

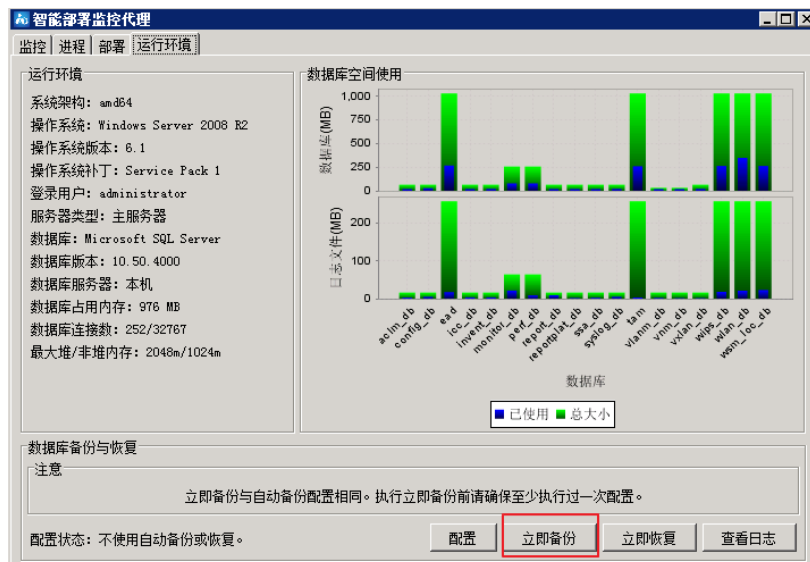
知 使用BYOD证书快速部署工具更新用户证书的典型配置

BYOD 罗孝晨 2016-08-04 发表

目前EIA版本在对于使用BYOD证书快速部署工具时的处理逻辑是：当用户执行证书自动部署时，会把证书序列号记录到数据库中，当用户后续再执行证书自动部署时，如果证书没有失效或吊销，则从CA上查询到该证书下发该终端。用户证书快到时期，可以直接执行一个SQL语句，这样当终端重新执行证书自动部署时都会重新申请新的证书。

无

1、删除数据库表中的证书申请记录。首先打开监控代理通过DBMAN备份数据库。



2、使用SA用户登录到EIA组件所部署的服务器上的数据库，执行如下SQL语句：

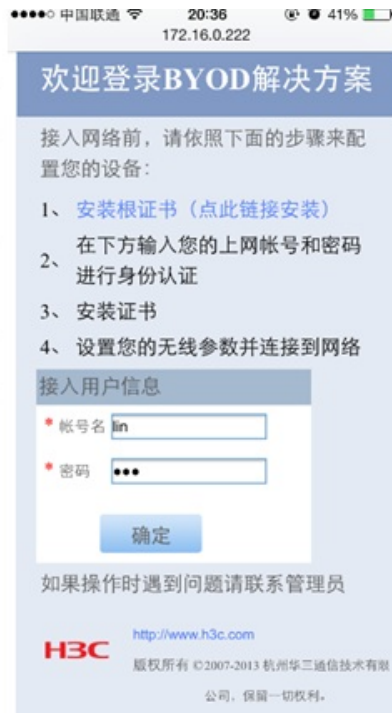
```
SQLQuery1. s... (sa (240))*
delete from ead.ead.TBL_BYOD_USER_CERT
GO
```

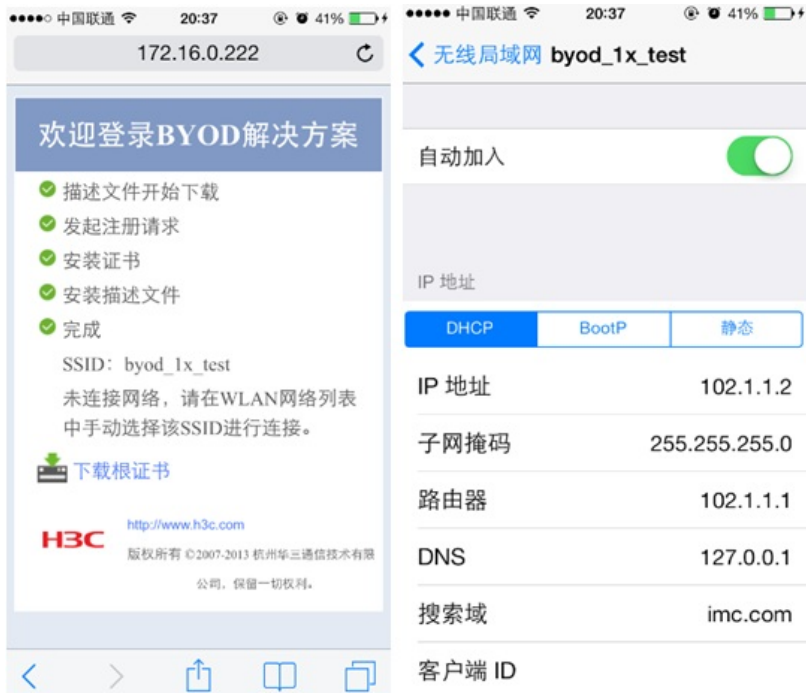
3、终端重新申请证书

(1) IOS终端配置：使用自带的浏览器打开<http://IP:Port/byod/deploy.jsf>。其中IP和Port分别为iMC服务器的IP地址和端口号。需要注意的是，打开<http://IP:Port/byod/deploy.jsf>有两种方式：用户手工在浏览器中输入<http://iMC-host/byod/deploy.jsf>。在接入设备的某个VLAN中启用Portal认证，然后在命令中将<http://iMC-host/byod/deploy.jsf>配置为Portal认证时需要推出的认证页面。用户使用浏览器访问任意网站时，都会自动打开该页面。

手机终端连接SSID，在浏览器中任意输入网址，页面被重定向至自动配置页面；然后点击安装根证书，进行证书安装，证书安装完成之后，在接入用户信息中输入用户名和密码，完成验证之后进行描述文件的安装。（具体操作步骤见截图）







(2) PC终端配置: PC终端连接SSID, 在浏览器中打开http://IP:Port/byod/deploy.jsf



点击页面中的“配置我的Windows设备”, 将会弹出“byoddeploytool”部署工具, 点击“保存”到指定目录后运行此工具 (或者直接点击“运行”)。



运行该工具, 填入对应的用户名、密码及证书私钥密码 (私钥密码为之前从服务器导出证书时的密码)。



填入信息之后点击确定，进行证书导入步骤



跳转到“证书导入向导”，点击下一步



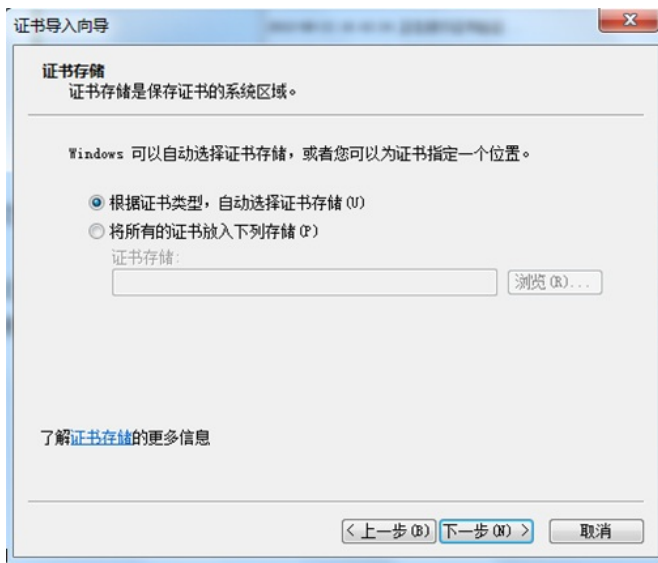
按照默认信息导入文件，点击下一步



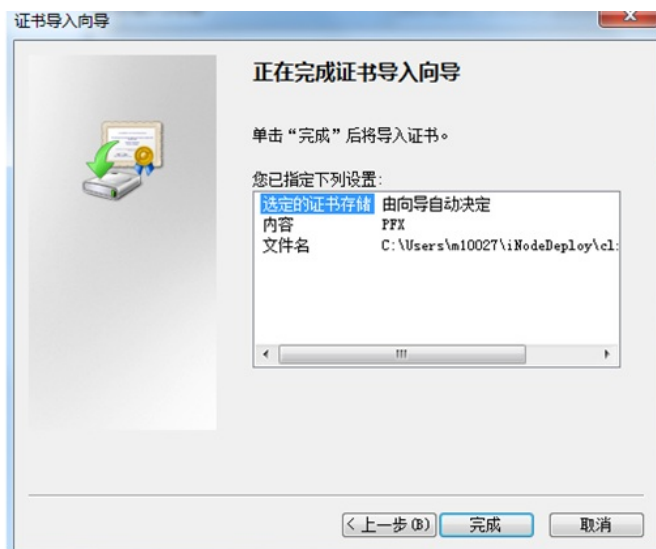
输入私钥密码（导出证书时的密码），点击下一步



选择证书存储位置，点击下一步




到此，完成证书导入



(3) Android平台快速部署流程：使用Android自带的浏览器打开<http://IP:Port/byod/deploy.jsf>

欢迎登录BYOD解决方案

为了更安全的接入网络，网络要求您的系统进行一些设置。
另外，您还需要进行有效的验证，例如账号密码。
接下来，点击下面的按钮进行设置吧。

 [配置我的android设备](#)

点击“配置我的Android设备”链接，下载并根据提示安装快速部署客户端软件。打开快速部署客户端软件，输入用户名、密码，点击“确定”即可开始自动部署。配置完成后，如果下发了Wi-Fi配置，Android会自动切换至下发的Wi-Fi网络。

- 1、删除用户证书之前确保进行数据库备份工作。
- 2、iMC服务器证书有效期由申请证书的时间和CA服务器证书配置的有效期决定（这个有效期在安装CA时指定，后期修改可能会导致问题，具体可以参考KMS案例《用户更改证书服务模板有效期后使用BYOD快速部署工具时无法申请用户证书的处理办法》）
- 3、客户端的证书有效期由客户端申请证书的时间和CA服务器上证书配置的有效期决定，客户端证书到期后，不能自动续订，必须重新进行一次证书部署流程。该案例主要针对证书快要到期时重新申请新的用户证书。