RDCManagerX

Administrator manual: connection manager for Remote Desktop (RDP)

Contents

1. What is RDCManagerX?
2. Getting started
3. Files
4. The tree
5. Search
6. Connecting and sessions
7. Display and scale
8. Properties and inheritance
9. Logon and password vault
10. Route: direct, gateway, Tailscale
11. Reachability (ping)
12. Wake-on-LAN
13. Options
14. Keyboard shortcuts
15. Troubleshooting

1. What is RDCManagerX?

RDCManagerX is a connection manager for Remote Desktop, similar to Microsoft Remote Desktop Connection Manager (RDCMan). You organise servers in groups, connect with a double-click and work with several sessions in tabs.

- **Works with your existing RDCMan files** (`.rdg`): open them without conversion, and they stay usable in RDCMan.
- **Dynamic resolution:** the session adapts to the window or pane, without reconnecting.
- **Reachability in the tree:** see at a glance which servers are online, including stale DNS records.
- **Password vault** with a master password (AES-256), off by default.
- **Routes** via an RD Gateway or a Tailscale network, per server or group.
- **Language:** English or Dutch (*File* > *Options*); by default the app follows the Windows display language.
- **Multi-view:** a grid of panes, each with its own tabs.
- **Experience** settings as in mstsc, including *Keep session active*.
- **Active Directory:** a group can be filled with the computers of an OU.
- **One exe, no installation.**

2. Getting started

Start `RDCManagerX.exe`. No installation is needed; your administrator puts the exe on a network share or distributes it through a launcher. At startup the files that were open when you last exited are reopened. Everything is collapsed then, except *Recent* and *Favorites*.

> Start the exe from a folder of its own (e.g. `%LOCALAPPDATA%\Programs\RDCManagerX`), not from Downloads: Windows looks for some DLLs next to the exe first. The app warns when it is started from Downloads.

What	Where
App settings (window, recent files, options)	`%APPDATA%\RDCManagerX\settings.json`
Remembered passwords and secrets	Windows Credential Manager, encrypted with your master password
Debug log (only with `/debuglog`)	`%LOCALAPPDATA%\RDCManagerX\debug.log`

You can also open a file from the command line: `RDCManagerX.exe path\to\file.rdg`.

3. Files

Format	Description
`.rdg`	The RDCMan format. RDCManagerX reads and writes it without changing anything RDCMan knows about. RDCManagerX's own settings (display, route, ping, Wake-on-LAN) go into a separate file next to it: `<file>.rdg.rdcx.json`.
`.rdcx`	Own format (JSON) with everything in one file. The default for a new file.

- You can have **several files open at once**, for example "Work" and "Private"; each file is its own node in the tree.
- **Save as** converts a file between `.rdg` and `.rdcx`.
- A `*` after the file name means: unsaved changes. *Automatic saving* can be turned on in Options.

- **Passwords are never stored in a file.** Passwords in an RDCMan `.rdg` are ignored when the file is opened.

---

4. The tree

On the left is the tree with files, groups and servers, sorted alphabetically with groups first. At the top are **Connected** (every server with an open session; it disappears again at disconnect), **Recent** (last connected servers, newest first) and **Favorites** (via *Server* > *Add to favorites*).

Server colours

Icon	Meaning
Blue	No session; reachability is not checked (or the first check is still running)
Green	No session; reachable
Red	No session; not reachable
Orange	Reachable, but a different computer answers at that address: the DNS record is probably stale
Icon with dot	Session: orange dot = connecting, green dot = connected, red dot = error

Selecting a server that has an open tab shows that tab. Move servers and groups by dragging them.

---

5. Search

Press `Ctrl` + `F` (or click the search box above the tree) and type part of the name. The tree then shows only servers whose **display name or host name** matches, with their groups above them; everything is expanded. Clear the search box (or press `Esc`) to see everything again. Ideal in large files.

