

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.

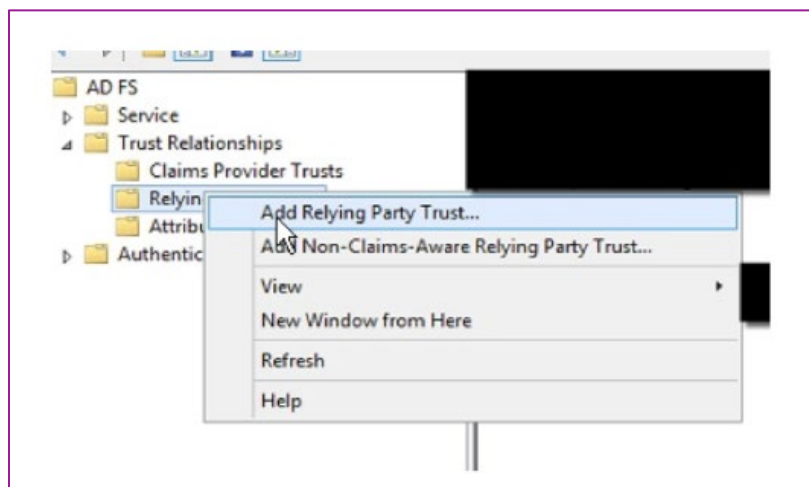
You will need to provide us with your ADFS server name.

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



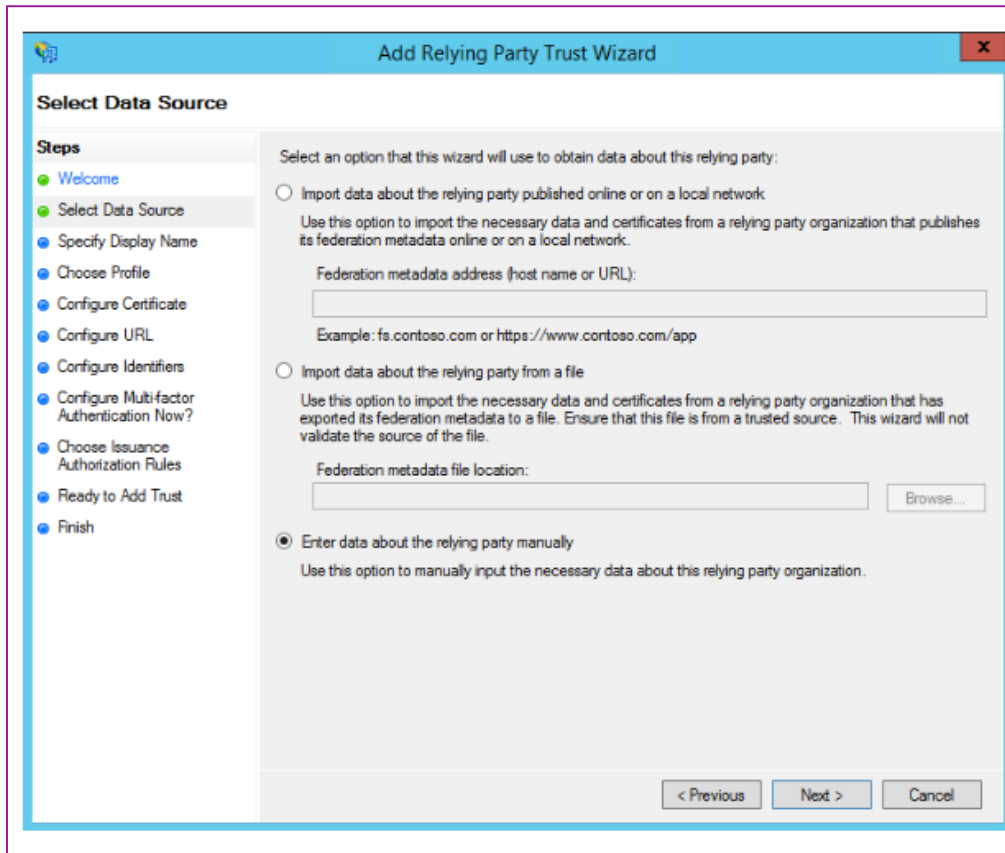
Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=*.mutare.com, OU=Ess...	CN=COMODO RSA Dom...	8/1/2017	10/26/2020		
Token-decrypting					
CN=ADFS Encryption - adfs...	CN=ADFS Encryption - ad...	3/4/2018	3/4/2019		Primary
Token-signing					
CN=ADFS Signing - adfs.m...	CN=ADFS Signing - adfs...	3/4/2018	3/4/2019		Primary

Add a Relying Party Trust



Customer Initials:

Select 'Enter data about this relying party manually'.



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 Multifactor 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.

