

# HTTPS证书安装

IOS 7.1版本中，若使用WEB的安装方式，只能使用HTTPS来通讯，因此需要在应用服务器上部署SSL证书。

## 文档目录:

- [SSL证书获取](#)
- [J2EE应用服务器上安装SSL证书](#)
  - [附录1: TOMCAT服务器证书部署](#)
  - [附录2: WEBSPHERE服务器证书部署](#)
  - [附录3: WEBLOGIC 10/12c服务器证书部署](#)
  - [附录4: 在J2EE服务器上发布APP. WAR](#)
- [IIS上安装SSL证书及发布ipa](#)
- [部署完成后的问题诊断](#)
- [升级Tomcat](#)

## SSL证书获取

请用户向CA厂商获取证书。

获取证书后，按照以下的说明进行证书部署。

## J2EE应用服务器上安装SSL证书

由于tomcat使用ssl配置https时，爆发出了严重安全漏洞，按照apache官方建议，升级tomcat到7.0.85及以后版本，修复安全漏洞。

查看tomcat版本方法：执行<tomcat>/bin/version.sh或version.bat

```
[root@centos7 bin]# ./version.sh
Using CATALINA_BASE:   /home/smartbi/apache-tomcat-7.0.90
Using CATALINA_HOME:   /home/smartbi/apache-tomcat-7.0.90
Using CATALINA_TMPDIR: /home/smartbi/apache-tomcat-7.0.90/temp
Using JRE_HOME:        /home/smartbi/jdk1.8.0_172
Using CLASSPATH:       /home/smartbi/apache-tomcat-7.0.90/bin/bootstrap.jar:/home/smartbi/apache-tomcat-7.0.90/bin/tomcat-juli.jar
Server version: Apache Tomcat/7.0.90
Server built:   Jul 2 2018 17:05:37 UTC
Server number:  7.0.90.0
OS Name:        Linux
OS Version:     3.10.0-693.el7.x86_64
Architecture:   amd64
JVM Version:    1.8.0_172-b11
JVM Vendor:     Oracle Corporation
[root@centos7 bin]#
```

Tomcat下载地址：Tomcat官网

升级Tomcat详情请参见 [升级Tomcat](#)。

## 附录1: TOMCAT服务器证书部署

1. 进入服务器安装目录的conf 子目录，编辑 server.xml文件
2. 修改里面的SSL设置，改法如下：

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="xx/xx/xx.keystore"
    keystorePass="xxxx" />
```

需要注意修改的就是端口号和证书路径，证书密码。  
说明：注意防火墙是否禁用端口。

1. 阿里云证书配置tomcat https访问参考如下：

```
<Connector port="8443" protocol="HTTP/1.1"
    maxThreads="150"
    SSLEnabled="true"
    scheme="https"
    secure="true"
    clientAuth="false"
    keystoreFile="/xxx/xxx/xxx.pfx"
    keystoreType="PKCS12"
    keystorePass="xxx"
    SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
    TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256" />z
```

- a. 注：如参考以上配置无法通过https访问，请参考以下修改配置。

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
    maxThreads="150"
    SSLEnabled="true"
    scheme="https"
    secure="true"
    clientAuth="false"
    keystoreFile="/xxx/xxx/xxx.pfx"
    keystoreType="PKCS12"
    keystorePass="xxx"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
    TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256" />
```

## 附录2：WEBSPPHERE服务器证书部署

以WAS8.5举例说明

1. 进入服务器管理页面，“安全性”——“SSL证书和密钥管理”



2. 进入“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提供安全通信。SSL 安全性可用于建立端点的入站通信和出站通信。要建立安全通信，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套接字层 (SSL)。在本版本中，可以为整个应用程序处理环境定义单一配置。此功能使您能够集中管理安全通信。另外，通过覆盖缺省的单元级 SSL 配置，可以在多节点环境中建立信任区域。

如果已使用迁移实用程序将受保护的环境迁移到此版本，那么将为各个端点恢复旧的安全套接字层 (SSL) 配置。但是，需要重新配置 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

##### 管理 FIPS

☒ 当发生 SSL 配置更改时动态更新运行时

应用

复位

3. 选择对应的服务器或集群的入站设置

### 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，单元、节点、服务器或集群。

#### 本地拓扑

##### 入站

smartsvr03Node03Cell

nodes

smartsvr03Node03(NodeDefaultSSLSettings,192.168.1.10)

##### 出站

smartsvr03Node03Cell

nodes

smartsvr03Node03(NodeDefaultSSLSettings)

4. 进入管理证书

### 此端点的特定 SSL 配置

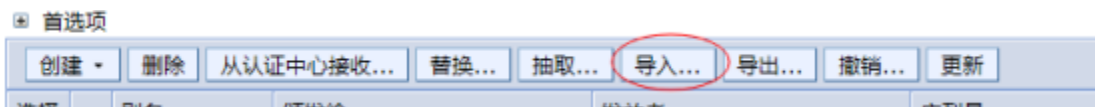
SSL 配置  
NodeDefaultSSLSettings

更新证书别名列表

管理证书

密钥库中的证书别名

5. 填写证书存放的路径，导入证书，



注意选择证书别名，选择上面用OpenSSL工具生成的pfx文件，密码默认为：ServerPassword

● 密钥库文件

\* 密钥文件名  
d:\192.168.1.10.pfx

类型  
PKCS12

\* 密钥文件密码  
.....

