服务器 SSL 证书安装配置指南

Weblogic

更新日期：2017-3-3

GlobalSign China Co., Ltd.

http://cn.globalsign.com Email：support-china@globalsign.com 电话：021-31395560 传真：021-60761793

第一步：生成证书请求文件(CSR)

进入 Java_JRE\bin 目录，如 cd C:\PROGRA~1\Java\jre1.5.0_06\bin，运行如下命令：

```
keytool -genkey -alias weblogic –keyalg RSA –keysize 2048 -keystore c:\ca\keystore.jks
输入 keystore 密码：********
```

输入 keystore 密码，务必牢记此密码。

```
您的名字与姓氏是什么？
  [Unknown]：  cn.globalsign.com
您的组织单位名称是什么？
  [Unknown]：  IT Dept.
您的组织名称是什么？
  [Unknown]：  GlobalSign China Co., Ltd.
您所在的城市或区域名称是什么？
  [Unknown]：  Shanghai
您所在的州或省份名称是什么？
  [Unknown]：  Shanghai
该单位的两字母国家代码是什么
  [Unknown]：  CN
```

您的名字与姓氏是什么？（这里输入域名，如: cn.globalsign.com）
您的组织单位名称是什么？（这里输入部门名称，如: IT Dept）
您的组织名称是什么？（这里输入公司名称名称，如： GlobalSign China Co., Ltd.）
您所在的城市或区域名称是什么？（这里输入城市，如：Shanghai）
您所在的州或省份名称是什么？（这里输入省份，如：Shanghai）
该单位的两字母国家代码是什么？（这里输入 2 位国家代码，如： CN）

```
CN=cn.globalsign.com, OU=IT Dept, O= GlobalSign China Co., Ltd., L=Shanghai, ST=Shanghai, C=CN
正确吗？
  [否]：  Y
```

请核对信息，如果确认无误后请直接输入 Y 并回车

```
输入<weblogic>的主密码
        （如果和 keystore 密码相同，按回车）：
```

不需要另外设置独立密码，这里回车即可。

```
keytool -certreq -alias weblogic -file certreq.csr -keystore c:\ca\keystore.jks
输入 keystore 密码：********
```

输入密码后回车，这时会生成一个 certreq.csr 的文件，此文件为证书请求文件（CSR）。

第二步：提交 CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。
我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取并安装服务器证书

1. 获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第二段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 intermediate.cer（文本格式）。

```
keytool -import -alias inter -keystore c:\ca\keystore.jks -trustcacerts -file c:\ca\intermediate.cer
```

2. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 server.cer（文本格式）。

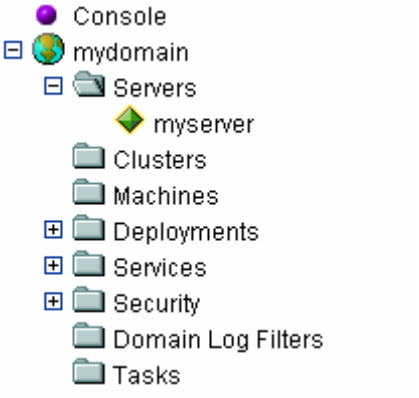
```
keytool -import -alias weblogic -keystore c:\ca\keystore.jks -trustcacerts -file c:\ca\server.cer
```

