Netzwerkfunktionen

In diesem Abschnitt können Sie netzwerkbezogene Richtlinien konfigurieren.

> Wi-Fi-Einstellungen können vom System bereitgestellt und verwaltet werden, über die **Wi-Fi-Einstellungen**. Je nach Wert, der bei **Wi-Fi-Konfiguration** eingestellt ist, haben Benutzer möglicherweise eingeschränkte oder keine Kontrolle über das Hinzufügen/Ändern von Netzwerken.

Zustand des drahtlosen Geräts

1. Wi-Fi-Status

Steuert den aktuellen Wi-Fi-Status und ermöglicht dem Benutzer, diesen zu ändern.

Benutzerwahl (Standard): Der Benutzer darf Wi-Fi aktivieren/deaktivieren.

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

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

2. Mindest-Sicherheitsstufe für Wi-Fi

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

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

Persönliches Netzwerk: Verhindert die Nutzung offener Wi-Fi-Netzwerke; erfordert mindestens eine persönliche Sicherheitsfunktion (z. B. WPA2-PSK).

Unternehmensnetzwerk: Erfordert Unternehmens-EAP-Netzwerke; verbietet Wi-Fi-Netzwerke mit einem niedrigeren Sicherheitsniveau.

Unternehmensnetzwerk mit 192 Bit: Erfordert Unternehmensnetzwerke mit 192 Bit; die strengste Option.

3. Status von Ultra-Weitband (UWB)

Steuert den Status der Ultra-Weitband-Einstellung und ob der Benutzer sie aktivieren oder deaktivieren kann.

Benutzerwahl (Standard): Der Benutzer kann Ultra-Weitband aktivieren oder deaktivieren.

Deaktiviert: UWB ist deaktiviert und der Benutzer kann diese Einstellung über die Einstellungen nicht ändern (Android 14+).

Gerätekonnektivitätsverwaltung

4. Bluetooth-Freigabe

Steuert, ob das Teilen über Bluetooth erlaubt ist.

Erlaubt: Bluetooth-Freigabe ist erlaubt (standardmäßig bei vollständig verwalteten Geräten, Android 8+).

Nicht erlaubt: Bluetooth-Freigabe ist nicht erlaubt (standardmäßig für verwaltete Profile, Android 8+).

5. Wi-Fi konfigurieren

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

Wi-Fi-Konfiguration zulassen (Standard): Der Benutzer darf Wi-Fi-Netzwerke konfigurieren.

Wi-Fi-Konfiguration verbieten: Das Hinzufügen neuer Wi-Fi-Konfigurationen ist nicht zulässig. Der Benutzer kann zwischen bereits konfigurierten Netzwerken wechseln (Android 13+; vollständig verwaltete und firmeneigenen Arbeitsumgebungen).

Das Konfigurieren von Wi-Fi verbieten: Verhindert das Konfigurieren von Wi-Fi-Netzwerken. Bei vollständig verwalteten Geräten werden benutzerkonfigurierte Netzwerke entfernt und nur Netzwerke beibehalten, die über **Wi-Fi-Konfigurationen** konfiguriert

wurden. Bei firmeneigenen Arbeitsumgebungen bleiben bestehende Netzwerke unverändert, aber Benutzer können keine Wi-Fi-Netzwerke hinzufügen, entfernen oder ändern.

> Wenn die Wi-Fi-Konfiguration deaktiviert ist und das Gerät beim Start keine Verbindung herstellen kann, kann das System die **Notfallverbindung** anzeigen, damit der Benutzer sich vorübergehend verbinden und die Richtlinie aktualisieren kann.

6. Einstellungen für Wi-Fi Direct

Steuerelemente zum Konfigurieren und Verwenden von Wi-Fi Direct-Einstellungen. Unterstützt auf firmeneigenen Geräten mit Android 13 und höher.

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

Deaktivieren: Der Benutzer darf Wi-Fi Direct nicht verwenden.

7. Einstellungen für den mobilen Hotspot

Steuert die Einstellungen für die mobile Hotspot-Funktion. Je nach gewählter Einstellung kann die Nutzung verschiedener Formen der mobilen Hotspot-Funktion teilweise oder vollständig eingeschränkt werden.

Alle Verbindungsarten zulassen (Standard): Ermöglicht die Konfiguration und Nutzung aller Verbindungsarten.

