

Administering certificates



This section is about how to administer certificates from console.

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

Keystore Configuration

This tool walks you through the process of configuring keystores to use with SSL connectors (for the web container, etc.).

Keystores start out as locked against editing and also not available for usage by other components in the server. The **Editable** flag indicates whether the keystore has been unlocked for editing (by entering the keystore password), which lasts for the current login session. The **Available** flag indicates whether that password has been saved in order to make the keystore available to other components in the server.

Keystore File	Type	Contents	Editable	Available
geronimo-default	JKS	Keystore locked		 1 key ready

[New Keystore](#)

The certificates in Geronimo are stored in a keystore located in `<geronimo_home>\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 on **New Keystore**. You will be prompted with a keystore name and a password, enter those values and click **Create Keystore**, for this example we entered `sample_keystore` and password respectively.

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

Keystore Configuration

This tool walks you through the process of configuring keystores to use with SSL connectors (for the web container, etc.).

Keystores start out as locked against editing and also not available for usage by other components in the server. The **Editable** flag indicates whether the keystore has been unlocked for editing (by entering the keystore password), which lasts for the current login session. The **Available** flag indicates whether that password has been saved in order to make the keystore available to other components in the server.

Keystore File	Type	Contents	Editable	Available
geronimo-default	JKS	Keystore locked		 1 key ready
sample_keystore	JKS	0 Keys and 0 Certs		

[New Keystore](#)

To create a private key click on the keys on the keystore you just created and then click on **Create Private Key**. Enter valid data in the appropriate field data.

Keystore Configuration

On this screen you can configure the settings to generate a new private key. The next screen will let you review this information before generating the private key and accompanying certificate.

Alias for new key: Geronimo_Key

Password for new key:

Confirm Password:

Key Size: 2048

Algorithm: MD5withRSA

Valid for (# of days) : 120

Certificate Identity

Server Hostname (CN): server_name

Company/Organization (O): Apache

Division/Business Unit (OU): Geronimo

City/Locality (L): LL

State/Province (ST): ST

Country Code (2 char) (C): CC

Review Key Data

Cancel

Click on **Review Key Data** and then on **Generate Key**. You should now see the key you just generated listed in the Keystore Configuration portlet.

Keystore Configuration

This screen lists the contents of a keystore.

	Alias	Type	Certificate Fingerprint
View	Geronimo_Key	Private Key	04:08:62:C0:51:B7:0B:21:91:0C:BC:F6:0E:E9:AF:1C

[Add Trust Certificate](#)
[Create Private Key](#)
[Change keystore password](#)
[Return to keystore list](#)

You now can use that certificate by configuring an HTTPS connector as described in <http://cwiki.apache.org/GMOxDOC22/adding-new-listeners-for-the-web-containers.html>. Remember to make the certificate and keystore available by clicking on the "lock". For this example we have modified the existing TomcatWebSSLConnector, we specified the new keystore and saved the configuration.

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

Network Listeners

Edit connector TomcatWebSSLConnector

(* denotes a required attribute)

Attribute	Type	Value	Description
*uniqueName	String	TomcatWebSSLConnector	A name that is different than the name for any other web connectors in the server (no spaces in the name please)
*address	String	0.0.0.0	The host name or IP to bind to. The normal values are 0.0.0.0 (all interfaces) or localhost (local connections only).
*keystoreFile	String	var/security/kestores/geronimo-de	The file that holds the keystore (relative to the Geronimo install dir)
*port	Integer	8443	The TCP port number on which this Connector will create a server socket and await incoming connections. Your operating system will allow only one server application to listen to a particular port number on a particular IP address.
keyAlias	String	Geronimo_Key	The alias used to for the server certificate in the keystore. If not specified the first key read in the keystore will be used.
keystorePass	String	*****	Set the password used to access the keystore file. This is also the password used to access the server private key within the keystore (so the two passwords must be set to be the same on the keystore).
keystoreType	String	JKS	Set the keystore type. There is normally no reason not to use the default (JKS).

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

<https://localhost:8443/console>

Certificate Viewer: "Apache Geronimo"

General

Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)

Apache Geronimo

Organization (O)

Apache Foundation

Organizational Unit (OU)

Unknown

Serial Number

43:0C:E1:CC

Issued By

Common Name (CN)

Apache Geronimo

Organization (O)

Apache Foundation

Organizational Unit (OU)

Unknown

Validity

Issued On

25/08/05

Expires On

23/08/15

Fingerprints

SHA1 Fingerprint

C1:36:4C:57:6B:D5:3F:FC:98:C5:EE:9E:80:D5:02:00:E3:38:55:7B

MD5 Fingerprint

A6:77:EB:E0:92:3F:33:40:82:96:00:88:CF:71:D6:63

Close