SAML Options

SAML (Security Assertion Markup Language) enables you to access multiple web applications using one set of login credentials. This is also known as SSO (Single Sign-On).

Appvance AIQ supports SAML 2.0 protocol SSO. Appvance behaves as an application or service provider in a SAML SSO architecture.

It has been tested against SAML identity providers, including Okta (>http://okta.com) and Auth0 (>https://auth0.com/) and Akamai (>https://www.akamai.com/).

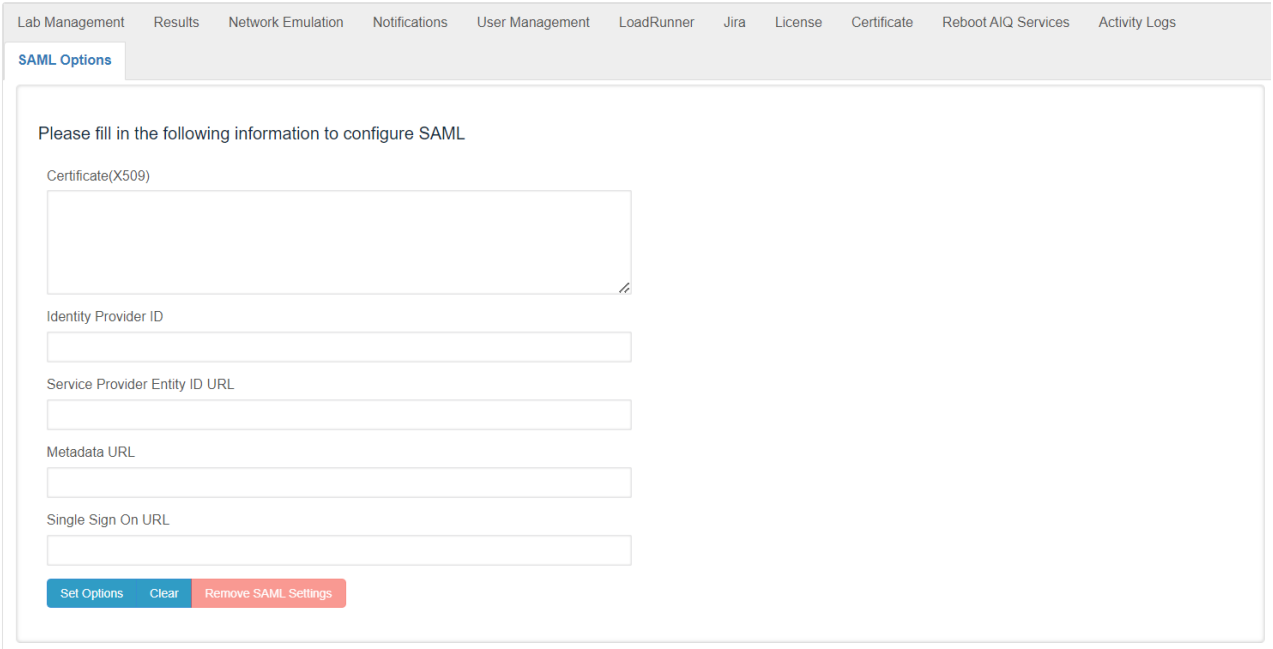
Full SAMLv2 specs can be found here >http://saml.xml.org/saml-specifications

Security overview of SAMLv2: >http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

Configuring SSO

When using SSO the standard login still applies. Only the appvance owner user can enable SSO.

1. Login to AIQ as an administrator user.
2. Navigate to **Global Options** > **Admin Options** > **SAML Options**.
3. There you can define the SAML configuration



4. Every field is required. Following are the specs for each field. Configure the following fields:
   - **Certificate (X.509)** - This is the certificate of SAML usually they have the next format
     `-----BEGIN CERTIFICATE----- ... -----END CERTIFICATE-----`
   - **Identity Provider ID** - An Identity Provider is a federation partner that vouches for the identity of a user. The Identity Provider authenticates the user and provides an authentication token (that is, information that verifies the authenticity of the user)
   - **Service Provider Entity ID URL** - This is a service name configured in the SAML IDP. This is very important as SAML is a security environment, Appvance needs to have knowledge of the IDP endpoint but also IDP needs to be aware of SAML existence.
     Appvance uses the Service Provider Entity ID URL (also called audience restrictions) as the consumer URL.
   - **Metadata URL** - Some SAML IDP provides some configuration requirements, usually in a metadata URL. IF the IDP does not provide this field, you can use Single Sign-On URL
   - **Single Sign-On URL** - This is the URL the user will be redirected to if they choose to
5. Upon setting the values, the welcome page SSO button will become enabled. By default, it is disabled.
6. The SSO user's role is always “User”. They will start with the string “sso.” and the username provided by the SAML IDP service.

Configuring your the Identity Provider

You will need to provide the following URL to the Identity Provider that points to your AIQ controller server (app service provider):

`https://<aiq controller DNS or IP>:8443/AppvanceServer/saml`

Last updated: October 16, 2026

Revision #6
Created 2026-07-31 16:29:21 UTC by Admin
Updated 2026-10-16 19:47:11 UTC by mmora