정책 - Android

- 요약
- 앱 관리
- 키오스크 모드
- 보안
- 멀티미디어
- 셀룰러
- 네트워킹
- 시스템
- 위치 및 지오펜스
- 사용자 관리
- 개인 사용
- 교차 프로필 정책
- 상태 보고
- 기타
- 규정 준수 규칙

요약
Android 정책은 시스템의 핵심 엔터티로, 관리되는 기기에 적용되고 시행되는 규칙을 정의합니다 .

대시보드의 정책 섹션에서 정책을 찾아보고 새 정책을 만들 수 있습니다. Android 정책을 열려면 표에서 정책 행을 클릭하세요 . 시스템이 정책 편집기 페이지를 엽니다.

정책은 등록 토큰 과 연결할 수 있으며, 그러면 프로비저닝 과정에서 기기에 자동으로 적용됩니다 . 프로비저닝 후에도 기기에 할당된 정책을 변경할 수 있습니다.

각 기기는 한 번에 하나의 정책에만 연결할 수 있습니다.

많은 정책 옵션은 특정 기기 유형 (완전 관리형, 전용, 작업 프로필) 및 Android 버전에만 적용됩니다 .
지원되지 않는 설정은 기기에서 무시되거나 규정 미준수로 보고될 수 있습니다.

정책 편집기 레이아웃
정책 편집기는 확장 가능한 섹션 집합으로 구성됩니다 . 페이지 상단에서는 항상 다음을 편집할 수 있습니다:

이름 (필수)
ID (읽기 전용)
설명 (선택 사항)

아래 섹션은 정책 편집기 패널 (예: 앱 관리, 보안, 네트워킹, 시스템, 개인 사용, 교차 프로필 정책 등)과 일치합니다 . 저장된 정책을 열면 설정이 변경된 섹션은 이미 열려 있고 나머지는 닫혀 있습니다. 이 설명서의
장 페이지를 사용하여 각 패널을 자세히 이해하세요 .

저장, 삭제 및 연결된 기기
정책 저장 을 사용하여 변경 사항을 적용하세요 . 보류 중인 편집이 없거나 라이선스가 만료된 경우 버튼이 비활성화됩니다 .

기존 정책 (ID가 있음)을 연 경우 페이지 하단에 정책 삭제 작업과 연결된 기기 목록이 표시되어 현재 해당 정책을 사용 중인 기기 수를 확인할 수 있습니다.

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 .

□□ □□□□□ □ □□ □□□ □□□ □□□□ □□□□□□ .

키오스크 모드
키오스크 모드를 사용하면 기기의 기능을 단일 앱 또는 여러 앱으로 제한할 수 있습니다. 단일 앱과 다중 앱 키오스크 모드 중 선택은 비즈니스 목표에 따라 달라집니다 .

단일 앱 키오스크 모드 에서는 기기가 단일 애플리케이션용으로 구성되며 최종 사용자가 기기의 다른 앱에 액세스할 수 없습니다. 또한 앱을 종료할 수 없으므로 해당 특정 앱을 위한 전용 기기가 됩니다. 이 모드를

사용하려면 앱 관리 섹션에서 앱을 지정하고 설치 유형 을 키오스크 로 설정합니다 .

다중 앱 키오스크 모드 에서는 기기에서 여러 애플리케이션에 액세스할 수 있습니다. 최종 사용자는 사용자 지정 런처를 통해 여러 앱 사이를 탐색할 수 있습니다. 이 모드를 사용하려면 키오스크 사용자 지정 런처 옵션을 켭니다.

키오스크 모드가 활성화되면 최종 사용자가 시스템 설정 및 상태 표시줄과 같은 특정 시스템 기능에 액세스할 수 있는지도 구성할 수 있습니다.

키오스크 사용자 지정 런처

키오스크 사용자 지정 런처가 활성화되었는지 여부입니다 . 이 옵션은 홈 화면을 앱 관리 설정을 통해 설치된 앱만 사용하도록 기기를 잠그는 런처로 대체합니다 . 앱은 단일 페이지에 알파벳순으로 표시됩니다 .

전원 버튼 동작

키오스크 모드에서 사용자가 전원 버튼을 길게 눌렀을 때 기기의 동작을 설정합니다 .

사용 가능 (기본값): 키오스크 모드의 기기에서 사용자가 전원 버튼을 길게 누르면 전원 메뉴 (예: 전원 끄기, 다시 시작)가 표시됩니다 .

차단됨: 키오스크 모드의 기기에서 사용자가 전원 버튼을 길게 눌러도 전원 메뉴 (예: 전원 끄기, 다시 시작)가 표시되지 않습니다. 참고: 이 경우 사용자가 기기를 끌 수 없게 될 수 있습니다.

시스템 오류 경고

키오스크 모드에서 충돌했거나 응답하지 않는 앱에 대한 시스템 오류 대화상자를 차단할지 여부를 지정합니다 . 차단되면 시스템은 사용자가 UI에서 "앱 닫기 " 옵션을 선택한 것처럼 앱을 강제 종료합니다 .

차단됨 (기본값): 충돌 및 앱 응답 없음 (ANR)과 같은 모든 시스템 오류 대화상자가 차단됩니다 . 차단되면 시스템은 사용자가 UI에서 앱을 닫은 것처럼 앱을 강제 종료합니다 .
활성화: 충돌 및 앱 응답 없음 (ANR)과 같은 모든 시스템 오류 대화상자가 표시됩니다 .

시스템 탐색
키오스크 모드에서 활성화되는 탐색 기능 (예: 홈, 개요 버튼)을 지정합니다 .
비활성화 (기본값): 홈 및 개요 버튼에 액세스할 수 없습니다.
홈만: 홈 버튼만 활성화됩니다 .
활성화: 홈 및 개요 버튼이 활성화됩니다 .

상태 표시줄
키오스크 모드에서 시스템 정보 및 알림이 비활성화되는지 여부를 지정합니다 .
비활성화 (기본값): 키오스크 모드에서 시스템 정보 및 알림이 비활성화됩니다 .
시스템만 : 상태 표시줄에 시스템 정보만 표시됩니다 .
활성화: 키오스크 모드에서 상태 표시줄에 시스템 정보 및 알림이 표시됩니다 . 참고: 이 정책을
적용하려면 kioskCustomization.systemNavigation을 사용하여 기기의 홈 버튼을 활성화해야 합니다.

기기 설정
키오스크 모드에서 설정 앱이 허용되는지 여부를 지정합니다 .
허용 (기본값): 키오스크 모드에서 설정 앱에 대한 액세스가 허용됩니다 .
차단됨: 키오스크 모드에서 설정 앱에 대한 액세스가 허용되지 않습니다.

보안
이 섹션에서는 보안 관련 정책을 구성할 수 있습니다.

보안 위험 작업

상태 보고서에서 기기가 SecurityRisk를 보고할 때 수행할 작업을 선택하세요 .

지원되는 SecurityRisk 유형:

알 수 없는 OS: Play Integrity API가 기기에서 알 수 없는 OS가 실행 중임을 감지합니다
(basicIntegrity 검사는 성공하지만 ctsProfileMatch는 실패).

손상된 OS: Play Integrity API가 기기에서 손상된 OS가 실행 중임을 감지합니다 (basicIntegrity 검사 실패).

하드웨어 기반 평가 실패: 기기 무결성 필드에 MEETS_STRONG_INTEGRITY 레이블이 표시되지
않으면 Play Integrity API가 기기에 강력한 시스템 무결성 보장이 없음을 감지합니다 .

사용 가능한 작업:

회사 데이터 초기화 (기본값): 등록을 해제하고 업무 데이터를 초기화합니다 (완전 관리형이면 전체
기기, 프로필 소유이면 작업 프로필만).

작업 없음: 기기를 등록된 상태로 두고 자동으로 아무 작업도 수행하지 않습니다.

회사 데이터 초기화 를 선택하면 초기화 옵션도 구성할 수 있습니다:

초기화 보호 유지: 기기를 초기화할 때 초기화 보호 (FRP) 데이터를 유지합니다 .

외부 저장소 초기화: 초기화를 수행할 때 기기의 외부 저장소 (예: SD 카드)도 추가로 초기화합니다 .

eSIM 초기화: 회사 소유 기기의 경우 기기를 초기화할 때 기기에서 모든 eSIM을 제거합니다 . 개인
소유 기기의 경우 기기에서 관리되는 eSIM(ADD_ESIM 명령을 통해 추가된 eSIM)을 제거하며, 개인
소유 eSIM은 제거되지 않습니다.

1. 최대 잠금 시간

기기가 잠길 때까지 사용자 활동에 허용되는 최대 시간 (초)입니다. 값이 0이면 제한이 없습니다.