获取密钥文件别名

要导入的证书别名  
192.168.1.10

已导入的证书别名

6. 导入后回到上层菜单选择导入的证书别名保存，并重启服务器。

## 常规属性

名称

smartsvr03Node03

方向

入站

## 此端点的特定 SSL 配置

SSL 配置

NodeDefaultSSLSettings

更新证书别名列表

管理证书

密钥库中的证书别名

192.168.1.10

应用

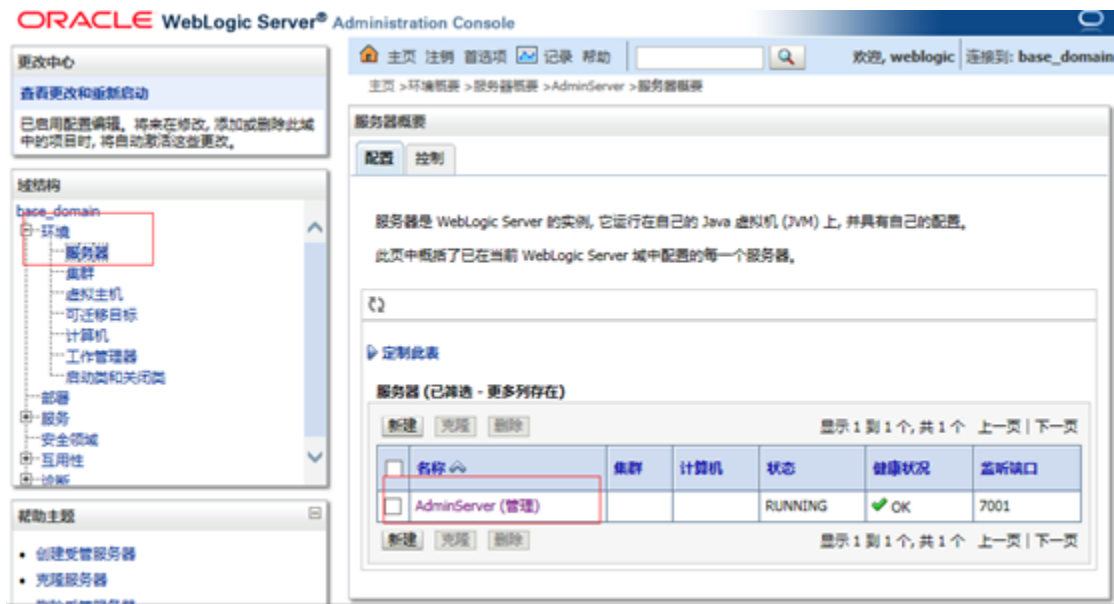
确定

复位

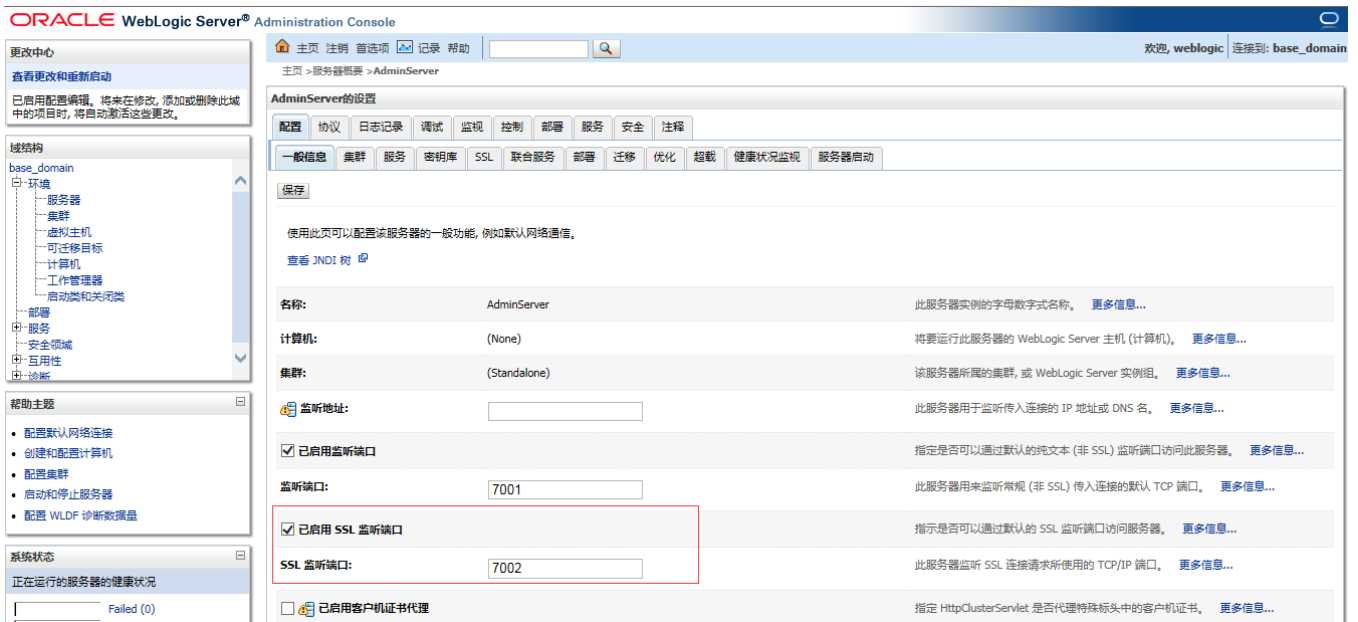
取消

## 附录3：WEBLOGIC 10/12c服务器证书部署

1、进入服务器管理页面，“环境”——“服务”——“AdminServer”



2、启动SSL端口。



3、进入“密钥库”页面，点击更改按钮，设为“定制标识和Java标准信任”，设置“密钥库标识”和“密钥库信任”信息。

“密钥库标识”为pfx的路径。

“密钥库类型”为“PKCS12”

“密码”上面用OpenSSL工具生成的pfx文件密码默认为：ServerPassword

配置
协议
日志记录
调试
监视
控制
部署
服务
安全
注释

一般信息
集群
服务
密钥库
SSL
联合服务
部署
迁移
优化
超载
健康状况监视
服务器启动
Web 服务
Coherence

保存

密钥库可以确保私有密钥和可信证书颁发机构 (CA) 的安全存储和管理。在此页中, 您可以查看和定义各种密钥库配置。这些设置有助于管理消息传输的安全。

密钥库:

定制标识和 Java 标准信任 [更改](#)

查找服务器的标识和信任密钥库时应该使用哪些配置规则? [更多信息...](#)

— 标识 —

定制标识密钥库:

/home/weblogic/Oracle/Midd

标识密钥库的源。对于 JKS 密钥库, 该源为路径和文件名。对于 Oracle 密钥库服务 (KSS) 密钥库, 该源为 KSS URI。 [更多信息...](#)

定制标识密钥库类型:

PKCS12

密钥库的类型。此项一般为 JKS。如果使用的是 Oracle 密钥库服务, 此项为 KSS [更多信息...](#)

定制标识密钥库密码短语:

.....

