

9.8 - Installation and Configuration

Installation and Configuration — Knowledge Base articles.

- [Installation and Configuration Knowledge Base Overview](#)
- [Update an Expired AIQ Certificate](#)
- [AIQ 5.0 Database Upgrade](#)
- [AIQ Best Practices for Stable Test Execution](#)
- [AIQ AI Implementation Strategy](#)
- [AIQ Project Branching Best Practices](#)
- [Antivirus Settings for AIQ Hosts](#)
- [AIQ Install Script for Ubuntu EC2 Machines](#)
- [Appvance IQ not working with Java 32 bit version.](#)
- [Checking if a machine is ready to run Appvance IQ](#)
- [Troubleshoot Chrome Issues on Mac M1/M2 for AIQ](#)
- [Disable "Are you sure you want to leave this page" notice in IE9](#)
- [Downgrade macOS Mojave to High Sierra - Obsolete](#)
- [Enterprise-Managed Chrome Policies for AIQ Testing](#)
- [Troubleshoot Slow AIQ ZIP Extraction](#)
- [ocsGitHub Runner Timeout](#)
- [Use Chrome Developer Tools for AIQ Troubleshooting](#)
- [Reset an AIQ User Password Securely](#)
- [Find What Is Using an AIQ Port](#)
- [Change the AIQ Test Node Port](#)
- [Configure Multiple IP Addresses for AIQ IP Spoofing](#)
- [Change the AIQ Test Node Port from 8443 to 443](#)
- [Convert PEM Keys to PPK for Windows SSH Clients](#)

- [Install AIQ as a Linux Service](#)
- [AIQ Install Preparation Checklist - Installation and Configuration](#)
- [Install Google Chrome on Ubuntu for AIQ Testing](#)
- [Resolve Java Heap Memory Errors During Scenario Execution](#)
- [Load Balancer SSL Certificate Redirect for AIQ](#)
- [macOS Required Configurations for AIQ - Duplicate Review](#)
- [McAfee Performance Impact on AIQ for Windows](#)
- [Troubleshoot AIQ Login 500 Errors](#)
- [Enable Secure Remote MySQL Access for AIQ Environments](#)
- [Troubleshoot the AIQ Options Page Not Loading](#)
- [Upgrade AIQ on Linux](#)
- [What Is AIQ?](#)
- [Use Conditional Waits in Scenario Editor](#)
- [Legacy AIQ Upgrade Script Reference](#)
- [Legacy Test Designer Client Icons on macOS](#)
- [Configure Outlook 365 Email Clients with OAuth 2.0](#)
- [Manage AIQ Repository Configuration with REST APIs](#)
- [docsApple Safari: Mac Configuration](#)
- [Legacy Firefox Playback Error Popup Guidance](#)
- [Obsolete Internet Explorer Whitelist Prompt Guidance](#)
- [How can I fix a "Plugin Container for Firefox has stopped working" at the end of each test case completion](#)
- [Do We Need a License for Each Machine?](#)
- [Install a new SSL certificate to AIQ controller](#)
- [macOS Cannot Verify AIQ App Developer Warning](#)
- [What is the Required Java Version for AIQ?](#)
- [Troubleshoot Windows RDP Access for Non-Administrator Accounts](#)
- [Legacy Chrome HTTPS 8443 Troubleshooting for AIQ](#)
- [Legacy Firefox HTTPS Localhost Troubleshooting for AIQ](#)
- [Enabling Chrome Flash plugin and other settings using Chrome Browser Cloud Management](#)
- [Upgrade the AIQ Controller and Test Nodes](#)
- [Install the AIQ Certificate on an iPhone](#)
- [Best Practices to Improve AIQ Performance](#)

- [Identify AIQ Java Processes in Windows Task Manager](#)
- [How to encrypt scenario's ec2 cloud config files using API calls](#)
- [Legacy Outlook Email Status Update via HTTP Call](#)
- [Upgrade the AIQ Designer Proxy](#)

Installation and Configuration Knowledge Base Overview

Installation and Configuration Knowledge Base Overview

Last reviewed: September 21, 2026

This overview page organizes installation and configuration maintenance articles for AIQ administrators. Use it as an index and retire duplicate troubleshooting pages when a canonical article exists.

When to use this guidance

- You are looking for AIQ environment setup, service, browser, database, or node configuration guidance.
- You need to decide whether an older article should be updated, consolidated, or removed.
- You are maintaining the Installation and Configuration book.

Recommended approach

1. Start with the current AIQ installation guide for supported versions and prerequisites.
2. Use individual KB pages only for targeted troubleshooting or environment-specific notes.
3. Prefer one canonical page per task, then redirect or consolidate redundant articles.

4. Replace legacy terms with current AIQ terminology such as Scenario Editor and AISG.
5. Review dates and notes whenever a page is updated.

Note: This page is an index/overview, not a replacement for version-specific installation documentation.

Last updated: September 21, 2026

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

Update an Expired AIQ Certificate

Update an Expired AIQ Certificate

Use this procedure when an AIQ certificate has expired or is about to expire. Certificate changes should be planned because they can affect browser access, integrations, load balancers, test nodes, and API clients.

Preparation checklist

- Confirm which certificate expired: AIQ application, load balancer, repository, database, or integration certificate.
- Collect the new certificate, private key, intermediate chain, hostname, expiration date, and owner.
- Back up the existing certificate files and configuration before replacing them.
- Schedule a maintenance window if AIQ services, proxy services, or load balancer rules must restart.
- Notify users and integration owners when the certificate change affects external access.

Validation workflow

1. Install the renewed certificate and full chain in the approved location.
2. Restart only the services required for the certificate to take effect.
3. Validate browser access, API access, test-node connectivity, and any load-balanced URL.
4. Check logs for TLS, hostname, trust-chain, or expired-certificate errors.
5. Record the new expiration date and renewal owner.

Last updated: October 9, 2026

AIQ 5.0 Database Upgrade

AIQ 5.0 Database Upgrade

Use this page as a controlled checklist for upgrading the AIQ database to the version required by AIQ 5.0. Database upgrades should be planned, backed up, and validated before the environment is returned to users.

Pre-upgrade checks

- Confirm the current AIQ version, target AIQ 5.0 build, database engine, and supported upgrade path.
- Create a verified database backup or snapshot before running upgrade steps.
- Confirm available disk space, maintenance window, rollback plan, and stakeholder approval.
- Stop or quiesce AIQ services according to the approved upgrade procedure.
- Review custom integrations, scheduled jobs, and reporting dependencies that may rely on database content.

Validation workflow

1. Run the upgrade in a lower environment first when possible.
2. Apply the database upgrade steps exactly once and record any warnings.
3. Start AIQ services and verify login, scenario execution, reports, and integrations.
4. Monitor logs and database health after the first post-upgrade executions.

