

IDERA

SQL Compliance Manager

Getting Started Guide

From purchase to productive — faster than you think.



What It Does



Installation



Your First Win



Alerting & Reports



Week-by-Week Plan

What Is SQL Compliance Manager?

Audit, alert, and report on your SQL Server estate — all from one place.

SQL Compliance Manager is a secure, lightweight auditing and reporting solution for Microsoft SQL Server. It answers the most important compliance question:

"Who did what, when, where, and how -- across every SQL Server in your environment."

Originally built in partnership with Ernst & Young to deliver exactly what auditors need. Average performance overhead is typically less than 5% -- no changes to SQL Server files or services.

<5%

Average performance overhead on audited SQL Servers — granular filtering keeps it that way.



Audit

Track logins, schema changes, SELECT/DML on sensitive tables



Alert

Get notified via email, SNMP, or Windows Event Log in real time



Report

Pre-built templates for HIPAA, PCI DSS, SOX, GDPR, and more

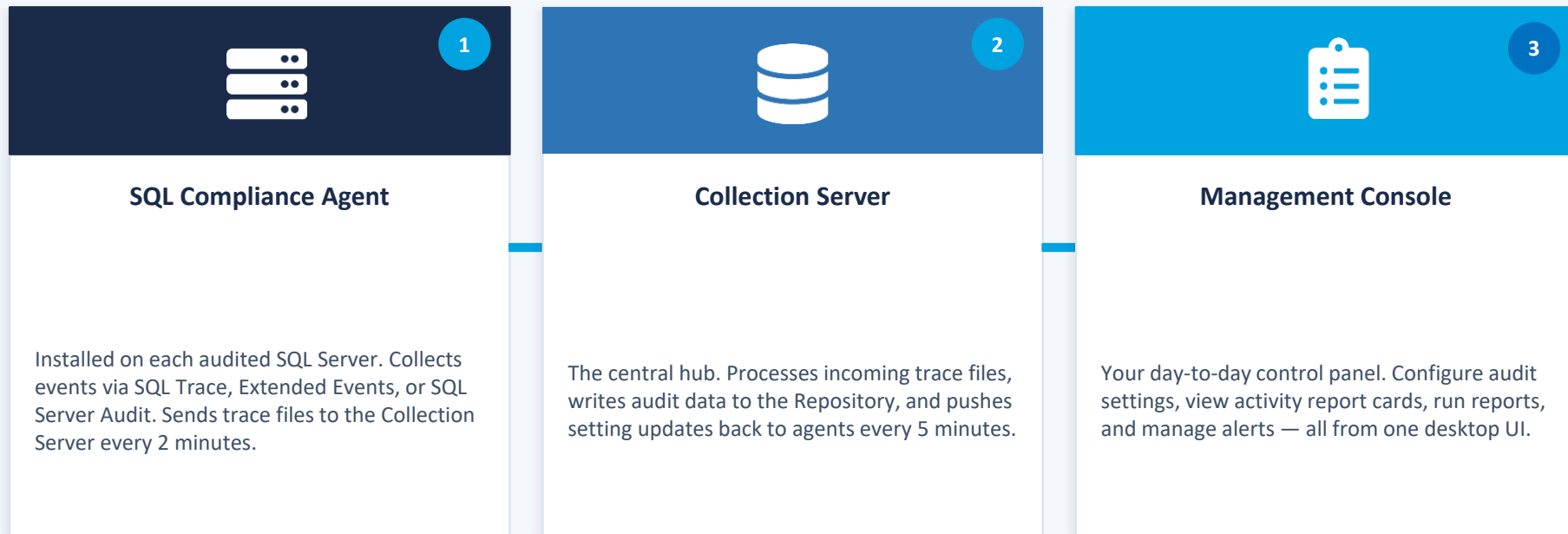



Protect

Tamper-proof repository ensures auditors trust your data

How It Works

Three lightweight components — nothing installed inside SQL Server itself.



 *SQL Compliance Manager runs entirely outside SQL Server processes and never modifies your SQL Server files or services.*

Before You Install

Check these items first and setup is smooth.

