Mutare Voice™ Configuration for SAML with ADFS

Mutare Voice (SAM) can be configured to use SAML2 authentication with various identity providers. This document outlines how to configure Mutare Voice to use SAML2 with Azure Active Directory.

What You Need to Begin

You will need the following information to begin:

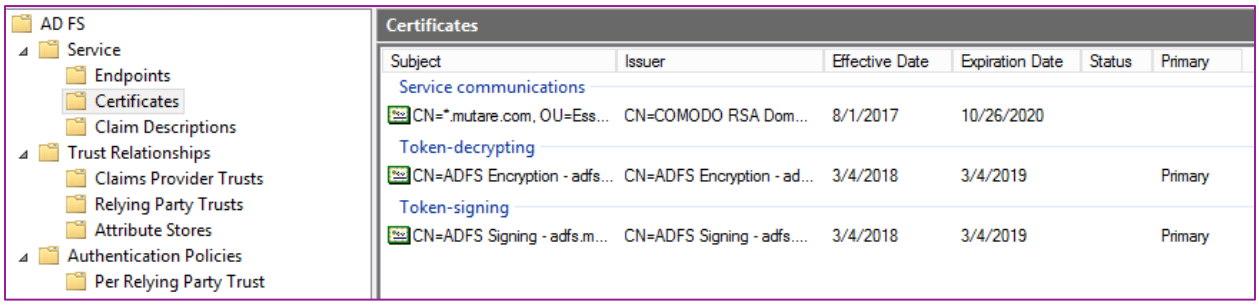
1. Full URL to the Mutare Voice. For the examples below, the URL is https://a-dev-sam.mutare.com
2. Admin access to the Azure AD server
3. Your token signing certificate
4. Your SAML Login URL
5. Your SAML Logout URL

ADFS Configuration

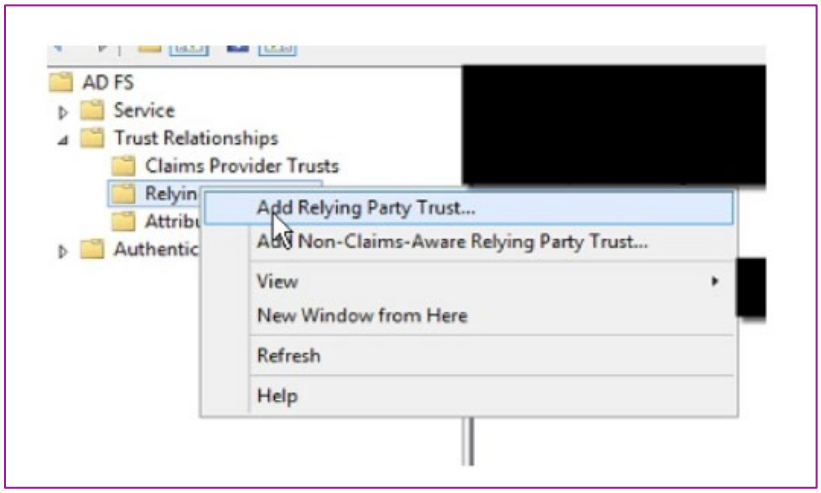
Navigate to your ADFS server.

You will need to provide us with your ADFS server name.

Download your Token-signing certificate, we will need this.