Maintenance note: Do not retry schema changes blindly after a failed upgrade. Preserve logs and restore from the approved backup if rollback is required.

Last updated: October 8, 2026

AIQ Best Practices for Stable Test Execution

Last reviewed: September 30, 2026

Use this article as a checklist for building AIQ tests and environments that are easier to maintain, debug, and scale.

What changed in this article

- Refocused the generic best-practices page on stable execution, maintainable scenarios, data control, and environment readiness.
- Added specific practices for locator strategy, waits, test data, Test Node capacity, browser versions, logs, and result review.
- Removed vague guidance and replaced it with concrete checks that support Scenario Editor and current AIQ terminology.

Validation workflow

1. Review locator, wait, and data strategy before expanding a scenario suite.
2. Validate browser/Test Node capacity and dependency versions before high-volume runs.
3. Use execution logs and result trends to tune the suite instead of making untracked one-off changes.

Review note: This page now complements performance and installation articles without duplicating their detailed procedures.

Last updated: September 30, 2026

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

AIQ AI Implementation Strategy

Last reviewed: September 30, 2026

Use this article as a planning checklist for introducing AIQ AI capabilities such as AISG into a governed testing program.

What changed in this article

- Updated the strategy page to use AISG terminology and governance language instead of vague AI adoption wording.
- Added planning checks for application readiness, data privacy, validation coverage, human review, rollout stages, success metrics, and ownership.
- Added guidance to treat generated scenarios as reviewable assets that require validation before production use.

Validation workflow

1. Choose a narrow application area and define success criteria before enabling AI-assisted generation.
2. Review generated scenarios, validations, data usage, and evidence with application owners.
3. Expand only after the team has measured maintainability, coverage value, and false-positive/false-negative behavior.

Review note: This page now reads like an implementation plan rather than a generic AI positioning article.

Last updated: September 30, 2026

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

AIQ Project Branching Best Practices

AIQ Project Branching Best Practices

Use project branching to manage test changes safely across maintenance, feature work, and release validation.

Recommended guidance

- Keep branch names clear and tied to a change, release, or maintenance objective.
- Avoid long-lived branches that drift from the main project baseline.
- Validate scenarios in the branch before merging or promoting.
- Document major data, environment, or integration differences between branches.

Validation workflow

1. Create a branch for the planned change.
2. Apply and validate the scenario, data, or configuration update.
3. Review execution output and affected suites.
4. Merge, promote, or retire the branch according to the project workflow.

Last updated: September 20, 2026

Antivirus Settings for AIQ Hosts

Recommended guidance

Antivirus or endpoint protection tools can affect AIQ installation, browser execution, file extraction, repositories, logs, and Test Node performance. Coordinate any exclusions with the customer's IT/security team and document exactly what was approved.

Symptoms to investigate

- Slow extraction, installation, startup, or upgrade operations.
- Browser drivers, temporary files, downloaded artifacts, or logs being quarantined.
- Intermittent Test Node failures or unusually slow scenario playback.
- Repository or dependency files blocked during execution.

Safe review process

1. Confirm the antivirus product, policy owner, affected host, and exact AIQ path.
2. Review logs from both AIQ and the endpoint protection tool.
3. Request the narrowest possible approved exclusion, never a broad system-wide bypass.
4. Retest installation, extraction, browser playback, and Test Node execution after policy changes.
5. Record the approved policy, date, and owner in environment documentation.

Last updated: October 6, 2026

AIQ Install Script for Ubuntu EC2 Machines

Recommended guidance

Use installation scripts only when they match the approved AIQ version, operating system, and deployment model. Treat old EC2 install scripts as environment-specific automation that must be reviewed before reuse.

Before running an install script

- Confirm the supported Ubuntu version, EC2 instance type, storage, network, DNS, and firewall rules.
- Review the script contents before execution; do not run unknown or outdated scripts blindly.
- Use approved repositories, package sources, certificates, and installation artifacts.
- Store secrets outside the script and inject them through approved secure mechanisms.
- Confirm backup, rollback, monitoring, and access requirements before installation.

Post-install validation

1. Confirm AIQ services start correctly after reboot.
2. Validate browser, Test Node, database, repository, and file permissions.
3. Check Output Logs and system logs for startup errors.
4. Run a small Scenario Editor smoke test and a Service Suite smoke test.
5. Document the installed AIQ version, OS version, instance details, and configuration changes.

Obsolescence note: If the script targets an old AIQ release, old Ubuntu release, or retired infrastructure pattern, update the script before use or replace it with the current deployment process.

Last updated: October 5, 2026

Appvance IQ not working with Java 32 bit version.

When working with Appvance IQ + java 32 bit version, the test scenarios might not run and throw some connect errors on the test controller and in the error logs you might see the below error.

Error: missing `server' JVM at `C:\Program Files (x86)\Java\jre1.8.0_111\bin\server\jvm.dll'.

Solution:

To Fix The "Missing "server" JVM at `C:\Program Files (x86)\Java\jre1.8.0_111\bin\server\jvm.dll'. Please install or use the JRE or JDK that contains these missing components. Press any key to continue . . "

follow the steps:

Go to [oracle.com](https://www.oracle.com) and install java jre7 or jre8 (if not already installed)

After that go to C:\Program Files (x86)\Java\jre1.8.0_111\bin

Here create an folder called "Server" (without " ")

Now go into the C:\Program Files (x86)\Java\jre1.8.0_111\bin\client folder

COPY all data of this folder into the new C:/Program files/java/jre7/bin/Server

Rerun the test scenario to fix the issue!

Last updated: June 02, 2023

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

Checking if a machine is ready to run Appvance IQ

Use the following information to determine the status of system requirements for running Appvance AIQ on your machine

The Readiness Check utility requires a few details about the systems where you plan to run Appvance IQ. Upon execution, the utility gathers specific hardware and software details about your machine(s) and generates a compatibility report indicating any missing Appvance IQ prerequisites.

Steps

1. Download and extract [AIQ_EndUserSystem_ReadinessCheck.zip](#) to every machine where you plan use Appvance IQ. This includes your workstation/notebook, Controller and Test Node machines.
2. Ensure that you have access to the **64-bit, Java 1.8 Runtime Environment (JRE)**. This 64-bit JRE environment can either from a [64-bit JDK 1.8](#) or [64-bit JRE 1.8](#) installation.
3. Run the check on each machine using **java -jar AIQ_EndUserSystem_ReadinessCheck.jar**
4. Send the generated report file, **AIQ_EndUserSystem_ReadinessReport.txt**, to your Appvance contact.

