

iMobile

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«RDP-FIDO-GATE»

Версия 1.25.1

Руководство пользователя

IM.RDP-FIDO.RU.03

Листов 12

АННОТАЦИЯ

Настоящее руководство описывает работу пользователя с клиентскими программами RDP-FIDO-GATE: подготовку к работе, регистрацию ключа, подключение к удалённому компьютеру, работу с потоком FIDO Stream и консолью SSH, защиту входа в клиент. Основная часть относится к клиенту для Windows версии 1.25.0; отличия клиентов для Linux (1.25.1) и Android (0.9.1, предварительная бета-версия) приведены в отдельных подразделах.

Установку программы и настройку шлюза на удалённом компьютере выполняет администратор по руководству по установке и администрированию.

СОДЕРЖАНИЕ

1. Назначение	4
2. Условия работы	4
3. Начало работы	4
3.1. Активация клиента для Windows	4
3.2. Добавление сессии	5
3.3. Регистрация ключа	5
4. Основные операции	5
4.1. Подключение по RDP	5
4.2. Подключение в режиме FIDO Stream	6
4.3. Консоль SSH	6
4.4. Управление сессиями	7
4.5. Защита входа в клиент	7
4.6. Обновление клиента	9
4.7. Клиент для Linux	9
4.8. Клиент для Android	10
5. Сообщения и типичные затруднения	10
6. Завершение работы	11
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	12

1. НАЗНАЧЕНИЕ

Клиент хранит список удалённых компьютеров (сессий) и подключает к ним только после подтверждения личности: касания ключа безопасности FIDO2, подтверждения через Windows Hello либо ввода одноразового кода из приложения-аутентификатора. Порт удалённого рабочего стола на компьютере закрыт для всех; шлюз на этом компьютере открывает его адресу пользователя примерно на 90 секунд после успешной проверки.

Клиент позволяет:

- подключаться по RDP штатным средством операционной системы с подстановкой сохранённых имени и пароля;
- подключаться в режиме FIDO Stream — к экрану компьютера с малой задержкой, со звуком, геймпадом и передачей файлов;
- открывать консоль SSH с сохранёнными паролями, командами и помощником;
- защитить вход в сам клиент паролем или ключом.

2. УСЛОВИЯ РАБОТЫ

Для работы нужны:

- установленный клиент: в Windows — программа RDP FIDO Client из меню «Пуск», в Linux — `rdpfido-gui` или команда `rdpfido`, в Android — приложение RDP FIDO;
- второй фактор: ключ безопасности FIDO2 (USB или NFC), Windows Hello на рабочем компьютере либо, если шлюз настроен на коды, приложение-аутентификатор на телефоне;
- сведения от администратора: адрес компьютера, порт шлюза (обычно 7440) и одноразовый код регистрации ключа, который действует 15 минут;
- учётная запись на удалённом компьютере (имя и пароль): после открытия порта вход проверяет сама операционная система;
- для клиента в Windows — адрес электронной почты для активации и доступ в интернет при активации.

В редакции Free клиент для Windows сохраняет не более 10 сессий и показывает рекламную плитку; в редакции Pro этих ограничений нет.

3. НАЧАЛО РАБОТЫ

3.1. Активация клиента для Windows

Без активации клиент подключается 14 дней с первого запуска; число оставшихся дней показано в строке состояния.

- 1) Нажмите кнопку «Аккаунт».
- 2) Введите адрес электронной почты и нажмите «Получить код». На указанный адрес придёт письмо с кодом.
- 3) Введите код в поле «Код из письма» и нажмите «Активировать». Появится сообщение «Аккаунт активирован.».

Клиенты для Linux и Android активации не требуют.

3.2. Добавление сессии

- 1) Нажмите «Добавить» (Ctrl+N).
- 2) Заполните поля: «Лейбл» — название плитки; «Сервер RDP» — имя или адрес компьютера; «Логин», «Домен», «Пароль» — учётная запись на этом компьютере. Пароль сохраняется в зашифрованном виде.
- 3) В поле «Протокол» выберите способ подключения: «RDP (mstsc)», «FIDO Stream (игры, низкая задержка)» или «Консоль SSH (терминал, пароли, помощник ИИ)».
- 4) В группе «Шлюз FIDO» оставьте флажок «Требовать подтверждение FIDO-ключом при подключении». Поле «Адрес» оставьте пустым, если шлюз находится на том же адресе, что и сервер; порт — 7440, если администратор не назвал другой.
- 5) Нажмите «Проверить». Ответ вида «Шлюз на ИМЯ, ключей: 0, окно доступа 90 с.» означает, что шлюз доступен.

