Resolve AppDynamics SSL/TLS Issues after DigiCert Root G2 Update

Contents

Introduction

This document describes how to address **SSL (Secure Socket Layer)/ TLS (Transport Layer Security)** certificate trust issues in AppDynamics Agents.

Prerequisites

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

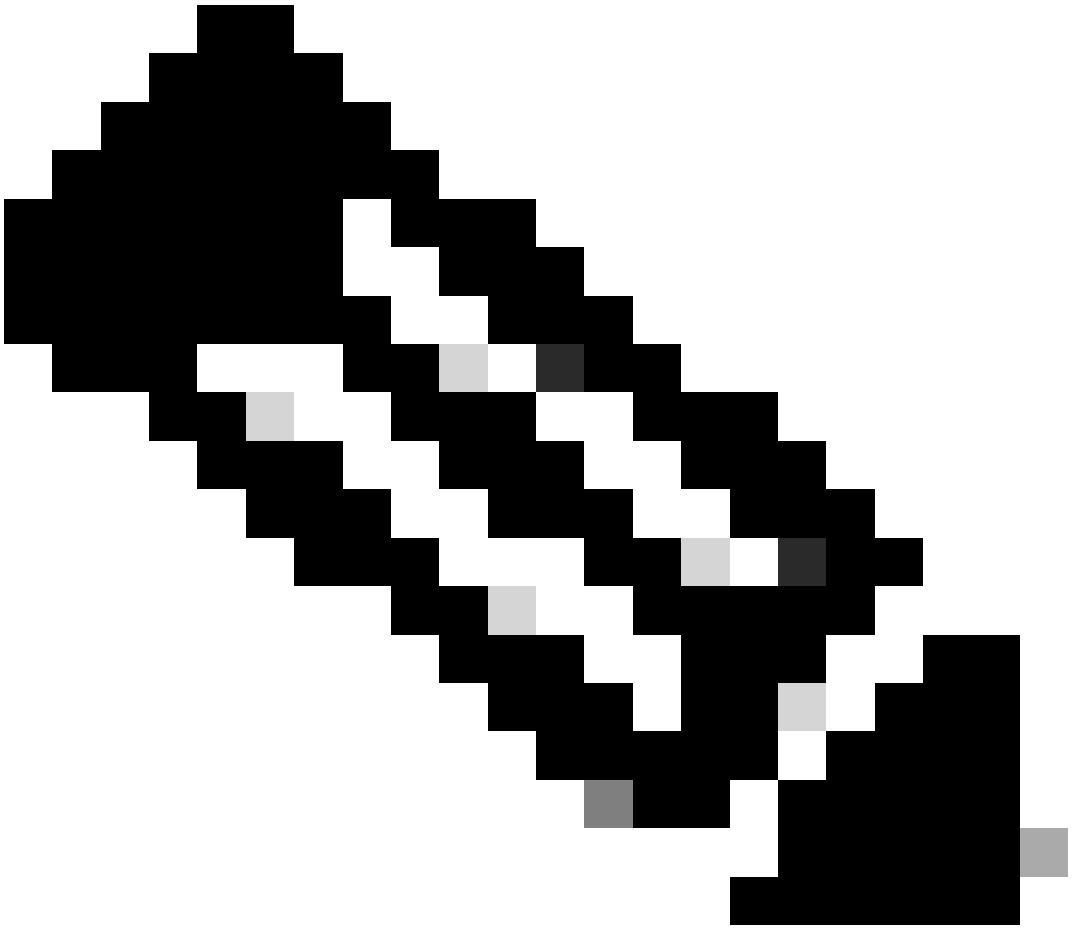
This document describes how to address SSL (Secure Socket Layer)/ TLS (Transport Layer Security) certificate trust issues in AppDynamics Agents after the recent migration from DigiCert Global Root CA to DigiCert Global Root G2.

It provides detailed steps to ensure proper configuration and restore seamless connectivity.

