interweb

Generated on 28/10/2026 10:52

KNOWLEDGE BASE · PUBLIC DOCUMENT

Making Remote Desktop on a Windows VPS safer

VPS & Servers

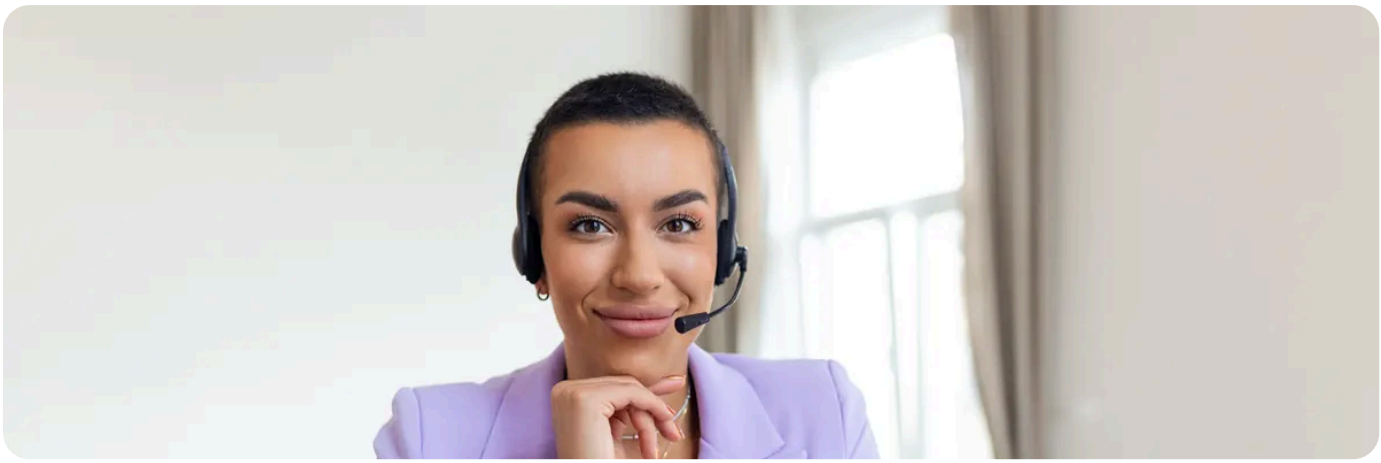
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-1412	v2026.10.10	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/1412

Making Remote Desktop on a Windows VPS safer

VPS & Servers Created on **October 10, 2026** 4 min read



A Windows Server with port 3389 open to the internet is probed by automatic programs **every day**, guessing passwords. Remote Desktop (RDP) is the most attacked way into a Windows server. The defences that count most, in order: a **long, unique password**, **account lockout** after failed attempts, **limiting who can connect** (by IP address in the firewall) and keeping **Windows up to date**. This article assumes you are already connected to the server (**connecting to a Windows VPS**). On an unmanaged VPS, Windows security is yours.

Step by step

1. **Change the Administrator password** to a long phrase you use nowhere else. It is what weighs most: a weak password is the most common way a Windows server is compromised.

2. **Create a user of your own,** a member of the administrators, and use it day to day. Afterwards you can disable "Administrator" (automatic attempts nearly always aim at that name). Test the new user in a second session before disabling the old one.

3. **Switch on account lockout.** In *Local Security Policy* (`secpol.msc`), *Account Policies*, *Account Lockout Policy*: set how many failed attempts lock the account and for how long. Pick values that will not lock you out on the first slip.

4. **Require Network Level Authentication (NLA).** In *System Properties*, *Remote* tab, leave ticked the option that only allows connections from computers using network level authentication. It forces authentication before a session opens.

5. **Limit who can connect.** In *Windows Defender Firewall with Advanced Security*, open the inbound Remote Desktop rule, *Scope* tab, and under *Remote IP address* put only your address (or the office's). You find yours in **your public IP address**.

6 **Limit who is entitled to connect** with the *Remote Desktop Users* group: only accounts in it (and the administrators) get in over RDP.

7 **Keep Windows Update on** and reboot when it asks. RDP flaws keep being found and fixed, and a server without updates is left with the known ones open.

Seeing who tried to get in

Event Viewer, under *Windows Logs*, *Security*, records the attempts: event **4625** is a failed logon, **4624** a successful one (type 10 is remote). Many failures a minute from unknown addresses are the internet's background noise; a 4624 from an address you do not recognise is the alarm.

Measure	How much it helps
Long, unique password	A lot. It weighs the most.
Account lockout	A lot. It stops the guessing.
Limiting the firewall to your IP	A lot, if your IP is stable. It nearly closes the door to the rest of the world.
Network Level Authentication	Quite a lot. Stops sessions opening for anyone who has not yet proved who they are.
Changing port 3389	Little. It cuts the noise from sweeps, but it is not protection: whoever looks will find it.
Windows Update	A lot, long term. Closes known flaws.

! **Limiting by IP will lock out whoever changes address.**
If your IP changes (mobile data, home connections), the rule stops recognising you and you have no way in. Always keep the panel console as a fallback, since it does not go through the network: **I have lost access to the server**. And test the rule in a second session before closing the first.

! **Changing the RDP port**
means editing the Windows registry (the `PortNumber` key under `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`), opening the new port in the firewall and rebooting. A mistake there can leave you without access. It gains little; put your effort into the measures above.

A tunnel or VPN in front of RDP is the strongest:
Port 3389 stops being visible on the internet. It is more work to set up and keep, and it is yours. See also **keeping your VPS secure** and, if the server publishes a website, **publishing a website with IIS**.

NEED A HAND?

Locked yourself out of the Windows server after touching these rules? Tell us the service name and we will give you the console.

Open a support ticket →

SEE ALSO

- **Connecting to a Windows VPS with Remote Desktop** →
- **Publishing a website on Windows Server with IIS** →
- **How to find your public IP address** →
- **Keeping your VPS secure** →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-1412 · v2026.10.10 · Generated on 28/10/2026 10:52