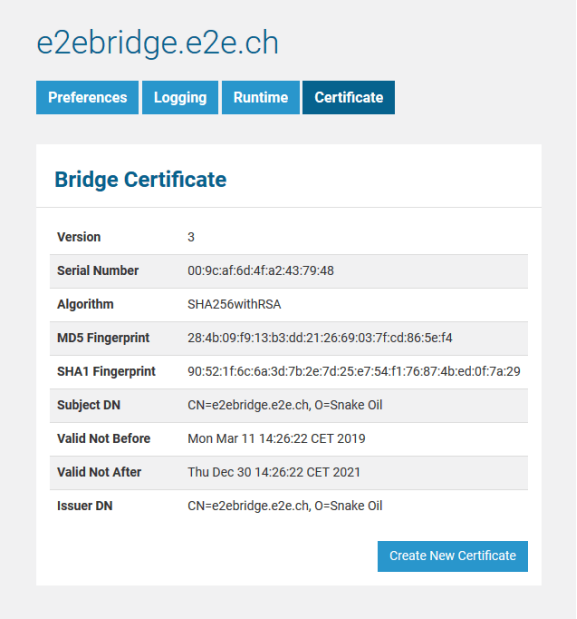
Managing the Bridge Certificate

Switch to the **Certificate** tab in the information/working area.
All users have access to the certificate information. However, only users who are member of a group, to which the role **ADMIN** has been assigned, can create a new certificate.

Figure: Bridge Certificate



The certificate tab shows the details of the currently used self-signed certificate of the Bridge.

On this Page:

Related Pages:

- Importing and Exporting Proxy Server Certificates
- Tomcat: SSL Configuration HOW-TO

Renewing the Self-signed Certificate

If the certificate has expired (see **Valid Not After**), administrators can create a new certificate by clicking **Create New Certificate**. The Bridge will generate a new certificate without any further confirmation. To enable the new certificate, you have to restart the Bridge. The new certificate will be valid for another 1025 days.

> Make sure that you are updating your certificate if it still uses MD5 algorithm (which is deprecated as insecure). If you are updating your Bridge from a version that is still accepting MD5 certificates to a newer version, you may get locked out of your Bridge installation.

Newer Bridge versions will create self-signed certificates using SHA256.

Installing a Purchased Server Certificate

Prerequisites

- To create a new Tomcat keystore and to import the purchased certificate to it, you need a machine with a Java Development Kit (JDK) installed. This does not necessarily have to be the machine the Bridge is running on.
- The certificate must be available as PKCS12 file (.p12), containing the certificate as well as the intermediate and private keys. If you have already installed the certificate for your proxy services, you can just export the installed certificate as described in Importing and Exporting Proxy Server Certificates.

Creating a New keystore

1. Import the certificate into a new Tomcat keystore called **tomcat.keystore**. The keystore password has to be **changeit**.

```
<path to your JDK>/jdk1.7.0_80/bin/keytool -importkeystore -
srckeystore <filename of the certificate>.p12 -srcstoretype pkcs12 -
srcstorepass <password of the certificate file> -destkeystore tomcat.
keystore -deststoretype jks -deststorepass changeit
```

Execute this command in the same folder the certificate file resides in. The output of the command should look like:

```
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries
failed or cancelled
```

2. Create a Tomcat alias in keystore **tomcat.keystore**.

```
<path to your JDK>/jdk1.7.0_80/bin/keytool -changealias -alias 1 -
destalias tomcat -keystore tomcat.keystore -storepass changeit
```

3. Verify the keystore.

```
<path to your JDK>/bin/keytool -list -keystore tomcat.keystore -
storetype jks -storepass changeit
```

The output of the command should look like:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
tomcat, Sep 23, 2015, PrivateKeyEntry,
Certificate fingerprint (SHA1): 20:97:3D:5C:42:04:[...]
```

Please note: Without further configuration both passwords have to be *changeit*.

Installing the New keystore

1. Stop the Bridge.
2. Make a backup of your old tomcat.keystore file.
3. Replace the existing **tomcat.keystore** in folder **<your Bridge data directory>/servlets/conf** by the new one.
4. Restart the Bridge.
   If something went wrong, restore the Tomcat backup.

For more information on Tomcat SSL configuration, refer to Tomcat: SSL Configuration HOW-TO.