

# Detection of Calendar Entries, Detection Strategy DET0674

Archived: 2026-04-05 15:34:00 UTC

## AN1774

Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it.

On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.

### Log Sources

## AN1775

Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it.

On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.

### Log Sources

---

Source: <https://attack.mitre.org/detectionstrategies/DET0674#AN1774>