

Table of Contents

Table of Contents	1
UserGate Client для Linux	2
UserGate Client для Linux 7.4.1	3
Общие сведения	4
Установка UserGate Client	5
Работа UserGate Client в связке с UserGate NGFW	9
Настройка VPN-соединения на устройстве пользователя	11
Ошибки VPN-подключений	15
UserGate Client для Linux 7.5.0	17
Общие сведения	18
Установка UserGate Client	19
Настройка VPN-подключений с помощью UserGate Client	21
Ошибки VPN-подключений	23

Общие сведения

Product: UserGate Client

Version: 7.4.1

Technology: VPN

Приложение UserGate Client для Linux является компонентом экосистемы UserGate SUMMA. Приложение устанавливается на компьютеры пользователей и обеспечивает безопасный доступ в корпоративную сеть, защищенную системами безопасности UserGate.

UserGate Client поддерживает следующие функции:

- Установление защищенного соединения с VPN-сервером UserGate NGFW.
- Аутентификация пользователей посредством сертификата или логина с паролем.
- Поддержка функции раздельного туннелирования (split tunneling). Функция позволяет модифицировать таблицу маршрутизации компьютера пользователя при установлении VPN-соединения в соответствии с параметрами, заданными администратором на VPN-сервере.

Основными компонентами UserGate Client являются:

- `usergate-client-agent` — системная служба приложения. Обеспечивает:
 - поддержку VPN-протоколов;
 - реализацию методов аутентификации;
 - управление VPN-соединениями;
 - настройку виртуальных сетевых интерфейсов, маршрутизации, раздельного туннелирования, DNS.
- `usergate-client-gui` — модуль, отвечающий за взаимодействие с пользователем через графический интерфейс. Выполняет:
 - отображение состояния VPN-соединения;
 - управление профилями;
 - взаимодействие с системным хранилищем секретов;
 - управление журналированием;
 - отображение событий, связанных с подключением.

Установка UserGate Client

Product: UserGate Client

Version: 7.4.1

Technology: VPN

UserGate Client для Linux поставляется в виде DEB- или RPM-пакета. Скачать последнюю версию приложения можно [с официального сайта UserGate](#).

Минимальные системные требования

Минимальные системные требования для установки приложения:

- Операционная система:
 - Astra Linux версий 1.7 или 1.8;
 - Ubuntu версий 22.04 или 24.04;
 - РЕД ОС версий 7.3 или 8.0.
- Оперативная память (RAM): не менее 4 ГБ.
- Свободное дисковое пространство: минимум 500 МБ.

Порядок установки приложения

Для установки клиента с помощью DEB-пакета в операционных системах Astra Linux или Ubuntu:

1. Скачайте пакет `usergate-client-*.deb` из личного кабинета.
2. Выполните команду `sudo dpkg -i usergate-client-*.deb`.

Если появится сообщение об отсутствии в системе необходимых для работы приложения программных пакетов, выполните команду: `sudo apt install -f`.

Пакетный менеджер загрузит необходимые пакеты и установит клиент.

Компоненты UserGate Client устанавливаются в каталог `/opt/usergate-client/bin`.

Для проверки статуса установленного клиента используйте команду `sudo service usergate-client-agent status`.

Все данные между компонентами клиента шифруются с применением протокола TLS, что исключает возможность перехвата и модификации трафика. Ключи генерируются при старте сервиса.

Чувствительные данные пользователя хранятся в системном хранилище секретов. Каждому пользователю доступны только свои профили подключений.

Журналы приложения создаются для каждого пользователя отдельно в домашнем каталоге `/home/<username>/.usergate-client`.

Для удаления клиента используйте команду `sudo dpkg -r usergate-client`.

Для удаления клиента вместе с журналами используйте команду `sudo dpkg --purge usergate-client`.

Примечание Для обновления приложения с версии 1.0 до версии 7.x необходимо удалить старую версию приложения и затем установить новую.

Для установки клиента с помощью RPM-пакета в операционной системе РЕД ОС:

1. Скачайте пакет `usergate-client-*.rpm` из личного кабинета.
2. Выполните команду `dnf install <имя_пакета>`.

Для удаления клиента используйте команду `dnf remove <имя_пакета>`.

Загрузка корневого сертификата удостоверяющего центра

Для того чтобы UserGate Client при подключении мог проверять сертификат VPN-сервера, необходимо загрузить в систему корневой сертификат удостоверяющего центра.

Для загрузки корневого сертификата в систему на Ubuntu или Astra Linux:

1. Сохраните файл сертификата `*.crt` в директории `/usr/local/share/ca-certificates/`.
2. Выполните команду: `sudo update-ca-certificates`.