Sample Output

```
Administrator: Command Prompt
C:\Utilities>java -jar AIQ_EndUserSystem_ReadinessCheck.jar
Appvance CompatCheck: Qualifying this Machine...

Running Windows checks...

Running Java checks...

Running Port checks...

Running Environment Vars check...

Running Browser checks on Windows machine...

Running Internet Connection check...

Message: Report generated in 'AIQ_EndUserSystem_ReadinessReport.txt'

C:\Utilities>
```

```
AIQ_EndUserSystem_ReadinessReport.txt - Notepad
File Edit Format View Help
# Copyright (c) 2017 Appvance Inc
# All rights reserved.
#
# Machine Compatibility Report Version : 0.1
#
# Hostname : EC2AMAZ-ROU6BDI
# Date : Friday, 13/08/2021/09:24:52

OS : Windows 64
JVM Home : C:\Program Files\AdoptOpenJDK\jdk-8.0.252.09-hotspot\jre
JVM Version : 1.8.0_252
JVM Bitness : 64
Appvance IQ's Required Ports :
8080 : AVAILABLE
9090 : AVAILABLE
9091 : AVAILABLE
9443 : AVAILABLE
9095 : AVAILABLE
8443 : AVAILABLE
9999 : AVAILABLE

Browsers Found on this Machine :
Internet Explorer : C:\Program Files\Internet Explorer\iexplore.exe
Internet Explorer x86 : C:\Program Files (x86)\Internet Explorer\iexplore.exe
Firefox : C:\Program Files\Mozilla Firefox\firefox.exe
Chrome x86 : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Internet Connection : SUCCESS (no proxy detected)
```

Last updated: October 25, 2023

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

Troubleshoot Chrome Issues on Mac M1/M2 for AIQ

Troubleshoot Chrome Issues on Mac M1/M2 for AIQ

Use this article when Chrome behaves inconsistently on Apple Silicon Macs used for AIQ authoring, playback, or browser validation. Confirm Chrome, macOS, driver, and security settings before changing AIQ configuration.

Common checks

- Install the Apple Silicon version of Chrome unless the environment explicitly requires Rosetta.
- Confirm the Chrome version matches the browser driver or automation dependency used by the test.
- Review macOS privacy and security prompts for screen recording, accessibility, files, and network access.
- Check whether extensions, profiles, or cached browser data are affecting playback.
- Run a clean-profile smoke test before changing the scenario.

Validation workflow

1. Record the Mac model, macOS version, Chrome version, and AIQ version.
2. Reproduce the issue with a small known-good scenario.
3. Update Chrome/driver alignment and permissions if needed.
4. Capture logs and screenshots before escalating persistent failures.

Last updated: October 8, 2026

Disable "Are you sure you want to leave this page" notice in IE9

The "**Are you sure you want to leave this page**" notice in Internet Explorer 9 is a browser-level dialog and is not part of the page's DOM. Therefore, it cannot be handled like a regular HTML element using Appvance/Sahi selectors.

This notice is typically triggered by JavaScript running on the page, such as the `beforeunload` event.

To prevent the notice from appearing, disable Active scripting in Internet Explorer:

1. Select **Start**, enter **Internet Options**, and select **Internet Options**.
2. Select the **Security** tab.
3. Click **Custom Level**.
4. Scroll down to **Scripting**.
5. Under **Active scripting**, select **Disable**.
6. Click **OK** and apply the changes.

Disabling Active scripting prevents the page's JavaScript from triggering the browser-level confirmation dialog.

“ **Note:** Disabling Active scripting can affect other JavaScript-based functionality on the page. Use this setting only when required for the test environment.

Last updated: August 17, 2026

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

Downgrade macOS Mojave to High Sierra - Obsolete

Obsolete guidance

This article is obsolete for current AIQ documentation. Downgrading macOS Mojave to High Sierra is not current AIQ installation guidance and should not be recommended as a standard troubleshooting path.

Current recommendation

- Use a macOS version supported by the target AIQ release.
- Review current AIQ install guides and system requirements before changing the operating system.
- Coordinate OS changes with the customer's IT or device management team.
- Prefer supported browser/runtime/configuration fixes over OS downgrades.

Disposition

Flag this page for deletion or archival unless a customer-specific legacy environment still requires it. If retained, label it clearly as historical and not current installation guidance.

Last updated: October 7, 2026

Enterprise-Managed Chrome Policies for AIQ Testing

Recommended guidance

Enterprise-managed Chrome policies can change how Scenario Editor tests behave. Before changing a scenario, confirm whether Chrome policies control downloads, popups, certificates, extensions, permissions, proxy settings, site isolation, or automatic updates.

Symptoms of policy interference

- Downloads are blocked or saved to an unexpected location.
- Camera, microphone, location, clipboard, or notification prompts behave differently than expected.
- Extensions, certificates, proxy settings, or security warnings cannot be changed by the user.
- Playback differs between a corporate workstation and a clean Test Node.
- Chrome updates occur automatically and change test behavior.

Recommended checks

1. Open Chrome policy information on the affected machine and identify managed settings.
2. Compare the affected machine with a known-good Test Node.
3. Coordinate policy changes with IT instead of bypassing enterprise controls.
4. Document required browser policies for AIQ execution environments.
5. Retest affected scenarios after policy, browser, driver, or Test Node changes.

Important: Do not instruct users to bypass security policies. Work with the customer's IT team to define approved settings for AIQ testing.

Last updated: October 5, 2026

Troubleshoot Slow AIQ ZIP Extraction

Recommended guidance

Slow AIQ ZIP extraction is usually caused by endpoint protection scanning, slow disk I/O, network shares, insufficient space, file permission checks, or extracting from a blocked/downloaded archive. Diagnose the host before assuming the AIQ package is defective.

Checks to run

- Confirm the ZIP file size, checksum, source, and whether the download completed cleanly.
- Extract on local fast storage instead of a network share when possible.
- Check free disk space, disk health, CPU, memory, and active endpoint scanning.
- Confirm the user has permission to create files in the target directory.
- Review antivirus/EDR logs for scans, quarantines, or policy blocks.

Recommended workflow

1. Copy the ZIP to a local installation directory.
2. Verify the file before extraction.
3. Use approved extraction tools and avoid interrupting the process mid-write.
4. If extraction is still slow, coordinate with IT on temporary narrow exclusions for the installation path.
5. Document the final extraction time and any host policy changes.

Last updated: October 6, 2026

ocsGitHub Runner Timeout

Use Chrome Developer Tools for AIQ Troubleshooting

Use Chrome Developer Tools for AIQ Troubleshooting

Use Chrome Developer Tools to inspect application behavior during troubleshooting, but rely on AIQ execution output and logs for repeatable test evidence.

