



# Enforcive®

## Enterprise Security

### Highlights Version 8.3.03

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 8.3.03

### Application Access Control

SEC-566



A new version of the SWPON command was added to the interactive swap feature to enable account swapping with the user specified. The new command is SWPONT. It has a keyword parameter of USER in addition to the existing RSN parameter. The syntax is as follows:

**RMTOBJ/SWPONT RSN('TEST SWPON')**

**USER(TEST\_USER)**

This enables the customer to specify the swapped account directly in the interactive swap command.

The original SWPON command still works with the RSN parameter only, as before.

### Compliance

SEC-598



New Object Authority commands were introduced to manage compliance object authority templates. The commands enable a user to manage compliance object authority templates from his own in-house software.

The commands are:

- **CRTTPLOBJA**: Create a compliance object authority template
- **CHGTPLOBJA**: Change a compliance object authority template (add or remove users from an existing template)
- **DLTTPLOBJA**: Delete a compliance object authority template

The feature applies to compliance templates only. A compliance policy must already exist or a system group must have been defined for the policy.

### Data Providers

SEC-546, 908



The System Audit Data Provider now provides full support for all action type journal codes. All the fields and their descriptions are included and have underscore and quotes to be compatible with Splunk. Additionally, the Key Value Pair message format was added to the System Audit Data Provider header.

## Encryption

SEC-227 Field Encryption and Field Security can now encrypt fields of up to 4,000 characters.

In the Encryption module, in the Field Encryption and Field Security sub-modules, the maximum length of the encrypted field was previously 256 characters. The Encryption module now supports fields of up to 4,000 characters in those 2 sub-modules. In the Field Encryption sub-module, when a field longer than 256 characters is selected, the only field authorizations available are Full Control and Field view and deny update.

SEC-881, 883, 833

The maximum number of field registry entries in all relevant sub-modules (Field Encryption, Field Security, Field Masking, Field Scrambling) has been increased to 32,000. Previously, the maximum was 990 entries.

## General

SEC-592



Added support for General Data Protection Regulation (GDPR) in the Accelerator Package. Additional content is added to the following modules when installing the Accelerator Package:

- Report Generator. A new report group named GDPR which contains predefined reports of all report types. The name of each report in the group begins with GDPR.
- Alert Center. Additional predefined alerts of all alert types including Encryption. The name of each new alert begins with GDPR.
- Compliance. A new compliance policy named GDPR which includes many predefined templates.

By implementing the predefined reports, alerts, and compliance templates, the customer will be compliant with GDPR.

If you have purchased the Accelerator Package, perform the following steps in order to see and access the GDPR changes:

- 1) Access the Green Screen Enforce menu and select Customer License Codes.
- 2) Enter Option 2 (Change) next to Accelerator Package.
- 3) In the Customer License Code screen, press F16 (Execute).
- 4) After the update completes in the Green Screen menu, close the GUI Client and re-open it.

The following table shows the mapping of GDPR articles to the relevant modules in Enterprise Security:

Enterprise Security to GDPR Mapping													
GDPR Category	Article	Compliance	Application access control / Audit	Encryption	Central audit	Firewall	Session timeout/ Inactive Users	Msg Queues	Alert center	Report Generator	File audit	System audit	Security Risk Assessment
Protection of personal data	5, 24, 25, 28, 47	✓	✓	✓		✓	✓						
Privacy/confidentially	5,28,32	✓	✓	✓		✓	✓						
Integrity of data	5, 32		✓		✓				✓	✓	✓		
Encryption / Pseudonymisation	6, 25, 32, 34			✓									
Access control/malicious accidental damage	25, 32	✓	✓			✓	✓	✓	✓	✓	✓		
Compliance to regulations	R:90	✓	✓		✓					✓			✓
Risk assessment	32, 35												✓
Logging and auditing	30		✓		✓	✓		✓		✓	✓	✓	
Security settings and policy	25, 30, 32, 35	✓	✓	✓		✓	✓			✓	✓	✓	
Protection of data processing	5, 44 - 49	✓	✓			✓							
Data breach notification	33, 34		✓		✓			✓	✓	✓	✓	✓	
Personal Data minimization	5, 16, 17, 47, 89				✓						✓	✓	

## Report Generator

SEC-633      The Network Attributes Report was added. It is based on the command to retrieve the network attributes of the system.



