Bamboo Health

OpenBeds SSO Integration

Internal / External	External
Update Date	01/14/2022
Last Updated By:	Emily Hunter

Purpose

Provides information and steps to federate OpenBeds with external entities through OIDC or SAML SSO.

Configuration Details

Entity ID (Prep)	urn:amazon:cognito:sp:us-east-1_cpSbfkXsl
Reply URL	https:// sso.prep.openbeds.net/saml2/idpresponse
Entity ID (Production)	urn:amazon:cognito:sp:us-east-1_43Rcqm7mi
Reply URL	https:// sso-prod-prod.openbeds.net/saml2/idpresponse

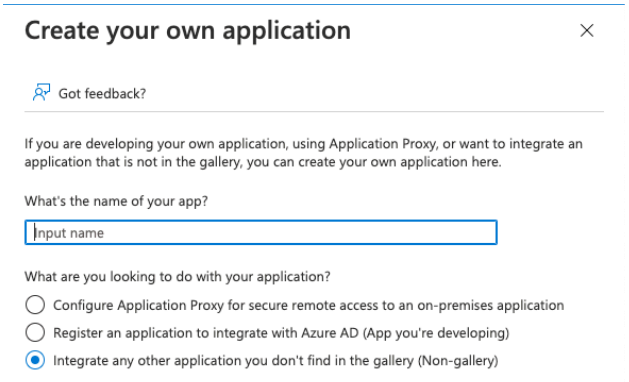
Information

Provides information and steps to federate OpenBeds with external entities through OIDC or SAML SSO. The configuration documented is for configuring single sign on with Azure AD.

Organization Instructions

Navigate to the following screen:

Azure Active Directory -> Enterprise Applications -> New application -> Create your own application



Create your own application

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

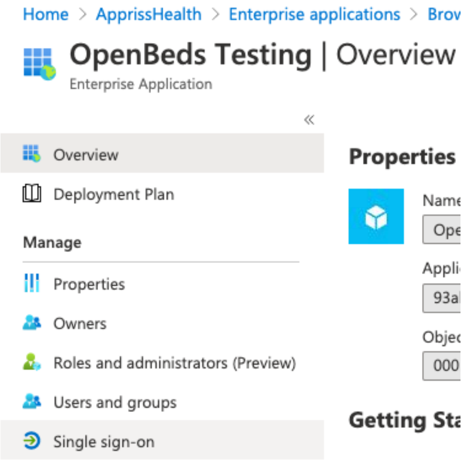
What's the name of your app?

Input name

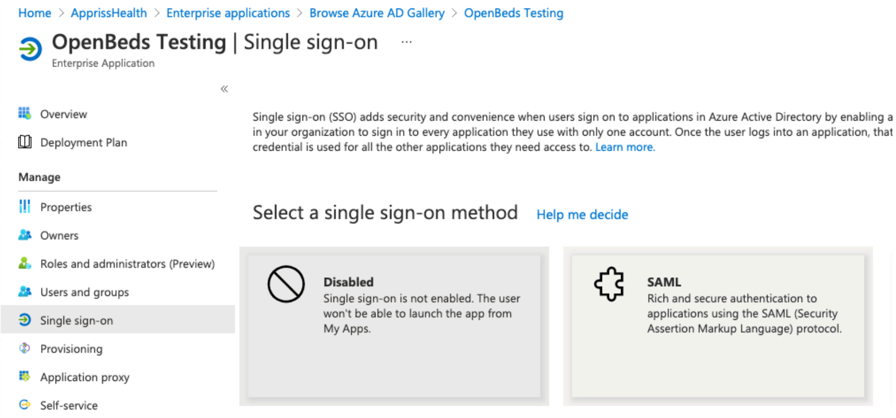
What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

On the Overview screen, select Single sign-on



Then select SAML



Home > ApprissHealth > Enterprise applications > Browse Azure AD Gallery > OpenBeds Testing
OpenBeds Testing | Single sign-on ···
Enterprise Application
«
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