In 2023, DigiCert initiated the transition to the DigiCert Global Root G2 signing certificate for issuing public TLS/SSL certificates. This change was prompted by Mozilla updated trust policy, which mandates that root certificates be updated every 15 years, and distrusting older certificates starting in 2025.

The new signing certificate employs the more secure SHA-256 algorithm, replacing the older SHA-1 standard. As part of this transition, AppDynamics updated its SSL certificates for domain .saas.appdynamics.com to utilize the second-generation certificates on 2025-06-10.

This update caused some application agents to lose connectivity with SaaS Controllers due to their inability to recognize the new certificate. To ensure uninterrupted connectivity, it is crucial to update AppDynamics agent trust store to include the new DigiCert Global Root G2 and IdenTrust certificates.



> **Note**: This change primarily affects agents that are using the custom truststore or using a very old version of OS/java where the required certificate are not included in the default OS/Java truststore.

Problem

There is a connectivity problem between the AppDynamics Agents and the Controller, and the logs are showing errors related to SSL configuration or communication.

Example error message in the logs: "PKIX path building failed: xxxx: unable to find valid certification path to requested target attempting validation"

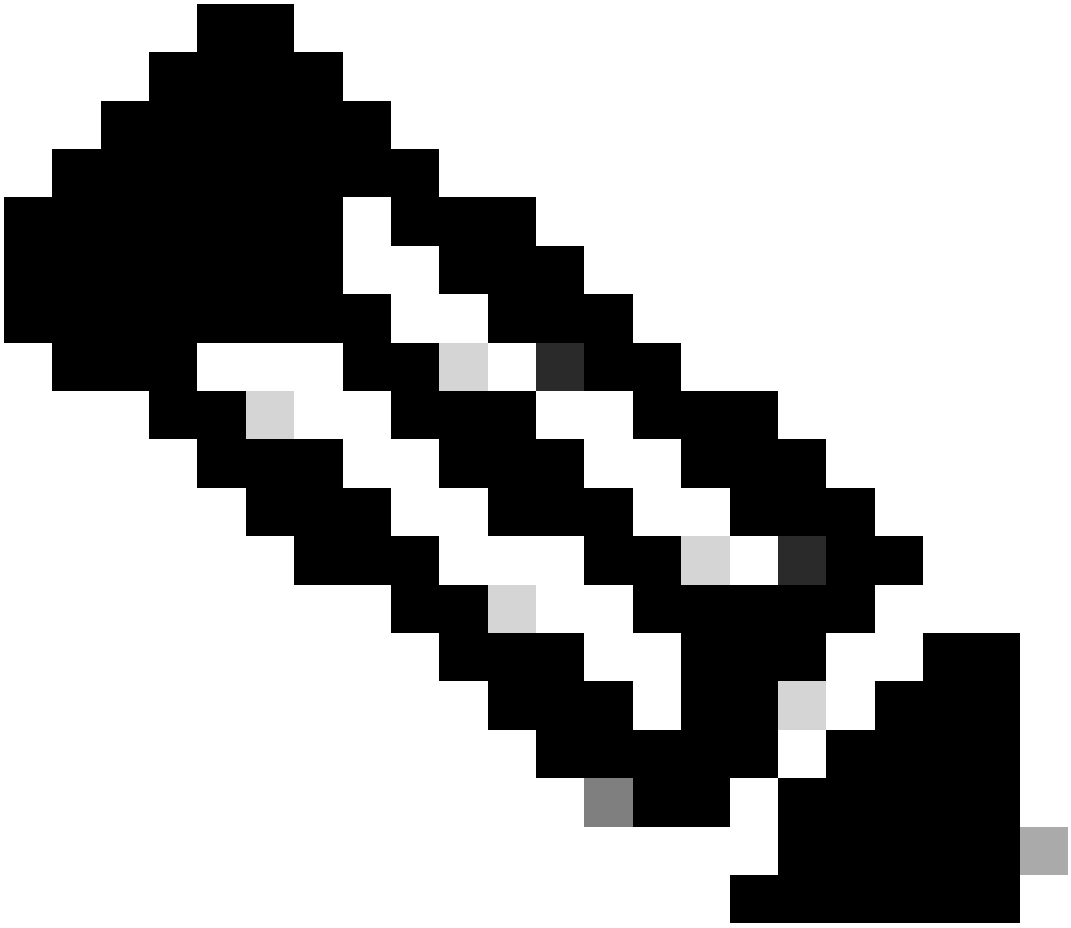
Solution

Step 1. Download Certificates

- DigiCert Global Root G2:
  - Visit DigiCert Trusted Root Authority Certificates
  - Search for "DigiCert Global Root G2" and download the certificate.

- IdenTrust:
  - Go to IdenTrust Commercial Root CA 1
  - Copy the certificate content and save it as a file (for example, Identrustcommercial.cer or Identrustcommercial.pem)

Step 2. Identify Truststore Location



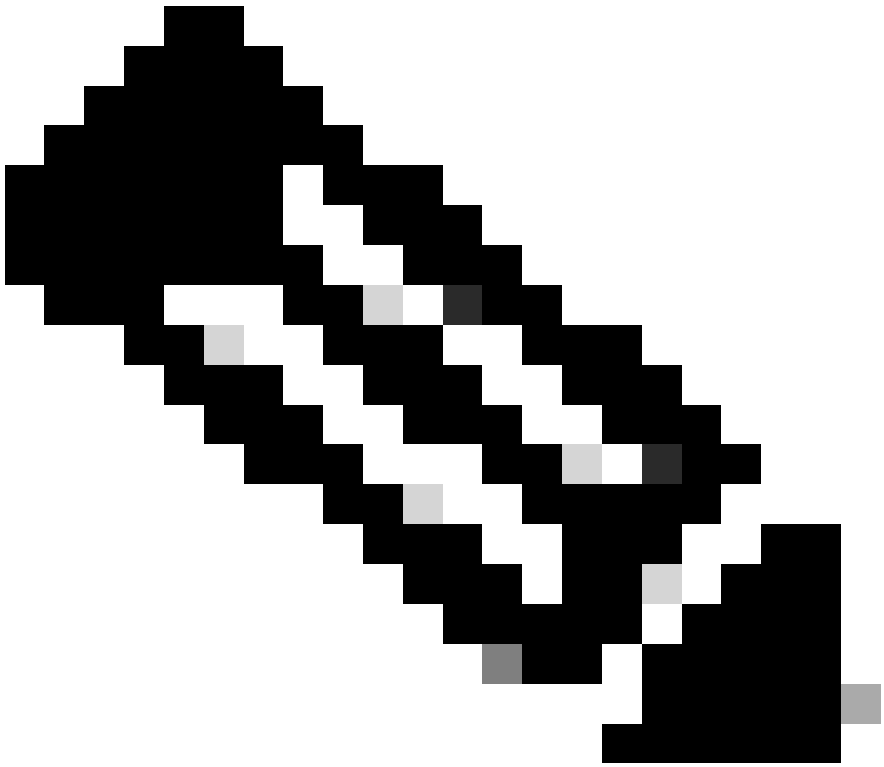
Note: Truststore Location is needed in Step 3. Import Certificates to the Truststore

---

- **Java, Database or Machine Agent**
  - JVM Argument Truststore Property
    1. Check if -Djavax.net.ssl.trustStore property in set as a JVM arguments when launching the agent.
    2. If this property is set, inspect the keystore file specified by this property to confirm it includes both certificates (DigiCert Global Root G2 and IdenTrust root certificates). *(If property is not set, proceed to the next step.)*
  - Controller Info XML
    1. The Agent can be configured to use keystore defined in the controller-info.xml file in your agent conf directory.
    2. Check for the controller-keystore-filename setting.
    3. If present, inspect the specified keystore file to confirm both the certificates are included.

(If not found, proceed to the next step.)

