Audit

iSecurity

Product Description

Audit is a leading security auditing application that examines IBM i QAUDJRN events in real time and triggers alerts and other responsive actions to potential threats.

Audit is provided with more than 200 built-in reports which can be executed "Out-of-the-Box" and, if necessary, can be adapted to site specifications using **Audit's** powerful report generator and scheduler which requires no programming!

Audit is available both in an Eclipse-based GUI version as well as in the native "green-screen" interface.

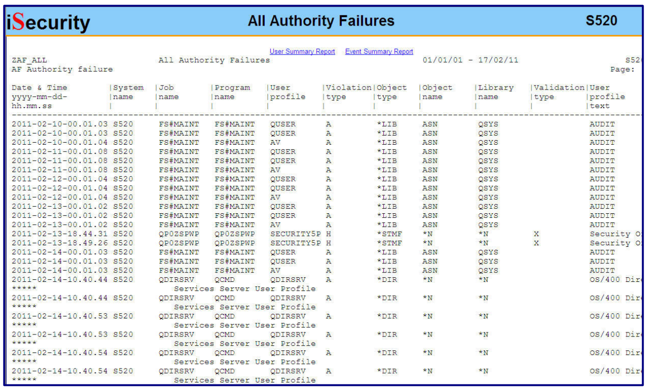
The Audit Solution

Recent industry regulations such as PCI, SOX, HIPAA and others, have placed security auditing as a key component of any organizational IT security program.

Simply creating a security policy and purchasing security software tools is not enough. Management must ensure that security polices and procedures are properly implemented and enforced. In addition, managers must be able to evaluate and test the effectiveness of these policies on an on-going basis.

Audit solves this challenge and more, by enhancing native IBM i auditing and adding several robust new features and capabilities. **Audit** provides a user-friendly interface for working with the large, often confusing, number of system values and parameters provided by OS/400 and is designed for ease-of-use by non-technical personal, such as auditors and managers. Indeed, the user interface provides clear explanations for all audit types, parameters, fields and field values.

Audit's real-time detection identifies security events as they occur and records details in a history log, which enables site personnel to exploit the powerful query and reporting features that are included with the product. More importantly, real-time detection triggers alerts and immediate corrective actions with the optional iSecurity **Action** module.



