

KeyTalk automated Tomcat certificate renewal installation instructions

Introduction

Serving HTTPS traffic via Linux-based Tomcat webserver requires assigning a server SSL certificate for each SSL host defined by Tomcat. Typically, these certificates have a long lifetime. Decreasing certificate lifetime improves security, but increases maintenance work to generate and assign new certificates. This document explains you how to setup the KeyTalk Linux client to automatically renew Tomcat SSL certificates.

When set up, KeyTalk will periodically perform the following actions for each configured Tomcat SSL host:

1. Check the lifetime of the currently installed certificate
2. If the certificate is about to expire (typically less than 10% lifetime):
 - a. Retrieve a new SSL certificate from your KeyTalk server
 - b. Install and effectuate the retrieved certificate to the configured Tomcat SSL host.

The remaining document describes how to configure your KeyTalk client and server for automatic Tomcat SSL host certificate renewal.

System Requirements

Before installing the KeyTalk client with Tomcat certificate renewal script please make sure that your server meets the following requirements:

- Ubuntu 20.04 LTS x64 or Ubuntu 22.04 LTS x64 or Ubuntu 24.04 LTS x64
- Tomcat v8 or above installed with SSL module enabled

Installation and Configuration of Tomcat

Step 1: Install JAVA

Tomcat requires Java to be installed on the server so that any Java web application code can be executed.

Installing Java

```
sudo apt update
sudo apt install default-jdk openssl
```

Step 2: Install Tomcat

Ubuntu 24

```
sudo apt install tomcat10 tomcat10-*

sudo systemctl daemon-reload
sudo systemctl start tomcat10
sudo systemctl enable tomcat10
sudo systemctl restart tomcat10
```

Open in web browser **http://server_domain_or_IP:8080**

KeyTalk client configuration

Install and customize KeyTalk client

Before installing the KeyTalk client, make sure you have Tomcat installed, otherwise the Tomcat certificate renewal script will not be installed.

Extract:

```
tar -xf KeyTalkClient-<version>.linux.tar
```

Install using:

```
sudo ./install.sh
```

Alternatively, you can install from .deb package:

```
sudo apt -y update
sudo apt -y install KeyTalkClient_<version>.deb
```

Customize KeyTalk installation with a RCCD file:

```
sudo /usr/local/bin/keytalk/ktconfig --rccd-path <path-to-rccd>
```

Notice: RCCD installation for Tomcat integration must be done as root because the Tomcat certificate renewal script invoked by cron is also run as root and therefore will expect the KeyTalk configuration under '/root/tmp/' and '/root/.keytalk'

Test your installation is correct:

```
sudo /usr/local/bin/keytalk/ktclient --provider <keytalk-provider> --service <keytalk-service> --user <keytalk-user>
> --password <keytalk-password> --save-pfx
```

Configure Tomcat certificate renewal

NOTE : Configurations mentioned here are samples. The tomcat.ini file has to be updated based on user requirement.

Update the Tomcat certificate renewal configuration found at `/etc/keytalk/tomcat.ini` :

1: Specify Tomcat host(s) for which you want KeyTalk to automatically renew SSL certificates

Example IP-based Host:

```
"Host" : "localhost:8443"
```

Example name-based VHost:

```
"Host" : "localhost:443",
"ServerName" : "localhost",
```

2: Specify your Keystore password

Example:

```
"KeystorePassword" : "changeit",
```

3: "Keystorelocation" : "/etc/keytalk/keystore",

4: Specify KeyTalk server credentials

Example passwordless login:

```
"KeyTalkUser" : "www.example.com",
```

Example login with password:

```
"KeyTalkUser" : "www.example.com",
"KeyTalkPassword" : "secret"
```

Configure Tomcat for SSL

Open server.xml file in edit mode. The file is available under the Tomcat directory, default path is `/etc/tomcat/server.xml` or `/etc/tomcatX/server.xml` (where X is Tomcat version number).

1: Incase tags to Connector element `<Connector port="8443">` are commented, uncomment the tags. NOTE : The comments in the server.xml file are enclosed in `<!--` and `-->`.

2: Update the Connector element to be similar to the one shown here in example:

To enable SSL, update the values for port, keystoreFile, KeystorePass, ClientAuth, SSLprotocol. where - KeystoreFile and KeystorePass have values mentioned in tomcat.ini file.

```
<Connector port="8443" protocol="<DEFAULT_PROTOCOL>" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="/etc/keytalk/keystore" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
```

NOTE : To change port number to a privileged port (<1023) you have to grant special permissions to Tomcat. Please follow https://github.com/KeyTalk/windows-linux-client/tree/master/Software/Documentation/Tomcat_over_privileged_ports.md to enable Tomcat to use the privileged ports. Do not forget to update the required port in the above connector.

3: Save server.xml

4: Run tomcat.sh to initialize JAVA Keystore. /usr/local/bin/keytalk/tomcat.sh <KEYSTORE_PASSWORD> <KEYSTORE_LOCATION>

Example:

```
/usr/local/bin/keytalk/tomcat.sh changeit /etc/keytalk/keystore
```

5: Do a test run by calling (Make sure your default Python version is 2.7.x) :

```
sudo /usr/local/bin/keytalk/renew_tomcat_ssl_cert
sudo /usr/local/bin/keytalk/renew_tomcat_ssl_cert --force (for force renewal)
```

6: In your browser, navigate to the host you configured and check that it is SSL enabled. For Example: <https://localhost:8443>

7: Once everything works as expected, enable certificate renewal cron job by Uncommenting the relevant line in

```
/etc/cron.d/keytalk-tomcat
```

Enjoy!

Troubleshooting

Location of Tomcat certificate renewal log

```
~/tmp/kttomcatcertrenewal.log
```

My current certificate won't renew

By default, the renewal script will only refresh the certificate if the currently installed certificate for this Host has left than 10% of its validity duration left. In some cases, such as first-time installation of a certificate, a changed tomcat.ini (Host configuration), or changed KeyTalk service configuration, you may want to force a refresh sooner.

To force a refresh, even though the current certificate is not about to expire, use:

```
sudo /usr/local/bin/keytalk/renew_tomcat_ssl_cert --force
```

My certificate is not trusted by browsers at the client

Possible reasons are:

- The browser at your client did not install the required CA certificates to verify the full certificate chain.
- There is a `Subject Alternative Name` defined in the browser which takes precedence over the Common name. If this is the case, please update (or remove) the `Subject Alternative Name` field in your KeyTalk service.
- Your Tomcat host configuration has an incorrect "ServerName" or "Host" directive.

Possible Resolution:

- Restart web browser.

I still can't solve my problem

Please create a problem report with

```
sudo /usr/local/bin/keytalk/ktprgen
```

and send it to support@keytalk.com