1.1.3.3.1.

WebGeronimoSSLSSL

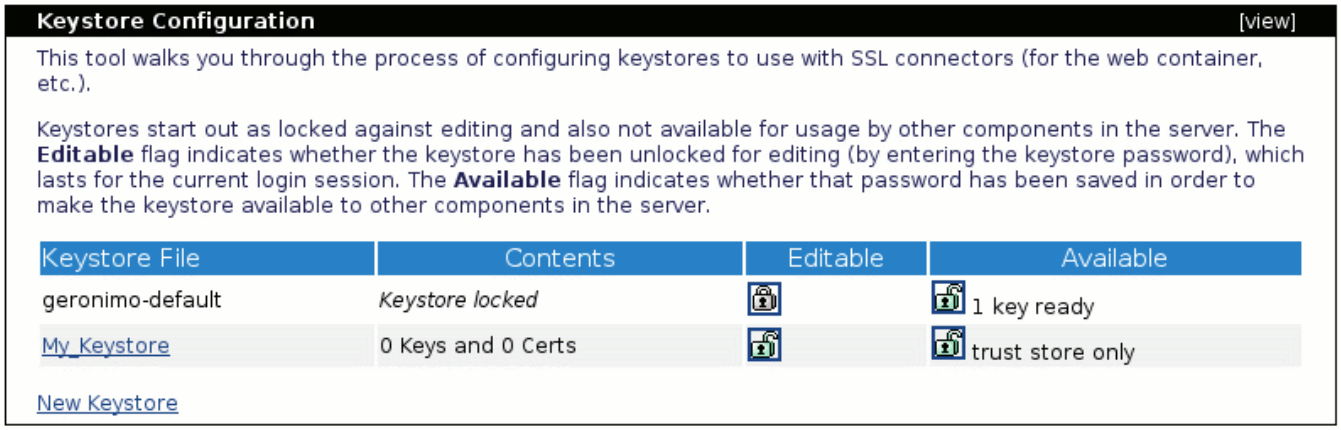
(CSR)CA

1.1.3.1. CSRCA

Geronimo **<geronimo_home>\var\security\keystores geronimo-default**

Geronimo **Keystores Keystore Configuration**

New Keystore Create Keystore My_Keystorepassword



Review Key Data

Keystore Configuration [view]

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: My_Private_Key
Password for new key: *******
Confirm password: *******
Key Size: 1024
Algorithm: MD5withRSA
Valid for (# of days): 999

Certificate Identity

Server Hostname (CN): localhost
Company/Organization (O): Apache
Division/Business Unit (OU): Geronimo
City/Locality (L): My_City
State/Province (ST): My_State
Country Code (2 char) (C): CC

Review Key Data

Cancel

Generate Key

Keystore Configuration [view]

This screen lists the contents of a keystore.

	Alias	Type	Certificate Fingerprint
view	My_Private_Key	Private Key	D1:EC:8F:36:42:E1:8D:77:AF:16:F0:10:54:DD:91:4C

Add Trust Certificate Create Private Key Return to keystore list

Certificate Signing Request (CSR)**Return to keystore list**

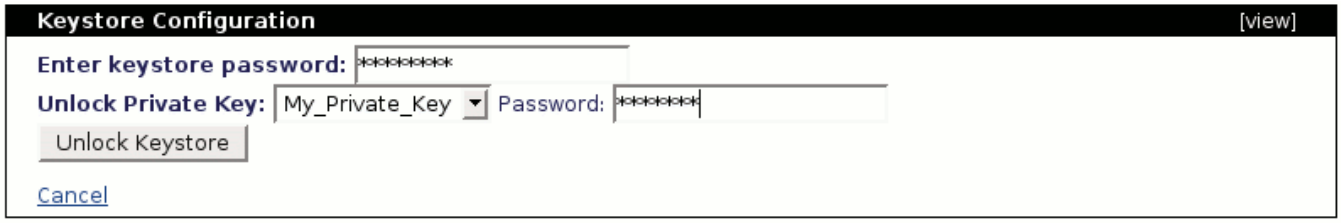
Keystore Configuration [view]

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	Contents	Editable	Available
geronimo-default	*Keystore locked*		1 key ready
My_Keystore	1 Key and 0 Certs		

