

Change Control Solution for Databases

Highlights

- **Enforces change control policies for your entire database environment** – including changes to critical structures, data, permissions, and configuration files – both inside and outside the database
- **Monitors all SQL changes (DDL, DML, DCL) non-invasively**, without impacting performance or requiring changes to databases or applications.
- **Enhances data security** by monitoring changes that undermine security, such as “logic bombs” planted by disgruntled employees.
- **Improves data governance** by detecting unauthorized or accidental changes that affect data integrity.
- **Provides separation of duties** by storing all audit information in a secure, tamper-proof repository.
- **Reduces operational risks from unauthorized change**, including unplanned downtime and introduction of security vulnerabilities
- **Increases IT efficiency** by automating change reconciliation and compliance workflows (audit report distribution and approvals, escalation processes, etc.)
- **Centralizes real-time, policy-based controls and auditing** for your entire database infrastructure (Oracle, IBM DB2 and Informix, Microsoft, Sybase).

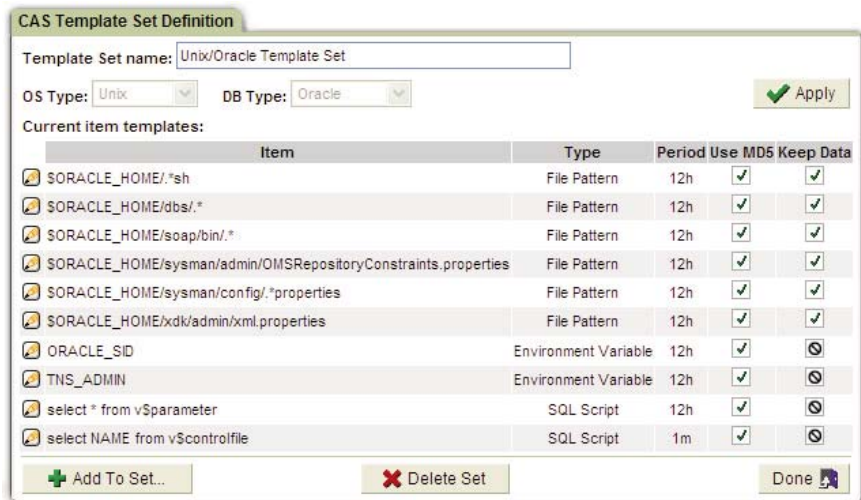
Most organizations have change control policies that govern how and when changes are made to production databases. Enforcing these policies, however, requires real-time, tamper-proof controls that can detect violations without impacting the performance or stability of your environment.

Guardium's *Change Control Solution for Databases* provides granular visibility into all changes to database objects – including database schemas, security permissions, data values, and external configuration files – without the performance and complexity drawbacks of database-resident utilities such as trace logs, transaction logs, or native auditing.

This practical, appliance-based solution allows you to easily automate the time-consuming process of tracking all database changes and reconciling them with authorized work orders, which is increasingly required to meet auditors' requirements (SOX, PCI, data privacy regulations, etc.).

You can also generate real-time, policy-based alerts whenever unauthorized changes are detected – such as changes made without change control IDs, during production periods, or using unauthorized user IDs – and optionally block them.

The result is effective protection from unauthorized activities by both trusted insiders and malicious outsiders, and enhanced data security, integrity, and availability for critical data and systems.



- > **Monitors all database changes, including changes to configuration files:** *Change Control Solution for Databases* provides granular visibility into changes to all database objects – including database structures, permissions, data, and configuration files. This screen shot shows configuration files, environment variables, and shell scripts that are monitored because changes could represent a security threat to the database. To accelerate implementation, the solution ships with a series of pre-configured templates for all popular OS and database combinations.

Unified architecture for real-time database security and continuous fine-grained auditing

Change Control Solution for Databases is built on Guardium SQL Guard™, the most widely-used solution for database activity monitoring, security, and auditing.

The Guardium architecture monitors database activities by continuously analyzing all SQL network traffic as well as local privileged user access (console, shared memory, named pipes, etc.).

Guardium's change control system consists of the following components:

✓ **Hardened Linux-Based Appliance:** Built on an industry-standard, high-performance 1U server, the appliance can typically hold 3 to 6 months of detailed audit information. To support separation of duties and create a verifiable audit trail, there is no root access to the appliance and all audit data is encrypted when archived to external storage devices (e.g., EMC Centera, Tivoli Storage Manager, and other archiving systems).

