

# CA Enterprise Log Manager r12.1

CA Enterprise Log Manager is designed to simplify IT security activity compliance reporting and investigations. It collects, normalizes and archives activity logs from multiple sources and provides search, analysis, reporting and alerting capabilities to reduce the cost and complexity of proving compliance. Overall, the solution helps improve your security, risk management and IT operations.

## Business Value

Collecting, storing and reviewing activity log data for extended time periods is not only a compliance mandate for many organizations, it is a best practice that helps improve security risk management and IT operations. To effectively comply with these requirements, you must have an automated and repeatable process for identifying and addressing policy and controls violations. When faced with a breach, you'll want to know who did what, when - and fast. Log management can quickly provide answers and efficiently generate a complete record of all system activity - helping you better provide external auditors and other internal stakeholders with the information that they need, when they need it.

## Product Overview

CA Enterprise Log Manager automates log collection, normalization and archiving across your IT environment. It is designed to streamline IT activity compliance audits with preconfigured reports and interactive, multidimensional log analysis tools. It delivers rapid time-to-value with a soft-appliance model that is easy to deploy and manage, all while helping to improve your overall security posture.

## Delivery Approach

CA Services provides a rapid implementation service for CA Enterprise Log Manager delivered through CA internal staff and a network of established partners chosen to help achieve a successful deployment and realize the desired business results as quickly as possible. Through our proven nine-stage methodology, best practices and expertise, CA can help you achieve faster time-to-value for your product implementation.

## What's New

CA Enterprise Log Manager r12.1 delivers the following new key capabilities:

- **Transparent User Interface Integration** - CA Enterprise Log Manager provides quick and relevant investigation of IT activity launched in context from other products' interfaces. The ability to access CA Enterprise Log Manager reports and queries directly from leading CA Security products like CA Access Control and CA Identity Manager not only increases efficiencies, but also improves the user experience.
- **Network Operations Center Integration** - Incidents that affect network operations and service availability are forwarded to CA Spectrum and other network and systems management applications.



- Helpdesk Integration and Incident Response Automation - Control violations and other incidents are forwarded, tracked and documented through CA Service Desk or other enterprise help desk systems.
- Open Access to IT Activity Reports and Log Data - Access the embedded log store directly from web portals, mashups and external reporting utilities through standard ODBC/JDBC interfaces.
- Log Management for the Virtual Data Center - Get more out of your IT investment and reduce your data center costs by deploying CA Enterprise Log Manager r12.1 on VMware ESX server environments.

## Features

CA Enterprise Log Manager delivers key capabilities and features that help you automate and streamline current manual and resource-intensive log management processes.

- IT Activity Compliance Reporting - provides predefined and customizable reports mapped to common security auditing guidelines and compliance regulations (such as PCI DSS, SOX, HIPAA, FISMA, and more) that can be emailed or run on schedule or on demand.
- Multidimensional Log Analysis - delivers visual log analysis tools with drill down capabilities that speeds the identification of policy violations.
- High-performance Log Collection - collects logs from host operating systems, applications and devices at sustained high-event rates. Its federated architecture allows distributed log collection and querying, helping to provide the scale necessary to handle high-volume loads from numerous log data sources.
- Efficient Log Compression and Archiving - provides both online and offline log storage options and compresses logs by up to a 40:1 ratio, thus reducing log storage costs.
- Automatic Content and Program Updates - provides automatic content and program updates, including new compliance reporting templates, new queries, product integrations and more.
- Easy to Deploy and Manage Soft-Appliance - delivers a soft-appliance package of hardened OS, an embedded data store, and the CA Enterprise Log Manager software. It installs quickly to provide rapid value with agentless log collection, graphical search and analysis, and out-of-the-box queries and reports.
- CA Identity and Access Management and Mainframe Integration - provides secure, enterprise-wide collection, archiving and forensic query of all identity and access activities including logs from CA SiteMinder, CA Access Control, CA Identity Manager, CA DLP and more, as well as IT activities from mainframe systems.

