

Table of Contents

Table of Contents	1
UserGate Client	2
UserGate Client для Windows	3
EndPoint Client for Windows 7.5.x	4
Общие сведения	5
Лицензирование	6
Установка UserGate Client	8
Работа UserGate Client в связке с UserGate MC	11
Работа UserGate Client в связке с UserGate NGFW	13
Установка VPN-соединения с помощью UserGate Client для Windows	15
UserGate Client для Linux	17
UserGate Client для Linux 7.4.1	18
Общие сведения	19
Установка UserGate Client	20
Работа UserGate Client в связке с UserGate NGFW	24
Настройка VPN-соединения на устройстве пользователя	26
Ошибки VPN-подключений	30
UserGate Client для Linux 7.5.0	32
Общие сведения	33
Установка UserGate Client	34
Настройка VPN-подключений с помощью UserGate Client	36
Ошибки VPN-подключений	38
UserGate Client для macOS	41
UserGate Client для macOS 7.4.1	42
Общие сведения	43
Установка UserGate Client	44
Работа UserGate Client в связке с UserGate NGFW	47
Настройка VPN-соединения на устройстве пользователя	49
Ошибки VPN-подключений	52
UserGate Client для macOS 7.5.0	54
Общие сведения	55
Установка UserGate Client	56
Настройка VPN-подключений с помощью UserGate Client	57
Ошибки VPN-подключений	59

Общие сведения

Product: UserGate Client

Version: 7.5.x

Приложение UserGate Client для Windows является компонентом экосистемы UserGate SUMMA. Приложение защищает устройства пользователей от угроз безопасности и предотвращает их использование в качестве источника атак на сетевую инфраструктуру.

UserGate Client для Windows поддерживает следующие функции:

- Установление защищенного соединения с VPN-сервером UserGate NGFW по протоколу IPsec (IKEv2).
- Аутентификация пользователей посредством x.509-сертификатов или с помощью методов EAP, PEAP.
- Поддержка режима многофакторной аутентификации пользователей с использованием одноразовых кодов TOTP.
- 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.
- Централизованное управление сетевыми параметрами, политиками безопасности и контентной фильтрации на устройстве пользователя через систему UserGate Management Center.
- Проверка устройства пользователя на соответствие требованиям безопасности, реализованная на основе HIP-профилей.
- Сбор телеметрической информации, журналов ОС, других данных о безопасности устройства пользователя и передача их в систему анализа событий UserGate SIEM, где эти данные могут быть использованы для автоматического реагирования на угрозы безопасности.

Лицензирование

Product: UserGate Client
Version: 7.5.x

UserGate Client не является самостоятельным продуктом и предназначен для интеграции с UserGate Management Center (MC) или UserGate NGFW, а его функциональные возможности зависят от выбранного варианта интеграции и приобретенных лицензий.

Функция	UserGate NGFW	UserGate MC	
	Подписка UserGate Client	Базовая лицензия UserGate Client	Базовая лицензия UserGate Client + подписка на модуль NAC
VPN	+	+	+
Настройка параметров VPN	Диалоговое окно на конечном устройстве	Централизованно на MC	Централизованно на MC
Пользователи	Только VPN-пользователи	Все	Все
Телеметрия состояния	+	+	+
Телеметрия событий	–	+	+
Host Information Profile (HIP)	+	–	+
Настройка локального межсетевого экрана конечного устройства	–	+	+
Блокировка на локальном межсетевом экране конечного устройства	–	–	+

Интеграция с UserGate NGFW

При интеграции UserGate Client с UserGate NGFW доступны следующие функции клиента:

- VPN-подключение — установление защищенного туннеля между конечным устройством с установленным UserGate Client и VPN-сервером UserGate. Настройка параметров VPN выполняется непосредственно в приложении UserGate Client на конечном устройстве.
- Сбор телеметрии — передача на UserGate NGFW информации о состоянии конечного устройства.
- Контроль доступа с использованием HIP-профилей — управление доступом конечных устройств к сетевым ресурсам с помощью правил межсетевого экрана UserGate NGFW, в которых HIP-профиль используется в качестве одного из условий применения правила.

