Enforcive®
Enterprise Security

Highlights Version 8.3.08

These icons indicate:

❌ A change that may require action. For example, you may need to modify automation programs or exit programs or perform other actions before or after installing the product.

⚠️ A change in behavior or a change to the user interface. You should be aware of the change, but no action may be required.

✔️ New function or an enhancement in the indicated software.
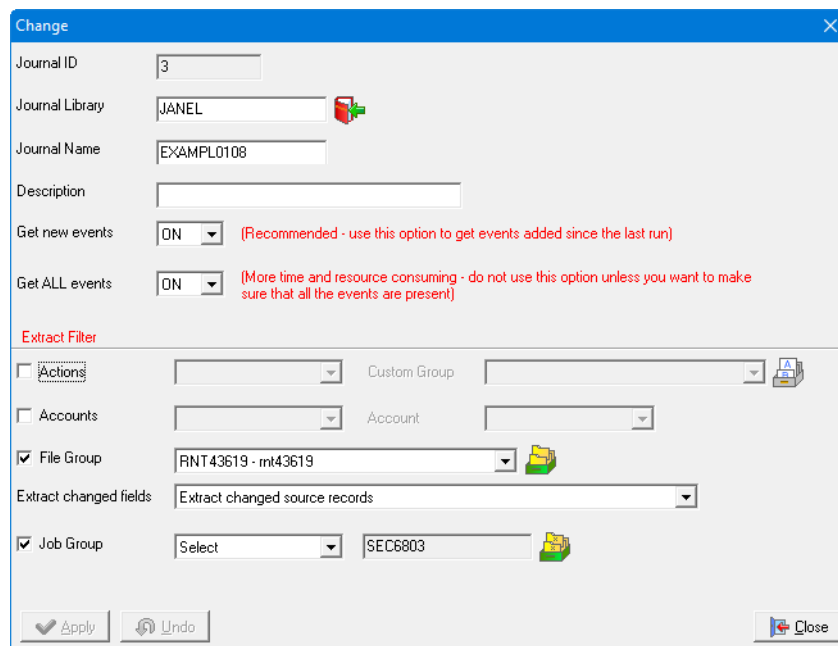

Features included in version 8.3.08

Central Audit

SEC-6803   In the File Audit tab of the Data Extraction screen, new functionality was added to the Extract Filter in the Add/Change dialog.
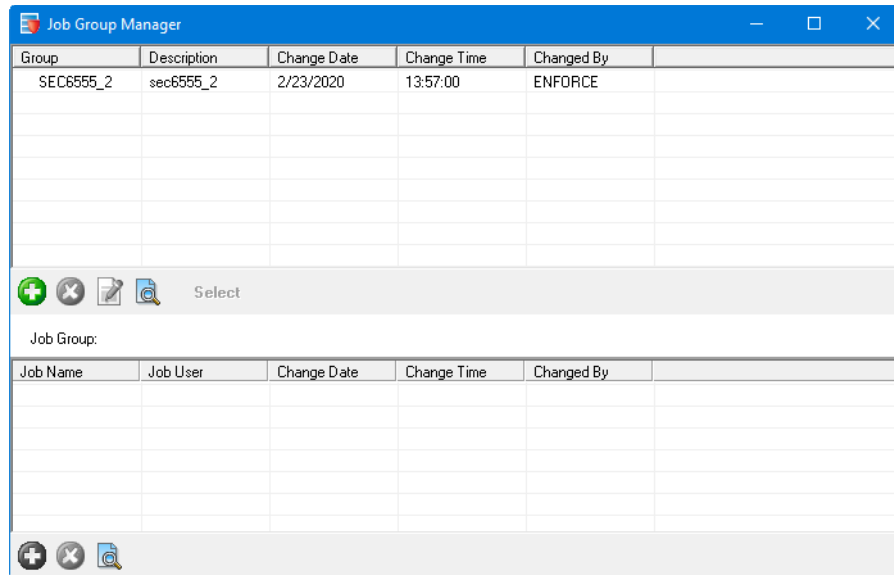
⚠️
✔️   When Accounts is selected, **Omit User ID** and **Omit User Group** are available in addition to Select User ID and Select User Group.

The Job Group field enables you to filter by job group. The available options are **Select** and **Omit**.

Click the Job Groups button 📂 to open the Job Group Manager.

Click the required job group in the upper pane and click **Select**.

Control Panel

SEC-6555   Under Report size, File audit Maximum Events to Process, the *NOMAX option was added (*NOMAX means a limitation 5,000,000 events in the output of the reports).

