

RDP-FIDO-GATE

User Guide

Document ID	IM.RDP-FIDO.INT.03
Document version	1.0
Date of issue	2026-10-06
Applies to	RDP-FIDO-GATE 1.25.1
Language	English
Publisher	iMobile

Contents

- 1. Purpose 3
- 2. Conditions of use 3
- 3. Getting started 3
 - 3.1. Activating the Windows client 3
 - 3.2. Adding a session 4
 - 3.3. Enrolling a key 4
- 4. Main operations 5
 - 4.1. Connecting over RDP 5
 - 4.2. Connecting in FIDO Stream mode 5
 - 4.3. SSH console 6
 - 4.4. Managing sessions 6
 - 4.5. Locking the client 6
 - 4.6. Updating the client 7
 - 4.7. Linux client 7
 - 4.8. Android client 8
- 5. Messages and common difficulties 8
- 6. Finishing work 8

About this document

This guide explains how a user works with the RDP-FIDO-GATE client applications: getting ready, enrolling a key, connecting to a remote computer, using FIDO Stream and the SSH console, and locking the client itself. Most of it concerns the Windows client, version 1.25.0; what differs in the Linux client (1.25.1) and the Android client (0.9.1, pre-beta) is described in separate subsections.

Installing the product and setting up the gate on the remote computer is the administrator's job and is covered by the Installation and Administration Guide.

1. Purpose

The client keeps a list of remote computers (sessions) and connects to them only after you prove who you are: by touching a FIDO2 security key, confirming through Windows Hello, or typing a one-time code from an authenticator app. The Remote Desktop port on the computer is closed to everyone; after a successful check the gate on that computer opens it to your address for about 90 seconds.

With the client you can:

- connect over RDP using the operating system's own client, with the saved user name and password filled in;
- connect in FIDO Stream mode to the computer's screen with low latency, with sound, a gamepad and file transfer;
- open an SSH console with saved passwords, commands and an assistant;
- lock the client itself with a password or a key.

2. Conditions of use

You need:

- the client installed: on Windows the RDP FIDO Client application in the Start menu, on Linux `rdpfido-gui` or the `rdpfido` command, on Android the RDP FIDO app;
- a second factor: a FIDO2 security key (USB or NFC), Windows Hello on your computer, or, if the gate is set to codes, an authenticator app on your phone;
- details from the administrator: the computer's address, the gate port (usually 7440) and a one-time key enrollment code, valid for 15 minutes;
- an account on the remote computer (user name and password): once the port is open, sign-in is checked by the operating system itself;
- for the Windows client, an e-mail address for activation and internet access at activation time.

In the Free edition the Windows client stores at most 10 sessions and shows an advertising tile; the Pro edition has neither restriction.

3. Getting started

3.1. Activating the Windows client

Without activation the client connects for 14 days from first run; the status bar shows how many days are left.

1. Click "Account".

2. Enter your e-mail address and click "Send code". A message with a code is sent to that address.
3. Type the code into "Code from the email" and click "Activate". The message "Account activated." appears.

The Linux and Android clients need no activation.

3.2. Adding a session

1. Click "Add" (Ctrl+N).
2. Fill in the fields: "Label" is the name of the tile; "RDP server" is the computer's name or address; "Login", "Domain" and "Password" are the account on that computer. The password is saved encrypted.
3. In "Protocol" choose how to connect: "RDP (mstsc)", "FIDO Stream (gaming, low latency)" or "SSH console (terminal, passwords, AI assistant)".
4. In the "FIDO gate" group leave "Require FIDO key confirmation when connecting" ticked. Leave "Address" empty if the gate is at the same address as the server; the port is 7440 unless the administrator gave another.
5. Click "Test". A reply such as "Gate on NAME, keys: 0, access window 90 s." means the gate is reachable.

Figure 1. The New session window of the Windows client with the RDP protocol selected

3.3. Enrolling a key

1. In the session window click "Enroll key...".
2. Enter the "Enrollment code" from the administrator and a "Key name", by which the key is told apart in the list on the computer.
3. In "Store key on" choose "External key or phone", "This computer (Windows Hello, fingerprint/PIN)" or "Any — let Windows choose".

4. Click "Enroll" and confirm the Windows prompt: touch the key or confirm through Windows Hello.
5. When the window reports that the key is enrolled, close it and click "Save".

The tile now carries a FIDO badge: the key is enrolled and the gate's certificate is remembered. From this moment the client refuses to talk to a gate that presents a different certificate.

Enroll a second key the same way (the administrator issues a new code): if the only key is lost, access can be restored only by the administrator from the computer's console.

If the gate is set to one-time codes, the client shows a QR code and a secret instead of asking for a key touch. Scan the QR code with your authenticator app and type the first code the app shows.

4. Main operations

4.1. Connecting over RDP

1. Click the session tile, or select it and press Enter. The tile shows "Confirming with key...".
2. Confirm the Windows prompt by touching the key or using Windows Hello. If the gate works with one-time codes, enter the 6-digit code from your authenticator app; a code is accepted once.
3. The status bar shows "Access granted for 90 s (key "..."). Connecting...", and the Remote Desktop window opens with the user name and password filled in.

Access stays open while the session window is open. Clicking a tile whose session is already running brings its window to the front. About 12 seconds after connecting, the client takes a picture of the session window for the tile.

4.2. Connecting in FIDO Stream mode

The mode is chosen in the session's "Protocol" field. You connect the same way, with a click on the tile and the key confirmation. The stream window opens.

Keys	Action
Ctrl+Alt+Shift+M	Session menu
Ctrl+Alt+Shift+Z	Capture or release the mouse
Ctrl+Alt+Shift+X	Full screen
Ctrl+Alt+Shift+D	Send Ctrl+Alt+Del to the computer
Ctrl+Alt+Shift+Q	Disconnect
Ctrl+Alt+O	Show stream metrics
Ctrl+Alt+R	Request control in a shared session

- File transfer. Drag files or folders into the stream window, or use the send-files item of the session menu; they arrive on the remote computer in the "RDP FIDO" folder of its downloads directory. A file placed on the remote computer in the `Outbox` subfolder of that folder is sent to your computer.
- Shared session. Several participants can join one stream; one of them controls it. While control is not yours, a view-only notice is shown at the top of the window. The session menu lists the participants, issues an invitation and hands control over.
- Stream settings (quality balance, audio, microphone, codec, connection direction) are in the "FIDO Stream" group of the session window; for a first connection leave them on automatic.

FIDO Stream is not available with a gate that is set to one-time codes.

4.3. SSH console

The console opens with a click on a tile whose protocol is "SSH console", or with "SSH console..." in the context menu of any tile. Console tiles are gathered on the "SSH" tab; the Tab key switches tabs. A session can have its own "SSH port", "Key file" and "ssh options".

The console window has a terminal and a side panel with three tabs:

- Passwords — saved passwords. A click on an entry types the password into the terminal; an entry marked for automatic entry answers its own prompt by itself.
- Commands — saved commands; a click runs the command, and the insert button types it without Enter.
- Assistant — a conversation with an artificial intelligence model that suggests commands. The service address, the model and the access key are set under the gear icon. A suggested command runs only on your click unless you choose otherwise. Terminal text is sent to the model only while the "sees the console" option is ticked.

The panel tabs are switched with Ctrl+Shift+1, 2 and 3; copy is Ctrl+Shift+C and paste Ctrl+Shift+V. The SSH port opens with the key only on computers that run the Linux gate and where the administrator has put that port under protection.

4.4. Managing sessions

Keys	Action
Enter or click	Connect
Ctrl+N	New session
Ctrl+F	Search by name, address, login
F2	Rename
F4	Edit
F5	Reload the list
Del	Delete the session together with its saved password and picture
Tab	Switch between the "Desktops" and "SSH" tabs

The tile's context menu also offers duplicating a session, copying its address, taking a picture for the tile and moving the tile left or right. Deleting a session does not remove the key on the remote computer: that is done by the administrator.

Once a minute the client checks the protected computers. A red frame and the words "RDP EXPOSED — NO KEY NEEDED!" on a tile mean that the Remote Desktop port answers without a key; report it to the administrator.

4.5. Locking the client

Entry to the client can be locked in one of two ways. Open "Settings" (the gear button) and find the "Entry lock" group.

Entry password (a master password):

1. Click "Password...", type the password into "New password" and "Once more" (at least 4 characters) and confirm.
2. At every start the client asks for the password before it shows the session list. The same password additionally encrypts the saved passwords of sessions and of the SSH console and the assistant's access key.

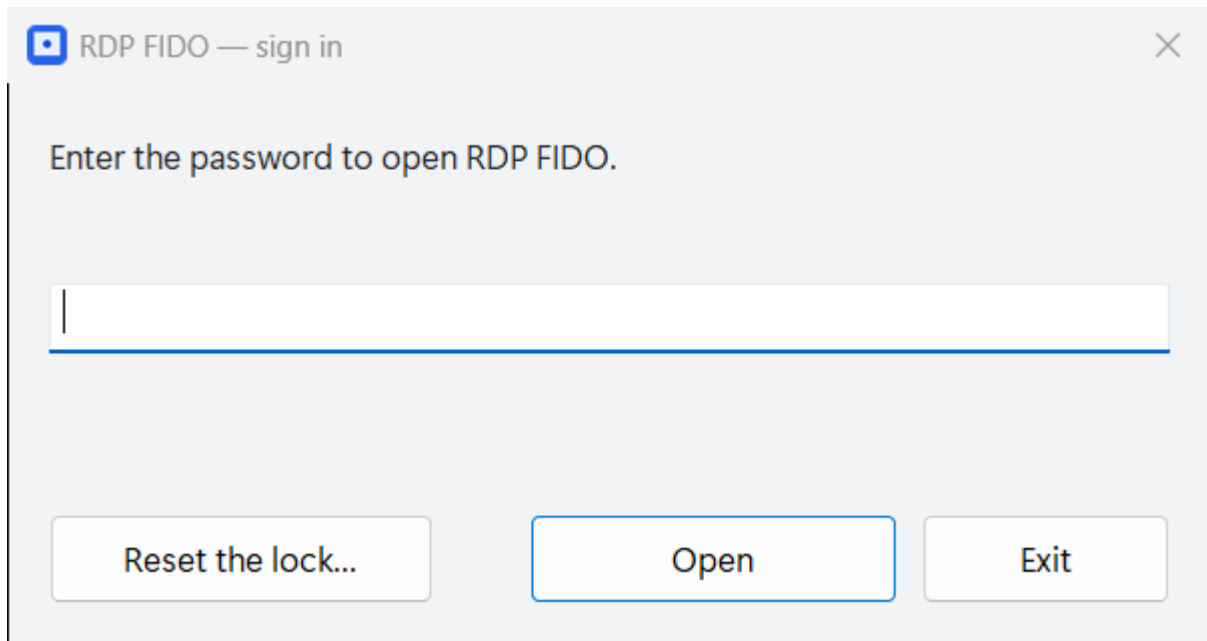


Figure 2. The password prompt shown when the client starts

FIDO2 key at entry: click "FIDO2 key...", then "Bind the key" and confirm with a key that has a PIN or a fingerprint reader. The key guards the entry only and does not encrypt the saved passwords.

Five wrong passwords in a row cost nothing; after that the client makes you wait before each further attempt, from 30 seconds up to 15 minutes. "Remove the lock" takes the lock off after you enter the password or confirm with the key once more.

Note. A forgotten password or a lost key cannot be recovered. "Reset the lock..." in the entry window removes the lock and deletes the saved passwords of sessions and of the SSH console, the assistant's access key and the history of conversations with it. Sessions, commands and settings are kept.

4.6. Updating the client

At start the client checks for a new version and offers to install it; open sessions are not interrupted. The setting "Check for and download updates automatically" and the "Check for updates" button are in the settings window. A version more than one year old does not connect until the update is installed.

4.7. Linux client

The `rdpfido-gui` window (RDP FIDO in the applications menu) holds the session list and buttons for adding and editing a session, enrolling a key, connecting, starting a stream and setting the entry lock. The same actions are available from the command line:

```
rdpfido add --name office --host srv.example.com --user user1 --password
rdpfido enroll office CODE --fingerprint THUMBPRINT
rdpfido connect office          # key confirmation, then FreeRDP
rdpfido stream office           # FIDO Stream
rdpfido ssh office              # open the port and start ssh
rdpfido console office          # SSH console
rdpfido lock password           # set the entry password
```

`--fingerprint` is the gate certificate thumbprint obtained from the administrator: the client checks it before sending the enrollment code. Session passwords are kept in the desktop keyring; if there is none, the password is asked for when connecting. The window has no tile or button for the SSH console; it is started

with the command.

4.8. Android client

1. Tap "+", enter the computer's address and the user name, and choose the protocol: "FIDO Stream (games, low latency)" or "RDP (external client)".
2. Tap the enroll-key button, choose the key (this phone with biometrics, a security key over NFC, or a security key over USB) and enter the enrollment code.
3. To connect, tap the tile and confirm with your fingerprint, the screen lock or the key. In FIDO Stream mode the stream screen opens; in RDP mode the connection is handed to the installed RDP app and the session password is placed on the clipboard.

The entry lock is switched on with the lock icon in the session list. The app is a pre-beta; sign-in with one-time codes, shared sessions and file transfer are not implemented in it.

5. Messages and common difficulties

Message or symptom	What to do
"Could not reach the gate. The machine is off or unreachable."	Check the gate address and port in the session and your network connection; contact the administrator
"The enrollment code was not accepted."	The code is single-use and valid for 15 minutes; ask the administrator for a new one
"No matching key found."	Insert an enrolled key and try again
"This key is not enrolled on the target machine."	Enroll the key for this computer
"The gate's certificate does not match the pinned one."	Do not continue; tell the administrator. After a confirmed reinstall of the gate, enroll the key again
"Too many attempts. Wait and try again."	Wait 5 minutes
"The one-time code is wrong, expired or already used."	Wait for the next code; check that the phone sets its clock automatically
"Access from your country is blocked by the target machine's settings."	Contact the administrator
"Activation required"	Activate the client with your e-mail address
"Free version limit"	Delete a session you no longer need or move to the Pro edition
"Update required"	The version is more than a year old; install the update
The confirmation passed but the Remote Desktop window did not open	Check the user name and password in the session; tell the administrator that the Remote Desktop port cannot be reached

Error details are written to `client.log` in the directory `%LOCALAPPDATA%\RdpFidoClient` (on Linux `~/.config/rdpfido`); on Android the log opens with the "Log" button.

6. Finishing work

To end a session, sign out on the remote computer or close the session window; the gate then closes the port. A FIDO Stream session ends with `Ctrl+Alt+Shift+Q` or by closing its window.

The client is closed by closing its window. If RDP sessions are still active, the client warns you: the session windows keep working and the firewall grant that was issued expires by itself. Saved sessions stay in your user profile and are there at the next start.

Take your security key with you when you leave your desk. If other people use the computer, switch on the entry lock.

Document history

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