Лицензирование

Для интеграции с UserGate NGFW требуется приобрести подписку UserGate Client для UserGate NGFW. Подписка приобретается на срок от 1 года до 5 лет и определяет количество интегрируемых конечных устройств. Поставка лицензий осуществляется наборами: 10, 100 или 1000 устройств.

По истечении срока действия подписки:

- правила межсетевого экрана на UserGate NGFW, использующие HIP-профили в качестве условий фильтрации, перестают действовать;
- остаётся возможность установления VPN-подключений с VPN-серверами UserGate.

Для продолжения работы функции контроля доступа с использованием HIP-профилей необходимо продлить подписку.

Подробнее об интеграции UserGate Client с UserGate NGFW — в разделе « [Работа UserGate Client в связке с UserGate NGFW](#) ».

Подробнее о лицензировании UserGate NGFW — в разделе « [Лицензирование UserGate NGFW](#) ».

Интеграция с UserGate Management Center

При интеграции UserGate Client с UserGate MC доступны следующие функции клиента:

- Централизованное управление конечными устройствами (за исключением контроля соответствия требованиям безопасности через HIP-профили).
- VPN-подключение — установление защищенного туннеля между конечным устройством с установленным UserGate Client и VPN-сервером UserGate. Параметры VPN-подключений централизованно настраиваются администратором на UserGate MC и автоматически передаются на управляемые конечные устройства.
- Сбор телеметрии и событий безопасности с конечных устройств.
- Проверка конечных устройств на соответствие требованиям безопасности с помощью HIP-профилей (контроль комплаенса).
- Управление доступом в сеть по результатам проверки комплаенса непосредственно на уровне конечного устройства.

Лицензирование

Для интеграции конечных устройств с UserGate Management Center предусмотрены следующие лицензии:

- базовая лицензия UserGate Client;
- подписка на модуль NAC.

Базовая лицензия UserGate Client

Базовая лицензия UserGate Client является обязательной для интеграции конечных устройств с UserGate MC.

С базовой лицензией конечным устройствам доступны функции централизованного управления (за исключением контроля соответствия требованиям безопасности через HIP-профили), VPN-подключения и сбор телеметрии.

Лицензия приобретается наборами по 10, 100, 1000 или 10 000 устройств. Срок действия лицензии не ограничен.

Дополнительный модуль NAC

Подписка на модуль NAC приобретается дополнительно к базовой лицензии. Поставляется на срок от 1 до 5 лет наборами по 10, 100, 1000 или 10 000 устройств.

Модуль NAC предоставляет доступ к функциям контроля комплаенса и управления доступом в сеть на уровне межсетевого экрана на конечном устройстве.

По истечении срока действия лицензии NAC контроль доступа на основе комплаенса прекращается. Правила межсетевого экрана, использующие HIP-профиль в качестве условия фильтрации, перестают работать. Для продолжения работы необходимо продлить подписку.

Подробнее об интеграции с UserGate MC — в разделе « [Работа UserGate Client в связке с UserGate MC](#) ».

Подробнее о лицензировании UserGate MC — в разделе « [Лицензирование UserGate MC](#) ».

Установка UserGate Client

Product: UserGate Client
Version: 7.5.x

UserGate Client для Windows поставляется в формате установочного MSI- или EXE-файла, позволяющего выполнить установку вручную или с использованием инструментов автоматизации.

Минимальные системные требования

Минимальные системные требования для установки приложения:

- Операционная система: Windows 10 (64-bit) или Windows 11 (64-bit).
- Оперативная память (ОЗУ): не менее 2 ГБ.
- Процессор: тактовая частота от 2 ГГц.
- Свободное дисковое пространство: минимум 200 МБ.

Порядок установки приложения

Для установки приложения в ручном режиме запустите установочный файл. Во время установки запустится мастер настройки клиента, который предложит задать параметры подключения к UserGate Management Center — IP-адрес и код конечного устройства, созданный в центре управления. При работе без UserGate Management Center нажмите Cancel и введите параметры подключения к VPN-серверу UserGate NGFW.

