

# Сети

В этом разделе вы можете настроить политики, связанные с сетевыми подключениями.

Конфигурации Wi-Fi могут быть предоставлены и управляемы системой через **Конфигурации Wi-Fi**. В зависимости от значения, установленного в поле **Настройка Wi-Fi**, пользователи могут иметь ограниченный контроль над добавлением/изменением сетей или не иметь его вовсе.

## Состояние радиомодуля устройства

### 1. Состояние Wi-Fi

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

**Выбор пользователя (по умолчанию):** Пользователю разрешено включать/отключать Wi-Fi.

**Включено:** Wi-Fi включен, и пользователю запрещено его отключать (Android 13+).

**Отключено:** Wi-Fi выключен, и пользователю запрещено его включать (Android 13+).

### 2. Минимальный уровень безопасности Wi-Fi

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

**Открытая сеть (по умолчанию):** Устройство может подключаться к любым типам сетей Wi-Fi.

**Персональная сеть:** Запрещает открытые сети Wi-Fi; требует как минимум уровень безопасности персональной сети (например, WPA2-PSK).

**Корпоративная сеть:** Требует сети с корпоративной защитой EAP; запрещает использование сетей Wi-Fi с уровнем безопасности ниже этого уровня.

**Корпоративная сеть 192 бит:** Требует сети с корпоративной защитой 192 бит; самый строгий вариант.

### 3. Состояние сверхширокополосной связи (UWB)

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

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

**Отключено:** UWB отключен, и пользователю запрещено переключать его через настройки (Android 14+).

## Управление подключением устройства

### 4. Обмен данными через Bluetooth

Управляет тем, разрешен ли обмен данными через Bluetooth.

**Разрешено:** Обмен данными через Bluetooth разрешен (по умолчанию на полностью управляемых устройствах, Android 8+).

**Запрещено:** Обмен данными через Bluetooth запрещен (по умолчанию в рабочих профилях, Android 8+).

### 5. Настройка Wi-Fi

Управляет правами на настройку Wi-Fi. В зависимости от выбранного варианта, пользователь может иметь полный контроль над настройкой сетей Wi-Fi, ограниченный или не иметь его вовсе.

**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 корпоративных устройствах).

**Запретить настройку Wi-Fi:** Запрещает настройку сетей Wi-Fi. Для полностью управляемых устройств это удаляет сети, настроенные пользователем, и оставляет только те, что были настроены через **Конфигурации Wi-Fi**. Для рабочих профилей на корпоративных устройствах существующие сети не затронуты, но пользователи не могут добавлять, удалять или изменять Wi-Fi сети.

Если настройка Wi-Fi отключена и устройство не может подключиться при загрузке, система может показать **аварийный выход в сеть**, чтобы пользователь мог временно подключиться и обновить политику.

## 6. Настройки Wi-Fi Direct

Управляет настройкой и использованием параметров Wi-Fi Direct. Поддерживается на устройствах, принадлежащих компании, с Android 13 и выше.

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

**Запретить:** Пользователю запрещено использовать Wi-Fi Direct.

## 7. Настройки режима модема

Управляет настройками режима модема. В зависимости от установленного значения, пользователю может быть частично или полностью запрещено использование различных форм раздачи интернета.

**Разрешить все виды раздачи (по умолчанию):** Разрешает настройку и использование всех видов раздачи интернета.

**Запретить раздачу через Wi-Fi:** Запрещает пользователю использовать раздачу интернета через Wi-Fi (на корпоративных устройствах с Android 13+).

**Запретить все виды раздачи:** Запрещает все формы раздачи интернета (на полностью управляемых устройствах и в рабочих профилях на корпоративных устройствах).

## 8. Политика Wi-Fi SSID

Ограничения на то, к каким SSID Wi-Fi может подключаться устройство (это не влияет на то, какие сети могут быть настроены на устройстве). Поддерживается на устройствах, принадлежащих компании, с Android 13 и выше.

**Черный список SSID (по умолчанию):** Устройство не может подключаться к сетям Wi-Fi, чьи SSID указаны в списке, но может подключаться к другим сетям.

**Белый список 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 будет интерпретироваться как разрешенные или запрещенные SSID.

В интерфейсе редактора политик список SSID обозначается как **Разрешенные Wi-Fi SSID** для белых списков и **Запрещенные Wi-Fi SSID** для черных списков.

## 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 в себя:

**SSID:** SSID, к которому применяется настройка роуминга (обязательное поле).

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

# Сетевые ограничения

## 10. Отключение Bluetooth

Отключен ли Bluetooth. Рекомендуется использовать эту настройку вместо «Bluetooth config disabled», так как параметр «Bluetooth config disabled» может быть обойден пользователем.

## 11. Отключение передачи контактов через Bluetooth

Отключена ли передача контактов через Bluetooth.

## 12. Отключение настройки Bluetooth

Отключена ли возможность настройки Bluetooth.

## 13. Отключение сброса настроек сети

Отключена ли возможность сброса настроек сети.

## 14. Отключение исходящего режима Beam

Отключена ли возможность передачи данных через NFC (Android Beam).

# VPN

## 15. Приложение Always On VPN

Укажите имя пакета Always On VPN, чтобы гарантировать, что данные из указанных управляемых приложений всегда будут проходить через настроенный VPN.

Примечание: Для работы этой функции требуется развертывание VPN-клиента, поддерживающего функции Always On и VPN для отдельных приложений.

## 16. Блокировка сети при отключении VPN

Запрещает использование сети, если VPN не подключен.

## 17. Отключение настройки VPN

Отключена ли возможность настройки VPN.

# Прокси-сервер и сетевые службы

## 18. Приоритетная сетевая служба

Управляет тем, включена ли приоритетная сетевая служба в рабочем профиле. Например, организация может иметь соглашение с оператором о том, что рабочие данные передаются через выделенную для корпоративного использования сетевую службу (например, через сегмент сети 5G для предприятий). 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 сегментацию сети (network slicing) для предприятий, также настройте **Конфигурацию сегментации сети 5G** в панели политик **Сотовая связь** и назначьте приложения к сегменту, используя настройку **Приоритетная сеть**.

## 19. Рекомендуемый глобальный прокси-сервер

Глобальный HTTP-прокси, не зависящий от сети. Как правило, прокси-серверы следует настраивать для каждой отдельной сети в конфигурациях Wi-Fi. Глобальный прокси может быть полезен для нестандартных сценариев, таких как общая внутренняя фильтрация. Глобальный прокси является лишь рекомендацией, и некоторые приложения могут его игнорировать.

**Отключено**

## Прямой прокси

### Автоматическая настройка прокси (PAC)

#### 19.1. Хост

Хост прямого прокси-сервера.

#### 19.2. Порт

Порт прямого прокси-сервера.

#### 19.3. PAC URI

URI-адрес PAC-скрипта, используемого для настройки прокси-сервера.

#### 19.4. Исключенные хосты

Для прямого прокси-сервера — хосты, для которых прокси-сервер будет обходить. Имена хостов могут содержать подстановочные знаки, такие как **\*.example.com**.

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

## Конфигурации Wi-Fi

Определите конфигурации сетей Wi-Fi, которые система будет применять на устройствах. Используйте **Добавить конфигурацию Wi-Fi** для создания записи, а для её удаления используйте действие «Удалить».

## 20. Поля конфигурации Wi-Fi

Каждая конфигурация включает в себя:

**Имя конфигурации:** Обязательно.

**SSID:** Обязательно.

**Автоподключение:** Должно ли устройство подключаться к сети автоматически при нахождении в зоне действия.

**Fast Transition:** Должен ли клиент пытаться использовать функцию Fast Transition (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 (с общим ключом).

**WPA-PSK:** WPA/WPA2/WPA3-Personal (с общим ключом).

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

**Режим WPA3 192-bit:** Сеть WPA-EAP, допускающая только режим WPA3 192-bit.

## 20.2. Пароль (общий ключ)

Отображается, когда в поле «Безопасность» выбрано **WEP-PSK** или **WPA-PSK**. Ввод пароля обязателен.

## 20.3. Метод EAP (Enterprise)

Отображается, когда в поле «Безопасность» выбрано **WPA-EAP** или **Режим WPA3 192-bit**. Выберите один внешний метод EAP:

**EAP-TLS**

**EAP-TTLS**

**PEAP**

**EAP-SIM**

**EAP-AKA**

## 20.4. Аутентификация второй фазы

Отображается для методов с туннелированием (**EAP-TTLS** и **PEAP**).

**MSCHAPv2**

**PAP**

## 20.5. Учетные данные EAP от пользователей

При включении этой функции система автоматически применяет учетные данные EAP на устройствах для каждого отдельного пользователя. Вы можете настроить учетные данные пользователей в разделе **Пользователи**.

## 20.6. Клиентский сертификат

Для **EAP-TLS** вы можете назначить клиентский сертификат, используемый для аутентификации Wi-Fi. Для получения дополнительной информации ознакомьтесь со страницей [Управление сертификатами](#).

Если сертификат уже назначен, вы можете использовать **Открыть сертификат** для его просмотра или **Изменить сертификат**, чтобы выбрать другой.

В качестве альтернативы вы можете указать **Псевдоним пары ключей клиентского сертификата**, который ссылается на клиентский сертификат, хранящийся в связке ключей Android и разрешенный для аутентификации Wi-Fi.

Если установлены и **Клиентский сертификат**, и **Псевдоним пары ключей клиентского сертификата**, то псевдоним пары ключей игнорируется.

## 20.7. Идентификатор (Identity)

Идентификатор пользователя. Для туннелируемых внешних протоколов (PEAP, EAP-TTLS) это используется для аутентификации внутри туннеля, а **Анонимный идентификатор** используется в качестве идентификатора EAP вне туннеля. Для непрозрачных (non-tunneling) внешних протоколов это используется в качестве идентификатора EAP.

## 20.8. Анонимный идентификатор

Только для туннелируемых протоколов: указывает на идентификатор пользователя, передаваемый внешнему протоколу.

## 20.9. Пароль

Пароль пользователя. Если не указан, по умолчанию будет выводиться запрос пароля пользователю.

## 20.10. Сертификаты CA сервера

Список сертификатов CA, которые будут использоваться для проверки цепочки сертификатов хоста. Должен совпасть как минимум один сертификат CA. Для получения дополнительной информации ознакомьтесь со страницей [Управление сертификатами](#).

Используйте **Добавить сертификат CA сервера**, чтобы добавить записи, а для их удаления используйте действие «Удалить».

## 20.11. Совпадение суффикса домена

Список ограничений для доменного имени сервера. Записи используются в качестве требований к совпадению суффикса с DNS-именем (именами) альтернативного имени субъекта (SAN) сертификата сервера аутентификации.

---

Revision #10

Created 2026-06-24 08:10:45 UTC by Admin

Updated 2026-07-07 10:57:43 UTC by Admin