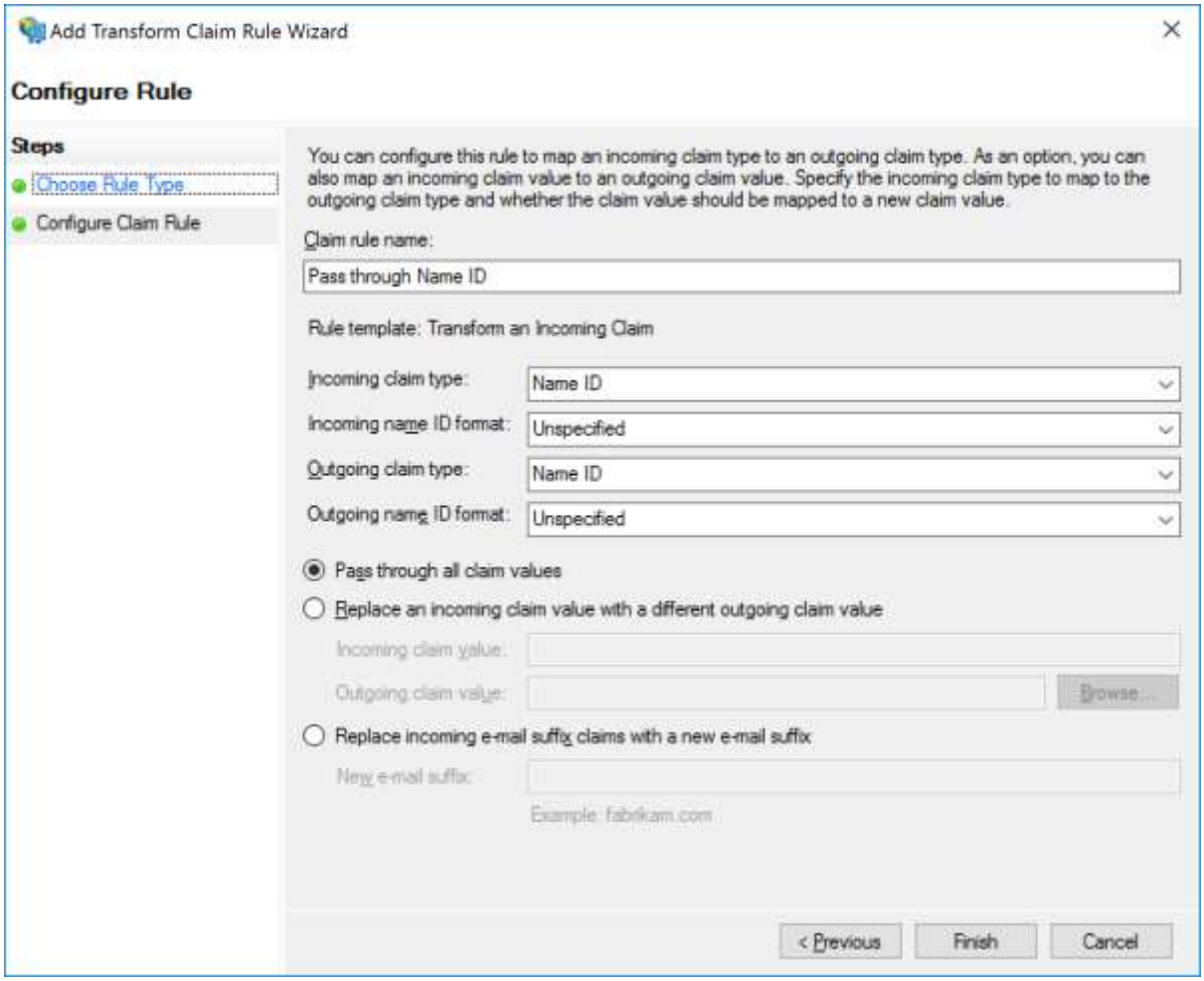
Add rules to pass through incoming claims.



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

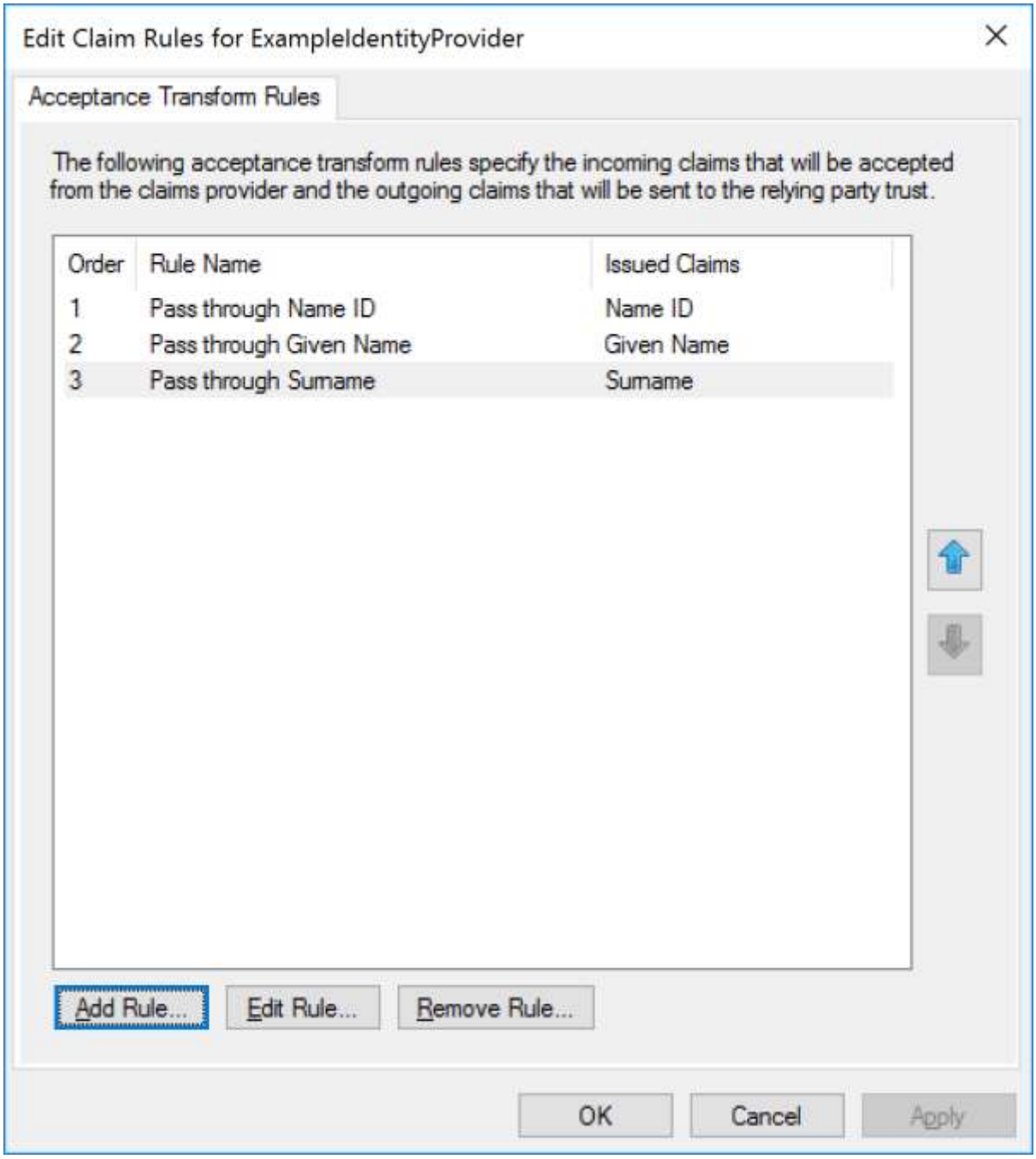


Pass through the name identifier.



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

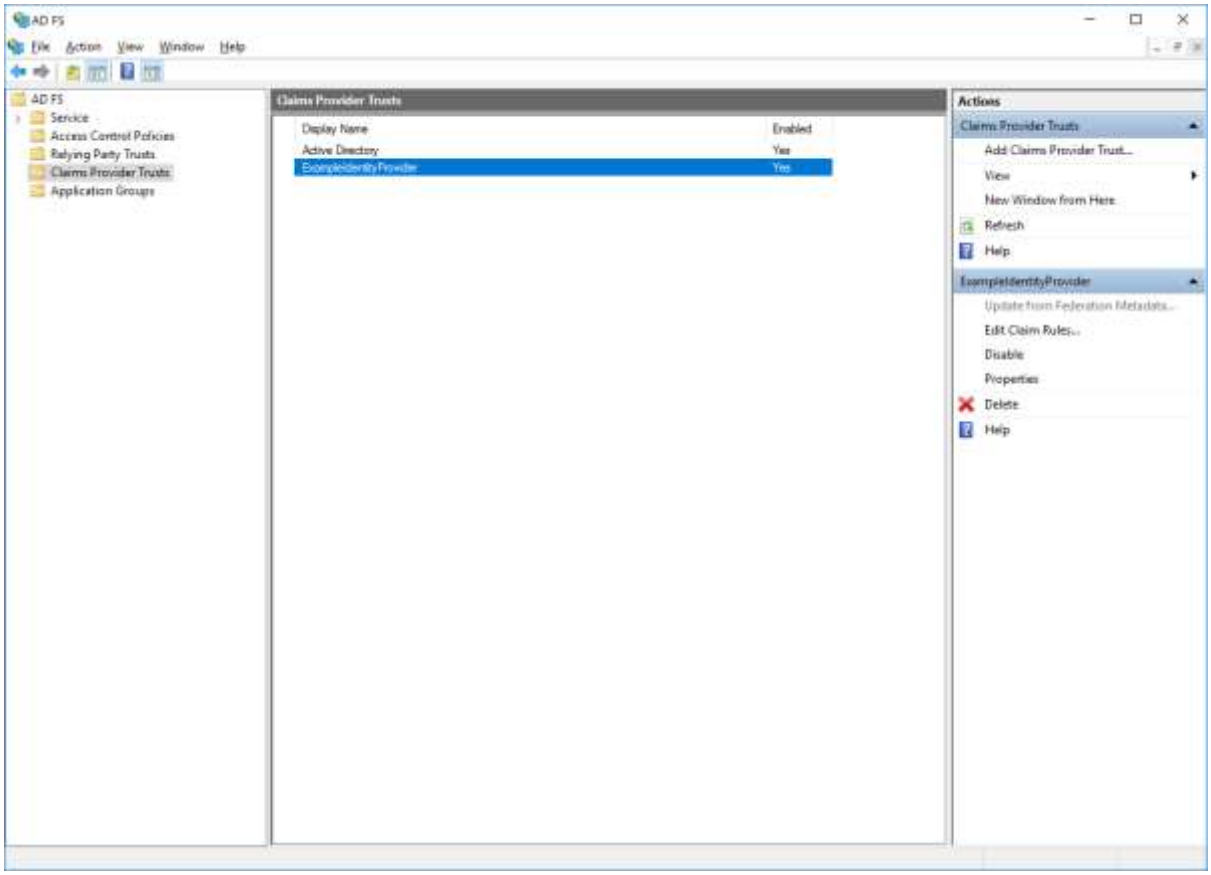
Add similar rules for the given name and surname.