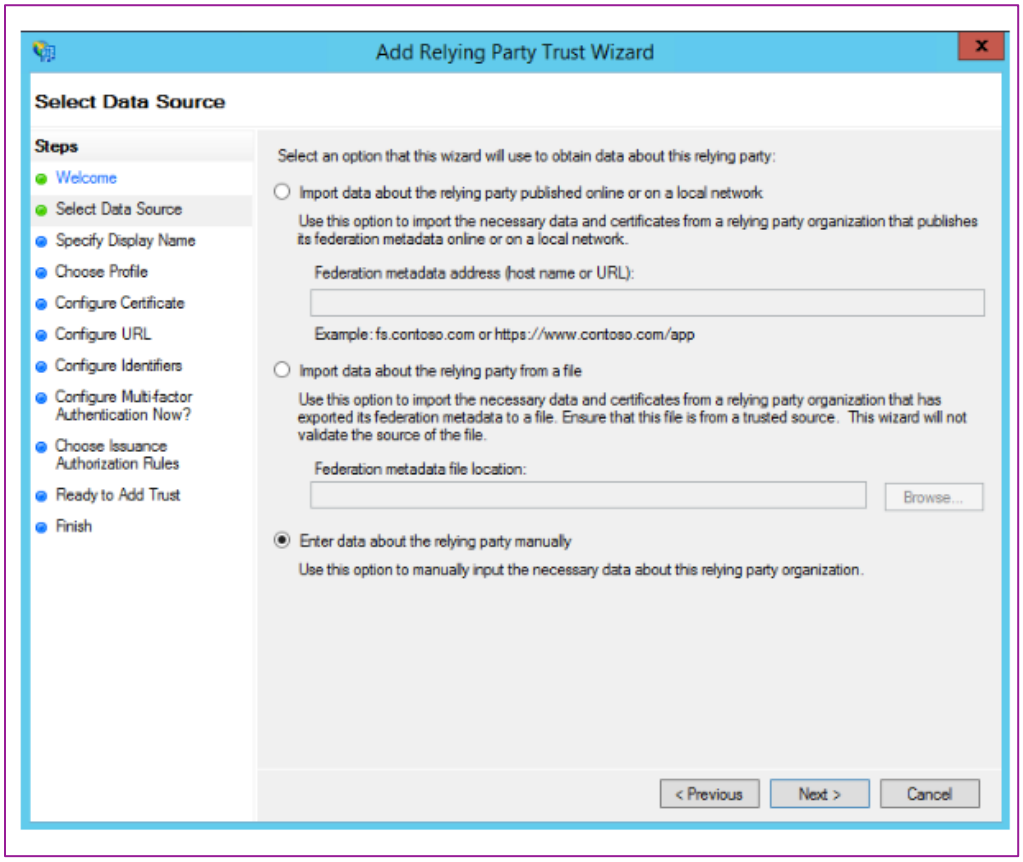


Add a Relying Party Trust



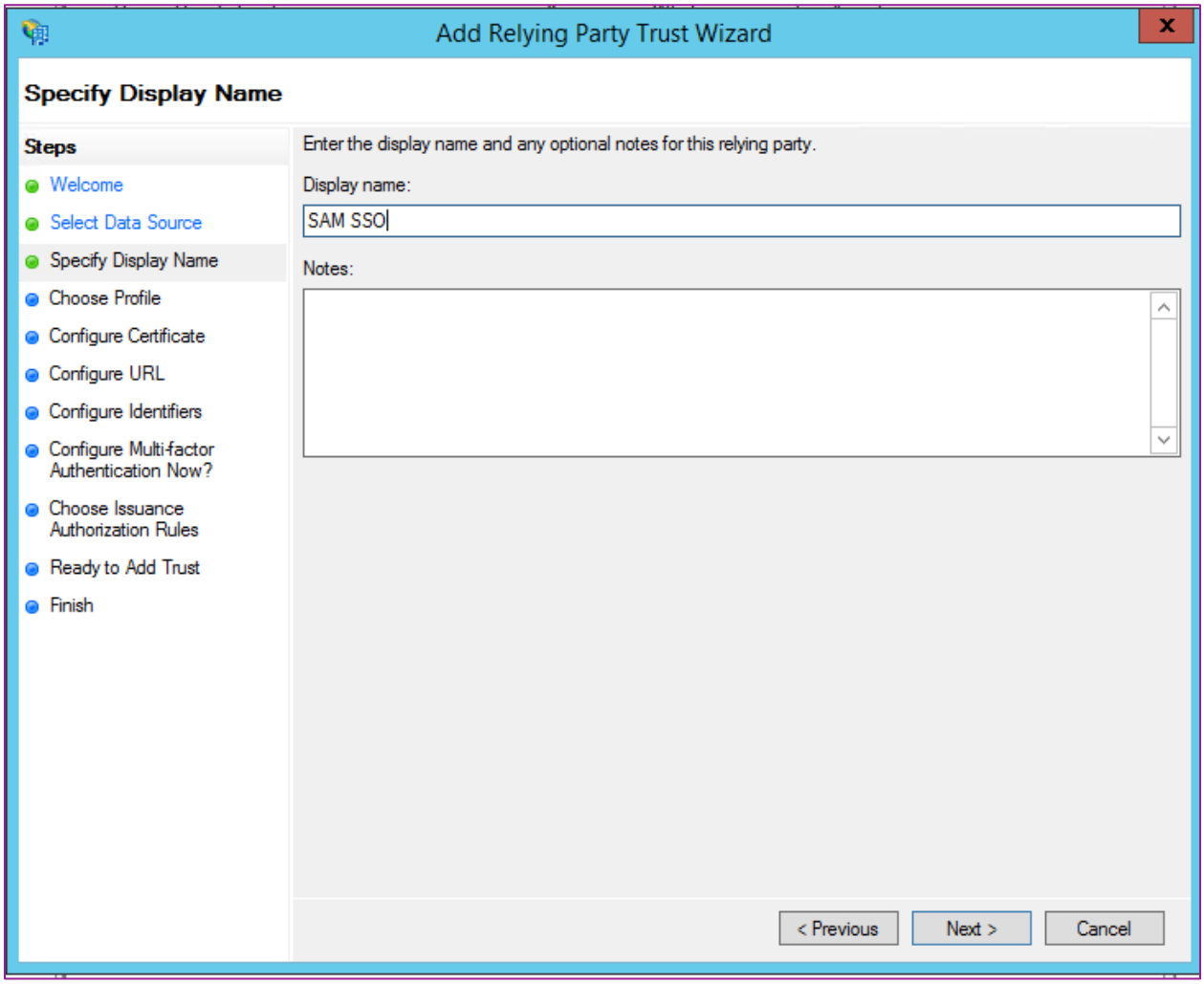
Customer Initials:

Select ‘Enter data about this relying party manually’.



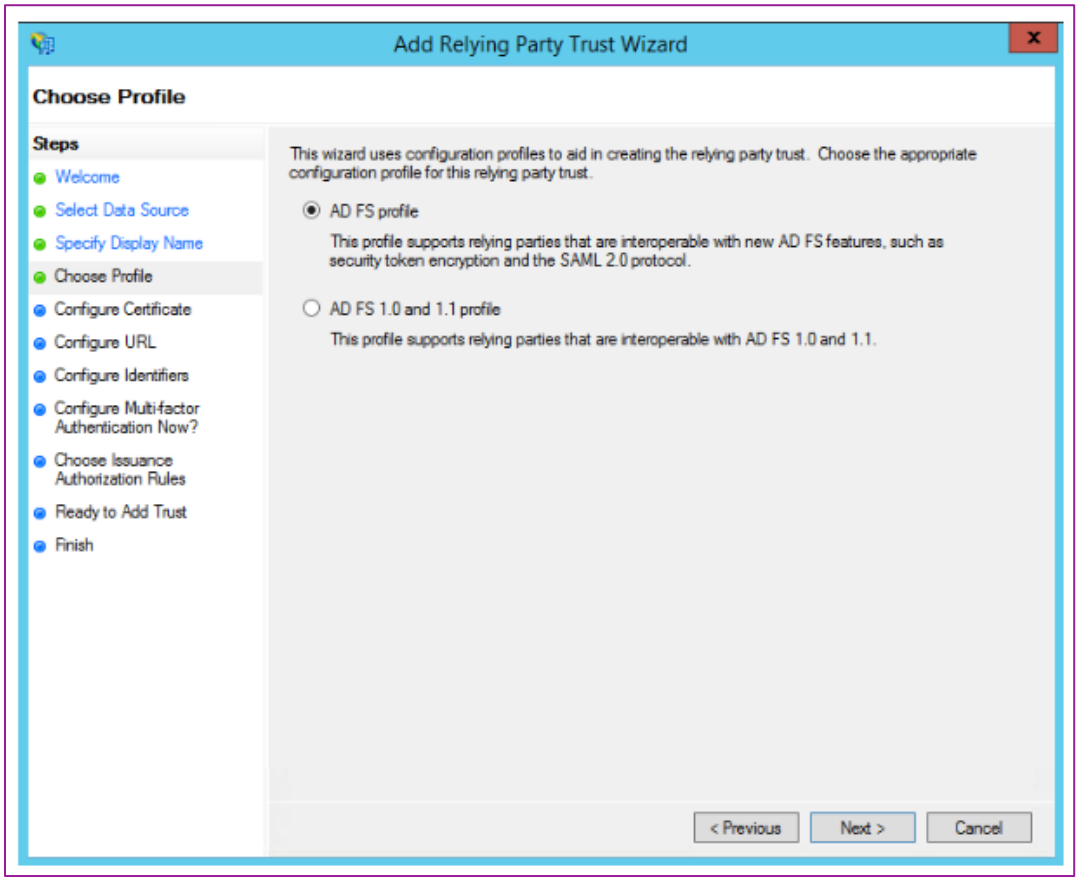
Customer Initials:

Enter ‘Display Name’



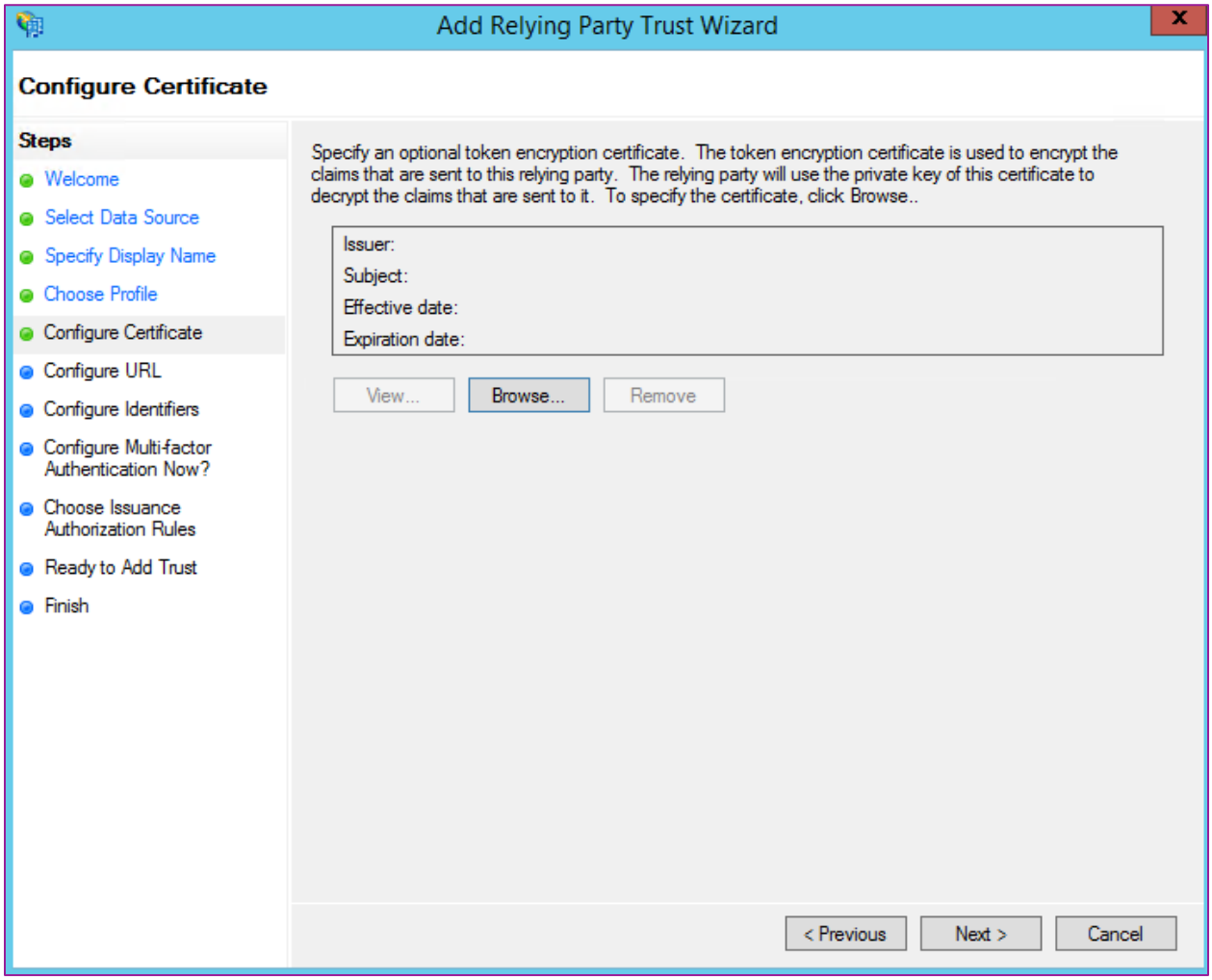
Customer Initials:

Select “AD FS profile”



Customer Initials:

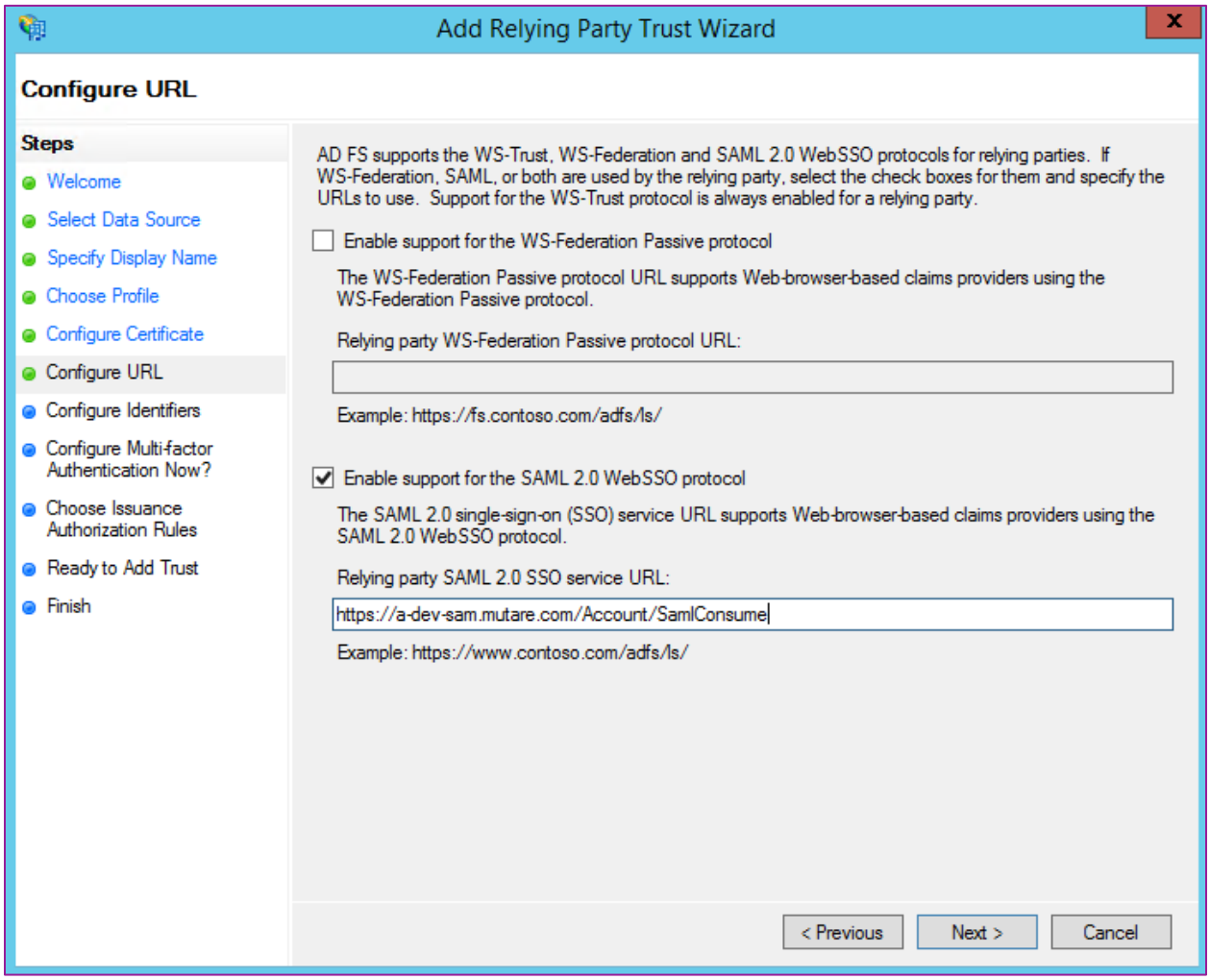
Leave the default values



Customer Initials:

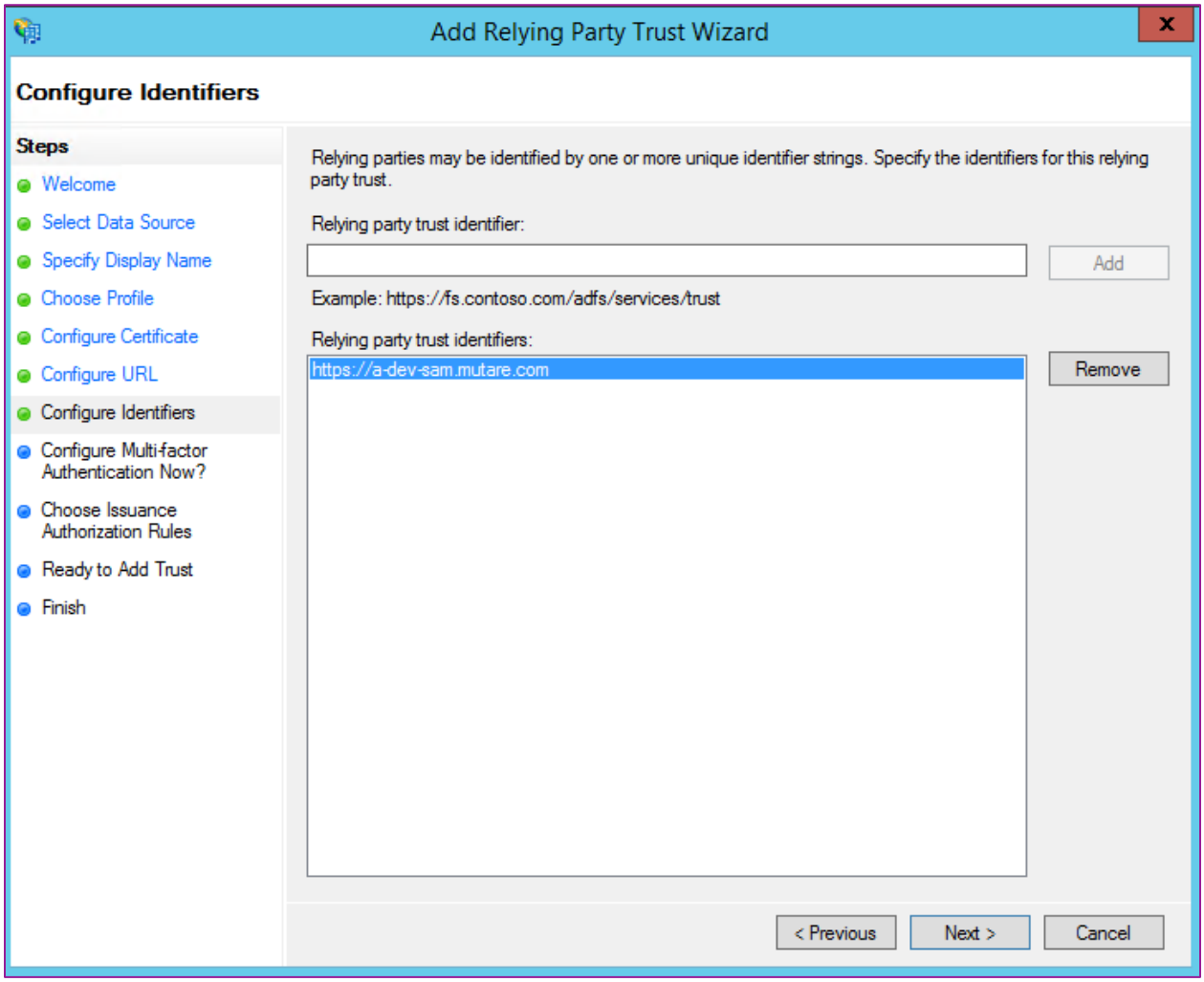
Check “Enable support for the SAML 2.0 WebSSO protocol”.

For the “Relying party SAML 2.0 SSO service URL” value, use the URL for the Mutare Voice website, followed by /Account/SamlConsume. See below.