Для загрузки корневого сертификата в систему на РЕД ОС:

1. Сохраните файл сертификата `*.crt` в директории `/etc/pki/ca-trust/source/anchors/`.

2. Выполните команду: `sudo update-ca-trust`.

Интерфейс приложения

После установки клиента в списке приложений пользователя появится приложение UserGate Client.

На вкладке **VPN-соединения** вы можете:

- создавать профили VPN-соединений;
- управлять VPN-соединением;
- просматривать в онлайн-режиме информацию о параметрах текущего соединения и его статусе.

На вкладке **Журналы** вы можете управлять журналированием работы приложения:

- устанавливать уровень детализации событий в журналах;
- экспортировать журналы в формате ZIP-архива;
- очищать журналы приложения;
- открывать папку с журналами приложения.

На вкладке **Статус соединения** вы можете просматривать и копировать в буфер обмена историю последнего VPN-соединения, инициированного этим клиентом.

Когда приложение UserGate Client запущено на компьютере пользователя, в строке состояния графического интерфейса операционной системы появляется значок приложения.

Нажав на значок приложения, вы можете:

- инициировать установку VPN-соединения, выбрав настроенный профиль;
- разорвать установленное VPN-соединение;
- перейти к настройке приложения;
- завершить работу приложения.

Подробнее о настройке VPN-соединений в приложении UserGate Client — в разделе « [Настройка VPN-соединения на устройстве пользователя](#) ».

Работа UserGate Client в связке с UserGate NGFW

Product: UserGate Client

Version: 7.4.1

Technology: VPN

Установление VPN-соединения с помощью UserGate Client возможно только с серверами, настроенными на UserGate NGFW.

Встроенный в ПО VPN-клиент использует следующие параметры для установления VPN-соединения:

- Протокол IPsec (IKEv2):
 - Аутентификация по сертификатам X.509 или логину с паролем (EAP MSCHAPv2). Поддерживается режим многофакторной аутентификации (TOTP).
 - Группы Диффи — Хеллмана: группа 2 Prime 1024, группа 14 Prime 2048, группа 16 Prime 4096.
 - Алгоритмы аутентификации и шифрования:
 - SHA1/AES128;
 - SHA256/AES128;
 - SHA384/AES128;
 - SHA1/AES256;
 - SHA256/AES256;
 - SHA384/AES256;
 - SHA1/3DES;
 - SHA256/3DES;
 - SHA384/3DES.
 - Срок действия ключей первой фазы составляет 2 часа, второй фазы — 1 час. За 30 секунд до окончания срока действия инициируется запрос на их обновление. Если ответ получен, считается, что фаза успешно обновлена. В случае отсутствия ответа повторные запросы отправляются каждые 5 секунд на протяжении 30 секунд. Если ни один из запросов не получает ответа, обновление ключей признается неуспешным, и соединение завершается с ошибкой Rekeying failed.
 - Функция DPD (Dead Peer Detection) работает в режиме On idle (при отсутствии трафика) с базовым интервалом 15 секунд и допускает до 6 неудачных попыток. Проверка доступности удаленного узла запускается, если в туннеле отсутствует трафик в течение двойного интервала — 30 секунд. При отсутствии ответа от сервера на проверочный запрос пакеты продолжают отправляться с интервалом 5 секунд до достижения максимально допустимого числа попыток. Если ответ получен, система возвращается к стандартному интервалу опроса. Если же ни на один из отправленных пакетов ответ не поступает, соединение разрывается.
- Протокол DTLS (при работе с UserGate NGFW версии 7.5.0 и выше):
 - Аутентификация по сертификатам X.509 или логину с паролем (EAP MSCHAPv2). Поддерживается режим многофакторной аутентификации (TOTP).
 - Алгоритмы аутентификации и шифрования:
 - DTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA;
 - DTLS_ECDHE_RSA_WITH_AES_256_CBC_SHA;
 - DTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256;
 - DTLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.
 - Срок действия ключа составляет 2 часа. За 30 секунд до окончания срока действия инициируется запрос на его обновление. Если ответ получен, считается, что ключ обновлен. В случае отсутствия ответа повторные запросы отправляются каждые 5 секунд на протяжении 30 секунд. Если ни один из запросов не получает ответа, обновление ключа признается неуспешным, и соединение завершается с ошибкой Rekeying failed.
 - Функция DPD работает в режиме On idle (при отсутствии трафика) с базовым интервалом 15 секунд и допускает до 5 неудачных попыток. Проверка доступности удаленного узла запускается, если в туннеле отсутствует трафик в течение двойного интервала — 30 секунд. При отсутствии ответа от сервера на проверочный запрос пакеты продолжают отправляться с интервалом 5 секунд до достижения максимально допустимого числа попыток. Если ответ получен, система возвращается к стандартному интервалу опроса. Если же ни на один из отправленных пакетов ответ не поступает, соединение разрывается.