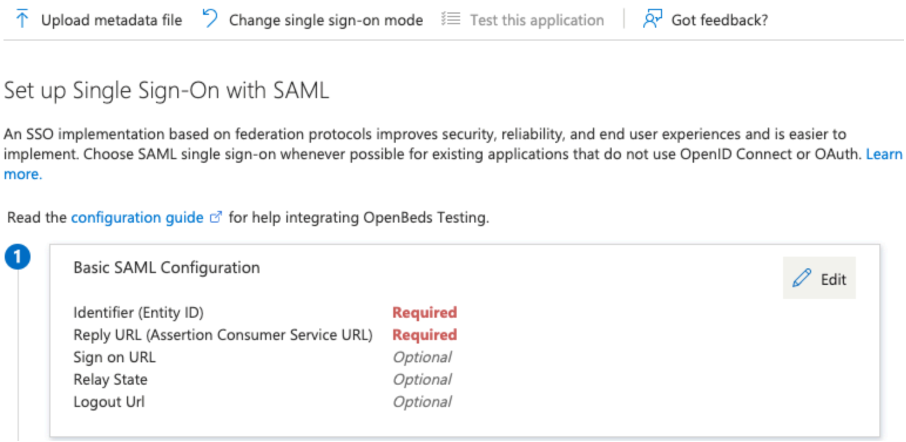
Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Select Edit on the Basic SAML Configurations panel:



Set up Single Sign-On with SAML

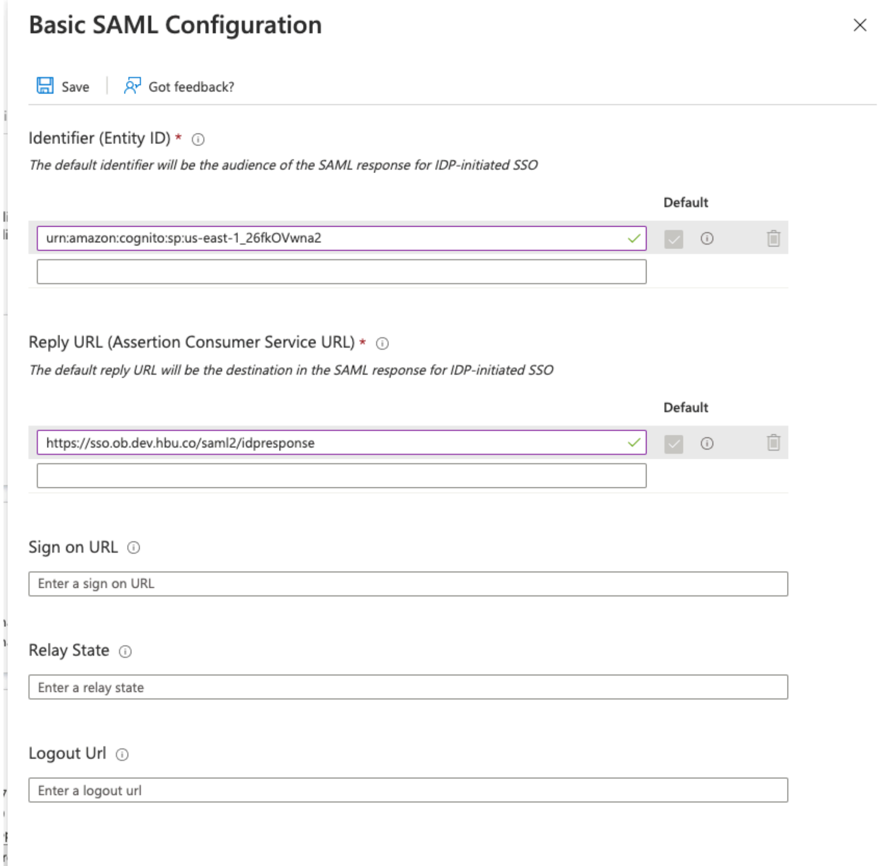
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating OpenBeds Testing.

1 Basic SAML Configuration

Identifier (Entity ID)	**Required**
Reply URL (Assertion Consumer Service URL)	**Required**
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

On the configuration screen. Input the Entity ID and the Reply URL for the environment you are configuring (dev, qa, prep, or production). Select save



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

urn:amazon:cognito:sp:us-east-1_26fkOVwna2

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://sso.ob.dev.hbu.co/saml2/idpresponse