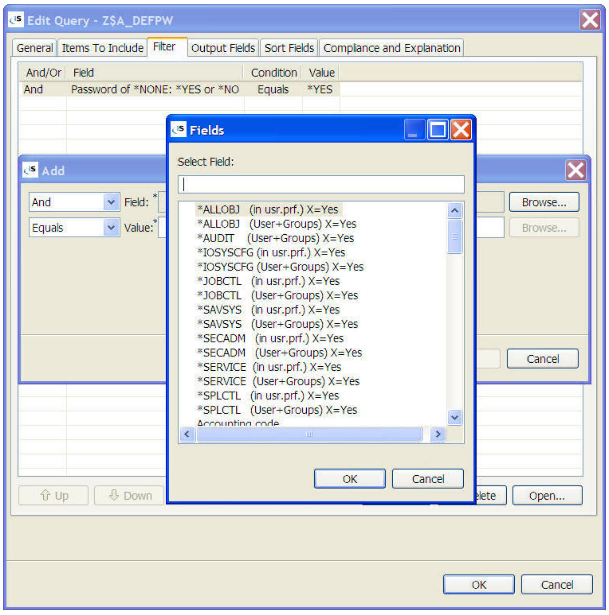
iSecurity All Authority Failures S520

User Summary Report Event Summary Report

```
ZAF_ALL                  All Authority Failures                    01/01/01 - 17/02/11                      S52
AF Authority failure                                                                                      Page:

Date & Time         |System  |Job       |Program   |User      |Violation|Object  |Object   |Library   |Validation|User
yyyy-mm-dd-         |name    |name      |name      |profile   |type     |type    |name     |name      |type      |profile
hh.mm.ss            |        |          |          |          |         |        |         |          |          |text
-------------------------------------------------------------------------------------------------------------------------
2011-02-10-00.01.03 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-10-00.01.03 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-10-00.01.04 S520      FS#MAINT   FS#MAINT   AV         A         *LIB     ASN       QSYS                  AUDIT
2011-02-11-00.01.08 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-11-00.01.08 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-11-00.01.08 S520      FS#MAINT   FS#MAINT   AV         A         *LIB     ASN       QSYS                  AUDIT
2011-02-12-00.01.04 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-12-00.01.04 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-12-00.01.04 S520      FS#MAINT   FS#MAINT   AV         A         *LIB     ASN       QSYS                  AUDIT
2011-02-13-00.01.02 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-13-00.01.02 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-13-00.01.02 S520      FS#MAINT   FS#MAINT   AV         A         *LIB     ASN       QSYS                  AUDIT
2011-02-13-18.44.31 S520      QP0ZSPWP   QP0ZSPWP   SECURITY5P H         *STMF    *N        *N         X          Security O
2011-02-13-18.49.26 S520      QP0ZSPWP   QP0ZSPWP   SECURITY5P H         *STMF    *N        *N         X          Security O
2011-02-14-00.01.03 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-14-00.01.03 S520      FS#MAINT   FS#MAINT   QUSER      A         *LIB     ASN       QSYS                  AUDIT
2011-02-14-00.01.03 S520      FS#MAINT   FS#MAINT   AV         A         *LIB     ASN       QSYS                  AUDIT
2011-02-14-10.40.44 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
2011-02-14-10.40.44 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
2011-02-14-10.40.53 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
2011-02-14-10.40.53 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
2011-02-14-10.40.54 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
2011-02-14-10.40.54 S520      QDIRSRV    QCMD       QDIRSRV    A         *DIR     *N        *N                    OS/400 Dir
*****                            Services Server User Profile
```

Sample HTML report; can be emailed to a list of recipients



Edit Query - Z$A_DEFPW

And/Or	Field	Condition	Value
And	Password of *NONE: *YES or *NO	Equals	*YES

Add

And Field: *

Equals Value: *

Fields

Select Field:

*ALLOBJ (in usr.prf.) X=Yes
*ALLOBJ (User+Groups) X=Yes
*AUDIT (User+Groups) X=Yes
*IOSYSCFG (in usr.prf.) X=Yes
*IOSYSCFG (User+Groups) X=Yes
*JOBCTL (in usr.prf.) X=Yes
*JOBCTL (User+Groups) X=Yes
*SAVSYS (in usr.prf.) X=Yes
*SAVSYS (User+Groups) X=Yes
*SECADM (in usr.prf.) X=Yes
*SECADM (User+Groups) X=Yes
*SERVICE (in usr.prf.) X=Yes
*SERVICE (User+Groups) X=Yes
*SPLCTL (in usr.prf.) X=Yes
*SPLCTL (User+Groups) X=Yes
Accounting code

Sample GUI report filter showing criteria and additional report tabs

Audit queries employ robust selection criteria such as AND/OR, equal/not equal, greater/less than, like/not like, included in list, etc. Only the information needed is included in reports, whose formats are fully customizable. Finally, **Audit** logs display security audit data in a standard message format with the actual data embedded in the message.

RAZ-LEE
Experts @ Security and Compliance
Raz-Lee Security Inc.
Website: www.razlee.com

Corporate HQ - USA
Email: marketing.us@razlee.com
Tel: 1-888-RAZLEE-4
Fax: 1-419-781-5851

