앱 관리

이 섹션에서는 앱 가용성, 설치, 업데이트 및 권한 관리와 관련된 정책을 설정할 수 있습니다.

관리되는 Google Play 계정은 기기가 프로비저닝될 때 자동으로 생성됩니다 .

1. Play 스토어 모드

이 모드는 Play 스토어에서 사용자가 사용할 수 있는 앱과 정책에서 앱이 제거될 때 기기에서의 동작을 제어합니다 .

허용 목록 (기본값): 정책에 있는 앱만 사용할 수 있으며 정책에 없는 앱은 기기에서 자동으로
제거됩니다 . Play 스토어에는 사용 가능한 앱만 표시됩니다 .

차단 목록: 모든 앱을 사용할 수 있으며 기기에 있으면 안 되는 앱은 애플리케이션 정책에서 차단됨
으로 명시적으로 표시해야 합니다. Play 스토어에는 차단된 앱을 제외한 모든 앱이 표시됩니다 .

2. 신뢰할 수 없는 앱 정책

기기에 적용되는 신뢰할 수 없는 앱 (알 수 없는 출처의 앱)에 대한 정책입니다 . 이 옵션은 사용자가 Play 스토어 외부에서 앱을 설치 (사이드로드 )할 수 있는지 결정하는 Android 시스템 설정을 제어합니다 .

허용 안 함 (기본값): 전체 기기에서 신뢰할 수 없는 앱 설치를 허용하지 않습니다.

개인 프로필만 : 직장 프로필이 있는 기기의 경우 기기의 개인 프로필에서만 신뢰할 수 없는 앱 설치를 허용합니다 .

허용: 전체 기기에서 신뢰할 수 없는 앱 설치를 허용합니다 .

3. Google Play Protect

Google Play Protect 앱 검증이 적용되는지 여부입니다 .

강제 적용 (기본값): 앱 검증을 강제로 활성화합니다 .

사용자 선택: 사용자가 앱 검증을 활성화할지 선택할 수 있습니다.

4. 기본 권한 정책

앱에 런타임 권한 요청을 부여하는 정책입니다 .
메시지 표시 (기본값): 사용자에게 권한 부여를 요청하는 메시지를 표시합니다 .
부여: 권한을 자동으로 부여합니다 .
거부: 권한을 자동으로 거부합니다 .

5. 앱 기능

완전 관리형 기기 또는 직장 프로필의 앱이 앱 기능을 노출하도록 허용되는지 제어합니다 . Android 16 이상이 필요합니다 .
허용됨 (기본값): 완전 관리형 기기 또는 직장 프로필의 앱이 앱 기능을 노출할 수 있습니다.
허용 안 됨: 완전 관리형 기기 또는 직장 프로필의 앱은 앱 기능을 노출할 수 없습니다.

6. 앱 설치 비활성화

사용자의 앱 설치가 비활성화되는지 여부입니다 .

7. 앱 제거 비활성화

사용자의 애플리케이션 제거가 비활성화되는지 여부입니다 .

8. 권한 정책

모든 앱에 대한 명시적 권한 또는 그룹 부여 /거부입니다 . 이러한 값은 기본 권한 정책 설정을 재정의합니다 . 권한 정책 추가 를 사용하여 항목을 만들고 삭제 동작으로 제거하십시오 .
각 항목에는 다음이 포함됩니다 :
Android 권한 /그룹: Android 권한 또는 그룹 (필수)입니다 (예: android.permission.READ_CALENDAR 또는 android.permission_group.CALENDAR).

정책: 부여 / 거부 / 메시지 표시 (기본 권한 정책 과 동일한 정책 옵션 사용).

9. 애플리케이션

정책에 포함해야 하는 애플리케이션 목록입니다 . 목록 콘텐츠의 동작은 Play 스토어 모드 에 설정된 값에 따라 달라집니다 .

Play 스토어 모드 가 허용 목록 으로 설정된 경우 정책에 있는 앱만 사용할 수 있으며 정책에 없는 앱은 기기에서 자동으로 제거됩니다 .