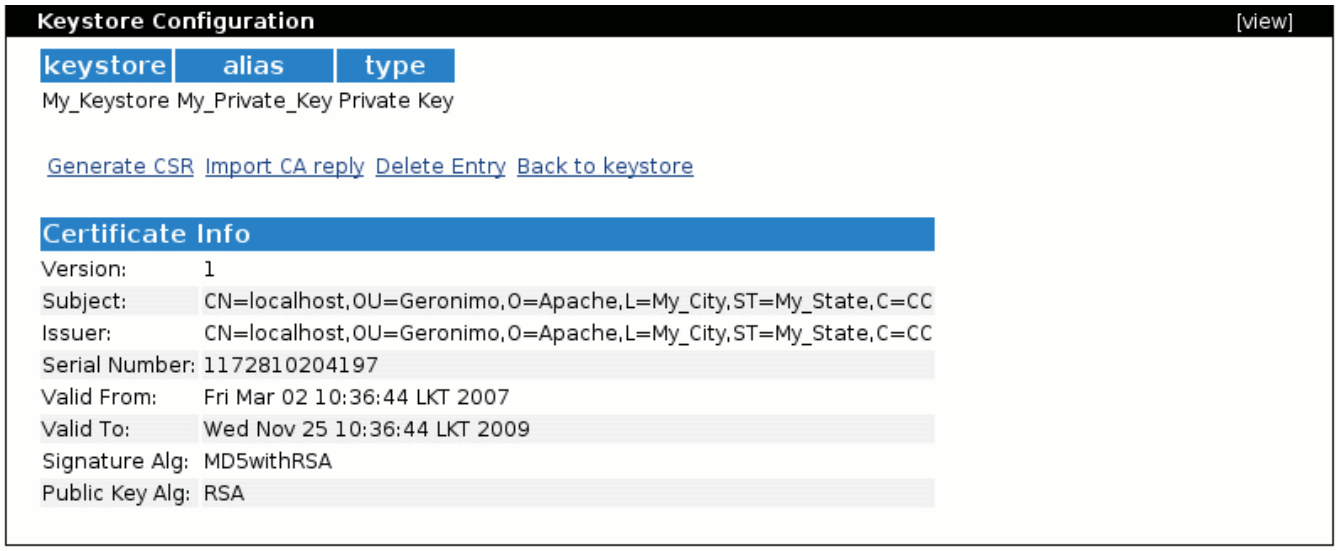
New Keystore



Unlock Keystore

(CSR)CA

CSR**Keystore Configuration view**



Generate CSR

PKCS10 CA

csr.txt


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqDCCARECAQAwajESMBAGA1UEAxMJbG9jYWxob3N0MREwDwYDVQQLEwhHZXJvbmltbz
EPMA0GA1UEChMGQXBhY2hlMRAwDgYDVQQHDAdNeV9DaXR5MREwDwYDVQQIDAhNeV9TdGF0
ZTELMAkGA1UEBhMCQ0MwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANTOM2j05ACU4N
49B4l51oxFSQX1SaX2+MBCWEpMILWriYxpBYRukMjyOOLBqreyUj6nv64j0qm1HgnOeYER