定制标识密钥库的加密密码短语。如果为空或空值, 打开密钥库时将不需要密码短语。 [更多信息...](#)

确认定制标识密钥库密码短语:

.....

— 信任 —

Java 标准信任密钥库:

/app/jdk1.7.0\_79/jre/lib/security/cacerts

Java 标准信任密钥库的位置。 [更多信息...](#)

Java 标准信任密钥库类型:

jks

Java 标准信任密钥库的类型。此项一般为 JKS。 [更多信息...](#)

Java 标准信任密钥库密码短语:

Java 标准信任密钥库的口令。创建密钥库时定义此口令。 [更多信息...](#)

确认 Java 标准信任密钥库密码短语:

保存

3、进入到”SSL“页面，设置“私有密钥别名“和”密码“

ORACLE WebLogic Server® Administration Console

更改中心
查看更改和重新启动
已启用配置编辑。将来在修改、添加或删除此域中的项目时, 将自动激活这些更改。
域结构
base\_domain
环境
服务器
集群
虚拟主机
可迁移目标
计算机
工作管理器
启动类和关闭类
部署
服务
安全领域
互操作性
诊断
帮助主题
配置标识和信任
设置 SSL
确认已启用主机名验证
配置定制主机名验证器
配置双向 SSL
系统状态
正在运行的服务器的健康状况

主页
注销
首选项
记录
帮助

欢迎, weblogic
连接到: b

主页 > 服务器概览 > AdminServer

AdminServer 的设置
配置
协议
日志记录
调试
监视
控制
部署
服务
安全
注释
一般信息
集群
服务
密钥库
SSL
联合服务
部署
迁移
优化
超载
健康状况监视
服务器启动
保存

在此页中, 您可以查看和定义此服务器实例的各种安全套接字层 (SSL) 设置。这些设置有助于管理消息传输的安全。

标识和信任位置:

密钥库 [更改](#)

指示 SSL 应在何处查找服务器的标识 (证书和私有密钥) 以及服务器的信任 (颁发机构)。 [更多信息...](#)

— 标识 —

私有密钥位置:

来自定制标识密钥库

定义私有密钥文件位置的密钥库属性。 [更多信息...](#)

私有密钥别名:

192.168.1.58

定义用于存储和检索服务器私有密钥的字符串别名的密钥库属性。 [更多信息...](#)

私有密钥密码短语:

.....

