



Inicio

Quiénes Somos

Formación

Publicaciones

Buscar...

Tutoriales.

Adictos al Trabajo / Tutoriales / SSL en Tomcat



Jose Carlos López

Ingeniero en Informática



Las mejores ofertas

1,21 €

EPSON LQ590 CINTA

## SSL en Tomcat

febrero 21, 2007

Jose Carlos López

1 Comentario

Tutoriales

39667 visitas



## SSL en Tomcat

### 1. Introducción

En este tutorial se describe cómo configurar Tomcat para acceder a las aplicaciones web empleando HTTP sobre SSL. Vamos a utilizar la técnica sencilla,

que es la que se describe en <http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>. Consiste en utilizar la herramienta keytool, distribuida con el kit de desarrollo de Java,

para generar un certificado autofirmado del servidor. También será necesario cambiar la configuración del fichero server.xml para activar un conector que permitirá

acceder a Tomcat a través de https.

### 2. Software necesario

La herramienta keytool se encuentra en el directorio bin de la instalación j2sdk. Si estamos usando una versión anterior a la 1.4, debemos descargar

la extensión de <http://java.sun.com/products/jsse/> e incluir los jars en el directorio \$JAVA\_HOME/jre/lib/ext.

Para los usuarios de una versión igual o superior a la 1.4, no es necesario descargar nada porque esta utilidad ya viene incluida.

### 3. Configurando el server.xml

Lo único que tenemos que hacer es descomentar la parte del siguiente elemento Connector:

#### Los más visitados de la semana

Web Service Security

VirtualBox. Configuración de la conexión de red.

El cálculo de la liquidación por despido: el finiquito.

SoapUI: jugando con web services

Configurando Notificaciones Push para desarrollos Android co...

#### Tags

Android, rest, SOLID, Tomcat, JSF, ESB, tutorial, Maven, Spring, Javascrpt, Test, Gradle, web, java, Sonar, HTML5, MAC, regular, phonegap, Autentia, iOS, J2SE, diseño, J2EE

#### Facebook



**AdictosAlTrabajo**

2 días hace

Hoy Juan Antonio Ortiz trae un nuevo tutorial. 'Configuración de #Nexus, #Sonar y #Jenkins tras un #Apache'

**AdictosAlTrabajo**



4 días hace

José Luis Rodríguez trae el primer tutorial de la semana: 'CDI: Conceptos avanzados'. Lectura de lunes obligada ;)

**AdictosAlTrabajo**

1 semana hace

Natalia Roales trae este tutorial técnico a nuestro portal. No te lo pierdas. 'El paralelismo en Java y framework Fork/Join'

**Adictos...**

445 Me gusta

Me gusta esta página

**Tweets**

Follow

**adictosaltrabajo**  
@adictosaltrabaj

26 Aug

Hoy @BastDagnal trae un nuevo tutorial. 'Configuración de #Nexus, #Sonar y #Jenkins tras un #Apache' [adictosaltrabajo.com/tutoriales/con...](http://adictosaltrabajo.com/tutoriales/con...)

**adictosaltrabajo**  
@adictosaltrabaj

24 Aug

Nuevo tutorial de la mano de @Jlrv 'CDI: Conceptos avanzados' [adictosaltrabajo.com/tutoriales/cdi...](http://adictosaltrabajo.com/tutoriales/cdi...)

**adictosaltrabajo**  
@adictosaltrabaj

21 Aug

¡NUEVO TUTORIAL! El paralelismo en #Java y el framework #Fork/Join por @atuncontomate [adictosaltrabajo.com/tutoriales/el-...](http://adictosaltrabajo.com/tutoriales/el-...)