Для организации защищенного VPN-соединения с UserGate NGFW необходимо:

1. Настроить VPN-сервер на UserGate NGFW. Подробнее о настройке VPN-сервера:

- для версий UserGate NGFW ниже 7.5.0 — в разделе « [VPN для удаленного доступа клиентов](#) »;
- для версий UserGate NGFW 7.5.0 и выше — в разделе « [Настройка VPN для удаленного доступа в сеть](#) ».

2. Установить приложение UserGate Client на компьютере пользователя. Подробнее об установке приложения UserGate Client — в разделе « [Установка UserGate Client](#) ».

3. Настроить VPN-клиент на компьютере пользователя. Подробнее о настройке VPN-клиента — в разделе « [Настройка VPN-соединения на устройстве пользователя](#) ».

Настройка VPN-соединения на устройстве пользователя

Product: UserGate Client

Version: 7.4.1

Technology: VPN

UserGate Client поддерживает установление защищенного соединения по протоколам IPsec (IKEv2) и DTLS (при работе с UserGate NGFW версии 7.5.0 и выше) с аутентификацией по сертификатам X.509 или логину с паролем с помощью метода EAP. Поддерживается режим многофакторной аутентификации с получением временных одноразовых паролей (TOTP).

Параметры подключения настраиваются в профиле VPN-соединения. В приложении можно создать несколько профилей с различными параметрами соединения для подключения к разным VPN-серверам.

Для создания профиля VPN-соединения откройте приложение UserGate Client, перейдите на вкладку **VPN-соединения** и нажмите **Добавить**.

Настройте параметры профиля соединения:

1. Укажите название соединения.
2. Укажите IP-адрес VPN-сервера или его доменное имя.

Примечание Если DNS-сервер разрешает адрес VPN-сервера в несколько IP-адресов, VPN-клиент выполнит подключение к первому доступному адресу.

3. Выберите протокол для установления VPN-соединения.

4. Выберите один из способов аутентификации:

- **Логин и пароль.** Введите логин пользователя и его пароль.
- **Сертификат.** Выберите заранее созданные файл сертификата в форматах DER, PEM или PKCS12, закрытый ключ и введите пароль закрытого ключа.

5. Сохраните параметры профиля, нажав **Сохранить**.

Примечание При использовании многофакторной аутентификации код запрашивается в отдельном окне при попытке установить соединение.

Инициировать установку VPN-соединения можно в окне приложения UserGate Client или через значок приложения в строке состояния:

- Для установления VPN-соединения в окне приложения включите соответствующий профиль приложения.

Статус соединения будет указан рядом с активным переключателем.

- Для установления VPN-соединения: в строке состояния нажмите на значок UserGate Client и в появившемся меню выберите соответствующий профиль в списке.

В случае успешного подключения на значке UserGate Client появится символ установленного соединения.

Статистику установленного соединения и параметры подключения можно посмотреть в свойствах активного профиля в окне приложения.

Маршруты, полученные от VPN-сервера, также можно посмотреть в терминале устройства пользователя с помощью команды: `ip r show table 777`.

Чтобы завершить VPN-соединение, отключите активный профиль в окне приложения или нажмите **Отключиться** в меню приложения в строке состояния.

Историю последнего подключения можно посмотреть в окне приложения на вкладке **Статус соединения**.

Если установить VPN-соединение не удалось, будет отображено окно с кратким описанием ошибки.

Нажав **Подробнее**, вы перейдете в раздел **Статус соединения**, где можно увидеть, на каком этапе установления соединения произошла ошибка.

Подробнее об ошибках соединения и возможных причинах их возникновения — в разделе « [Ошибки VPN-подключений](#) ».

Ошибки VPN-подключений

Product: UserGate Client
Version: 7.4.1
Technology: VPN

Ошибки, связанные с неудачными попытками подключения к VPN-серверу или с разрывом существующих VPN-соединений, записываются в журнал клиента и отображаются в разделе **Статус соединения** в окне приложения.

В таблице приведены варианты сообщений об ошибках и возможные причины их возникновения.

