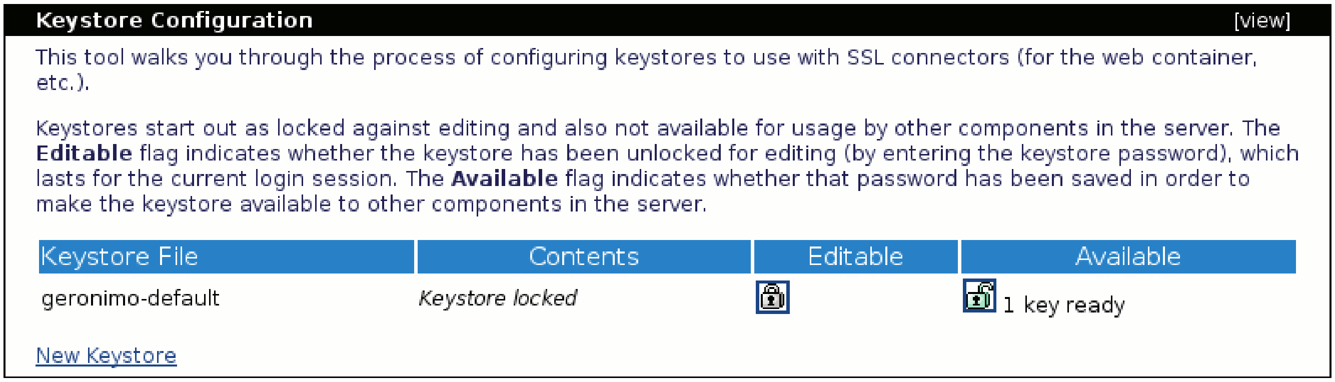
1.1.3.1.

1.1.3.
1.1.3.2.

Console Navigation **Keystore** **Keystore Configuration** SSL



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.

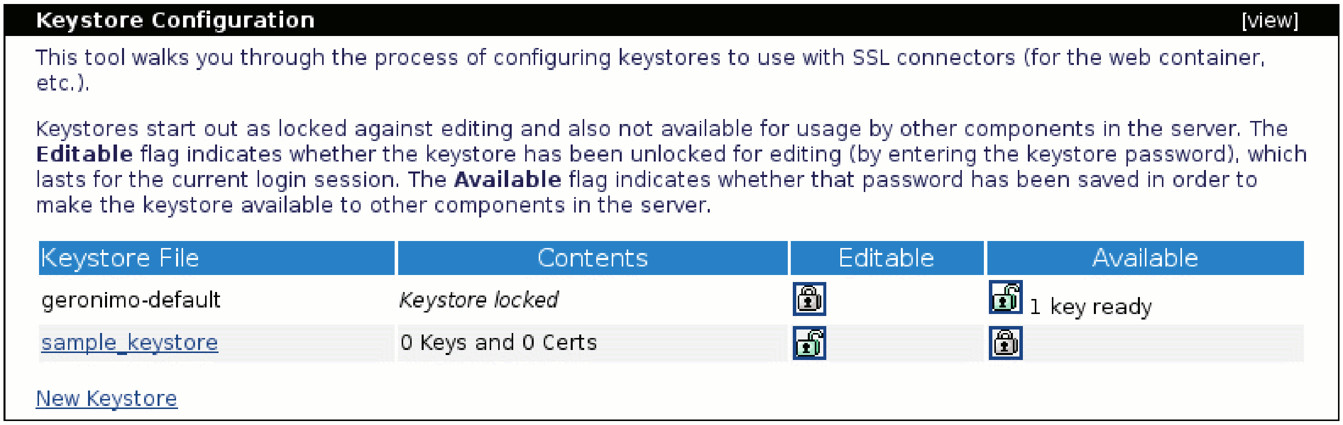
Keystore File	Contents	Editable	Available
geronimo-default	*Keystore locked*	🔒	🔓 1 key ready

New Keystore

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

New Keystore **Create Keystore** sample_keystorepassword

Available



Keystore Configuration [view]