Play 스토어 모드 가 차단 목록 으로 설정된 경우 모든 앱을 사용할 수 있으며 기기에 있으면 안 되는 앱은 애플리케이션 정책에서 차단됨 으로 명시적으로 표시해야 합니다.

새 앱을 추가하려면 애플리케이션 추가 버튼 (또는 애플리케이션 추가 아이콘)을 클릭하고 관리되는 Google Play에서 를 선택한 다음 Play 스토어에서 앱을 선택하고 앱 카드에서 선택 버튼을 클릭하십시오 .

Google Play에 게시되지 않았지만 기기에 이미 있는 앱 (예: 시스템 또는 제조업체 앱)을 추가하려면
애플리케이션 추가 를 클릭하고 패키지 이름으로 (사전 설치된 앱)을 선택한 다음 앱의 패키지 이름 (예: com.example.app)을 입력하고 추가 를 클릭하십시오 .앱은 강제 설치됨 설치 유형으로 추가됩니다 . 키오스크 사용자 지정 런처에 앱을 표시하려면 설치 유형 이 사전 설치됨 또는 강제 설치됨 이어야 합니다. 사용 가능 인 경우 앱이 표시되지 않습니다.

관리되는 Google Play에서 사용할 수 없는 앱은 애플리케이션 목록에서 Android 아이콘으로
표시됩니다 . Google Play에서 설치할 수 없으므로 기기에 이미 있어야 합니다. 앱이 없는 기기에서는
설치할 수 없습니다.

해당 국가의 Play 스토어에 게시된 모든 앱을 기본적으로 선택할 수 있습니다. 자체 비공개 앱 또는 웹
앱을 선택하려면 먼저 시스템에 업로드해야 합니다. 자세한 내용은 비공개 앱 페이지를 참조하십시오 .

각 앱은 카드에 시각적으로 포함된 자체 설정으로 구성할 수 있습니다:

9.1. 설치 유형

앱에 수행할 설치 유형입니다 .

사용 가능: 앱을 설치할 수 있습니다.

사전 설치됨: 앱이 자동으로 설치되며 사용자가 제거할 수 있습니다.

강제 설치됨: 앱이 자동으로 설치되며 사용자가 제거할 수 없습니다.

차단됨: 앱이 차단되어 설치할 수 없습니다. 이전 정책에서 앱이 설치된 경우 제거됩니다 .

설정에 필요: 앱이 자동으로 설치되며 사용자가 제거할 수 없고, 설치가 완료될 때까지 설정이 완료되지 않습니다.

키오스크 : 앱이 키오스크 모드로 자동 설치됩니다 . 기본 홈 인텐트로 설정되고 잠금 작업 모드에 허용 목록으로 등록됩니다 . 앱이 설치될 때까지 기기 설정이 완료되지 않습니다. 설치 후 사용자는 앱을
제거할 수 없습니다. 정책당 하나의 앱에만 이 설치 유형 을 설정할 수 있습니다. 정책에 이 설정이

있으면 상태 표시줄이 자동으로 비활성화됩니다 . 자세한 내용은 전용 키오스크 모드 페이지를
참조하십시오 .

9.2. 설치 제약 조건

앱 설치에 대한 제한 집합을 정의합니다 . 여러 제약 조건을 선택한 경우 앱을 설치하려면 모든 조건을 충족해야 합니다.

이 옵션은 설치 유형 이 사전 설치됨 또는 강제 설치됨 인 경우에만 표시됩니다 .

종량제가 아닌 네트워크 : 기기가 종량제가 아닌 네트워크 (예: Wi‑Fi)에 연결된 경우에만 앱을
설치합니다 .

충전 중: 기기가 충전 중일 때만 앱을 설치합니다 .

유휴 상태: 기기가 유휴 상태일 때만 앱을 설치합니다 .

