



WebSphere Application Server V6.1

证书安装使用指南



上海数字证书认证中心有限公司

2009/01/05



文档说明:

本文档是 BEA WebLogic Server9.2 证书安装使用指南，主要描述如何在 WebLogic 上产生密钥对，web 证书在线申请和如何将 web 证书安装到 WebLogic 服务器。

版本信息:

当前版本 3.0 技术支持中心

版权信息:

SHECA 是上海数字证书认证中心有限公司的注册商标和缩写。

UCA 是上海数字证书认证中心有限公司研究开发的通用证书系统的商标和缩写。

本文的版权属于上海数字证书认证中心有限公司，未经许可，任何个人和团体不得转载、粘贴或发布本文，也不得部分的转载、粘贴或发布本文，更不得更改本文的部分词汇进行转贴。

未经许可不得拷贝，影印。

Copyright @2008 上海数字证书认证中心有限公司

文档发行说明

当您阅读完本文档，您应该能解决如下问题：

- 1、WEB 服务器证书的请求文件 CSR 的产生；
- 2、WEB 服务器证书的在线申请；
- 3、WEB 服务器证书的安装；
- 4、WEB 服务器 SSL 安全配置；
- 5、WEB 服务器证书的导出（备份）和导入（恢复）；
- 6、SSL 双向认证的配置；
- 7、使您的系统信任 SHECA 根证书；

文档书写环境说明：

为了测试基于 WebSphere WEB 服务的 SSL 双向认证，本文档采用了最新的 WebSphere Application Server V6.1 WEB 服务。以下是本文档的具体试验环境：

WEB 服务器：Windows 2003 Enterprise Server English Edition + WebSphere Application Server V6.1

客户端：Windows XP Professional English Version + Service Pack 3

注：本文档并不包含 IBM http server 的服务器证书配置说明

安装环境：

Web 服务器，本文以 windows 操作系统为例。系统正确安装 JDK1.4 以上版本和 IBM WEBSphere Application server6.1 版本软件。

通过 KEYTOOL 工具为服务器申请证书：

本文采用标准的 Java keytool 方式，并基于标准的 Java keystore 方式为 WEB 服务器提供 Private key、Identity Cert 和 Trusted Cert 存储。

（注：本文档在命令行模式下执行的命令运行路径均需要定位于 **keytool.exe** 所在的路径，请遵照执行，以免差错）

1、产生密钥对：

在 windows 操作系统上打开“命令提示符”窗口，在命令行模式下运行以下命令以产生密钥既 jks 文件。

例：

```
.\keytool -genkey -keyalg rsa -keysize 1024 -alias test -keypass 123456  
-keystore testkeystore.jks -storepass 123456
```

此时系统会提示您输入你的信息，请确保以下内容和您提交到上海 CA 的内容一致，以保证服务器证书的签发。

Common Name（服务器域名或者 IP）

Organization name（组织名或公司名）

Organization unit name（组织单位名或部门名）

City or location name（城市或区域名）

State or province name（省份或者州名）

Country name（国家名的两位编码，中国为“CN”）

2、产生证书请求（CSR）：

再运行，例：

```
.\keytool -certreq -alias test -keystore testkeystore.jks -file server.csr  
-storepass 123456
```