Recommended guidance

- Use DevTools for local diagnosis of network, console, DOM, and performance symptoms.
- Do not require manual DevTools steps for automated Scenario Editor execution.
- Avoid capturing secrets, tokens, or personal data from network traces.
- Translate findings into stable locators, waits, validations, or environment fixes.

Validation workflow

1. Reproduce the issue in a controlled browser session.
2. Inspect console, network, DOM, or performance signals as needed.
3. Update the AIQ scenario or environment based on confirmed findings.
4. Validate the fix with a fresh AIQ execution.

Last updated: September 20, 2026

Reset an AIQ User Password Securely

Reset an AIQ User Password Securely

Last reviewed: September 21, 2026

Use this article when an administrator needs to restore access for an AIQ user without exposing or reusing shared passwords. Prefer the AIQ administration workflow and follow your organization's credential policy.

When to use this guidance

- A user cannot sign in and requires an administrator reset.
- You need to confirm the account exists and is assigned the correct role.
- You need an auditable support workflow for password resets.

Recommended approach

1. Confirm the requester is authorized for the target account.
2. Open AIQ administration and locate the user record under user management.
3. Use the reset or temporary credential workflow available for your AIQ version; do not publish default passwords in documentation or tickets.
4. Require the user to change the password at next sign-in and verify that the account works.
5. Record the support ticket or audit note without including the password value.

Note: Do not paste passwords into tickets, email, chat, or documentation. If a command-line reset is required, run it only from the controller with an authorized administrator account and follow the current installation runbook.

Last updated: September 21, 2026

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

Find What Is Using an AIQ Port

Find What Is Using an AIQ Port

Use this procedure when AIQ or a Test Node cannot start because a required port is already in use. Identify the process first, then decide whether to stop it, reconfigure it, or change the AIQ port assignment.

Before changing anything

- Confirm which AIQ component reports the port conflict.
- Record the port number and host where the conflict occurs.
- Check whether the process using the port belongs to AIQ, another service, or a previous failed startup.

Recommended workflow

1. Use the operating system's port/process tool to identify the process ID using the port.
2. Confirm the process owner and command before stopping anything.
3. If the process is stale, stop it using the approved server process-management method.
4. If another service legitimately uses the port, update the AIQ configuration and restart the affected component.

Do not terminate unknown production processes without confirming ownership and impact.

Last updated: September 18, 2026

Change the AIQ Test Node Port

Change the AIQ Test Node Port

Use this procedure only when your deployed AIQ version uses the TestNode Jetty configuration shown below. Confirm the target port is available and permitted by your network and firewall policies before making the change.

1. Stop the AIQ services.
2. Open `<appvance_package>\TestNode\etc\jetty.xml` in a text editor.
3. Locate `<Set name="port"><Property name="jetty.port" default="8080"/></Set>`.
4. Replace 8080 with the required port number.
5. Save the file and restart the AIQ services.
6. Verify that the Test Node is reachable on the new port.

Last updated: September 14, 2026

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

Configure Multiple IP Addresses for AIQ IP Spoofing

Configure Multiple IP Addresses for AIQ IP Spoofing

Last reviewed: September 21, 2026

This article explains the maintenance considerations for adding multiple source IP addresses for AIQ performance testing. Treat IP spoofing as an advanced network configuration that must be coordinated with infrastructure owners.

When to use this guidance

- A performance test requires traffic to originate from multiple source IPs.
- The test node host and network route tables support additional addresses.
- Network, firewall, and monitoring teams have approved the source ranges.

Recommended approach

1. Confirm the IP range, subnet mask, gateway, and routing requirements with the network team.
2. Apply the additional addresses on the test node host using the operating-system network tooling approved for that environment.

3. Restart or refresh only the services required for the OS to recognize the new addresses.
4. Run a small validation scenario and confirm traffic appears from the expected addresses.
5. Document the range and remove temporary addresses when testing is complete.

Note: Do not enable IP spoofing on shared hosts without network approval; misconfigured source addresses can disrupt routing or monitoring.

Last updated: September 21, 2026

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

Change the AIQ Test Node Port from 8443 to 443

Change the AIQ Test Node Port from 8443 to 443

Last reviewed: September 21, 2026

Use this page when a test node must listen on HTTPS port 443 instead of the default service port. Validate the change in a maintenance window because it affects controller-to-node communication.

When to use this guidance

- Security or network policy requires standard HTTPS port 443.
- No other service is already bound to port 443 on the test node.
- Firewall rules can be updated at the same time as the AIQ setting.

Recommended approach

1. Back up the current AIQ/test node configuration before editing ports.
2. Confirm port 443 is free on the host and allowed by host firewall and network firewall.
3. Update the test node port setting in the supported AIQ configuration file or administration setting for your version.
4. Restart the test node service and verify it binds to the new port.
5. Update any controller, load balancer, monitoring, or documentation references that still point to 8443.

Note: If another service already uses port 443, do not force the change; resolve the port conflict first.

Last updated: September 21, 2026

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

Convert PEM Keys to PPK for Windows SSH Clients

Convert PEM Keys to PPK for Windows SSH Clients

Last reviewed: September 21, 2026

Use this page when an administrator needs to connect to an AIQ host from a Windows SSH client that requires PuTTY private key format.

When to use this guidance

- You have an approved PEM private key for the AIQ host.
- Your Windows SSH client requires a PPK key.
- The key will be stored and protected according to your security policy.

Recommended approach

1. Install or use the approved PuTTYgen version from your organization's software catalog.
2. Open PuTTYgen and load the PEM private key.
3. Add or confirm a passphrase if policy requires it.
4. Save the converted PPK file in a protected location.
5. Test access with the target host and remove any unnecessary duplicate key files.

Note: Private keys are sensitive credentials. Do not upload them to documentation, tickets, or shared drives unless explicitly approved by security policy.

Last updated: September 21, 2026

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

Install AIQ as a Linux Service

Install AIQ as a Linux Service

Install AIQ as a Linux service when the application must start automatically after a reboot and be managed through the operating system service manager. Use a dedicated service account and document every environment-specific path.

Recommended setup

- Create or confirm the Linux account that will run AIQ.
- Verify Java, browser, driver, database, and file-system dependencies before enabling the service.
- Place environment variables, ports, and paths in the approved AIQ configuration files or service override.
- Use systemd or the supported service manager for start, stop, restart, and status operations.
- Send logs to a known location so startup failures can be diagnosed quickly.

Validation workflow

1. Start AIQ manually once and confirm it runs successfully.
2. Enable the service and start it through the service manager.
3. Reboot the host if allowed and confirm AIQ starts automatically.
4. Run a login and small scenario smoke test.
5. Document the service name, account, paths, ports, and log location.

