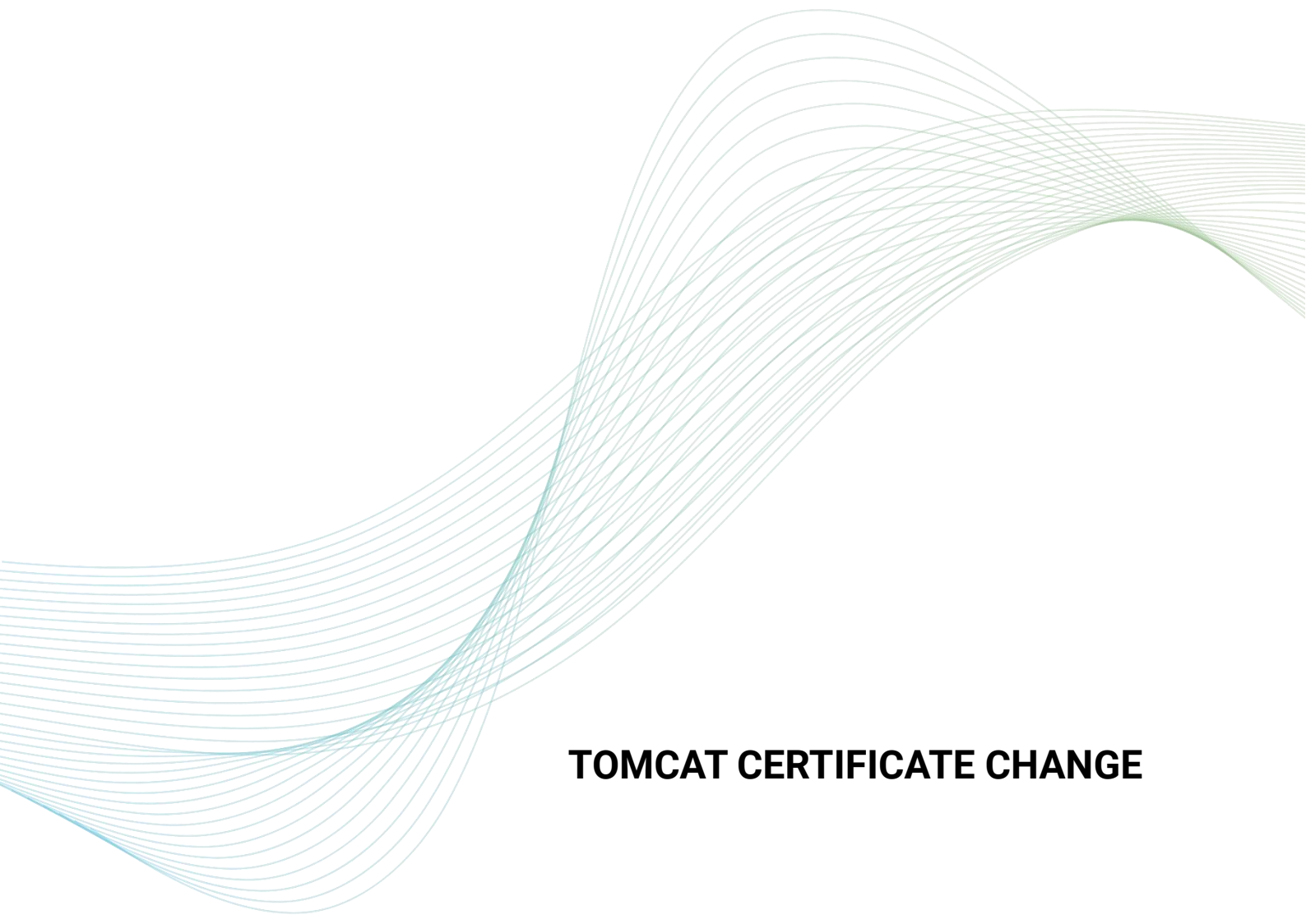


A decorative graphic consisting of numerous thin, overlapping wavy lines in light blue and green, flowing from the left side of the page towards the right, creating a sense of motion and depth.

TOMCAT CERTIFICATE CHANGE

Table of Contents

Table of Contents	2
1 Introduction	3
2 Prerequisites	4
2.1 Installing Keytool on Windows	4
3 Creating New Tomcat Certificate	6

1 Introduction

This guide provides step-by-step instructions to help you create and configure a certificate for Apache Tomcat. Whether you are installing a self-signed certificate or obtaining one from a trusted Certificate Authority (CA), this document will ensure a seamless setup process. The guide also includes essential prerequisites, such as verifying the availability of `keytool.exe` and configuring your Java SDK to prevent potential issues during implementation.

2 Prerequisites

Before creating a new certificate and reconfiguring Tomcat, ensure that the **keytool.exe** utility from the Java SDK package is installed. If not, install keytool on Windows first and after that create a new Tomcat certificate.

The description on how to install keytool on Windows is provided in more detail in the section below.

2.1 Installing Keytool on Windows

Step 1: Download the Java Development Kit (JDK)

1. Visit the Oracle JDK download page.
2. Select the appropriate JDK version for your Windows system.
3. Download the installer (e.g., jdk-21_windows-x64_bin.exe).

