IAP 文档

2022-03-4

百度智能云

目录

功能发布记录

功能发布记录

发布时间	功能概述
2022-01	• 上线多用户访问控制功能 • 下架安卓应用加固（专业版）-15日 商品
2021-10	• 下架安卓应用加固免费版功能 • 安卓应用加固支持aab格式文件
2021-10	• 上线安全检测功能，支持应用检测、固件检测
2021-03	• 支持安卓应用加固、安卓SDK加固、H5加固

产品描述

产品简介

应用加固

应用加固与安全检测，是百度安全旗下一款面向智能终端应用的安全加固产品和服务，依托百度公司20年的安全实践和技术积累，已拥有多项安全专利和行业资质。产品包括不限于代码保护、数据加密、运行时防护等数十项加固能力，可全面提高智能终端应用的安全指数，同时满足工信部及各地方监管部门的合规需求。 **安卓应用加固** 针对安卓应用，提供基于VPM的高级SO和DEX代码加固方案，高强度的资源和数据文件加密方案，具备反调试、防逆向、防重打包能力，有效保护应用安全。不同版本功能对比如下：

功能	专业版	旗舰版
DEX整体加固	√	√
防重打包	√	√
防静态反编译	×	√
基础反调试	√	√
DEX的VPM加固	√	√
SO代码加固	√	√
SO代码VPM加固	×	√
高级反调试	×	√
运行环境安全	×	√
资源加密	×	√
数据加密	×	√
H5加固	×	√

安卓SDK加固 针对安卓SDK，从代码安全、资源数据文件安全等方面对SDK进行全方位加固保护。

功能	说明
JAR包加固	对JAR包内的Java代码进行虚拟化保护，防止SDK核心逻辑被逆向分析
AAR包加固	对AAR包采取高级虚拟化方案进行加固保护，防止Java代码被反编译和恶意篡改
SO文件加固	SO加壳、SO Linker、SO防调用、SO VMP
防调用	防止SDK被非授权的第三方应用集成和调用

H5加固 针对小程序等H5页面，进行全方位的加固保护，可有效保护应用的代码和数据安全。

功能	说明
多样化的混淆方案	变量名称混淆，控制流混淆，指令替换，混淆代码插入，代码压缩
强化加密能力	字符串加密，代码整体加密，属性加密
运行时防护	反调试，运行时变形，域名锁定，禁止控制台输出

核心能力说明

能力	说明
DEX文件保护	通过DEX文件加壳、DEX分离、DEX代码VMP保护等方式，对DEX代码进行全面保护。
SO文件保护	通过SO代码加壳，SO动态混淆，SO库防篡改等技术手段，全方位保护SO文件安全。
数据文件加密	对应用中的本地文件、数据库、缓存数据等进行加密保护，避免数据文件被破解、窃取。
反调试、防篡改	使用高级反调试，签名保护等技术，可以有效防止动态分析、动态注入，避免应用被篡改。
运行环境安全	提供应用运行环境检测能力，可以精准识别ROOT、模拟器等环境风险因素，降低环境因素带来的安全风险。

安全检测

安全检测主要包括应用检测和固件检测，可针对不同类型的检测需求提供检测和报告服务。

应用检测

应用检测旨在为APK、IPA、SDK提供自动化应用检测及报告服务，报告提供风险说明及修复建议。具有全面、准确、规范、高效等优势，能够帮助客户及时发现漏洞及风险，提高APP安全防护能力。

核心技术

- **静态检测**：以预设的安全问题特征为指导，通过静态的语法分析、控制流/数据流分析等技术，对应用的代码、配置、资源进行分析，发现潜在的安全问题
- **动态检测**：基于稳定性高、可扩展性强的硬件虚拟化技术。通过模拟真实攻击的场景，检测应用对恶意攻击的防范能力。
- **内容检测**：采用人工智能技术对应用内的图像、文本库进行检测，排查涉政暴恐、色情污秽等违规违法内容。
- **深度检测**：自动化破解应用部分保护措施，发现应用深层次的安全问题。

固件检测

面向IoT设备厂商提供固件安全检测服务，针对设备固件进行安全风险检测，帮助识别固件安全漏洞，旨在帮助厂商发现IoT设备的安全风险，并提供安全修复建议，减少后续产品发布后存在的风险问题和更新成本。

核心技术

- **风险检测与分析**：覆盖16类安全检测能力，提供对CVE漏洞、配置风险、密钥安全、敏感信息泄露、 代码安全、应用安全等检测。
- **固件多类型扫描**：支持多系统类型，支持但不限于Android、Linux、 RTOS、 Yocto、OpenWrt、 uClinux等 系统类型固件。

- **自动黑盒扫描**：采取无侵入式自动化检测方式，在平台提交 二进制文件即可获得检测报告。
- **多级检测规则**：提供基础检测、等保2.0、等保3.0检测三种检测规则。

产品优势

高安全性

- 采用全数据加密保障方案，保障应用数据安全。
- 产品已应用于小度智能音箱、自动驾驶等业务，拥有百度系产品高安全性标准规格。

强兼容性

- 适配市面上TOP600机型。
- 兼容安卓操作系统4.0版本至最新版本。

性能优越

- 应用经加固后对应用启动时间的影响几乎为0（小于0.5秒）。
- 应用经加固后安装包大小增量控制在5%以内，大部分应用可实现比加固前小。

服务专业

- 自研自营，资深工程师及匀饮团队提供专业售前售后咨询服务，高质高效。
- 针对不同类型客户和使用场景，提供多种接入方式。
- 可提供整套移动应用安全解决方案（应用加固+漏洞扫描+隐私合规等）。