Last updated: October 8, 2026

AIQ Install Preparation Checklist - Installation and Configuration

AIQ Install Preparation Checklist - Installation and Configuration

Use this checklist to prepare the installation plan, access, configuration, and validation steps for an AIQ deployment. This version should contain the procedural install-readiness items, while the System Requirements checklist remains focused on platform requirements.

Installation readiness checks

- Confirm installation owner, target environment, maintenance window, and rollback plan.
- Verify hostnames, ports, certificates, service accounts, database access, repositories, and SMTP/integration requirements.
- Prepare installers, licenses, configuration files, backup/snapshot plan, and support contacts.
- Confirm test accounts, sample scenarios, and smoke-test criteria for post-install validation.
- Document customer-specific proxy, firewall, SSO, repository, and monitoring requirements.

Validation workflow

1. Complete pre-install checks and capture approvals.
2. Install or upgrade AIQ using the approved procedure.
3. Validate login, Controller health, Test Node connectivity, repository access, and a small execution.
4. Record open issues and follow-up actions before handing the environment to users.

Duplicate-content note: This article overlaps with the System Requirements checklist; keep this one as the procedural install checklist and consolidate duplicate requirement-only items into the requirements page.

Last updated: October 9, 2026

Install Google Chrome on Ubuntu for AIQ Testing

Install Google Chrome on Ubuntu for AIQ Testing

Install a supported Google Chrome release on the machine that will run browser-based AIQ tests. Follow your organization's approved Ubuntu package-management and browser-update process.

Before running tests:

1. Confirm that the Chrome version is supported by your deployed AIQ version.
2. Install Chrome on each applicable Test Node or execution host.
3. Verify that the AIQ service account can launch the browser.
4. Run a small Scenario Editor test to confirm recording or execution behavior.

Avoid relying on hard-coded package URLs or outdated dependency commands; Chrome installation requirements change by Ubuntu release.

Last updated: September 14, 2026

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

Resolve Java Heap Memory Errors During Scenario Execution

Resolve Java Heap Memory Errors During Scenario Execution

If Scenario Editor execution fails with a Java error such as “Could not reserve enough space” or a heap-allocation failure, verify the Java runtime and available system memory before changing AIQ settings.

1. Confirm that the installed Java runtime matches the operating system architecture (for example, use 64-bit Java on a 64-bit system).
2. Confirm that sufficient memory is available for the configured Java heap and concurrent execution load.
3. Restart the AIQ services after correcting the Java installation or memory configuration.
4. Re-run the scenario and review the output for the remaining root cause.

If the issue persists, collect the relevant AIQ and Java error logs for support analysis.

Last updated: September 14, 2026

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

Load Balancer SSL Certificate Redirect for AIQ

Load Balancer SSL Certificate Redirect for AIQ

Use this guidance when AIQ traffic is routed through a load balancer that terminates SSL/TLS or redirects HTTP traffic to HTTPS. Keep the certificate, redirect, and application URL configuration aligned so users and test nodes reach the correct endpoint.

Configuration checks

- Install the current certificate chain on the load balancer and confirm it includes intermediate certificates.
- Redirect HTTP to HTTPS only when the target AIQ URL and ports are correct.
- Confirm AIQ base URL, proxy headers, and forwarded protocol settings match the load balancer configuration.
- Verify that test nodes, integrations, and CI/CD jobs use the same externally reachable URL.
- Review certificate expiration, DNS, firewall, and health-check behavior.

Validation workflow

1. Open the AIQ URL from a user network and from any test-node network that must reach it.
2. Confirm there are no redirect loops or mixed-content warnings.
3. Run a login smoke test and a small execution through the load-balanced URL.
4. Document certificate owner, renewal date, DNS name, and load balancer rule.

Last updated: October 8, 2026

macOS Required Configurations for AIQ - Duplicate Review

Recommended guidance

This page duplicates the macOS required configuration topic. Keep one authoritative macOS configuration article and consolidate any unique current details into that page.

Consolidation checklist

- Compare this article with the install-guide macOS configuration page.
- Move unique supported content into the authoritative article.
- Remove old screenshots, old product names, and unsupported security-bypass wording.
- Delete or redirect this duplicate after content owner review.

Current recommendation

Use the primary macOS configuration guide for current AIQ setup. Retain this page only if it is needed temporarily during migration cleanup.

Last updated: October 7, 2026

McAfee Performance Impact on AIQ for Windows

Recommended guidance

McAfee or other endpoint security tools can slow AIQ on Windows by scanning installation folders, browser assets, temporary execution files, logs, repositories, or Test Node working directories. Treat this as an endpoint-policy coordination issue, not a reason to disable security controls broadly.

Evidence to collect

- AIQ operation affected: install, upgrade, startup, extraction, playback, or reporting.
- Host details, AIQ version, Windows version, browser version, and Test Node role.
- McAfee policy name, scan events, quarantine entries, and timestamps.
- Comparison between affected and unaffected hosts, if available.

Resolution workflow

1. Review AIQ logs and McAfee logs for matching timestamps.
2. Ask IT/security to evaluate narrow path/process exclusions for approved AIQ directories.
3. Retest the affected workflow after policy changes.
4. Keep exclusions limited, documented, and reviewed during upgrades.

Last updated: October 6, 2026

Troubleshoot AIQ Login 500 Errors

Troubleshoot AIQ Login 500 Errors

A 500 error during AIQ sign-in indicates a server-side failure. Do not delete configuration files or modify application data unless instructed by Appvance Support.

1. Confirm that the AIQ services are running and the application URL is reachable.
2. Check the AIQ server logs for the request time and capture the error details.
3. Confirm that the service account has access to the required AIQ directories and data stores.
4. Clear the browser session data or use a private window to rule out stale browser state.
5. If the issue began after an upgrade or configuration change, collect the affected version, deployment details, and logs before contacting support.

Last updated: September 14, 2026

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

Enable Secure Remote MySQL Access for AIQ Environments

Last reviewed: September 22, 2026

Use this article when an AIQ environment requires remote MySQL access for administration, diagnostics, or integrations. Apply least-privilege network and account controls.

Recommended guidance

- Confirm remote access is required; prefer local or bastion access when possible.
- Restrict bind address, firewall rules, and database grants to approved sources.
- Use TLS and secret management where supported.

Validation workflow

1. Identify the client host, database host, port, and approved access path.
2. Update MySQL bind and firewall settings only for the required network scope.
3. Create or update a least-privilege database account for the task.
4. Test connectivity from the approved source and verify logs.
5. Remove temporary access after the maintenance window when applicable.

Note: Opening MySQL broadly to the network is unsafe. Never use 0.0.0.0 access without compensating controls and approval.

