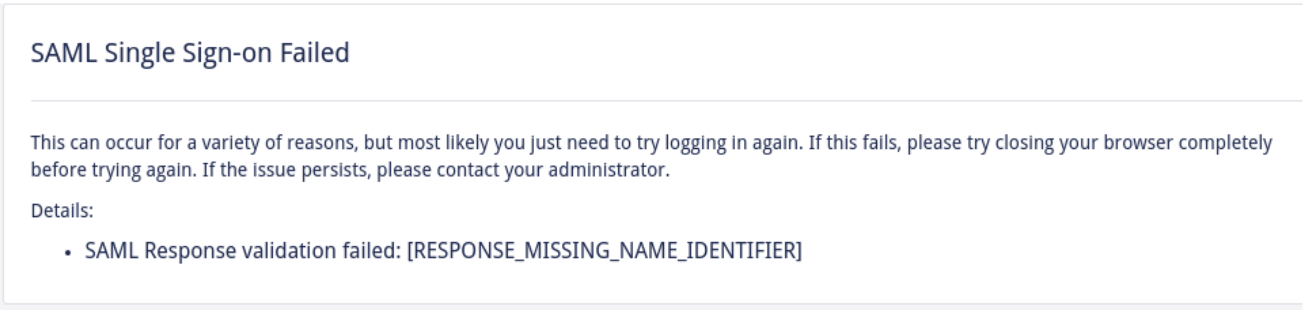
SLO: AD FS

This document describes how to configure Single Logout for AD FS. For general information, refer to Single Logout.

Read before enabling SLO if initial ADFS setup was done before Kantega SSO 3.5.0

If you configured ADFS using the provided PowerShell script or manual setup instructions ***before*** Kantega SSO **3.5.0**, enabling single logout may break login. We recommend applying the instructions below *before* enabling SLO. You'll know you have encountered the issue if you start seeing RESPONSE_MISSING_NAME_IDENTIFIER when trying to log in:



SAML Single Sign-on Failed

This can occur for a variety of reasons, but most likely you just need to try logging in again. If this fails, please try closing your browser completely before trying again. If the issue persists, please contact your administrator.

Details:

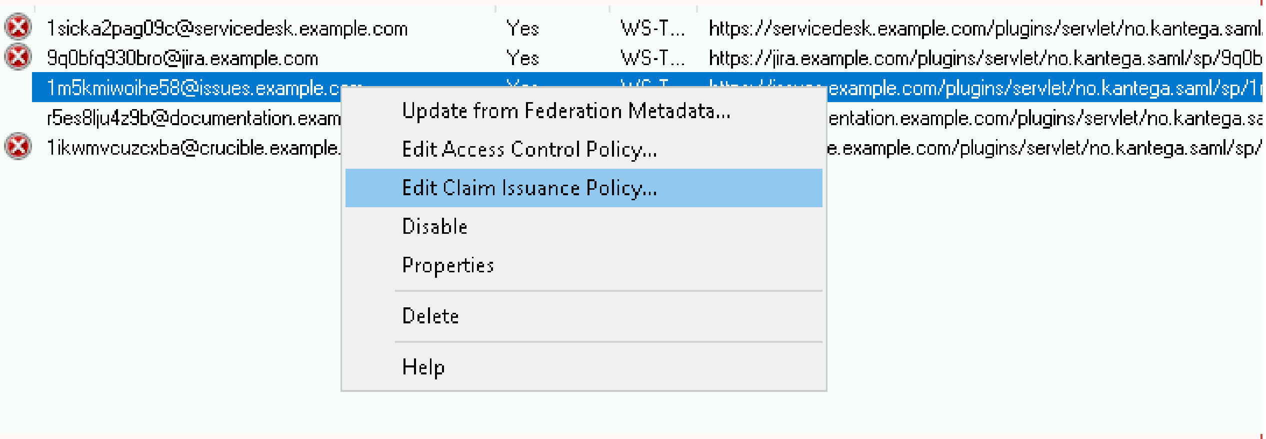
- SAML Response validation failed: [RESPONSE_MISSING_NAME_IDENTIFIER]

