Сеть

В этом разделе вы можете настроить политики, связанные с сетью.

> Конфигурации Wi-Fi могут предоставляться и управляться системой через **Конфигурации Wi-Fi**. В зависимости от значения параметра **Настройка Wi-Fi** пользователи могут иметь ограниченный контроль над добавлением и изменением сетей или не иметь его вовсе.

Состояние радиомодулей устройства

1. Состояние Wi-Fi

Управляет текущим состоянием Wi-Fi и тем, может ли пользователь изменить его состояние.

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено включать и выключать Wi-Fi.
>
> **Включено**: Wi-Fi включён, и пользователь не может его отключить (Android 13+).
>
> **Отключено**: Wi-Fi отключён, и пользователь не может его включить (Android 13+).

2. Минимальный уровень безопасности Wi-Fi

Минимально требуемый уровень безопасности сетей Wi-Fi, к которым может подключаться устройство. Поддерживается на Android 13 и выше для полностью управляемых устройств и рабочих профилей на устройствах компании.

> **Открытая сеть (по умолчанию)**: Устройство может подключаться ко всем типам сетей Wi-Fi.

Личная сеть: Запрещает открытые сети Wi-Fi; требуется как минимум личная безопасность (например, WPA2-PSK).

Корпоративная сеть: Требуются корпоративные сети EAP; сети Wi-Fi ниже этого уровня безопасности запрещены.

Корпоративная сеть 192-бит: Требуются корпоративные сети 192-бит; самый строгий вариант.

3. Состояние сверхширокополосной связи (UWB)

Управляет состоянием настройки сверхширокополосной связи и тем, может ли пользователь включать или отключать её.

Выбор пользователя (по умолчанию): Пользователю разрешено включать или отключать UWB.

Отключено: UWB отключена, и пользователь не может включать или отключать её через настройки (Android 14+).

Управление подключениями устройства

4. Общий доступ через Bluetooth

Управляет тем, разрешён ли общий доступ через Bluetooth.

Разрешено: Общий доступ через Bluetooth разрешён (по умолчанию на полностью управляемых устройствах, Android 8+).

Запрещено: Общий доступ через Bluetooth запрещён (по умолчанию в рабочих профилях, Android 8+).

5. Настройка Wi-Fi

Управляет правами настройки Wi-Fi. В зависимости от выбранного варианта пользователь имеет полный, ограниченный контроль или не имеет контроля над настройкой сетей Wi-Fi.

Разрешить настройку Wi-Fi (по умолчанию): Пользователю разрешено настраивать Wi-Fi.

Запретить добавление конфигурации Wi-Fi: Добавление новых конфигураций Wi-Fi запрещено. Пользователь может переключаться между уже настроенными сетями (Android 13+; полностью управляемые устройства и рабочие профили на устройствах компании).

Запретить настройку Wi-Fi: Запрещает настройку сетей Wi-Fi. На полностью управляемых устройствах это удаляет сети, настроенные пользователем, и оставляет только сети, настроенные через **Конфигурации Wi-Fi**. В рабочих профилях на устройствах компании существующие сети не затрагиваются, но пользователи не могут добавлять, удалять или изменять сети Wi-Fi.

> Если настройка Wi-Fi отключена и устройство не может подключиться во время загрузки, система может показать **аварийный выход для сети**, чтобы пользователь мог временно подключиться и обновить политику.

6. Настройки Wi-Fi Direct

Управляет настройкой и использованием Wi-Fi Direct. Поддерживается на устройствах компании под управлением Android 13 и выше.

Разрешить (по умолчанию): Пользователю разрешено использовать Wi-Fi Direct.

Запретить: Пользователю не разрешено использовать Wi-Fi Direct.

7. Настройки раздачи интернета

Управляет настройками раздачи интернета. В зависимости от заданного значения пользователю частично или полностью запрещается использовать различные способы раздачи интернета.

Разрешить любую раздачу интернета (по умолчанию): Разрешает настройку и использование всех способов раздачи интернета.

