SCC
Security Compliance Corp

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

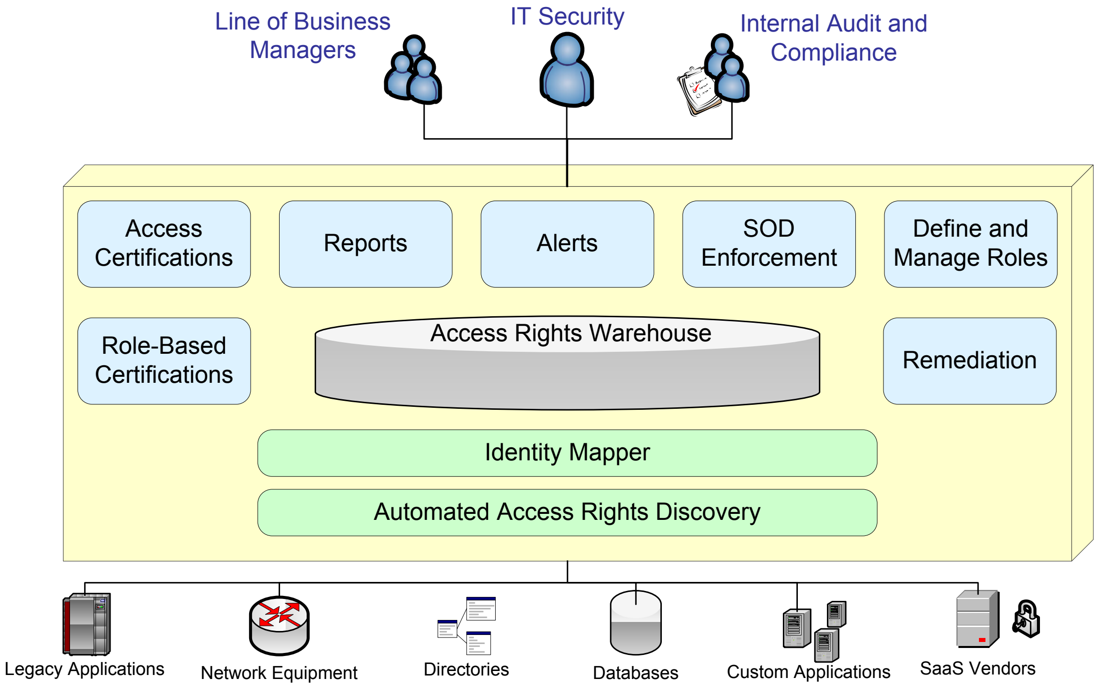
Privileges that are identified as inappropriate are flagged for removal, and remediation efforts are tracked within Access Auditor. Historical reports of certifications provide the evidence needed to show compliance with key user access controls.

CONTACT SCC

120 Village Square, Suite 76
Orinda, CA 94563
TEL: (925) 255-5686
FAX: (925) 226-4692
WEB: www.securitycompliancecorp.com
EMAIL: info@securitycompliancecorp.com

ACCESS AUDITOR Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers and business owners certify access rights with a simple web-based solution • Flexible rules-based workflow defines custom approvers at various phases of a certification	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 27001, PCI, and others)
Fuzzy ID and the Identity Mapper	• Link users from disparate applications even when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems even with no common attribute	• Solves one of IT's largest challenges, how to view access rights when no common attributes exist • Eliminates the need to modify applications to insert a unique identifier • Establishes a single repository of all access data across the entire enterprise
Role-Based Certifications and Role Definition Tool	• Define roles and role memberships • Perform certifications by roles and exceptions to improve accuracy and relevance • Perform what-if scenarios to define cross-application enterprise roles	• Improves relevance of certifications by reviewing a handful of roles instead of hundreds of privileges • Defines and manages roles by comparing role memberships and exceptions
Consolidated View of User Access Rights	• Custom reports show real-time and historical data • Orphaned user accounts from transfers and terminations are detected and reported • Historical record of access rights compliance	• Reveals users with inappropriate combinations of access rights • Discovers orphaned or lost user IDs • Provides documentary evidence of meeting access-related compliance controls
Real-Time Access and SOD Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions • Comprehensive cross-application separation of duties reports and alerts	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems • Warns business owners if users violate separation of duties rules
Automated Discovery	• User access rights and group memberships are automatically discovered and processed • Support provided for wide variety of commonly used applications without product customization	• 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



ABOUT SCC

Security Compliance Corporation's (SCC) Access Auditor® automates the periodic review and certification of user access rights and entitlements. SCC's workflow engine provides the ultimate flexibility in defining and managing the periodic attestation of user access rights. Founded in February 2005, Security Compliance Corporation is based in Orinda, CA.

CONTACT SCC

120 Village Square, Suite 76
Orinda, CA 94563
TEL: (925) 255-5686
FAX: (925) 226-4692
EMAIL: info@securitycompliancecorp.com
WEB: www.securitycompliancecorp.com