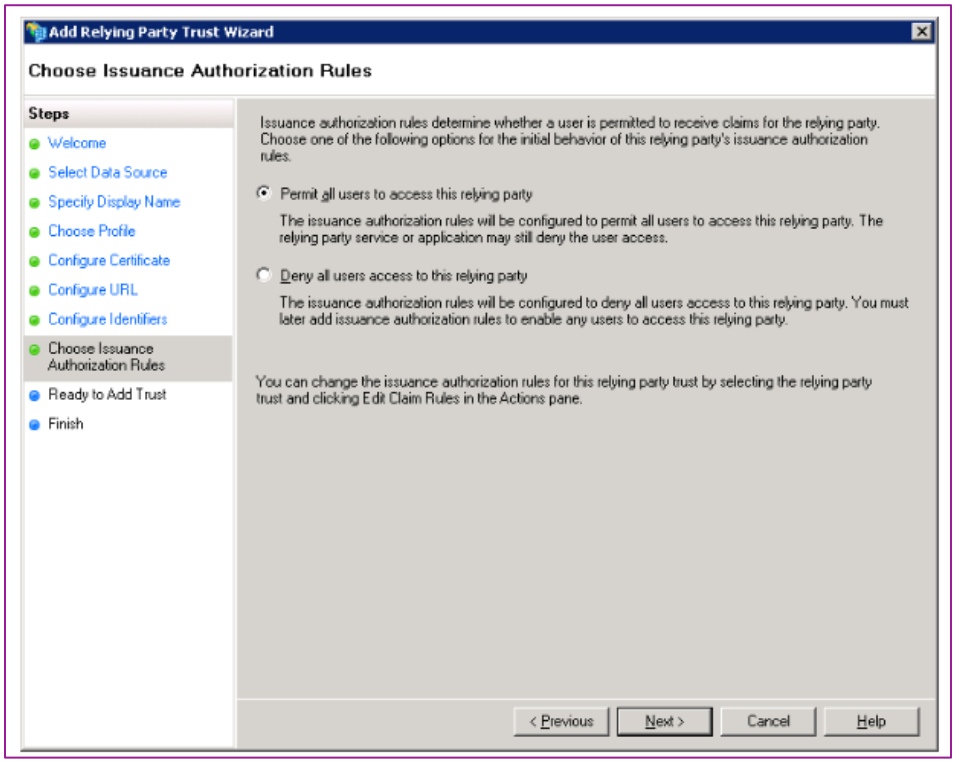
Customer Initials:

For the Relying party trust identifier, use the URL for the Mutare Voice website.

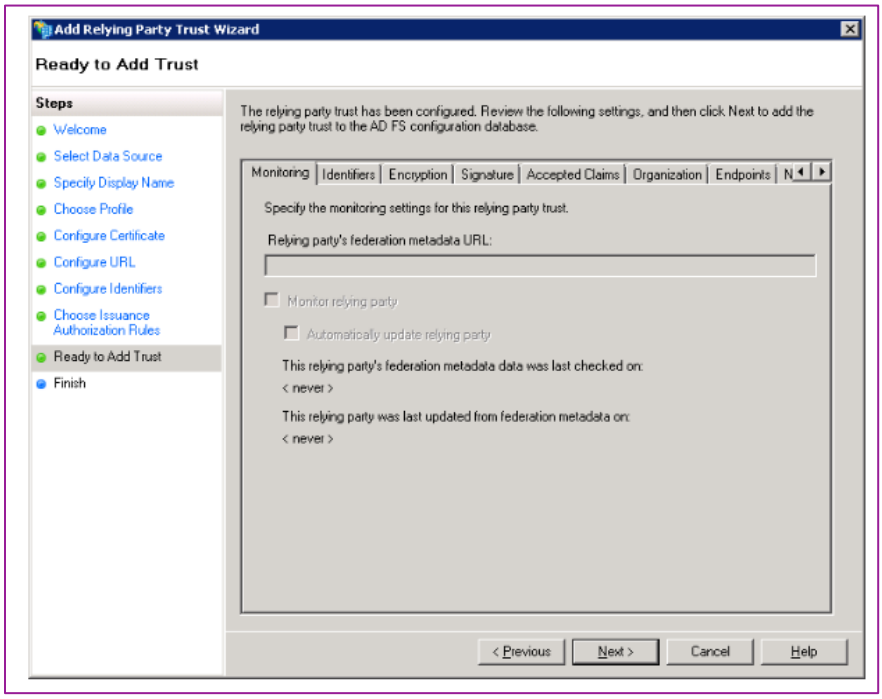


Customer Initials:

Check “Permit all users to access this relying party”