Tweet to @adictosaltrabaj

**Archivos**

Archivos

Elegir mes

```

1 <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
2
3 <!--
4
5 <Connector port="8443" maxHttpHeaderSize="8192"
6
7 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
8
9 enableLookups="false" disableUploadTimeout="true"
10
11 acceptCount="100" scheme="https" secure="true"
12
13 clientAuth="false" sslProtocol="TLS" />
14
15 -->

```

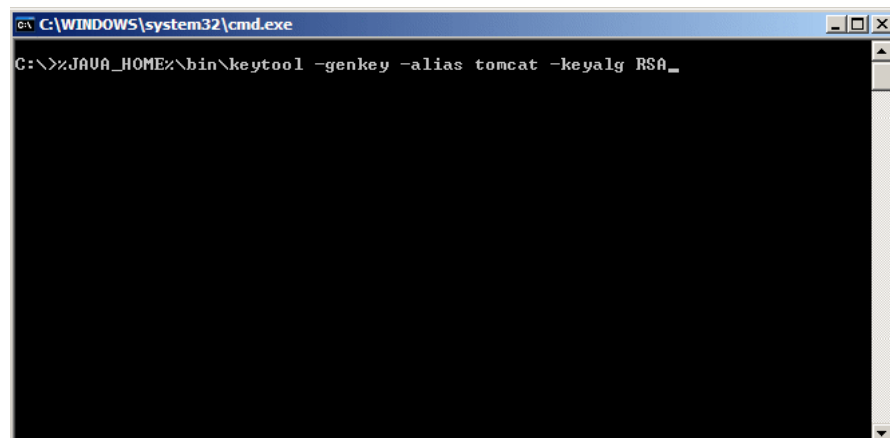
Con esto conseguimos activar el uso de SSL en el puerto 8443. No se solicita certificado al cliente durante el establecimiento de la conexión SSL (clientAuth = "false"),

por tanto, no es necesario cambiar nada en el navegador web que usemos, aunque si hay que crear el almacén de claves en el servidor.

#### 4. Creando el almacén de claves y un certificado autofirmado

Abrimos una consola y ejecutamos:

```
%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
```

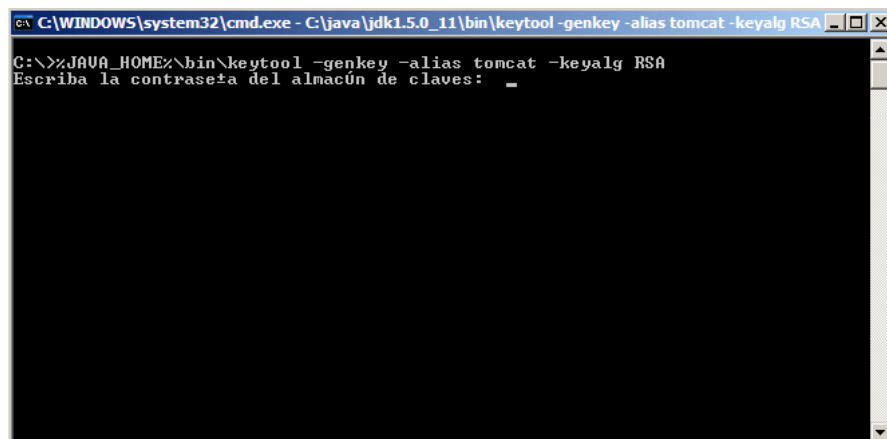


Nos pedirá una serie de datos para configurar el certificado. Lo primero que nos

pide es la contraseña para el almacén de claves:

La clave por defecto utilizada por Tomcat es "changeit" y es la que introduciremos. Si queremos usar cualquier otra clave, lo único que tenemos que hacer

es añadir al Connector el parámetro keystorePass especificando la clave a usar.



