Devolutions

Replacing Microsoft RD Gateway for secure, faster & auditable RDP

NOVEMBER 2025

TABLE OF CONTENTS

Discover how to replace Microsoft RD Gateway with a more secure, faster, and audit-ready RDP architecture that reduces internet exposure, yet without triggering unnecessary performance costs, operational friction, and governance gaps.

This use case is for organizations that currently rely on Microsoft Remote Desktop Gateway (RD Gateway) to provide Remote Desktop Protocol (RDP) access, but want a replacement that reduces the size of the attack surface, improves performance, and simplifies governance.

Key audiences and environments that will benefit include:

- **SMBs** that use Microsoft RD Gateway to expose RDP over the Internet, and want to shrink the external attack surface.
- **MSPs** that need secure, auditable RDP access into many client environments without maintaining multiple VPNs and brittle gateway configs.
- **Lean internal IT and security teams** looking to simplify remote access governance while enforcing MFA, just-in-time (JIT) approvals, and least privilege on RDP sessions.
- **Organizations in regulated or audit-heavy industries** (finance, healthcare, public sector, etc.) that must generate per-session evidence for remote administrative access.
- **Hybrid and remote-first environments** where admins, vendors, and contractors require fast, reliable RDP access from outside the corporate network without exposing RDP or over-relying on VPNs.

THE PROBLEM

It is widely established that RDP should never be exposed directly to the internet. Using RD Gateway solves this, but introduces problems that are difficult to manage; especially for lean IT teams in small and mid-sized businesses (SMBs). The issues and risks include:

- **Brute force and spray exposure against Active Directory.** RD Gateway uses Windows authentication (NTLM or Kerberos) over HTTP. Internet-facing gateways can be abused for password spraying and brute-force attempts against Active Directory if controls are not tightly enforced.
- **Performance overhead from TLS-in-TLS.** RD Gateway tunnels RDP TLS inside HTTPS, which adds extra wrapping and can degrade user experience compared to more direct, protocol-aware approaches.
- **MFA enforcement is difficult.** Integrating and consistently enforcing MFA on RD Gateway often requires third-party components and brittle configuration, which increases support burden and risk of bypass.
- **Limited application-level governance.** RD Gateway focuses on network entry. It does not natively answer who is allowed to access which server, under what approval, for how long, and with what evidence, which makes audits and investigations harder.

THE SOLUTION

Devolutions Gateway, combined with Devolutions Server and Remote Desktop Manager, provides secure, Just-in-Time (JIT) RDP access — but without using RD Gateway. Here is how the pieces seamlessly fit together:

- **Devolutions Gateway** brokers RDP at the application edge. There is no network-wide tunnel. Only the specific, approved RDP path is opened for the duration of the session.
- **Devolutions Server** is the control plane for identity, access policies, approvals, MFA, and detailed logging. The Gateway accepts only those connection requests that Devolutions Server has already authorized.

- **Remote Desktop Manager** gives administrators a simple, consistent way to launch sessions. Credential injection keeps passwords out of users' hands while maintaining a transparent experience.

The table below summarizes how Devolutions Gateway + Devolutions Server + Remote Desktop Manager directly addresses and solves each of the specific challenges discussed earlier:

Challenge	Devolutions' solution	How it works
RD Gateway can be abused for password spraying and brute-force attempts against Active Directory because it uses Windows authentication (NTLM/Kerberos) over HTTP.	Reduce exposure to external authentication attacks and contain blast radius.	Devolutions Server enforces SSO with MFA and evaluates RBAC and approvals before any connection is allowed. Devolutions Gateway accepts only pre-authorized session requests and opens a path strictly to the approved RDP host for the authorized window.
TLS-in-TLS overhead in RD Gateway degrades performance and user experience.	Faster, more reliable RDP without HTTPS tunneling.	Devolutions Gateway brokers only the RDP session using standard TLS, avoiding TLS-in-TLS wrapping and "hairpinned" tunnels (i.e., when traffic from a VPN client is routed back through the VPN gateway to another internal subnet). Traffic is protocol-scoped to the RDP session, which lowers latency and reduces bandwidth waste.

Enforcing MFA on RD Gateway is difficult and brittle.	Consistent, centrally managed MFA on every RDP session.	MFA is enforced at the control plane in Devolutions Server as part of session authorization. If approval is required, the request is routed, time-boxed, and recorded; only then does Devolutions Gateway broker the session.
RD Gateway focuses on network entry and lacks action-level least-privilege controls	Action-level control: the right person, to the right server, for the right amount of time	Devolutions Server applies per-host policies, approvals, schedules, and time limits tied to the RDP action. Remote Desktop Manager injects vaulted credentials so users never handle passwords, reducing lateral-movement risk.
RD Gateway logging lacks per-session, application-layer evidence for audits and investigations.	Clear, audit-ready trails that speed investigations.	Devolutions Server records requester, target host, start/stop times, approval or ticket references, JIT window, and credential-injection status. Optional session recording and SIEM forwarding provide complete, queryable evidence.

Operational complexity and support burden around gateway configuration and client behavior.	Simpler operations with a unified control plane and consistent client experience.	Centralize identity and policy in Devolutions Server, place Devolutions Gateway at the edge with valid TLS, and use Remote Desktop Manager as the single admin client. Standardize naming, approvals, retention, and scale out by adding another Gateway if needed.

IMPLEMENTATION

Establishing the infrastructure needed to realize all of the benefits described above is simple and straightforward:

- **Step 1: Download and install Devolutions Server.**
- **Step 2: Deploy and configure Devolutions Gateway to be used with Devolutions Server.**
- **Step 3: Create or update RDP connection entries in Remote Desktop Manager to use Devolutions Gateway.**

Full and detailed deployment and configuration instructions are provided for the products. Devolutions’ world-class support team is also available to provide advice and answers.

SUMMARY OF BENEFITS

- **Smaller attack surface.** No network-wide tunnel and no reliance on RD Gateway authentication paths that can be abused for password spraying.
- **Faster and more reliable access.** Direct, protocol-scoped brokering avoids TLS-in-TLS overhead and hairpin traffic.
- **Action-level control.** Policies decide who may connect to which server, under which conditions, and for how long.
- **Secrets stay hidden.** Credential injection prevents users from handling privileged passwords.
- **Audit-ready by default.** Per-session evidence and optional session recording simplify compliance and speed investigations.
- **Simpler operations.** A unified control plane with consistent client experience reduces configuration sprawl and support burden.
- **Fits SMB realities.** Start with a focused pilot, prove value quickly, and expand at your pace.

MOVING AHEAD

Discover how Devolutions can help your organization establish an architecture that is more secure, easier to manage and operate, and fully auditable.

Request a free trial or live demo of Devolutions Gateway + Devolutions Server + Remote Desktop Manager.

Prefer a customized path? Start a 30–90 day proof of concept (POC) with Devolutions Gateway, Devolutions Server, and Remote Desktop Manager in your own environment. Our team will map roles and RDP workflows, enable MFA and JIT approvals, and track results like time to connect, audit completeness, and reduction in exposed services. Request your POC today and see measurable value fast.

We also invite you to contact us for more information and guidance.