



链滴

微信消息加解密 JCE 无限制权限策略文件

作者: [guobing](#)

原文链接: <https://ld246.com/article/1475135400356>

来源网站: 链滴

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

今天做微信第三方平台开发，在微信消息加解密的过程中需要遇到一些问题。主要就是JCE无限制权限策略文件。默认的jdk里提供的包是有问题的。进行一些强度较高的加密会报错。

因为某些国家的进口管制限制，Java发布的运行环境包中的加解密有一定的限制。比如默认不允许25位密钥的AES加解密，解决方法就是修改策略文件。

官方网站提供了JCE无限制权限策略文件的下载：

<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>

下载后解压，可以看到local_policy.jar和US_export_policy.jar以及readme.txt。

如果安装了JRE，将两个jar文件放到%JRE_HOME%\lib\security下覆盖原来文件，记得先备份。

如果安装了JDK，将两个jar文件也放到%JDK_HOME%\jre\lib\security下。

附录：

由于信息安全在军事等方面极其重要，如在第二次世界大战期间，使用了无线电，若是能够成功解密方的机密情报，往往预示着战争的胜利，因此美国对加密解密等软件进行了出口限制，JDK中默认加的密钥长度较短，加密强度较低，而UnlimitedJCEPolicyJDK7中的文件则没有这样的限制，因此为获得更好的加密强度，需要替换掉那两个文件。