2. 충전 중 켜짐 유지

기기가 켜진 상태를 유지하는 배터리 연결 모드입니다 . 이 설정을 사용할 때는 기기가 켜진 상태에서
자체적으로 잠기지 않도록 최대 잠금 시간 을 지우는 것이 좋습니다.

AC 충전기: 전원이 AC 충전기입니다 .

USB 포트: 전원이 USB 포트입니다 .

무선 충전기: 전원이 무선입니다 .

3. 키가드 비활성화됨

true이면 기본 및 /또는 보조 디스플레이의 잠금 화면을 비활성화합니다 . 이 정책은 전용 기기 관리 모드에서만 지원됩니다 .

4. 비밀번호 요구 사항

비밀번호 요구 사항 정책입니다 .

비밀번호 요구 사항 구성 을 사용하여 하나 이상의 비밀번호 요구 사항 블록을 추가하세요 . 모두 지우기 를 사용하여 구성된 모든 비밀번호 요구 사항을 제거하세요 .

비밀번호 요구 사항은 자동 범위 (단일 요구 사항) 또는 별도의 기기 /작업 프로필 범위를 사용할 수 있습니다. 복잡성 기반 요구 사항은 동일한 범위의 품질 기반 요구 사항과 함께 사용해야 합니다.

4.1. 범위

비밀번호 요구 사항이 적용되는 범위입니다 .

자동: 범위가 지정되지 않습니다. 비밀번호 요구 사항은 작업 프로필 기기의 경우 작업 프로필에, 완전
관리형 또는 전용 기기의 경우 전체 기기에 적용됩니다 .

기기: 비밀번호 요구 사항이 기기에만 적용됩니다 .

작업 프로필: 비밀번호 요구 사항이 작업 프로필에만 적용됩니다 .

4.2. 비밀번호 기록 길이

비밀번호 기록의 길이입니다 . 이 필드를 설정하면 사용자는 기록에 있는 비밀번호와 동일한 새 비밀번호를 입력할 수 없습니다. 값이 0이면 제한이 없습니다.

4.3. 초기화 전 최대 비밀번호 실패 횟수

기기가 초기화되기 전까지 입력할 수 있는 잘못된 기기 잠금 해제 비밀번호 횟수입니다 . 값이 0이면 제한이 없습니다.

4.4. 비밀번호 만료 시간 (일)

이 설정은 지정된 일수가 지나면 사용자에게 정기적으로 비밀번호를 업데이트하도록 강제합니다 .

4.5. 비밀번호 잠금 해제 필요

기기 또는 작업 프로필이 강력한 인증 방식 (비밀번호, PIN, 패턴)으로 잠금 해제된 후 다른 인증 방식 (예: 지문, 신뢰 에이전트, 얼굴)으로 잠금 해제할 수 있는 기간입니다 . 지정된 기간이 지나면 강력한 인증 방식만
사용하여 기기 또는 작업 프로필의 잠금을 해제할 수 있습니다.

기기 기본값: 시간 제한이 기기 기본값으로 설정됩니다 .

매일: 시간 제한이 24시간으로 설정됩니다 .

4.6. 비밀번호 품질

필요한 비밀번호 품질입니다 .

복잡성 높음: 높은 비밀번호 복잡성 등급을 다음과 같이 정의합니다 . Android 12 이상: 반복 (4444)
또는 연속 (1234, 4321, 2468) 시퀀스가 없는 PIN, 길이 8 이상, 영문자 길이 6 이상, 영숫자 길이 6 이상.

복잡성 보통: 보통 비밀번호 복잡성 등급을 다음과 같이 정의합니다 . 반복 (4444) 또는 연속 (1234, 4321, 2468) 시퀀스가 없는 PIN, 길이 4 이상, 영문자 길이 4 이상, 영숫자 길이 4 이상.

복잡성 낮음: 낮은 비밀번호 복잡성 등급을 다음과 같이 정의합니다 . 패턴, 반복 (4444) 또는 연속 (1234, 4321, 2468) 시퀀스가 있는 PIN.

없음: 비밀번호 요구 사항이 없습니다.

약함: 기기는 최소한 보안 수준이 낮은 생체 인식 기술로 보호되어야 합니다. 여기에는 개인 신원을 인식할 수 있는 기술로서 대략 3자리 PIN과 동등한 수준 (오탐률 1,000분의 1 미만)의 기술이 포함됩니다 .

아무거나 : 비밀번호가 필요하지만 비밀번호에 포함되어야 하는 내용에 대한 제한은 없습니다.

숫자: 비밀번호에 숫자 문자가 포함되어야 합니다.
숫자 복합: 비밀번호에 반복 (4444) 또는 연속 (1234, 4321, 2468) 시퀀스가 없는 숫자 문자가 포함되어야 합니다.
영문자: 비밀번호에 영문자 (또는 기호) 문자가 포함되어야 합니다.
영숫자: 비밀번호에 숫자와 영문자 (또는 기호) 문자가 모두 포함되어야 합니다.
복합: 비밀번호는 passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols 등에 지정된 최소 요구 사항을 충족해야 합니다. 예를 들어 passwordMinimumSymbols가 2이면 비밀번호에 기호가 2개 이상 포함되어야 합니다.

4.7. 최소 길이
허용되는 최소 비밀번호 길이입니다 . 값이 0이면 제한이 없습니다.

4.8. 최소 영문자 수

비밀번호에 필요한 최소 영문자 수입니다.

4.9. 최소 소문자 수

비밀번호에 필요한 최소 소문자 수입니다.

4.10. 최소 대문자 수

비밀번호에 필요한 최소 대문자 수입니다.

4.11. 최소 비영문자 수
비밀번호에 필요한 최소 비영문자 (숫자 또는 기호) 수입니다.

4.12. 최소 숫자 자릿수

비밀번호에 필요한 최소 숫자 자릿수입니다 .

4.13. 최소 기호 수

비밀번호에 필요한 최소 기호 수입니다.

4.14. 통합 잠금
작업 프로필이 있는 Android 9 이상을 실행하는 기기에서 기기와 작업 프로필에 통합 잠금을 허용할지 여부를 제어합니다 . 다른 기기에는 영향을 주지 않습니다.
통합 잠금 허용: 기기와 작업 프로필에 공통 잠금을 허용합니다 .

별도 업무 잠금 필요: 작업 프로필에 별도 잠금이 필요합니다 .

5. 초기화 비활성화됨

설정에서 초기화가 비활성화되어 있는지 여부입니다 . 완전 관리형 기기에만 적용됩니다 .

6. 초기화 보호

초기화 보호를 위한 기기 관리자 이메일 주소입니다 . 기기에서 승인되지 않은 초기화가 발생하면 이러한
관리자 중 한 명이 Google 계정 이메일과 비밀번호로 로그인하여 기기의 잠금을 해제해야 합니다. 관리자를 지정하지 않으면 기기에서 초기화 보호가 제공되지 않습니다. 완전 관리형 기기에만 적용됩니다 .
관리자 이메일: 초기화 보호 사용 을 사용하여 관리자 구성을 시작하세요 . 그런 다음 관리자 이메일 추가 를 사용하여 주소를 추가하고 삭제 작업으로 제거하세요 .

7. 키가드 기능

비활성화할 수 있는 키가드 (잠금 화면) 기능입니다 .

7.1. 모두 비활성화
현재 및 향후 모든 키가드 사용자 지정을 비활성화합니다 .

7.2. 카메라 비활성화
보안 키가드 화면 (예: PIN)에서 카메라를 비활성화합니다 .

7.3. 알림 비활성화

보안 키가드 화면에서 모든 알림 표시를 비활성화합니다 .

7.4. 마스킹되지 않은 알림 비활성화

보안 키가드 화면에서 마스킹되지 않은 알림을 비활성화합니다 .

7.5. 신뢰 에이전트 상태 무시

보안 키가드 화면에서 신뢰 에이전트 상태를 무시합니다 .

7.6. 지문 비활성화

보안 키가드 화면에서 지문 센서를 비활성화합니다 .

7.7. 알림에 텍스트 입력 비활성화

보안 키가드 화면에서 알림에 텍스트 입력을 비활성화합니다 .

7.8. 얼굴 인증 비활성화

보안 키가드 화면에서 얼굴 인증을 비활성화합니다 .

7.9. 홍채 인증 비활성화

보안 키가드 화면에서 홍채 인증을 비활성화합니다 .

7.10. 모든 생체 인증 비활성화

보안 키가드 화면에서 모든 생체 인증을 비활성화합니다 .

7.11. 모든 바로가기 비활성화
Android 14 이상의 보안 키가드 화면에서 모든 바로가기를 비활성화합니다 .

멀티미디어
이 섹션에서는 카메라 /마이크 동작, USB 데이터 액세스, 인쇄, 디스플레이 관련 제한을 구성할 수 있습니다.

