

Admin Options

- [Admin Options](#)
- [Results](#)
- [Network Emulation](#)
- [Notifications](#)
- [Legacy LoadRunner Administration Settings](#)
- [Jira Integration Administration](#)
- [License](#)
- [Certificate](#)
- [Reboot AIQ Services](#)
- [Activity Logs](#)
- [SAML Options](#)

Admin Options

The Admin Options page gives you access to various AIQ system administration functions. Each function is described in separate topics within this section.

These functions are restricted to users with Administrator level access.

Last updated: July 10, 2023

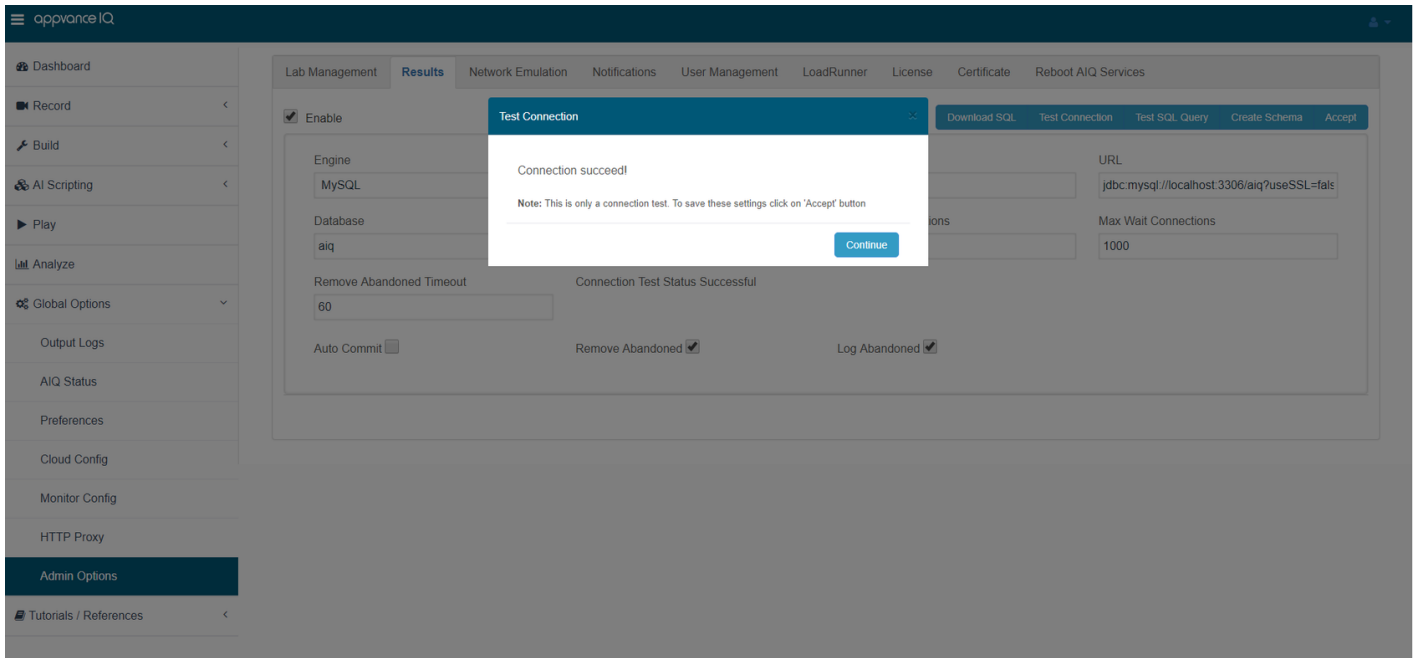
If you have any feedback on this topic, please contact us at documentation@appvance.ai

Results

Appvance IQ uses a relational database (RDBMS) for its Repository. AIQ logs every test operation, test step, and monitored resource to the Repository. AIQ supports MYSQL and Oracle databases. It is required to configure the databases to store the results. The results page has the option to configure these databases in Appvance IQ.

