



Global Compliance Solutions

ACCESS AUDITOR

Identity Compliance Made Simple

Access Auditor addresses the growing concern of user identity auditing and reporting. Designed from the ground up to meet security compliance requirements, Access Auditor automates the discovery, certification, and reporting of user access rights. Let Access Auditor streamline your compliance and governance initiatives:

Key Features

Discover Who Has
Access To What

Automate User Access
Rights Certifications

Enforce Separation
of Duties

Define and Manage Role
Definitions

Alert to Privilege
Changes

- ▶ **Consolidate enterprise-wide user privileges into a single repository**
- ▶ **Automate user access rights re-certification efforts with a simple and easy-to-customize workflow that maps to your business**
- ▶ **Initiate and track remediation efforts for inappropriate privileges**
- ▶ **Enforce separation of duties with cross-application rules that generate real-time alerts and reports**
- ▶ **Define and manage enterprise role definitions to highlight excessive user privileges not in a pre-defined role**
- ▶ **Issue proactive alerts to changes in sensitive privileges, users, or applications**

Consolidated View of Access Rights

Access Auditor discovers and imports access rights data from across the enterprise. Using a unique agent-less design, privileges from nearly any resource or custom application can be imported into Access Auditor. SCC's Identity Mapper then consolidates identities from disparate systems to give a unified view of each employee.

Access Auditor analyzes IT resources directly, retrieving its information from the system or application itself. It does not rely upon records maintained by any third-party tool and integrates with any identity management solution.

User Access Re-Certification

The heart of Access Auditor is a powerful certification engine that allows administrators to create multi-phase, customized approval workflows based on any number of user, role, or application criteria. Approvers are automatically notified when certifications are pending and progress is tracked to ensure completion.

Using SCC's workflow, re-certification efforts can now be distributed to managers and business owners across the organization. Access Auditor will automatically issue notification and reminders to keep the review process moving.

Separation of Duties

Separation of Duties (SOD) rules are a key component of any access rights control. Access Auditor provides a highly flexible SOD configuration engine. Any combination of user, role, or application data can be used to create cross-application conflict rules. SOD rules are then used in both reports and real-time alerts.

Compliance Reporting

All privileges discovered across the enterprise are correlated by both user and business application. Reports can show user profiles at any given time, summaries of current and historical reviews, status of certifications and remediation efforts, as well as real-time lists of users with access to specific privileges or applications.

Remediation Tracking

Privileges that are identified as inappropriate are flagged for removal, and remediation efforts are tracked within Access Auditor. Historical reports of certifications provide the evidence needed to show compliance with key user access controls.

