SAML SSO Integration

SAML (Security Assertion Markup Language)

SAML is an XML standard that allows you to exchange user authentication and authorization information between web domains.

Artifactory offers a SAML-based Single Sign-On service allowing federated Artifactory partners (identity providers) full control over the authorization process.

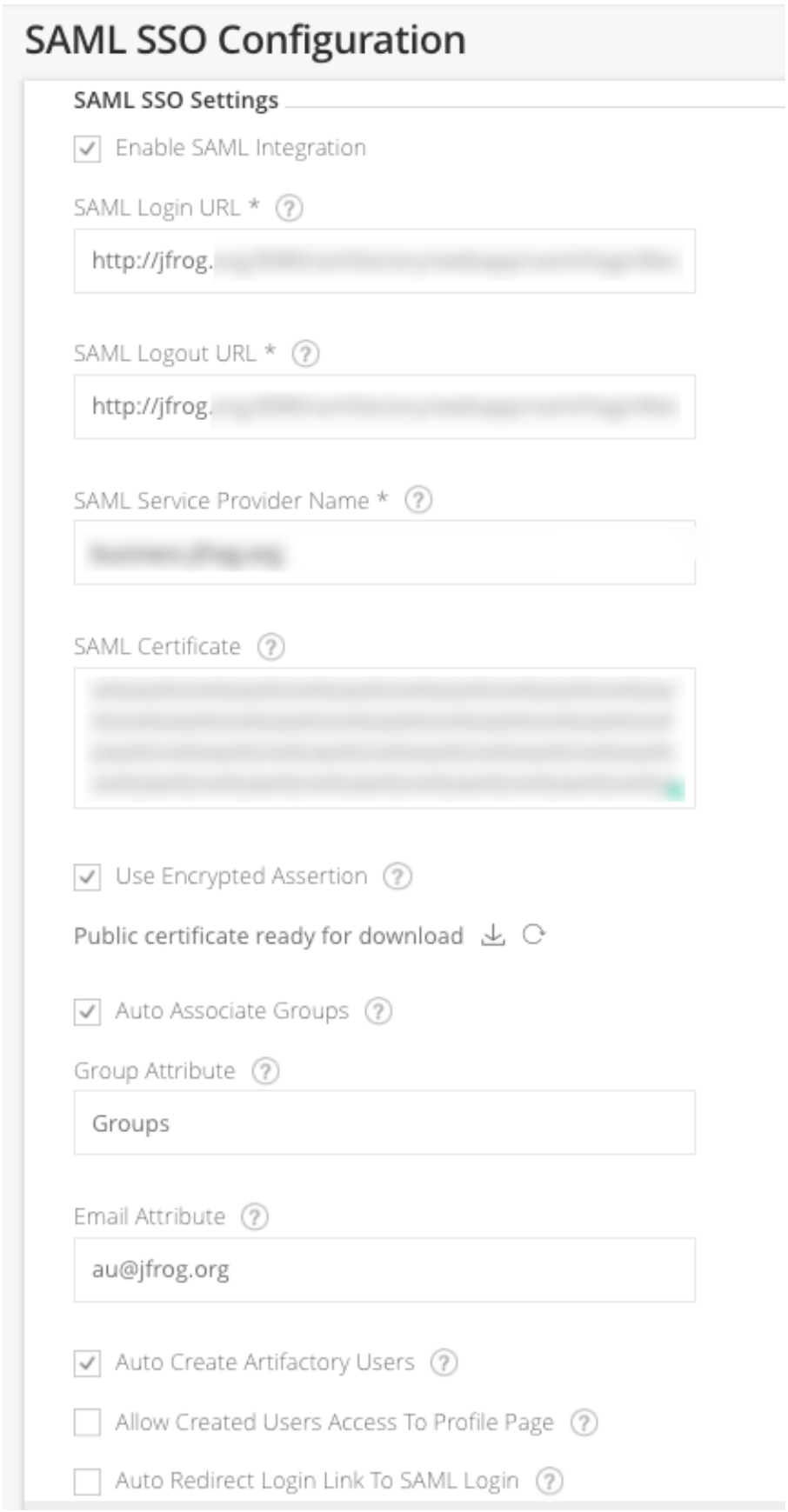
Using SAML, Artifactory acts as service provider which receives users' authentication information from external identity providers.