3.3. Регистрация ключа

- 1) В окне сессии нажмите «Зарегистрировать ключ...».
- 2) Введите «Код регистрации», полученный от администратора, и «Название ключа» — по нему ключ отличают в списке на компьютере.
- 3) В поле «Хранить ключ» выберите: «Внешний ключ или телефон», «Этот компьютер (Windows Hello, отпечаток/PIN)» или «Любой — выберет Windows».
- 4) Нажмите «Зарегистрировать» и подтвердите запрос Windows: коснитесь ключа или подтвердите через Windows Hello.
- 5) После сообщения «Готово. Ключ зарегистрирован на ИМЯ.» закройте окно регистрации и нажмите «Сохранить».

На плитке появляется отметка FIDO: ключ зарегистрирован, сертификат шлюза запомнен. С этого момента клиент откажется работать со шлюзом, предъявившим другой сертификат.

Зарегистрируйте второй ключ тем же способом (администратор выдаст новый код): при утрате единственного ключа доступ восстанавливает только администратор с консоли компьютера.

Если шлюз настроен на одноразовые коды, вместо касания ключа клиент показывает QR-код и секрет. Отсканируйте QR-код приложением-аутентификатором и введите первый код из приложения.

4. ОСНОВНЫЕ ОПЕРАЦИИ

4.1. Подключение по RDP

- 1) Щёлкните плитку сессии или выберите её и нажмите Enter. Плитка показывает «Подтверждение ключом...».

- 2) Подтвердите запрос Windows: коснитесь ключа либо используйте Windows Hello. Если шлюз работает с одноразовыми кодами, введите 6-значный код из приложения-аутентификатора; один код принимается один раз.
- 3) В строке состояния появляется «Доступ открыт на 90 с (ключ «...»). Подключение...», затем открывается окно удалённого рабочего стола с подставленными именем и паролем.

Пока окно сеанса открыто, доступ сохраняется. Повторный щелчок по плитке с активным сеансом выводит его окно на передний план. Примерно через 12 секунд после подключения клиент делает снимок окна сеанса для плитки.

4.2. Подключение в режиме FIDO Stream

Режим выбирается в поле «Протокол» сессии. Подключение выполняется так же: щелчок по плитке и подтверждение ключом. Открывается окно потока.

Клавиши	Действие
Ctrl+Alt+Shift+M	Меню сеанса
Ctrl+Alt+Shift+Z	Захватить или отпустить мышь
Ctrl+Alt+Shift+X	Полный экран
Ctrl+Alt+Shift+D	Послать на компьютер Ctrl+Alt+Del
Ctrl+Alt+Shift+Q	Отключиться
Ctrl+Alt+O	Показать сведения о потоке
Ctrl+Alt+R	Запросить управление в общем сеансе

- Передача файлов. Перетащите файлы или папки в окно потока либо выберите в меню сеанса «Отправить файлы на хост...»; они появятся на удалённом компьютере в папке «RDP FIDO» каталога загрузок. Файл, положенный на удалённом компьютере в подпапку Outbox этой папки, передаётся на ваш компьютер.
- Общий сеанс. К одному потоку могут подключиться несколько участников; управляет один. Пока управление не у вас, вверху окна показана надпись «Только просмотр». В меню сеанса доступны пункты «Участники...», «Пригласить...» и передача управления.
- Параметры потока (баланс качества, звук, микрофон, кодек, направление соединения) задаются в группе «FIDO Stream» окна сессии; для первого подключения оставьте значения «Автоматически».

Со шлюзом, настроенным на одноразовые коды, режим FIDO Stream недоступен.

4.3. Консоль SSH

Консоль открывается щелчком по плитке с протоколом «Консоль SSH» либо пунктом «Консоль SSH...» в контекстном меню любой плитки. Плитки консоли собраны на вкладке «SSH»; вкладки переключаются клавишей Tab. Для сессии можно задать «Порт SSH», «Файл ключа» и «Параметры ssh».