ПримечаниеПосле установки UserGate Client компьютер будет перезагружен. Это необходимо для корректной работы приложения.

Установка приложения в автоматическом режиме осуществляется с помощью групповых политик Microsoft Active Directory. Для публикации приложения в Active Directory требуется MSI-файл с инсталлятором и административный шаблон [UserGateClient.adm](#), который используется для указания IP-адреса UserGate Management Center и кода устройства пользователя, созданного в центре управления.

После завершения установки UserGate Client получает конфигурацию, назначенную ему в UserGate Management Center, и передает информацию об устройстве пользователя в центр управления.

Приложение UserGate Client для Windows имеет несколько вкладок для настройки параметров.

Вкладка	Описание
General	Информация об устройстве пользователя (пользователь, имя компьютера, IP-адрес для выхода в Интернет, версия Windows) и VPN-подключении (статус подключения; VPN IP-адрес подключения конечного устройства; количество байтов, переданных и полученных с момента подключения по VPN; длительность соединения). Параметры для настройки: • Флажок Save login — сохранение логина пользователя для VPN-подключения после перезагрузки конечного устройства. • Флажок Reconnect — переподключение к VPN-серверу в случае обрыва связи. В случае потери соединения будет отображено начальное окно интерфейса приложения. Если опция переподключения активна, приложение будет производить повторные попытки подключения к серверу; если функция отключена — будет отображено начальное окно с выбором сервера. • Флажок Popup in center — отображение начального окна интерфейса приложения в центре экрана в случае обрыва VPN-соединения

Вкладка	Описание
Logs	Настройка параметров журналирования. • Logging level — уровень детализации: ◦ Off — отключить ведение журнала диагностики; ◦ Critical — критические события; ◦ Error — журналировать только ошибки; ◦ Warning — журналировать ошибки и предупреждения; ◦ Info — журналировать ошибки, предупреждения и дополнительную информацию; ◦ Debug — максимальная детализация. Журнал находится в разделе: %ALLUSERSPROFILE%\UserGate\UserGate Client\var\log\usergateclient\ug_client.log. • Tooltips history — история оповещений. • Export logs — скачать журнал диагностики (после скачивания откроется архив с файлом журнала диагностики)
Network	Просмотр информации о сетевых параметрах и параметрах маршрутизации: • IPCONFIG — информация о всех сетевых адаптерах и текущей конфигурации TCP/IP. • ROUTING — записи локальной таблицы маршрутизации. • SOCKETS — список активных подключений (тип порта, адреса, состояние соединения, идентификатор процесса). Чтобы скопировать информацию, нажмите Copy
Policy	Просмотр информации о безопасности устройства пользователя (статус межсетевого экрана, антивируса, центров обновления и безопасности Windows). Значение индикации: • желтый — отключен; • зеленый — включен; • красный — не соответствует политикам безопасности
Advanced	Управление контентной фильтрацией (возможность самостоятельного отключения контентной фильтрации в соответствии с политиками, настроенными на сервере UserGate Management Center)

Параметры подключения к UserGate MC (IP-адрес UserGate MC и код для подключения устройства пользователя) можно посмотреть в файле C:\ProgramData\UserGate\UserGate Client\etc\main.cfg.

Важно! В случае обновления операционной системы конечного устройства с Windows 10 до Windows 11 требуется удалить приложение UserGate Client средствами операционной системы и выполнить его повторную установку. О порядке корректного удаления приложения — в разделе «[Удаление приложения](#)».

Журналирование

События работы UserGate Client фиксируются во внутреннем журнале и в журнале приложений Windows.

В журнале приложений Windows документируются следующие типы событий:

- Запуск и остановка сервиса (события UG0101 Service started и UG0102 Service stopped).
- Подключение к UserGate Management Center и потеря связи (события UG0201 MC connected и UG0202 MC connection lost).
- Подключение по VPN и завершение сессии, в том числе ошибки подключения — недоступность сервера, неправильно указанные данные (события UG0301 VPN connected и UG0302 VPN disconnected).
- Получение конфигурации от UserGate Management Center (событие UG0401 MC rules propagated).

Удаление приложения

Чтобы удалить приложение на устройстве пользователя перейдите в раздел **Пуск → Параметры → Приложения → Установленные приложения (Панель управления → Программы → Программы и компоненты** в Windows 10), найдите в списке приложений **UserGate Client** и выберите **Удалить**.

Важно! Для корректного удаления и обновления UserGate Client на конечном устройстве не должно быть активных правил локального межсетевого экрана, синхронизированных с UserGate MC.

После удаления приложения необходимо перезагрузить компьютер.

Product: UserGate Client

Version: 7.5.x

Интеграция конечных устройств с UserGate Management Center (UserGate MC) позволяет администратору централизованно управлять их конфигурацией и режимами работы.

Через платформу UserGate MC доступны следующие функции:

- Управление параметрами UserGate Client на конечных устройствах.
- Гибкая настройка политик безопасности через правила межсетевого экрана на конечном устройстве.
- Проверка соответствия конечных устройств требованиям безопасности с помощью HIP-профилей.
- Централизованное создание и распространение параметров VPN-подключений для UserGate Client.
- Передача данных телеметрии и событий безопасности конечных устройств на устройства UserGate LogAn и UserGate SIEM для анализа и автоматического реагирования на угрозы безопасности.

Регистрация конечных устройств на UserGate MC происходит через порт 4045. В процессе регистрации применяется пин-код, созданный на UserGate MC. Конечному устройству присваивается уникальный идентификатор, который будет использован в дальнейшем для взаимодействия с платформой управления. Подробнее о добавлении конечных устройств под управление UserGate MC — в разделе [«Добавление конечных устройств под управление UGMC»](#).

После регистрации конечное устройство запрашивает параметры конфигурации у UserGate MC каждые 10 секунд. UserGate MC отправляет на конечное устройство:

- параметры межсетевого экрана;
- параметры VPN-подключений;
- общие параметры шаблонов;
- библиотеки элементов;
- HIP-объекты и профили, если они используются в правилах межсетевого экрана.

Отправка конфигурации на конечное устройство происходит автоматически при ее изменении на управляющем UserGate MC.

Конечное устройство передает на UserGate MC следующие данные:

- Телеметрию системы:
 - данные о загрузке центрального процессора;
 - сведения о накопителях;
 - время непрерывной работы;
 - другую статистику производительности.
- Параметры для проверки соответствия HIP (подробнее — в разделе « [Проверка HIP на UserGate MC](#) »):
 - статус средств безопасности (состояние антивируса, межсетевого экрана, автоматических обновлений системы, BitLocker);
 - список активных процессов и служб;
 - перечень установленного программного обеспечения;
 - список установленных обновлений.

Данные о конфигурации отправляются конечным устройством только в случае наличия изменений.

При выполнении операций поиска в соответствующем разделе UserGate MC, конечное устройство отправляет на UserGate MC следующую дополнительную информацию:

- временные метки — текущее время и время последней загрузки конечного устройства с указанием часового пояса;
- сведения о подключенных USB-устройствах;
- сведения об элементах автозагрузки;

- данные о точках восстановления системы;
- расширенные данные о производительности;
- данные об обновлениях и ключах реестра.

UserGate Log Analyzer получает данные с конечных устройств не напрямую, а через UserGate Management Center (MC). Соединение между UserGate LogAn и UserGate MC защищено SSH-туннелем, по которому передается вся информация: телеметрия, журналы Windows и иные данные безопасности. Эти данные используются для последующего анализа и автоматического реагирования на угрозы.

Подробнее о централизованном управлении конечными устройствами с помощью UserGate MC — в разделе « [Централизованное управление конечными устройствами](#) ».

Проверка HIP на UserGate MC

В UserGate MC реализована возможность проверки конечного устройства на соответствие требованиям безопасности (комплаенса) с помощью HIP-профилей.

Технология HIP (Host Information Profile) предназначена для сбора и анализа данных о состоянии защиты конечных устройств. Она позволяет оценивать уровень соответствия устройств заданным требованиям безопасности и использовать эти данные для управления доступом к сетевым ресурсам.

С помощью HIP проверяется наличие и актуальность антивирусного ПО, состояние локального межсетевого экрана, версия операционной системы, установленные обновления и другие параметры безопасности. Администратор сети может настраивать [HIP-объекты](#) (например, требования к наличию антивируса или установленным обновлениям операционной системы). Эти объекты объединяются в [HIP-профили](#), которые задают правила проверки устройств. Результаты проверки HIP могут использоваться как условие для предоставления доступа. Например, доступ в корпоративную сеть или к критически важным приложениям может быть разрешен только устройствам, соответствующим заданным HIP-профилям.

Примечание Условия HIP-объекта при проверке не выполняются, если используется критерий «Ключи реестра» со строковым значением ключа, содержащим символы кириллицы.

Проверка соответствия конечных устройств требованиям безопасности производится следующим образом:

Конечное устройство отправляет на UserGate MC следующие данные:

- информацию о пользователях;
- данные о системе (версия, издание, NetBIOS-имя);
- список запущенных процессов;
- список запущенных служб;
- список установленного программного обеспечения (название, производитель ПО, версия);
- ключи реестра;
- список обновлений системы;
- элементы автозагрузки;
- информацию о защищенности системы (антивирус, межсетевой экран, BitLocker и т. п.);
- информацию о точках восстановления системы.

Для проверки на соответствие требованиям безопасности используются только HIP-профили, указанные в правилах межсетевого экрана в качестве одного из условий фильтрации. В случае успешной проверки правило межсетевого экрана будет отправлено на конечное устройство с установленным клиентом.

Примечание Если HIP-профиль не указан в параметрах правила межсетевого экрана на UserGate MC, такое правило применяется на всех конечных устройствах.

Product: UserGate Client

Version: 7.5.x

UserGate NGFW при работе в связке с конечными устройствами с установленным приложением UserGate Client может выполнять функции VPN-сервера, сервера контроля сетевого доступа и межсетевого экрана.

После установления VPN-соединения конечные устройства автоматически регистрируются на UserGate NGFW. Взаимодействие конечных устройств с UserGate NGFW производится по порту 4045 с использованием протокола HTTPS.

После регистрации на UserGate NGFW каждому новому конечному устройству присваивается уникальный идентификатор, который хранится в базе UserGate NGFW.

Конечное устройство периодически отправляет на UserGate NGFW данные телеметрии. UserGate NGFW на основе полученных данных выполняет проверку соответствия конечных устройств требованиям безопасности с помощью HIP-профилей. Информация о результате проверки передается далее для использования в правилах межсетевого экрана UserGate NGFW.

Примечание Если конечное устройство подключено к UserGate Management Center, регистрации на NGFW после установки VPN-соединения не произойдет. Функция проверки соответствия конечного устройства правилам политики безопасности будет производиться на UserGate MC.

Тайм-аут активности конечных устройств составляет две минуты, то есть, если в течение двух минут на UserGate NGFW не поступает информация от конечного устройства, оно считается неактивным. По истечении трех периодов неактивности запись о конечном устройстве удаляется из базы UserGate NGFW. При повторном подключении конечное устройство будет заново зарегистрировано. Если конечное устройство будет подключено до истечения этого времени, его запись будет обновлена.

После подключения к другому VPN-серверу конечное устройство будет зарегистрировано на новом UserGate NGFW.

Проверка HIP на UserGate NGFW

Проверка на соответствие требованиям безопасности (комплаенса) на UserGate NGFW происходит по следующей схеме.

Конечное устройство отправляет на UserGate NGFW данные телеметрии:

- информацию о пользователях;
- данные о системе (версия, издание, netbios-имя);
- список запущенных процессов;
- список запущенных служб;
- список установленного программного обеспечения (название, вендор, версия);
- ключи реестра, которые используются в HIP-объектах;
- список обновлений системы;
- элементы автозагрузки;
- информацию о защищенности системы (антивирус, межсетевой экран, BitLocker и т. п.);
- информацию о точках восстановления системы.