Configuring Database as Results Repository

1. Start Appvance IQ and login to Appvance IQ as an Administrator
2. Select the Admin Options tab from the Global Options
3. Select the Results tab
4. Click Enable check-box for all the options to show
5. Select MySQL or Oracle under Engine depending on what database needs to be configured
6. Provide valid user names and passwords for the database
7. URL of MYSQL or Oracle by default would be
'jdbc:mysql://localhost:3306/aiq?useSSL=false' or 'jdbc:oracle:thin:@localhost:1521:aiq'
respectively. When the database is installed and configured in the same instance as the controller machine, then localhost could be used but has to be changed to a different DNS depending on the database URL.
An AWS RDS instance Endpoint URL would look like this: sqlserver.c7nn5t4czzya.us-west-2.rds.amazonaws.com
8. Provide the valid name of the database
9. Click Accept to see the changes being saved successfully
10. All other fields can be left as default
11. Click 'Test Connection' to see the message Connection Succeed!



Last updated: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Network Emulation

Use the **Network Emulation** page to enable or disable the use of network emulating for testing with AIQ. Test parameters such as bandwidth and latency can be configured from here.

Lab Management

Results

Network Emulation

Notifications

User Management

LoadRunner

Jira

License

Certificate

Activity Logs

SAML Options

Test Designer Network Emulation Settings

Network Emulation is Disabled

Enable

Set Network Bandwidth (0 for unlimited)

kbps

Set Kbps

Set Latency (0 for no latency)

ms

Set Latency

Set Inject

☒Inject js

Network emulation is a technique for testing the performance of real applications over a virtual network. This is different from network simulation where virtual models of traffic, network models, channels, and protocols are applied. The aim is to assess performance, predict the impact of change, or otherwise optimize technology decision-making.

From [Wikipedia article on Network Emulation](#)

Last updated: July 10, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Notifications

Use the **Notifications** page to determine which users receive notifications from the system.

Lab Management

Results

Network Emulation

Notifications

User Management

LoadRunner

Jira

License

Certificate

Reboot AIQ Services

Activity Logs

SAML Options

Email Notification Settings

Accept

Username

appvance

Password

appvance

Host

test

Port

8443

☐ SSH

Last updated: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Legacy LoadRunner Administration Settings

Last reviewed: September 29, 2026

Use this page only when maintaining AIQ administration settings for environments that still execute LoadRunner assets.

What changed in this article

- Marked LoadRunner Admin as legacy administration content.
- Added checks for installation path, license availability, execution node access, environment variables, result storage, and permissions.
- Connected admin setup to the LoadRunner execution article so configuration is validated with a real test run.

Validation workflow

1. Confirm the LoadRunner installation and license details with the tool owner.
2. Configure AIQ paths, node access, and environment settings needed for execution.
3. Run a controlled LoadRunner script and verify AIQ can collect the expected results.

Review note: This page now keeps admin settings separate from script creation and execution guidance.

Last updated: September 29, 2026

If you have feedback on this topic, contact documentation@appvance.ai.

Jira Integration Administration

Use the Jira administration screen to maintain your integration with Atlassian Jira.

1. From AIQ navigate to **Global Options > Admin Options**.
2. Select the **Jira** tab.

The screenshot displays the 'Jira' tab in the 'Admin Options' section. The interface includes a top navigation bar with tabs: Lab Management, Results, Network Emulation, Notifications, User Management, LoadRunner, Jira (selected), License, Certificate, Activity Logs, and SAML Options. The main content area is divided into several sections:

- Jira Configuration:** A dropdown menu labeled 'Select a Configuration'.
- Configuration Name:** A text input field.
- Service Type:** A dropdown menu currently set to 'Jira Cloud'.
- Authentication:** Fields for 'Host' (http://id.atlassian.com/), 'Username', and 'Token' (masked with asterisks), along with a 'Connect' button.
- Project Setup:** A 'Projects' dropdown menu and a 'Load Issue Types' button.
- Issue Type Setup:** Fields for 'Issue Types', 'Transition On Failure', and 'Transition On Success', each with a dropdown menu.
- Table:** A table with columns 'Jira Field', 'Name', and 'Value'. It has an '+Add Row' button at the bottom right.