1. 카메라 액세스

카메라 사용 여부와 사용자가 카메라 액세스 토글에 액세스할 수 있는지 (Android 12+)를 제어합니다 . 일반적으로 카메라 비활성화는 완전 관리형 기기에서는 기기 전체에 적용되고, 직장 프로필 기기에서는 직장 프로필 내에서만 적용됩니다 .

사용자 선택 (기본값): 기본 기기 동작입니다 . 카메라를 사용할 수 있으며 (Android 12+) 사용자가
카메라 액세스를 토글할 수 있습니다.

비활성화 : 모든 카메라가 비활성화됩니다 (완전 관리형: 기기 전체, 직장 프로필: 직장 프로필 앱에만
해당). 카메라 액세스 토글은 관리 범위에서 효과가 없습니다.

강제 적용: 카메라를 사용할 수 있습니다. Android 12+를 실행하는 완전 관리형 기기에서는 사용자가
카메라 액세스를 토글할 수 없습니다. 다른 기기 /버전에서는 사용자 선택과 동일하게 동작합니다 .

2. 마이크 액세스

완전 관리형 기기에서 마이크 사용 여부와 사용자가 마이크 액세스 토글에 액세스할 수 있는지 (Android 12+) 를 제어합니다 . 이 설정은 완전 관리형이 아닌 기기에서는 효과가 없습니다.

사용자 선택 (기본값): 기본 동작입니다 . 마이크를 사용할 수 있으며 (Android 12+) 사용자가 마이크
액세스를 토글할 수 있습니다.

비활성화 : 마이크가 비활성화됩니다 (기기 전체). 마이크 액세스 토글은 효과가 없습니다.

강제 적용: 마이크를 사용할 수 있습니다. Android 12+에서는 사용자가 마이크 액세스를 토글할 수 없습니다. Android 11 이하에서는 사용자 선택과 동일하게 동작합니다 .

3. USB 데이터 액세스

USB를 통해 전송할 수 있는 파일 및 /또는 데이터를 제어합니다 . 회사 소유 기기에서만 지원됩니다 .

파일 전송 허용 안 함 (기본값): 파일 전송은 허용되지 않지만 다른 USB 데이터 연결 (예: 마우스 / 키보드)은 허용됩니다 .

데이터 전송 허용 안 함: 모든 유형의 USB 데이터 전송이 금지됩니다 (USB HAL 1.3+의 Android 12+). 지원되지 않으면 기기는 파일 전송 허용 안 함으로 대체됩니다 .

데이터 전송 허용: 모든 유형의 USB 데이터 전송이 허용됩니다 .

4. 인쇄

인쇄가 허용되는지 제어합니다 (Android 9+).

허용 (기본값): 인쇄가 허용됩니다 .

허용 안 함: 인쇄가 허용되지 않습니다 (Android 9+).

5. 화면 밝기 설정

화면 밝기 모드와 (선택적으로) 밝기 값을 제어합니다 .

화면 밝기 모드:

사용자 선택 (기본값): 사용자가 화면 밝기를 구성할 수 있습니다.

자동: 밝기가 자동으로 설정되며 사용자가 변경할 수 없습니다. 자동 조정의 일부로 사용되는 밝기 값을
설정할 수는 있습니다 (완전 관리형 Android 9+, 회사 소유 Android 15+의 직장 프로필).

고정: 밝기가 구성된 값으로 설정되며 사용자가 변경할 수 없습니다. 밝기 값이 필요합니다 (완전 관리형 Android 9+, 회사 소유 Android 15+의 직장 프로필).

화면 밝기:

1~255 범위의 값입니다 (1 = 가장 낮음, 255 = 가장 높음). 값이 0이면 밝기 값이 설정되지 않은
것입니다.

6. 화면 시간 초과 설정

사용자가 화면 시간 초과를 구성할 수 있는지와, 강제 적용 시 시간 초과 값을 제어합니다 .

화면 시간 초과 모드 필드에서 사용자 제어와 강제 적용 동작 중 하나를 선택합니다 .

사용자 선택 (기본값): 사용자가 화면 시간 초과를 구성할 수 있습니다.
강제 적용: 화면 시간 초과가 구성된 값으로 설정되며 사용자가 변경할 수 없습니다 (완전 관리형
Android 9+, 회사 소유 Android 15+의 직장 프로필).
화면 시간 초과:
시간 초과 기간 (초)입니다. 값은 0보다 커야 합니다. 최대 잠금 시간 보다 크면 시스템이 값을 제한하고
규정 미준수를 보고할 수 있습니다.

7. 화면 캡처 비활성화

화면 캡처가 비활성화되었는지 여부입니다 .

8. 볼륨 조정 비활성화

마스터 볼륨 조정이 비활성화되었는지 여부입니다 .

9. 물리적 미디어 마운트 비활성화

물리적 외부 미디어 마운트가 비활성화되었는지 여부입니다 .

셀룰러
이 섹션에서는 셀룰러 관련 정책을 구성할 수 있습니다.

1. 비행기 모드

사용자가 비행기 모드를 전환할 수 있는지 여부를 제어합니다 .

사용자 선택 (기본값): 사용자가 비행기 모드를 켜거나 끌 수 있습니다.

사용 안 함: 비행기 모드가 비활성화됩니다 . 사용자가 비행기 모드를 켤 수 없습니다. Android 9 이상에서 지원됩니다 .

2. 셀룰러 2G

사용자가 셀룰러 2G 설정을 전환할 수 있는지 여부를 제어합니다 .

사용자 선택 (기본값): 사용자가 셀룰러 2G를 켜거나 끌 수 있습니다.

사용 안 함: 셀룰러 2G가 비활성화됩니다 . 사용자가 설정을 통해 셀룰러 2G를 켤 수 없습니다.
Android 14 이상에서 지원됩니다 .

3. APN 재정의

재정의 APN이 활성화되는지 비활성화되는지 제어합니다 . 활성화하면 구성된 재정의 APN만 사용되며 기기의 다른 모든 APN은 무시됩니다 .

비활성화 (기본값): 구성된 모든 APN 설정은 기기에 저장되지만 비활성화되어 적용되지 않습니다.
기기의 다른 모든 APN은 계속 사용됩니다 .

활성화: 재정의 APN만 사용되며 다른 모든 APN은 무시됩니다 . 이 설정은 Android 10 이상의 완전
관리형 기기에서만 구성할 수 있습니다.

4. APN 설정

하나 이상의 APN 항목을 구성합니다 . APN 추가 를 사용하여 항목을 만들고 APN 제거 를 사용하여
삭제합니다 .

각 APN에는 필수 필드가 있습니다:

APN 유형: 이 APN에 사용할 트래픽 유형을 하나 이상 선택합니다 (관리 모드 및 Android 버전에 따라
지원 여부가 달라짐).

APN 이름: 이동통신사에서 제공하는 APN 식별자입니다 .

표시 이름: UI에 표시되는 알아보기 쉬운 이름입니다 .

선택적 APN 필드:

인증 유형, 사용자 이름, 비밀번호 : 통신사 인증을 구성합니다 (필요한 경우).

프로토콜 및 로밍 프로토콜 : IP 프로토콜 구성입니다 .

네트워크 유형: APN이 사용할 수 있는 셀룰러 기술을 제한합니다 (예: LTE/5G NR).

프록시 주소 및 프록시 포트: 데이터 트래픽용 HTTP 프록시입니다 (해당하는 경우).

MMS 프록시 주소, MMS 프록시 포트, MMSC(MMS 센터 URI): MMS 관련 설정입니다 .

숫자 사업자 ID(MCC+MNC) 및 통신사 ID: 통신사 식별 필드입니다 .

상시 연결 설정: 이 APN으로 활성화된 PDU 세션을 상시 연결로 유지할지 여부입니다 . Android 15
이상에서 지원됩니다 .

MVNO 유형: 이동 가상 네트워크 사업자 식별자 유형입니다 .

MTU IPv4 및 MTU IPv6: IPv4/IPv6 경로의 최대 전송 단위입니다 . Android 13 이상에서 지원됩니다 .

5. 셀 브로드캐스트 구성 비활성화

셀 브로드캐스트 구성이 비활성화되었는지 여부입니다 .

6. 모바일 네트워크 구성 비활성화

모바일 네트워크 구성이 비활성화되었는지 여부입니다 .

7. 로밍 데이터 비활성화

로밍 데이터 서비스가 비활성화되었는지 여부입니다 .

8. 발신 전화 비활성화

발신 전화가 비활성화되었는지 여부입니다 .

9. SMS 비활성화

SMS 메시지 송수신이 비활성화되었는지 여부입니다 .

10. 5G 네트워크 슬라이싱 구성

기업용 5G 네트워크 슬라이싱을 사용하려면 우선 네트워크 서비스 설정을 구성합니다 . 최대 5개의 기업 슬라이스를 설정하고 애플리케이션을 특정 네트워크에 할당하여 트래픽 라우팅을 최적화할 수 있습니다.