6. Connecting and sessions

- **Connect:** double-click a server, or select it and press `Enter`. If it already has a tab, that tab is shown.
- **A whole group:** *Server* > *Connect all servers*. The credentials are asked only once.
- **Disconnect:** `Ctrl` + `D` or via the menu. The session on the server keeps running; the tab closes.
- **Tabs:** right-click a tab for *Reconnect*, *Disconnect*, *In a separate window*, *Full screen*, *Scale* and *Move to next pane*. Middle-click closes a tab.
- **Split view** (*View* menu): 2 side by side or stacked, 3 or 4 side by side, 2×2, 3×2, 4×2 or a custom layout (up to 6 columns × 3 rows). Each pane has its own tabs; each session follows the size of its pane.
- **Dragging tabs:** within a tab bar to change the order, or to another pane to show the session there.
- **Detach:** a session in a separate window or full screen; closing that window puts the session back.
- **Exiting with open sessions** asks for confirmation first.

> If a connection drops because of a network problem, the RDP client tries to reconnect by itself. If that fails, the tab stays open with the message; choose *Reconnect* then.

7. Display and scale

By default RDCManagerX uses **dynamic resolution**: the resolution of the session follows the size of the pane or window, without reconnecting. The **scale** (100% to 300%, or automatic according to your monitor) is set per server or group (Properties > Display) or temporarily per tab (right-click > Scale).

Other display modes (Properties > Display): *Window size at connect*, *Fixed size* and *Full screen*. If an older server does not support dynamic resolution, RDCManagerX can optionally reconnect with the new size.

8. Properties and inheritance

Right-click a file, group or server > *Properties* (`Alt` + `Enter`).

Tab	Contents
General	Name, host name, comment; for servers also Wake-on-LAN
Logon	User and domain, or a credential profile of the file
Connection	Port, administrative session (console), start program, load balancing
Route	Direct, via RD Gateway or via Tailscale; reachability (ping)
Display	Display mode, scale, fixed size, colour depth
Local resources	Clipboard, drives, printers, sound, smart cards, Windows key combinations
Active Directory	Groups only, does not inherit: link to an AD OU (e.g. `OU=Computers,DC=contoso,DC=com`). *Server* > *Refresh from Active Directory* fills the group with the computers in it (sub-OUs as subgroups, only when they contain computers; or flat), using your own Windows account. They become normal servers; computers that are gone are removed on refresh (not with an open session), servers you added yourself stay. DNS names must match the domain of the OU (or *Allowed DNS suffixes*); others are skipped. After a refresh the app shows what is new, renamed, removed and skipped. The first time per server + OU the app asks for confirmation, with a warning when the server is outside this PC's domain.
Experience	Connection speed and display options as in mstsc (background, font smoothing, animations, visual styles), bitmap caching, automatic reconnect, and *Keep session active*: while you are not working in the session it gets a tiny mouse movement now and then, so the server does not lock or start its screen saver.
Security	Server authentication (certificate check)

Inheritance: each tab has the checkbox *Inherit from parent group* at the top (for a file: *from default settings*). A setting on a group or on the file itself applies to everything below it, unless a group or server has its own setting. That way you set, for example, the user name or the ping once for a whole group.

> **Files from others:** when a file turns on sharing local drives, ports, printers, plug-and-play devices or the microphone, a start program, always sending Windows key combinations to the server or *Keep session active*, RDCManagerX tells you when opening it, with the servers involved. The message only comes back when those settings change; files you save yourself count as approved.

9. Logon and password vault

RDCManagerX asks for the password at every connection, unless it is remembered. Remembering is only possible when **File > Options > Allow remembering passwords** is on; it is off by default.

