



Enforcive®

Enterprise Security

Highlights Version 8.3.06

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 8.3.06

Alerts

SEC-2913 The email alert has been reformatted so that each event appears in a separate line.

Application Access Control

SEC-4141 Object Group Manager has a new multi-selection option in the add library, add object and remove member functions.

Central Audit

SEC-3764 Added support to include *ALL files in a File Group for a specific library for Central Audit > Data Extraction > File Audit > Add or Change > edit File Groups.



SEC-4320 In the Data Extraction File Audit tab, the **Extract Changed Fields** field in the Add dialog now has 3 options:



Extract changed fields and selected fields in File Group

Extract all fields or as defined in File Group

Extract changed fields if defined as selected fields in File Group

Encryption

SEC-232 Added support for IFS folder encryption.



To encrypt an entire folder:

1. Click **Add** in the IFS Registry Manager panel.

2. In the File Path field, enter the path of the folder you want to encrypt.
3. In the File Name field, enter an asterisk.
4. Fill in the remaining fields accordingly and click **Add**.
5. Start encryption for this registry. The encryption status changes to yellow (under encryption) and the process of encrypting all documents within this folder begins. At the end of the process, the status will be changed to red (encrypted).
6. Add authorities as desired.

From this point, any document added to this folder will automatically be encrypted.

Note: Encrypting an entire folder does not encrypt sub folders.

LPAR Replication

SEC-3366 Added Data Providers module to support direct single and multiple LPAR Replication.

Report Generator

SEC-2374 The Account name field was added to the query wizard in the Application Audit report type.

SEC-3385 The Account Permissions report type was added to display the permissions assigned to different Account Types. The following is a sample report:



Account Permission - User													
File View													
PDF	HTML	CSV	Edit	Save	Delete								
Account	Description	Status	User Group	Administration Roles	Application Type	Time Permissions	Server Permission	Event Type	Log Recording	Optimization	Function Name	Function Permission	
ABY	ABY user	*ENABLED			ACCOUNT SWAPP								
					FTP SERVER	YES	WARNING	ALL	N		CREATE LIBRARY	YES	
					FTP SERVER	YES	WARNING	ALL	N		DELETE LIBRARY	YES	
					FTP SERVER	YES	WARNING	ALL	N		SET DIRECTORY	YES	
					FTP SERVER	YES	WARNING	ALL	N		LIST FILES	YES	
					FTP SERVER	YES	WARNING	ALL	N		DELETE FILES	YES	
					FTP SERVER	YES	WARNING	ALL	N		SEND FILES	YES	
					FTP SERVER	YES	WARNING	ALL	N		RECEIVE FILES	YES	
					FTP SERVER	YES	WARNING	ALL	N		RENAME FILES	YES	
					FTP SERVER	YES	WARNING	ALL	N		CL COMMAND	YES	
					FTP CLIENT	YES	WARNING	ALL	N		CREATE LIBRARY	YES	
					FTP CLIENT	YES	WARNING	ALL	N		DELETE LIBRARY	YES	
					FTP CLIENT	YES	WARNING	ALL	N		SET DIRECTORY	YES	
					FTP CLIENT	YES	WARNING	ALL	N		LIST FILES	YES	
					FTP CLIENT	YES	WARNING	ALL	N		DELETE FILES	YES	
					FTP CLIENT	YES	WARNING	ALL	N		SEND FILES	YES	
					FTP CLIENT	YES	WARNING	ALL	N		RECEIVE FILES	YES	
					FTP CLIENT	YES	WARNING	ALL	N		RENAME FILES	YES	
					FTP CLIENT	YES	WARNING	ALL	N		CL COMMAND	YES	
					RMTCMD	YES	WARNING	ALL	N		PROGRAM CALL	YES	
					RMTCMD	YES	WARNING	ALL	N		COMMAND CALL	YES	
					RMTSQL	NO	WARNING	ALL	N			NO	
					DDM	YES	WARNING	ALL	N		ADD MEMBER	YES	
					DDM	YES	WARNING	ALL	N		CHANGE	YES	
					DDM	YES	WARNING	ALL	N		CHANGE DATA AREA	YES	
					DDM	YES	WARNING	ALL	N		CHANGE MEMBER	YES	
					DDM	YES	WARNING	ALL	N		CLEAR	YES	
					DDM	YES	WARNING	ALL	N		CLEAR DATA QUEUE	YES	
					DDM	YES	WARNING	ALL	N		COMMAND	YES	

