Permissions overview

- The purpose of a permission is to protect the **privacy** of an Android user. Android apps must request permission to **access sensitive** user data (such as contacts and SMS), as well as certain **system features** (such as camera and internet). Depending on the feature, the system might grant the permission **automatically** or might prompt the user to approve the **request**.
- A central design point of the Android **security architecture** is that no app, **by default**, has permission to perform any operations that would **adversely impact** other apps, the operating system, or the user. This includes reading or writing the user's private data (such as contacts or emails), reading or writing another app's files, performing network access, keeping the device awake, and so on.

Permission approval

An app must publicize the permissions it requires by including <uses-permission> tags in the app manifest. For example,

- If your app lists normal permissions in its manifest (that is, permissions that don't pose much risk to the user's privacy or the device's operation), the system automatically grants those permissions to your app.
- If your app lists dangerous permissions in its manifest (that is, permissions that could potentially affect the user's privacy or the device's normal operation), such as the SEND_SMS permission above, the user must explicitly agree to grant those permissions.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.developer.anas.mateshare">
    <uses-permission android:name="android.permission.INTERNET"/>
    <application
       ...
    </application>
</manifest>
```

Protection levels

Permissions are divided into several protection levels. The protection level affects whether runtime permission requests are required

There are most two important protection levels that affect third-party apps:

- Normal permissions
- Dangerous permissions

Normal permissions

Normal permissions cover areas where your app needs to access data or resources outside the app's sandbox, but where there's very little risk to the user's privacy or the operation of other apps. For example, permission to set the time zone is a normal permission.If an app declares in its manifest that it needs a normal permission, the system automatically grants the app that permission at install time.

Example:- INTERNET, BLUETOOTH, SET_ALARM, ACCESS_WIFI_STATE

Dangerous permissions

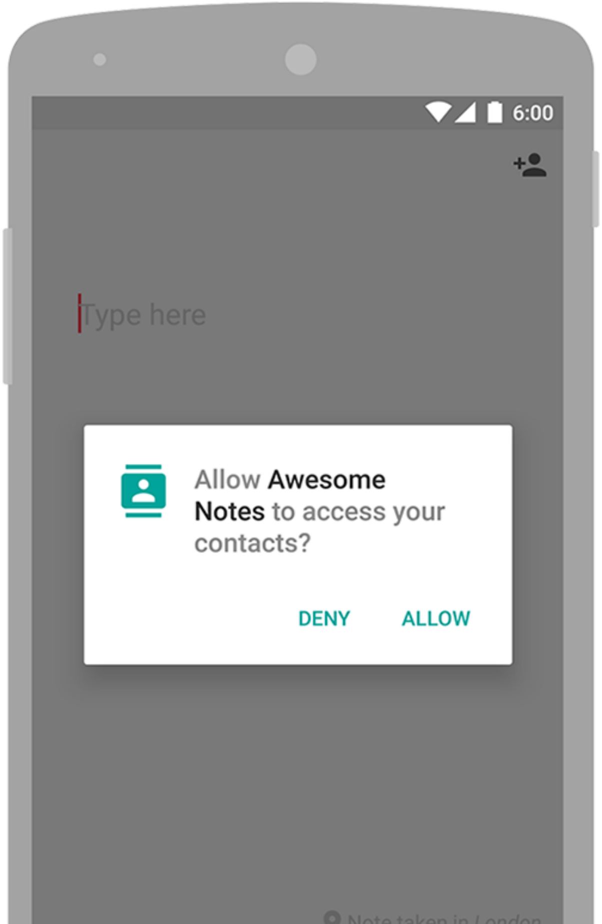
Dangerous permissions cover areas where the app wants **data or resources** that involve the user's private information, or could **potentially** affect the user's stored data or the operation of other apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to **explicitly grant** the permission to the app.