See [Integration with Atlassian Jira for information on configuring Jira.](#)

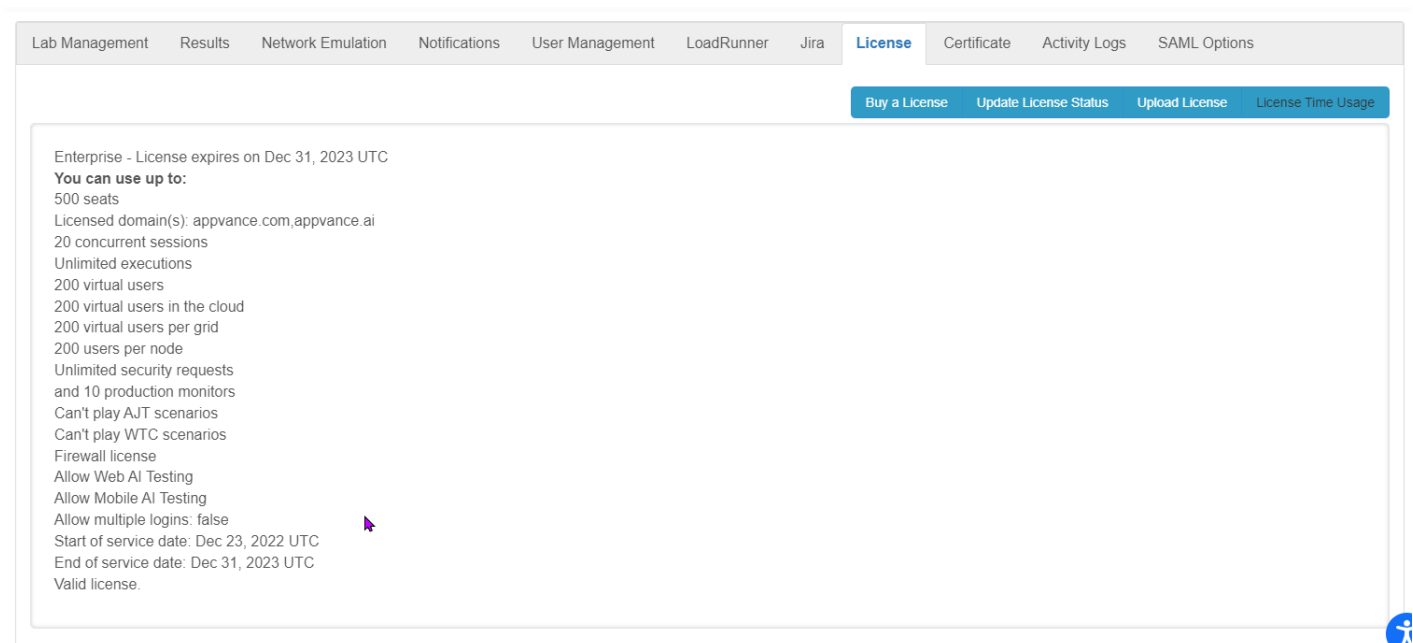
Last updated: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

License

Appvance delivers the free trial version of Appvance IQ with a simple commercial license with:

- 100 virtual user minutes for 15 days with 5 virtual users
 - 5 virtual users in the cloud
 - 5 virtual users in the grid
 - 5 users per node
- 100 security requests
- 50 production monitors with no access to run any Appvance AI
- Access to Appvance support
- Access to resources such as:
 - Appvance User Guide
 - Training videos
 - Confluence wiki and Knowledge Bases



The screenshot shows the Appvance web interface with a navigation bar at the top containing links: Lab Management, Results, Network Emulation, Notifications, User Management, LoadRunner, Jira, License (highlighted), Certificate, Activity Logs, and SAML Options. Below the navigation bar is a sub-menu for the License page with options: Buy a License, Update License Status, Upload License, and License Time Usage. The main content area displays the following license details:

Enterprise - License expires on Dec 31, 2023 UTC
You can use up to:
500 seats
Licensed domain(s): appvance.com, appvance.ai
20 concurrent sessions
Unlimited executions
200 virtual users
200 virtual users in the cloud
200 virtual users per grid
200 users per node
Unlimited security requests
and 10 production monitors
Can't play AJT scenarios
Can't play WTC scenarios
Firewall license
Allow Web AI Testing
Allow Mobile AI Testing
Allow multiple logins: false
Start of service date: Dec 23, 2022 UTC
End of service date: Dec 31, 2023 UTC
Valid license.

Accessing the Licenses page requires Administrator level access.

The following options are available from this page:

- **Buy a License** opens the [Appvance](#) website. From there you can contact Appvance Support to investigate licensing details.
- **Update License Status** can be used to refresh a license and update the status of the license.
- **Upload License** is used to upload the license file (.lic) provided by Appvance. Clicking **Upload License** will open up the File Manager to browse for the license file that needs to be uploaded.