✓ **Change Auditing System (CAS):** Monitors changes to external database configuration objects such as:

- Configuration files (e.g., which ports are being used)
- Environment/registry variables (e.g., is encryption enabled)
- OS files
- Shell scripts
- Executables (Java, etc.)

To accelerate implementation, the solution ships with a series of pre-configured templates for all popular OS and database combinations.

✓ **AuditGuard:** Automates compliance auditing processes, including aggregation and normalization of audit information across multiple database platforms and locations, scheduled report distribution to oversight teams, and electronic sign-offs. Supports information sharing with external systems such as change management tools (Remedy, Peregrine, in-house solutions, etc.), enabling IT to automatically create reports that compare actual database changes with approved work orders.

✓ **HealthGuard:** Performs a network auto-discovery of the entire database environment (users, applications, database instances, tables, servers, etc.) and creates an interactive map with drill-down capabilities. Helps quickly identify both authorized and unauthorized users, applications, and databases.

Why native logging utilities are impractical for database change control

Database-resident functions such as trace logs, transaction logs, and native auditing, are impractical for five important reasons. They:

- Can easily be disabled by privileged users such as database administrators
- Provide limited audit information about the who, what, when, and where of database changes
- Require modifications to database configurations (which vary by database platform)
- Degrade the performance of critical production systems
- Cannot identify end-users who change data via server-based applications such as SAP and Oracle EBS, because these applications "pool" user traffic into a single stream that uses a common, generic ID to access the database

Timestamp	TICKET	Full Sql	BUS UNIT	APPROVER ID	DESCRIPTION
2007-01-22 20:03:29	CHANGE REQUEST 23	create table t3(i int)	HR	4612	Change security attributes per terminated employee cycle
2007-01-22 20:03:29	CHANGE REQUEST 23	drop table t3	HR	4612	Change security attributes per terminated employee cycle
2007-01-22 16:47:51	CHANGE REQUEST 22	drop table t2	FINANCE	7984	Add table for RIMS application
2007-01-22 16:47:47	CHANGE REQUEST 22	create table t2(i int)	FINANCE	7984	Add table for RIMS application

Records: 1 To 4 From 4

> **Integration with Change Management Systems:** Guardium's solution automates change reconciliation by comparing all detected changes with authorized change requests from deployed change management systems such as BMC Remedy, HP-Peregrine, and custom applications.

✓ **PolicyGuard:** Creates enterprise-wide policies for database access control, change control, and security exceptions (e.g., failed logins). Using drop-down menus, policies can be easily customized to provide a range of responses including real-time alerts, blocking, detailed logging, and custom actions. To simplify implementation, PolicyGuard automatically suggests policies via a “learning mode” that analyzes all monitored traffic and automatically filters activities by number of occurrences, in order to identify anomalous or random events. By creating a baseline and identifying both normal business processes and what appear to be abnormal activities, the system automatically suggests policies you can use to enforce corporate controls.

Other available modules include:

- **Compliance Accelerators** for SOX, PCI, and data privacy laws: Libraries of pre-configured policies and reports using best practices controls consistent with guidelines of Big 4 audit firms.
- **End-User ID Monitoring** for positively identifying application user IDs associated with database queries and activities, for standard applications (Oracle EBS, PeopleSoft, SAP, etc.).
- **Central Manager**, a Web console for centralized management of configurations, policies, and audit reporting in distributed environments.

Monitors changes to:

- **Database structures** such as tables, triggers, and stored procedures
- **Critical data values** such as values affecting financial transactions
- **Security objects** such as users, roles, and permissions
- **External database objects** such as database configuration files, environment and registry variables, shell scripts, OS files, and executables (e.g., Java programs)

DML Change Control Reconciliation Report

Start Date: 2006-02-08 00:00:00 End Date: 2006-02-16 23:00:00

Timestamp	DB User Name	Event User Name	Event Type	Event Value Str	Sql	Total access
2006-02-15 19:22:18	FINANCE	Tom Smith - CPO	RECONCILE REQUEST	CHANGE 32	INSERT INTO FINANCE.CUSTOMER_DATA (FINANCE.CUSTOMER_DATA.FULL_NAME,FINANCE.CUSTOMER_DATA.ACCOUNT_NUMBER,FINANCE.CUSTOMER_DATA.MOTHERS_MAIDEN_NAME, FINANCE.CUSTOMER_DATA.SOCIAL_SECURITY_NUMBER,FINANCE.CUSTOMER_DATA.ADDRESS1,FINANCE.CUSTOMER_DATA.CITY, FINANCE.CUSTOMER_DATA.STATE,FINANCE.CUSTOMER_DATA.ZIP) VALUES (?,?-?-?-?,?-?-?-?,?-?-?-?,?-?-?-?)	1

