Netzwerk

In diesem Abschnitt können Sie Richtlinien im Zusammenhang mit dem Netzwerk konfigurieren.

> Wi-Fi-Konfigurationen können durch das System über **Wi-Fi-Konfigurationen** bereitgestellt und verwaltet werden. Je nach dem unter **Wi-Fi konfigurieren** festgelegten Wert haben Benutzer möglicherweise nur begrenzten oder gar keinen Zugriff auf das Hinzufügen/Ändern von Netzwerken.

Funkstatus des Geräts

1. Wi-Fi-Status

Steuert den aktuellen Wi-Fi-Status und ob der Benutzer diesen ändern kann.

Wahl des Benutzers (Standard): Der Benutzer darf Wi-Fi aktivieren/deaktivieren.

Aktiviert: Wi-Fi ist eingeschaltet und der Benutzer darf es nicht ausschalten (Android 13+).

Deaktiviert: Wi-Fi ist ausgeschaltet und der Benutzer darf es nicht einschalten (Android 13+).

2. Mindest-Wi-Fi-Sicherheitsstufe

Die erforderliche Mindestsicherheitsstufe für Wi-Fi-Netzwerke, mit denen sich das Gerät verbinden kann. Unterstützt ab Android 13 für vollständig verwaltete Geräte und Arbeitsprofile auf unternehmenseigenen Geräten.

Offenes Netzwerk (Standard): Das Gerät kann sich mit allen Arten von Wi-Fi-Netzwerken verbinden.

Persönliches Netzwerk: Verbietet offene Wi-Fi-Netzwerke; erfordert mindestens persönliche Sicherheit (zum Beispiel WPA2-PSK).

Unternehmensnetzwerk: Erfordert EAP-Unternehmensnetzwerke; verbietet Wi-Fi-Netzwerke unterhalb dieser Sicherheitsstufe.

192-Bit-Unternehmensnetzwerk: Erfordert 192-Bit-Unternehmensnetzwerke; strengste Option.

3. Ultra-Breitband (UWB)-Status

Steuert den Status der Ultra-Breitband-Einstellung und ob der Benutzer diese ein- oder ausschalten kann.

Wahl des Benutzers (Standard): Der Benutzer darf UWB ein- oder ausschalten.

Deaktiviert: UWB ist deaktiviert und der Benutzer darf es nicht über die Einstellungen umschalten (Android 14+).

Geräte-Konnektivitätsmanagement

4. Bluetooth-Freigabe

Steuert, ob die Bluetooth-Freigabe zulässig ist.

Zulässig: Die Bluetooth-Freigabe ist erlaubt (Standard bei vollständig verwalteten Geräten, Android 8+).

Untersagt: Die Bluetooth-Freigabe ist untersagt (Standard bei Arbeitsprofilen, Android 8+).

5. Wi-Fi konfigurieren

Steuert die Berechtigungen zur Wi-Fi-Konfiguration. Je nach gewählter Option hat der Benutzer die volle, begrenzte oder gar keine Kontrolle bei der Konfiguration von Wi-Fi-Netzwerken.

Wi-Fi konfigurieren erlauben (Standard): Der Benutzer darf Wi-Fi konfigurieren.

Hinzufügen von Wi-Fi-Konfigurationen untersagen: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist untersagt. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete Geräte und unternehmenseigene Arbeitsprofile).

Wi-Fi-Konfiguration untersagen: Das Konfigurieren von Wi-Fi-Netzwerken ist untersagt. Bei vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und es bleiben nur über **Wi-Fi-Konfigurationen** konfigurierte Netzwerke beibehalten. Bei unternehmenseigenen Arbeitsprofilen sind bestehende Netzwerke nicht betroffen, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen, entfernen oder ändern.

> Wenn die Wi-Fi-Konfiguration deaktiviert ist und das Gerät beim Booten keine Verbindung herstellen kann, kann das System die **Netzwerk-Notausgang** anzeigen, um dem Benutzer eine vorübergehende Verbindung zu ermöglichen und die Richtlinie zu aktualisieren.

6. Wi-Fi-Direct-Einstellungen

Steuert die Konfiguration und Nutzung von Wi-Fi-Direct-Einstellungen. Wird auf unternehmenseigenen Geräten mit Android 13 und höher unterstützt.

Zulassen (Standard): Der Benutzer darf Wi-Fi Direct verwenden.

Untersagen: Der Benutzer darf kein Wi-Fi Direct verwenden.

7. Tethering-Einstellungen

Steuert die Tethering-Einstellungen. Je nach gewähltem Wert wird dem Benutzer die Nutzung verschiedener Formen des Tetherings teilweise oder vollständig untersagt.

Alle Tethering-Arten erlauben (Standard): Erlaubt die Konfiguration und Nutzung aller Formen des Tetherings.

Wi-Fi-Tethering untersagen: Verhindert, dass der Benutzer Wi-Fi-Tethering verwendet (unternehmenseigene Android 13+).

Alle Tethering-Arten untersagen: Verbietet alle Formen des Tetherings (vollständig verwaltete Geräte + unternehmenseigene Arbeitsprofile).

8. Wi-Fi-SSID-Richtlinie

Beschränkungen für die Wi-Fi-SSIDs, mit denen sich das Gerät verbinden kann (dies hat keinen Einfluss darauf, welche Netzwerke auf dem Gerät konfiguriert werden können). Wird auf unternehmenseigenen Geräten mit Android 13 und höher unterstützt.

SSID-Denylist (Standard): Das Gerät kann sich mit keinem Wi-Fi-Netzwerk verbinden, dessen SSID in der Liste steht, kann sich aber mit anderen Netzwerken verbinden.

SSID-Allowlist: Das Gerät kann sich nur mit den aufgeführten SSIDs verbinden. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **SSID hinzufügen**, um Einträge hinzuzufügen. Je nach gewähltem Richtlinientyp wird die Liste als erlaubte oder verbotene SSIDs interpretiert.

In der Benutzeroberfläche des Richtlinien-Editors wird die SSID-Liste für Allowlisten als **Erlaubte Wi-Fi-SSIDs** und für Denylists als **Verbotene Wi-Fi-SSIDs** bezeichnet.

9. Wi-Fi-Roaming-Einstellungen

Konfigurieren Sie den Wi-Fi-Roaming-Modus pro SSID. Verwenden Sie **Wi-Fi-Roaming-Einstellung hinzufügen**, um Einträge zu erstellen.

Jeder Eintrag enthält:

SSID: Die SSID, für die die Roaming-Einstellung gilt (erforderlich).

Wi-Fi-Roaming-Modus: Standard / Deaktiviert / Aggressiv. Die Optionen „Deaktiviert“ und „Aggressiv“ erfordern Android 15+ und werden nur auf vollständig verwalteten Geräten sowie Arbeitsprofilen auf unternehmenseigenen Geräten unterstützt.

Netzwerkbeschränkungen

10. Bluetooth deaktiviert

Ob Bluetooth deaktiviert ist. Diese Einstellung wird der Option „Bluetooth-Konfiguration deaktiviert“ vorgezogen, da die Bluetooth-Konfiguration vom Benutzer umgangen werden kann.

11. Bluetooth-Kontaktsymbole-Freigabe deaktiviert

Ob die Bluetooth-Kontaktsymbole-Freigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob die Konfiguration von Bluetooth deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Android Beam (ausgehend) deaktiviert

Ob die Verwendung von NFC zum Senden von Daten aus Apps deaktiviert ist.

VPN

15. Always-on-VPN-App

Geben Sie einen Paketnamen für die Always-on-VPN-App an, um sicherzustellen, dass Daten von den angegebenen verwalteten Apps immer über ein konfiguriertes VPN gesendet werden.

> Hinweis: Diese Funktion erfordert den Einsatz eines VPN-Clients, der sowohl die Always-on- als auch die App-spezifische VPN-Funktion unterstützt.

16. VPN-Lockdown

Verhindert die Nutzung des Netzwerks, wenn keine VPN-Verbindung besteht.

17. VPN-Konfiguration deaktiviert

Ob die Konfiguration von VPN deaktiviert ist.

Proxy und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Steuert, ob ein bevorzugter Netzwerkdienst im Arbeitsprofil aktiviert ist. Beispielsweise kann eine Organisation mit einem Mobilfunkanbieter vereinbart haben, dass geschäftliche Daten über einen speziellen Netzwerkdienst für die Unternehmensnutzung gesendet werden (z. B. ein Enterprise-Slice in 5G-Netzen). Dies hat keine Auswirkungen auf vollständig verwaltete Geräte.

Deaktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil deaktiviert.

Aktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsprofil aktiviert.

> Wenn Sie Enterprise-Network-Slicing verwenden, konfigurieren Sie zusätzlich die **5G-Network-Slicing-Konfiguration** im Bereich **Mobilfunk** und weisen Apps einem Slice über die Einstellung **Bevorzugter Netzwerkdienst** zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. Normalerweise sollten Proxys pro Netzwerk in den Wi-Fi-Konfigurationen eingerichtet werden. Ein globaler Proxy kann bei ungewöhnlichen Konfigurationen, wie etwa einer allgemeinen internen Filterung, nützlich sein. Der globale Proxy ist lediglich eine Empfehlung und einige Apps ignorieren ihn möglicherweise.

Deaktiviert

Direkt-Proxy

Proxy-Autokonfiguration (PAC)

19.1. Host

Der Host des Direkt-Proxys.

19.2. Port

Der Port des Direkt-Proxys.

19.3. PAC-URI

Die URI des zum Konfigurieren des Proxys verwendeten PAC-Skripts.

19.4. Ausgeschlossene Hosts

Bei einem Direkt-Proxy sind dies die Hosts, für die der Proxy umgangen wird. Hostnamen können Platzhalter wie ***.example.com** enthalten.

Verwenden Sie **Ausgeschlossenen Host hinzufügen**, um Einträge hinzuzufügen (nur für Direkt-Proxy verfügbar).

Wi-Fi-Konfigurationen

Definieren Sie Wi-Fi-Netzwerkkonfigurationen, die das System auf Geräten anwendet. Verwenden Sie **Wi-Fi-Konfiguration hinzufügen**, um einen Eintrag zu erstellen und diesen mit der Löschaktion wieder zu entfernen.

20. Wi-Fi-Konfigurationsfelder

Jede Konfiguration umfasst:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatischer Verbindungsaufbau: Gibt an, ob das Netzwerk automatisch verbunden werden soll, wenn es in Reichweite ist.

Fast Transition: Gibt an, ob der Client versuchen soll, Fast Transition (IEEE 802.11r-2008) mit dem Netzwerk zu nutzen.

Versteckte SSID: Gibt an, ob die SSID ausgestrahlt wird.

MAC-Randomisierungsmodus: Hardware oder Automatisch (Android 13+).

20.1. Sicherheit

Wi-Fi-Sicherheitsoptionen:

WEP-PSK: WEP (Pre-Shared Key).

WPA-PSK: WPA/WPA2/WPA3-Personal (Pre-Shared Key).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

WPA3 192-Bit-Modus: WPA-EAP-Netzwerk, das nur den WPA3 192-Bit-Modus zulässt.

20.2. Passphrase (Pre-Shared Key)

Wird angezeigt, wenn die Sicherheit auf **WEP-PSK** oder **WPA-PSK** eingestellt ist. Die Passphrase ist erforderlich.

20.3. EAP-Methode (Enterprise)

Wird angezeigt, wenn die Sicherheit auf **WPA-EAP** oder **WPA3 192-Bit-Modus** eingestellt ist. Wählen Sie eine EAP-äußere Methode:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentifizierung der Phase 2

Wird für Tunneling-äußere Methoden (**EAP-TTLS** und **PEAP**) angezeigt.

MSCHAPv2

PAP

20.5. EAP-Anmeldedaten von Benutzern

Wenn diese Funktion aktiviert ist, wendet das System EAP-Anmeldedaten automatisch auf Benutzerbasis auf den Geräten an. Sie können Benutzeranmeldedaten im Bereich **Benutzer** konfigurieren.

20.6. Client-Zertifikat

Für **EAP-TLS** können Sie ein Client-Zertifikat zuweisen, das für die Wi-Fi-Authentifizierung verwendet wird. Weitere Informationen finden Sie auf der Seite **Zertifikatsverwaltung**.

Wenn bereits ein Zertifikat zugewiesen ist, können Sie **Zertifikat öffnen** verwenden, um es anzuzeigen, oder **Zertifikat ändern**, um ein anderes auszuwählen.

Alternativ können Sie einen **Alias für das Client-Zertifikatsschlüsselpaar** angeben, der auf ein im Android-Schlüsselbund gespeichertes und für die Wi-Fi-Authentifizierung zugelassenes Client-Zertifikat verweist.

> Wenn sowohl das**Client-Zertifikat** als auch der **Alias für das Client-Zertifikatsschlüsselpaar** festgelegt sind, wird der Schlüsselpaar-Alias ignoriert.

20.7. Identität

Identität des Benutzers. Bei Tunneling-äußeren Protokollen (PEAP, EAP-TTLS) wird dies zur Authentifizierung innerhalb des Tunnels verwendet, während die **Anonyme Identität** für die EAP-Identität außerhalb des Tunnels verwendet wird. Bei Protokollen ohne Tunneling dient dies als EAP-Identität.

20.8. Anonyme Identität

Nur für Tunneling-Protokolle gibt dies die Identität des Benutzers an, die dem äußeren Protokoll übermittelt wird.

20.9. Passwort

Passwort des Benutzers. Wenn nicht angegeben, wird der Benutzer standardmäßig zur Eingabe aufgefordert.

20.10. Server-CA-Zertifikate

Liste der CA-Zertifikate, die zur Überprüfung der Zertifikatskette des Hosts verwendet werden sollen. Mindestens ein CA-Zertifikat muss übereinstimmen. Weitere Informationen finden Sie auf der Seite **Zertifikatsverwaltung**.

Verwenden Sie **Server-CA-Zertifikat hinzufügen**, um Einträge hinzuzufügen, und die Löschaktion, um sie zu entfernen.

20.11. Übereinstimmung der Domänen-Suffixe

Eine Liste von Einschränkungen für den Server-Domänennamen. Die Einträge werden als Anforderungen für die Suffix-Übereinstimmung mit dem(n) DNS-Namen des alternativen Subjektnamens eines Authentifizierungsserver-Zertifikats verwendet.

Revision #10
Created 2026-06-24 08:06:30 UTC by Admin
Updated 2026-07-07 10:53:41 UTC by Admin