

iMobile

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«RDP-FIDO-GATE»

Версия 1.25.1

Руководство по установке и администрированию

IM.RDP-FIDO.RU.02

Листов 13

АННОТАЦИЯ

Настоящее руководство описывает установку, первоначальную настройку, проверку, обновление, резервное копирование, удаление и диагностику программы RDP-FIDO-GATE. Руководство предназначено для администратора, который устанавливает шлюз на защищаемые компьютеры, клиент — на рабочие места пользователей и, при необходимости, хаб на сервер организации.

Описаны версии: шлюз и клиент для Windows 1.25.0, пакеты для Linux 1.25.1, клиент для Android 0.9.1 (предварительная бета-версия), хаб 1.22.0.

СОДЕРЖАНИЕ

1. Общие сведения	4
2. Требования к среде	4
2.1. Программные требования	4
2.2. Сетевые порты	4
3. Установка	5
3.1. Шлюз для Windows	5
3.2. Клиент для Windows	6
3.3. Шлюз для Linux	6
3.4. Клиент для Linux	6
3.5. Клиент для Android	7
3.6. Хаб и реле	7
4. Первоначальная настройка	7
4.1. Регистрация первого ключа	7
4.2. Параметры шлюза	8
4.3. Вход по одноразовым кодам	8
4.4. Дополнительные порты (шлюз для Linux)	8
4.5. Ограничение по странам	9
4.6. Привязка шлюза к хабу	9
5. Проверка работоспособности	9
6. Обновление	10
7. Резервное копирование и восстановление	10
8. Удаление	11
9. Диагностика	11
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	13

1. ОБЩИЕ СВЕДЕНИЯ

Программа состоит из шлюза и клиента. Шлюз — служба на защищаемом компьютере (далее — хост): он закрывает порт RDP в сетевом экране хоста и открывает его адресу, с которого предъявлен зарегистрированный ключ FIDO2 или одноразовый код. Клиент — программа пользователя: хранит сессии, запрашивает подтверждение ключом и запускает подключение.

Необязательные части — хаб `rdpfido-cloud` и реле `rdpfido-relay` — устанавливаются на сервер организации с публичным адресом, если хосты недоступны из сети напрямую.

Установка шлюза не отнимает доступ к хосту: порт RDP продолжает работать как прежде и закрывается только в момент регистрации первого ключа. Аварийный возврат к обычному доступу — команда `unlock` (см. раздел «Диагностика»).

Команды шлюза выполняются с правами администратора. В Windows исполняемый файл находится в каталоге `%ProgramFiles%\RdpFidoGate`. Сообщения командной строки и журнал шлюза — на английском языке.

2. ТРЕБОВАНИЯ К СРЕДЕ

2.1. Программные требования

Часть	Операционная система	Дополнительно
Шлюз для Windows	Windows 10 версии 1903 и новее, Windows 11, Windows Server; x64	Права администратора, включённый брандмауэр Windows, удалённый рабочий стол
Клиент для Windows	Windows 10 версии 1903 и новее, Windows 11; x64	Права администратора не нужны; ключ FIDO2 или Windows Hello; для консоли SSH — <code>ssh</code> , <code>curl</code> и среда <code>WebView2</code>
Шлюз для Linux	Ubuntu 22.04 и 24.04, Astra Linux, РЕД ОС 7.3, ALT Linux p10; x86_64	<code>systemd</code> , <code>nftables</code> или <code>iptables</code> ; для RDP — <code>xrdp</code> ; для FIDO Stream — сеанс X11
Клиент для Linux	Те же дистрибутивы	GTK 3, SDL 2, FreeRDP 2 или 3; связь ключей рабочего стола для паролей
Клиент для Android	Android 9 и новее	NFC или USB OTG для ключей безопасности; приложение RDP для режима RDP
Хаб и реле	Linux x86_64 с <code>systemd</code> (Debian, Ubuntu)	Публичный адрес, запись DNS с подстановкой

Пакеты для Linux проверены поставщиком на Ubuntu 24.04, Astra Linux «Орёл» 2.12, РЕД ОС 7.3 и ALT Linux p10.

