Devolutions

Remote desktop security and password management

OCTOBER 2025

TABLE OF CONTENTS

The real world challenges of password management in remote desktop operations 4

Emerging password management threats targeting remote desktop operations 6

How SMBs can reduce password risk in remote desktop operations 7

How Remote Desktop Manager helps SMBs strengthen password management for remote access 9

The final word 11

Next steps 12

For small and mid-sized businesses (SMBs), remote desktop access is not an option. It is an essential, affordable, and practical way that IT teams diagnose issues, apply fixes, and keep operations running across offices, remote users, branch locations, and cloud workloads. That is the good news.

The bad news is that the convenience, flexibility, versatility, and cost-effectiveness of remote access often run on the weakest link in IT security: passwords. Attackers know this, and they exploit it every day. In fact, recent analysis found that nearly 41% of successful logins across websites protected by Cloudflare used credentials that were already exposed.

The negative impact for SMBs is clear and unavoidable. Consider the following:

- According to Devolutions' State of IT Security in SMBs 2024–2025 survey report, **43% of SMBs faced at least one cyberattack in the past year.**
- Microsoft's research indicates that **breaches cost SMBs about $254,000 USD on average per incident**, and some reach several million dollars — which is enough to disrupt hiring plans, delay projects, or even threaten business continuity.
- On a global scale, IBM's 2025 Cost of a Data Breach Report puts the **average breach cost at $4.44 million USD**, underscoring how catastrophic weak authentication and poor credential hygiene can become once attackers gain access.

This white paper focuses on the intersection of remote desktop management and password security for SMB IT teams. Here is our path:

- We start by identifying the **most significant password-related risks** that undermine remote access programs.
- Next, **we examine emerging threats**, including AI-powered phishing and the lingering effects of pandemic-driven remote work patterns that expanded the attack surface for remote access.
- Then, we look at a **practical, affordable playbook** to reduce these risks.
- Finally, we highlight how **Devolutions' Remote Desktop Manager helps SMBs strengthen password management** when connecting to servers, endpoints, network devices, and cloud resources.

THE REAL WORLD CHALLENGES OF PASSWORD MANAGEMENT IN REMOTE DESKTOP OPERATIONS

Below are the most persistent challenges and risks that IT teams face when managing passwords for remote access.

- **Password reuse and credential stuffing:** Attackers do not need to hunt for zero-day exploits when reused credentials keep working. As noted earlier, Cloudflare observed that 41% of successful logins across sites it protects involved passwords that were already compromised. What's more, research by Bitwarden **found high rates of reuse and "minor-tweak" updates after breaches**, which leaves accounts only marginally harder to guess. In addition, Verizon's Data Breach Investigations Report (DBIR) highlights that **reused credentials continue to be a main driving force behind Basic Web Application Attacks.**

- **Weak, default, and unchanged passwords:** Default credentials and weak secrets still lurk in infrastructure, peripherals, and line-of-business systems. IBM highlights that **86% of organizations have never changed their router's default admin password.**

- **Privileged and shared accounts with little (if any) oversight:** Devolutions' State of IT Security in SMBs 2024–2025 survey report found that **52% of SMBs still manage privileged access manually** — with spreadsheets, shared vaults, or no formal system at all — making it difficult to enforce least privilege, rotate secrets, or trace actions to individuals.

- **Lack of centralized management and visibility:** Devolutions' State of IT Security in SMBs 2024–2025 survey report revealed that **less than 60% of SMBs use an essential password manager solution**, leaving blind spots that impede governance and auditability. Without a central system to store, rotate, and inject credentials, IT teams struggle to maintain policy, revoke access quickly, or prove compliance.

- **Social engineering and multi-factor authentication (MFA) gaps:** Phishing is still the quickest path to valid credentials, and attackers often combine convincing lures with previously stolen username/password pairs. **Once a password is captured or guessed, remote access tools can become the attacker's front door**. And even where MFA is deployed, coverage may be spotty, applied to only a few accounts, or weakened by push-fatigue and prompt-bombing.

