Devolutions

Devolutions Server

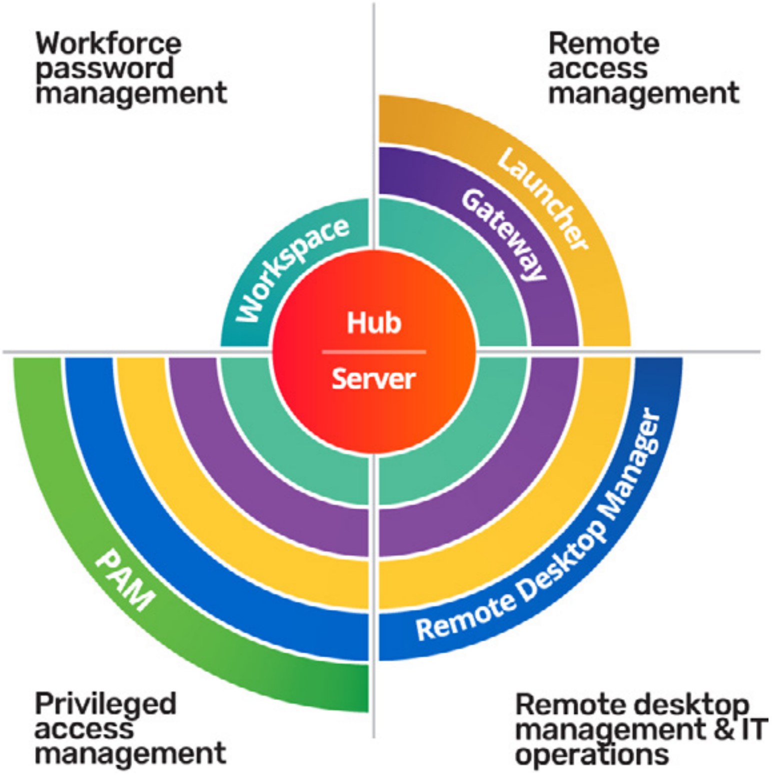
# TECHNICAL SPECIFICATIONS

# Technical specifications

## Devolutions Server

Modern organizations face growing challenges in securing IT resources, ensuring compliance, and maintaining efficiency. **Devolutions Server (DVLS)** addresses these needs by centralizing credential and remote connection management while enhancing security and streamlining team access.

DVLS integrates with identity providers, enforces strong authentication and access controls, and provides scalable vaulting for sensitive data. It enables secure, audited access through role-based permissions, automated password rotation, remote session management, and just-in-time privilege elevation.


Workforce password management
Remote access management
Launcher
Gateway
Workspace
Hub
Server
Remote Desktop Manager
PAM
Privileged access management
Remote desktop management & IT operations

# System requirements

## Sizing recommendations

The following sizing recommendations provide general guidance for hardware and infrastructure requirements based on typical usage patterns and user load. These recommendations should be adjusted based on specific workload characteristics, performance requirements, and anticipated growth.

- **Minimum:** 4 CPU cores, 8GB RAM (small deployments)
- **Recommended:** 4-8 CPU cores, 8GB RAM (medium deployments)
- **Enterprise:** 8+ CPU cores, 16+ GB RAM (large deployments)
- **Storage:** SSD recommended for optimal performance
- **Architecture:** x64

| Deployment size | Users | Recommended configuration |
|---|---|---|
| Basic | 1-20 | 4 CPU cores, 8 GB RAM |
| Mid-range | 21-75 | 4 CPU cores, 8 GB RAM |
| Large | 75 or more | HA configuration, 8+ CPU cores, 16+ GB RAM |

## Operating systems

| Operating System | Supported Versions | Software Dependencies |
|---|---|---|
| **Windows Server** | Windows Server 2016 or later (Standard/Datacenter edition) | Microsoft IIS 10.0 or higher, .NET 9.0 (.NET and ASP.NET Core) |
| **Linux (support in beta)** | Ubuntu 22.04 (other distributions are untested) | Built-in Kestrel web server, .NET 9.0 (.NET and ASP.NET Core) |

## Database requirements

| Database System | Supported Versions | Notes |
|---|---|---|
| **Microsoft SQL Server** | SQL Server 2016 or higher (Express, Standard, or Enterprise editions) | SQL authentication or Windows authentication is supported |
| **Azure SQL** | Current version | Supports SQL logins only |
| **AWS RDS for SQL Server** | SQL Server 2016 or higher | Available in all AWS regions |

## Additional components

| Component | Requirement | Purpose |
|---|---|---|
| **Devolutions Server Console** | Windows only, must be installed on Windows Server | Required for managing server instance(s) |
| **Windows Server** | 2016 domain/forest functional level or higher | Recommended for Active Directory integration |
| **Devolutions PowerShell Module** | PowerShell 7.4+ | Necessary to deploy DVLS on Linux. |

# Deployment options

DVLS offers flexible deployment methods for various organizational needs, from strict on-premises security requirements to cloud-based scalability. These options ensure that organizations can implement DVLS in a way that aligns with their specific infrastructure, security policies, and operational requirements.

DVLS requires two primary infrastructure components: a web server and a Microsoft SQL database, with flexible options on where those components are deployed.

## Topologies

Devolutions Server offers multiple deployment topologies to accommodate organizational needs, security requirements, and infrastructure environments.

| Topology | Configuration | Description | Best for |
|---|---|---|---|
| **Single Server** | DVLS and SQL Server on the same machine | Simplest deployment with all components on a single server | Small teams, testing environments, or organizations with limited IT resources |
| **Dual Servers** | DVLS and SQL Server on separate machines | Separates web application tier from database tier for improved performance | Growing organizations with moderate usage requirements |
| **High Availability** | DVLS with SQL Server cluster | SQL database set up in an active-passive SQL cluster for failover protection | Organizations requiring minimal downtime and data protection |
| **Load Balancing** | Multiple DVLS servers with a load balancer and a SQL cluster | A load balancer distributes traffic across multiple DVLS instances | Large enterprises with high concurrency needs |
| **Manual Failover** | Duplicate DVLS servers with SQL cluster | Secondary DVLS server available for manual connection if the primary fails | Organizations with DR requirements but limited automation resources |

## Deployment types

DVLS offers multiple deployment types to suit different organizational needs and infrastructure requirements. Each deployment model provides unique advantages and can be customized to meet specific security, compliance, and operational requirements.

| Deployment type | Description | Best for | Key benefits | Implementation options |
|---|---|---|---|---|
| **On-Premises** | All components are hosted within your controlled infrastructure | Organizations with strict regulatory compliance, data sovereignty requirements, or existing infrastructure investments | Complete control over security, updates, and maintenance | Single server, distributed servers |
| **Cloud-Based** | Deploy in Microsoft Azure (VM/App Services), AWS (EC2), or other cloud platforms | Organizations seeking scalability and global accessibility | Elastic resources, managed services (Azure SQL/RDS), integrated authentication | Azure VMs, App Services, AWS EC2 |
| **Hybrid** | Strategic combination of cloud and on-premises components | Organizations with mixed requirements | Flexible deployment options | |

## Security specifications

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

## Identity providers

DVLS 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 Okta groups |
| PingOne | Advanced directory integration, customizable user attribute mapping |
| Microsoft Active Directory | Domain user synchronization, automatic user provisioning from AD, and group membership mapping |
| Devolutions Server (built-in) | Custom role assignment, granular permission management, self-contained authentication system |

# Multi-factor authentication (MFA) support

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

| Method | Description |
|---|---|
| Email MFA | Time-based verification codes with configurable expiration policies |
| SMS Authentication | Real-time mobile verification with fallback options |
| Duo Security | Push-based authentication with biometric support |
| RADIUS | Enterprise-grade network authentication |
| Authenticator (TOTP) | Authenticator apps generate time-based one-time passwords |
| Backup Codes | Available as an alternative to MFA when not available |

## Data protection

DVLS implements comprehensive data protection across multiple security domains using industry-standard encryption. Devolutions Server uses our open-source cryptographic library GitHub - Devolutions/devolutions-crypto: Devolutions Cryptographic Library

## Access control

DVLS has two security mechanisms that control access to the Devolutions Server system and the entries and resources stored within DVLS. 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 DVLS.*

| Control type | Configuration | Scenario |
|---|---|---|
| Application Access | Approved application list with platform-specific controls for Windows, Mac, Linux, iOS, Android, Web access, CLI/Scripting access, Workspace, Launcher, Devolutions Workspace browser extension, and PowerShell. | Controls which client applications can access the system based on platform and application type |
| IP Restrictions | Single IP configuration, Masked IP ranges, Allow/Deny lists | Restricts access based on client IP addresses, can be configured to allow or deny specific IPs or ranges |
| Time-Based Access | Day selection (weekdays/weekends/custom), Time window definition, Timezone configuration, Custom schedule options | Restricts access based on time of day and day of week |
| GeoIP Restrictions | Country selection, Allow/Deny lists, MaxMind GeoIP integration | Restricts access based on the geographic location of the client IP address |
| Tor Exit Node Blocking | Enable/disable Tor blocking | Block access from Tor exit nodes to prevent anonymous access |

## Resource-level controls

*Once logged in, administrators can tightly control resource-level access in many different ways.*

| Control Type | Implementation | Configuration |
|---|---|---|
| Custom Templates | Security templates, Role-based templates, User group templates | Predefined security configurations, Template inheritance, and Custom security rules |
| Temporary Access | Time-limited access grants, Access request workflow | Duration settings, Approval workflow, Start/end time configuration |
| Conditional Access Policies | Policy-based access control manages user login access. | Rule combinations (AND/OR), Action definitions (Allow/Deny/MFA), Policy targeting |
| Role-Based Access | Role hierarchy, Permission inheritance, Repository-level controls | Role assignments, Permission sets, Repository access rules |

# Role-based access control (RBAC)

DVLS implements a role-based access control system that manages system access, permissions, and security boundaries based on defined roles and responsibilities.

| Role | Access level | Permissions |
|---|---|---|
| Administrator | Full System Access | All system permissions, including configuration, user management, security policies, and vault access |
| User | Standard Access | Create/Edit/Delete within the assigned scope, launch connections |
| ReadOnly | View-Only Access | View entries and connections, no modification rights |
| Restricted | Limited Access | Custom-defined limited 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 |
|---|---|
| Syslog | When the Syslog server becomes unreachable, with specific failure and exception messages. |
| Scheduler | When the scheduler service goes offline, switches between active and standby modes, when no standby scheduler is available, or when the active scheduler changes. |
| Backup | When system backups complete successfully, when backup operations fail, or when backup validation fails. |
| Gateway | When a gateway is created, updated, or deleted (ChangeManagement), or when its online status changes between online and offline (System). |
| Gateway Recording | When session recording automatic cleanup completes successfully, when cleanup completes with warnings, or when recording storage is almost full. |
| Gateway Farm | When a gateway farm is created, updated, or removed from the system. |
| Entry | When entries are created, modified, deleted, viewed, or copied, or when passwords are changed or viewed. This includes detailed tracking of attachment operations and permission changes. |
| Vault | When vault data is downloaded for autofill (UserActivity), user vaults are transferred to shared vaults (Administration). |
| Authentication Provider Sync | When user or group synchronization encounters errors or completes with warnings, including details about the synchronization process. |
| Security | When security dashboard tasks are ignored or restored, or when sealed entries are unsealed by users. |
| ServerCore | When emergency login is used to access the system. |
| Expiration | When entries expire or are approaching their expiration date, include details about the affected entries. |
| Gateway Centralized Update | When gateway updates are requested, started, completed successfully, cancelled, or when update processes fail with specific error details. |
| SMTP | When SMTP operations fail, including general failures, failures are sent with specific error details. |

| | |
|---|---|
| AdminLog | When administrative actions are logged in the system, they provide details about the action, user, and affected components. |
| DatasourceLog | When datasource events occur, including details about the category, message type, and log content. |
| PamPrivilegedAccount | When privileged accounts are created, modified, deleted, synchronized, or when password operations occur, including details about the account and provider. |
| PAM Providers | When PAM providers are created, modified, deleted, synchronized, or when password operations occur, including details about the provider configuration. |
| PAM Checkout | When privileged account checkouts are requested, approved, denied, or cancelled, including details about the checkout process and approvers. |
| PAM Team Folder | When PAM folders are created, modified, or deleted, the following details are included: folder configuration and permissions. |
| PAM Checkout Policy | When checkout policies are created, modified, or deleted, with policy configuration details. |
| PAM OTP Template | When OTP templates are created, modified, or deleted, including details about template configuration. |
| User | When user accounts are created, modified, deleted, or when user permissions change, including details about the affected user. |
| Role | Include details about the affected role when roles are created, modified, or deleted or when role permissions change. |

## Log retention & storage options

| Policy Type | Description | Options |
|---|---|---|
| Retention Periods | Defines how long logs are kept in the system | Custom, 1 Month, 3 Months, 6 Months, 1 Year, 2 Years, 7 Years, Never |
| Cleanup Strategies | Methods for handling older log data | Archive (move to archive tables), Purge (permanent deletion) |
| Log Types Managed | Different log categories with individual retention policies | System Backup Records, Connection Activity Logs, Authentication Attempt Tracking, Login Session History, System Event Messages, Privileged Access Management Audit Trail, User Profile Modification History |
| Scheduling | Automated cleanup task configuration | Enable/disable scheduled cleanup, Set cleanup time (default: 2:00 AM UTC) |
| Archiving Options | Secondary retention for archived logs | Custom period, Predefined periods, Never delete |

# Alerts and notifications

DVLS provides comprehensive alerts and notifications to ensure administrators and users remain informed about critical system events, security incidents, and operational activities. The platform offers multiple notification channels, configurable delivery mechanisms, and customizable alert criteria to match organizational requirements.

## Events

DVLS offers a flexible event subscription system that allows administrators to configure which events trigger notifications and through which channels they are delivered. Users can subscribe to specific event types based on their role and responsibilities, ensuring they receive timely alerts about relevant system activities without being overwhelmed by unnecessary notifications.

| Event Category | Event Type | Description | Severity Level |
|---|---|---|---|
| System | Service Status Changes | Notifications when services go online/offline | Information/Warning |
| System | System Failures and Errors | Critical system errors and failures | Error |
| System | Authentication Events | Emergency logging and authentication activities | Warning |
| System | Configuration Changes | System settings modifications | Information |
| System | Scheduler Events | Job success/failure and execution status | Information/Warning/Error |
| User Management | User Creation | New user account creation | Information |
| User Management | User Modification | User account updates | Information |
| User Management | User Deletion | User account removal | Information |
| User Management | User Login/Logout | User session activities | Information |
| User Management | Permission Changes | User role and permission modifications | Information |
| Connection | Connection Creation | New connection creation | Information |
| Connection | Connection Modification | Connection updates | Information |
| Connection | Connection Deletion | Connection removal | Information |
| Connection | Connection Usage | Session start/end tracking | Verbose/Information |
| Connection | Connection Failures | Failed connection attempts | Error |
| Connection | Connection Imports | Bulk connection imports | Information |
| Connection | Password Viewing | Password view events | Information |

| | | | |
|---|---|---|---|
| Gateway | Gateway Status Changes | Gateway online/offline status | Information/Warning |
| Gateway | Gateway Failures | Gateway operation failures | Error |
| Gateway | Session Start/Interruption | Session activity tracking | Verbose/Warning |
| Gateway | Recording Events | Quota limits and free space warnings | Warning |
| Communication | Email Delivery Success/Failure | Email transmission status | Information/Error |
| Communication | Message Processing Events | Message handling status | Verbose |
| PAM | Provider Management | Creation, modification, and deletion of PAM providers | Information |
| PAM | Account Management | Creation, modification, and deletion of privileged accounts | Information |
| PAM | Password Management | Password resets and updates | Information/Warning |
| PAM | Folder Management | Creation, modification, deletion, and export of PAM folders | Information |
| PAM | OTP Template Management | Creation, modification, and deletion of OTP templates | Information |
| PAM | Checkout Policy Management | Creation, modification, and deletion of checkout policies | Information |
| PAM | Checkout Activities | Checkout creation, approval, denial, expiration | Information/Warning |
| Access Request | Request Creation | New access request submission | Information |
| Access Request | Request Approval/Denial | Decision on access requests | Information |
| Access Request | Request Expiration | Access request timeout | Information |
| Access Request | Access Granted | Temporary access provision | Information |

