Сеть

Раздел **Сеть** редактора политик Apple настраивает сети Wi-Fi и VPN на устройствах, устанавливает сертификаты и ограничивает функции подключения, такие как AirDrop и Bluetooth. Каждая сеть Wi-Fi, VPN и сертификат устанавливаются как отдельный профиль конфигурации, который можно увидеть на устройстве в разделе **Настройки > Основные > VPN и управление устройством** (Mac: **Системные настройки > Основные > Управление устройством**, или **Конфиденциальность и безопасность > Профили** в macOS 13 и 14) и на панели **Профили, сертификаты и безопасность** страницы устройства.

> Сертификаты берутся со страницы **Сертификаты**: сначала импортируйте их там. Политика только ссылается на них, поэтому сертификат никогда не копируется в политику.

Ограничения

- **Разрешить AirDrop**
- **Разрешить входящие запросы AirPlay**
- **Разрешить изменение Bluetooth**
- **Разрешить изменение общего доступа по Bluetooth**
- **Разрешить доступ приложения «Файлы» к сетевым дискам**
- **Разрешить изменение общего доступа к интернету**
- **Разрешить кэширование содержимого**
- **Разрешить общий доступ к файлам iTunes**

Сети Wi-Fi

Нажмите **Добавить сеть Wi-Fi** и заполните:

- **Имя сети (SSID)**: имя сети, до 32 символов.
- **Безопасность**: нет (открытая сеть), WEP, WPA или WPA2, WPA2 или WPA3, только WPA3 или любая.
- **Пароль**: пароль личной сети.
- **Подключаться автоматически** и **Скрытая сеть** (для сетей, которые не транслируют своё имя).

- **Прокси**: нет, вручную (сервер и порт) или автоматически (URL файла PAC; пусто — чтобы найти настройки в сети с помощью WPAD).
- **Имя профиля** (необязательно) и **Применяется к**, чтобы ограничить сеть определёнными типами устройств.

Корпоративные сети (802.1X)

Включите **Корпоративная сеть (802.1X)**, когда пользователи аутентифицируются по своим учётным данным или сертификату вместо общего пароля.

- **Аутентификация**: PEAP, TTLS (с внутренней аутентификацией, например MSCHAPv2) или TLS (только сертификат).
- **Учётные данные пользователя устройства**: каждое устройство использует EAP-идентификатор, анонимный идентификатор и пароль своего пользователя, заданные на странице «Пользователи». Устройства без пользователя не получают сеть.
- **Идентификатор**, **Анонимный идентификатор** и **Пароль**: одинаковые для каждого устройства. Идентификатор может содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$. Оставьте пароль пустым, чтобы пользователь ввёл его на устройстве.
- **Сертификат идентификации**: клиентский сертификат, который представляет устройство (обязателен для TLS). См. параметры сертификатов ниже.
- **Доверенные сертификаты**: сертификаты CA, которые выпустили сертификат вашего сервера RADIUS. Они устанавливаются вместе с сетью.
- **Доверенные имена серверов**: имена сертификатов сервера RADIUS, которые принимают устройства, например radius.example.com или *.example.com.

VPN

Нажмите **Добавить VPN**, чтобы настроить VPN IKEv2 или Cisco IPSec, встроенный в iOS, iPadOS и macOS (приложение VPN не требуется).

- **Тип** и **Сервер**. Для IKEv2 также **Удалённый идентификатор** (идентификатор сервера; пусто означает адрес сервера) и **Локальный идентификатор**, который может содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$.
- **Аутентификация** устройства: сертификат (со страницы «Сертификаты», сертификат пользователя устройства или запрошенный у сервера SCEP), общий секрет (с необязательным именем группы для IPSec) или ничего для серверов IKEv2, которые проверяют только имя пользователя и пароль.
- **Доверенные сертификаты**: сертификаты CA вашего VPN-сервера, устанавливаемые вместе с VPN. Для IKEv2 вы также можете задать ожидаемые

издателя и имя сертификата сервера.
- **Имя пользователя и пароль**: пользователь также аутентифицируется по имени пользователя (переменные разрешены) и паролю (EAP для IKEv2, XAuth для IPSec). Оставьте пароль пустым, чтобы пользователь ввёл его на устройстве.
- **Имя VPN** (отображается в «Настройках») и **Применяется к**.

Подключение

- **Пользователь подключается в «Настройках»**: VPN установлен, и пользователь включает его при необходимости.
- **По требованию**: устройство подключает VPN автоматически. С параметром **кроме доверенных сетей Wi-Fi** VPN не используется в перечисленных вами сетях Wi-Fi, например в офисной сети.
- **Всегда включён** (IKEv2, только iPhone и iPad под надзором): весь трафик проходит через VPN в сотовой сети и Wi-Fi, и пользователь не может выключить его. Другие устройства не получают этот VPN. Если в VPN используется имя пользователя, пароль должен быть задан в политике.
- **VPN для отдельных приложений**: только некоторые приложения используют VPN. Выберите VPN для каждого приложения в разделе **Управление приложениями** (поле **VPN** приложения, недоступно на Mac) и при необходимости перечислите домены Safari, которые его используют.

> Сначала протестируйте VPN «Всегда включён» или «По требованию» на тестовом устройстве: если сервер недоступен, у устройства может не быть подключения.

Глобальный прокси, шифрованный DNS и фильтр веб-содержимого

Эти параметры применяются ко всему трафику устройства. Включайте их соответствующим переключателем.

- **Глобальный HTTP-прокси** (iPhone и iPad под надзором, Mac): весь HTTP-трафик проходит через прокси в любой сети. Задайте сервер и порт (с необязательными именем пользователя и паролем) или автоматическую конфигурацию (URL файла PAC; пусто — чтобы найти её в сети). **Разрешить страницы входа Wi-Fi** позволяет пользователю входить в общедоступные сети Wi-Fi без прокси.

- **Шифрованный DNS**: устройство разрешает имена с помощью вашего DNS-сервера через DNS over HTTPS (URL сервера) или DNS over TLS (имя сервера), при необходимости только для некоторых доменов. На устройствах под надзором вы можете запретить пользователю выключать его.
- **Фильтр веб-содержимого** (iPhone и iPad под надзором): встроенный в iOS фильтр ограничивает сайты для взрослых, используя списки всегда разрешённых или всегда заблокированных веб-сайтов, либо разрешает только список веб-сайтов, отображаемых как закладки в Safari.

> Неверный прокси или DNS-сервер может оставить устройства без подключения: сначала опробуйте настройки на тестовом устройстве.

Сертификаты

Нажмите **Добавить сертификат**, чтобы установить сертификат отдельно: центр сертификации, которому должны доверять Safari и приложения, или идентификатор, используемый приложениями. Сертификаты сети Wi-Fi или VPN не нужно добавлять здесь.

Параметры сертификатов

- **Сертификат со страницы «Сертификаты»**: один и тот же сертификат на каждом устройстве. Нажмите **Выбрать сертификат**, чтобы выбрать его.
- **Сертификат пользователя устройства**: каждое устройство получает клиентский сертификат, привязанный к его пользователю. Устройства, пользователь которых не имеет сертификата, его не получают. Когда вы привязываете к пользователю другой сертификат, устройства обновляются.
- **Запрошен у сервера SCEP**: каждое устройство запрашивает собственный сертификат у вашего сервера SCEP (например, Microsoft NDES), поэтому закрытый ключ никогда не покидает устройство. Задайте URL сервера, запрос, если сервер его требует, субъект (например, CN=$EMAIL$), альтернативные имена, размер ключа и назначение ключа.

> Клиентские сертификаты (.p12), защищённые старым шифрованием RC2, нельзя установить на устройства Apple. Перед импортом экспортируйте их снова с шифрованием 3DES или AES.

Безопасность

Профили, содержащие пароли или закрытые ключи, отправляются только на устройство, для которого они созданы: устройство должно подписать свой запрос сертификатом управления. Пароли и сертификаты не записываются в журналы.

Revision #6
Created 2026-11-10 15:18:03 UTC by Admin
Updated 2026-11-12 09:57:43 UTC by Admin