

z/OS 3.2 IBM Education Assistant

Solution Name: zSecure 3.1 service stream enhancements (SSEs) up to 2025-02

Solution Element(s): 5655-ABB 5655-ABC 5655-ABA 5655-ABD 5655-ABE 5655-ABG 5655-CC1

July 2025



Agenda

- Trademarks
- Objectives
- Overview
- zSecure Admin Web UI
- zSecure Command Verifier enhancements
- Compliance advances
- Unit Of Work ID
- Running started tasks under MSTR
- IBM Threat Detection for z/OS
- Report type RESOURCE
- Ideas
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks:
 - Center for Internet Security, CIS, and CIS Benchmark are trademarks of the Center for Internet Security (an independent nonprofit organization)
 - ACF2 is a trademark of Broadcom

Objectives

Describe new function added to zSecure 3.1 after September 2023

- zSecure Admin 3.1.1 with web user interface (z/OSMF plug-in)
- zSecure Command Verifier enhancements
- Compliance standard advances
- Selection of events by Unit-Of-Work ID
- Running started tasks under MSTR
- and more

Notes:

- zSecure function updates typically ship in sets called Service Stream Enhancements. These were provided in [April 2024](#), [October 2024](#), and [January 2025](#).
- In addition, there are quarterly STIG updates (Dec23, Mar24, May24, Aug24, Nov24, Mar25)
- And timely compatibility updates for new z/VM, CICS, etc. releases

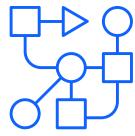
Overview

- Who (Audience)
 - Systems programmers, Security administrators, Auditors, Compliance Assessors
- What (Solution)
 - Makes security administration, security compliance, and security compliance checking easier
- Wow (Benefit / Value, Need Addressed)
 - Reduces need for green screen skills by allowing web browser interaction
 - Improved capturing and tracking of security events
 - Improved compliance standard coverage and automation

zSecure Admin Web UI

Based on customer feedback, the new zSecure Admin GUI addresses a need to simplify RACF administration and provide a more user-friendly environment for experienced and new RACF admins.

[ZVISUAL-I-27](#)



Simplified management

A web-based zSecure plugin for z/OSMF to administer, control and customize certain security tasks



Secure administration

Establishes secure connection directly with RACF via z/OSMF and verifies user credentials



Pre-built role management

Access to functions is based on customizable roles with pre-built roles for helpdesk, admins etc.



Modern design

Based on IBM Carbon, the design language of the interface is easy to grasp and use

Quick functionality overview

zSecure Admin 3.1.1 Web-based GUI

• Menu options

- A full-fledged menu is available with multiple RACF options:
 - USER
 - GROUP
 - DATASET
 - RESOURCE
 - SETTINGS
 - CERTIFICATES

• RACF line commands

- Use common line commands such as COPY or DELETE for RACF entries directly through the GUI

• Customization

- Ability to customize various aspects of the GUI such as individual fields, layout of the applications etc.

• Multi-system support via CKNSERVE

- Access Live RACF database of multiple systems from one location.

• Character-set support

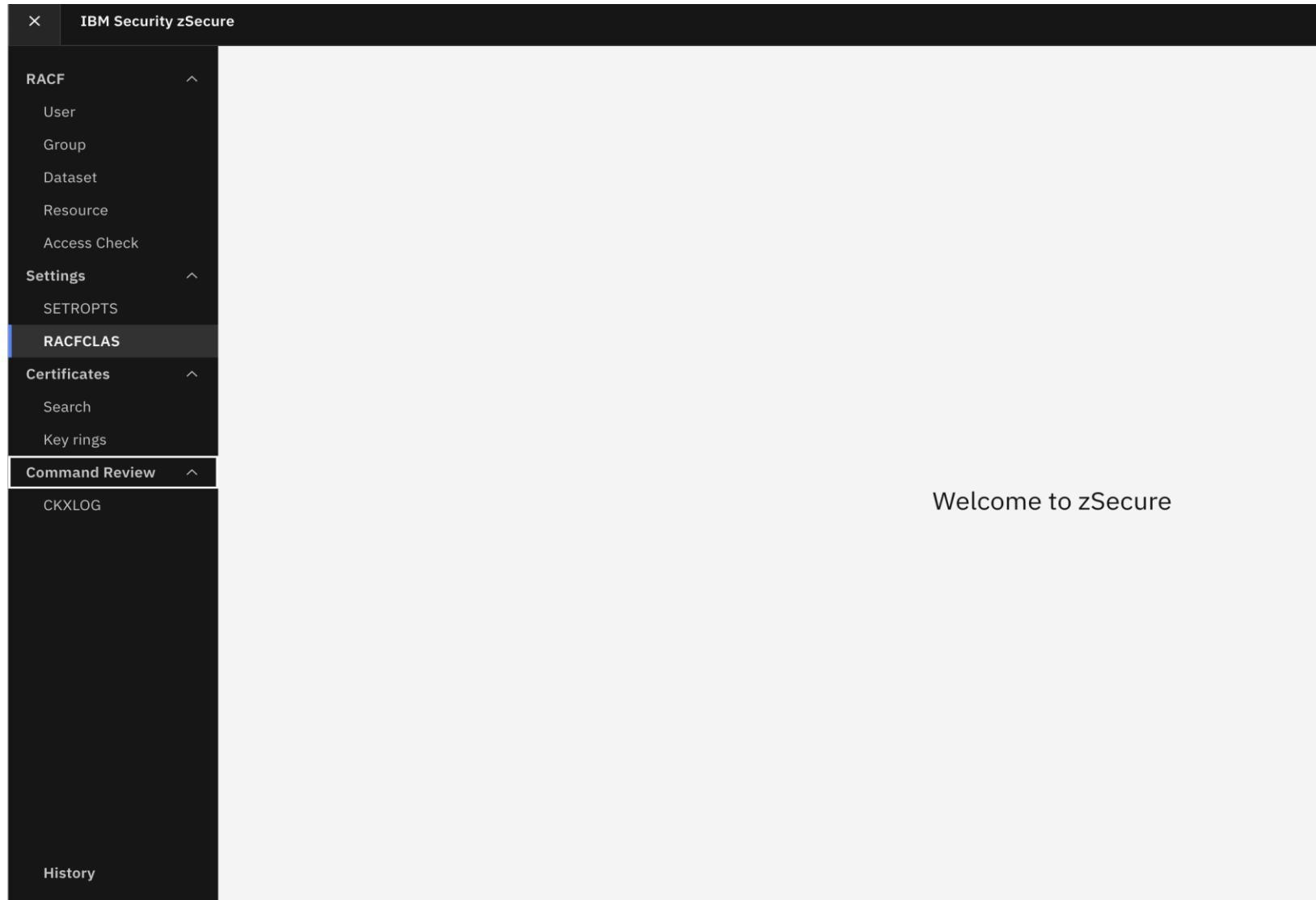
- Support for non-standard character sets such as Danish, Hebrew and more.

Export, Ticket ID support and more...

Quickly export data in PDF or Excel formats

Integrate with Helpdesk workflows with support of Ticket-ID and Ticket descriptions

Expanded Drop Down Menu



User Selection

IBM Security zSecure



RACF / User /

User selection

Show userids that fit all of the following criteria

[Reset form fields](#) [Clear input fields](#)

Userid

user profile key or filter

Name

name/part of name, no filter

Owned by

group or userid, or filter

Default group

group or filter

Connect group

group or filter

Installation data

data scan, no filter except *

Other Fields



Attributes



Segments



Run

User Selection – Other Fields

IBM Security zSecure

RACF / User /

User selection

Show userids that fit all of the following criteria

Reset form fields Clear input fields

Userid user profile key or filter	Name name/part of name, no filter	Owned by group or userid, or filter	Default group group or filter
Connect group group or filter	Installation data data scan, no filter except *		
Other Fields			
Last logon/connect - Select - <input type="button" value="yyyy-mm-dd"/>	Last logon/update - Select - <input type="button" value="yyyy-mm-dd"/>	Password changed - Select - <input type="button" value="yyyy-mm-dd"/>	Passphrase changed - Select - <input type="button" value="yyyy-mm-dd"/>
Creation date - Select - <input type="button" value="yyyy-mm-dd"/>	Revoke date - Select - <input type="button" value="yyyy-mm-dd"/>	Schedule name schedule name or filter	Complex complex name or filter
MFA factor name factor name or filter	MFA policy name policy name name or filter	Password Interval number or Y/N	Passphrase Interval number or Y/N
Logdays Selection <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat			
Attributes			
Segments			
<input type="button" value="Run"/>			

User Selection – Attributes

IBM Security zSecure

RACF / User /

User selection

Show userids that fit all of the following criteria

Userid ⓘ
user profile key or filter

Name ⓘ
name/part of name, no filter

Owned by ⓘ
group or userid, or filter

Default group ⓘ
group or filter

Connect group ⓘ
group or filter

Installation data ⓘ
data scan, no filter except *

Other Fields

Attributes

System wide and group authorizations ⓘ

Logical operator
 OR AND

Logon status ⓘ

Logical operator
 OR AND

User properties ⓘ

Logical operator
 OR AND

CKGRACF features ⓘ

Logical operator
 OR AND

Segments

Reset form fields Clear input fields

Special Operations Auditor RO-auditor Group-special Group-oper Group-audit Class-auth

Revoked Inactive Protected Password expired Revoked group Certificate Pass phrase Phrase expired When day/time ID mapping Password legacy

Phrase legacy MFA MFA active MFA fallback Password

Has RACLINK Restricted User audited Mixed case password

Queued commands Schedules Userdata MultiAuthority

Run

User Selection – Segment selection

IBM Security zSecure

RACF / User /

User selection

Show userids that fit all of the following criteria

Userid ?
user profile key or filter

Name ?
name/part of name, no filter

Owned by ?
group or userid, or filter

Default group ?
group or filter

Connect group ?
group or filter

Installation data ?
data scan; no filter except *

Other Fields

Attributes

Segments (1 active filters)

Presence

CICS - Transaction processing user

Absence

- Select segment -

Find users without a specific segment

Show segments

All BASE CICS CSDATA DCE DFP EIM KERB LANGUAGE LNOTES NDS NETVIEW OMVS OPERPARM OVM PROXY TSO WORKATTR

CICS (Selection criteria)

Operator Identification ?

Operator priority ?
- Select -

Terminal time-out value ?
- Select -

XRF Re-signon option ?
- Select -

Operator class ?
- Select -

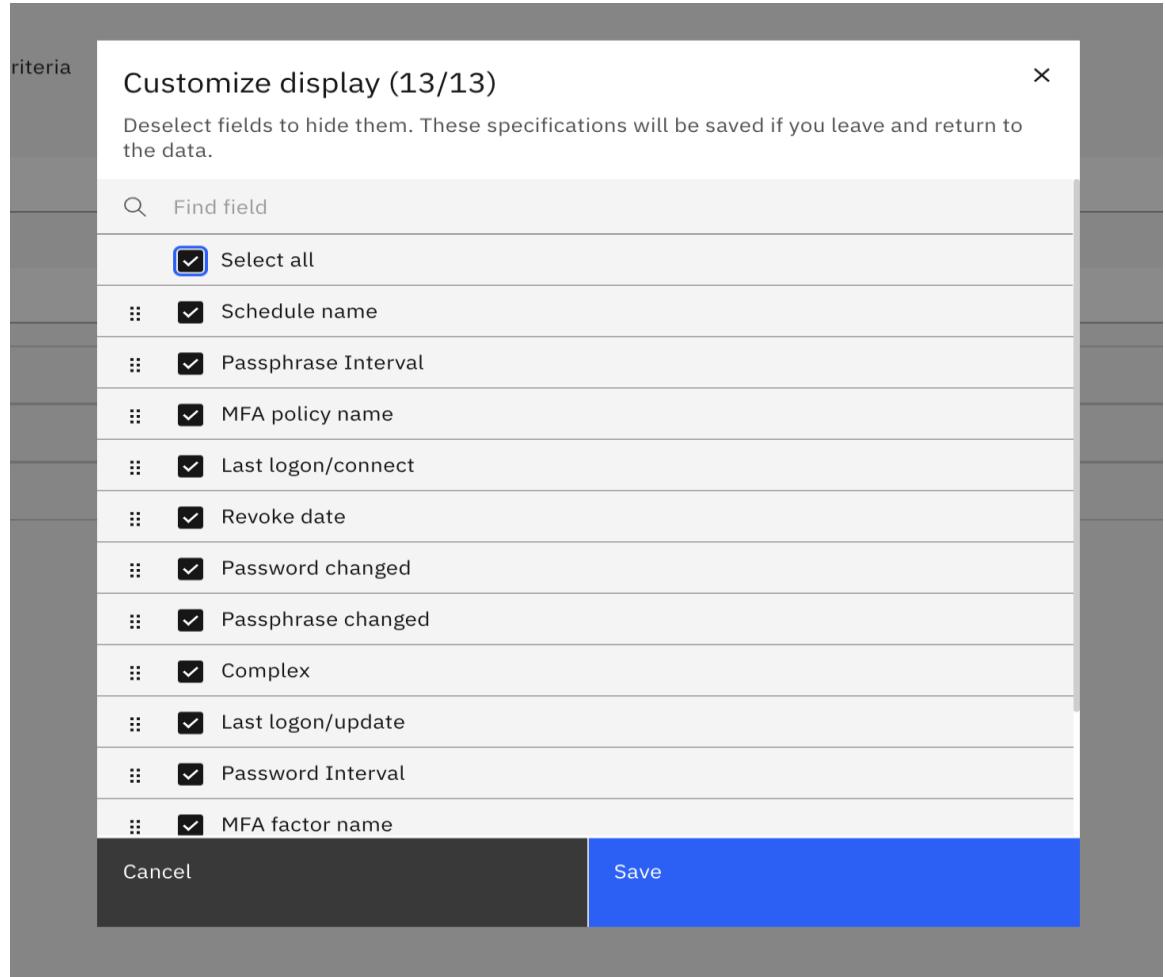
Resource SecurityLvl keys ?

Transaction SecurityLvl keys ?

Run

Reset form fields ? Clear input fields ?

Customization options for fields in selection and selection results pages



The screenshot shows a table titled "User selection results" with columns "User" and "Complex". The table lists several user entries with their respective User IDs and Complex values. Overlaid on the table is a modal dialog titled "Customize display (51/51)". This dialog has a similar message and search bar as the first one. Its list of checked items includes: User, Complex, Name, DfltGrp, Owner, Revoked, Inactive, Restricted, Protected, Special, Operator, and Auditor. At the bottom of the dialog are "Cancel" and "Save" buttons. The "Save" button is highlighted with a blue background. The main table below the dialog shows pagination at the bottom: "Items per page: 20" and "1–20 of 4178 items".

User Selection results – Select Users, Search bar, Search by column

IBM Security zSecure

RACF / User / User Selection Results /

User selection results

All users

Search by column: All ▾

[Download Report](#)

User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth
\$\$TEST12	PLEX1	\$\$SSTEST9 FDFD	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$\$TEST13	PLEX1	\$\$SSTEST9	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$\$TES2	PLEX1	TES2	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$\$TES5	PLEX1	TES5	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$CRMBSHT	PLEX1	TES5	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$\$SSTEST7	PLEX1	MIKI	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–
\$\$SSTEST9	PLEX1	\$\$SSTEST9	SYSAUTH	SYSAUTH	Revoked	–	–	Protected	–	Operator	–	–	–	–
\$TESTM	PLEX1	\$TESTM	CRMB	CRMB	–	–	–	Protected	Special	–	Auditor	–	–	–
\$TESTM1	PLEX1	\$TESTM1	CRMB	CRMB	Revoked	–	–	Protected	Special	–	Auditor	–	–	–
AEISA	PLEX1	EISA ALICE1	OMVS	ROOT	–	Inactive	–	–	Special	Operator	–	–	–	–
BL	PLEX1	LAUFMAN, BLAINE J.	OMVS	IBMUSER	Revoked	Inactive	–	–	Special	Operator	–	–	–	–
CRMAINT	PLEX1	CONSUL GROUP ADMIN	CRMA	CRMA	–	Inactive	–	–	Special	–	–	–	GroupSOA	ClAuth
CRMAROB	PLEX1	ROB VAN HOBOKEN	CRMA	CRMA	–	Inactive	–	–	Special	–	–	–	–	–

Items per page: 20 ▾ 1–20 of 179 items

1 ▾ of 9 pages ▶ ▷

User selection results - Action button options

RACF / User / User Selection Results /

User selection results

[Download Report](#)

All users

User selection results															
Search by column:		All	Press Enter to search												
User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth	
⋮	\$\$TEST12	PLEX1	\$\$SSTEST9 FDFD	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	
Show additional information		\$\$SSTEST9	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
RACF list user all		TES2	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
Revoke user		TES5	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
Resume user		TES5	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
Change password or phrase and resume		MIKI	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
Copy User ID		\$\$SSTEST9	SYSAUTH	SYSAUTH	–	–	–	Protected	–	Operator	–	–	–	–	
Delete User ID		\$\$TESTM	CRMB	CRMB	–	–	–	Protected	–	Operator	–	–	–	–	
Add or delete permit for this User ID		\$\$TESTM1	CRMB	CRMB	Revoked	–	–	Protected	Special	–	Auditor	–	–	–	
Show application segments		EISA ALICE1	OMVS	ROOT	–	Inactive	–	–	Special	Operator	–	–	–	–	
Show connects		LAUFMAN, BLAINE J.	OMVS	IBMUSER	Revoked	Inactive	–	–	Special	Operator	–	–	–	–	
⋮	CRMAINT	PLEX1	CONSUL GROUP ADMIN	CRMA	CRMA	–	Inactive	–	–	Special	–	–	–	GroupSOA	ClAuth
⋮	CRMAROB	PLEX1	ROB VAN HOBOKEN	CRMA	CRMA	–	Inactive	–	–	Special	–	–	–	–	–

