网络

在本部分中，你可以配置与网络相关的政策。

Wi‑Fi 配置可以由系统通过 WiFi 配置 预置和管理。根据 配置 Wi‑Fi上设置的值，用户对添加 /
修改网络可能拥有有限的控制权或没有控制权。

设备无线状态

1. Wi‑Fi 状态

控制 Wi‑Fi 的当前状态以及用户是否可以更改其状态。
用户选择（默认） ：允许用户启用 /禁用 Wi‑Fi。
已启用 ：Wi‑Fi 处于开启状态，不允许用户将其关闭（ Android 13+）。
已禁用 ：Wi‑Fi 处于关闭状态，不允许用户将其开启（ Android 13+）。

2. 最低 Wi‑Fi 安全级别

设备可连接的 Wi‑Fi 网络的最低要求安全级别。在 Android 13
及以上版本上，支持完全受管设备以及公司所有设备上的工作配置文件。
开放网络（默认） ：设备可以连接所有类型的 Wi‑Fi 网络。
个人网络 ：不允许开放 Wi‑Fi 网络；要求至少达到个人安全级别（例如 WPA2‑PSK）。
企业网络 ：要求企业 EAP 网络；不允许低于此安全级别的 Wi‑Fi 网络。
192 位企业网络 ：要求 192 位企业网络；这是最严格的选项。

3. 超宽带 (UWB) 状态

控制超宽带设置的状态以及用户是否可以将其开启或关闭。

用户选择（默认） ：允许用户开启或关闭 UWB。

已禁用 ： UWB 已禁用，不允许用户通过设置将其开启（ Android 14+）。

设备连接管理

4. 蓝牙共享

控制是否允许蓝牙共享。

允许 ：允许蓝牙共享（完全受管设备上的默认值， Android 8+）。

不允许 ：不允许蓝牙共享（工作配置文件上的默认值， Android 8+）。

5. 配置 Wi‑Fi

控制 Wi‑Fi 配置权限。根据所选选项，用户在配置 Wi‑Fi 网络时拥有完全、有限或无控制权。

允许配置 Wi‑Fi（默认） ：允许用户配置 Wi‑Fi。

不允许添加 Wi‑Fi 配置 ：不允许添加新的 Wi‑Fi 配置。用户可以在已配置的网络之间切换（ Android
13+；完全受管和公司所有的工作配置文件）。

不允许配置 Wi‑Fi：不允许配置 Wi‑Fi
网络。对于完全受管设备，这会移除用户配置的网络，仅保留通过 WiFi 配置
配置的网络。对于公司所有的工作配置文件，现有网络不受影响，但用户无法添加 /移除 /修改 Wi‑Fi
网络。

当禁用配置 Wi‑Fi 且设备在启动时无法连接时，系统可以显示 网络逃生通道
，让用户临时连接并刷新政策。

6. Wi‑Fi 直连设置

控制 Wi‑Fi 直连设置的配置和使用。在运行 Android 13 及以上版本的公司所有设备上受支持。

允许（默认）：允许用户使用 Wi-Fi 直连。

不允许：不允许用户使用 Wi-Fi 直连。

7. 网络共享设置

控制网络共享设置。根据设置的值，用户会被部分或完全禁止使用不同形式的网络共享。

允许所有网络共享（默认）：允许配置和使用所有形式的网络共享。

不允许 **Wi-Fi** 网络共享：不允许用户使用 Wi-Fi 网络共享（公司所有 Android 13+）。

不允许所有网络共享：不允许所有形式的网络共享（完全受管 + 公司所有的工作配置文件）。

8. Wi-Fi SSID 政策

限制设备可以连接到哪些 Wi-Fi SSID（这不会影响可以在设备上配置哪些网络）。在运行 Android 13 及以上版本的公司所有设备上受支持。

SSID 拒绝列表（默认）：设备无法连接到任何 SSID 已列出的 Wi-Fi 网络，但可以连接到其他网络。

SSID 允许列表：设备只能连接到已列出的 SSID。SSID 列表不能为空。

使用 添加 **SSID**添加条目。根据所选政策类型，该列表会被解释为允许或拒绝的 SSID。

在政策编辑器界面中，对于允许列表，SSID 列表标记为 允许的 **Wi-Fi SSID**；对于拒绝列表，标记为 拒绝的 **Wi-Fi SSID**。

9. Wi-Fi 漫游设置

按 SSID 配置 Wi-Fi 漫游模式。使用 添加 **Wi-Fi** 漫游设置 创建条目。

每个条目包括：

SSID：漫游设置适用的 SSID（必填）。

Wi-Fi 漫游模式：默认 / 已禁用 / 积极。已禁用和积极需要 Android 15+，并且仅在完全受管设备和公司所有设备上的工作配置文件中受支持。

网络限制

10. 蓝牙已禁用

是否禁用蓝牙。优先使用此设置而不是 “蓝牙配置已禁用 ”，因为用户可以绕过 “蓝牙配置已禁用 ”。

11. 蓝牙联系人共享已禁用

是否禁用蓝牙联系人共享。

12. 蓝牙配置已禁用

是否禁用蓝牙配置。

13. 网络重置已禁用

是否禁用重置网络设置。

14. 传出 Beam 已禁用

是否禁用使用 NFC 从应用传输数据。

VPN

15. 始终开启的 VPN 应用

指定始终开启的 VPN 包名，以确保指定受管应用的数据始终通过已配置的 VPN。

注意：此功能需要部署同时支持始终开启和按应用 VPN 功能的 VPN 客户端。

16. VPN 锁定

当 VPN 未连接时不允许联网。

17. VPN 配置已禁用

是否禁用 VPN 配置。

代理和网络服务

18. 优先网络服务

控制是否在工作配置文件上启用优先网络服务。例如，组织可能与运营商达成协议，通过专供企业使用的运营
商网络服务发送工作数据（例如 5G 网络上的企业切片）。这对完全受管设备没有影响。
已禁用 ：工作配置文件上的优先网络服务已禁用。
已启用 ：工作配置文件上的优先网络服务已启用。

如果你使用企业网络切片，还请在 蜂窝网络 政策面板下配置 5G 网络切片配置 ，并使用应用的
优先网络 设置将其分配到切片。

19. 推荐的全局代理

与网络无关的全局 HTTP 代理。通常，应在 WiFi
配置中按网络配置代理。全局代理可能对常规内部过滤等特殊配置有用。全局代理仅是建议，某些应用可能会
忽略它。
已禁用
直接代理
代理自动配置 (PAC)

19.1. 主机

直接代理的主机。

19.2. 端口

直接代理的端口。

19.3. PAC URI

用于配置代理的 PAC 脚本 URI。

19.4. 排除的主机

对于直接代理，指绕过代理的主机。主机名可以包含通配符，例如 ***.example.com**。

使用 添加排除的主机 添加条目（仅适用于直接代理）。

Wi-Fi 配置

定义系统将在设备上应用的 Wi-Fi 网络配置。使用 添加 **Wi-Fi** 配置 创建条目，并使用删除操作将其移除。

20. Wi-Fi 配置字段

每个配置包括：

配置名称 ：必填。

SSID：必填。

自动连接 ：是否应在网络处于范围内时自动连接。

快速转换 ：客户端是否应尝试使用快速转换 (IEEE 802.11r-2008) 连接网络。

隐藏 **SSID**：SSID 是否会被广播。

MAC 随机化模式 ：硬件或自动 (Android 13+)。

20.1. 安全

Wi-Fi 安全选项：

WEP-PSK：WEP（预共享密钥）。

WPA-PSK：WPA/WPA2/WPA3-Personal（预共享密钥）。

WPA‑EAP：WPA/WPA2/WPA3-Enterprise（可扩展身份验证协议）。
WPA3 192 位模式 ：仅允许 WPA3 192 位模式的 WPA‑EAP 网络。

20.2. 密码短语（预共享密钥）
当安全类型为 WEP‑PSK或WPA‑PSK时显示。密码短语为必填项。

20.3. EAP 方法（企业）
当安全类型为 WPA‑EAP或WPA3 192 位模式 时显示。选择一种 EAP 外部方法： EAP‑TLS
EAP‑TTLS
PEAP
EAP‑SIM
EAP‑AKA

20.4. 第 2 阶段身份验证
仅对隧道外部方法（ EAP‑TTLS和 PEAP）显示。
MSCHAPv2
PAP

20.5. 来自用户的 EAP 凭据
启用后，系统会按用户自动在设备上应用 EAP 凭据。您可以在 用户 部分配置用户凭据。

20.6. 客户端证书
对于 EAP‑TLS，您可以分配用于 Wi‑Fi 身份验证的客户端证书。有关详细信息，请阅读 证书管理 页面。如果已分配证书，您可以使用 打开证书 查看，或使用 更改证书 选择其他证书。
或者，您可以指定 客户端证书密钥对别名 ，它引用存储在 Android 密钥库中并允许用于 Wi‑Fi
身份验证的客户端证书。

如果同时设置了 客户端证书 和客户端证书密钥对别名 ，则忽略密钥对别名。

20.7. 身份

用户身份。对于隧道外部协议 (PEAP、 EAP‑TTLS)，它用于在隧道内进行身份验证，而 匿名身份 用于隧道外的 EAP 身份。对于非隧道外部协议，它用于 EAP 身份。

20.8. 匿名身份

仅适用于隧道协议，表示向外部协议呈现的用户身份。

20.9. 密码

用户密码。如果未指定，则默认提示用户输入。

20.10. 服务器 CA 证书

用于验证主机证书链的 CA 证书列表。至少有一个 CA 证书必须匹配。有关详细信息，请阅读 证书管理 页面。

使用 添加服务器 CA 证书 添加条目，并使用删除操作将其移除。

20.11. 域后缀匹配
服务器域名的约束列表。这些条目用作对身份验证服务器证书备用使用者名称的 DNS
名称进行后缀匹配的要求。

Revision #18
Created 2026-06-24 08:11:27 UTC by Admin
Updated 2026-11-12 09:58:41 UTC by Admin