

服务器 SSL 证书安装配置指南

Websphere Application Server 7

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 ssl -keyalg RSA -keysize 2048 -keystore c:\ssl.jks  
输入 keystore 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 < ssl > 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，完成后在 C 盘根目录下就会生成一个 ssl.jks 的 JAVA 证书池文件，在证书办法并导入前请妥善保存此文件。

```
keytool -certreq -alias ssl -keystore c:\ssl.jks -file c:\certreq.csr  
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 -trustcacerts -keystore c:\ssl.jks -alias inter -file 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）。

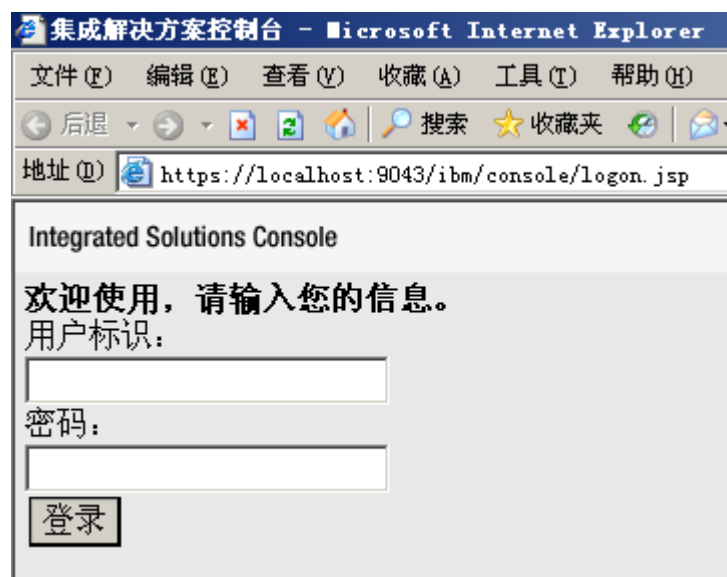
```
keytool -import -trustcacerts -keystore c:\ssl.jks -alias ssl -file server.cer
```

第三步全部完成后，表示证书已经完全安装到 `ssl.jks` 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：安装服务器证书

将合成好的 JKS 文件导入到服务器上

打开“管理控制台”，输入管理帐户，点击“登录”，



在“安全性”下，点击“SSL 证书和密钥管理”



点击“管理端点安全配置”

SSL 配置

安全套接字层（SSL）协议在远程服务器进程或端点之间建立安全通信，必须对该端点指定证书和 SSL 配置。

在本产品的先前版本中，需要为每个端点手动配置安全配置。此功能使您能够集中管理安全通信。另外，通过

如果已使用迁移实用程序将受保护的环境迁移到此版本，配置 SSL 才能利用集中管理功能。

配置设置

管理端点安全配置

管理证书到期

- 使用美国联邦信息处理标准（FIPS）算法。注意：
- 当发生 SSL 配置更改时动态更新运行时

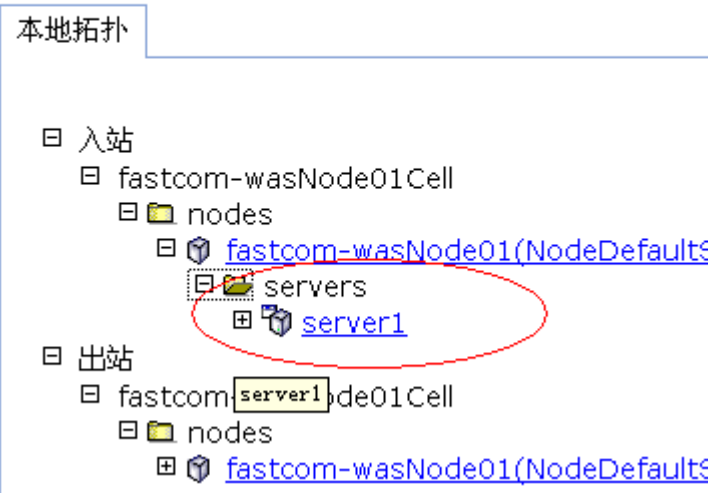
应用

复位

在“本地拓扑”下的“入站”下，选择“Server1”

SSL 证书和密钥管理 > 管理端点安全配置

显示所选作用域的安全套接字层（SSL）配置，例如，单



在屏幕右侧点击“密钥库和证书”

相关项

- [SSL 配置](#)
- [动态出站端点 S](#)
- [SL 配置](#)
- [密钥库和证书](#)
- [密钥集](#)
- [密钥集组](#)
- [密钥管理器](#)
- [信任管理器](#)
- [认证中心 \(CA\)](#)
- [客户机配置](#)

命令辅助

[查看上一个操作制命令](#)

点击“NodeDefaultKeyStore”

SSL 证书和密钥管理

[SSL 证书和密钥管理](#) > [管理端点安全配置](#) > [seri](#)

定义密钥库类型，包含密码术、RACF(R)、CMS、Jav

密钥库的用法

SSL 密钥库

田 首选项

新建	删除	更改密码...	交换签署者
选择	名称	描述	
您可以管理以下资源:			
<input checked="" type="checkbox"/>	NodeDefaultKeyStore	fastcom-was 密钥库	
<input type="checkbox"/>	NodeDefaultTrustStore	fastcom-was 信任库	

在页面右边的“其他属性”中点击“个人证书”

其他属性

- [签署者证书](#)
- [个人证书](#)
- [个人证书请求](#)
- [定制属性](#)

页面帮助

[关于此页面的更多](#)

点击“导入”

SSL 证书和密钥管理

