

Devolutions



Devolutions
Cloud

TECHNICAL SPECIFICATIONS

Technical specifications

Devolutions Cloud

Devolutions Cloud is a secure, cloud-based privileged password and secrets management solution tailored for businesses of all sizes. It enables centralized management of credentials, session launch configurations, documents, and sensitive information through an intuitive web interface. Fully integrated with other Devolutions products, it supports role-based access, single sign-on (SSO), privilege access management (PAM) features, and scalable user provisioning via Azure Active Directory (AD) or Okta.

System requirements

Cloud-hosted via Devolutions in Microsoft Azure, Devolutions Cloud is continuously updated, ensuring low maintenance and overhead for IT teams of all sizes.

Client access requirements

- **Browser:** Latest versions of Chrome, Edge, Firefox, or Safari
- **Devolutions Workspace:** iOS, Android, Windows, macOS, Linux, and browser extensions.
- **Remote Desktop Manager (RDM):** Windows, macOS, Linux, iOS, and Android
- **Devolutions Launcher:** Windows

Security specifications

Devolutions Cloud delivers comprehensive security capabilities through layered protection mechanisms, including identity management with various authentication providers, multi-factor authentication (MFA), robust zero-knowledge data encryption, granular role-based access controls, and extensive audit logging to maintain compliance standards and ensure full visibility into system activities.

Identity providers

Devolutions Cloud natively supports various identity providers, allowing users to authenticate and access resources seamlessly while maintaining robust security standards across the organization. These integrations enable centralized identity management, simplified user access, and enhanced security through standardized authentication protocols.

Identity provider	Enterprise integration features
Microsoft Entra ID	Enterprise directory synchronization, automated access management based on Entra ID groups
Okta	Automated user provisioning, role-based access control with groups
Devolutions Account	Custom role assignment, granular permission management, and a self-contained authentication system through a Devolutions Account

Multi-factor authentication (MFA) support

Devolutions Cloud offers comprehensive multi-factor authentication (MFA) capabilities to enhance security beyond username and password authentication. By implementing multiple verification layers, organizations can significantly reduce the risk of unauthorized access and credential-based attacks, ensuring that only legitimate users can access sensitive information and systems.

Method	Description
Identity provider MFA	Leverage the built-in MFA abilities of either Entra ID or Okta
Security key	A secure hardware key that may be used to provide MFA protection
Passkey	Passkeys integrate with the operating system or browser and provide fast and secure MFA
Authenticator (TOTP)	Authenticator apps generate time-based one-time passwords
Backup Codes	Used as a fallback when MFA methods are unavailable

Data protection

Devolutions Cloud implements comprehensive data protection across multiple security domains using industry-standard encryption. Devolutions Cloud also uses Microsoft's Transparent Data Encryption technology to add an additional layer of encryption for data at rest.

Access control

Two core security mechanisms control access to Devolutions Cloud and its resources, and the entries and resources stored within Devolutions Cloud. These controls work together to create a comprehensive security framework that protects the system and its contents.

Application access

Controls that allow/disallow logins to Devolutions Cloud.

Control type	Configuration	Scenario
IP Restrictions	Single IP configuration or IP ranges.	Restricts access based on client IP addresses, can be configured to allow or deny specific IPs or ranges
Tor Exit Node Blocking	Enable/disable Tor blocking	Block access from Tor exit nodes to prevent anonymous access

Resource-level controls

Administrators can tightly control resource-level access through various methods.

Control Type	Implementation	Configuration
Temporary access	Time-limited access grants, access request workflow	Duration settings, approval workflow, start/end time configuration
Role-based access control (RBAC)	Role hierarchy, permission inheritance, repository-level controls	Role assignments, vault, folder, and entry access rules

System permissions

A user defined as an administrator has all of the following permissions. The below permissions may also be assigned individually to users, user groups, or application identities.

- **Create privileged access vaults**
- **Create vault**
- **Manage entry templates**
- **Manage password templates**
- **Manage system configuration**
- **Manage users and user groups**
- **View administration logs and user activity**
- **Release lock**
- **Manage system images**
- **Manage scheduled reports**
- **Manage product licenses**
- **Manage privileged access tasks**
- **Manage privileged access providers**
- **Manage Devolutions Gateways**
- **Manage application services**

Role-based access control (RBAC)

Devolutions Cloud implements a role-based access control system that manages vault access.

Vault role	Permissions
Vault owners	All vault permissions.
Contributors	View all entry information with modification rights.
Privileged operators	View entries and sensitive values without modification rights. Ability to launch connections and view entry passwords.
Operators	View entries and sensitive values without modification rights. Ability to launch connections.
Privileged readers	View entries and sensitive values without modification rights.
Readers	View entries without modification rights
Restricted	Can only view a vault.
Custom	Custom-defined permissions.

