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

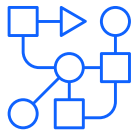
- Who (Audience)
  - Systems programmers, Security administrators, Auditors, Compliance Assessors
- What (Solution)
  - Makes security administration, security compliance, and security compliance checking easier
- Wow (Benefit / Value, Need Addressed)
  - Reduces need for green screen skills by allowing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

zSecure Admin Web UI

Feature highlights

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

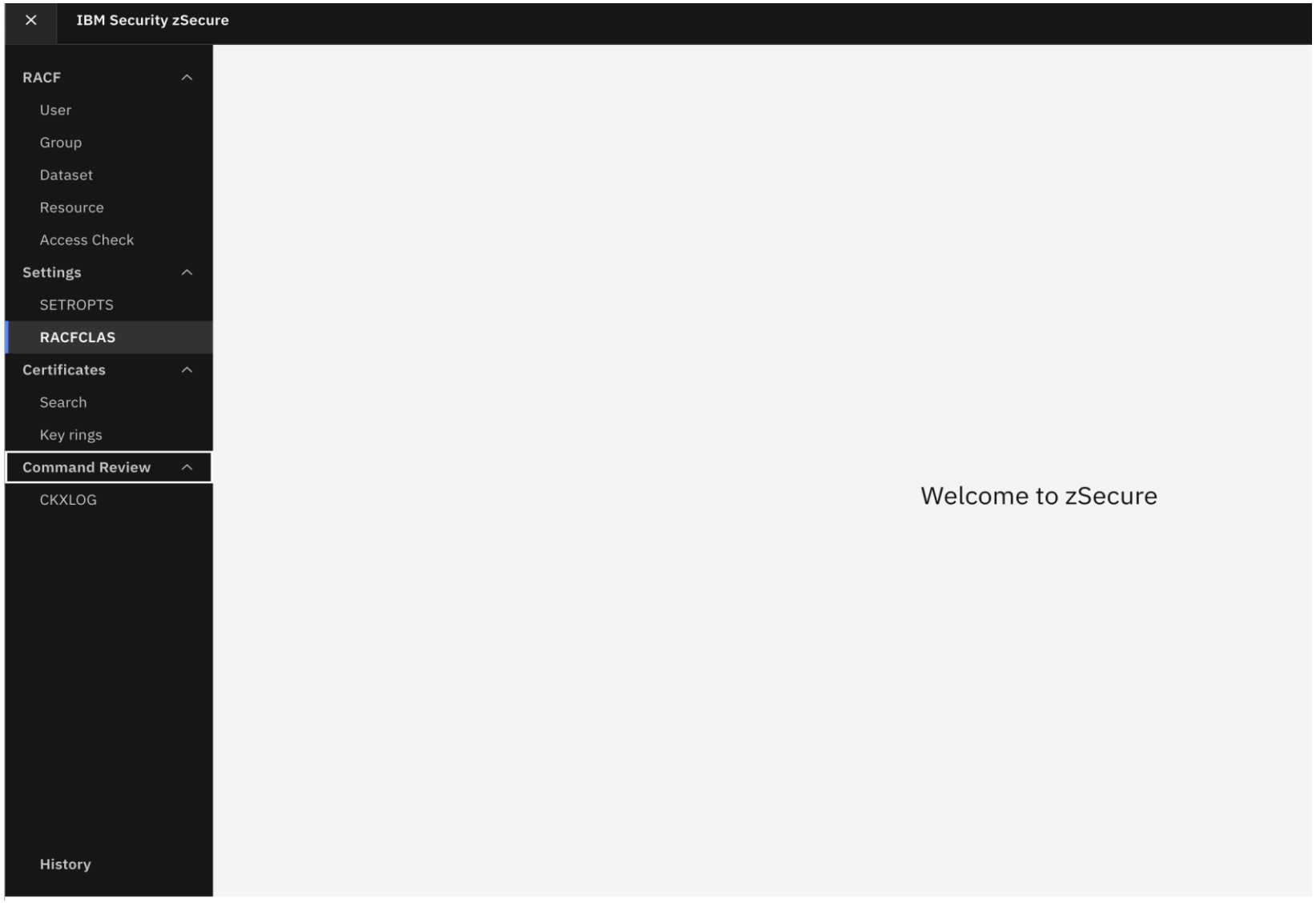
- Support for non-standard character sets such as Danish, Hebrew and more.

