? ??

이 섹션에서는 앱 사용 가능 여부 , 설치 , 업데이트 및 권한 관리에 관련된 정책을 설정할 수 있습니다 .

> 관리되는 Google Play 계정은 장치가 프로비저닝될 때 자동으로 생성됩니다 .

1. ??? ??? ??

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

허용 목록 (기본값): 정책에 포함된 앱만 사용 가능하며 , 정책에 없는 앱은 자동으로 기기에서 제거됩니다 . Play 스토어에는 사용 가능한 앱만 표시됩니다 .

차단 목록 : 모든 앱이 사용 가능하며 , 기기에 설치되면 안 되는 앱은 애플리케이션 정책에서 명시적으로 차단 해야 합니다 . Play 스토어에서는 차단된 앱을 제외한 모든 앱이 표시됩니다 .

2. ??? ? ?? ? ??

신뢰할 수 없는 앱 (알 수 없는 출처의 앱)에 대한 정책 : 이 설정은 기기에 적용되는 정책으로 , 사용자가 Play 스토어 외부에서 앱을 설치 (사이드로딩)할 수 있는지 여부를 결정하는 Android 시스템 설정을 제어합니다 .

허용 안 함 (기본값): 기기 전체에서 신뢰할 수 없는 앱 설치를 허용하지 않습니다 .

개인 프로필에만 적용 : 업무 프로필이 있는 기기의 경우 , 신뢰할 수 없는 앱 설치를 기기의 개인 프로필에만 허용합니다 .

허용 : 신뢰할 수 없는 앱 설치를 전체 기기에 대해 허용합니다 .

3. Google Play ??

Google Play 보호 앱 검증 강제 여부 .

강제 (기본): 앱 검증을 강제로 활성화합니다 .

사용자 선택 : 사용자가 앱 검증 기능을 활성화할지 여부를 선택할 수 있습니다 .

4. ?? ?? ??

앱의 런타임 권한 요청에 대한 정책입니다 .

프롬프트 (기본값): 사용자가 권한을 부여하도록 알림을 표시합니다 .

허용 : 권한을 자동으로 부여합니다 .

거부 : 권한을 자동으로 거부합니다 .

5. ? ??

완전 관리되는 기기 또는 업무 프로필 내 앱이 앱 기능을 노출할 수 있는지 여부를 제어합니다 . Android 16 이상이 필요합니다 .

허용 (기본값): 완전 관리되는 기기 또는 업무 프로필 내 앱이 앱 기능을 노출할 수 있습니다 .

허용되지 않음 : 완전히 관리되는 기기 또는 업무 프로필 내 앱은 앱 기능을 노출할 수 없습니다 .

6. ??? ? ? ????? ?

사용자가 앱을 설치하는 것을 비활성화할 수 있습니다 .

7. ? ??? ????? ? ????

사용자가 앱을 제거하는 기능을 비활성화할 수 있습니다 .

8. ?? ??

모든 앱에 대해 명시적인 권한 부여 , 그룹 권한 , 또는 권한 거부 설정을 할 수 있습니다 . 이러한 값은 기본 권한 정책 설정을 재정의합니다 .

권한 정책 추가 기능을 사용하여 항목을 생성하고 , 삭제 기능을 통해 항목을 삭제할 수 있습니다 .

각 항목에는 다음이 포함됩니다 :

Android 권한 /그룹 : 필요한 Android 권한 또는 그룹 (필수)입니다 . 예를 들어 **android.permission.READ_CALENDAR** 또는 **android.permission_group.CALENDAR** 입니다 .

정책 : 허용 / 거부 / 요청 (기본 권한 정책 과 동일한 정책 옵션 사용).

9. ??????

정책에 반드시 포함되어야 하는 애플리케이션 목록입니다 . 목록 내용의 동작은 `Play 스토어 모드 에 설정된 값에 따라 달라집니다 .

