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 .

Revision #6
Created 2026-11-10 15:16:52 UTC by Admin
Updated 2026-11-12 09:56:38 UTC by Admin