SEC-3794 The Command Control Definition report type was added to display all commands with their definitions. The following is a sample report:



System	Command name	Command library name	Authorized	Log Recording	S/W/R	Status
SYSI69	ADDIRE	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	ADDTCPHTE	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	CHGSMTPA	QTCP	YES	ALL	WARNING	INACTIVE
SYSI69	CHGTCPHTE	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	CHGUSRPRF	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	CRTLIB	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	DLTLIB	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	ENDJOB	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	ENDSBS	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	RMVTCPHTE	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	RNMTCPHTE	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	SNDDST	QSYS	YES	ALL	WARNING	INACTIVE
SYSI69	STRSQL	QSQL	YES	ALL	WARNING	INACTIVE
SYSI69	WRKDIR	QSYS	YES	ALL	WARNING	INACTIVE

SEC-3795 The System Audit User Defined report type was added to display system journal entries with journal code value U (user-defined events). The following is a sample report:



Timestamp	Serial Number	User Profile	Remote Port	Remote Address	Job Name	User	Job Number	Program Name	Program Library Name	Receiver	Receiver Library	Action Type
2019-06-03-13:24:02.026704	S21B171V	KAHNT	16,865	10.22.88.6	QPADEV00F	KAHNT	657098	EXUSRFORC	RMT0BJ	NEWRCV0113	AUDJRNLIB	CP
2019-06-03-13:24:50.770944	S21B171V	KAHNT	16,865	10.22.88.6	QPADEV00F	KAHNT	657098	EXUSRFORC	RMT0BJ	NEWRCV0113	AUDJRNLIB	CP
2019-06-03-13:28:27.071136	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	655563	EXUSRFORC	RMT0BJ	NEWRCV0113	AUDJRNLIB	CP
2019-06-03-13:30:46.603760	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	655563	EXUSRFORC	RMT0BJ	NEWRCV0113	AUDJRNLIB	CP
2019-06-03-13:30:47.362928	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	655563	EXUSRFORC	RMT0BJ	NEWRCV0113	AUDJRNLIB	CP
2019-06-05-11:38:12.016176	S21B171V	ENFORCE	1,271	10.22.88.4	QPADEV00C	ENFORCE	657968	BSYSALRMNT	RMTSMP	NEWRCV0113	AUDJRNLIB	FI
2019-06-05-11:39:35.986208	S21B171V	ENFORCE	1,271	10.22.88.4	QPADEV00C	ENFORCE	657968	RUNINTELI	RMT0BJ	NEWRCV0113	AUDJRNLIB	FI
2019-06-05-16:52:09.611200	S21B171V	KAHNT	1,045	10.22.88.4	QPADEV00C	KAHNT	658321	BSYSALRMNT	RMTSMP	NEWRCV0114	AUDJRNLIB	FI
2019-06-05-18:17:28.240080	S21B171V	KAHNT	1,045	10.22.88.4	QPADEV00C	KAHNT	658321	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-05:47:27.030960	S21B171V	JANEL	59,232	10.22.82.41	QPADEV00C	JANEL	658697	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-05:48:17.484576	S21B171V	JANEL	59,232	10.22.82.41	QPADEV00C	JANEL	658697	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-05:48:40.194976	S21B171V	JANEL	59,232	10.22.82.41	QPADEV00C	JANEL	658697	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-06:00:43.810880	S21B171V	ENFORCEGUIL			BSFAPCH	QTMHHTTP	658695	ALALRMNT	RMTSMP	NEWRCV0114	AUDJRNLIB	LA
2019-06-06-06:47:05.002064	S21B171V	KAHNT	1,100	10.22.88.4	QPADEV00F	KAHNT	658743	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-07:53:22.985240	S21B171V	KAHNT	1,161	10.22.88.4	QPADEV00F	KAHNT	658773	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-08:25:41.807856	S21B171V	KAHNT	1,094	10.22.88.4	QPADEV00G	KAHNT	658816	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-09:32:00.377216	S21B171V	KAHNT			BSFAPCH	QTMHHTTP	658695	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-09:33:18.933088	S21B171V	BSAFE			BSFAPCH	QTMHHTTP	658695	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-09:33:19.316080	S21B171V	BSAFE			BSFAPCH	QTMHHTTP	658695	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-06-12:00:22.082272	S21B171V	QSECOFR	53,186	10.22.82.46	QPADEV00R	QSECOFR	658866	BSYSALRMNT	RMTSMP	NEWRCV0114	AUDJRNLIB	FI
2019-06-06-14:03:18.484056	S21B171V	QSECOFR	53,186	10.22.82.46	QPADEV00R	QSECOFR	658866	BSYSALRMNT	RMTSMP	NEWRCV0114	AUDJRNLIB	FI
2019-06-06-15:25:51.350608	S21B171V	QSECOFR	53,186	10.22.82.46	QPADEV00R	QSECOFR	658866	BSYSALRMNT	RMTSMP	NEWRCV0114	AUDJRNLIB	FI
2019-06-06-16:42:41.193344	S21B171V	QSECOFR	53,186	10.22.82.46	QPADEV00R	QSECOFR	658866	EXUSRFORC	RMT0BJ	NEWRCV0114	AUDJRNLIB	CP
2019-06-11-07:56:32.243856	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	661449	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP
2019-06-11-09:13:59.464672	S21B171V	ENFORCEGUIL			BSFAPCH	QTMHHTTP	661449	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP
2019-06-11-10:15:44.916128	S21B171V	ENFORCEGUIL			BSFAPCH	QTMHHTTP	661449	ALALRMNT	RMTSMP	NEWRCV0115	AUDJRNLIB	LA
2019-06-11-10:16:45.301424	S21B171V	JANEL			QPADEV00C	JANEL	661443	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP
2019-06-11-10:37:42.721040	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	661449	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP
2019-06-11-10:38:17.970112	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	661449	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP
2019-06-11-14:16:58.205936	S21B171V	ENFORCE			BSFAPCH	QTMHHTTP	661553	EXUSRFORC	RMT0BJ	NEWRCV0115	AUDJRNLIB	CP

