# 移动应用安全

# 常见问题

# 产品文档

腾讯云

# 文档目录

常见问题
应用加固
安全测评

# 常见问题
# 应用加固

最近更新时间：2020-01-10 17:32:17

### 应用加固上传失败的原因有哪些？

- 上传的应用未签名，目前移动应用安全仅允许上传已签名应用。
- 已加固的 apk 不可进行重复加固，只需要重签名即可。
- 部分浏览器可能存在不兼容情况，尝试换其他浏览器登录。
- 登录状态有问题，尝试退出浏览器清除缓存后，再重新登录。
- 应用存在安全风险。

注意：

- 若第三方杀毒引擎提示您的应用存在安全风险，移动应用安全则会拒绝您的应用上传、同时拒绝对应用进行加固。一旦出现该情形，建议您检查应用中是否存在违规行为。
- 若您将存在安全风险的应用发布出去，极大可能被渠道市场拒绝，且无法在用户手机安装。对于此类应用，加固能否成功并非最核心要素，因为渠道分发、用户手机都会有类似的安全扫描，移动应用安全采信的第三方杀毒引擎也极有可能被各分发市场、用户手机上安装的安全软件采信。

### 如何查看 apk 的签名信息？

安装好 Java，并配置环境变量。在 cmd 中执行：keytool -printcert -jarfile *.apk 即可看到 apk 的签名 MD5 字段信息。确认加固前后 apk 的签名信息是否一致。

### 加固失败并提示“应用存在安全风险”是什么原因？

- 说明应用被国内外杀毒引擎判定为恶意，移动应用安全将会拒绝对此类应用进行加固，请检查应用是否有违规行为。
- 移动应用安全采信了第三方杀毒引擎判定结果，若您的应用被杀毒引擎判定为恶意，加固已经没有意义。因该类应用将无法上架正规应用市场，且无法安装到用户手机，也注定会被手机的安全防护软件拦截。此类问题非加固造成，需仔细检查应用是否违规。
- 若确认应用本身无风险问题，可在官网进行 申诉。

### 应用加固后无法安装或登录闪退如何处理？

请确保加固后已重新签名，且加固前后签名保持一致。

### 应用加固后部分功能异常是什么原因？

通常是因为未（正确）签名导致，请排查以下可能问题：

- 应用加固前后签名不一致，或者未签名。
- 应用本身有签名、文件 MD5 校验等校验机制。
- 多次重复加固极易导致程序异常，请确保只加固一次。推荐使用 移动应用安全控制台 在线加固，请勿用第三方加固包或移动应用安全加固包再次加固。

### 如何进行应用加固？

您只需要确保使用已签名的安装包在 移动应用安全控制台 直接提交加固即可，可参见 快速入门 进行操作。

### 应用加固为什么必须重签名？

应用加固不可避免的会破坏原有签名，加固后必须对加固包重签名才能发布至应用市场，否则会被提示“应用未签名”，请务必确保加固前后的签名一致。

### 移动应用安全版本更新动态如何查看？

移动应用安全版本更新动态可参见 更新日志。

### 使用应用加固基础版的用户如何反馈问题？

使用应用加固基础版的用户，若在使用过程中若遇到问题，可以发送邮件至 MS_service@tencent.com 进行反馈，我们收到反馈后，会排期进行处理，应用加固基础版暂不支持实时的响应服务。

> 说明：
> 应用加固企业版享7 * 24小时技术支持服务。如您对应用加固有个性化需求，请联系移动应用安全客服 QQ：1783961938。

### 移动应用安全加固是否支持 SAAS 服务？

移动应用安全加固已全面升级为 SAAS 版，旧版 PC 工具已暂停维护。

# 安全测评

最近更新时间：2020-03-17 16:42:59

### 安全测评能解决什么问题？

虽然通过应用加固，可以对 App 程序进行整体的保护。但对于 App 的编程代码、第三方控件、以及残留信息等方面，是否存在代码风险，已知漏洞，是否存在后门等恶意代码，是否存在违法违规，暴露自身运行逻辑的敏感信息，就需要进行全面的安全测评，发现潜在的应用安全问题。

### 腾讯云应用安全检测能力如何？

腾讯云安全测评，包括代码风险、漏洞扫描、第三方 SDK 检测、恶意代码扫描，以及敏感词检测等全方面的安全测评能力。基于腾讯的全网终端覆盖，对于新风险、新威胁，能够第一时间反馈至应用安全测评能力，并转化为腾讯云用户的价值。

### 安全测评发现的问题，应该怎么办？

- 安全测评报告中，不仅会提供直观的测评结果，同时会将问题的具体位置、相关代码反馈用户，使用户能够快速定位到问题。
- 针对每一项测评结果中发现的问题，均配以相应的解决建议，建议具体到配置某个参数、代码，从而帮助用户快速解决问题。

### 应用在什么阶段进行安全测评？

- 建议用户在开发阶段中，可根据需要进行安全测评，及时发现并解决问题。
- 在应用发布前的测试阶段，建议进行安全测评，确保待发布应用的安全性。

### 使用未加固安装包，还是已加固安装包进行安全测评？

因为加固后部分代码已加密加壳，建议用户使用未加固安装包进行检测，能够更深度的发现潜在的风险和漏洞。