

RDP-FIDO-GATE

Installation and Administration Guide

Document ID	IM.RDP-FIDO.INT.02
Document version	1.0
Date of issue	2026-10-06
Applies to	RDP-FIDO-GATE 1.25.1
Language	English
Publisher	iMobile

Contents

- 1. General information 3
- 2. Environment requirements 3
 - 2.1. Software 3
 - 2.2. Network ports 3
- 3. Installation 4
 - 3.1. Gate for Windows 4
 - 3.2. Client for Windows 5
 - 3.3. Gate for Linux 5
 - 3.4. Client for Linux 5
 - 3.5. Client for Android 5
 - 3.6. Hub and relay 5
- 4. Initial configuration 6
 - 4.1. Enrolling the first key 6
 - 4.2. Gate settings 6
 - 4.3. Sign-in with one-time codes 6
 - 4.4. Extra ports (Linux gate) 7
 - 4.5. Country restriction 7
 - 4.6. Linking a gate to the hub 7
- 5. Verification 7
- 6. Updating 8
- 7. Backup and recovery 8
- 8. Removal 8
- 9. Troubleshooting 9

About this document

This guide covers installation, initial configuration, verification, updating, backup, removal and troubleshooting of RDP-FIDO-GATE. It is written for the administrator who installs the gate on the protected computers, the client on users' workstations and, where needed, the hub on the organisation's server.

It describes the gate and client for Windows 1.25.0, the Linux packages 1.25.1, the Android client 0.9.1 (pre-beta) and the hub 1.22.0.

1. General information

The product has two halves. The gate is a service on the protected computer (the host): it closes the RDP port in the host's firewall and opens it to the address that presented an enrolled FIDO2 key or a one-time code. The client is the user's application: it keeps sessions, asks for the key confirmation and starts the connection.

Two optional parts, the hub `rdpfido-cloud` and the relay `rdpfido-relay`, are installed on a server of the organisation with a public address when the hosts cannot be reached from the network directly.

Installing the gate does not take access away: the RDP port keeps working as before and closes only when the first key is enrolled. The emergency way back to ordinary access is the `unlock` command (see Troubleshooting).

Gate commands are run with administrator rights. On Windows the executable is in `%ProgramFiles%\RdpFidoGate`. The command line and the gate log are in English.

2. Environment requirements

2.1. Software

Component	Operating system	Also needed
Gate for Windows	Windows 10 version 1903 or later, Windows 11, Windows Server; x64	Administrator rights, Windows Firewall switched on, Remote Desktop
Client for Windows	Windows 10 version 1903 or later, Windows 11; x64	No administrator rights; a FIDO2 key or Windows Hello; for the SSH console <code>ssh</code> , <code>curl</code> and the WebView2 runtime
Gate for Linux	Ubuntu 22.04 and 24.04, Astra Linux, RED OS 7.3, ALT Linux p10; x86_64	<code>systemd</code> , <code>nftables</code> or <code>iptables</code> ; <code>xrdp</code> for RDP; an X11 session for FIDO Stream
Client for Linux	The same distributions	GTK 3, SDL 2, FreeRDP 2 or 3; a desktop keyring for passwords
Client for Android	Android 9 or later	NFC or USB OTG for security keys; an RDP app for RDP mode
Hub and relay	Linux x86_64 with <code>systemd</code> (Debian, Ubuntu)	A public address, a wildcard DNS record

The vendor verified the Linux packages on Ubuntu 24.04, Astra Linux Orel 2.12, RED OS 7.3 and ALT Linux p10.

2.2. Network ports

Port	Open on	Purpose
TCP 7440	Host	Client-to-gate confirmation channel (HTTPS); must be reachable by clients at all times

Port	Open on	Purpose
TCP 3389	Host	RDP; opened by the gate for one address for the access window
UDP 7441 and following	Host	FIDO Stream; opened for the client's address during a session, one port per participant
TCP 443	Hub	Client connections and the gates' outgoing links
UDP 7443	Relay	Forwarding of FIDO Stream datagrams

If the host is behind a router with address translation, forward TCP 7440 and TCP 3389 on the router, plus UDP 7441 for FIDO Stream. Forwarding port 3389 does not by itself give access: the port stays closed in the host's firewall. Where forwarding is not possible, use the hub.