SEC-4071 Added a dropdown list to all fields in the Report Groups properties.


SQL Statement Audit

SEC-2183 In the Add SQL Statement Policy dialog, there is now a **Job Name Selection Type** field, with a default value of **Select**. You can also select **Omit** to omit the specified job and select all others.

Additionally, when **Account** is selected, there are two new fields available in the Account Type dropdown list: **Omit User ID** and **Omit User Group**, to omit the selected user or user group and select all the others.

Note: This feature is available for OS version V7R3M0 and higher.

System Audit

- SEC-1167 Added the option of *CURCHAIN in the receiver selection to select all receivers. Also added the System Audit Global Settings dialog to control the number of records. The dialog is accessed by clicking the **System Audit Global Settings** button  in the toolbar. The minimum number of records is 2000; the maximum number is 5000.

Fixes included in version 8.3.06

This list includes all relevant changes and fixes since version 8.3.05:

Accelerator Package

- SEC-3775 The Accelerator Package is now correctly restored when performing the upgrade.

Alerts

- SEC-2867 The Alert format for all alert types was changed to include more information.
- SEC-3251 Two new options were added to the Accounts field dropdown list for SQL Audit alerts - **Omit User ID** and **Omit User Group**.
- SEC-3719 The System audit alert now starts correctly after performing an IPL.
- SEC-3797 The **Special Group Authority** optional field in the System Audit alert now works correctly when the special authority of a group profile is changed to or from *NONE.
- SEC-3937 The ES Health Monitor Alert now correctly reports the status of the Data Provider.
- SEC-4005 The ES Health Monitor Alert Collector job now displays the correct status when not running.