In this case, Artifactory is no longer responsible for authentication of the user although it still has to redirect the login request to the identity provider and verify the integrity of the identity provider's response.

Page Contents

Artifactory's SAML configuration

SAML SSO integration is configured in the **Admin** module under **Security | SAML SSO.**



Enable SAML Integration	When checked, SAML integration is enabled and users may be authenticated via a SAML server.

SAML Login URL	The SAML login URL.
SAML Logout URL	The SAML logout URL.
SAML Service Provider Name	The SAML service provider name. This should be a URI that is also known as the entityID, providerID, or entity identity. For more details, see section 8.3.6 of the SAML v2 specification.
Use Encrypted Assertion	When set, an X.509 public certificate will be created by Artifactory. Download this certificate and upload it to your IDP and choose your own encryption algorithm. This process will let you encrypt the assertion section in your SAML response.

Auto Associate Groups	When set, in addition to the groups the user is already associated with, he will also be associated with the groups returned in the SAML login response.
	
	Note that the user's association with the returned groups is not persistent. It is only valid for the current login session in the browser (i.e. this will not work for logins using the SAML user id and API Key).
	
	Also, the association will not be reflected in the UIs Groups settings page. Instead, you can see this by enabling this SAML logger in your *$ARTIFACTORY_HOME/etc/logback.xml* file as follows:
	
	`<logger name="org.artifactory.addon.sso.saml">`
	`  <level value="debug"/>`
	`</logger>`

Group Attribute	The group attribute in the SAML login XML response. Note that Artifactory will search for a case-sensitive match to an existing group.
Email Attribute	If **Auto Create Artifactory Users** is enabled or an internal user exists, Artifactory will set the user's email to the value in this attribute that is returned by the SAML login XML response.
SAML Certificate	The X.509 certificate that contains the public key.
Auto Create Artifactory Users	When checked, for new users accessing Artifactory for the first time via SAML, Artifactory will create a user that will persist in the data base.
Allow Created Users Access To Profile Page	When checked, users created after authenticating using SAML, will be able to access their profile. This means they are able to generate their API Key. If *Auto Create Artifactory Users* is enabled, once logging into Artifactory, users can set their password for future use.
Auto Redirect Login Link to SAML Login	When checked, clicking on the login link will direct the users to the configured SAML login URL.

To use SAML-based SSO in Artifactory:

1. Login to Artifactory with administrator privileges.
2. In the **Admin** module, go to **Security | SAML SSO.**
3. Enable the SAML integration by checking the **Enable SAML Integration** checkbox.
4. Enable or disable "Auto Create Artifactory users" (Using SAML login). If enabled, new users will persist in the database.
5. Enable or disable "Allow Users Access to Profile Page". If enabled users will be able to access their profile without having to provide a password.
6. Provide the **SAML Login URL** and **SAML Logut URL**

> **SAML Logout URL**
>
> In order to simultaneously logout from your SAML provider and Artifactory, you need to correctly set your provider's logout URL **SAML Logout URL** field. Setting this incorrectly will keep your users logged in with the SAML provider even after logging out from Artifactory.

7. Provide the service provider name (Artifactory name in SAML federation)
8. Provide the X.509 certificate that contains the public key. The public key can use either the DSA or RSA algorithms. Artifactory uses this key to verify SAML response origin and integrity. Make sure to match the embedded public key in the X.509 certificate with the private key used to sign the SAML response.

> **Custom URL base**
>
> For your SAML SSO settings to work, make sure you have your Custom URL Base configured.