- Agent cacerts.jks File
  1. Check for a file named cacerts.jkswithin the conffolder of agent installation directory.
  2. Inspect this file to verify both the certificates are included.
     (If not found, proceed to the next step.)

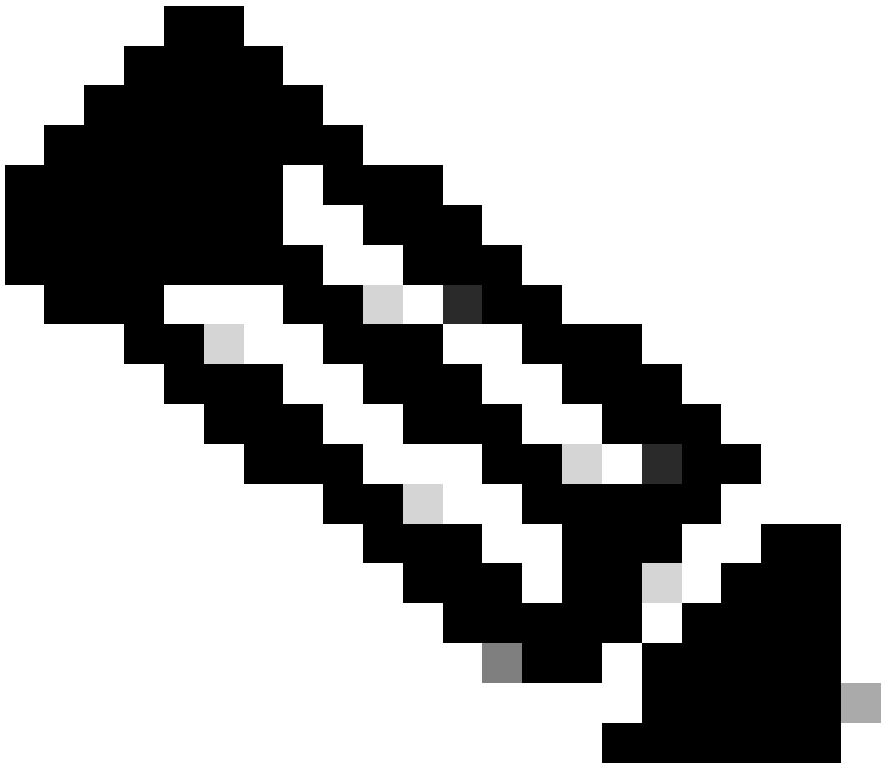


Note: Agent Installation Directory

For Java Agent: **AGENT_HOME/verxxx/conf** or **AGENT_HOME/conf**

For Machine or DB Agent: **AGENT_HOME/conf**

- JRE Default Truststore
  1. If none of the previous configurations are found,as a fallback, the agent uses the JRE default truststore, typically located at**JRE_HOME/lib/security/cacerts**.
  2. Inspect this file to ensure the certificates are included.