Example: CAMERA, LOCATION, SMS, STORAGE

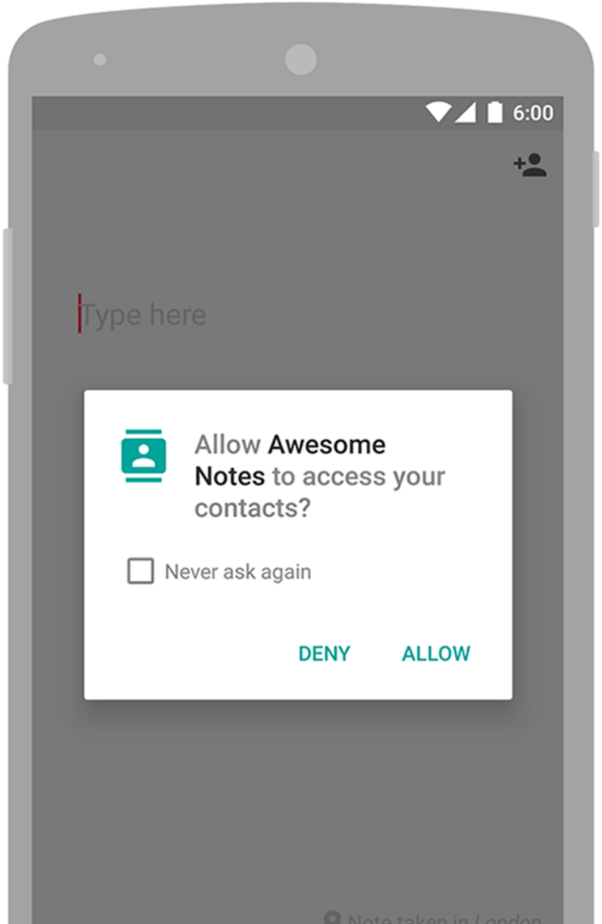
Request Prompts dangerous permissions

- Runtime requests (Android 6.0 and higher)

  If the device is running Android 6.0 (API level 23) or higher, and the app's targetSdkVersion is 23 or higher, the user isn't notified of any app permissions at install time. Your app must ask the user to grant the dangerous permissions at runtime. When your app requests permission, the user sees a system dialog telling the user which permission group your app is trying to access. The dialog includes a **Deny** and **Allow** button.



Allow **Awesome Notes** to access your contacts?



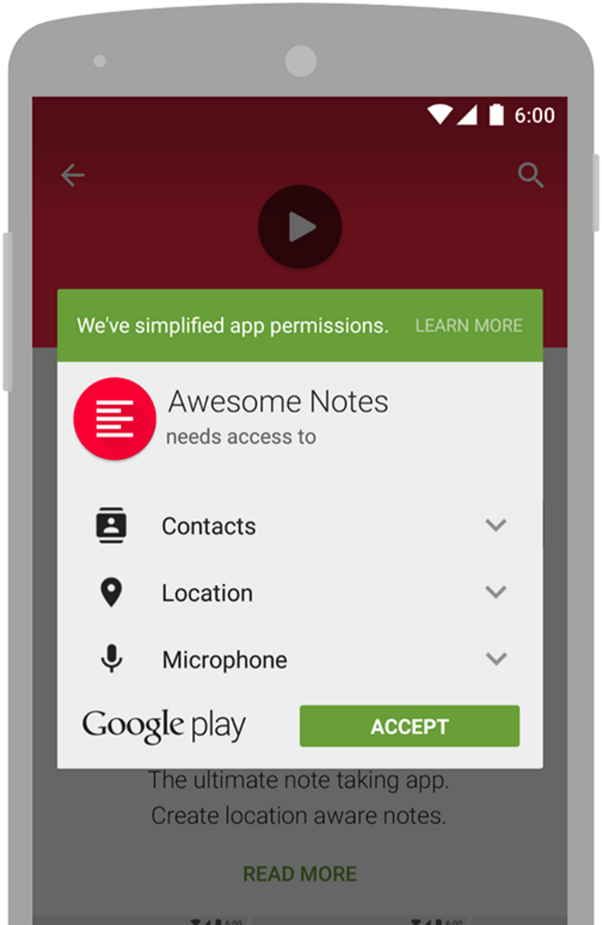
Allow **Awesome Notes** to access your contacts?