产生证书请求文件“server.csr”；

3、申请服务器证书：

将“server.csr”文件提交 SHECA，CA 处理完毕申请，用户下载证书，证书可以使用 PEM 格式；

申请服务器证书：

第一步：登陆<http://www.sheca.com>，点击**证书申请** → [立即申请安全站点证书，请点击>>](#)；

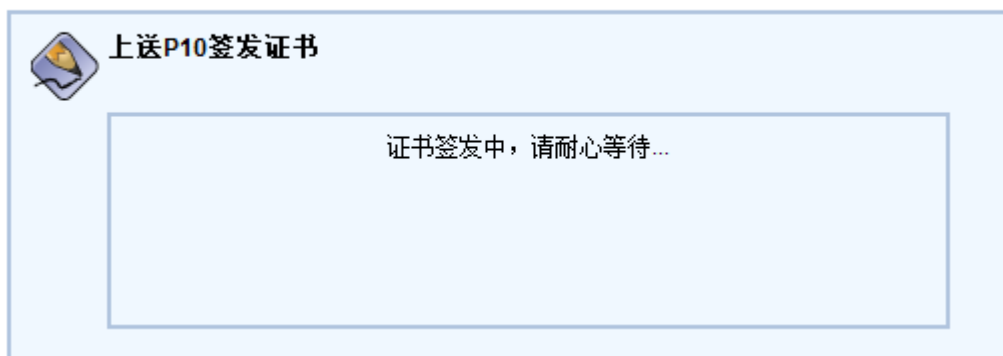
在方框里输入从 SHECA 证书受理点获取的密码信封序列号和信封密码

(注:由于申请的是 WEB 服务器证书,所以设定的私钥密码不起作用)

第二步：完成输入后，进入下一个页面,此时选择勾选“**高级选项**”，并选择“**用户自上送 P10 证书请求**”并在最底部的输入框内贴入证书请求中去除 BEGIN 以及 END 的部分内容，如下图所示

第三步：请耐心等待证书签发

上送P10签发证书

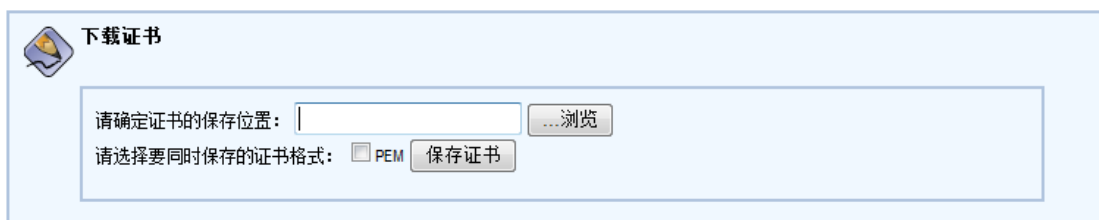


上送P10签发证书

证书签发中，请耐心等待...

第四步：请选择证书保存的路径，如需保存为 PEM 格式，则勾选“PEM”，并点击保存证书。

下载证书



下载证书

请确定证书的保存位置： ...浏览

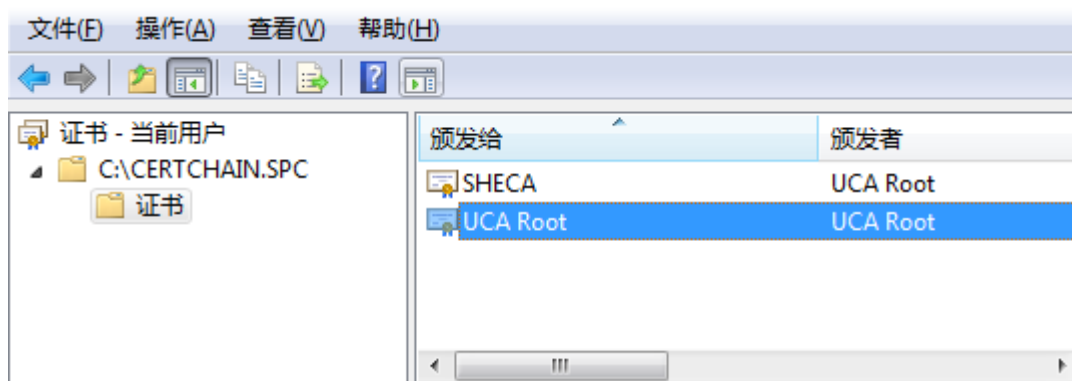
请选择要同时保存的证书格式： PEM 保存证书

第五步：申请完证书之后，将证书文件复制到 **keytool.exe** 工具以及 **testkeystore.jks** 文件所在的目录下。有必要说明的是，以上各种文件可以是 PEM 或 DER 格式。