Items per page: 20 ▾ 1–20 of 179 items

1 ▾ of 9 pages ▶

Action example

RACF / User / User Selection Results /

User selection results

[Download Report](#)

All users

Search by column:		All	▼	<input type="text"/> Press Enter
	User	Complex	Name	
⋮	\$\$TEST12	PLEX1	\$S\$TEST9 FDFD	
⋮	\$\$TEST13	PLEX1	\$S\$TEST9	
⋮	\$\$TES2	PLEX1	TES2	
⋮	\$\$TES5	PLEX1	TESS5	
⋮	\$CRMBSHT	PLEX1	TES5	
⋮	\$S\$TEST7	PLEX1	MIKI	
⋮	\$S\$TEST9	PLEX1	\$S\$TEST9	
⋮	\$TESTM	PLEX1	\$TESTM	
⋮	\$TESTM1	PLEX1	\$TESTM1	
⋮	AEISA	PLEX1	EISA ALICE1	
⋮	BL	PLEX1	LAUFMAN, BLAII	
⋮	CRMAINT	PLEX1	CONSUL GROUP	
⋮	CRMAROB	PLEX1	ROB VAN HOBOK	

RACF listuser \$\$TEST12 output

```
listuser $$TEST12
C4R913I LISTUSER $$TEST12
USER=$$TEST12 NAME=$$TEST9 FDFD          OWNER=SYSAUTH   CREATED=24.123
  DEFAULT-GROUP=SYSAUTH PASSDATE=N/A    PASS-INTERVAL=N/A PHRASEDATE=N/A
  ATTRIBUTES=OPERATIONS
  ATTRIBUTES=PROTECTED
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=UNKNOWN
  CLASS AUTHORIZATIONS=None
  INSTALLATION-DATA=NEW OMVS SEGMENTS WITH MINIMUM VALUES
  NO-MODEL-NAME
  LOGON ALLOWED (DAYS)      (TIME)
-----
ANYDAY                      ANYTIME
  GROUP=SYSAUTH   AUTH=USE     CONNECT-OWNER=SYSAUTH   CONNECT-DATE=24.123
    CONNECTS= 00 UACC=None   LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=None
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=None SPECIFIED
CATEGORY-AUTHORIZATION
  NONE SPECIFIED
SECURITY-LABEL=None SPECIFIED
C4R400W No ticket identifier set
C4R740I No Command Audit Trail for USER $$TEST12
```

Show less ^

ok

	Auditor	ROAudit	GroupSOA	ClAuth
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
tor	-	-	-	-
	Auditor	-	-	-
	Auditor	-	-	-
tor	-	-	-	-
tor	-	-	-	-
	-	-	GroupSOA	ClAuth

Items per page: 20 ▾

1 ✓ of 9 pages ◀ ▶

Copy Command

Copy User ID
Specify copy action to perform from User ID **\$\$TEST12**

Page 1
Copy User ID Page 2
Segments data

To id* ⓘ
Name* ⓘ **\$\$TEST9 FDFD**

Owner* ⓘ **SYSAUTH** Default group* ⓘ **SYSAUTH**

Installation data ⓘ

NEW OMVS SEGMENTS WITH MINIMUM VALUES

Authentication ⓘ

Password Phrase Password & Phrase Protected / No-change

New Password* Repeat Password*

Copy permits only (target id may be a group or a user) ⓘ
 Copy USERDATA and CUSTOMDATA ⓘ
 Specify values for segments data ⓘ
 Revoke new userid ⓘ
 Issue ADDSD/RDEF for dataset and resource profiles related to the user ⓘ
 Copy RACFVARS profiles/members too ⓘ

Cancel Next

Press Enter

Name	Auditor	ROA
\$\$TEST9 FDFD	-	-
\$\$TEST9	-	-
TES2	-	-
TES5	-	-
TES5	-	-
MIKI	-	-
\$\$TEST9	-	-
\$\$TESTM	Auditor	-
\$\$TESTM1	Auditor	-
EISA ALICE1	-	-
LAUFMAN, BLAI	-	-
CONSUL GROUP	-	-
ROB VAN HOBOM	-	-

Copy Command – segment data

Copy User ID
Specify copy action to perform from User ID **\$\$TEST12**

Page 1 Page 2
Copy User ID Segments data

Specify OMVS data for new userid ⓘ

Do not create OMVS segment
 AUTOUID
 Copy UID from the source(Source UID value is)
 Specify new UID value

Shared UID ⓘ

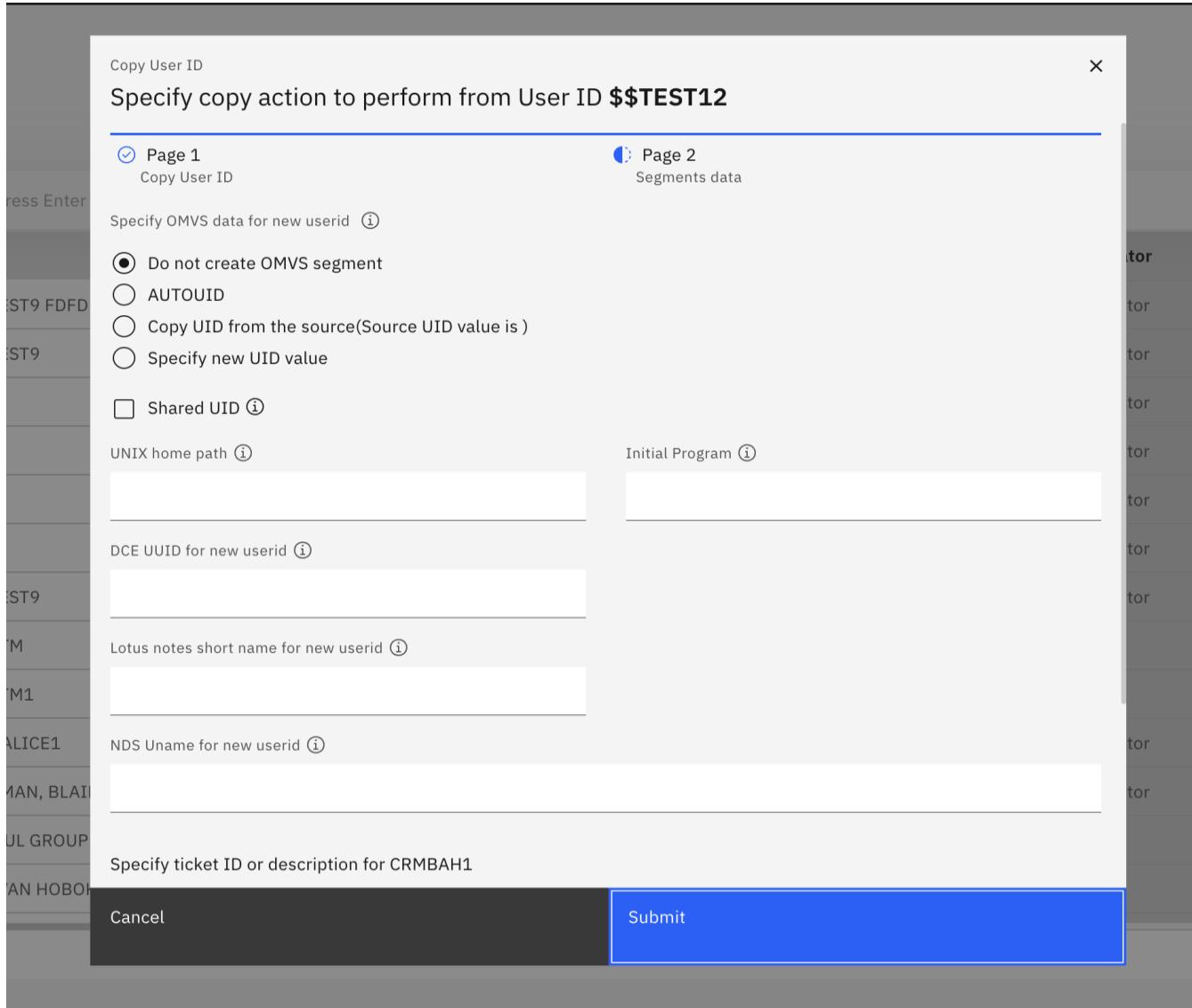
UNIX home path ⓘ Initial Program ⓘ

DCE UUID for new userid ⓘ

Lotus notes short name for new userid ⓘ

NDS Uname for new userid ⓘ

Specify ticket ID or description for CRMBAH1



The dialog box is titled 'Copy User ID' and specifies the action is for User ID '\$\$TEST12'. It is divided into two pages: 'Page 1' (selected) which handles 'Copy User ID', and 'Page 2' which handles 'Segments data'. Under 'Page 1', there are options for specifying OMVS data for the new userid, including creating a new segment (selected), using AUTOUID, copying from source, or specifying a new UID. There are also fields for 'UNIX home path' and 'Initial Program'. Below these are fields for DCE UUID, Lotus notes short name, and NDS Uname. At the bottom, there is a field for 'Specify ticket ID or description for CRMBAH1' and buttons for 'Cancel' and 'Submit'.

Copy Command response output

RACF / User / User Selection Results /

User selection results

All users

Copy User ID \$\$TES2 from \$\$TEST12 is not successful

User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	CIAut
\$\$SSTEST7	PLEX1	MIKI	SYSAUTH	SYSAUTH	-	-	-	Protected	-	Operator	-	-	-	-
\$\$SSTEST9	PLEX1	\$\$SSTEST9	SYSAUTH	SYSAUTH	Revoked	-	-	Protected	-	Operator	-	-	-	-
\$\$TESTM	PLEX1	\$\$TESTM	CRMB	CRMB	-	-	-	Protected	Special	-	Auditor	-	-	-
\$\$TESTM1	PLEX1	\$\$TESTM1	CRMB	CRMB	Revoked	-	-	Protected	Special	-	Auditor	-	-	-
AEISA	PLEX1	EISA ALICE1	OMVS	ROOT	-	Inactive	-	-	Special	Operator	-	-	-	-
BL	PLEX1	LAUFMAN, BLAINE J.	OMVS	IBMUSER	Revoked	Inactive	-	-	Special	Operator	-	-	-	-
CRMAINT	PLEX1	CONSUL GROUP ADMIN	CRMA	CRMA	-	Inactive	-	-	Special	-	-	-	GroupSOA	CIAutl
CRMAROB	PLEX1	ROB VAN HOBOKEN	CRMA	CRMA	-	Inactive	-	-	Special	-	-	-	-	-
CRMASCH	PLEX1	HANS SCHOONE 1	CRMA	CRMA	-	-	-	-	Special	-	-	-	-	-
CRMASC2	PLEX1	HANS SCHOONE	CRMA	CRMA	-	Inactive	-	-	Special	-	Auditor	-	-	-
CRMAUTO	PLEX1	ZTEAM AUTOTASKSCXVXC	SYS1	SYS2	-	-	-	-	Special	Operator	Auditor	-	-	-
CRMBAB1	PLEX1	ALAN BROWN	CRMB	CRMB	-	-	-	-	Special	Operator	-	-	-	-
CRMBAG1	PLEX1	ANURAG GOTHI \$ #	CRMB	CRMB	-	Inactive	-	-	-	-	Auditor	-	-	-

Items per page: 20 ▾ 1–20 of 179 items | 1 ▾ of 9 pages ▶ ▷

History Tab

The screenshot shows a modal window titled "History" with a search bar and a table of audit log entries. The table has columns: Operation Type, zSecnode, Status, Date Time, and Response Details. The entries are:

Operation Type	zSecnode	Status	Date Time	Response Details
Add or delete permit for User ID	PLEX1	Failed	2025-02-14 09:15:07	View Detail
Change password or phrase and resume	PLEX1	Success	2025-02-14 09:14:49	View Detail
Delete User ID	PLEX1	Success	2025-02-14 09:14:27	View Detail
Copy User ID	PLEX1	Failed	2025-02-14 09:10:54	View Detail

At the bottom, there are pagination controls: "Items per page: 10" dropdown, "1–4 of 4 items" text, "1" dropdown, "of 1 page", and navigation arrows.

Click on View Detail for more information

Field Modification on detail page

IBM Security zSecure

RACF / User / User Selection Results / User Detail /

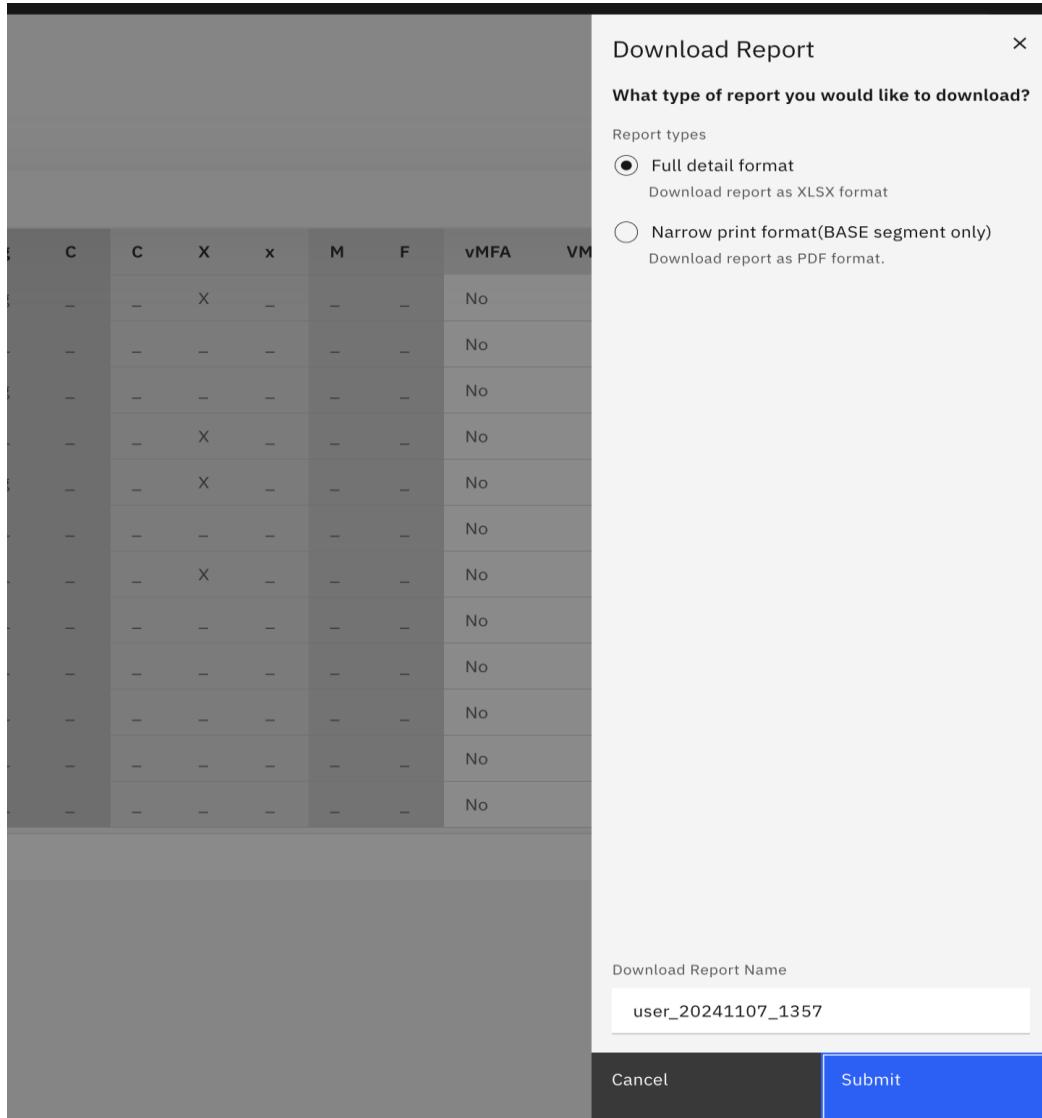
User detail

User TESTER overview

At least one field was modified successfully

User <small>(i)</small> TESTER	Complex <small>(i)</small> SPL87NOD	Name <small>(i)</small> TEST USER	
Installation data <small>(i)</small>			
Owner <small>(i)</small> CRMB	Owner's user name <small>(i)</small>	User's default group <small>(i)</small> CRMB	Dfltgrp's user name <small>(i)</small>
Owner's installation data <small>(i)</small> CRM WERKNEMERS			
Dfltgrp's installation data <small>(i)</small> CRM WERKNEMERS			
Userdata			
System access			
Statistics			
Password			
Password phrase			
Authentication status			

zSecure plugin for z/OSMF – Download report



RACF.GROUP – group selection

IBM Security zSecure

RACF / Group /

Group selection

Show groups that fit all of the following criteria

Group id ⓘ
group profile key or filter

Owner ⓘ
group or userid, or filter

Subgroup of ⓘ
group or filter

With subgroup ⓘ
group or filter

Installation data ⓘ
data scan, no filter except *

Profile Fields

Connect fields

Segments

Run

This screenshot shows the 'Group selection' page in the IBM Security zSecure interface. At the top, there are navigation links for 'RACF' and 'Group'. The main title is 'Group selection' with the subtitle 'Show groups that fit all of the following criteria'. Below this, there are four input fields for filtering groups: 'Group id' (containing 'group profile key or filter'), 'Owner' (containing 'group or userid, or filter'), 'Subgroup of' (containing 'group or filter'), and 'With subgroup' (containing 'group or filter'). There is also a section for 'Installation data' with the value 'data scan, no filter except *'. Below these are three expandable sections: 'Profile Fields', 'Connect fields', and 'Segments', each with a collapse icon. At the bottom right is a large blue 'Run' button.