Step 2: Install the JDK

1. Run the downloaded installer.
2. Follow the on-screen instructions to complete the installation.
3. Note the installation directory (e.g., C:\Program Files\Java\jdk-21).

Step 3: Set the JAVA_HOME Environment Variable

1. Open the Start Menu and search for **Environment Variables**.
2. Select **Edit the system environment variables**.
3. In the **System Properties** window, click **Environment Variables**.
4. Under **System variables**, click the **New** button and add:
 - **Variable name:** JAVA_HOME
 - **Variable value:** Path to the JDK installation (e.g., C:\Program Files\Java\jdk-21).
5. Click the **OK** button to save.

Step 4: Update the PATH Environment Variable

1. In the Environment Variables window, find the **Path** variable under **System variables** and select **Edit**.
2. Click the **New** button and add the path to the JDK's bin directory (e.g., C:\Program Files\Java\jdk-21\bin).
3. Click the **OK** button to save.

Step 5: Verify the Installation

-
1. Open a new Command Prompt window.
 2. Type **keytool** and press **Enter**.
 3. You should see the keytool command options, confirming successful installation.

3 Creating New Tomcat Certificate

Step 1: Create a Keystore

1. Open a Command Prompt.
2. Run the following command:

```
"C:\Program Files\Java\jdk-21\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -keystore keystore.jks -storepass password -validity 365 -keysize 2048
```

3. Provide the required information (e.g., name, organization, etc.).

```
D:\temp\tomcat-certs>"C:\Program Files\Java\jdk-21\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -keystore keystore.jks -storepass password -validity 365 -keysize 2048
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
[Unknown]: Andrey Teterev
What is the name of your organizational unit?
[Unknown]: AppMill
What is the name of your organization?
[Unknown]: AppMill
What is the name of your City or Locality?
[Unknown]: Warszawa
What is the name of your State or Province?
[Unknown]: Mazowia
What is the two-letter country code for this unit?
[Unknown]: PL
Is CN=Andrey Teterev, OU=AppMill, O=AppMill, L=Warszaw, ST=Mazowia, C=PL correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 365 days
for: CN=Andrey Teterev, OU=AppMill, O=AppMill, L=Warszaw, ST=Mazowia, C=PL
```

Step 2: Generate a Certificate Signing Request (CSR)

1. Run the following command to generate a CSR:

```
"C:\Program Files\Java\jdk-21\bin\keytool.exe" -certreq -alias tomcat -file appmill.com.csr -keystore keystore.jks -storepass password
```

2. The generated **appmill.com.csr** file will be used to request a certificate from a Certificate Authority (CA).

```
D:\temp\tomcat-certs>"C:\Program Files\Java\jdk-21\bin\keytool.exe" -certreq -alias tomcat -file appmill.com.csr -keystore keystore.jks -storepass password
```

Step 3: Obtain the SSL Certificate

1. Submit the CSR to your chosen CA.
2. Obtain the SSL certificate files, which usually include the primary certificate, intermediate certificates, and root certificate.
3. For a self-signed certificate, run the following command:

```
"C:\Program Files\Java\jdk-21\bin\keytool.exe" -gencert -alias tomcat -infile appmill.com.csr -outfile appmill.com.crt -keystore keystore.jks -storepass password -validity 365
```

Step 4: Convert the Keystore to PKCS12 Format

1. Run the following command:

```
"C:\Program Files\Java\jdk-21\bin\keytool.exe" -importkeystore -srckeystore keystore.jks -destkeystore keystore.p12 -deststoretype PKCS12 -srcalias tomcat -deststorepass password -srcstorepass password
```

```
C:\Program Files\Java\jdk-21\bin>keytool -import -alias tomcat -keystore D:\temp\tomcat-certs\keystore.jks -file D:\temp\tomcat-certs\appmill.com.crt
Enter keystore password:
Certificate reply was installed in keystore
C:\Program Files\Java\jdk-21\bin>
```

Step 5: Extract the Certificate and Key from keystore

1. Extract the private key:

```
"C:\Program Files\AppMill\Clients\tomcat\bin\openssl.exe" pkcs12 -in keystore.p12 -nodes -
nocerts -out appmill.com.key -passin pass:password
```

2. Extract the certificate:

```
"C:\Program Files\AppMill\Clients\tomcat\bin\openssl.exe" pkcs12 -in keystore.p12 -nokeys -out
appmill.com.crt -passin pass:password
```

Step 6: Configure Tomcat for the New Certificate and Key

1. Locate the **httpd.conf** file in the conf directory of your Tomcat installation (e.g., C:\Program Files\AppMill\Clients\tomcat\conf).
2. Update the HTTPS port configuration by modifying the following lines:
 - SSLCertificateFile: Path to your new certificate (e.g., appmill.com.crt)
 - SSLCertificateKeyFile: Path to your new key (e.g., appmill.com.key)