Last updated: September 22, 2026

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

Troubleshoot the AIQ Options Page Not Loading

Troubleshoot the AIQ Options Page Not Loading

Last reviewed: September 21, 2026

Use this article when the AIQ Options or Global Options page does not load in a browser. Start with browser/session checks, then validate AIQ services and logs.

When to use this guidance

- The AIQ application loads partially but Options does not.
- A browser shows a blank page, spinner, or server error.
- Administrators need a safe triage path before restarting services.

Recommended approach

1. Refresh the session and test in a supported browser profile without extensions.
2. Confirm the user has permission to access Options or Global Options.
3. Check browser developer tools for failed requests and HTTP status codes.
4. Review AIQ server logs for matching errors at the time of the failed load.
5. Restart affected AIQ services only after collecting evidence and confirming impact.

Note: The original title contained a spelling error; use “Appvance” or “AIQ” in future references.

Last updated: September 21, 2026

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

Upgrade AIQ on Linux

Recommended guidance

Plan AIQ upgrades on Linux as controlled maintenance activities. Confirm the target AIQ version, operating system compatibility, database requirements, browser/Test Node compatibility, integrations, repositories, and rollback plan before making changes.

Pre-upgrade checklist

- Back up the database, configuration files, certificates, repositories, and custom scripts.
- Record the current AIQ version, OS version, Java/runtime dependencies, browser versions, and Test Node configuration.
- Review release notes for breaking changes, deprecated features, and migration steps.
- Notify users and schedule downtime if required.
- Confirm there is enough disk space for backups, packages, logs, and rollback files.

Upgrade validation

1. Confirm AIQ services start cleanly after the upgrade.
2. Validate login, Scenario Editor playback, Service Suite execution, reports, integrations, and repository access.
3. Run representative smoke tests before releasing the environment to users.
4. Review Output Logs and server logs for migration or compatibility errors.
5. Document the final version, date, validation results, and any follow-up actions.

Rollback note: Do not begin the upgrade unless the team knows how to restore the previous database, files, and application version if validation fails.

Last updated: October 5, 2026

What Is AIQ?

What Is AIQ?

AIQ is Appvance's software quality platform for designing, executing, and analyzing automated tests across web, API, mobile, and performance-testing workflows.

Use AIQ to organize test assets, run tests on available Test Nodes, review execution results, and investigate failures. Available capabilities depend on the licensed AIQ version and deployment configuration.

For detailed instructions, use the relevant Scenario Editor, Service Suite, Test Controller, or analysis documentation.

Last updated: September 14, 2026

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

Use Conditional Waits in Scenario Editor

Use Conditional Waits in Scenario Editor

Use conditional waits when a Scenario Editor test needs to wait for application state, such as an element becoming visible, enabled, populated, or ready for interaction. Prefer conditional waits over fixed pauses whenever the timing depends on the application or network.

When to use a conditional wait

- A page or component loads asynchronously.
- A button is disabled until validation completes.
- Search results, modal dialogs, or messages appear after an action.
- A stored value or validation depends on content generated during the run.

Good practices

1. Wait for the smallest stable condition that proves the page is ready.
2. Use stable locators and avoid waits tied only to visual position.
3. Set reasonable timeouts so real failures are not hidden.
4. Review repeated wait failures as application, environment, locator, or data issues before increasing timeout values.

Last updated: September 18, 2026

Legacy AIQ Upgrade Script Reference

Legacy AIQ Upgrade Script Reference

Last reviewed: September 21, 2026

This page is retained as a legacy reference for older AIQ upgrade processes that used helper scripts. For current upgrades, follow the supported AIQ upgrade guide for your version.

When to use this guidance

- You are reviewing an older environment that references a Python upgrade script.
- You need to understand historical upgrade notes before migrating to current guidance.
- You are deciding whether to consolidate or retire legacy upgrade pages.

Recommended approach

1. Identify the installed AIQ version and the target supported version.
2. Use the current official upgrade procedure as the source of truth.
3. Back up configuration, database, DPLs, certificates, and custom integrations before any upgrade.
4. Treat legacy scripts as historical references unless Support explicitly instructs you to use them.
5. After upgrade, validate sign-in, scenario execution, reports, integrations, and test nodes.

Note: Legacy upgrade scripts can be version-specific. Do not run an old script against a current environment without Support confirmation.

Last updated: September 21, 2026

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

Legacy Test Designer Client Icons on macOS

Last reviewed: September 22, 2026

This page is retained as a legacy reference for older Test Designer client icon setup on macOS. Current AIQ documentation should prefer supported launch and access methods for the active version.

Recommended guidance

- Use this only when maintaining an older macOS client workflow.
- Prefer current AIQ access methods over manual icon workarounds.
- Do not treat legacy desktop client setup as current Scenario Editor guidance.

Validation workflow

1. Confirm whether the environment still uses the legacy Test Designer client.
2. Check the current AIQ version documentation for supported macOS access.
3. If a legacy icon is still required, follow the organization's macOS application management process.
4. Validate launch behavior with a non-admin user if applicable.
5. Plan to retire this page once legacy clients are no longer supported.

Note: Legacy Test Designer client references should be consolidated or removed when no longer relevant.

Last updated: September 22, 2026

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

Configure Outlook 365 Email Clients with OAuth 2.0

Last reviewed: September 29, 2026

Use this article when AIQ-related email testing or service flows require OAuth 2.0 access to Outlook 365 mailboxes.

What changed in this article

- Corrected OAuth 2.0 formatting and clarified the article is about Outlook 365 email client configuration.
- Added checks for Azure app registration, tenant consent, scopes, redirect URI, mailbox permissions, token lifetime, and refresh behavior.
- Added a security warning to avoid basic authentication, app-password reuse, and storing client secrets in article text or scripts.

Validation workflow

1. Confirm the tenant allows the selected OAuth flow and mailbox access pattern.
2. Validate app registration, scopes, redirect URI, and consent with the Microsoft 365 administrator.
3. Run a test authentication flow and verify mail access without exposing tokens or client secrets in logs.

Review note: Updated the page toward OAuth 2.0 security requirements and away from older password-based mail automation.

Last updated: September 29, 2026

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

Manage AIQ Repository Configuration with REST APIs

Last reviewed: September 22, 2026

Use these repository REST APIs only for supported AIQ administration and automation workflows. Treat repository names, branch data, and credentials as sensitive operational configuration.

Recommended guidance

- Use least-privilege accounts or tokens for repository automation.
- Validate API behavior in a non-production environment before automating changes.
- Avoid storing repository credentials or tokens in documentation, scripts, or logs.

