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。用户证书快到期时,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:



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<u>http://IP:Port//byod/deploy.jsf</u>有两种方式:用户手工在 浏览器中输入<u>http://iMC-host/byod/deploy.jsf</u>。在接入设备的某个VLAN中启用Portal认证,然后在命令 行中将<u>http://iMC-host/byod/deploy.jsf配置为Portal</u>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)





••••• 中国联通 夺 20:37 ⑧ 🖲 41% 🌅 🕯	••••• 中国联通 令	20:37	• 41% • + • •
172.16.0.222 C	〈 无线局域网	byod_1x_te	est
- 赤畑発見DVのD知りた安			
从迎豆求BYOD胜伏万条	自动加入		
◎ 描述文件开始下载			
❷ 发起注册请求			
❷ 安装证书	ID that		
❷ 安装描述文件	IP JULI		
◎ 完成	DHCP	BootP	静态
SSID: byod_1x_test	ID thit		102112
未连接网络,请在WLAN网络列表	IF JUJI		102.1.1.2
中手动选择该SSID进行连接。	子网掩码	2	55.255.255.0
🔤 下载根证书	아슈 슈 요요		
http://www.h3c.com	珀田 器		102.1.1.1
H3C 版权所有 © 2007-2013 杭州华三通信技术有限	DNS		127.0.0.1
	搜索域		imc.com
< > ① ① ⑦	客户端 ID		

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



欢迎登录BYOD解决方	ī案
HBC Intelligent Management	t Center
BYOD解決方面为用户提供一种输入网络的方式。这种方式为每个用户建立了一个考置通 通。 提强规定。所有在这个网络中被创建、传输、处理、以及存抽的信息和数据(包括个人信 图)。都会在一定范围内按到建设、年程和反通。 未经授权使用实盘用网络可能会导致严重后常。如雇用或会约关系统止。严重的可能还要来 银恒位的民事实则事责任。	AL网络之前,重要对应的铁嘴语行一些安全社鼓器。 主此过程中,可能需要验证您的上网络号和密码。 ち由下方您的铁嘴所使用的操作系统开始就置。

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")。

怎想运行	或保存此	文件吗?
	名称: 类型: 来源:	byoddeploytool.exe 应用程序 172.16.0.222 运行 (8) 保存 (S) 即消
	el Inter	net 的文件可能对您有所帮助,但此文件类型可计算机。如果您不信任其来源,请不要运行或付

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)。

🔅 配置我的Wind	dows设备 🗆 🗆 🔀
50	
用户名:	ma
密码:	•••
证书私钥密码:	•••••
确认私钥密码:	•••••
注:设置的证书私 的私钥密码。	、钥密码即为证书安装向导页面中 确定

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

	次迎使用证书导入向导 这个向导帮助您将证书、证书信任列表和证书吊销列 表从磁盘复制到证书存储。
	用某保护新提迟建立步至均落连接的信息。"证书存储 是保存证书的系统区域。 单击"下一步"继续。
	(上一歩 (8)) 下一步 (8) > 取消

按照默认信息导入文件,点击下一步

要导入的文件 指定要导入的文件。		
文件名(F):		
C:\Users\m10027\iNodeDeploy\	clientCert.p12 浏览(R)
注意:用下列格式可以在一个文件	牛中存储一个以上证书:	
个人信息交换- PKCS #12 (.P	FX, . P12)	
加密消息语法标准- PKCS #7	证书(. P7B)	
Microsoft 序列化证书存储(:	SST)	
了解证书文件格式的详细信息		
		The State

输入私钥密码(导出证书时的密码),点击下一步

书导入向:	7
为了	保证安全,已用密码保护私钥。
为私	钥键入密码。
Cê1	码(0):
l	
E]启用强私钥保护。如果启用这个选项,每次应用程序使用私钥时,您都会 得到提示 (2)。]标志此密钥为可导出的密钥。这将允许您在稍后备份或传输密钥 (0)。
	〗包括所有扩展属性 ⑷。
了解保护	紙钿的更多信息
	< 上一步 (B)) 下一步 (B) > 取消

选择证书存储位置,点击下一步

动选择证书存储(U)
下列存储(2)
[浏览 (R)

到此,完成证书导入

	正在完成证书导入向导
Ş	单击"完成"后将导入证书。 您已指定下列设置: <mark>透完的证书存储</mark> 由向导自动决定 内容 FFX 文件名 C:\Vsers\m10027\iNodeDeploy\cl:
	< +

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



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。