Logging

DVLS provides comprehensive logging capabilities for operational monitoring, security auditing, and compliance reporting. The platform captures detailed event information across multiple domains and offers flexible configuration options for log management, retention, and distribution to various destinations.

Event types

Event type	Example events
Access control	Events related to managing user access to vault entries, temporarily or permanently. This includes granting, revoking, approving, denying, or expiring access permissions for entries or vaults.
Attachments	Tracks operations involving attachments associated with entries, such as adding, deleting, editing, or revealing attachment data.
Authentication	Covers login attempts, successful logins, and user logouts. These events help track user authentication flows and access history.
Check-outs	Refers to the lifecycle of check-out requests on vault entries, such as their creation, approval, denial, completion, revocation, and updates. It often includes policy enforcement for privileged access.
Configuration	Logs changes to system-wide settings or administrative configurations, typically indicating updates that could impact behavior or security posture.
Documentation	Captures modifications to internal documentation resources like handbook pages or attached documentation in entries.
Entries	Covers the entire lifecycle of vault entries: creation, editing, moving, checking in/out, viewing credentials, and permanent deletion. These events are critical for auditing sensitive item access and changes.
Gateway	Tracks sessions and state changes related to Devolutions Gateway activity, such as session starts, terminations, failures, and gateway configuration changes.
Group	Log operations on user groups within the platform, such as group creation, deletion, editing, and updates via the organization synchronizer.
License management	Includes adding, deleting, or editing various license types, such as product licenses or user-specific licensing artifacts.
Messaging	Logs are used when secure messages or external communications (e.g., Devolutions Send links or emails) are sent. They are often used for auditing secure information sharing.
PAM (Privileged Access Management)	Events tied to PAM-specific features, including template management, script tasks, and interactions with PAM providers or policies.
Password template	It covers creating, modifying, or deleting password generation templates used to enforce credential strength and standardization.
PAM propagation	Describes the success or failure of PAM password update propagations to downlevel systems.

Reporting	Covers scheduled report generation, such as creation, updates, deletions, and execution, which is used for visibility and compliance tracking.
System logging	Captures internal logs tied to system components for diagnostics (e.g., checkout policies), which helps with debugging and diagnostics.
Users	Represents lifecycle and state changes for user accounts, creation, deletion, and edits.
Vaults	Tracks all activity within or about vaults, including creation, editing, migration, deletion, downloading for offline or autofill use, and health diagnostics.

Integration with the Devolutions ecosystem

Remote Desktop Manager

Remote Desktop Manager (RDM) seamlessly connects with Devolutions Cloud, offering a comprehensive cross-platform solution for credential management. Available on Windows, Mac, Linux, iOS, and Android, RDM provides secure access to Devolutions Cloud-stored credentials with detailed permission controls to ensure proper access management across your organization.

- **Authentication and access control**
 - Supports SSO integrations
 - Includes privileged account management capabilities
 - Features role-based access control (RBAC) for granular permissions
- **Data synchronization**
 - Supports importing and exporting vault data between RDM and Devolutions Cloud
 - Allows multi-vault operations
- **Security features**
 - Encrypted credential storage and transmission
 - Support for One-Time Password (OTP) integration
 - Privileged Access Management (PAM) integration
 - Devolutions Gateway integration
 - Comprehensive audit logging of all credential access
- **Administrative controls**
 - User-specific settings and permissions
 - Vault ownership and access management
 - Activity monitoring and reporting
- **Additional capabilities**
 - Favorites management across platforms
 - Custom security templates and policies
 - Connection logging and monitoring
 - Push notifications for mobile platforms (iOS/Android)

Devolutions Launcher

Integrating Devolutions Launcher with Devolutions Cloud provides centralized credential management, enhanced security controls, simplified deployment, and comprehensive audit logging. This integration transforms Launcher from a basic connection tool into a remote access solution with robust security features and administrative capabilities.

Devolutions Workspace browser extension

Integrating the Devolutions Workspace browser extension with Devolutions Cloud transforms it from a basic browser password manager into an enterprise-grade credential management solution with comprehensive security controls and administrative capabilities.