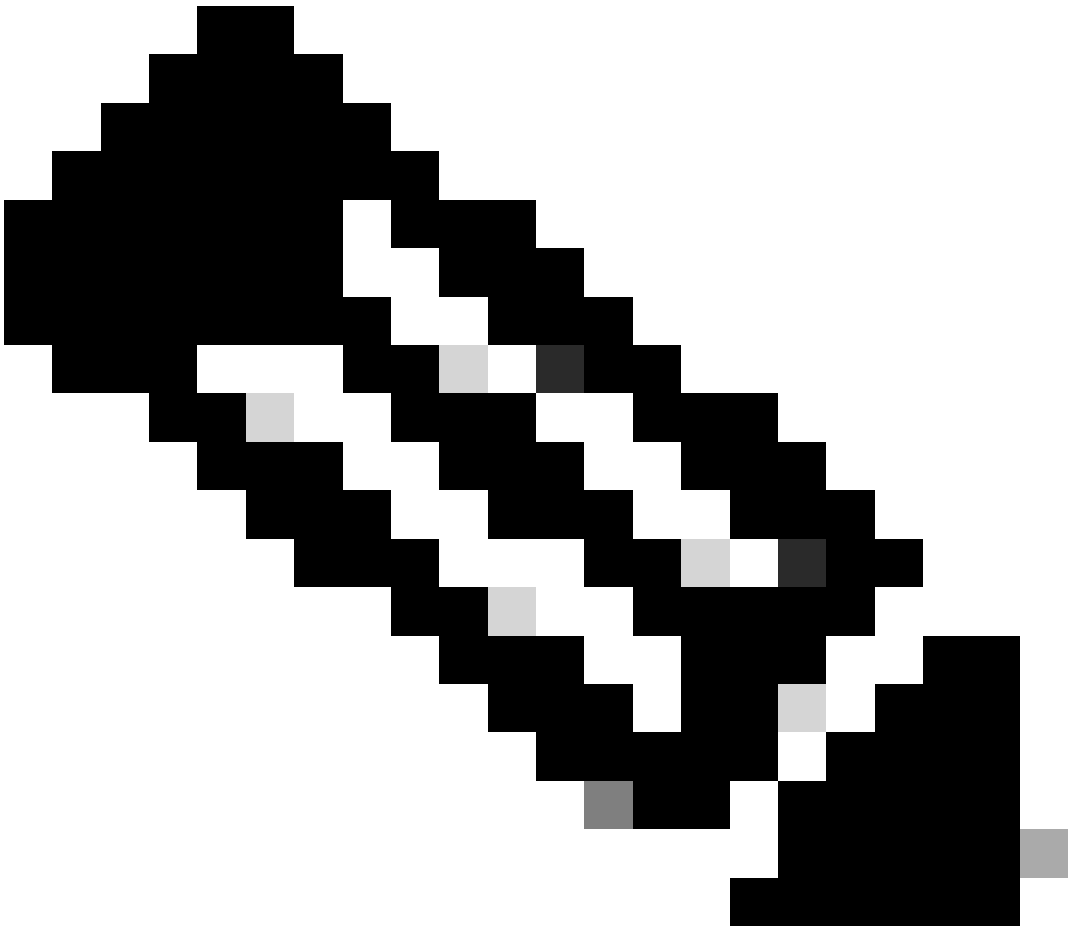
Note: If you are using IBM Websphere or IBM Websphere Liberty Profile, then the **JRE_HOME** is inside AppServer or Liberty Directory under Websphere installation directory respectively, that is, **IBM_WEBSPHERE_HOME/AppServer/java/** or **IBM_WEBSPHERE_HOME/Liberty/java/**

- **Analytics agent**
    - Check If the path (including name) of the agent truststore is specified using the **<ad.controller.https.trustStorePath>** element in the agent configuration file **analytics-agent.properties** then agent loads that trustore.
    - If not specified in the**ad.controller.https.trustStorePath,** it loads the default Java truststore of the JVM being instrumented, **<JRE_HOME>/lib/security/cacerts** (default password **changeit**)
    - If not specified in the **ad.controller.https.trustStorePath** and analytics agent is being used as a Machine agent extension then it loads the truststore used by machine agent.
- **DotNet Agent**
    - For **Windows**:
        - Navigate to the certificate installation view by going to**Run> MMC.exe>** select**File**from the **toolbar** and select**Add/Remove Snap-in**.
        - **Add or Remove Snap-ins**window opens, select**Certificates> ClickAdd. Certificate snap-in**window opens. Select**Computer Account> Choose Local or Another**

Computer accordingly >ClickFinish>OK.

- **Expand Certificates (Local Computer) >** Select the**Trusted Root Certification Authority** folder and expand to show the**Certificates**folder.
- Double Click on the**Certificates folder**and notice the list of existing trusted certificates. Identify if both the**DigiCert Global Root G2 and IdenTrust root certificates**are present otherwise import the missing certificates.