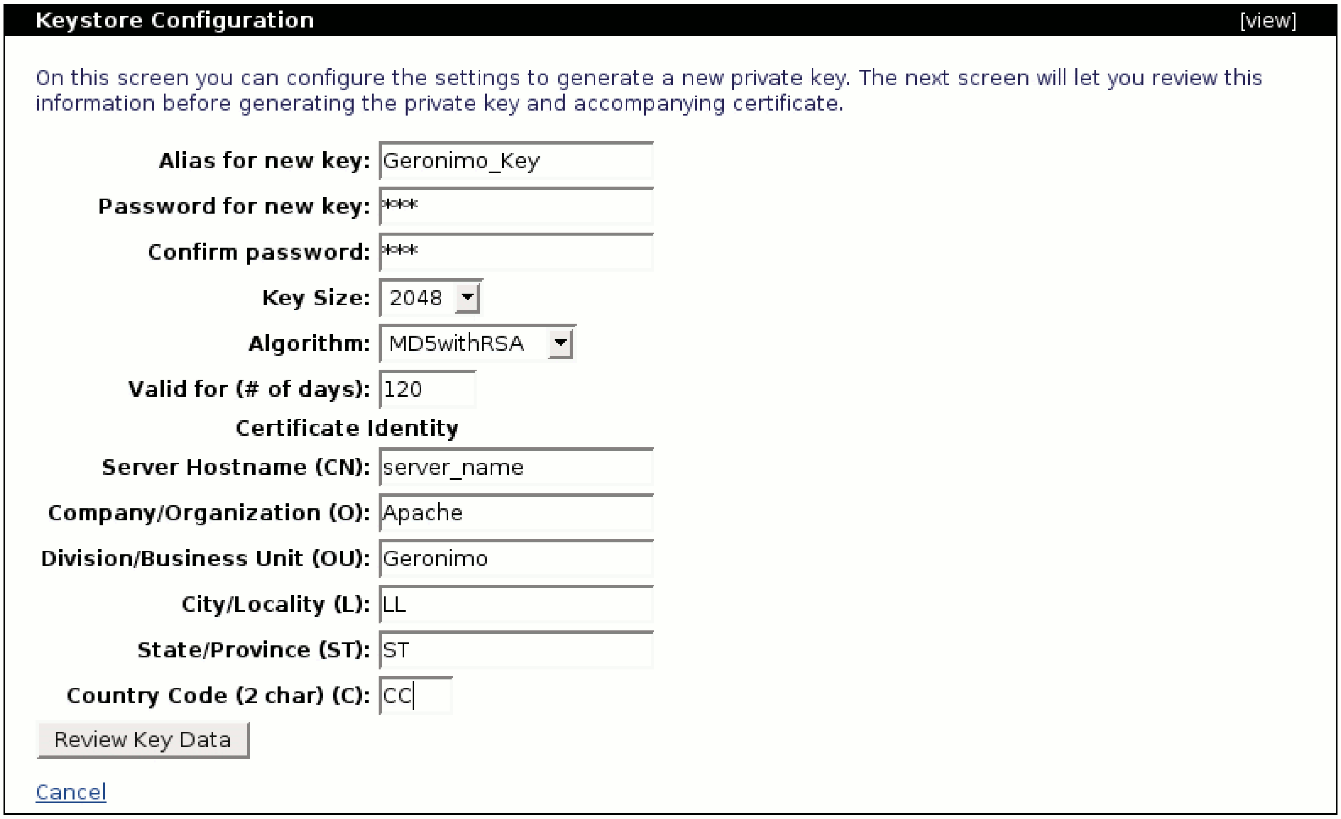
This tool walks you through the process of configuring keystores to use with SSL connectors (for the web container, etc.).

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
sample_keystore	0 Keys and 0 Certs	🔓	🔒

New Keystore

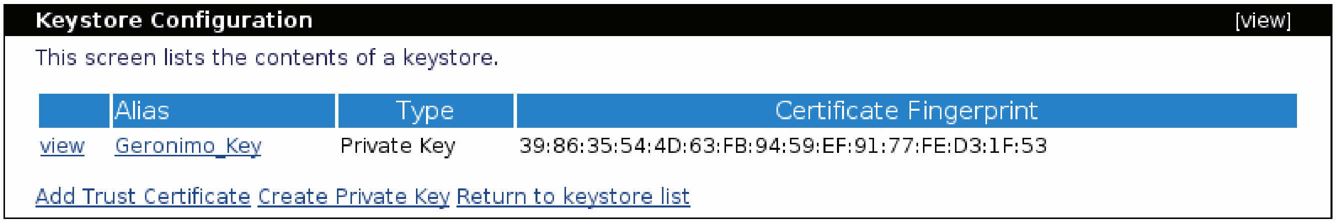
Create Private Key



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 **Generate Key** Keystore Configuration



