

# CA Audit r8

CA AUDIT STREAMLINES SECURITY EVENT CONSOLIDATION PROCESSES BY CENTRALLY AGGREGATING AND NORMALIZING SECURITY DATA ACROSS YOUR ENTERPRISE, AND HELPS YOU VERIFY COMPLIANCE USING EFFECTIVE LOG ANALYSIS AND COMPLIANCE REPORTING TOOLS.

## Overview

Today's organizations depend on audit data to provide proof of compliance with regulations. Not an easy task since security events come from different log sources, in inconsistent formats, and in massive volumes. CA Audit centrally consolidate, normalize, and store security events enabling IT professionals simplify compliance reporting and event monitoring processes.

## Benefits

CA Audit enables you to demonstrate compliance, reduce risk and reduce the cost and complexity of security event consolidation and monitoring operations.

## The CA Advantage

With CA Audit you can centrally consolidate, store and display security data in a modular fashion. This provides you with a lot of flexibility to deploy modular components as needed and optimally design your architecture without constraint of cost. CA Audit integrates with CA Identity & Access Management (IAM) solutions to provide rich analysis of "who did what", which is critical in delivering proof of compliance.

---

## CA Audit Simplifies Security Event Consolidation

As today's enterprise infrastructure expands to include more machines, devices and applications, managing security-related data has become an increasingly complex task. Multiply this by the events being generated by all other security-related solutions, each with their own proprietary data capture model. This disparate infrastructure of security systems and platforms utilizes different protocols and lacks central management and correlation capabilities, leaving an organization with mounds of data, but very little, in terms of valuable, useful information.

Additionally, with the rise in government regulations, organizations feel more pressured to meet stringent compliance requirements while documenting that they've implemented the correct security measures to comply with the regulation. In order to achieve this, they need to be able to provide intelligence and intuitive reporting to the vast amount of security data.

CA Audit enables organizations to collect, normalize and store enterprise-wide security related data to be used for auditing, reporting, compliance verification and event monitoring. CA Audit offers a scalable, centralized repository to store and analyze audit logs and security data from a diverse set of systems. Regardless of the event's source, through event normalization, CA Audit converts information into a common, intuitive format that facilitates quick analysis and reporting. Centrally managed policies are then applied to the centralized repository so that data retention rules can be enforced and alerts or additional actions can be initiated in response to the detection of suspicious activity, while ensuring availability of data for audit or compliance purposes.

CA Audit eliminates event guesswork by normalizing data to a common, intuitive format—regardless of the data's source. These intelligent agents allow organizations to normalize, aggregate, and filter at the source of the data, reducing network traffic and bandwidth, and securely communicating a delivery status to the audit server through encrypted communications. CA Audit's flexible architecture enables organizations to manage and view the audit data through its web-based user interface.

---

## Key Capabilities and Features

**CROSS-PLATFORM DATA COLLECTION** CA Audit collects data from an extensive variety of sources, including: operating systems, applications, network devices, security devices, mainframe, access control systems, web services, and more. CA Audit allows for central security event monitoring in heterogeneous environments from highly distributed and disparate networks, complex computing environments, LAN through the WAN, and wired networks through wireless networks.

**ALERT MANAGEMENT** Offers customizable support for creating policies that can be used to initiate alerts or other actions. Critical events can be filtered, logged and monitored through a log file, and actions such as email alerts, pages, etc. can be executed through established policies.

**POLICY MANAGEMENT** CA Audit defines your organization's central auditing policy and performs remote distribution of rules to the client from one central host. This policy-based approach provides security administrators with a powerful, easy-to-use centralized auditing solution. As part of its Policy Management engine, CA Audit provides a rich set of out-of-the box rules and rules templates that the customers can readily tap into. In addition, the user-friendly Rule Builder wizard allows for easy creation of new rules that are specific to their environment. CA continuously adds to this policy library and provides additional rules and templates that are easily downloadable through the administrator interface.

**CENTRAL SECURITY DATA REPOSITORY** Audit collects security data from a variety of sources and stores it in a central repository, built around a scalable relational database. This allows for easy access, viewing and reporting for historical and post-event analysis. Through the audit administrator web interface users can access the central repository from any location.

**REAL-TIME TOOLS FOR COLLECTION, VIEWING, AND REPORTING** Audit contains customizable viewers of security information that enables organizations to make information available to users that are relative to their role. CA Audit offers hundreds of out-of-the box reports and graph functions, making it easy to quickly analyze the security data collected. Integration with third party reporting tools is also available.

**FLEXIBLE ARCHITECTURE** Flexible and modular solution architecture and design allow CA Audit to easily integrate with a variety of technologies and third-party devices, and scale based on customer adoption and infrastructure growth. Further, this solution flexibility also allows CA Audit to perform consistently across the entire spectrum of computing/network environment ranging from desktops to the mainframe, local area networks through wide area networks, and wired networks through wireless networks. CA Audit closely integrates with complementary solution sets that CA provides within security management, such as CA Security Information Management, CA Identity and Access Management, CA Threat Management and Unicenter® solutions. Centralized, role based interface enables organizations to easily manage highly distributed data and solutions environment cost effectively, without the need to rearrange existing organizational responsibilities or workflows. CA Audit ensures secure collection and transmission of data through strong encryption methods.

**MULTI-LANGUAGE SUPPORT** CA Audit serves the global market by providing internationalization and enhanced language support for English, French, Italian, German, Spanish, Traditional and Simplified Chinese, Brazilian Portuguese, Korean, and Japanese. Third-party integrations are localized on a case-by-case basis.