2.2. Сетевые порты

Порт	Где открыт	Назначение
TCP 7440	Хост	Канал подтверждения клиент — шлюз (HTTPS); должен быть доступен клиентам постоянно
TCP 3389	Хост	RDP; открывается шлюзом для одного адреса на окно доступа
UDP 7441 и следующие	Хост	FIDO Stream; открывается на время сеанса для адреса клиента, по одному порту на участника
TCP 443	Хаб	Обращения клиентов и исходящие соединения шлюзов
UDP 7443	Реле	Пересылка датаграмм FIDO Stream

Если хост находится за маршрутизатором с трансляцией адресов, на маршрутизаторе пробрасываются TCP 7440 и TCP 3389, а для FIDO Stream — UDP 7441. Проброс порта 3389 сам доступа не даёт: порт остаётся закрытым в сетевом экране хоста. Если проброс невозможен, используется хаб.

Клиенту для Windows нужен исходящий доступ по HTTPS к учётному серверу поставщика `accounts.new-imobile.com` — для активации и обновлений. Шлюзу, клиентам для Linux и Android доступ к серверам поставщика не нужен.

3. УСТАНОВКА

Установочные пакеты загружаются с сайта поставщика: страница продукта <https://new-imobile.com/rdp/>. Исполняемые файлы и пакеты для Windows не имеют цифровой подписи кода, поэтому Windows может показать предупреждение о неизвестном издателе.

3.1. Шлюз для Windows

- 1) Загрузите на хост `RdpFidoGate-Setup.msi` либо объединённый установщик `RdpFido-Setup.exe` и на его первой странице выберите «Хост».
- 2) Запустите установщик и подтвердите запрос контроля учётных записей. При новой установке установщик спрашивает способ входа: ключ FIDO (по умолчанию) или одноразовый код.
- 3) Нажмите «Установить». Установщик создаёт самоподписанный сертификат и привязывает его к порту шлюза, включает удалённый рабочий стол с проверкой подлинности на уровне сети (NLA), открывает порт шлюза в брандмауэре, регистрирует службу `RdpFidoGate` с автоматическим запуском и устанавливает драйвер виртуального геймпада `ViGEmBus`.
- 4) На последней странице показаны одноразовый код регистрации ключа (действует 15 минут), адреса хоста и порт шлюза. Сохраните код для регистрации первого ключа.

Установка без диалогов:

```
msiexec /i RdpFidoGate-Setup.msi /qn GATEPORT=7440 GATEGRANT=90 GATEUV=1 GATELANG=ru
RdpFido-Setup.exe host /qn GATEPORT=7440
```

Параметр	Значение
GATEPORT	Порт шлюза, по умолчанию 7440
GATEGRANT	Окно доступа в секундах, по умолчанию 90
GATEUV=1	Требовать проверку пользователя ключом (PIN или биометрия), а не только касание
GATEAUTH=totp	Вход по одноразовому коду вместо ключа FIDO
GATELANG	Язык диалогов: ru, en, de, fr, es, zh

В тихом режиме код регистрации не показывается; его выдаёт команда `RdpFidoGate.exe code`.

3.2. Клиент для Windows

- 1) На рабочем месте пользователя запустите `RdpFidoClient-Setup.msi` либо `RdpFido-Setup.exe` с выбором «Клиент». Клиент ставится в профиль пользователя (`%LOCALAPPDATA%\Programs\RdpFidoClient`), права администратора не требуются.
- 2) Без диалогов: `msiexec /i RdpFidoClient-Setup.msi /qn` или `RdpFido-Setup.exe client /qn`.
- 3) При первом запуске пользователь активирует клиент по адресу электронной почты (см. руководство пользователя). Без активации клиент подключается 14 дней.

3.3. Шлюз для Linux

```
sudo apt install ./rdpfido-gate_1.25.1_amd64.deb           # Ubuntu, Astra Linux
sudo dnf install ./rdpfido-gate-1.25.1-1.x86_64.rpm       # РЕД ОС
sudo apt-get install ./rdpfido-gate-1.25.1-alt1.x86_64.rpm # ALT Linux
sudo rdpfido-gate setup
```

Для прочих дистрибутивов: распакуйте `rdpfido-1.25.1-linux-x86_64.tar.gz` и выполните `sudo ./install.sh gate`.

Команда `setup` создаёт сертификат шлюза, проверяет `xrdr` (ключ `--install-xrdr` устанавливает его), ставит службы `rdpfido-gate` и `rdpfido-guard`, открывает порт шлюза в `ufw` или `firewalld` и печатает код регистрации и отпечаток сертификата. Служба `rdpfido-guard` ставит запрещающие правила при загрузке до запуска сети; `xrdr` запускается только после неё.

3.4. Клиент для Linux

```
sudo apt install ./rdpfido-client_1.25.1_amd64.deb       # Ubuntu, Astra Linux
sudo dnf install ./rdpfido-client-1.25.1-1.x86_64.rpm    # РЕД ОС
sudo apt-get install ./rdpfido-client-1.25.1-alt1.x86_64.rpm # ALT Linux
```

Пакет ставит правило `udev`, которое даёт пользователю за консолью доступ к ключу FIDO без прав `root`. Если в системе нет `libfido2`, используется копия из пакета.

3.5. Клиент для Android

Загрузите RdpFido-0.9.1-prebeta.apk, сверьте контрольную сумму с файлом SHA256SUMS и разрешите установку из выбранного источника. Отпечаток SHA-256 сертификата подписи APK: BF:FD:EA:D2:45:2E:D2:BD:1A:AD:02:E6:9A:0A:F9:5B:2C:A1:58:85:5A:AE:4F:CB:62:55:CA:0E:48:C2:60:BA. Приложение активации не требует.

3.6. Хаб и реле

Хаб нужен только хостам без публичного адреса. Он устанавливается на сервер организации.

- 1) Создайте запись DNS типа A с подстановкой для имён шлюзов (например, *.g.example.com) и запись для имени туннеля, указывающие на сервер. Сертификат TLS хабу не нужен.
- 2) Распакуйте rdpfido-cloud-1.22.0-linux-x86_64.tar.gz и из каталога архива выполните `sudo ./install.sh`. Сценарий создаёт пользователя rdpfido-cloud, каталоги /var/lib/rdpfido-cloud и /var/log/rdpfido-cloud, устанавливает программу, службу systemd и начальный файл /etc/rdpfido-cloud/cloud.json.
- 3) В cloud.json задайте domainSuffix (суффикс имён шлюзов), tunnelHost и, при наличии реле, список relays.
- 4) Запустите службу и откройте порт: `sudo systemctl enable --now rdpfido-cloud`, TCP 443 в сетевом экране.

Веб-кабинет хаба слушает адрес 127.0.0.1 (параметр adminPort, по умолчанию 8790) по HTTP без шифрования; наружу его выводят только через обратный прокси-сервер с TLS. Учётные записи кабинета создаёт команда `rdpfido-cloud user add ЛОГИН`. Значение "adminPort": 0 отключает кабинет; для работы хаба он не обязателен. Реле rdpfido-relay поставляется в том же архиве вместе со своим описанием; оно слушает UDP 7443 (параметр --port), его адрес указывается в списке relays хаба или в параметре streamRelays шлюза.

4. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

4.1. Регистрация первого ключа

- 1) Получите код регистрации: он показан установщиком, новый выдаёт `RdpFidoGate.exe code` (Linux: `sudo rdpfido-gate code`).
- 2) Пользователь в клиенте создаёт сессию для хоста и регистрирует ключ этим кодом (см. руководство пользователя). Код одноразовый и действует 15 минут.
- 3) После регистрации первого ключа шлюз закрывает порт RDP. Зарегистрируйте второй ключ на случай утраты первого: без действующего ключа доступ восстанавливается только с консоли хоста.

Передавайте пользователю вместе с кодом отпечаток сертификата шлюза (строка Thumbprint в выводе команд `status` и `code`): клиент для Linux сверяет его при

регистрации, клиент для Windows показывает начало закреплённого отпечатка в окне сессии после регистрации.

Управление ключами: `keys` — список, `remove-key N` — удаление (действует сразу), `key-role N lead` или `key-role N watch` — роль ключа в общем сеансе FIDO Stream.

Команда `code --keep` выдаёт многоразовый код, предназначенный для демонстрационных стендов. На рабочих хостах его не применяйте; отменяется командой `code --clear`.

4.2. Параметры шлюза

Параметры хранятся в разделе `config` файла `gate.json` (Windows: `%ProgramData%\RdpFidoGate`, Linux: `/var/lib/rdpfido-gate`). Перед правкой остановите службу, после правки запустите её.

Параметр	Назначение
<code>grantSeconds</code>	Окно доступа в секундах (по умолчанию 90, не более 600)
<code>requireUserVerification</code>	Требовать PIN или биометрию ключа
<code>streamEnabled, streamFiles</code>	Разрешить FIDO Stream и передачу файлов в нём
<code>streamShared, streamMaxParticipants</code>	Совместный доступ к потоку и число участников (по умолчанию 4, не более 8)
<code>streamRelays</code>	Список реле вида <code>{"address": "relay.example.com:7443", "name": "eu-1"}</code>
<code>allowPrivateAddresses</code>	Пропускать адреса локальной сети мимо фильтра стран (по умолчанию да)

FIDO Stream показывает действующий графический сеанс хоста и сам пароль операционной системы не запрашивает; если это недопустимо, задайте `"streamEnabled": false`.

4.3. Вход по одноразовым кодам

Способ входа выбирается при установке и меняется командой `RdpFidoGate.exe auth totp` (возврат — `auth fido`); служба при этом перезапускается. Учётная запись приложения-аутентификатора регистрируется из клиента по коду регистрации либо на самом хосте: `RdpFidoGate.exe totp add "Имя"` печатает QR-код в консоли, `totp test N` код проверяет код. В этом режиме открывается только RDP.

4.4. Дополнительные порты (шлюз для Linux)

```
sudo rdpfido-gate ports add 22      # закрыть SSH; несколько портов — через пробел
sudo rdpfido-gate ports            # что закрыто сейчас
sudo rdpfido-gate ports remove 22
```

Не более 16 портов; порт самого шлюза добавить нельзя. Установленные соединения не разрываются, поэтому команду можно выполнять из сеанса SSH; до его закрытия проверьте из другого терминала, что ключ открывает порт.

4.5. Ограничение по странам

- 1) Загрузите файлы статистики пяти региональных регистраторов (delegated-ripencc-latest, delegated-arin-extended-latest, delegated-apnic-latest, delegated-lacnic-latest, delegated-afrinic-latest) и выполните `RdpFidoGate.exe geoip-import` с именами всех пяти файлов.
- 2) Проверьте свой внешний адрес: `RdpFidoGate.exe geo test АДРЕС`.
- 3) Включите фильтр: `RdpFidoGate.exe geo allow RU KZ` и перезапустите службу. Состояние — `geo show`, отключение — `geo clear`.

Адрес, которого нет в таблице, отклоняется. Определение страны по адресу приблизительно; фильтр дополняет проверку ключа, но не заменяет её.

4.6. Привязка шлюза к хабу

- 1) На хабе: `rdpfido-cloud code --label ИМЯ` — код привязки, действует 15 минут.
- 2) На хосте: `RdpFidoGate.exe cloud link hub.example.com:443 КОД` (Linux: `sudo rdpfido-gate cloud link ...`). Служба перезапускается и держит исходящее соединение с хабом.
- 3) Команда `cloud link` сообщает публичное имя шлюза вида `<идентификатор>.<суффикс>`; пользователь вводит его в клиенте как адрес сервера и шлюза, порт 443. Состояние привязки показывает `cloud status`, отвязка — `cloud unlink`.

Через хаб работает клиент версии 1.22 и новее. Права доступа, настраиваемые в веб-кабинете хаба, шлюзы выпущенных версий не применяют: доступ определяют ключи, зарегистрированные на шлюзе.

5. ПРОВЕРКА РАБОТОСПОСОБНОСТИ

- 1) На хосте: `RdpFidoGate.exe status` (Linux: `sudo rdpfido-gate status`). Ожидаются строки `Service: running`, число ключей, `Protection is active`, `Firewall on in all profiles: yes`, `Inbound by default: blocked`.
- 2) С рабочего места: `Test-NetConnection ХОСТ -Port 7440` должен вернуть `TcpTestSucceeded : True`. В клиенте кнопка «Проверить» в окне сессии показывает имя хоста, число ключей и окно доступа.
- 3) С компьютера без ключа: `Test-NetConnection ХОСТ -Port 3389` должен завершиться неудачей — порт не отвечает.
- 4) Подключение из клиента с ключом должно открыть сеанс; в `gate.log` появляется запись `granted RDP access to АДРЕС`.
- 5) Самопроверка криптографических функций: `RdpFidoGate.exe selftest`; кодеры FIDO Stream — `RdpFidoGate.exe stream encoders`; связь с хабом — `cloud status`.

В Linux правила шлюза показывает `sudo nft list table inet rdpfido` или `sudo iptables -S RDPFIDO`.

6. ОБНОВЛЕНИЕ

Каждая версия работает один год с даты выпуска. За 30 дней до срока клиент и шлюз предупреждают; после срока клиент не подключается, а шлюз проверяет ключ, но не открывает доступ, пока не обновлён. Срок показывает строка `Support` команды `status`.

- Клиент для Windows при запуске запрашивает у учётного сервера поставщика подписанный манифест, загружает новую версию, сверяет контрольную сумму SHA-256 и предлагает установку. Настройка «Автоматически проверять и загружать обновления» и кнопка «Проверить обновления» находятся в окне настроек. Без доступа к серверу поставщика новая версия ставится пакетом MSI поверх прежней.
- Шлюз для Windows обновляется установкой нового пакета MSI поверх прежнего: служба останавливается, файл заменяется, ключи и настройки сохраняются.
- Шлюз для Windows может обновляться из клиента: при включённом в сессии флажке «Автоматически обновлять шлюз на этой машине» клиент после проверки ключа FIDO передаёт шлюзу новый исполняемый файл. Шлюз принимает только более новую версию, сверяет контрольную сумму, заменяет файл с резервной копией `.bak` и возвращает прежний, если служба не запустилась. Обновление может запустить любой пользователь, вошедший по зарегистрированному ключу FIDO2, поэтому регистрируйте на шлюзе только ключи доверенных лиц.
- Пакеты для Linux обновляются установкой новой версии пакета той же командой, что при установке; служба шлюза перезапускается, ключи сохраняются. Шлюз для Linux из клиента не обновляется.
- Хаб обновляется повторным запуском `install.sh` из нового архива и перезапуском службы; приложение для Android — установкой нового APK.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

Часть	Что копировать	Особенности восстановления
Шлюз для Windows	Каталог <code>%ProgramData%\RdpFidoGate</code>	Сертификат шлюза хранится в хранилище сертификатов компьютера и в копию не входит. После переустановки Windows создаётся новый сертификат; клиенты откажутся подключаться, пока ключ не зарегистрирован заново
Шлюз для Linux	Каталог <code>/var/lib/rdpfido-gate</code>	Содержит ключи, настройки, сертификат и его закрытый ключ; восстановление каталога сохраняет отпечаток

Часть	Что копировать	Особенности восстановления
Клиент для Windows	Каталог %LOCALAPPDATA%\RdpFidoClient	Пароли зашифрованы для учётной записи Windows: в другом профиле сессии откроются без паролей
Клиент для Linux	Каталог ~/.config/rdpfido	Пароли хранятся в связке ключей рабочего стола и копируются её средствами
Хаб	Каталог /var/lib/rdpfido-cloud, файл /etc/rdpfido-cloud/cloud.json	Содержит секреты привязки шлюзов

Копирование выполняется средствами операционной системы при остановленной службе шлюза. Каталоги шлюза и хаба содержат секреты (секреты одноразовых кодов, секрет привязки к хабу) и должны храниться с ограниченным доступом.

8. УДАЛЕНИЕ

- Шлюз для Windows: «Параметры» → «Приложения» → RDP FIDO Gate либо `msiexec /x RdpFidoGate-Setup.msi`. Служба, её правила брандмауэра и привязка сертификата удаляются, каталог данных сохраняется. Порт RDP при этом не открывается. Чтобы вернуть обычный доступ по RDP, до удаления выполните `RdpFidoGate.exe unlock` либо после удаления включите в брандмауэре группу правил «Удалённый рабочий стол».
- Клиент для Windows: «Параметры» → «Приложения» → RDP FIDO Client. Сохранённые сессии остаются в %LOCALAPPDATA%\RdpFidoClient; для полного удаления сотрите этот каталог.
- Linux: удаление пакета `rdpfido-gate` выполняет `rdpfido-gate uninstall` — службы и правила снимаются, изменения в `ufw` и `firewalld` отменяются. Каталог данных удаляется командой `apt purge`. Данные клиента остаются в `~/.config/rdpfido`.
- Хаб: сценария удаления нет. Остановите и отключите службу `rdpfido-cloud`, удалите программу, файл службы и каталоги, созданные при установке.

9. ДИАГНОСТИКА

Журналы: шлюз для Windows — %ProgramData%\RdpFidoGate\gate.log; шлюз для Linux — /var/lib/rdpfido-gate/gate.log и `journalctl -u rdpfido-gate`; клиент — `client.log` в каталоге данных; хаб — /var/log/rdpfido-cloud/rdpfido-cloud.log. Файл журнала ограничен 4 МБ, сохраняется один предыдущий файл. Команда `RdpFidoGate.exe diag` выводит сводку причин, по которым RDP может быть недоступен.

Признак	Причина	Действие
«Не удалось подключиться к шлюзу»	Порт 7440 недоступен	Проверить службу, проброс порта, сетевой экран на пути
«Код регистрации не принят»	Код использован или истёк	Выдать новый командой <code>code</code>

Признак	Причина	Действие
«Сертификат шлюза не совпадает с сохранённым»	Шлюз переустановлен либо подмена узла	Сверить отпечаток с выводом status; при совпадении зарегистрировать ключ заново
«Счётчик ключа не увеличился»	Возможна копия ключа	Удалить ключ (remove-key) и зарегистрировать заново
«Слишком много попыток»	8 неудач за 5 минут с адреса	Подождать 5 минут
«Доступ из вашей страны запрещён»	Фильтр стран	geo test АДРЕС, затем geo allow или geo clear
Подтверждение прошло, RDP не открывается	Порт 3389 не проброшен на маршрутизаторе либо неверны учётные данные сессии	Проверить проброс и учётную запись; status показывает действующие разрешения
В status предупреждение о брандмауэре	Брандмауэр выключен или входящие разрешены по умолчанию	RdpFidoGate.exe harden
Шлюз сообщает об истёкшем сроке версии	Версии больше года	Установить обновление

Если ключи утрачены или шлюз неисправен, доступ возвращается с консоли хоста командой RdpFidoGate.exe unlock (Linux: sudo rdpfido-gate unlock): защита снимается, зарегистрированные ключи сохраняются. Команда arm возвращает защиту. Шлюз закрывает только порт RDP (в Linux — и добавленные порты), поэтому другие средства удалённого управления хостом продолжают работать.

Обращения в поддержку: support@new-imobile.com, форма на сайте <https://new-imobile.com/contact>.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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