10.1. 기본 우선 네트워크

애플리케이션 목록에 없는 애플리케이션 또는 앱의 우선 네트워크 가 설정되지 않은 애플리케이션에 대한 기본 우선 네트워크 ID입니다. 지정된 네트워크 ID에 대한 구성이 있어야 합니다 (우선 네트워크 없음 으로 설정된 경우 제외).

참고: com.google.android.apps.work.clouddpc 및 com.google.android.gms와 같은 중요한
앱은 이 기본 설정에서 제외됩니다 .

10.2. 네트워크 서비스 구성

네트워크 구성 추가 를 사용하여 슬라이스 구성을 만듭니다. 최대 5개의 구성을 추가할 수 있습니다. 각 구성에는 다음이 포함됩니다 :

우선 네트워크 ID(자동 할당): 네트워크 ID는 자동으로 할당되며 변경할 수 없습니다.

기본 연결로 대체: 기기 전체 기본 네트워크로의 대체가 허용되는지 여부입니다 . 허용되지 않으면 5G 슬라이스를 사용할 수 없을 때 앱이 인터넷에 액세스할 수 없습니다.

일치하지 않는 네트워크 : 이 구성이 적용되는 앱이 우선 서비스 이외의 네트워크를 사용할 수 있는지
여부입니다 . 허용 안 함 으로 설정하면 기본 연결로 대체 도 허용 안 함 이어야 합니다. Android 14
이상이 필요합니다 .

네트워킹
이 섹션에서는 네트워킹 관련 정책을 구성할 수 있습니다.

Wi‑Fi 구성은 WiFi 구성 을 통해 시스템에서 프로비저닝하고 관리할 수 있습니다. Wi‑Fi 구성 에
설정된 값에 따라 사용자는 네트워크 추가 /수정에 대한 제어 권한이 제한되거나 전혀 없을 수 있습니다.

기기 라디오 상태

1. Wi‑Fi 상태

Wi‑Fi의 현재 상태와 사용자가 상태를 변경할 수 있는지 제어합니다 .

사용자 선택 (기본값): 사용자가 Wi‑Fi를 활성화 /비활성화할 수 있습니다.

활성화: Wi‑Fi가 켜져 있으며 사용자가 끌 수 없습니다 (Android 13+).

비활성화 : Wi‑Fi가 꺼져 있으며 사용자가 켤 수 없습니다 (Android 13+).

2. 최소 Wi‑Fi 보안 수준

기기가 연결할 수 있는 Wi‑Fi 네트워크의 최소 필수 보안 수준입니다 . Android 13 이상의 완전 관리형 기기 및 회사 소유 기기의 직장 프로필에서 지원됩니다 .

개방형 네트워크 (기본값): 기기가 모든 유형의 Wi‑Fi 네트워크에 연결할 수 있습니다.

개인 네트워크 : 개방형 Wi‑Fi 네트워크를 허용하지 않으며 최소 개인 보안 (예: WPA2‑PSK)이
필요합니다 .

기업 네트워크 : 기업 EAP 네트워크가 필요하며 이 보안 수준 미만의 Wi‑Fi 네트워크는 허용하지
않습니다.

192‑비트 기업 네트워크 : 192‑비트 기업 네트워크가 필요하며 가장 엄격한 옵션입니다 .

3. 초광대역 (UWB) 상태

초광대역 설정의 상태와 사용자가 이를 켜거나 끌 수 있는지 제어합니다 .

사용자 선택 (기본값): 사용자가 UWB를 켜거나 끌 수 있습니다.

비활성화 : UWB가 비활성화되며 사용자가 설정을 통해 토글할 수 없습니다 (Android 14+).

기기 연결 관리

4. Bluetooth 공유

Bluetooth 공유가 허용되는지 제어합니다 .

허용: Bluetooth 공유가 허용됩니다 (완전 관리형 기기에서 기본값, Android 8+).

허용 안 함: Bluetooth 공유가 허용되지 않습니다 (직장 프로필에서 기본값, Android 8+).

5. Wi‑Fi 구성

Wi‑Fi 구성 권한을 제어합니다 . 선택한 옵션에 따라 사용자가 Wi‑Fi 네트워크 구성에 대해 완전한 권한, 제한된 권한 또는 권한 없음을 갖습니다.

Wi‑Fi 구성 허용 (기본값): 사용자가 Wi‑Fi를 구성할 수 있습니다.

Wi‑Fi 구성 추가 허용 안 함: 새 Wi‑Fi 구성을 추가할 수 없습니다. 사용자는 이미 구성된 네트워크
간에 전환할 수 있습니다 (Android 13+, 완전 관리형 및 회사 소유 직장 프로필).

Wi‑Fi 구성 허용 안 함: Wi‑Fi 네트워크 구성을 허용하지 않습니다. 완전 관리형 기기의 경우 사용자가
구성한 네트워크를 제거하고 WiFi 구성 을 통해 구성된 네트워크만 유지합니다 . 회사 소유 직장
프로필의 경우 기존 네트워크는 영향을 받지 않지만 사용자가 Wi‑Fi 네트워크를 추가 /제거 /수정할 수 없습니다.

Wi‑Fi 구성이 비활성화되어 있고 부팅 시 기기가 연결할 수 없으면 시스템에서 네트워크 이스케이프
해치 를 표시하여 사용자가 일시적으로 연결하고 정책을 새로 고칠 수 있도록 할 수 있습니다.

6. Wi‑Fi 다이렉트 설정

Wi-Fi 다이렉트 설정 구성 및 사용을 제어합니다 . Android 13 이상을 실행하는 회사 소유 기기에서 지원됩니다 .

허용 (기본값): 사용자가 Wi-Fi 다이렉트를 사용할 수 있습니다 .

허용 안 함 : 사용자가 Wi-Fi 다이렉트를 사용할 수 없습니다 .

7. 테더링 설정

테더링 설정을 제어합니다 . 설정된 값에 따라 사용자는 다양한 형태의 테더링 사용이 부분적으로 또는 완전히 제한됩니다 .

모든 테더링 허용 (기본값): 모든 형태의 테더링 구성 및 사용을 허용합니다 .

Wi-Fi 테더링 허용 안 함 : 사용자가 Wi-Fi 테더링을 사용할 수 없습니다 (회사 소유 Android 13+).

모든 테더링 허용 안 함 : 모든 형태의 테더링을 허용하지 않습니다 (완전 관리형 + 회사 소유 직장 프로필).

8. Wi-Fi SSID 정책

기기가 연결할 수 있는 Wi-Fi SSID에 대한 제한입니다 (기기에 구성할 수 있는 네트워크에는 영향을 주지 않음). Android 13 이상을 실행하는 회사 소유 기기에서 지원됩니다 .

SSID 차단 목록 (기본값): SSID가 목록에 있는 Wi-Fi 네트워크에는 연결할 수 없지만 다른 네트워크에는 연결할 수 있습니다 .

SSID 허용 목록 : 나열된 SSID에만 연결할 수 있습니다 . SSID 목록은 비워 둘 수 없습니다 .

SSID 추가 를 사용하여 항목을 추가합니다 . 선택한 정책 유형에 따라 목록이 허용 또는 거부된 SSID로 해석됩니다 .

정책 편집기 UI에서 SSID 목록은 허용 목록의 경우 허용된 **Wi-Fi SSID**, 차단 목록의 경우 거부된 **Wi-Fi SSID**로 표시됩니다 .

9. Wi-Fi 로밍 설정

SSID별로 Wi-Fi 로밍 모드를 구성합니다 . **Wi-Fi** 로밍 설정 추가 를 사용하여 항목을 만듭니다 .

각 항목에는 다음이 포함됩니다 :

SSID: 로밍 설정이 적용되는 SSID입니다 (필수).
Wi‑Fi 로밍 모드: 기본 / 비활성화 / 적극적. 비활성화 및 적극적은 Android 15+가 필요하며 완전
관리형 기기 및 회사 소유 기기의 직장 프로필에서만 지원됩니다 .

네트워크 제한

10. Bluetooth 비활성화

Bluetooth가 비활성화되었는지 여부입니다 . Bluetooth 구성 비활성화는 사용자가 우회할 수 있으므로 이 설정을 더 권장합니다 .

11. Bluetooth 연락처 공유 비활성화

Bluetooth 연락처 공유가 비활성화되었는지 여부입니다 .

12. Bluetooth 구성 비활성화

Bluetooth 구성이 비활성화되었는지 여부입니다 .

13. 네트워크 재설정 비활성화

네트워크 설정 재설정이 비활성화되었는지 여부입니다 .