Wi-Fi-Tethering deaktivieren: Verhindert, dass der Benutzer Wi-Fi als Hotspot nutzt (bei Android-Geräten ab Version 13 im Besitz des Unternehmens).

Alle Verbindungsfreigabe-Optionen deaktivieren: Verhindert alle Arten von Verbindungsfreigabe (vollständig verwaltet + firmeneigene Arbeitsumgebungen).

8. Wi-Fi SSID-Richtlinie

Einschränkungen, zu welchen Wi-Fi SSIDs sich das Gerät verbinden kann (diese Einstellung beeinflusst nicht, welche Netzwerke auf dem Gerät konfiguriert werden können). Unterstützt auf firmeneigenen Geräten mit Android 13 oder höher.

SSID-Sperrliste (Standard): Das Gerät kann sich nicht mit Wi-Fi-Netzwerken verbinden, deren SSID in dieser Liste aufgeführt ist, kann aber mit anderen Netzwerken verbunden werden.

SSID-Zulassungsliste: Das Gerät kann sich nur mit den in dieser Liste aufgeführten Wi-Fi-Netzwerken verbinden. Die SSID-Liste darf nicht leer sein.

Verwenden Sie **"SSID hinzufügen"**, um Einträge hinzuzufügen. Je nach ausgewähltem Richtlinientyp wird die Liste als Liste der zulässigen oder der verbotenen SSIDs interpretiert.

Im Policy Editor-Interface wird die SSID-Liste als **Zulässige Wi-Fi-SSIDs** für Erlaubnislisten und als **Verbotene Wi-Fi-SSIDs** für Sperrlisten bezeichnet.

9. Wi-Fi-Roaming-Einstellungen

Konfigurieren Sie den Wi-Fi-Roaming-Modus pro SSID. Verwenden Sie **Hinzufügen der Wi-Fi-Roaming-Einstellungen**, um Einträge zu erstellen.

Jeder Eintrag enthält:

SSID: Der SSID, für den die Roaming-Einstellungen gelten (erforderlich).

Wi-Fi-Roaming-Modus: Standard / Deaktiviert / Aggressiv. Die Optionen "Deaktiviert" und "Aggressiv" erfordern Android 15 oder höher und werden nur auf vollständig verwalteten Geräten und Unternehmensprofilen auf firmeneigenen Geräten unterstützt.

Netzwerkbeschränkungen

Bluetooth deaktiviert

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

11. Bluetooth-Kontaktfreigabe deaktiviert

Ob die Bluetooth-Kontaktfreigabe deaktiviert ist.

12. Bluetooth-Konfiguration deaktiviert

Ob die Bluetooth-Konfiguration deaktiviert ist.

13. Netzwerk-Reset deaktiviert

Ob das Zurücksetzen der Netzwerkeinstellungen deaktiviert ist.

14. Ausgehendes Beam deaktiviert

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

VPN

15. Immer verbunden VPN-App

Geben Sie einen Paketnamen für das "Always On VPN" an, um sicherzustellen, dass Daten von den konfigurierten verwalteten Apps immer über ein VPN übertragen werden.

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

16. VPN-Sperre

Verhindert Netzwerkzugriff, wenn keine VPN-Verbindung besteht.

17. VPN-Konfiguration deaktiviert

Ob die VPN-Konfiguration deaktiviert ist.

Proxy- und Netzwerkdienste

18. Bevorzugter Netzwerkdienst

Aktiviert den bevorzugten Netzwerkdienst für das Arbeitskonto. Beispielsweise kann ein Unternehmen eine Vereinbarung mit einem Mobilfunkanbieter haben, die besagt, dass Arbeitsdaten über einen speziellen Mobilfunkdienst für Unternehmen übertragen werden (z. B.

einen dedizierten Kanal in 5G-Netzwerken). Dies hat keine Auswirkungen auf vollständig verwaltete Geräte.

Deaktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsbereich deaktiviert.

Aktiviert: Der bevorzugte Netzwerkdienst ist im Arbeitsbereich aktiviert.

> Wenn Sie Network Slicing im Unternehmensbereich verwenden, konfigurieren Sie außerdem **5G-Netzwerk-Slicing-Konfiguration** im Bereich **Mobilfunk** der Richtlinie und weisen Sie Apps mithilfe ihrer **Bevorzugte Netzwerk**-Einstellung einem Slice zu.

19. Empfohlener globaler Proxy

Der netzwerkunabhängige globale HTTP-Proxy. Proxies sollten in der Regel pro Netzwerk in den WLAN-Einstellungen konfiguriert werden. Ein globaler Proxy kann für ungewöhnliche Konfigurationen, z. B. allgemeine interne Filterung, nützlich sein. Der globale Proxy ist nur eine Empfehlung, und einige Apps können ihn ignorieren.

Deaktiviert

Direkter Proxy

Automatische Proxy-Konfiguration (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, das zur Konfiguration des Proxys verwendet wird.

19.4. Ausgeschlossene Hosts

Für einen direkten Proxy sind dies die Hosts, für die der Proxy umgangen wird. Hostnamen dürfen Platzhalter enthalten, z. B. ***.example.com**.

Verwenden Sie **Hinzufügen ausgeschlossener Hosts**, um Einträge hinzuzufügen (nur für direkten Proxy verfügbar).

WLAN-Konfigurationen

Definieren Sie WLAN-Netzwerkkonfigurationen, die das System auf Geräten anwendet. Verwenden Sie **Hinzufügen einer WLAN-Konfiguration**, um einen Eintrag zu erstellen, und entfernen Sie ihn mit der Löschfunktion.

20. Felder für die Wi-Fi-Konfiguration

Jede Konfiguration beinhaltet:

Konfigurationsname: Erforderlich.

SSID: Erforderlich.

Automatische Verbindung: Legt fest, ob automatisch eine Verbindung zu dem Netzwerk hergestellt werden soll, wenn es in Reichweite ist.

Schneller Übergang: Gibt an, ob der Client versuchen soll, den schnellen Übergang (IEEE 802.11r-2008) für das Netzwerk zu verwenden.

Verstecktes SSID: Gibt an, ob das SSID übertragen wird.

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

20.1. Sicherheit

Wi-Fi-Sicherheitsoptionen:

WEP-PSK: WEP (vorgegebener Schlüssel).

WPA-PSK: WPA/WPA2/WPA3-Personal (Vorgegebener Schlüssel).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Erweitertes Authentifizierungsprotokoll).

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

20.2. Passphrase (vorgegebener Schlüssel)

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-Außenmethode:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Authentifizierung in Phase 2

Wird für das Tunneling von äußeren Methoden (**EAP-TTLS** und **PEAP**) angezeigt.

MSCHAPv2

PAP

20.5. EAP-Anmeldedaten von Benutzern

Wenn aktiviert, wendet das System automatisch EAP-Anmeldedaten auf Geräten pro Benutzer an. Sie können Benutzeranmeldedaten im Abschnitt **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 ein Zertifikat bereits zugewiesen ist, können Sie mit "**Zertifikat öffnen**" dieses anzeigen oder mit "**Zertifikat ändern**" ein anderes auswählen.

Alternativ können Sie einen **Client-Zertifikats-Schlüsselpaar-Alias** angeben, der auf ein im Android-Schlüsselbund gespeichertes Client-Zertifikat verweist und für die Wi-Fi-Authentifizierung verwendet wird.

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

20.7. Identität

Identität des Benutzers. Für Tunneling von äußeren Protokollen (PEAP, EAP-TTLS) wird dies zur Authentifizierung innerhalb des Tunnels verwendet, und **die anonyme Identität** wird für die EAP-Identität außerhalb des Tunnels verwendet. Für nicht-tunnelnde äußere Protokolle wird dies für die EAP-Identität verwendet.

20.8. Anonyme Identität

Nur für Tunneling-Protokolle: Dies gibt die Identität des Benutzers an, der dem äußeren Protokoll präsentiert wird.

20.9. Passwort

Passwort des Benutzers. Wenn nicht angegeben, wird der Benutzer aufgefordert, ein Passwort einzugeben.

20.10. Server-CA-Zertifikate

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

Verwenden Sie **das Hinzufügen des Server-CA-Zertifikats**, um Einträge hinzuzufügen und sie mit der Löschfunktion zu entfernen.

20.11. Das Domänenpräfix stimmt überein

Eine Liste von Einschränkungen für den Server-Domänennamen. Die Einträge werden als Suffix-Übereinstimmungsanforderungen für den/die DNS-Namen des alternativen Betreffnamens eines Authentifizierungsserver-Zertifikats verwendet.

Revision #35
Created 2025-12-17 09:32:54 UTC by Admin
Updated 2026-04-22 15:48:48 UTC by Admin