- For **Linux**:
  - The location of the trust store varies between Linux distributions. Common locations include:**/etc/ssl/certs** (OS like CentOS/RHEL/Debian)



Note: If the **DigiCert Global Root G2 or IdenTrust certificates** are missing from all these checked locations, you need to add them. Refer to the steps mentioned in "Step 3. Import Certificates to the Truststore" to import the certificates to the truststore.

Step 3. Import Certificates to the Truststore

- **Java, Database, Machine or Analytics Agent**

- Open your terminal or command prompt and use this keytool command to import **DigiCert Global Root G2 & IdenTrust Root Certificates**.

```
keytool -import -trustcacerts -alias <alias-name> -file <root_certificate_file_name> -keysto
```

Replace:

- <alias-name>: A unique alias (for example, digicertglobalrootg2, identrustcoomercial).
- <root_certificate_file_name>: Path to the certificate file (for example, /home/username/Downloads/DigiCertGlobalRootG2.crt).
- <agent_truststore_path>: Path to the agent truststore file (for example, /opt/appdynamics/agent/ver25.x.x.x/conf/cacerts.jks).
- <truststore_password>: Truststore password (default: changeit, unless customized).

- Example for Importing **DigiCert Global Root G2 Certificate**.

```
keytool -import -trustcacerts -alias digicertglobalrootg2 -file /home/username/Downloads/Dig
```

- Example for Importing **IdenTrust Commercial Root Certificate**.

```
keytool -import -trustcacerts -alias identrustcommercial -file /home/username/Downloads/iden
```

- **DotNet Agent**

  - For **Windows**:
    - Navigate to the certificate installation view by going to**Run> MMC.exe>** select**File**from the **toolbar** and select**Add/Remove Snap-in**.
    - **Add or Remove Snap-ins**window opens, select**Certificates> ClickAdd. Certificate snap-in**window opens. Select**Computer Account> Choose Local or Another Computer accordingly >ClickFinish>OK**.
    - **Expand Certificates (Local Computer) >** Select the**Trusted Root Certification Authority** folder and expand to show the**Certificates**folder.
    - Right-click **Certificates**folder and select**All Tasks > Import.**Certificate Import Wizard opens, go through the instructions and **add** the missing**DigiCert Global Root G2 certificate and/or IdenTrust Root Certificate.**

  - For **Linux**:

    - Copy the downloaded **DigiCert Global Root G2 & IdenTrust Root Certificate** files into the identified trust store directory.

    - Update the Trust Store by running the command.

```
sudo update-ca-certificates
```