The following is a sample report:

System Name	Pending system name	Local network ID	Local control point name	Default local location	Default mode
SYSI61		APPN	SYSI61	SYSI61	

SEC-1026 The Maintenance Report was added to display all maintenance events in the Central Audit.



The following is a sample report:

System	Date	Time	Job Name	Job Number	Program Name	Job User	User	Event Type
SYSI66	6/18/2018	13:19:03	BSFDP00001	241181	BDPFA2	BSAFE	BSAFE	W-WARI
SYSI66	6/18/2018	14:05:08	BSFDP00001	241192	BDPFA2	BSAFE	BSAFE	W-WARI
SYSI66	6/26/2018	15:46:19	QRWTSRVR	240349	LDRPSTBJE	QUSER	ENFORCEGUI	W-WARI
SYSI66	7/4/2018	09:17:36	QRWTSRVR	240349	LDRPSTBJE	QUSER	ENFORCEGUI	W-WARI

## Fixes included in version 8.3.03

This list includes all relevant changes and fixes since version 8.3.2:

### Alerts

SEC-564 Added detailed formatting in alerts for the following entry types: OW, RJ, CO, DO, ZC, ZR.

SEC-732 The Alert Center Message Queue monitor now sends alerts as expected.

SEC-752 An incorrect timestamp in the History Log Alert type was corrected.

- SEC-812 In System Audit alerts, updating a group or alert no longer requires a restart of the job for the changes to take effect.
- SEC-940 The MCH1202 error no longer occurs in File Audit alerts.
- SEC-1038 The Alert Manager now opens as expected.

## Application Access Control

- SEC-728 The Database log exit program now appropriately sets the library list at the database logon stage.
- SEC-826 SQL statements that include an UPDATE with Embedded Select have been corrected to be logged as updates.
- SEC-902 SWPOFF no longer fails with the CPF9898 error when the Initial Menu is defined as SYSTEM in the User Profile.
- SEC-1003 The Object Group Manager job will now function properly when an object exists in two or more object groups and the user does not have permission to these object groups.
- SEC-1022 The file CTC0001P is no longer locked by BSFAPCH server when updating command control.

## Compliance

- SEC-680 The Compliance report now shows the correct system values for multi-system.
- SEC-787 The deviation calculations in the Compliance Assessment are now correct.

## Data Providers

- SEC-530 The System Audit Data Provider now correctly displays the Password Expired \*NO indicator.
- SEC-531 In System Audit Data Provider, when using CHGUSRPRF to grant the \*JOBCTL special authority and then remove it, the activity is captured correctly in Splunk.
- SEC-532 All action types of System Audit Data Provider now appear correctly in Splunk.
- SEC-616 The "Syntactic error in Conditions" error no longer occurs when using the condition filter within the System Audit Data Provider module.
- SEC-624 It is now possible to start or end real-time monitor jobs from the green screen, using the commands **STRDPRJOB** (Start DP Real-time monitor job) and **ENDDPRJOB** (End DP Real-time monitor job).
- SEC-639 Improved performance of the RCVJRNE job in the System Audit Data Provider.
- SEC-664 The CPF225E error no longer occurs in the Message Queue Data Provider.
- SEC-715 Data Provider History log performance improvement.
- SEC-746 Application Audit Data Providers now send a message with severity 00 (instead of 80) at the end of the job.
- SEC-747 Improved condition filtering performance of the System Audit Data Provider.
- SEC-785 The System Audit Data Provider error message "Unable to Send to SYSLOG" was improved to include more details.
- SEC-793 Improved performance of QHST Log Audit Data Provider.

- SEC-801 Modifications have been made to the error log function in the Data Provider modules to provide a detailed error log when communication errors are detected.
- SEC-825 The Data Provider history log job no longer fails with the CPF9898 error when there are more than 26 files with the same date.
- SEC-838 The escape message CPF0818 is no longer logged to the System Audit Data Provider joblog.
- SEC-920 The System Audit Data Provider no longer fails with the MCH1202 (Decimal Data) error.
- SEC-1193 In the File Audit Data Provider, the destination (**dst**) field now contains a value.

## Disaster Recovery and High Availability

- SEC-768 The BSFHAROLC program now changes or creates the ENFREP user profile for LPAR replication correctly.