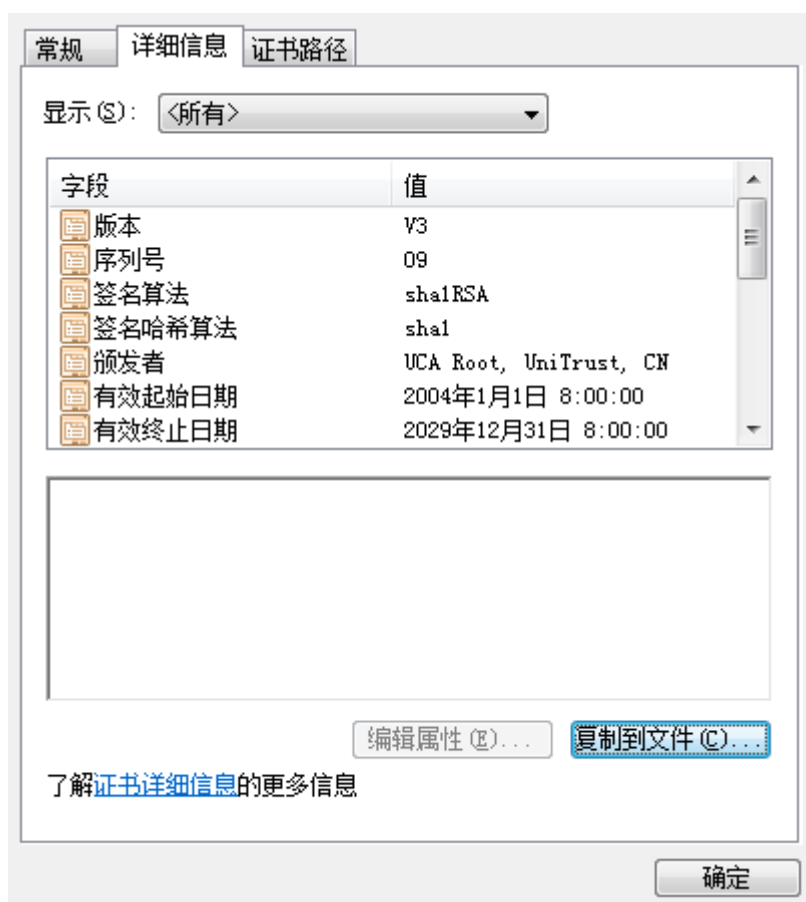
服务器证书导入：

1、导入根证书 UCA Root:

将 CertChain.SPC 文件打开，选中 UCA Root 这张证书右键选择“打开”



在详细信息的标签栏中选择“复制到文件”



将此证书保存为文件 root.cer，并放置于 keytool.exe 同一目录下，运行以下命令导入根证书：

```
.keytool -import -trustcacerts -alias root -file root.cer -storepass 123456  
-keystore testkeystore.jks
```

2、导入中级证书 SHECA

按照步骤一，同样的将 CertChain.SPC 文件当中的 SHECA 证书导出为 sheca.cer，并放置于 keytool.exe 目录下，运行以下命令以导入中级证书：

```
.keytool -import -trustcacerts -alias sheca -file sheca.cer -storepass 123456  
-keystore testkeystore.jks
```

3、导入服务器证书：

将得到的服务器证书 UserCert.der 放入 keytool.exe 所在的文件夹中,并继续在命令行模式中执行以下命令导入服务器证书到 testkeystore.jks 中.

```
.keytool -import -trustcacerts -alias test -keystore testkeystore.jks -file  
UserCert.der -storepass 123456
```

(注:此时会提示认证回复已安装在 keystore 中)

4、证书查看：

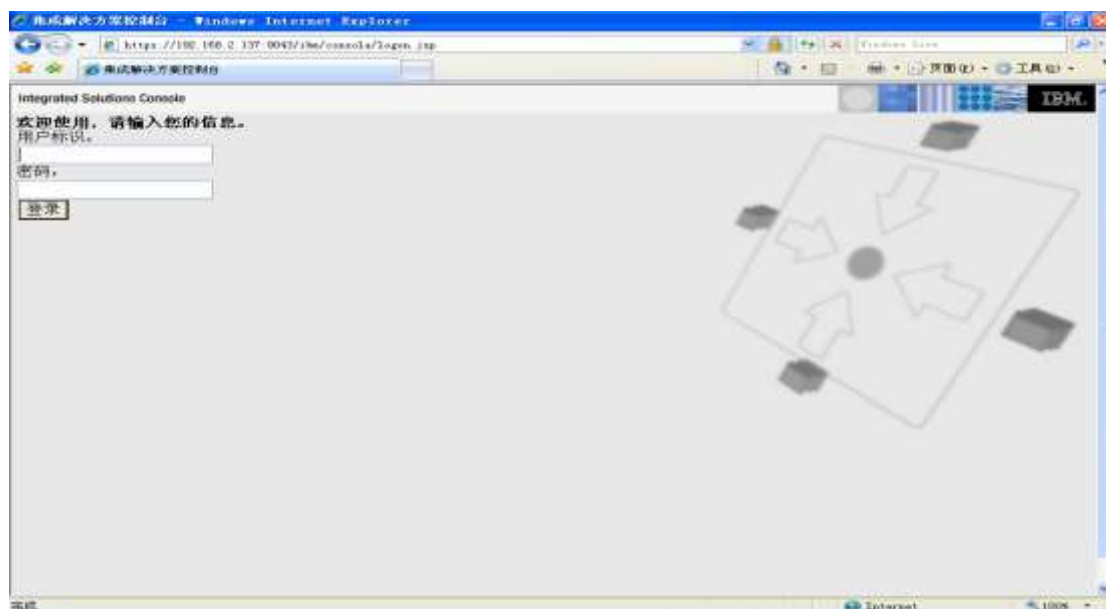
使用以下命令查看证书是否正确导入：

```
.keytool -list -v -keystore testkeystore.jks -storepass 123456
```

(如能查询到三张证书且形成完整的证书链路则为正确导入)

配置 WEBSPHERE APPLICATION SERVER6.1

访问<http://hostname:port/IBM/console>，输入用户名和密码(软件概要文件配置时设置的。)



然后登录控制台页面，选中左边菜单中“安全性”→“SSL 证书和密钥管理”→选中列表中的“密钥库和证书”，点击打开，选择新建密钥库，设置证书。



密钥库和证书配置完成之后选择“SSL 设置”，如图：

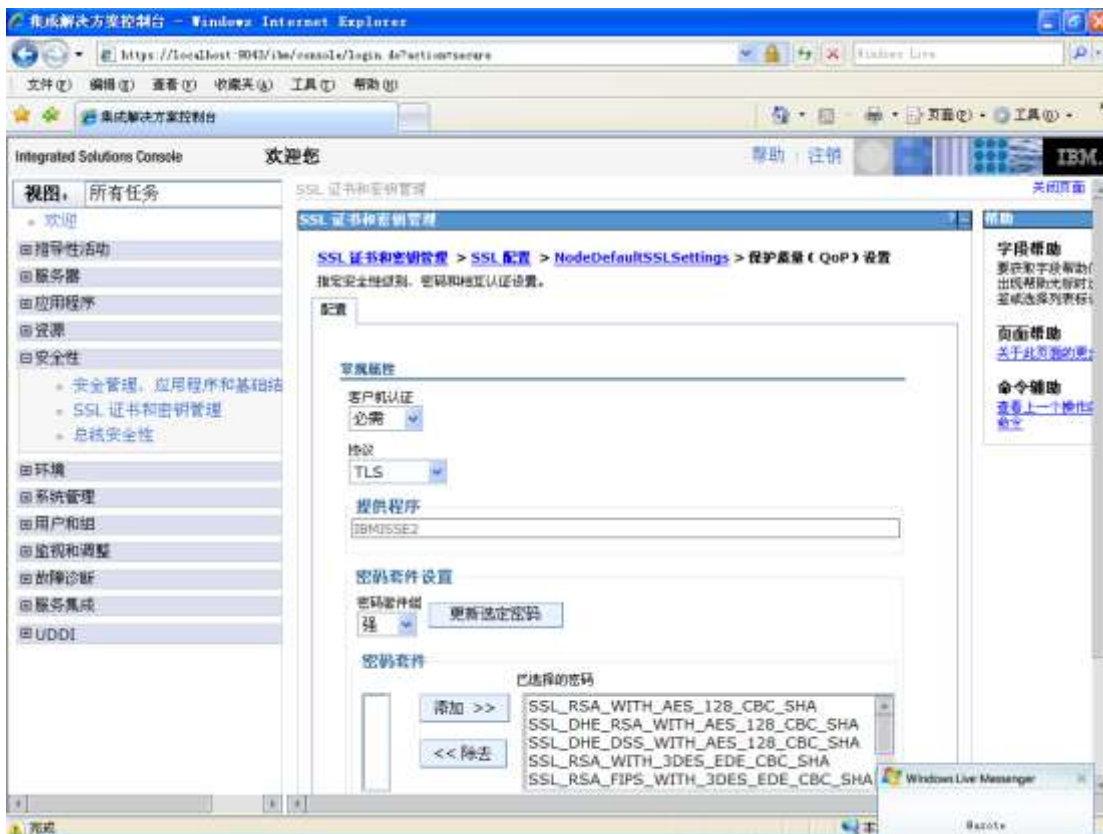


根据实际情况设置使用的密钥库和信任库。

确认应用的配置，然后保存主配置。

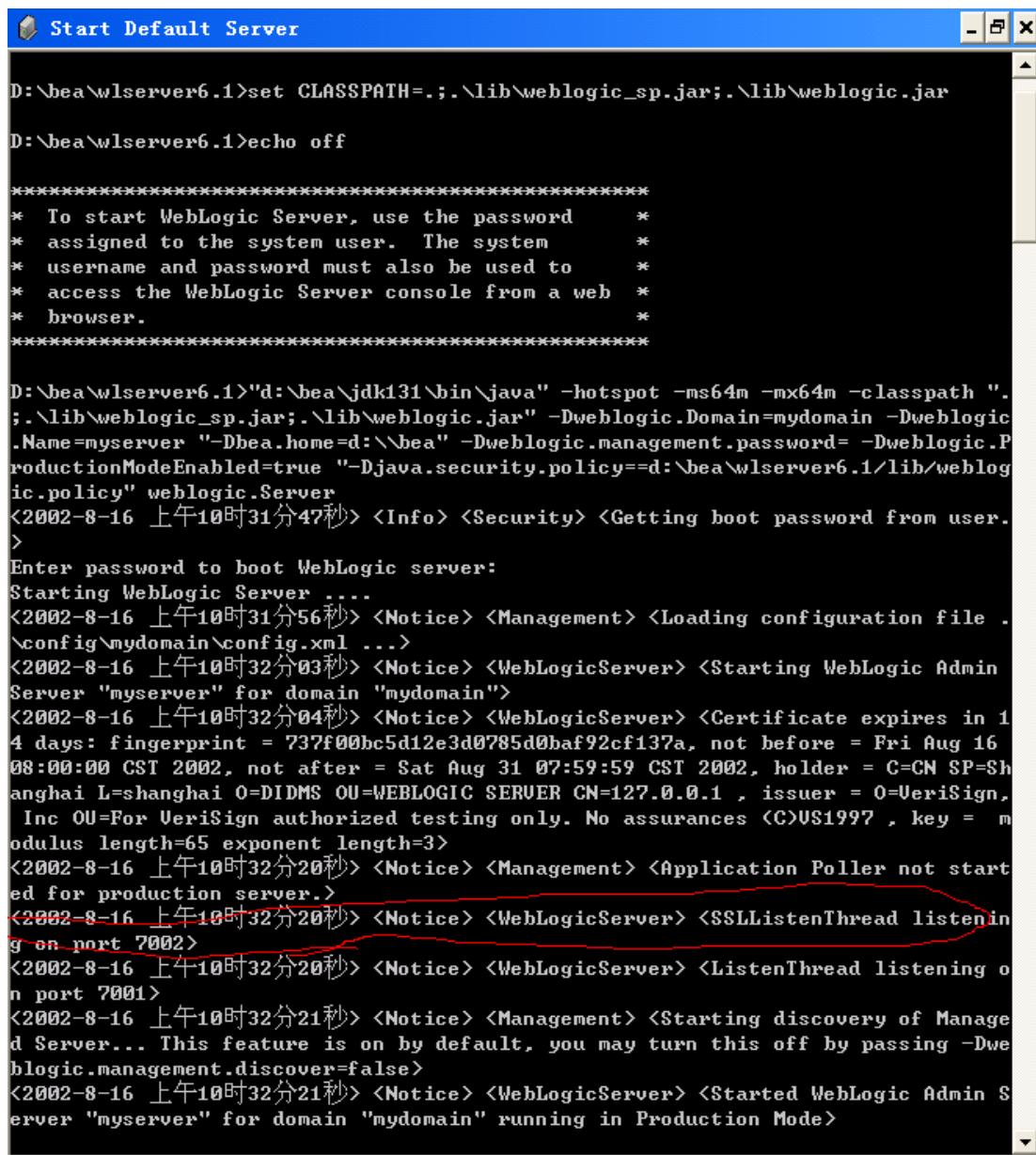


如果要开启双向认证，在“SSL 设置”→“Qop 设置”处选择客户机认证为“必需”，如图：



保存配置后。

连接 <https://hostname:port> 测试是否成功。



```
D:\bea\wlserver6.1>set CLASSPATH=.;.\lib\weblogic_sp.jar;.\lib\weblogic.jar
D:\bea\wlserver6.1>echo off

*****
* To start WebLogic Server, use the password          *
* assigned to the system user. The system            *
* username and password must also be used to        *
* access the WebLogic Server console from a web      *
* browser.                                           *
*****

D:\bea\wlserver6.1>"d:\bea\jdk131\bin\java" -hotspot -ms64m -mx64m -classpath ".
;.\lib\weblogic_sp.jar;.\lib\weblogic.jar" -Dweblogic.Domain=mydomain -Dweblogic
.Name=myserver "-Dbea.home=d:\bea" -Dweblogic.management.password= -Dweblogic.P
roductionModeEnabled=true "-Djava.security.policy=d:\bea\wlserver6.1\lib\weblog
ic.policy" weblogic.Server
<2002-8-16 上午10时31分47秒> <Info> <Security> <Getting boot password from user.
>
Enter password to boot WebLogic server:
Starting WebLogic Server ....
<2002-8-16 上午10时31分56秒> <Notice> <Management> <Loading configuration file .