RACF.DATASET – dataset selection

The screenshot shows the 'Dataset selection' page of the IBM Security zSecure web interface. At the top, there's a navigation bar with icons for home, search, and user profile, and the text 'IBM Security zSecure'. Below the navigation is a breadcrumb trail 'RACF / Dataset /'. The main title 'Dataset selection' is followed by the subtitle 'Show dataset profiles that fit all of the following criteria'. On the right side, there are two buttons: 'Reset form fields' and 'Clear input fields'. The left side contains several filter sections with dropdown menus and placeholder text: 'Dataset Profile' (with 'EGN mask' selected), 'Owned by' (placeholder 'group or userid, or filter'), 'Installation data' (placeholder 'substring or *'), 'High level qual' (placeholder 'qualifier or filter'), 'Profile Fields' (with a dropdown menu), 'Access List' (with a dropdown menu), and 'Segments' (with a dropdown menu). A large blue 'Run' button is located at the bottom right of the filter area.

Dataset selection

Show dataset profiles that fit all of the following criteria

Dataset Profile ①

EGN mask

Owned by ①

group or userid, or filter

Installation data ①

substring or *

High level qual ①

qualifier or filter

Profile Fields

Access List

Segments

Run

RACF.RESOURCE – resource selection

The screenshot shows the 'Resource selection' page of the IBM Security zSecure interface. At the top, there's a navigation bar with icons for home, search, and user profile, and the text 'IBM Security zSecure'. Below the navigation is a breadcrumb trail: 'RACF / Resource /'. The main title 'Resource selection' is followed by the subtitle 'Show resource profiles that fit all of the following criteria'. On the left, there's a sidebar with dropdown menus for 'Resource Profile' (selected), 'Installaton data', 'Profile Fields', 'Access List', and 'Segments'. On the right, there are several input fields: 'Class Name' (containing 'class or filter'), 'Owned by' (containing 'group or userid, or filter'), and three dropdown menus for 'Profile Fields', 'Access List', and 'Segments'. At the bottom right is a blue 'Run' button.

IBM Security zSecure

RACF / Resource /

Resource selection

Show resource profiles that fit all of the following criteria

Resource Profile ⓘ

EGN mask

Installaton data ⓘ

substring or *

Profile Fields

Access List

Segments

Class Name ⓘ

class or filter

Owned by ⓘ

group or userid, or filter

Run

RACF.Access Check

The screenshot shows the 'Access Check' page of the IBM Security zSecure interface. At the top, there is a navigation bar with icons for home, search, and settings. Below the navigation bar, the URL 'RACF / Access Check /' is displayed. The main title 'Access Check' is centered above the form fields. On the right side of the title, there is a link 'Clear input fields' with a trash icon. The form consists of three input fields: 'Userid*' (with a placeholder 'Userid'), 'Class*' (with a placeholder 'DATASET or class'), and 'Profile*' (with a placeholder 'EGN mask'). To the right of these fields is a blue 'Run' button. The background of the page is light gray.

IBM Security zSecure

RACF / Access Check /

Access Check

Userid* ⓘ

Class* ⓘ

Profile* ⓘ

DATASET or class

EGN mask

Run

RACF.SETTINGS – SETROPTS

IBM Security zSecure

RACF / Settings SETROPTS Selection Results / Settings SETROPTS Details /

SETROPTS system settings detail

System setting overview for 8017

Security complex name ⓘ	System name ⓘ
S8017NOD	8017

General RACF properties

Data set protection options

RACF remote sharing options

Default languages

DASD data set protection

Terminal protection

TAPE data set protection

Program protection

Auditing options

Mandatory Access Control options

Identification/Authentication options

Job Entry Subsystem options

RVARY password settings

Password Rules

Submit changes

RACF.SETTINGS – RACF class settings

IBM Security zSecure

RACF / Settings RACFCLAS Selection Results /

RACF class settings

RACF class settings results

Class	Active	Description	Generic	GenCmd	Audit	Logopt	Global	RacList	GenList	Stats	Complex	System	RC	Oper	Pos	Gr
\$C4R	Active	???	Generic	GenCmd	Audit	Profile	Global	RacList		Stats	S8017NOD	8017	4	25		
\$C4RQAR1	Active	???			Audit	Profile					S8017NOD	8017	4	30		
\$C4RQAR2		???				Profile					S8017NOD	8017	4	31		
\$C4RQAR3	Active	???				Profile					S8017NOD	8017	4	32		
#TESEMP		???				Profile					S8017NOD	8017	4	301		
#TESEMPM		???				Profile					S8017NOD	8017	4	301	#	
@LINUX	Active	???	Generic	GenCmd	Audit	Profile	RacList				S8017NOD	8017	4	493		
ACCTNUM	Active	TSO account numbers	Generic	GenCmd		Profile	RacList				S8017NOD	8017	4	126		
ACEECHK	Active	Monitor privilege escalation by ACEE or user token modificat				Profile	RacList				S8017NOD	8017	4	605		
ACICSPCT	Active	CICS program control table	Generic	GenCmd		Profile					S8017NOD	8017	4	5	BO	
AIMS		Resource class for APSB security	Generic	GenCmd		Profile					S8017NOD	8017	4	4		
ALCSAUTH		Supports the Airline Control System/MVS (ALCS/MVS) product				Profile					S8017NOD	8017	4	548		
APPCLU	Active	Verify ID of partner logical units during VTAM session estab	Generic	GenCmd		Profile					S8017NOD	8017	4	118		
APPCPOR		Controls which user IDs can access the system from a given L	Generic	GenCmd		Profile					S8017NOD	8017	4	87		
APPCSERV		Controls whether a program being run by user can act as a se	Generic	GenCmd		Profile					S8017NOD	8017	8	84		

Items per page: 20 ▾ 1–20 of 282 items

1 ▾ of 15 pages ▶

RACF.CERTIFICATES – Certificate selection

The screenshot shows the 'Certificate selection' page of the IBM Security zSecure interface. The top navigation bar includes links for 'IBM Security zSecure', 'RACF', 'Certificates', and 'Search'. The main title 'Certificate selection' is displayed above a search bar. Below the search bar, there is a message: 'Show certificate that fit all of the following criteria'. The search form contains several filter fields:

- Certificate label (1)**: A text input field labeled 'label or filter'.
- Certificate type/owner (1)**: A group of checkboxes for 'Site', 'Certauth', and 'Personal', with a 'filter(* or %)' input field next to it.
- Trust (1)**: A group of checkboxes for 'Trust', 'NoTrust', and 'HighTrust'.
- Start Validity(From:To) (1)**: Two date range inputs for start validity.
- End Validity(From:To) (1)**: Two date range inputs for end validity.
- Creation date(From:To) (1)**: Two date range inputs for creation date.
- Complex (1)**: An input field for 'complex name or filter'.
- Summary by owner (1)**: A checkbox for generating a summary by owner.

A large blue 'Run' button is located at the bottom right of the search area.

RACF.CERTIFICATES – Key rings

IBM Security zSecure

RACF / Certificates / Key rings /

Certificates key rings selection

Show certificate that fit all of the following criteria

Key ring name ⓘ

Key ring owner ⓘ

owner or filter

Creation date ⓘ

- Select -

yyyy-mm-dd

Certificate label ⓘ

Complex ⓘ

complex name or filter

Digital certificates ⓘ

- Select -

Run

This screenshot shows the 'Certificates key rings selection' page in the IBM Security zSecure interface. It features several input fields for specifying search criteria: 'Key ring name' (empty), 'Key ring owner' (set to 'owner or filter'), 'Creation date' (set to '- Select -' with a date input field showing 'yyyy-mm-dd'), 'Certificate label' (empty), 'Complex' (empty), and '# Digital certificates' (empty). At the bottom right is a blue 'Run' button.

RACF.CKXLOG – Command Review CKXLOG

The screenshot shows the 'CKXLOG selection' page within the IBM Security zSecure interface. The top navigation bar includes links for 'Command Review' and 'CKXLOG'. The main title 'CKXLOG selection' is displayed above a search criteria section. The criteria section contains four input fields: 'Userid' (containing 'user profile key or filter'), 'Job name' (containing 'job name or EGN mask'), 'System' (containing 'system or EGN mask'), and 'Class' (containing 'class or EGN mask'). Below these are fields for 'Profile' (containing 'profile or EGN mask') and 'Ticket id' (containing 'search'). A dropdown menu for 'Summarize By' is shown with the option '- Select -'. In the bottom right corner, there is a blue 'Run' button.

Dark theme support

IBM Security zSecure

RACF / User / User Selection Results /

User selection results

All users

Search by column: All ▾ Press Enter to search

Add user/segment

User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth
\$\$\$\$AAA1	PLEX1		CRMB	CRMBMT1	Revoked	-	-	-	-	-	-	-	-	-
\$\$\$\$AAA2	PLEX1	TEST USER2	CRMB	CRMBXYZ	Revoked	-	Restricted	Protected	-	-	-	-	-	-
\$\$\$\$AA91	PLEX1	TEST USER2	CRMB	CRMBXYZ	Revoked	-	Restricted	-	-	-	-	-	-	-
\$\$\$\$AOP2	PLEX1	TEST USER2	CRMB	CRMBXYZ	Revoked	-	Restricted	Protected	-	-	-	-	-	-
\$\$\$\$001	PLEX1	\$\$\$\$001	CRMB	CRMBAH1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAAA7	PLEX1		CRMB	CRMBMT1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAACC	PLEX1		CRMB	CRMBMT1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAA2	PLEX1		CRMB	CRMBAH1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAA3	PLEX1		CRMB	CRMBAH1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAA88	PLEX1	\$\$\$\$AAA88	CRMB	CRMBMT1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAPAA	PLEX1	TEST USER	CRMB	CRMBMT1	-	-	-	Protected	-	-	-	-	-	-
\$\$\$\$AAPW	PLEX1	\$\$\$AAPW \$\$\$AAPRER3	CRMB	CRMB	Revoked	-	-	Protected	-	-	-	-	-	-
\$\$AAPH12	PLEX1		CRMB	CRMBAH1	-	-	-	Protected	-	-	-	-	-	-

Items per page: 20 ▾ 1–20 of 4178 items

1 ▾ of 209 pages

SHOWLOG

Web UI – failed COPY

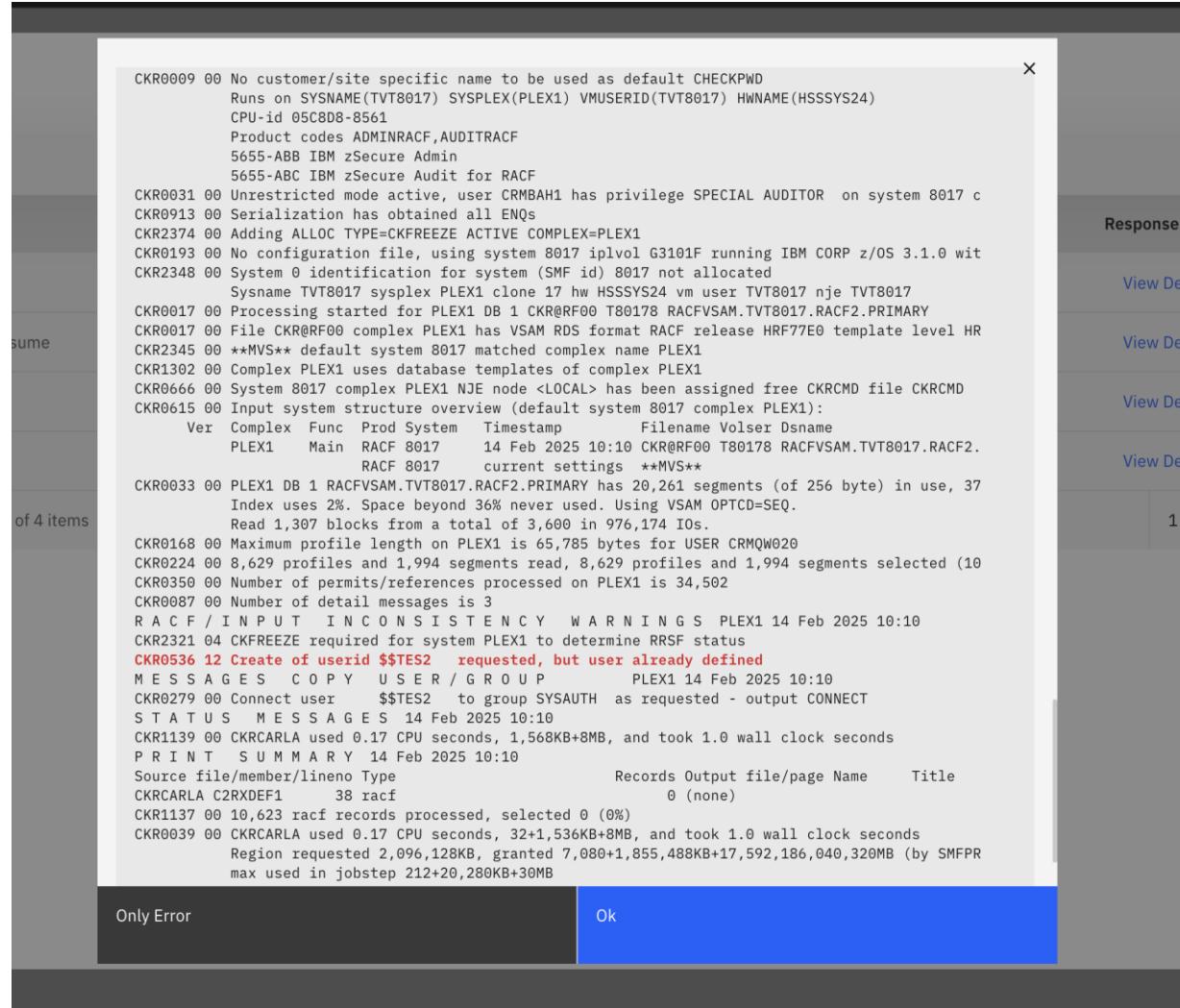
The screenshot shows a web-based interface for monitoring database operations. A modal dialog box is overlaid on the main table, displaying an error message: "CKR0536 12 Create of userid \$\$TES2 requested, but user already defined". The main table lists two rows of data:

zSecnode	Status	Date Time	Response Details
PLEX1	Failed	2025-02-14 09:15:07	View Detail
PLEX1	Success	2025-02-14 09:14:49	View Detail

At the bottom of the modal, there are two buttons: "Full SYSPRINT" and "Ok".

Click on View Detail for more information

Web UI - Copy output (Full SYSPRINT)



CKR0009 00 No customer/site specific name to be used as default CHECKPWD
Runs on SYSNAME(TVT8017) SYSPLEX(PLEX1) VMUSERID(TVT8017) HWNAME(HSSSYS24)
CPU-id 05C8D8-8561
Product codes ADMINRACF,AUDITRACF
5655-ABB IBM zSecure Admin
5655-ABC IBM zSecure Audit for RACF

CKR0031 00 Unrestricted mode active, user CRMBAH1 has privilege SPECIAL AUDITOR on system 8017 c

CKR0913 00 Serialization has obtained all ENQs

CKR2374 00 Adding ALLOC TYPE=CKFREEZE ACTIVE COMPLEX=PLEX1

CKR0193 00 No configuration file, using system 8017 iplvol G3101F running IBM CORP z/OS 3.1.0 wit

CKR2348 00 System 0 identification for system (SMF id) 8017 not allocated
Sysname TVT8017 sysplex PLEX1 clone 17 hw HSSSYS24 vm user TVT8017 nje TTVT8017

CKR0017 00 Processing started for PLEX1 DB 1 CKR@RF00 T80178 RACFVSAM.TVT8017.RACF2.PRIMARY

CKR0017 00 File CKR@RF00 complex PLEX1 has VSAM RDS format RACF release HRF77E0 template level HR

CKR2345 00 **MVS** default system 8017 matched complex name PLEX1

CKR1302 00 Complex PLEX1 uses database templates of complex PLEX1

CKR0666 00 System 8017 complex PLEX1 NJE node <LOCAL> has been assigned free CKRCMD file CKRCMD

CKR0615 00 Input system structure overview (default system 8017 complex PLEX1):

Ver	Complex	Func	Prod	System	Timestamp	Filename	Volser	Dname
	PLEX1	Main	RACF	8017	14 Feb 2025 10:10	CKR@RF00	T80178	RACFVSAM.TVT8017.RACF2.
				RACF	8017			current settings **MVS**

CKR0033 00 PLEX1 DB 1 RACFVSAM.TVT8017.RACF2.PRIMARY has 20,261 segments (of 256 byte) in use, 37
Index uses 2%. Space beyond 36% never used. Using VSAM OPTCD=SEQ.
Read 1,307 blocks from a total of 3,600 in 976,174 IOs.