Validation workflow

1. Confirm the AIQ version and supported repository API endpoints.
2. Authenticate with an approved account and call read-only endpoints first.
3. Validate repository name, branch, and status responses before triggering pull or save operations.
4. Log execution IDs and non-sensitive response details for traceability.
5. Review and rotate credentials used by repository integrations.

Note: Delete and save operations can change repository configuration. Use them only with explicit admin intent.

Last updated: September 22, 2026

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

docsApple Safari: Mac Configuration

Legacy Firefox Playback Error Popup Guidance

Legacy Firefox Playback Error Popup Guidance

This page is legacy Firefox/Test Designer troubleshooting content. Current Scenario Editor tests should use supported browser versions, Test Node logs, and execution output instead.

Recommended guidance

- Do not use this as guidance for new Scenario Editor tests.
- Confirm whether the asset still depends on legacy Firefox or old Designer playback.
- Prefer supported browser and driver combinations for current AIQ releases.
- Flag obsolete Firefox-specific workarounds for removal or consolidation.

Validation workflow

1. Reproduce the issue in a supported browser first.
2. Review AIQ output, Test Node logs, browser version, and driver version.
3. Use legacy notes only if maintaining an older asset.
4. Document the migration or retirement recommendation.

Last updated: September 20, 2026

Obsolete Internet Explorer Whitelist Prompt Guidance

This page is retained only to flag that Internet Explorer whitelist-prompt guidance is obsolete for current AIQ testing.

What changed in this article

- Marked the IE whitelist prompt workflow as obsolete because Internet Explorer is no longer a current browser target.
- Removed the implication that teams should maintain IE-specific site whitelist steps for new AIQ work.
- Added migration checks toward supported Chromium-based browsers and current browser policy management.

Validation workflow

1. Do not add new AIQ coverage that depends on Internet Explorer whitelist behavior.
2. Reproduce the workflow in a supported browser and review browser policy or certificate settings there.
3. Document any remaining IE dependency as legacy risk and plan migration.

Review note: This page should be archived or deleted once no customer requires the historical IE reference.

Last updated: October 2, 2026

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

How can I fix a "Plugin Container for Firefox has stopped working" at the end of each test case completion

Applicable for Firefox 43 or lower.

To stop this error pop-up - Go to the folder where Firefox is installed

Default location is: C:\Program Files (x86)\Mozilla Firefox

Remove all the entries that are plugin-container.exe and you should stop receiving those error pop-up.

Last updated: June 02, 2023

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

Do We Need a License for Each Machine?

No. A separate license is not required for each machine used to execute a test.

A single AIQ license on the **Controller** is sufficient when executing a test across multiple machines.

For example, if a test is distributed across four machines, you do not need four separate licenses. The machines can execute the test through the Controller using the single Controller license.

Last updated: August 17, 2026

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

Install a new SSL certificate to AIQ controller

Connect to the AIQ Controller server and find the folder where AppvanceIQ is installed. Find the keystore file called appvance.jks in the following path:

Keystore

```
/opt/aiq/aiq_distribution/TestNode/etc/appvance.jks
```

then depending on the certificate files you received from your certificate authority use the following commands to add your certificate files to the keystore.

Provide 'appvance' as password when requested.

Root Certificate

1. Install the SSL Certificate (**root**) file to your keystore using the following command:

```
$JAVA_HOME/bin ./keytool -importcert -keystore appvance.jks -alias root -file <root cer  
file name>
```

2. Choose **Y** or **Yes** to trust the certificate.

Intermediate certificate

1. Install the SSL Certificate (**intermediate**) file to your keystore using the following command:

```
$JAVA_HOME/bin ./keytool -importcert -keystore appvance.jks -alias nsdroot -file  
<intermediate cer file name>
```

2. Choose **Y** or **Yes** to trust the certificate.

Server certificate

1. Install the SSL Certificate (**server**) file to your keystore using the following command:

```
$JAVA_HOME/bin ./keytool -importcert -keystore appvance.jks -alias nsdserver -  
trustcacerts -file <server name crt> <mydomain.com.crt>
```

The **Certificate reply was installed in keystore** message is displayed.

2. Choose **Y** or **Yes** to trust the certificate.

Last updated: April 13, 2023

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

macOS Cannot Verify AIQ App Developer Warning

Recommended guidance

macOS may block an AIQ application when Gatekeeper cannot verify the developer or when the file is quarantined after download. Treat this as a macOS security workflow; the user or administrator must approve the app through the approved company process.

Before troubleshooting

- Confirm the AIQ package came from an approved Appvance distribution channel.
- Verify macOS version, CPU architecture, AIQ version, checksum, and installer type.
- Check customer security policy, device management, and administrator requirements.
- Do not document bypasses that weaken macOS security controls.

Validation workflow

1. Have the user or administrator approve the app using the approved macOS flow.
2. Launch AIQ and confirm required permissions are granted by the user.
3. Run login, Scenario Editor, Service Suite, and browser smoke tests.
4. Document version, source, and approval owner without exposing credentials.

Last updated: October 7, 2026

What is the Required Java Version for AIQ?

The current required version of Java for AIQ is Java 11. Even though it is an older release, Java 11 remains the best fit for AIQ at the moment.

Java 11 still actively supported and will still receive security patches and updates for a period of years after active support ends.

For more information, refer to the end-of-life, release policy and support schedules here:

[Java/OpenJDK](#)

Last updated: April 13, 2023

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

Troubleshoot Windows RDP Access for Non-Administrator Accounts

Troubleshoot Windows RDP Access for Non-Administrator Accounts

Last reviewed: September 21, 2026

Use this article when a non-administrator account cannot connect to a Windows AIQ host using Remote Desktop. Coordinate changes with the system owner and follow access-control policy.

When to use this guidance

- A user can authenticate but cannot open an RDP session.
- The account is intended for operational access without local administrator rights.
- You need to separate Windows access issues from AIQ application issues.

Recommended approach

1. Confirm the host is reachable and RDP is enabled by policy.
2. Verify the user is allowed to log on through Remote Desktop Services.
3. Check local or domain group membership, Group Policy, and any deny-logon settings.
4. Review Windows event logs for the rejected session.
5. Apply the least-privilege group or policy change and retest.

Note: Do not grant local administrator rights simply to solve RDP access unless policy explicitly requires it.

Last updated: September 21, 2026

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

Legacy Chrome HTTPS 8443 Troubleshooting for AIQ

This page is retained as a legacy reference for older Chrome HTTPS port 8443 issues in AIQ environments.

What changed in this article

- Shortened the long question title and removed Designer-centric wording.
- Marked the localhost/8443 Chrome troubleshooting flow as legacy because current browser and certificate behavior may differ.
- Added checks for certificate trust, exact URL/port, proxy settings, browser version, and whether the issue reproduces in current supported execution paths.