## Notification channels

DVLS offers multiple notification channels that enable administrators to deliver timely alerts about critical system events, security incidents, and operational activities to relevant stakeholders. These channels can be configured independently to ensure appropriate communication based on event severity, recipient roles, and organizational preferences.

| Channel | Configuration | Capabilities |
|---|---|---|
| Email Notifications | Email server settings, HTML templates, recipient configuration, and enable/disable options. | Configurable email templates with support for individual and group recipients, HTML-formatted messages with event details, subject line customization, and notification level filtering. |
| In-App Notifications | Enable/disable option and user preferences. | Real-time notifications are available within the web interface, with a notification center for viewing and managing alerts, status indicators (read/unread), a notification dashboard, and a mark all as read functionality. |
| Slack Integration | Bot OAuth Access Token, channel name, and enable/disable option. | Post activity logs to Slack channels with configurable bot tokens and channel names, formatted messages with links to relevant resources, connection event notifications, and import notifications. |
| Syslog Integration | Server hostname/IP, port number, protocol (TCP/UDP), enable/disable option, and heartbeat interval. | Forward events to syslog servers with standardized logging format, configurable syslog targets, support for different protocols, and service status monitoring. |
| Secure Message Notifications | Enable/disable option and email notification option. | Secure internal messaging for sensitive notifications, used for access requests and approvals, support for attachments, localized message content, and push notification integration. |
| Push Notifications | Device registration, notification type preferences, and enable/disable options. | Mobile device notifications are configurable per device, supporting various notification types and device-specific targeting. |

# Integration with the Devolutions ecosystem

## Remote Desktop Manager

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

- **Authentication and access control**
  - Platform-specific access controls can be configured per user
  - Supports Windows Authentication integration
  - 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 DVLS
  - Allows multi-vault operations and repository selection
  - Includes version control for exported files
  - Maintains data encryption during transfer with master key options
- **Security features**
  - Encrypted credential storage and transmission
  - Support for One-Time Password (OTP) integration
  - Privileged Access Management (PAM) integration
  - Comprehensive audit logging of all credential access
- **Administrative controls**
  - Granular application access settings per platform
  - 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 DVLS 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.

- **Centralized security:** Centralized credential management, role-based access control, and enforced security policies
- **Credential management:** Secure access to centrally stored credentials, including privileged accounts and OTP
- **Access control:** Granular access control through user permissions, vault-based organization, and audit logging
- **Compliance and auditing:** Complete audit trail of connections and credentials usage

# Devolutions Workspace browser extension

Integrating Devolutions Workspace browser extension with DVLS 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/location-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**
  - DVLS manages Gateway access permissions through role-based security
  - Administrators can control who has access to Gateway resources
  - Integration with the DVLS authentication system for unified access management
- **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**
  - Centralized Gateway configuration and remote version updates through DVLS
  - Integration with DVLS user management
  - Unified logging and monitoring
  - Gateway health monitoring and notifications
- **Enterprise features**
  - Support for multiple authentication methods (Windows, Azure AD, etc.)
  - Integration with privileged access management (PAM)
  - Detailed activity logging and reporting

# Devolutions Workspace

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

- **Centralized credential management -**
  Unified access to DVLS vaults, privileged accounts, and secure password management through an intuitive web interface
- **Enterprise security integration**
  - Seamless integration with DVLS 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 and location-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 DVLS vaults
  - Built-in secure messaging for access requests and approvals
  - Offline mode support for continuous access
- **Compliance and auditing**
  - Comprehensive activity logging integrated with DVLS
  - Detailed credential usage tracking
  - Access request audit trails
  - Secure attachment handling with encryption