CKR0168 00 Maximum profile length on PLEX1 is 65,785 bytes for USER CRMQW020

CKR0224 00 8,629 profiles and 1,994 segments read, 8,629 profiles and 1,994 segments selected (10

CKR0350 00 Number of permits/references processed on PLEX1 is 34,502

CKR0087 00 Number of detail messages is 3

R A C F / I N P U T I N C O N S I S T E N C Y W A R N I N G S PLEX1 14 Feb 2025 10:10

CKR2321 04 CKFREEZE required for system PLEX1 to determine RRFS status

CKR0536 12 Create of userid \$\$TES2 requested, but user already defined

M E S S A G E S C O P Y U S E R / G R O U P PLEX1 14 Feb 2025 10:10

CKR0279 00 Connect user \$\$TES2 to group SYSAUTH as requested - output CONNECT

S T A T U S M E S S A G E S 14 Feb 2025 10:10

CKR1139 00 CKRCARLA used 0.17 CPU seconds, 1,568KB+8MB, and took 1.0 wall clock seconds

P R I N T S U M M A R Y 14 Feb 2025 10:10

Source file/member/lineno	Type	Records	Output file/page	Name	Title
CKRCARLA	C2RXDEF1	38 racf	0	(none)	

CKR1137 00 10,623 racf records processed, selected 0 (0%)

CKR0039 00 CKRCARLA used 0.17 CPU seconds, 32+1,536KB+8MB, and took 1.0 wall clock seconds
Region requested 2,096,128KB, granted 7,080+1,855,488KB+17,592,186,040,320MB (by SMFPR
max used in jobstep 212+20,280KB+30MB

Only Error Ok

ISPF UI – SHOWLOG (1)

The highlighting comes from the CARLa engine and is also available in ISPF
The SYSPRINT is now captured and accessible while still in the program

```
SYSPRINT DISPLAY FOR FAILED COMMAND          Query failed RC=12
Command ==> _____                         Scroll==> CSR
Use RESET to show all lines, or XF 12 10 to fin
CKR0981 12 Invalid REMOVE_OPT "TOUSERTYPO      "
CKR0983 12 Expecting primary command list separator/terminator instead of delim
CKR0000 12 CKRCARLA terminated due to input errors
***** Bottom of Data *****
```

RESET and FIND 12 10 lets you navigate to

```
SYSPRINT DISPLAY FOR FAILED COMMAND          Line 186 of 312
Command ==> _____                         Scroll==> CSR
Use RESET to show all lines, or XF 12 10 to fin
Include CKRCMDV (ISPF variable)
 1 |copy user=crmbjti tousertypo=test
CKR0981 12 Invalid REMOVE_OPT "TOUSERTYPO      "
CKR0983 12 Expecting primary command list separator/terminator instead of delim
```

You can go back to the severe error display with XF 12 10
(12 is the message return code)

ISPF UI – SHOWLOG (2)

The SYSPRINT is of course also available when there are no errors.
You can bring it up with the primary command SHOWLOG

```
SHOWLOG CURRENT SYSPRINT
Command ===> _____ Scroll===> CSR
CKR0615 00 Input system structure overview (default system ZS14 complex BASE):
      Ver Complex Func Prod System      Timestamp          Filename Volser Dsnam
      BASE        Main   RACF ZS14        21 Mar 2025 23:45 CKR1UN00 CONA69 CRMA.
                           RACF ZS14        21 Mar 2025 23:45 CKR1CF00 CON028 CRMA.

CKR0168 00 Maximum profile length on BASE is 67,025 bytes for PROGRAM CKREXP
CKR0224 00 9,055 profiles and 2,563 segments read, 9,055 profiles and 2,563 seg
CKR0350 00 Number of permits/references processed on BASE is 23,103
CKR0087 00 Number of detail messages is 169
V S A M   O R   V V D S   I N C O N S I S T E N C I E S   BASE 21 Mar 2025 23:45

CKR0293 08 Volume not mounted on any system for cluster comp on G2205 SYS2.IOD
CKR0293 08 Volume not mounted on any system for cluster comp on PLX241 PLX.V3R2
CKR0286 08 No VT0C and no VVDS entry for cluster component on CA001P CA1.V1R1
CKR0286 08 No VT0C and no VVDS entry for cluster component on CA001P CA1.V1R1
```

zSecure Command Verifier

zSecure Command Verifier – CSDATA (1)

Policy profiles for Custom Data management

[ZCMD-I-80](#)

Because of the sensitive nature of certain fields in the CSDATA segment, your organization might need to maintain control over the CSDATA fields in RACF profiles, beyond the controls that RACF provides.

RACF command authorization allows verification on the Custom Data (CSDATA) field names, by using *Field-level Access Checking*. However, it is not possible to implement granular control to prevent system administrators from managing all CSDATA fields. Profiles in the FIELD class are not verified at all for System-SPECIAL users. In addition, RACF does not provide separate controls for changing the value versus deleting the Custom Data field.

zSecure Command Verifier provides additional controls for the CSDATA fields. These controls are in addition to the RACF requirements like System-SPECIAL or UPDATE access to the applicable profiles in the FIELD class.

zSecure Command Verifier – CSDATA (2)

The Command Verifier policy profiles for the Custom Data fields have the following format:

C4R.*class*.CSDATA.*fieldname*.*profile-identification*

The following table shows the *profile-identification*.

Table 59. Profiles used for verification of Custom Data fields. The entries in this table reflect the Class and Field and show the corresponding profile-identification that is part of the policy profile.

Class	Field	Profile-identification
USER	<i>fieldname</i>	<i>owner.userid</i>
GROUP	<i>fieldname</i>	<i>owner.group</i>
DATASET	<i>fieldname</i>	<i>hlq.rest-of-profile</i>
General Resource	<i>fieldname</i>	<i>profile</i>

The profiles in the preceding table describe the policies that verify whether the command as entered by the terminal user is accepted or rejected. The policy profiles for the various commands are very similar;

zSecure Command Verifier – CSDATA (3)

- C4R.*class*.CSDATA.*fieldname.profile-identification*

This policy profile specifies the authorization to set or delete a Custom Data field in the CSDATA segment. The *class* can be USER, GROUP, DATASET, or the name of a General Resource class, for example, FACILITY. The *profile-identification* can be one of the values that are shown in the last column in [Table 59 on page 209](#). If a general resource profile in the RACF command is longer than 200 characters, the *profile-identification* in the Command Verifier policy profile uses only the first 200 characters. The following access levels are supported:

No profile found

The policy is not implemented. Only standard RACF authorization is used to control management of Custom Data fields.

NONE/READ – command is rejected

UPDATE – can update the field

CONTROL – can update or delete the field

Command Verifier – segment deletion (NOCSDATA)

Previously, modification and deletion both required UPDATE

[ZCMD-I-75](#)

Now, deletion requires CONTROL

This applies to

- C4R.class.segment
- C4R.class.segment.=RACUID

This is an incompatible change introduced in the November 2024 update.

Command Verifier – ACL ID validation

This applies to

[ZCMD-I-14](#)

- C4R.*.ACL./GROUP.=HLQTYPE.**
- C4R.*.ACL./GROUP.*.**

The message C4R602E that the “ID is not a group” is changed into “ID does not exist”, and new message C4R727E is issued when the ID is a user.

Command Verifier – REXX in =PSTCMD

[ZCMD-I-58](#)

The APPLDATA of =PRECMD and =PSTCMD profiles can be used to specify the command that is to be run before and after the original RACF command. The Command Verifier policy can specify multiple commands, that are separated by a semicolon (;), up to 255 characters. Command Verifier executes each command in the order that it is provided before moving on to the next command. If a command fails, all the following commands are not executed.

The command can be a REXX exec; the maximum length of the REXX exec name is 8 and the name is preceded by special character %. Because the REXX exec is executed by System REXX, the REXX exec must reside in a REXX library that is allocated by the System REXX address space (see ["Example 5" on page 62](#)). For more information about System REXX, see section "Planning to use system REXX" in *z/OS MVS Programming: Authorized Assembler Services Guide*.

Command Verifier – Self-grant for HLQ

[ZCMD-I-52](#)

This applies to

- C4R.class.ACL.=RACUID.access.profile
- C4R.class.ACL.=RACGPID.access.profile
- C4R.class.ACL.=RACUID.access.profile

This profile is used to specify the authority of the terminal user to issue a PERMIT command that changes the access level of him/herself. It also applies to the **DELETE** option of the **PERMIT** command. An exception applies to class DATASET to allow users to manage their own data set profiles where the user ID matches the High Level Qualifier (HLQ) of the profile.

If you implement this profile, make sure to set the SETROPTS NOADDCREATOR option. Otherwise, a RACF administrator can automatically be added to the access list of resource profiles, without any possibility for the administrator to remove this questionable access level.

The qualifier =RACUID in the policy profile cannot be covered by generic characters. It must be present in the exact form shown.

No profile found

The control is not implemented. The terminal users are not prevented from adding, changing, or removing themselves on an access list.

Command Verifier – Improve audit trail

[ZAUDIT-I-371](#)

- This requirement stated that zSecure Command Verifier “must be updated to not only check if another 'remove' item is already present in the Audit Trail but also check on the RC from the previous command and if the currently executed one has a lower RC it must overwrite the existing entry.”

This sample represents the removal of the password interval from a user that failed:

C4R739I Attrib: INTERV Removed on 22.252/07:53 by C2PSUSER CMD-RC=04

When this situation needs to be corrected, another password nointerval command is executed.
As this has the same meaning of 'removal' the Audit Trail is not updated

This was translated into the following Conditions of Satisfaction for the Command Audit Trail improvement:

- CAT updated if current command has lower RC for same action.
- CAT unchanged if current command has higher or equal RC for same action as already recorded in the CAT.

Note: for dataset profiles successful command for change of access level is to be recorded

Command Verifier – Control display commands

[ZCMD-I-48](#)

“The customer wants to prevent users from listing their own user ID in RACF. They had a pen tester in and he listed his user ID, including running the SEARCH CLASS(class) USER(user) command to gather intelligence about his access. Preventing a hacker from issuing these commands might slow them down a little.”

Description

Implement policy profiles for SEARCH and List commands

SR CLASS(class)	C4R.<class>.DISPLAY.<profile-specific>	Fill in the defaults for <profile-specific>, e.g. <prefix> or "/SCOPE" The /SCOPE is done for non-dataset or when NOMASK.
SR NOMASK	C4R.<class>.DISPLAY./SCOPE	Unscoped scan (not just your own resources, but everything)
SR MASK(prefix,mask)	C4R.<class>.DISPLAY.<prefix>	For explicit search/list
LD DA(<dsname>)	C4R.DATASET.DISPLAY.<dsname>	For explicit search/list
LD prefix(<dsname>)	C4R.DATASET.DISPLAY.<dsname>	For explicit search/list (treat as <dsname>.*).
RL <class> <profile>	C4R.<class>.DISPLAY.<profile>	For explicit search/list
SR FILTER(filter)	C4R.<class>.DISPLAY.<filter>	For explicit search/list; <class> from other keyword.
SR USER(id)	C4R.SEARCH.USER.<id>	Work as somebody else
SR UID(id)	C4R.SEARCH.UID.<id>	Ugly scan on alternate index OMVS UID
SR GID(id)	C4R.SEARCH.GID.<id>	Ugly scan on alternate index OMVS GID

Compliance standards

Compliance standards zSecure Audit 3.1.0



IBM z/OS STIG v9

z/OS standards developed by DISA for the DoD to secure DoD computing systems.¹



z/OS Products STIG (latest)

z/OS Products standards developed by DISA for the DoD to secure DoD computing systems.¹



zSecure STIG v1.2

IBM Security zSecure for RACF Security Technical Implementation Guide (STIG). Developed by zSecure and DISA.¹



PCI-DSS

Payment Card Industry Data Security Standard (PCI-DSS)³



IBM z/OS V2R5 with RACF v1.1.0

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for IBM Z System.²



IBM Db2 for z/OS Benchmark v1.0

This CIS Benchmark is the product of a community Consensus process and consists of secure configuration guidelines developed for IBM Z System.²

March 2025 documentation updates technote:
[IBM Security zSecure 3.1.0 Compliance Standards \(PDF\)](https://public.cyber.mil/stigs/)

Source 1: <https://public.cyber.mil/stigs/>

Source 2: https://www.cisecurity.org/benchmark/ibm_z

Source 3: <https://www.pcisecuritystandards.org>

Compliance updates zSecure Audit 3.1 (1)

IBM APAR	Description
OA67548 (base) OA67549 (ACF2) OA67549 (zSCC)	STIG quarterly updates (March 2025) zSecure Audit support for: z/OS RACF STIG V9R3, z/OS ACF2 STIG V9R3, and z/OS TSS STIG V9R3 and new versions for the z/OS Products STIG
OA67279 (base) OA67280 (ACF2) OA67281 (zSCC)	zSecure version 3.1.0 SSE3 (January 2025) - Further automation for CIS Benchmark for RACF (6 NEW controls) - Further automation for IBM DB2 for z/OS Benchmark v1.0.0 (3 NEW controls)
OA67173 (base) OA67174 (ACF2) OA67175 (zSCC)	STIG quarterly updates (November 2024) zSecure Audit support for: z/OS RACF STIG V9R2, z/OS ACF2 STIG V9R2, and z/OS TSS STIG V9R2
OA66990 (base) OA66991 (ACF2) OA66992 (zSCC)	zSecure version 3.1.0 SSE2 (October 2024) - Further automation for CIS Benchmark for RACF (16 NEW controls) - IBM DB2 for z/OS Benchmark v1.0.0 (NEW standard) - Existing zSecure Audit PCI-DSS controls converter to version 4 (zSecure Audit only) - IBM zSecure STIG for ACF2 1.1
OA66794 (base) OA66795 (ACF2) OA66848 (zSCC)	STIG quarterly updates zSecure Audit support for: z/OS RACF STIG V9R1, z/OS ACF2 STIG V9R1, and z/OS TSS STIG V9R1

Compliance updates zSecure Audit 3.1 (2)

IBM APAR	Description
OA66278 (base) OA66279 (ACF2) OA66280 (zSCC)	zSecure version 3.1.0 SSE1 (April 2024) - Further automation for CIS Benchmark for RACF - Separate z/OS Products STIGs introduced in zSCC - IBM zSecure STIG for RACF 1.1
OA65870 (base) OA65871 (zSCC)	STIG quarterly updates zSecure Audit support for: z/OS STIG ACF2 8.13, z/OS STIG TSS 8.11, and CIS Benchmark for RACF 1.1.0

DISA STIG in zSecure Audit 3.1.0

- Latest version update: March 2025
- z/OS STIG:
 - ACF2 Versions:
8.10,8.11,
8.12,8.13,8.14,8.15,9.01,9.02,9.03
 - RACF Versions:
8.10,8.11,**8.12,8.13,8.14,9.01,9.02,9.03**
 - TSS Versions:
8.09,8.10,8.11,8.12,8.13,9.01,9.02,9.03

z/OS STIG v9.03

	ACF2 z/OS	RACF z/OS	TSS z/OS
Total	221	217	226
Ready	204	205	73
Missing	17	12	164
%	92%	94%	32%

z/OS Products STIG (latest)

	ACF2 z/OS Products	RACF z/OS Products	TSS z/OS Products
Total	154	174	179
Ready	148	174	35
Missing	6	0	144
%	96%	100%	20%

IBM Z System CIS benchmark

- CIS benchmark replaced outdated GSD331 support in AU.R.

IBM Z System

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for IBM Z System

CIS Benchmarks are freely available in PDF format for non-commercial use:

[DOWNLOAD LATEST CIS BENCHMARK →](#)

Included in this Benchmark

FREE DOWNLOAD

CIS Benchmark

Safeguard IT systems against cyber threats with these CIS Benchmarks. Click to download a PDF from the list of available versions.

[LEARN MORE ABOUT CIS BENCHMARK →](#)

Java

Recent versions available for CIS Benchmark:

- IBM CICS Transaction Server 6.1 (1.0.0)
- IBM Db2 13 for z/OS (1.0.0)
- IBM z/OS V2R5 with RACF (1.1.0)
- RHEL8 on IBM Z Linux (1.0.0)



Discover the CIS Benchmarks

Learn what they are, how to use them, and how to get involved in their development.

[LEARN MORE →](#)

Discover More Configuration Guides

There are more than 100 CIS Benchmarks across 25+ vendor product families.

[VIEW ALL CIS BENCHMARKS →](#)

View all active and archived CIS

Benchmarks

CIS Benchmark with RACF vs DISA STIG

- Industry-defined vs government-defined
- Based on STIG/NIST, but also developed by industry consensus and peer-reviewed
- Improvements to standard are more dynamic, everyone can submit a comment or request for enhancement:
<https://workbench.cisecurity.org/registration>

- Establishes baseline of “best practices” vs prescriptive access controls
- More ICSF recommendations (+13 new compared to 5 in DISA STIG)
- Protection of JESJOBS class profiles (15 new controls)
- More UNIX recommendations (+10 new recommendations)

- DISA also has the Products STIG controls

January 2025

CIS z/OS Benchmark with RACF 1.1.0	RACF z/OS
Total	219
Ready	203
Missing	16
%	93%

Compliance Standards technote

[ZAUDIT-I-378](#)

All currently supported controls are listed in the following technote:

[zSecure 3.1.0 Compliance Standards March 2025 \(PDF\)](#)

Note that the PCI-DSS controls were converted to multi-standard syntax and upgraded to the 4.0 level in the October 2024 update.