密钥库属性, 定义用来检索服务器私有密钥的密码短语。 [更多信息...](#)

确认私有密钥密码短语:

.....

证书位置:

来自定制标识密钥库

用于定义信任证书位置的密钥库属性。 [更多信息...](#)

— 信任 —

信任证书颁发机构:

来自定制信任密钥库

用于定义证书颁发机构位置的密钥库属性。 [更多信息...](#)

高级

## 附录4：在J2EE服务器上发布APP. WAR

1. 下载app.war，并用winrar软件打开
2. 将新生成的RootCA.cer根证书，替换app.war中的原有证书

3. 修改app.war/index.htm文件中的相关链接，确保它使用HTTPS并且IP或域名与上述生成证书时输入的IP或域名一致

```
colspan="4" align="left">
<a href = "http://192.168.1.56:8080/app/RootCer.cer">
<span class = "btn-text">安装测试证书</span>
</a>
td>

d style="text-align: center"><strong>iOS</strong></td>
d>标准版<br/>(程序大小3.3M)</td>
d><u><font color="#0066cc"><A href="https://192.168.1.56:8080/app
d>适用于iPad/iPhone</td>

d style="text-align: center"><strong>安卓</strong></td>
d>标准版<br/>(程序大小3.2M)</td>
d><u><font color="#0066cc"><A href="http://192.168.1.56:8080/app/Smartbi.apk">Smartbi apk</a></u></td>
d>适用于安卓系统</td>
```

4. 修改app.war/Smartbi.plist文件中的相关链接，确保它使用HTTPS并且IP或域名与上述生成证书时输入的IP或域名一致

```
<dict>
<key>assets</key>
<array>
<dict>
<key>kind</key>
<string>software-package</string>
<key>url</key>
<string>https://192.168.1.56:8080/app/Smartbi.ipa</string>
</dict>
<dict>
<key>kind</key>
<string>display-image</string>
<key>url</key>
<string>https://192.168.1.56:8080/app/logo_144.png</string>
</dict>
</array>
<key>metadata</key>
<dict>
<key>bundle-identifier</key>
```

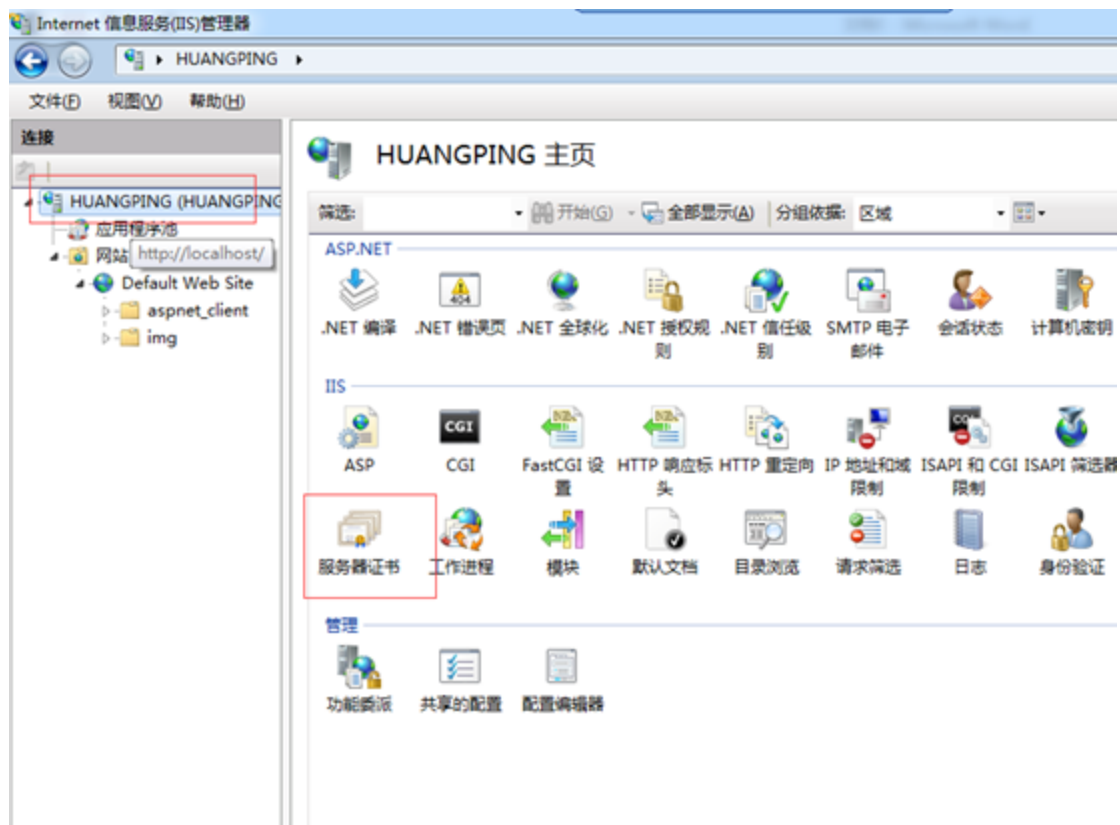
- 5. 参考smartbi在各应用服务器上的部署方式将修改后的app.war发布到服务器
- 6. iPad/iPhone中通过Safari访问IPA安装界面并点击该链接安装证书