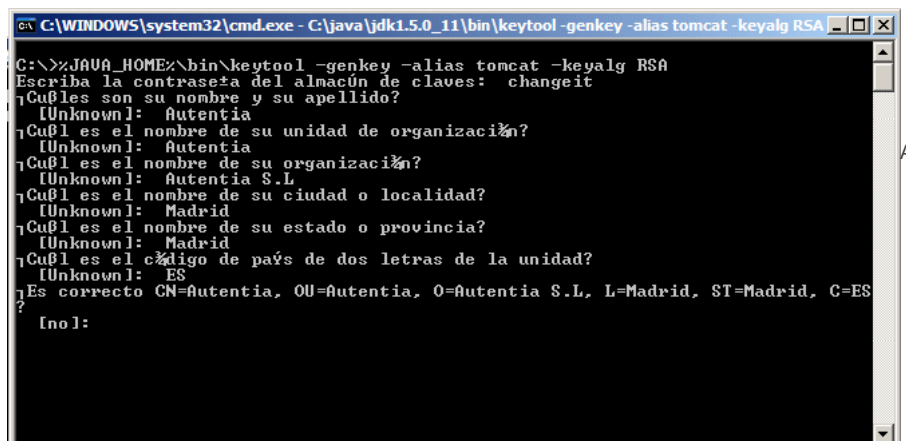
```
C:\WINDOWS\system32\cmd.exe - C:\java\jdk1.5.0_11\bin\keytool -genkey -alias tomcat -keyalg RSA
C:\>%JAVAHOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
Escriba la contraseña del almacén de claves: _
```

```
1 <Connector port="8443" maxHttpHeaderSize="8192"
2
3 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
4
5 enableLookups="false" disableUploadTimeout="true"
6
7 acceptCount="100" scheme="https" secure="true"
8
9 clientAuth="false" sslProtocol="TLS"
10
11 keystorePass="mi_clave"/>
```

keystorePass="mi\_clave"/>

A continuación nos pide nuestro nombre, el nombre de nuestra unidad de organización, el nombre de nuestra organización, la ciudad o localidad, el estado

o provincia, y el código del país. Nos pregunta si los datos introducidos son correctos e introducimos si.



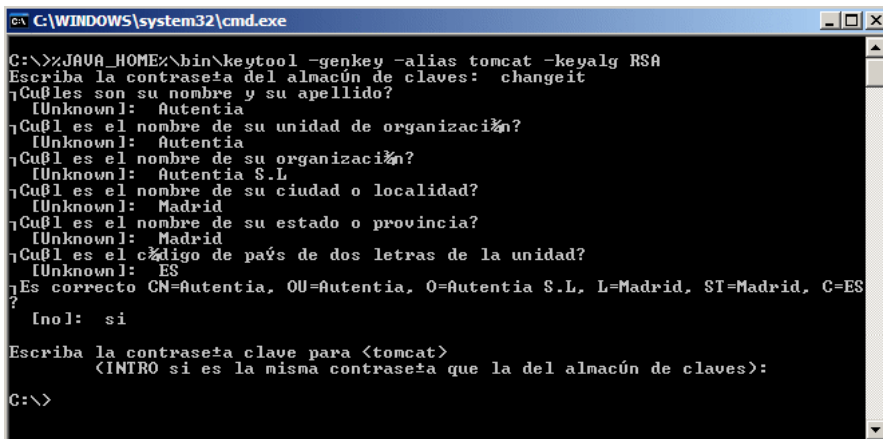
```
C:\WINDOWS\system32\cmd.exe - C:\java\jdk1.5.0_11\bin\keytool -genkey -alias tomcat -keyalg RSA
C:\>%JAVAHOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
Escriba la contraseña del almacén de claves: changeit
¿Cuáles son su nombre y su apellido?
[Unknown]: Autentia
¿Cuál es el nombre de su unidad de organización?
[Unknown]: Autentia
¿Cuál es el nombre de su organización?
[Unknown]: Autentia S.L
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: Madrid
¿Cuál es el nombre de su estado o provincia?
[Unknown]: Madrid
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: ES
¿Es correcto CN=Autentia, OU=Autentia, O=Autentia S.L, L=Madrid, ST=Madrid, C=ES
?
[no]:
```

continuación nos pide la contraseña clave para <tomcat>. Aunque nos permite introducir una distinta, **siempre** debemos poner la misma contraseña

aquí que la que tenemos en nuestro almacén de claves (Nos da la opción de pulsar INTRO para este efecto).

Nota: Esto se indica en la ayuda de Tomcat en <http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>. Tomcat lanzaría un java.io.IOException: Cannot recover key si no usaramos la misma clave

Y ya hemos terminado, el proceso nos ha creado un archivo .keystore en el home del usuario:

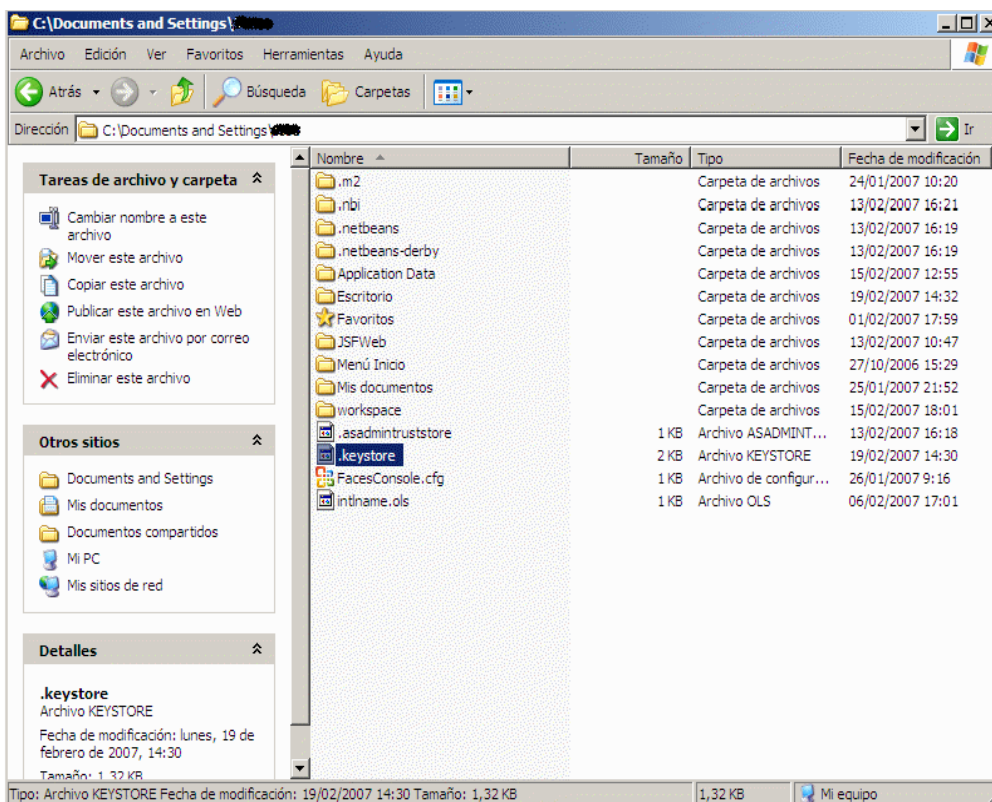


C:\Documents and Settings\user en sistemas Windows XP

C:\Winnt\Profiles\user en sistemas multi-usuario Windows NT

C:\Windows\Profiles\user en sistemas multi-usuario Windows 95/98

C:\Windows en sistemas de un sólo usuario Windows 95/98



Tomcat utiliza por defecto este .keystore para buscar los certificados (el que se encuentra en el directorio home del usuario). Si quisieramos utilizar un almacén situado

en otra ubicación, unicamente debemos añadir al Connector el parámetro keystoreFile especificando la ruta absoluta al fichero, o una ruta relativa resuelta a partir del

%CATALINA\_BASE%.

Suponiendo que mi fichero se encuentra en C:\keyStores\mykeystore:

```

1 <Connector port="8443" maxHttpHeaderSize="8192"
2
3 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
4
5 enableLookups="false" disableUploadTimeout="true"
6
7 acceptCount="100" scheme="https" secure="true"
  
```

```

8
9 clientAuth="false" sslProtocol="TLS"
10
11 keystoreFile="C:\keyStores\mykeystore"/>