CIS IBM Db2 for z/OS Benchmark (1.0.0)

- Provides prescriptive guidance for establishing a secure configuration posture for IBM® Db2® for z/OS®.
- Intended for Db2 for z/OS system, database, and application administrators, security specialists, and auditors who plan to develop, deploy, assess, or secure solutions that incorporate IBM Db2 for z/OS.
- Can be downloaded via <http://workbench.cisecurity.org>.
- Peer-reviewed standard: expert community is encouraged to submit feedback and suggestions
- 78 recommendations (controls):
 - ❖ **Installation and Configuration:** Securing the system data sets and configuring the security system parameters
 - ❖ **Securing the database:** Securely connecting to and accessing the DB2 subsystem, protecting data with encryption and privacy controls
 - ❖ **Audit:** Enabling auditing
- !!Only available with zSCC entitlement via ISPF or zSCC dashboard!!

CIS IBM Db2 for z/OS Benchmark

January 2025

CIS DB2 for z/OS Benchmark 1.0.0	RACF z/OS	ACF2 z/OS
Total	78	78
Ready	70	67
Missing	8	11
%	90%	86%

Underlying DB2 report types

In order to build the controls, several new Db2 report types have been added.

In RED (RESOURCE – DB2) the following options appeared:

- AC Db2 Access control DB2_ACCESS
- CT Db2 Permission/Mask DB2_CONTROL
- TC Db2 Table columns DB2_COLUMN
- AP Db2 Audit policies DB2_AUDITPOLICY

Note that TC and AP are only available with a zSCC entitlement

RE.D DB2 resource additions AC, AP, CT and TC

zSecure Suite - Resource - DB2		
Option ==>		
R Regions	Region overview and system privileges (DSNADM, MDSNSM)	
AC Access controls	Access controls on privileges	
AP Audit policies	Audit security policies	
BP Buffer pools	Memory areas that can hold data pages	
CL Collections	Groups of packages with the same qualifier	
CT Permission/Mask	Control records for row permissions and column masks	
DB Databases	Sets of tables, indexes, and table spaces	
GV Variables	Global variables (session scope named memory variables)	
JR Java archives	Sets of files comprising Java applications	
PK Packages	Packages (pre-bound SQL statements)	
PN Plans	Plans (control structures created during BIND)	
SC Schemas	Logical classifications of database objects	
SG Storage groups	Sets of storage objects (volumes)	
SP Stored procs	Stored procedure and user function routines	
SQ Sequences	User defined objects defining a numerical sequence	
TB Tables/views	Tables and views	
TC Columns	Table columns	
TS Table spaces	Table spaces (data set name space for storing tables)	
UT User data types	Distinct types	

Report type DB2_CONTROL (1)

- Shows objects from Db2 SYSCONTROLS
- Row permission controls
- Column mask controls
- CARLa samples CKADQDL / CKALQDL
- Entitled for zSecure Audit and zSCC
- Shipped in April 2024 SSE
- Shipped UI option RE.D.CT in October 2024 SSE

zSecure Suite - DB2 - Permission/Mask

Command ==> _____

Show permissions/masks that fit all of the following criteria:

Permission/mask name	(name or filter)
Table name	(name or filter)
Permission/Mask	(R/M or blank)
Show implicit records	
Column name	(name or filter)
DB2ID	(identifier or filter)
Complex	(complex or filter)
System	(system or filter)

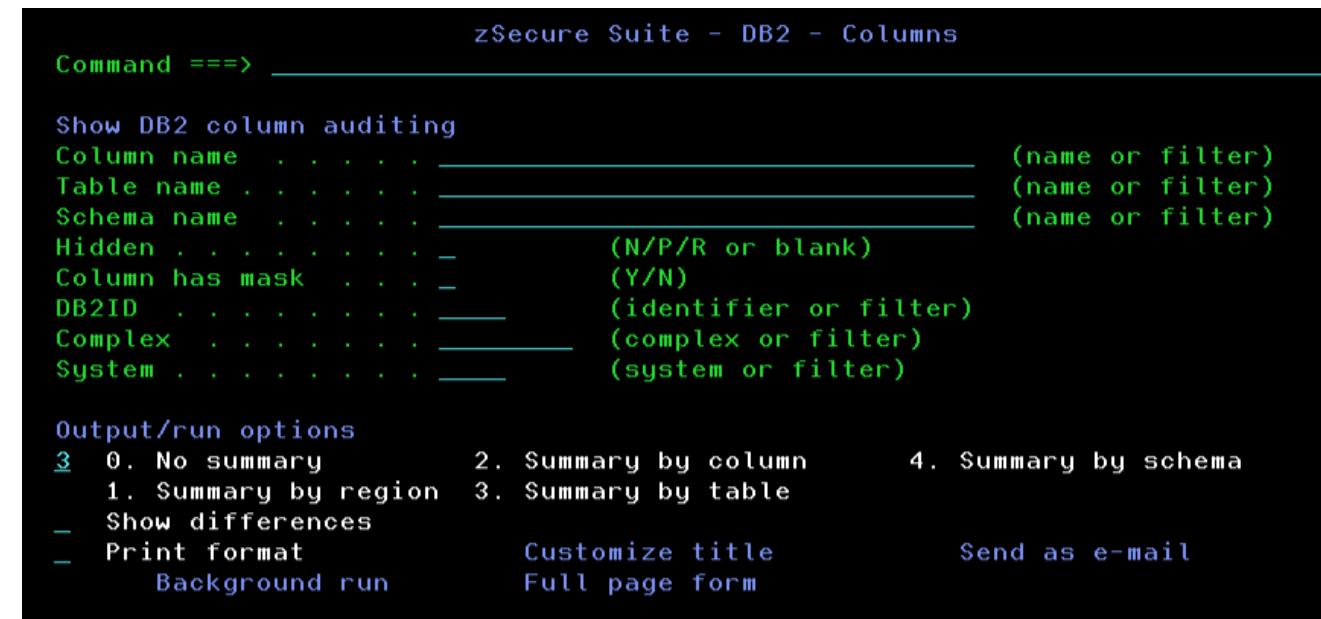
Output/run options

_ 0. No summary	1. Summary by region	2. Summary by permission/mask name
_ Show differences		
_ Print format	Customize title	Send as e-mail
Background run	Full page form	

Report type DB2_CONTROL (2)

Report type DB2_COLUMN

- Shows objects from Db2 SYSCOLUMN and SYSCOLAUTH
- Column level permissions (internal)
- Column level permissions (RACF or ACF2)
- CARLa sample CKADQDM
- Entitled for zSCC only
- Shipped report type in October 2024
- Exploitation CIS benchmark for Db2 in October 2024
- Shipped UI option RE.D.TC in October 2024



In a next release the CARLa script will have the CKC prefix

RE.D.TC column protection detail

```
DB2 columns display
Command ==> _____
DB2 column records for tables like RIDERS

Identification
System name           ZS45      complex PLEX1
- DB2 System identification   DBC1
Table schema          SCBIKE
Column name           RIDERFIRSTNAME
Table name            RIDERS

Properties             Statistics
Hidden                N
Column mask exists    No

Resource prefix        DBC1.SCBIKE.RIDERS.RIDERFIRSTNAME

Class     Resource name
- MDSNTB  DBC1.SCBIKE.RIDERS.RIDERFIRSTNAME.REFERENCES
- MDSNTB  DBC1.SCBIKE.RIDERS.RIDERFIRSTNAME.UPDATE

Userid    RU Grantee>>LastGranted      L Grantor
- group-  u F#DB2ADM   8Jul24 14:50:30    CRMBRT1
- group-  r F#DB2USR   8Jul24 14:50:30    CRMBRT1

Userid    RU Id      RI Name           DfltGrp  RvC InstData
- other-   -uacc-
- group-  RU F#DB2ADM                           DB2 ADMIN

*****
***** Bottom of
```

Report type DB2_AUDITPOLICY

- Shows objects from Db2 SYSAUDITPOLICY
- Audit settings more granular than TRACE
- CARLa sample CKADQDU
- Entitled for zSCC only
- Added in January 2025

```
zSecure Suite - DB2 - Audit policies

Command ==> _____
Show DB2 audit policies
Audit policy name . . . . . _____ (name or filter)
Startup . . . . . - _____ (Y,S,T,N or blank)
Active . . . . . - _____ (Y/N or blank)
Checking . . . . . - _____ (Y/N or blank)
Context . . . . . - _____ (Y/N or blank)
Execute . . . . . - _____ (A/C or blank)
DB2ID . . . . . _____ (identifier or filter)
Complex . . . . . _____ (complex or filter)
System . . . . . _____ (system or filter)

Advanced selection criteria
- Categories _____ Objects
Output/run options
- 0. No summary 1. Summary by region
- Show differences
- Print format Customize title
- Background run Full page form
Send as e-mail
```

In a next release the CARLa script will have the CKC prefix

RE.D.AP Db2 Audit Policy Detail

```
DB2 audit policies display
Command ==> _____
All DB2 auditpolicy records

Identification
Audit policy name          AUDIT3
System name                 ZS14      complex NM87
DB2 System identification   DBD1

Categories
DBAdmin                     I_SYSADM
SYSAdmin                    All
Checking                     None
Context                      None
Execute                      None
Validate                     None
Object maintenance           None
Security maintenance         All

Objects
Object name                 All
Object schema               All
Object type                 All

Properties
Start up                   Tamperproof
Active                      Yes
Active SMF                  Yes
Active IFCID SMF            83 140 141 270 271 361
Collection name              Database name

Statistics
Creation timestamp           29Apr2024 13:24
Alter timestamp              29Apr2024 13:24
```

Analyzes the Db2 control blocks to figure out what IFCids will be written to the official z/OS audit trail as SMF type 102 IFCids

Report type DB2_ACCESS

- Shows Db2 objects that have an access list either through Db2 internal security or through the standard Db2 external access control module DSNX@XAC.
- CARLa sample CKADQDP
- Entitled for zSecure Audit and zSCC
- Has been in the CARLa engine since zSecure 2.3.1
- Exploitation CIS benchmark for DB2 in October 2024
- Shipped UI option RE.D.AC in October 2024

```
zSecure Suite - DB2 - Access controls
Command ==> _____
Show DB2 access controls that fit all of the following criteria:
DB2ID . . . : . . : _____ (identifier or filter)
Object class . . . : _____ (class or filter)
Object name . . . : _____ (name or filter)
Grantee . . . : _____ (grantee or filter)
SAF resource class _____ (class or filter)
SAF resource name _____ (name or filter)
Access using . . . : _ 1. DB2zparm 2. SAF defined 3. Internal
Complex . . . : _____ (complex or filter)
System . . . : _____ (system or filter)

Advanced selection criteria
- Privileges _ Other
Output/run options
- Summary Order by _ region _ object type _ object _ grantee (1-4)
- Show differences
- Print format Customize title Send as e-mail
- Background run Full page form
```

RE.D.AC Db2 Access Control - Privileges

```
Command ===> zSecure Suite - DB2 - Access controls

Granted privileges
  Bufferpools
    USE
  Collections
  OR  CREATEIN      — PACKADM
  Databases
  OR  — CREATETAB   — CREATETS     — DBADM      — DBCTRL
  — DBMAINT       — DISPLAYDB    — DROP        — IMAGCOPY
  — LOAD          — RECOVERDB    — REORG      — REPAIR
  — STARTDB       — STATS        — STOPDB
  Java archives
    USE
  Packages
  OR  BIND          — COPY         — EXECUTE
  Plans
  OR  BIND          — EXECUTE
  Schemas
  OR  ALTERIN       — CREATEIN     — DROPIN
  Sequences
  OR  ALTER          — ALTERIN      — DROPIN      — USAGE
  Session variables
  OR  — DROPIN      — READ         — WRITE
  Storage groups
    USE
  Stored procedure and user function routines
  OR  ALTERIN       — DISPLAY      — DROPIN      — EXECUTE
  Tables/views
  OR  — ALTER        — DELETE       — INDEX      — INSERT
  — LOAD          — REFERENCES   — SELECT      — TRIGGER
  — UNLOAD        — UPDATE
  Table columns
  OR  REFERENCES    — UPDATE
  Tablespaces
    USE
  User authorities
  OR  — ACCESSCTRL   — ARCHIVE     — BINDADD    — BINDAGENT
  — BSDS          — CREATEALIAS  — CREATEDBA   — CREATEDBC
  — CREASECUROBJ  — CREATESG    — CREATETMTAB — DATAACCESS
  — DEBUGSESSION   — DISPLAY      — EXPLAIN    — MONITOR1
  — MONITOR2       — RECOVER      — SECADM     — SQLADM
  — STOPALL        — STOSPACE    — SYSADM     — SYSCTRL
  — SYSDBADM      — SYSOPR      — TRACE
  User data types
  OR  — ALTERIN      — DROPIN      — USAGE

With effective use authority = (Y/N/blank)
With effective grant authority = (Y/N/blank)
```

RE.D.AC Db2 Access Control - Other

For example,
request -undef-

```
zSecure Suite - DB2 - Access controls

Command ==> _____
Show DB2 access control records that fit all of the following criteria:
External security
Userid . . . : : : : : _____ (userid, filter, or keyword)
Mapped to id : : : : : _____ (userid, groupid, or filter)
When criteria . . . : : : _____ (criteria or filter)
ACF2 rule subject type : : : 1. role 2. user 3. uid
ACF2 rule subject mask : : : _____ (class or filter)

Internal security
Grantor : : : : : _____ (grantor or filter)
With use authority : : : = (Y/N/blank)
With grant authority : : : = (Y/N/blank)

Other
Object schema . . . : : : _____ (schema or filter)
Object database : : : : _____ (database or filter)
Object resource : : : : _____ (object or filter)
```

RE.D.AC Db2 Access Control – results display

Report types ACF2_DB2_RULE / _RULELINE

- Shows rules from ACF2/DB2 product
- Support ACF2/DB2 add-on product to ACF2
- Entitled for zSCC
- Shipped in engine in October 2024



CIS IBM Db2 for z/OS Benchmark (1.0.0) (1)

```
Z Security Compliance Center - Main menu
Option ===> _____
```

SE	Setup	Options and input data sets
RA	RACF	RACF Administration
AA	ACF2	ACF2 Administration
AU	Audit	Audit security and system resources
RE	Resource	Resource protection reports
EV	Events	Event reporting from SMF and other logs
CO	CARLa	Work with CARLa queries and libraries
IN	Information	Information and documentation
LO	Local	Locally defined options
X	Exit	Exit this panel

Input complex: PL87, NMPIPL87

Product/Release
5655-CC1 IBM Z Security and Compliance Center V1 for z/OS 3.2.E

```
Z Security Compliance Center - Audit - Compliance
Option ===> _____
```

C	Configure	Configuration and site assertions
E	Evaluate	Run standard evaluation
H	History log	Assertion, override, and configuration logs
S	Subsets	Rule subsets
T	Test rule	Single rule evaluation and configuration

CIS IBM Db2 for z/OS Benchmark (1.0.0) (2)

Z Security Compliance Center - Comp Row 1 to 15 of 38
Command ==> _____ Scroll ==> [CSR](#)

Subset name _____ (name for subset; ? for list of defined subsets)
Description _____

Type **SAVE** to save, **RUN** to execute, **CONFIG** to configure, or **RESET** to remove all selections. Type **OPTIONS** to set the print/runtime options.
Valid line commands: **S** (Show controls), **U** (Unselect all), **Z** (Select all),
A (Run all controls in evaluation), **R** (Run selected controls in evaluation),
B (Configure all controls in evaluation), **C** (Configure selected controls)
Showing controls for: RACF

Evaluation	#Controls	#Selected
zOS_STIG	211	0
Prods_STIG	190	0
Db2_CIS	71	0
zOS_CIS	195	0
PCI-DSS	13	0
zSecure_STIG	12	0
Ab_AID_STIG	7	0
Auditor_STIG	3	0
CatSol_STIG	2	0
Com_Srv_STIG	3	0
RA1_TM_STIG	11	0

CIS IBM Db2 for z/OS Benchmark (1.0.0)

UI OPTIONS TO SET THE PRIMARY RUNTIME OPTIONS.

Valid line commands: **S** (Select), **U** (Unselect), **V** (View control member),
E (Edit customization member), **R** (Run control), **C** (Configure control)

Control	Standard	Description	Member	CKACUST	S
CIS-DB2-2.2.9	Db2_CIS	Dynamic query-related tbs	CKCHD229	_____	-
CIS-DB2-2.2.10	Db2_CIS	SYSIBM.SYSINDEXES	CKCHD22A	_____	-
CIS-DB2-2.2.11	Db2_CIS	SYSIBM.SYSOBJROLEDEP	CKCHD22B	_____	-
CIS-DB2-2.2.12	Db2_CIS	Package-related tables	CKCHD22C	_____	-
CIS-DB2-2.2.13	Db2_CIS	SYSIBM.SYSPACKAUTH	CKCHD22D	_____	-
CIS-DB2-2.2.14	Db2_CIS	SYSIBM.SYSPARMS	CKCHD22E	_____	-
CIS-DB2-2.2.15	Db2_CIS	SYSIBM.SYSPLAN	CKCHD22F	_____	-
CIS-DB2-2.2.16	Db2_CIS	SYSIBM.SYSPLANAUTH	CKCHD22G	_____	-
CIS-DB2-2.2.17	Db2_CIS	SYSIBM.SYSQUERY	CKCHD22H	_____	-
CIS-DB2-2.2.18	Db2_CIS	SYSIBM.SYSRESAUTH	CKCHD22I	_____	-
CIS-DB2-2.2.19	Db2_CIS	SYSIBM.SYSROLES	CKCHD22J	_____	-
CIS-DB2-2.2.20	Db2_CIS	SYSIBM.SYSROUTINEAUTH	CKCHD22K	_____	-
CIS-DB2-2.2.21	Db2_CIS	SYSIBM.SYSROUTINES	CKCHD22L	_____	-
CIS-DB2-2.2.22	Db2_CIS	SYSIBM.SYSROUTINESTEXT	CKCHD22M	_____	-
CIS-DB2-2.2.23	Db2_CIS	SYSIBM.SYSSCHEMAAUTH	CKCHD22N	_____	-
CIS-DB2-2.2.24	Db2_CIS	SYSIBM.SYSSEQUENCEAUTH	CKCHD22O	_____	-
CIS-DB2-2.2.25	Db2_CIS	SYSIBM.SYSSEQUENCES	CKCHD22P	_____	-
CIS-DB2-2.2.26	Db2_CIS	SYSIBM.SYSSTMT	CKCHD22Q	_____	-
CIS-DB2-2.2.27	Db2_CIS	SYSIBM.SYSSTOGROUP	CKCHD22R	_____	-
CIS-DB2-2.2.28	Db2_CIS	SYSIBM.SYSTABAUTH	CKCHD22S	_____	-

IBM Z Security and Compliance Center

zSecure Audit integration with IBM Z Security and Compliance Center (zSCC)

We show full assessment of the following standards in the zSCC dashboard:

- All *separate* z/OS Products STIGs (previously bundled together)
 - zSecure STIG for RACF and ACF2 v1.1 and v1.2
 - STIG for z/OS RACF
 - 8.12,8.13,8.14,9.01,9.02,9.03
 - STIG for z/OS ACF2
 - 8.12,8.13,8.14,8.15,9.01,9.02,9.03
- z/OS with RACF CIS Benchmark 1.0.0, 1.1.0
- z/OS Db2 CIS Benchmark version 1.0.0
(Only with zSCC license)

CIS IBM Db2 for z/OS – dashboard: Profiles

Profiles

[View docs](#) 

A profile is a collection of related controls. After you gather the configuration information of your resources and prepare your systems for scanning, you can create profiles to define the list of controls that you'd like to validate against.

Filters: [Clear filter](#)

Environment Type

Profile family

Category

z/OS	CIS	All
----------------------	---------------------	---------------------

 Search



[Create](#)

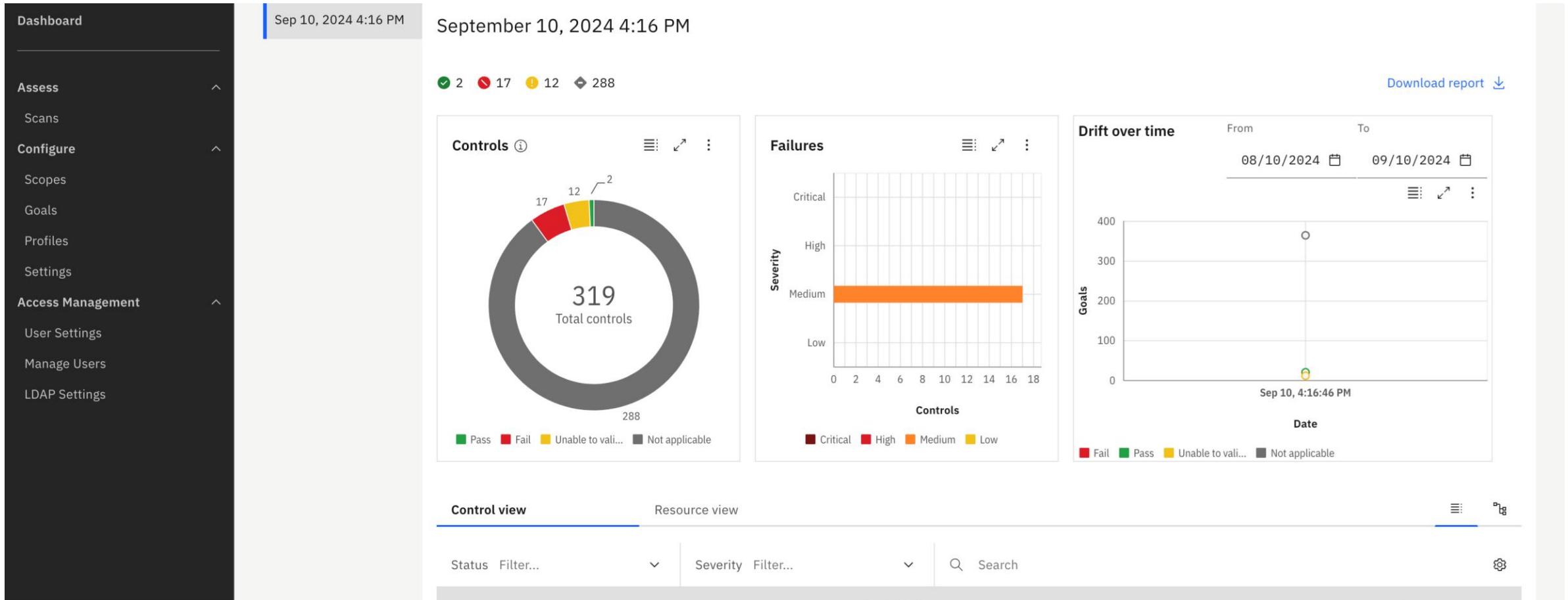


Name	Description	Type	Controls	
Db2_zOS_CIS_1.0.0	CIS IBM Db2 for z/OS Benchmark	Predefined	319	
RACF_zOS_CIS_1.0.0	CIS benchmark IBM z/OS V2R5 with RACF	Predefined		
RACF_zOS_CIS_1.1.0	CIS benchmark IBM z/OS V2R5 with RACF	Predefined		

Items per page: [50](#) ▾ 1–3 of 3 items

1 ▾ 1 of 1 page ▶ ▷

CIS IBM Db2 for z/OS - dashboard: Scans



CIS IBM Db2 for z/OS – dashboard: Results

The screenshot shows the IBM Z Security and Compliance Center dashboard for a scan titled "C09 - Db2_zOS_CIS". The main content area displays the following information:

Scan Summary: Db2 active log, archive log, and table space data sets must be encrypted.

Control ID: CIS-DB2-2.5.1 : Db2_dsns_encrypted

Severity: Medium

Status: FAIL

Number of goals: 1

Goals: ID: 6002460 Db2 active log, archive log, and table space data sets must be encrypted.

Pass: 6 | Fail: 1 | Unable to validate: 0 | Not applicable: 0

Environment: ZOS

Resource category: All

Resource type: All

Resource: All

Expected value:

Resource status	All	Search	Detail	
Status	Resource	Resource type	Actual value	Detail
🔴	SVPLEX4.C09.sensdsn:Dataset=DB2X4ARC.D4P9.ARC1.D21097.T1529101.B0089920	ibmzos_stig_sensdsn_Dataset		
🟢	SVPLEX4.C09.sensdsn:Dataset=DB2X4ARC.D4P9.ARC1.D25258.T0350140.A0116002	ibmzos_stig_sensdsn_Dataset	IST.RTS.DATAKEY	

New features in zSCC 1.2.1 dashboard

Goals for security patches have been added to the PCI-DSS for z/OS profiles (3.2.1 and 4.0)

LDAP connections can be secured with digital certificates

Administrator can use new Request logs option to download first failure capture information in a compressed file, for help with diagnosing errors.

Unit of Work ID (UOWID)

Unit of Work ID and tracking tokens

For linking events together, it is important to understand that they pertain to the same overall “stream”. The Unit of Work ID and tracking tokens can help with that.



From an event display, use **F**(ind matching records)

```
_ Unit of Work Id: USIBMWZ.TEC2T0R1.C30C1EF64A6C  
_ Tracking token: BAQ.1.TECPLEX.TEC2.2020-11-02T14:22:17.247495
```

to see

```
Tracking token event  
Command ==> _____ 5 s elapsed, 0.8 s CPU  
_____  
Date/time event Description Scroll==> CSR  
— 2Nov20 10:22:17.24 KENISHI CICS transaction TEC2A0R1 CSMI  
— 2Nov20 10:22:17.24 KENISHI CICS transaction TEC2T0R1 CSMI  
— 2Nov20 10:22:18.47 z/OS Connect ZCEESRVR API GET healthcareinfo findPatient, user KENISHI, HTTPresp 200, 0.004s 0/180 bytes in/  
***** Bottom of Data *****
```

This applies to CICS, Db2, and z/OS Connect events.



Running started tasks under MSTR

Start Access Monitor under MSTR

[ZSECURE-I-111](#)

“We are relying on Access Monitor.

We need to see all possible SAF calls as early in the IPL as possible to ensure we do not break a task or some other critical piece of software tech.”

This change was applied to the zSecure Admin Access Monitor (C2PACMON), zSecure Alert (C2POLICE), and zSecure SMF extractor (CKQEXSMF) started tasks.

“The current release of zSecure Access Monitor supports running the STC under the MSTR subsystem. This allows starting the STC earlier in the IPL process. Several changes have been made to the startup JCL, and to the configuration data sets. An updated example member is provided in SCKRPROC. The most visible change is that the SYSTSPRT ddname has been replaced by the C2PTSPRT ddname. If you plan to run the STC under MSTR, you need to review the STC procedure. Your existing procedure might refer to SYSOUT data sets and use variables for the sysout class. These should be removed and replaced by ALLOC statements in the C2PAMALC member in the data set allocated to the SC2PSAMP dd-name (usually identified through JCL variable &C2PACPRM). For more information about the C2PAMALC member, see sections “Preparing the JCL” and “Dynamic allocation member C2PAMALC”. When running the STC under MSTR, you should also ensure the presence of “TIME=NOLIMIT” on the EXEC statement.”

Support for IBM Threat Detection for z/OS (5698-CA1)

Support new DFSMS Top Activity records

DFSMS determines top job and data set activity in 5 seconds intervals

Written out in SMF 98
(about 2GB / day)

- Subtype 5 – Enhanced Format data set read activity
- Subtype 6 – Basic data set read activity
- Subtype 7 – Enhanced Format data set write activity
- Subtype 8 – Basic data set write activity

zSecure Audit can be used to see those records in EV.U and EV.D

EV.D display of SMF 98-5/6/7/8

```

IBM Security zSecure SMF display                               Line 1 of 476375
Command ==> _____ Description                               Scroll==> CSR
SMF records for all data sets
Date/time
17Oct26 00:00:00.16 job VGENC0A read 2789k bytes, 2789k bytes read from PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.16 ELVIS job DVP1C0A read 63M32 bytes, 63M32 bytes read from Linear top data set DIV.THRBDIVP.G512.C0A.J1.DATA on 1P0307, Encrypted, Extended
17Oct26 00:00:00.18 T015032 job T015032 read 25680 bytes, 16080 bytes read from PDS top data set T015032.A.ASM on SGT402, Fixed length
17Oct26 00:00:00.20 job VGENC0A wrote 1110k bytes, 1110k bytes written to PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.20 ELVIS job DVP1C0A wrote 62M91 bytes, 62M91 bytes written to Linear top data set DIV.THRBDIVP.G512.C0A.J1.DATA on 1P0307, Encrypted, Extended
17Oct26 00:00:00.20 SETUP job SMF wrote 143k4 bytes, 143k4 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.SVT.C0A.DATA on IFA021
17Oct26 00:00:00.20 SETUP job SMF wrote 163k8 bytes, 163k8 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.WKLDPROF.C0A.DATA on IFA021
17Oct26 00:00:00.20 SETUP job SMF wrote 1909k bytes, 1909k bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.WKLDPROF.C0A.DATA on IFA021
17Oct26 00:00:00.20 SYSADM1 job D4PAMSTR wrote 8192 bytes, 8192 bytes written to Linear top data set DBX4.D4PA.LOGCOPY1.DS01.DATA on DBX40C, Encrypted, Extended
17Oct26 00:00:00.20 SYSADM1 job D4PAMSTR wrote 8192 bytes, 8192 bytes written to Linear top data set DBX4.D4PA.LOGCOPY2.DS03.DATA on DBX416, Encrypted, Extended
17Oct26 00:00:00.23 T015032 job T015032 wrote 4800 bytes, 4800 bytes written to PDS top data set T015032.ISPF.PROFILE on 9SX40B, Fixed length
17Oct26 00:00:00.40 job VGENC00 read 1875k bytes, 1875k bytes read from PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.40 CICS job CICS2A03 read 12288 bytes, 12288 bytes read from KSDS Data top data set ADSUFILE.VF04D.DATAENDB.DATA on X4RLS6, VSAM RLS
17Oct26 00:00:00.40 CICS job CICS2A03 read 4096 bytes, 4096 bytes read from KSDS Data top data set ADSUFILE.VF04D.TRMNALDB.DATA on X4RLS2, VSAM RLS
17Oct26 00:00:00.40 SETUP job CATALOG read 20480 bytes, 20480 bytes read from KSDS Data top data set CATALOG.X4TS03 on X4TS03
17Oct26 00:00:00.40 SYSADM1 job D4P0DBM1 read 105M0 bytes, 105M0 bytes read from Linear top data set NSTDB2.DSNDBD.CFCDB09.STATUS09.I0001.A001 on DBX409, Extended
17Oct26 00:00:00.40 SYSADM1 job D4P0DBM1 read 12M94 bytes, 12M94 bytes read from Linear top data set NSTDB2.DSNDBD.CFCDB06.STAHIS06.I0001.A001 on DBX410, Extended
17Oct26 00:00:00.44 MOSCHEN job ENCMASA read 126k7 bytes, 126k2 bytes read from PS top data set SYS26283.T173635.RA000.ENCMASA.R0203736 on SGT204, Fixed length
17Oct26 00:00:00.44 T016282 job T016282 read 6240 bytes, 6240 bytes read from PDS top data set T016282.ISPF.PROFILE on X4USER, Fixed length
17Oct26 00:00:00.47 job VGENC00 wrote 659k5 bytes, 659k5 bytes written to PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.47 SETUP job CICS2A03 wrote 32768 bytes, 24576 bytes written to Linear top data set IXGLPLEX4.CICS.T6V02A03.DFHLOG.SVPLEX4.DATA on SGT11B, Encr
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 1790k bytes, 1786k bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.WKLDPROF.C00.DATA on IFA001
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 188k4 bytes, 188k4 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.PERFRPT.C00.DATA on IFA00B
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 4096 bytes, 4096 bytes written to Linear top data set IXGLPLEX4.ADSW.CICSVR.F01DACC.T00.DATA on SGT128
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 4096 bytes, 4096 bytes written to Linear top data set IXGLPLEX4.ADSW.CICSVR.F02DACT.C00.DATA on SGT103
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 4096 bytes, 4096 bytes written to Linear top data set IXGLPLEX4.ADSW.CICSVR.F07DNTOR.C00.DATA on SGT11B
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 49152 bytes, 49152 bytes written to Linear top data set IXGLPLEX4.CICS.T6V02A03.DFHLOG.A0013147.DATA on SGT114, Encr
17Oct26 00:00:00.47 SETUP job IXGLGGR wrote 8192 bytes, 8192 bytes written to Linear top data set IXGLPLEX4.CICS.T6V02A03.DFHLOG.SVPLEX4.DATA on SGT11B, Encrypt
17Oct26 00:00:00.47 SYSADM1 job D4P0MSTR wrote 102k4 bytes, 102k4 bytes written to Linear top data set DBX4.D4P0.LOGCOPY1.DS02.DATA on DBX418
17Oct26 00:00:00.47 SYSADM1 job D4P0MSTR wrote 102k4 bytes, 102k4 bytes written to Linear top data set DBX4.D4P0.LOGCOPY2.DS01.DATA on DBX419
17Oct26 00:00:00.50 MOSCHEN job ENCMASA wrote 143k3 bytes, 142k8 bytes written to PS top data set SYS26283.T173635.RA000.ENCMASA.R0203736 on SGT204, Fixed leng
17Oct26 00:00:00.52 SETUP job CATALOG read 40960 bytes, 40960 bytes read from KSDS Data top data set CATALOG.SVPLEX4.WORKLOAD on X4USER
17Oct26 00:00:00.52 SETUP job ZFS read 32768 bytes, 32768 bytes read from Linear top data set OMVSSPA.OE7201.ZFS.DATA on USSFSS
17Oct26 00:00:00.52 SYSADM1 job CICS3A51 read 12288 bytes, 8192 bytes read from Linear top data set DBX4.DSNDBD.DSNDDB06.SYSTSIXS.I0001.A001 on DBX415, Encrypted
17Oct26 00:00:00.52 SYSADM1 job D4P5DBM1 read 285672 bytes, 285672 bytes read from Linear top data set DBX4.DSNDBD.DSNDDB06.SYSTSIPT.I0001.A001 on DBX403, Encrypted
17Oct26 00:00:00.52 SYSADM1 job D4P5DBM1 read 409k6 bytes, 409k6 bytes read from Linear top data set NSTDB2.DSNDBD.CFCDB04.SHIFTS04.I0001.A001 on DBX407, Extended
17Oct26 00:00:00.53 job VGENC09 read 2445k bytes, 2445k bytes read from PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.56 ELVIS job PGENC09 read 1840 bytes, 1840 bytes read from PDS top data set ISP.SISP MENU on D83XL1, Fixed length
17Oct26 00:00:00.59 job VGENC09 wrote 1028k bytes, 1028k bytes written to PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.59 SETUP job IXGLGGR wrote 278k5 bytes, 278k5 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.SVT.C09.DATA on IFA01C
17Oct26 00:00:00.59 SETUP job IXGLGGR wrote 401k4 bytes, 401k4 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.WKLDPROF.C09.DATA on IFA001
17Oct26 00:00:00.59 SETUP job IXGLGGR wrote 548k9 bytes, 548k9 bytes written to Linear top data set IXGLGGR.IFASMF.SVPLEX4.PERFRPT.C09.DATA on IFA019
17Oct26 00:00:00.59 SYSADM1 job D4P9MSTR wrote 4096 bytes, 4096 bytes written to Linear top data set DBX4.D4PB.LOGCOPY2.DS01.DATA.BKUP0316 on DBX413, Encrypted
17Oct26 00:00:00.60 job VGENC08 read 2982k bytes, 2982k bytes read from PDSE top data set PDSE.IST.GENTEST.MOSCHEN1 on SG2005
17Oct26 00:00:00.60 CICS job CICS2A81 read 12288 bytes, 12288 bytes read from KSDS Data top data set ADSUFILE.VF05D.ITEMACT.DATA on X4RLS7, VSAM RLS, Encrypted
17Oct26 00:00:00.60 CICS job CICS2A81 read 12288 bytes, 12288 bytes read from KSDS Data top data set ADSUFILE.VF06D.PARTS.DATA on X4RLS2, VSAM RLS, Encrypted
17Oct26 00:00:00.60 CICS job CICS2A81 read 20480 bytes, 12288 bytes read from KSDS Data top data set ADSUFILE.VF06D.ITEMACT.DATA on X4RLS5, VSAM RLS
17Oct26 00:00:00.60 CICS job CICS2A81 read 24576 bytes, 24576 bytes read from KSDS Data top data set ADSUFILE.VF06D.HOTEL1.DATA on X4RLS5, VSAM RLS
17Oct26 00:00:00.60 CICS job CICS2A81 read 28572 bytes, 24576 bytes read from KSDS Data top data set ADSUFILE.VF08D.HOTEL1.DATA on X4RLS8, VSAM RLS, Encrypted
17Oct26 00:00:00.60 CICS job CICS2A81 read 32768 bytes, 20480 bytes read from KSDS Data top data set ADSUFILE.VF04D.INVENTOR.DATA on X4RLS4, VSAM RLS
17Oct26 00:00:00.60 CICS job CICS2A81 read 36864 bytes, 8192 bytes read from KSDS Data top data set ADSUFILE.VF07D.VENDOR.DATA on X4RLS3, VSAM RLS
17Oct26 00:00:00.60 CICS job CICS2A81 read 40960 bytes, 28672 bytes read from KSDS Data top data set ADSUFILE.VF06D.HOTEL1.DATA on X4RLS8, VSAM RLS
17Oct26 00:00:00.60 CICS job CICS2A81 read 46592 bytes, 20480 bytes read from ESDS top data set CT$61.T6V82A81.DPHINTRA.DATA on X4C1C1
17Oct26 00:00:00.60 CICS job CICS2A81 read 49152 bytes, 16384 bytes read from KSDS Data top data set ADSUFILE.VF01D.INVENTOR.DATA on X4RLSB, VSAM RLS, Encrypted
17Oct26 00:00:00.60 CICS job CICS2A81 read 7680 bytes, 3072 bytes read from KSDS Index top data set ADSUFILE.VF08D.DATAENDB.INDEX on X4RLS6, VSAM RLS, Encrypted
17Oct26 00:00:00.60 CICS job CICS2A82 read 40960 bytes, 40960 bytes read from ESDS top data set CT$61.T6V82A82.DPHINTRA.DATA on X4C1C1

