Disaster Recovery for Identity

Recover Active Directory and Entra ID 90% faster with the market's first SaaS-based disaster recovery solution

When disaster strikes your identity infrastructure, every minute of downtime costs your organization – in terms of money, productivity, and reputation. Traditional recovery approaches are slow, complex, and vulnerable to the same attacks that caused the outage. Disaster Recovery for Identity changes the game by delivering always-on, cloud-based protection that gets your business back up and running in minutes, not days.

SaaS-based identity protection

Disaster Recovery for Identity is the first-to-market comprehensive SaaS solution for protecting on-premises Active Directory environments. Built on the Quest unified identity cloud platform, it's always on, always updated, and always available – even when your data center isn't.

Unlike traditional VM snapshots or manual recovery processes, Disaster Recovery for Identity provides consistent, malware-free backups that can be restored rapidly from anywhere. This means you can recover critical identity services in minutes or hours instead of days or weeks, significantly reducing downtime costs and business impact.

Advanced recovery capabilities

Immutable cloud backups

Protect your identity infrastructure with truly secure backups that cannot be altered or removed for a specified timeframe. Disaster Recovery for Identity provides:

- **Air-gapped storage** that remains accessible even when on-premises storage is compromised.
- **Authentication capabilities** that don't depend on Active Directory, creating a true recovery safety net.
- **Highly secure backups** that are always encrypted with a randomized password only known to the system.

Benefits:

- Slash recovery time by 90% — automation eliminates manual steps.
- Protect critical identities with immutable cloud backups secure from on-prem compromises.
- Launch recovery instantly without hardware provisioning or physical data center access.
- Eliminate reliance on multiple teams — identity admins can manage recovery independently.
- Reduce infrastructure costs with cloud-based disaster recovery

When disaster strikes your identity infrastructure, every minute of downtime costs your organization – in terms of money, productivity, and reputation.

Automated recovery processes

Eliminate the risk of human error during high-pressure recovery operations with:

- **Fully automated recovery workflows** that handle all 40+ high-level steps required for AD forest recovery.
- **Simplified recovery options** are accessible through an intuitive interface that requires minimal specialized knowledge.
- **Consistent data restoration** that avoids the replication conflicts common with VM snapshot approaches.

Ideal for hybrid environments

Protect your entire identity infrastructure through a single platform:

- **Unified management** for both on-premises Active Directory and cloud-based Entra ID resources.
- **Centralized control** through a single console that reduces training requirements and administrative costs.
- **Flexible deployment options** that adapt to your specific regulatory and compliance requirements.

Enhanced security and compliance

Disaster Recovery for Identity goes beyond basic backup and restore functionality to provide comprehensive security features:

- **Malware-free recovery ensures** that restored systems don't reintroduce the original infection.
- **Validated supply chain risk management** practices that exceed industry standards.
- **ISO/IEC 27001, 27017 and 27018 certified platform** built on enterprise-grade security principles.

This SaaS solution is a key component of the Quest integrated approach to the NIST Cybersecurity Framework, covering all critical pillars of identity resilience — Identify, Protect, Detect, Respond, Recover and Govern — all from a single interface.

Unlike manual recovery processes, Disaster Recovery for Identity provides consistent, malware-free backups that can be restored rapidly from anywhere.

Enhanced security and compliance

When attackers target your identity infrastructure, traditional approaches often fall short. Consider past high-profile attacks where organizations have had to dispatch team members across continents to retrieve offline Active Directory servers unaffected by the attack. With Disaster Recovery for Identity, such extreme measures become unnecessary – you can recover from anywhere, at any time, without physical access to your infrastructure.

Our solution addresses the most critical gaps in conventional recovery strategies:

- **Immediate availability** when on-premises systems are completely compromised.
- **Independence from virtualization teams** who might not prioritize or understand AD recovery requirements.
- **Protection against ransomware** that specifically targets backup systems.

For organizations in highly-regulated industries like banking, government, insurance, and healthcare that must maintain on-premises infrastructure, Disaster Recovery for Identity delivers cloud benefits without requiring full cloud migration – providing the best of both worlds for security, compliance, and operational efficiency.

> Disaster Recovery for Identity changes the traditional recovery game with cloud-based protection that gets your business back up and running in minutes, not days.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

SYSTEM REQUIREMENTS

Services

- Web browser
- Server for the hybrid agent
- Domain Controllers to be backed up require a DC agent installed on the Domain Controller

Supported web browsers

- Microsoft Edge
- Google Chrome (latest version)
- Mozilla Firefox (latest version)

Supported OS for agents

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025