Update an Expired AIQ Certificate

Update an Expired Appvance Certificate

This process will let you manually update the Appvance Certificate on an existing build when the Certificate is expired.

This process should only be used if it is impossible to upgrade to the 5.2.5.1 release of AIQ which contains an updated certificate.

Requirements

- Contact Appvance customer support to obtain the following files:
  - appvance.jks (only needed for Controller and Test Nodes)
  - localhost.jks (only needed for Controller and Test Nodes)
  - ca.zip

  For the 2025 Certificate upgrade, the files are attached below.
- Controller Access: You will need access to the AIQ Controller via RDP or SSH to replace some files in the Controller.
- End Users/Testers will need to modify their local installations of the Web Designer client.

Steps for End Users

These steps will allow testers to continue working with their scripts using the same AIQ build that has an expired certificate.

1. Remove the contents of the **`ca`** folder located at `$HOME/Web Designer/NetworkProxy/NetworkProxy/certgen/X509CA/ca` and replace them with the files inside the `ca.zip` file.

2. Remove the contents of the **`certs`** folder located at `$HOME/Web Designer/NetworkProxy/NetworkProxy/certs`
3. Add the certificate `new_ca.cer` to the end user's operating system and trust it.
   The `new_ca.cer` certificate is contined in the `ca.zip` file. You can also download it from https://aiq-certificate.s3.us-west-1.amazonaws.com/2025/new_ca.cer.
   - Windows: Double-click on `new_ca.cer` and install the certificate in the **Trusted Root Certificates** folder.
   - Mac OS: Double click on `new_ca.cer` and install the **Appvance 2025** certificate in **KeychainAccess** app.

AIQ Controller Test Nodes

When connecting to the AIQ Controller you will have to accept the security warning displayed by the browser. A red message will display in left of the browser's URL.

This update is only required for AIQ versions prior to AIQ 5.2.5.1. If you have AIQ 5.2.1 or later installed, you do not need to perform this update.

