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 .

Revision #6
Created 2026-11-10 15:16:51 UTC by Admin
Updated 2026-11-12 09:56:36 UTC by Admin