```

New fields for SMF 98-5/6/7/8

- New type=SMF fields
 - BYTES_READ
 - BYTES_WRITTEN
- Existing fields populated
 - JOBNAME
 - USER
 - DSN
 - VOLSER
- Entitled in zSecure Audit, zSCC, and zSecure Alert

Support new TDz anomalous activity alerts

SMF 98-5/6/7/8 records are input to AI engine in the Threat Detection for z (TDz) product

TDz exploits WIC to find most anomalous behavior and writes SMF 83 subtype 8.

zSecure Audit can be used to format 83-8 (and 98-5/6/7/8)

zSecure Alert can pass on the 83-8 as alerts 1807/2807

SMF 83-8 sent to QRadar SIEM and ArcSight

New fields for SMF 83-8

- New type=SMF fields
- Records are slightly confusing as they report on activity of a different system in the sysplex than where the record is written.
- Existing fields populated
 - ANOMALY_ID
DATASET_ACTIVITY
AGGR_DATASET_SIZE
 - SYSPLEX
SYSNAME
JOBNAME
USER
DSN
VOLSER
BYTES_WRITTEN
BYTES_READ
- Entitled in zSecure Audit, zSCC, and zSecure Alert

EV.A.T – events from Threat Detection

In the EV(ents) menu, there is a new Applications menu with TDz

zSecure Suite - Events - Applications		
Option ==> <input type="text"/>		
0 Omegamon	Omegamon events from SMF	
T TDz	Threat Detection for z/OS events from SMF	
zSecure Suite - Events - TDz		
Command ==> <input type="text"/>		
Show records that fit all of the following criteria:		
Anomaly ID	<input type="text"/>	(ID or EGN mask)
Userid	<input type="text"/>	(userid or EGN mask)
Jobname	<input type="text"/>	(jobname or EGN mask)
Data set name . . .	<input type="text"/>	
Volume	<input type="text"/>	(volume or EGN mask)
Intent	<input checked="" type="radio"/> 1. Read <input type="radio"/> 2. Write	
Sysplex	<input type="text"/>	(sysplex or EGN mask)
System name	<input type="text"/>	(system name or EGN mask)
Advanced selection criteria		
<input type="checkbox"/> Date and time		
Output/run options		
<input checked="" type="checkbox"/> Include detail	<input type="checkbox"/> Summarize	
<input type="checkbox"/> Print format	<input type="checkbox"/> Customize title	
		<input type="checkbox"/> Send as e-mail
<input type="checkbox"/> Background run		

Report type RESOURCE

Report type RESOURCE

The report type was added in 2012, but now there is a menu option RE.R

```
zSecure Suite - Resource

Command ==> _____  
  
Show resources that fit all of the following criteria  
Resource name . . . _____  
Resource class . . . _____ (Class or EGN mask)  
Sensitivity . . . _____ (Sensitivity or EGN mask)  
Sensitivity priority ____ (Operator + priority)  
System . . . . . _____ (System or EGN mask)  
Complex . . . . . _____ (Complex or EGN mask)  
  
Additional selection criteria  
- RACF                    - ACF2  
  
Output/run options  
- Show differences  
- Print format            Send as e-mail  
    Background run        Full detail form        Narrow print
```

```
zSecure Suite Display Selection

Command ==> _____  
  
Name      Summary   Records   Title  
- RACFGRES      1   139566   General resources and their RACF protection  
- RACFGPRF      1   139566   RACF general resource profiles and their resources  
***** Bottom of Data *****
```

Report type RESOURCE – class, resource

```
General resources and their RACF protection
Command ==> _____ Line 1 of 56
All resources   Scroll==> CSR
Complex       Classes
NMPIPL87      56
System  Class  Act Gen Rcl Resources
ZS14    ACICSPCT Yes Yes No     206
ZS14    APPL     Yes Yes Yes    9
ZS14    CCICSCMD Yes Yes No    104
ZS14    CONSOLE   Yes Yes Yes   2
ZS14    CRYPTOZ   Yes Yes Yes   27
ZS14    CSFKEYS   Yes Yes Yes   25
ZS14    DASDVOL   No  Yes No    267
ZS14    DEVICES   Yes Yes Yes   26
ZS14    DSNADM    Yes Yes No    355
ZS14    FACILITY  Yes Yes Yes  3878
ZS14    FIELD     Yes Yes Yes   4
ZS14    IIMS      Yes Yes No    47
ZS14    JESINPUT   Yes Yes No   3536
4 Jun 2024 14:38
```

```
General resources and their RACF protection
Command ==> _____ Line 1 of 104
All resources   Scroll==> CSR
Complex       Classes
NMPIPL87      56
System  Class  Act Gen Rcl Resources
ZS14    CCICSCMD Yes Yes No    104
Resource
allcommands
ASSOCIATION
ATOMSERVICE
AUTINSTMODEL
AUTOINSTALL
BRFACILITY
BUNDLE
BUNDLEPART
System  Sensitivity GlbAcc  UACC   IDSAcc  Wrn Failure Success Re
ZS14    CICSOther    NONE      NONE    No  READ   READ   READ   ZS
ZS14    CICSADCBI  NONE      NONE    No  READ   READ   READ   ZS
ZS14    <more>      NONE      NONE    No  READ   READ   READ   ZS
ZS14    <more>      NONE      NONE    No  READ   READ   READ   ZS
ZS14    <more>      NONE      NONE    No  READ   READ   READ   ZS
ZS14    <more>      NONE      NONE    No  READ   READ   READ   ZS
ZS14    <more>      NONE      NONE    No  READ   READ   READ   ZS
ZS14    CICSBndlPI  NONE      NONE    No  READ   READ   READ   ZS
4 Jun 2024 14:38
```

Detail - contributing member/grouping profiles

```
General resources and their RACF protection                               Line 1 of 23
Command ==> _____                                         Scroll==> CSR
All resources                                         4 Jun 2024 14:38

Complex Ver System   Resource location
- NMPIPL87      ZS14    Z$14.CICS.CICS55.CMD
                           Z$14.CICS.CICS56.CMD
                           Z$14.CICS.CICS62.CMD
                           Z$14.CICS.CICS61.CMD

Sensitivity Condition          Access  Pri Privilege
CICSAINSTMA                  ALTER    4 Can remove a terminal AUTOINSTALL model definition from the local CICS system
CICSAINSTMI                  READ     2 Can check whether a terminal AUTOINSTALL model is installed in the local CICS system

Class   Resource
- CCICSCMD AUTINSTMODEL
  Class  Profile
  - VCICSCMD CMDSYSP4
  - VCICSCMD CMDSYSP3
  - CCICSCMD *
    UACC    IDSAcc  GlbAcc  Wrn Failure Success
    NONE           No  READ    READ
    User    Access  ACL id  When          Name        DfltGrp  RI
    -group-  READ    VESGRP
    -group-  UPDATE  SYSPROG
    -group-  ALTER   CRMB
    CRMBJU2  ALTER   CRMBJU2
    CRMBJU1  READ    CRMBJU1
                                          [REDACTED]      TEST0001
                                          CRMB
*****
***** Bottom of Data *****
```

New data set sensitivity types

Non-VSAM

- AccMonData
- CEF Carla
- zSecFreeze
- SMFadapters
- DB2 ArchLog
- DB2 Drivers
- zSCC Parm

VSAM:

- DB2 ActLog
- DB2 SysCtlg
- DB2 TbSpace

New sensitivity types for CSFSERV resources

Sensitivity type	ZConcern text
CSFBRCKR	Can use the CKDS KEYS utility to list labels and display key attributes and record metadata in the CKDS
CSFBRCKU	Can use the CKDS KEYS utility to modify metadata, archive and recall records in the CKDS
CSFBRCKC	Can use the CKDS KEYS utility to delete records in the CKDS
CSFBRCKA	Can use the CKDS KEYS utility functions without access to the CSFKEYS profile for the label
CSFBRPKR	Can use the PKDS KEYS utility to list labels and display key attributes and record metadata in the PKDS
CSFBRPKU	Can use the PKDS KEYS utility to modify metadata, archive and recall records in the PKDS
CSFBRPKC	Can use the PKDS KEYS utility to delete records in the PKDS
CSFBRPKA	Can use the PKDS KEYS utility functions without access to the CSFKEYS profile for the label
CSFBRTKR	Can use the PKCS11 TOKEN utility and display data in the TKDS
CSFBRTKU	Can use the PKCS11 TOKEN utility to modify metadata, archive and recall records in the TKDS
CSFCMK	Can use the change master key utility, including the panel for a local change master key, the Coordinated KDS Administration service, and CSFEUTIL
CSFCONV	Can use the PCF CKDS to ICSF CKDS conversion utility
CSFCRC	Can use the Coordinated KDS Administration callable service
CSFDKCS	Can use the Master Key Entry utility
CSFGKF	Can generate key fingerprint required by KGUP if key lifecycle auditing is enabled
CSFKGUPR	Can use the ADD, RENAME and OPKYLOAD functions of the Key Generator Utility Program
CSFKGUPU	Can use the DELETE and UPDATE functions of the Key Generator Utility Program
CSFOPKL	Can use the Operational Key Load utility to load keys to the CKDS
CSFPCAD	Can activate and deactivate cryptographic processors
CSFPKDR	Can use the PKDS reencipher and PKDS activate utilities
CSFPMCI	Can use the pass phrase master key/KDS initialization utility
CSFREFR	Can use the refresh CKDS or PKDS utility, including the panels for a local refresh, the Coordinated KDS Administration service, and CSFEUTIL (CKDS) and CSFPUTIL (PKDS)
CSFRSWS	Can use the Administrative control functions utility to enable dynamic CKDS/PKDS access
CSFRWP	Can use the CKDS Conversion2 - rewrap option
CSFSMK	Can use the Set Master Key utility
CSFSSWS	Can use the Administrative control functions utility to disable dynamic CKDS/PKDS access
CSFUDM	Can use the User Defined Extensions (UDX) management functions

Ideas

Ideas

[ZSECURE-I-574](#) Display X.509 Extended key usage

(No formal Idea.) Update Certificate algorithm to include RSASSA-PSS parm

[ZSECURE-I-593](#) Display new Quantum Safe Algorithms in help panels

[ZAUDIT-I-376](#) Ability to retract a configuration assertion

[ZSECURE-I-597](#) Allow use of System symbols in the SETUP Files dialog

[ZSECURE-I-564](#) Ability to use ONLYAT with CKGRACF Commands
(NOPROPAGATE keyword.)

[ZSECURE-I-573](#) Access Monitor reports: add profile key used

[ZALERT-I-137](#) Add master key type to alert 1617

New zSecure Redbook

Security impact forecasting (SG24-8578)

In this Redbook we explain how to use the zSecure Admin components **Access Monitor** and **RACF-Offline** together to forecast the impact of your RACF security definition changes so you can apply them with confidence.