Запретить раздачу интернета по Wi-Fi: Запрещает пользователю использовать раздачу интернета по Wi-Fi (устройства компании, Android 13+).

Запретить любую раздачу интернета: Запрещает все способы раздачи интернета (полностью управляемые устройства и рабочие профили на устройствах компании).

8. Политика SSID Wi-Fi

Ограничения на то, к каким SSID Wi-Fi может подключаться устройство (это не влияет на то, какие сети можно настроить на устройстве). Поддерживается на устройствах компании под управлением Android 13 и выше.

Список запрещённых SSID (по умолчанию): Устройство не может подключаться к сетям Wi-Fi, SSID которых указаны в списке, но может подключаться к другим сетям.

Список разрешённых SSID: Устройство может подключаться только к указанным SSID. Список SSID не должен быть пустым.

Используйте **Добавить SSID**, чтобы добавить записи. В зависимости от выбранного типа политики список интерпретируется как разрешённые или запрещённые SSID.

В интерфейсе редактора политик список SSID обозначен как **Разрешённые SSID Wi-Fi** для списков разрешений и **Запрещённые SSID Wi-Fi** для списков запретов.

9. Настройки роуминга Wi-Fi

Настройте режим роуминга Wi-Fi для каждого SSID. Используйте **Добавить настройку роуминга Wi-Fi**, чтобы создать записи.

Каждая запись включает:

SSID: SSID, к которому применяется настройка роуминга (обязательно).

Режим роуминга Wi-Fi: По умолчанию / Отключено / Агрессивный. Для «Отключено» и «Агрессивный» требуется Android 15+, и они поддерживаются только на полностью управляемых устройствах и в рабочих профилях на устройствах компании.

Сетевые ограничения

10. Bluetooth отключён

Отключён ли Bluetooth. Предпочитайте этот параметр параметру «Конфигурация Bluetooth отключена», поскольку пользователь может обойти отключение конфигурации Bluetooth.

11. Общий доступ к контактам через Bluetooth отключён

Отключён ли общий доступ к контактам через Bluetooth.

12. Конфигурация Bluetooth отключена

Отключена ли настройка Bluetooth.

13. Сброс сетевых настроек отключён

Отключён ли сброс сетевых настроек.

14. Исходящая передача через Beam отключена

Отключена ли передача данных из приложений через NFC Beam.

VPN

15. Приложение Always On VPN

Укажите имя пакета Always On VPN, чтобы данные из указанных управляемых приложений всегда проходили через настроенный VPN.

> Примечание. Для этой функции требуется развернуть VPN-клиент, поддерживающий как Always On, так и VPN для отдельных приложений.

16. Блокировка VPN

Запрещает работу сети, когда VPN не подключён.

17. Конфигурация VPN отключена

Отключена ли настройка VPN.

Прокси и сетевые службы

18. Приоритетная сетевая служба

Управляет тем, включена ли приоритетная сетевая служба в рабочем профиле. Например, у организации может быть соглашение с оператором о том, что рабочие данные передаются через сетевую службу оператора, предназначенную для корпоративного использования (например, корпоративный слайс в сетях 5G). Это не влияет на полностью управляемые устройства.

Отключено: Приоритетная сетевая служба отключена в рабочем профиле.

Включено: Приоритетная сетевая служба включена в рабочем профиле.

> Если вы используете корпоративный слайсинг сети, также настройте **Конфигурация слайсинга сети 5G** на панели политики **Сотовая связь** и назначьте приложения слайсу с помощью их параметра **Приоритетная сеть**.

19. Рекомендуемый глобальный прокси

Глобальный HTTP-прокси, не зависящий от сети. Обычно прокси следует настраивать для каждой сети в конфигурациях Wi-Fi. Глобальный прокси может быть полезен для необычных конфигураций, например для общей внутренней фильтрации. Глобальный прокси является лишь рекомендацией, и некоторые приложения могут его игнорировать.

Отключено

Прямой прокси

Автонастройка прокси (PAC)

19.1. Хост

Хост прямого прокси.

19.2. Порт

Порт прямого прокси.

19.3. URI PAC

URI скрипта PAC, используемого для настройки прокси.