Signed and encrypted Assertions

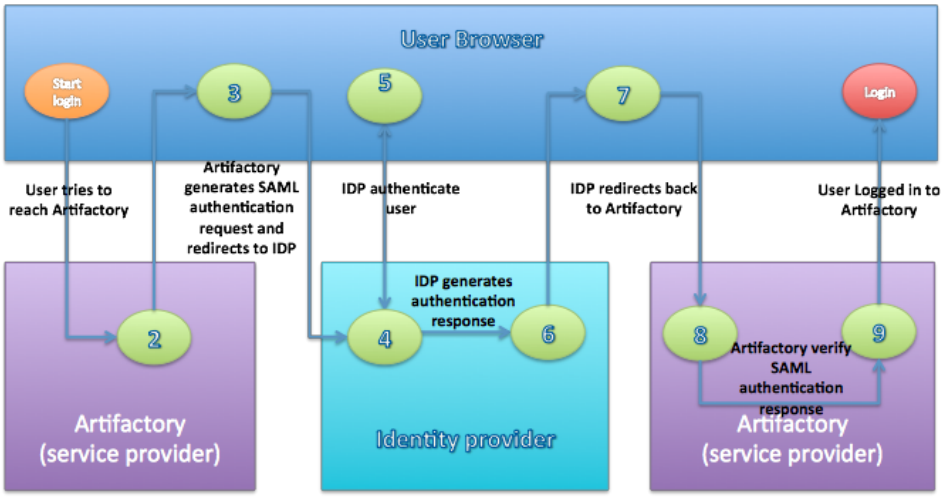
1. Please make sure your SAML IdP (Identity Provider) provides a signed login Assertion - this is mandatory for the Assertion verification by Artifactory.

2. Signed Logout is also currently unsupported by Artifactory.

Understanding Artifactory's SAML-based SSO Login Process

1. The user attempts to reach a hosted Artifactory, Home Page.
2. Artifactory generates a SAML authentication request.
3. The SAML request is encoded and embedded into the identity provider URL.
4. Artifactory sends a redirect to the user's browser. The redirect URL includes the encoded SAML authentication request that should be submitted to the identity provider.
5. The identity provider decodes the SAML message and authenticates the user. The authentication process can proceed by asking for valid login credentials or by checking for valid session cookies.
6. The identity provider generates a SAML response that contains the authenticated user's username. In accordance with the SAML 2.0 specification, this response is digitally signed with the identity provider's private DSA/RSA keys.
7. The identity provider encodes the SAML response and returns that information to the user's browser. The identity provider redirects back to Artifactory with the signed response.
8. Artifactory's ACS verifies the SAML response using the partner's public key. If the response is successfully verified, the ACS redirects the user to the destination URL.
9. The user has been redirected to the destination URL and is logged in to Artifactory.

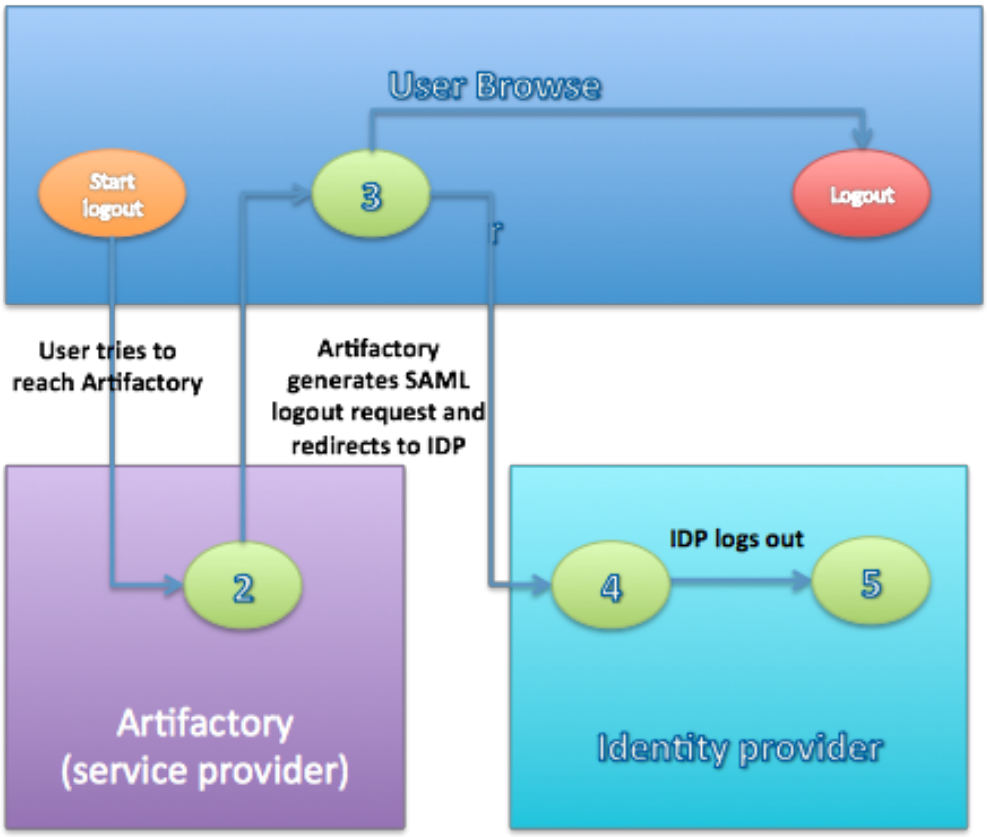
Figure (2) Artifactory's SAML-based SSO login process.



