Rete

In questa sezione puoi configurare le policy relative alla rete.

> Le configurazioni Wi-Fi possono essere fornite e gestite dal sistema tramite **Configurazioni WiFi**. A seconda del valore impostato su **Configura Wi-Fi**, gli utenti possono avere un controllo limitato o nullo sull'aggiunta/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 utente (predefinita): All'utente è consentito abilitare/disabilitare il Wi-Fi.

Attivato: Il Wi-Fi è attivo e all'utente non è consentito disattivarlo (Android 13+).

Disattivato: Il Wi-Fi è disattivato e all'utente non è consentito attivarlo (Android 13+).

2. Livello di sicurezza Wi-Fi minimo

Il livello di sicurezza minimo richiesto delle reti Wi-Fi a cui il dispositivo può connettersi. Supportato su Android 13 e versioni successive, per i dispositivi con gestione completa e i profili di lavoro sui dispositivi di proprietà dell'azienda.

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

Rete personale: Non consente le reti Wi-Fi aperte; richiede almeno la sicurezza personale (ad esempio WPA2-PSK).

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

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

3. Stato ultra wideband (UWB)

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

Scelta utente (predefinita): All'utente è consentito attivare o disattivare UWB.

Disattivato: UWB è disattivato e all'utente non è consentito attivarlo o disattivarlo tramite le impostazioni (Android 14+).

Gestione della connettività del dispositivo

4. Condivisione Bluetooth

Controlla se la condivisione Bluetooth è consentita.

Consentito: La condivisione Bluetooth è consentita (predefinito sui dispositivi con gestione completa, Android 8+).

Non consentito: La condivisione Bluetooth non è consentita (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 ha il controllo completo, limitato o nullo sulla configurazione delle reti Wi-Fi.

Consenti la configurazione del Wi-Fi (predefinito): All'utente è consentito configurare il Wi-Fi.

Non consentire l'aggiunta di configurazioni Wi-Fi: L'aggiunta di nuove configurazioni Wi-Fi non è consentita. L'utente può passare da una rete già configurata all'altra (Android 13+; gestione completa e profili di lavoro su dispositivi aziendali).

Non consentire la configurazione del Wi-Fi: Non consente di configurare le reti Wi-Fi. Per i dispositivi con gestione completa, rimuove le reti configurate dall'utente e mantiene solo le

reti configurate tramite **Configurazioni WiFi**. Per i profili di lavoro sui dispositivi aziendali, le reti esistenti non sono interessate, ma gli utenti non possono aggiungere/rimuovere/modificare le reti Wi-Fi.

> Quando la configurazione del Wi-Fi è disattivata e il dispositivo non riesce a connettersi all'avvio, il sistema può mostrare la **procedura di emergenza per la 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 dell'azienda con Android 13 e versioni successive.

Consenti (predefinito): All'utente è consentito usare Wi-Fi Direct.

Non consentire: All'utente non è consentito usare Wi-Fi Direct.

7. Impostazioni di tethering

Controlla le impostazioni di tethering. In base al valore impostato, all'utente è parzialmente o completamente vietato usare diverse forme di tethering.

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

Non consentire il tethering Wi-Fi: Vieta all'utente di usare il tethering Wi-Fi (dispositivi aziendali Android 13+).

Non consentire alcun tethering: Vieta tutte le forme di tethering (gestione completa + profili di lavoro su dispositivi aziendali).

8. Policy SSID Wi-Fi

Restrizioni sugli SSID Wi-Fi a cui il dispositivo può connettersi (questo non influisce sulle reti che possono essere configurate sul dispositivo). Supportato sui dispositivi di proprietà dell'azienda con Android 13 e versioni successive.

Lista di blocco SSID (predefinita): Il dispositivo non può connettersi a nessuna rete Wi-Fi il cui SSID è elencato, ma può connettersi ad altre reti.

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

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

Nell'interfaccia dell'editor delle policy, l'elenco degli SSID è etichettato come **SSID Wi-Fi consentiti** per le liste di consentiti e **SSID Wi-Fi non consentiti** per le liste di blocco.

9. Impostazioni di roaming Wi-Fi

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

Ogni voce include:

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

Modalità di roaming Wi-Fi: Predefinita / Disattivata / Aggressiva. Disattivata e Aggressiva richiedono Android 15+ e sono supportate solo sui dispositivi con gestione completa e sui profili di lavoro dei dispositivi aziendali.

Restrizioni di rete

10. Bluetooth disattivato

Indica se il Bluetooth è disattivato. Preferisci questa impostazione a Configurazione Bluetooth disattivata, perché la configurazione Bluetooth disattivata può essere aggirata dall'utente.

11. Condivisione contatti Bluetooth disattivata

Indica se la condivisione dei contatti Bluetooth è disattivata.

12. Configurazione Bluetooth disattivata

Indica se la configurazione del Bluetooth è disattivata.

13. Ripristino rete disattivato

Indica se il ripristino delle impostazioni di rete è disattivato.

14. Beam in uscita disattivato

Indica se l'uso di NFC per inviare dati dalle app tramite beam è disattivato.

VPN

15. App VPN Always On

Specifica un nome pacchetto VPN Always On per assicurarti che i dati delle app gestite specificate passino sempre attraverso una VPN configurata.

> Nota: questa funzionalità richiede la distribuzione di un client VPN che supporti sia la funzionalità Always On sia quella VPN per app.

16. Blocco VPN

Impedisce la connessione di rete quando la VPN non è connessa.

17. Configurazione VPN disattivata

Indica se la configurazione della VPN è disattivata.

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 può avere un accordo con un operatore affinché i dati di lavoro vengano 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 con gestione completa.

Disattivato: Il servizio di rete preferenziale è disattivato sul profilo di lavoro.

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

> Se usi il network slicing aziendale, configura anche **Configurazione del network slicing 5G** nel pannello della policy **Cellulare** e assegna le app a uno slice tramite la loro impostazione **Rete preferenziale**.

19. Proxy globale consigliato

Il proxy HTTP globale indipendente dalla rete. In genere, i proxy dovrebbero essere configurati per rete nelle configurazioni WiFi. Un proxy globale può essere utile per configurazioni particolari come il filtraggio interno generale. Il proxy globale è solo un consiglio e alcune app potrebbero ignorarlo.

Disattivato

Proxy diretto

Configurazione automatica del proxy (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 usato per configurare il proxy.

19.4. Host esclusi

Per un proxy diretto, gli host per cui il proxy viene ignorato. I nomi host possono contenere caratteri jolly come ***.example.com**.

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

Configurazioni Wi-Fi

Definisci le configurazioni di rete 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 della configurazione Wi-Fi

Ogni configurazione include:

Nome configurazione: obbligatorio.

SSID: obbligatorio.

Connessione automatica: indica se connettersi automaticamente alla rete quando è nel raggio d'azione.

Transizione rapida: indica se il client deve tentare di usare la transizione rapida (IEEE 802.11r-2008) con la rete.

SSID nascosto: indica se l'SSID verrà trasmesso.

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

20.1. Sicurezza

Opzioni di sicurezza Wi-Fi:

WEP-PSK: WEP (chiave precondivisa).

WPA-PSK: WPA/WPA2/WPA3-Personal (chiave precondivisa).

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 (chiave precondivisa)

Visualizzato quando la sicurezza è **WEP-PSK** o **WPA-PSK**. La passphrase è obbligatoria.

20.3. Metodo EAP (Enterprise)

Visualizzato quando la sicurezza è **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 fase 2

Visualizzato per i metodi esterni con tunneling (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenziali EAP dagli utenti

Se attivato, il sistema applica automaticamente le credenziali EAP sui dispositivi per singolo utente. Puoi configurare le credenziali degli utenti nella sezione **Utenti**.

20.6. Certificato client

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

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

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

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

20.7. Identità

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

all'esterno del tunnel. Per i protocolli esterni senza tunneling, viene usata per l'identità EAP.

20.8. Identità anonima

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

20.9. Password

Password dell'utente. Se non specificata, per impostazione predefinita viene richiesta all'utente.

20.10. Certificati CA del server

Elenco dei certificati CA da usare per verificare la catena di certificati 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 dei suffissi di dominio

Un elenco di vincoli per il nome di dominio del server. Le voci vengono usate come requisiti di corrispondenza dei suffissi rispetto ai nomi DNS del nome alternativo del soggetto di un certificato del server di autenticazione.

Revision #7
Created 2026-11-10 15:13:00 UTC by Admin
Updated 2026-11-12 09:52:45 UTC by Admin