



CENTRE FOR
CYBERSECURITY
BELGIUM

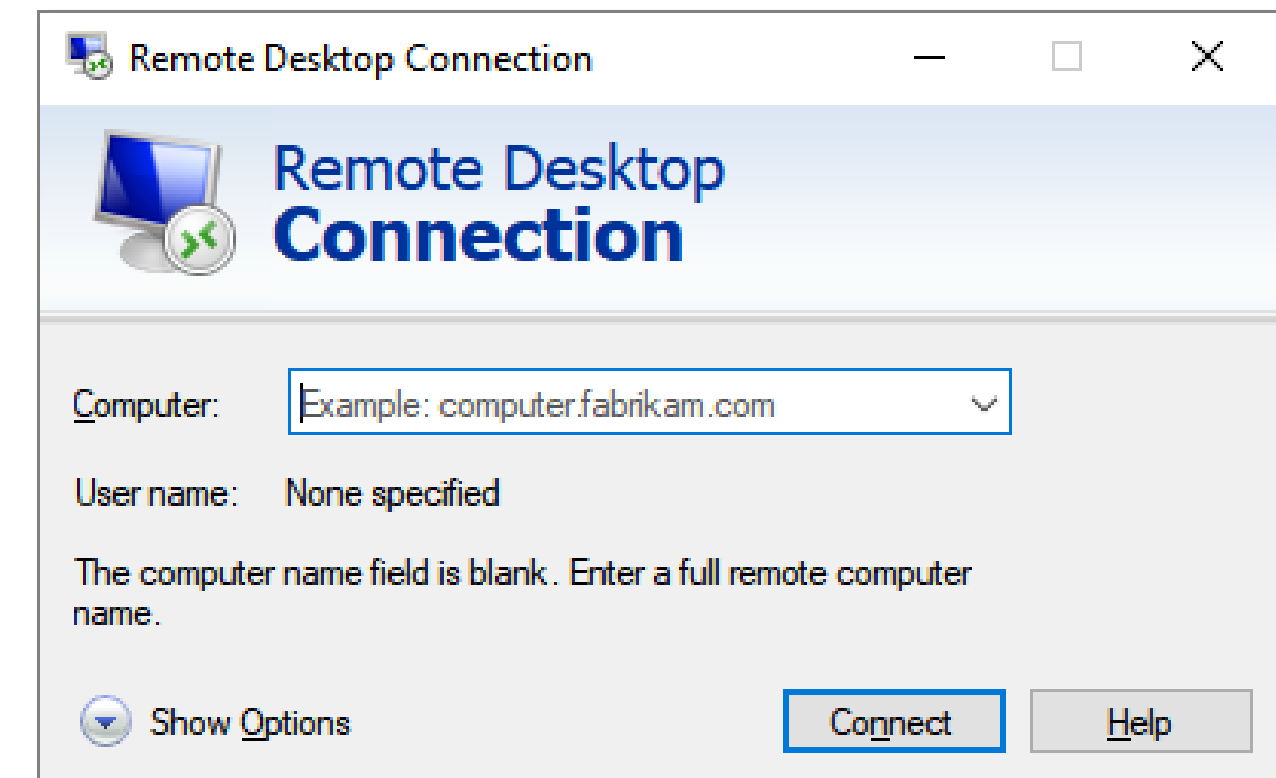


● Remote Desktop Protocol (RDP)

Webinar – 20 November 2024



What is RDP?

- **Remote access** and control
- Protocol found across **different operating systems**
- **Authenticated** login with credentials
- **Standard** TCP port 3389



Source: <https://lb.islonline.com/staticpool/2c6e8073/static/licwww/resources/v1/images/rdp/rdp-window.png>

● Why can RDP represent a security risk?

-  Commonly **targeted** by threat actors
 - Used in **90%** of intrusions in 2023 ([Sophos](#)) for initial access and data exfiltration
 - Installed by default: not detected by anti-intrusion tools and blends in with normal behavior
-  Popular among a variety of threat actors
 - **Cybercriminals** – including ransomware
 - **Advanced Persistent Threats (APT)**

● How to secure RDP?

Secure configuration with:



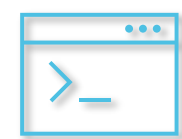
- Secure, encrypted tunneling using a **VPN**



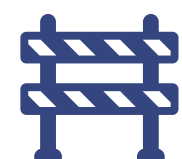
- **Restrict** RDP access to specific **IP addresses** and/or specific **users**; or segment access using **zero-trust network access**



- Enable **network-level authentication** (NLA)






- **Change the default port** to prevent automated attacks



- **Restricted Admin mode** to prevent sending credentials

● How to secure RDP?

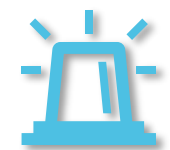
-  • Protect against credentials-based attacks using **multifactor authentication** (2FA) **on all accounts**, including privileged accounts
 - 2FA stops **99%** of credentials-based attack (source: [Microsoft, 2019](#))
-  • Set up a **password policy** to prevent password reuse
-  • Implement **account lockout policy** to avoid bruteforcing

● Good cyber hygiene is key



- **Update** your systems as soon as possible!

- After thorough **testing**
- **Prioritize** vulnerabilities with a critical/high CVSS score and actively exploited vulnerabilities



- Enable **logging** so you can **monitor for suspicious behaviour**



- Hamper lateral movement and privilege escalation:

- **Implement network segmentation**
- **Limit user privileges**



- **User awareness**



Looking for more **advice**?

Read our dedicated articles at
<https://atwork.safeonweb.be/recent-news-tips-and-warning/>

For detailed technical guidance:
<https://www.cisecurity.org/insights/white-papers/exploited-protocols-remote-desktop-protocol-rdp>



—
Questions?

●— What would you like to learn about?

Make yourself heard!

Give us your feedback and ideas:

- In the **chat**
- Via email at
info@ccb.belgium.be



● Did you know...

...that we have interesting
vacancies?

Scan the QR code and discover
our job offers for you.





CENTRE FOR
CYBERSECURITY
BELGIUM



Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