9.3. 자동 업데이트 모드

앱의 자동 업데이트 모드를 제어합니다 .

기본값: 사용자에 대한 영향을 최소화하기 위해 앱이 낮은 우선순위로 자동 업데이트됩니다 . 다음 제약
조건을 모두 충족하면 앱이 업데이트됩니다 . (1) 기기가 활발하게 사용되지 않음, (2) 기기가 종량제가
아닌 네트워크에 연결됨, (3) 기기가 충전 중임. 개발자가 새 업데이트를 게시한 후 24시간 이내에
기기에 알림이 전송되며, 그 후 위 제약 조건이 충족되는 다음 번에 앱이 업데이트됩니다 .

연기됨: 앱이 오래된 상태가 된 후 최대 90일 동안 자동으로 업데이트되지 않습니다. 앱이 오래된
상태가 된 후 90일이 지나면 사용 가능한 최신 버전이 낮은 우선순위로 자동 설치됩니다 (기본 자동
업데이트 모드 참조). 앱이 업데이트된 후에는 다시 오래된 상태가 된 후 90일이 지날 때까지 자동으로
업데이트되지 않습니다. 사용자는 언제든지 Play 스토어에서 앱을 수동으로 업데이트할 수 있습니다.

높은 우선순위 : 앱이 가능한 한 빨리 업데이트됩니다 . 제약 조건이 적용되지 않습니다. 새 업데이트가
제공되면 기기에 즉시 알림이 전송됩니다 .

9.4. 최소 버전 코드

기기에 실행되는 앱의 최소 버전입니다 . 설정하면 기기는 앱을 최소 이 버전 코드로 업데이트하려고
시도합니다 . 앱이 최신 상태가 아니면 기기에 규정 미준수 세부정보 가 포함되고 규정 미준수 사유 가 APP_NOT_UPDATED(으)로 설정됩니다 . 앱은 이미 이 값 이상의 버전 코드로 Google Play에 게시되어 있어야 합니다. 정책당 최대 20개의 앱이 최소 버전 코드를 지정할 수 있습니다.

9.5. 위임된 범위

Android Device Policy에서 앱에 위임된 범위입니다 . 다른 앱에 특별한 Android 권한 선택 항목을 부여할 수 있습니다:

인증서 설치: 인증서 설치 및 관리에 대한 액세스를 부여합니다 .

관리되는 구성: 관리되는 구성 관리에 대한 액세스를 부여합니다 .

제거 차단: 제거 차단에 대한 액세스를 부여합니다 .

권한: 권한 정책 및 권한 부여 상태에 대한 액세스를 부여합니다 .

패키지 액세스: 패키지 액세스 상태에 대한 액세스를 부여합니다 .

시스템 앱: 시스템 앱 활성화에 대한 액세스를 부여합니다 .

9.6. 우선 네트워크

이 앱에 사용할 우선 네트워크 서비스입니다 . 설정하면 앱이 사용 가능한 경우 연결에 지정된 기업 네트워크 슬라이스를 사용합니다 . 이는 셀룰러 패널의 5G 네트워크 슬라이싱 구성 섹션에서 구성된 네트워크
슬라이스와 일치해야 합니다.

9.7. 기본 권한 정책

앱이 요청하는 모든 권한에 대한 기본 정책입니다 . 지정하면 모든 앱에 적용되는 정책 수준의 기본 권한 정책 을 재정의합니다 . 모든 앱에 적용되는 권한 정책 은 재정의하지 않습니다.

메시지 표시 (기본값): 사용자에게 권한 부여를 요청하는 메시지를 표시합니다 .

부여: 권한을 자동으로 부여합니다 .

거부: 권한을 자동으로 거부합니다 .

9.8. 연결된 직장 및 개인 앱

앱이 사용자 동의를 조건으로 기기의 직장 프로필과 개인 프로필 간에 자체적으로 통신할 수 있는지
제어합니다 (Android 11 이상).

허용 안 됨 (기본값): 앱이 프로필 간에 통신하지 못하도록 합니다.

