

Liquibase Secure vs Liquibase Community

Explore the key differences between Liquibase Secure and Liquibase Community, along with a comprehensive comparison of their features.

65+ Database Types and Modern Database Platforms Covered

Liquibase Secure

For enterprises that need speed with enterprise controls for governance, security, and compliance, where every driver, extension, and policy is already tested and packaged.

Liquibase Community

For developers who want freedom and flexibility to manage database change on their own terms.

Govern AI-Generated Database Change and Drive AI Modernization

Implement Agent Safe Governance Across Your Database Estate:

AI is changing how database changes are created. Liquibase Secure governs how they reach production.

Liquibase Secure helps enterprises validate, track, and govern every database change before and after production, whether created by humans or AI.

Not available

Gain a Comprehensive View with Change Intelligence:

Get a better way to understand database change, identify risk earlier, and triage failures faster. Gain visibility and control across every database change.

Liquibase Secure provides full observability so enterprises can move fast with trust and accountability.

Not available

Liquibase MCP for Changelog Generation:

Streamline and accelerate database change delivery across your entire environment with a unified, natural language interface that eliminates context switching and removes the complexity of writing database specific, context aware changes.

Use plain language to quickly generate production-ready code that provides syntax, schema compliance, rollback logic, and cross-database compatibility effortlessly.

Not available

Make Your Databases AI Ready:

Pave the way for whatever AI brings by building trust into your database foundation. Enforce consistency and data lineage across Snowflake, Databricks, MongoDB, and 65+ database types.

Ensure schema changes are standardized, governed, and traceable across environments.

Not supported in product
Manual effort and ongoing maintenance required.

Keep Pace with AI Changes Securely:

Reduce downtime and protecting business continuity regardless of whether changes originate from humans or AI with Liquibase Secure.

With automated and custom rollback capabilities, teams can speed development, instantly undo bad deployments, minimizing downtime and reducing MTTR.

Not available

Deploy Faster Than Ever with Liquibase Secure Deployment Connectors:

Bring governed database change into the tools you already use including popular deployment models so you get stronger governance and auditability without rebuilding your workflows.

Govern database change across human developers, AI assistants, CI/CD pipelines, and production environments while integrating into existing and AI-enabled workflows.

Not available

Ensure Compliance and Be Audit-Ready

Traceability and Audit Readiness

Liquibase Secure automatically tracks who changed what, where, and when. With compliance-ready history reports, structured logging, and user identity for every change, audit prep that used to take weeks now takes minutes—ensuring you're always ready for SOX, HIPAA, or PCI-DSS requirements.

Compliance-ready traceability available out of the box.

Limited capabilities

Reports, structured logging, and ChangelogHistory not supported.

Compliance Support and Reporting

Liquibase Secure enhances database compliance by integrating compliance directly into CI/CD pipelines through features like automated audit trails, governance, and policy enforcement using custom checks, and RBAC support. Prevent risky changes before they reach production, and help teams stay audit-ready.

Support adherence to regulations such as SOX, HIPAA, PCI-DSS, SOC 2, DORA, and GDPR by providing visibility and evidence for audits.

Not supported in product

Manual effort and ongoing maintenance required.

Robust Policies

Designed to enforce governance, standards, and compliance within database change management, Liquibase Secure makes it easy to deploy policies across your systems. Policies make it possible for organizations to define and automatically enforce rules and best practices for database changes, ensuring consistency and quality.

Policy checks and custom policy checks enable organizations to implement highly specific and complex governance rules tailored to their unique requirements.

Not supported in product

Manual effort and ongoing maintenance required.

Credential Management

Liquibase Secure centralizes and protects database credentials, removing the risks of hard-coded passwords or ad hoc sharing. With integrations into secrets managers and strict access controls, teams can ensure only authorized users and processes can connect to sensitive environments.

Securely manage credentials with integrations for HashiCorp Vault, AWS Secrets Manager, and other enterprise secret stores.