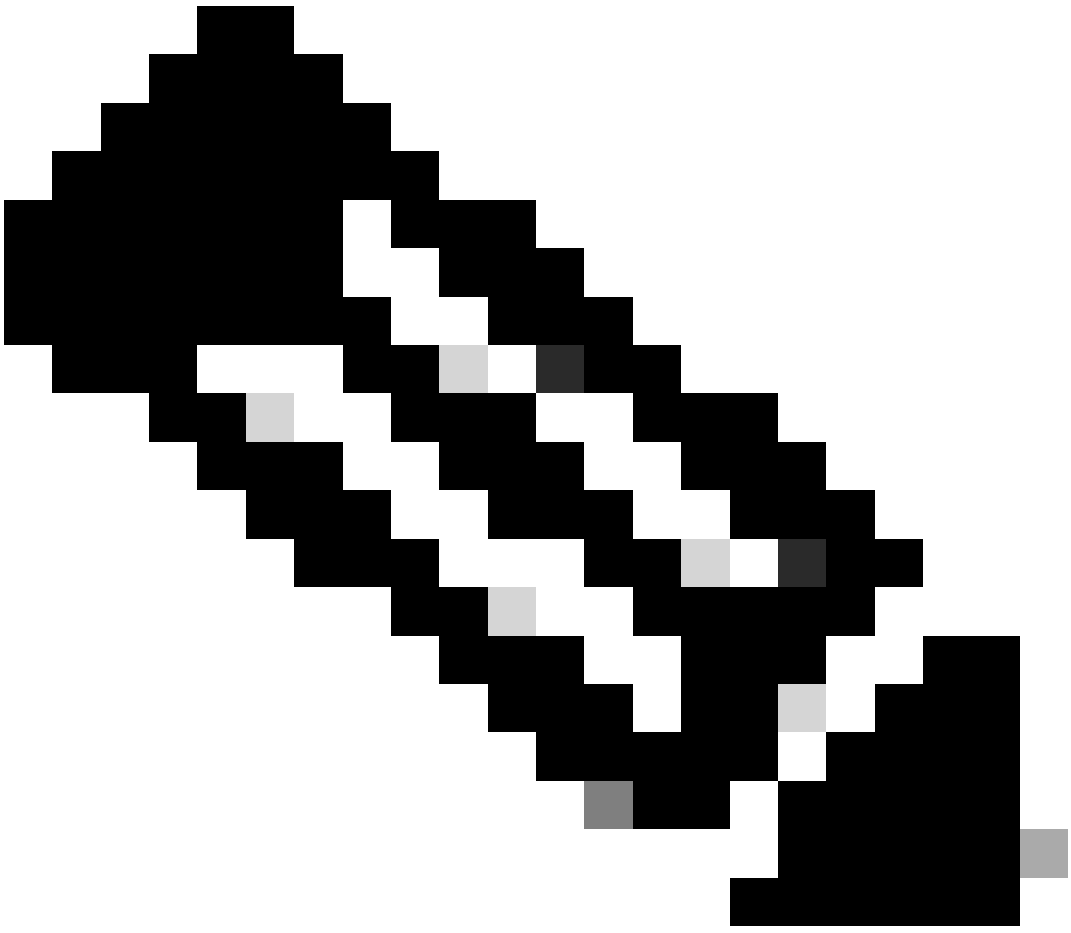
Step 4. Verify the Import

- **Java, Database, Machine or Analytics Agent**
  - To verify the certificates were successfully added, run the command:

    ```
    keytool -list -v -keystore <agent_truststore_path> -storepass <truststore_password> | grep -
    ```

    Replace:

    - `<agent_truststore_path>`: Path to the agent truststore file.
    - `<truststore_password>`: The truststore password.



Note: Ensure both **DigiCert Global Root G2** and **IdenTrust Commercial Root CA 1** appear in the output.

- **DotNet Agent**
    - For **Windows**:
        - Navigate to the certificate installation view by going to**Run**> **MMC.exe**> select**File**from the **toolbar** and select**Add/Remove Snap-in**.
        - **Add or Remove Snap-ins**window opens, select**Certificates**> **ClickAdd. Certificate snap-in**window opens. Select**Computer Account**> **Choose Local or Another Computer accordingly** >**ClickFinish**>**OK**.
        - **Expand Certificates (Local Computer)** > Select the**Trusted Root Certification Authority** folder and expand to show the**Certificates**folder.
        - Double Click on the**Certificates folder**and you must see both the**DigiCert Global Root G2 and IdenTrust root certificates**there.
    - For **Linux**:
        - Run the command and check if**DigiCert Global Root G2 & IdenTrust Root Certificate**exists:

```
awk '/-----BEGIN CERTIFICATE-----/,/-----END CERTIFICATE-----/ {
    print > "/tmp/current_cert.pem"
    if (/-----END CERTIFICATE-----/) {
        system("openssl x509 -noout -subject -in /tmp/current_cert.pem | grep -E \"Digi
        close("/tmp/current_cert.pem")
    }
}' /etc/ssl/certs/ca-certificates.crt
```

Step 5. Restart the Agent

Finally, restart your AppDynamics agent. This allows the changes to take effect.

Related Information

Support Advisory: Adding DigiCert and IdenTrust Root SSL Certificates to Agent Trust Stores

Need Further Assistance?

If you have a question or experiencing issues, please create asupport ticketwith these details:

- Logs from the agent.
- Details of the truststore location and certificates added.
- Any error messages encountered.