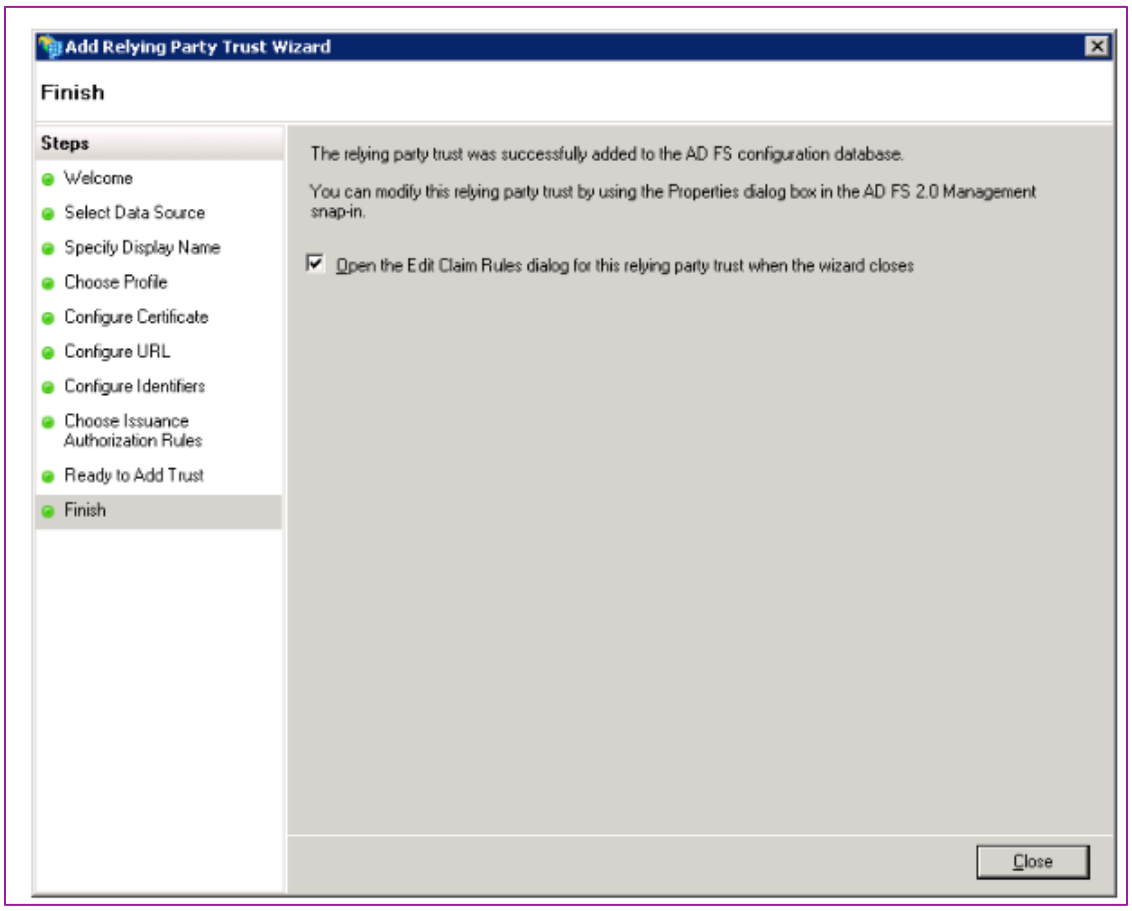


Review

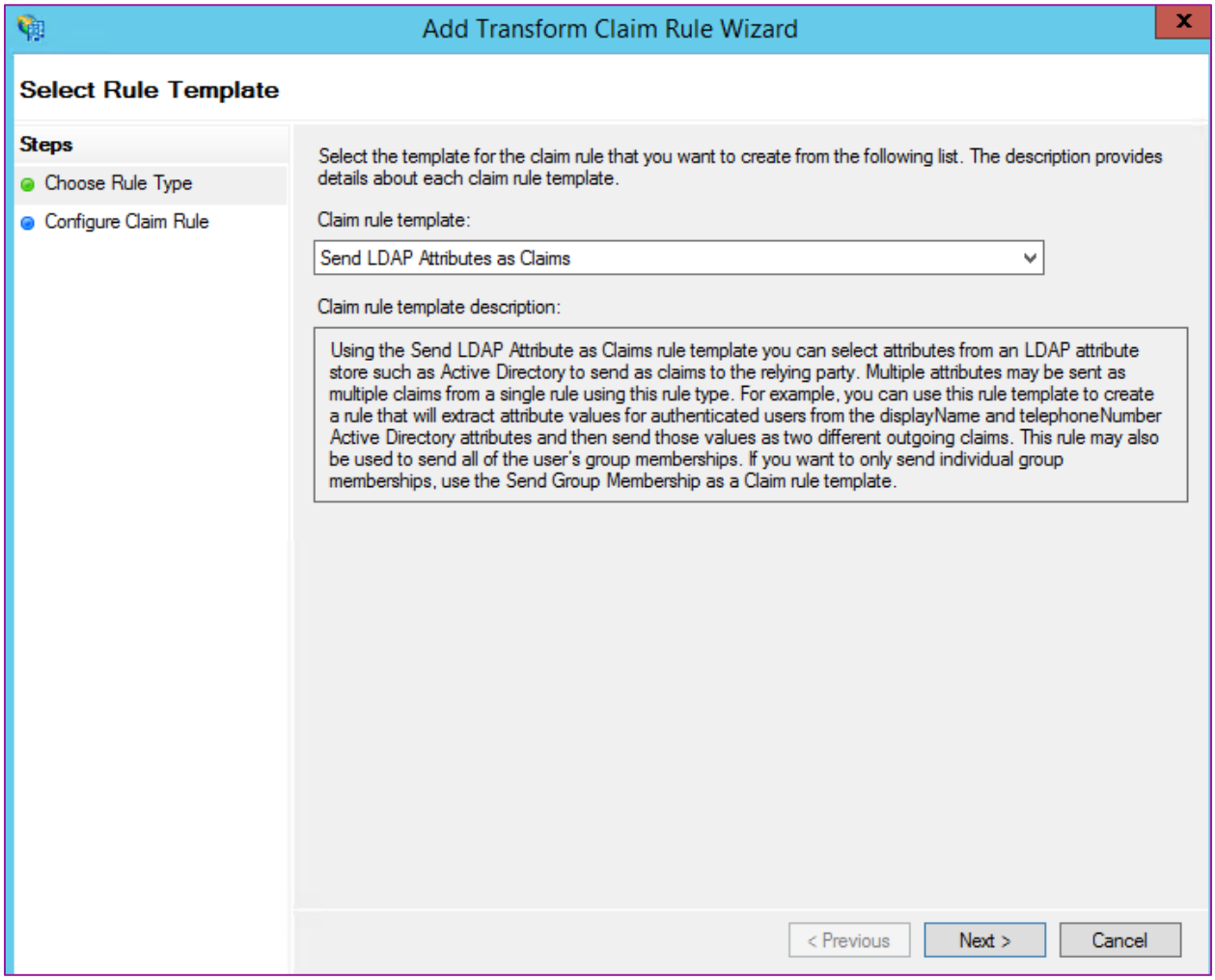


Customer Initials:

Check “Open the Edit Claim Rules dialog for this relying party trust when the wizard closes” to set up the needed claims.