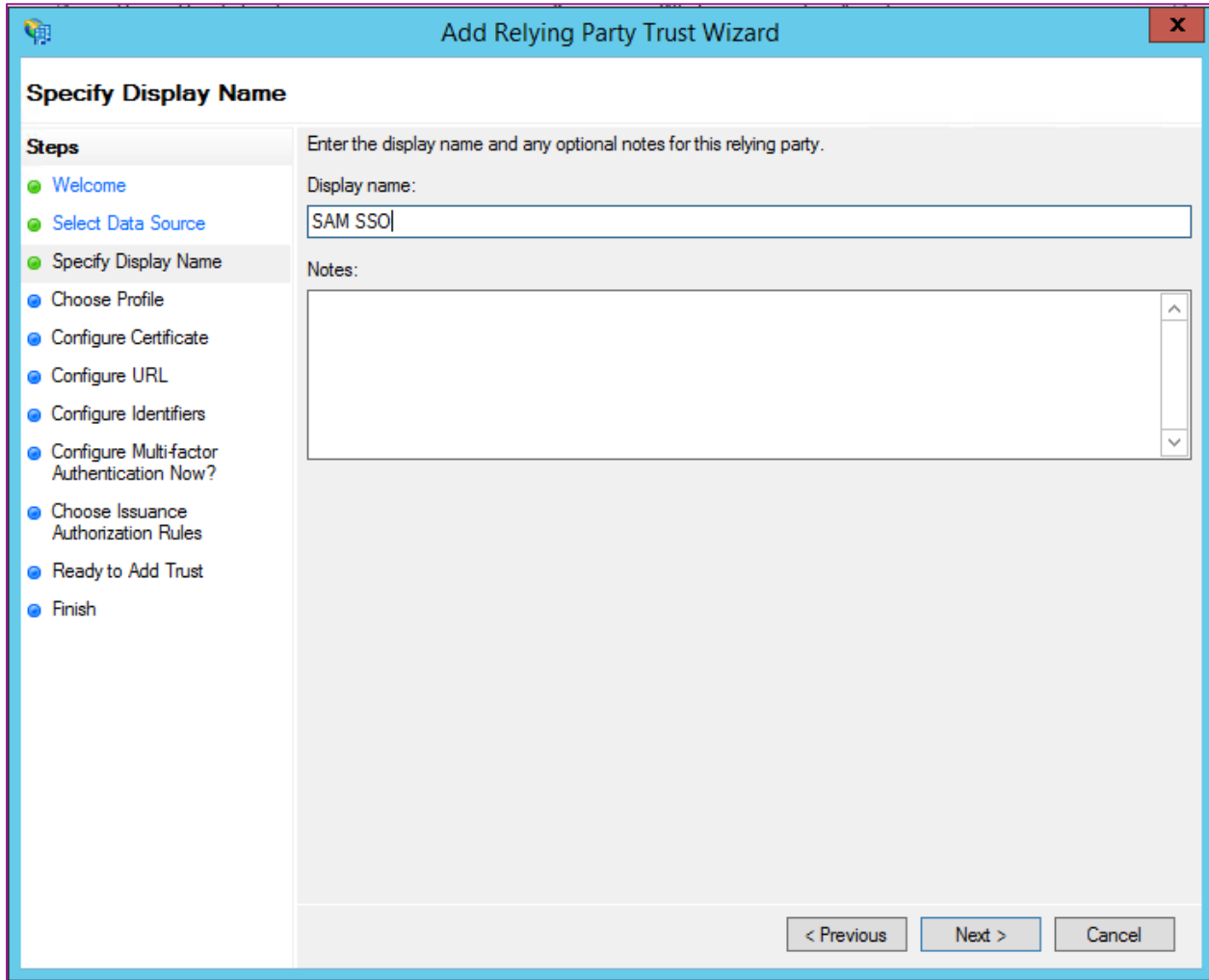
Federation metadata file location:

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

< Previous Next > Cancel

Customer Initials:

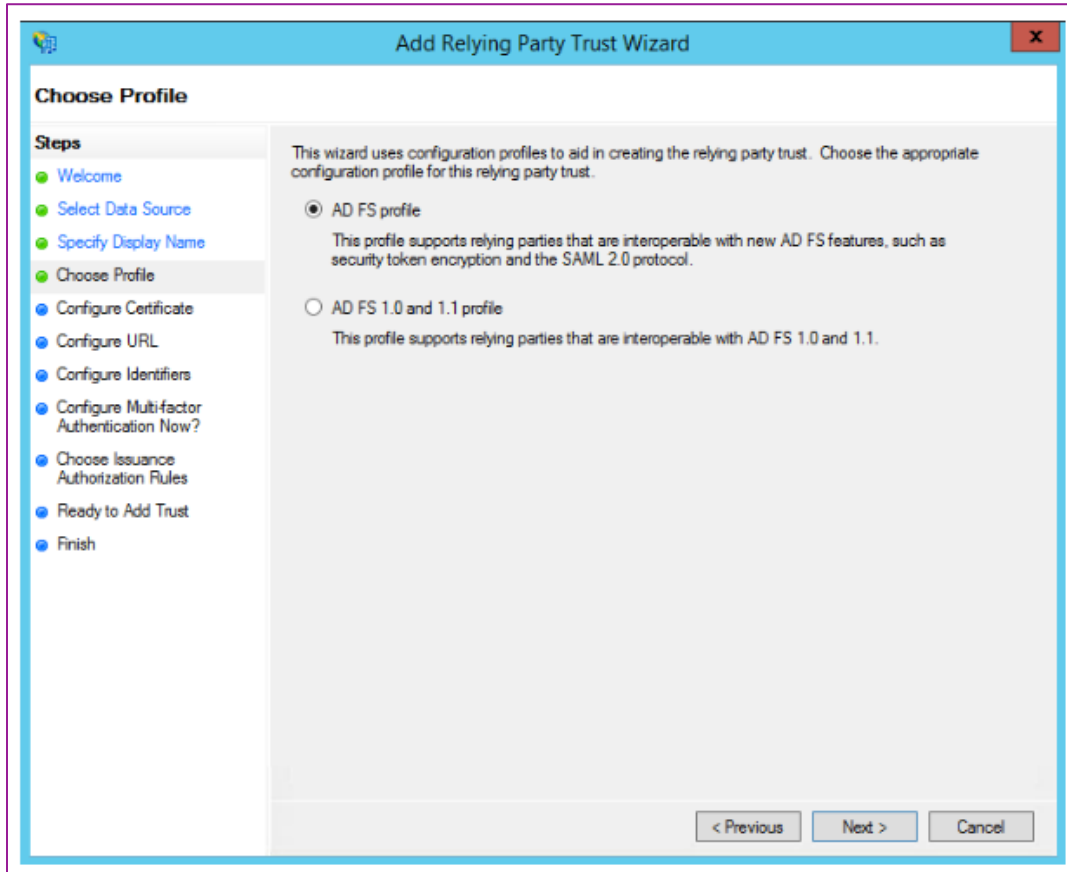
Enter 'Display Name'