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

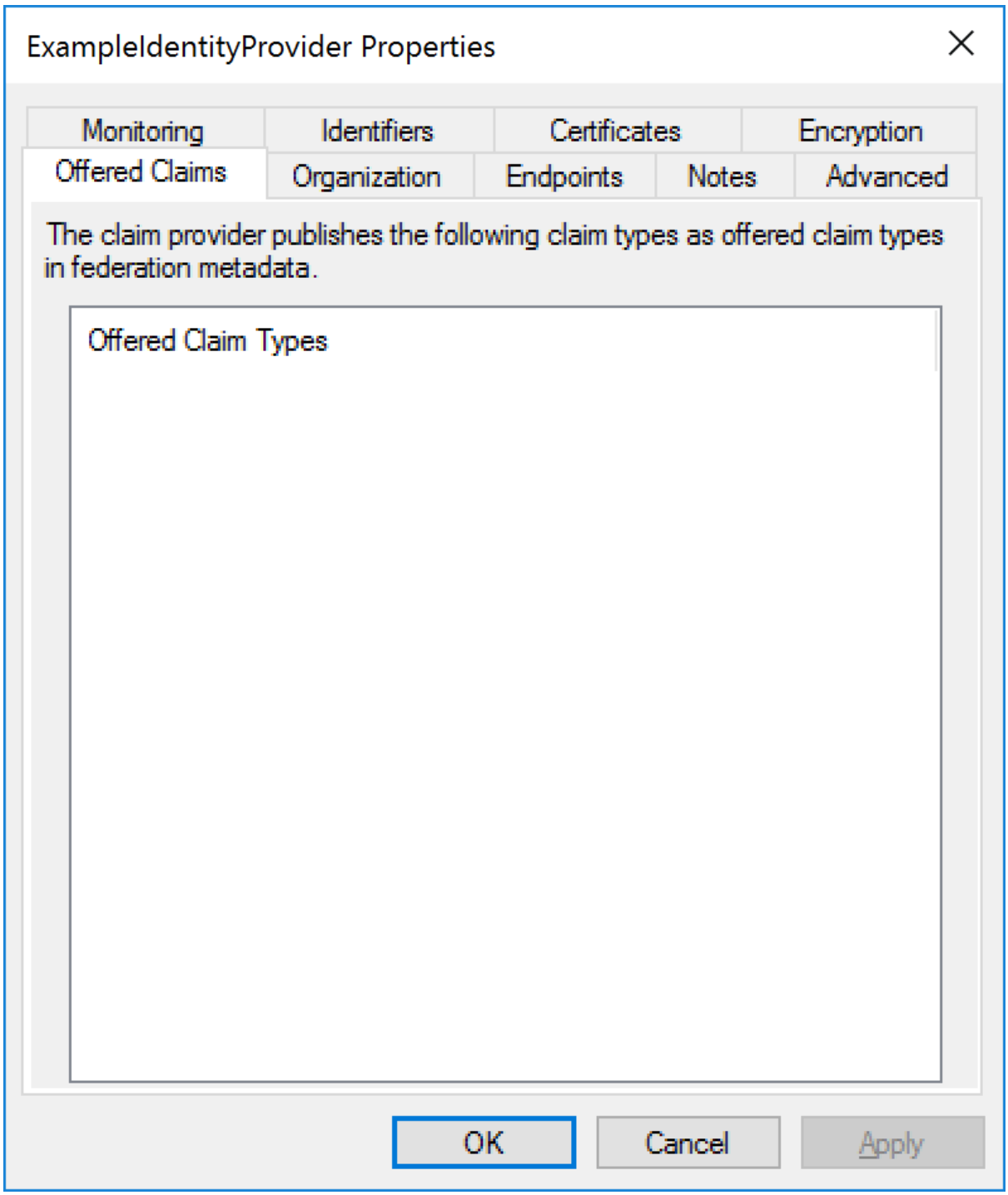
Reviewing Claims Provider Configuration

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

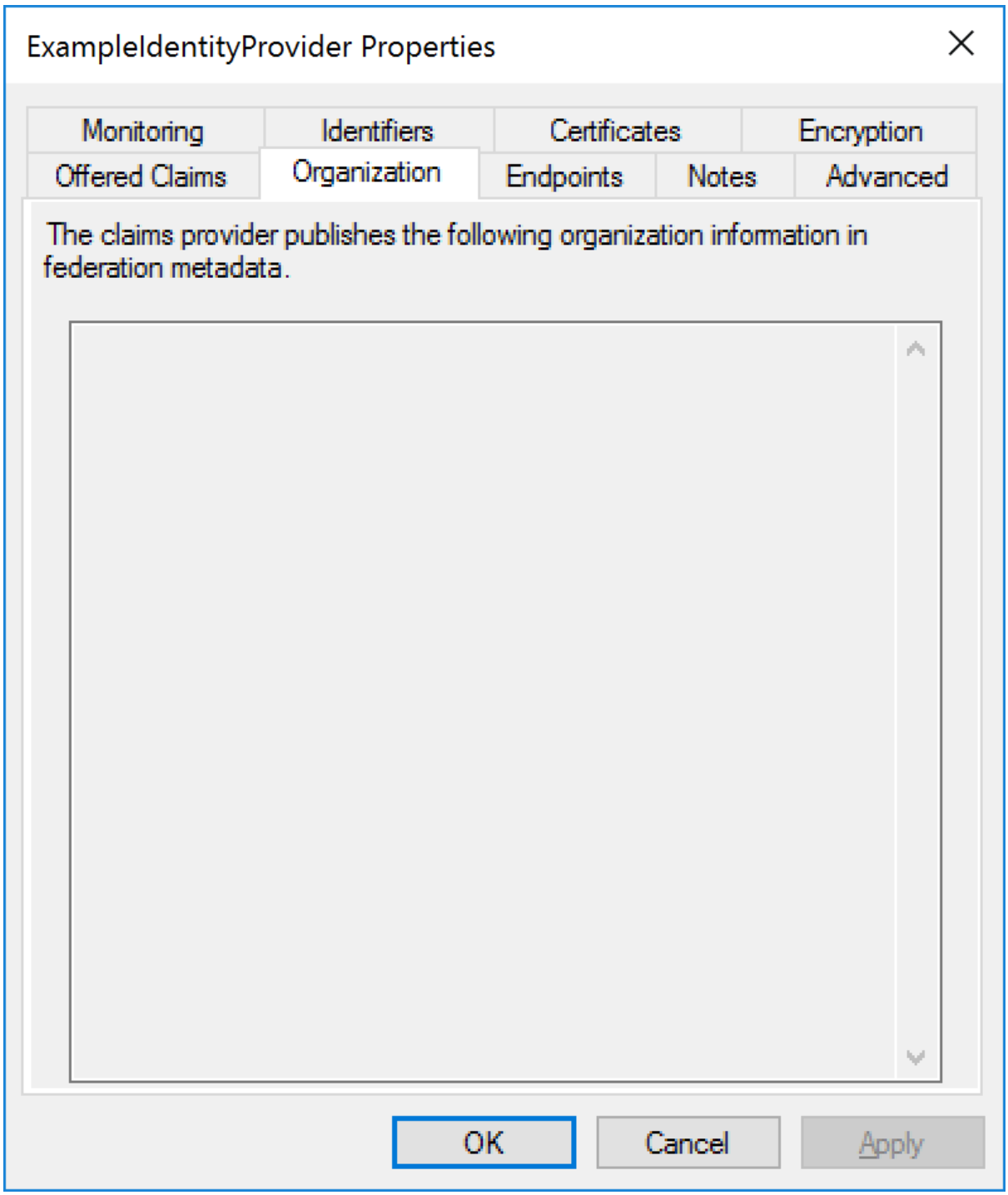


The offered claims are specified through the identity provider's SAML metadata.