Sign on URL

Enter a sign on URL

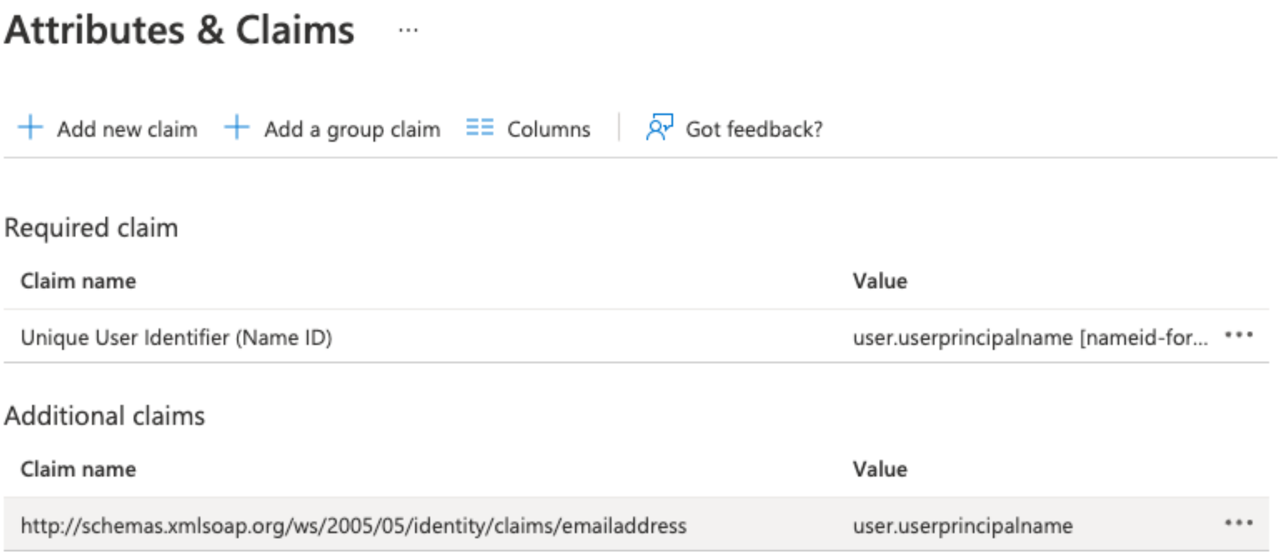
Relay State

Enter a relay state

Logout Url

Enter a logout url

Select edit on Attributes & Claims. Depending upon how users are created within your organization, you may or may not need to change any settings on this page. The important option is to ensure the following claim name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress) contains the user’s email address:



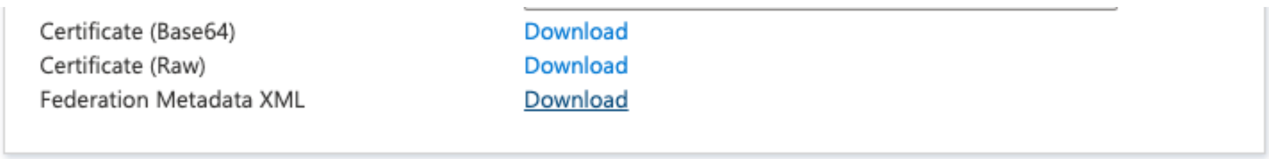
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... •••

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.userprincipalname •••

Finally, please select download under Federation Metadata XML. You will need to provide this file to Bamboo Health to complete the federation:



Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Appendix A

SAML 2.0 Support

Does Bamboo Health support SAML 2.0 SSO?	Yes
Does Bamboo Health support IdP-initiated Single Sign-on?	No
Does Bamboo Health support SP-initiated Single Sign-on?	Yes
Does Bamboo Health require SP-initiated Single Sign-on?	Yes
Does Bamboo Health support SAML 2.0 HTTP-POST Bindings?	For receipt of AuthnResponse
Does Bamboo Health accept a digital signature with the SAML Assertion?	Yes
Does Bamboo Health require that the signing certificate be an externally hosted and trusted Certificate Authority (CA)?	Bamboo will pin to the signing certificate present in the metadata – it can be a self-signed certificate generated for SAML purposes or a certificate signed by a trusted root CA
Does Bamboo Health support encrypting the AuthnResponse message?	No
Does Bamboo Health support Single Log-out?	No
Will Bamboo Health non-production environments accessible?	Bamboo may request integrations with the following non-production environments: • Development – for Bamboo's internal development of the system

	• QA – for Bamboo’s QA engineers to perform pre-release tests • Prep – for Bamboo and our partner to perform user acceptance testing Bamboo will request these environments be configured against an IdP where Bamboo employees can create accounts for testing.
What are the SLOs for non-production SAML systems?	Bamboo does not provide a customer facing SLO for development or QA SAML environments. Bamboo will ensure that the prep environment is available for regularly scheduled user acceptance testing.
What is the SLO for production SAML systems	99.9%