Netzwerk

In diesem Abschnitt können Sie netzwerkbezogene Richtlinien konfigurieren.

> Wi-Fi-Konfigurationen können vom System über **WiFi-Konfigurationen** bereitgestellt und verwaltet werden. Je nach Wert, der für **Wi-Fi konfigurieren** festgelegt ist, haben Benutzer möglicherweise eingeschränkte oder keine Kontrolle über das Hinzufügen/Ändern von Netzwerken.

Funkstatus des Geräts

1. Wi-Fi-Status

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

Benutzerauswahl (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. Mindestsicherheitsstufe für Wi-Fi

Die erforderliche Mindestsicherheitsstufe von Wi-Fi-Netzwerken, mit denen das Gerät eine Verbindung herstellen kann. Unterstützt unter Android 13 und höher, für vollständig verwaltete Geräte und Arbeitsprofile auf unternehmenseigenen Geräten.

Offenes Netzwerk (Standard): Das Gerät kann eine Verbindung zu allen Arten von Wi-Fi-Netzwerken herstellen.

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

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

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

3. Ultrabreitband-Status (UWB)

Steuert den Status der Ultrabreitband-Einstellung und ob der Benutzer sie ein- oder ausschalten kann.

Benutzerauswahl (Standard): Der Benutzer darf UWB ein- oder ausschalten.

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

Gerätekonnektivitätsverwaltung

4. Bluetooth-Freigabe

Steuert, ob die Bluetooth-Freigabe zulässig ist.

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

Nicht zulässig: Die Bluetooth-Freigabe ist nicht zulässig (Standard in Arbeitsprofilen, Android 8+).

5. Wi-Fi konfigurieren

Steuert die Berechtigungen zum Konfigurieren von Wi-Fi. Je nach ausgewählter Option hat der Benutzer volle, eingeschränkte oder keine Kontrolle beim Konfigurieren von Wi-Fi-Netzwerken.

Konfigurieren von Wi-Fi zulassen (Standard): Der Benutzer darf Wi-Fi konfigurieren.

Hinzufügen von Wi-Fi-Konfigurationen nicht zulassen: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist nicht zulässig. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete und unternehmenseigene

Arbeitsprofile).

Konfigurieren von Wi-Fi nicht zulassen: Verbietet das Konfigurieren von Wi-Fi-Netzwerken. Auf vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und nur über **WiFi-Konfigurationen** konfigurierte Netzwerke beibehalten. Bei unternehmenseigenen Arbeitsprofilen sind vorhandene Netzwerke nicht betroffen, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen/entfernen/ändern.

> Wenn das Konfigurieren von Wi-Fi deaktiviert ist und das Gerät beim Start keine Verbindung herstellen kann, kann das System den **Netzwerk-Notzugang** anzeigen, damit der Benutzer vorübergehend eine Verbindung herstellen und die Richtlinie aktualisieren kann.

6. Wi-Fi-Direct-Einstellungen

Steuert das Konfigurieren und Verwenden von Wi-Fi-Direct-Einstellungen. Unterstützt auf unternehmenseigenen Geräten mit Android 13 und höher.

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

Nicht zulassen: Der Benutzer darf Wi-Fi Direct nicht verwenden.

7. Tethering-Einstellungen

Steuert die Tethering-Einstellungen. Je nach festgelegtem Wert ist dem Benutzer die Nutzung verschiedener Tethering-Formen teilweise oder vollständig untersagt.

Gesamtes Tethering zulassen (Standard): Ermöglicht die Konfiguration und Nutzung aller Tethering-Formen.

Wi-Fi-Tethering nicht zulassen: Untersagt dem Benutzer die Nutzung von Wi-Fi-Tethering (unternehmenseigen, Android 13+).

Gesamtes Tethering nicht zulassen: Untersagt alle Tethering-Formen (vollständig verwaltete und unternehmenseigene Arbeitsprofile).

8. Wi-Fi-SSID-Richtlinie

Einschränkungen, mit welchen Wi-Fi-SSIDs das Gerät eine Verbindung herstellen kann (dies wirkt sich nicht darauf aus, welche Netzwerke auf dem Gerät konfiguriert werden können). Unterstützt auf unternehmenseigenen Geräten mit Android 13 und höher.

SSID-Sperrliste (Standard): Das Gerät kann keine Verbindung zu Wi-Fi-Netzwerken herstellen, deren SSID aufgeführt ist, aber zu anderen Netzwerken.

SSID-Zulassungsliste: Das Gerät kann nur eine Verbindung zu den aufgeführten SSIDs herstellen. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **SSID hinzufügen**, um Einträge hinzuzufügen. Je nach ausgewähltem Richtlinientyp wird die Liste als zulässige oder abgelehnte SSIDs interpretiert.

In der Benutzeroberfläche des Richtlinieneditors wird die SSID-Liste bei Zulassungslisten als **Zulässige Wi-Fi-SSIDs** und bei Sperrlisten als **Abgelehnte 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. Deaktiviert und Aggressiv erfordern Android 15+ und werden nur auf vollständig verwalteten Geräten und Arbeitsprofilen auf unternehmenseigenen Geräten unterstützt.

Netzwerkeinschränkungen

10. Bluetooth deaktiviert

Ob Bluetooth deaktiviert ist. Bevorzugen Sie diese Einstellung gegenüber „Bluetooth-Konfiguration deaktiviert“, da die Option „Bluetooth-Konfiguration deaktiviert“ vom Benutzer umgangen werden kann.

11. Bluetooth-Kontaktfreigabe deaktiviert

Ob die Bluetooth-Kontaktfreigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob das Konfigurieren von Bluetooth deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Ausgehender Beam deaktiviert

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

VPN

15. Always-On-VPN-App

Geben Sie einen Paketnamen für Always-On-VPN an, um sicherzustellen, dass Daten bestimmter verwalteter Apps immer über ein konfiguriertes VPN geleitet werden.

> Hinweis: Diese Funktion erfordert die Bereitstellung eines VPN-Clients, der sowohl Always-On- als auch App-spezifische VPN-Funktionen unterstützt.

16. VPN-Lockdown

Untersagt die Netzwerknutzung, wenn das VPN nicht verbunden ist.

17. VPN-Konfiguration deaktiviert

Ob das Konfigurieren von VPN deaktiviert ist.

Proxy- und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Steuert, ob der bevorzugte Netzwerkdienst im Arbeitsprofil aktiviert ist. Beispielsweise kann eine Organisation eine Vereinbarung mit einem Mobilfunkanbieter haben, dass Arbeitsdaten über einen für die Unternehmensnutzung reservierten Netzwerkdienst des Anbieters gesendet werden (z. B. ein Unternehmens-Slice in 5G-Netzwerken). Dies hat keine Auswirkung 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 außerdem **5G-Network-Slicing-Konfiguration** im Richtlinien-Panel **Mobilfunk** und weisen Sie Apps über ihre Einstellung **Bevorzugtes Netzwerk** einem Slice zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. In der Regel sollten Proxys pro Netzwerk in WiFi-Konfigurationen konfiguriert werden. Ein globaler Proxy kann für ungewöhnliche Konfigurationen wie eine allgemeine interne Filterung nützlich sein. Der globale Proxy ist lediglich eine Empfehlung und einige Apps ignorieren ihn möglicherweise.

Deaktiviert

Direkter Proxy

Proxy-Autokonfiguration (PAC)

19.1. Host

Der Host des direkten Proxys.

19.2. Port

Der Port des direkten Proxys.

19.3. PAC-URI

Die URI des PAC-Skripts, mit dem der Proxy konfiguriert wird.

19.4. Ausgeschlossene Hosts

Bei einem direkten Proxy 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 direkten 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 entfernen Sie ihn über die Löschaktion.

20. Felder der Wi-Fi-Konfiguration

Jede Konfiguration umfasst:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatisch verbinden: Ob automatisch eine Verbindung zum Netzwerk hergestellt werden soll, wenn es in Reichweite ist.

Fast Transition: Ob der Client versuchen soll, Fast Transition (IEEE 802.11r-2008) mit dem Netzwerk zu verwenden.

Versteckte SSID: Ob die SSID gesendet 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 Sicherheit auf **WEP-PSK** oder **WPA-PSK** gesetzt ist. Die Passphrase ist erforderlich.

20.3. EAP-Methode (Enterprise)

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

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Phase-2-Authentifizierung

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

MSCHAPv2

PAP

20.5. EAP-Anmeldeinformationen von Benutzern

Wenn aktiviert, wendet das System EAP-Anmeldeinformationen automatisch pro Benutzer auf Geräten an. Sie können Benutzeranmeldeinformationen im Bereich **Benutzer** konfigurieren.

20.6. Clientzertifikat

Für **EAP-TLS** können Sie ein Clientzertifikat für die Wi-Fi-Authentifizierung zuweisen. Weitere Informationen finden Sie auf der Seite **Zertifikatsverwaltung**.

Wenn bereits ein Zertifikat zugewiesen ist, können Sie über **Zertifikat öffnen** es anzeigen oder über **Zertifikat ändern** ein anderes auswählen.

Alternativ können Sie einen **Alias für das Clientzertifikat-Schlüsselpaar** angeben, der auf ein im Android-Schlüsselspeicher gespeichertes Clientzertifikat verweist, das für die Wi-Fi-Authentifizierung zugelassen ist.

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

20.7. Identität

Identität des Benutzers. Bei tunnelnden äußeren Protokollen (PEAP, EAP-TTLS) wird sie zur Authentifizierung innerhalb des Tunnels verwendet, und die **anonyme Identität** wird für die EAP-Identität außerhalb des Tunnels verwendet. Bei nicht tunnelnden äußeren Protokollen wird sie für die EAP-Identität verwendet.

20.8. Anonyme Identität

Nur für tunnelnde Protokolle: Gibt die Identität des Benutzers an, die dem äußeren Protokoll präsentiert wird.

20.9. Passwort

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

20.10. Server-CA-Zertifikate

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

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

20.11. Übereinstimmungen von Domänensuffixen

Eine Liste von Einschränkungen für den Serverdomänennamen. Die Einträge werden als Suffix-Übereinstimmungsanforderungen gegen die DNS-Namen des alternativen Antragstellernamens eines Authentifizierungsserverzertifikats verwendet.

Revision #19
Created 2026-06-24 08:06:30 UTC by Admin
Updated 2026-11-12 09:54:02 UTC by Admin