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



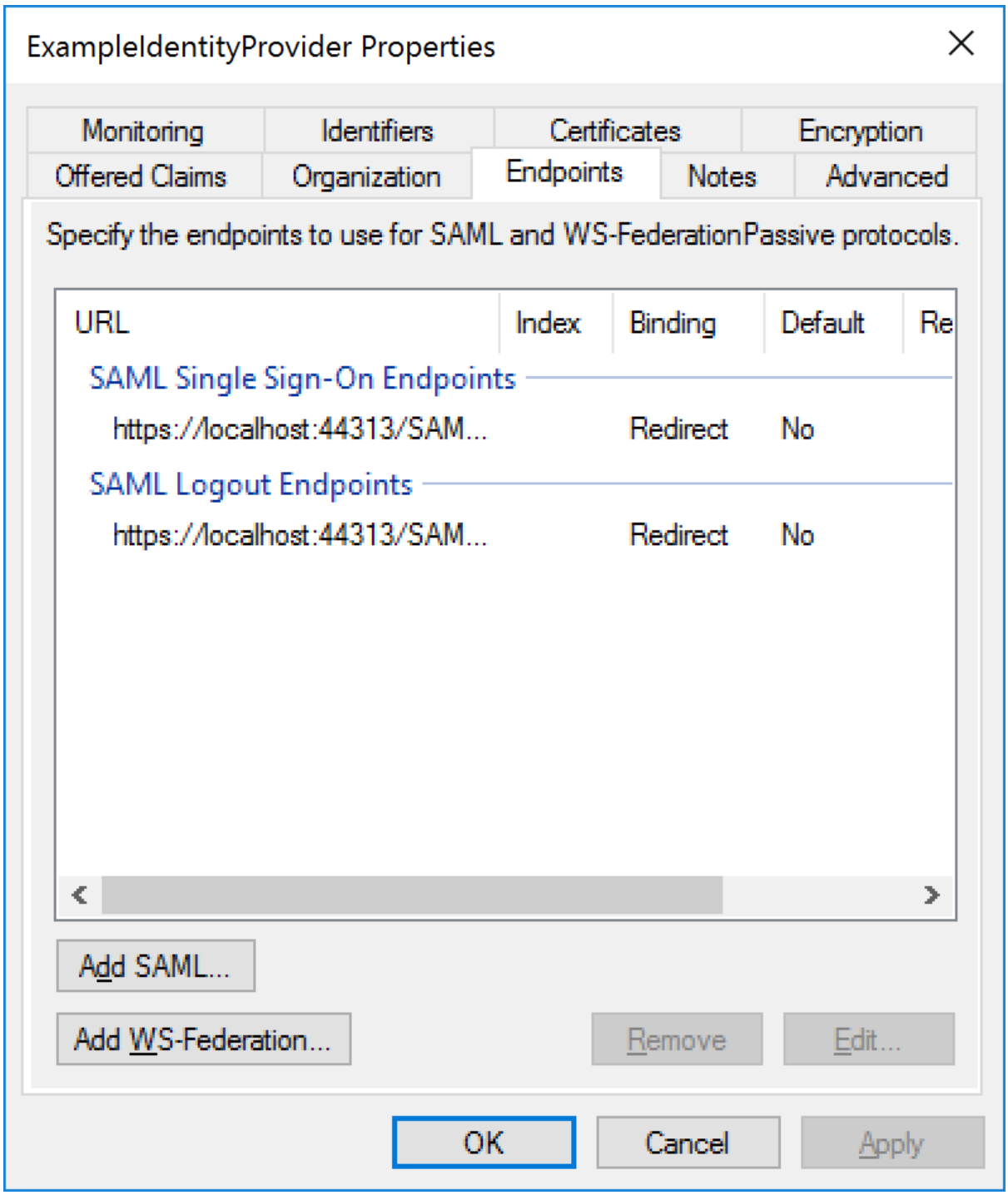
The organization information from the imported SAML metadata, if any, is displayed.



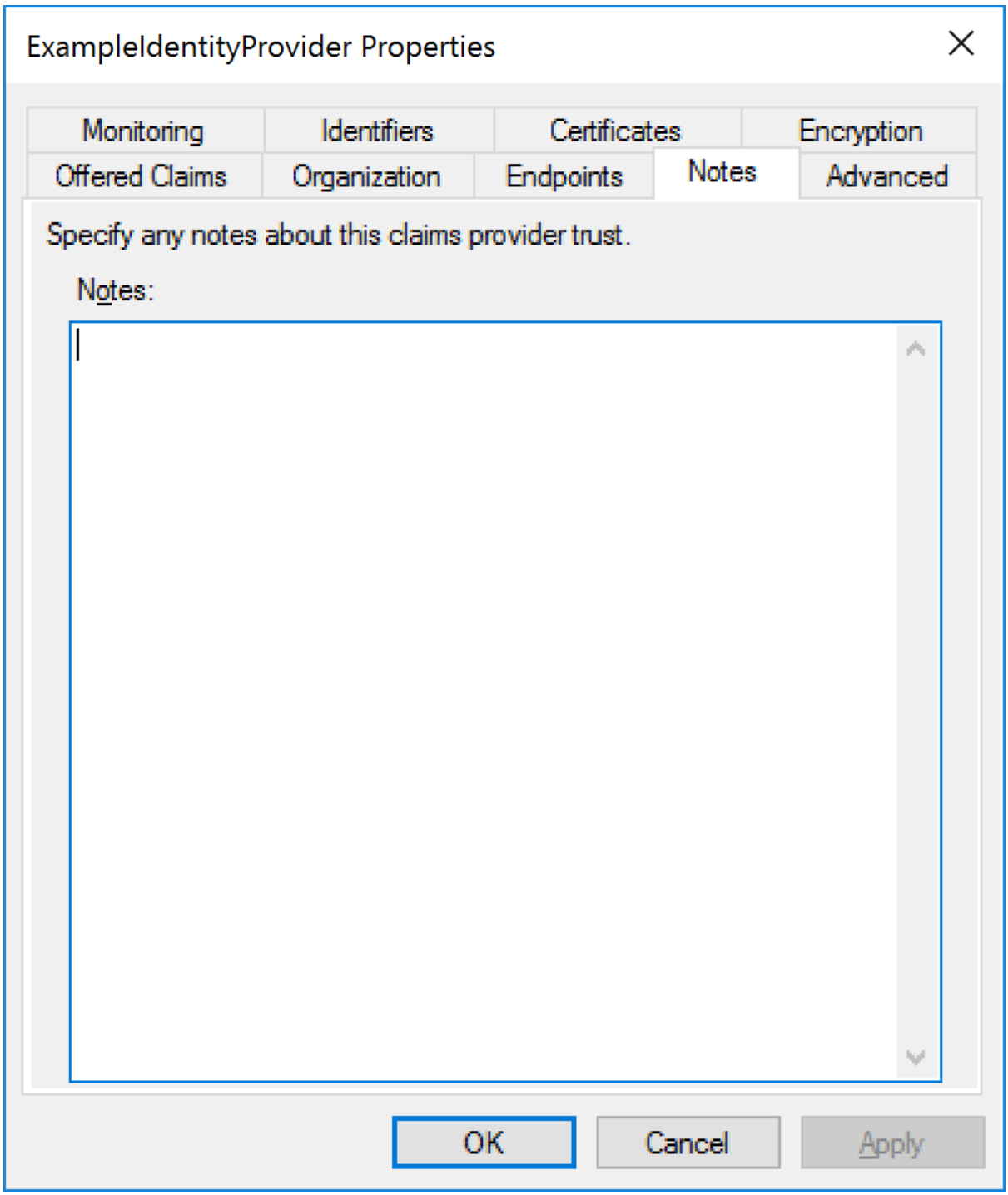
The endpoints are the URLs and SAML bindings used when communicating with the identity provider.

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.

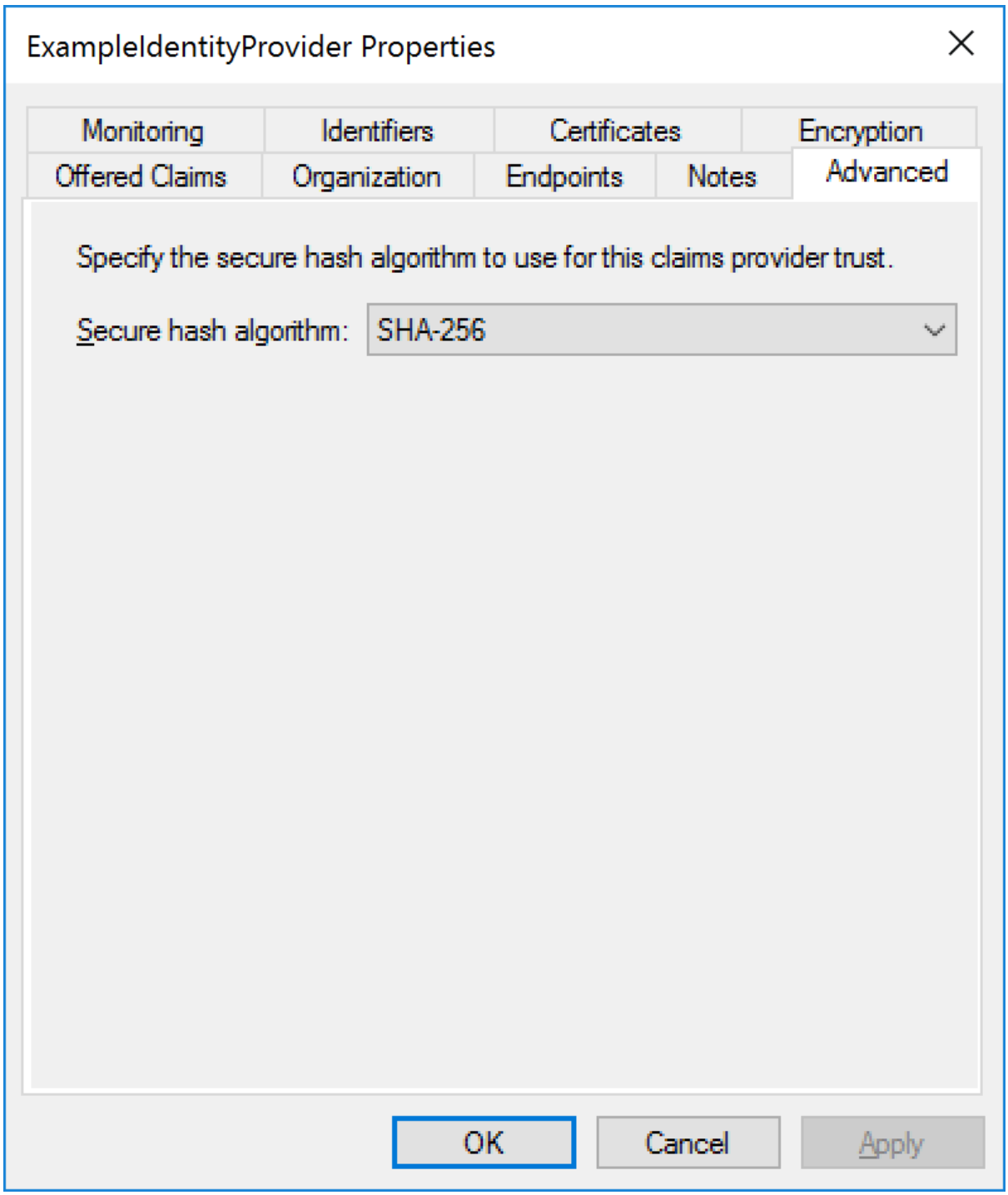


Notes are internal to ADFS and for documentation purposes only.

