

SLO: Azure AD

To configure Single logout in AAD, begin by enabling SLO in Kantega SSO from the **Single Logout** menu. As of Kantega SSO 3.5.0 the logout URL should be populated already and you can simply enable SLO and click save.

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

SAML provider logout URL

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 If that doesn't help, note that some IDPs do not publish SLO endpoints in their metadata until Single Logout has been activated on the IDP.

If the SAML provider logout URL for AAD isn't already configured, this must be configured first:

If the AAD logout URL isn't specified already, you will either need to input this directly in the form Single Logout configuration input, or refresh AAD metadata which we'll do here.

Common Kerberos **SAML** User provisioning

Identity providers

TEST TOOLS
Run test
Test results

SETTINGS
Overview
IdP and username settings
Group memberships
Known domains
Redirect mode
IdP trust certificate
Metadata
Advanced SAML settings
Single Logout
URLs and cert for IdP setup

Single Logout configuration for Azure AD

i We've noticed you're also using Kerberos. Note that SAML Single Logout won't be used for Kerberos sessions. To enable SAML Single Logout for Azure AD, logout URLs for the SP must be configured in the IDP and vice versa.

- If the IDP supports metadata import, the easiest way to configure SLO is to enable SLO here, then perform a metadata import on both sides. You can [refresh IDP metadata here](#) (or use the left menu).
- SLO endpoints for JIRA are not exposed in metadata until SLO has been enabled here.
- Some IDPs similarly don't expose their SLO endpoints until SLO has been configured on the IDP side.
- The service provider information you need to configure the IDP can be found under [URLs and cert for Idp setup](#) (or use left menu).

See our [setup guides](#) for more information.

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

SAML provider logout URL

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 If that doesn't help, note that some IDPs do not publish SLO endpoints in their metadata until Single Logout has been activated on the IDP.

Navigate to the **Metadata** menu. If the metadata URL is already filled you can simply click Save to do the refresh.

Common Kerberos **SAML** User provisioning

Identity providers

TEST TOOLS
Run test
Test results

SETTINGS
Overview
IdP and username settings
Group memberships
Known domains
Redirect mode
IdP trust certificate
Metadata
Advanced SAML settings
Single Logout
URLs and cert for IdP setup

Users and group syncing

Metadata for Azure AD

Metadata URL:

Download federation metadata from a file published online

Refresh now

Metadata file: No file chosen

Upload metadata from a file on your computer

Metadata xml

Paste metadata XML here

Otherwise, you will first need to either obtain the "App Federation Metadata Url", or upload "Federation Metadata XML" as a file (or use XML cut&paste) from AAD. This can be obtained via the AAD management portal. Log into <https://portal.azure.com> then navigate to Azure Active Directory >> Enterprise Applications >> *Atlassian app*. Then select *Single Sign-on* from the menu.

3

SAML Signing Certificate

Status	Active
Thumbprint	1927E74B8171C648C37679B610AE86684DD07F20
Expiration	24/02/2022, 22:26:53
Notification Email	admin@kantegasso.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/9fe0273d-5bd6-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

After refreshing metadata, the Single Logout menu page should have a logout URL and you can enable SLO and continue with setup.

Once SLO has been enabled and the AAD logout URL configured, you now have partial Single Logout (IDP): Users can click "Logout in" the Atlassian app and be signed out of the app and the IDP. The user will land on AAD's logout confirmation page.

Configuring a Logout URL for the service provider (**does not work with AAD currently**)

A logout URL can optionally be configured for each SP (e.g. Jira, Confluence) in AAD. This should enable real but **it does not work**. AAD correctly notifies one session participant but won't accept LogoutResponse messages from that entity on its own endpoint, so the protocol breaks down. It works as a basic return URL as long as there is only a **single session** participant, which is pretty much useless..

- If **omitted**, the initiating service provider is never sent a LogoutResponse at the end of single logout. The user is then signed out of the Atlassian app and AAD, and lands on AAD's logout confirmation page. This works because Kantega SSO terminates the session on the way out and doesn't actually require the LogoutResponse for anything other than to "landing" the user somewhere.
- If **included**, the AAD sends a LogoutResponse back to the initiating SP at the end of single logout. The user is signed out of the IDP and SP as above, but instead lands on the Atlassian app's logout confirmation page.

Locate the Basic SAML configuration card and click to edit.

issues.example.com - SAML-based sign-on

Enterprise Application

Overview Getting started Deployment Plan Manage Properties Owners Users and groups **Single sign-on** Provisioning Self-service

Change single sign-on mode Switch to the old experience Test this application

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating issues.example.com.

1 Basic SAML Configuration

Identifier (Entity ID)	https://issues.example.com/plugins/servlet/no.kantega.saml/s/p/ee6mqgwkp07c/login
Reply URL (Assertion Consumer Service URL)	https://issues.example.com/plugins/servlet/no.kantega.saml/s/p/ee6mqgwkp07c/login
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

To fill the logout URL, either save Service Provider Metadata from Kantega SSO (Obtained from "URLs and cert for IDP setup") and upload to AAD as shown below, or simply cut&paste the Logout URL manually.

Basic SAML Configuration

Save Upload metadata file

Identifier (Entity ID) (Required)

This value must be unique across all applications in your (Azure Active Directory) tenant. It should follow one of the patterns provided below the textbox.

Patterns: https://*.kantega.org/plugins/servlet/no.kantega.saml/sp/h823t5iafcv/login

Reply URL (Assertion Consumer Service URL) (Required)

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML. It should follow one of the patterns provided below the textbox.

Patterns: https://*.kantega.org/plugins/servlet/*

Sign on URL (Optional)

This URL contains the sign-in page for this application that will perform the service provider-initiated single sign-on. It should follow one of the patterns provided below the textbox. Leave it blank if you want to perform identity provider initiated single sign-on.

Relay State (Optional)

Optionally, a SAML RelayState parameter can be provided. The RelayState instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout URL (Optional)

This URL is used to send the SAML Logout response back to the application.