DATAFORGE MCP SERVER

Security and Control Overview

Technical controls for governed AI-agent access to enterprise data engineering workflows.

Important: This document describes product-level technical controls. It does not claim or represent third-party security certification.

Control objective

DataForge lets external MCP clients and Talos operate the data platform without introducing a separate AI write path. Agent actions remain subject to identity, authorization, validation, confirmation, and operational-evidence controls.

Trust boundary

Customer data and processing remain in the customer-managed cloud. DataForge coordinates governed platform objects while execution runs on the customer's Databricks or Snowflake compute. MCP clients connect to the DataForge control plane and do not receive direct, privileged access to the customer's data plane through DataForge.

Control summary

Customer-controlled data plane Customer data and processing stay in the customer-managed cloud and run on customer Databricks or Snowflake compute.	**OAuth authentication** Interactive MCP clients use OAuth 2.1 with PKCE. Agents operate as an authenticated user rather than through a shared AI identity.
Authorization on every call Project roles and database-enforced permissions are checked when tools run.	**Save-time validation** Agent and human changes pass the same schema and expression validation before persistence.
Destructive-action confirmation Destructive operations require explicit confirmation enforced by the server.	**Read-only defaults** Read-only behavior is the default where applicable. SQL access to customer data is off by default until separately enabled by the customer.
Shared operational telemetry Talos and MCP clients use the same tool registry and telemetry model. Outcomes, latency, release version, and data shape can be recorded without logging customer values.	**No AI bypass** External agents do not receive reduced validation, broader permissions, or a forgiving write path.

Identity and access flow

1. The MCP client initiates OAuth authentication. 2. The user signs in through the normal DataForge identity flow. 3. The client receives time-bounded access. 4. Each project-scoped operation re-checks the user's role when the tool runs. 5. Destructive operations require an additional explicit confirmation.

Change-control path

An agent request is dispatched through the same DataForge tool registry used by Talos. A proposed change passes schema constraints, SQL-expression parsing, and role checks before it can persist. A rejected write returns structured recovery information to the agent. A successful write becomes a governed platform object with the same platform behavior as a human-authored change.

Data-access posture

Metadata access supports agent planning without requiring unrestricted customer-data access. Optional SQL access is separately controlled, off by default, and uses a dedicated read-only connection when enabled. Secrets and token fields are excluded or redacted from telemetry.

Operational evidence

The MCP server can record request outcomes, latency, release version, and the shape of arguments and results. DataForge uses this evidence to diagnose behavior across the governed tool surface while avoiding customer values in shape-only telemetry. Customers should confirm their required retention, export, and review procedures during architecture review.

Questions for your architecture review

- Which user roles may connect external MCP clients?
- Will optional SQL data access remain disabled or be enabled for specific workflows?
- Which destructive operations require organizational approval beyond server confirmation?
- What network, identity-provider, and session requirements apply to this deployment?
- What telemetry retention and review process does the organization require?
- Which Databricks or Snowflake environments and projects are in scope?

Request an architecture review
Bring your identity, network, compute, and AI-client requirements.

dataforgelabs.com/mcp/security
info@dataforgelabs.com

This overview is informational and reflects the product controls described by DataForge as of August 2026. Specific deployment configuration and contractual commitments should be confirmed with DataForge.