Kantega SSO requires a *name identifier claim* in the SAML Response from ADFS (or any other IDP) when SLO is enabled. This uniquely identifies the user's IDP session, and we need it to be able to initiate SLO later. Most IDPs send it by default but ADFS only does so when explicitly configured. Unfortunately, older versions of our PowerShell script for ADFS did not include it. From Kantega SSO 3.5.0 onwards, it's included by default and you should be able to disregard the rest of this section.

To remedy this, you can either:

- Rerun the setup wizard and create a new configuration using the provided script which as of Kantega SSO 3.5.0 and newer configures the name identifier claim by default.
- Or: Just add the claim manually to the relying party you already have. Usually easier in an existing environment.

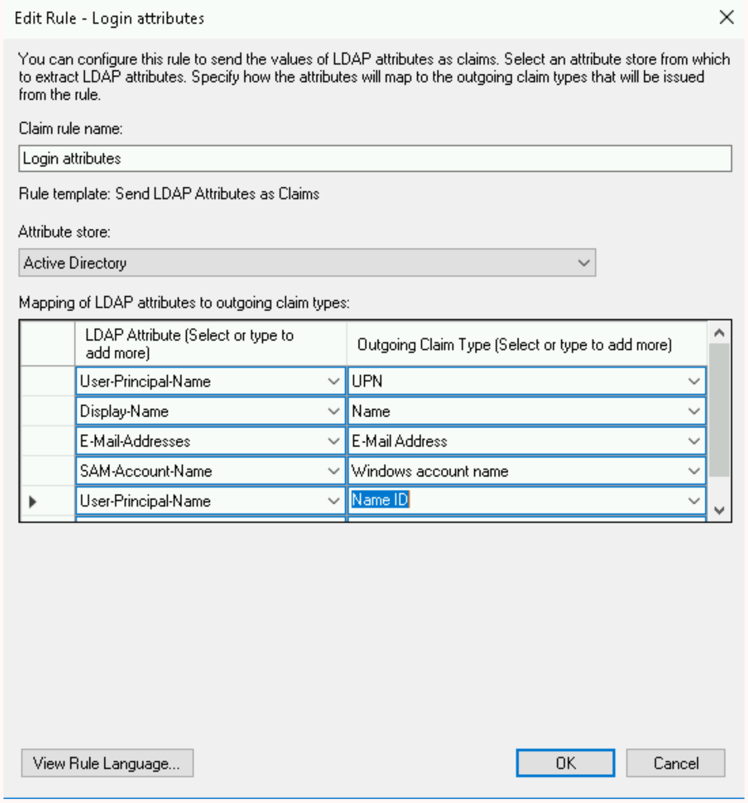
To add the claim manually (or check if the claim is already there or not if you're unsure of which version was used for initial setup), open the AD FS Management application on your Windows server and navigate to Relying Party Trusts. Locate and right click the relying party in question and "Edit Claim Issuance Policy":



1sicka2pag09c@servicedesk.example.com	Yes	WS-T...	https://servicedesk.example.com/plugins/servlet/no.kantega.saml
9q0bfq930bro@jira.example.com	Yes	WS-T...	https://jira.example.com/plugins/servlet/no.kantega.saml/sp/9q0b
1m5kmiwoihe58@issues.example.c			example.com/plugins/servlet/no.kantega.saml/sp/1
r5es8lju4z9b@documentation.exam			entation.example.com/plugins/servlet/no.kantega.sa
1ikwmvcuzcxba@crucible.example.			e.example.com/plugins/servlet/no.kantega.saml/sp/

Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help

In the next dialog, add "Name ID" as an outgoing claim as shown in the below screenshot.