## What's New in CA Audit

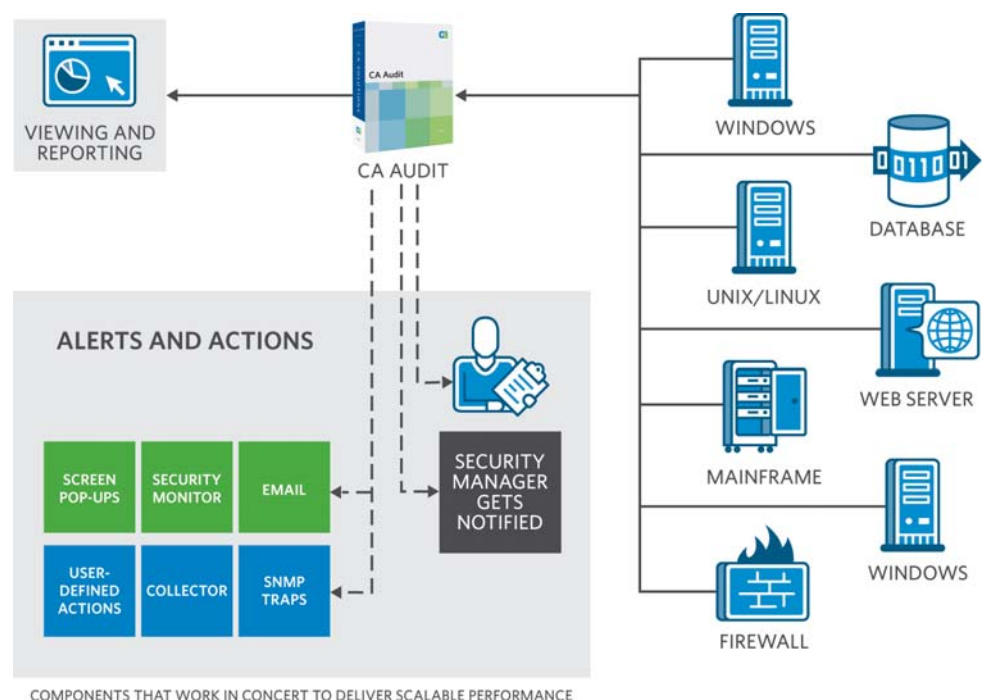
The main focus for CA Audit r8 is ease-of-use, localization, manageability and visualization. The primary new features and enhancements made are as follows:

- **Web-Based Interface** CA Audit is now accessible and administered through a standard web interface, making the system accessible from any desktop or laptop computer. The web interface is easy to navigate through, making it uncomplicated to learn and set up. In addition, new web interfaces for the CA Audit Policy Manager, Viewer and Reporter are now available.
  - Web-based Policy Manager Policy versioning allows new policies to be tested and approved before production use. In addition, the Policy Manager now allows for separation of policy maker, checker, and distribution duties.
  - Web-based Viewer and Reporter Easy access to the CA Audit Viewer and Reporter from anywhere without installing “thick clients” on analyst workstations.
- **Wizard-based Rules Creation** Extensive correlation and analysis tools provide out of the box value enabling quicker security implementation and faster ROI. With the easy to use wizard interface, you can easily access or download rule templates or create new rules to monitor and correlate events in your environment.
- **New Agent Support** CA Audit supports an increasing number of 3rd party solutions out of the box, giving you the ability to start auditing your environment right away. Event data is collected, normalized, aggregated and correlated either at source or within a distributed management hierarchy. It is also possible to configure CA Audit in an agent-less architecture or configure the generic agent to access log files.

FIGURE A

CA Audit implementations start with event recorders that capture events from both managed and unmanaged event sources, which can include a variety of devices or applications. Captured events follow a specific path as they are processed. Events are processed according to policies that you create, distribute, and manage from a central policy manager server. Certain events can trigger actions and alerts as defined by the rules you set. Other implementation scenarios make use of additional capabilities of CA Audit such as filtering and displaying events, monitoring security in near real-time, sending events to an SMTP server for email notifications, reporting and other management functions useful for compliance and status monitoring purposes.

HOW CA AUDIT WORKS



---

## Reduce Risk, Streamline Audit Process and Verify Compliance with CA Audit

CA Audit offers unique benefits to help your organization:

- Reduce risk through real-time data collection, consolidation and analysis of security data across the infrastructure.
- Streamline complex audit processes by providing centralized data collection, normalization, and consolidation across a variety vendors and technologies — allowing you focus on critical events in a time critical manner.
- Achieve government, industry and corporate regulatory/policy compliance, especially along with CA Access Control, by providing network, systems, and application level access control, auditing, data collection and reporting.

---

## The CA Advantage

CA Audit streamlines compliance related security event auditing processes and closely integrates with CA Identity and Access Management solution to deliver a broader view and reporting of enterprise security.

CA Audit is an integral part of CA's Security Information Management solution, and an important part of EITM — CA's overall approach to transforming IT management. CA unifies and simplifies IT management across the enterprise for greater business results.

CA Technology Services™ and our partners can help you assess your current IT situation, define your goals and implement solutions to gain measurable results. To keep your CA solutions operating at peak performance, CA support delivers unparalleled technical and customer support worldwide, and we offer training and certification through CA Education.

---

## Next Steps

CA Audit enables organizations to collect and store enterprise-wide security related data to be used for auditing, reporting, compliance verification and event monitoring. CA Audit offers a scalable, centralized repository that allows organizations to store and analyze audit logs and security data from a diverse set of systems. Organizations can use CA Audit to help meet regulatory compliance requirements by generating compliance-specific system audits and customized reports.

To learn more, and see how CA software solutions enable other organizations to unify and simplify IT management for better business results, visit [ca.com/customers](http://ca.com/customers).