操作系统	版本名称	下载地址	说明
安装测试证书			
iOS	标准版 (程序大小3.3M)	Smartbi ipa	适用于iPad/iPhone
安卓	标准版 (程序大小3.2M)	Smartbi apk	适用于安卓系统

7. 点击IPA安装链接进行安装

## IIS上安装SSL证书及发布ipa

1、打开IIS7，选择根节点，如下

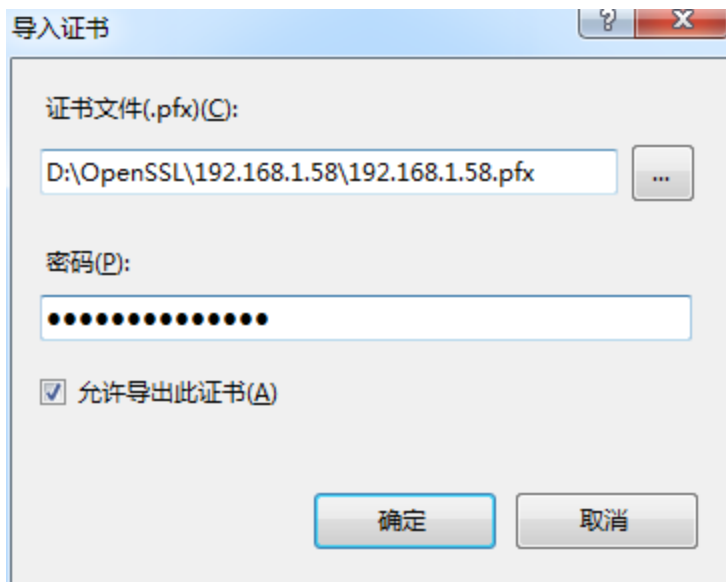


2、接下来可以在右边找到操作栏，选择导入

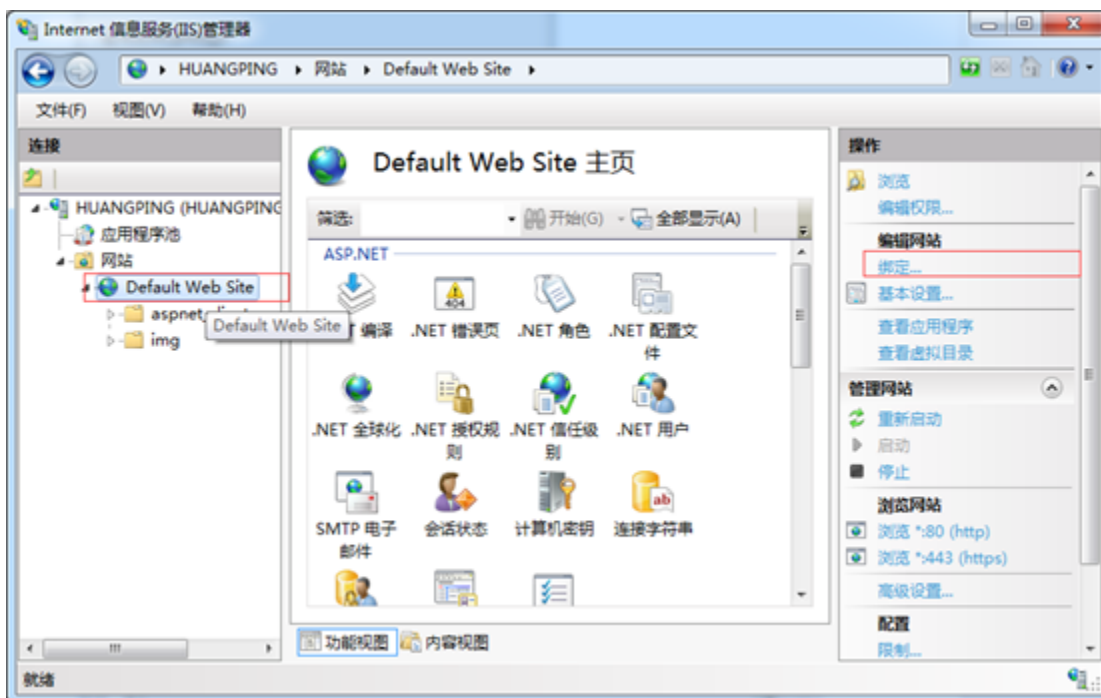


3、选择上面用OpenSSL工具生成的pfx文件，密码默认为：ServerPassword





4、选择一个你要启用https的站点，注间是站点不是其中的某个虚拟目录，点击绑定



5、点击“添加”，选择“类型”和上面导入的ssl证书，并确定。

添加网站绑定

类型(T): **https** IP 地址(I): 全部未分配 端口(O): 443

主机名(H):

SSL 证书(S):

未选定

未选定

192.168.1.58

查看(V)...