Application Access Control

- SEC-2121 Corrected error when opening the Priority Level dialog from the User Group Manager.
- SEC-3039 The library and file name is now retrieved when retrieving database file information.
- SEC-3504 Two new columns, **From Date** and **To Date**, were added to the Swap List.

Central Audit

- SEC-1025 Data extraction from System Audit into Central Audit no longer fails with error CPF7054.
- SEC-3620 An error message is no longer displayed when adding a File Audit Extraction definition when a definition to the same journal already exists.
- SEC-4011 In the File Audit Extract Scheduler, it is no longer possible to change the journal and journal library.

Compliance

- SEC-3136 View results for Object Authority Check Deviations have been corrected to display expected objects. Additionally, the **Authorization List**, **Owner** and **Primary Group** rows are now omitted if their policy value is *NONE or Not Specified.

Control Panel

SEC-2395 Added delays in the rollover maintenance job (BSFRMON) for Data Provider, SQL Extract and Encryption Auditing. The delays are controlled via the Tools option in the Control Panel.

Data Providers

SEC-3347 Additional editable parameters were added to the Global Settings dialog. Changes made to the parameters take effect when the Real-time monitor jobs are restarted.

The **Error Handling** tab enables you to configure a message queue to receive any error messages and to configure error handling.

The **Additional Parameters 1** tab displays the DBCS CCSID and allows you to configure the delay before writing the trace file, the delay in the QHST work job and the number of errors from SYSLOG before sending the Health Alert.

The **Additional Parameters 2** tab displays the delay while creating the IFS files and allows you to configure the delay while retrieving the journal in System Audit and the routing data parameter of the Submit Job.

SEC-3635 In the History Log Data Provider Collection Policy tab, in the Select Message ID/Group dialog, the Exclude Message group option was added to exclude the specified message group and select all the others.

SEC-4136 In the Statistic Report for the System Audit Data Provider Real-time monitor job, the Job Start Date field has been corrected.

Encryption

SEC-1734 The IFS Encryption sub module is now available from OS version 7.3 and up only.

SEC-3227 The default values in the User Log Recording Manager are now **Not Active** and **Include by List**.

Extended Security

SEC-3364 If a user is disabled by entering his password too many times and the user is added to the Inactive Users file by the scheduled Inactive Users job, the Disable Date is set to the system date.

Firewall Manager

SEC-3544 When adding or changing a rule, if Group is selected for the Destination IP Address type, a warning message appears if the IP Address group entered is not defined in the IP Group list.

General


SEC-2908 The GUI will now be accessible when changing the current ASP group to a non-*SYSBAS group.

SEC-2978, 3613

The Uninstall process now correctly identifies and deletes most Enforcive-related objects. See the Uninstall instructions for objects that require manual deletion.

- SEC-3525 When performing an upgrade, the file RMTFIL/RMTRPTMSG will be created if it does not exist.
- SEC-3784 Corrected GUI error BSG0004 when SEC2338 exists as a physical file in QGPL.

Report Generator

- SEC-2350 The System Audit report with a periodic run type now saves the timestamp correctly.
- SEC-2512 Report Generator report 103 no longer returns the error **No data found matching selected criteria**.
- SEC-3189 Additional selection criteria were added to the Swap not used X days report type.
- SEC-3242 The **Swap Date To** and **Swap Time To** fields were added to the Swap Settings report type.
- SEC-3346 The Administration Roles report type now includes restricted security officers that have no module permissions assigned.
- SEC-3844  Improved the performance of the System Audit Report type. It is recommended to reduce the number of events in the report. In the Control Panel, select Report Size and change the value in System Audit Maximum Events to Process.
- SEC-4024 Submit Job now works correctly when QTEMP or QGPL are included in the QSYSLIBL system value.

SQL Statement Audit

- SEC-4680 In SQL Statement Policy, it is now possible to define both file groups and user groups (accounts).
- If a user group is defined for more than one SQL Statement Audit policy, when running interactive SQL (*SQL) from the green screen, only events from the first policy are monitored.

User Profiles

- SEC-3769 Copying a user profile no longer generates an error when the copied user is disabled.