第三步全部完成后，表示证书已经完全安装到 keystore 这个文件中，请备份此文件并妥善保存，以后如有更换服务器或重装系统，就可以直接使用此文件。

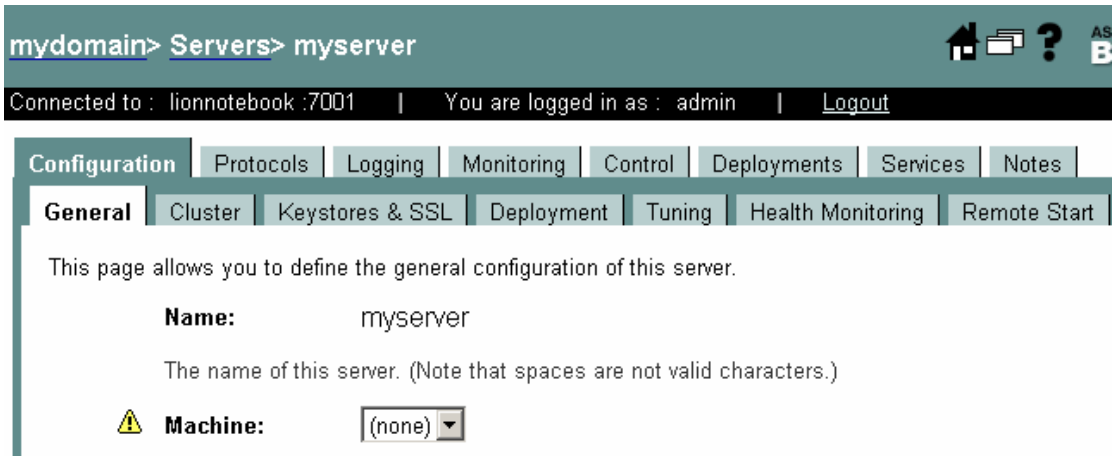
第四步、配置 WebLogic 8.1 使其支持 SSL 双向认证

（1）、设置用户通过SSL加密通道访问Web服务器

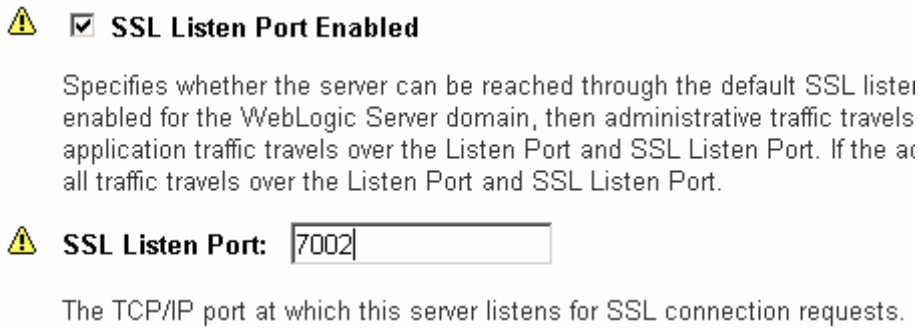
展开左边树形目录，选择新建的服务“myserver”。



选择“**General**”面板



选中“SSL Listen Port Enabled”选项，并为SSL Listen Port分配端口（默认是7002）。设置完成后点击“Apply”按钮。



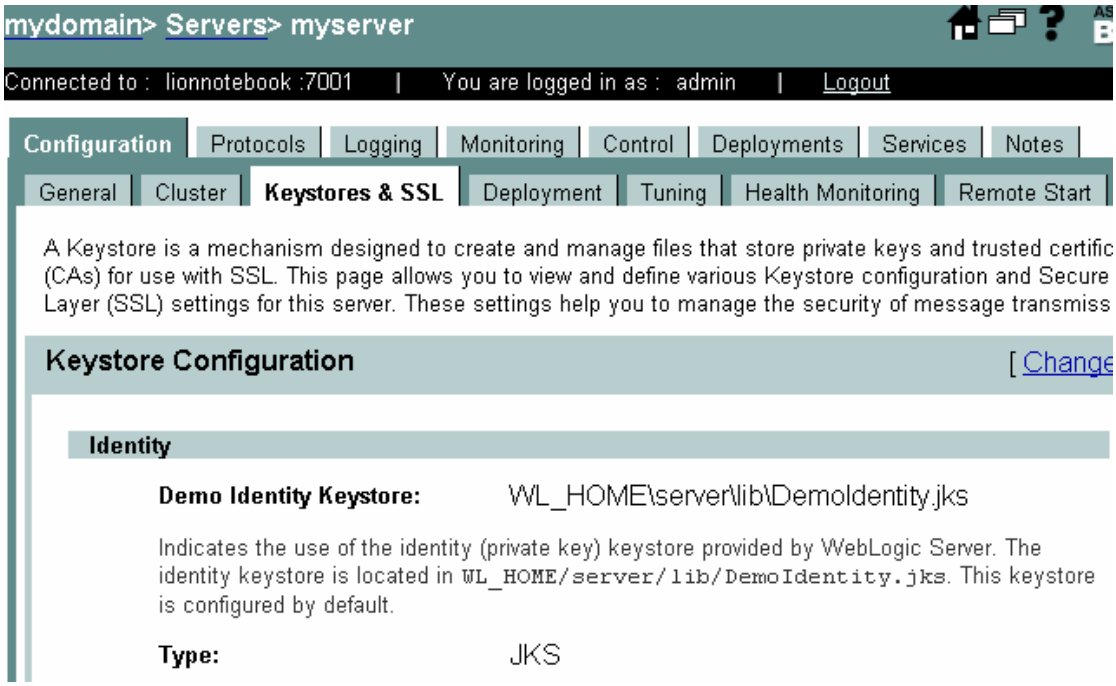
你可以把这个端口号改为443，那么在以SSL通道访问网站的时候就不用加端口号了。