确定 取消

网站绑定

类型	主机名	端口	IP 地址	绑定信息
http		80	*	
https		443	*	

添加(A)...

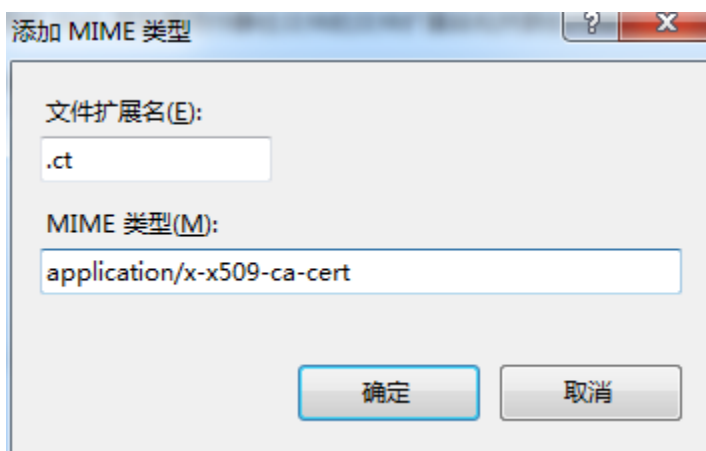
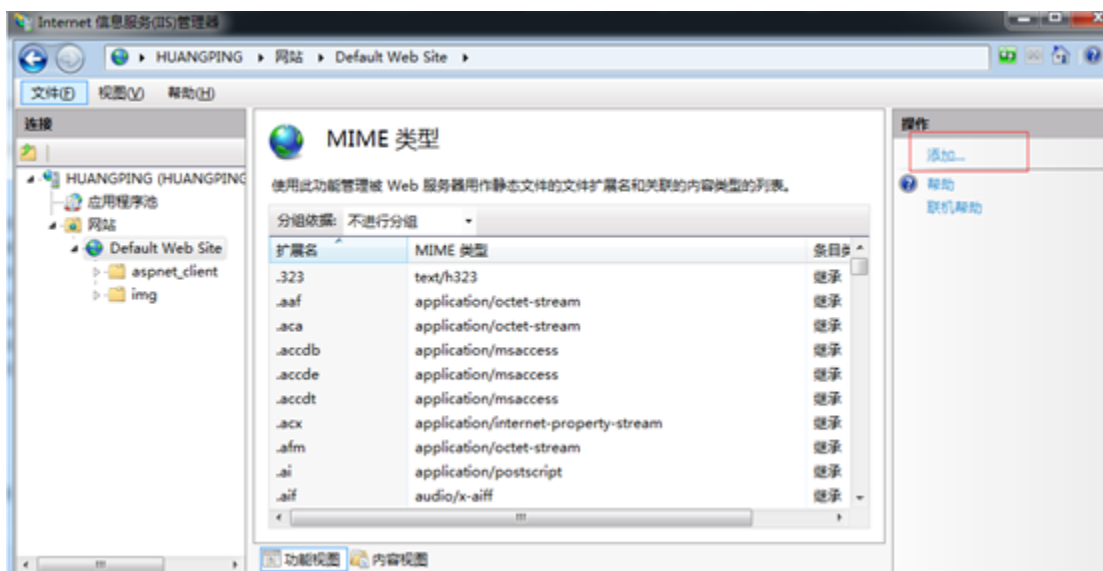
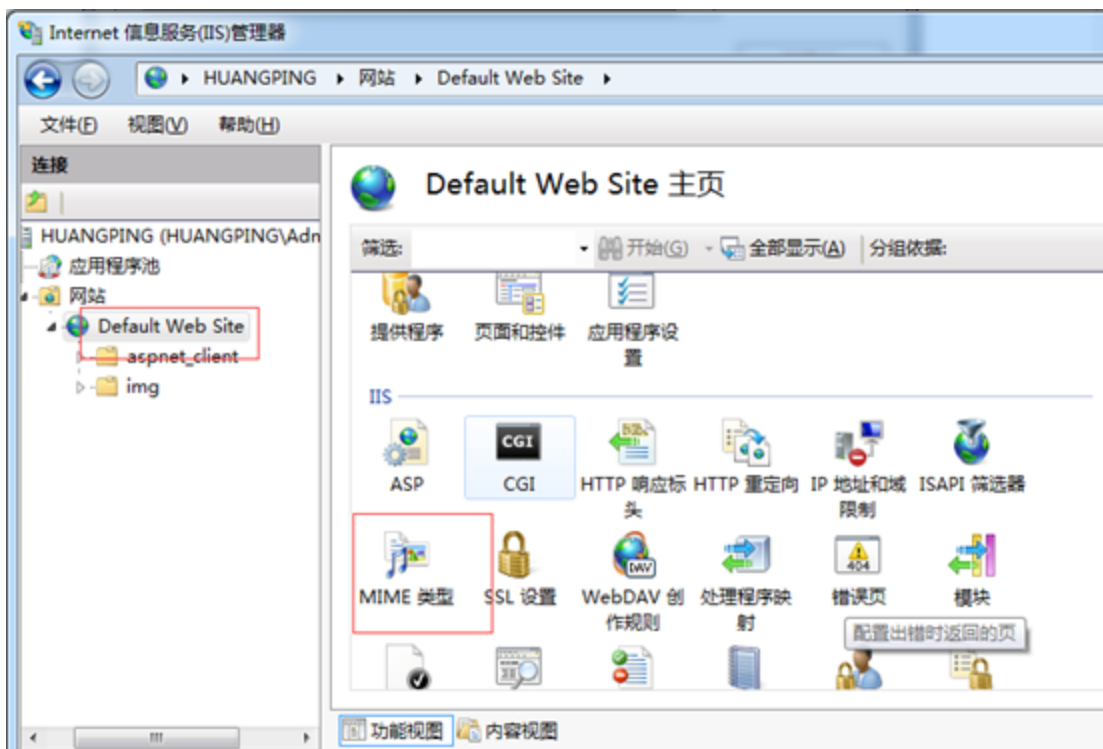
编辑(E)...