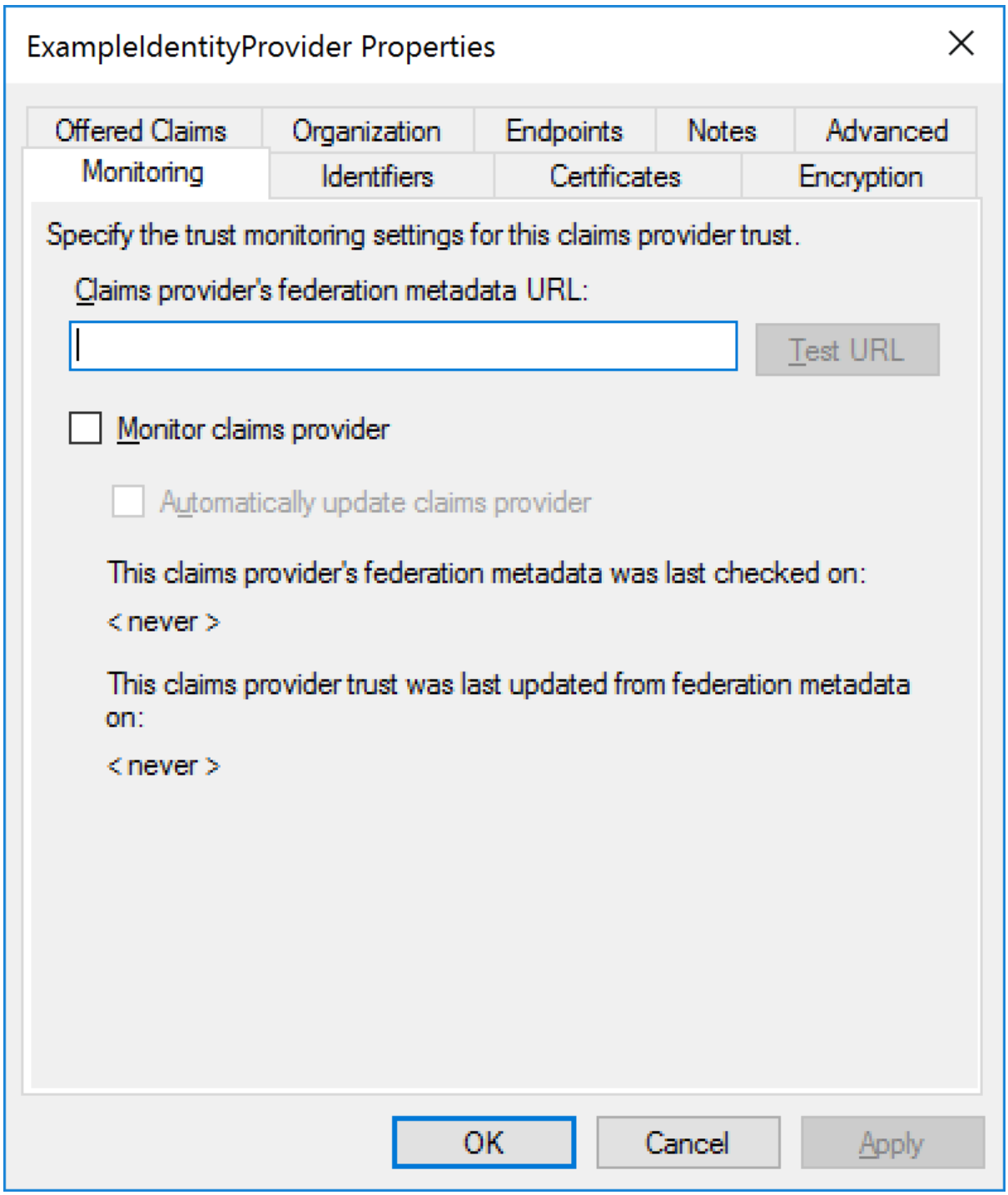


Either SHA-1 or SHA-256 may be specified as the signature algorithm.

SHA-256 is recommened.

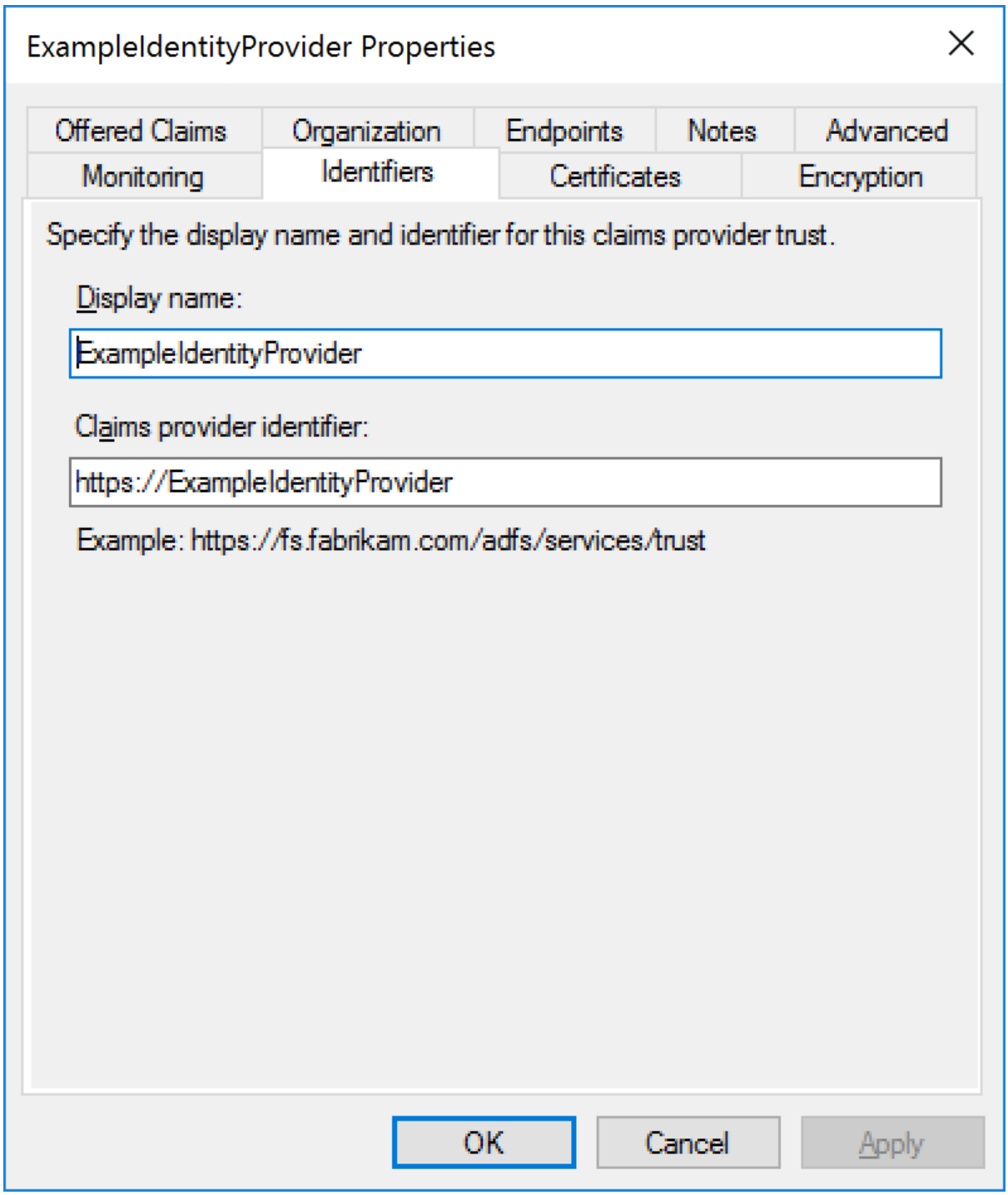


ADFS supports monitoring a URL for SAML metadata updates.



Claims provider identifiers correspond to SAML metadata entity IDs.