- **Password cracking is getting faster:** Consumer-grade GPUs and turnkey tools are shrinking crack times dramatically. Hive Systems reports that **cracking times fell by 20% in 2025 versus 2024**. For example, an 8-character lowercase password can now be cracked through brute force in about 3 weeks using modern gear.
- **Incomplete audit trails for privileged activity:** When admins share accounts or store secrets outside a centralized system, it becomes hard to answer "who did what, where, and when." **This impairs incident response and compliance evidence.**
- **Sprawl across protocols, platforms, and locations:** SMB IT teams juggle RDP, SSH, VNC, web consoles, hypervisors, network devices, and cloud control planes. **Passwords and keys sprawl across those silos, multiplying the risk of duplicates and stale entries.**
- **Orphaned access and offboarding gaps:** Former employees and contractors sometimes retain access longer than they should, especially to SaaS, VPN, and remote management tools. A 2024 study reported that **63% of businesses may have former employees who can still access organizational data**, underscoring how frequently access revocation is overlooked.
- **Non-human identities and service accounts:** SMBs increasingly rely on service accounts, API tokens, and automation identities to run jobs and orchestrate infrastructure. **These identities often have broad permissions and weak lifecycle management.** Recent reporting highlights rising concern about governance for non-human identities and the need for centralized oversight comparable to human accounts.

The overall takeaway is clear: remote desktop programs often hinge on passwords, and these everyday gaps — reuse, shared admin accounts, default credentials, weak offboarding, and incomplete auditing — **create reliable entry points for attackers.**

Fixing the fundamentals is non-negotiable, but the threat landscape is not standing still. Adversaries are accelerating with automated cracking rigs, large-scale credential theft, and smarter social engineering. Next, we will look at the emerging threats and risks that intensify these pressures.

EMERGING PASSWORD MANAGEMENT THREATS TARGETING REMOTE DESKTOP OPERATIONS

The risk picture around remote desktop identity is shifting quickly. Beyond the "usual suspects" covered in the previous section, a host of emerging threats are reshaping how attackers breach accounts and devices in SMB environments:

- **Session-token theft and "pass-the-cookie" attacks:** Even if a password isn't stolen, a valid session token can hand attackers the same access. Major vendors report a surge in campaigns that swipe browser cookies or tokens and replay them to bypass authentication. For example, Google recently announced expanded protections (e.g., Device Bound Session Credentials), specifically because **cookie-theft malware continues to enable account hijacking without passwords.**
- **Adversary-in-the-Middle (AiTM) at scale:** As more organizations adopt MFA, **attackers are increasingly deploying reverse-proxy kits** to intercept credentials and session tokens in real time, effectively "phishing the MFA."
- **Malicious OAuth apps and consent-grant abuse:** Attackers are sidestepping passwords entirely by persuading users to consent to rogue OAuth applications. **Once granted, these apps can read mail, files, or admin APIs without another login.** Recent research documented large-scale campaigns using fake Microsoft OAuth apps to breach thousands of accounts across hundreds of tenants, with the goal of long-lived access that evades password resets. In addition, flaws and misconfigurations in Microsoft Entra ID integrations (e.g., nOAuth) have shown that cross-tenant auth weaknesses can enable full account takeover, even when MFA and Conditional Access are in place — affecting about 10% of SaaS apps if unpatched.
- **Automated "bad bots" probing identity edges and remote consoles:** Sophisticated automation now targets login pages, mobile API endpoints, and web admin consoles that front remote access. **For SMBs, this means more relentless testing of edge portals and remote gateways for weak authentication or token reuse.**

The common thread across these emerging threats is that they target everything around the password: session tokens, consent grants, mobile authentication flows, and traffic obfuscation. As a result, **a cybersecurity defense approach that is essentially about combining strong passwords and basic MFA isn't enough**. We discuss this further and dive deeper in the next section, where we explore practical, affordable mitigations that SMB IT teams can put in place.

HOW SMBS CAN REDUCE PASSWORD RISK IN REMOTE DESKTOP OPERATIONS

Below are practical controls that SMBs can roll out in weeks (and in some cases, even days). Each control is focused on tightening identity for remote desktop and admin access, but without overwhelming small teams or incurring excessive and unsustainable costs.