Audit

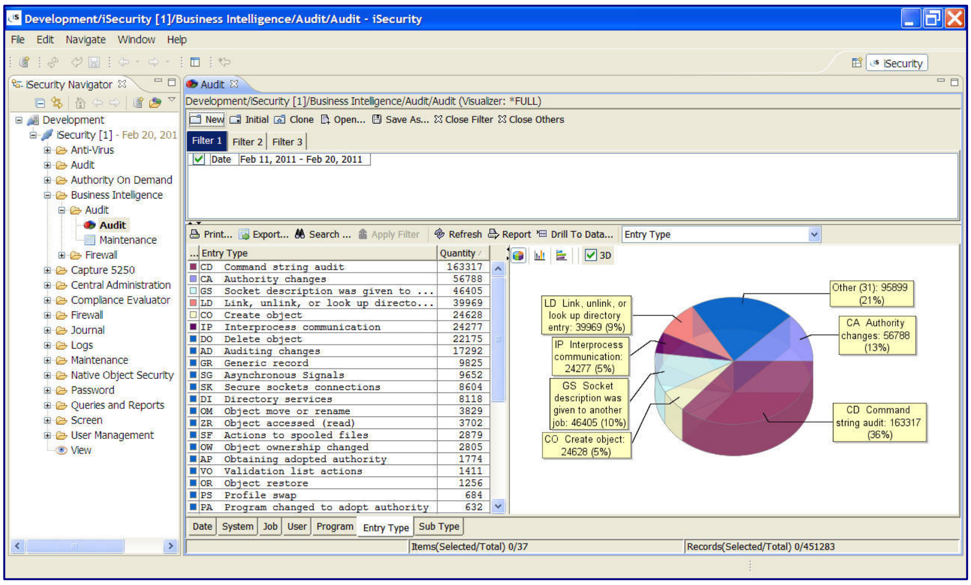
iSecurity

Key Features

- > Monitors user activities and object access in real-time
- > Triggers alert messages and corrective actions using **iSecurity Action**
- > Simple to use – no technical knowledge required
- > More than 200 predefined queries and reports
- > Query Wizard – creates queries quickly and easily without programming
- > Time groups apply rules and filters at predefined times
- > "Backward Glance" feature –- quickly look at what happened to your system in the last few minutes
- > View multiple audit types with one query
- > Sort query data in any order
- > Design custom output for query data – select and sort data fields
- > Report Scheduler – automatically run reports at specified times
- > Explains parameters and data values with a single keystroke
- > **Audit** Scheduler – change audit scope automatically at designated times

Benefits

- > Specially designed for non-technical users such as auditors, managers and administrators
- > Enables compliance with Sarbanes-Oxley (SOX), PCI, HIPAA, and site and auditor-defined regulations
- > Minimizes throughput delay and resource usage
- > Simple, intuitive audit parameter definition process
- > Full text explanations of audit types, fields, field values and other data make parameter definition easy and error-free
- > Scheduler feature minimizes performance impact during peak periods
- > Powerful query and report generator provides the data you need when you need it, without tying up IT resources
- > Integrates with **iSecurity Visualizer** to produce rich graphical presentations of audit data
- > Integrates with i**Security Central Admin** to support single-console reporting in multi-LPAR environments
- > Superior human engineering ensures security implementation quickly, efficiently and without requiring expensive security consultants



Development/iSecurity [1]/Business Intelligence/Audit/Audit (Visualizer: *FULL)

☑ Date Feb 11, 2011 - Feb 20, 2011

...	Entry Type	Quantity
■	CD Command string audit	163317
■	CA Authority changes	56788
□	GS Socket description was given to ...	46405
■	LD Link, unlink, or look up directo...	39969
□	CO Create object	24628
■	IP Interprocess communication	24277
■	DO Delete object	22175
■	AD Auditing changes	17292
■	GR Generic record	9825
■	SG Asynchronous Signals	9652
■	SK Secure sockets connections	8604
■	DI Directory services	8118
■	OM Object move or rename	3829
■	ZR Object accessed (read)	3702
■	SF Actions to spooled files	2879
■	OW Object ownership changed	2805
■	AP Obtaining adopted authority	1774
■	VO Validation list actions	1411
■	OR Object restore	1256
■	PS Profile swap	684
■	PA Program changed to adopt authority	632

Items(Selected/Total) 0/37

Records(Selected/Total) 0/451283

RAZ-LEE
Experts @ Security and Compliance

Raz-Lee Security Inc.
Website: www.razlee.com

Corporate HQ - USA
Email: marketing.us@razlee.com
Tel: 1-888-RAZLEE-4
Fax: 1-419-781-5851