Understanding the Artifactory's SAML-based SSO Logout Process

1. The user attempts to reach a hosted Artifactory logout link.
2. Artifactory logs the client out and generates a SAML logout request.
3. Artifactory redirects to the identity provider with the encoded SAML logout request.
4. The identity provider decodes the SAML message and logs the user out.
5. The user is redirected to the configured URL in the identity provider.

Figure (3) Artifactory's SAML-based SSO logout process.



Artifactory Profiles and Bindings

Artifactory currently supports the Web Browser SSO and Single Logout Profiles.

The Web Browser SSO Profile uses HTTP redirect binding to send the AuthnRequest from the service provider to the identity provider, and HTTP POST to send the authentication response from the identity provider to the service provider.

Similar to the previous profile, the Single Logout Profile uses HTTP redirect binding to send the LogoutRequest from the service provider to the identity provider and HTTP POST to send the logout response from the identity provider to the service provider.

If your IDP supports uploading service provider metadata, you can use the following metadata XML:

Figure (4) Artifactory's service provider metadata XML.

Artifactory SP metadata XML

```
<ns2:EntityDescriptor xmlns="http://www.w3.org/2000/09/xmldsig#" xmlns:ns2="urn:oasis:names:tc:SAML:2.0:
metadata"          entityID="<SP_NAME_IN_FEDERATION>">
        <ns2:SPSSODescriptor WantAssertionsSigned="true" AuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                <ns2:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</ns2:NameIDFormat>
                <ns2:AssertionConsumerService index="1" Location="<ARTIFACTORY_URL>/webapp/saml
/loginResponse" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        </ns2:SPSSODescriptor>
</ns2:EntityDescriptor>
```

NOTE! that to use the service provider metadata:

Do not forget to update the following fields in the service provider metadata XML:

- entityID - Artifactory's ID in the federation. Must match SAML Service Provider Name in Artifactory's SAML configuration page.
- Location - Artifactory's home URL

After SAML Setup

Using SAML, Artifactory automatically redirects the request to IDP which Authenticates the user and after a successful login redirects back to Artifactory.

If "Anonymous User" is enabled, Artifactory doesn't have to authenticate the user therefore it doesn't redirect to the IDP. If the user still wants to sign in through SAML, they can do so by clicking the "SSO login" link in the login page.

Login Failure

In case of IDP failover or bad configuration, Artifactory allows you to bypass SAML login by using Artifactory login page:

http://<ARTIFACTORY_URL>/webapp/#/login

This URL can be used by internal users who need to log in directly to Artifactory.

Using API Key with SAML Users

While SAML provides access to Artifactory UI, it is also possible for SAML users to generate an API key that can be used instead of a password for basic authentication or in a dedicated REST API header, this is very useful when working with different clients, e.g. docker, npm, maven, etc. or using Artifactory REST API.

In order to allow SAML users access to an API key you will need to make sure that the "**Auto Create Artifactory Users**" and "**Allow Created Users Access To Profile Page**" check boxes are checked. This means that SAML users are also saved in Artifactory database and can access their profile page in order to generate, retrieve and revoke their API key.