2fRtk6ERBGGRG//HprVBZzXFV5T/kwB4Ocg8NKQFWibLtT9MSjQyYBy0NGRgGL8krn+LDL
/YucueG+NbPfDzKD4xAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAp0g6oJ2WLllBmXpCnbcd
iyHtWAtFCODRKJaTzC09N+/0s+BugiGOxTGLB65C0xbIeumSog8Yxy26LFTtcvIP1lC7wg
V1e1KaJBTuuop7jOYFo4Tpx3oCL7ZJ6BtHrx0vSNlOdnkY6y+ZUPmQcWJq6lLP85NWu9N5
B94KI7U/QpM=
-----END CERTIFICATE REQUEST-----
```

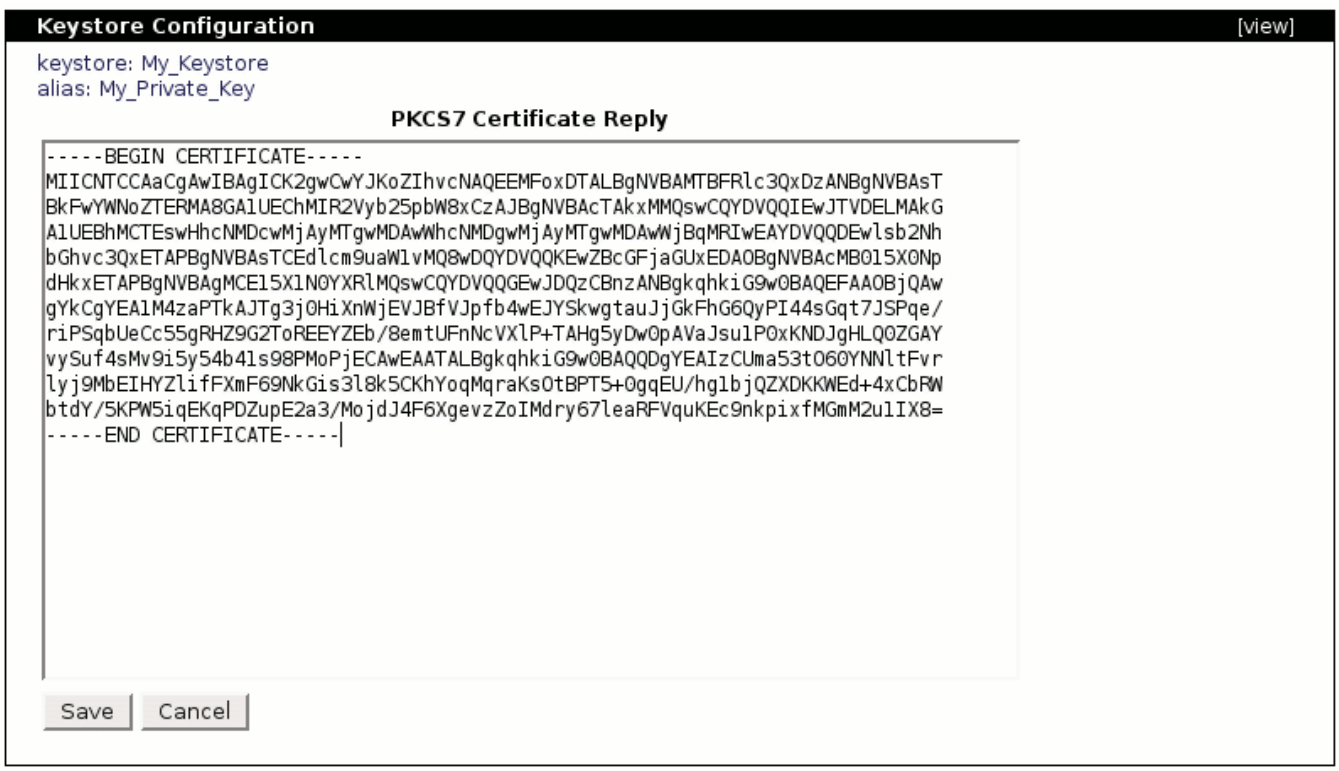

Back private key details

CACSRCACACA

csr_ca_reply.txt