## Benefits

Proof of Compliance, Simplified.

- Improve awareness of all IT security activities across your enterprise and streamline compliance audit tasks with out-of-the-box compliance reports and multidimensional log analysis tools, reducing the cost of proving compliance with regulations and internal policies.

Rapid Value. Lower Cost.

- Get results faster with a soft appliance that can be installed to generate compliance reports within an hour or less. Gain from lower total cost of ownership through centralized log management, embedded data store, and automatic, regular updates.

Identity Intelligence, Connected.

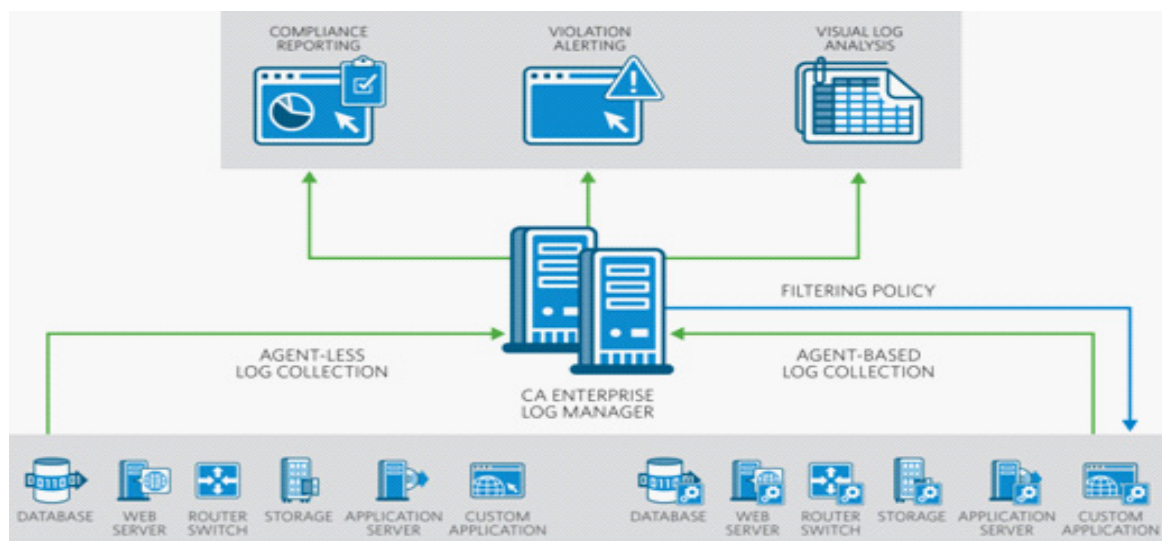
- Achieve transparent access to IT security activity reports and alerts from CA Access Control, CA Identity Manager, CA SiteMinder, CA DLP and other leading CA Security products, thereby improving your security investigation and risk mitigation efforts.

## Why CA

CA Enterprise Log Manager not only provides native and transparent access to IT security activity reports and alerts from CA Access Control, CA Identity Manager, CA SiteMinder, CA DLP and other leading CA Security products, but also integrates with other CA products in support of Enterprise IT Management (EITM). EITM is CA's vision for a dynamic and secure approach that integrates and automates the management of applications, databases, networks, security, storage and systems across departments and disciplines to help maximize the full potential of each. CA's comprehensive portfolio of modular IT management solutions helps you unify IT and simplify the management of today's complex computing environments across the enterprise for greater business results.

## How CA Enterprise Log Manager Works

CA Enterprise Log Manager implementations start with event log collectors that capture events from both managed and unmanaged event sources, which can include a variety of devices and applications. Captured events are normalized, classified and then inserted and stored in an embedded data store. The data store can be easily queried and used for visual log analysis and compliance reporting. If the query results indicate a possible policy violation, the data store will invoke an action.



Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only.