Validation workflow

1. Confirm the current supported browser and AIQ URL before following older Chrome troubleshooting steps.
2. Verify certificate trust, proxy settings, port 8443 reachability, and controller service status.
3. If the issue is browser-specific, record the Chrome version and compare with another supported browser path.

Review note: This article should not be used as the primary setup guide for current AIQ browser testing.

Last updated: October 2, 2026

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

Legacy Firefox HTTPS Localhost Troubleshooting for AIQ

Last reviewed: September 30, 2026

This page is retained as a legacy reference for older Firefox HTTPS localhost issues in AIQ environments.

What changed in this article

- Shortened the long question-style title and marked the Firefox/Designer localhost workflow as legacy.
- Replaced Designer wording with AIQ terminology while noting that old Firefox certificate/profile behavior may no longer match current browser versions.
- Added checks for trusted certificate, localhost URL, port 8443, browser version, proxy settings, and whether the issue still reproduces in supported browsers.

Validation workflow

1. Confirm the current supported browser path before troubleshooting an older Firefox localhost issue.
2. Verify certificate trust, URL/port, proxy settings, and whether the AIQ service is reachable on localhost.
3. If the issue is Firefox-specific, document the browser version and compare with a supported Chrome/Edge execution path.

Review note: This page should not be used as primary setup guidance for current AIQ browser testing.

Last updated: September 30, 2026

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

Enabling Chrome Flash plugin and other settings using Chrome Browser Cloud Management

Upgrade the AIQ Controller and Test Nodes

Use this article to plan and validate an AIQ Controller and Test Node upgrade with backups, compatibility checks, and post-upgrade smoke tests.

What changed in this article

- Rewrote the title with current AIQ Controller and Test Node terminology.
- Added upgrade planning checks for backup, version compatibility, maintenance window, Test Node sequencing, browser/runtime dependencies, and rollback readiness.
- Added post-upgrade validation for login, node heartbeat, scenario execution, logs, and reports.

Validation workflow

1. Back up required configuration and data, confirm target version compatibility, and schedule a maintenance window.
2. Upgrade the controller and Test Nodes according to the approved release procedure and verify services start cleanly.
3. Run smoke tests covering login, node heartbeat, one small execution, report access, and integration checks.

Review note: This page now emphasizes controlled upgrade validation instead of only procedural upgrade steps.

Last updated: October 2, 2026

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

Install the AIQ Certificate on an iPhone

Last reviewed: September 29, 2026

Use this article when an iPhone must trust the AIQ recording or proxy certificate for mobile traffic testing.

What changed in this article

- Corrected grammar from “a iPhone” to “an iPhone” and clarified the certificate is for AIQ/mobile traffic workflows.
- Added iOS-specific checks for profile installation, certificate trust settings, Wi-Fi/proxy configuration, and Safari/app validation.
- Added a warning that MDM, VPN, or corporate device policies can block manual certificate trust changes.

Validation workflow

1. Install the AIQ certificate profile on the iPhone using the approved delivery method.
2. Enable full trust for the certificate in iOS certificate trust settings if required.
3. Open the target site or app and confirm traffic is captured without TLS/certificate errors.

Review note: This page now aligns with iOS proxy/certificate setup used for AIQ mobile traffic recording.

Last updated: September 29, 2026

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

Best Practices to Improve AIQ Performance

Best Practices to Improve AIQ Performance

Use these practices to keep AIQ executions stable, maintainable, and meaningful. Performance depends on scenarios, Test Nodes, controller health, data, browsers, and the target application.

Recommended guidance

- Validate scenarios with small runs before scaling.
- Use condition-based waits instead of unnecessary fixed sleeps.
- Size Test Nodes for the expected browser, service, mobile, or performance workload.
- Document environment and version changes before comparing results.

Validation workflow

1. Run a focused validation execution.
2. Review output, errors, active users, and Test Node health.
3. Tune scenario logic, data, and environment settings in controlled steps.
4. Record the execution ID, environment, and assumptions with performance findings.

Last updated: September 20, 2026

Identify AIQ Java Processes in Windows Task Manager

Identify AIQ Java Processes in Windows Task Manager

Last reviewed: September 21, 2026

Use this article to identify which Java process belongs to an AIQ service before restarting, monitoring, or collecting diagnostics.

When to use this guidance

- Multiple Java processes are running on the AIQ host.
- You need to avoid stopping the wrong service.
- Support asks for process ID, memory, or command-line details.

Recommended approach

1. Open Task Manager with administrative visibility on the AIQ host.
2. Enable columns such as PID, command line, and working directory.
3. Match each Java process to its AIQ service by path, command-line arguments, service name, and start time.
4. Use Resource Monitor or service management tools if Task Manager does not show enough detail.
5. Record the PID and service name in the support ticket before taking action.

Note: Do not end Java processes as a first step. Stop or restart AIQ services through the supported service controls whenever possible.

Last updated: September 21, 2026

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

How to encrypt scenario's ec2 cloud config files using API calls

Legacy Outlook Email Status Update via HTTP Call

Last reviewed: September 30, 2026

This page is retained as a legacy integration reference for environments that still update Outlook email status through an HTTP call.

What changed in this article

- Marked the Outlook HTTP-call procedure as legacy and integration-specific because Microsoft authentication and Graph/API behavior can change.
- Added checks for OAuth/token handling, endpoint ownership, least-privilege permissions, response validation, and audit logging.
- Added guidance to avoid hard-coded credentials and to confirm whether Microsoft Graph or a maintained integration should replace this approach.

Validation workflow

1. Confirm the customer still needs this legacy HTTP-call workflow and identify the supported endpoint.
2. Validate authentication, permission scope, request body, expected status code, and failure response in a controlled test.
3. Document token storage and audit requirements before using the workflow in shared automation.

Review note: This page now warns that Outlook status changes should use maintained Microsoft/API practices where available.

Last updated: September 30, 2026

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

Upgrade the AIQ Designer Proxy

Recommended guidance

Upgrade the AIQ Designer Proxy only when the target AIQ version, browser setup, and customer environment require it. Treat old “Appvance Designer” wording as legacy; use AIQ and Scenario Editor terminology for current guidance.

Before upgrading

- Confirm the current proxy version, target version, AIQ version, browser version, and operating system.
- Back up configuration, certificates, and any customer-specific proxy settings.
- Review firewall, antivirus, proxy, and certificate trust requirements.
- Schedule downtime if the proxy affects active recording or playback.

Validation workflow

1. Install or replace the proxy using the approved package.
2. Confirm the proxy starts and listens on the expected port.
3. Run a Scenario Editor recording or playback smoke test.
4. Review logs for certificate, permission, or connection errors.

Last updated: October 6, 2026