허용됨: 사용자 동의를 받은 후 앱이 프로필 간에 통신할 수 있도록 합니다.

9.9. Always On VPN 잠금 예외

VPN이 연결되지 않았고 잠금 사용 이 활성 상태일 때 앱의 네트워킹이 허용되는지 지정합니다 . Android 10 이상을 실행하는 기기에서만 지원됩니다 .

강제 적용 (기본값): 앱이 상시 VPN 잠금 설정을 따릅니다.
예외: 앱이 상시 VPN 잠금 설정에서 제외됩니다 .

9.10. 직장 프로필 위젯

직장 프로필에 설치된 앱이 홈 화면에 위젯을 추가할 수 있는지 지정합니다 .
허용됨: 애플리케이션이 홈 화면에 위젯을 추가할 수 있습니다.
허용 안 됨: 애플리케이션이 홈 화면에 위젯을 추가할 수 없습니다.

9.11. 사용자 제어 설정

지정된 앱에 사용자 제어가 허용되는지 지정합니다 . 사용자 제어에는 강제 중지 및 앱 데이터 지우기와 같은 사용자 동작이 포함됩니다 (Android 11 이상). 앱에 extensionConfig가 활성화된 경우 이 설정과 관계없이 사용자 제어가 허용되지 않습니다. 키오스크 앱의 경우 허용됨 을 사용하여 사용자 제어를 허용할 수 있습니다. 지정되지 않음: 사용자 제어 허용 여부를 결정하기 위해 앱의 기본 동작을 사용합니다 .
허용됨: 앱에 사용자 제어가 허용됩니다 .
허용 안 됨: 앱에 사용자 제어가 허용되지 않습니다.

9.12. 사용 안 함

앱이 비활성화되는지 여부입니다 . 비활성화해도 앱 데이터는 유지됩니다 .

9.13. 자격 증명 제공자 허용
Android 14 이상에서 앱이 자격 증명 제공자 역할을 하도록 허용되는지 여부입니다 .

9.14. 관리되는 구성

앱의 관리되는 설정을 구성하려면 관리되는 구성 사용 버튼을 클릭하십시오 . 앱에 관리되는 구성이 이미 설정되어 있으면 관리되는 구성 버튼으로 구성을 수정하거나 구성 제거 버튼으로 삭제할 수 있습니다.

관리되는 구성 옵션은 이 기능을 지원하는 앱에서만 사용할 수 있습니다.

9.15. 권한 정책

앱에 대한 명시적 권한 부여 또는 거부입니다 . 이러한 값은 모든 앱에 적용되는 기본 권한 정책 및 권한 정책 을 재정의합니다 .
권한 정책 추가 를 사용하여 앱 카드에 하나 이상의 권한 규칙을 추가하고 삭제 동작으로 제거하십시오 .

9.16. 트랙 ID

기기가 액세스할 수 있는 앱의 비공개 테스트 트랙 ID 목록입니다 . 여러 트랙 ID를 선택하면 기기는 액세스 가능한 모든 트랙 중 최신 버전을 받습니다. 트랙 ID를 선택하지 않으면 기기는 앱의 프로덕션 트랙에만
액세스할 수 있습니다.

트랙 ID 옵션은 조직에서 사용할 수 있는 트랙 ID가 하나 이상 있는 앱에서만 사용할 수 있습니다. 특정

앱의 비공개 테스트 트랙에 조직을 추가하는 방법에 대한 자세한 내용은 여기 를 참조하십시오 .

10. 기본 애플리케이션 설정

지원되는 유형에 대해 기본 앱을 설정합니다 . 하나 이상의 유형에 기본 앱이 설정되면 해당 프로필에서
사용자가 기본 앱을 변경할 수 없습니다.

기본 애플리케이션 유형 당 하나의 기본 애플리케이션 설정만 허용됩니다 . 기본 애플리케이션
목록에는 중복이 없어야 합니다.

