Devolutions

Remote desktop management, without the chaos

A Devolutions playbook

MARCH 2026

TABLE OF CONTENTS

Abstract

Managing remote desktops has become a multi-protocol, multi-tool workflow subject to security and efficiency expectations. This playbook provides a practical model for system administrators to:

1. **Consolidate** remote sessions and supporting **tools** into one controlled platform;
2. **Reduce** credential **exposure** through user management tools and auditable workflows; and
3. **Scale** day-to-day **administration** with repeatable patterns.

Introduction

In many environments, remote desktop management isn't a single tool: it's a patchwork of RDP/SSH/VNC clients, web consoles, VPN steps, password managers, and documentation that drifts out of date, out of sight, and out of mind.

That fragmentation creates two predictable problems: **operational drag** (time lost to rework and context switching) and **unnecessary risk** (credentials shared too broadly, access rights that don't match roles, and limited evidence during audits or incidents).

Recent security surveys highlight the stakes.

- Verizon's 2025 DBIR lists **credential abuse** and **exploitation of vulnerabilities** as the top two most common initial access vectors in breaches (6).
- Many IT departments still struggle with basic password hygiene: a 2022 survey of IT and cybersecurity leaders revealed that **46% were storing passwords in shared spreadsheets or documents**, and an additional **8% were writing them on paper notes** (Hitachi ID Systems and Pulse Q&A).
- Remote connections themselves pose a risk: Microsoft notes that **without protections** like Remote Credential Guard, Remote Desktop **credentials can be sent to and stored on the remote host** (2024).

Eliminating all risk and achieving a perfect operational efficiency score is impossible. But **designing remote access so it can be governed and managed efficiently *is* possible.** This playbook demonstrates how to operationalize this model with **Devolutions Remote Desktop Manager** (RDM).

The remote desktop ~~chaos~~ management playbook

1. Consolidate: centralize sessions, tools, credentials, and more

Consolidation and standardization begin by treating IT operations as a manageable environment rather than a disorganized pile of shortcuts. Devolutions RDM is that environment by design: it centralizes remote connection technologies and credentials, giving teams a consistent interface for day-to-day remote work.

Serving as a "single pane of glass" for everyday IT workflows, Devolutions RDM comes with dashboards for at-a-glance session information, tabbed views within a main window to switch easily between active sessions, and a vault structure for organizing connections and other entries into logical folders (supporting time-saving features like inheritance and batch editing).

In addition to remote session management, Devolutions RDM **offers a solution to the password hygiene problem** with the following three ways to store, manage, and secure credentials:

- **Built-in credential management functions;**
- **Integration with third-party password managers.** For example:

bitwarden 1Password DASHLANE KeePass

ManageEngine Password Manager Pro Delinea Secret Server LastPass Zoho Vault

StickyPassword RoboForm

- **Integration with Devolutions data sources**, either self-hosted or cloud-based (both included with the purchase of Devolutions RDM).

Teams can also securely store supporting artifacts such as documentation, files, images, license keys, and other sensitive information often scattered across shared drives, ticketing systems, and personal notes.

Consolidate checklist

- Inventory and de-duplicate existing sessions and tools.
- Convert your most-used connection types first (the top 20% that represent the majority of daily work): Devolutions RDM supports **over 100** remote protocols and technologies as entry types.
- Replace personal inventories (spreadsheets, ad hoc notes) with shared vault structures (folders, naming conventions, and labels aligned to how your team actually operates).
- Centralize credentials using RDM's built-in credential management functions, an external password manager, and/or a Devolutions data source.
- Store connection context with the session (for example, operational notes in the session's documentation tab).

2. Govern: control credential exposure and produce evidence

Remote-access risk is usually a user management problem: who can connect, who can change entries, who can reveal secrets, and what gets logged. Devolutions RDM supports granular, role-based access controls (RBAC) so access can map to real operational roles.

A common governance pattern is to separate "can use/connect" from "can reveal," so technicians can operate sessions while reducing unnecessary password exposure. In Devolutions RDM, users can be granted access to use entries without being granted the privilege to reveal passwords.

Governance also requires proof. Devolutions RDM's auditing and reporting capabilities include an audit trail intended to track password-related actions and help answer "who did what, when, and where." More importantly for real-world governance, this kind of logging supports demonstrating controls during internal audits and regulatory/compliance reviews

Govern checklist

- Map roles to allowed actions (view, connect, edit).
- Apply least privilege controls (minimum access and scope for each role).
- Restrict password-reveal privileges; prefer connect workflows that reduce exposure.
- Enable audit trails/reports and run periodic access reviews.

3. Scale: reduce manual work with repeatable patterns

Chaos grows when every connection is executed manually. Without a remote connection manager, launching a remote session often becomes a predictable sequence of manual steps:

- **Locate the asset name, hostname, or IP address.**
- **Retrieve the correct credentials for the target.**
- **Establish the required network path (for example, connect to a VPN or jump host).**
- **Open the appropriate client tool (such as Microsoft's Remote Desktop Connection for RDP).**
- **Enter connection parameters and credentials.**
- **Troubleshoot until the session succeeds.**

And that's just one scenario. In practice, teams often need pre- and post-steps as well: running scripts, mapping drives, launching supporting tools, or capturing evidence for troubleshooting and auditing.

Scaling remote administration means turning these ad hoc routines into repeatable patterns (templates, inheritance, and automation) so that workflows are consistent across the team and rendered as efficient as possible. Devolutions RDM is designed to reduce multi-step remote work into streamlined processes that can be standardized, shared, and governed.

High-impact examples

- **One-click session launching:** convert multi-step workflows into a consistent "launch and go" path.
- **VPN orchestration:** associate a VPN entry with many sessions and start the VPN automatically at session launch.

- **Post-launch automation:** run actions on connect or disconnect (for example, map drives, set environment variables, open required tools, start logging, and clean up artifacts).
- **Credential injection/brokering:** launch sessions with associated credentials to reduce repeated copying of secrets across tools, reducing friction and discouraging unsafe workarounds.
- **AI-assisted operations:** use RDM's MCP server with the AI model of your choice to draft scripts, generate or translate documentation and entry details, and automate routine maintenance tasks where appropriate.

Scale checklist

- Standardize your most common session types with templates and inheritance (so new entries inherit safe defaults).
- Prefer credential injection/brokering for shared workflows to reduce unnecessary credential exposure and enable consistent access patterns.
- Automate repeatable pre- and post-steps (scripts, environment setup, evidence collection, cleanup) to reduce manual overhead and variance across technicians.
- Establish VPN/session pairings and automate VPN startup where required.
- Document exceptions and edge cases, then convert them into templates or automation so they stop being tribal knowledge.

Conclusion

By consolidating the remote-desktop environment, governing credential exposure and permissions, and scaling with repeatable patterns, remote desktops become **manageable**. IT teams can **reduce operational drag** and **lower avoidable risk** without slowing down response. Devolutions RDM is built to support that operating model across diverse technologies while providing the control and evidence modern environments require.

Works cited

1. Verizon. 2025. 2025 *Data Breach Investigations Report: Executive Summary*. Accessed January 26, 2026. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

2. Hitachi ID Systems, and Pulse Q&A. 2022. "Enterprises Lack Confidence in Their Secret and Password Management" [Infographic]. *Bravura Security*, May 5, 2022. https://www.bravurasecurity.com/hubfs/Images/Infographics/Hitachi%20ID_2022-05-05_Enterprises%20lack%20confidence%20in%20their%20secret%20and%20password%20management_full.png

3. Microsoft. 2024. "Remote Credential Guard." *Microsoft Learn*. Last updated November 11, 2024. https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard.