移动端升级扩展包使用手册

移动端升级扩展包 MobileUpdate 主要的作用是方便用户对 Smartbi 移动端程序的安装与升级，使得用户可以直接访问产品部署的服务器就能进行上述操作。

文档目录：

1、使用场景

移动端升级扩展包 MobileUpdate 主要提供给两类用户使用，一种是客户的移动设备只能访问内部网络，另一种是客户的移动端版本是经过定制化的。

2、扩展包部署

扩展包的名称为 MobileUpdate.ext，可以从这里下载，或者从思迈特处获取该扩展包的最新版。然后参照“扩展包部署”文档，部署到服务器后重启服务器即可使用。成功部署后可以在“**用户名-》系统监控-》扩展包**”页面上看到类似下面的记录。

加载顺序	名称	别名	描述	版本	加载路径	原始路径	打包日期	优先级
1	ipadextension	MobileExtension	移动设备扩展包,支持IPAD,IPHONE与安卓设备	2.0	C:/Smartbi/Tomcat/temp/smartbiExtension6025843299973342765.tmp	C:/Smartbi/Tomcat/webapps/smartbi/WEB-INF/extensions/ipad.ext	2014-09-02 09:57:23	20
2	webmoblie	移动端WEB版	主要用于 android phone	1.0	C:/Smartbi/Tomcat/temp/smartbiExtension3731251898160212915.tmp	C:/Smartbi/Tomcat/webapps/smartbi/WEB-INF/extensions/WEB_moblie.ext	2014-09-02 09:57:26	40
3	smartbiradar	SmartbiRadar	雷达图	1.0	C:/Smartbi/Tomcat/temp/smartbiExtension7891286421637544952.tmp	C:/Smartbi/Tomcat/bin/ext/smartbiradar.ext	2012-12-25 11:03:26	100
4	pictureplayer	PicturePlayer	图片播放器	1.0	C:/Smartbi/Tomcat/temp/smartbiExtension7805308463239099880.tmp	C:/Smartbi/Tomcat/bin/ext/pictureplayer.ext	2014-03-06 14:10:42	100
5	mobileupdate	移动版本发布包	用于移动版本的安装与升级	1.0	C:/Smartbi/Tomcat/temp/smartbiExtension6810580993207639453.tmp	C:/Smartbi/Tomcat/bin/ext/MobileUpdate.ext	2014-09-09 11:45:00	100
6	demo	Demo	Demo	1.0	C:/Smartbi/Tomcat/temp/smartbiExtension9108630134214663081.tmp	C:/Smartbi/Tomcat/bin/ext/demo.ext		100

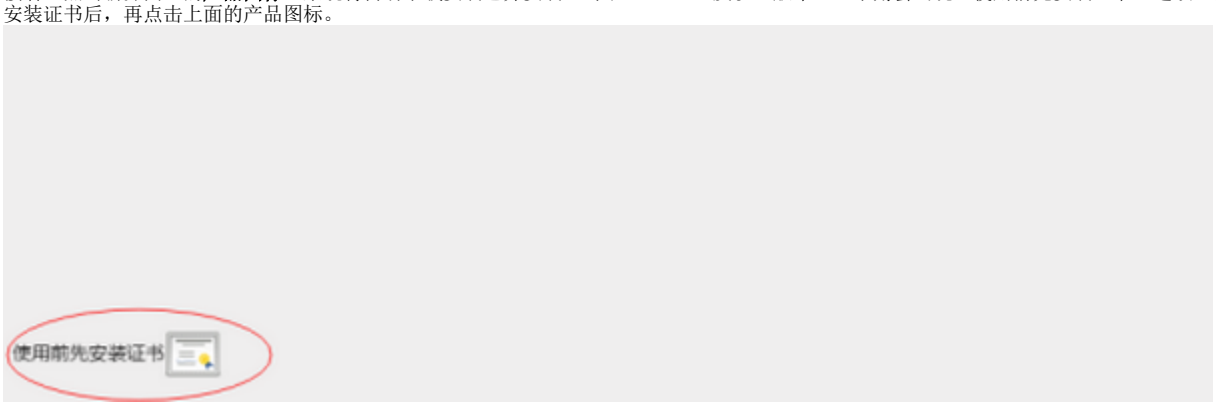
3、操作步骤

下面以 IOS 系统为例介绍操作步骤，安卓系统 Android 类同。

3.1 首次安装

在 iPad/iPhone 设备上用系统自带的 Safari 浏览器访问如下安装链接，比如：http://192.168.1.109:18080/smartbi/app.htm，将出现如下所示界面。点击其中 iOS 操作系统对应的 Smartbi Mobile 安装地址。

接着，点击新界面上的**产品图标**，系统将自动下载安装包并安装。对于 IOS 7.1 及以上版本，左下角会出现“使用前先安装证书”选项。需要先点击它安装证书后，再点击上面的产品图标。



在安装产品前需要先点击安装好证书（只需要安装一次）。关于证书的生成及部署的进一步说明请参考附录。

3.2 版本升级

当移动版app 需要升级的时候，系统管理员首先要用新的 ipa 包替换掉扩展包中 MobileUpdate.ext\vision\package\Smartbi_Small.ipa 文件。然后再修改 MobileUpdate.ext\vision\updateiosinfo.txt 文件，文件共两行，如下红色字体。

2014-04-02 10:00:00
IOS 2.3 版本升级

第一行填入新的IPA程序的打包时间，第二行填入升级的原因。完成上述动作后，当用户使用移动端进行登录时，就会看到版本升级的提示，点击“确认”后就会自动转入安装链接界面，点击图标后，自动执行升级。

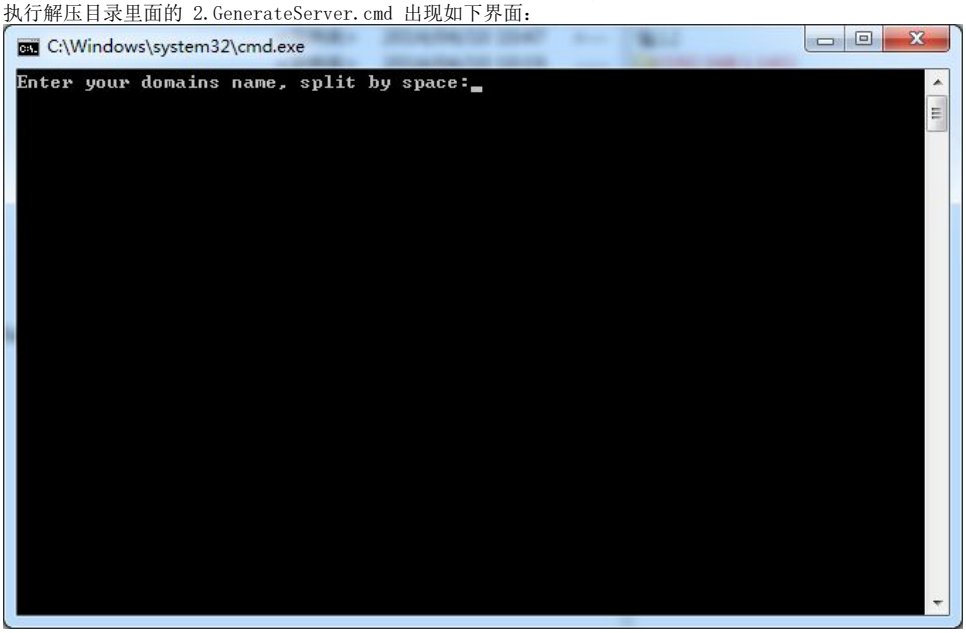
4、附录

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。

4.1 附录1：SSL证书生成

强烈建议用户使用自己的证书或者由专业 CA 生成的证书，若没有，可以使用下载文档中的 "OpenSSL证书工具.zip"来自己生成证书。

- 下载并解压 OpenSSL 工具包。　　下载链接：　OpenSSL.zip
- 执行解压目录里面的 1.GenerateRootCA.cmd 生成根证
- 将 RootCA目录里面的 RootCA.cer放入扩展包的vision目录替换原来的RootCA.cer。
- 执行解压目录里面的 2.GenerateServer.cmd 出现如下界面：



这时候需要填入应用服务器的IP或者域名（使用IP还是域名由移动端设置时填入的服务器地址决定，即苹果设备下载移动端访问的地址要与SSL证书颁发的地址保持一致），多个域名与
IP之间使用空格分开。

- 上一步成功执行后，将产生一个对应IP或者域名的目录，将.pfx、.pem和.cer文件拷入应用服务器的bin目录，
这个文件就是服务器需要使用证书了。
- 参考下面的附录进行服务端的证书部署。

4.2 附录2：Tomcat服务器证书部署

1、进入 Tomcat 服务器安装目录的　conf 子目录下，编辑 server.xml 文件。

2、在server.xml中找到以下信息并将注释放开。

server.xml

```
73      <!-- A "Connector" using the shared thread pool-->
74      <!--
75      <Connector executor="tomcatThreadPool"
76                 port="8080" protocol="HTTP/1.1"
77                 connectionTimeout="20000"
78                 redirectPort="8443" />
79      -->
80      <!-- Define a SSL HTTP/1.1 Connector on port 8443
81           This connector uses the JSSE configuration, when using APR, the
82           connector should be using the OpenSSL style configuration
83           described in the APR documentation -->
84      <!--
85      <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
86                 maxThreads="150" scheme="https" secure="true"
87                 clientAuth="false" sslProtocol="TLS" />
88      -->
89
90      <!-- Define an AJP 1.3 Connector on port 8009 -->
91      <Connector port="18081" protocol="AJP/1.3" redirectPort="18443" URIEncoding="UTF-8"/>
92
```

找到这段代码，将注释放开

3、修改里面的SSL设置，因Tomcat不同这里可能存在有两种不同的配置方式。需要注意修改的就是端口号和证书路径。

配置方式一：修改里面的SSL设置，需要注意修改的就是端口号和证书路径。

```
<Connector port="8443" maxHttpHeaderSize="8192" SSLEnabled="true"
 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
 enableLookups="false" disableUploadTimeout="true"
 acceptCount="100" scheme="https" secure="true"
 clientAuth="false" sslProtocol="TLS"
 keystoreType="PKCS12"
 keystoreFile=" XXX\XXX\XXX.pfx"
 keystorePass="ServerPassword"
 />
```

注：如果使用上述配置启动时提示SSLCertificateFile或SSLCertificateKeyFile属性没有设置，则使用下述的格式

```
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
                          SSLCertificateFile="${catalina.base}/bin/XXX.cer"
                          SSLCertificateKeyFile="${catalina.base}/bin/XXX.pem"
                          SSLPassword="ServerPassword"/>
```

配置方式二：如果没有找到配置方式一的代码，直接采取此配置方式即可：

找到第2步骤中server.xml取消注释的这段代码，修改成如下信息，对应端口号信息和证书信息需要进行修改，证书的路径可以是相对路径也可以是绝对路径，如可以将证书放在Tomcat/bin目录下：

server.xml

```
73      <!-- A "Connector" using the shared thread pool-->
74      <!--
75      <Connector executor="tomcatThreadPool"
76                 port="8080" protocol="HTTP/1.1"
77                 connectionTimeout="20000"
78                 redirectPort="8443" />
79      -->
80      <!-- Define a SSL HTTP/1.1 Connector on port 8443
81           This connector uses the JSSE configuration, when using APR, the
82           connector should be using the OpenSSL style configuration
83           described in the APR documentation -->
84
85      <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
86                 maxThreads="150" scheme="https" secure="true"
87                 clientAuth="false" sslProtocol="TLS"
88                 SSLCertificateFile="${catalina.base}/bin/XXX.cer"
89                 SSLCertificateKeyFile="${catalina.base}/bin/XXX.pem"
90                 SSLPassword="ServerPassword"/>
91
```

证书和端口号信息需要根据实际环境进行更改

详细信息如下：

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS"
                      SSLCertificateFile="${catalina.base}/bin/XXX.cer"
                      SSLCertificateKeyFile="${catalina.base}/bin/XXX.pem"
                      SSLPassword="ServerPassword"/>
```

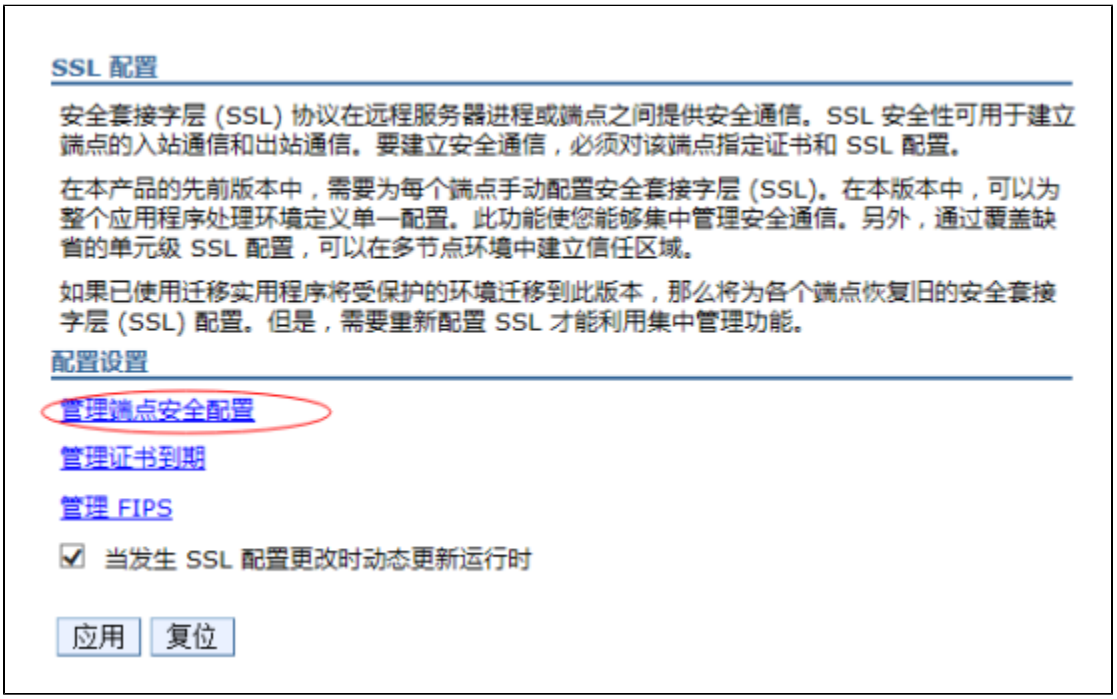
4、修改后，同时修改 MobileUpdate.ext 扩展包中的 META-INF/mobileupdate.properties 文件，把里面的端口号改为对应的端口号。

4.3 附录3：WebSphere服务器证书部署

以 WebSphere 8.5 应用服务器举例说明。

1、进入服务器管理页面，“安全性”——“SSL证书和密钥管理”。

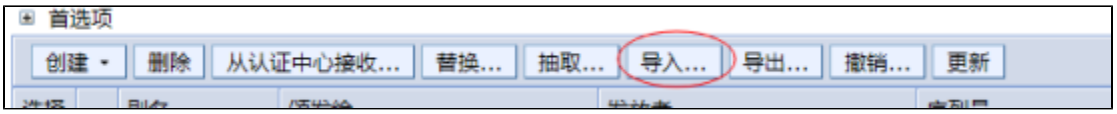
2、进入“管理端点安全配置”。



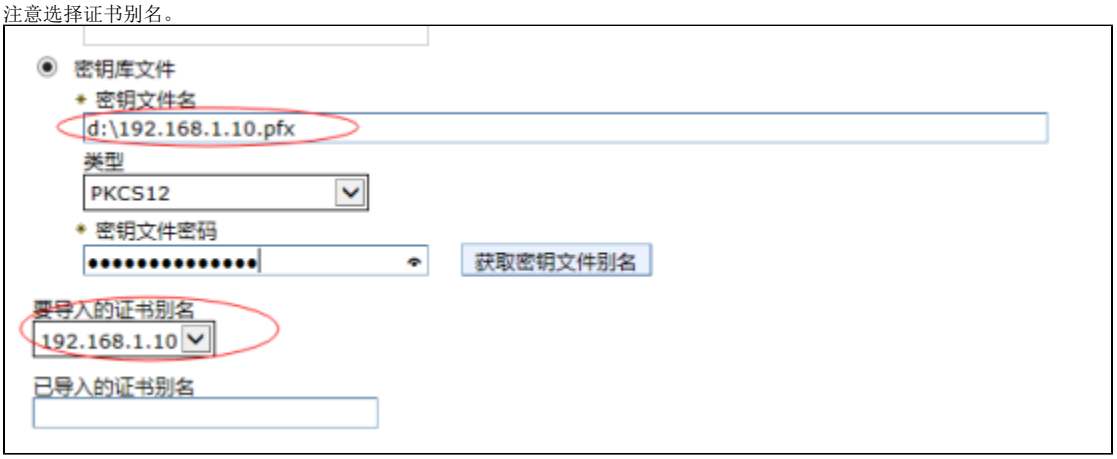
3、选择对应的服务器或集群的入站设置。

4、进入管理证书。

5、填写证书存放的路径，导入证书。



注意选择证书别名。



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