14. 발신 빔 비활성화

NFC를 사용하여 앱에서 데이터를 빔으로 전송하는 것이 비활성화되었는지 여부입니다 .

VPN

15. 상시 연결 VPN 앱

지정된 관리 앱의 데이터가 항상 구성된 VPN을 통해 전송되도록 하려면 상시 연결 VPN 패키지 이름을 지정합니다 .

참고: 이 기능을 사용하려면 상시 연결 및 앱별 VPN 기능을 모두 지원하는 VPN 클라이언트를 배포해야 합니다.

16. VPN 잠금

VPN이 연결되지 않은 경우 네트워킹을 허용하지 않습니다.

17. VPN 구성 비활성화

VPN 구성이 비활성화되었는지 여부입니다 .

프록시 및 네트워크 서비스

18. 우선 네트워크 서비스

직장 프로필에서 우선 네트워크 서비스가 활성화되는지 제어합니다 . 예를 들어 조직이 이동통신사와 협약하여 직장 데이터를 기업용 전용 통신사 네트워크 서비스 (예: 5G 네트워크의 기업 슬라이스)를 통해 전송할 수 있습니다. 이 설정은 완전 관리형 기기에는 영향을 주지 않습니다.

비활성화 : 직장 프로필에서 우선 네트워크 서비스가 비활성화됩니다 .

활성화: 직장 프로필에서 우선 네트워크 서비스가 활성화됩니다 .

기업 네트워크 슬라이싱을 사용하는 경우 5G 네트워크 슬라이싱 구성 을 Cellular 정책 패널에서도
구성하고 우선 네트워크 설정을 사용하여 앱을 슬라이스에 할당합니다 .

19. 권장 글로벌 프록시

네트워크 독립적인 글로벌 HTTP 프록시입니다 . 일반적으로 프록시는 WiFi 구성에서 네트워크별로 구성해야 합니다. 글로벌 프록시는 일반 내부 필터링과 같은 특수한 구성에 유용할 수 있습니다. 글로벌 프록시는 권장 사항일 뿐이며 일부 앱은 이를 무시할 수 있습니다.
비활성화
직접 프록시
프록시 자동 구성 (PAC)

19.1. 호스트

직접 프록시의 호스트입니다 .

19.2. 포트

직접 프록시의 포트입니다 .

19.3. PAC URI
프록시를 구성하는 데 사용되는 PAC 스크립트의 URI입니다.

19.4. 제외된 호스트
직접 프록시의 경우 프록시가 우회되는 호스트입니다 . 호스트 이름에는 *.example.com과 같은
와일드카드가 포함될 수 있습니다.
제외된 호스트 추가 를 사용하여 항목을 추가하세요 (직접 프록시에만 사용 가능).

WiFi 구성
시스템이 기기에 적용할 Wi‑Fi 네트워크 구성을 정의합니다 . Wi‑Fi 구성 추가 를 사용하여 항목을 만들고 삭제 작업으로 제거하세요 .

20. Wi‑Fi 구성 필드

각 구성에는 다음이 포함됩니다 :
구성 이름: 필수입니다 .
SSID: 필수입니다 .
자동 연결: 범위 내에 있을 때 네트워크에 자동으로 연결할지 여부입니다 .

고속 전환: 클라이언트가 네트워크와 함께 고속 전환 (IEEE 802.11r-2008)을 사용하려고 시도할지 여부입니다 .
숨겨진 SSID: SSID를 브로드캐스트할지 여부입니다 .
MAC 무작위화 모드: 하드웨어 또는 자동 (Android 13 이상).

20.1. 보안
Wi‑Fi 보안 옵션:
WEP‑PSK: WEP(사전 공유 키).
WPA‑PSK: WPA/WPA2/WPA3-Personal(사전 공유 키).
WPA‑EAP: WPA/WPA2/WPA3-Enterprise(확장 가능 인증 프로토콜).
WPA3 192비트 모드: WPA3 192비트 모드만 허용하는 WPA‑EAP 네트워크입니다 .

20.2. 암호 문구 (사전 공유 키)

보안이 WEP‑PSK 또는 WPA‑PSK일 때 표시됩니다 . 암호 문구는 필수입니다 .

20.3. EAP 방식 (엔터프라이즈)
보안이 WPA‑EAP 또는 WPA3 192비트 모드 일 때 표시됩니다 . EAP 외부 방식을 하나 선택하세요 : EAP‑TLS
EAP‑TTLS
PEAP
EAP‑SIM
EAP‑AKA

20.4. 2단계 인증
터널링 외부 방식 (EAP‑TTLS 및 PEAP)에 표시됩니다 . MSCHAPv2
PAP

20.5. 사용자의 EAP 자격 증명

활성화하면 시스템이 기기에서 사용자별로 EAP 자격 증명을 자동 적용합니다 . 사용자 섹션에서 사용자 자격 증명을 구성할 수 있습니다 .

20.6. 클라이언트 인증서

EAP-TLS의 경우 Wi-Fi 인증에 사용되는 클라이언트 인증서를 할당할 수 있습니다 . 자세한 내용은 인증서___ 관리___ 페이지를 참조하세요 .

인증서가 이미 할당된 경우 인증서 열기 를 사용하여 확인하거나 인증서 변경 을 사용하여 다른 인증서를 선택할 수 있습니다 .

또는 Android 키체인에 저장되어 Wi-Fi 인증에 허용된 클라이언트 인증서를 참조하는 클라이언트 인증서 키 쌍 별칭 을 지정할 수 있습니다 .

> 클라이언트 인증서 와 클라이언트 인증서 키 쌍 별칭 이 모두 설정된 경우 키 쌍 별칭은 무시됩니다 .

20.7. ID

사용자의 ID입니다 . 터널링 외부 프로토콜 (PEAP, EAP-TTLS)의 경우 터널 내부 인증에 사용되며 , 터널 외부의 EAP ID에는 익명 **ID**가 사용됩니다 . 비터널링 외부 프로토콜의 경우 EAP ID에 사용됩니다 .

20.8. 익명 ID

터널링 프로토콜에만 적용되며 , 외부 프로토콜에 제시되는 사용자의 ID를 나타냅니다 .

20.9. 비밀번호

사용자의 비밀번호입니다 . 지정하지 않으면 기본적으로 사용자에게 입력하라는 메시지가 표시됩니다 .

20.10. 서버 CA 인증서

호스트의 인증서 체인을 확인하는 데 사용할 CA 인증서 목록입니다 . 하나 이상의 CA 인증서가 일치해야 합니다 . 자세한 내용은 인증서___관리___ 페이지를 참조하세요 .

서버 **CA** 인증서 추가 를 사용하여 항목을 추가하고 삭제 작업으로 제거하세요 .

20.11. 도메인 접미사 일치

서버 도메인 이름에 대한 제약 조건 목록입니다 . 항목은 인증 서버 인증서의 대체 주체 이름 DNS 이름에 대한 접미사 일치 요구 사항으로 사용됩니다 .

시스템
이 섹션에서는 시스템 관련 정책을 구성할 수 있습니다.

1. 최소 API 레벨

허용되는 최소 Android API 레벨입니다 .

2. 암호화 정책

암호화가 활성화되어 있는지 여부입니다 .
기본값: 이 값은 무시되며, 즉 암호화가 필요하지 않습니다.
비밀번호 없이 사용: 암호화는 필요하지만 부팅 시 비밀번호가 필요하지 않습니다. 비밀번호와 함께 사용: 암호화가 필요하며 부팅 시 비밀번호가 필요합니다 .

3. 자동 날짜 및 시간

회사 소유 기기에서 자동 날짜, 시간 및 시간대가 활성화되어 있는지 여부입니다 .
사용자 선택 (기본값): 자동 날짜, 시간 및 시간대를 사용자가 선택하도록 합니다.
강제 적용: 기기에서 자동 날짜, 시간 및 시간대를 강제 적용합니다 .

4. 개발자 설정

개발자 설정 (개발자 옵션 및 안전 부팅)에 대한 액세스를 제어합니다 .
사용 안 함 (기본값): 모든 개발자 설정을 비활성화하고 사용자가 해당 설정에 액세스하지 못하도록
합니다.
허용됨: 모든 개발자 설정을 허용합니다 . 사용자는 설정에 액세스하고 선택적으로 구성할 수 있습니다.

5. Common Criteria 모드

정보 기술 보안 평가를 위한 공통 평가 기준 (CC)에 정의된 보안 표준인 Common Criteria 모드를 제어합니다 . Common Criteria 모드를 사용하도록 설정하면 기기의 특정 보안 구성 요소가 강화됩니다 (예: Bluetooth 장기 키의 AES-GCM 암호화, 일부 네트워크 인증서에 대한 추가 검증, 암호화 정책 무결성 검사). Common Criteria 모드는 Android 11 이상을 실행하는 회사 소유 기기에서만 지원됩니다 . 경고: Common Criteria 모드는 일반적으로 매우 민감한 조직에만 필요한 엄격한 보안 모델을 적용합니다 . 표준 기기 사용이 영향을
받을 수 있으므로 필요한 경우에만 사용하도록 설정하세요 .