Edit Rule - Login attributes

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:

Login attributes

Rule template: Send LDAP Attributes as Claims

Attribute store:

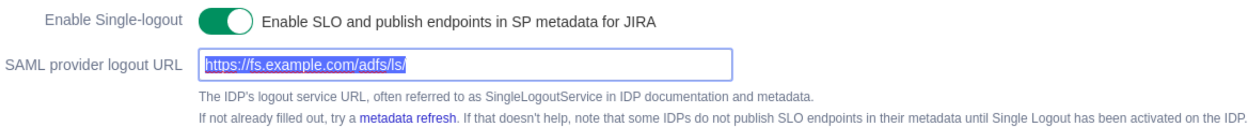
Active Directory

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)
User-Principal-Name	UPN
Display-Name	Name
E-Mail-Addresses	E-Mail Address
SAM-Account-Name	Windows account name
User-Principal-Name	Name ID

ADFS should now send the required name identifier claim, and you can enable SLO without breaking login.

Begin configuration by navigating to your ADFS IDP and select **Single Logout** from the navigation menu. As of Kantega SSO 3.5.0 The logout URL should be populated and you can enable Single Logout and click "Save":

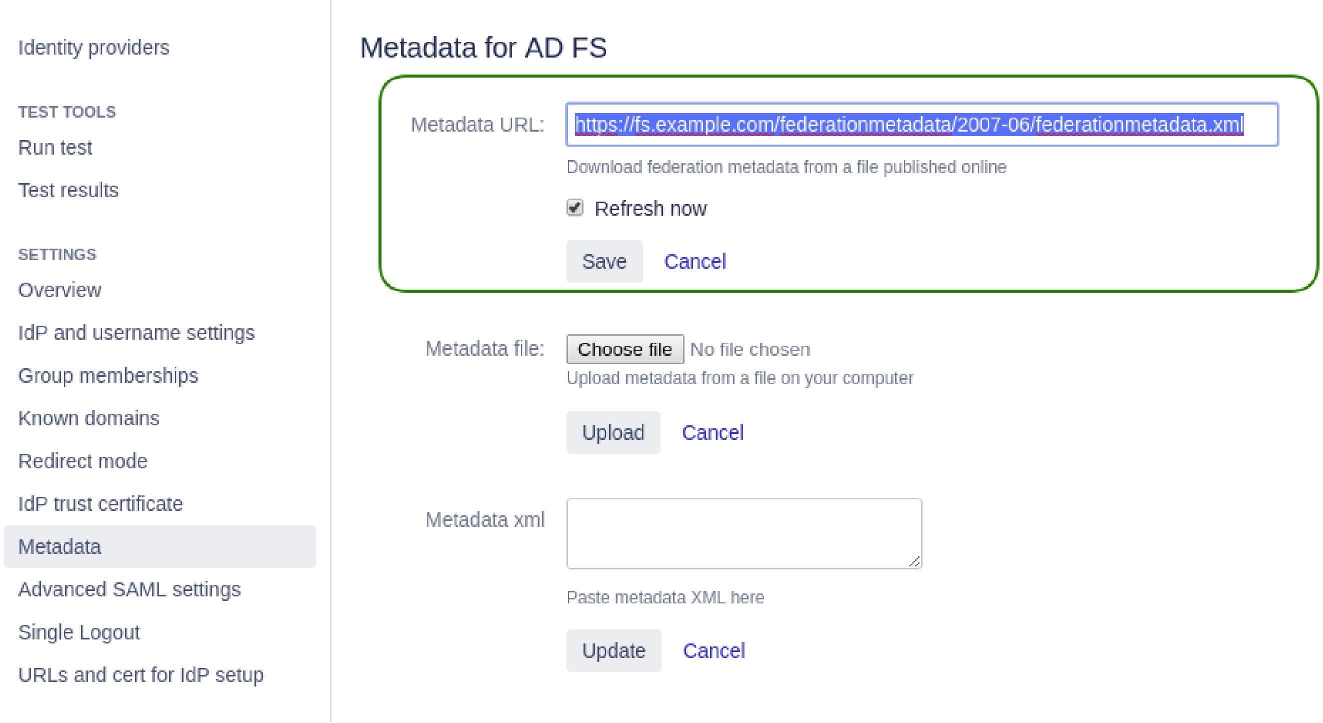


Enable Single-logout: Enable SLO and publish endpoints in SP metadata for JIRA

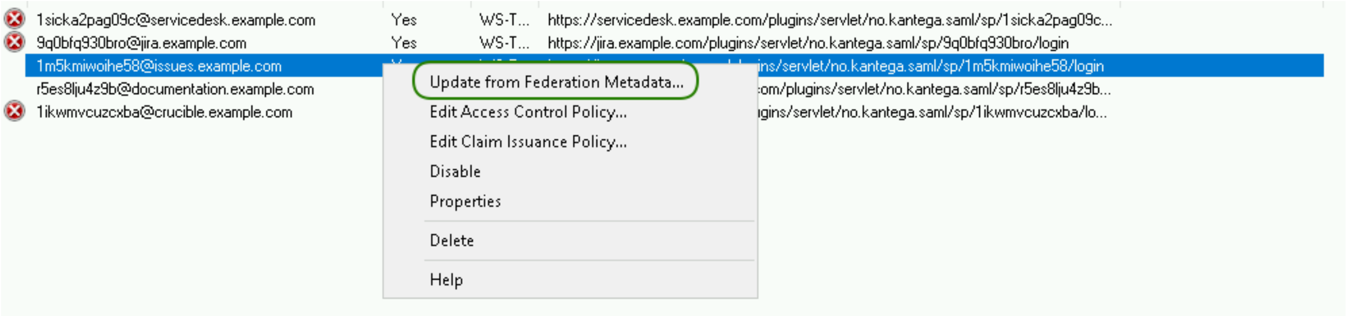
SAML provider logout URL: https://fs.example.com/adfs/ls/

The IDP's logout service URL, often referred to as SingleLogoutService in IDP documentation and metadata.
If not already filled out, try a metadata refresh. If that doesn't help, note that some IDPs do not publish SLO endpoints in their metadata until Single Logout has been activated on the IDP.

Read the following if the SAML provider logout URL for ADFS isn't already configured:

> If the ADFS logout URL isn't specified already, it's most likely becaues your configuration predates Kantega SSO 3.5.0 where this URL wasn't being imported yet. It needs to be configured before Single Logout will work. You can either fill it manually, or do a *metadata refresh* against ADFS to obtain it. To refresh from metadata, use the indicated link in the nav menu. The ADFS metadata URL should already be on file and all you should have to do is click save. You may optionally upload a file.
>
> 
>
>
>
> Metadata for AD FS
>
> Metadata URL: https://fs.example.com/federationmetadata/2007-06/federationmetadata.xml
> Download federation metadata from a file published online
> ☑ Refresh now
> Save Cancel
>
> Metadata file: Choose file No file chosen
> Upload metadata from a file on your computer
> Upload Cancel
>
> Metadata xml
> Paste metadata XML here
> Update Cancel
>
> Now go back to the Single Logout menu and if the logout URL is now populated, enable SLO and save.

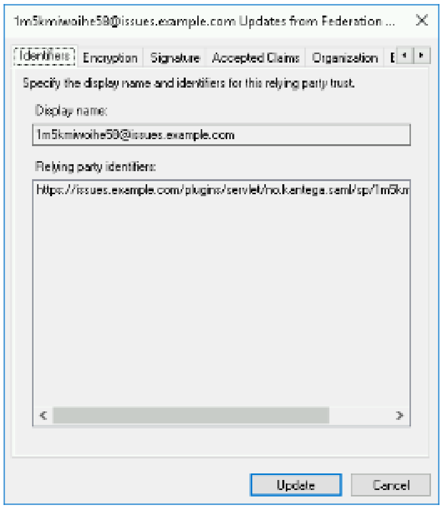
We next need to configure ADFS. This will also be done by doing a metadata refresh. Open the AD FS Management application and navigate to Relying Party Trusts. Find the relying party for your application and right click it for this menu:



1sicka2pag09c@servicedesk.example.com	Yes	WS-T...	https://servicedesk.example.com/plugins/servlet/no.kantega.saml/sp/1sicka2pag09c...
9q0bfq930bro@jira.example.com	Yes	WS-T...	https://jira.example.com/plugins/servlet/no.kantega.saml/sp/9q0bfq930bro/login
1m5kmiwoihe58@issues.example.com			ins/servlet/no.kantega.saml/sp/1m5kmiwoihe58/login
r5es8lju4z9b@documentation.example.com			om/plugins/servlet/no.kantega.saml/sp/r5es8lju4z9b...
1ikwmvcuzcxba@crucible.example.com			gins/servlet/no.kantega.saml/sp/1ikwmvcuzcxba/lo...

Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help

Click the Update button in the dialog that pops up.

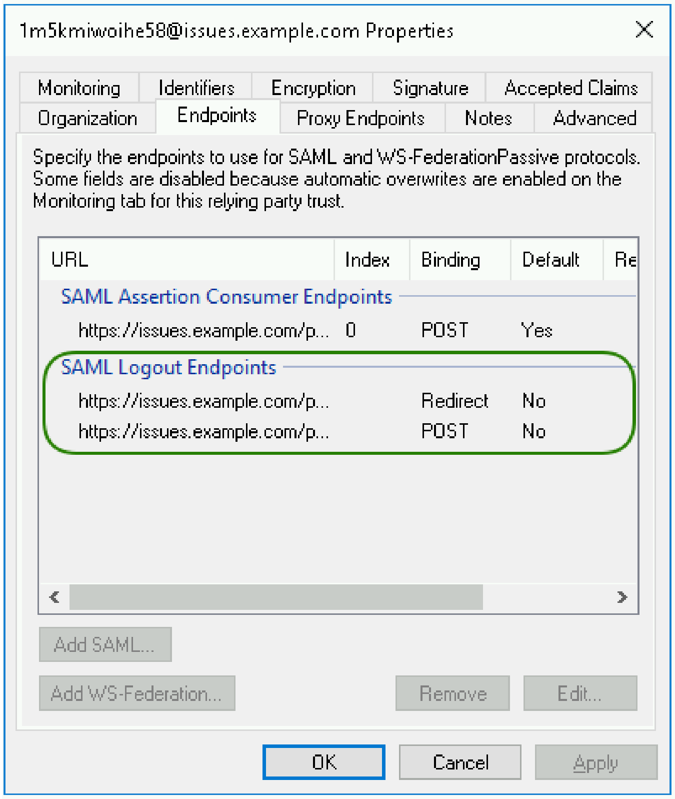

1m5kmiwoihe58@issues.example.com Updates from Federation ...

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

Display name: 1m5kmiwoihe58@issues.example.com

Relying party identifiers: https://issues.example.com/plugins/servlet/no.kantega.saml/sp/1m5km

To verify the import was successful, you may optionally right click the relying party again and this time select Properties. Navigate to the Endpoints tab and you should see that SAML Logout Endpoints have been detected:


1m5kmiwoihe58@issues.example.com Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols. Some fields are disabled because automatic overwrites are enabled on the Monitoring tab for this relying party trust.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://issues.example.com/p...	0	POST	Yes	
SAML Logout Endpoints				
https://issues.example.com/p...		Redirect	No	
https://issues.example.com/p...		POST	No	

Single Logout should now be enabled and working for new AD FS logins.

- Clicking *logout* from the Atlassian app should now also terminate the user's ADFS session.
- Users can also initiate logout from ADFS (IDP initiated logout), which will now also notify/terminate the Atlassian session (if initiated in the same browser - see section on caveats for more information).