The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The current step is "Specify Display Name". On the left, a "Steps" list shows the progression: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, there is a "Display name:" label and a text input field containing "SAM SSO". Underneath is a "Notes:" label and a large text area for notes. At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

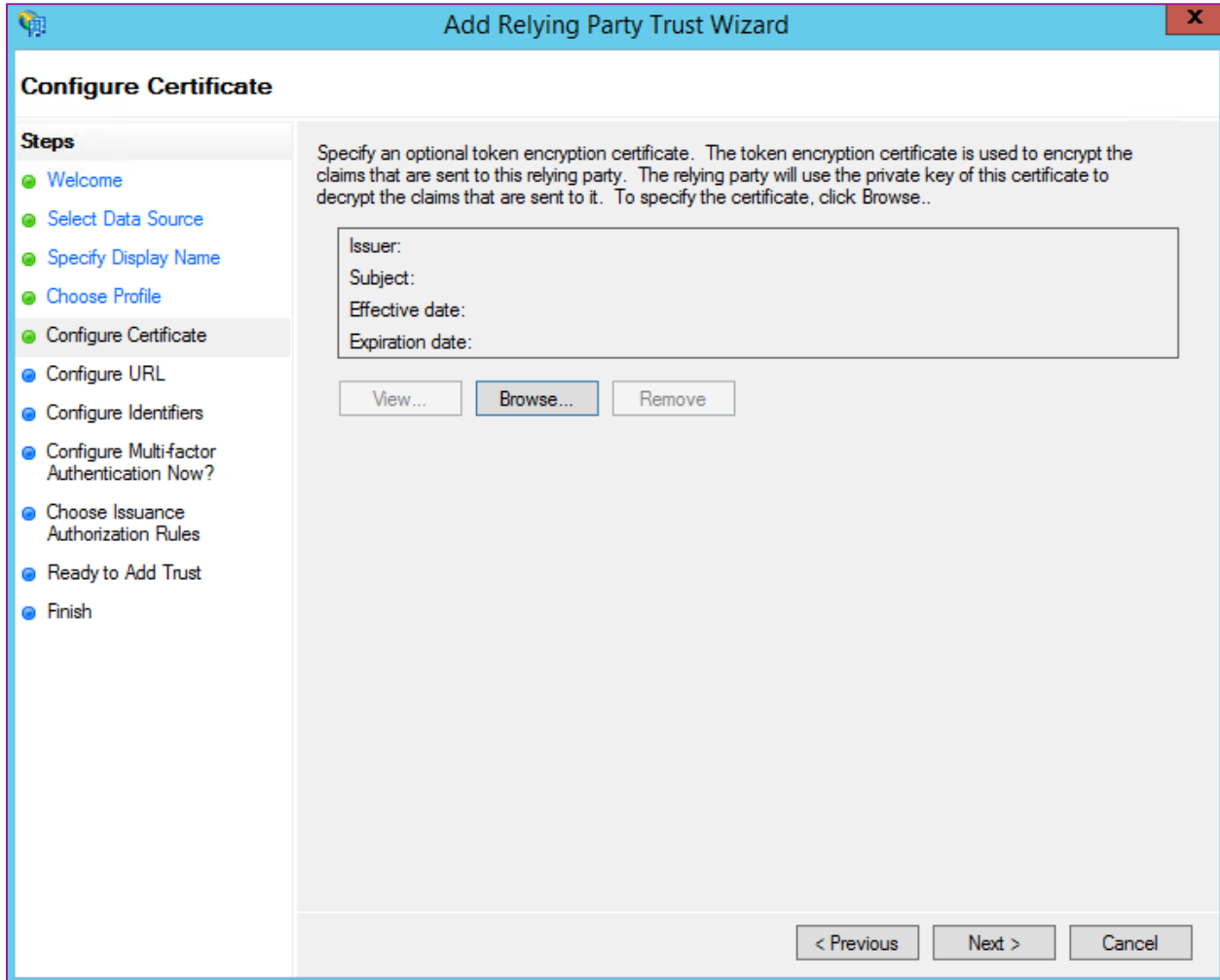
Customer Initials:

Select "AD FS profile"



Customer Initials:

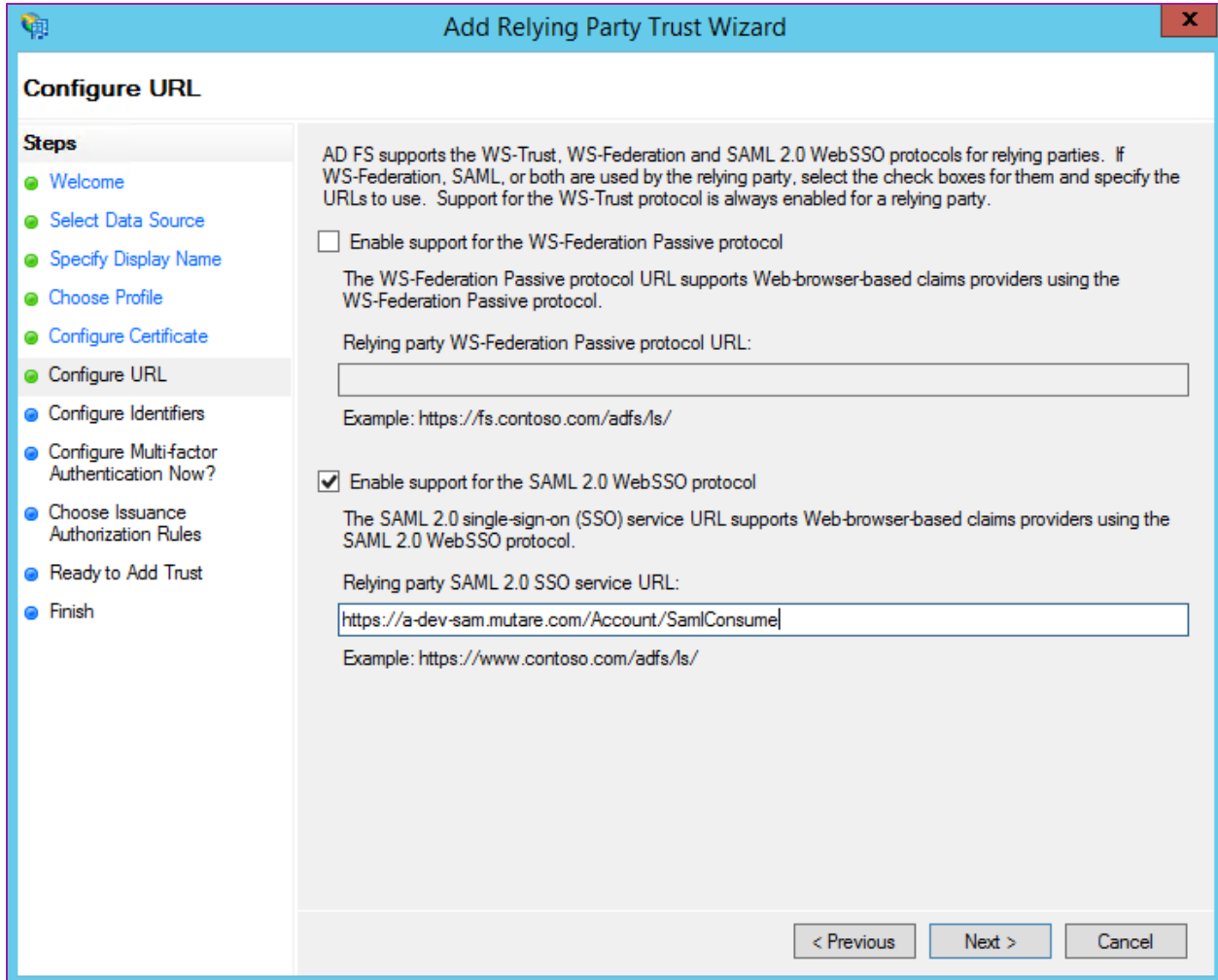
Leave the default values



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.



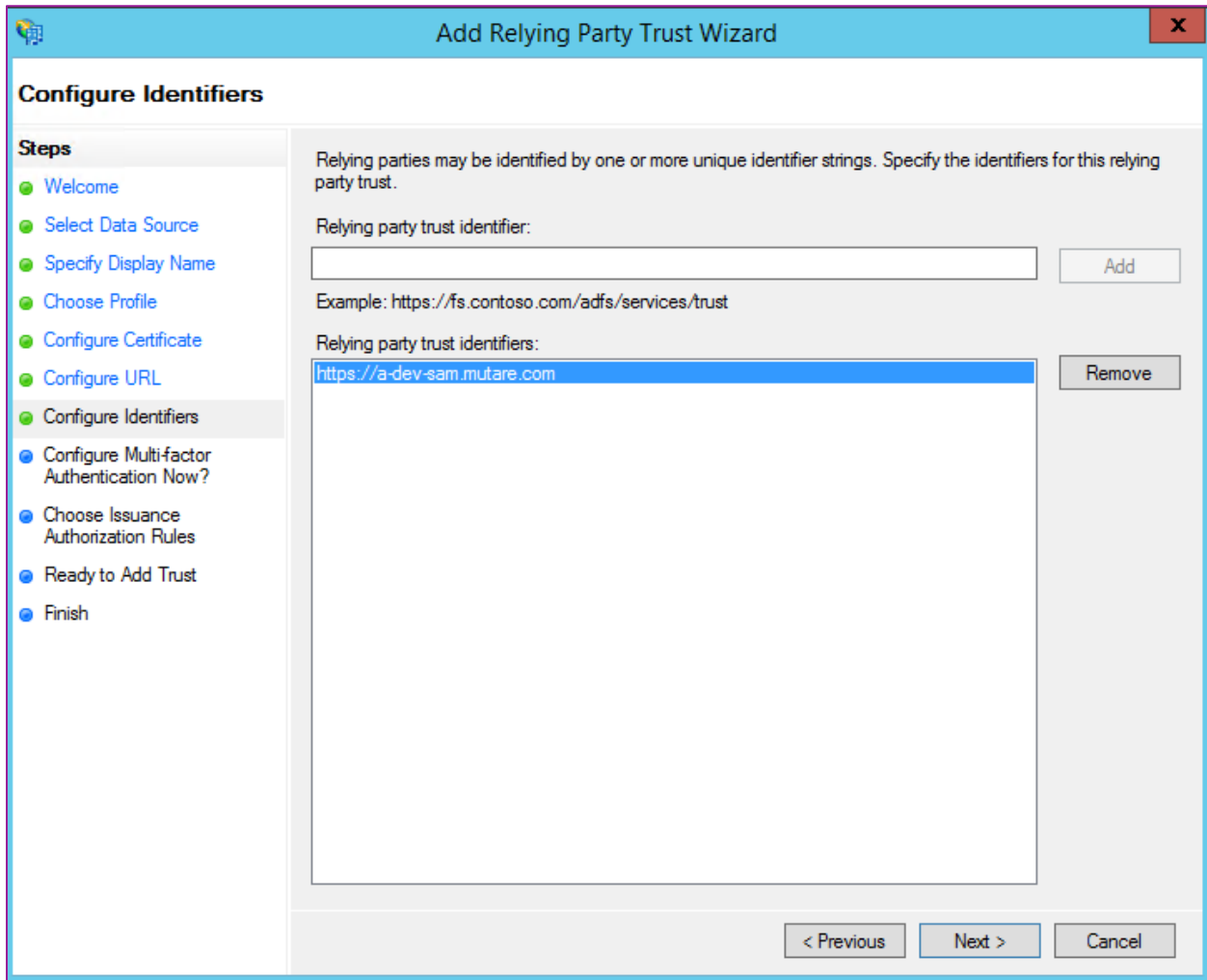
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The wizard has a sidebar with steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (current), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains instructions and two options:

- 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: [text box]. 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: [text box containing https://a-dev-sam.mutare.com/Account/SamlConsume]. Example: https://www.contoso.com/adfs/ls/

At the bottom right, there are buttons for '< Previous', 'Next >', and 'Cancel'.

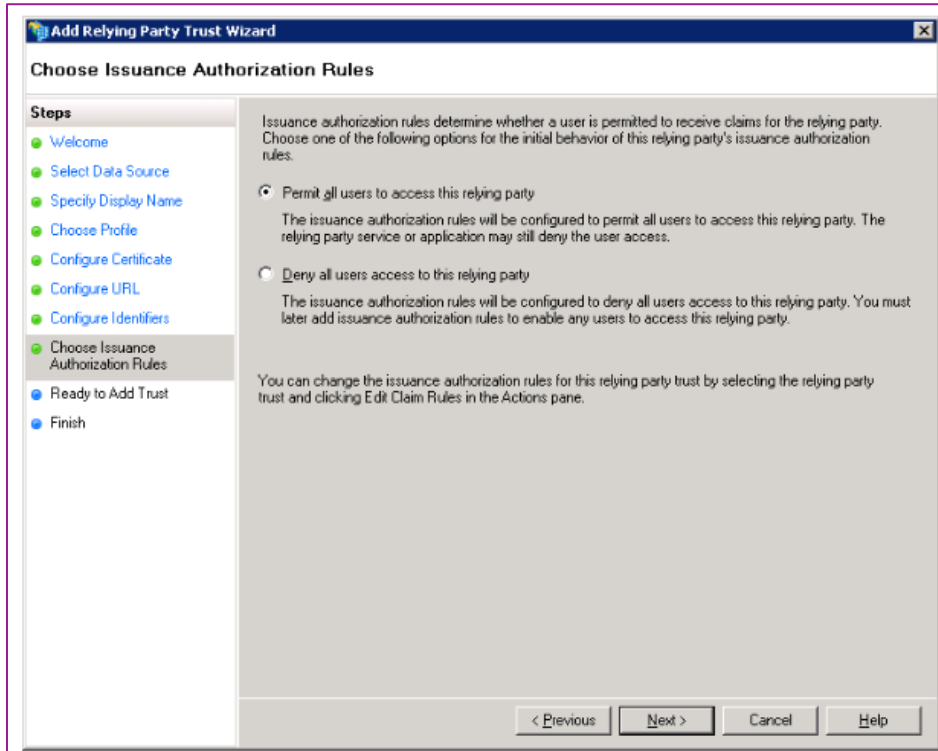
Customer Initials:

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

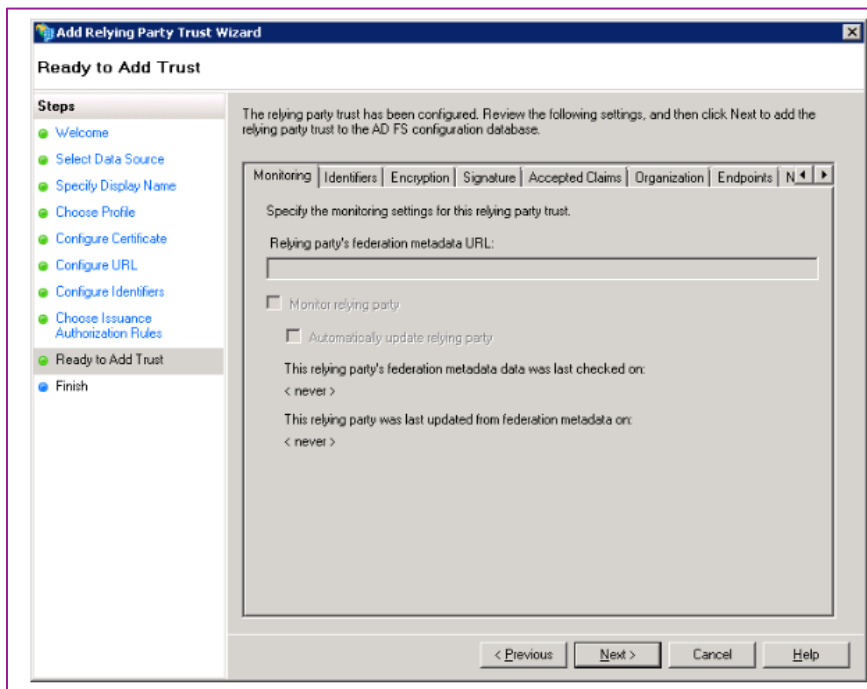


Customer Initials:

Check “Permit all users to access this relying party”

