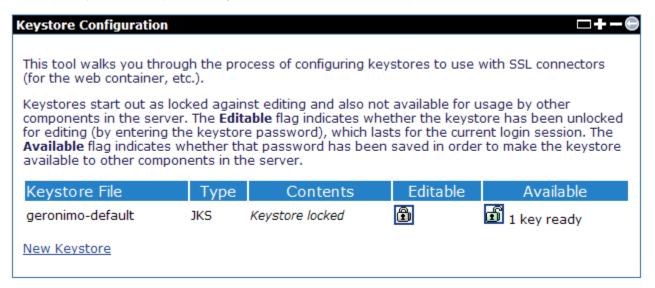
Administering certificates

Administering Security

Administering security realms \$\square\$

This section is about how to administer certificates from the administration console.

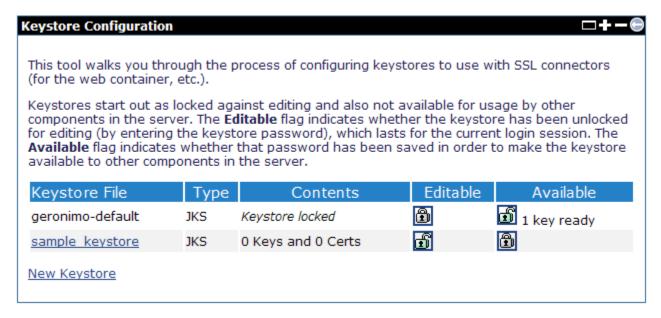
To administer SSL certificates, the **Keystore Configuration** portlet is available by selecting **Keystore** on the **Console Navigation** menu on the left side. From this portlet, you can either import an existing certificate or create a new certificate request.



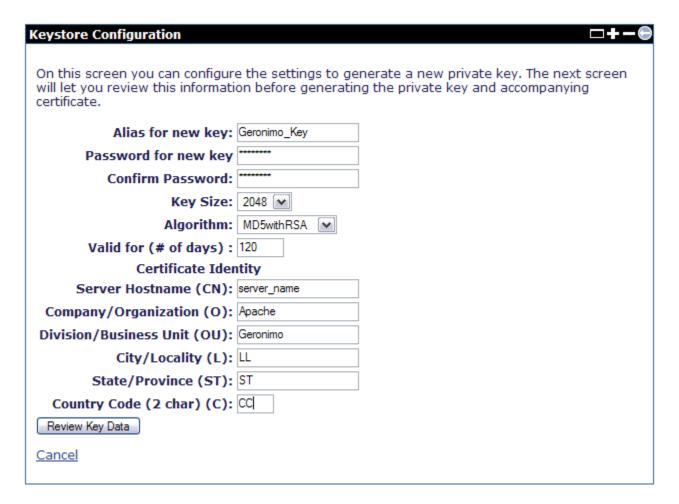
The certificates in Geronimo are stored in a keystore located in \var\security\keystores\geronimo-default.

If you want to use a different keystore other than the one provided by default, you can create one by clicking **New Keystore**. You will be prompted with a keystore name and a password, enter those values and click **Create Keystore**. For this example, the keystore is named sample_keystore.

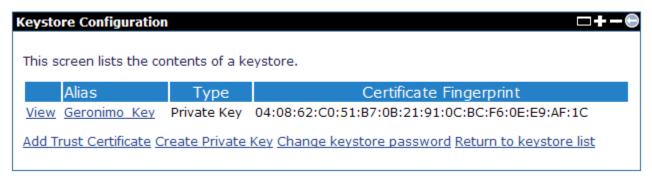
The keystore you just created does not yet contain any certificates nor key as depicted in the following figure. Also note that the keystore is by default locked, that is the closed lock in the **Available** column. After you create the certificate, you will need to click on the lock to make that certificate available, and you will be prompted with the passwords for the keystore and certificate.



To create a private key, click the keystore you just created and on the next page click Create Private Key. Enter valid data in the appropriate field.

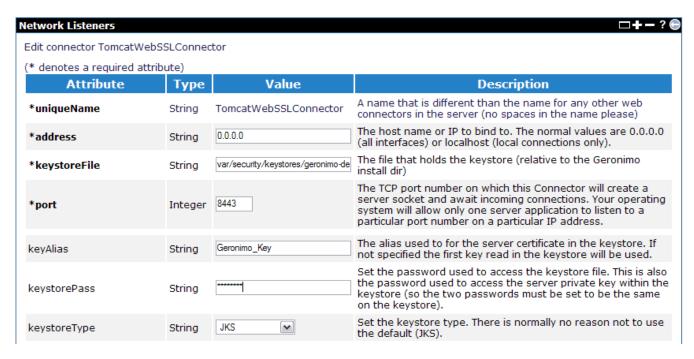


Click Review Key Data and on the next page click Generate Key. You should now see the key you just generated listed in the Keystore.



Now you can use this key by configuring an HTTPS connector as described in https://cwiki.apache.org/confluence/display/GMOxDOC30/Add+new+HTTPS+listener. Remember to make the certificate and keystore available by clicking the "lock" icon. For this example, you can modified the existing TomcatWebSSLConnector, specified the new keystore and saved the configuration.

For this configuration to take effect, you need to restart the connector. Click the **stop** link corresponding to the network listener you just updated, in this case TomcatWebSSLConnector, and then click **start**. Now this connector is using the new keystore and certificate.



If you now point your browser to that particular port, you should see the server is using the certificate you created. For this example, because you are using the existing SSL connector, point your browser to:

https://localhost:8443/console