删除(R)

浏览(B)

关闭(C)

- 6、点击“MIME类型”，点击“添加”，添加新的MIME类型。
- | 扩展名              | MIME类型                     |
|------------------|----------------------------|
| .plist           | application/plist          |
| .ipa             | application/octet-stream   |
| .mobileprovision | application/octet-stream   |
| .ct              | application/x-x509-ca-cert |



7、将OPENSSL中生成的RootCA.cer修改名称为RootCA.ct放到iis目录下

8、将ipa文件放到iis目录下

9、将ipa.rar中的文件放到iis目录下。

文件名	扩展名	大小	日期时间
[.]	<DIR>		2015/04/17 15
[aspnet_client]	<DIR>		2015/04/17 10
[img]	<DIR>		2015/04/17 14
app_for_iOS	ipa	14.8 MB	2015/03/24 15
app_https	plist	1.1 KB	2015/04/17 14
iisstart	htm	689 B	2015/04/17 10
index	htm	672 B	2015/04/17 15
logo_144	png	18.7 KB	2013/11/08 17
RootCer	ct	1.6 KB	2015/04/17 14
web	config	502 B	2015/04/17 15
welcome	png	180.6 KB	2015/04/17 10

修改index.html和app\_https.plist文件中的服务器地址

```
</head>
<body>
  <ul class = "download-ul">
    <li>
      <a href = "http://192.168.1.58/RootCer.ct">
        <span class = "btn-text">安装证书</span>
      </a>
    </li>
  </ul>
  <ul class = "download-ul">
    <li>
      <a id = "downloadIOSText" href = "itms-services://?action=download-manifest&url=https://192.168.1.58/app_https.plist">
        <span class = "btn-text">下载APP安装</span>
      </a>
    </li>
  </ul>
</body>
```

```
1 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1
2 <plist version="1.0">
3 <dict>
4   <key>items</key>
5   <array>
6     <dict>
7       <key>assets</key>
8       <array>
9         <dict>
10          <key>kind</key>
11          <string>software-package</string>
12          <key>url</key>
13          <string>https://192.168.1.58/app_for_iOS.ipa</string>
14        </dict>
15        <dict>
16          <key>kind</key>
17          <string>display-image</string>
18          <key>url</key>
19          <string>http://192.168.1.58/logo_144.png</string>
20        </dict>
21      </array>
22      <key>metadata</key>
23      <dict>
24        <key>bundle-identifier</key>
25        <string>cn.com.smartbi.SpreadsheetReport</string>
26        <key>bundle-version</key>
```

10、将根证书RootCA.cer发送到移动端，下载安装。（若移动端设置有锁屏密码，安装时需要输入锁屏密码）

## 部署完成后的问题诊断

1. 在手机上无法访问到安装页面  
请检查应用服务器和手机是否在同一个网络环境，并且对应端口没有被防火墙阻止。
2. 安装证书后，点击页面上的链接，提示无法链接服务器  
请确认根证书和app下载链接的IP或域名是一致的，并且已经替换掉app.war/RootCer.cer。