Ошибка соединения	Сообщение об ошибке в журнале	Возможная причина ошибки
Ошибка разрешения доменного имени / DNS resolution error	ErrorUnknownServer	Доменное имя VPN-сервера, указанное в параметрах подключения клиента, не определяется DNS-сервером. Вероятные причины: - Не получен ответ от DNS-сервера. - Неверно указано доменное имя VPN-сервера в параметрах подключения на клиенте. - На DNS-сервере не определено доменное имя VPN-сервера
Сервер не отвечает / No response from server	- NoResponse; - DeadPeerDetected; - IkeRekeyFailed; - EspRekeyFailed	Ошибка появляется в момент истечения таймера на клиенте при ожидании пакета от VPN-сервера. Возможные причины: - Тайм-аут ожидания IKE_INIT response. - Тайм-аут механизма DPD (не получен ответ от VPN-сервера). - Тайм-аут IKE_AUTH. - Тайм-аут в процессе пересоздания ключей IKE-туннеля. - Тайм-аут в процессе пересоздания ключей ESP-туннеля
Ошибка аутентификации / Authentication error	- AuthenticationFailed; - InvalidLoginOrPassword; - MfaTimeout	Возможные причины: - Неверный пароль, логин, сертификат клиента или временный пароль MFA. - Тайм-аут ввода временного пароля MFA
Сертификат сервера недействителен / Server certificate is invalid	- InvalidServerSignature; - ServerNameNotFound	Ошибка проверки сертификата сервера. Возможные причины: - Неуспешная проверка цифровой подписи сертификата VPN-сервера. - CN, указанный в сертификате, не соответствует адресу VPN-сервера
Ошибка конфигурации / Configuration error	ConfigurationSystemFailed	Ошибка применения конфигурации на клиенте. Возможные причины: - Ошибка применения маршрутов. - Ошибка получения и применения IP-адреса клиента

Ошибка соединения	Сообщение об ошибке в журнале	Возможная причина ошибки
Ошибка в параметрах криптографии / Error in cryptography parameters	- InvalidDhGroups; - IkeSecurityIncompatible; - EspSecurityIncompatible	Параметры криптографии, предложенные сервером, не применимы для клиента. Возможные причины: - Неподдерживаемая DH-группа. - Неподдерживаемые параметры ESP (алгоритмы шифрования и аутентификации). - Неподдерживаемые параметры IKE (алгоритмы шифрования и аутентификации). - На сервере выключен туннельный интерфейс
Сервер принудительно разорвал соединение / Server forcibly terminated the connection	TerminateFromServer	Сервер завершил сессию: От сервера получено сообщение IKE_DELETE
Обнаружен вход в систему под другой учетной записью / Login detected under a different user account.	Logout	Отслеживание входа другого пользователя в систему: - Агент обнаружил появление в операционной системе активной сессии с новой учетной записью во время установленного VPN-соединения. - При установлении VPN-соединения агент обнаружил, что в операционной системе зарегистрировано более одной учетной записи с активными сессиями

Общие сведения

Product: uClient

Version: 7.5.x

Technology: VPN

UserGate Client — компонент экосистемы UserGate SUMMA. Клиент устанавливается на устройства пользователей для обеспечения безопасного доступа к корпоративной сети, защищенной системами безопасности UserGate.

UserGate Client поддерживает следующие функции:

- Установление защищенного соединения с VPN-сервером UserGate по протоколам IPsec (IKEv2) и DTLS (при работе с UserGate NGFW версии 7.5.0 и выше).
- Аутентификация пользователей по сертификатам X.509 или логину с паролем с помощью метода EAP.
- Поддержка Рутокен ЭЦП 3.0 в качестве источника сертификатов для аутентификации.
- Поддержка режима многофакторной аутентификации с получением временных одноразовых паролей (TOTP).
- Поддержка функции раздельного туннелирования (split tunneling). Функция позволяет модифицировать таблицу маршрутизации устройства пользователя при установлении VPN-соединения в соответствии с параметрами, заданными администратором на VPN-сервере.

Основными компонентами UserGate Client являются:

- `usergate-client-agent`— системная служба приложения. Обеспечивает:
 - поддержку VPN-протоколов;
 - реализацию методов аутентификации;
 - управление VPN-соединениями;
 - настройку виртуальных сетевых интерфейсов, маршрутизации, раздельного туннелирования, DNS.
- `usergate-client-gui`— модуль, отвечающий за взаимодействие с пользователем через графический интерфейс. Выполняет:
 - отображение состояния VPN-соединения;
 - управление профилями;
 - взаимодействие с системным хранилищем секретов;
 - управление журналированием;
 - отображение событий, связанных с подключением.