SSL 证书和密钥管理 > 管理端点安全配置 > server1 > 密钥库和证书 > NodeDefaultKeys

管理个人证书。

管理选项

创建... 删除... 从认证中心接收... 替换... 抽取... **导入...** 导出...

选择	别名	颁发给	颁发者	序列号
<input type="checkbox"/>	default	CN=192.168.133.129, OU=fastcom-wasNode01Cell, OU=fastcom-wasNode01, O=IBM, C=US	CN=192.168.133.129, OU=Root Certificate, OU=fastcom-wasNode01Cell, OU=fastcom-wasNode01, O=IBM, C=US	1535
<input type="checkbox"/>		CN=192.168.133.129, OU=Root Certificate, OU=fastcom-wasNode01Cell, OU=fastcom-wasNode01, O=IBM, C=US	CN=192.168.133.129, OU=Root Certificate, OU=fastcom-wasNode01Cell, OU=fastcom-wasNode01, O=IBM, C=US	1535

您可以管理以下资源:

输入 JKS 文件的位置: “c:\ssl.jks”, 类型选择“JKS”, 输入保护密码, 然后点击“获取密钥文件别名”

[SSL 证书和密钥管理](#) > [管理端点安全配置](#) > [server1](#) > [密钥库和证书](#) > [NodeD](#)
 从密钥库文件或现有密钥库中导入证书 (包括专用密钥)。
 常规属性

受管密钥库
 密钥库
 NodeDefaultKeyStore ((cell):fastcom-wasNode01Cell:(node
 密钥库密码

密钥库文件
 * 密钥文件名
 c:\ssl.jks
 类型
 JKS
 * 密钥文件密码
 ●●●●●●

要导入的证书别名
 (无)

已导入的证书别名

WAS 会从 JKS 文件中读取密钥对的别名, 选择 JKS 中的密钥对别名, 并输入导入到 WAS 后的别名, 然后点击“确定”

[SSL 证书和密钥管理](#) > [管理端点安全配置](#) > [server1](#) > [密钥库和证书](#) > [NodeD](#)
 从密钥库文件或现有密钥库中导入证书 (包括专用密钥)。
 常规属性

受管密钥库
 密钥库
 NodeDefaultKeyStore ((cell):fastcom-wasNode01Cell:(node
 密钥库密码

密钥库文件
 + 密钥文件名
 c:\ssl.jks
 类型
 JKS
 + 密钥文件密码
 ●●●●●●

要导入的证书别名
 ssl

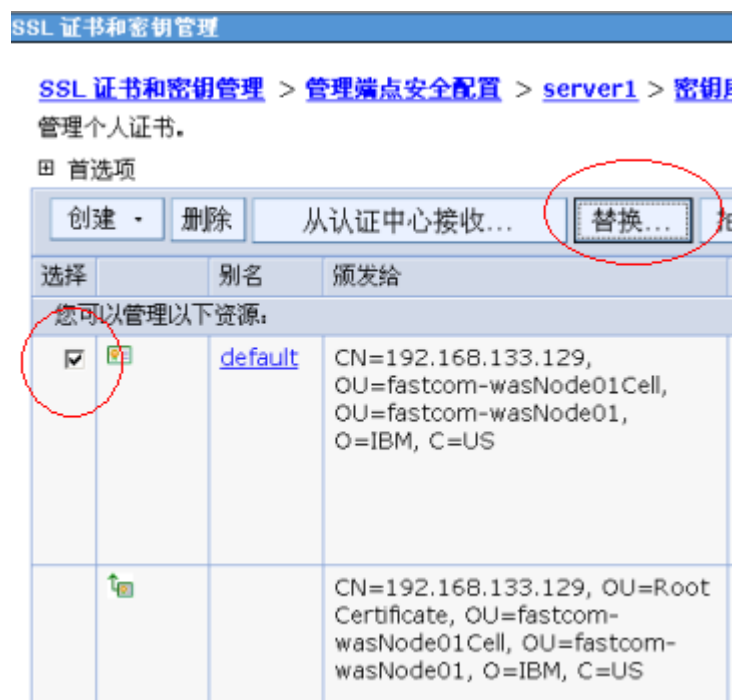
已导入的证书别名
 Ssl

这时可以看到，WAS 中多了一个 SSL 别名的密钥对，点击“保存”到主配置



[密钥管理](#) > [管理端点安全配置](#) > [server1](#) > [密钥库和](#)

选中“default”别名，点击“替换”



选择“替换为‘SSL’”，点击“确定”

SSL 证书和密钥管理

[SSL 证书和密钥管理](#) > [管理端点安全配置](#) > [serv](#)
[书](#) > [替换证书](#)

将一个证书替换为新证书。还将替换签署者证书。

常规属性

旧证书
default

替换为
ssl

在替换后删除旧的证书

删除旧的签署者

应用
确定
复位
取消

点击“保存”到主配置

onsole admin, 欢迎您

m-wasNode01Cell, 概要文件 = AppSrv01

管理

消息

⚠ 已更改了您的本地配置。您可以：
直接

- [保存到主配置。](#)
- [查看更改。](#)

保存或放弃之前

⚠ 要使这些更改生效，可能需要重新启动服务器。

[密钥管理](#) > [管理端点安全配置](#) > [server1](#) > [密钥库和](#)

重新启动 WAS 服务器进程，证书已经替换上去了

按照以上的步骤配置完成后就可以使用 https://www.domain.com 来访问了。
如有任何疑问或问题请直接与我们联系，谢谢！