应用场景

政策合规

满足国家相关法律、法规对应用安全的审核需求，保证应用能够合法、合规地正常上线。比如等保认证及各类第三方监管等。

程序防篡改、防盗版

通过代码加固、签名保护等机制，避免竞争对手或者黑客对APP进行篡改盗版，影响产品口碑。

商业模式保护

通过代码加固，高强度的数据加密等技术，避免黑客破解，绕过程序的收费鉴权机制。

代码和知识产权保护

通过SO加固、DEX加固、反调试等技术，避免黑客通过对程序进行反编译，窃取核心代码和知识产权。

产品定价

计费概述

应用加固与安全检测有安卓应用加固专业版、安卓应用加固旗舰版、安卓SDK加固、H5加固、应用检测、固件检测等多个版本。具体价格请参考：应用加固与安全检测定价。

计费方式

应用加固与安全检测所属商品目前均以预付费形式进行售卖，用户可在控制台进行自助购买。

计费规则

安卓应用加固专业版

时长	APP个数	备注
1年	1	用户可自定义购买的加固APP个数

安卓应用加固旗舰版

时长	APP个数	备注
1年	1	用户可自定义购买的加固APP个数

安卓SDK加固

时长	SDK个数	备注
1年	不限	不限制加固的SDK个数

H5加固

时长	H5个数	备注
1年	不限	不限制加固的H5个数

应用检测

- 包年购买

时长	APP个数	备注
1年	1	单个APP包年不限检测次数，用户可根据实际需求购买多个APP

- 按次购买

检测次数	备注
1	单次检测，可购买多次

固件检测

- 按次购买

检测次数	备注
1	单次检测，可购买多次

操作指南

加固管理

应用加固

安卓应用加固

加固准备 使用加固之前需要准备好待加固的apk/aab文件。

> 待加固的apk/aab文件，需要使用正式发布签名证书进行签名。

上传应用

本操作适用于安卓应用加固专业版、旗舰版。

1. 登录应用加固与安全检测控制台
2. 在控制台左侧导航栏，选择应用加固，进入控制台页面。
3. 点击“上传应用”后，在弹窗中选择“加固方案”和“加固文件”，选择加固文件时会打开本地文件夹，选择待加固的apk/aab文件即可。

加固设置

本操作仅适用于安卓应用加固旗舰版。

如果加固方案选择为“安卓应用加固（旗舰版）”，可在上传应用时进行加固设置：

1. 选择已有配置文件并可进行编辑，或者添加新的配置文件。
2. 配置文件项操作同加固设置。

加固应用 应用上传后，系统会根据预先设定的规则进行加固，界面会实时显示当前加固状态，加固状态有如下几种：

- 加固成功：已完成加固，可以下载加固后的apk/aab文件进行后续操作。
- 加固中：加固引擎有多个加固任务正在排队，系统将依照先后顺序依次进行加固。
- 加固失败：由于系统策略或者其他问题导致，可点击“查看原因”浏览具体报错信息。

安卓SDK加固

加固准备 使用加固之前需要准备好待加固的jar/aar文件。

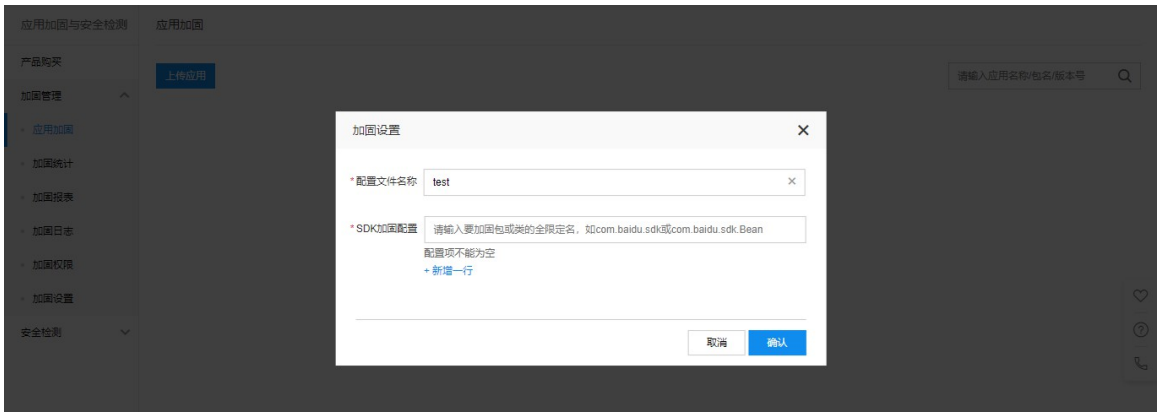
上传应用

1. 登录应用加固与安全检测控制台
2. 在控制台左侧导航栏，选择应用加固，进入控制台页面。
3. 点击“上传应用”后，在弹窗中选择“加固方案”和“加固文件”，选择加固文件时会打开本地文件夹，选择待加固的jar/aar文件即可。

加固设置

在上传应用时进行加固设置：

1. 选择已有配置文件并可进行编辑，或者添加新的配置文件。
2. 配置文件名称，自定义设定。
3. SDK加固配置，根据自身加固需求进行设定。



加固应用 应用上传后，系统会根据预先设定的规则进行加固，界面会实时显示当前加固状态，加固状态有如下几种：

- 加固成功：已完成加固，可以下载加固后的jar/aar文件进行后续操作。
- 加固中：加固引擎有多个加固任务正在排队，系统将依照先后顺序依次进行加固。
- 加固失败：由于系统策略或者其他问题导致，可点击“查看原因”浏览具体报错信息。

H5加固

操作步骤

1. 登录应用加固与安全检测控制台

2. 在控制台左侧导航栏，选择应用加固，进入控制台页面内进行操作

H5加固使用流程和安卓应用加固使用流程类似。您可在IAP的应用加固页面，上传对应js文件，并且选择加固方案为H5加固即可。

签名方法和验证

签名方法 目前Android7.0以下的手机使用v1版本签名，7.0以上手机支持v1、v2, 更高版本的手机可能支持v3、v4；早期v1签名是使用jdk自带的jarsigner，现在已经不推荐使用； 目前推荐使用Android SDK自带的apksigner，在Android SDK安装目录下。 **签名工具目录** SDK/build-tools/版本号/apksigner.bat (或SDK/build-tools/版本号/lib/apksigner.jar)，版本号需大于等于25。

使用 apksigner 工具为 apk 签名的语法如下（两种签名方式）

```
 apksigner sign --ks keystore.jks [signer_options] app-name.apk
apksigner sign --key key.pk8 --cert cert.x509.pem [signer_options] app-name.apk
```

在您使用 apksigner 工具为 apk 签名时，必须提供签名者的私钥和证书。您可以通过两种不同的方式添加此信息：

- 使用 --ks 选项指定密钥库文件。
- 使用 --key 和 --cert 选项分别指定私钥文件和证书文件。私钥文件必须使用 PKCS #8 格式，证书文件必须使用 X.509 格式。
- 使用 [signer_options] 可指定应用于签名者的基本设置。 **重要选项** 以下选项指定要应用于签名者的基本设置。

设置	说明
--out	您将要保存已签名 apk的位置。如果未明确提供此选项，则 apk 软件包将就地签名，并替换输入的 apk文件。
--min-sdk-version	apksigner 用来确认 apk 签名将通过验证的最低 Android 框架 API 级别。该级别值越高，表示该工具在为应用签名时可使用的安全参数越强，但这会限制 apk 只能用于搭载更新版本 Android 的设备。
--max-sdk-version	apksigner 用来确认 apk 签名将通过验证的最高 Android 框架 API 级别。默认情况下，该工具会使用尽可能高的 API 级别。
--v1-signing-enabled	确定 apksigner 是否会使用基于 JAR 的传统签名方案为给定的 apk 软件包签名。默认情况下，该工具会使用 --min-sdk-version 和 --max-sdk-version 的值来决定何时采用此签名方案。
--v2-signing-enabled	确定 apksigner 是否会使用 apk 签名方案 v2 为给定的 apk 软件包签名。默认情况下，该工具会使用 --min-sdk-version 和 --max-sdk-version 的值来决定何时采用此签名方案。
--v3-signing-enabled	确定 apksigner 是否会使用 apk 签名方案 v3 为给定的 apk 软件包签名。默认情况下，该工具会使用 --min-sdk-version 和 --max-sdk-version 的值来决定何时采用此签名方案。
--v4-signing-enabled	确定 apksigner 是否会使用 apk 签名方案 v4 为给定的 apk 软件包签名。此方案会在单独的文件 (apk-name.apk.idsig) 中生成签名。如果为 true 并且apk 未签名，则系统会根据 --min-sdk-version 和 --max-sdk-version 的值生成 v2 或 v3 签名。然后，该命令会根据已签名的 apk 的内容生成 .idsig 文件。使用 only 仅生成 v4 签名，而不会修改 apk 及其在调用前具有的任何签名；如果apk 没有v2 或 v3 签名，或者签名使用的密钥不同于为当前调用提供的密钥，则 only 会失败。默认情况下，该工具会使用 --min-sdk-version 和 --max-sdk-version 的值来决定何时采用此签名方案。
--v4-no-merkle-tree	默认情况下，.idsig 文件包含 apk 文件的完整 Merkle 树。使用此标志时，apksigner 会生成一个 apk 签名方案 v4 .idsig 文件，且不会嵌入完整的 Merkle 树。此选项会减小签名文件的大小，但会强制任何需要该树的工具重新计算大小，或者再次调用apksigner 工具。
-v、--verbose	使用详细输出模式。

密钥和证书选项 以下选项用于指定签名者的私钥和证书。

设置	说明
--ks	签名者的私钥和证书链包含在给定的基于 Java 的密钥库文件中。如果文件名设为 "NONE"，则包含密钥和证书的密钥库不需要指定文件，某些 PKCS # 11 密钥库就是这种情况。
--ks-key-alias	表示签名者在密钥库中的私钥和证书数据的别名的名称。如果与签名者关联的密钥库包含多个密钥，则必须指定此选项。
--ks-pass	包含签名者私钥和证书的密钥库的密码。您必须提供密码才能打开密钥库。apksigner 工具支持以下格式：1）pass:- 密码与 apksigner sign 命令的其余部分一起提供（内嵌在其中）。2）env: - 密码存储在给定的环境变量中。3）file: - 密码存储在给定文件中的某一行。4）stdin - 密码作为标准输入流中的某一行提供。这是 --ks-pass 的默认行为。

注意事项 如果一个文件中包含多个密码，请分别在不同的行中指定这些密码。apksigner 工具会根据您指定 APK 签名者的顺序将密码与签名者相关联。

如果您为签名者提供了两个密码，apksigner 会将第一个密码视为密钥库密码，将第二个密码视为密钥密码。

使用 release.jks（密钥库中唯一的密钥）为 apk 签名：

```
$ apksigner sign --ks release.jks app.apk
```

使用私钥和证书（存储为不同的文件）为 apk 签名：

```
$ apksigner sign --key release.pk8 --cert release.x509.pem app.apk
```

签名保留源文件，生产新文件：

```
$apksigner sign --key release.pk8 --cert release.x509.pem --out app.sign.apk app.apk
```

签名禁用v3、v4

```
$ apksigner sign --ks release.jks --v3-signing-enabled false --v4-signing-enabled false app.apk
```

