

IBM Security zSecure V2.4.0
Service Stream Enhancement (SSE)

*MQ auditing, Command Audit Trail,
compliance automation, and other
enhancements*
IBM Security zSecure Messages Guide



Chapter 1. About this document

This document describes the documentation updates as a result of the Service Stream Enhancement (SSE) for MQ auditing, Command Audit Trail, compliance automation, and other enhancements (APAR numbers OA59807, OA59823, OA59861, and OA59862).

The following enhancements were made for this zSecure V2.4.0 SSE:

- MQ auditing:
 - New report types:
 - MQ_AUTHINFO to report on MQ authentication information objects.
 - MQ_CHLAUTH to report on MQ channel authentication records.
 - The MQ_REGION reports show the following:
 - Authentication information object for user ID and password authentication.
 - Certificates that the queue manager and queue sharing group use.
 - Presence of various switch profiles.
 - The MQ_CHANNEL report type identifies the security exit and the user data that is passed to it, as well as the channel's certification label.
 - The disposition of inbound transmissions has been added to the MQ_INIT reports.
- STIG controls:
 - Automation of more STIG controls: 17 for RACF, 8 for ACF2, and 8 for Top Secret.
 - Equivalent of STIG controls RACF0570 and RACF0580 that allow for password phrases in addition to passwords are provided in the zSecure Extra standard.
 - General improvements for checking general access and logging requirements.
- Command Verifier:
 - Various enhancements have been made to the Command Audit Trail.
 - Multiple commands can now be specified in a pre-command or post-command policy profile.
- Selection on audit and global audit settings are added to the RA.D and RA.R menu options.
- Db2 102 IFCid 106 events (Security parameters at start-up/reload) are now sent to IBM QRadar SIEM and Micro Focus ArcSight.
- Performance improvements are made for ACF2 TRUSTED reporting.
- ICSF settings are added to the IPL parameters report.
- Automatic sensitivities are added, for example, for inaccessible LPA or linklist libraries.
- New fields FALLBACK_DATASET are added to the SENSDSN report type to identify secondary, duplex, or backup RACF data sets.

The documentation updates apply to zSecure V2.4.0. Each of the following links includes a PDF file with the updates for the subject publication: :

- [*zSecure CARLa-Driven Components Installation and Deployment Guide*](#)
- [*zSecure Messages Guide*](#)
- [*zSecure Admin and Audit for RACF User Reference Manual*](#)
- [*zSecure Audit for ACF2 User Reference Manual*](#)
- [*zSecure Audit for Top Secret User Reference Manual*](#)
- [*zSecure CARLa Command Reference*](#)
- [*zSecure Command Verifier User Guide*](#)

Note:

- The revision bars in the margin indicate updates since publication of [Further Automation Of DISA STIG Resource Controls And Other Enhancements \(OA59004, OA59006\)](#) on April 11, 2020.
- Referenced or linked topics that have not changed are not included in this document. You can find them in the publication that the chapter applies to.
- The *zSecure (Admin and) Audit User Reference Manuals* and the *zSecure CARLa Command Reference* are available to licensed clients only. To access the zSecure V2.4.0 licensed documentation, you must sign in to the [IBM Security zSecure Suite Library](#) with your IBM ID and password. If you do not see the licensed documentation, your IBM ID is probably not yet registered. Send a mail to zDoc@nl.ibm.com to register your IBM ID.

Incompatibility warnings**STIG members renamed for controls AAMV0410 and AAMV0420**

<i>Table 1. SCKRCARL generic member names renamed for RACF, ACF2, and Top Secret systems</i>			
Original member name	Renamed - for RACF system	Renamed - for ACF2 systems	Renamed - for Top Secret systems
C2RGM410	CKAGM410	C2AGM410	CKTGM410
C2RGM420	CKAGM420	C2AGM420	CKTGM420

Multiline mixed SBCS/DBCS strings

With previous versions of CARLa and CKGRACF, within a string literal crossing a line boundary, if a line ended with a shift-in (SI) character and an optional space, and if the next line started with a shift-out (SO) character, the SI character, optional space, and SO character were trimmed away by the parser. This trimming behavior has been extended as follows.

Within a string literal crossing a line boundary, if a continuation line starts with an SO character, optionally preceded by Single-byte Character Set (SBCS) space characters, lines immediately preceding this line are trimmed away if they entirely consist of SBCS spaces. Trailing SBCS spaces in the line before these blank lines, if any, are trimmed away as well. If the trimmed line ends with an SI character and the continuation line starts with an SO character, these SI and SO characters are trimmed away, too.

Double-byte Character Set (DBCS) space characters are typically used for non-Roman character languages, like Japanese.

For more information, see "Syntax rules" in *zSecure CARLa Command Reference*.

Chapter 2. zSecure Messages Guide

The following messages were updated or added:

CKR1747 **Missing FS up link at *callid* from *DIREaddr1* on system *system* while processing *DIREaddr2* *relativepathname***

Explanation

A root directory entry DIRE1 could not be related to its file system. This may cause the path evaluation for DIRE2 to fail, which might cause incorrect output for the ATTR, AUDITCONCERN and AUDITPRIORITY fields. See the Electronic Support Web site for possible maintenance associated with this message. If you cannot find applicable maintenance, follow the procedures described in [Contacting IBM Support](#) to report the problem.

Severity

24

CKR2079 **CKFCOLL PARMLIB members due to simulated IPLPARM in *source***

Explanation:

This message shows, in continuation lines, the PARMLIB member names that will be processed because of a DEBUGSIMIPLPARM command parameter in the CKFCOLL input.

Severity

00

C4R915E **Pre-command failed, processing terminated**

Explanation:

The specified pre-command abended or failed with a return code greater than 4. Remaining pre-commands, the main RACF command, and post-commands (if any) are not executed.

User response:

If the specified pre-command is incorrect, contact your zSecure Command Verifier administrator to correct the specified pre-command.

C4R916E **Main RACF command failed, processing terminated**

Explanation:

The specified main RACF command abended or failed with a return code greater than 4. Post-commands (if any) are not executed.

User response:

Correct the specified main RACF command.

C4R917E **Post-command failed, processing terminated**

Explanation:

The specified post-command abended or failed with a return code greater than 4. Remaining post-commands are not executed.

User response:

If the specified post-command is incorrect, contact your zSecure Command Verifier administrator to correct the specified post-command.

C4R998W **Could not open C4RDEBUG, debug processing will be skipped**

Explanation:

zSecure Command Verifier could not open the C4RDEBUG file. Debug processing is skipped.