В окне консоли — терминал и боковая панель с вкладками:

- «Пароли» — сохранённые пароли. Щелчок по записи вводит пароль в терминал; запись с флажком автоматического ввода отвечает на свой запрос сама.
- «Команды» — сохранённые команды; щелчок выполняет команду, «Вставить» вводит её без Enter.
- «Помощник» — диалог с моделью искусственного интеллекта, которая предлагает команды. Адрес сервиса, модель и ключ доступа задаются под значком шестерёнки. Предложенная команда выполняется только по вашему щелчку, если вы не включили иное. Текст терминала передаётся модели только при установленном флажке «Видит консоль».

Вкладки панели переключаются сочетаниями Ctrl+Shift+1, 2, 3; копирование — Ctrl+Shift+C, вставка — Ctrl+Shift+V. Порт SSH открывается ключом только на компьютерах со шлюзом для Linux, где администратор добавил этот порт под защиту.

4.4. Управление сессиями

Клавиши	Действие
Enter или щелчок	Подключиться
Ctrl+N	Новая сессия
Ctrl+F	Поиск по имени, адресу, логину
F2	Переименовать
F4	Изменить
F5	Перечитать список
Del	Удалить сессию вместе с сохранённым паролем и снимком
Tab	Переключить вкладки «Рабочие столы» и «SSH»

Контекстное меню плитки содержит также пункты «Дублировать», «Копировать адрес», «Сделать снимок для плитки», «Сдвинуть влево» и «Сдвинуть вправо». Удаление сессии не удаляет ключ на удалённом компьютере: это делает администратор.

Раз в минуту клиент проверяет защищаемые компьютеры. Красная рамка и надпись «ПОСТОРОННИЙ ДОСТУП К RDP!» на плитке означают, что порт удалённого рабочего стола отвечает без ключа; сообщите об этом администратору.

4.5. Защита входа в клиент

Вход в клиент можно закрыть одним из двух способов. Откройте «Настройки» (кнопка со значком шестерёнки), группа «Защита входа».

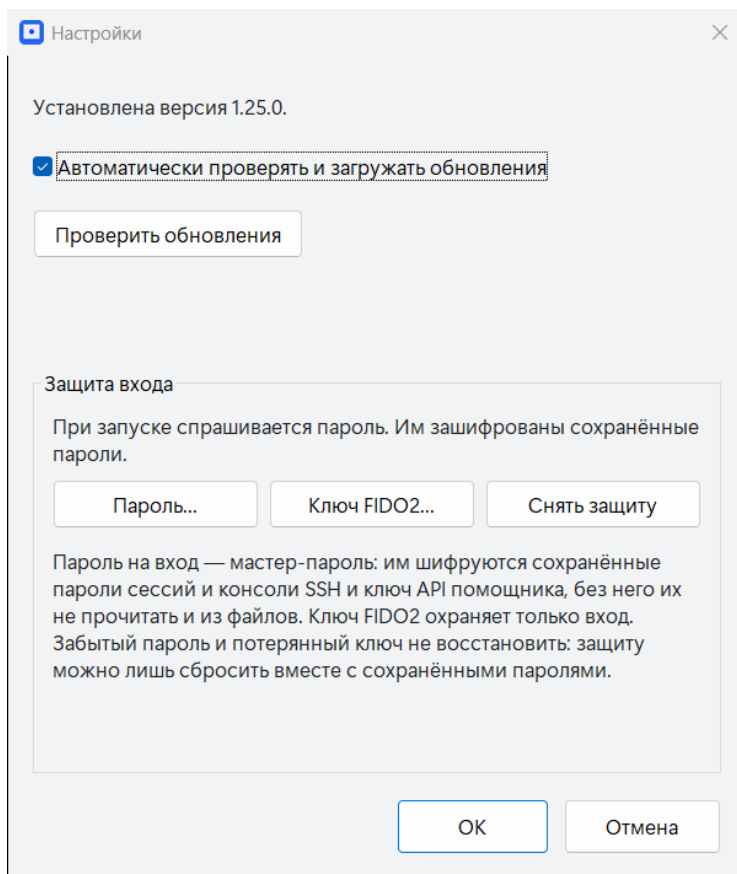


Рисунок 1 – Окно настроек клиента для Windows: группа «Защита входа» при заданном пароле

Пароль на вход (мастер-пароль):

- 1) Нажмите «Пароль...», введите пароль в поля «Новый пароль» и «Ещё раз» (не менее 4 знаков) и подтвердите.
- 2) При каждом запуске клиент спрашивает пароль до показа списка сессий. Этим паролем дополнительно зашифрованы сохранённые пароли сессий и консоли SSH и ключ доступа помощника.

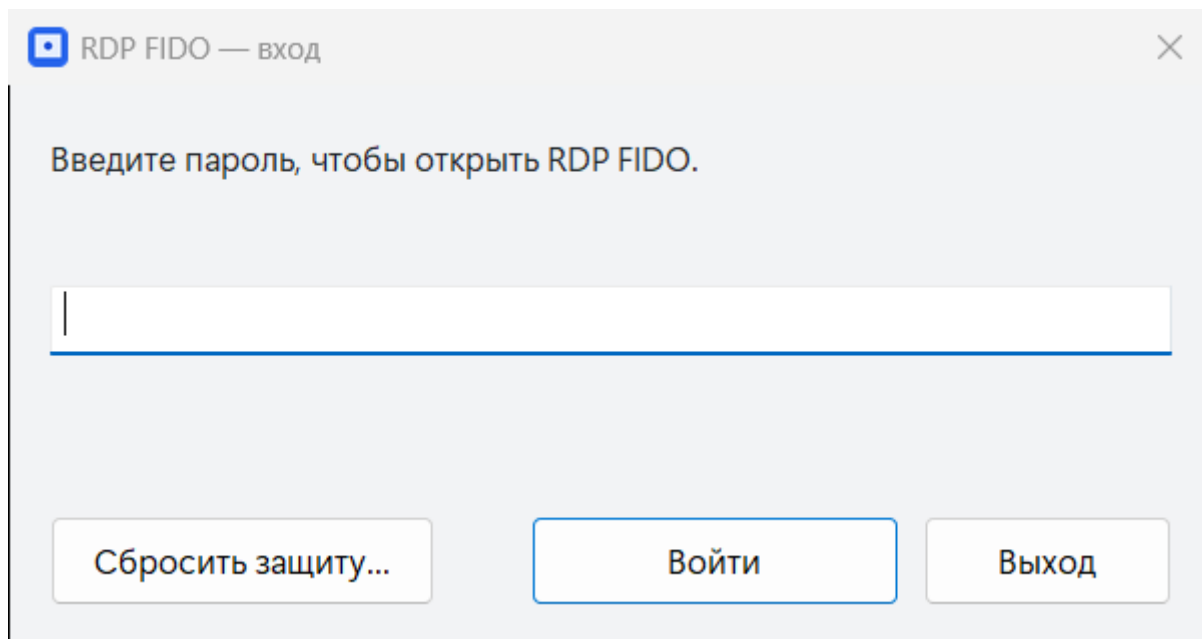


Рисунок 2 – Запрос пароля при запуске клиента

Ключ FIDO2 на вход: нажмите «Ключ FIDO2...», затем «Привязать ключ» и подтвердите ключом с PIN или отпечатком. Ключ охраняет только вход и сохранённые пароли не шифрует.

Пять неверных паролей подряд допускаются без задержки; далее перед каждой попыткой клиент требует подождать от 30 секунд до 15 минут. Кнопка «Снять защиту» отключает защиту после повторного ввода пароля или подтверждения ключом.

Примечание – Забытый пароль и утраченный ключ не восстанавливаются. Кнопка «Сбросить защиту...» в окне входа снимает защиту и удаляет сохранённые пароли сессий и консоли SSH, ключ доступа помощника и историю разговоров с ним. Сессии, команды и настройки сохраняются.

4.6. Обновление клиента

При запуске клиент проверяет наличие новой версии и предлагает установить её; открытые сеансы при этом не прерываются. Настройка «Автоматически проверять и загружать обновления» и кнопка «Проверить обновления» находятся в окне настроек. Версия старше одного года не подключается, пока не установлено обновление.

