RDCManagerX

Handleiding voor beheerders: verbindingsbeheer voor Extern bureaublad (RDP)

Inhoud

1. Wat is RDCManagerX?
2. Starten
3. Bestanden
4. De boom
5. Zoeken
6. Verbinden en sessies
7. Weergave en schaal
8. Eigenschappen en overerving
9. Aanmelden en wachtwoordkluis
10. Route: direct, gateway, Tailscale
11. Bereikbaarheid (ping)
12. Wake-on-LAN
13. Opties
14. Sneltoetsen
15. Problemen oplossen

1. Wat is RDCManagerX?

RDCManagerX is een verbindingsbeheerder voor Extern bureaublad, vergelijkbaar met Microsoft Remote Desktop Connection Manager (RDCMan). Je beheert servers in groepen, verbindt met een dubbelklik en werkt met meerdere sessies in tabs.

- **Werkt met je bestaande RDCMan-bestanden** (`.rdg`): openen zonder conversie, en ze blijven in RDCMan bruikbaar.
- **Dynamische resolutie:** de sessie past zich aan het venster of vak aan, zonder opnieuw te verbinden.
- **Bereikbaarheid in de boom:** zie in een oogopslag welke servers online zijn, inclusief verouderde DNS-records.
- **Wachtwoordkluis** met hoofdwachtwoord (AES-256), standaard uit.
- **Routes** via een RD Gateway of een Tailscale-netwerk, per server of groep.
- **Taal:** Nederlands of Engels (*Bestand* > *Opties*); standaard volgt de app de weergavetaal van Windows.
- **Multi-view:** een raster van vakken, elk met eigen tabs.
- **Gebruikerservaring** zoals in mstsc, met *Sessie actief houden*.
- **Active Directory:** een groep vullen met de computers van een OU.
- **Eén exe, geen installatie.**

2. Starten

Start `RDCManagerX.exe`. Er is geen installatie nodig; je beheerder zet de exe op een netwerkshare of verspreidt hem via een launcher. Bij het starten worden de bestanden die bij het afsluiten open stonden weer geopend. Alles staat dan ingeklapt, behalve *Recent* en *Favorieten*.

> Start de exe vanuit een eigen map (bijv. `%LOCALAPPDATA%\Programs\RDCManagerX`), niet vanuit Downloads: Windows zoekt sommige DLL's eerst naast de exe. De app waarschuwt als hij vanuit Downloads gestart wordt.

Wat	Waar
App-instellingen (venster, recente bestanden, opties)	`%APPDATA%\RDCManagerX\settings.json`
Onthouden wachtwoorden en geheimen	Windows Referentiebeheer, versleuteld met je hoofdwachtwoord
Debuglog (alleen met `/debuglog`)	`%LOCALAPPDATA%\RDCManagerX\debug.log`

Een bestand openen vanaf de opdrachtregel kan ook: `RDCManagerX.exe pad\naar\bestand.rdg`.

3. Bestanden

Formaat	Toelichting
`.rdg`	Het formaat van RDCMan. RDCManagerX leest en schrijft het zonder iets te veranderen aan wat RDCMan kent. Extra instellingen van RDCManagerX (weergave, route, ping, Wake-on-LAN) komen in een apart bestand ernaast: `<bestand>.rdg.rdcx.json`.
`.rdcx`	Eigen formaat (JSON) met alles in één bestand. Standaard bij een nieuw bestand.

- Je kunt **meerdere bestanden tegelijk** open hebben, bijvoorbeeld "Werk" en "Privé"; elk bestand is een eigen knoop in de boom.
- **Opslaan als** zet een bestand om tussen `.rdg` en `.rdcx`.
- Een `*` achter de bestandsnaam betekent: niet-opgeslagen wijzigingen. *Automatisch opslaan* kan aan in Opties.

- **Wachtwoorden staan nooit in een bestand.** Wachtwoorden in een `.rdg` van RDCMan worden bij het openen genegeerd.

---

4. De boom

Links staat de boom met bestanden, groepen en servers, alfabetisch met groepen eerst. Bovenaan staan **Verbonden** (elke server met een open sessie; verdwijnt weer bij verbreken), **Recent** (laatst verbonden servers, nieuwste eerst) en **Favorieten** (via *Server > Aan favorieten toevoegen*).

Kleuren van een server

Icoon	Betekenis
🟦 Blauw	Geen sessie; bereikbaarheid wordt niet gecontroleerd (of de eerste controle loopt nog)
🟩 Groen	Geen sessie; bereikbaar
🟥 Rood	Geen sessie; niet bereikbaar
🟧 Oranje	Bereikbaar, maar op dat adres antwoordt een andere computer: het DNS-record is waarschijnlijk verouderd
Icoon met stip	Sessie: 🟧 oranje stip = verbinden, groene stip = verbonden, rode stip = fout

Selecteer een server die een open tab heeft, dan wordt die tab getoond. Servers en groepen verplaats je door ze te slepen.

---

5. Zoeken

Druk op `Ctrl`+`F` (of klik in het zoekvak boven de boom) en typ een deel van de naam. De boom toont dan alleen servers waarvan de **weergavenaam of hostnaam** overeenkomt, met de groepen erboven; alles staat daarbij uitgeklapt. Maak het zoekvak leeg (of druk op `Esc`) om weer alles te zien. Ideaal in grote bestanden.

6. Verbinden en sessies

- **Verbinden:** dubbelklik op een server, of selecteer hem en druk op `Enter`. Is er al een tab, dan wordt die getoond.
- **Een hele groep:** *Server* > *Alle servers verbinden*. De aanmeldgegevens worden één keer gevraagd.
- **Verbreken:** `Ctrl` + `D` of via het menu. De sessie op de server blijft doorlopen; de tab sluit.
- **Tabs:** rechtsklik op een tab voor *Opnieuw verbinden*, *Verbreken*, *In een eigen venster*, *Volledig scherm*, *Schaal* en *Naar het volgende vak verplaatsen*. Middelklik sluit een tab.
- **Gesplitst scherm** (menu *Beeld*): 2 naast of boven elkaar, 3 of 4 naast elkaar, 2×2, 3×2, 4×2 of een eigen indeling (tot 6 kolommen × 3 rijen). Elk vak heeft eigen tabs; elke sessie volgt de grootte van haar vak.
- **Tabs slepen:** binnen een tabbalk om de volgorde te wijzigen, of naar een ander vak om de sessie daar te tonen.
- **Losmaken:** een sessie in een eigen venster of volledig scherm; sluiten van dat venster zet de sessie terug.
- **Afsluiten met open sessies** vraagt eerst om bevestiging.

> Valt een verbinding weg door een netwerkstoring, dan probeert de RDP-client zelf opnieuw te verbinden. Lukt dat niet, dan blijft de tab staan met de melding; kies dan *Opnieuw verbinden*.

---

7. Weergave en schaal

Standaard gebruikt RDCManagerX **dynamische resolutie**: de resolutie van de sessie volgt de grootte van het vak of venster, zonder opnieuw te verbinden. De **schaal** (100% tot 300%, of automatisch volgens je monitor) stel je per server of groep in (Eigenschappen > Weergave) of tijdelijk per tab (rechtsklik > Schaal).

Andere weergavemodi (Eigenschappen > Weergave): *Venstergrootte bij verbinden*, *Vaste grootte* en *Volledig scherm*. Ondersteunt een oude server geen dynamische resolutie, dan verbindt RDCManagerX desgewenst opnieuw met de nieuwe afmeting.

---

8. Eigenschappen en overerving

Rechtsklik op een bestand, groep of server > *Eigenschappen* (`Alt` + `Enter`).

Tab	Inhoud
Algemeen	Naam, hostnaam, opmerking; bij servers ook Wake-on-LAN
Aanmelden	Gebruiker en domein, of een credential-profiel van het bestand
Verbinding	Poort, beheersessie (console), startprogramma, load-balancing
Route	Direct, via RD Gateway of via Tailscale; bereikbaarheid (ping)
Weergave	Weergavemodus, schaal, vaste grootte, kleurdiepte
Lokale bronnen	Klembord, stations, printers, geluid, smartcards, Windows-toetsen
Active Directory	Alleen bij een groep, erft niet over: koppeling aan een AD-OU (bijv. `OU=Computers,DC=contoso,DC=com`). *Server* > *Verversen vanuit Active Directory* vult de groep met de computers daarin (sub-OU's als subgroepen, alleen als er computers in zitten; of plat), met je eigen Windows-account. Ze worden gewone servers; verdwenen computers gaan bij verversen weg (niet met een open sessie), zelf toegevoegde servers blijven. DNS-namen moeten bij het domein van de OU passen (of bij *Toegestane DNS-suffixen*); andere worden overgeslagen. Na het verversen toont de app wat er nieuw, hernoemd, verwijderd en overgeslagen is. De eerste keer per server + OU vraagt de app om bevestiging, met een waarschuwing als de server buiten het domein van deze pc valt.
Gebruikerservaring	Verbindingssnelheid en weergave-opties zoals in mstsc (achtergrond, vloeiende lettertypen, animaties, visuele stijlen), bitmapcache, automatisch opnieuw verbinden, en *Sessie actief houden*: zolang je niet in de sessie werkt, krijgt die af en toe een kleine muisbeweging, zodat de server niet vergrendelt of de schermbeveiliging start.
Beveiliging	Serverauthenticatie (certificaatcontrole)

Overerving: elk tabblad heeft bovenaan het vinkje *Overnemen van bovenliggende groep* (bij een bestand: *van standaardinstellingen*). Zet je een instelling op een groep of op het bestand zelf, dan geldt die voor alles eronder, tenzij een groep of server een eigen instelling heeft. Zo stel je bijvoorbeeld de gebruikersnaam of de ping één keer in voor een hele groep.

> **Bestanden van anderen:** zet een bestand bij het verbinden het delen van lokale schijven, poorten, printers, plug-and-play-apparaten of de microfoon, een startprogramma, Windows-toetscombinaties altijd naar de server of *Sessie actief houden* aan, dan meldt RDCManagerX dat bij het openen, met de betrokken servers. De melding komt pas terug als die instellingen veranderen; bestanden die je zelf opslaat gelden als goedgekeurd.

9. Aanmelden en wachtwoordkluis

Bij elke verbinding vraagt RDCManagerX het wachtwoord, tenzij het onthouden is. Onthouden kan pas als **Bestand > Opties > Onthouden van wachtwoorden toestaan** aan staat; standaard staat dat uit.

- Bij het aanzetten stel je een **hoofdwachtwoord** in (minimaal 16 tekens, geen voor de hand liggend patroon zoals herhalingen, toetsenbordreeksen of "Wachtwoord2026!"; een zin van een paar woorden is sterk en makkelijk te onthouden). Onthouden wachtwoorden worden daarmee versleuteld (AES-256, sleutel afgeleid met PBKDF2) en daarbovenop door Windows beschermd.
- Het vinkje *Wachtwoord onthouden* in de aanmeldvraag staat nooit vanzelf aan.
- Los daarvan zet *Gebruikersnaam en domein onthouden* de ingevulde naam bij de server in het bestand (bij een groep verbinden: bij de groep), zoals op het tabblad Aanmelden; het wachtwoord valt daar niet onder.
- Een onthouden wachtwoord hoort bij de **hosts** waarvoor je het gebruikt hebt. Wijst een server (bijvoorbeeld uit een bestand van iemand anders) hetzelfde account naar een andere host, of laat hij de verbinding via een (andere) gateway lopen, dan vraagt RDCManagerX eerst of het wachtwoord daar gebruikt mag worden (standaard *Nee*; dan typ je het zelf in). Bij een groep komt er één lijst met een vinkje per nieuwe host (standaard uit; hosts uit Active Directory gemarkeerd). Met een wachtwoord uit de kluis is serververificatie altijd verplicht (direct en via een gateway): kan de server zich niet bewijzen, bijvoorbeeld met een niet-vertrouwd certificaat, dan wordt er niet verbonden en typ je het wachtwoord zelf. Via Tailscale krijg je dan een waarschuwing, omdat de certificaatnaam daar nooit klopt. Bij Tailscale komt de wachtwoordvraag pas als het netwerk draait; de goedkeuring hoort dan bij het apparaat (de MagicDNS-naam) in jouw tailnet, niet bij de naam in het bestand.
- De kluis vergrendelt na een instelbaar aantal minuten zonder gebruik (Opties, standaard 15; **0 = nooit**, dan ontgrendel je één keer per sessie van RDCManagerX). Handmatig: *Bestand* > *Wachtwoordkluis vergrendelen*.
- Hoofdwachtwoord wijzigen: *Bestand* > *Hoofdwachtwoord wijzigen* of de knop in Opties.
- Wordt een onthouden wachtwoord door de server geweigerd, dan wordt het automatisch vergeten. Handmatig: *Server* > *Onthouden wachtwoord vergeten*.
- **Credential-profielen** (Bestand > Credential-profielen): gedeelde gebruikersnamen per bestand, zoals in RDCMan.

> Hoofdwachtwoord vergeten? Dat is niet te herstellen. De kluis kan alleen worden geleegd; daarna stel je een nieuw hoofdwachtwoord in.

10. Route: direct, gateway, Tailscale

Op de tab **Route** kies je hoe een server bereikt wordt:

Route	Toelichting
Direct	Rechtstreeks, eventueel via de RDCMan-gatewayinstelling op dezelfde tab (die staat in de `.rdg`).
Via RDP-gateway	Een gateway uit *Bestand* > *RDP-gateways*: server, poort, gebruiksmethode en aanmeldgegevens. Het gateway-wachtwoord kan in de kluis. **Nog niet getest** met een echte RD Gateway.
Via Tailscale-netwerk	Een netwerk uit *Bestand* > *Tailscale-netwerken*. RDCManagerX wordt zelf tijdelijk een apparaat in het tailnet; Tailscale hoeft op deze pc niet geïnstalleerd te zijn. Vul bij *Adres in het tailnet* de MagicDNS-naam (bijv. `srv01`) of het 100.x-adres in. De naam die een apparaat zichzelf geeft en apparaten die vanuit een ander tailnet gedeeld zijn tellen standaard niet mee; toestaan kan per netwerk in *Bestand* > *Tailscale-netwerken* (opgeslagen op deze pc, niet in het bestand). De verbindingsstatus toont het gekozen apparaat met zijn 100.x-adres.

Netwerken en gateways horen bij het bestand; auth keys en wachtwoorden staan alleen in de kluis van je eigen pc. Via Tailscale verschijnt een certificaatwaarschuwing (naam `127.0.0.2`); de verbinding zelf is door Tailscale versleuteld.

> **Tailscale alleen met een ACL.** Het standaardbeleid van Tailscale staat álles toe: elk apparaat in het tailnet mag elk ander apparaat bereiken. Stel daarom in de Tailscale-adminconsole (Access controls) een ACL in die RDP (TCP 3389) alleen toestaat van de RDCManagerX-node (`tag:rdpclient`) naar de doel-pc's (`tag:rdpserver`), en haal de regel weg die alles toestaat. Zet ook MFA en device approval aan. Het voorbeeld staat in `README.md`.

11. Bereikbaarheid (ping)

Zet op een bestand, groep of server: Eigenschappen > Route > *Bereikbaarheid tonen in de boom* (eerst het overerf-vinkje uitzetten). RDCManagerX controleert die servers dan op de achtergrond:

1. een ping; komt er geen antwoord, dan een korte verbinding met de RDP-poort (Windows blokkeert ping vaak);

2. is de server bereikbaar, dan wordt via NetBIOS gecontroleerd of er echt de verwachte computer op dat adres zit.

Het resultaat zie je aan de kleur in de boom (zie De boom) en in de statusbalk bij een geselecteerde server, bijvoorbeeld *"dc01 is online (3 ms)"*. Het interval (standaard 30 seconden) stel je in bij Opties. Alleen servers met route *Direct* worden gecontroleerd; meerdere tegelijk, zonder dat de app daar trager van wordt.

> **Oranje** betekent meestal een verouderd DNS-record: het adres is via DHCP aan een ander apparaat uitgedeeld, maar het oude record staat nog in de DNS. Oplossing: DNS-scavenging aanzetten en het oude record verwijderen (zie Problemen oplossen).

---

12. Wake-on-LAN

Vul bij een server (Eigenschappen > Algemeen) het MAC-adres in, eventueel met broadcastadres en poort. Daarna wek je de computer met *Server* > *Wake-on-LAN-signaal versturen*.

---

13. Opties

Bestand > *Opties*:

- Taal: Systeem, English of Nederlands (geldt bij de volgende start)
- Aantal servers in *Recent*
- Thema: Systeem, Licht of Donker (ook via *Beeld* > *Thema*; geldt bij de volgende start als er sessies open zijn)
- Automatisch opslaan
- Onthouden van wachtwoorden toestaan, automatisch vergrendelen, hoofdwachtwoord wijzigen
- Interval voor de bereikbaarheidscontrole
- Dagelijks controleren op een nieuwe versie (standaard aan)

Nieuwe versie: met die optie aan vraagt de app eens per dag bij het starten aan GitHub wat de nieuwste release is. Is er een nieuwere, dan meldt hij dat één keer per versie, met de vraag of de downloadpagina open moet. Er wordt nooit iets automatisch gedownload of geïnstalleerd; GitHub ziet alleen het IP-adres van de pc. Handmatig kan het altijd via *Help* > *Controleren op updates*.

Instellingen worden alleen opgeslagen als ze in die sessie zijn gewijzigd; twee open vensters overschrijven elkaars instellingen dus niet.

---

14. Sneltoetsen

In de boom (de toetsen gaan naar de sessie zodra die de focus heeft):

Toets	Actie
`Enter`	Verbinden (of naar de open tab)
`Ctrl` + `D`	Verbreken
`Alt` + `Enter`	Eigenschappen
`F2`	Naam wijzigen
`Del`	Verwijderen
`Ctrl` + `N`	Nieuwe server
`Ctrl` + `G`	Nieuwe groep
`Ctrl` + `F`	Zoeken
`Ctrl` + `S`	Opslaan
`Ctrl` + `O`	Bestand openen
Middelklik op tab	Tab sluiten

15. Problemen oplossen

Debuglog

Start met `RDCManagerX.exe /debuglog` en bekijk `%LOCALAPPDATA%\RDCManagerX\debug.log`. Wachtwoorden komen nooit in het log.

Server oranje in de boom (verkeerde computer)

Controleer met:

```
nslookup <naam>          (welk adres geeft de DNS?)
nbtstat -A <ip-adres>    (welke computer zit er echt?)
```

Verwijder het verouderde record op een domeincontroller en zet DNS-scavenging aan (aging op de zone, scavenging op de server), afgestemd op de DHCP-leaseduur:

```
Remove-DnsServerResourceRecord -ZoneName contoso.local -RRType A -Name <naam> -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
```

Wachtwoord wordt niet onthouden / kluis vraagt niets

Controleer of *Onthouden van wachtwoorden toestaan* aan staat in Opties. Staat het hoofdwachtwoord niet in je geheugen, dan kan alleen de kluis worden geleegd.

Tailscale

- Op de doel-pc moet Tailscale draaien, en de firewall moet RDP (TCP 3389) toestaan vanaf `100.64.0.0/10` op de adapter `Tailscale`.
- Doel-pc pas bereikbaar nadat je er lokaal hebt ingelogd? Zet in het Tailscale-menu op de doel-pc *Run unattended* aan; dan verbindt Tailscale ook zonder aanmelding (na een herstart). Uitzetten kan nog: *Disconnect* (of `tailscale down`) haalt de pc uit het tailnet tot *Connect*; *Exit* sluit alleen het pictogram; de service *Tailscale* stoppen zet hem helemaal uit.
- Lukt verbinden niet sinds de ACL? Controleer of de doel-pc de tag `tag:rdpserver` heeft en de auth key de tag `tag:rdpclient`.

- Vul bij *Adres in het tailnet* de MagicDNS-naam of het 100.x-adres in, niet het e-mailadres van het account.
- *Test verbinding* in Bestand > Tailscale-netwerken laat zien of het netwerk opstart.

Dynamische resolutie werkt niet direct na het aanmelden

Sommige servers hebben na het aanmelden even nodig; RDCManagerX probeert het tot ongeveer 25 seconden lang opnieuw.

Zwart beeld na een tijd niets doen (sessie blijft verbonden)

Blijft het beeld zwart terwijl de sessie verbonden is, en werkt het meteen weer na opnieuw verbinden, dan ligt het meestal aan de **doel-pc** (vooral Windows 10/11 en laptops met twee GPU's): de schermbeveiliging of het uitschakelen van het scherm, samen met het *WDDM-beeldstuurprogramma voor Extern bureaublad*, laat het RDP-beeld zwart achter.

- Controleren op de doel-pc: `Tools dp-check.ps1` (leest alleen).
- Oplossen op de doel-pc, als administrator vanuit het account waarmee je via RDP aanmeldt: `Tools dp-blackscreen-fix.ps1`. Dit zet de schermbeveiliging uit, het WDDM-stuurprogramma voor RDP uit en het scherm op netstroom nooit uit; eerst wordt een back-up gemaakt, `-Undo` zet alles terug. Daarna de pc opnieuw opstarten.
- Een script dat niet ondertekend is, start je zonder het beleid te wijzigen met `powershell -NoProfile -ExecutionPolicy Bypass -File rdp-blackscreen-fix.ps1`.
- Met de hand: *gpedit.msc* > *Computerconfiguratie* > *Beheersjablonen* > *Windows-onderdelen* > *Extern bureaublad-services* > *Host voor Extern bureaublad-sessies* > *Omgeving voor externe sessies* > "*WDDM-beeldstuurprogramma gebruiken voor Extern bureaublad-verbindingen*" = *Uitgeschakeld*, en de schermbeveiliging uitzetten.

RDCManagerX, handleiding voor beheerders. De volledige technische documentatie (bouwen, Tailscale-bridge, ACL's) staat in `README.md` bij de broncode.