만약 Play 스토어 모드 가 허용 목록 으로 설정된 경우 , 정책에 포함된 앱만 사용 가능하며 , 정책에 없는 앱은 자동으로 기기에서 제거됩니다 .

만약 Play 스토어 모드 가 블랙리스트 로 설정된 경우 , 모든 앱이 사용 가능하며 , 기기에 설치되어서는 안 되는 앱은 애플리케이션 정책에서 명시적으로 차단 해야 합니다 .

새로운 앱을 추가하려면 , 앱 추가 버튼 (또는 앱 추가 아이콘)을 클릭한 다음 , Play 스토어에서 앱을 선택하고 앱 카드에서 선택 버튼을 클릭하세요 .

> 귀하의 국가에서 Play 스토어에 게시된 모든 앱은 기본적으로 선택 가능합니다 . 비공개 앱 또는 웹 앱을 선택하려면 먼저 해당 앱을 시스템에 업로드해야 합니다 . 자세한 내용은 개인___앱_페이지를 참조하십시오 .

각 앱은 자체 설정으로 구성할 수 있으며 , 이러한 설정은 시각적으로 카드 형태로 표시됩니다

9.1. ?? ??

앱 설치 유형 .

사용 가능 : 앱을 설치할 수 있습니다 .

사전 설치 : 앱은 자동으로 설치되며 , 사용자가 제거할 수 있습니다 .

강제 설치 : 앱은 자동으로 설치되며 , 사용자가 제거할 수 없습니다 .

차단됨 : 앱은 차단되어 설치할 수 없습니다 . 이전 정책에 의해 설치된 경우 , 앱은 제거됩니다 .

설정 필요 : 앱은 자동으로 설치되며 , 사용자가 제거할 수 없고 , 설치가 완료될 때까지 설정 완료를 방해합니다 .

키오스크 : 앱은 자동으로 설치되며 , 키오스크 모드로 설정되며 , 기본 홈 인텐트로 지정되고 , 잠금 작업 모드에 등록됩니다 . 장치 설정은 앱이 설치될 때까지 완료되지 않습니다 . 설치 후에는 사용자가 앱을 제거할 수 없습니다 . 이 설치 유형 은 정책당 하나의 앱에만 적용할 수 있습니다 . 이 설정이 정책에 포함된 경우 , 상태 표시줄이 자동으로 비활성화됩니다 . 자세한 내용은 관련 키오스크_____모드___ 페이지를 참조하십시오 .

9.2. ?? ?? ??

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

> 이 옵션은 "설치 유형 "이 "미리 설치 " 또는 "강제 설치 "인 경우에만 표시됩니다 .

제한 없는 네트워크 : 앱은 장치가 제한 없는 네트워크 (예 : Wi-Fi)에 연결되어 있을 때만 설치됩니다 .

충전 중 : 앱은 장치가 충전 중일 때만 설치됩니다 .

유휴 상태 : 앱은 장치가 유휴 상태일 때만 설치됩니다 .

9.3. ?? ???? ??

앱의 자동 업데이트 모드를 제어합니다 .

기본 설정 : 앱은 사용자에게 미치는 영향을 최소화하기 위해 낮은 우선순위로 자동으로 업데이트됩니다 . 앱은 다음 조건을 모두 충족할 때 업데이트됩니다 . (1) 장치가 현재 사용 중이지 않음 , (2) 장치가 데이터 요금이 부과되지 않는 네트워크에 연결되어 있음 , (3) 장치가 충전 중임 . 개발자가 새 업데이트를 게시한 후 24시간 이내에 장치에 업데이트가 있다는 알림이 표시되며 , 이후 위 조건을 충족하는 경우 앱이 업데이트됩니다 .