4.7. Клиент для Linux

Окно `rdpfido-gui` (в меню — «RDP FIDO») содержит список сессий и кнопки «Добавить», «Изменить», «Зарегистрировать ключ...», «Подключиться», «Поток (FIDO Stream)», «Защита входа». Те же действия доступны из командной строки:

```
rdpfido add --name office --host srv.example.com --user user1 --password  
rdpfido enroll office КОД --fingerprint ОТПЕЧАТОК  
rdpfido connect office      # подтверждение ключом и запуск FreeRDP  
rdpfido stream office      # поток FIDO Stream  
rdpfido ssh office         # открыть порт и запустить ssh  
rdpfido console office     # консоль SSH  
rdpfido lock password      # задать пароль на вход
```

Параметр `--fingerprint` — отпечаток сертификата шлюза, полученный от администратора: клиент сверяет его до отправки кода регистрации. Пароли сессий хранятся в связке ключей рабочего стола; если её нет, пароль запрашивается при подключении. Плитки и кнопки для консоли SSH в окне нет — она вызывается командой.

4.8. Клиент для Android

- 1) Нажмите «+», введите адрес компьютера и имя пользователя, выберите протокол: «FIDO Stream (игры, низкая задержка)» или «RDP (внешний клиент)».
- 2) Нажмите «Зарегистрировать ключ на этой машине», выберите ключ — «Этот телефон (биометрия)», «Ключ безопасности по NFC» или «Ключ безопасности по USB» — и введите код регистрации.
- 3) Для подключения коснитесь плитки и подтвердите вход отпечатком, блокировкой экрана или ключом. В режиме FIDO Stream открывается экран потока; в режиме RDP подключение передаётся установленному приложению RDP, а пароль сессии помещается в буфер обмена.

Защита входа включается значком замка в списке сессий. Приложение является предварительной бета-версией; вход по одноразовым кодам, совместный доступ и передача файлов в нём не реализованы.

5. СООБЩЕНИЯ И ТИПИЧНЫЕ ЗАТРУДНЕНИЯ

Сообщение или признак	Что делать
«Не удалось подключиться к шлюзу. Машина выключена или недоступна.»	Проверьте адрес и порт шлюза в сессии и подключение к сети; обратитесь к администратору
«Код регистрации не принят.»	Код одноразовый и действует 15 минут; попросите у администратора новый
«Подходящий ключ не найден.»	Вставьте зарегистрированный ключ и повторите
«Этот ключ не зарегистрирован на целевой машине.»	Зарегистрируйте ключ для этого компьютера
«Сертификат шлюза не совпадает с сохранённым.»	Не продолжайте; сообщите администратору. После подтверждённой переустановки шлюза зарегистрируйте ключ заново
«Слишком много попыток. Подождите и попробуйте снова.»	Подождите 5 минут
«Одноразовый код неверный, устарел или уже использован.»	Дождитесь следующего кода; проверьте, что время на телефоне устанавливается автоматически

Сообщение или признак	Что делать
«Доступ из вашей страны запрещён настройками целевой машины.»	Обратитесь к администратору
«Требуется активация»	Активируйте клиент по адресу электронной почты
«Лимит бесплатной версии»	Удалите ненужную сессию или перейдите на редакцию Pro
«Требуется обновление»	Версии больше года; установите обновление
Подтверждение прошло, окно удалённого рабочего стола не открылось	Проверьте имя и пароль в сессии; сообщите администратору, что порт удалённого рабочего стола недоступен

Подробности ошибок записываются в файл `client.log` в каталоге `%LOCALAPPDATA%\RdpFidoClient` (в Linux — `~/.config/rdpfido`); в Android журнал открывается кнопкой «Журнал».

6. ЗАВЕРШЕНИЕ РАБОТЫ

Чтобы завершить сеанс, выйдите из системы на удалённом компьютере или закройте окно сеанса; после этого шлюз закрывает порт. Поток FIDO Stream завершается сочетанием `Ctrl+Alt+Shift+Q` или закрытием окна.

Клиент закрывается обычным закрытием окна. Если есть активные сеансы RDP, клиент предупреждает об этом: окна сеансов продолжают работать, а выданное разрешение сетевого экрана истечёт само. Сохранённые сессии остаются в профиле пользователя и доступны при следующем запуске.

Уходя с рабочего места, заберите ключ безопасности. Если компьютером пользуются другие люди, включите защиту входа в клиент.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Версия документа	Дата	Версия программы	Содержание изменения
1.0	2026-10-06	1.25.1	Первая редакция документа