签名指定sdk version（sdk version会影响生产的签名版本）

```
$ apksigner sign --ks release.jks --min-sdk-version 20 --max-sdk-version 27 app.apk
```

签名验证和查看方法 人工简单查看 解压apk/META-INF/XXXX.SF(如CERT.SF，不是MANIFEST.SF)，查看开始部分，如果不包含X-Android-APK-Signed字样则为v1， 如：

```
 Signature-Version: 1.0
SHA1-Digest-Manifest-Main-Attributes: NdvTTYSDLv+xfCdISs2OUVv3OXY=
Created-By: 1.6.0_37 (Sun Microsystems Inc.)
SHA1-Digest-Manifest: sN1jczINBspGueVoYodPfvNRYKA=
```

包含X-Android-APK-Signed字样，则冒号后面跟的版本就是签名版本，如下面是v1和v2版本

```
 Signature-Version: 1.0
Created-By: 1.0 (Android)
SHA1-Digest-Manifest: EsSraWdS5nUZen7L+SDZDNTr230=
X-Android-APK-Signed: 2
```

包含X-Android-APK-Signed字样，则冒号后面跟的版本就是签名版本，如下面是v2和v3版本

```
 Signature-Version: 1.0
Created-By: 1.0 (Android)
SHA1-Digest-Manifest: EsSraWdS5nUZen7L+SDZDNTr230=
X-Android-APK-Signed: 2, 3
```

工具查看(通过工具会输出详细的签名信息) 在SDK/build-tools/版本（如30.0.2）/apksigner.bat或SDK/build-tools/版本（如30.0.2）/lib/apksigner.jar两种工具。

- 工具一使用：

```
SDK/build-tools/版本（如30.0.2）/apksigner.bat verify --verbose xxx.apk
```

- 工具二使用：

```
java -jar SDK/build-tools/版本（如30.0.2）/lib/apksigner.jar --verbose xxx.apk
```

示例(v1+v2)：

```
 E:\Android\Sdk\build-tools\30.0.2\apksigner.bat verify --verbose .\cdd.apk
&amp;nbsp;
Verifies
Verified using v1 scheme (JAR signing): true
Verified using v2 scheme (APK Signature Scheme v2): true
Verified using v3 scheme (APK Signature Scheme v3): false
Verified using v4 scheme (APK Signature Scheme v4): false
Verified for SourceStamp: false
Number of signers: 1
```

示例（v1）：

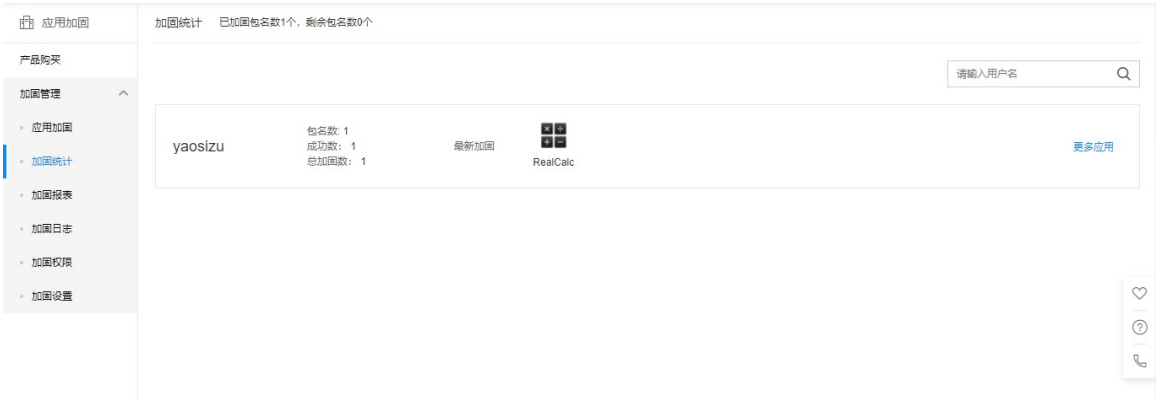
```
 Verifies
Verified using v1 scheme (JAR signing): true
Verified using v2 scheme (APK Signature Scheme v2): false
Verified using v3 scheme (APK Signature Scheme v3): false
Verified using v4 scheme (APK Signature Scheme v4): false
Verified for SourceStamp: false
Nuer of signers: 1
```

更详细说明 https://developer.android.com/studio/command-line/apksigner?hl=zh-cn#options

加固统计

操作步骤

1. 登录应用加固与安全检测控制台。
2. 点击左侧导航栏“加固管理-加固统计”，查看自身和所属子用户加固的加固统计。
   - 展示信息：包名数、成功数、总加固数，以及最新加固的应用和所有加固的应用
   - 更多应用：点击可查看用户加固过的所有应用，如果应用已被删除会进行标记



加固报表

操作步骤

1. 登录应用加固与安全检测控制台。
2. 点击左侧导航栏“加固管理-加固报表”，查看加固统计自身和所属子用户的加固统计报表。
   - 日期筛选：点击选择特定日期查看加固统计
   - 加固统计：可查看日加固、周加固、月加固、累计加固的统计

- 报表查看：点击选择日加固、周加固、月加固，查看对应时间维度加固的折线图统计

加固日志

操作步骤

1. 登录应用加固与安全检测控制台。
2. 点击左侧导航栏“加固管理-加固日志”，查看自身和所属子用户的详细加固日志。

项目	含义
名称	应用的名称
IP	应用的IP地址
包名	加固的APP的包名
证书	APP对应的加固证书文件
调用方式	可选择加固的方式：web、client、全部
状态	筛选加固状态，包含：加固中、加固成功、加固失败、已删除、全部
上传情况	可点击按时间升序、降序，对加固日志进行排序查看
操作	针对状态为加固成功的加固日志，可下载加固成功后的APP

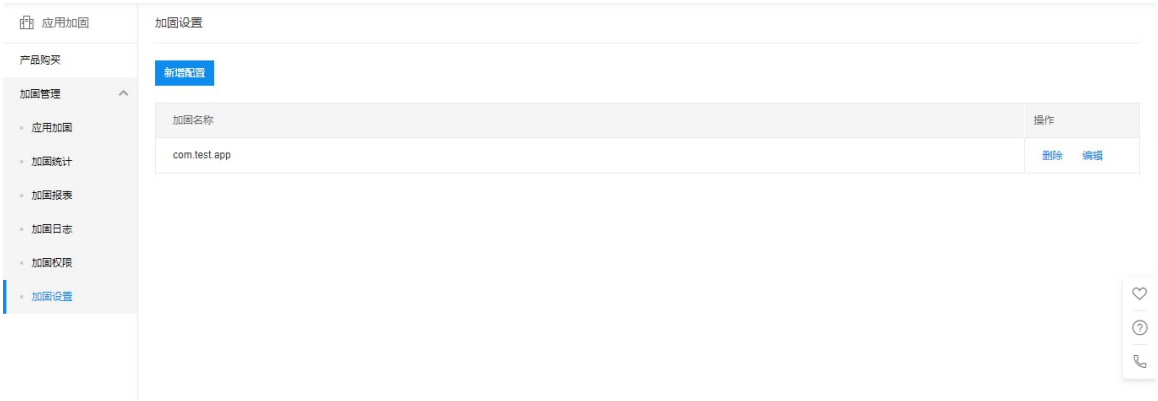
加固设置

操作步骤

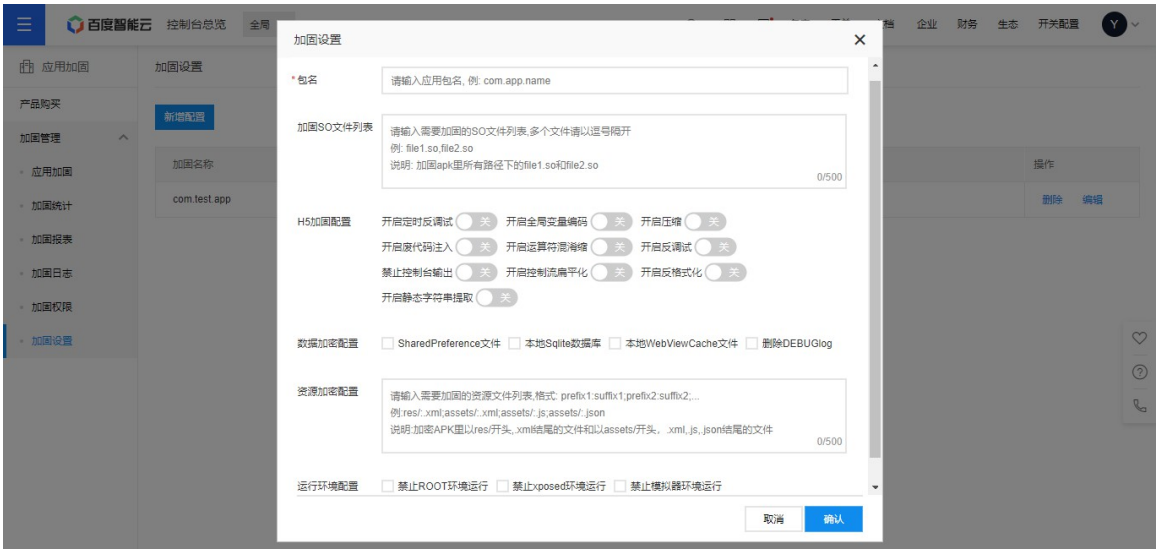
1. 登录应用加固与安全检测控制台。
2. 点击左侧导航栏“加固管理-加固设置”，进入加固设置界面。