19.4. Исключённые хосты

Для прямого прокси — хосты, для которых прокси обходится. Имена хостов могут содержать подстановочные знаки, например ***.example.com**.

Используйте **Добавить исключённый хост**, чтобы добавить записи (доступно только для прямого прокси).

Конфигурации Wi-Fi

Определите конфигурации сети Wi-Fi, которые система будет применять на устройствах. Используйте **Добавить конфигурацию Wi-Fi**, чтобы создать запись, и удалите её действием удаления.

20. Поля конфигурации Wi-Fi

Каждая конфигурация включает:

Имя конфигурации: обязательно.

SSID: обязательно.

Автоподключение: подключаться ли к сети автоматически, когда она в зоне действия.

Быстрый переход: должен ли клиент пытаться использовать быстрый переход (IEEE 802.11r-2008) при работе с сетью.

Скрытый SSID: будет ли SSID транслироваться.

Режим рандомизации MAC: аппаратный или автоматический (Android 13+).

20.1. Безопасность

Параметры безопасности Wi-Fi:

WEP-PSK: WEP (общий ключ).

WPA-PSK: WPA/WPA2/WPA3-Personal (общий ключ).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (расширяемый протокол аутентификации).

Режим WPA3 192-бит: сеть WPA-EAP, разрешающая только режим WPA3 192-бит.

20.2. Парольная фраза (общий ключ)

Отображается, если для безопасности выбран **WEP-PSK** или **WPA-PSK**. Парольная фраза обязательна.

20.3. Метод EAP (Enterprise)

Отображается, если для безопасности выбран **WPA-EAP** или **Режим WPA3 192-бит**. Выберите один внешний метод EAP:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Аутентификация на этапе 2

Отображается для туннелирующих внешних методов (**EAP-TTLS** и **PEAP**).

MSCHAPv2

PAP

20.5. Учётные данные EAP от пользователей

Если включено, система автоматически применяет учётные данные EAP на устройствах для каждого пользователя. Учётные данные пользователей можно настроить в разделе **Пользователи**.

20.6. Клиентский сертификат

Для **EAP-TLS** можно назначить клиентский сертификат, используемый для аутентификации Wi-Fi. Дополнительные сведения см. на странице **Управление сертификатами**.

Если сертификат уже назначен, используйте **Открыть сертификат**, чтобы просмотреть его, или **Изменить сертификат**, чтобы выбрать другой.

Кроме того, можно указать **Псевдоним пары ключей клиентского сертификата**, который ссылается на клиентский сертификат, хранящийся в хранилище ключей Android и разрешённый для аутентификации Wi-Fi.

> Если заданы и **Клиентский сертификат**, и **Псевдоним пары ключей клиентского сертификата**, псевдоним пары ключей игнорируется.

20.7. Идентификатор

Идентификатор пользователя. Для туннелирующих внешних протоколов (PEAP, EAP-TTLS) он используется для аутентификации внутри туннеля, а **Анонимный идентификатор** используется как идентификатор EAP вне туннеля. Для нетуннелирующих внешних протоколов он используется как идентификатор EAP.

20.8. Анонимный идентификатор

Только для туннелирующих протоколов: указывает идентификатор пользователя, предъявляемый внешнему протоколу.

20.9. Пароль

Пароль пользователя. Если не указан, по умолчанию запрашивается у пользователя.

20.10. Сертификаты CA сервера

Список сертификатов CA, используемых для проверки цепочки сертификатов хоста. Должен совпадать хотя бы один сертификат CA. Дополнительные сведения см. на странице **Управление сертификатами**.

Используйте **Добавить сертификат CA сервера**, чтобы добавить записи, и удаляйте их действием удаления.

20.11. Совпадения суффиксов домена

Список ограничений для доменного имени сервера. Записи используются как требования совпадения суффикса с DNS-именем (именами) альтернативного имени субъекта сертификата сервера аутентификации.

Revision #6
Created 2026-11-10 15:18:11 UTC by Admin
Updated 2026-11-12 09:57:53 UTC by Admin