# Client access methods

DVLS 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 DVLS through standard web browsers:***

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

## REST API

*DVLS offers a comprehensive REST API for programmatic access.*

- **Authentication**
  - OAuth 2.0 token-based authentication
  - Support for bearer token authorization
  - Optional Windows Authentication integration
  - Pre-authentication proxy support
- **Features**
  - JSON-based request/response format
  - Comprehensive error handling
  - Access controls
  - Support for both synchronous and asynchronous operations

## PowerShell integration

- **PowerShell module capabilities**
  - Credential management operations
  - User and permission administration
  - System configuration
  - Automated password rotation
  - Security policy management
  - Vault operations
- **Security features**
  - Secure credential handling using SecureString
  - Integrated Windows Authentication support
  - Role-based access control
  - Audit logging of PowerShell operations
- **Common operations**
  - User management
  - Password resets
  - Access control configuration
  - Vault management
  - System health monitoring
  - Backup and maintenance tasks

# Backups

Devolutions Server provides robust backup functionality to protect and preserve your data. These backups ensure your critical information remains secure and can be reliably restored when needed.

## Backup types

| Backup Type | Features | Description |
|---|---|---|
| **Database Backup** | Password protection, AES256/ZipCrypto encryption, configurable timeout | Creates secure SQL Server database backups using native SQL mechanisms with optional encryption and compression. Supports full or differential backup strategies. |
| **Web Files Backup** | Password protection, encryption, and integrity validation | Creates encrypted backups of web application files, preserving configurations, customizations, and system settings for complete recovery. |

## Backup triggers

| Trigger Type | Description | Configuration Options |
|---|---|---|
| **Manual** | User-initiated backup through the web interface | On-demand execution for pre-maintenance or pre-upgrade scenarios |
| **Scheduled** | Automated backup based on a defined schedule | Start date/time, Interval in days/hours, Retention period |

## Backup management

- **Retention policies**
  - Configurable history length (number of backups to retain)
  - Automatic cleanup of older backup files
  - Custom retention based on backup type
- **Validation**
  - Automated integrity checks after backup creation
  - Verification of backup file accessibility
  - Consistency validation for database backups

# Reporting

DVLS (Devolutions Server) 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

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

### Administration reports

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

- Administration Logs
- System Permissions
- Administrator Permissions
- Gateway Security Configuration

### Activity reports

***Track user interactions and system behaviors for comprehensive auditing:***

- Activity Logs
- User Activity
- Login History
- Login Attempts
- Last Login
- Datasource Logs

### Security reports

*Evaluate security posture and access controls:*

- Password Analyzer
- Vault Permissions
- Connection Permissions
- Non-Default Permissions
- User-Centric Gateway Permissions

### PAM reports

*Monitor privileged access management activities:*

- PAM Recent Activities
- PAM Last Password Update Log

### Entry reports

*Track connection and entry management:*

- Connection Expired Entries
- Deleted Entries

## Event types and activities

*The reporting system captures detailed information across various operational domains:*

| Category | Activities tracked |
|---|---|
| **System Events** | Syslog events, scheduler operations, backup processes, service status changes |
| **Gateway Management** | Gateway status (creation/updates/deletion), recording operations, and farm configuration |
| **Entry Management** | Creation, modification, deletion, credential access, and permission changes |
| **Vault Activities** | Data operations, permission changes, transfers between vaults |
| **Security Events** | Configuration changes, authentication activities, and emergency access usage |
| **PAM Operations** | Account management, checkout processes, policy enforcement |
| **User Activity** | Login events, administrative actions, and permission modifications |

## Report configuration

*DVLS offers flexible report configuration options:*

### Scheduling options

- One-time or recurring reports
- Multiple recurrence patterns (daily, weekly, monthly, custom)
- Configurable end conditions

### Delivery methods

- CSV export format
- Automated email distribution
- On-demand generation
- Historical report storage

### Permission controls

- Role-based report access
- Administrative privilege requirements
- Delegated reporting capabilities

# 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/server/overview/what-is-server/

**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)