可以直接这么访问：

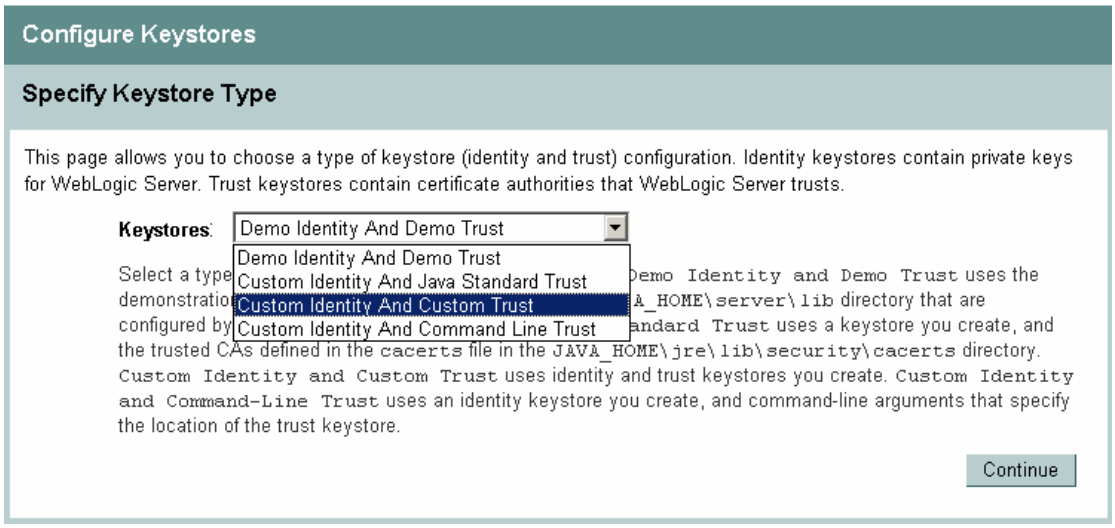
https://YourSiteDomainName/

（2）、配置支持SSL所必需的Keystore文件

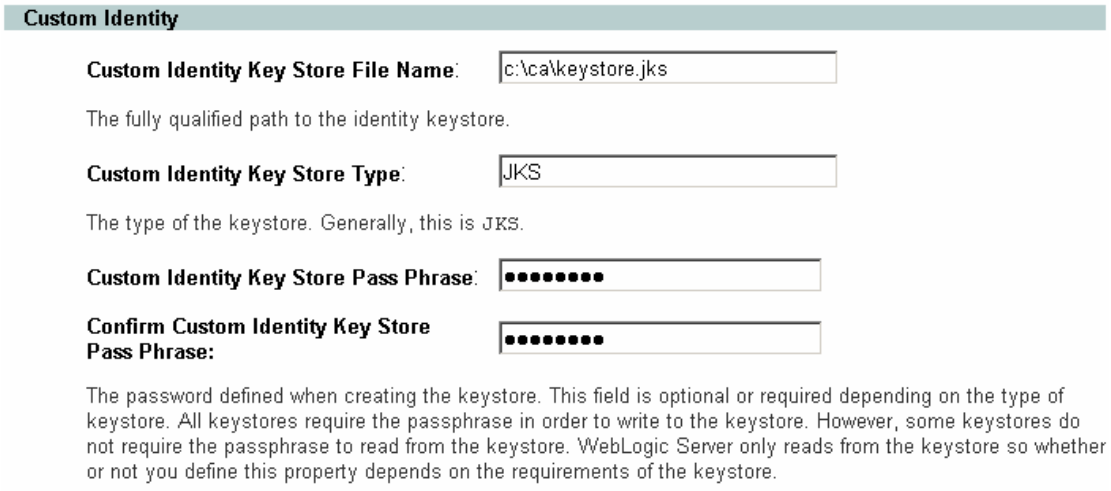
切换到“**Keystores & SSL**”面板，为了让WebLogic使用我们指定的服务器证书和指定的专用用户证书登陆，单击“**Change**”



