Networking

In questa sezione è possibile configurare le policy relative al networking.

> Le configurazioni Wi-Fi possono essere fornite e gestite dal sistema tramite le **configurazioni WiFi**. A seconda del valore impostato in **Configura Wi-Fi**, gli utenti potrebbero avere un controllo limitato o nullo sull'aggiunta o la modifica delle reti.

Stato radio del dispositivo

1. Stato Wi?Fi

Controlla lo stato attuale del Wi-Fi e se l'utente può modificarne lo stato.

Scelta dell'utente (predefinito): L'utente può abilitare o disabilitare il Wi-Fi.

Abilitato: Il Wi-Fi è attivo e l'utente non può disattivarlo (Android 13+).

Disabilitato: Il Wi-Fi è disattivato e l'utente non può attivarlo (Android 13+).

2. Livello minimo di sicurezza Wi?Fi

Il livello minimo di sicurezza richiesto per le reti Wi-Fi a cui il dispositivo può connettersi. Supportato su Android 13 e versioni successive, per i dispositivi completamente gestiti e i profili di lavoro sui dispositivi di proprietà aziendale.

Rete aperta (predefinito): Il dispositivo può connettersi a tutti i tipi di reti Wi-Fi.

Rete personale: Vieta le reti Wi-Fi aperte; richiede almeno una sicurezza di tipo personale (ad esempio WPA2-PSK).

Rete aziendale: Richiede reti EAP aziendali; vieta le reti Wi-Fi con un livello di sicurezza inferiore.

Rete aziendale a 192 bit: Richiede reti aziendali a 192 bit; l'opzione più restrittiva.

3. Stato ultra-wideband (UWB)

Controlla lo stato dell'impostazione ultra-wideband e se l'utente può attivarla o disattivarla.

Scelta dell'utente (predefinito): L'utente può attivare o disattivare l'UWB.

Disabilitato: L'UWB è disabilitato e l'utente non può attivarlo tramite le impostazioni (Android 14+).

Gestione connettività del dispositivo

4. Condivisione Bluetooth

Controlla se la condivisione Bluetooth è consentita.

Consentito: La condivisione Bluetooth è consentita (predefinito sui dispositivi completamente gestiti, Android 8+).

Vietato: La condivisione Bluetooth è vietata (predefinito sui profili di lavoro, Android 8+).

5. Configura Wi?Fi

Controlla i privilegi di configurazione del Wi-Fi. A seconda dell'opzione selezionata, l'utente avrà un controllo completo, limitato o nullo sulla configurazione delle reti Wi-Fi.

Consenti configurazione Wi-Fi (predefinito): L'utente può configurare il Wi-Fi.

Vieta aggiunta configurazione Wi-Fi: L'aggiunta di nuove configurazioni Wi-Fi è vietata. L'utente può passare tra le reti già configurate (Android 13+; dispositivi completamente gestiti e profili di lavoro su dispositivi di proprietà aziendale).

Vieta configurazione Wi-Fi: Vieta la configurazione delle reti Wi-Fi. Per i dispositivi completamente gestiti, questa opzione rimuove le reti configurate dall'utente e mantiene solo quelle configurate tramite **configurazioni WiFi**. Per i profili di lavoro su dispositivi di proprietà aziendale, le reti esistenti non vengono influenzate, ma gli utenti non possono aggiungere/rimuovere/modificare le reti Wi-Fi.

> Quando la configurazione Wi-Fi è disabilitata e il dispositivo non può connettersi all'avvio, il sistema può mostrare la **via di fuga della rete** per consentire all'utente di connettersi temporaneamente e aggiornare la policy.

6. Impostazioni Wi-Fi Direct

Controlla la configurazione e l'uso delle impostazioni Wi-Fi Direct. Supportato sui dispositivi di proprietà aziendale con Android 13 e versioni successive.

Consentito (predefinito): L'utente può utilizzare il Wi-Fi Direct.

Vietato: L'utente non può utilizzare il Wi-Fi Direct.

7. Impostazioni tethering

Controlla le impostazioni di tethering. In base al valore impostato, l'utente può avere un divieto parziale o totale nell'uso di diverse forme di tethering.

Consenti tutto il tethering (predefinito): Consente la configurazione e l'uso di tutte le forme di tethering.

Vieta tethering Wi-Fi: Impedisce all'utente di utilizzare il tethering Wi-Fi (dispositivi Android di proprietà aziendale 13+).

Vieta tutto il tethering: Vieta tutte le forme di tethering (dispositivi completamente gestiti + profili di lavoro su dispositivi di proprietà aziendale).

8. Policy SSID Wi-Fi

Restrizioni su quali SSID Wi-Fi il dispositivo può connettersi (questo non influisce sulle reti che possono essere configurate sul dispositivo). Supportato sui dispositivi di proprietà aziendale con Android 13 e versioni successive.

Denylist SSID (predefinito): Il dispositivo non può connettersi a nessuna rete Wi-Fi il cui SSID sia presente nell'elenco, ma può connettersi ad altre reti.

Allowlist SSID: Il dispositivo può connettersi solo agli SSID elencati. L'elenco degli SSID non deve essere vuoto.

Usa **Aggiungi SSID** per aggiungere le voci. A seconda del tipo di policy selezionata, l'elenco viene interpretato come SSID consentiti o negati.

Nell'interfaccia utente dell'Editor di Policy, l'elenco degli SSID è etichettato come **SSID Wi-Fi consentiti** per le allowlist e **SSID Wi-Fi negati** per le denylist.

9. Impostazioni roaming Wi-Fi

Configura la modalità di roaming Wi-Fi per singolo SSID. Usa **Aggiungi impostazione roaming Wi-Fi** per creare le voci.

Ogni voce include:

SSID: L'SSID a cui si applica l'impostazione di roaming (obbligatorio).

Modalità roaming Wi-Fi: Predefinito / Disabilitato / Aggressivo. Le opzioni Disabilitato e Aggressivo richiedono Android 15+ e sono supportate solo su dispositivi completamente gestiti e profili di lavoro su dispositivi di proprietà aziendale.

Restrizioni di rete

10. Disabilitazione Bluetooth

Indica se il Bluetooth è disabilitato. Si consiglia questa impostazione rispetto a "Disabilita configurazione Bluetooth", poiché quest'ultima può essere aggirata dall'utente.

11. Disabilitazione condivisione contatti Bluetooth

Indica se la condivisione dei contatti tramite Bluetooth è disabilitata.

12. Disabilitazione configurazione Bluetooth

Indica se la configurazione del Bluetooth è disabilitata.

13. Disabilitazione ripristino rete

Indica se il ripristino delle impostazioni di rete è disabilitato.

14. Disabilitazione Android Beam in uscita

Indica se l'uso del NFC per trasmettere dati dalle app è disabilitato.

VPN

15. App Always On VPN

Specifica il nome del pacchetto per l'app Always On VPN per garantire che i dati delle app gestite specificate passino sempre attraverso una VPN configurata.

> Nota: questa funzione richiede l'installazione di un client VPN che supporti sia le funzioni Always On che quelle per app specifica (per-app VPN).

16. Blocco VPN (VPN lockdown)

Vieta l'uso della rete quando la VPN non è connessa.

17. Disabilitazione configurazione VPN

Indica se la configurazione della VPN è disabilitata.

Proxy e servizi di rete

18. Servizio di rete preferenziale

Controlla se il servizio di rete preferenziale è abilitato sul profilo di lavoro. Ad esempio, un'organizzazione potrebbe avere un accordo con un operatore per cui i dati di lavoro vengono inviati tramite un servizio di rete dell'operatore dedicato all'uso aziendale (ad esempio, uno slice aziendale sulle reti 5G). Questo non ha effetto sui dispositivi completamente gestiti.

Disabilitato: Il servizio di rete preferenziale è disabilitato sul profilo di lavoro.

Abilitato: Il servizio di rete preferenziale è abilitato sul profilo di lavoro.

> Se utilizzi lo slicing della rete aziendale, configura anche la **Configurazione dello slicing della rete 5G** nel pannello della policy **Cellulare** e assegna le app a uno slice utilizzando l'impostazione **Rete preferenziale**.

19. Proxy globale consigliato

Il proxy HTTP globale indipendente dalla rete. In genere, i proxy dovrebbero essere configurati per singola rete nelle impostazioni Wi-Fi. Un proxy globale può essere utile per configurazioni insolite, come il filtraggio interno generale. Il proxy globale è solo un suggerimento e alcune app potrebbero ignorarlo.

Disabilitato

Proxy diretto

Proxy auto-config (PAC)

19.1. Host

L'host del proxy diretto.

19.2. Porta

La porta del proxy diretto.

19.3. URI PAC

L'URI dello script PAC utilizzato per configurare il proxy.

19.4. Host esclusi

Per un proxy diretto, gli host per i quali il proxy viene saltato. I nomi degli host possono contenere caratteri jolly come ***.example.com**.

Usa **Aggiungi host escluso** per aggiungere le voci (disponibile solo per il proxy diretto).

Configurazioni WiFi

Definisci le configurazioni delle reti Wi-Fi che il sistema applicherà sui dispositivi. Usa **Aggiungi configurazione Wi-Fi** per creare una voce e rimuoverla con l'azione di eliminazione.

20. Campi di configurazione Wi-Fi

Ogni configurazione include:

Nome configurazione: Obbligatorio.

SSID: Obbligatorio.

Connessione automatica: Indica se la rete deve connettersi automaticamente quando è nell'intervallo di copertura.

Fast Transition: Indica se il client deve tentare di utilizzare la funzione Fast Transition (IEEE 802.11r-2008) con la rete.

SSID nascosto: Indica se l'SSID verrà trasmesso.

Modalità randomizzazione MAC: Hardware o Automatica (Android 13+).

20.1. Sicurezza

Opzioni di sicurezza Wi-Fi:

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

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

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

Modalità WPA3 a 192 bit: Rete WPA-EAP che consente solo la modalità WPA3 a 192 bit.

20.2. Passphrase (Pre-Shared Key)

Viene mostrata quando la sicurezza è impostata su **WEP-PSK** o **WPA-PSK**. La passphrase è obbligatoria.

20.3. Metodo EAP (Enterprise)

Viene mostrata quando la sicurezza è impostata su **WPA-EAP** o **Modalità WPA3 a 192 bit**. Seleziona un metodo EAP esterno:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticazione di fase 2

Mostrata per i metodi di tunneling esterni (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenziali EAP dagli utenti

Quando abilitata, il sistema applica automaticamente le credenziali EAP sui dispositivi su base utente. È possibile configurare le credenziali dell'utente nella sezione **Utenti**.

20.6. Certificato client

Per **EAP-TLS**, è possibile assegnare un certificato client utilizzato per l'autenticazione Wi-Fi. Per ulteriori informazioni, leggi la pagina **Gestione certificati**.

Se un certificato è già assegnato, puoi usare **Apri certificato** per visualizzarlo o **Cambia certificato** per selezionarne uno diverso.

In alternativa, puoi specificare **l'alias della coppia di chiavi del certificato client**, che fa riferimento a un certificato client memorizzato nel keychain di Android e consentito per l'autenticazione Wi-Fi.

> Se vengono impostati sia **Certificato client** che **Alias della coppia di chiavi del certificato client**, l'alias della coppia di chiavi viene ignorato.

20.7. Identità

Identità dell'utente. Per i protocolli esterni di tunneling (PEAP, EAP-TTLS), questa viene utilizzata per l'autenticazione all'interno del tunnel, mentre l'**Identità anonima** viene utilizzata per l'identità EAP all'esterno del tunnel. Per i protocolli esterni senza tunneling, questa viene utilizzata per l'identità EAP.

20.8. Identità anonima

Solo per i protocolli di tunneling, questa indica l'identità dell'utente presentata al protocollo esterno.

20.9. Password

Password dell'utente. Se non specificata, l'impostazione predefinita è richiedere l'inserimento all'utente.

20.10. Certificati CA del server

Elenco dei certificati CA da utilizzare per verificare la catena di certificazione dell'host. Almeno un certificato CA deve corrispondere. Per ulteriori informazioni, leggi la pagina **Gestione dei certificati**.

Usa **Aggiungi certificato CA del server** per aggiungere voci e rimuoverle con l'azione di eliminazione.

20.11. Corrispondenze suffisso di dominio

Un elenco di vincoli per il nome di dominio del server. Le voci vengono utilizzate come requisiti di corrispondenza del suffisso rispetto al nome (o ai nomi) DNS del nome soggetto alternativo di un certificato di un server di autenticazione.

Revision #7
Created 2026-06-24 08:05:06 UTC by Admin
Updated 2026-06-24 09:39:31 UTC by Admin