> 说明：加固设置适用于安卓应用加固旗舰版。

3. 点击新增配置、或者编辑已有配置文件，可删除已存在的配置文件。



4. 进行加固设置配置：输入加固包名、加固SO文件列表、资源加密配置，勾选所需的H5加固配置、数据加密配置、运行环境配置选项，点击确认加固设置生效



安全检测

应用检测

检测准备

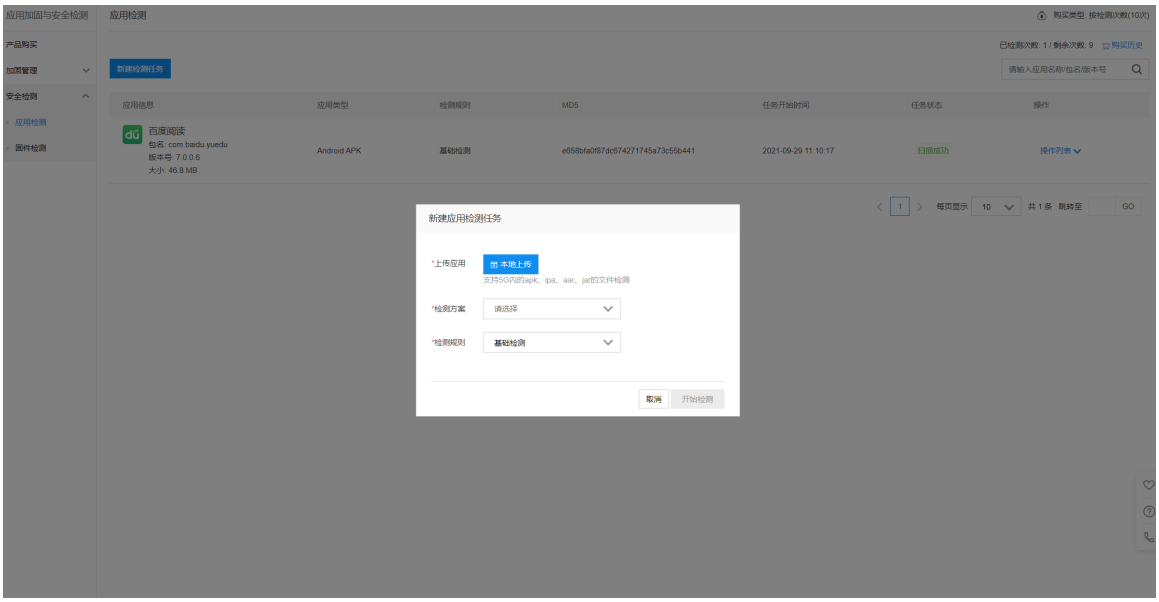
使用应用检测前需要准备好待检测的应用文件。

> 支持5G内的apk、ipa、aar、jar的文件检测

上传应用

本操作适用于应用检测。

1. 登录应用加固与安全检测控制台
2. 在控制台左侧导航栏，选择应用检测，进入控制台页面。
3. 点击“新建检测任务”后，在弹窗中选择“检测方案”和“检测规则”，并上传应用文件，打开本地文件夹，选择需要检测的应用文件。



检测结束

应用检测任务创建后，会开始进行扫描：

- 扫描成功：已完成应用检测，用户可根据需要在线查看或下载检测报告。
- 扫描中：应用检测需要等待时间，通常为5-10分钟。
- 检测失败：检测应用文件失败。

应用检测报告

应用检测报告示意图如下：

固件检测

检测准备

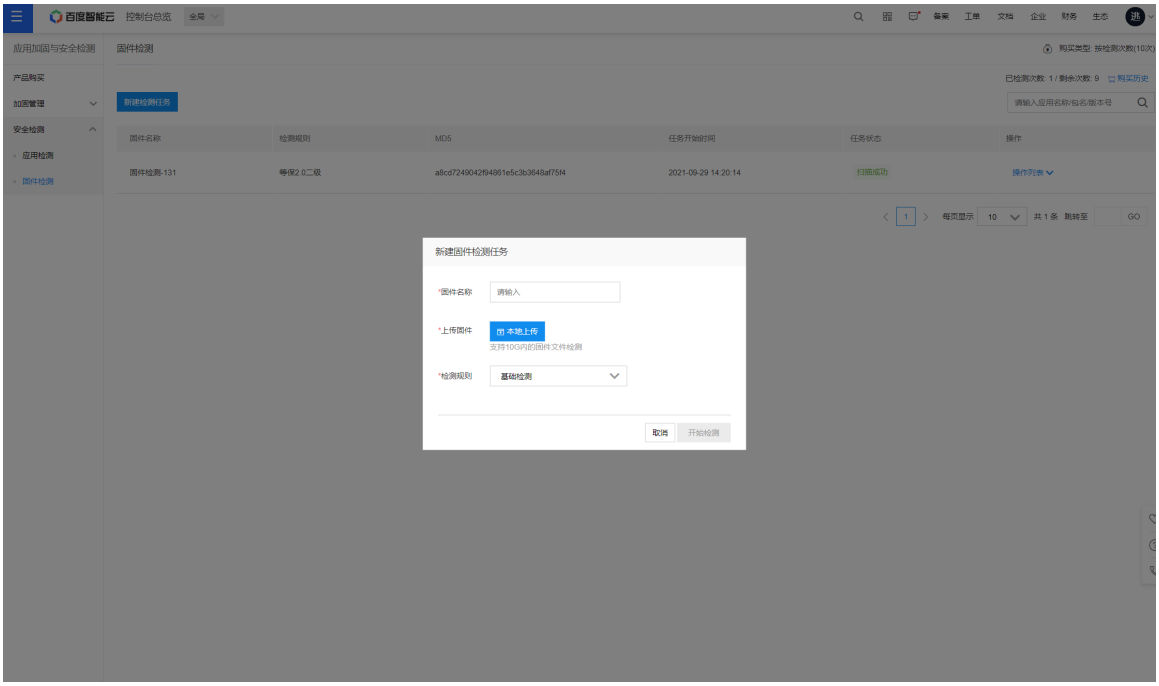
使用固件检测前需要准备好待检测的固件文件。

> 支持10G内的固件文件检测

上传固件

本操作适用于固件检测。

1. 登录应用加固与安全检测控制台
2. 在控制台左侧导航栏，选择固件检测，进入控制台页面。
3. 点击“新建检测任务”后，在弹窗中选择“检测规则”，并上传固件文件，打开本地文件夹，选择需要检测的固件文件。