Keystore Configuration
[view]

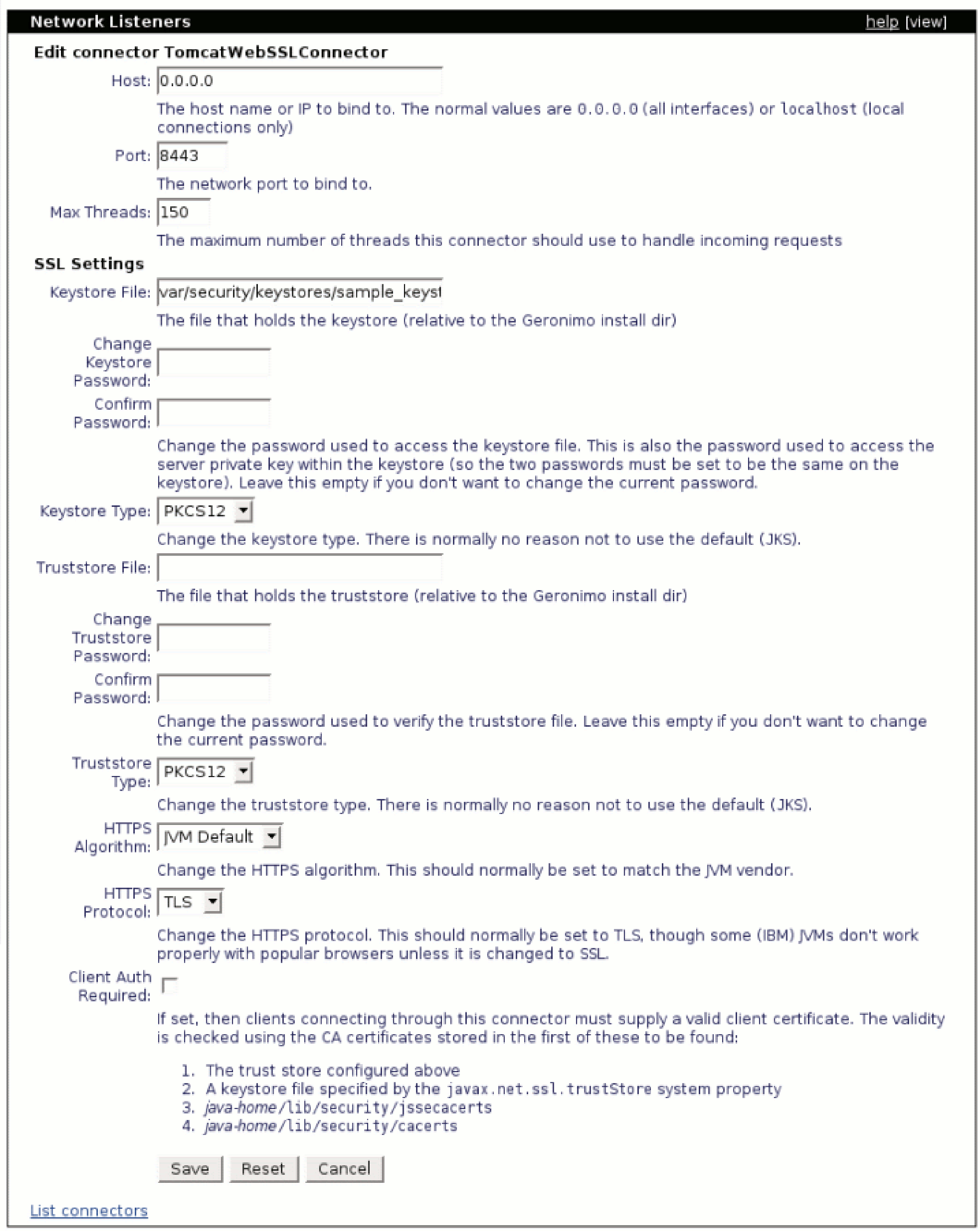
This screen lists the contents of a keystore.