## 升级Tomcat

升级Tomcat的方法如下：

### 1、停止服务

关闭smartbi的cmd窗口或在windows的服务中停止smartbi的服务。

### 2、修改现有的Tomcat目录

进入安装目录，把Tomcat改名为Tomcat\_back

### 3、复制新的Tomcat

复制新版本Tomcat到安装目录

软件 (D:) > Smartbi_Insight >				
名称	修改日期	类型	大小	
Infobright	2018/10/14 13:53	文件夹		
jdk	2018/10/14 13:52	文件夹		
MySQL	2018/10/14 13:52	文件夹		
SmartbiUnionServer	2018/10/14 13:53	文件夹		
smartbixmla	2018/10/14 13:51	文件夹		
Tomcat	2018/11/7 16:18	文件夹		
Tomcat_back	2018/11/6 15:00	文件夹		
Configuration.ico	2011/12/20 9:51	图标	8 KB	
Configuration	2014/3/6 11:08	Internet 快捷方式	1 KB	
Dashboard.ico	2018/3/6 13:52	图标	162 KB	
help.ico	2015/11/20 18:18	图标	164 KB	
online	2016/8/4 9:19	Internet 快捷方式	1 KB	
readme.txt	2013/12/26 17:45	文本文档	1 KB	
setting.ico	2015/11/20 18:18	图标	165 KB	
SmartbiInstall.log	2018/10/14 13:53	文本文档	1 KB	
start.ico	2015/11/20 18:18	图标	162 KB	
stop.ico	2015/11/20 18:18	图标	161 KB	
unSmartBI.ico	2015/11/20 18:18	图标	161 KB	
Web Intelligence.ico	2018/3/6 13:52	图标	162 KB	
Web Intelligence	2014/3/6 11:08	Internet 快捷方式	1 KB	

#### 4、迁移smartbi配置

如下图所示，复制Tomcat\_back/bin目录下的红色方框内文件到Tomcat/bin目录下

名称	修改日期	类型	大小
fonts.zip	2014/2/20 18:59	360压缩 ZIP 文件	1,212 KB
install_smartbi_service.cmd	2018/5/31 15:22	Windows 命令脚本	1 KB
log4j.properties	2007/3/28 15:43	PROPERTIES 文件	1 KB
log4j-1.2.13.jar	2007/4/20 14:46	Executable Jar File	350 KB
msvcr110.dll	2012/11/6 1:20	应用程序扩展	855 KB
ProcessList.exe	2014/11/28 11:00	应用程序	9 KB
service.bat	2016/11/29 14:56	Windows 批处理	7 KB
smartbi.properties	2018/10/25 16:47	PROPERTIES 文件	1 KB
smartbi-config.xml	2018/11/6 14:59	XML 文档	3 KB
Smartbi-license.xml	2018/8/3 17:01	XML 文档	30 KB
startup.cmd	2016/12/2 9:58	Windows 命令脚本	2 KB
stop.cmd	2015/10/10 11:25	Windows 命令脚本	1 KB
tcnative-1.dll	2012/12/4 8:54	应用程序扩展	1,536 KB
ThreadDump.cmd	2016/8/31 10:11	Windows 命令脚本	1 KB
ThreadDump.jar	2016/8/30 17:32	Executable Jar File	3 KB
ThreadDump.sh	2016/1/25 15:13	Shell Script	1 KB
tomcat7.exe	2012/12/4 8:54	应用程序	98 KB
tomcat7w.exe	2013/6/9 11:31	应用程序	128 KB
tt.csv	2010/3/24 14:37	XLS 工作表	1 KB
uninstall_smartbi_service.cmd	2018/5/31 15:21	Windows 命令脚本	1 KB
unzipfont.bat	2015/4/14 10:57	Windows 批处理	1 KB

注意：windows版本安装包，可能还需要复制tcnative-1.dll替换原来自带的tcnative-1.dll。

如果使用的https加密协议，还需要把对应的证书文件复制到Tomcat/bin目录下。

## 5、迁移扩展包

如下图所示，复制Tomcat\_back/bin/ext目录下的所有ext文件到Tomcat/bin/ext目录下

软件 (D:) > Smartbi_Insight > Tomcat_back > bin > ext			
名称	修改日期	类型	大小
demo.ext	2018/7/30 15:36	360压缩	48,530 KB
pictureplayer.ext	2014/3/6 22:10	360压缩	138 KB
smartbiradar.ext	2012/12/25 11:03	360压缩	87 KB
SpreadsheetAuditingProcess.ext	2016/8/3 10:30	360压缩	34 KB

## 6、迁移动态链接库

复制Tomcat\_back/bin/dynamicLibraryPath的所有文件到Tomcat/bin/dynamicLibraryPath目录下

如果Tomcat\_back/bin/dynamicLibraryPath目录为空，则忽略这个步骤

## 7、迁移smartbi的备份文件

复制Tomcat\_back/bin/smartbi\_repoBackup的所有文件到Tomcat/bin/smartbi\_repoBackup目录下

## 8、迁移smartbi的war包

复制Tomcat\_back/webapps目录下所有文件到Tomcat/webapps目录下