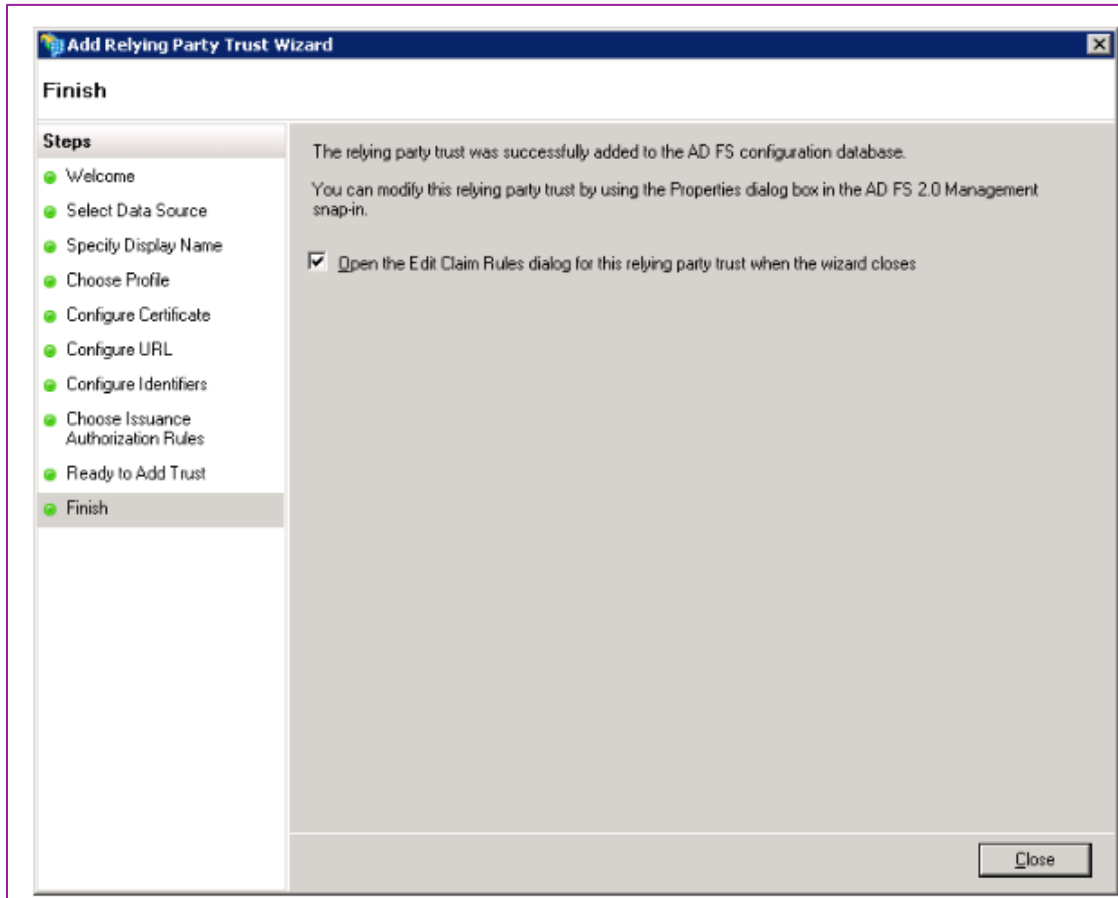


Review



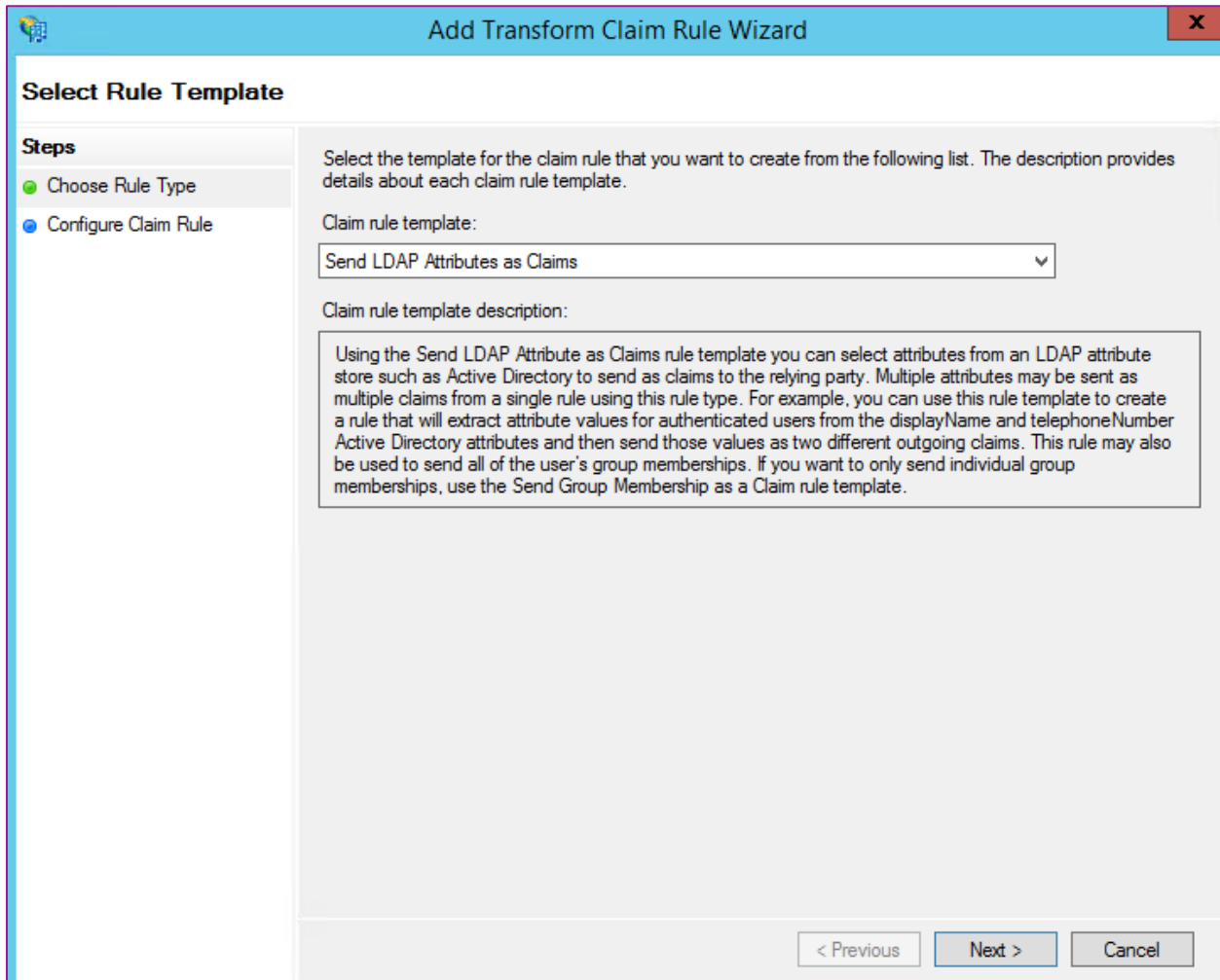
Customer Initials:

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



Customer Initials:

Select "Send LDAP Attributes as Claims"



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

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

Edit Rule - SAM Claim Rule
X

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:

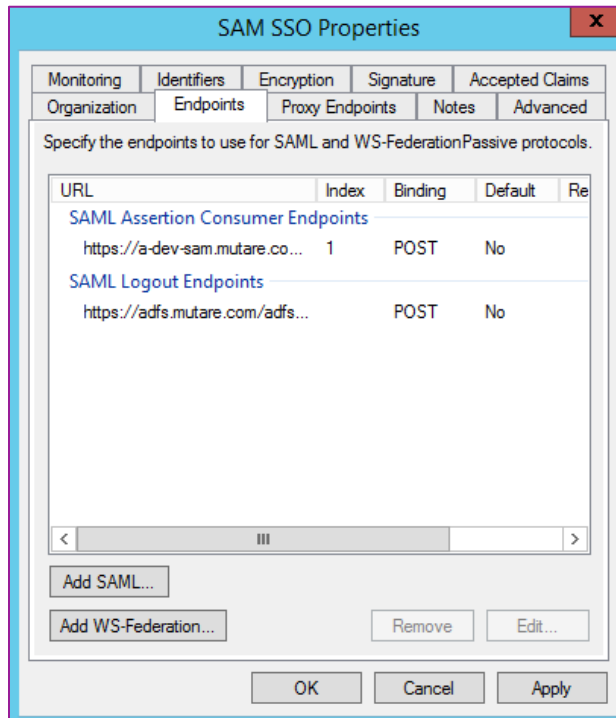
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name ▼	Name ID ▼
*	▼	▼

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

Customer Initials:

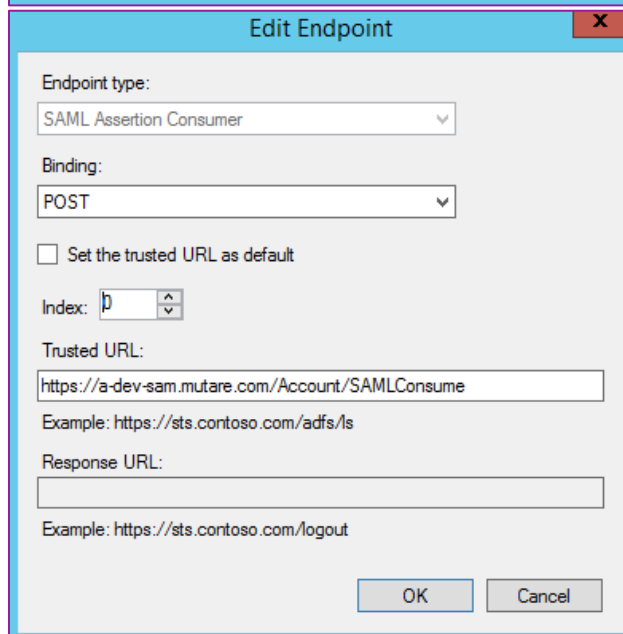
- Endpoint type = SAML Assertion Consumer
- Binding = POST
- Index = 0
- The Trusted URL = the Mutare Voice URL plus “/Account/SAMLConsume”. See below.



The screenshot shows the 'SAM SSO Properties' dialog box with the 'Endpoints' tab selected. The dialog contains a table of endpoints and several control buttons.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://a-dev-sam.mutare.co...	1	POST	No	
SAML Logout Endpoints				
https://adfs.mutare.com/adfs...		POST	No	

Buttons: Add SAML..., Add WS-Federation..., Remove, Edit..., OK, Cancel, Apply



The screenshot shows the 'Edit Endpoint' dialog box. It contains the following fields and controls:

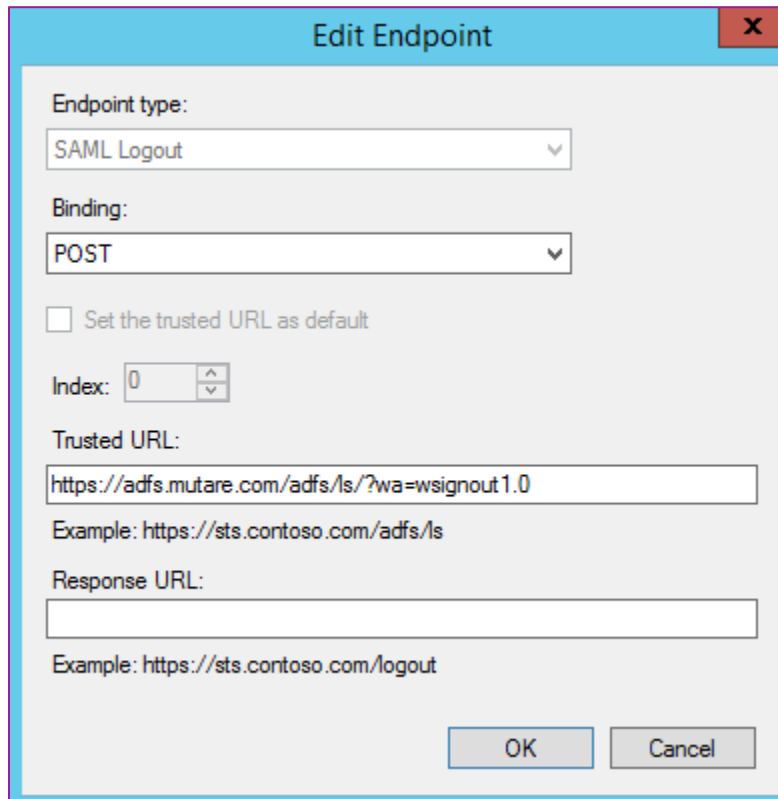
- Endpoint type: SAML Assertion Consumer (dropdown)
- Binding: POST (dropdown)
- Set the trusted URL as default
- Index: 0 (spin box)
- Trusted URL: https://a-dev-sam.mutare.com/Account/SAMLConsume (text box)
- Example: https://sts.contoso.com/adfs/ls
- Response URL: (empty text box)
- Example: https://sts.contoso.com/logout

Buttons: OK, Cancel

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.



Edit Endpoint

Endpoint type:
SAML Logout

Binding:
POST

Set the trusted URL as default

Index: 0

Trusted URL:
https://adfs.mutare.com/adfs/ls/?wa=wsignout1.0
Example: https://sts.contoso.com/adfs/ls

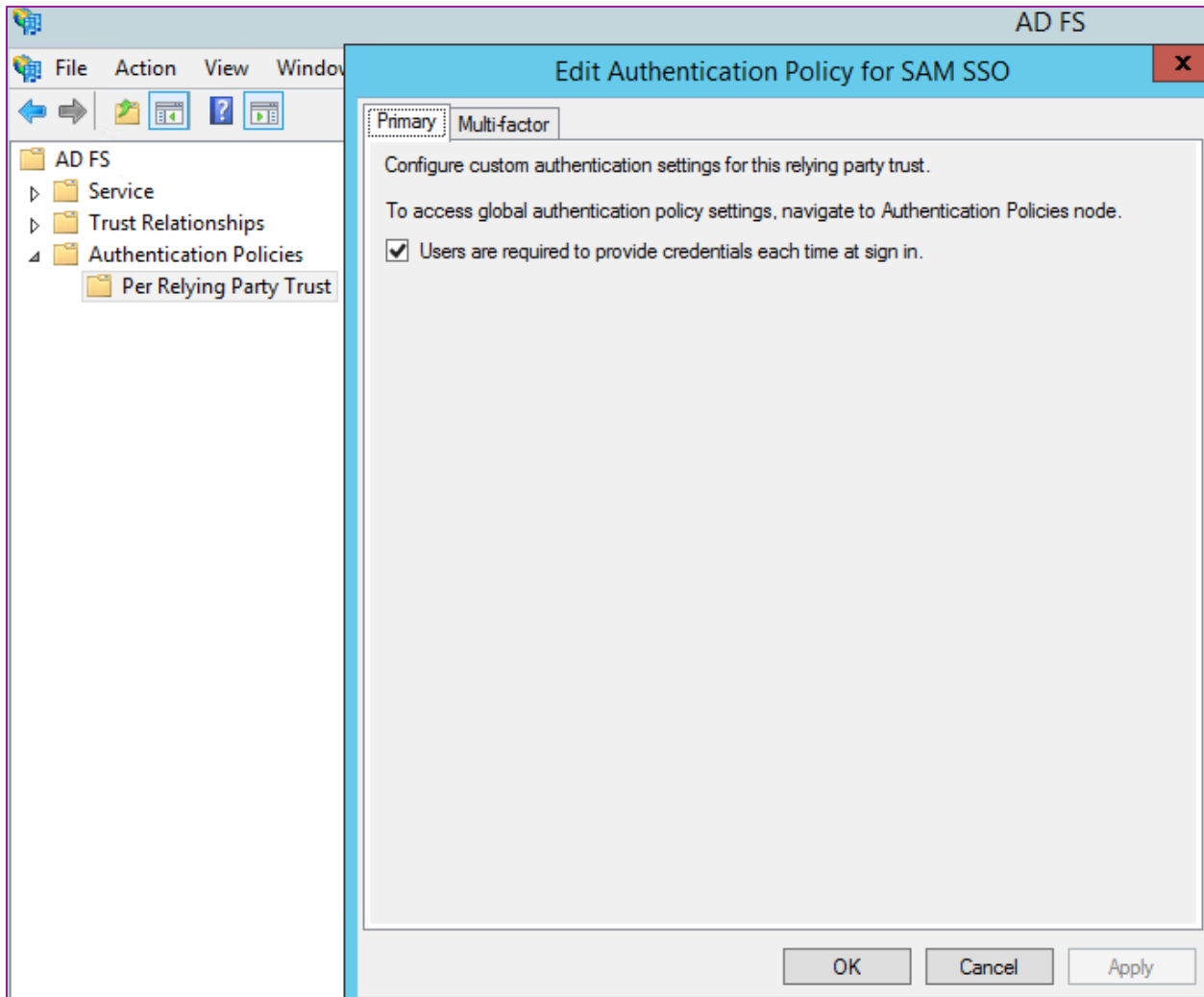
Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

Customer Initials:

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"

Customer Initials: