免费 FortiToken Mobile 在 FortiGate 绑定时遇到的问题及处理方法

版本	1.0
时间	2023 年 12 月
支持的版本	FortiOS v6.0.x, 6.2.x, v6.4.x, v7.0.x, v7.2.x
作者	张彦龙
状态	已审核
反馈	support_cn@fortinet.com

目录

一. 描述

FortiToken Mobile 只需通过在手机上安装 FortiToken 动态令牌软件，根据系统时间和令牌种子等来生成一次性口令。用户在正确输入账号和密码后，会被提示再次输入一次性口令即可完成动态口令二次认证。默认情况下，每台 FortiGate 都自带两个免费的 FortiToken Mobile license。如果需要更多数量的 FortiToken，则需要向厂家销售申请单独购买。

本例仅针对防火墙自带的两个免费 FortiToken 在配置使用过程中遇到的问题及处理方法做说明。

二. 组件

FortiGate-VM64 v6.4.8,build1914,211117 (GA)

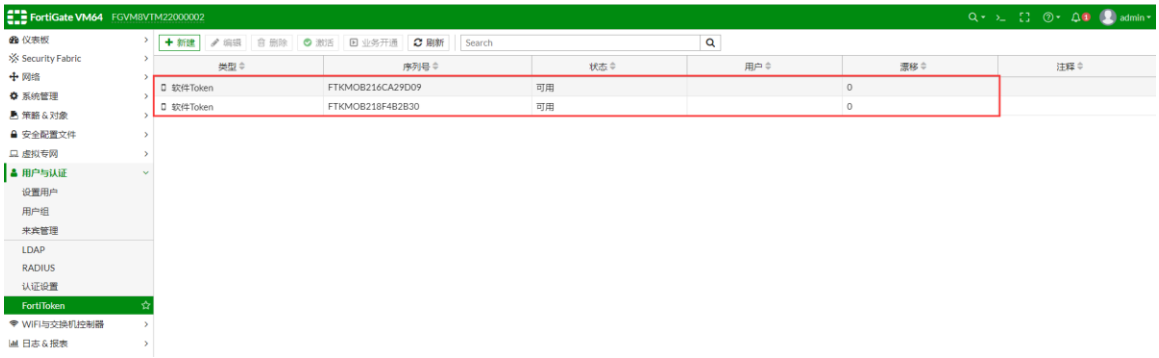
FortiToken Mobile : v5.4.2.0117

手机终端版：IphoneX 15.3.1

三. 配置

3.1. 查看免费的 FortiToken

菜单“用户与认证---FortiToken”可以看到两个免费软 Token 且状态显示为“可用”



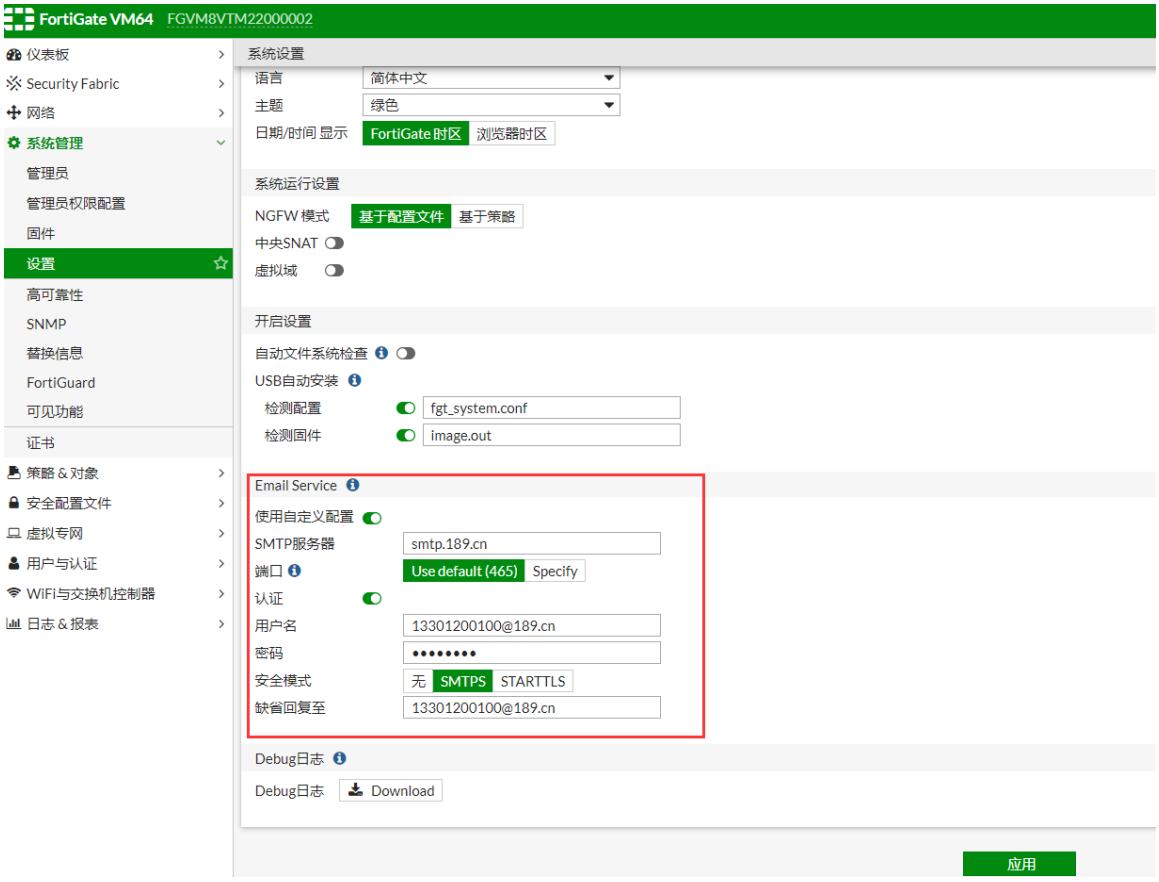
3.2. 定义发件邮件服务

防火墙将通过自定义的邮件服务器来给用户邮箱发送 Token 码激活邮件。

SMTP 服务器：配置发件邮件服务器地址。

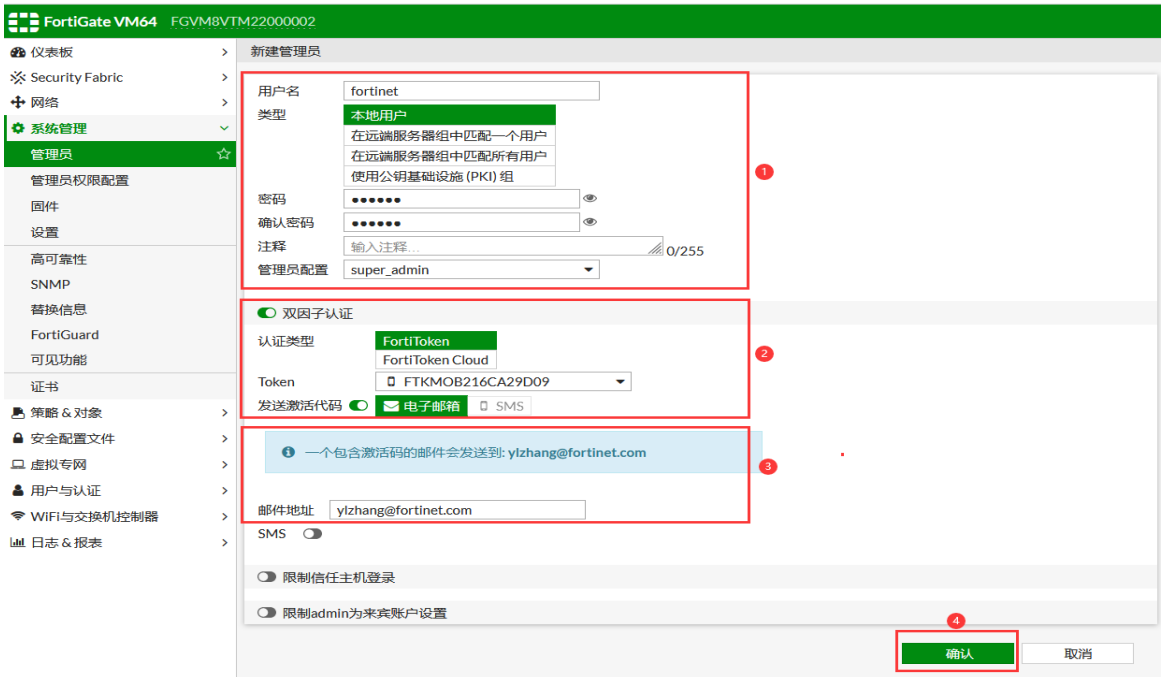
启用认证：然后配置邮箱的用户名密码

缺省回复至：配置以 13301200100@189.cn 为发件源邮箱地址



3.3. 创建管理员用户并绑定 Fortitoken

管理员用户可以是本地用户也可以是通过 LDAP, RADIUS, TACACS+的远程认证用户，下面以本地管理员为例:



新建管理员： 填写用户名及密码，设置管理 profile

启用双因子认证： 在此处选择一个未分配的 token 给新创建的管理员用户。

填写邮件地址： 用户的邮箱地址，需要准确填写，可用于接收 token 的激活码。

点击“确认” 后，此时双因子配置完成，可以看到新建的 fortinet 用户绑定的双因子序列号信息

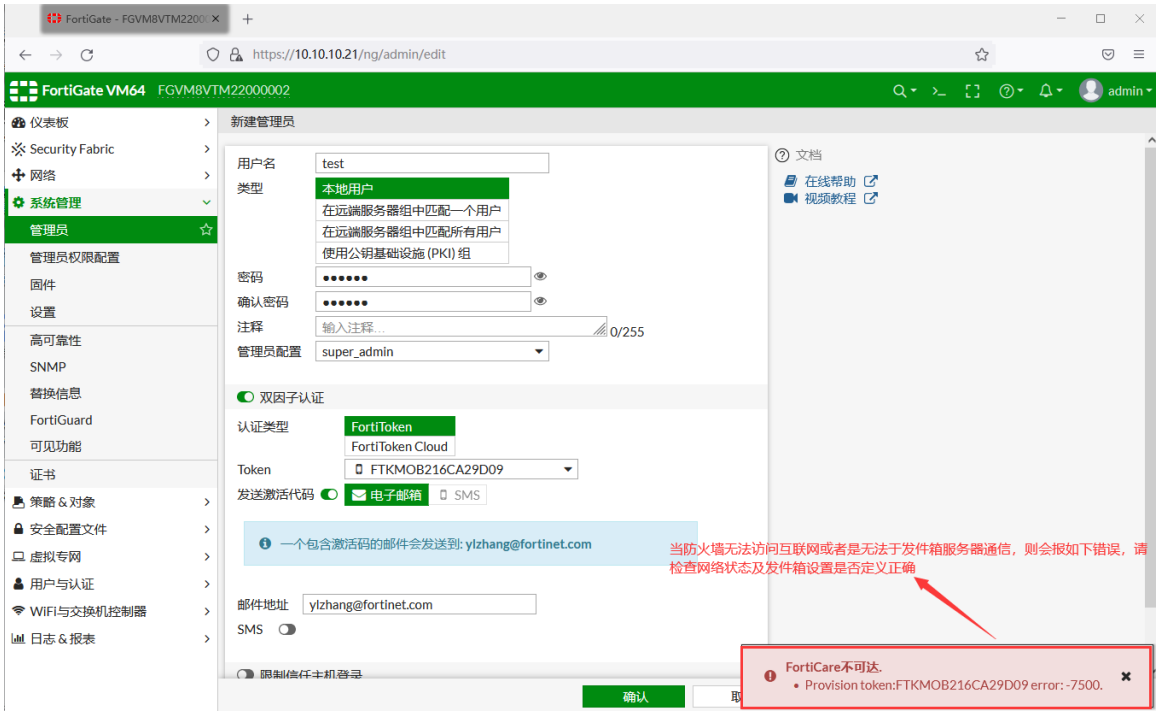
3.4. 绑定 FortiToken 故障现象一

故障现象：

当启用双因子并配置完成点击“确认”报如下图所示错误“FortiCare 不可达”时，如何解决？

解决方案：

由于启用并绑定双因子认证时，防火墙要连接到 Fortiguard 校验 token 状态，因此防火墙必须可以于 Internet 及与自定义的邮件服务器通信正常，否则点击“确认”会报以下错误且无法保存。



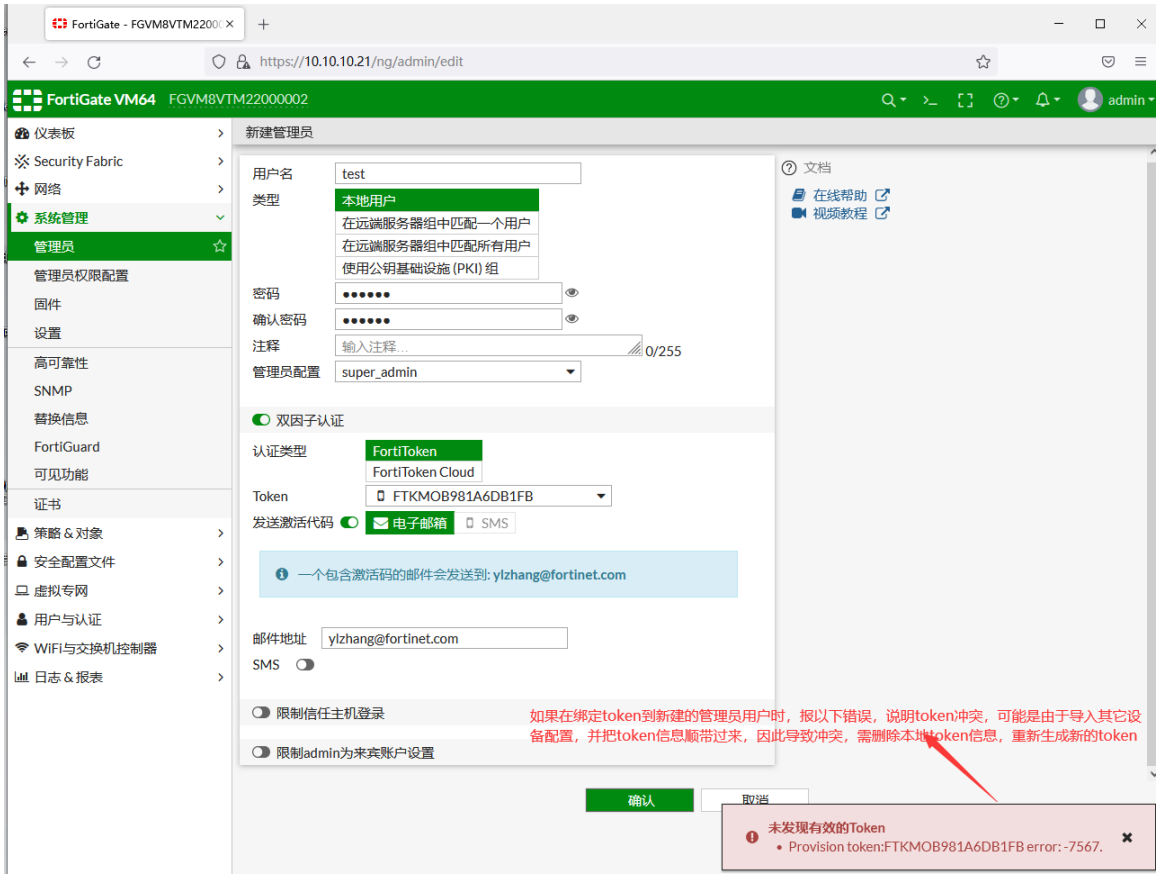
3.5. 绑定 FortiToken 故障现象二

故障现象：

当启用双因子并配置完成点击“确认”会报如下图所示错误“未发现有效的 Token”时，如何解决？

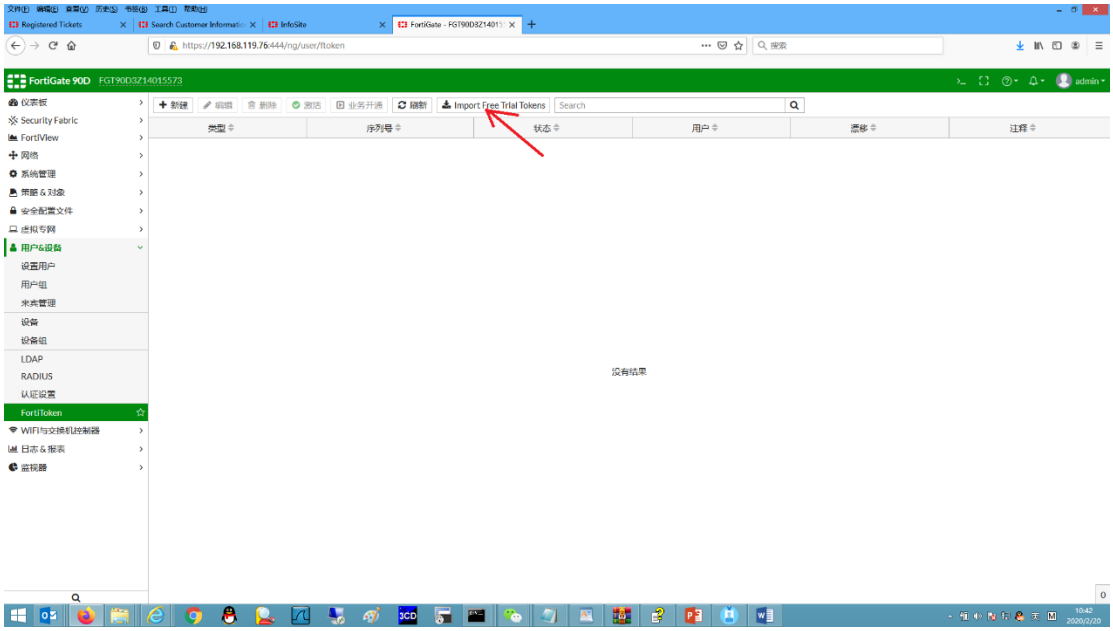
解决方案：

说明存在 Fortitoken 冲突，出现这种情况可能是导入其它设备备份的配置文件所携带 Fortitoken 与原设备冲突所致，因此需删除现有的 token，重新生成新的免费 token。参考 3.6 如何生成新的免费 token



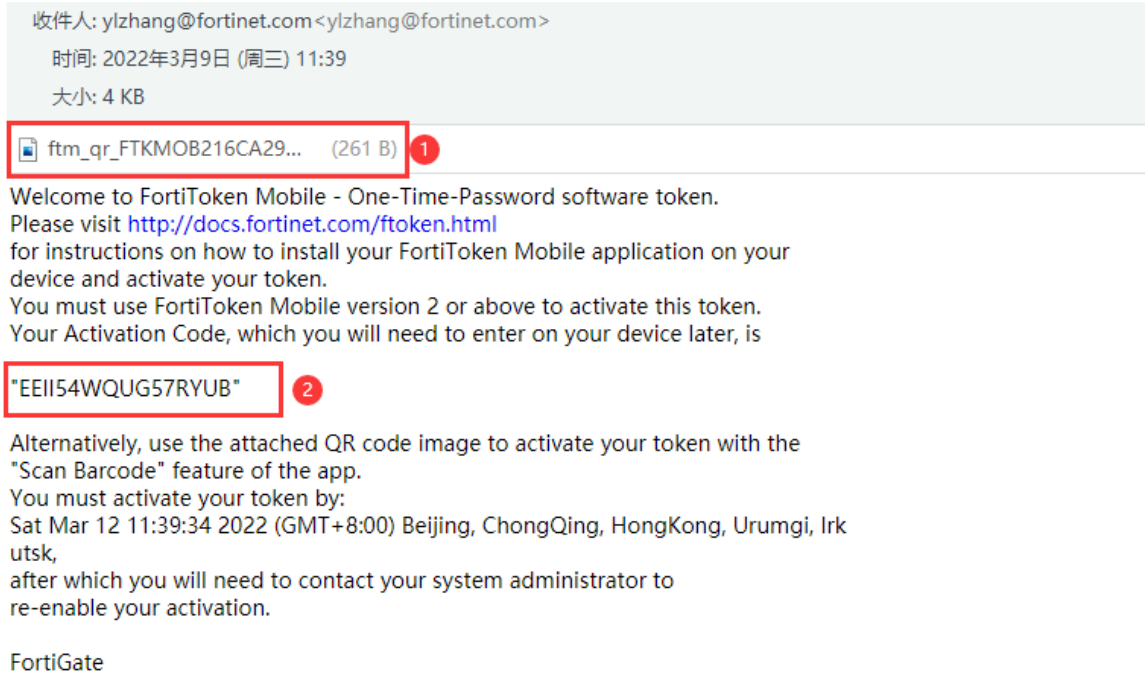
3.6. 如何生成新的免费 token

“用户&设备”----“FortiToken”管理界面，删除现有所有的 Token（注意先取消或删除调用此 FortiToken 序列号的配置），然后单击“Import Free Trial Tokens”按钮，重新导入生成新的免费试用 Token。



3.7. 邮箱将收到一封 token 激活邮件

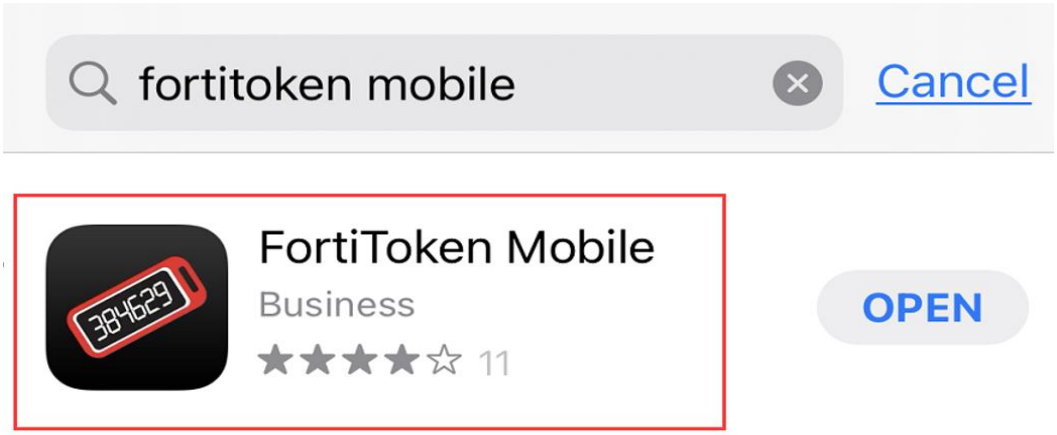
收到的激活邮件附带一个包含激活二维码的图片及收到输入的激活码，内容如下，红色标注部分分别为二维码图片和激活码，手机通过扫描二维码或者手动填写激活码来完成绑定。



3.8. Iphone 手机安装 FortiToken

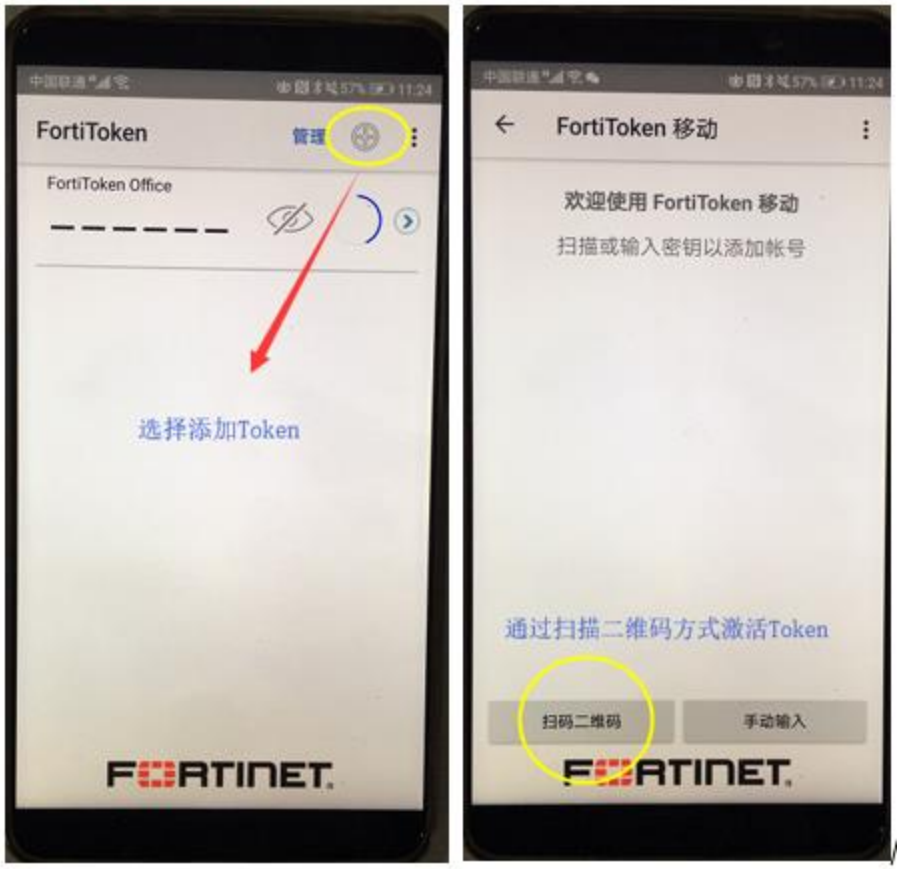
用户手机下载并安装 FortiToken Mobile 应用。iOS 可以从 App store 中下载。Andriod 因为 Google 市场无法访问，需要时可以找 Fortinet 工程师索取。

以 iphone 手机为例，在 App store 搜索 fortitoken mobile 并安装。



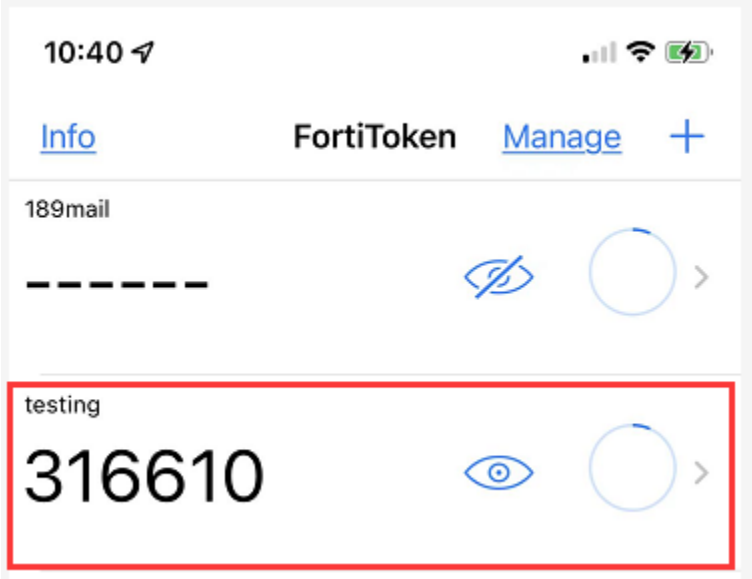
3.9. 绑定 FortiToken 激活码

打开应用的界面如下，如图，有两种方式输入用户的激活码：扫描二维码或手动输入。二维码或手动输入的激活码都在用户接收的邮件中。扫描邮件内的二维码或手动输入激活码后，即可激活。



3.10. 查看激活码

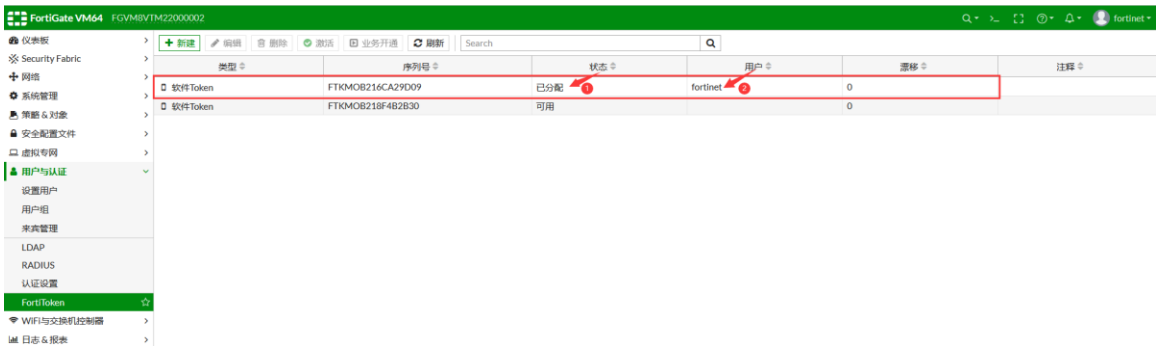
打开 FortiToken Mobile APP 后，屏幕上即可启动 6 数字的动态口令码且每 60 秒更新一次动态密码，这样就可以实现将本地管理员账号+双因子 Token 应用到设备管理中。



3.11. 查看 token 分配的状态

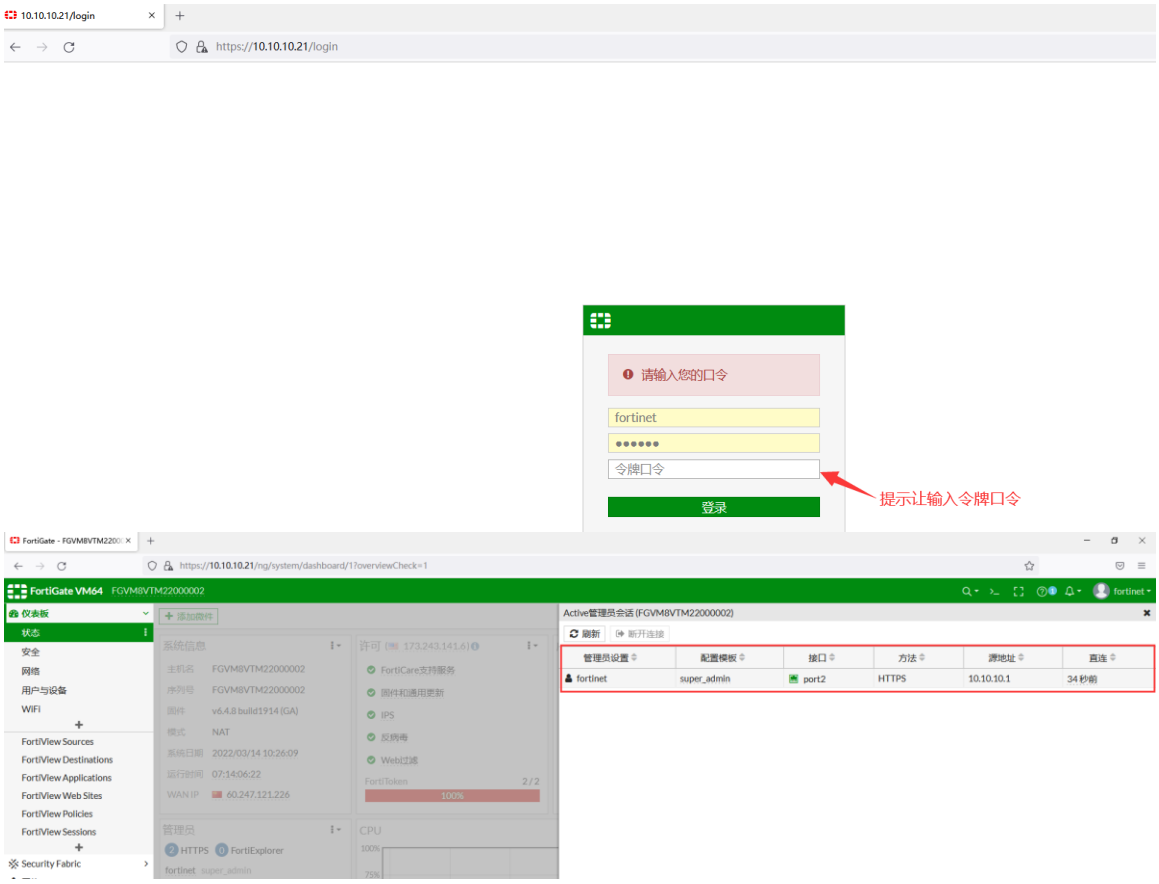
当手机 token 完成绑定后，在菜单“用户与认证---FortiToken”可以看到其中一个 Token 状态显

示“已分配”，且分配用户为 fortinet



四. 测试

登录 FortiGate GUI，输入用户名及密码后，弹出输入双因子口令，输入 token 口令后即可完成双因子登录。



五. 补充内容

- 每个令牌只能在一台 FortiGate 设备上使用；
- 每个令牌只能绑定一个用户；

- 可以将令牌从用户上解除绑定，每次绑定用户均需要再次激活。
- HA 模式下只可以使用 2 个免费试用软件 FortiToken。

六. 参考文档资料

FortiClient 下载：

https://handbook.fortinet.com.cn/VPN%E6%8A%80%E6%9C%AF/FortiClient_VPN/FortiClient%E4%B8%8B%E8%BD%BD.html

FortiToken Mobile APP 下载：

https://handbook.fortinet.com.cn/%E7%94%A8%E6%88%B7%E4%B8%8E%E8%AE%A4%E8%AF%81/FortiToken%E8%AE%A4%E8%AF%81/FortiToken_Mobile_APP%E8%BD%AF%E4%BB%B6%E4%B8%8B%E8%BD%BD%E4%B8%8E%E5%AE%89%E8%A3%85.html

从原来设备的配置文件导入到新的设备，两台墙 Fortitoken 冲突参考链接：
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Cannot-provision-soft-Fortitoken-with-error-no/ta-p/192610

报“没有找到有效的 token”也可能发成在 HA 场景下，只有主设备的 token 可用，如果备设备未注册，则会报此错误，
https://community.fortinet.com/t5/FortiGate/Technical-Tip-ERROR-No-valid-token-found-Unable-to-Provision/ta-p/191230

本链接描述了如何修复 Token 状态为错误/锁定/ Provision Timed Out。
https://community.fortinet.com/t5/FortiGate/Technical-Note-Fix-Licensed-Mobile-Token-with-Error-Locked/ta-p/194364

本链接描述了修复导入 FortiTokens 时发生内部服务器错误说明
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Internal-Server-Error-while-importing-FortiTokens/ta-p/190300