Not supported in product

Manual credential storage and management.

Strengthen Security and Eliminate Risk Without Slowing Production

Separation of Duties & Secure Credential Management

Liquibase Secure delivers strict separation of duty enforcement, secure credential management, and built-in support for modern authentication methods. This means developers, Ops, and DBAs can accelerate database change delivery without compromising compliance or security.

Get built-in credential protections, modern authentication support, and full audit trails.

Manual effort

Relies on custom integrations.

Enforcing DB Standards in Development

With Liquibase Secure's Secure Developer features, enforcing database standards isn't left to chance or after-the-fact reviews. Standards are embedded into the developer's own tools and workflow, ensuring high quality and consistent changes from the very start.

Liquibase Secure bakes database standards right into each developer's workflow.

Not supported in product

Manual effort and ongoing maintenance required.

Deployment-Ready DB Standards Enforcement

With Secure Developer features, enforcing database standards isn't left to chance or after-the-fact reviews. Standards are embedded into the developer's own tools and workflow, ensuring high quality and consistent changes from the very start.

Build customizable policies and enforcement built into your CI/CD pipeline.

Not supported in product

Manual effort and ongoing maintenance required.

Insider Threat Mitigation

With Liquibase Secure, insider threats are dramatically reduced: all schema changes are tracked, unauthorized edits are flagged, and drift is reconciled for true database governance.

Automated snapshots, baselines, and real-time reconciliation help keep every database secure, compliant, and trustworthy.

Not supported in product

Manual effort and ongoing maintenance required.

Risk Remediation and Recovery

With automated and custom rollback capabilities, teams can instantly undo bad deployments, minimizing downtime and reducing MTTR.

Liquibase Secure makes recovering from risky or breaking database changes fast and reliable.

Not available

Governance Reliability & Supply Chain Security

Liquibase Secure ensures your entire database delivery pipeline is secure and compliant by providing a full Software Bill of Materials (SBOM), rapid SLA-backed Common Vulnerabilities and Exposures (CVE) patching, and expert support.

Verify component integrity, minimize risk, and meet supply chain security standards.

Not available

Gain Full Visibility & Control Over Every Change

Visibility & Continuous Improvement

With Liquibase Secure, teams gain end-to-end visibility for risk troubleshooting and continuous improvement—ensuring the database is as observable and adaptable as the rest of your stack.

Get actionable observability tailored for database change management.

Not supported in product

Manual effort required.

Risk Remediation and Recovery

With automated and custom rollback capabilities, teams can instantly undo bad deployments, minimizing downtime and reducing mean time to recover—no manual scripts or database restores required. It's recovery built into every release, so incidents are resolved quickly and confidently.

Liquibase Secure makes recovering from risky or breaking database changes fast and reliable.

Manual effort required

Logging & Reporting

Liquibase Secure captures detailed, structured logs for every database change. These structured logs and reports support audits, compliance checks, and can be integrated into existing dashboards and Security Information and Event Management (SIEM) tools for continuous monitoring.

Advanced Operational Insights

Structured logging, dashboards, and reports for audits, compliance, and monitoring.

Basic Logs

Track applied changeSets in database tables.

Reduce Downtime & Accelerate Safe Releases

Drift Detection

Liquibase actively monitors for drift—differences between environments or between deployed databases and tracked changelogs. When drift is detected, teams can receive integrated alerts, and can reconcile deviations by either updating code or rolling back unauthorized changes.

Advanced Drift Detection

Customers can automate scans and proactively monitor changes, support alerts, and address schema drift before it impacts releases.

Basic Drift Awareness

Run manual diffs between two database states.

Policy Enforcement

Liquibase Secure can detect unauthorized schema changes by taking snapshots and comparing them to authorized changelogs in version control. If a schema change appears in Production outside an approved deployment (an out-of-band change), Liquibase Secure flags it immediately.

Policy Guardrails

Apply default + custom rules to block risky operations before deployment.

Not available

Rollback

When a deployment goes wrong, whether it causes downtime, data corruption, or unexpected behavior the first question is: how do we quickly and safely get back to a stable state? With auto-generated and custom-defined rollback scripts for deployed changelogs, teams are always one command away from recovering the database to its last known good state, even during emergencies. Liquibase employs a practice for production model to make sure a team can minimize downtime.

Granular Rollback

Undo individual ChangeSets for precise recovery.

Basic Rollback

Revert the last change or roll back to a specific point in time.

Increase Developer Productivity & Remove Roadblocks

Liquibase Secure Developer, our new VS Code extension

Create Liquibase resources such as changelogs, changesets, changetypes, and more directly inside the IDE developers already use every day. Once resources are created and customized, they can test run operations, apply security policies, and check audit trails before moving code into automated pipelines.

Liquibase Secure Developer

Makes building and testing database operations feel as natural as writing application code.

Traditional

Utilizes the CLI

Object Support

From tables and indexes to functions, triggers, and stored procedures, Liquibase Secure tracks and manages changes across a full range of database objects. This ensures complete visibility and control, not just over schema but over all database assets critical to application stability.

Advanced

Access the full set of capabilities from each database for more flexibility and automation.

Basic

Execute basic database migrations with manual configuration and setup required.

Workflow Automation (Flow Files)

Flow files orchestrate end-to-end database changes. They enforce consistency, integrate safety checks, eliminate manual steps, and automatically capture rollback scripts and audit logs. Teams can standardize patterned deployments and workflows while reducing risk, increasing security and improving velocity.

Flows

Reusable pipelines for compliance, CI/CD, and release automation.

Manual

Manual scripting and ad-hoc execution.

Testing & QA

With open source, you're responsible for validating integrations and ensuring compatibility across your environments. With Liquibase, our team does the heavy lifting of continuous testing across supported databases, regression coverage, and ongoing product QA so you can focus on delivery.

Comprehensive

End-to-end test automation and validation integrated with database changes.

Basic

Basic unit and integration testing only.

Installation & Upgrade

Liquibase Secure makes setup and upgrades simple and reliable. With a one-step install that includes certified drivers, extensions, and integrations, teams can get up and running quickly. Every build is fully tested and certified for compatibility, and upgrades are guided to minimize downtime. SLA-backed patches and hotfixes ensure stability, while built-in configuration checks keep environments safe and consistent.

Easy & Seamless

- One-Step install with certified drivers, extensions, and integrations.
- Fully tested and certified builds for compatibility.
- SLA-backed patches, hotfixes, and guided upgrades with minimal downtime.

DIY Setup

- Extensions and drivers installed manually.
- Database and extension compatibility must be verified by the user.
- Community fixes with no SLA.

Get Dedicated Enterprise Support When It Matters Most

Support

Liquibase Secure provides enterprise-grade support to ensure safe and successful adoption. Customers have access to SLA-backed dedicated support, and technical account managers who understand the environment. From onboarding to troubleshooting, our team is committed to helping you achieve reliable, secure database change management.

Dedicated Support

SLA-backed dedicated support, technical account management, and Professional services for secure adoption.

Community-based Support

Community-based support (forums, GitHub).

Professional Services

Our professional services team can help accelerate results and deliver your database change management goals on time to keep you ahead of the market with guidance, expertise, and best practices.

Accelerate your goals with a true partner invested in your success.

Not available

Through Liquibase

Vulnerability Remediation SLA

Liquibase Secure provides a defined service level agreement (SLA) for addressing security vulnerabilities. Customers get clear timelines for fixes, proactive notifications, and guaranteed patch delivery, helping teams reduce exposure and maintain compliance.

Critical vulnerabilities patched and delivered within 14 days.

No SLA

Community-driven fixes.