

Enforcive™ / Enterprise Security



End to End Security and Compliance Management for the IBM i Enterprise

Enforcive™/ Enterprise Security is the single most comprehensive and easy to use security and compliance solution for IBM i (AS/400). With over twenty fully integrated GUI-controlled security, auditing and compliance modules, this software suite enables system administrators, security officers and auditors to easily manage security and compliance tasks efficiently and effectively.



Security Lockdown

Access Control
User Profile Management
Object Authority



Auditing

Application Audit
File Audit
SQL Statement Audit



Compliance Management

Template-based deviation Control
Intrusion Detection System
Templates specific for SOX, PCI, Cobit 4.1



Reports Generator

Over 200 ready-to-run reports
Create and share reports automatically
Various file format options

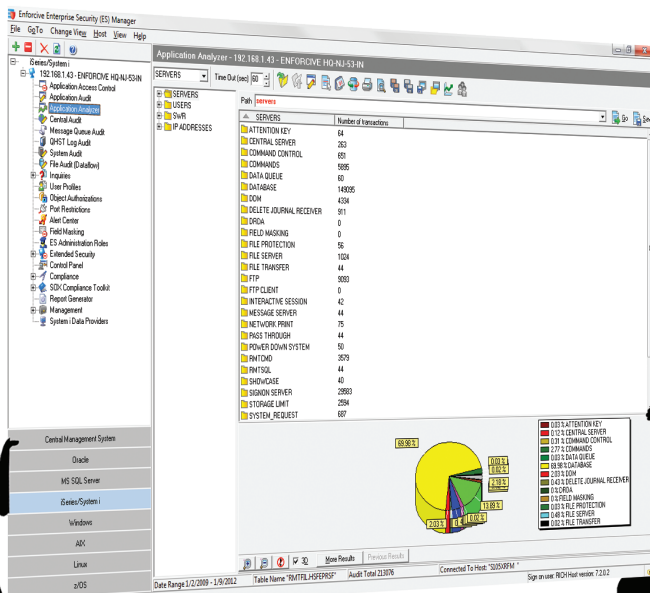
Managing Security: Beyond the Green Screen

In response to today's world of privacy breaches, complex regulatory requirements and evolving threats, Enforcive enables security officers to identify suspicious behavior on the network, drill down to the appropriate user, IP address or object and take appropriate action quickly. The enterprise-wide perspective that Enforcive provides significantly enhances current green screen reporting capabilities.

Multiple System Management

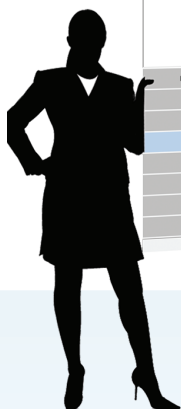
Managing security by grouping systems, significantly reduces reporting overload and simplifies enterprise level security policy implementation via:

- A common interface to manage multiple servers/partitions
- Access Control Policy Replication to remote systems
- A User Profile Propagation across systems
- Across-System Compliance reporting and auditing



Graphical User Interface: Empowering Security

Enforcive/Enterprise Security is fully GUI enabled. This allows security officers to easily roll out access management policies and makes journals and logs easy to manage and interpret. Security officers can monitor high-level policies enterprise-wide and drill down to the user or object in a matter of seconds. It also gives organizations the opportunity to involve "non-green screen" IT professionals in security related tasks.