[IBM Redbook](#)

Draft Document for Review February 14, 2025 9:12 am SG24-8578-00



IBM RACF Security Impact Forecasting using IBM zSecure

Bill White

Mike Riches

Elijah Swift

Jeroen Tiggelman

Scott Woolley

Tom Zeehandelaar



IBM Z

Security



Redbooks

Upgrade considerations

Interactions & Dependencies

- Software Dependencies
 - Runs on any currently supported z/OS release
 - The zSecure portfolio and zSCC are priced software products
 - Besides the solution elements, there are some solution packages that contain several of them:
<https://community.ibm.com/community/user/security/blogs/jeroen-tigelman/2019/12/01/ibm-security-zsecure-administration-auditing-and-c>
- Hardware Dependencies
 - None, except as possibly implied by z/OS releases in support

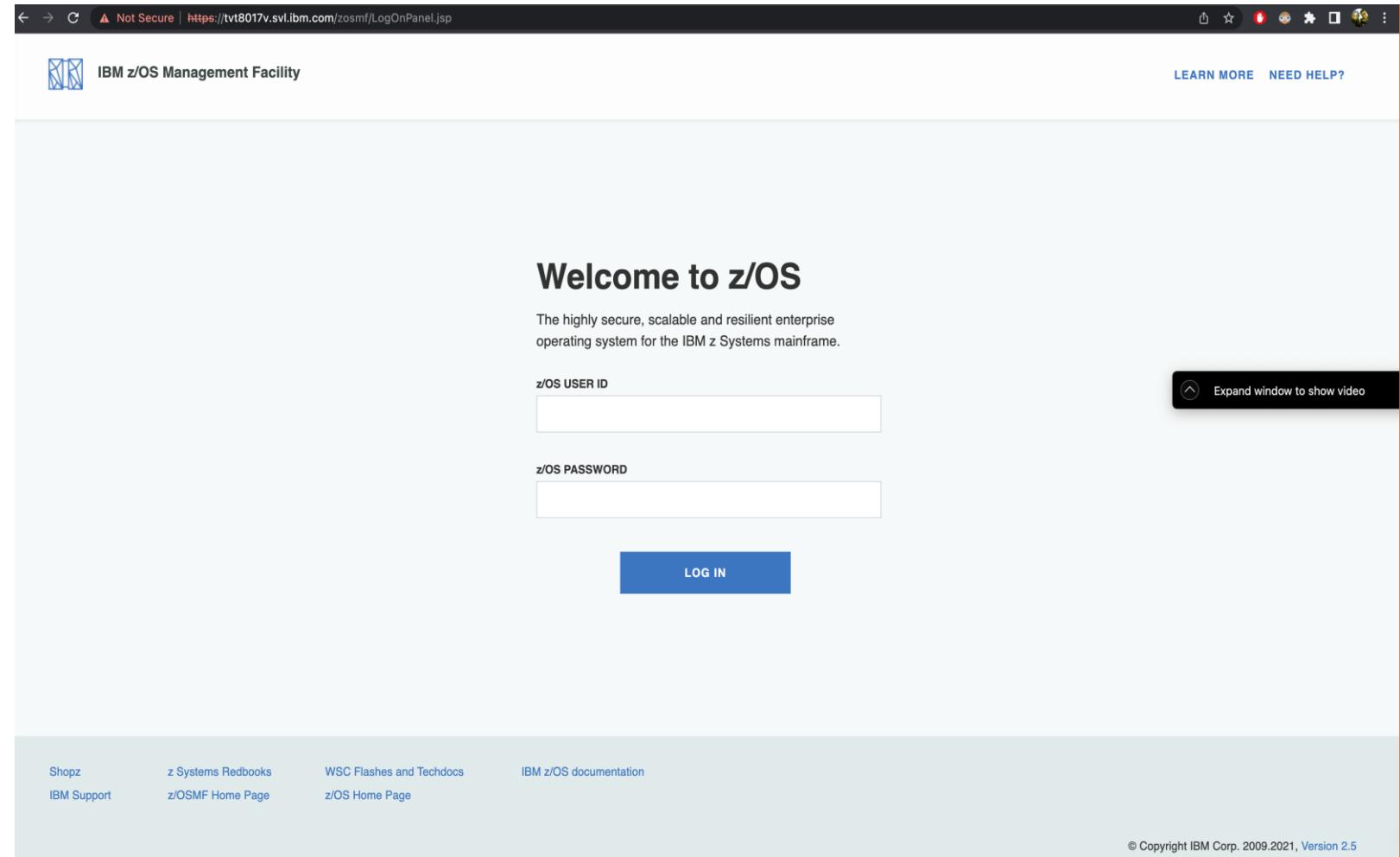
Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level:
No, runs on any currently supported z/OS release

For z/OS 3.2, zSecure 3.2 is required

zSecure Admin plugin for z/OSMF

- Authentication of plugin through z/OSMF, over HTTPS session
- As secure or insecure as you make z/OSMF
- Modern, runs on cross-platform web-browsers.
- Designed and implemented using IBM Carbon, IBM's open source design system for products and digital experiences.

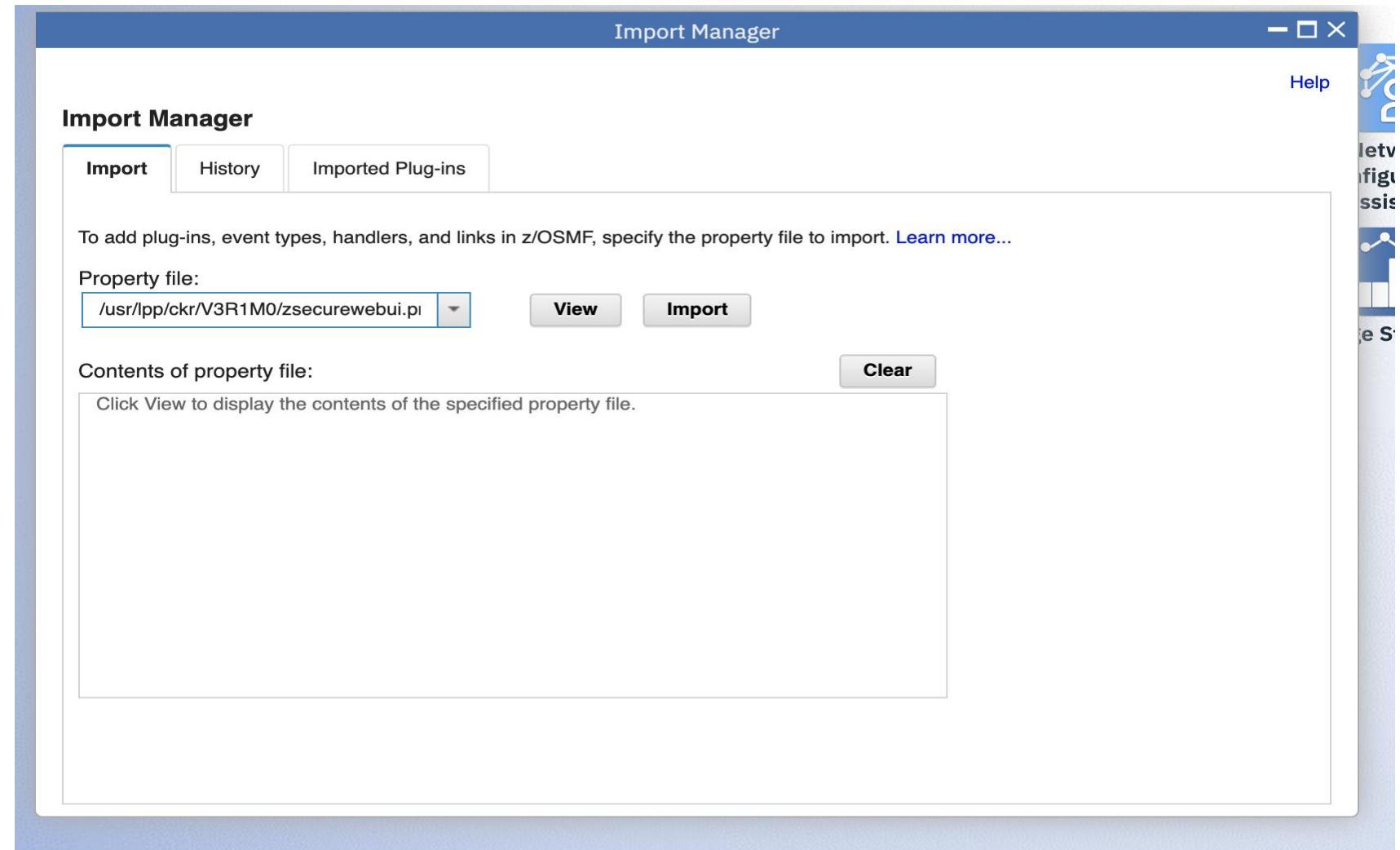


Installation & Configuration

- Required APARs for Compliance can be found in the [Compliance technote](#)
- Required APARs for the Service Stream Enhancements are in
 - <https://community.ibm.com/community/user/security/blogs/jeroen-tiggelman/2025/02/02/ibm-zsecure-31-multi-system-support-in-the-web-ui> (January 2025)
 - <https://community.ibm.com/community/user/security/blogs/jeroen-tiggelman/2024/11/18/ibm-security-zsecure-admin-311-and-other-recent-zs> (October 2024)
 - <https://community.ibm.com/community/user/security/blogs/jeroen-tiggelman/2024/04/12/ibm-security-zsecure-31-db2-secure-row-and-column> (April 2024)
- These blog entries also point out migration considerations
- **Changes are required for the setup of the started tasks that can now run under MSTR!**
- Note that the October update introduced the zSecure Admin Web UI. This update comes with a new license (including open source). The Web UI plug-in identifies itself as zSecure Admin 3.1.1. Since other components are shared between Admin, Audit, etc. these still use the release level 3.1.0.

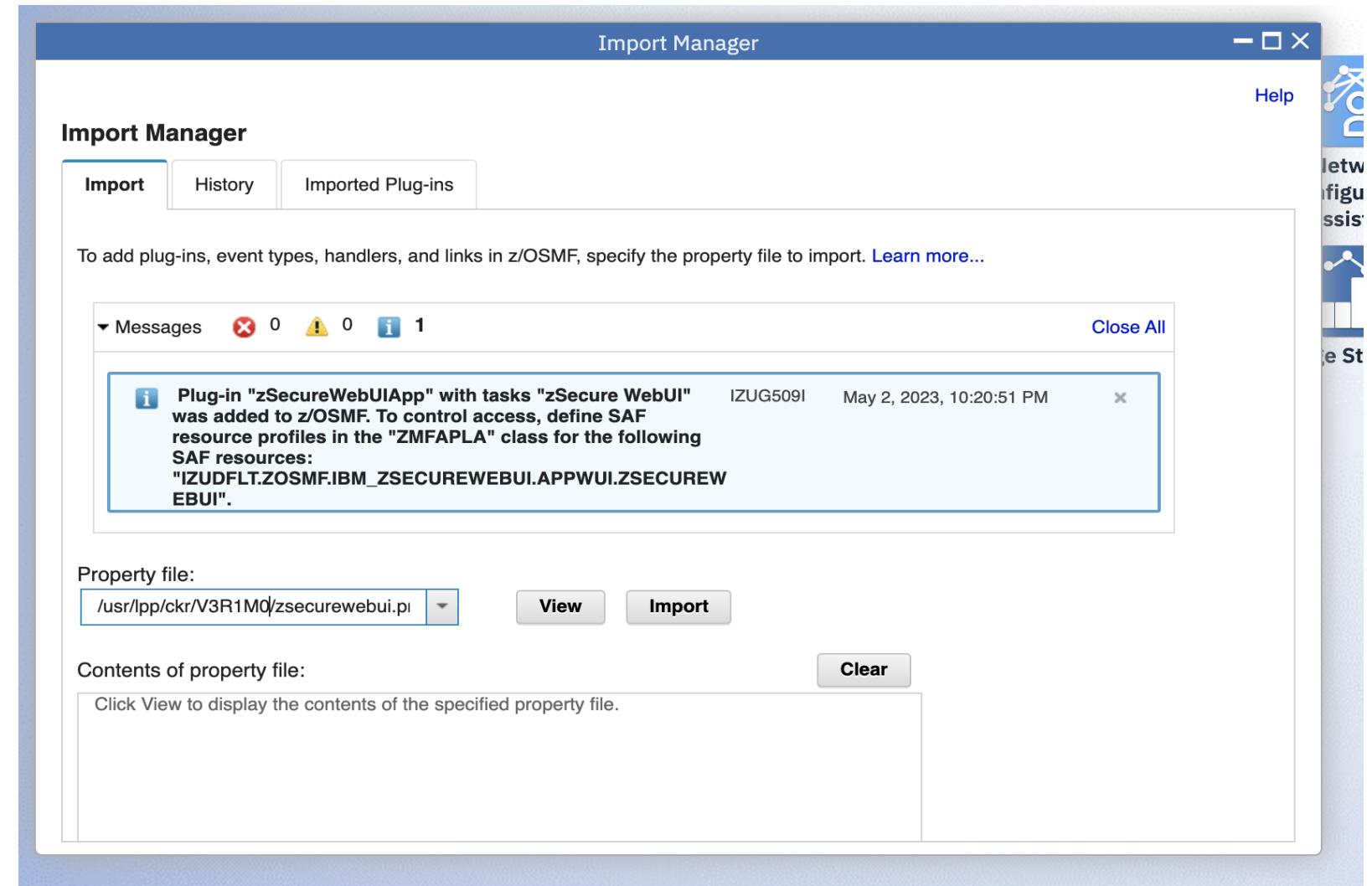
zSecure plug-in for z/OSMF (Installation) (1)

- Administrator needs to import zSecure plugin into z/OSMF via import manager
- Pre-requisite : Installation of source-code and properties file of plugin into proper location



zSecure plug-in for z/OSMF (Installation) (2)

- A message is displayed to indicate whether the plug-in was added. If so the plug-in and its tasks are added to the z/OSMF dashboard.

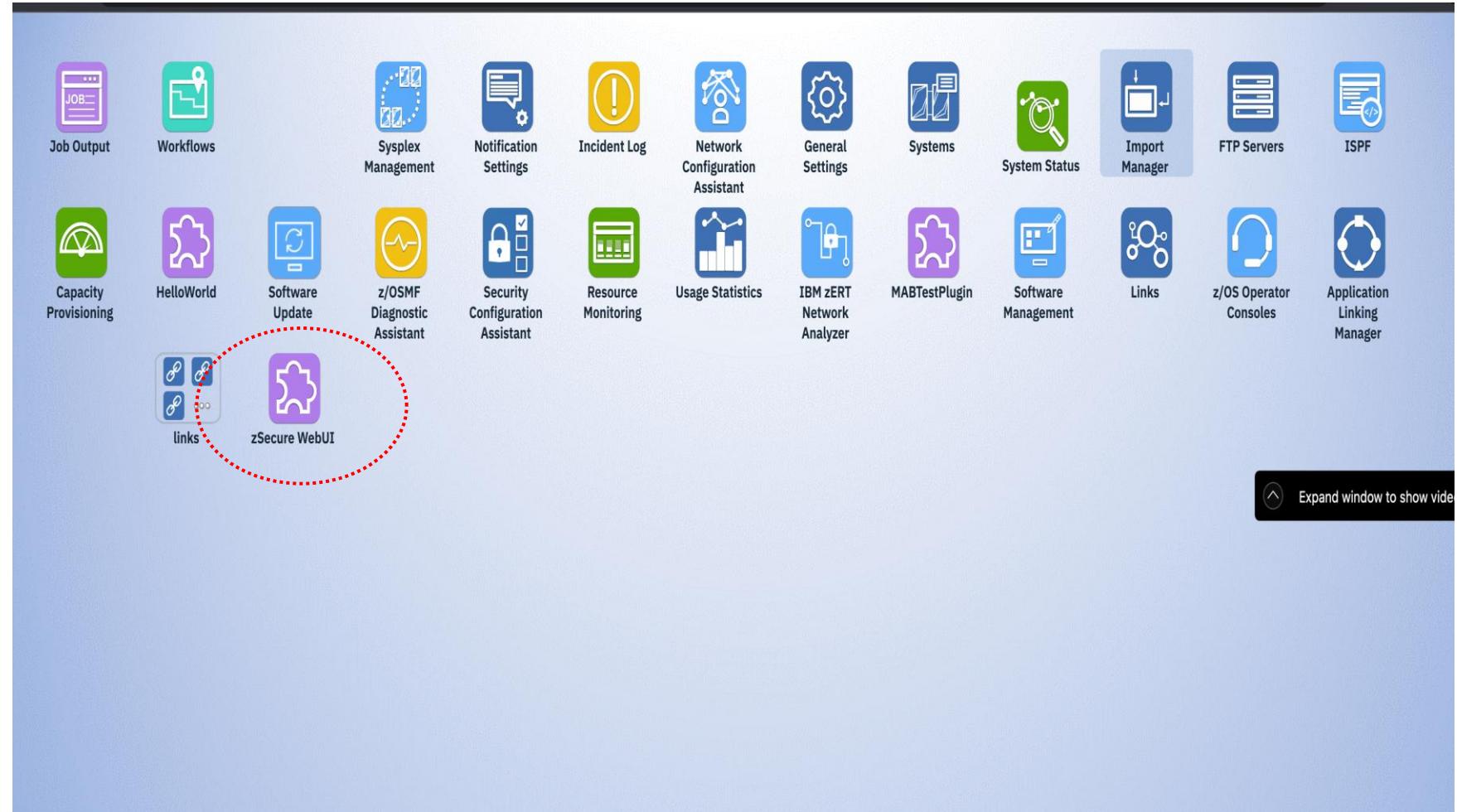


zSecure plug-in for z/OSMF (Authorization)

- Security is based on following two concepts.
 - **User authentication** : User's credentials are verified by the z/OS host system through the SAF interface or a security management product (for example, RACF) when a user attempts to log in to z/OSMF.
 - **User authorization** : Access to your application is controlled through SAF resource profile <safPrefix>.<taskSAFResourceName>, where <safPrefix> is configured in z/OSMF and is by default IZUDFLT and <taskSAFResourceName> is the SAF resource name you specified for the task in the plug-in property file. The SAF resource profile is defined in the ZMFAPLA class.
 - IZUDFLT.ZOSMF.IBM_ZSECUREWEBUI.APPWUI.ZSECUREWEBUI

zSecure plug-in for z/OSMF

- Once imported, the plug-in can be started from z/OSMF desktop by double-clicking the zSecure WebUI icon.



Summary

- zSecure regularly ships Service Stream Enhancements. These are communicated through the [Z Security Community](#).
- The October update introduced the zSecure Admin Web UI, which will replace zSecure Visual (which will be [end of marketing](#) in September 2025)
- The CIS Benchmark for Db2 is only available with a zSCC entitlement. Do not be surprised when major future compliance-specific enhancements such new report types require a zSCC entitlement. (But simple updates of existing report types like SMF are likely to be provided in zSecure Audit as well.)

Appendix

- Top level blog entry to find relevant zSecure announcements:
 - <https://community.ibm.com/community/user/security/blogs/jeroen-tiggelman/2018/11/09/ibm-security-zsecure-today>