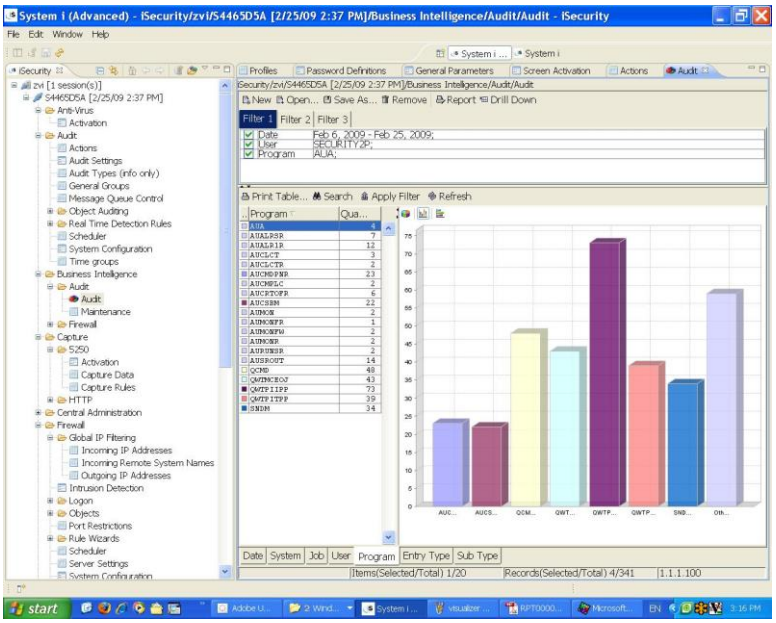
Compliance Pack

Comprehensive Compliance & Reporting Solution

The iSecurity Compliance Pack provides automatic and sophisticated reporting capabilities covering all types of security-related information, in all formats, for the System i server.

The Compliance Pack enables companies to meet the requirements of the Sarbanes-Oxley, PCI and HIPAA security regulations, as well as COBIT implementation guidelines. Automatic corrective actions further empower the pack.

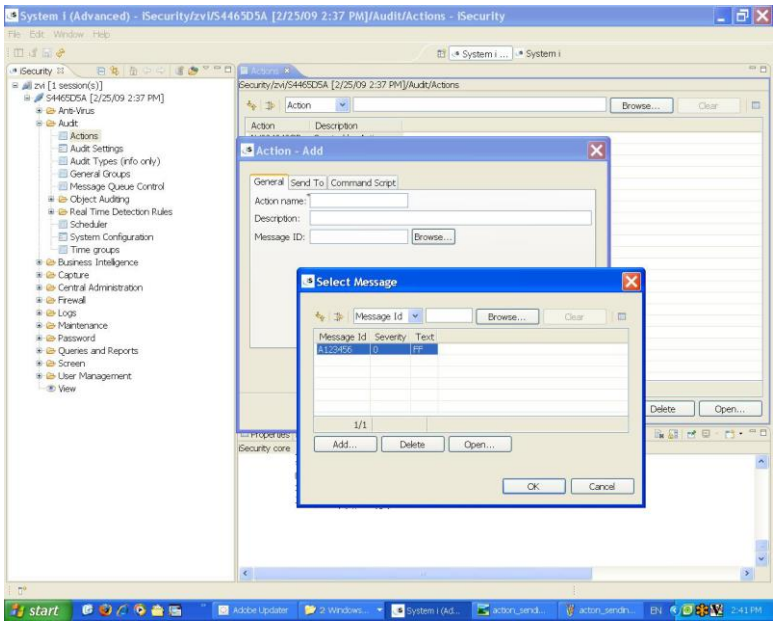
The Compliance Pack monitors and enforces compliance and security policy implementation for all System i resources, including unauthorized access to objects, network facilities, system values, application data, and more.



Visualizer for Audit Block Diagram Screen

Compliance Pack Features

- Supports SOX, HIPAA, PCI, and other compliance regulations
- Over 300 built-in queries and reports customizable to site policies and auditor specifications
- Advanced report generator for filtering records, setting sort and output fields, and printing reports in various formats
- Report Scheduler executes at user-defined times
- Allows for easy definition of automatic security alerts, including sending informative e-mails and operator, SMS or SYSLOG messages, and executing corrective programs and CL scripts
- Enables ongoing system-wide monitoring and tuning of resources
- Advanced business intelligence (BI) interface for intelligent investigation of suspicious events based on data extracted from the system audit journal (QAUDJRN)



Action – Sending Alert Messages Screen

iSecurity Compliance Pack Products

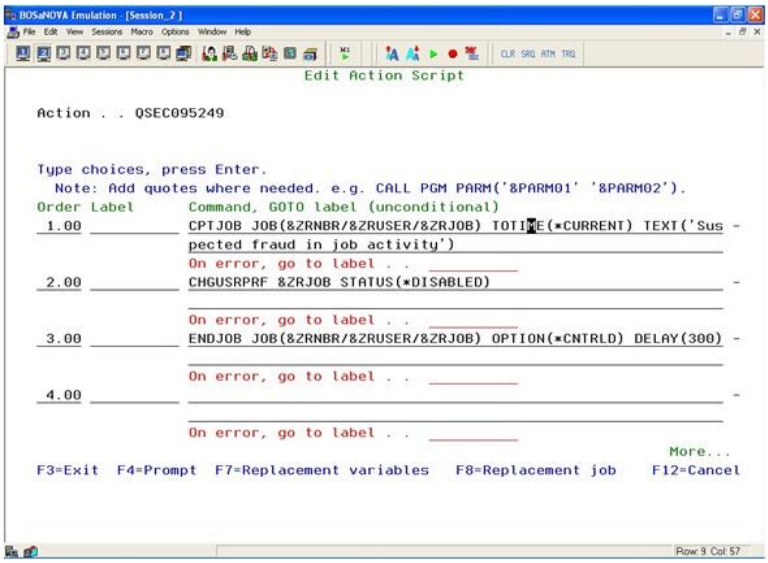
Audit - Examines user activity and object access in real-time, records the details in a history log, and triggers alerts and other actions in response to security threats. Audit enhances native System i auditing to help continuously evaluate the enforcement and effectiveness of security policies and procedures.

Visualizer for Audit - Provides at-a-glance graphic views of log data extracted by Audit from the system audit journal (QAUDJRN) and enables IT managers to drill-down to the relevant data and analyze suspicious security-related events. Visualizer uses business intelligence techniques to analyze large amounts of data without tying up system resources.

Action - Intercepts security breaches and other events in real-time and takes immediate corrective action, such as sending alert messages to Message queue, SMS or SYSLOG, or automatically executing a program or CL script.

System Control - Controls and monitors system resources, jobs, and message queues to enhance system stability.

Assessment - Comprehensive review of the server's security status including scores and improvement suggestions. The information is integrated into a historical database for subsequent system analysis, providing suggestions to correct any potential security breaches.



System Control – Edit Action Script Screen

Powered by RAZ-LEE