```

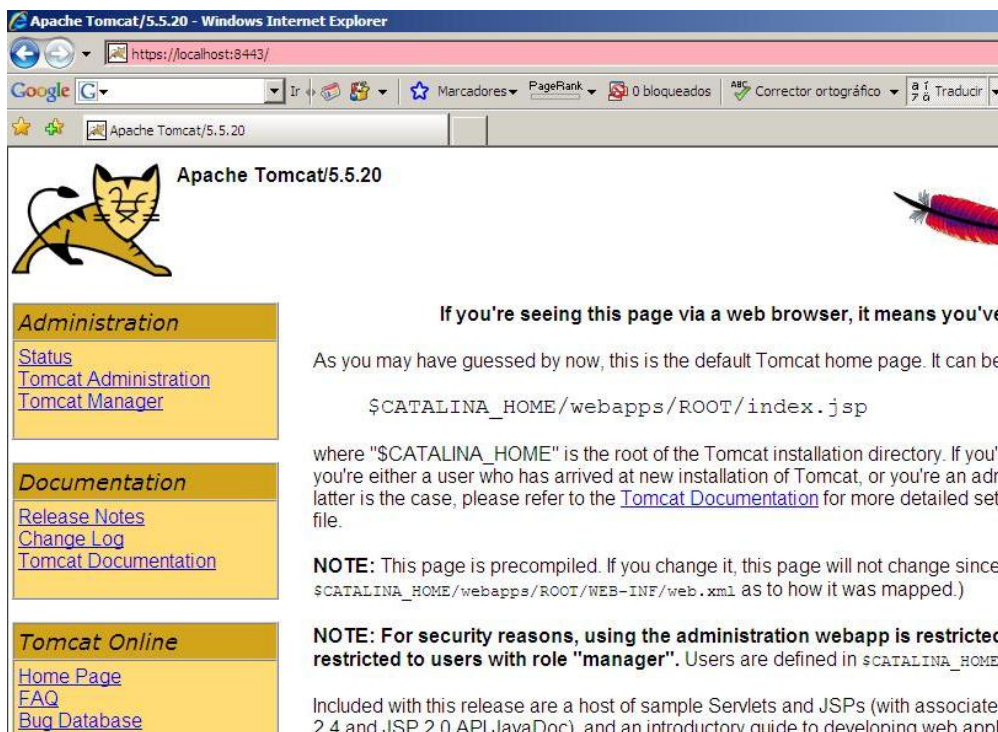
Suponiendo que mi %CATALINA\_BASE% apunta a C:\servidores\tomcat y mi fichero se encuentra en C:\servidores\tomcat\keystores\mykeystore

```

1 <Connector port="8443" maxHttpHeaderSize="8192"
2
3 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
4
5 enableLookups="false" disableUploadTimeout="true"
6
7 acceptCount="100" scheme="https" secure="true"
8
9 clientAuth="false" sslProtocol="TLS"
10
11 keystoreFile="keyStores\mykeystore"/>

```

Ahora, arrancamos tomcat y probamos en el navegador <https://localhost:8443> para ver si funciona:



Perfecto, ya tenemos habilitada la configuración SSL en nuestro tomcat.

## 5. Acerca del autor

José Carlos López Díaz. Ingeniero en Informática

[jclopez@autentia.com](mailto:jclopez@autentia.com)

---

Comparte este artículo!

---



Esta obra está licenciada bajo [licencia Creative Commons de Reconocimiento-No comercial-Sin obras derivadas 2.5](#)

### Respuesta (1)

**martha garcia**

octubre 31, 2014 at 2:38 am · Responder

El tutorial esta muy bien... de hecho todo perfecto solo quiero saber porque me sale un error en el certificado Direccion no coincidente. ¿Que hago????? o mas bien que hice mal? muchas gracias por su tiempo y ayuda

### Deja un comentario

---

#### Tags

Android angularjs Apache  
Autentia hadoop HTML5 iOS  
java Javascript JSF  
Maven phonegap rest SOA  
Sonar Spring Test Tomcat  
WebServices Zk

---

#### Lo último

Comunicación entre directivas en AngularJS  
Configuración de Nexus, Sonar y Jenkins tras un Apache  
CDI: Conceptos avanzados  
El paralelismo en Java y el framework Fork/Join  
Promesas en AngularJS

---

#### Datos de contacto

Edificio BestPoint Avd. de Castilla, 1, Planta 2, Oficina 21B (San Fernando de Henares)  
**Phone:** 916 75 33 06  
**E-Mail:** [info@adictosaltrabajo.com](mailto:info@adictosaltrabajo.com)  
**Web:** <http://www.autentia.com>

---

#### Powered by



Copyright 2003-2015 © All Rights Reserved | Texto legal y condiciones de  
uso