연기 : 앱은 최신 버전이 출시된 후 최대 90일 동안 자동으로 업데이트되지 않습니다 . 최신 버전이 출시된 후 90일이 지나면 , 최신 버전이 자동으로 설치되지만 우선 순위가 낮습니다 (기본 자동 업데이트 모드 참조 : 기본 자동 업데이트 모드). 앱이 업데이트된 후 , 다시 최신 버전이 출시될 때까지는 90일 동안 자동으로 업데이트되지 않습니다 . 사용자는 언제든지 Play 스토어에서 앱을 수동으로 업데이트할 수 있습니다 .

우선순위 높음 : 앱은 가능한 한 빨리 업데이트됩니다 . 어떤 제약도 적용되지 않으며 , 새로운 업데이트가 제공되면 즉시 장치에 알림이 전송됩니다 .

9.4. ?? ?? ??

이 설정은 장치에서 실행되는 앱의 최소 버전을 지정합니다 . 설정된 경우 , 장치는 앱을 최소 해당 버전 코드 이상으로 업데이트하려고 시도합니다 . 앱이 최신 버전이 아니면 , 장치에는 비준수 세부 정보 와 비준수 사유 가 **APP_NOT_UPDATED**로 설정되어 표시됩니다 . 앱은 이 값 이상의 버전 코드로 이미 Google Play에 게시되어 있어야 합니다 . 정책당 최대 20개의 앱에서 최소 버전 코드를 지정할 수 있습니다 .

9.5. ??? ?? ??

Android 기기 정책에서 앱에 위임된 권한 범위입니다 . 다른 앱에 특정 Android 권한을 부여할 수 있습니다

인증서 설치 : 인증서 설치 및 관리에 대한 접근 권한을 부여합니다 .

관리 구성 : 관리 구성 설정 및 관리에 대한 접근 권한을 부여합니다 .

앱 제거 방지 : 앱 제거 방지 기능에 대한 접근 권한을 부여합니다 .

권한 : 권한 정책 및 권한 부여 상태에 대한 접근 권한을 제공합니다 .

패키지 접근 권한 : 패키지 접근 권한 상태에 대한 접근 권한을 부여합니다 .

시스템 앱 : 시스템 앱 활성화를 위한 접근 권한을 부여합니다 .

9.6. ?? ?? ????

이 앱에서 사용할 우선 네트워크 서비스입니다 . 설정된 경우 , 앱은 사용 가능한 경우 지정된 기업 네트워크 슬라이스를 사용하여 연결을 수행합니다 . 이는 **5G** 네트워크 슬라이싱 구성 섹션의 셀룰러 패널에 구성된 네트워크 슬라이스와 일치해야 합니다 .

9.7. 기본 권한 정책

이 설정은 앱에서 요청하는 모든 권한에 대한 기본 정책입니다 . 지정된 경우 , 이 설정은 모든 앱에 적용되는 정책 레벨의 기본 권한 정책 를 대체합니다 . 하지만 모든 앱에 적용되는 권한 정책 는 대체하지 않습니다 .

프롬프트 (기본값): 사용자가 권한을 부여하도록 알림을 표시합니다 .

허용 : 권한을 자동으로 부여합니다 .

거부 : 권한을 자동으로 거부합니다 .

9.8. ??? ?? ?? ? ??

사용자 동의 하에 , 앱이 기기의 업무용 및 개인용 프로필 간에 자체적으로 통신할 수 있는지 여부를 제어합니다 (Android 11 이상).

허용되지 않음 (기본값): 앱이 프로필 간에 통신하는 것을 방지합니다 .

허용 : 사용자의 동의를 얻은 후 앱이 프로필 간에 통신할 수 있도록 허용합니다 .

9.9. ?? ??? VPN? ?? ?? ??

VPN이 연결되지 않았거나 잠금 기능이 활성화된 상태에서도 앱이 네트워크를 사용할 수 있는지 여부를 지정합니다 . Android 10 이상을 실행하는 기기에서만 지원됩니다 .

강제 (기본값): 앱은 항상 연결된 VPN 보안 설정을 준수합니다 .