```
-----BEGIN CERTIFICATE-----
MIICNTCCAaCgAwIBAgICK2gwCwYJKoZIhvcNAQEEMFoxDTALBgNVBAMTBFRlc3QxDzANBgNVBAsT
BkFwYWNoZTERMA8GA1UEChMIR2Vyb25pbW8xCzAJBgNVBAcTAkxMMQswCQYDVQQIEwJTVDELMAkG
A1UEBhMCTEswHhcNMDcwMjAyMTgwMDAwWhcNMDgwMjAyMTgwMDAwWjBqMRIwEAYDVQQDEwlsb2Nh
bGhvc3QxETAPBgNVBAsTCEdlcm9uaW1vMQ8wDQYDVQQKEwZBcGFjaGUxEDAOBgNVBAcMB015X0Np
dHkxETAPBgNVBAgMCE15X1N0YXRlMQswCQYDVQQGEwJDQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEA1M4zaPTkAJTg3j0HiXnWjEVJBfVJpfb4wEJYSkwgtauJjGkFhG6QyPI44sGqt7JSPqe/
riPSqbUeCc55gRHZ9G2ToREEYZEb/8emtUFnNcVXlP+TAHg5yDw0pAVaJsu1P0xKNDJgHLQ0ZGAY
vySuf4sMv9i5y54b41s98PMoPjECAwEAATALBgkqhkiG9w0BAQQDgYEAIzCUma53tO60YNNltFvr
lyj9MbEIHYZlifFXmF69NkGis3l8k5CKhYoqMqraKsOtBPT5+0gqEU/hg1bjQZXDKKWEd+4xCbRW
btdY/5KPW5iqEKqPDZupE2a3/MojdJ4F6XgevzZoIMdry67leaRFVquKEc9nkpixfMGmM2u1IX8=
-----END CERTIFICATE-----
```


private key details **Import CA reply** CA **Save**



CA **Issuer Back to keystore Return to keystore list**

Keystore Configuration [view]

keystore	alias	type
My_Keystore	My_Private_Key	Private Key

Generate CSR Import CA reply Delete Entry Back to keystore

Certificate Info

Version:	3
Subject:	C=CC, ST=My_State, L=My_City, O=Apache, OU=Geronimo, CN=localhost
Issuer:	C=LK, ST=ST, L=LL, O=Geronimo, OU=Apache, CN=Test
Serial Number:	11112
Valid From:	Sat Feb 03 00:00:00 LKT 2007
Valid To:	Sun Feb 03 00:00:00 LKT 2008
Signature Alg:	MD5withRSA
Public Key Alg:	RSA

CSRCACACSRCACA

My_Own_CA_Certificate.txt


```
-----BEGIN CERTIFICATE-----
MIICJTCCAZCgAwIBAgICK2cwCwYJKoZIhvcNAQEEMFoxDTALBgNVBAMTBFRlc3QxDzANBgNVBAsT
BkFwYWNoZTERMA8GA1UEChMIR2Vyb25pbW8xCzAJBgNVBAcTAkxMMQswCQYDVQQIEwJTVDELMAkG
A1UEBhMCTEswHhcNMDcwMjAyMTgwMDAwWhcNMDgwMjAyMTgwMDAwWjBaMQ0wCwYDVQQDEwRUZXN0
MQ8wDQYDVQQLEwZBcGFjaGUxETAPBgNVBAoTCEdlcm9uaW1vMQswCQYDVQQHEwJMTDELMAkGA1UE
CBMCU1QxCzAJBgNVBAYTAkxLMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCUZl1e1eTKLoh0
15vfYqqvhk6Iviva7BWQxZ6mOV9Ye2mii37Btmxajnngz0jKfiwHKqWRQBp6CUzbd9gfZrz2go9g
TwsUBWQwSf6iVypKX1q0Y4WhtTwLcEx78Lx5XN1YCqk34pn4by26SJiHdugs7/ClOiIlcpCt9QVa
Q9BH7wIDAQABMAsGCSqGSIb3DQEBBAOBgQAnmoT/dLvJa7jGstvZJLrsWtMwWQNVJ1ZQmbrDGq9u
oFnkAH1mGHIDbaz2avy/wotHJUIysGBlDP0btk5GVskl45EG/feWHLgCVmqwf3NkdRdLl+CznBBJ
KCC5tINbcI6GqXsbO8hhjIrOGweNyV1653WEvZiQVuMYaHTnGNx+RA==
-----END CERTIFICATE-----
```


Keystore Configuration **Add Trust Certificate** **Trusted Certificate** CA

Keystore Configuration [view]

This screen lets you input a certificate to import into the keystore. Paste the content of the certificate file in the text area and specify an alias to store it under in the keystore. The next step will let you review the certificate before committing it to the keystore.

Trusted Certificate