OS & .NET

- .NET 4.6.2 installed on the Collection Server machine
- .NET 4.0 on each SQL Server you plan to audit
- .NET 3.5 for the SQL Compliance Agent

SQL Server

- Collection Server SQL instance version \geq highest audited SQL Server version
- SQL Server 2008 R2 through SQL Server 2022 supported
- Amazon RDS supported as an audited instance (not for hosting the Repository)

Account

- Windows account for the Collection Service and Agent services
- Account needs 'Log on as a Service' rights (installer grants this automatically)
- Admin rights on the machine running the installer

Network

- Agents communicate to Collection Server every 2–5 minutes (outbound)
- Open required ports between audited servers and Collection Server
- Web browser (Chrome, Edge, Firefox) for the IDERA Dashboard web console

Installing SQL Compliance Manager

Typical setup installs all components in one pass.

1 Run the Installer

Log on with admin rights. Run SQLCMInstall.EXE from the installation kit. Click SQL Compliance Manager on the Quick Start window.

2 Choose Setup Type

Select Typical to install the Collection Server, Repository, Agent, and Management Console together. Custom lets you separate components across machines.

3 Configure the Repository

Point the installer at the SQL Server instance to host your audit data Repository. The setup program creates the Repository databases automatically.

4 Set Service Accounts

Enter the Windows account that will run the Collection Service and Agent. The installer automatically grants 'Log on as a Service' to this account.

5 Deploy Agents to Targets

After setup, use the Management Console to deploy agents to additional SQL Server instances you want to audit. Agents can also be deployed silently via MSI.

6 Register with Dashboard

The IDERA Dashboard provides a web console for browser-based access. Register locally (same machine) or point to an existing Dashboard installation.

Your First Win in Under an Hour

Get a SQL Server registered, auditing, and showing data — today.

1



Register a SQL Server

Open the Management Console. Right-click Audited SQL Servers and select Register SQL Server. Enter the instance name and service account credentials.

2



Apply a Compliance Preset

Pick a regulation template (e.g. HIPAA, PCI DSS, SOX) from the built-in library. SQL Compliance Manager pre-configures what events to audit — no manual event-picking required.

3



Select Databases to Audit

Choose which databases on that instance should be audited. You can start with one production database and expand later.

4



Check the Activity Report Card

Click the server in the Explore Activity tree. You'll see an Activity Report Card showing up to 30 days of events, statistics, and short-term trends — within minutes of setup.

What SQL Compliance Manager Does for You

The capabilities that make the biggest difference for DBAs and admins.



Regulation Templates

One-click configuration for HIPAA, PCI DSS, SOX, GDPR, CIS, DISA STIG, FERPA, NERC. Templates set event filters automatically.



Sensitive Column Tracking

Flag columns containing PII, payment data, or SSNs. Any unauthorized access is captured and flagged instantly.



Real-Time Alerts

Rules trigger alerts on suspicious events — unauthorized backups, privilege escalation, failed logins. Notify via email, SNMP, or Windows Event Log.



Pre-Built Compliance Reports

Generate audit-ready reports from built-in templates. Publish via SQL Server Reporting Services for self-service auditor access.

Privileged User Auditing

Track all DBA and sysadmin activity separately from regular users. Self-auditing logs what SQL CM admins change in the tool itself.



Deep Audit Capture

Capture before-and-after DML record values, full SQL statements executed, and transaction status (Begin, Commit, Rollback). Tamper-proof storage with integrity checks.

Common Mistakes to Avoid

A few setup decisions that are easy to get wrong — and how to get them right.



Auditing everything on day one



Start with one or two high-priority databases and one regulation template. Expand after you've validated event volume and storage usage.



Collection Server SQL version mismatch



The Collection Server's SQL instance must be the same version or newer than the highest audited SQL Server. A lower version causes collection failures.



Wrong service account permissions



The service account needs 'Log on as a Service' (auto-granted by installer) and read access to audited databases. Least-privilege, but complete.



Skipping the Activity Report Card



This is your fastest health check. If the report card shows zero events after 10 minutes, the agent likely isn't reaching the Collection Server.



Forgetting to archive old audit data



The Repository grows with every audited event. Set up regular archival via the CLI to keep the Repository lean and queries fast.

Best Practices for DBAs & Admins

What experienced users do to get the most out of SQL Compliance Manager.

Start with a Template, Then Tune

Regulation templates are your fastest path to coverage. After a week, review the audit volume and remove event types that are generating noise without compliance value.

Set Alerts Before You Need Them

Configure alerts for failed logins, privilege escalation, and sensitive column access from day one. Alerts are only useful if they're in place before an incident occurs.

Schedule Reports for Auditors

Use SQL Server Reporting Services to publish reports on a schedule. Give your auditors read-only access so they can self-serve — this dramatically reduces DBA time spent on audit requests.