Fixes included in version 8.3.08

This list includes all relevant changes and fixes since version 8.3.07:

Alerts

SEC-5273   In the File Audit alert, the alert monitor now displays the alert message correctly.

Application Access Control

SEC-4566   In Application access control, the object level library list now displays correctly.

SEC-5775   In Application access control, the FTP exit program now works correctly when searching for an object group.

SEC-6197   The Database exit program now retrieves the permissions correctly if the create procedure is in use by SQL.

SEC-6243   The Application Access Control retrieve library list is now fixed (QSYS2 now appears in the library list).

SEC-6466   File protection now writes events to the Application audit if the QTEMP library exists in QSYSLIBL.

Central Audit

SEC-4524   Data extraction of system audit to Central Audit now works correctly.

SEC-5539   In Central Audit under Data Extraction, the File Audit job now checks the receiver dates before they are processed.

SEC-5875   When members in journaled source files (such as QCLSRC or QRPGLESRC) are changed, all the records are written in the journal and extracted to Central Audit only if the value of the record change date is greater than or equal to the last run date. Thus, only new changed records will be extracted into Central Audit.

SEC-6525   Messages with severity 80 will no longer be sent to the QSYSOPR message queue because of empty Central Audit Rollover partitions.

SEC-6641   The **Omit User ID** and **Omit User Group** options have been added in Central Audit in the Accounts field under the File Audit tab in Data Extraction.

Compliance

SEC-5953   In the File Shares category, when Exclusive List is selected on the Template Attributes screen of the Add Compliance Template Wizard, the file shares not appearing in the list are considered deviations.

SEC-6639   In the IFS Object Authority category, the report is now generated when one of the objects is out of compliance.

SEC-6674   In the Adopted Authority category, Check deviation now works correctly when there is a log violation only and no deviation is found.

SEC-6696   In the Adopted Authority category, Check deviation performance was improved.

Data Providers

SEC-5982   In the System Audit Data Provider, on the Collection Policy tab, the **JOPGMLIB** and **JEOBJT** fields were added to the Condition criteria:

SEC-6177   In the File Audit Data Provider, handling has been corrected when Custom Group is selected as the group type for Action Group.

SEC-6178   For the QHST Data Provider, the message is no longer truncated for OS V7R2M0 and higher.

SEC-6269   In the System Audit Data Provider, on the Destination tab, when SYSLOG server is selected as the Connection type, the **Key-value pair** message format option was added.

SEC-6313   The QHST Data Provider Real-Time monitor job no longer stops sending data to Splunk after upgrading for OS V7R1M0 and higher.

Encryption

SEC-6029   Deletion of master keys now works correctly.

SEC-6246   The ENCAUDAJE job is no longer started when Encryption is not in use.

Extended Security

SEC-5977   An option is now available to set a disabled user to *NONE as part of the Inactive Users scheduled job.

File Audit

SEC-6331   In the Filter Select File screen, the dropdown issue when entering the file name in the File field was fixed.

Report Generator

SEC-6017   Report Generator Fields with null values are now changed to a legitimate value.

SEC-6239   In the QHST Log report type, the error message **Value cannot be converted to type implied by receiver** is no longer generated.

SEC-6285   Report print files now retain the spool files after printing. The print files attribute is set to SAVE(*YES).

SEC-6337   In the System Audit (detailed) report type, if no data is retrieved from the selected criteria, the error message is now "No data found matching selected criteria".

SEC-6355   In the User Group Members report type, the limitation of 100 members per user group was removed.

SEC-6512   In the Application Audit report type, the date range in the report layout when the substring is defined in the Query wizard now appears correctly.

SEC-6590   An error no longer occurs when adding a report to an existing report group.

SEC-6710   When a Report Generator job is submitted and an error is found during the SQL phase of the job, an error report is now printed only if external switch 8 is turned on during the job.

SEC-6925   The Account Permission report type for system policy accounts now works correctly when there are no permissions in a system policy account.

SEC-6979   The Application Audit report type for the database report now has no missing events or truncated SQL statements.

SQL Statement Audit

SEC-5542   SQL statement Audit enhancements now support OS V7R1M0 and higher (instead of V7R3M0 only).

System Audit

SEC-6516   In System Audit, when filtering by Action Group *AUTFAIL, Action Type PW and user name, the events are now displayed correctly.

User Profiles

SEC-5730   Delete User Profile in a cluster environment now works correctly with DLTPRFCLU.

SEC-5851   When deleting user profiles via the user interface in remote partitions, clusters using power HA are handled correctly.