	Alias	Type	Certificate Fingerprint
view	Geronimo_Key	Private Key	39:86:35:54:4D:63:FB:94:59:EF:91:77:FE:D3:1F:53

Add Trust Certificate Create Private Key Return to keystore list

HTTPSHTTPSTomcatWebSSLConnector

TomcatWebSSLConnector **stop** **start**



Edit connector TomcatWebSSLConnector

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: 8443

The network port to bind to.

Max Threads: 150

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

SSL Settings

Keystore File: var/security/keystores/sample_keyst

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

Change Keystore Password:

Confirm Password:

Change 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). Leave this empty if you don't want to change the current password.

Keystore Type: PKCS12

Change 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)

Change Truststore Password:

Confirm Password:

Change the password used to verify the truststore file. Leave this empty if you don't want to change the current password.

Truststore Type: PKCS12

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

HTTPS Algorithm: JVM Default

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

HTTPS Protocol: TLS

Change 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.

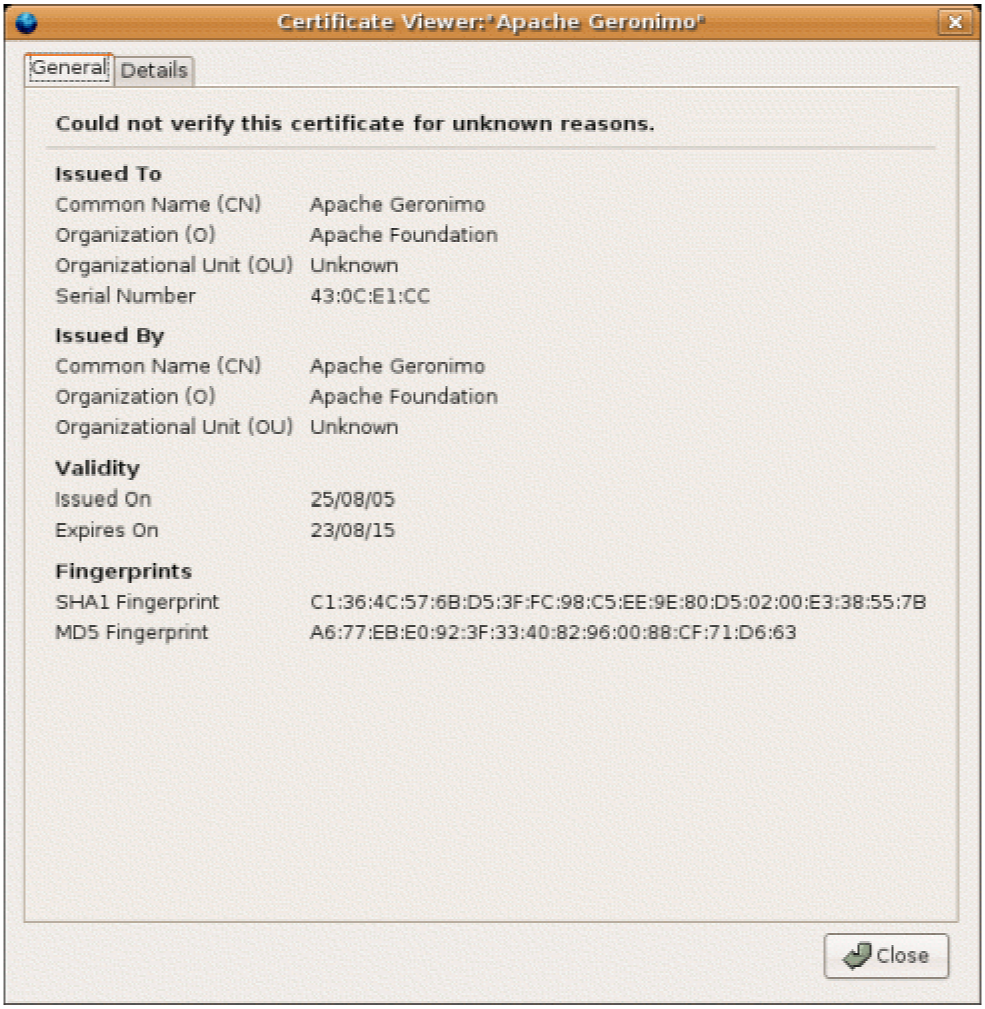
Client Auth Required: ☐

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`

SSL

https://localhost:8443/console



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