Security Lockdown

Enforcive/ Enterprise Security provides piece of mind regarding external accessibility. Easily protect exit points, manage user profiles and implement group policies for all enterprise systems. Lockdown is first performed in “warning mode” to allow for the gathering of pertinent security events and reveal usage patterns. Once thorough analysis has been conducted, security lockdown and access control can commence through the use of the following modules:

Application Access Control

- Comprehensive exit point control incl. ODBC, JDBC, FTP, Remote Command, IFS, etc
- Flexible user profile and group permissions
- Exit Point based access management by IP address range
- Granular access management down to library, object, object group and IFS
- Account swapping for adopted authority for both the interactive and TCP/IP environments
- Replication of policies across multiple servers
- File protection that prevents power user access
- Securing commands - IBM, third party and custom commands **-New!**

User Profile Manager

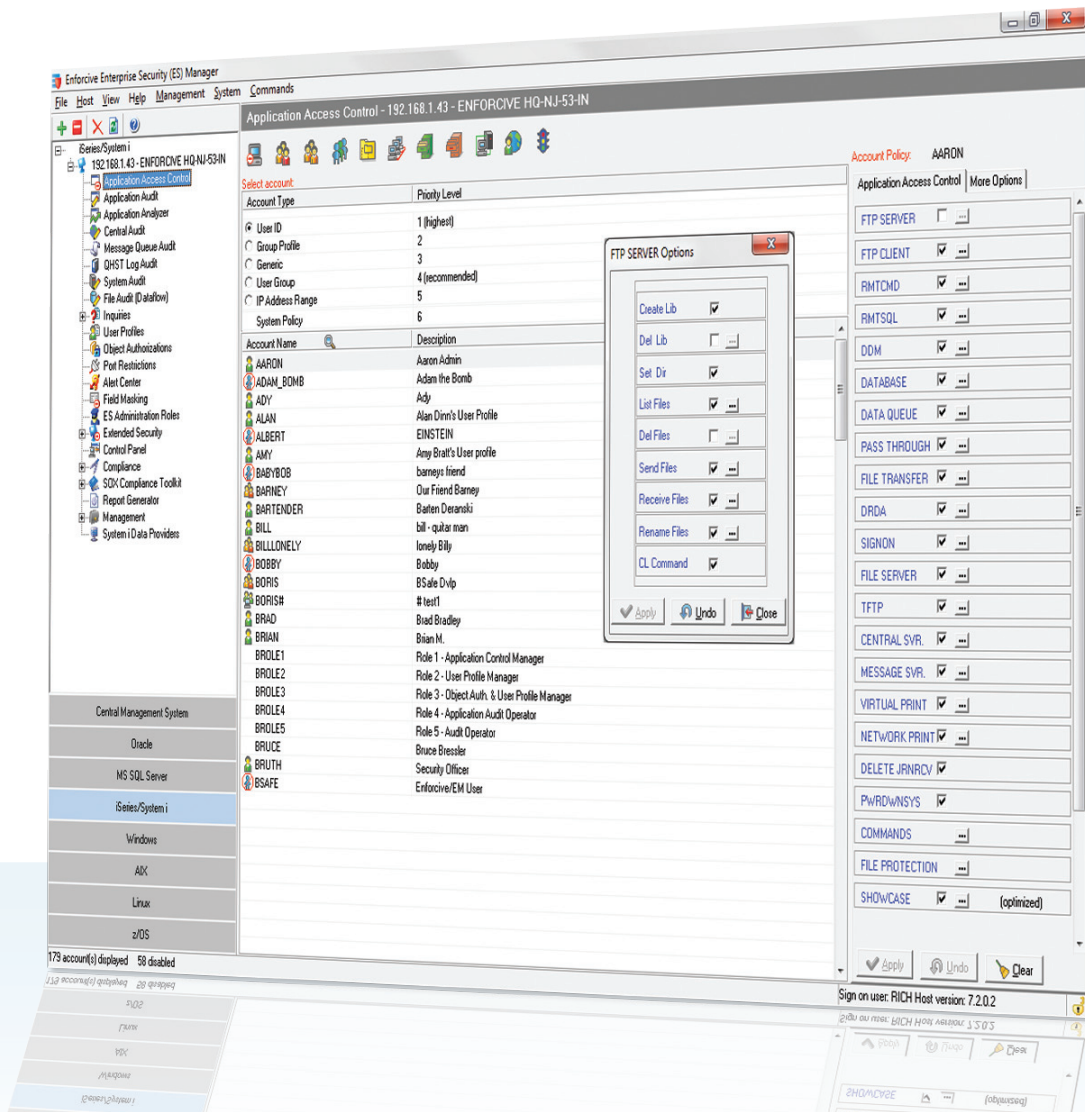
- Efficient and effective portal for IBM i user management
- Replication of User Profiles across servers/partitions
- Password Management

Object Authorization Manager

GUI-based control of native object authority

Session Time-Out & Inactive User Management

Capability to set session time-outs and policies for inactive users for different groups of users. In active user managements includes ad-hoc restoration of deleted user profiles.



Auditing

Powerful auditing and reporting capabilities offer a documented audit trail of your system's security definitions, events and activities with high granularity of user, IP address, object, field, etc. This is accomplished through the following functionality:

Application Audit

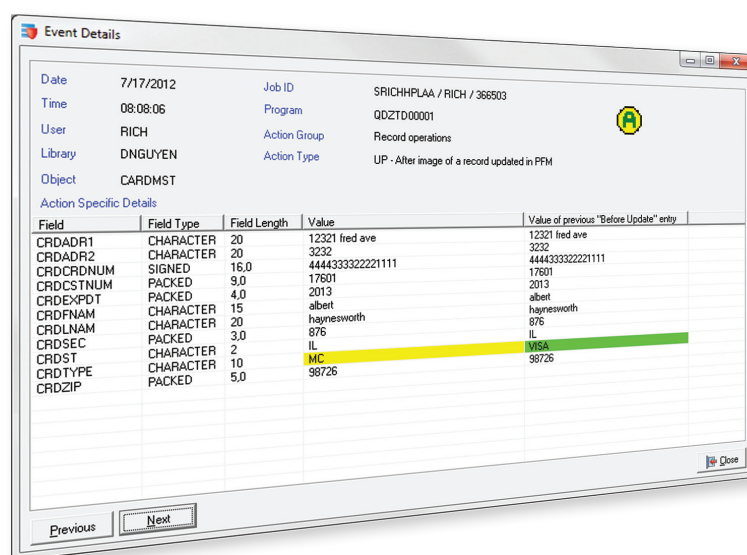
Detailed log of network and native exit point activity with powerful filtering tools.

Application Analyzer

A graphical viewpoint of application access activity to the IBM i helping identify trends in user activity, specific library and file access, application usage types such as ODBC and remote command.

File Audit

Field level auditing of files provides comprehensive tracking with "Before" and "After" views of changes to sensitive data.



The screenshot shows a window titled "Event Details" with a table of field-level audit data. The table has columns for Field, Field Type, Field Length, Value, and Value of previous "Before Update" entry. The data is as follows:

Field	Field Type	Field Length	Value	Value of previous "Before Update" entry
CRDADR1	CHARACTER	20	12321 fred ave	12321 fred ave
CRDADR2	CHARACTER	20	3232	3232
CRDCRDNUM	SIGNED	16,0	4444333322221111	4444333322221111
CRDCSTNUM	PACKED	9,0	17601	17601
CRDEXPDT	PACKED	4,0	2013	2013
CRDFNAM	CHARACTER	15	albert	albert
CRDLNAM	CHARACTER	20	haynesworth	haynesworth
CRDSEC	PACKED	3,0	876	876
CRDST	CHARACTER	2	IL	IL
CRDTYPE	CHARACTER	10	MC	MSA
CRDZIP	PACKED	5,0	98726	98726

System Audit

A log for the System Journal including tools to manage logging policies, view events and create reports.

System Inquiries

Predefined reports of native security definitions, sensitive authorities, system values and users with default password based on industry best practices.

Message Queue (MSGQ) & System History (QHST) Monitors -New!

Analyze and report on the behavior of users, applications and devices and group messages to specific business processes.

SQL Statement Audit -New!

Monitor and audit internal SQL events on the system, including interactive SQL processes, QSHELL database functions, embedded SQL in high level languages and queries. With this ability, security officers can quickly identify suspicious SQL statements.

Enforce for Syslog: **-New!**

Organizations looking to consolidate IBM i events with events from other platforms can do so using Syslog Data Provider. Security officers can easily configure Enforce/ Enterprise Security to export events in syslog format to third party log management and SIEM products.

Cross-Platform Audit (Optional Add-On)

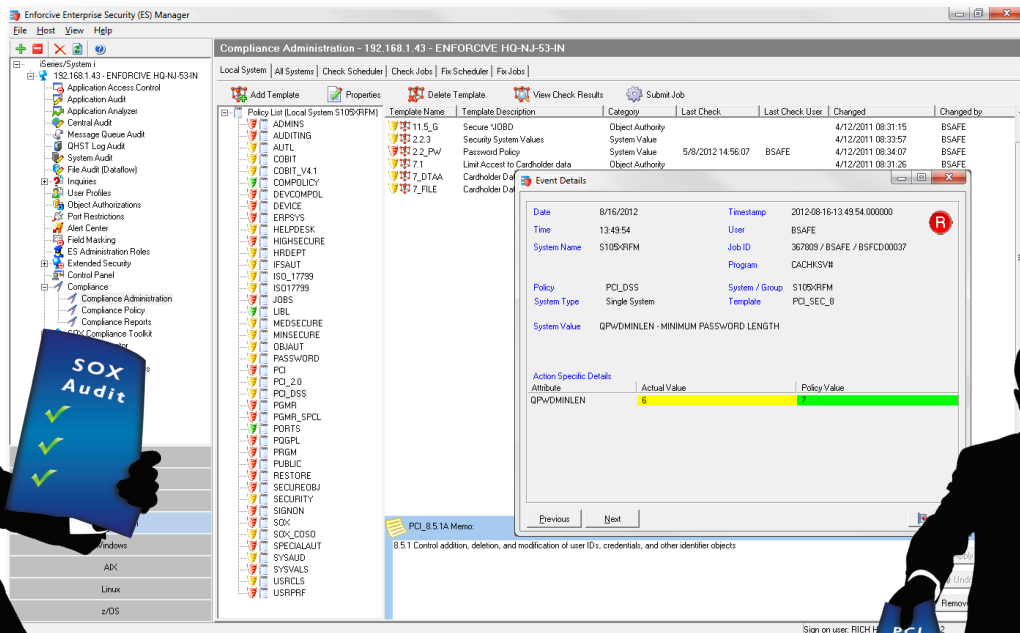
Log management software built into the Enterprise Security Manager's interface for consolidating events from different platforms and databases into a uniform database for correlation, reporting alerting and viewing through dashboards. The CPA tracks user activity across multiple IBM i servers/partitions as well as across other platforms (z/OS, Windows, AIX, Linux) and databases (DB2, Oracle, MS SQL Server, Sybase, Progress). The CPA offers the ability for organizations to take large amounts of logs from expensive production environments, and transferred to a dedicated environment for auditing and medium to long-term storage.

Compliance Management

Simplify enterprise-wide compliance management and deviation monitoring with pre-defined templates that address regulatory requirements such as SOX, PCI DSS and COBIT. Enforce assists diverse teams in unifying their compliance efforts by eliminating redundancy and reducing the complexity of regulatory adherence. Compliance can be achieved by using:

Policy Compliance Manager (Optional Add-On)

Template-based control of native definitions, deviation reporting and remediation. Templates can be defined using every parameter provided by the operating system. Once defined, the template can be checked against the actual definitions in the system. The check produces a report showing any deviations from your template(s). After checking the deviations, you have the option of aligning the actual definitions in the system with the specified policy through a fix function. Templates can be created for password settings, object definitions, user auditing etc. Included are also options for system responses such as disabling a user or revoking special authority status for particularly egregious violations.



View policy deviations

Compliance Accelerator Packages (Optional Add-On)

Extensive sets of predefined reports, alerts and compliance definitions mapped to specific regulatory standards such as SOC, PCI DSS, ISS 17991 and COBIT 4.1. This package allows companies to speed up their regulatory compliance projects by leveraging Enforcive's experience of IBM i based compliance.

Deviation Monitoring and Enforcement

Once compliance templates are in place, system administrators, security officers and auditors can view deviations from compliance policy throughout the enterprise. Enforcing compliance rules can be achieved with the click of a mouse. The benefits of managing compliance through templates include:

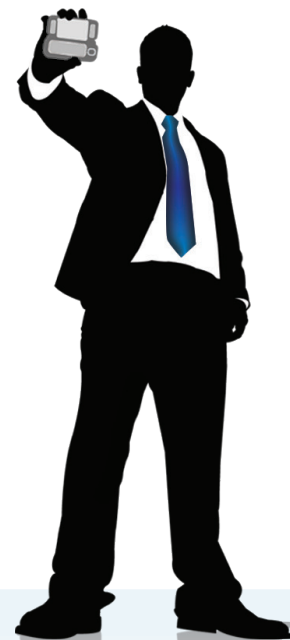
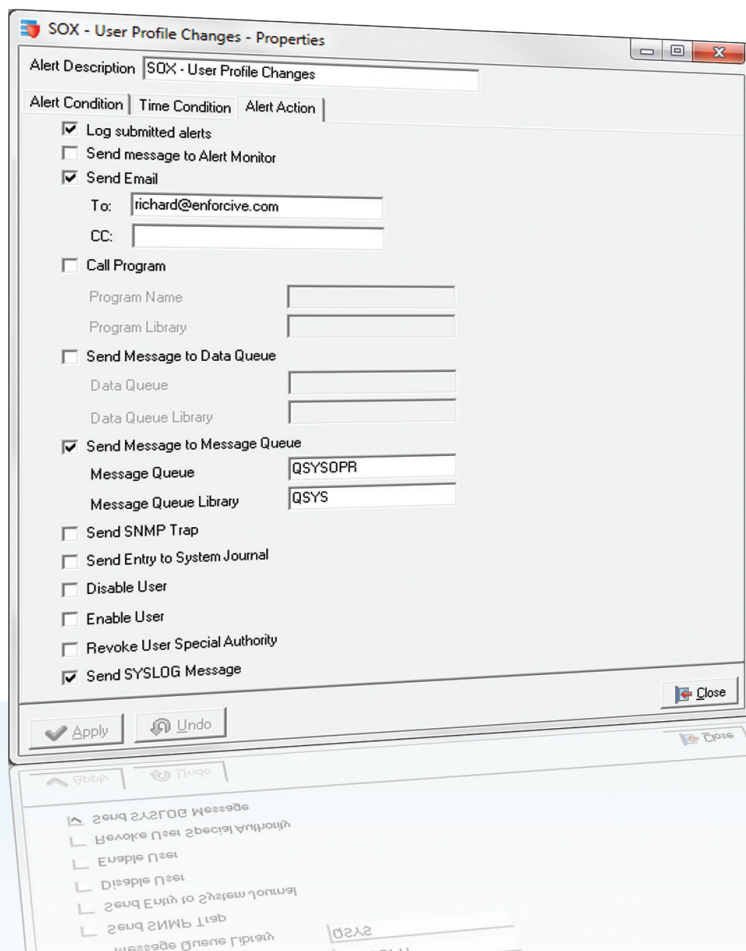
- Improved Synergy between Business and Technology Units
- Accelerated Compliance Timelines
- Protection of Consumer Data (PCI, State Privacy Regulations)
- Ensuring Data Integrity
- Centralized Security Policy Enforcement (PCI, SOX, GLBA, Canadian Bill 198)
- Streamlined Management of User Capabilities (SOX, HIPAA, Base III, COBIT)
- Segregation of Duties

Administration Role Manager

Separation of Duties is provided by the capability to define the level of access to the Enforcive product based on role. Offload your help desks tasks while maintaining security and compliance requirements.

