

Rete

In questa sezione, puoi configurare le policy relative alla rete.

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

Stato della radio del dispositivo

Stato di Wi-Fi

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

Scelta dell'utente (predefinito): all'utente è consentito abilitare o disabilitare il Wi-Fi.

Attivato: il Wi-Fi è attivo e l'utente non può disabilitarlo (Android 13 e versioni successive).

Disattivato: il Wi-Fi è disattivato e l'utente non può riattivarlo (Android 13 e versioni successive).

2. Livello minimo di sicurezza Wi-Fi

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

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

Rete personale: Impedisce la connessione a reti Wi-Fi aperte; richiede almeno una sicurezza di livello 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; è l'opzione più restrittiva.

3. Stato della tecnologia Ultra Wideband (UWB)

Controlla lo stato dell'impostazione Ultra Wideband e se l'utente può attivare o disattivare questa funzionalità.

Scelta dell'utente (predefinita): L'utente può attivare o disattivare l'Ultra Wideband.

Disattivato: UWB è disattivato e l'utente non può attivarlo o disattivarlo tramite le impostazioni (Android 14 e versioni successive).

Gestione della connettività dei dispositivi

4. Condivisione via Bluetooth

Controlla se la condivisione via Bluetooth è consentita.

Consentito: La condivisione via Bluetooth è consentita (impostazione predefinita per i dispositivi completamente gestiti, Android 8+).

Non consentito: La condivisione via Bluetooth non è consentita (impostazione predefinita per i profili aziendali, Android 8+).

5. Configurare 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): L'utente può 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 all'altra tra quelle già configurate (Android 13+; profili di lavoro aziendali e dispositivi di proprietà dell'azienda).

Non consentire la configurazione di reti Wi-Fi: Impedisce la configurazione di nuove reti Wi-Fi. Per i dispositivi gestiti centralmente, questa opzione rimuove le reti configurate dall'utente e mantiene solo le reti configurate tramite **configurazioni Wi-Fi**. Per i profili di lavoro aziendali, le reti esistenti non vengono modificate, ma gli utenti non possono aggiungere, rimuovere o modificare le reti Wi-Fi.

Quando la configurazione Wi-Fi è disabilitata e il dispositivo non riesce a connettersi all'avvio, il sistema può mostrare la **funzione di bypass della rete** per consentire all'utente di connettersi temporaneamente e aggiornare le policy.

6. Impostazioni Wi-Fi Direct

Controlli per la configurazione e l'utilizzo delle impostazioni Wi-Fi Direct. Supportato su dispositivi aziendali con Android 13 e versioni successive.

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

Non consentire: L'utente non può utilizzare Wi-Fi Direct.

7. Impostazioni di tethering

Controlla le impostazioni di tethering. In base al valore impostato, l'utente può essere parzialmente o completamente impedito di utilizzare diverse forme di tethering.

Consenti tutte le modalità di tethering (predefinito): Consente la configurazione e l'utilizzo di tutte le forme di tethering.

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

Disabilita tutte le funzionalità di tethering: Impedisce l'utilizzo di qualsiasi tipo di tethering (dispositivi completamente gestiti e profili di lavoro aziendali).

8. Policy relativa all'SSID Wi-Fi

Restrizioni sulle reti Wi-Fi a cui il dispositivo può connettersi (questo non influisce sulle reti che possono essere configurate sul dispositivo). Supportato su dispositivi aziendali con Android 13 e versioni successive.

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

Elenco delle reti Wi-Fi consentite: Il dispositivo può connettersi solo alle reti con SSID presenti nell'elenco. L'elenco degli SSID non deve essere vuoto.

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

Nell'interfaccia utente 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 per il 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'identificativo SSID a cui si applica l'impostazione di roaming (obbligatorio).

Modalità roaming Wi-Fi: Predefinita / Disabilitata / Aggressiva. Le opzioni Disabilitata e Aggressiva richiedono Android 15 o superiore e sono supportate solo su dispositivi completamente gestiti e profili di lavoro su dispositivi aziendali.

Restrizioni di rete

Bluetooth disabilitato

Bluetooth disabilitato. Preferire questa impostazione rispetto a "Configurazione Bluetooth disabilitata" perché quest'ultima può essere modificata dall'utente.

11. Condivisione contatti Bluetooth disabilitata

Se la condivisione contatti tramite Bluetooth è disabilitata.

12. Configurazione Bluetooth disabilitata

La configurazione di Bluetooth è disabilitata.

13. Ripristino di rete disabilitato

Se il ripristino delle impostazioni di rete è disabilitato.

14. Trasmissione in uscita disabilitata

Se l'utilizzo di NFC per trasferire dati dalle app è disabilitato.

VPN

App VPN sempre attiva

Specifica un nome pacchetto VPN sempre attiva per garantire che i dati delle app gestite indicate vengano sempre trasmessi tramite una VPN configurata.

Nota: questa funzionalità richiede la distribuzione di un client VPN che supporti sia la funzionalità VPN sempre attiva che le funzionalità VPN specifiche per app.

16. Blocco VPN

Impedisce la connessione alla rete quando la VPN non è attiva.

17. Configurazione VPN disabilitata

La configurazione VPN è disabilitata.

Servizi proxy e di rete

18. Servizio di rete preferenziale

Abilita o disabilita il servizio di rete preferenziale sul profilo di lavoro. Ad esempio, un'organizzazione potrebbe avere un accordo con un operatore che prevede l'utilizzo di una rete dedicata ai servizi aziendali (ad esempio, una rete aziendale su reti 5G) per il traffico dati aziendale. Questa impostazione non ha effetto sui dispositivi completamente gestiti.

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

Attivato: Il servizio di rete preferenziale è attivo nel profilo di lavoro.

Se utilizzi il network slicing aziendale, configura anche **Configurazione del Network Slicing 5G** nella sezione **Cellulare** e assegna le applicazioni a una slice utilizzando la loro impostazione **Rete Preferenziale**.

19. Proxy globale consigliata

Il proxy HTTP globale indipendente dalla rete. In genere, i proxy dovrebbero essere configurati per ogni rete nelle impostazioni Wi-Fi. Un proxy globale può essere utile per configurazioni particolari, come la filtrazione interna generale. Il proxy globale è solo un suggerimento e alcune app potrebbero ignorarlo.

Disabilitato

Proxy diretto

Proxy di configurazione automatica (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, sono gli host per i quali il proxy viene ignorato. I nomi host possono contenere caratteri jolly come ***.example.com**.

Utilizza **Aggiungi host esclusi** per aggiungere voci (disponibile solo per proxy diretto).

Configurazioni Wi-Fi

Definisci le configurazioni di rete Wi-Fi che il sistema applicherà sui dispositivi. Utilizza **Aggiungi configurazione Wi-Fi** per creare una voce e rimuovila con l'azione di eliminazione.

20. Campi di configurazione Wi-Fi

Ogni configurazione include:

Nome della configurazione: Obbligatorio.

SSID: Obbligatorio.

Connessione automatica: Indica se la rete deve connettersi automaticamente quando è disponibile.

Transizione rapida: Indica se il dispositivo deve tentare di utilizzare la transizione rapida (IEEE 802.11r-2008) con la rete.

SSID nascosto: Indica se il nome della rete (SSID) verrà trasmesso.

Modalità di randomizzazione MAC: Hardware o Automatica (Android 13 e versioni successive).

20.1. Sicurezza

Opzioni di sicurezza Wi-Fi:

WEP-PSK: WEP (chiave precondivisa).

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

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Protocollo di autenticazione estendibile).

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

20.2. Password (Chiave precondivisa)

Mostrato quando la sicurezza è **WEP-PSK** o **WPA-PSK**. La password è richiesta.

20.3. Metodo EAP (Enterprise)

Mostrato quando la sicurezza è **WPA-EAP** o **WPA3 a 192 bit**. Seleziona un metodo EAP esterno:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticazione, fase 2

Mostrato per il tunneling dei metodi esterni (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenziali EAP fornite dagli utenti

Quando abilitata, il sistema applica automaticamente le credenziali EAP ai dispositivi, configurandole su base individuale per ogni utente. È possibile configurare le credenziali degli utenti nella sezione **Utenti**.

20.6. Certificato client

Per **EAP-TLS**, è possibile assegnare un certificato client utilizzato per l'autenticazione Wi-Fi. Per maggiori informazioni, consulta la pagina [Gestione dei certificati](#).

Se un certificato è già assegnato, è possibile utilizzare **Apri certificato** per visualizzarlo oppure **Cambia certificato** per selezionarne uno diverso.

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

Se sono impostati sia il **certificato client** sia **l'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 di tunneling esterni (PEAP, EAP-TTLS), questo viene utilizzato per l'autenticazione all'interno del tunnel, e **l'identità anonima** viene utilizzata per l'identità EAP all'esterno del tunnel. Per i protocolli esterni che non utilizzano il tunneling, questo viene utilizzato per l'identità EAP.

20.8. Identità anonima

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

20.9. Password

Password dell'utente. Se non specificata, verrà richiesto l'inserimento da parte dell'utente.

20.10. Certificati CA del server

Elenco dei certificati CA da utilizzare per verificare la catena di certificati dell'host. Almeno un certificato CA deve corrispondere. Per maggiori informazioni, consultare la pagina [Gestione dei certificati](#).

Utilizza **Aggiungi certificato CA del server** per aggiungere elementi e rimuoverli utilizzando l'azione di eliminazione.

20.11. Il suffisso del dominio corrisponde

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

Revision #39

Created 2025-12-17 09:32:06 UTC by Admin

Updated 2026-06-11 16:17:33 UTC by Admin