- When you turn it on you set a **master password** (at least 16 characters, no obvious pattern such as repetitions, keyboard runs or "Password2026!"; a sentence of a few words is strong and easy to remember). Remembered passwords are encrypted with it (AES-256, key derived with PBKDF2) and additionally protected by Windows.
- The *Remember password* checkbox in the logon prompt is never ticked by itself.
- Separately, *Remember user name and domain* stores the name with the server in the file (when connecting a group: with the group), as on the Logon tab; the password is not included.
- A remembered password belongs to the **hosts** you used it for. When a server (for example from someone else's file) points the same account at another host, or routes the connection through another gateway, RDCManagerX first asks whether the password may be used there (default *No*; then you type it yourself). For a group there is one list with a check box per new host (unchecked by default; hosts from Active Directory marked). A password from the vault always requires server authentication (direct and via a gateway): when the server cannot prove its identity, for example with an untrusted certificate, the connection is refused and you type the password yourself. Via Tailscale you get a warning instead, because the certificate name never matches there. On Tailscale the password is asked once the network runs; the approval then belongs to the device (its MagicDNS name) in your tailnet, not to the name in the file.
- The vault locks after a configurable number of minutes without use (Options, default 15; **0 = never**, then you unlock once per RDCManagerX session). Manually: *File* > *Lock password vault*.
- Change the master password: *File* > *Change master password* or the button in Options.
- If the server rejects a remembered password, it is forgotten automatically. Manually: *Server* > *Forget remembered password*.
- **Credential profiles** (File > Credential profiles): shared user names per file, as in RDCMan.

> Forgot your master password? It cannot be recovered. The vault can only be emptied; after that you set a new master password.

10. Route: direct, gateway, Tailscale

On the **Route** tab you choose how a server is reached:

Route	Description
Direct	Directly, optionally via the RDCMan gateway setting on the same tab (stored in the `.rdg`).
Via RDP gateway	A gateway from *File* > *RDP gateways*: server, port, usage method and credentials. The gateway password can be stored in the vault. **Not tested yet** against a real RD Gateway.
Via Tailscale network	A network from *File* > *Tailscale networks*. RDCManagerX itself temporarily becomes a device in the tailnet; Tailscale does not need to be installed on this PC. In *Address in the tailnet* enter the MagicDNS name (e.g. `srv01`) or the 100.x address. The name a device gives itself and devices shared from another tailnet do not count by default; they can be allowed per network in *File* > *Tailscale networks* (stored on this PC, not in the file). The connection status shows the chosen device with its 100.x address.

Networks and gateways belong to the file; auth keys and passwords are stored only in the vault on your own PC. Via Tailscale a certificate warning appears (name `127.0.0.2`); the connection itself is encrypted by Tailscale.

> **Tailscale only with an ACL.** Tailscale's default policy allows everything: every device in the tailnet may reach every other device. So set up an ACL in the Tailscale admin console (Access controls) that allows RDP (TCP 3389) only from the RDCManagerX node (`tag:rdpclient`) to the target PCs (`tag:rdpserver`), and remove the allow-all rule. Also turn on MFA and device approval. The example is in `README.md`.

11. Reachability (ping)

Turn on for a file, group or server: Properties > Route > *Show reachability in the tree* (clear the inherit checkbox first). RDCManagerX then checks those servers in the background:

1. a ping; if there is no reply, a short connection to the RDP port (Windows often blocks ping);
2. if the server is reachable, NetBIOS is used to check that the expected computer really is at that address.

You see the result in the colour in the tree (see The tree) and in the status bar for a selected server, e.g. "*dc01 is online (3 ms)*". The interval (30 seconds by default) is set in Options. Only servers with route *Direct* are checked; several at once, without slowing down the app.

> **Orange** usually means a stale DNS record: the address was handed out by DHCP to another device, but the old record is still in DNS. Solution: enable DNS scavenging and delete the old record (see Troubleshooting).

---

12. Wake-on-LAN

Enter the MAC address for a server (Properties > General), optionally with broadcast address and port. Then wake the computer with *Server* > *Send Wake-on-LAN packet*.

---

13. Options

File > *Options*:

- Language: System, English or Dutch (applies at the next start)
- Number of servers in *Recent*
- Theme: System, Light or Dark (also via *View* > *Theme*; applies at the next start if sessions are open)
- Automatic saving
- Allow remembering passwords, automatic locking, change master password
- Interval of the reachability check
- Check daily for a new version (on by default)

New version: with that option on, the app asks GitHub once a day at startup which release is the latest. If there is a newer one, it says so once per version and asks whether to open the download page. Nothing is ever downloaded or installed automatically; GitHub only sees the IP address of the PC. You can always check by hand with *Help* > *Check for updates*.

Settings are only saved if they were changed in that session; two open windows therefore do not overwrite each other's settings.

14. Keyboard shortcuts

In the tree (keys go to the session as soon as it has focus):

Key	Action
`Enter`	Connect (or go to the open tab)
`Ctrl` + `D`	Disconnect
`Alt` + `Enter`	Properties
`F2`	Rename
`Del`	Delete
`Ctrl` + `N`	New server
`Ctrl` + `G`	New group
`Ctrl` + `F`	Search
`Ctrl` + `S`	Save
`Ctrl` + `O`	Open file
Middle-click on tab	Close tab

15. Troubleshooting

Debug log

Start with `RDCManagerX.exe /debuglog` and look at `%LOCALAPPDATA%\RDCManagerX\debug.log`. Passwords never go into the log.

Server orange in the tree (wrong computer)

Check with:

```
nslookup <name>          (which address does DNS return?)
nbtstat -A <ip-address>  (which computer is really there?)
```

Delete the stale record on a domain controller and enable DNS scavenging (aging on the zone, scavenging on the server), matched to the DHCP lease time:

```
Remove-DnsServerResourceRecord -ZoneName contoso.local -RRType A -Name <name> -RecordData <i
Set-DnsServerZoneAging -Name contoso.local -Aging $true -NoRefreshInterval 3.00:00:00 -Refre
Set-DnsServerScavenging -ScavengingState $true -ScavengingInterval 1.00:00:00 -ApplyOnAllZon
```

Password is not remembered / vault asks nothing

Check that *Allow remembering passwords* is on in Options. If you no longer know the master password, the vault can only be emptied.

Tailscale

- Tailscale must be running on the target PC, and the firewall must allow RDP (TCP 3389) from `100.64.0.0/10` on the adapter `Tailscale`.
- Target PC only reachable after you logged on there? Turn on *Run unattended* in the Tailscale menu on the target PC; then Tailscale also connects without a logon (after a restart). You can still switch it off: *Disconnect* (or `tailscale down`) takes the PC off the tailnet until *Connect*; *Exit* only closes the tray icon; stopping the *Tailscale* service stops it completely.
- Connecting fails since you set up the ACL? Check that the target PC has the tag `tag:rdpserver` and the auth key the tag `tag:rdpclient`.

- In *Address in the tailnet* enter the MagicDNS name or the 100.x address, not the account's e-mail address.
- *Test connection* in File > Tailscale networks shows whether the network starts.

Dynamic resolution does not work right after logon

Some servers need a moment after logon; RDCManagerX keeps retrying for about 25 seconds.

Black screen after being idle (session stays connected)

When the screen stays black while the session is connected, and it works again right after reconnecting, the cause is usually the **target PC** (especially Windows 10/11 and laptops with two GPUs): the screen saver or turning off the display, together with the *WDDM graphics display driver for Remote Desktop*, leaves the RDP picture black.

- Check on the target PC: `Tools dp-check.ps1` (read only).
- Fix on the target PC, as administrator from the account you log on with over RDP: `Tools dp-blackscreen-fix.ps1`. It turns off the screen saver, the WDDM driver for RDP and turning off the display on AC power; it saves a backup first, `-Undo` restores everything. Restart the PC afterwards.
- Run an unsigned script without changing the policy: `powershell -NoProfile -ExecutionPolicy Bypass -File rdp-blackscreen-fix.ps1`.
- By hand: *gpedit.msc* > *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Remote Session Environment* > "*Use WDDM graphics display driver for Remote Desktop Connections*" = *Disabled*, and turn off the screen saver.

RDCManagerX, administrator manual. The full technical documentation (building, Tailscale bridge, ACLs) is in `README.md` with the source code.