Request Prompts dangerous permissions

- Install-time requests (Android 5.1.1 and below)

  If the device is running Android 5.1.1 (API level 22) or lower, or the app's targetSdkVersion is 22 or lower while running on any version of Android, the system automatically asks the user to grant all dangerous permissions for your app at install-time

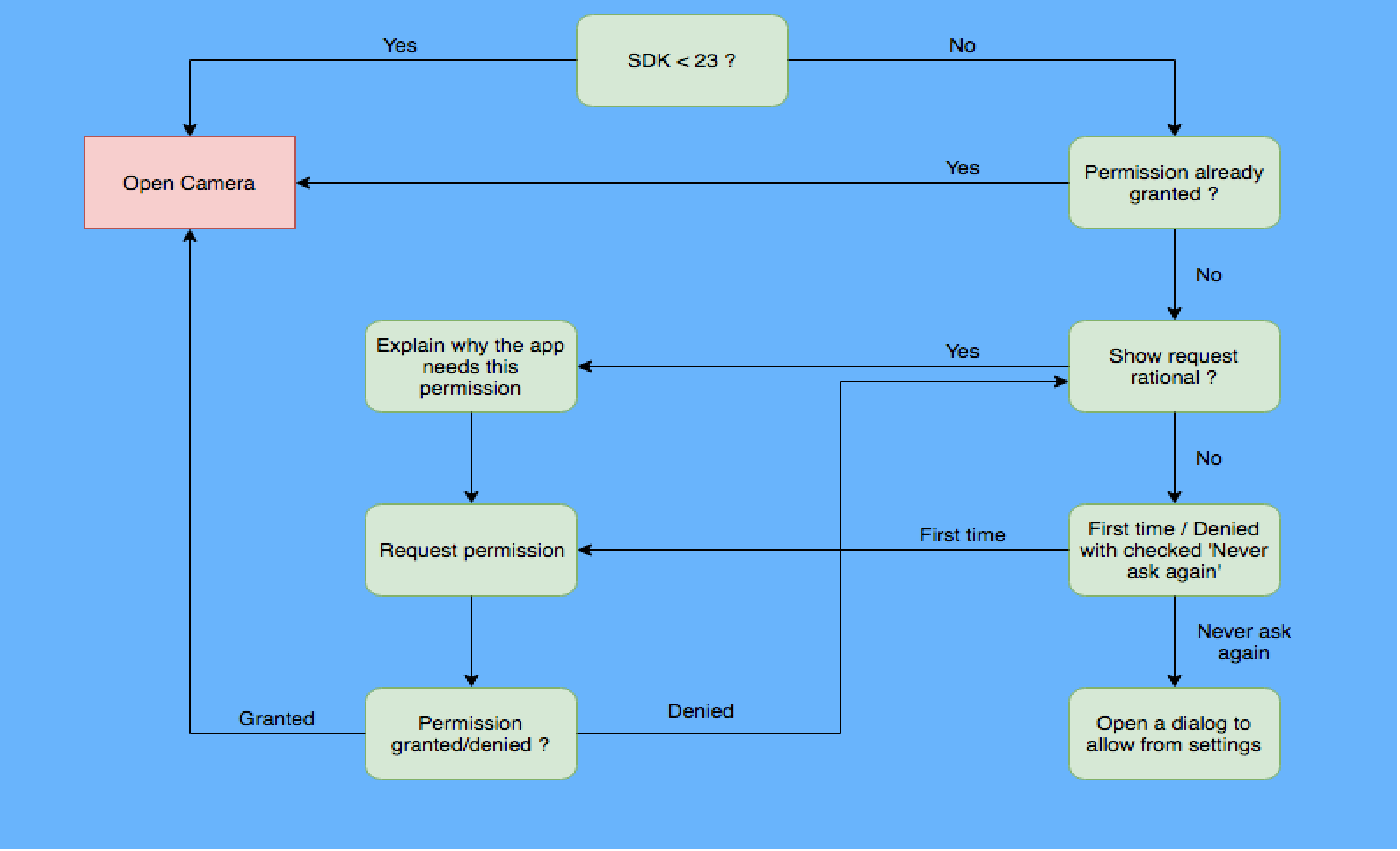
  If the user clicks Accept, all permissions the app requests are granted. If the user denies the permissions request, the system cancels the installation of the app.



We've simplified app permissions.

Awesome Notes
needs access to

The ultimate note taking app.
Create location aware notes.


SDK < 23 ?
Yes
No
Open Camera
Yes
Permission already granted ?
No
Explain why the app needs this permission
Yes
Show request rational ?
No
Request permission
First time
First time / Denied with checked 'Never ask again'
Never ask again
Granted
Permission granted/denied ?
Denied
Open a dialog to allow from settings

Run time permissions cases

- **Case 1:**

  The permission never asked before.

- **Case 2:**

  The permission asked before but user denied without checking ‘Never ask again’.

- **Case 3:**

  The permission asked before but user denied with checking ‘Never ask again’.