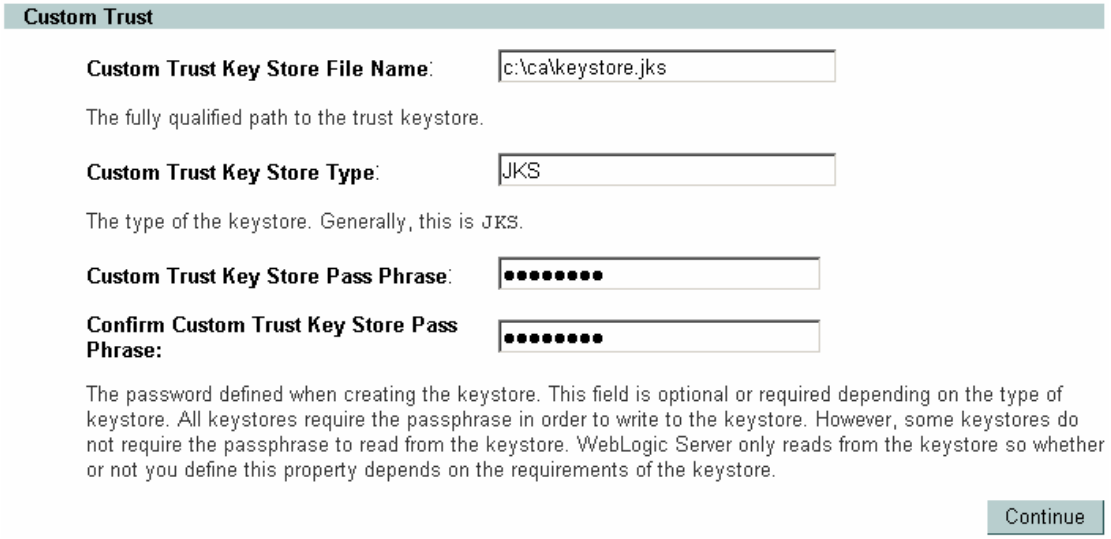
在Keystores下拉菜单中，选择“Custom Identity And Custom Trust”



在Custom Identity中填写keystore.jks的绝对路径，以及keystore的访问密码，这里的访问密码就是前面设置的“password”：（如下图）

