Devolutions

Service outages: Prepare, act, and recover

A Devolutions playbook

JANUARY 2026

TABLE OF CONTENTS

Abstract

Recent outages at major cloud and network providers have shown that even mature platforms fail, and when they occur they can cascade to the cloud-based services organizations depend on, including Devolutions online services.

For IT teams, the key question is not whether an outage will occur, but whether administrators and technicians can still reach critical credentials and remote sessions when it does.

This white paper outlines a concise playbook to help IT teams maintain access to mission-critical data and recover quickly when services are unavailable.

Introduction

Major outages at providers such as Cloudflare, Microsoft Azure, or AWS are a reminder that no cloud or network is infallible. When these providers experience issues, downstream services such as Devolutions online services can be temporarily affected, even though the underlying cause lies outside Devolutions' infrastructure.

For organizations that rely on Devolutions Hub Business, Devolutions Remote Desktop Manager, Devolutions Workspace, Devolutions Portal, and other tools, the real differentiator is **preparation**: whether teams can keep working and restore normal operations without improvising under pressure.

This playbook presents a three-phase approach tailored to Devolutions customers and solutions: **prepare before the outage, act during the incident, and recover once services are restored.** The goal is to keep critical access and operational knowledge usable even when services are degraded or offline.

Prepare: build resilience before the outage

Most of the work that determines whether an outage becomes a minor event or a major incident happens **ahead of time**.

1. Enable and test offline access

Offline access is the first line of defense. **Devolutions Remote Desktop Manager** and **Devolutions Workspace** can use a local cache of supported data sources (such as our cloud-hosted or self-hosted data sources, **Devolutions Hub Business** and **Devolutions Server**, respectively) when the primary source is unavailable, so users can keep working during cloud or internal network outages. (Devolutions n.d.-a, "Offline mode"; Devolutions n.d.-b, "Offline mode")

In Devolutions Hub Business, administrators can enable offline mode per user, which creates a read-only cache of that user's entries that can be accessed from Devolutions Remote Desktop Manager or Workspace when the data source is unreachable.

Critically, offline mode should not only be configured, but **tested during a planned window** so that both administrators and end users know how it behaves.

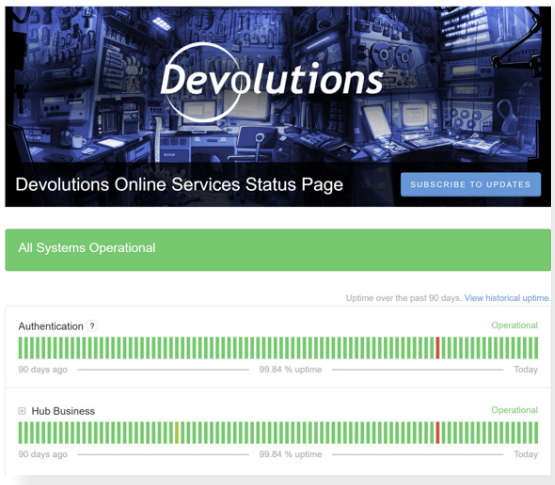
2. Define backup and disaster recovery paths

Backup and disaster recovery (DR) provide the second layer of resilience. Administrators can leverage the **Devolutions PowerShell module** to quickly create backup packages of their entries by selecting the relevant scope and exporting the data: in **Devolutions Hub Business**, a prebuilt PowerShell script for exporting entry data can be accessed directly from the administration interface. (Devolutions n.d., "PowerShell scripting"; Devolutions n.d., "Backup and recovery steps for Devolutions Hub Business entries") Saving these exports in a hardened, access-controlled location gives the team a simple but effective way to restore critical entries if Hub becomes unavailable.

As with offline mode, the DR plan should be exercised in a controlled test to verify that restoration works as designed.

3. Monitor status and health

Monitoring closes the loop. Devolutions provides a **status page** with real-time and historical information on the health of its cloud services. (Devolutions n.d., *Devolutions Online Services Status Page*) At a glance, on-call staff can see whether authentication, regional Hub instances, or ancillary services are fully operational, degraded, or in a partial outage, along with incident descriptions and timestamps.



This page is especially useful when login failures or latency are reported: it helps teams quickly determine whether they are facing a local connectivity issue, a broader Internet problem, or an active cloud-provider incident.

Administrators can also subscribe to status updates so that they are notified as soon as an incident is created, updated, or resolved. Combined with internal monitoring, this gives on-call staff a clear, consolidated picture of service health during an outage.

PREPARATION CHECKLIST

Identify **data sources** and **vaults** that must remain accessible during an outage.

- Enable **offline mode** for those data sources and users, and run a brief, scheduled offline test.
- Configure regular **backups** or exports, store them in a secure, access-controlled location, and periodically test restoration.
- Document relevant **status pages** in incident runbooks and ensure on-call staff know how to use them.

Act: operate effectively during the outage

When an outage occurs, the priority is to keep people productive while avoiding changes that complicate recovery.

Teams should quickly confirm the scope of the incident, activate offline access where needed, and keep a clear record of any manual workarounds. For many organizations, switching Devolutions Remote Desktop Manager or Workspace to offline mode is the most impactful step, because cached connections and credentials remain available even while primary data sources are down.

DURING-OUTAGE CHECKLIST

- **Confirm the incident** using internal monitoring, Devolutions' status page, and major cloud provider status pages.
- **Communicate** early with affected teams, set expectations, and remind users how to activate offline mode.
- **Switch to offline mode** where appropriate so users can keep accessing cached entries for critical systems.
- **Avoid** configuration **changes** in core systems unless required for containment or safety.
- **Record** manual workarounds and temporary access patterns for later reconciliation.

Recover: return to normal and strengthen your posture

Once services are restored, recovery should focus on validation and learning, not simply turning everything back on.

RECOVERY CHECKLIST

- Transition users back to online mode and verify that data sources are synchronizing correctly. Devolutions Remote Desktop Manager's offline mode can also be configured to automatically sync changes made while offline back to the data source once connectivity is restored.
- If data loss or corruption is suspected, follow documented DR procedures to restore from backups or recovery kits.
- Reconcile any remaining manual changes during an internal post-incident review, updating entries, documentation, and runbooks as needed.

Conclusion

Service and network outages will continue, but they don't have to compromise access or paralyze operations. By enabling and testing offline mode, maintaining disciplined backup and recovery practices, and following clear checklists before, during, and after an incident, IT teams can stay in control during disruption and significantly reduce the impact of future incidents.

Works cited

1. Devolutions. n.d. “Backup and recovery steps for Devolutions Hub Business entries.” *Devolutions Documentation*. Accessed December 4, 2025. https://redirection.devolutions.com/hub-disaster-recovery.

2. Devolutions. n.d. “PowerShell scripting.” *Devolutions Documentation*. Accessed December 12, 2025. https://redirection.devolutions.com/rdm-powershell-scripting.

3. Devolutions. n.d. *Devolutions Online Services Status Page*. Accessed December 5, 2025. https://status.devolutions.info/.

4. Devolutions. n.d.-b. “Offline mode [Devolutions Workspace].” *Devolutions Documentation*. Accessed December 4, 2025. https://redirection.devolutions.com/workspace-offline-mode.

5. Devolutions. n.d.-a. “Offline mode [Devolutions Remote Desktop Manager].” *Devolutions Documentation*. Accessed December 4, 2025. https://redirection.devolutions.com/rdm-offline-mode.