- **Move to phishing-resistant MFA for admin and remote access:** Adopt FIDO2/passkeys (platform or security keys) for all externally exposed and privileged logins, and only fall back to number-matching push only where passkeys aren't feasible. Start with remote portals (RDP gateways, web admin consoles, VPNs) and any role that can change identity settings or password policy.
- **Bind sessions to devices to neutralize token theft:** Today's attacks often steal session cookies/tokens (no password required). Where available, turn on Device-Bound Session Credentials and Token Protection, so that stolen tokens can't be replayed from another device. These features are rolling out specifically to stop cookie-theft and pass-the-cookie attacks. It is also smart to pair device-bound tokens with shorter session lifetimes and reauthentication on sensitive actions.
- **Centralize secrets and use credential injection:** Keep admin passwords, SSH keys, API tokens, and RDP creds in a central vault, and launch sessions via credential injection so users never see or handle the password. This eliminates copy-paste leakage, curbs shoulder-surf risks, and supports rotation without breaking workflows. It is also a good move to enforce per-user accountability, which means that users authenticate to the vault (with MFA), and not to each endpoint.

- **Enforce least-privilege with Just-in-Time (JIT) elevation and approvals:** Replace standing admin rights with time-bounded elevation that requires approval and MFA, and record who did what. Start with domain admins, remote management servers, hypervisors, and any account able to reset passwords.
- **Close the offboarding gap with automated deprovisioning (SCIM/IDP):** Automate account shutdown the moment HR marks a departure. Use the identity provider's SCIM connectors to propagate deletes across SaaS and admin tools. Also maintain a list of non-SCIM apps and script their offboarding. The list should be audited at least quarterly, but monthly is even better.
- **Modernize the password policy:** Adhere to NIST SP 800-63B and allow long passphrases (up to 64+ chars); encourage 15+ characters for single-factor logins; drop mandatory periodic resets unless there's evidence of compromise; allow paste in fields; and screen new passwords against known breaches. It is also advisable to pair any policy changes with a one-time reset to unique passphrases for all privileged accounts.
- **Harden the edges:** rate-limit and bot-filter login endpoints: Protect login pages for RDP gateways, VPNs, web admin consoles, and SaaS SSO with WAF rules, rate-limiting, and leaked-credential checks to blunt credential stuffing and brute force. Also set per-IP and per-account thresholds, add CAPTCHA/step-up after a few failures, and configure an alert on spikes.
- **Reduce remote desktop exposure and require pre-auth checks:** Do not expose RDP directly to the internet. Put it behind a gateway/zero-trust access layer, require MFA, and enable Network Level Authentication (NLA). If vendor access is necessary, then require time-boxed access, manage approvals, and apply session recording (see next tip).
- **Record and audit privileged sessions:** Use session recording and maintain tamper-resistant audit trails. This establishes individual accountability, accelerates investigations, and satisfies compliance evidence requirements. It is also a best practice to store recordings and logs in a separate, write-restricted repository.
- **Govern OAuth consent and monitor non-human identities:** Block user-consent to unverified OAuth apps for admin scopes, review existing grants, and restrict risky permissions by policy. Catalog service accounts/API tokens, put them under vault control, and rotate on schedule.

- **Shorten session lifetimes and require re-auth for high-risk actions:** Even with strong MFA, long-lived sessions increase exposure to token theft. Use conditional access to shorten token lifetimes for privileged apps and require step-up (MFA or passkey) before password changes, role elevation, or vault checkout.
- **Educate for modern attacks:** Awareness training should match today's patterns: QR-code phishing to mobile, reverse-proxy AiTM pages, and MFA prompt-bombing. Update policies and playbooks with "how to spot" examples.

These measures build a layered identity foundation that assumes passwords may be phished or stolen, and instead leans on phishing-resistant factors, device-bound tokens, centralized vaulting, least-privilege elevation, and hardened login edges.

Next, we look at how a purpose-built tool streamlines these controls inside real remote desktop workflows.

HOW REMOTE DESKTOP MANAGER HELPS SMBS STRENGTHEN PASSWORD MANAGEMENT FOR REMOTE ACCESS

Devolutions' Remote Desktop Manager (RDM) gives SMB IT teams an effective and controlled way to launch remote sessions, while keeping credentials controlled, hidden, and auditable. Here are the key ways that RDM helps SMBs strengthen password management for remote access:

- **Centralize secrets and inject credentials:** Store passwords, SSH keys, API tokens, and other secrets in a secured vault and inject them directly into RDP, SSH, VNC, web consoles, and more — so users never see or copy/paste the raw secret. Vault options include Devolutions Hub Business (cloud), Devolutions Server (self-hosted), or various reputable third-party vaults (e.g., KeePass, 1Password, LastPass, Keeper).

- **Enforce least privilege with check-out, approvals, and role-based access control (RBAC):** Require check-out (with optional approvals and justifications), so privileged accounts are used by one person at a time. RBAC limits who can view, launch, or modify entries, reducing collisions and oversharing while creating clear individual accountability.
- **Strengthen the "first hop" with SSO and MFA:** When paired with Devolutions Hub or Devolutions Server, protect vault access with single sign-on (e.g., Entra ID/ Okta/Ping) and enforced multi-factor authentication. Apply conditional access so higher-risk roles and locations face stronger requirements.
- **Reduce exposure with secure gateways and JIT access:** Pair RDM with Devolutions Gateway to proxy protocols (RDP/SSH, etc.) through an authenticated relay. Enable JIT connections to segmented networks — no standing VPNs or open RDP ports — tightening what is reachable from the internet while keeping performance high.
- **Record privileged sessions and preserve audit trails:** Record RDP/SSH/VNC sessions and link the footage and metadata to the exact credential and entry used. Centralized logs, reports, and audits help answer who accessed what, when, and what they did. This supports incident response, compliance, and auditing.
- **Standardize modern password policy and health:** Apply consistent password policies at the vault level and use built-in generators, analyzers, and health checks to eliminate weak or reused passwords.
- **Automate rotation and lifecycle for high-risk accounts:** Integrate RDM with Devolutions PAM to automate password rotation at check-in or on a schedule. Short, time-boxed access windows minimize standing privileges without disrupting established workflows.
- **Harden session launch with policy controls:** Enforce Network Level Authentication (where applicable), clipboard/redirection policies, and other session-level constraints from the entry template so every connection launches with the right security posture—no manual tweaks required.
- **Integrate with existing tools and vaults:** Use RDM's Integration Center to connect with popular third-party PAM/vault platforms (e.g., CyberArk, Delinea/ Thycotic, One Identity Safeguard). Where supported, route sessions through the external provider's session brokers so credentials remain shielded end-to-end.

- **Segment access with granular delegation:** Partition credentials and connections by folder, team, or project. Apply fine-grained permissions (view, edit, launch, check-out, approve) to maintain separation of duties across admins, contractors, and support tiers.
- **Detect risky entries and streamline cleanup:** Run password-health reports to flag weak, duplicate, or stale credentials; quickly bulk-fix issues with guided tooling. Entry history and versioning make it easy to audit changes and roll back safely.
- **Support operational scale with automation:** Use PowerShell/CLI and APIs to script bulk imports, rotate secrets, sync directories, or update entry templates, thereby reducing manual effort and ensuring policy is applied uniformly.
- **Improve vendor and break-glass workflows:** Require approvals and session recording for external/vendor access and keep break-glass entries under strict check-out, justification, and expiry. This preserves agility during incidents without sacrificing control or traceability.

All of these measures align with the realities of small IT teams and relatively limited SMB budgets. They can be implemented in phases, prioritized by risk, and integrated with existing processes and tooling.

THE FINAL WORD

Remote desktop has become a core operational capability. It enables rapid support, efficient administration, and continuity across distributed environments. **However, this also means that remote desktop concentrates risk around identity.** Weak and reused passwords, shared accounts without oversight, incomplete offboarding, and gaps in auditing give attackers entry points into servers, endpoints, and cloud consoles. **While strong and unique passwords are still vital, they are absolutely not enough on their own.**

For SMBs, consolidating these controls into a single operational interface reduces complexity and accelerates day-to-day work. **RDM brings these capabilities together so that policy enforcement, auditing, and privilege management remain consistent as remote sessions are launched and managed.**

NEXT STEPS

To evaluate fit and value in your environment and per your specific use cases, move forward with any of the following no-risk, no-cost options:

- **Start a free trial:** Launch a full-featured evaluation of RDM and other Devolutions solutions and products in order to experience and assess functionality like credential injection, RBAC, session recording, gateway routing, and password rotation in your existing workflows.
- **Book a live, guided demo:** Schedule a scenario-based walkthrough with a product specialist. Typical agendas include privileged session workflows (check-out, approvals, JIT elevation), policy templates for remote protocols (RDP/SSH/VNC), audit and reporting outputs, and integrations with existing identity providers and vaults.
- **Run a proof of concept (POC):** Define success criteria and pilot scope via a POC (30-90 days; minimal time investment). This is the ideal way to evaluate and validate measurable improvements in password hygiene, auditability, and time-to-connect, without disrupting production.