사용 안 함 (기본값): Common Criteria 모드를 비활성화합니다 .

사용: Common Criteria 모드를 사용하도록 설정합니다 .

6. Memory Tagging Extension (MTE)

기기에서 Memory Tagging Extension(MTE)을 제어합니다 .

사용자 선택 (기본값): 사용자는 기기에서 MTE를 사용하거나 사용하지 않도록 선택할 수 있습니다 (
기기가 지원하는 경우).

적용됨: MTE가 사용 설정되며 사용자가 변경할 수 없습니다 (Android 14 이상, 전체 관리형 기기 및
회사 소유 기기의 직장 프로필에서 지원).

사용 안 함: MTE가 비활성화되어 있으며 사용자가 변경할 수 없습니다 (Android 14 이상, 전체 관리형
기기에서만 지원).

7. 콘텐츠 보호

콘텐츠 보호 (기만적인 앱을 검사하는 기능)의 사용 여부를 제어합니다 . Android 15 이상에서 지원됩니다 .

사용 안 함 (기본값): 콘텐츠 보호가 비활성화되어 있으며 사용자가 변경할 수 없습니다.

적용됨: 콘텐츠 보호가 사용 설정되어 있으며 사용자가 변경할 수 없습니다 (Android 15 이상).

사용자 선택: 콘텐츠 보호가 정책에 의해 제어되지 않으며 사용자가 선택할 수 있습니다 (Android 15 이상).

8. 어시스트 콘텐츠

AssistContent를 어시스턴트 앱 (예: Circle to Search)과 같은 권한 있는 앱으로 보낼 수 있는지 여부를 제어합니다 . AssistContent에는 스크린샷과 패키지 이름 같은 앱 정보가 포함됩니다 . Android 15 이상에서 지원됩니다 .

허용됨 (기본값): 어시스트 콘텐츠를 권한 있는 앱으로 보낼 수 있습니다 (Android 15 이상).

허용 안 함: 어시스트 콘텐츠를 권한 있는 앱으로 보내는 것이 차단됩니다 (Android 15 이상).

9. 창 생성 사용 안 함

앱 창 외에 창 생성이 비활성화되는지 여부입니다 . 이 옵션을 사용하면 다음 시스템 UI가 표시되지 않습니다: 토스트 및 스낵바, 전화 활동 (수신 전화 등) 및 우선순위 전화 활동 (진행 중인 통화 등), 시스템 알림, 시스템 오류 및 시스템 오버레이.

10. 네트워크 이스케이프 해치

네트워크 이스케이프 해치의 사용 여부입니다 . 부팅 시 네트워크 연결을 설정할 수 없는 경우 이스케이프
해치가 사용자에게 메시지를 표시하여 기기 정책을 새로 고치기 위해 일시적으로 네트워크에 연결하도록 합니다. 정책을 적용한 후 임시 네트워크는 잊혀지고 기기는 부팅을 계속합니다 . 이렇게 하면 마지막 정책에 적합한 네트워크가 없고 기기가 잠금 작업 모드의 앱으로 부팅되거나 사용자가 기기 설정에 액세스할 수 없는 경우 네트워크에 연결하지 못하는 상황을 방지할 수 있습니다.

11. 기본 활동

특정 인텐트 필터와 일치하는 인텐트를 처리하기 위한 기본 활동 목록입니다 . 예를 들어 IT 관리자는 이 기능을 통해 웹 링크를 자동으로 여는 브라우저 앱이나 홈 버튼을 탭할 때 사용되는 런처 앱을 선택할 수 있습니다.

기본 활동 추가 를 사용하여 항목을 만듭니다. 항목 내에서 작업 추가 및 카테고리 추가 를 사용하여 인텐트 필터를 구성합니다 .

11.1. 수신자 활동

기본 인텐트 처리기가 되어야 하는 활동입니다 . 이는 Android 구성 요소 이름 (예: com.android.enterprise.app/.MainActivity)이어야 합니다. 또는 앱의 패키지 이름일 수 있으며, 이 경우 Android Device Policy가 인텐트를 처리하기 위해 앱에서 적절한 활동을 선택합니다 .

11.2. 작업

필터에서 일치시킬 인텐트 작업입니다 . 필터에 작업이 포함된 경우 일치하려면 인텐트의 작업이 해당 값 중 하나여야 합니다. 작업이 포함되지 않은 경우 인텐트 작업은 무시됩니다 .

11.3. 카테고리

필터에서 일치시킬 인텐트 카테고리입니다 . 인텐트에는 필요한 카테고리가 포함되며, 일치하려면 해당
카테고리가 모두 필터에 포함되어야 합니다. 즉, 필터에 카테고리를 추가해도 해당 카테고리가 인텐트에
지정되지 않는 한 일치에 영향을 주지 않습니다.

12. 허용된 입력 방법

허용된 입력 방법을 지정합니다 .

모두 허용: 제한이 적용되지 않습니다. 모든 입력 방법이 허용됩니다 .

시스템 기본만: 시스템에 기본 제공되는 입력 방법만 허용됩니다 .

시스템 기본 및 제공된 항목만: 제공된 입력 방법과 시스템에 기본 제공되는 입력 방법만 허용됩니다 .

12.1. 허용된 입력 방법

허용된 입력 방법 패키지 이름입니다 . 허용된 입력 방법 이 시스템 기본 및 제공된 항목만 으로 설정된
경우에만 적용됩니다 .

입력 방법 추가 를 사용하여 항목을 추가하고 삭제 작업으로 제거합니다 .

13. 허용된 접근성 서비스

허용된 접근성 서비스를 지정합니다 .

모두 허용: 모든 접근성 서비스를 사용할 수 있습니다.

시스템 기본만: 시스템에 기본 제공되는 접근성 서비스만 사용할 수 있습니다.

시스템 기본 및 제공된 항목만: 제공된 접근성 서비스와 시스템에 기본 제공되는 접근성 서비스만
사용할 수 있습니다.

13.1. 허용된 접근성 서비스

허용된 접근성 서비스입니다 . 허용된 접근성 서비스 가 시스템 기본 및 제공된 항목만 으로 설정된
경우에만 적용됩니다 .

접근성 서비스 추가 를 사용하여 항목을 추가하고 삭제 작업으로 제거합니다 .

14. 시스템 업데이트 정책

시스템 업데이트 관리를 위한 구성입니다 .

기본: 사용자가 시스템 업데이트를 수락해야 하는 일반적으로 기본 업데이트 동작을 따릅니다.

자동: 업데이트가 제공되는 즉시 자동으로 설치합니다 .

기간 지정: 일일 유지 관리 기간 내에 자동으로 설치합니다 . 또한 이 설정은 Play 앱이 해당 기간 내에 업데이트되도록 구성합니다 . 포그라운드에 지속적으로 고정된 앱을 Play에서 업데이트할 수 있는
유일한 방법이므로 키오스크 기기에 특히 권장됩니다 .

연기: 자동 설치를 최대 30일까지 연기합니다 .

14.1. 유지 관리 기간 (Windowed 전용)

시스템 업데이트 정책 이 Windowed로 설정된 경우 from 및 to 필드를 사용하여 일일 유지 관리 기간을
정의할 수 있습니다.

14.2. 시스템 업데이트 동결 기간

기기에서 실행되는 OS 버전을 동결하기 위해 무선 (OTA) 시스템 업데이트가 연기되는 매년 반복되는
기간입니다 . 기기가 무기한 동결되는 것을 방지하려면 각 동결 기간은 최소 60일 간격으로 구분되어야 합니다. 각 동결 기간은 90일을 초과할 수 없습니다.

시스템 업데이트 동결 기간 추가 를 사용하여 항목을 만듭니다.

15. 자격 증명 제공자 기본값

Android 14 이상에서 자격 증명 제공자 역할을 할 수 있는 앱을 제어합니다 .

허용 안 함 (기본값): credentialProviderPolicy가 지정되지 않은 앱은 자격 증명 제공자 역할을 할 수 없습니다.

시스템 제외 허용 안 함: credentialProviderPolicy가 지정되지 않은 앱은 OEM 기본 자격 증명
제공자를 제외하고 자격 증명 제공자 역할을 할 수 없습니다.

위치 및 지오펜스
이 패널은 기기 위치 보고, 위치 적용, 지오펜스 정의를 제어하는 Android 정책 설정을 모읍니다. Cerberus Enterprise가 기기 위치를 수집하거나 기기가 구성된 영역에 들어오거나 나가는 것을 감지하도록 하려면 이 패널을 사용합니다 .

위치 보고

위치 보고

기기 지오로케이션 보고를 활성화합니다 . 이 설정을 통해 수집된 위치 데이터는 대시보드 위치 지도, 기기 개요 위치 기록, 지오펜스 처리에 사용됩니다 .

위치 기록과 지오펜스 이벤트는 90일 동안 보존되며, 이보다 오래된 데이터는 매일 밤 자동으로
삭제됩니다 . 등록된 각 기기의 최신 위치는 항상 보존되므로 지도에 계속 표시됩니다 .

완전히 관리되지 않는 기기에서는 위치 데이터가 Cerberus Enterprise 앱에 필요한 위치 권한이
있는지와 기기의 위치 서비스가 활성화되어 있는지에 따라 달라질 수 있습니다.

개인 Apple 기기 (사용자 등록)에서는 위치 및 지오펜스가 기본적으로 꺼져 있습니다. Apple 정책에서
개인 기기의 위치 및 지오펜스 가 켜져 있고 사용자가 Cerberus Enterprise 앱에 대해 위치를 허용한 경우에만 사용할 수 있습니다.

위치 모드

회사 소유 기기의 기기 위치 설정을 제어합니다 .

사용자 선택: 위치 서비스가 정책에 의해 제한되지 않습니다.
강제 적용: 기기에서 위치 서비스가 활성화됩니다 .
비활성화 : 기기에서 위치 서비스가 비활성화됩니다 .

위치 공유 비활성화

직장 앱의 위치 공유를 비활성화합니다 . 프로필 소유자 기기에서는 직장 프로필에 영향을 줍니다. 완전 관리형 기기에서는 기기 전체의 위치를 비활성화하고 기기 위치 모드를 재정의합니다 .

활성 지오펜스가 있을 때의 자동 동작
활성 지오펜스가 작동하려면 위치 보고가 필요합니다 . 하나 이상의 지오펜스가 활성 상태이면 Cerberus Enterprise가 관련 위치 설정을 자동으로 일관되게 유지합니다 .

위치 보고 는 활성 지오펜스가 있는 동안 강제로 켜집니다.
위치 모드 가 강제 적용 으로 강제 설정됩니다 .
위치 공유 비활성화 가 강제로 해제됩니다 .

하나 이상의 지오펜스가 활성 상태일 때 위치 보고 를 비활성화하려고 하면 Cerberus Enterprise가 확인 대화상자를 표시합니다 . 계속하면 정책의 모든 활성 지오펜스가 비활성화됩니다 .

지오펜스 목록
정책에는 최대 10개의 지오펜스 를 포함할 수 있습니다. 지오펜스 이름은 정책 내에서 고유해야 합니다.

지오펜스 추가 를 사용하여 새 항목을 만듭니다. 각 지오펜스에는 다음과 같은 주요 필드가 있습니다:

이름: 필수이며 고유해야 합니다.
위도 및 경도: 영역의 중심입니다 .
반경 (m): 필수이며 200~10000미터입니다 .
설명: 관리자를 위한 선택적 메모입니다 .
진입 보고 및 이탈 보고: 생성할 전환 이벤트를 선택합니다 .
활성: 지오펜스를 삭제하지 않고 활성화 또는 비활성화합니다 .

각 지오펜스에서 진입 보고 또는 이탈 보고 중 하나 이상이 활성 상태로 유지되어야 합니다.

이전에는 최소 반경이 100미터였습니다 . 200미터보다 작은 기존 지오펜스는 계속 작동하며,
이동하거나 이름을 변경하더라도 정책을 저장할 때 그대로 유지됩니다 . 반경을 변경하면 최소 200 미터여야 합니다.

지도 편집 도구

각 지오펜스 카드에는 해당 영역의 지도 미리보기가 포함됩니다 . 지도나 숫자 필드에서 형상을 편집할 수 있습니다.

영역 편집이 잠금 해제된 경우 지도를 클릭하여 지오펜스 중심을 이동합니다 .
현재 위치 버튼을 사용하여 지도를 현재 브라우저 위치로 중심에 맞춥니다.
지도 재중심 버튼을 사용하여 해당 지오펜스의 기본 보기로 복원합니다 .
잠금 버튼을 사용하여 지오펜스 형상이 실수로 변경되지 않도록 합니다.

지오펜스 데이터가 표시되는 위치

지오펜스 전환은 Android 기기 개요 페이지의 위치 패널에 있는 지오펜스 탭에서 검토할 수 있습니다. 이 탭에서는 전용 지도에 필터링 도구 및 전환 목록과 함께 전환이 표시됩니다 .

사용자 관리

사용자 추가 사용 안 함
새 사용자 및 프로필 추가가 비활성화되는지 여부입니다 . managementMode가 DEVICE_OWNER인 기기의 경우 이 필드는 무시되며 사용자는 사용자를 추가하거나 제거할 수 없습니다.

계정 수정 사용 안 함
계정 추가 또는 제거가 비활성화되는지 여부입니다 .

사용자 자격 증명 구성 사용 안 함
사용자 자격 증명 구성이 비활성화되는지 여부입니다 .

사용자 제거 사용 안 함
다른 사용자 제거가 비활성화되는지 여부입니다 .

사용자 아이콘 설정 사용 안 함
사용자 아이콘 변경이 비활성화되는지 여부입니다 .

배경 화면 설정 사용 안 함
배경 화면 변경이 비활성화되는지 여부입니다 .

회사 계정 설정 인증
회사 계정 설정 중 사용자가 인증하는 방식을 제어합니다 . 이 옵션은 관리 Google 도메인 (Google Workspace)으로 지원되는 Android 엔터프라이즈에서만 사용할 수 있습니다.

기기 설정 /등록 중에 이 정책은 회사 계정 로그인이 필요한지 여부에 영향을 주지만, Google Admin Console 설정인 Google을 사용하여 인증 및 등록 토큰 유형에 따라 인증이 여전히 필요할 수 있습니다.

이미 등록된 기기의 경우 이 정책은 기기가 관리 Google Play 계정으로 관리되는 경우 (즉, Google 등록을 사용하여 인증 없이 등록된 경우)에만 적용됩니다 .

자세한 내용과 문제 해결은 Google 등록을 사용하여 인증 을 참조하세요 .

차단된 계정 유형

사용자가 관리할 수 없는 계정 유형입니다 . 이 옵션은 기기 사용자가 승인되지 않은 계정을 추가하지 못하도록 합니다.

차단된 계정 유형 추가 를 사용하여 하나 이상의 계정 유형을 추가합니다 .

각 항목에는 계정 유형 필드 (필수)가 있습니다. com.google과 같은 문자열을 입력합니다 . 삭제 작업을 사용하여 항목을 제거합니다 .

개인 사용

회사 소유 기기를 업무 및 개인 용도로 프로비저닝 할 때 작업 프로필 외부에서 사용자가 개인 용도로 기기를 운영하는 방식을 제한하는 규칙을 지정할 수 있습니다.

이 섹션은 작업 프로필이 있는 회사 소유 기기에만 적용됩니다 . 완전 관리형 또는 개인 소유 기기에는
영향을 주지 않습니다.

1. 카메라 비활성화됨

카메라가 비활성화되어 있는지 여부입니다 .

2. 화면 캡처 비활성화됨

화면 캡처가 비활성화되어 있는지 여부입니다 .

3. 최대 업무 중지 일수

작업 프로필을 꺼 둘 수 있는 기간을 제어합니다 .

4. Bluetooth 공유

작업 프로필이 있는 회사 소유 기기의 개인 프로필에서 Bluetooth 공유를 허용할지 여부를 제어합니다 .

5. 프라이빗 공간

기기에서 프라이빗 공간을 허용할지 여부를 제어합니다 .

6. Play Store 모드

Play Store

(**):**

:

7.

Play Store

Play Store **+**

7.1.

:

:

:

8.

교차 프로필 정책
개인 프로필과 직장 프로필이 있는 기기에만 적용됩니다 .

교차 프로필 복사 /붙여넣기

한 프로필 (개인 또는 직장)에서 복사한 텍스트를 다른 프로필에 붙여넣을 수 있는지 여부입니다 .

허용 안 함 (기본값): 직장 프로필에서 복사한 텍스트를 개인 프로필에 붙여넣지 못하도록 합니다. 개인 프로필에서 복사한 텍스트는 직장 프로필에 붙여넣을 수 있습니다.

허용: 어느 프로필에서 복사한 텍스트든 다른 프로필에 붙여넣을 수 있습니다.

교차 프로필 데이터 공유

한 프로필 (개인 또는 직장)의 데이터를 다른 프로필의 앱과 공유할 수 있는지 여부입니다 . 특히 인텐트를 통한 단순 데이터 공유를 제어합니다 . 연락처 검색, 복사 /붙여넣기,
또는 연결된 직장 및 개인 앱과 같은 기타 교차 프로필 통신 채널 관리는 별도로 구성됩니다 .

허용 안 함: 개인 프로필에서 직장 프로필로, 직장 프로필에서 개인 프로필로 데이터가 공유되지 않도록 합니다.

직장에서 개인으로 공유 허용 안 함 (기본값): 사용자가 직장 프로필의 데이터를 개인 프로필의 앱과 공유하지 못하도록 합니다. 개인 데이터는 직장 앱과 공유할 수 있습니다.

허용: 어느 프로필의 데이터든 다른 프로필과 공유할 수 있습니다.

직장 프로필 위젯 기본값

직장 프로필 위젯의 기본 동작입니다 . 특정 앱이 위젯 정책을 정의하지 않으면 여기에 설정된 기본값을 따릅니다.

교차 프로필 앱 기능

개인 프로필 앱이 직장 프로필 앱의 앱 기능을 호출할 수 있는지 제어합니다 . Android 16 이상이 필요합니다 .

이 설정은 정책 수준의 앱 기능 옵션 (앱 관리 섹션)에 따라 달라집니다 . 앱 기능이 허용 안 함 으로
설정된 경우 API는 허용 으로 설정된 교차 프로필 앱 기능을 거부합니다 .

개인 프로필의 직장 연락처

직장 프로필에 저장된 연락처를 개인 프로필의 연락처 검색 및 수신 전화에 표시할 수 있는지 여부입니다 .

허용 (기본값): 직장 프로필 연락처가 개인 프로필에 표시되도록 허용합니다 .

허용 안 함: 개인 앱이 직장 프로필 연락처에 액세스하고 직장 연락처를 조회하지 못하도록 합니다.

시스템 제외 허용 안 함: OEM 기본 다이얼러, 메시지, 연락처 앱 (Android 14+)을 제외한 대부분의
개인 앱이 직장 프로필 연락처에 액세스하지 못하도록 합니다.

개인 프로필의 직장 연락처가 구성되면 선택적으로 제외할 패키지 이름 항목 목록을 정의할 수 있습니다. 선택한 모드에 따라 이러한 예외는 개인 앱에 대한 허용 목록 또는 차단 목록으로 작동합니다 .

상태 보고

이 섹션에서는 기기에서 검색할 데이터를 구성할 수 있습니다. 상태 데이터는 기기 상태 대시보드 페이지에서 확인할 수 있습니다.

애플리케이션 보고서
앱 보고서가 활성화되어 있는지 여부입니다 . (설치된 앱에 대해 보고되는 정보입니다 .)

이 옵션은 시스템 (컴패니언 앱 통합용)에 필요하며 항상 활성화되어 있어 비활성화할 수 없습니다.

제거된 앱 포함
제거된 앱이 애플리케이션 보고서에 포함되는지 여부입니다 .

기기 설정
기기 설정 보고가 활성화되어 있는지 여부입니다 . (기기의 보안 관련 기기 설정에 대한 정보입니다 .)

소프트웨어 정보
소프트웨어 정보 보고가 활성화되어 있는지 여부입니다 . (기기 소프트웨어에 대한 정보입니다 .)

메모리 정보
메모리 보고가 활성화되어 있는지 여부입니다 . (메모리 및 저장소 측정과 관련된 이벤트입니다 .)

네트워크 정보
네트워크 정보 보고가 활성화되어 있는지 여부입니다 . (기기 네트워크 정보입니다 .)

디스플레이 정보
디스플레이 보고가 활성화되어 있는지 여부입니다 . 작업 프로필이 있는 개인 소유 기기에서는 보고 데이터를 사용할 수 없습니다. (기기 디스플레이 정보입니다 .)

전원 관리 이벤트
전원 관리 이벤트 보고가 활성화되어 있는지 여부입니다 . 작업 프로필이 있는 개인 소유 기기에서는 보고 데이터를 사용할 수 없습니다.

하드웨어 상태
하드웨어 상태 보고가 활성화되어 있는지 여부입니다 . 작업 프로필이 있는 개인 소유 기기에서는 보고 데이터를 사용할 수 없습니다.

시스템 속성
시스템 속성 보고가 활성화되어 있는지 여부입니다 .

Common Criteria 모드
Common Criteria 모드 보고가 활성화되어 있는지 여부입니다 .

기타

1. 이스터 에그 게임 비활성화

설정의 이스터 에그 게임이 비활성화되었는지 여부입니다 .

2. 첫 사용 힌트 건너뛰기

첫 사용 시 힌트를 건너뛰는 플래그입니다 . 기업 관리자는 앱이 최초 시작 시 사용자 자습서 및 기타 소개 힌트를 건너뛰도록 시스템 권장 사항을 활성화할 수 있습니다.

3. 간단한 지원 메시지

관리자가 기능을 비활성화한 경우 설정 화면에서 사용자에게 표시되는 메시지입니다 . 메시지가 200자를 초과하면 잘릴 수 있습니다.

4. 긴 지원 메시지

기기 관리자 설정 화면에서 사용자에게 표시되는 메시지입니다 .

5. 소유자 잠금 화면 정보

잠금 화면에 표시할 기기 소유자 정보입니다 .

6. 설정 작업

설정 프로세스 중에 수행할 작업입니다 . 등록 중에 기기 설정에 필요한 하나 이상의 앱을 사용자가 열도록 요구할 수 있습니다.
설정 작업 추가 를 사용하여 항목을 만들고 삭제 작업으로 제거합니다 .

6.1. 앱 실행

실행할 앱의 패키지 이름

6.2. 제목

앱을 실행해야 하는 이유를 사용자에게 설명하는 사용자 대상 메시지를 제공합니다 .

6.3. 설명

앱을 실행해야 하는 이유를 사용자에게 설명하는 사용자 대상 메시지를 제공합니다 .

7. 기업 표시 이름 공개 여부

기업 표시 이름이 기기에 표시되는지 여부를 제어합니다 (예: 회사 소유 기기의 잠금 화면 메시지).
표시 (기본값): 기업 표시 이름이 기기에 표시됩니다 (Android 7+의 직장 프로필 및 Android 8+의 완전 관리형 기기에서 지원).
숨김: 기업 표시 이름이 기기에 표시되지 않습니다.

규정 준수 규칙
기기 또는 작업 프로필이 아래 나열된 정책 설정 중 하나라도 준수하지 않으면 Android Device Policy가 기본적으로 즉시 기기 또는 작업 프로필 사용을 차단합니다 :

비밀번호 요구 사항
암호화 정책
키가드 비활성화됨
허용된 입력 방식
허용된 접근성 서비스

기기 또는 업무 프로필이 10일 후에도 규정을 준수하지 않으면 Android Device Policy가 기기를 공장 초기화하거나 업무 프로필을 삭제합니다 .

이 섹션에서는 기본 규정 준수 적용 규칙을 재정의하거나 새 규칙을 추가할 수 있습니다.

규칙

특정 정책을 기기에 적용할 수 없을 때의 동작을 정의하는 규칙 목록입니다 .

규칙 추가 를 사용하여 새 규칙을 만드세요. 각 규칙 카드는 삭제 작업으로 제거할 수 있습니다.

설정 이름

적용할 최상위 정책입니다 . 예: 애플리케이션 또는 비밀번호 요구 사항.

필수입니다 . 값은 지원되는 최상위 정책 이름과 일치해야 하며, 그렇지 않으면 필드가 유효하지 않은 것으로 표시됩니다 .

차단까지 일수

기기 또는 작업 프로필이 차단되기 전까지 정책이 규정을 준수하지 않는 일수입니다 . 액세스를 즉시
차단하려면 0으로 설정하세요 . 차단까지 일수 는 초기화까지 일수 보다 작아야 합니다. 회사 소유 기기에만 적용됩니다 .

허용 범위: 0–300.

차단 범위

차단 작업의 범위를 지정합니다 . 회사 소유 기기에만 적용됩니다 .

기본값 (새 규칙): 작업 프로필.

작업 프로필: 차단 작업은 작업 프로필의 앱에만 적용됩니다 . 개인 프로필의 앱은 영향을 받지 않습니다

.

전체 기기: 차단 작업이 개인 프로필의 앱을 포함한 전체 기기에 적용됩니다 .

초기화까지 일수
기기 또는 작업 프로필이 초기화되기 전까지 정책이 규정을 준수하지 않는 일수입니다 .
초기화까지 일수 는 차단까지 일수 보다 커야 합니다. 회사 소유 기기에만 적용됩니다 .

필수입니다 . 기본값 (새 규칙): 1.

허용 범위: 1–300.

초기화 보호 유지
기기에서 초기화 보호 데이터를 유지할지 여부입니다 . 이 설정은 작업 프로필에 적용되지 않습니다.

기본값 (새 규칙): 사용.