10.1. 기본 애플리케이션 유형

구성할 앱 카테고리를 선택하십시오 (예: 브라우저, 전화, SMS, 지갑 또는 어시스턴트 ). 가용성은 Android 버전 및 관리 모드에 따라 달라집니다 .

10.2. 기본 애플리케이션 범위

기본 앱이 적용될 위치를 선택하십시오 (완전 관리형, 직장 프로필 또는 개인 프로필). 선택한 유형에서
지원하는 범위만 선택할 수 있습니다.

선택한 범위 중 기기의 관리 모드에 적용할 수 있는 범위가 없으면 기기가 규정 비준수 세부 정보를
보고합니다 .

10.3. 기본 애플리케이션

선택한 유형의 기본값으로 설정할 수 있는 앱 목록입니다 . 설치되어 있고 자격을 갖춘 첫 번째 앱이 기본값으로 설정됩니다 .

범위에 완전 관리형 또는 직장 프로필 이 포함된 경우 각 앱은 애플리케이션 목록에도 있어야 하며
설치 유형 이 차단됨 으로 설정되지 않아야 합니다.

11. 개인 키 선택

개인 키 규칙 선택 에 일치하는 규칙이 없을 때 사용자가 개인 키 별칭을 선택할 수 있도록 기기에 UI를 표시하도록 허용합니다 .

Android P 미만의 기기에서는 이 설정을 사용하면 기업 키가 취약해질 수 있습니다.

12. 개인 키 규칙 선택

앱의 개인 키 액세스를 제어합니다 . 이 규칙은 Android Device Policy가 지정된 앱에 부여할 개인 키 (있는 경우)를 결정합니다 . 액세스는 앱이 KeyChain.choosePrivateKeyAlias(또는 모든 오버로드)를 호출하여 지정된 URL에 대한 개인 키 별칭을 요청할 때 부여되거나 , URL별 규칙이 아닌 규칙 (즉, urlPattern이 설정되지 않았거나 빈 문자열 또는 .*로 설정된 경우)의 경우 Android 11 이상에서 앱이 먼저 KeyChain.choosePrivateKeyAlias를 호출하지 않고도 KeyChain.getPrivateKey를 호출할 수 있도록 직접 부여됩니다 . 앱이 KeyChain.choosePrivateKeyAlias를 호출할 때 choosePrivateKeyRules가 두 개 이상 일치하면 마지막으로 일치하는 규칙이 반환할 키 별칭을 정의합니다 .

개인 키 규칙 추가 를 사용하여 항목을 만들고 삭제 동작으로 제거하십시오 .

12.1. 개인 키 별칭

사용할 개인 키의 별칭입니다 .

12.2. URL 패턴

요청 URL과 일치시킬 URL 패턴입니다 . 설정하지 않거나 비어 있으면 모든 URL과 일치합니다 . java.util.regex.Pattern의 정규식 구문을 사용합니다 .

12.3. 패키지 이름

이 규칙이 적용되는 패키지 이름입니다 . 각 앱의 서명 인증서 해시는 Play에서 제공한 해시와 비교하여 확인됩니다 . 패키지 이름을 지정하지 않으면 KeyChain.choosePrivateKeyAlias 또는 모든 오버로드를
호출하는 모든 앱에 별칭이 제공됩니다 (단, Android 11 이상에서도 KeyChain.choosePrivateKeyAlias를 호출하지 않으면 제공되지 않습니다). 여기에 지정된 패키지와 동일한 Android UID를 가진 앱은 KeyChain.choosePrivateKeyAlias를 호출할 때 액세스 권한을 갖습니다.

패키지 이름 추가 를 사용하여 항목을 추가하고 삭제 동작으로 제거하십시오 .

앱을 삭제하려면 앱 카드 하단의 휴지통 아이콘을 클릭하십시오 .

Revision #61
Created 2025-12-17 09:34:23 UTC by Admin
Updated 2026-11-12 09:56:41 UTC by Admin