The Windows client needs outgoing HTTPS access to the vendor's account server

`accounts.new-imobile.com` for activation and updates. The gate and the Linux and Android clients need no access to the vendor's servers.

3. Installation

Installation packages are downloaded from the vendor's site; the product page is <https://new-imobile.com/rdp/>. The Windows executables and packages carry no code-signing signature, so Windows may warn about an unknown publisher.

3.1. Gate for Windows

1. Download `RdpFidoGate-Setup.msi` to the host, or the combined installer `RdpFido-Setup.exe` and choose "Host" on its first page.
2. Run the installer and confirm the User Account Control prompt. On a new installation the installer asks how users will sign in: with a FIDO key (the default) or with a one-time code.
3. Click "Install". The installer creates a self-signed certificate and binds it to the gate port, enables Remote Desktop with Network Level Authentication (NLA), opens the gate port in the firewall, registers the `RdpFidoGate` service for automatic start and installs the ViGEmBus virtual gamepad driver.
4. The last page shows the one-time key enrollment code (valid for 15 minutes), the host's addresses and the gate port. Keep the code for enrolling the first key.

Unattended installation:

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

Property	Meaning
GATEPORT	Gate port, 7440 by default
GATEGRANT	Access window in seconds, 90 by default
GATEUV=1	Require user verification by the key (PIN or biometrics), not just a touch
GATEAUTH=totp	Sign-in with a one-time code instead of a FIDO key
GATELANG	Dialog language: <code>ru</code> , <code>en</code> , <code>de</code> , <code>fr</code> , <code>es</code> , <code>zh</code>

In silent mode the enrollment code is not shown; obtain it with `RdpFidoGate.exe code`.

3.2. Client for Windows

1. On the user's workstation run `RdpFidoClient-Setup.msi`, or `RdpFido-Setup.exe` and choose "Client". The client is installed into the user's profile (`%LOCALAPPDATA%\Programs\RdpFidoClient`); no administrator rights are needed.
2. Unattended: `msiexec /i RdpFidoClient-Setup.msi /qn` or `RdpFido-Setup.exe client /qn`.
3. On first run the user activates the client with an e-mail address (see the User Guide). Without activation the client connects for 14 days.

3.3. Gate for 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      # RED OS
sudo apt-get install ./rdpfido-gate-1.25.1-alt1.x86_64.rpm # ALT Linux
sudo rdpfido-gate setup
```

On other distributions unpack `rdpfido-1.25.1-linux-x86_64.tar.gz` and run `sudo ./install.sh gate`.

The `setup` command creates the gate certificate, checks `xrdp` (the `--install-xrdp` switch installs it), installs the `rdpfido-gate` and `rdpfido-guard` services, opens the gate port in `ufw` or `firewalld`, and prints the enrollment code and the certificate thumbprint. The `rdpfido-guard` service applies the blocking rules at boot before the network starts; `xrdp` starts only after it.

3.4. Client for 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  # RED OS
sudo apt-get install ./rdpfido-client-1.25.1-alt1.x86_64.rpm # ALT Linux
```

The package installs a `udev` rule that lets the user at the console reach a FIDO key without root rights. If the system has no `libfido2`, the copy from the package is used.

3.5. Client for Android

Download `RdpFido-0.9.1-prebeta.apk`, compare its checksum with the `SHA256SUMS` file and allow installation from the chosen source. SHA-256 fingerprint of the APK signing certificate: `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`. The app needs no activation.

3.6. Hub and relay

The hub is needed only for hosts without a public address. It is installed on a server of the organisation.

1. Create a wildcard DNS A record for the gate names (for example `*.g.example.com`) and a record for the tunnel name, both pointing to the server. The hub needs no TLS certificate.
2. Unpack `rdpfido-cloud-1.22.0-linux-x86_64.tar.gz` and run `sudo ./install.sh` from the archive directory. The script creates the `rdpfido-cloud` user, the directories `/var/lib/rdpfido-cloud` and `/var/log/rdpfido-cloud`, and installs the program, the `systemd` service and a starting `/etc/rdpfido-cloud/cloud.json`.
3. In `cloud.json` set `domainSuffix` (the suffix of gate names), `tunnelHost` and, if a relay is used, the `relays` list.
4. Start the service and open the port: `sudo systemctl enable --now rdpfido-cloud`, and TCP 443 in the firewall.

The hub's web cabinet listens on 127.0.0.1 (the `adminPort` setting, 8790 by default) over unencrypted HTTP; expose it only through a reverse proxy with TLS. Cabinet accounts are created with `rdpfido-cloud user add LOGIN`. Setting `"adminPort": 0` switches the cabinet off; the hub does not need it to work. The relay `rdpfido-relay` comes in the same archive with its own readme; it listens on UDP 7443 (the `--port` option), and its address goes into the hub's `relays` list or the gate's `streamRelays` setting.

4. Initial configuration

4.1. Enrolling the first key

1. Get an enrollment code: the installer showed one, and `RdpFidoGate.exe code` (Linux: `sudo rdpfido-gate code`) issues a new one.
2. In the client the user creates a session for the host and enrolls a key with that code (see the User Guide). The code is single-use and valid for 15 minutes.
3. Once the first key is enrolled, the gate closes the RDP port. Enroll a second key in case the first is lost: without a working key, access can be restored only from the host's console.

Give the user the gate certificate thumbprint together with the code (the `Thumbprint` line printed by `status` and `code`): the Linux client checks it at enrollment, and the Windows client shows the beginning of the pinned thumbprint in the session window after enrollment.

Key management: `keys` lists them, `remove-key N` removes one (with immediate effect), `key-role N lead` or `key-role N watch` sets a key's role in a shared FIDO Stream session.

The `code --keep` command issues a reusable code meant for demonstration machines. Do not use it on production hosts; `code --clear` cancels it.

4.2. Gate settings

Settings are kept in the `config` section of `gate.json` (Windows: `%ProgramData%\RdpFidoGate`, Linux: `/var/lib/rdpfido-gate`). Stop the service before editing the file and start it afterwards.

Setting	Purpose
<code>grantSeconds</code>	Access window in seconds (90 by default, 600 at most)
<code>requireUserVerification</code>	Require the key's PIN or biometrics
<code>streamEnabled, streamFiles</code>	Allow FIDO Stream and file transfer within it
<code>streamShared, streamMaxParticipants</code>	Shared stream sessions and the number of participants (4 by default, 8 at most)
<code>streamRelays</code>	A list of relays such as <code>{"address": "relay.example.com:7443", "name": "eu-1"}</code>
<code>allowPrivateAddresses</code>	Let local network addresses bypass the country filter (on by default)

FIDO Stream shows the host's current desktop session and does not itself ask for the operating system password; if that is unacceptable, set `"streamEnabled": false`.

4.3. Sign-in with one-time codes

The sign-in method is chosen at installation and changed with `RdpFidoGate.exe auth totp` (back with `auth fido`); the service restarts. An authenticator-app account is enrolled from the client with an enrollment code, or on the host itself: `RdpFidoGate.exe totp add "Name"` prints a QR code in the console and `totp test N CODE` checks a code. In this mode only RDP opens.

4.4. Extra ports (Linux gate)

```
sudo rdpfido-gate ports add 22      # close SSH; several ports separated by spaces
sudo rdpfido-gate ports           # what is closed now
sudo rdpfido-gate ports remove 22
```

At most 16 ports; the gate's own port cannot be added. Established connections are not cut, so the command may be run from an SSH session; before closing that session, check from another terminal that the key opens the port.

4.5. Country restriction

1. Download the statistics files of the five regional internet registries (delegated-ripenncc-latest, delegated-arin-extended-latest, delegated-apnic-latest, delegated-lacnic-latest, delegated-afrinic-latest) and run `RdpFidoGate.exe geoip-import` with the names of all five files.
2. Check your own external address: `RdpFidoGate.exe geo test ADDRESS`.
3. Switch the filter on with `RdpFidoGate.exe geo allow` followed by the two-letter country codes, and restart the service. `geo show` reports the state, `geo clear` switches the filter off.

An address that is not in the table is rejected. Country lookup by address is approximate; the filter complements the key check and does not replace it.

4.6. Linking a gate to the hub

1. On the hub: `rdpfido-cloud code --label NAME` gives a link code valid for 15 minutes.
2. On the host: `RdpFidoGate.exe cloud link hub.example.com:443 CODE` (Linux: `sudo rdpfido-gate cloud link ...`). The service restarts and keeps an outgoing connection to the hub.
3. The `cloud link` command reports the gate's public name, of the form `<id>.<suffix>`; the user enters it in the client as the server and gate address, port 443. `cloud status` shows the state of the link and `cloud unlink` removes it.

Working through the hub needs client version 1.22 or later. The access rights configured in the hub's web cabinet are not applied by the gates of the released versions: access is determined by the keys enrolled on the gate.

5. Verification

1. On the host run `RdpFidoGate.exe status` (Linux: `sudo rdpfido-gate status`). Expect Service: running, the number of keys, Protection is active, Firewall on in all profiles: yes and Inbound by default: blocked.
2. From a workstation, `Test-NetConnection HOST -Port 7440` must return `TcpTestSucceeded : True`. In the client the "Test" button of the session window reports the host name, the number of keys and the access window.
3. From a computer without a key, `Test-NetConnection HOST -Port 3389` must fail: the port does not answer.
4. Connecting from the client with a key must open a session; `gate.log` then contains a line `granted RDP access to ADDRESS`.
5. Self-test of the cryptographic functions: `RdpFidoGate.exe selftest`; FIDO Stream encoders: `RdpFidoGate.exe stream encoders`; the hub link: `cloud status`.

On Linux the gate's rules are shown by `sudo nft list table inet rdpfido` or `sudo iptables -S RDPFIDO`.

6. Updating

Every version works for one year from its release date. Thirty days before the end the client and the gate give warnings; after it the client does not connect, and the gate still checks the key but opens no access until it is updated. The `Support` line of the `status` command shows the date.

- The Windows client asks the vendor's account server for a signed manifest at start, downloads the new version, checks its SHA-256 checksum and offers to install it. The setting "Check for and download updates automatically" and the "Check for updates" button are in the settings window. Without access to the vendor's server, install the new MSI package over the old one.
- The Windows gate is updated by installing a new MSI package over the old one: the service is stopped, the file replaced, keys and settings kept.
- The Windows gate can also be updated from the client: when "Automatically update the gate on this machine" is ticked in a session, the client sends the gate a new executable after the FIDO key check. The gate accepts only a newer version, checks the checksum, replaces the file keeping a `.bak` copy, and puts the old file back if the service does not start. An update can be started by any user who signed in with an enrolled FIDO2 key, so enroll keys on a gate only for trusted people.
- The Linux packages are updated by installing the new package with the same command as for installation; the gate service restarts and the keys are kept. The Linux gate is not updated from the client.
- The hub is updated by running `install.sh` from the new archive and restarting the service; the Android app by installing the new APK.

7. Backup and recovery

Component	What to copy	Notes on recovery
Gate for Windows	The directory <code>%ProgramData%\RdpFidoGate</code>	The gate certificate is kept in the computer's certificate store and is not part of the copy. After Windows is reinstalled a new certificate is created; clients refuse to connect until a key is enrolled again
Gate for Linux	The directory <code>/var/lib/rdpfido-gate</code>	Holds the keys, the settings, the certificate and its private key; restoring the directory keeps the thumbprint
Client for Windows	The directory <code>%LOCALAPPDATA%\RdpFidoClient</code>	Passwords are encrypted for the Windows user account: in another profile the sessions open without passwords
Client for Linux	The directory <code>~/.config/rdpfido</code>	Passwords live in the desktop keyring and are copied with its own tools
Hub	The directory <code>/var/lib/rdpfido-cloud</code> and the file <code>/etc/rdpfido-cloud/cloud.json</code>	Holds the link secrets of the gates

Copy with operating system tools while the gate service is stopped. The gate and hub directories contain secrets (one-time-code secrets, the hub link secret) and must be stored with restricted access.

8. Removal

- Gate for Windows: Settings, Apps, RDP FIDO Gate, or `msiexec /x RdpFidoGate-Setup.msi`. The service, its firewall rules and the certificate binding are removed; the data directory stays. The RDP port is not opened by this. To return to ordinary RDP access, run `RdpFidoGate.exe unlock` before uninstalling, or enable the "Remote Desktop" rule group in the firewall afterwards.

- Client for Windows: Settings, Apps, RDP FIDO Client. Saved sessions stay in `%LOCALAPPDATA%\RdpFidoClient`; delete that directory to erase them.
- Linux: removing the `rdpfido-gate` package runs `rdpfido-gate uninstall`, which removes the services and rules and reverts the changes made in `ufw` and `firewalld`. `apt purge` deletes the data directory. Client data stays in `~/.config/rdpfido`.
- Hub: there is no uninstall script. Stop and disable the `rdpfido-cloud` service, then delete the program, the service file and the directories created at installation.

9. Troubleshooting

Logs: Windows gate — `%ProgramData%\RdpFidoGate\gate.log`; Linux gate — `/var/lib/rdpfido-gate/gate.log` and `journalctl -u rdpfido-gate`; client — `client.log` in its data directory; hub — `/var/log/rdpfido-cloud/rdpfido-cloud.log`. A log file is limited to 4 MB and one previous file is kept. `RdpFidoGate.exe diag` prints a summary of everything that decides whether RDP is reachable.

Symptom	Cause	Action
"Could not reach the gate"	Port 7440 is not reachable	Check the service, the port forwarding and firewalls on the path
"The enrollment code was not accepted"	The code was used or has expired	Issue a new one with <code>code</code>
"The gate's certificate does not match the pinned one"	The gate was reinstalled, or an impostor host	Compare the thumbprint with the <code>status</code> output; if it matches, enroll the key again
"The key's counter did not increase"	Possibly a cloned key	Remove the key (<code>remove-key</code>) and enroll it again
"Too many attempts"	8 failures within 5 minutes from the address	Wait 5 minutes
"Access from your country is blocked"	Country filter	<code>geo test ADDRESS</code> , then <code>geo allow</code> or <code>geo clear</code>
Confirmation passes but RDP does not open	Port 3389 is not forwarded on the router, or the session's credentials are wrong	Check the forwarding and the account; <code>status</code> lists the active grants
<code>status</code> warns about the firewall	The firewall is off or inbound traffic is allowed by default	<code>RdpFidoGate.exe harden</code>
The gate reports that its support year is over	The version is more than a year old	Install the update

If the keys are lost or the gate malfunctions, access is restored from the host's console with `RdpFidoGate.exe unlock` (Linux: `sudo rdpfido-gate unlock`): protection is lifted and the enrolled keys are kept. The `arm` command restores protection. The gate closes only the RDP port (on Linux also the added ports), so other means of remote management of the host keep working.

Support: support@new-imobile.com, or the form at <https://new-imobile.com/contact>.

Document history

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