Полученные от конечного устройства данные расшифровываются и передаются для сравнения [с HIP-профилями](#). Информация о результате проверки используется в правилах межсетевого экрана UserGate NGFW. Если конечное устройство соответствует всем условиям правила межсетевого экрана на UserGate NGFW, это правило становится активным для данного конечного устройства.

Примечание Условия HIP-объекта при проверке не выполняются, если используется критерий «Ключи реестра» со строковым значением

ключа, содержащим символы кириллицы.

Примечание Для работы с конечными устройствами UserGate Client необходимо наличие соответствующей лицензии на UserGate NGFW. Подробнее — в разделе «[Лицензирование](#)». В случае отсутствия соответствующей лицензии регистрации конечного устройства на UserGate NGFW не произойдет; будет установлено только VPN-соединение.

Для подключения конечного устройства к UserGate NGFW:

1. В выбранной зоне UserGate NGFW разрешите подключение конечных устройств. Для этого в параметрах зоны разрешите сервис «Подключение конечных устройств».
2. Укажите данные для установки защищенного соединения между конечным устройством и UserGate NGFW. Для этого в веб-консоли UserGate NGFW в разделе **Настройки → Консоль администратора → Настройки** укажите сертификат и профиль для установки защищенного соединения. При подключении конечное устройство будет проверять актуальность сертификата UserGate NGFW. В случае смены сертификата на UserGate NGFW при наличии уже подключенных конечных устройств необходимо распространить корневой сертификат удостоверяющего центра (Root CA); сертификат необходимо поместить в хранилище локального компьютера «Доверенные корневые центры сертификации».
3. Настройте UserGate NGFW в качестве VPN-сервера. Подробнее о настройке UserGate NGFW в качестве VPN-сервера для сценария удаленного подключения конечных устройств — в разделе «[VPN для удаленного доступа клиентов \(Remote access VPN\)](#)».

После установки VPN-соединения регистрация конечного устройства произойдет автоматически. Политики безопасности, настроенные на UserGate NGFW, также будут применены к конечным устройствам. Для проверки на соответствие требованиям безопасности (комплаенса) конечное устройство будет отправлять телеметрию на UserGate NGFW с периодичностью в 1 минуту.

Конечное устройство будет производить попытку регистрации каждый раз после подключения к новому VPN-серверу.

Установка VPN-соединения с помощью UserGate Client для Windows

Product: UserGate Client

Version: 7.5.x

Встроенный в приложение UserGate Client для Windows VPN-клиент использует следующие параметры для установления VPN-соединения:

- Протокол для установления защищенного соединения: IPsec (IKEv2).
- Аутентификация с помощью x.509-сертификатов или с помощью методов EAP, PEAP.
- Функция DPD (Dead Peer Detection), работающая в режиме On idle (при отсутствии трафика) с интервалом 15 секунд и максимальным количеством неудачных попыток — 6. Проверка доступности соседнего узла активируется в случае отсутствия трафика в туннеле в течение двойного интервала времени (30 секунд). Если не получен ответ от сервера на запрос проверки, пакеты продолжают отсылаться до максимально разрешенного количества попыток с интервалом 5 секунд. Если ответ получен, происходит возврат к первоначальному интервалу. Если ответ не получен — соединение разрывается.
- Группы Диффи — Хеллмана: группа 2 Prime 1024, группа 14 Prime 2048, группа 16 Prime 4096.
- Алгоритмы аутентификации и шифрования (фазы 1 и 2): SHA1/AES128, SHA256/AES128, SHA384/AES128, SHA1/AES256, SHA256/AES256, SHA384/AES256, SHA1/3DES, SHA256/3DES, SHA384/3DES.
- Максимальный размер данных, шифруемых одним ключом (фаза 2): не ограничен.

При работе в связке с UserGate Management Center параметры параметров VPN-подключений централизованно задаются администратором сети [на UserGate MC](#) и передаются на управляемое конечное устройство по его запросу.