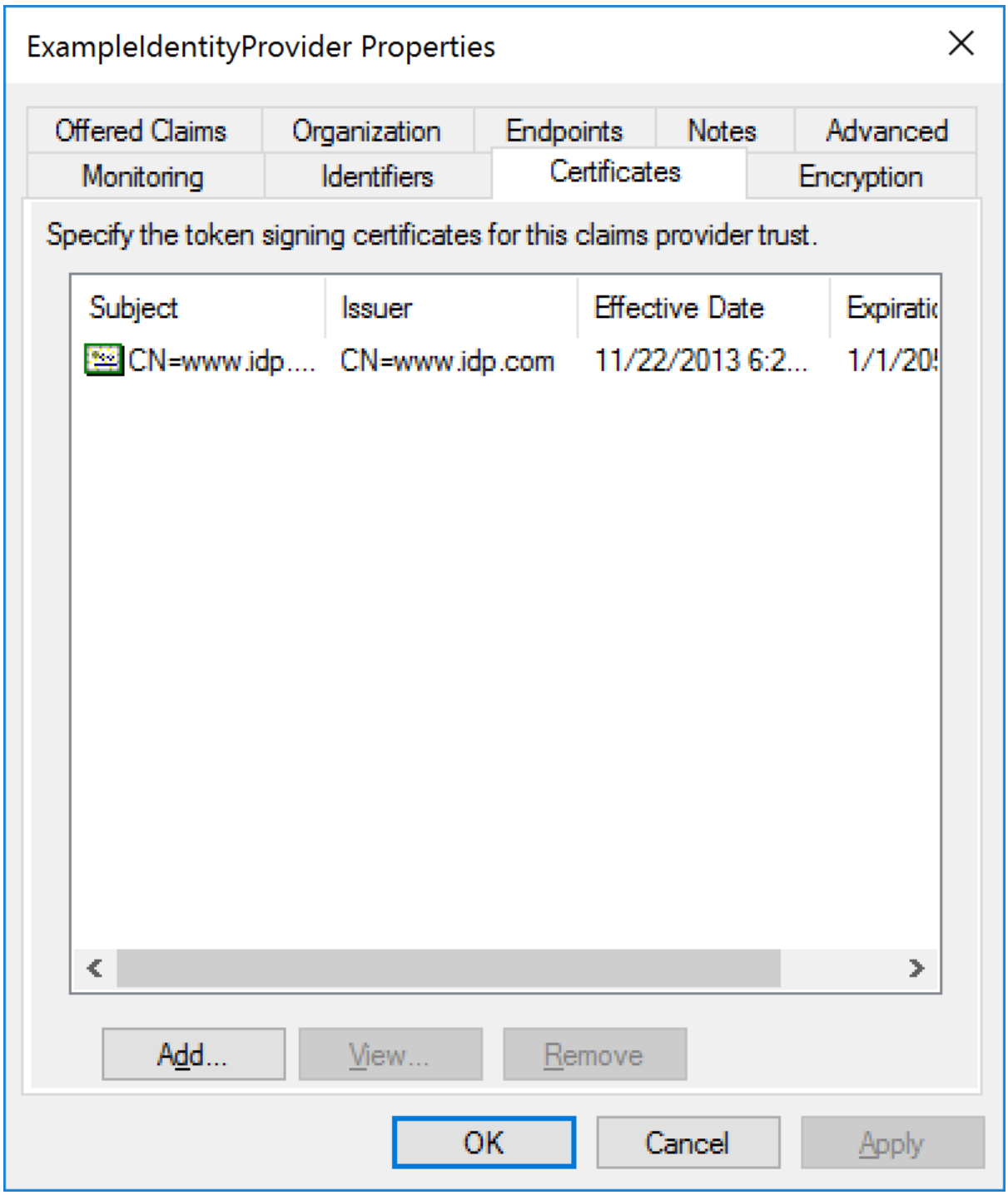
The claims provider identifier must match exactly with the identity provider's configured name.



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

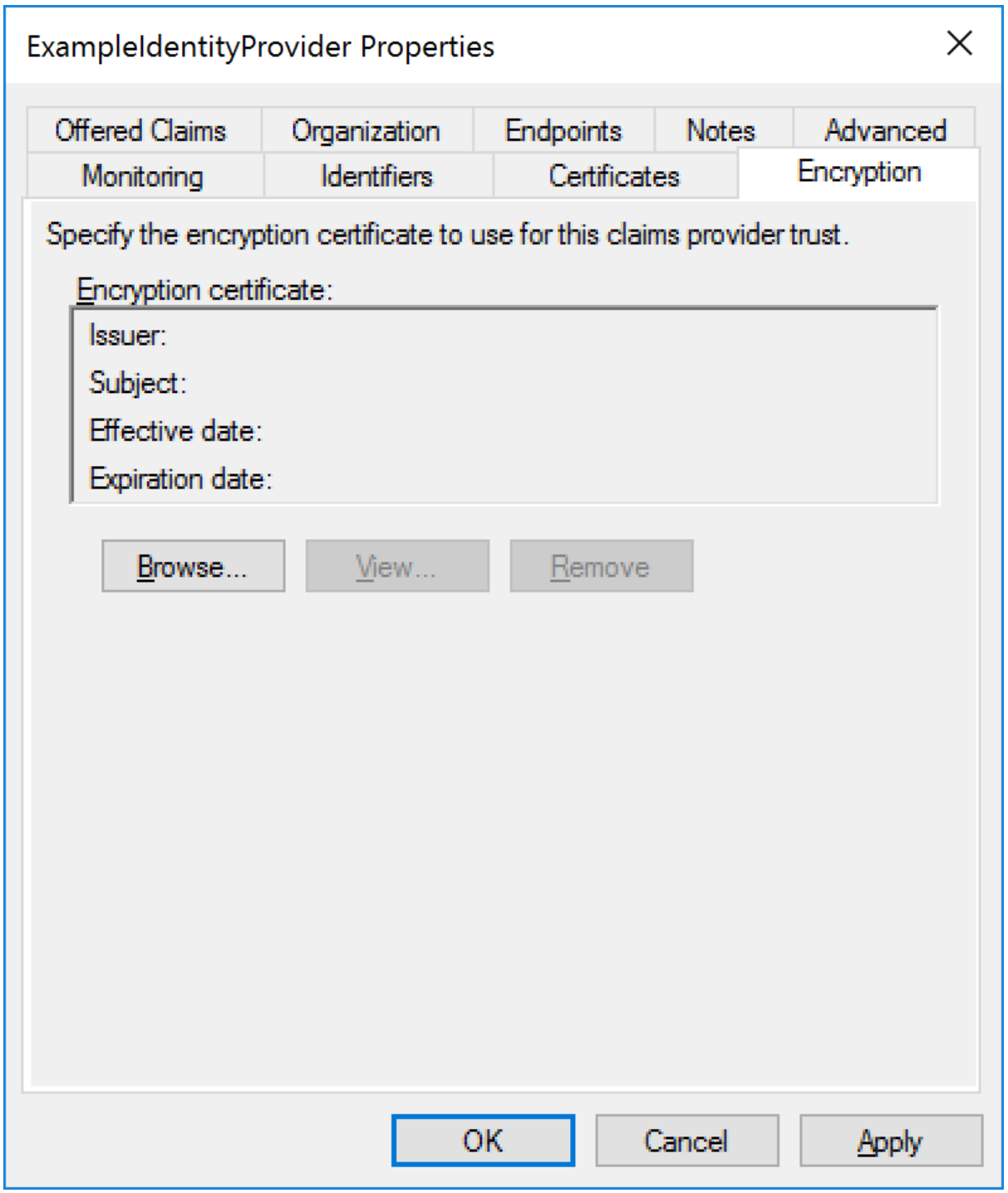
If specified, it's the identity provider's signature certificate.