Установка UserGate Client

Product: uClient
Version: 7.5.x
Technology: VPN

UserGate Client для Linux поставляется в виде DEB- и RPM-пакетов для установки в операционных системах Linux. Скачать последнюю версию приложения можно [с официального сайта UserGate](#).

Минимальные системные требования

Минимальные системные требования для установки приложения:

- Операционная система:
 - Astra Linux версий 1.7 или 1.8;
 - Ubuntu версий 22.04 или 24.04;
 - РЕД ОС версий 7.3 или 8.0.
- Оперативная память (RAM): не менее 4 ГБ.
- Свободное дисковое пространство: минимум 500 МБ.

Порядок установки приложения

Для установки клиента с помощью DEB-пакета в операционных системах Astra Linux или Ubuntu:

1. Скачайте пакет `usergate-client-*.deb` из личного кабинета.
2. Выполните команду: `sudo dpkg -i usergate-client-*.deb`.

Если появится сообщение об отсутствии в системе необходимых для работы приложения программных пакетов, выполните команду: `sudo apt install -f`.

Пакетный менеджер загрузит необходимые пакеты и установит клиент.

Компоненты UserGate Client устанавливаются в каталог `/opt/usergate-client/bin`.

Для проверки статуса установленного клиента используйте команду: `sudo service usergate-client-agent status`.

Все данные между компонентами клиента шифруются с применением протокола TLS, что исключает возможность перехвата и модификации трафика. Ключи генерируются при старте сервиса.

Чувствительные данные пользователя хранятся в системном хранилище секретов. Каждому пользователю доступны только свои профили подключений.

Журналы приложения создаются для каждого пользователя отдельно в домашнем каталоге `/home/<username>/.usergate-client`.

Для удаления клиента используйте команду: `sudo dpkg -r usergate-client`.

Для удаления клиента вместе с журналами используйте команду: `sudo dpkg --purge usergate-client`.

Примечание Для обновления приложения с версии 1.0 до версии 7.x необходимо удалить старую версию приложения и затем установить новую.

Для установки клиента с помощью RPM-пакета в операционной системе РЕД ОС:

1. Скачайте пакет `usergate-client-*.rpm` из личного кабинета.
2. Выполните команду: `dnf install <имя_пакета>`.

Для удаления клиента используйте команду: `dnf remove <имя_пакета>`.

Загрузка корневого сертификата удостоверяющего центра

Для того чтобы UserGate Client при подключении мог проверять сертификат VPN-сервера, необходимо загрузить в систему корневой сертификат удостоверяющего центра.

Для загрузки корневого сертификата в систему на Ubuntu или Astra Linux:

1. Сохраните файл сертификата `*.crt` в каталог `/usr/local/share/ca-certificates/`.
2. Выполните команду: `sudo update-ca-certificates`.

Для загрузки корневого сертификата в систему на РЕД ОС:

1. Сохраните файл сертификата `*.crt` в каталог `/etc/pki/ca-trust/source/anchors/`.

2. Выполните команду: `sudo update-ca-trust`.

Важно! Для работы с USB-токеном Рутокен ЭЦП 3.0 необходимо установить библиотеку `libtpkcs11` еср. Подробнее о работе с устройствами Рутокен ЭЦП — [на официальном портале документации Рутокен](#). Библиотеку можно скачать [в центре загрузки Рутокен](#).

Интерфейс приложения

После установки клиента в списке приложений пользователя появится приложение UserGate Client.

На вкладке **VPN-соединения** вы можете:

- создавать профили VPN-соединений;
- управлять VPN-подключениями;
- просматривать в режиме реального времени информацию о параметрах текущего соединения и его статусе.

На вкладке **Журналы** вы можете управлять журналированием работы приложения:

- устанавливать уровень детализации событий в журналах;
- экспортировать журналы в формате ZIP-архива;
- очищать журналы приложения;
- открывать папку с журналами приложения.

На вкладке **Статус соединения** вы можете просматривать и копировать в буфер обмена историю последнего VPN-соединения, инициированного этим клиентом.

Когда приложение UserGate Client запущено на компьютере пользователя, в строке состояния графического интерфейса операционной системы Linux появляется значок приложения.

Нажав на значок приложения, вы можете:

- инициировать установку VPN-соединения, выбрав настроенный профиль;
- разорвать установленное VPN-соединение;
- перейти к настройке приложения;
- завершить работу приложения.

Подробнее о настройке VPN-подключений в приложении UserGate Client — в разделе « [Настройка VPN-подключений с помощью UserGate Client](#) ».