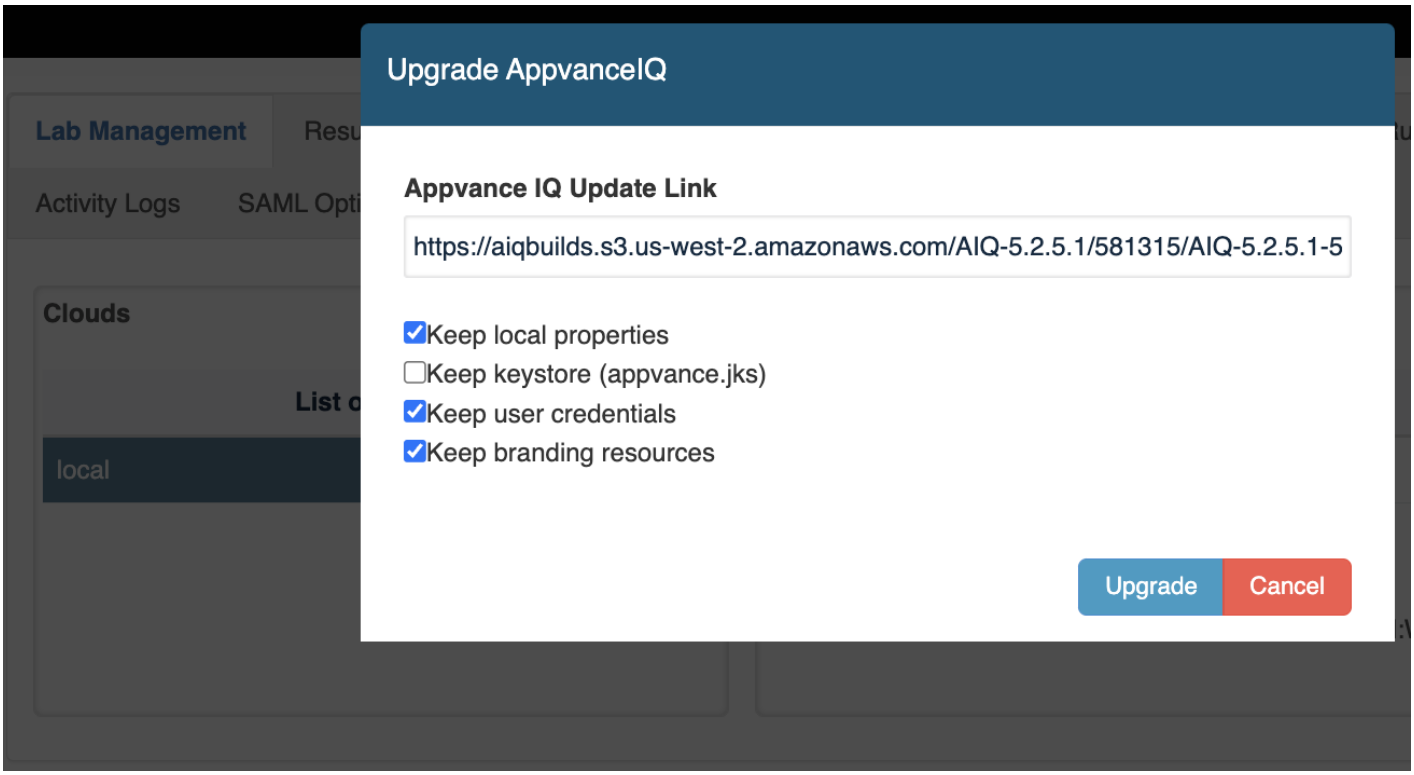
1. Connect to the AIQ Controller and replace the **`appvance.jks`** file located at `aiq_distribution/TestNode/etc/appvance.jks`.
   If you have Test Nodes, replace this file in the Test Nodes as well.
2. Connect to the AIQ Controller and replace the **`localhost.jks`** file located at `aiq_distribution/NetworkProxy/config/localhost.jks`.
   If you have Test Nodes, replace this file in the Test Nodes as well.
3. Connect to the AIQ Controller and remove the contents of the **`ca`** folder located at `aiq_distribution/NetworkProxy/certgen/X509CA/ca`, and replace them with the files inside the `ca.zip` file.
   If you have Test Nodes, update this folder in the Test Nodes as well.
4. Connect to the AIQ Controller and remove the contents of the **`certs`** folder located at `aiq_distribution/NetworkProxy/certs`.
5. Add the certificate (**`new_ca.cer`**) to the AIQ Controller operating system and trust it. This file is located in the `ca.zip` file.
   - Windows: Double-click on `new_ca.cer` and install the certificate in the **Trusted Root Certificates** folder.
   - Mac OS: Double click on `new_ca.cer` and install the **Appvance 2025** certificate in **KeychainAccess** app.

   If you have Test Nodes, add and trust the certificate in the Test Nodes as well.
6. Recreate the Controller domain certificate.
   a. Log in to AIQ and navigate to **Admin Options** > **Certificate**.
   b. Provide the DNS or IP of your Controller (for example `ec2-18-144-104-71.us-west-1.compute.amazonaws.com`) so the domain certificate is properly signed with the new `ca` certificate.

   This will reboot the AIQ controller, so your team should be notified about this before you proceed.

Upgrading using Lab Management

If you are upgrading from a version less equals or less than 5.2.5 to an AIQ version with new certificate, you must deselect the “**Keep keystore (appvance.jks)**” option in the **Upgrade Appvance IQ** dialog in Lab Management.



If you do not deselect this option, the new certificate will not be installed in the Controller’s `appvance.jks`. You will receive “unsecure” error messages and warnings from the browser when navigating to that Controller even after recreating the Certificate.

Using AWS Console

If you do not have access to RDP you can also install the new Appvance certificate using the AWS console.

1. Connect to the node.
2. Open a powershell terminal.
3. Paste the following commands:

```
# Define the path to the certificate
$certPath = "C:\AIQ\aiq_distribution\NetworkProxy\certgen\X509CA\ca\new_ca.crt"
# Install the certificate
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cert.Import($certPath)
```

```
$store = New-Object System.Security.Cryptography.X509Certificates.X509Store("Root",
"LocalMachine")
$store.Open("ReadWrite")
$store.Add($cert)
$store.Close()
```

This will install and trust the AIQ certificate.

File Download Links

Here are the required files for the 2025 AIQ Certificate upgrade:

- localhost.jks
- appvance.jks
- ca.zip

Last updated: March 04, 2025

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

---

Revision #7
Created 2026-07-31 15:38:37 UTC by Admin
Updated 2026-11-17 22:00:27 UTC by AI_Mananger