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://adfs.componentspace.com/adfs/services/trust",
  "Description": "ADFS",
  "SignAssertion": true,
  "SignLogoutRequest": true,
  "SignLogoutResponse": true,
  "WantLogoutRequestSigned": true,
  "WantLogoutResponseSigned": true,
  "AssertionConsumerServiceUrl": "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 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://adfs.componentspace.com/adfs/services/trust",
"RelayState": "RPID=https://ExampleServiceProvider"
```

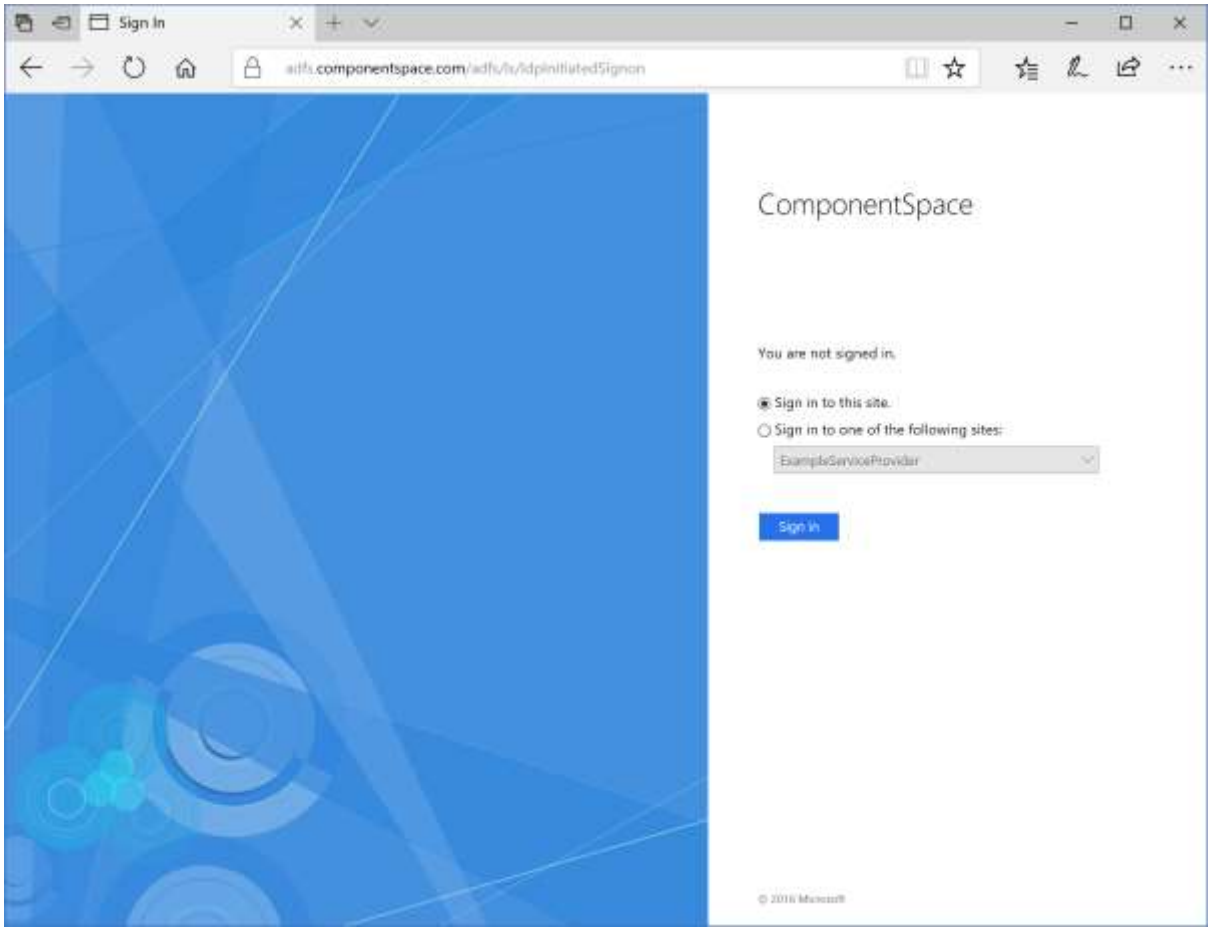
SP-Initiated SSO

Browse to:

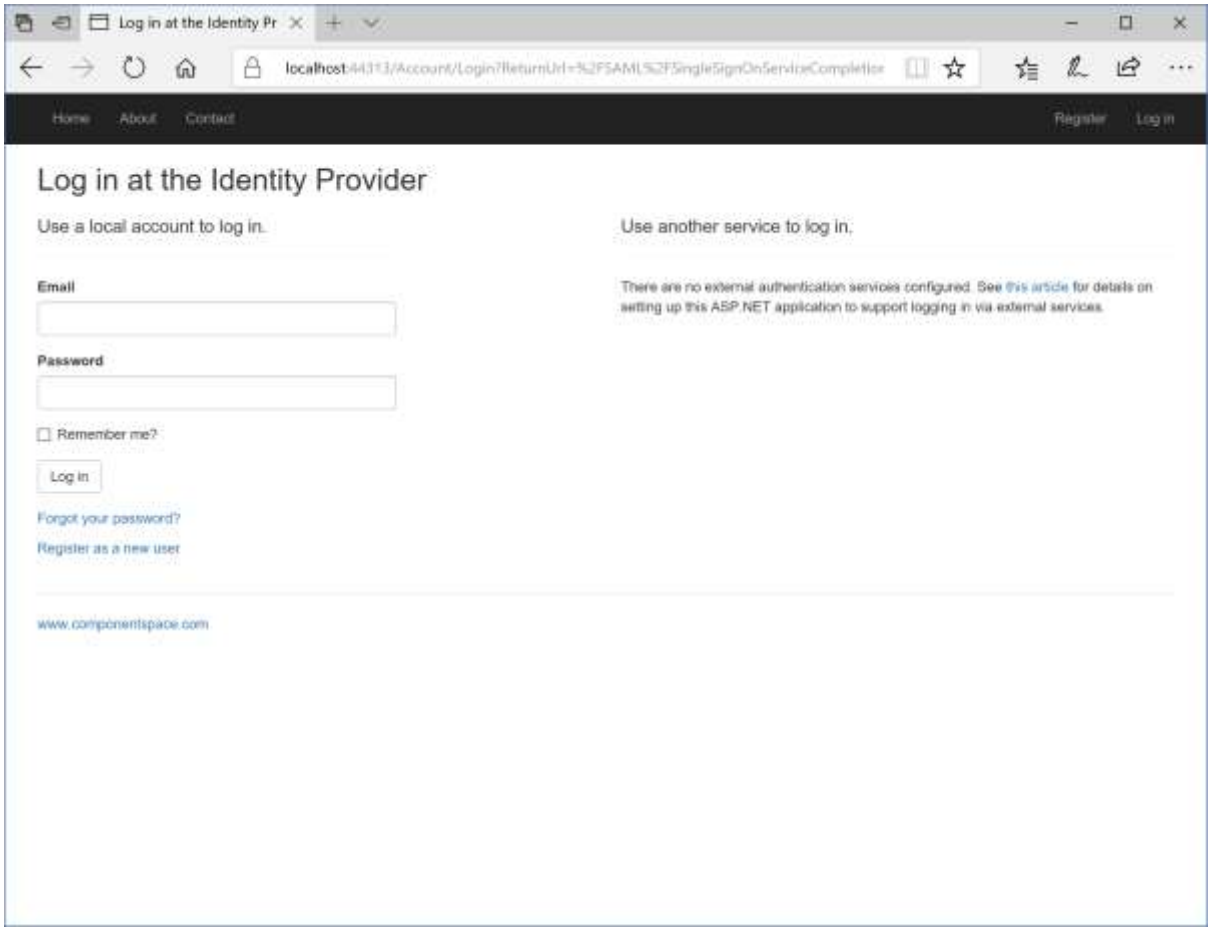
https://<server-name>/adfs/ls/IdpInitiatedSignon

For example:

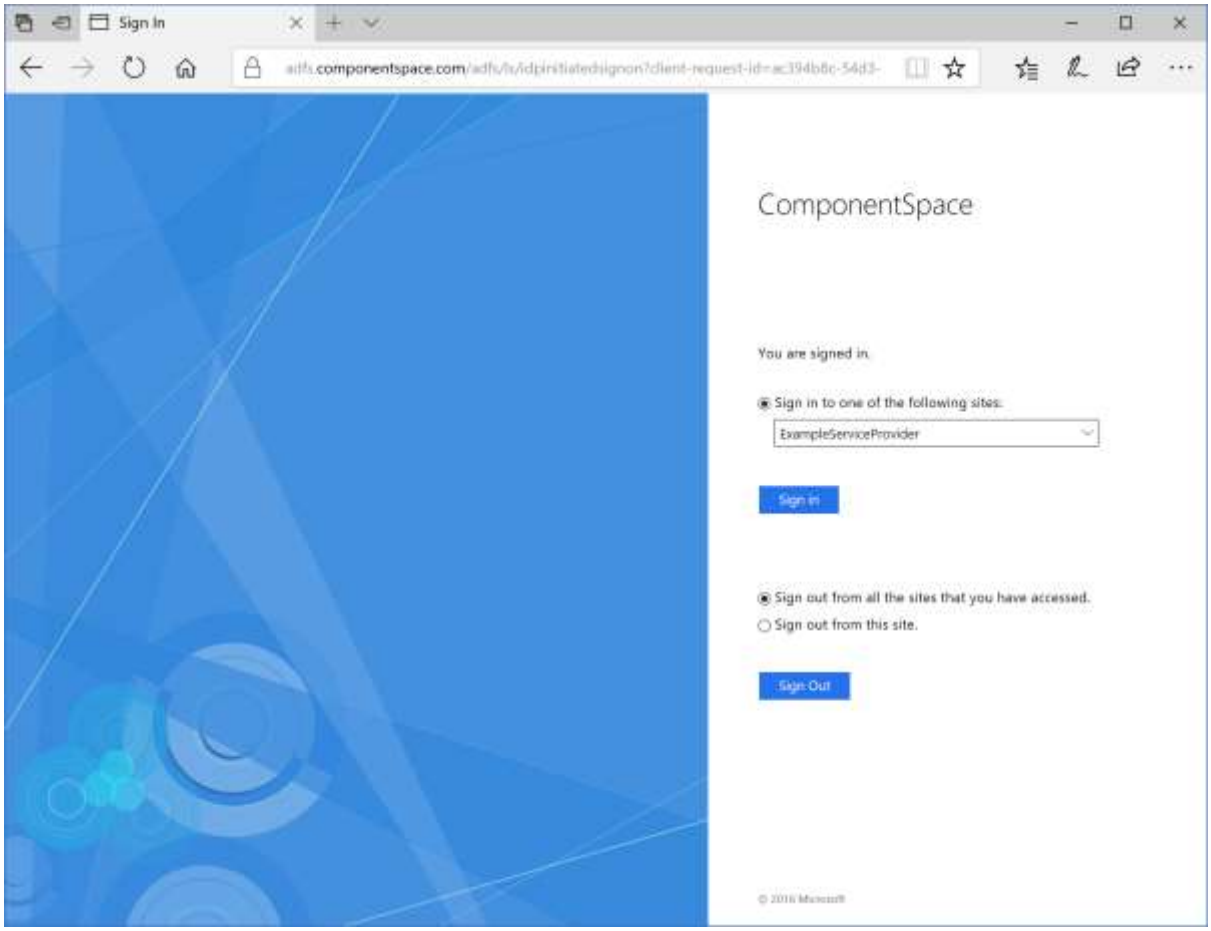
https://adfs.componentspace.com/adfs/ls/IdpInitiatedSignon



Click the button to sign into this site.

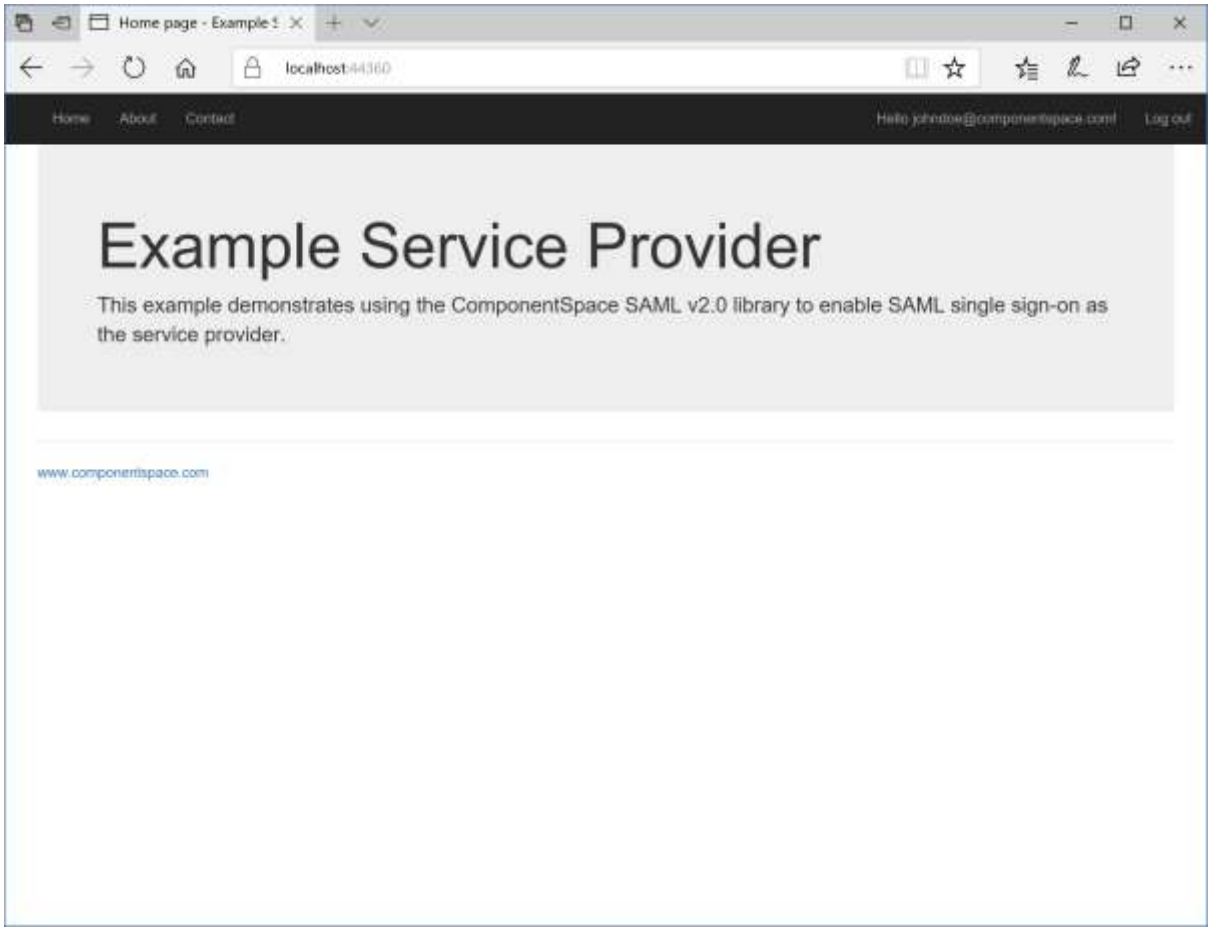


Login at the example identity provider.



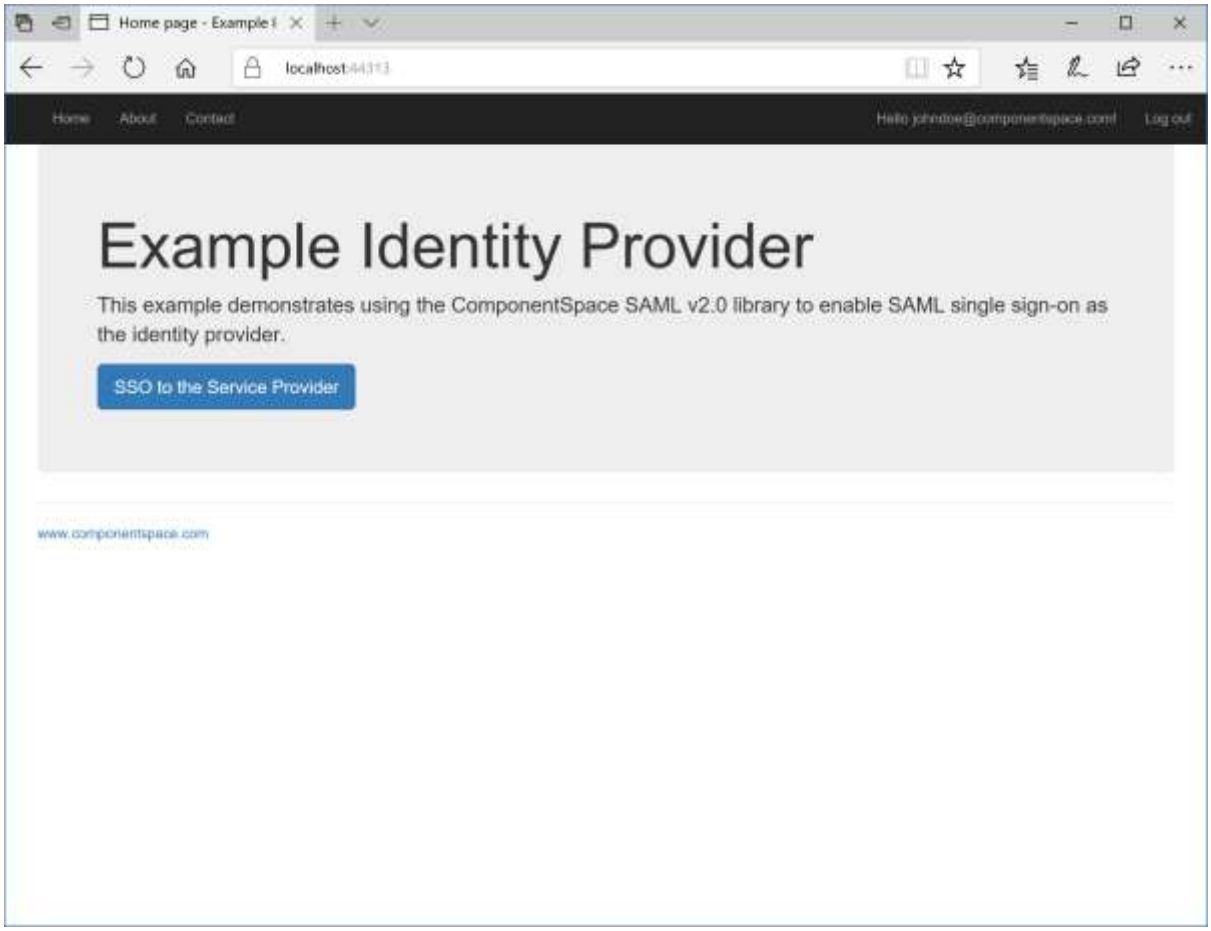
Select the relying party and click the Sign in button.

The user is automatically logged in at the service provider.

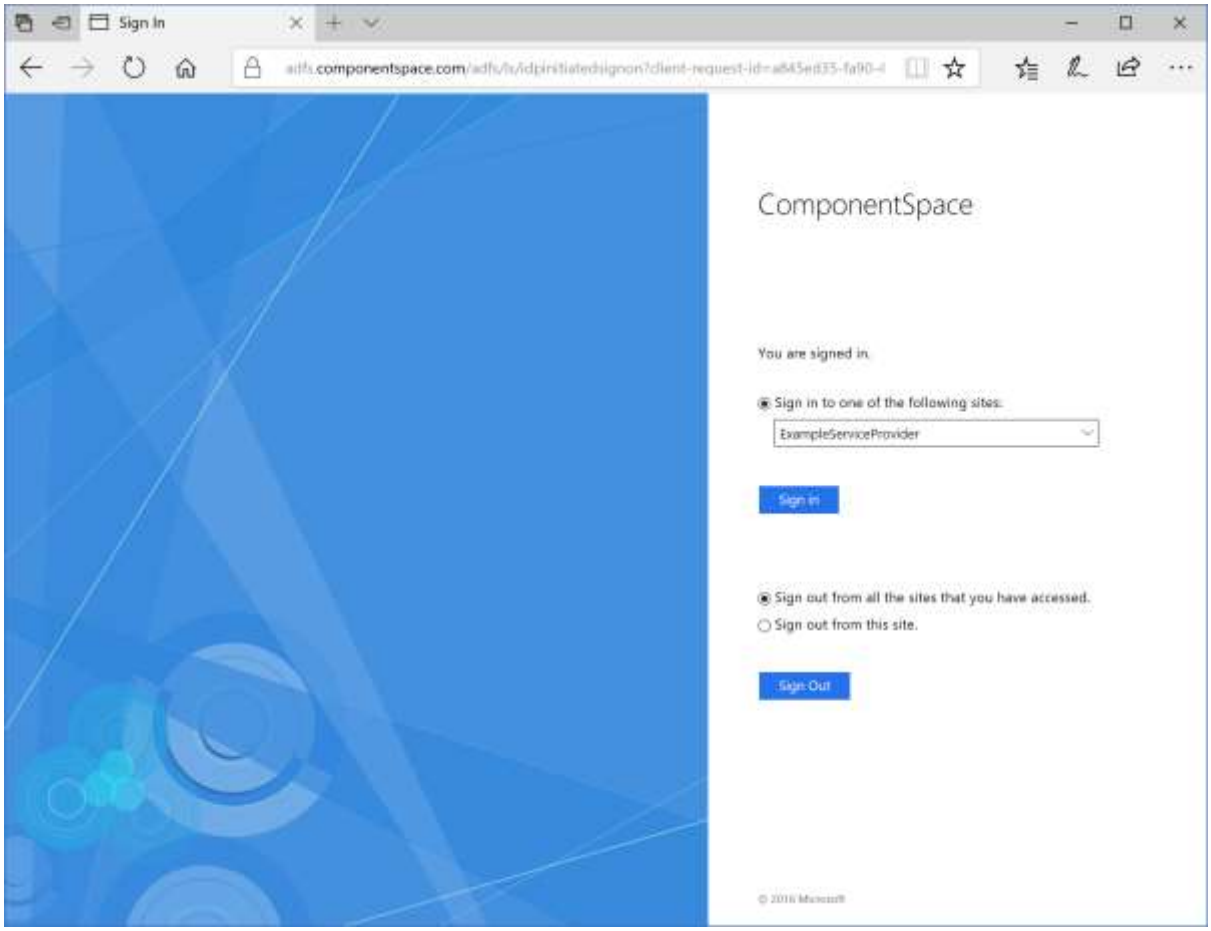