\config\mydomain\config.xml ...>
<2002-8-16 上午10时32分03秒> <Notice> <WebLogicServer> <Starting WebLogic Admin
Server "myserver" for domain "mydomain">
<2002-8-16 上午10时32分04秒> <Notice> <WebLogicServer> <Certificate expires in 1
4 days: fingerprint = 737f00bc5d12e3d0785d0baf92cf137a, not before = Fri Aug 16
08:00:00 CST 2002, not after = Sat Aug 31 07:59:59 CST 2002, holder = C=CN SP=Sh
anghai L=shanghai O=DIRMS OU=WEBLOGIC SERVER CN=127.0.0.1 , issuer = O=VeriSign,
Inc OU=For VeriSign authorized testing only. No assurances (C)US1997 , key = m
odulus length=65 exponent length=3>
<2002-8-16 上午10时32分20秒> <Notice> <Management> <Application Poller not start
ed for production server.>
<2002-8-16 上午10时32分20秒> <Notice> <WebLogicServer> <SSLListenThread listenin
g on port 7002>
<2002-8-16 上午10时32分20秒> <Notice> <WebLogicServer> <ListenThread listening o
n port 7001>
<2002-8-16 上午10时32分21秒> <Notice> <Management> <Starting discovery of Manage
d Server... This feature is on by default, you may turn this off by passing -Dwe
blogic.management.discover=false>
<2002-8-16 上午10时32分21秒> <Notice> <WebLogicServer> <Started WebLogic Admin S
erver "myserver" for domain "mydomain" running in Production Mode>
```

以后，你可以通过如下方式访问 WEB 服务：<https://hostname:7002/>