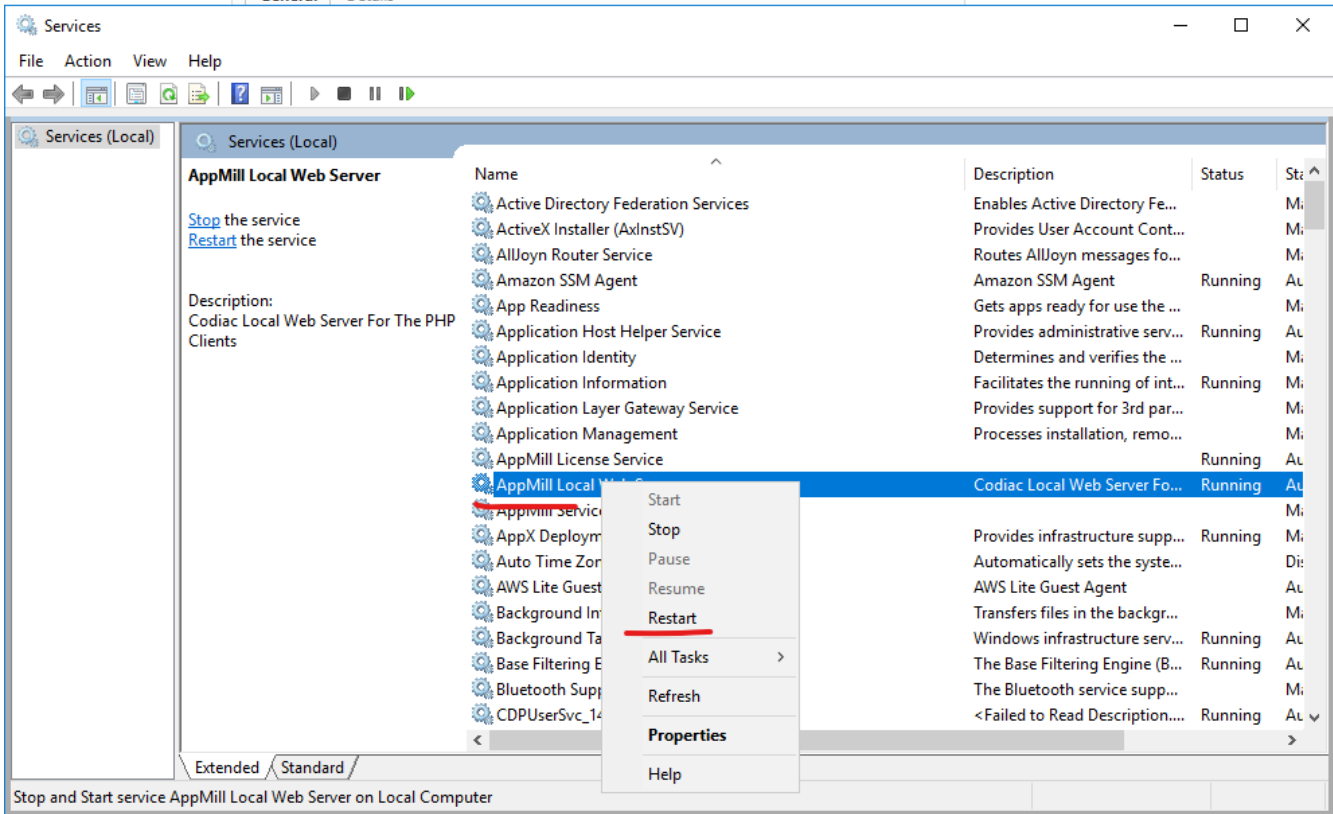
354		
355	<IfModule ssl_module>	
356	<VirtualHost *:8888>	
357	DocumentRoot	"C:/Program Files/AppMill/Clients/tomcat/modules-plus/system/html/default"
358	ServerName	"default"
359	ServerAlias	"default"
360		
361	SSLEngine	on
362	#Protocols	http/1.1
363	#Header always set	Strict-Transport-Security "max-age=94608000"
364	#SSLCACertificateFile	" "
365	#SSLCertificateChainFile	" "
366	SSLCertificateFile	"D:/temp/tomcat-certs/appmill.com.crt" }
367	SSLCertificateKeyFile	"D:/temp/tomcat-certs/appmill.com.key" }
368	SetEnvIf User-Agent	".*MSIE [6-9].*" ssl-unclean-shutdown
369		
370	<FilesMatch "\.(cgi shtml phtml php)\$">	
371	SSLOptions	+StdEnvVars
372	</FilesMatch>	

Step 7: Restart Tomcat

Restart the Tomcat server to apply the changes. To restart the **AppMill Local Web Server** on the device, please follow the steps below:

1. Enter **Services** to the search area in the Taskbar.
2. Open the **Services** application.
3. In the **Services** application window:
 - a. select the **AppMill Local Web Server** application and
 - b. click the **Restart** link at the top right corner of the window
 - or
 - c. right click on the **AppMill Local Web Server** application and select the **Restart** option from the list
 - or

- d. click the **Stop** and then **Start** links at the top right corner of the window.



Step 8: Verify the Installation

1. Open a browser and navigate to your site using: <https://127.0.0.1:8888>

