

RDP-FIDO-GATE

Delivery Specification and Third-Party Components

Document ID	IM.RDP-FIDO.INT.05
Document version	1.0
Date of issue	2026-10-06
Applies to	RDP-FIDO-GATE 1.25.1
Language	English
Publisher	iMobile

Contents

- 1. Product identification 3
- 2. Delivery set 3
 - 2.1. Contents 3
 - 2.2. Method of delivery 4
 - 2.3. Documentation 4
- 3. Operating environment 4
 - 3.1. Supported platforms 4
 - 3.2. Hardware and software requirements 5
- 4. Licensing 5
 - 4.1. Editions and terms of use 5
 - 4.2. Activation 5
 - 4.3. Updates 6
- 5. Interface languages 6
- 6. Third-party components 6
- 7. Known limitations 7

About this document

This document defines what is delivered with RDP-FIDO-GATE version 1.25.1, the environment the product requires, the licensing terms in functional outline and the third-party software components the product contains.

Prices, delivery dates and the parties' details are not part of this document; they are set in the contract.

1. Product identification

Item	Value
Product	RDP-FIDO-GATE
Version	1.25.1
Release date	2026-10-06
Type of software	Remote access control software: a multi-factor authentication gate (FIDO2 key or TOTP one-time code) in front of RDP, SSH and other TCP ports, with client applications
Deployment	Client and server components, all installed on the customer's equipment
Publisher	iMobile

Keeps the Remote Desktop (RDP) port, and on Linux also SSH and other chosen TCP ports, closed in the computer's own firewall and opens them for a short time only to the address that presented an enrolled FIDO2 key or a TOTP one-time code. It consists of a gate service, clients for Windows, Linux and Android, its own screen-streaming protocol (FIDO Stream) and an optional relay server (hub) that the customer hosts.

Every part is installed on the customer's equipment. The gate is a service on each protected computer (Windows or Linux). The client is an application on users' workstations (Windows, Linux) and an app on Android devices. The optional hub `rdpfido-cloud` and relay `rdpfido-relay` go on a customer server with a public address when the gates cannot be reached directly. The vendor's servers run only the account server (activation of the Windows client, edition terms) and the update distribution; session data never passes through them. The hub operated by the vendor is a private service and is not part of the delivery.

2. Delivery set

2.1. Contents

- `RdpFido-Setup.exe` — the combined Windows installer: asks for the computer's role (host or client) and runs the embedded MSI package
- `RdpFidoGate-Setup.msi` — the gate for Windows: `RdpFidoGate.exe` (service, FIDO Stream agent, ViGEmBus virtual gamepad driver package) and `THIRD-PARTY-LICENSES.txt`
- `RdpFidoClient-Setup.msi` — the client for Windows: `RdpFidoClient.exe` (session manager, FIDO Stream window, SSH console) and `THIRD-PARTY-LICENSES.txt`
- Linux gate packages `rdpfido-gate` (deb, rpm, rpm for ALT): `rdpfido-gate`, the systemd services `rdpfido-gate` and `rdpfido-guard`, the stream agent `rdpfido-stream-host`, a readme and licence notices
- Linux client packages `rdpfido-client` (deb, rpm, rpm for ALT): `rdpfido`, `rdpfido-gui`, `rdpfido-viewer`, `rdpfido-console`, FFmpeg decoding libraries, a copy of `libfido2`, a udev rule, a readme and licence notices

- The archive `rdpfido-1.25.1-linux-x86_64.tar.gz` (both halves and `install.sh`) and the checksum file `SHA256SUMS`
- `RdpFido-0.9.1-prebeta.apk` — the Android client, with a `SHA256SUMS` file
- The archive `rdpfido-cloud-1.22.0-linux-x86_64.tar.gz` — the hub `rdpfido-cloud`, the relay `rdpfido-relay`, `install.sh`, `systemd` unit files, the web cabinet files and a `readme`
- Documentation: this set, plus the guides and the change log on the vendor's site
- There is no licence file or licence key: the Pro edition is assigned to an account (e-mail address) on the vendor's account server

2.2. Method of delivery

Download from the vendor's site: the product page <https://new-imobile.com/rdp/> ; Windows installers at the permanent links <https://accounts.new-imobile.com/updates/RdpFido-Setup.exe>, [RdpFidoGate-Setup.msi](https://accounts.new-imobile.com/updates/RdpFidoGate-Setup.msi), [RdpFidoClient-Setup.msi](https://accounts.new-imobile.com/updates/RdpFidoClient-Setup.msi); the Linux packages and the hub archive are published next to the guide <https://new-imobile.com/download/rdp-fido-gate/linux/README.en.md>; the Android app is at <https://new-imobile.com/download/rdp-fido-gate/android/RdpFido-0.9.1-prebeta.apk>. Updates of the Windows client are delivered from the vendor's account server.

2.3. Documentation

The documentation set consists of:

- Product Description and Functional Specification
- Installation and Administration Guide
- User Guide
- Software Lifecycle, Maintenance and Support
- Delivery Specification and Third-Party Components (this document)
- Security and Data Protection Statement
- a country annex for the customer's jurisdiction

3. Operating environment

3.1. Supported platforms

- Gate for Windows, version 1.25.0 (5 October 2026): Windows 10 version 1903 or later, Windows 11, x64; Windows Server with Remote Desktop enabled (the vendor runs it on Windows Server 2019)
- Client for Windows, version 1.25.0 (5 October 2026): Windows 10 version 1903 or later, Windows 11, x64
- Gate and client for Linux, version 1.25.1 (6 October 2026), x86_64: Ubuntu 22.04 and 24.04, Astra Linux, RED OS 7.3, ALT Linux p10; other `systemd` distributions from the `tar.gz` archive. Verified by the vendor on Ubuntu 24.04, Astra Linux Orel 2.12, RED OS 7.3 and ALT Linux p10
- Client for Android, version 0.9.1 (pre-beta, 6 October 2026): Android 9 or later
- Hub `rdpfido-cloud` and relay `rdpfido-relay`, version 1.22.0 (28 September 2026): Linux x86_64 with `systemd` (Debian, Ubuntu)

3.2. Hardware and software requirements

- Gate for Windows: administrator rights for installation; Windows Firewall switched on; Remote Desktop Services; gate port TCP 7440 reachable by clients; for FIDO Stream, UDP 7441 and the following ports, and for hardware encoding an NVIDIA, Intel or AMD GPU with a hardware encoder
- Client for Windows: no administrator rights; a FIDO2 key (USB or NFC) or Windows Hello; the built-in `mstsc` client; for the SSH console, the system `ssh` and `curl` and the WebView2 runtime; internet access to the vendor's account server for activation and updates
- Gate for Linux: root rights, systemd, nftables or iptables; an xrdp server for RDP; an X11 desktop session for FIDO Stream
- Client for Linux: GTK 3, SDL 2, FreeRDP 2 or 3; a FIDO2 key (USB or NFC); a desktop keyring (Secret Service) to save passwords; a Chromium-family browser for the SSH console window
- Client for Android: Android 9 or later; a fingerprint or screen lock for the phone-as-key mode; NFC or USB OTG for security keys; an installed third-party RDP client app for RDP
- Hub and relay: a Linux server with a public address, TCP 443 open (UDP 7443 for the relay), a wildcard DNS record for gate names
- The vendor sets no processor, memory or disk requirements beyond those of the operating system

4. Licensing

4.1. Editions and terms of use

Two editions, Free and Pro; the difference applies in the Windows client. Free: at most 10 saved sessions and an advertising tile in the client window. Pro: unlimited sessions and no advertising. Key verification and the gate, FIDO Stream, the SSH console, the entry lock and all other functions are the same in both editions. The gate, the Linux client and the Android client do not check the edition and have no limits. The edition is bound to the user's account (e-mail address); the client receives the edition terms from the account server in signed form. Every released version works for one year from its release date and then requires an update. The licensing unit and the licence term are set by the contract.

4.2. Activation

Only the Windows client needs activation. Without it the client connects for 14 days from first run; after that connecting is blocked until activation. The user enters an e-mail address, receives a code and types it into the client. The client sends to the vendor's account server (<https://accounts.new-imobile.com>, HTTPS): when requesting the code — the e-mail address, the product identifier `rdp-fido-client` and the interface language; on activation — the e-mail address, the code and the product identifier; then, when reading the edition terms — the account token, the product identifier, the client version, the interface language and an installation identifier (the first 16 bytes of the SHA-256 of the Windows MachineGuid with a fixed prefix). Addresses and names of protected computers, credentials and session details are not sent. The gate and the Linux and Android clients need no activation and do not contact the vendor's servers.

4.3. Updates

The Windows client asks the account server for an update manifest at start (when the setting is on) and on the user's command, sending the product identifier and its own version. The manifest is signed with the server's key (ECDSA P-256, the public key is built into the client); the client downloads the file, checks its SHA-256 against the manifest and replaces itself with the user's consent. The Windows gate is updated by installing a new MSI package or from the client: after a successful FIDO key check the client sends the gate a new executable, the gate checks its SHA-256, replaces itself keeping a backup and rolls back if the service does not start. The Linux packages, the Android app and the hub are updated by installing the new version over the old one. One year after a version's release date an update is mandatory.

5. Interface languages

Windows client and installers: Russian, English, German, French, Spanish, Chinese. Linux client: Russian, English. Android client: English, Russian. Gate command line and log: English. Hub web cabinet: Russian, English.

6. Third-party components

Component	Version	Licence	Purpose
ViGEmBus	1.21.44 2.0	BSD-3-Clause	Virtual gamepad driver for FIDO Stream; the driver package is embedded in the Windows gate
ViGEmClient (заголовочные файлы / headers)	—	MIT	The user-mode contract of the ViGEmBus driver; compiled into the Windows gate
NVIDIA Video Codec SDK headers (nv-codec-headers)	—	MIT	Headers for the NVENC encoder and NVDEC decoder; the driver's own libraries are loaded at run time
Opus (libopus)	1.5.2	BSD-3-Clause	Audio codec of the FIDO Stream channel; compiled into the executables
QR Code generator library (Project Nayuki)	—	MIT	Shows the QR code when an authenticator app is enrolled (one-time-code mode)
xterm.js	5.3.0	MIT	Terminal emulator of the SSH console page
Microsoft Edge WebView2 SDK	—	BSD-3-Clause	Loader and headers for the SSH console window in the Windows client; the WebView2 runtime itself is not shipped
OpenSSL	3	Apache-2.0	TLS and cryptography in the Linux programs and the hub; linked statically
libfido2	1.15	BSD-2-Clause	FIDO2 key access in the Linux client; the bundled copy is used when the system has none
OpenH264	2.4.1	BSD-2-Clause	Software H.264 encoder of the Linux FIDO Stream agent; built from source
FFmpeg (libavcodec, libavutil)	6.1.2	LGPL-2.1-or-later	H.264 and HEVC decoding in the Linux stream window; separate shared libraries built with decoders only
AndroidX (Core, Activity, Lifecycle, Biometric), Jetpack Compose	—	Apache-2.0	User interface and biometric prompt libraries in the Android client
Kotlin Standard Library, kotlinx.coroutines	—	Apache-2.0	Kotlin language runtime in the Android client

Each third-party component is used under its own licence, named in the table. The table is a human-readable component list; a machine-readable bill of materials (SPDX or CycloneDX) is not part of this delivery.

7. Known limitations

- The product restricts network access to a port and does not replace operating system authentication: once the port is open, sign-in is checked by the account password (with NLA on Windows). When several hosts share one external address (NAT), the access window is open to every host behind that address
- Every version works for one year from its release date; after that the client does not connect and the gate opens no access until an update is installed
- The Windows client requires activation through the vendor's account server within 14 days; there is no offline activation
- The Windows executables and packages carry no code-signing signature
- An update of the Windows gate can be started from the client by any user who signed in with an enrolled FIDO2 key; there is no separate setting to switch this off (it is off only in one-time-code mode)
- The Windows gate protects the RDP port only; SSH and other ports are protected only by the Linux gate. The Linux gate is not updated from the client
- In one-time-code mode only RDP opens; FIDO Stream and gate updates from the client are unavailable; the Android client does not support this mode
- Only RDP and calls to the gate pass through the hub; extra ports and the SSH console need the gate's direct address. The access rules kept by the hub cabinet are not applied by the gates of the released versions
- FIDO Stream on a Linux host: X11 sessions only (no Wayland), software H.264 encoding without HEVC, AV1 or HDR; the Linux stream window decodes in software
- The gate certificate is self-signed; trust is established by its thumbprint on first contact unless the thumbprint is checked manually
- The Android client is a pre-beta: verified on a single phone, the entry lock of version 0.9.1 only in an emulator; RDP opens in a third-party app; shared sessions and file transfer are not implemented
- Not verified with a physical security key: the Linux client (tested with a virtual key, PIN entry not tested) and unlocking the client with a FIDO2 key (tested with a software key)
- There is no central management of keys across gates; logs are local files of limited size
- The product holds no security certifications

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	1.25.1	First issue