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.

Revision #59
Created 2025-12-17 09:34:15 UTC by Admin
Updated 2026-11-12 09:56:35 UTC by Admin