Если конечное устройство не интегрировано с UserGate MC, введите параметры соединения в начальном окне графического интерфейса приложения UserGate Client:

- адрес VPN-сервера (IP-адрес или FQDN);
- параметры аутентификации (логин с паролем или сертификат).

Примечание При использовании FQDN для подключения, если имени VPN-сервера соответствует несколько IP-адресов, клиент устанавливает соединение по первому адресу, который отвечает на запросы.

Примечание Для корректного установления VPN-подключения с UserGate NGFW по протоколу IKEv2 логин и пароль, используемые клиентом, не должны содержать символы кириллицы.

Для установления VPN-соединения:

1. В строке состояния нажмите на значок UserGate Client.



2. В появившемся окне выберите VPN-сервер для подключения и нажмите **Connect**.

3. При необходимости введите имя пользователя и пароль, затем нажмите **Next**.

При успешном установлении соединения в окне приложения отобразится статус VPN Connected и данные установившегося соединения.

Если администратором VPN-сервера настроена функция раздельного туннелирования, маршруты, полученные от VPN-сервера, будут добавлены в таблицу маршрутизации конечного устройства при установлении соединения.

Чтобы разорвать VPN-соединение, нажмите **Disconnect** в окне приложения.

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](#) ».

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](#) ».

Product: uClient
Version: 7.5.x
Technology: VPN

UserGate Client предназначен для подключений к VPN-серверам 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.

Общие сведения

Product: UserGate Client

Version: 7.4.1

Technology: VPN

Приложение UserGate Client для macOS 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.

Product: UserGate Client

Version: 7.4.1

Technology: VPN

UserGate Client для macOS поставляется в виде PKG-файла. Скачать последнюю версию приложения можно [с официального сайта UserGate](#).

Минимальные системные требования

Минимальные системные требования для установки приложения:

- Операционная система:
 - macOS Tahoe (26);
 - macOS Sequoia (15).
- Оперативная память (RAM): не менее 4 ГБ.
- Свободное дисковое пространство: минимум 500 МБ.

Порядок установки приложения

Для установки клиента запустите PKG-файл и следуйте указаниям установщика.

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 добавьте сертификат в связку ключей (keychain) в раздел «Система».

Примечание Для работы с клиентом на macOS время жизни серверного сертификата должно быть не более 825 дней.

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 соединения, инициированного

ЭТИМ КЛИЕНТОМ.

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

Product: UserGate Client

Version: 7.4.1

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.

Для установления соединения включите соответствующий профиль на странице **VPN-соединения**.

Статус соединения будет указан рядом с активным переключателем.

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

Чтобы завершить VPN-соединение, отключите активный профиль в окне приложения.

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 macOS поставляется в виде PKG-файла для установки в операционной системе macOS. Скачать последнюю версию приложения можно [с официального сайта UserGate](#).

Минимальные системные требования

Минимальные системные требования для установки приложения:

- Операционная система:
 - macOS Tahoe (26);
 - macOS Sequoia (15).
- Оперативная память (RAM): не менее 4 ГБ.
- Свободное дисковое пространство: минимум 500 МБ

Порядок установки приложения

Для установки клиента запустите PKG-файл и следуйте указаниям установщика.

Для корректного удаления UserGate Client воспользуйтесь программой деинсталляции, установленной на компьютере вместе с клиентом.

Важно! Для работы с USB-токеном Рутокен ЭЦП 3.0 необходимо установить библиотеку libtpkcs11еср. Подробнее о работе с устройствами Рутокен ЭЦП — [на официальном портале документации Рутокен](#). Библиотеку можно скачать [в центре загрузки Рутокен](#).

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 добавьте сертификат в связку ключей (keychain) в раздел «Система».

Примечание Для работы с клиентом на macOS время жизни серверного сертификата должно быть не более 825 дней.

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.

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

Product: uClient
Version: 7.5.x
Technology: VPN

UserGate Client предназначен для подключений к VPN-серверам 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 приложение 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 приложении 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 для 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

Чтобы инициировать подключение к VPN-серверу включите выбранный профиль соединения в окне приложения UserGate Client. 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.

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

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.