Enable Self-Auditing (Trusted Source)

Turn on console change tracking so that SQL CM admin activity -- what settings they enable or disable -- is itself logged. Auditors will ask whether the audit tool itself is audited.

Use the CLI for Maintenance

Automate archival and grooming tasks using the command-line interface. Keeping the Repository lean (archive data older than 90 days) maintains query performance.

Audit Privileged Accounts Separately

Create a dedicated audit rule for sysadmin and db_owner accounts. Tracking DBA activity separately from application user activity makes it easier to spot anomalies.

Real-World Use Cases

How teams like yours are using SQL Compliance Manager every day.

Healthcare

HIPAA

Situation:

A hospital DBA team needed to prove that only authorized roles accessed patient data in their EHR database.

How:

Applied the HIPAA template to the EHR SQL Server, enabled Sensitive Column tracking for patient ID and date-of-birth columns. Generated the HIPAA Audit History report for their quarterly compliance review.



Audit prep time cut from days to hours.

Financial Services

SOX / PCI DSS

Situation:

A bank's compliance team needed evidence that database changes were authorized and logged before their annual external audit.

How:

Configured schema change auditing and privileged user tracking on all production SQL Servers. Set up automated daily reports delivered to the compliance team via SSRS.



External auditors accepted the reports directly — no manual data pulls.

Retail

PCI DSS

Situation:

A retailer processing card payments needed to demonstrate that cardholder data columns were never accessed outside of business hours.

How:

Enabled Sensitive Column auditing on payment tables and set up an alert rule firing on any SELECT of those columns outside 8am–6pm on weekdays.



First after-hours access attempt alerted within minutes of the event.

Your First Month — Week by Week

A realistic ramp-up plan for DBAs and admins.

Week 1



Install & First Audit

- Install Collection Server, Repository, and Management Console
- Register your most critical SQL Server instance
- Apply one regulation template (HIPAA, PCI, SOX)
- Verify the Activity Report Card shows live events
- Deploy agent to one additional server

Week 2



Alerts & Sensitive Data

- Enable Sensitive Column tracking on PII or payment tables
- Configure alert rules for failed logins and privilege escalation
- Set up email notifications for high-priority alerts
- Register additional SQL Servers to the audit scope
- Review alert noise — tune or suppress non-actionable events

Week 4



Reports & Steady State

- Generate your first compliance report from a built-in template
- Schedule automated reports via SQL Server Reporting Services
- Set up archival schedule via CLI to manage Repository growth
- Share read-only auditor access to the web dashboard
- Document your audit scope and alert configuration

Helpful Resources

Everything you need is a click away.



Product Wiki

wiki.idera.com/display/SQLCM

Full documentation, how-to guides, architecture details, and release notes.



Getting Started Guide

idera.com/lp/gettingstartedguides/sql-compliance-manager

Idera's official getting started document — deep dive on features and configuration.



Product Page

idera.com/products/sql-compliance-manager

Latest version info, free trial download, and feature overview.



Customer Portal

idera.com/support

Access your license, download updates, and submit support tickets.



Release Notes

wiki.idera.com/display/SQLCM/Release+Notes

Stay current on new features, fixed issues, and known limitations.



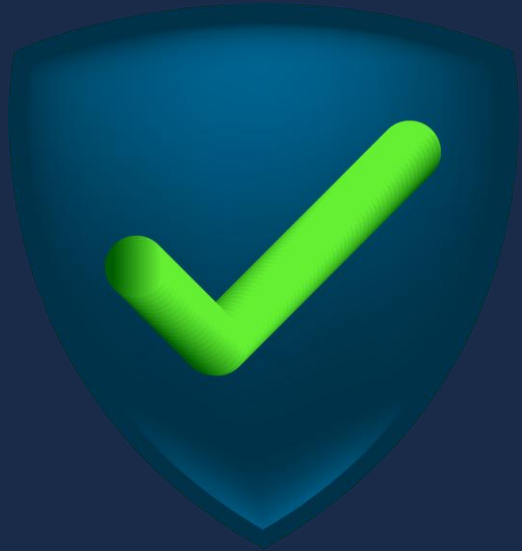
Free Trial

idera.com/products/sql-compliance-manager

Two-week fully functional trial — includes all features, no credit card needed.

You're ready.

Your SQL server estate is about to become a whole lot more auditable with SQL Compliance Manager.



Install the product and register your first SQL Server



Apply a regulation template and validate the Activity Report Card



Reach out to Idera support — they're here to help

IDERA

Idera · Helping teams build, manage, and protect data for over 25 years.