Alert Center- Intrusion Detection System (IDS)

The Alert Center creates instant notifications of transactions, data events and compliance deviations. Alert delivery can take a number of different formats including email, on-screen display, messages in Syslog or SNMP format and can be configured to include system responses such as disabling a user or revoking special authority.



Reports Auditors Will Appreciate

Enforcive/ Enterprise Security offers versatile reporting capabilities. Enforcive's Report Generator provides control over integrating and presenting system data to meet the specific needs of an organization. Information such as power user activities, changes to sensitive data and system by system comparisons can be organized to best meet audit criteria using scope definitions, field selection, filter criteria, field sorting and Boolean Logic. These reports can be configured to automatically run and send the results to security officers and auditors for review. The Report Generator comes with an ever growing number of predefined reports.

Report Examples:

- PCI DSS Compliance
- SOX Compliance
- HIPAA Compliance
- Canadian Bill 198 Compliance
- GLBA Compliance
- Basel III Compliance
- System Value
- Power User Activities
- User Profile Changes
- Detailed System Audit
- Object Authority
- Object Description
- Field-Level Auditing

Enforcive™ All Objects in a Library PRODDATA Sorted by Size

Enforcive™ System Value Comparison Between Multiple Systems

Enforcive™ Users with "All Objects" Special Authority

Enforcive™ SOX Compliance - Invalid Sign-on Attempts

Enforcive™ System Value Deviation Report - Across Multiple Systems

Run Date: 09/14/2012

System Value Name	System Value Description	TEMPLATE	Systems						
			MSDEV	BARNEY	BSF51	BSF53	MSPRG	OCEAN	
QPWDEXPITV	Password expiration interval	60	60	90	60	30	60	15	
QPWDLMTAJC	Limit adjacent digits in password	1	1	0	0	1	1	1	
QPWDLMTCHR	Limit characters in password	#, @	*NONE	#, @, \$	#, @	*NONE	#	\$	
QPWDLMTREP	limit repeated characters in password	0	2	2	2	0	0	0	
QPWDLVL	Password level	1	0	0	1	3	1	0	
QPWDMAXLEN	Maximum password length	10	10	10	10	10	10	10	
QPWDMINLEN	Minimum password length	5	4	7	6	5	6	6	
QPWDPOSDF	Limit password character position	1	1	1	0	0	1	0	
QPWDRQDDGT	Require digit in password	1	1	1	1	1	1	1	
QPWDRQDDIF	Duplicate password control	4	5	7	1	4	5	5	
QPWDVLDPGM	Password validation program	*NONE	*NONE	*NONE	*NONE	*NONE	*NONE	*NONE	



About Enforcive

Enforcive provides comprehensive security solutions to help businesses reduce workloads, satisfy auditors and improve responsiveness to security threats. For over two decades, Enforcive has been providing solutions within mission critical environments using platforms including IBM i, System z, AIX, Linux and Windows. Our expertise and commitment to innovation enables us to offer the best of breed solutions to our customers.

Enforce your policy by:

- Defining clear access control and segregation of duties
- Implementing comprehensive and demonstrable security and compliance policies
- Automating compliance related administration tasks
- Leveraging Enforcive's predefined reports, alerts and compliance templates for specific regulations including SOX, PCI and COBIT
- Addressing your medium to long term audit log archiving requirements
- Offloading resource hogging compliance related tasks from your production environment

Enforcive, Inc.
Toll Free USA: 877-237-8024
International: +972-9-9610400
info@enforcive.com
www.enforcive.com