예외 : 이 앱은 항상 연결된 VPN 보안 설정에서 제외됩니다 .

9.10. ?? ??? ??

작업 프로필에 설치된 앱이 홈 화면에 위젯을 추가할 수 있는지 여부를 지정합니다 .

허용 : 이 애플리케이션은 홈 화면에 위젯을 추가할 수 있습니다 .

허용되지 않음 : 이 애플리케이션은 홈 화면에 위젯을 추가할 수 없습니다 .

9.11. ??? ?? ??

특정 앱에 대해 사용자 제어가 허용되는지 여부를 지정합니다 . 사용자 제어에는 앱 강제 종료 및 앱 데이터 삭제와 같은 사용자 작업이 포함됩니다 (Android 11 이상). 앱에 **extensionConfig**가 활성화된 경우 , 이 설정에 관계없이 사용자 제어가 허용되지 않습니다 . 키오스크 앱의 경우 , 허용 을 사용하여 사용자 제어를 허용할 수 있습니다 .

지정되지 않음 : 앱의 기본 동작을 사용하여 사용자 제어가 허용되는지 또는 제한되는지를 결정합니다 .

허용 : 앱에 대한 사용자 제어가 허용됩니다 .

허용되지 않음 : 이 앱에 대한 사용자 제어는 허용되지 않습니다 .

9.12. ?????

앱이 비활성화되었는지 여부 . 비활성화된 경우에도 앱 데이터는 보존됩니다 .

9.13. ?? ?? ??? ??? ?????

Android 14 이상 버전에서 앱이 자격 증명 공급자 역할을 수행할 수 있는지 여부 .

9.14. ?? ??

앱의 관리 설정 구성을 하려면 , 관리 구성 활성화 버튼을 클릭하세요 . 앱에 이미 관리 구성이 설정되어 있는 경우 , 관리 구성 버튼을 사용하여 구성을 수정하거나 , 구성 삭제 버튼을 사용하여 삭제할 수 있습니다 .

> 관리 구성 기능은 해당 기능을 지원하는 앱에만 제공됩니다 .

9.15. ?? ??

앱에 대한 명시적인 권한 허용 또는 거부 설정입니다 . 이러한 값은 모든 앱에 적용되는 기본 권한 정책 및 권한 정책 을 대체합니다 .

앱 카드에 대한 권한 규칙을 추가하려면 추가 권한 정책 을 사용하고 , 삭제 작업을 통해 해당 규칙을 제거할 수 있습니다 .

9.16. ?? ID

앱의 클로즈드 테스트 트랙 ID 목록입니다 . 기기가 액세스할 수 있는 트랙 ID는 다음과 같습니다 . 여러 트랙 ID 가 선택된 경우 , 기기는 액세스 가능한 모든 트랙 중에서 최신 버전을 받습니다 . 트랙 ID가 선택되지 않은 경우 , 기기는 앱의 프로덕션 트랙만 사용할 수 있습니다 .

> 트랙 **ID** 옵션은 조직에서 사용할 수 있는 트랙 ID가 하나 이상 있는 앱에만 제공됩니다 . 특정 앱에 대한 클로즈드 테스트 트랙에 조직을 추가하는 방법에 대한 자세한 내용은 여기 에서 확인하세요 .

10. ?? ? ??

지원되는 유형에 대해 기본 앱을 설정합니다 . 최소 하나의 유형에 대해 기본 앱이 설정된 경우 , 사용자는 해당 프로필에서 기본 앱을 변경할 수 없습니다 .

> 각 기본 애플리케이션 유형 에 대해 기본 애플리케이션 설정은 하나만 허용됩니다 . 기본 애플리케이션 목록에는 중복 항목이 포함되어서는 안 됩니다 .

10.1. ?? ?????? ??

설정할 앱 범주를 선택하세요 (예 : 브라우저 , 다이얼러 , SMS, 지갑 또는 어시스턴트). 사용 가능 여부는 Android 버전 및 관리 모드에 따라 다릅니다 .