检测结束

固件检测任务创建后，会开始进行扫描：

- 扫描成功：已完成固件检测，用户可根据需要在线查看或下载检测报告。
- 扫描中：固件检测需要等待时间，通常为5-10分钟。
- 检测失败：检测固件文件失败。

固件检测报告

固件检测报告示意图如下：

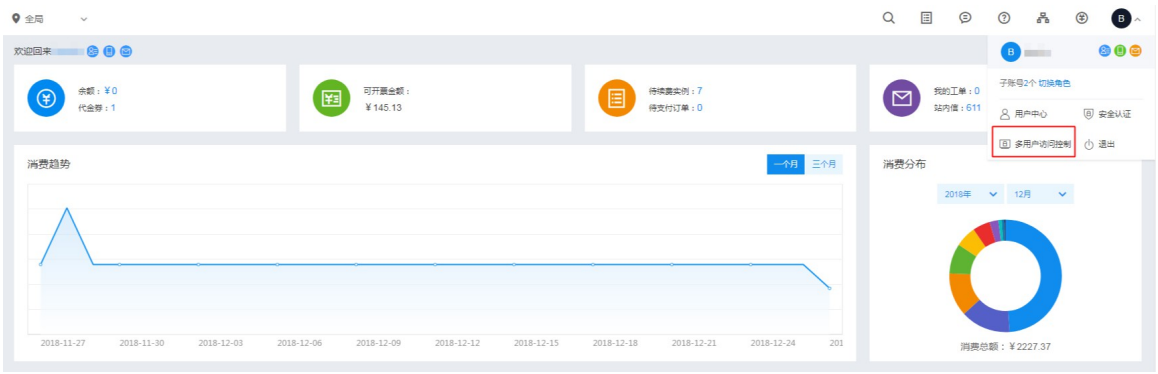
多用户访问控制

功能介绍

多用户访问控制，主要用于帮助用户管理云账户下功能的访问权限，适用于企业内的不同角色，可以对不同的工作人员赋予使用产品的不同权限，当您的企业存在多用户协同操作功能时，推荐您使用多用户访问控制。

创建用户

1. 主账号用户登录后在控制台选择“多用户访问控制”进入用户管理页面。



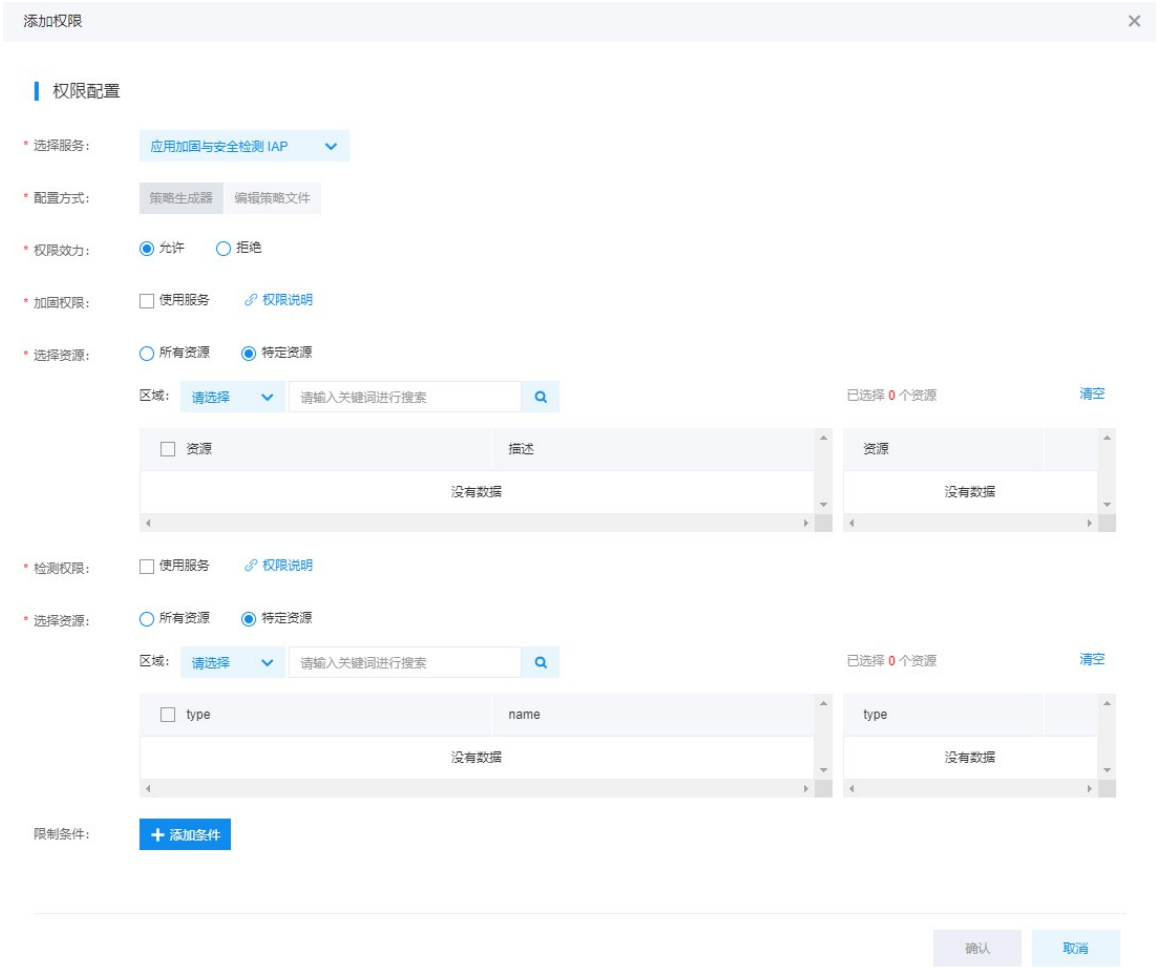
2. 在左侧导航栏点击“用户管理”，在“子用户管理列表”页，点击“新建用户”。

3. 在弹出的“新建用户”对话框中，完成填写“用户名”和确认，返回“子用户管理列表”区可以查看到刚刚创建的子用户。

配置策略

IAP支持用户自定义策略，实现对IAP不同功能的权限控制。

1. 用户先通过左侧导航栏进入【策略管理】，然后点击“创建策略”，用户填写策略名称并选择服务类型为“应用加固与安全检测IAP”，其中策略生成方式默认为策略生成器，不需要修改。



2. 权限效力：选择允许或拒绝，代表所创建权限是被允许或被拒绝

3. 加固权限：勾选“使用服务”，选择资源的不同情况说明

资源	说明
所有资源	包含加固权限下的所有功能
特定资源	可选加固权限下的不同功能 1. 安卓应用加固（专业版） 2. 安卓应用加固（旗舰版） 3. 安卓SDK加固 4. H5加固

