Networking

In this section, you can configure networking-related policies.

> Wi-Fi configurations can be provisioned and managed by the system via **WiFi configurations**. Depending on the value set on **Configure Wi-Fi**, users may have limited or no control over adding/modifying networks.

Device radio state

1. Wi?Fi state

Controls current state of Wi-Fi and if the user can change its state.

User choice (default): User is allowed to enable/disable Wi-Fi.

Enabled: Wi-Fi is on and the user is not allowed to turn it off (Android 13+).

Disabled: Wi-Fi is off and the user is not allowed to turn it on (Android 13+).

2. Minimum Wi?Fi security level

The minimum required security level of Wi-Fi networks that the device can connect to. Supported on Android 13 and above, for fully managed devices and work profiles on company-owned devices.

Open network (default): The device can connect to all types of Wi-Fi networks.

Personal network: Disallows open Wi-Fi networks; requires at least personal security (for example WPA2-PSK).

Enterprise network: Requires enterprise EAP networks; disallows Wi-Fi networks below this security level.

192-bit enterprise network: Requires 192-bit enterprise networks; strictest option.

3. Ultra wideband (UWB) state

Controls the state of the ultra wideband setting and whether the user can toggle it on or off.

User choice (default): The user is allowed to toggle UWB on or off.

Disabled: UWB is disabled and the user is not allowed to toggle it via settings (Android 14+).

Device connectivity management

4. Bluetooth sharing

Controls whether Bluetooth sharing is allowed.

Allowed: Bluetooth sharing is allowed (default on fully managed devices, Android 8+).

Disallowed: Bluetooth sharing is disallowed (default on work profiles, Android 8+).

5. Configure Wi?Fi

Controls Wi-Fi configuring privileges. Depending on the selected option, the user has full, limited, or no control in configuring Wi-Fi networks.

Allow configuring Wi-Fi (default): The user is allowed to configure Wi-Fi.

Disallow add Wi-Fi config: Adding new Wi-Fi configurations is disallowed. The user can switch between already configured networks (Android 13+; fully managed and company-owned work profiles).

Disallow configuring Wi-Fi: Disallows configuring Wi-Fi networks. For fully managed devices this removes user-configured networks and retains only networks configured via **WiFi configurations**. For company-owned work profiles, existing networks are not affected but users cannot add/remove/modify Wi-Fi networks.

> When configuring Wi-Fi is disabled and the device cannot connect at boot time, the system can show the **network escape hatch** to let the user temporarily connect and refresh policy.

6. Wi?Fi direct settings

Controls configuring and using Wi-Fi direct settings. Supported on company-owned devices running Android 13 and above.

Allow (default): The user is allowed to use Wi-Fi direct.

Disallow: The user is not allowed to use Wi-Fi direct.

7. Tethering settings

Controls tethering settings. Based on the value set, the user is partially or fully disallowed from using different forms of tethering.

Allow all tethering (default): Allows configuration and use of all forms of tethering.

Disallow Wi-Fi tethering: Disallows the user from using Wi-Fi tethering (company-owned Android 13+).

Disallow all tethering: Disallows all forms of tethering (fully managed + company-owned work profiles).

8. Wi?Fi SSID policy

Restrictions on which Wi-Fi SSIDs the device can connect to (this does not affect which networks can be configured on the device). Supported on company-owned devices running Android 13 and above.

SSID denylist (default): The device cannot connect to any Wi-Fi network whose SSID is listed, but can connect to other networks.

SSID allowlist: The device can connect only to the SSIDs listed. The SSID list must not be empty.

Use **Add SSID** to add entries. Depending on the selected policy type, the list is interpreted as allowed or denied SSIDs.

In the Policy Editor UI, the SSID list is labeled **Allowed Wi-Fi SSIDs** for allowlists and **Denied Wi-Fi SSIDs** for denylists.

9. Wi?Fi roaming settings

Configure Wi-Fi roaming mode per SSID. Use **Add Wi-Fi roaming setting** to create entries.

Each entry includes:

SSID: The SSID to which the roaming setting applies (required).

Wi-Fi roaming mode: Default / Disabled / Aggressive. Disabled and Aggressive require Android 15+ and are supported only on fully managed devices and work profiles on company-owned devices.

Network restrictions

10. Bluetooth disabled

Whether bluetooth is disabled. Prefer this setting over Bluetooth config disabled because Bluetooth config disabled can be bypassed by the user.

11. Bluetooth contact sharing disabled

Whether bluetooth contact sharing is disabled.

12. Bluetooth config disabled

Whether configuring bluetooth is disabled.

13. Network reset disabled

Whether resetting network settings is disabled.

14. Outgoing beam disabled

Whether using NFC to beam data from apps is disabled.

VPN

15. Always On VPN app

Specify an Always On VPN package name to ensure that data from specified managed apps will always go through a configured VPN.

> Note: This feature requires deploying a VPN client that supports both Always On and per-app VPN features.

16. VPN lockdown

Disallows networking when the VPN is not connected.

17. VPN config disabled

Whether configuring VPN is disabled.

Proxy and network services

18. Preferential network service

Controls whether preferential network service is enabled on the work profile. For example, an organization may have an agreement with a carrier that work data is sent via a carrier network service dedicated for enterprise use (for example, an enterprise slice on 5G networks). This has no effect on fully managed devices.

Disabled: Preferential network service is disabled on the work profile.

Enabled: Preferential network service is enabled on the work profile.

> If you use enterprise network slicing, also configure **5G Network Slicing Configuration** under the **Cellular** policy panel and assign apps to a slice using their **Preferential Network** setting.

19. Recommended global proxy

The network-independent global HTTP proxy. Typically, proxies should be configured per-network in WiFi configurations. A global proxy may be useful for unusual configurations like general internal filtering. The global proxy is only a recommendation and some apps may ignore it.

Disabled

Direct proxy

Proxy auto-config (PAC)

19.1. Host

The host of the direct proxy.

19.2. Port

The port of the direct proxy.

19.3. PAC URI

The URI of the PAC script used to configure the proxy.

19.4. Excluded hosts

For a direct proxy, the hosts for which the proxy is bypassed. Host names may contain wildcards such as ***.example.com**.

Use **Add excluded host** to add entries (available for direct proxy only).

WiFi configurations

Define Wi-Fi network configurations that the system will apply on devices. Use **Add Wi-Fi configuration** to create an entry and remove it with the delete action.

20. Wi?Fi configuration fields

Each configuration includes:

Configuration name: Required.

SSID: Required.

Auto connect: Whether the network should be connected to automatically when in range.

Fast Transition: Whether the client should attempt to use Fast Transition (IEEE 802.11r-2008) with the network.

Hidden SSID: Whether the SSID will be broadcast.

MAC randomization mode: Hardware or Automatic (Android 13+).

20.1. Security

Wi-Fi security options:

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 mode: WPA-EAP network allowing only WPA3 192-bit mode.

20.2. Passphrase (Pre?Shared Key)

Shown when Security is **WEP-PSK** or **WPA-PSK**. The passphrase is required.

20.3. EAP method (Enterprise)

Shown when Security is **WPA-EAP** or **WPA3 192-bit mode**. Select one EAP outer method:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Phase 2 authentication

Shown for tunneling outer methods (**EAP-TTLS** and **PEAP**).

MSCHAPv2

PAP

20.5. EAP credentials from users

When enabled, the system automatically applies EAP credentials on devices on a per-user basis. You can configure user credentials in the **Users** section.

20.6. Client certificate

For **EAP-TLS**, you can assign a client certificate used for Wi-Fi authentication. For more information read the **Certificate management** page.

If a certificate is already assigned, you can use **Open certificate** to view it or **Change certificate** to select a different one.

Alternatively, you can specify **Client certificate key pair alias**, which references a client certificate stored in the Android keychain and allowed for Wi-Fi authentication.

> If both **Client certificate** and **Client certificate key pair alias** are set, the key pair alias is ignored.

20.7. Identity

Identity of user. For tunneling outer protocols (PEAP, EAP-TTLS), this is used to authenticate inside the tunnel, and **Anonymous identity** is used for the EAP identity outside the tunnel. For non-tunneling outer protocols, this is used for the EAP identity.

20.8. Anonymous identity

For tunneling protocols only, this indicates the identity of the user presented to the outer protocol.

20.9. Password

Password of user. If not specified, defaults to prompting the user.

20.10. Server CA certificates

List of CA certificates to be used for verifying the host’s certificate chain. At least one CA certificate must match. For more information read the **Certificate management** page.

Use **Add Server CA certificate** to add entries and remove them with the delete action.

20.11. Domain suffix matches

A list of constraints for the server domain name. The entries are used as suffix match requirements against the DNS name(s) of the alternative subject name of an authentication server certificate.

Revision #53
Created 2022-03-28 10:17:35 UTC by Admin
Updated 2026-06-11 16:16:49 UTC by Admin