CONTACT SCC

120 Village Square, Suite 76

Orinda, CA 94563

TEL: (866) 657-4550

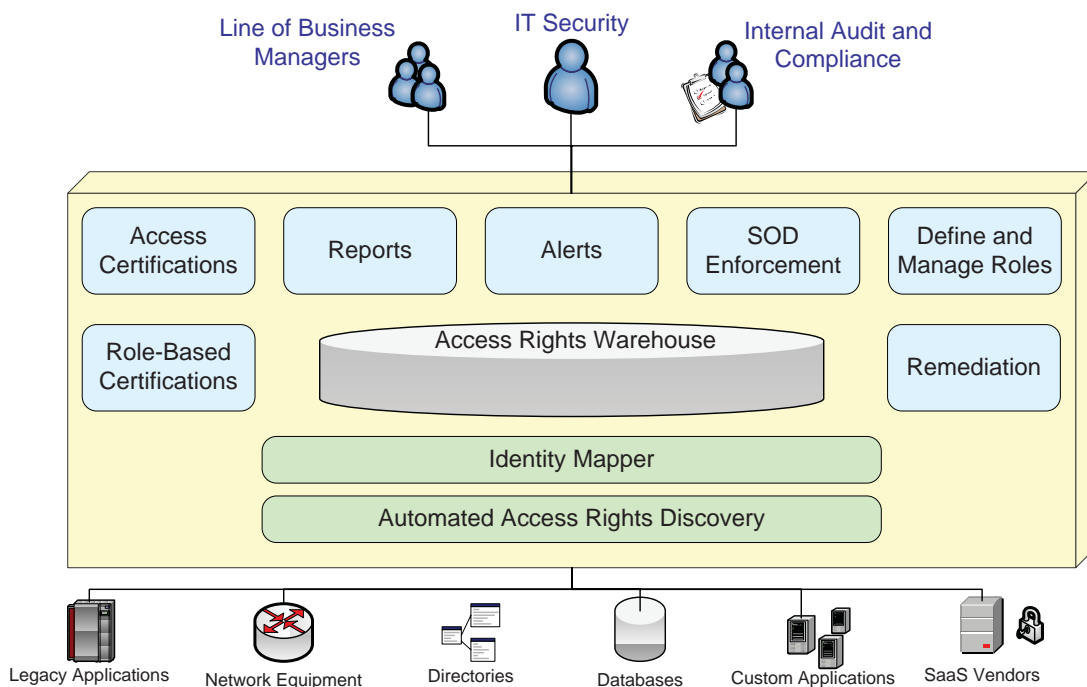
FAX: (925) 226-4692

WEB: www.securitycompliancecorp.com

EMAIL: info@securitycompliancecorp.com

ACCESS AUDITOR Key Features

| FEATURE | DETAILS | BENEFITS |
|---|--|--|
| Entitlement Reviews and Access Certification | <ul style="list-style-type: none"> Managers review and approve the access rights for their direct reports Business owners certify entitlements for all audited applications | <ul style="list-style-type: none"> Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 17799, and others) |
| Consolidated View of User Access Rights | <ul style="list-style-type: none"> Identity Mapper links user privileges from disparate systems Access data is organized by business application | <ul style="list-style-type: none"> Establishes a single repository of all access data across the entire enterprise Enhances understanding by relating privileges to applications that are familiar to users |
| Integration with Existing Systems and Processes | <ul style="list-style-type: none"> No agents required for deployment Compatible with all identity management products and data repositories | <ul style="list-style-type: none"> Accelerates deployment by minimizing impact to existing enterprise systems and applications Provides simple data import methods from both off-the-shelf and custom applications |
| Real-Time Alerting | <ul style="list-style-type: none"> System monitors for changes to user access data Simple interface for configuring custom alerts and actions | <ul style="list-style-type: none"> Generates alerts if access data has changed since the last audit scan Detects unauthorized changes to systems |
| Automated Discovery | <ul style="list-style-type: none"> User access rights and group memberships are automatically discovered and processed Support provided for wide variety of commonly used applications without product customization | <ul style="list-style-type: none"> Consolidates user data from diverse systems and groups by user and application Enables Access Auditor to provide a near real-time view of user entitlements |
| Role-Based Access Controls | <ul style="list-style-type: none"> Define and manage enterprise role definitions Certifications and reports based on user roles | <ul style="list-style-type: none"> Simplifies and streamlines access rights certifications Easily identify excessive user privileges not in a pre-defined role |
| Separation of Duties (SOD) | <ul style="list-style-type: none"> Create cross-application privilege conflict rules Report on violations to policies Alert administrators and business owners when violations are detected | <ul style="list-style-type: none"> Prevents fraud by limiting excessive privileges Enforces key SOD compliance controls Highlights individuals with inappropriate access rights |



ABOUT SCC

Security Compliance Corporation is the leader in identity compliance solutions. Founded by veteran Silicon Valley security executives, SCC delivers world-class solutions for automating user access rights certifications and enforcing separation of duties. SCC's customers include well-known brands in retail, healthcare, and financial services.

CONTACT SCC

120 Village Square, Suite 76
Orinda, CA 94563

TEL: (866) 657-4550

FAX: (925) 226-4692

EMAIL: info@securitycompliancecorp.com

WEB: www.securitycompliancecorp.com