Настройка VPN-подключений с помощью UserGate Client

Product: uClient
Version: 7.5.x
Technology: VPN

UserGate Client предназначен для подключений к VPN-серверами UserGate.

Порядок настройки VPN-подключений

Чтобы настроить подключение UserGate Client к UserGate NGFW:

1. Настройте VPN-сервер на UserGate NGFW. О настройке VPN-сервера читайте в руководстве администратора UserGate NGFW:
 - для версий UserGate NGFW 7.5.0 и выше — в разделе « [Настройка VPN для удаленного доступа в сеть](#) »;
 - для остальных версий — в разделе « [VPN для удаленного доступа клиентов](#) ».
2. Установите UserGate Client на устройство пользователя. Подробнее об установке приложения — в разделе « [Установка UserGate Client](#) ».
3. Настройте параметры VPN-подключения в приложении. Подробнее о настройке — в главе « [Настройка параметров подключения в UserGate Client](#) ».

Настройка параметров подключения в UserGate Client

UserGate Client поддерживает VPN-соединения по протоколам IPsec (IKEv2) и DTLS (при работе с UserGate NGFW версии 7.5.0 и выше) с аутентификацией по сертификатам X.509 или логину с паролем по методу EAP-MSCHAPv2

Встроенный в приложение VPN-клиент использует следующие параметры VPN-подключений:

- Протокол IPsec (IKEv2):
 - Группы Диффи — Хеллмана:
 - группа 2 Prime 1024;
 - группа 14 Prime 2048;
 - группа 16 Prime 4096.
 - Алгоритмы аутентификации и шифрования:
 - SHA1/AES128;
 - SHA256/AES128;
 - SHA384/AES128;
 - SHA1/AES256;
 - SHA256/AES256;
 - SHA384/AES256;
 - SHA1/3DES;
 - SHA256/3DES;
 - SHA384/3DES.
 - Срок действия ключей первой фазы составляет 2 часа, второй фазы — 1 час. За 30 секунд до окончания срока действия инициируется запрос на их обновление. Если ответ получен, считается, что фаза успешно обновлена. В случае отсутствия ответа повторные запросы отправляются каждые 5 секунд на протяжении 30 секунд. Если ни один из запросов не получает ответа, обновление ключей признается неуспешным, и соединение завершается с ошибкой Rekeying failed.
 - Функция DPD (Dead Peer Detection) работает в режиме On idle (при отсутствии трафика) с базовым интервалом 15 секунд и допускает до 6 неудачных попыток. При отсутствии ответа от сервера на проверочный запрос пакеты продолжают отправляться с интервалом 5 секунд до достижения максимально допустимого числа попыток. Если ответ получен, система возвращается к стандартному интервалу опроса. Если же ни на один из отправленных пакетов ответ не поступает, соединение разрывается.
- Протокол DTLS (при работе с UserGate NGFW версии 7.5.0 и выше):
 - Алгоритмы аутентификации и шифрования:
 - DTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA;
 - DTLS_ECDHE_RSA_WITH_AES_256_CBC_SHA;
 - DTLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256;
 - DTLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.

- Срок действия ключа составляет 2 часа. За 30 секунд до окончания срока действия инициируется запрос на его обновление. Если ответ получен, считается, что ключ обновлен. В случае отсутствия ответа повторные запросы отправляются каждые 5 секунд на протяжении 30 секунд. Если ни один из запросов не получает ответа, обновление ключа признается неуспешным, и соединение завершается с ошибкой Rekeying failed.
- Функция DPD работает в режиме On idle (при отсутствии трафика) с базовым интервалом 15 секунд и допускает до 5 неудачных попыток. При отсутствии ответа от сервера на проверочный запрос пакеты продолжают отправляться с интервалом 5 секунд до достижения максимально допустимого числа попыток. Если ответ получен, система возвращается к стандартному интервалу опроса. Если же ни на один из отправленных пакетов ответ не поступает, соединение разрывается.

Настраиваемые параметры подключения задаются в профиле VPN-соединения. В приложении можно создать несколько профилей с различными параметрами соединения для подключения к разным VPN-серверам.

Для создания профиля VPN-соединения в приложении UserGate Client перейдите на вкладку **VPN-соединения** и нажмите **Добавить**.

Настройте параметры профиля соединения:

1. Укажите название соединения.
2. Укажите IP-адрес VPN-сервера или его доменное имя.

Примечание Если DNS-сервер разрешает адрес VPN-сервера в несколько IP-адресов, VPN-клиент выполнит подключение к первому доступному адресу.