4. 检测权限：勾选“使用服务”，选择资源的不同情况说明

资源	说明
所有资源	包含检测权限下的所有功能
特定资源	可选检测权限下的不同功能 1. 应用检测 2. 固件检测

用户授权

在“用户管理->子用户管理列表页”的对应子用户的“操作”列选择“添加权限”，并为用户选择系统权限或自定义策略进行授权。

子用户登录

主账号完成对子用户的授权后，可以将链接发送给子用户；子用户可以通过IAM用户登录链接登录主账号的管理控制台，根据被授权的策略对主账户功能进行操作和查看。

其他详细操作参考：多用户访问控制

常见问题

1. 安卓应用加固支持AAB格式加固吗？

支持

2. 加固后的APK文件是否需要重新签名？

APK加固后需要重新签名，且加固前与加固后签名使用的证书必须一致，可以使用任何合法的签名工具进行签名。

3. 安卓应用加固专业版和旗舰版有什么区别？

安卓应用加固不同版本区别

4. 安卓SDK加固支持什么格式的文件类型？

JAR、AAR格式文件

服务等级协议SLA

协议生效时间：2021年10月12日

本服务等级协议（Service Level Agreement，以下简称 "SLA"）规定了百度智能云向客户提供的应用加固与安全检测IAP（In-App Protection，简称"IAP"）的服务可用性等级指标及赔偿方案。

1. 定义

服务周期：用户所购买服务的有效期

服务周期总分钟数：服务周期内的总天数 * 24（小时） * 60（分钟）计算

服务不可用：在某一分钟内，用户无法通过百度智能云的IAP服务进行相关产品（安卓应用、安卓SDK、H5）的加固操作

服务不可用分钟数：服务周期内使用IAP服务不可进行加固操作的分钟数之和

2. 服务可用性

2.1 服务可用性计算公式

$$服务可用性=\left(\frac{服务周期总分钟数-服务不可用分钟数}{服务周期总分钟数}\right)\times 100\%$$

2.2 服务可用性承诺

百度智能云IAP服务承诺一个服务周期内IAP的服务可用性不低于99.95%；如IAP服务未达到上述服务可用性承诺，客户可以根据本协议第3条约定的赔偿方案获得赔偿。赔偿范围不包括以下原因所导致的服务不可用：

（1）预先通知用户后进行系统维护，包括割接、维修、升级和模拟故障演练等引起的服务不可用；

（2）任何IAP服务所属设备以外的网络、设备故障或配置调整引起的服务不可用；

（3）用户自身应用程序原因（包含但不限于应用被黑客攻击、应用非法，应用程序开发不规范等）引起的服务不可用；

（4）用户未遵循IAP服务使用文档、操作使用不当、或其他疏忽引起的服务不可用；

（5）用户未遵循任何百度智能云产品条款引起的服务不可用；

（6）用户对百度智能云提供的服务造成安全威胁或存在欺诈和违法行为而导致的服务不可用；

（7）用户维护不当或保密不当致使数据、口令、密码等丢失或泄漏所引起的服务不可用；

（8）不可抗力或者其他意外事件引起的服务不可用；

（9）其他非百度智能云原因所造成的服务不可用。

3. 赔偿方案

3.1 赔偿标准

根据用户某一百度智能云账号下IAP服务可用性比例，按照下表中的标准计算赔偿金额，赔偿方式仅限于用于购买IAP服务的代金券，赔偿总额不超过用户所购买IAP服务有效期内费用的50%。

服务可用性	赔偿代金券金额
低于99.95%但等于或高于99%	服务有效期内服务费用的10%
低于99%但等于或高于95%	服务有效期内服务费用的20%
低于95%	服务有效期内服务费用的50%

3.2 赔偿申请时限

赔偿申请必须限于在百度智能云IAP服务没有达到服务可用性承诺比例的相关月份结束后两个月内提出。超出申请时限的赔偿申请将不被受理。百度智能云收到您的赔偿申请且在您资料提交齐全的情况下启动赔偿申请审核，审核期间可能会与您核实相关

情况，并根据核实的结果对您提出的赔偿申请依据本等级服务协议及相关协议作出处理。

4. 其他说明

(1) 在法律法规允许的范围内，百度智能云负责对本协议进行解释说明。

(2) 本协议一经公布立即生效，百度智能云有权对本SLA条款作出修改。如本SLA条款有任何修改，百度智能云将以网站公示或发送邮件的方式通知您。如您不同意百度智能云对SLA所做的修改，您有权停止使用IAP服务，如您继续使用IAP服务，则视为您接受修改后的SLA。

(3) 本协议项下百度智能云对于用户所有的通知均可通过网页公告、站内信、电子邮件、手机短信或其他形式等方式进行；该等通知于发送之日视为已送达收件人。因用户未及时获知百度智能云的服务变更或终止条款遭受损失的，百度智能云不承担任何责任。

(4) 本协议的订立、执行和解释及争议的解决均应适用中国法律并受中国法院管辖。如双方就本协议内容或其执行发生任何争议，双方应尽量友好协商解决；协商不成时，任何一方均可向北京市海淀区人民法院提起诉讼。

(5) 本协议构成双方对本协议之约定事项及其他有关事宜的完整协议，除本协议规定的之外，未赋予本协议各方其他权利。

(6) 如本协议中的任何协议无论因何种原因完全或部分无效或不具有执行力，本协议的其余协议仍应有效并且有约束力。

(7) 关于用户约束条款，详见百度智能云用户服务协议中的"用户的权利与义务"相关条款内容。

(8) 关于服务商免责条款，详见百度智能云用户服务协议中的"免责声明"相关条款内容。