10.2. ?? ?????? ??

기본 앱을 적용할 위치를 선택하세요 (전체 관리 , 업무 프로필 또는 개인 프로필). 선택한 유형에서 지원하는 범위만 선택할 수 있습니다 .

> 선택한 범위 중 하나라도 장치의 관리 모드에 적용되지 않으면 , 장치는 규정 미준수 상태임을 알립니다 .

10.3. ?? ??????

선택한 유형에 대해 기본으로 설정할 수 있는 앱 목록입니다 . 설치되어 있고 해당 조건을 충족하는 첫 번째 앱이 기본 앱으로 설정됩니다 .

> 만약 권한에 완전 관리 또는 작업 프로필 이 포함되어 있다면 , 각 앱은 애플리케이션 목록에 존재해야 하며 , 설치 유형 이 차단 으로 설정되어 있으면 안 됩니다 .

11. ?? ? ??

개인 키 선택 규칙에 일치하는 항목이 없을 경우 , 사용자가 개인 키 별칭을 선택할 수 있도록 장치에 UI를 표시할 수 있습니다 . 개인 키 선택 규칙 .

> Android P 이전 버전의 기기에서는 이 설정을 변경하면 기업용 키가 보안에 취약해질 수 있습니다 .

12. ?? ? ??? ?????

개인 키에 대한 앱의 접근 권한을 제어합니다 . 이 규칙은 Android 장치 정책에서 지정된 앱에 어떤 개인 키 (있는 경우)를 부여할지 결정합니다 . 앱이 특정 URL에 대한 개인 키 별칭을 요청하기 위해 KeyChain.choosePrivateKeyAlias (또는 해당 오버로드)를 호출하거나 , Android 11 이상에서 urlPattern이

설정되지 않았거나 , 빈 문자열이거나 , ".*"인 URL에 특정되지 않은 규칙의 경우 , 앱이 KeyChain.getPrivateKey를 직접 호출할 수 있도록 접근 권한을 부여합니다 . 앱이 KeyChain.choosePrivateKeyAlias를 호출할 때 , 일치하는 choosePrivateKeyRules가 여러 개 있는 경우 , 마지막으로 일치하는 규칙이 반환할 키 별칭을 정의합니다 .

개인 키 규칙 추가 기능을 사용하여 항목을 만들고 , 삭제 기능을 사용하여 항목을 삭제할 수 있습니다 .

12.1. ?? ? ??

사용할 개인 키의 별명입니다 .

12.2. ??? URL ?????

요청 URL과 일치하는 URL 패턴입니다 . 설정하지 않거나 비워두면 모든 URL과 일치합니다 . java.util.regex.Pattern의 정규 표현식 구문을 사용합니다 .

12.3. ??? ??

해당 규칙이 적용되는 패키지 이름입니다 . 각 앱의 서명 인증서 해시가 Play에서 제공하는 해시와 비교하여 검증됩니다 . 패키지 이름을 지정하지 않으면 KeyChain.choosePrivateKeyAlias 또는 이 메서드의 모든 변형을 호출하는 모든 앱에 대해 해당 별칭이 제공됩니다 (하지만 KeyChain.choosePrivateKeyAlias를 호출하지 않으면 적용되지 않습니다 . Android 11 이상에서도 마찬가지입니다). 여기에 지정된 패키지와 동일한 Android UID를 가진 모든 앱은 KeyChain.choosePrivateKeyAlias를 호출할 때 접근 권한을 갖습니다 .

패키지 이름 을 추가하여 항목을 등록하고 , 삭제 기능을 사용하여 항목을 제거할 수 있습니다 .

> 앱을 삭제하려면 , 앱 카드 하단의 휴지통 아이콘을 클릭하세요 .

Revision #40
Created 2025-12-17 09:34:23 UTC by Admin
Updated 2026-04-22 15:52:05 UTC by Admin