- **Centralized management:** Unified credential vault system, organization-wide security policies, and centralized user access controls
- **Enterprise security:** Role-based access management, privileged account protection, and multi-factor authentication integration
- **Access governance:** Granular permission controls, vault-based organization, and time-based restrictions
- **Compliance and auditing:** Detailed credential usage tracking, comprehensive audit trails, and compliance reporting
- **Administrative control:** Simplified credential provisioning, emergency access procedures, and automated credential rotation

Devolutions Gateway

- **Centralized access control**
 - Devolutions Cloud manages Gateway access permissions through role-based security
 - Administrators can control who has access to Gateway resources
- **Enhanced security**
 - Token-based authentication using JWT (JSON Web Tokens)
 - Secure token generation and validation
 - Audit logging of Gateway access and activities
- **Automated session management**
 - Automatic session token generation and validation
 - Session monitoring and termination capabilities
 - Token revocation for security incidents
- **Simplified administration**
 - Unified logging and monitoring
 - Gateway health monitoring and notifications
- **Enterprise features**
 - Integration with privileged access management (PAM)
 - Detailed activity logging and reporting

Devolutions Workspace

Integrating Devolutions Workspace with Devolutions Cloud transforms browser-based access into a comprehensive vault management solution with advanced security controls and seamless integration capabilities.

- **Centralized credential management** - Unified access to Devolutions Cloud vaults, privileged accounts, and secure password management through an intuitive web interface
- **Enterprise security integration**
 - Seamless integration with Devolutions Cloud role-based access controls
 - Multi-factor authentication support
 - Privileged Access Management (PAM) features for sensitive credentials
 - Real-time push notifications for security events
- **Advanced access controls**
 - Granular vault permissions and access policies
 - Time-based access restrictions
 - IP filtering and Tor exit node blocking
 - Temporary access request workflows
- **Operational efficiency**
 - Browser extension integration for automated password filling
 - Real-time synchronization with Devolutions Cloud vaults
 - Built-in secure messaging for access requests and approvals
 - Offline mode support for continuous access
- **Compliance and auditing**
 - Comprehensive activity logging integrated with Devolutions Cloud
 - Detailed credential usage tracking
 - Access request audit trails
 - Secure attachment handling with encryption

Client access methods

Devolutions Cloud offers multiple methods for clients to access and interact with the system, ensuring flexibility and compatibility with different use cases and organizational needs. These methods provide secure, efficient access while maintaining robust security controls and audit capabilities.

Web interface

The web interface provides comprehensive access to Devolutions Cloud through standard web browsers:

- **Core features**
 - Credential and connection management
 - User and permission administration
 - Vault access and management
 - Privileged Access Management (PAM) configuration
 - Gateway configuration
 - Detailed activity logging and reporting
- **Security features**
 - Role-based access control (RBAC)
 - Multi-factor authentication support
 - Session management
 - IP-based access restrictions

PowerShell integration

- **PowerShell module capabilities**
 - Entry management operations
 - User and permission administration
 - System configuration
 - Logging management
 - Vault operations

Backups

Devolutions Cloud provides robust backup functionality to protect and preserve your data. These disaster recovery backups ensure your critical information remains secure and can be reliably restored. Customers may export their vault data through a JSON file export or a PowerShell script.

Reporting

Devolutions Cloud provides comprehensive reporting capabilities that help organizations monitor system activity, ensure security compliance, and efficiently manage privileged access. These detailed reports deliver actionable insights into user activities, security events, administrative actions, and vault operations.

Report categories

Devolutions Cloud reporting is organized into five main categories to help administrators efficiently access the information they need:

User reports

Monitor administrative changes and system operations to ensure governance and compliance:

- Users
- Group members
- External users
- Privileged users

General logs

Track user interactions and system behaviors for comprehensive auditing:

- Activity Logs
- User Activity
- Administration logs
- Provisioning logs

Security reports

Evaluate security posture and access controls:

- Password analyzer
- Vault permissions
- User-group permissions

Privileged access

Monitor privileged access management activities:

- Tasks
- Check-out requests

Entry reports

Track connection and entry management:

- Temporary access
- Entry security analyzer
- Deleted entries
- Vault health

Report configuration

Devolutions Cloud offers flexible report configuration options:

Scheduling options

- One-time or recurring reports
- Multiple recurrence patterns (daily, weekly, or monthly)

Delivery methods

- On-demand CSV export format
- Automated email distribution

ABOUT DEVOLUTIONS

Devolutions empowers IT teams to secure access, credentials, and remote connections through an integrated platform built for real-world complexity.

From workforce password management to privileged access and remote connection control, our solutions are tailored to the needs of IT professionals, business users, and external partners alike. Headquartered in Quebec, Canada, we remain proudly independent and committed to making advanced IT solutions accessible, usable, and affordable – for organizations of all sizes.



Devolutions Documentation:

<https://docs.devolutions.net/cloud/overview/devolutions-cloud/>



Forum: <https://forum.devolutions.net/>

Reach out to our experts:

Email: sales@devolutions.net

Phone: +1(844) 463-0419

Monday to Friday 8 a.m. to 5 p.m. EST (UTC-4)