



服务器 SSL 证书安装配置指南

Weblogic

更新日期：2017-3-3

GlobalSign China Co., Ltd.

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
```

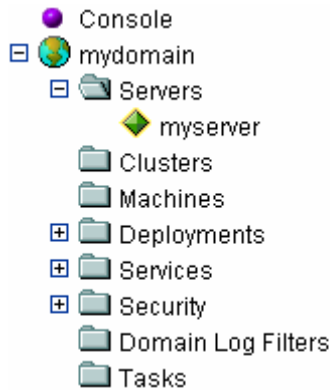
2. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 `server.cer`（文本格式）。

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

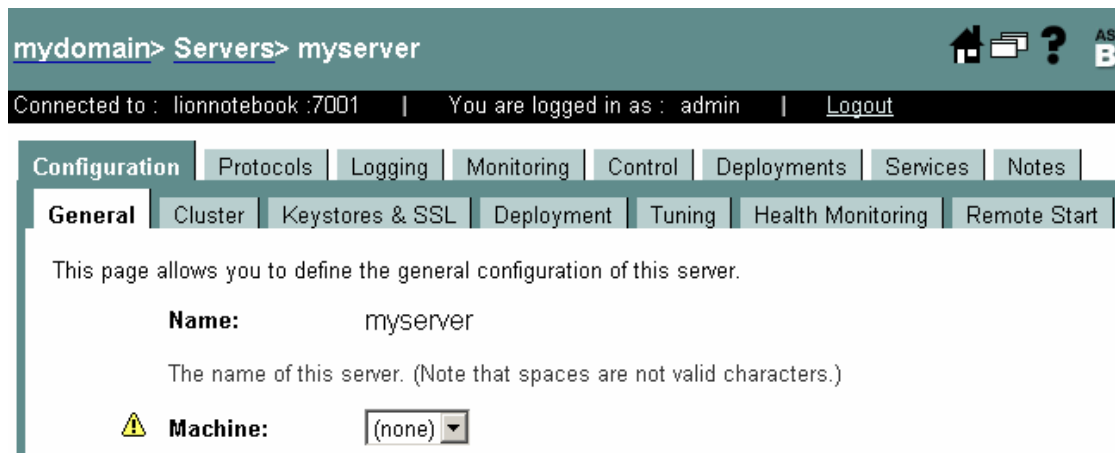
第三步全部完成后，表示证书已经完全安装到 `keystore` 这个文件中，请备份此文件并妥善保存，以后如有更换服务器或重装系统，就可以直接使用此文件。

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。

SSL Listen Port Enabled

Specifies whether the server can be reached through the default SSL listen enabled for the WebLogic Server domain, then administrative traffic travels application traffic travels over the Listen Port and SSL Listen Port. If the all traffic travels over the Listen Port and SSL Listen Port.

SSL Listen Port:

The TCP/IP port at which this server listens for SSL connection requests.

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**”

mydomain> Servers> myserver

Connected to : lionnotebook :7001 | You are logged in as : admin | [Logout](#)

Configuration | Protocols | Logging | Monitoring | Control | Deployments | Services | Notes

General | Cluster | **Keystores & SSL** | Deployment | Tuning | Health Monitoring | Remote Start

A Keystore is a mechanism designed to create and manage files that store private keys and trusted certificate (CAs) for use with SSL. This page allows you to view and define various Keystore configuration and Secure Layer (SSL) settings for this server. These settings help you to manage the security of message transmission.

Keystore Configuration [\[Change \]](#)

Identity

Demo Identity Keystore: WL_HOME\server\lib\Demoidentity.jks

Indicates the use of the identity (private key) keystore provided by WebLogic Server. The identity keystore is located in WL_HOME/server/lib/DemoIdentity.jks. This keystore is configured by default.

Type: JKS

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

Configure Keystores

Specify Keystore Type

This page allows you to choose a type of keystore (identity and trust) configuration. Identity keystores contain private keys for WebLogic Server. Trust keystores contain certificate authorities that WebLogic Server trusts.

Keystores:

Select a type of keystore configuration. Demo Identity and Demo Trust uses the keystore and trust keystores you create, and the trusted CAs defined in the cacerts file in the JAVA_HOME\jre\lib\security\cacerts directory. Custom Identity and Custom Trust uses identity and trust keystores you create. Custom Identity and Command-Line Trust uses an identity keystore you create, and command-line arguments that specify the location of the trust keystore.

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）

Custom Identity**Custom Identity Key Store File Name:**

The fully qualified path to the identity keystore.

Custom Identity Key Store Type:

The type of the keystore. Generally, this is JKS.

Custom Identity Key Store Pass Phrase: **Confirm Custom Identity Key Store Pass Phrase:**

The password defined when creating the keystore. This field is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.

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）

Custom Trust**Custom Trust Key Store File Name:**

The fully qualified path to the trust keystore.

Custom Trust Key Store Type:

The type of the keystore. Generally, this is JKS.

Custom Trust Key Store Pass Phrase: **Confirm Custom Trust Key Store Pass Phrase:**

The password defined when creating the keystore. This field is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.

[Continue](#)

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。

Configure Keystores

Review SSL Private Key Settings

Changes to the Identity and Trust keystore configuration may require changes to the default settings for the SSL attributes. This page allows you to change the keystore-related SSL attributes.

Private Key Alias:

The alias you used when loading the private key for WebLogic Server into the identity keystore.

Passphrase:

Confirm Passphrase:

The password used to retrieve the private key for WebLogic Server from the identity keystore.

[Continue](#)

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“[\[Show\]](#)”

Trust

Trusted Certificate Authorities: from Custom Trust Keystore

The mechanism in which the trusted certificate authorities (CAs) file is stored.

Advanced Options [\[Show \]](#)

[View server log](#) [View JNDI tree](#)

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）

Server Attributes

 **Two Way Client Cert Behavior:**

The form of SSL that should be used. Selecting **Client Certs Not Requested** enables one-way SSL (implied by the Client Certs Requested But Not Enforced option). Selecting **Client Certs Requested But Not Enforced** enables two-way SSL. With this option, the server requests a certificate from the client, but the connection continues if the client does not present a certificate. Selecting **Client Certs Requested And Enforced** also enables two-way SSL and requires a client to present a certificate. However, if a certificate is not presented, the SSL connection is terminated.

 **Cert Authenticator:**

The name of the Java class that implements the `weblogic.security.acl.CertAuthenticator` class, which is deprecated in this release of WebLogic Server. This field for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured.

Other Attributes

SSLRejection Logging Enabled

Specifies whether warning messages are logged in the server log when SSL connections are rejected.

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）

如有任何疑问或问题请直接与我们联系，谢谢！