- **License Time Usage** downloads a report (in csv format) with information on all the scenarios that have been run, including the date and the virtual user minutes spent on each of the scenarios and the scenario file used.

Last updated: July 10, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

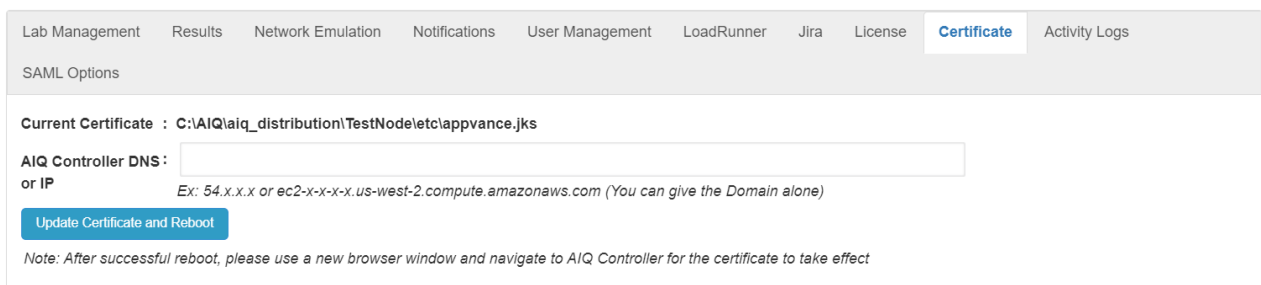
Certificate

Appvance IQ supports HTTPS and Secure Socket Layer (SSL) protocols. These protocols use the Java Cryptography Architecture to work with SSL certificates.

The AIQ protocol handler will throw an `SSLHandshakeException` when connecting to a server over SSL protocols when the server-side SSL certificate is unknown. AIQ, when accessing as a SAAS model, is required to update the certificate on the server machines.

Configuring a Certificate

1. Login to AIQ as an Admin user.
2. Navigate to **Global Options > Admin Options > Certificate**.
3. Provide the valid domain or IP address of the controller instance and click **Update Certificate and Reboot**.



The screenshot shows the 'Certificate' tab in the Appvance IQ Admin interface. The top navigation bar includes 'Lab Management', 'Results', 'Network Emulation', 'Notifications', 'User Management', 'LoadRunner', 'Jira', 'License', 'Certificate' (selected), and 'Activity Logs'. Below the navigation bar is a section titled 'SAML Options'. The main content area displays the 'Current Certificate' as 'C:\AIQ\aiq_distribution\TestNode\etc\appvance.jks'. There is a text input field for 'AIQ Controller DNS' or IP, with a placeholder example: '54.x.x.x or ec2-x-x-x.us-west-2.compute.amazonaws.com (You can give the Domain alone)'. A blue button labeled 'Update Certificate and Reboot' is positioned below the input field. A note at the bottom states: 'Note: After successful reboot, please use a new browser window and navigate to AIQ Controller for the certificate to take effect'.

4. A new 'appvance.jks' certificate for the domain provided will be generated, and the controller instance will reboot.
5. After a successful reboot, please use a new browser window to navigate to the AIQ Controller for the certificate to take effect.

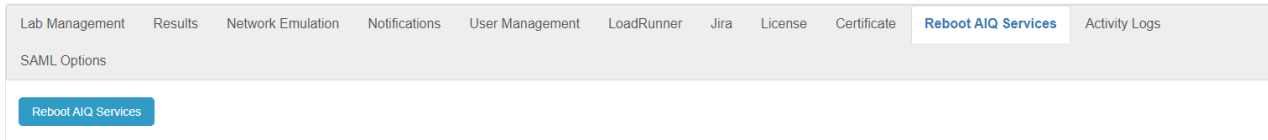
Last updated: July 07, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Reboot AIQ Services

Use the Reboot AIQ Services screen to restart the AIQ services as needed.

1. Login to AIQ as an administrator user.
2. Navigate to **Global Options > Admin Options > Reboot AIQ Services**.



3. Click **Reboot AIQ Services**.

Last updated: July 07, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Activity Logs

Use the **Activity Logs** screen to view AIQ system logs. From here you can see activity by role, user, date and the log message.