IdP-Initiated SSO

Browse to the example identity provider and login.



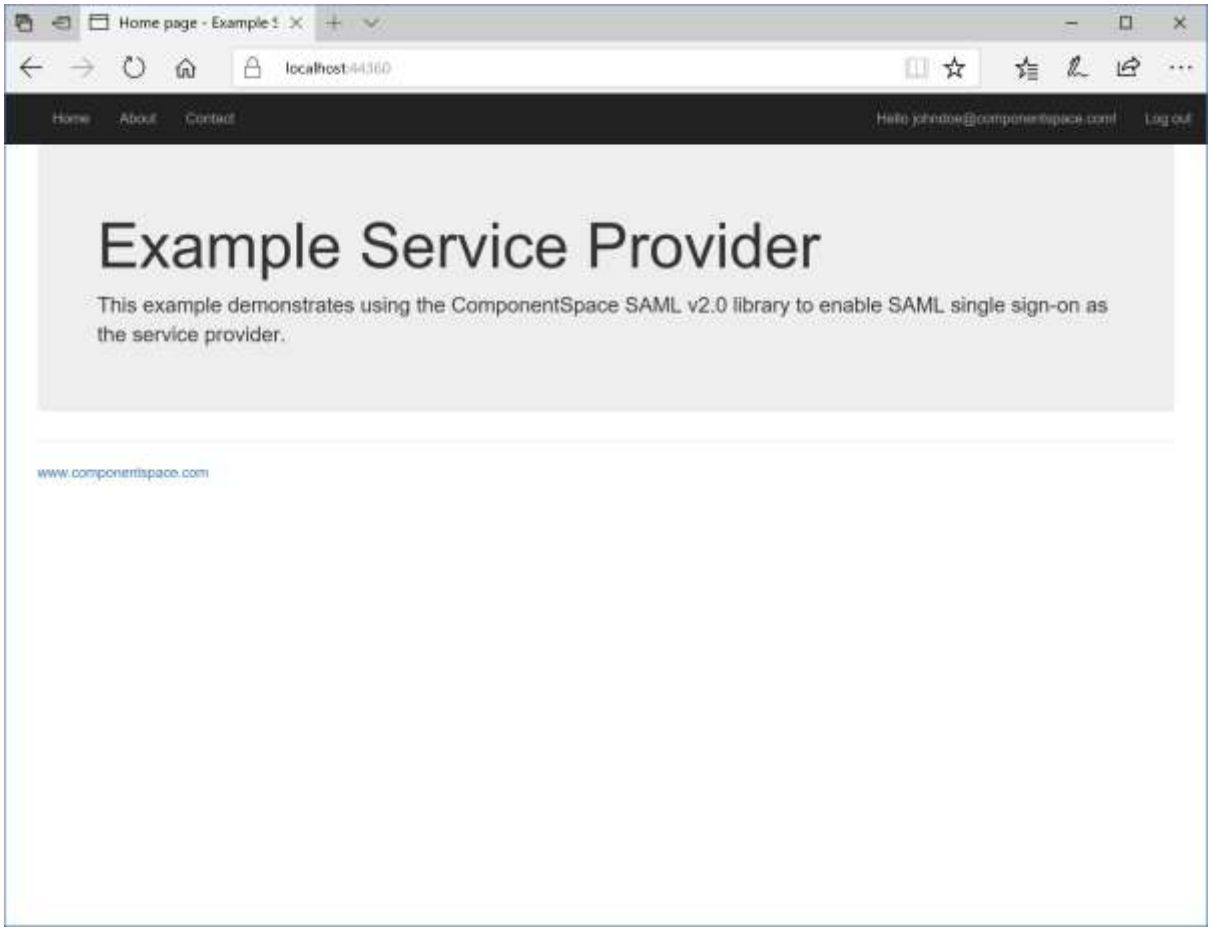
Click the button to browse to the service provider.



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.

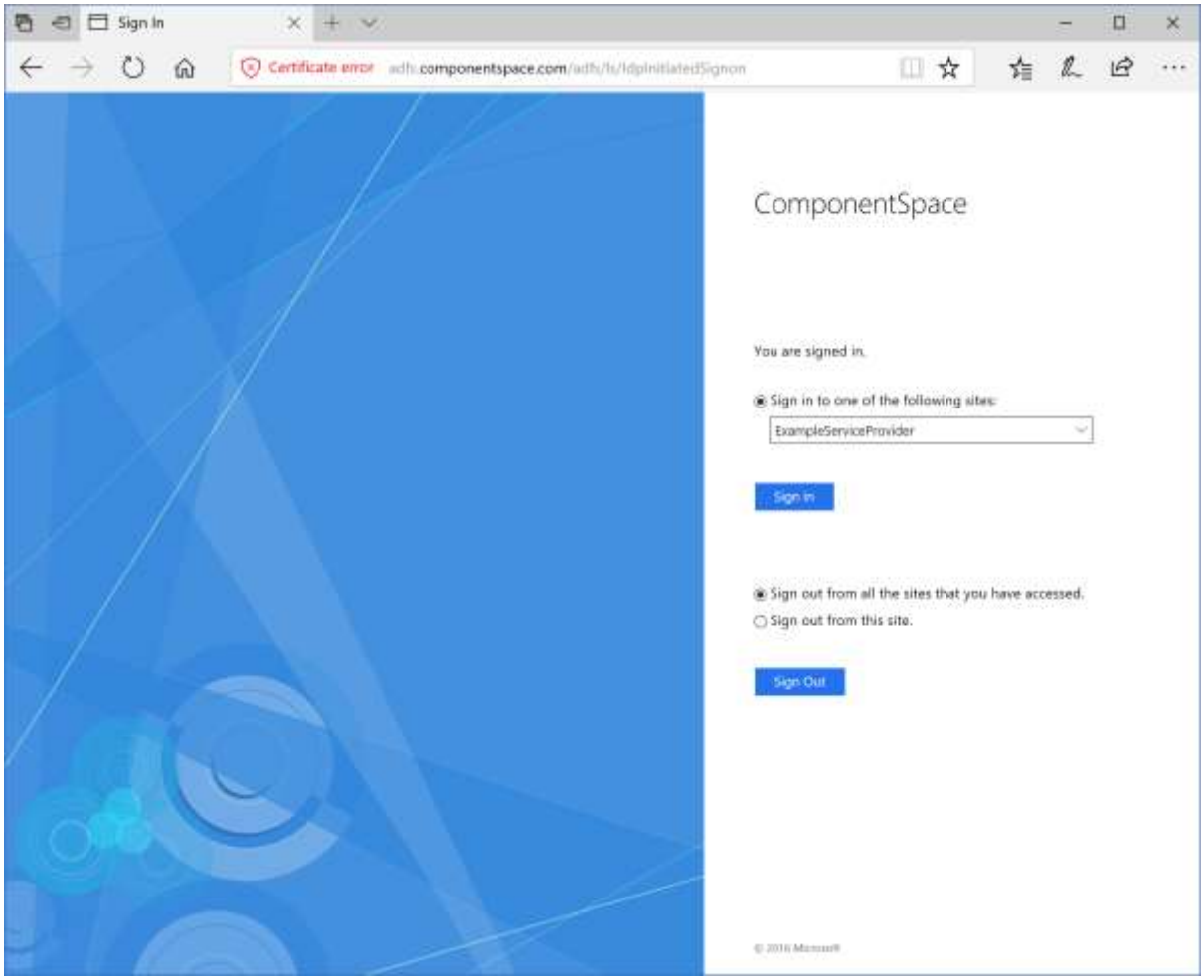
IdP-initiated SLO may be invoked from:

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.

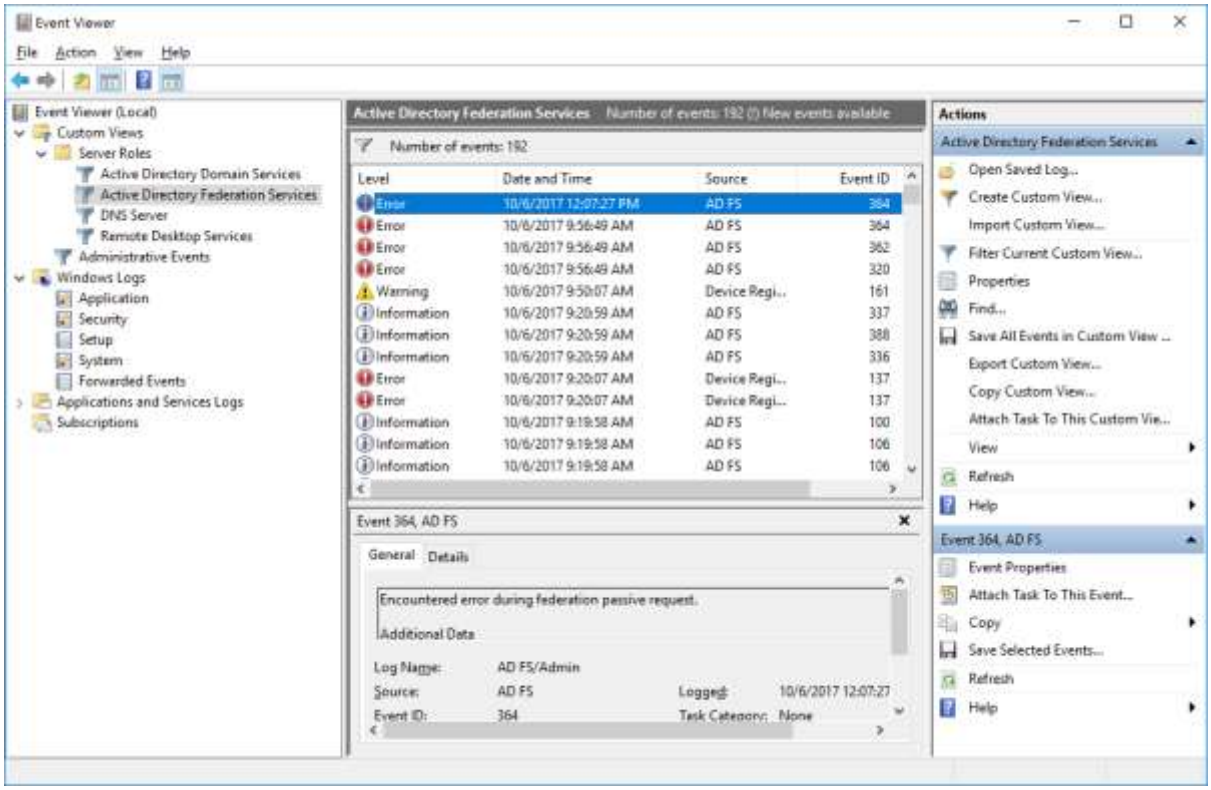
When using Microsoft Edge, no error occurs but the user is still logged into ADFS.

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