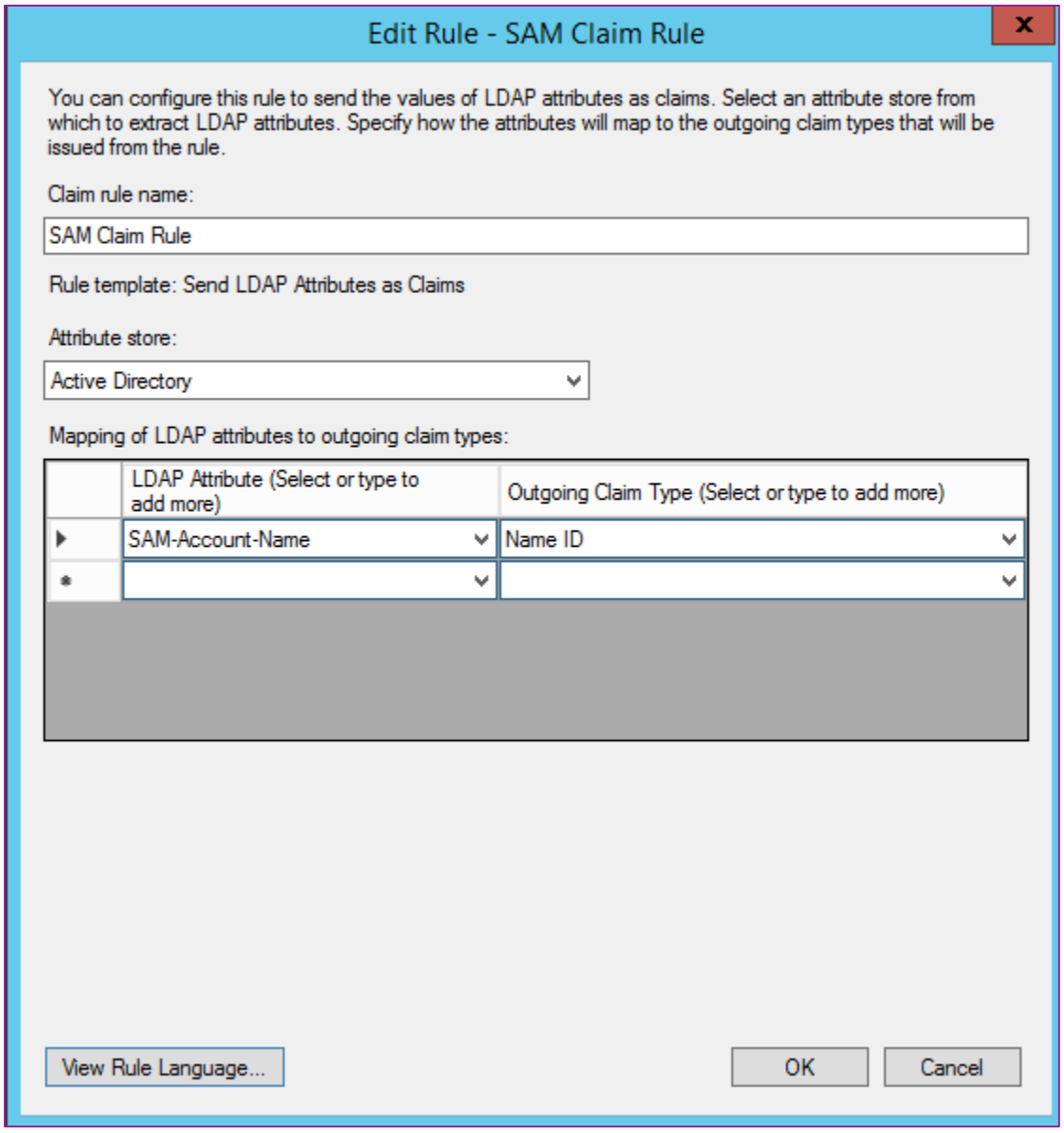
Select “Send LDAP Attributes as Claims”



Customer Initials:

Add the following Claim rule names:

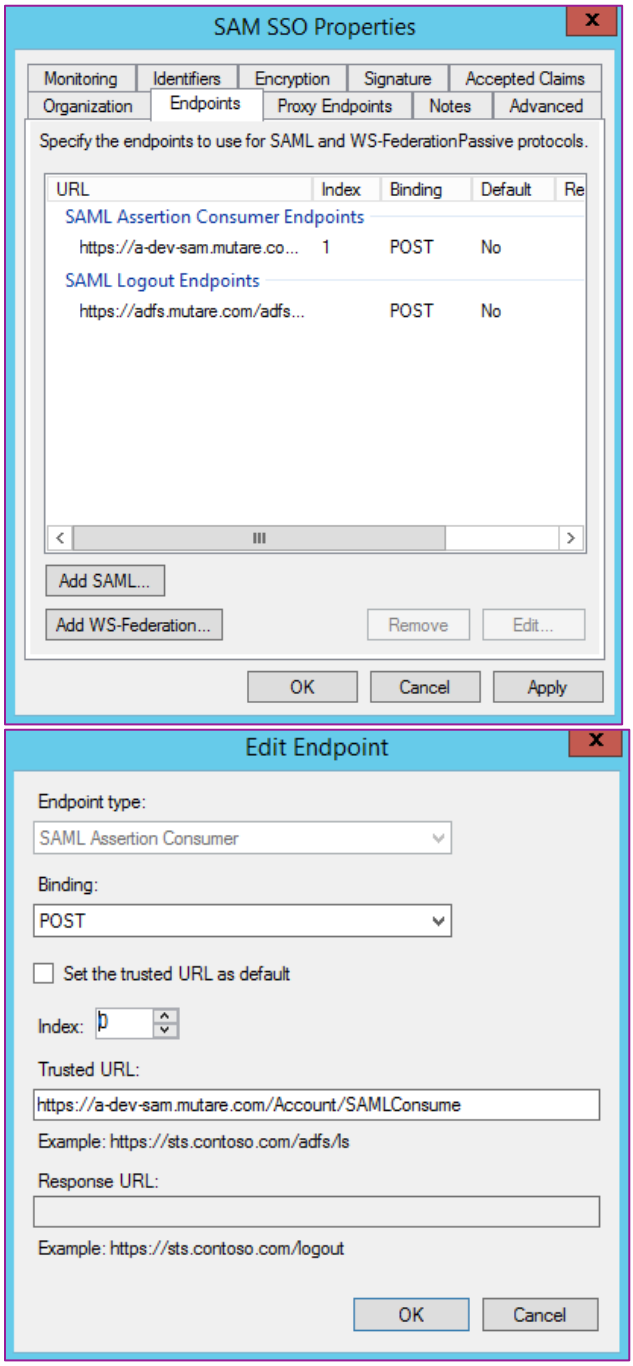
- Attribute store = Active Directory Identifier = the Mutare Voice website URL
- LDAP Attribute = MutareVoice-Account-Name
- Outgoing Claim Type = Name ID



Navigate to your relying party trust properties endpoints and add a new endpoint.

Customer Initials:

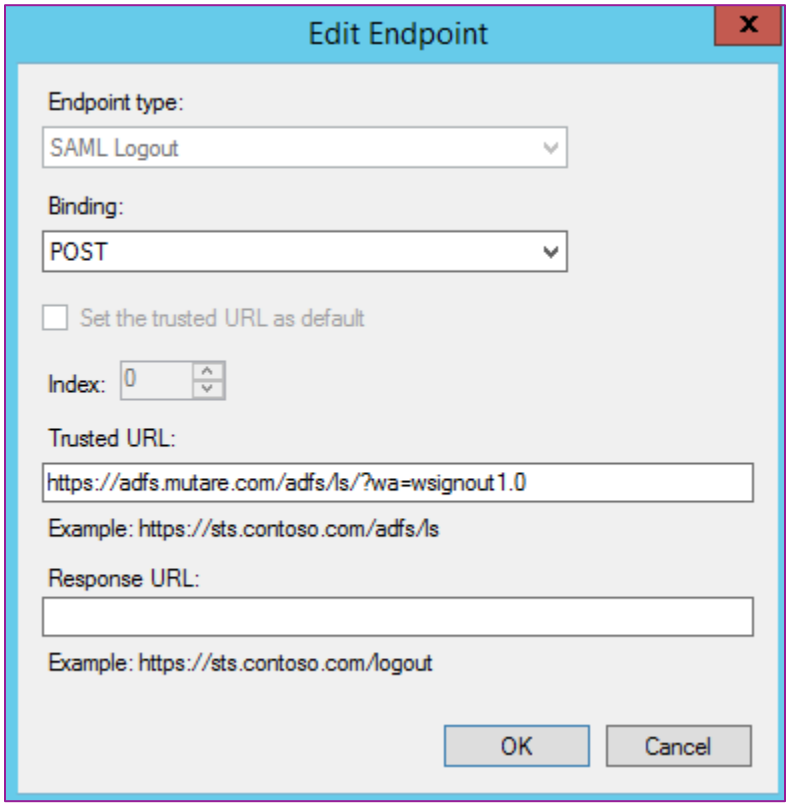
- Endpoint type = SAML Assertion Consumer
- Binding = POST
- Index = 0
- The Trusted URL = the Mutare Voice URL plus “/Account/SAMLConsume”. See below.



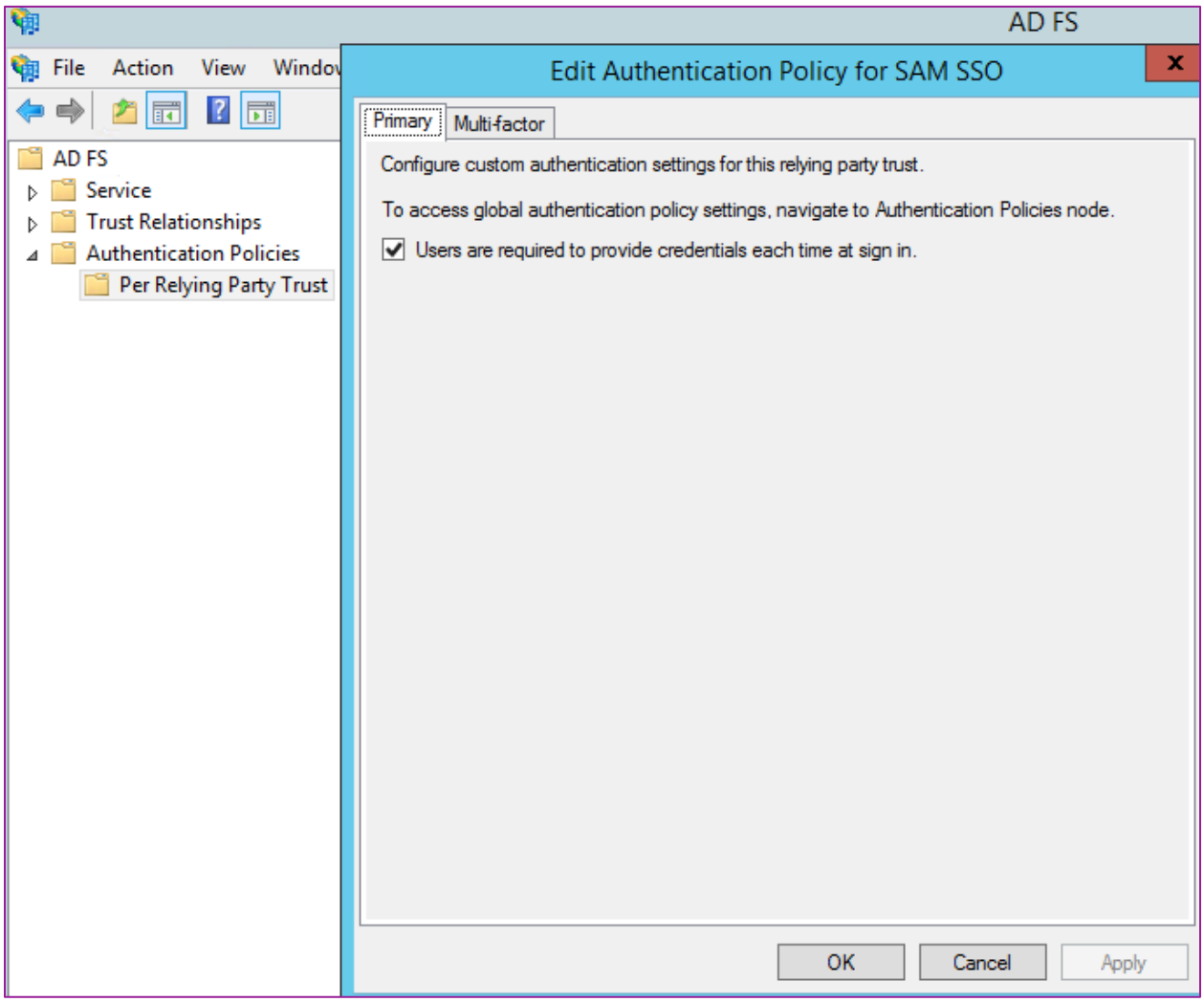
Add another endpoint for logout.

Customer Initials:

- Endpoint type = SAML Logout
- Binding = POST
- Index = 0
- URL = Follow the following structure where adfs.mutare.com = your ADFS server name
- You will need to provide us with this URL.



Navigate to Authentication Policies, Per Relying Party Trust, and Edit Authentication Policy for the relying party trust you just added and check “Users are required to provide credentials each time at sign in”.



Customer Initials:

Mutare Voice Configuration

In the Mutare Voice System Settings, access the SAML section:

1. SAMLLogin – This is the URL to the client's ADFS server login. e.g. https://adfs.mutare.com/adfs/ls/
2. SAMLLogout - This is the URL to the client's ADFS server logout. e.g. https://adfs.mutare.com/adfs/ls/?wa=wsignout1.0
3. SAMLTokenSigningCertificateLocation – This is the path to where Mutare will store the client's ADFS Token Signing Certificate. e.g. C:\VitalLinkWebs\SAM\CI\Dev\Certificates\Mutare_ADFS_Token-Signing.cer
4. SAMLIdentifier – This is the URL to Mutare Voice. e.g. https://a-dev-sam.mutare.com
5. IsSAMLEnabled – This enables/disables SAML in Mutare Voice. e.g. true/false
6. SAMLLoginLinkText – This is the text for the back door login page to access SAML login. e.g. "Login with ADFS"