Records: 1 To 1 From 4

Unreconciled DDL Activity

Start Date: 2006-02-01 00:00:00 End Date: 2006-02-15 23:00:00

Timestamp	DB User Name	SQL Verb	Sql	Count
2006-02-09 20:41:58	Conference Room	CREATE TABLE	CREATE TABLE dbo.test_table { [1] char(?) NULL, [2] bigint NULL, [4] char(?) NULL } ON [PRIMARY]	1
2006-02-10 03:55:27	SA	CREATE TABLE	CREATE TABLE dbo.Customers { [Customer Name] char(?) NULL, [Phone number] char(?) NULL, [Contact] char(?) NULL } ON [PRIMARY]	1
2006-02-10 14:44:47	SYS	ALTER TABLE	ALTER TABLE "FINANCE"."CUSTOMER_DATA" MODIFY("ADDRESS2" NULL, "FAX" NULL)	1

Records: 1 To 3 From 38

Unreconciled DML

Start Date: 2006-02-10 17:00:00 End Date: 2006-02-16 00:00:00

Timestamp	DB User Name	SQL Verb	Sql	Total access
2006-02-10 17:17:39	Conference Room	DELETE	create procedure dbo.dt_droppropertiesbyid @id int, @property varchar(?) as set nocount on if (@property is null) or (@property = ?) delete from dbo.dtproperties where objectid=@id	2
2006-02-10 17:17:39	Conference Room	DELETE	create procedure dbo.dt_dropuserobjectbyid @id int as set nocount on delete from dbo.dtproperties where objectid=@id	1

Records: 1 To 2 From 22

> **Auto-Reconciliation of Database Changes.** *Change Control Solution for Databases* tracks all changes to database schemas and associates detected changes with standard change request IDs. It thus provides full audit visibility into changes that were actually executed, down to the SQL statement level. In addition, via policies, it automatically identifies exceptions to the change control process in real-time.

Audit Process Definition

Description [View](#) [Run Once Now](#)

Active *There is no schedule associated with this process*

Keep for a minimum of **days or** **runs**

CSV File Label:

Receivers

	Receiver	Action Required	To-Do List	Email Notification
<input checked="" type="checkbox"/>	auditor John Smith	<input type="radio"/> Review <input checked="" type="radio"/> Review and Sign	<input checked="" type="checkbox"/> Add	<input checked="" type="radio"/> No <input type="radio"/> Link Only <input type="radio"/> Results
+ Add	<input type="text" value="-----"/> <input type="button" value="v"/>	<input checked="" type="radio"/> Review <input type="radio"/> Review and Sign	<input checked="" type="checkbox"/> Add	<input checked="" type="radio"/> No <input type="radio"/> Link Only <input type="radio"/> Results

Audit Tasks

[+ Report: DML Reconciliation Report \[DML Reconciliation Report\] {now -7 day to now}](#)

[+ Report: Unreconciled DDL \[Unreconciled DDL\] {now -7 day to now}](#)

[+ Report: Unreconciled DML \[Unreconciled DML\] {now -7 day to now}](#)

[+ Add Audit Task](#)

Roles

No roles have been assigned to this Process [Roles...](#)

[Back](#) [Remove](#) [Clone](#) [Comment](#) [Modify Schedule...](#) [Save](#) [Done](#)

> **Increases IT efficiency:** Guardium's solution increases IT efficiency by automating report generation, change reconciliation and compliance workflows (audit report distribution and approvals, escalation processes, etc.).

About Guardium

Guardium, the database security company, develops the most widely-used solution for database activity monitoring, security and auditing. Founded in 2002, Guardium was the first company to address the core data security gap by delivering a practical, appliance-based platform that both protects databases in real-time and automates the entire compliance auditing process. The company's blue-chip customer base includes organizations in all major geographies and industries.

Guardium's investors include Cisco Systems and leading venture capital firms. The company has partnerships with IBM, EMC, HP, Microsoft, Oracle, and Sybase, and is a member of IBM's prestigious Data Governance Council.