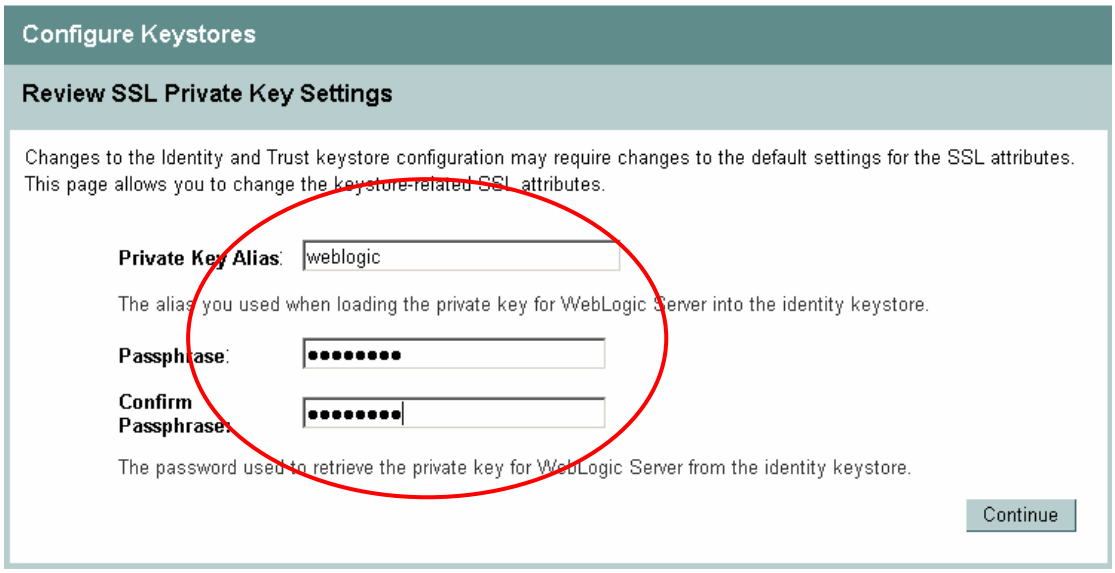


由于我们使用了同一个keystore来存放服务器证书和用户证书信任链，所以在Custom Trust中也填写与Custom Identity同样的内容：（如下图）



完成后，点击Continue进入下一步设置

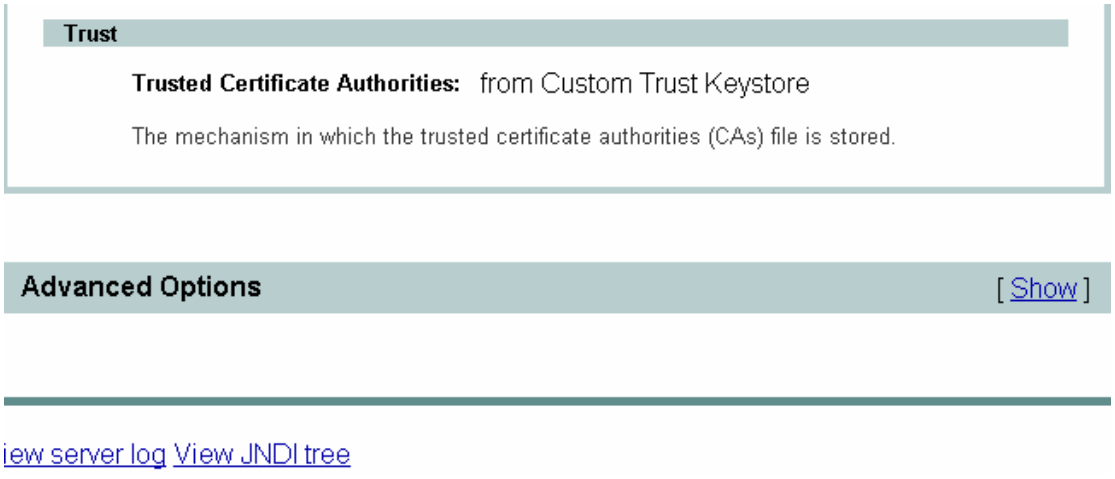
在**ReView SSL Private Key Settings**中，需要填写前面生成服务器证书密钥对时设置的私钥别名和密码，由于我们直接回车，则说明设置的“weblogic”密码是和Key Store访问密码同样的密码“password”，填写完成后，点击“Continue”按钮完成设置。



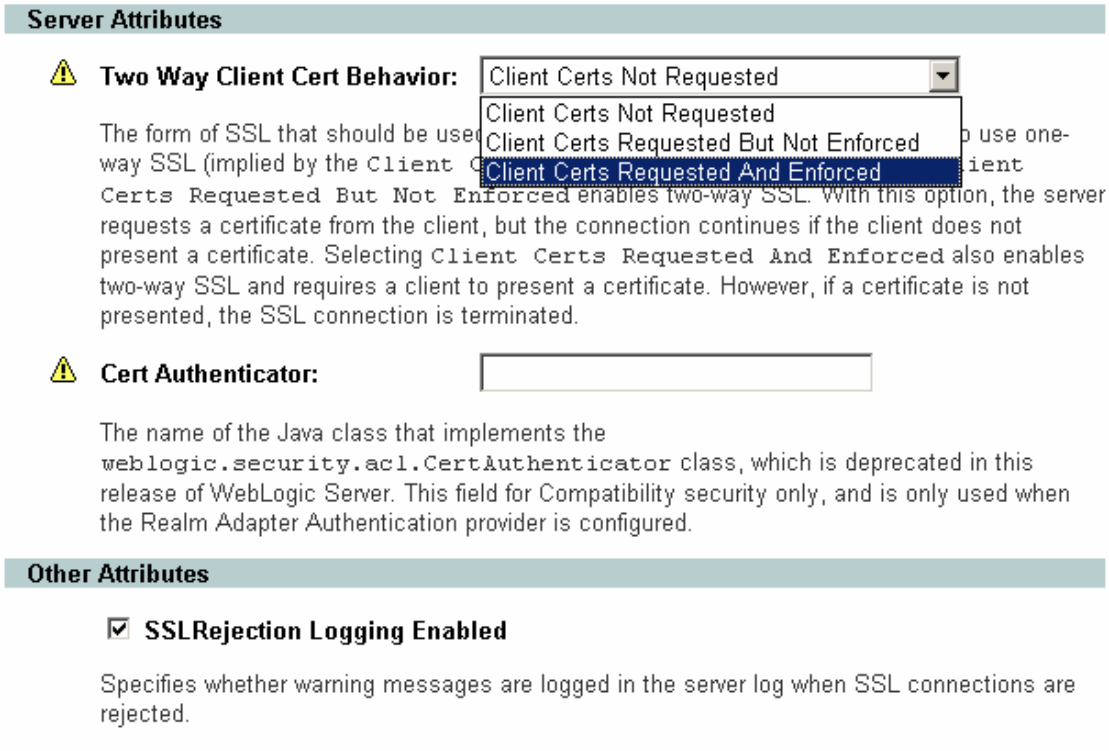
Private Key Alias是生成keystore文件时设置的服务器证书别名，即weblogic，当时设置密码时直接回车，所以**Passphrase**也是password

如果要启用客户端认证，还需作以下设置，若只使用服务器证书，这一步可以忽略。

在完成了Key Store的基本设置后，页面会自动转到“**Keystores & SSL** ”面板，拖拽滑动条滚动到该页最底部“**Advanced Options**”，单击“[Show]”



在展开的高级属性页的底部找到“**Server Attributes**”，将“**Two Way Client Cert Behavior:**”改为“Client Certs Requested And Enforced”（启用并强制客户端证书认证）或者“Client Certs Requested But Not Enforced”（启用但不强制客户端证书认证）



启用并强制客户端证书认证

全部设置完成后，重新启动 Weblogic，访问
https://你的域名 （如果你将SSL端口设置为443，可以这么访问）
https://你的域名:7002 （如果使用的是默认7002端口，可以这么访问）

如有任何问题或疑问请直接与我们联系，谢谢！