```
-----BEGIN CERTIFICATE-----
MIICJTCCAZCgAwIBAgICK2cwCwYJKoZIhvcNAQEEMFoxDTALBgNVBAMTBFRlc3QxDzANBgNVBAsT
BkFwYWNoZTERMA8GA1UEChMIR2Vyb25pbW8xCzAJBgNVBAcTAkxMMQswCQYDVQQIEwJTVDELMAkG
A1UEBhMCTEswHhcNMDcwMjAyMTgwMDAwWhcNMDgwMjAyMTgwMDAwWjBaMQ0wCwYDVQQDEwRUZXN0
MQ8wDQYDVQQLEwZBcGFjaGUxETAPBgNVBAoTCEdlcm9uaW1vMQswCQYDVQQHEwJMTDELMAkGA1UE
CBMCU1QxCzAJBgNVBAYTAkxLMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCUZlleleTKLoh0
l5vfYqqvhk6Iviva7BWQxZ6mOV9Ye2mii37Btmxajnngz0jKfiwHKqWRQBp6CUzbd9gfZrz2go9g
TwsUBWQwSf6iVypKX1q0Y4WhtTwLcEx78Lx5XN1YCqk34pn4by26SJiHdugs7/Cl0iIlcpCt9QVa
Q9BH7wIDAQABMAsGCSqGSIb3DQEBBAOBgQAnmoT/dLvJa7jGstvZJLrsWtMwWQNVJ1ZQmbrDGq9u
oFnkAH1mGHIDbaz2avy/wotHJUIysGBlDP0btk5GVskl45EG/feWHLgCVmqwf3NkdRdLl+CznBBJ
KCC5tINbcI6GqXsbO8hhjIrOGweNyV1653WEvZiQVuMYaHTnGNx+RA==
-----END CERTIFICATE-----
```


Alias for certificate: My_Own_CA_Certificate

Review Certificate

Cancel

Review Certificate **Import Certificate**

Keystore Configuration [view]

This screen lists the contents of a keystore.

	Alias	Type	Certificate Fingerprint
view	My_Trust_CA	Trusted Certificate	E7:04:A8:42:24:58:7C:E5:CC:FD:71:0C:44:A6:01:00
view	My_Private_Key	Private Key	45:2C:C9:23:2A:07:83:23:45:68:08:7D:53:C2:B8:C2

Add Trust Certificate Create Private Key Return to keystore list

HTTP

Apache Geronimo8443HTTPSHTTPS

GeronimoTomcatJetty

Geronimo **Web Server** Network Listener

Network Listeners help [view]

Name	Protocol	Port	State	Actions	Type
TomcatWebSSLConnector	HTTPS	8443	running	stop edit delete	Tomcat Connector
TomcatWebConnector	HTTP	8080	running	stop edit delete	Tomcat Connector
TomcatAJPConnector	AJP	8009	running	stop edit delete	Tomcat Connector

Add new HTTP listener for Tomcat
Add new HTTPS listener for Tomcat
Add new AJP listener for Tomcat

Network Listener **Add new HTTPS listener for Tomcat**

Network Listeners help [view]

Add new HTTPS listener for Tomcat

Unique Name: SSL_Client_Authentication

A name that is different than the name for any other web connectors in the server (no spaces in the name please)

Host: 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)

Port: 443

The network port to bind to.

Max Threads: 50

The maximum number of threads this connector should use to handle incoming requests

SSL Settings

Keystore File: /var/security/keystores/My_Keystore

The file that holds the keystore (relative to the Geronimo install dir)

Keystore Password: ********

Confirm Password: ********

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).

Keystore Type: JKS

Set the keystore type. There is normally no reason not to use the default (JKS).

Truststore File:

The file that holds the truststore (relative to the Geronimo install dir)

Truststore Password:

Confirm Password:

Set the password used to verify the truststore file.

Truststore Type: JKS

Set the truststore type. There is normally no reason not to use the default (JKS).

HTTPS Algorithm: Sun

Set the HTTPS algorithm. This should normally be set to match the JVM vendor.

HTTPS Protocol: TLS

Set the HTTPS protocol. This should normally be set to TLS, though some (IBM) JVMs don't work properly with popular browsers unless it is changed to SSL.

Client Auth Required: ☑

If set, then clients connecting through this connector must supply a valid client certificate. The validity is checked using the CA certificates stored in the first of these to be found:

1. The trust store configured above
2. A keystore file specified by the `javax.net.ssl.trustStore` system property
3. *java-home*`/lib/security/jssecacerts`
4. *java-home*`/lib/security/cacerts`

Save Reset Cancel

List connectors

Save truststore(trustoretruststore) **var/security/keystores/<your_keystore>** Geronimo

Client Auth Required HTTPSCA

1.
2. javax.net.ssl.trustStore system property
3. java-home/lib/security/jssecacerts
4. java-home/lib/security/cacerts

HTTPS