3. Выберите протокол для установления VPN-соединения.
4. Выберите один из способов аутентификации:

- **Логин и пароль** — аутентификация по методу EAP-MSCHAPv2. Введите логин пользователя и его пароль.
- **PKI** — аутентификация с использованием сертификата X.509. В качестве источника сертификата можно использовать:
 - **Локальное хранилище устройства**. Выберите заранее созданные файл сертификата и закрытый ключ, затем введите пароль закрытого ключа.
 - **USB-токен** (поддерживается Рутокен ЭЦП 3.0). Выберите подключенный к системе USB-токен, а затем сертификат из списка сертификатов, доступных на токене.
- **EAP-TLS** — аутентификация по методу EAP с использованием сертификата X.509. Этот способ аутентификации доступен только для протокола IKEv2. Выберите заранее созданные файл сертификата и закрытый ключ, затем введите пароль закрытого ключа.

Примечание При использовании аутентификации с помощью EAP-TLS поддерживается только протокол TLS версии 1.2.

5. Сохраните параметры профиля, нажав **Сохранить**.

Примечание При использовании многофакторной аутентификации код запрашивается в отдельном окне при попытке установить соединение.

Важно! В случае возврата UserGate Client с версии 7.5.0 на версию 7.4.1 необходимо обновить конфигурацию профилей соединений с аутентификацией по сертификату, чтобы они продолжили работать корректно.

Подключение к VPN-серверу

Инициировать подключение к VPN-серверу можно в окне приложения UserGate Client или через значок приложения в строке состояния:

- Для установления VPN-соединения в окне приложения включите выбранный профиль соединения. Статус соединения будет указан рядом с активным переключателем. Если в профиле приложения используется способ аутентификации с сертификатом, находящимся на USB-токене, при установлении соединения необходимо ввести ПИН-код для доступа к сертификату.
- Для установления VPN-соединения: в строке состояния нажмите на значок UserGate Client и в появившемся меню выберите соответствующий профиль в списке. В случае успешного подключения на значке UserGate Client появится символ установленного соединения.

Статистику установленного соединения и параметры подключения можно посмотреть в свойствах активного профиля в окне приложения.

Маршруты, полученные от VPN-сервера, также можно посмотреть в терминале устройства пользователя с помощью команды: `ip r show table 777`.

Чтобы завершить VPN-соединение, отключите активный профиль в окне приложения или нажмите **Отключиться** в меню приложения в строке состояния.

Если установить VPN-соединение не удалось, будет отображено окно с кратким описанием ошибки. Нажав **Подробнее**, вы перейдете в раздел **Статус соединения**, где можно увидеть, на каком этапе установления соединения произошла ошибка.

Подробнее об ошибках соединения и возможных причинах их возникновения — в разделе « [Ошибки VPN-подключений](#) ».

Ошибки VPN-подключений

Product: uClient
Version: 7.5.x
Technology: VPN

Ошибки, связанные с неудачными попытками подключения к VPN-серверу или с разрывом существующих VPN-соединений, записываются в журнал клиента и отображаются в разделе **Статус соединения** в окне приложения.

В таблице приведены варианты сообщений об ошибках и возможные причины их возникновения.

Ошибка соединения	Сообщение об ошибке в журнале	Возможная причина ошибки
Ошибка разрешения доменного имени / DNS resolution error	ErrorUnknownServer	Доменное имя VPN-сервера, указанное в параметрах подключения клиента, не определяется DNS-сервером. Вероятные причины: - Не получен ответ от DNS-сервера. - Неверно указано доменное имя VPN-сервера в параметрах подключения на клиенте. - На DNS-сервере не определено доменное имя VPN-сервера
Сервер не отвечает / No response from server	- NoResponse; - DeadPeerDetected; - IkeRekeyFailed; - EspRekeyFailed	Ошибка появляется в момент истечения таймера на клиенте при ожидании пакета от VPN-сервера. Возможные причины: - Тайм-аут ожидания IKE_INIT response. - Тайм-аут механизма DPD (не получен ответ от VPN-сервера). - Тайм-аут IKE_AUTH. - Тайм-аут в процессе пересоздания ключей IKE-туннеля. - Тайм-аут в процессе пересоздания ключей ESP-туннеля
Ошибка аутентификации / Authentication error	- AuthenticationFailed; - InvalidLoginOrPassword; - MfaTimeout	Возможные причины: - Неверный пароль, логин, сертификат клиента или временный пароль MFA. - Тайм-аут ввода временного пароля MFA
Сертификат сервера недействителен / Server certificate is invalid	- InvalidServerSignature; - ServerNameNotFound	Ошибка проверки сертификата сервера. Возможные причины: - Неуспешная проверка цифровой подписи сертификата VPN-сервера. - CN, указанный в сертификате, не соответствует адресу VPN-сервера
Ошибка конфигурации / Configuration error	ConfigurationSystemFailed	Ошибка применения конфигурации на клиенте. Возможные причины: - Ошибка применения маршрутов. - Ошибка получения и применения IP-адреса клиента

Ошибка соединения	Сообщение об ошибке в журнале	Возможная причина ошибки
Ошибка в параметрах криптографии / Error in cryptography parameters	- InvalidDhGroups; - IkeSecurityIncompatible; - EspSecurityIncompatible	Параметры криптографии, предложенные сервером, не применимы для клиента. Возможные причины: - Неподдерживаемая DH-группа. - Неподдерживаемые параметры ESP (алгоритмы шифрования и аутентификации). - Неподдерживаемые параметры IKE (алгоритмы шифрования и аутентификации). - На сервере выключен туннельный интерфейс
Сервер принудительно разорвал соединение / Server forcibly terminated the connection	TerminateFromServer	Сервер завершил сессию: От сервера получено сообщение IKE_DELETE
Обнаружен вход в систему под другой учетной записью / Login detected under a different user account	Logout	Отслеживание входа другого пользователя в систему: - Агент обнаружил появление в операционной системе активной сессии с новой учетной записью во время установленного VPN-соединения. - При установлении VPN-соединения агент обнаружил, что в операционной системе зарегистрировано более одной учетной записи с активными сессиями
Драйвер USB-токена недоступен / USB token software is unavailable	UsbTokenDriverUnavailable	При аутентификации по сертификату на USB-токене приложение обнаруживает, что драйвер USB-токена недоступен. Приложение не может получить доступ к USB-токену
Криптопровайдер недоступен / Cryptographic provider is unavailable	CryptoProviderUnavailable	При аутентификации по сертификату приложение обнаруживает, что криптопровайдер недоступен. Невозможно совершить криптографическую операцию для аутентификации
USB-токен не подключен / USB token is not connected	UsbTokenNotConnected	При аутентификации по сертификату на USB-токене приложение обнаруживает, что USB-токен не подключен
Выбранный сертификат недоступен / Selected certificate is unavailable	SelectedCertificateUnavailable	При аутентификации по сертификату приложение обнаруживает, что выбранный сертификат недоступен. Сертификат, сохранённый в VPN-соединении, не найден. Client не может получить доступ к выбранному сертификату или связанному с ним контейнеру
ПИН-код заблокирован / PIN is blocked	PinBlocked	USB-токен вернул состояние блокировки PIN-кода. Количество допустимых попыток ввода PIN-кода исчерпано
Неверный ПИН-код / Incorrect PIN	InvalidPin	USB-токен вернул ошибку неверного PIN-кода. Доступ к закрытому ключу не предоставлен
Ошибка сертификата / Certificate error	CertificateError	Приложение обнаружило, что сертификат не может быть использован. Возможные причины: - сертификат не соответствует ожидаемому формату; - отсутствует закрытый ключ; - не выполнена криптографическая операция
Драйвер USB-токена недоступен / USB token software is unavailable	UsbTokenDriverUnavailable	Приложение не может получить доступ к USB-токену. Возможная причина: драйвер/библиотека для работы с USB-токеном недоступны

Ошибка соединения	Сообщение об ошибке в журнале	Возможная причина ошибки
Криптопровайдер недоступен / Cryptographic provider is unavailable	CryptoProviderUnavailable	Не удалось выполнить аутентификацию по сертификату. Возможная причина: приложению не удалось получить доступ к криптографическому провайдеру
USB-токен не подключен / USB token is not connected	UsbTokenNotConnected	Не удалось выполнить аутентификацию по сертификату. Возможная причина: USB-токен не подключен
Выбранный сертификат недоступен / Selected certificate is unavailable	SelectedCertificateUnavailable	Сертификат, сохраненный в VPN-соединении, не найден. Приложение не может получить доступ к выбранному сертификату или связанному с ним контейнеру
ПИН-код заблокирован / PIN is blocked	PinBlocked	Введенный ПИН-код заблокирован. Возможная причина: количество допустимых попыток ввода ПИН-кода исчерпано
Неверный ПИН-код / Incorrect PIN	InvalidPin	Доступ к закрытому ключу не предоставлен. Введен неверный ПИН-код
Ошибка сертификата / Certificate error	CertificateError	Сертификат не может быть использован. Возможные причины: - Сертификат не соответствует ожидаемому формату. - Отсутствует закрытый ключ. - Не удалось выполнить криптографическую операцию.