## Encryption

- SEC-989 Error CPF501B is no longer received in Field Encryption when a file that has an absolute value, digit, zone or alternative collating sequence defined for the key field.
- SEC-576 Authorities are now copied correctly when copying the field registry of a hexadecimal field.

## File Audit

- SEC-819 File audit now supports Graphic field types.
- SEC-895 The File Audit report will continue processing when a file or member no longer exists on the system.

## File Protection

- SEC-848 The RNX8001 error no longer occurs when running initialization.

## General

- SEC-307 Logon performance has been improved.
- SEC-454 Resolved License Key translation issues for environments running under CCSID in German and French.
- SEC-585 The CPD0083 error no longer occurs when adding the Health monitor to the scheduler.
- SEC-894 An optional parameter was added to the command RMTOBJ/BSFHAROLC (initialize Enterprise Security) to indicate where to send the status messages. Entering the parameter \*JOB sends status messages to the job executing BSFHAROLC. Entering \*SYSOPR sends status messages to the QSYSOPR message queue. The command can also be run without any parameter, as previously.

## Inactive Users

- SEC-731 The Extended Security Restore Inactive User function now also restores the user as a member of a User Group to which they were defined prior to the delete operation.

SEC-742 The DLTPRFCLU job now correctly deletes user profiles due to inactivity in all configured nodes.

## Message Queue Audit

SEC-937 When adding a message queue schedule entry, a "Cannot retrieve job name" error is no longer received.

## Report Generator

- SEC-456 The "Cannot find action type" error no longer appears when viewing Import Report Definitions.
- SEC-492 The System Audit report defined with action type "SK" and Receiver \*CURCHAIN now includes all records in the specified date range.
- SEC-521 Corrected missing descriptions on reports in the Report Generator Module.
- SEC-609 The File Audit Report now correctly displays entry specific data.
- SEC-673 The System Value Change report and the User Profile Change report are now produced correctly.
- SEC-730 Corrected Report generator application audit error when selecting a function with "OR".
- SEC-743 Added the IFS output CCSID parameter to the Report Generator Global Settings.
- SEC-760 The System Audit (detailed) report with Run type Periodic now runs correctly.
- SEC-781 The File Shares report now displays the system name rather than the serial number.
- SEC-788 Report dates and times are now correct for reports with Periodic selected as the run type.
- SEC-811 The Program Information report will no longer move user spaces created with \*LIB QRPLOBJ.
- SEC-835 The User Profiles Report for a System Group now retrieves members of the remote user group from the remote system.
- SEC-837 The SQL Statements report displays the IP address field correctly, without an extra decimal point.
- SEC-928 The Disabled Profile report will continue processing when encountering a CPF2203 error.
- SEC-952 The Task Manage Condition Group in the Report Generator Module will now properly send reports to two different directories as defined.
- SEC-995 All fields in the Encryption Audit and Encryption Maintenance reports are now compatible with DBCS.
- SEC-1013 The Security Log report now reports the correct product version.
- SEC-1026 The Maintenance report type was added to display all events in the Central Audit.
- SEC-1188 The 'Could not process report query' error no longer occurs when running the System Audit (detailed) report.

## SQL Audit

SEC-591 The SQEXTRACT job no longer fails with RNX0115.

SEC-892 SQL Audit now logs inserts on systems running versions V6R1 and above up to (but not including) version V7R3.

## System Audit

- SEC-419 The "Error in Date format invalid input values" error no longer appears when accessing the System Audit module.
- SEC-504 The Action Groups \*OFCSR, \*OPTICAL and \*ATNEVT have been enabled in the Custom Action Group Manager and the Detailed Custom Action Group Manager.
- SEC-849 The Full Monitoring of User's Activity Report (Report #67) in System Audit Reports now displays the correct number of users.
- SEC-893 The System Audit filter now works correctly when User, Action Group \*AUTFAIL and Action Type PW are selected.
- SEC-978 When an entry is added to the System Audit Report Scheduler, the job runs correctly on the specified day.

## User Profiles

- SEC-782 User Profile ENFREP is now created when using the move procedure.
- SEC-821 The copy/replace/merge function now replicates as expected when adding a User Profile to an existing User Group.
- SEC-951 User Profiles are no longer disabled when using the "Generate Password" feature in the User Profile module and not selecting **Enable user**.
- SEC-959 User Profile replication is now correctly setting the password to expired.