

Настройка доступа к корпоративным точкам доступа WiFi с помощью профилей «Точка доступа WiFi iOS» и «Точка доступа WiFi Android»

Для настройки доступа к корпоративным точкам доступа WiFi следует настроить профиль «Точка доступа WiFi iOS» или «Точка доступа WiFi Android», соответственно устройству. Создание и настройка политики профилей описаны в документе «Руководство администратора — Профили (п.2.6.9)»

Доступ можно настроить одним из следующих способов:

Использовать общий пароль

Создать или настроить существующий профиль «Точка доступа WiFi iOS» или «Точка доступа WiFi Android». В политиках профиля указать:

1. «Тип безопасности» = Personal;
2. «Пароль» — ввести общий пароль для подключения.

Политики | Условия (не заданы) | Назначения | Владелец | Делегирование | Сохранить

* Порт прокси-сервера: Не задано

* Тип безопасности: Personal

* Список хостов, для которых нужно исключить использование прокси-сервера при подключении. Можно использовать подстановочные знаки: * и ?. Введите значение и нажмите добавить

Пароль: [masked]

* Обязательно при использовании Android 13 и выше. Список доменов для проверки сертификата AAA-сервера (обычно RADIUS). Можно перечислить несколько доменов через ";". Если домен, указанный в

не ниже 8.0

привилегии Knox или привилегия DO и версия Android не ниже 8.0 или привилегия PO и версия Android не ниже 8.0

Рисунок 1 — Политики для использования общего пароля

Использовать доменные логин и пароль

Создать или настроить существующий профиль «Точка доступа WiFi iOS» или «Точка доступа WiFi Android». В политиках профиля указать:

1. «Тип безопасности» = Enterprise,
2. «Тип EAP» = PEAP,
3. В политиках «Имя пользователя» и «Пароль пользователя» ввести доменные учетные данные пользователя.

В политике «Имя пользователя» допускается использование подстановок (см. «Руководство администратора — Настройка параметров профиля 2.6.9.2»).

Пример:

- `{{employee.exchange.emp_email}}`
- `{{userPrincipalName}}`
- `{{employee.exchange.emp_email_login}}`

The screenshot shows a configuration window for a network profile. Several fields are highlighted with red rectangles:

- Security Type:** A dropdown menu set to "Enterprise".
- EAP Type:** A dropdown menu set to "PEAP".
- User Name:** A text field containing the placeholder "Доменное имя пользователя или подстановка".
- User Password:** A text field containing the value "12345".

Other visible elements include a "List of hosts" section with a "Добавить" (Add) button, a "Password" field set to "Не задано" (Not set), and a "Second authentication phase" dropdown set to "MSCHAPV2".

Рисунок 2 — Политики для доступа по доменным реквизитам пользователя

Использовать сертификат пользователя (группы)

Вариант 1: Применить сертификат, полученный из УЦ (с приватным ключом).

1. Настроить подключение «SCEServer» в разделе «Подключения к серверам» (см. «Руководство администратора — Подключение к серверам 2.8.13»).
2. Заполнить раздел «Настройки SCEP» (см. «Руководство администратора — Настройки SCEP 2.8.14»).
3. Создать или настроить существующий профиль «Точка доступа WiFi iOS» или «Точка доступа WiFi Android». В политиках профиля указать:
 1. «Тип безопасности» = Enterprise;
 2. «Тип EAP» = TLS.

Скриншот экрана настроек «Wi-Fi» в Android. В разделе «Политики» видны следующие настройки:

- Тип безопасности: Enterprise (выбрано)
- Тип EAP: TLS (выбрано)

Другие видимые поля: Пароль (Не задано), * Обязательно при использовании Android 13 и выше. Список доменов для проверки сертификата AAA-сервера (обычно RADIUS). Можно перечислить несколько доменов через ";". Если домен, указанный в сертификате сервера, не будет найден в этом списке то подключение к точке доступа будет заблокировано. * Учётные данные (клиентский сертификат или настройки SCEP) (Не задано), Сертификат удостоверяющего центра WiFi сети (Не задано).

Рисунок 3 — Политики «Тип безопасности» «Тип EAP»

3. В политике «Учётные данные (клиентский сертификат или настройки SCEP)» необходимо указать сертификат формата PKCS12 из раздела «Клиентские сертификаты».

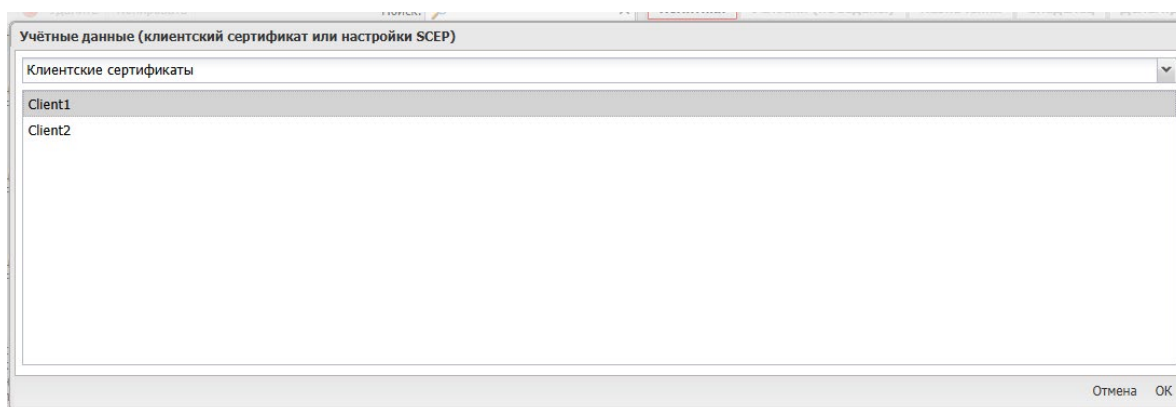


Рисунок 4 — Выбор клиентских сертификатов

Вариант 2: Получить сертификат по протоколу SCEP

1. Настроить подключение «SCEPServer» в разделе «Подключения к серверам» (см. «Руководство администратора — Подключение к серверам 2.8.13»).
2. Заполнить раздел «Настройки SCEP» (см. «Руководство администратора — Настройки SCEP 2.8.14»).
3. Создать или настроить существующий профиль «Точка доступа WiFi iOS» или «Точка доступа WiFi Android». В политиках профиля указать:
 1. «Тип безопасности» = Enterprise;
 2. «Тип EAP» = TLS.
 3. В политике «Учётные данные (клиентский сертификат или настройки SCEP)» выбрать «Настройки SCEP».

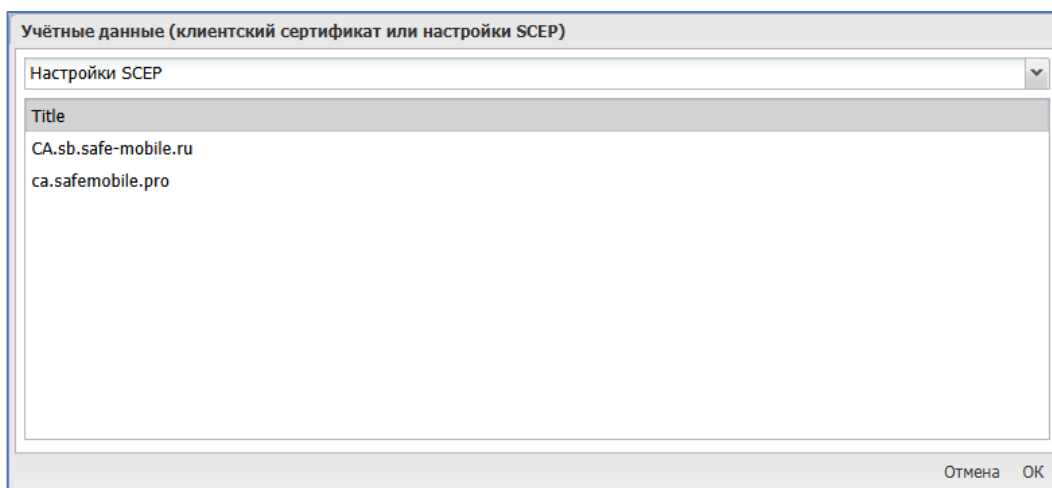


Рисунок 5 — Выбор настроек SCEP

Примечание

- Сертификаты, полученные по SCEP (формат PEM, без приватных ключей), отображаются в разделе «Клиентские сертификаты» наряду с устройствами.
- Необходимо убедиться в доступности серверов (SCEP, УЦ) для успешного развертывания сертификатов.

Настройка прокси

Возможна опциональная настройка использования прокси-сервера. За их настройку отвечают следующие политики профилей «Точка доступа WiFi iOS» или «Точка доступа WiFi Android»:

Для Android:

- «Прокси» — включение/отключение настроек прокси (Manual/не задано).
- «Использовать PAC(ProxyAutoConfig)» — использование PAC файла конфигурации прокси (Нет/Да).
- «URL прокси-сервера»:
 - указать URL прокси-сервера, если «Использовать PAC» = Нет,
 - указать URL файла PAC, если «Использовать PAC» = Да,
- «Порт прокси-сервера»:
 - указать порт прокси-сервера, если «Использовать PAC» = Нет,
 - указать порт файла PAC, если «Использовать PAC» = Да.
- «Список хостов, для которых нужно исключить использование прокси-сервера при подключении. Можно использовать подстановочные символы, например: *.example.com» — исключения для использования прокси (список URL).

The image shows a screenshot of the 'Proxy' settings dialog box on an Android device. The dialog has a title bar and several sections with labels and input fields. The 'Proxy' section is set to 'Manual'. The 'Use PAC (Proxy Auto Config)' section is set to 'No'. The 'Proxy URL' section is empty. The 'Proxy port' section is empty. The 'Security type' section is set to 'Enterprise'. The 'List of hosts for which proxy use should be excluded' section is empty, with a green plus icon to the right of the input field. The text in the dialog is in Russian.

Прокси	Manual
* Использовать PAC (Proxy Auto Config)	Нет
* URL прокси-сервера	Не задано
* Порт прокси-сервера	Не задано
* Тип безопасности	Enterprise
* Список хостов, для которых нужно исключить использование прокси-сервера при подключении. Можно использовать подстановочные символы, например: *.example.com	Введите значение и нажмите добавить

Рисунок 6 — Политики использования прокси для Android

Пример настройки

Прокси: Manual

* Использовать PAC (Proxy Auto Config): Да

* URL прокси-сервера: http://10.15.15.15/pac.conf

* Порт прокси-сервера: 80

* Тип безопасности: Enterprise

* Список хостов, для которых нужно исключить использование прокси-сервера при подключении. Можно использовать подстановочные символы, например: *.example.com

Введите значение и нажмите добавить

*.google.com

Пароль: Не задано

Рисунок 7 — Пример настроек для Android

Для IOS:

- «Прокси» — включение/отключение настроек прокси/автонастройку прокси, используя WPAD (Manual/не задано/auto).
- «URL прокси-сервера» — URL прокси-сервера.
- «Порт прокси-сервера» — порт прокси-сервера.
- «Логин прокси-сервера» — логин прокси-сервера. Политика доступна для изменения если политика «Прокси» = Manual.
- «Пароль прокси-сервера» — пароль прокси. Политика доступна для изменения если политика «Прокси» = Manual.
- «URL файла конфигурации PAC прокси-сервера» — URL файла конфигурации PAC (если используется).
- «Подключаться напрямую, если файл конфигурации (PAC) прокси-сервера недоступен» — политика определяет будет ли устройство подключать к интернету

если прокси недоступно (Да/нет/не задано). Не доступно для изменения, если не задан PAC.

* Прокси	Manual	
* URL прокси-сервера	Не задано	
* Порт прокси-сервера	Не задано	
Логин прокси-сервера	Не задано	
Пароль прокси-сервера	Не задано	
URL файла конфигурации (PAC) прокси-сервера	Не задано	
Подключаться напрямую если файл конфигурации (PAC) прокси-сервера недоступен	Нет	версия iOS не ниже 7.0

Рисунок 8 — Политики использования прокси для iOS

Пример настройки

* Прокси	Manual	
* URL прокси-сервера	http://10.15.15.15	
* Порт прокси-сервера	8080	
Логин прокси-сервера	user_name	
Пароль прокси-сервера	user_pass	
URL файла конфигурации (PAC) прокси-сервера	http://10.15.15.15/conf.pac	
Подключаться напрямую если файл конфигурации (PAC) прокси-сервера недоступен	Да	версия iOS не ниже 7.0

Рисунок 9 — Пример настроек для iOS