1. Login to AIQ as a user with administrator access.
2. Navigate to **Global Options > Admin Options > Activity Logs**.

Lab Management	Results	Network Emulation	Notifications	User Management	LoadRunner	Jira	License	Certificate	Reboot AIQ Services	Activity Logs
SAML Options										
Please select a range of logs 1 to 100 ▼										
Role	Username	Date		Message						
Owner	appvance	Fri Jun 09 16:36:40 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 16:36:39 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 15:48:56 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 15:48:55 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 15:48:55 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 15:48:54 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 11:19:30 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 11:19:29 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 11:19:28 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 09:02:25 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 09:02:24 GMT-06:00		User logged in appvance for services.						
Owner	appvance	Fri Jun 09 09:02:24 GMT-06:00		User logged in appvance for services.						

- You can select a range of activity logs. The oldest logs are in the lowest range of numbers. The most recent logs are in the highest range of numbers.
- You can sort the activity logs by:
 - Role
 - User Name
 - Date
 - Message

Last updated: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

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/>).

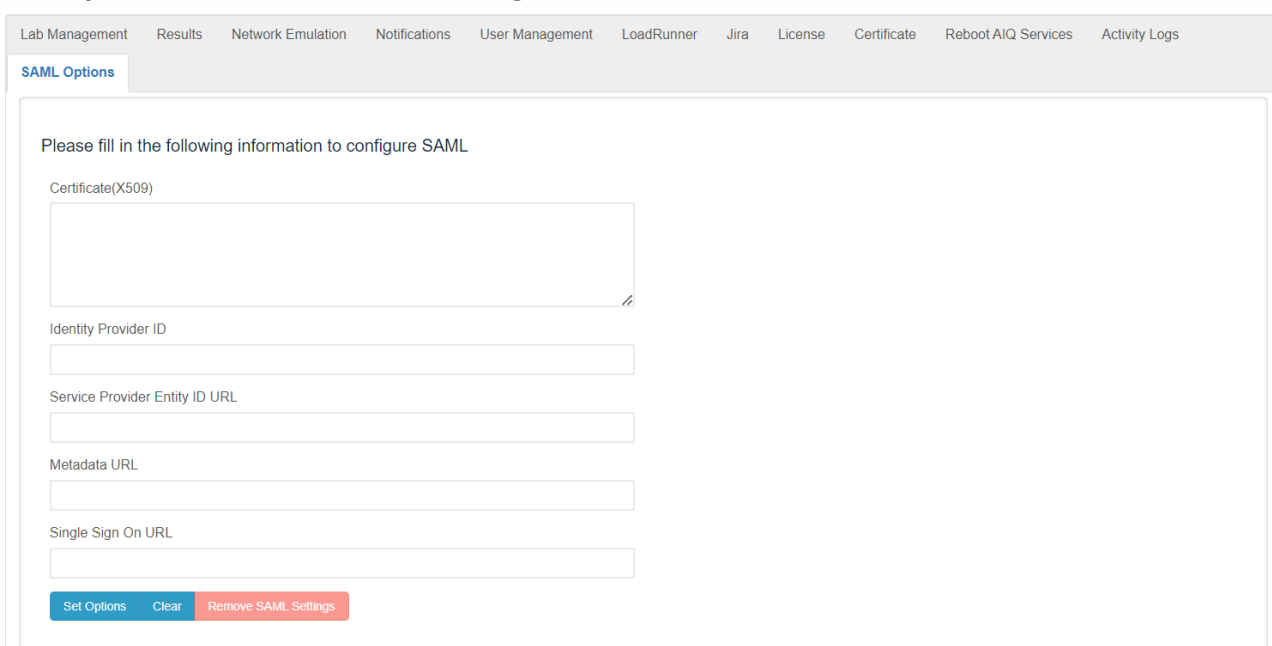
Full SAMLv2 specs can be found here <http://saml.xml.org/saml-specifications>

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



The screenshot shows the 'SAML Options' configuration page. At the top, there is a navigation bar with links: Lab Management, Results, Network Emulation, Notifications, User Management, LoadRunner, Jira, License, Certificate, Reboot AIQ Services, and Activity Logs. Below this, the 'SAML Options' tab is selected. The main content area has a heading 'Please fill in the following information to configure SAML'. It contains five input fields: 'Certificate(X509)' (a large text area), 'Identity Provider ID', 'Service Provider Entity ID URL', 'Metadata URL', and 'Single Sign On URL'. At the bottom of the form, there are three buttons: 'Set Options' (blue), 'Clear' (light blue), and 'Remove SAML Settings' (red).

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: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai