Replacing VPNs with **Devolutions Gateway** for RDP remote access

NOVEMBER 2025

TABLE OF CONTENTS

Discover how to enhance security and efficiency by reducing RDP exposure for remote access without a complex VPN deployment.

WHO IS THIS USE CASE FOR?

This use case is for organizations that rely on Virtual Private Networks (VPNs) to enable Remote Desktop Protocol (RDP) access. It is especially relevant for small and mid-sized businesses (SMBs) that must balance strong security with day-to-day operational simplicity.

Key audiences and environments that will benefit include:

- **Distributed teams and contractors:** Frequent third-party or temporary access that makes broad VPN provisioning impractical or risky.
- **Mixed infrastructure:** On-premises servers, cloud workloads, and edge devices where RDP remains a core administrative protocol.
- **Regulated contexts:** Organizations that need per-session evidence, least-privilege controls, and MFA enforcement without expanding the network's attack surface.
- **Lean IT operations:** Teams looking to reduce client friction, shorten time-to-connect, and simplify support while improving security posture.

THE PROBLEM

The Microsoft Remote Desktop Protocol (RDP) should never be exposed directly to the Internet. This is because open RDP endpoints — for example, TCP 3389 — are vulnerable to credential-stuffing, brute-force attempts, and discovery by automated scanners within minutes of exposure.

To avoid this, many organizations place RDP behind a VPN. While this reduces direct exposure, it introduces a different set of challenges that are often disproportionate to the simple, protocol-specific task of administering a host over RDP. Five challenges in particular stand out:

1. **VPNs are complex to deploy and maintain.** Implementing a reliable, resilient VPN service requires careful design (HA pairs, certificates, device posture checks, split-tunnel rules, DNS handling, and client distribution), plus ongoing patching of the VPN appliance itself. Each client platform (Windows, macOS, Linux, mobile) adds compatibility and support overhead. For lean IT teams, the ongoing operational burden is significant and in many cases unsustainable at an optimal level over the long term.

2. **VPN clients can degrade performance and reliability.** This is especially the case for users who only need a single remote desktop session. Full-tunnel configurations route all traffic through the private network, increasing latency and consuming bandwidth. Even split-tunnel designs still add overhead: additional encryption, MTU/MSS quirks, DNS resolution rules, and fail-open/fail-closed edge cases that trigger "it works fine on-site but not remotely!" frustrations and tickets.

3. **VPNs grant network-level reach, not application-level least privilege.** After a tunnel is established, users typically gain access to subnets, not just to a specific RDP target. This widens the attack surface and complicates enforcement of just-in-time access, approvals, and credential injection.

4. **Traditional VPNs only authenticate the tunnel.** They do not natively authorize the administrative action and designate who may RDP to which host, under what conditions, and for how long.

5. **VPN-level logging is typically too generic to be useful for RDP governance.** Logging can show that a user established a tunnel (who, when, and from what IP), but it typically cannot show what matters for audits and investigations: which server was accessed via RDP, at what exact time, for how long, under whose approval, and whether the user ever handled a password. Without this application-layer context, admins cannot reliably reconstruct events, prove least-privilege workflows, or demonstrate control effectiveness to auditors. What's required is per-session RDP visibility that covers session start/stop times, target host, requesting user, approver or change ticket, credential-injection status, and optional session recording. These are essential capabilities that a standard VPN does not provide on its own.

THE SOLUTION

Devolutions Gateway, used with Devolutions Server and Remote Desktop Manager, delivers secure, Just-in-Time (JIT) RDP access without a VPN or network-wide tunnels.

The Gateway brokers RDP at the application edge, so that users reach only the specific host and protocol they're authorized to access — and nothing else. What's more, connections are only accepted after Devolutions Server has evaluated and approved the request, enforcing identity (IdP + MFA), role-based access control (RBAC), and time-boxed policies before any session begins.

For end users, the experience is efficient and seamless: they launch an RDP entry as usual, while credential injection supplies secrets directly to the session, keeping passwords hidden. For security and compliance, every session is governed and tracked in Devolutions Server with rich, per-session details (requester, target host, start/stop times, approval/ticket, JIT duration, and credential-handling status), along with optional session recording and log forwarding to the SIEM. **The result is a least-privilege, auditable RDP workflow that reduces attack surface and operational friction—without the deployment, performance, and visibility drawbacks of traditional VPNs.**

The table below summarizes how Devolutions Gateway + Devolutions Server + Remote Desktop Manager directly addresses and solves each of the specific challenges of only using a VPN, as highlighted in the previous section:

Challenge	Devolutions' solution	How it works
VPNs are complex to set up and maintain.	Faster rollout, lower operational burden, and simpler day-2 operations	Use Devolutions Gateway as a lightweight RDP broker at the edge. Use Devolutions Server to centralize identity, SSO, MFA, RBAC, approvals, and time-boxed access. Use Remote Desktop Manager as one cross-platform admin client to reduce OS and version support churn.
VPNs are slow and unreliable for a single RDP task due to full or split tunnels, hairpin traffic, MTU and MSS quirks, and DNS issues.	Lower latency, quicker connect times, and fewer "works on site but not remotely" issues.	Route only the RDP session through Devolutions Gateway using standard TLS on well-known egress ports. Eliminate VPN drivers and split tunnel edge cases so non-RDP traffic is unaffected.

VPNs grant broad network reach instead of least privilege for a specific RDP host.	Tighter access scope and reduced lateral movement risk.	In Devolutions Server, define who may RDP to which target, and under what conditions. Configure Devolutions Gateway to expose only the approved session, not a subnet. Use Remote Desktop Manager to inject vaulted credentials, so that users do not see or handle secrets.
VPNs authenticate the tunnel, but not the administrative action, conditions, or duration.	The right person connects to the right server for the right amount of time.	In Devolutions Server, apply RBAC, MFA, device and user context, approvals, schedules, and session limits, before Devolutions Gateway brokers the session.
VPN logs are too generic and do not show what happened inside RDP.	Clear audit trails and faster investigations with evidence that answers audit questions.	Record per session details in Devolutions Server including requester, target host, start and stop times, approval or ticket references, JIT window, and credential injection status. Optionally capture session recording and forward logs to the SIEM.

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

- **Less to deploy and maintain:** Devolutions Gateway, Devolutions Server, and Remote Desktop Manager replace problematic VPN stacks with a simple, standardized setup that reduces patching, client issues, and extra work.
- **Faster, more reliable RDP access:** Only the RDP session is brokered, avoiding full or split tunnels, bottlenecks, and DNS quirks. Connect times drop and tickets fall.
- **True least privilege:** Access is scoped to a specific host and protocol, with Just-in-Time windows and approvals that close automatically.
- **Action-level control:** Policies decide who may connect to which server, under what conditions, and for how long, with MFA and RBAC enforced up front.
- **Secrets stay hidden:** Credential injection from the vault prevents users from handling privileged passwords and reduces lateral movement risk.
- **Audit-ready evidence:** Per-session records and optional session recording create clear, query-ready trails that speed investigations and simplify compliance.
- **Consistent admin experience:** Remote Desktop Manager gives teams one cross-platform tool and a predictable workflow across environments.
- **Scales with SMB realities:** Start small, prove value quickly, and expand without the cost and complexity of a traditional VPN program.

MOVING AHEAD

Learn more about how Devolutions can help your organization secure remote desktop access.

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.