Export, Ticket ID support and more...

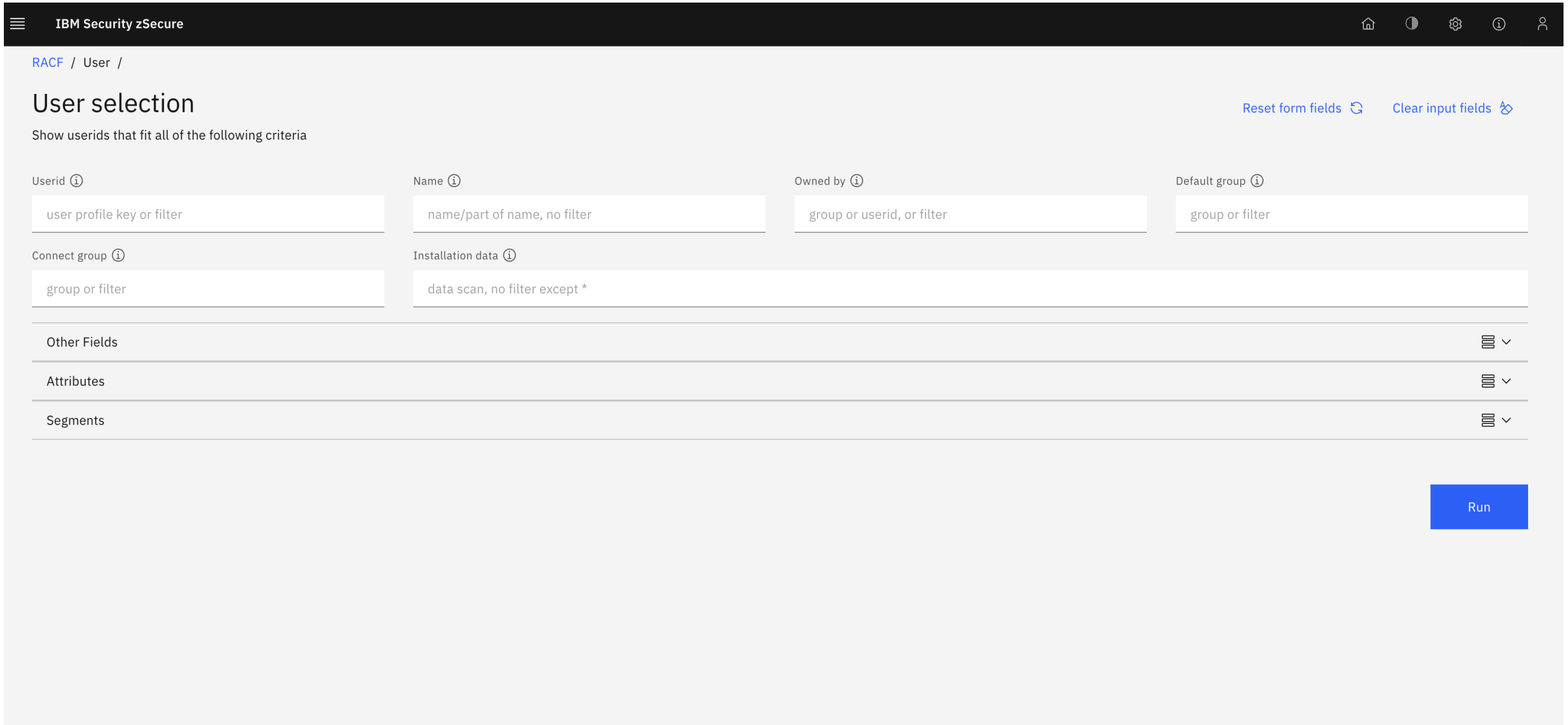
Quickly export data in PDF or Excel formats

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

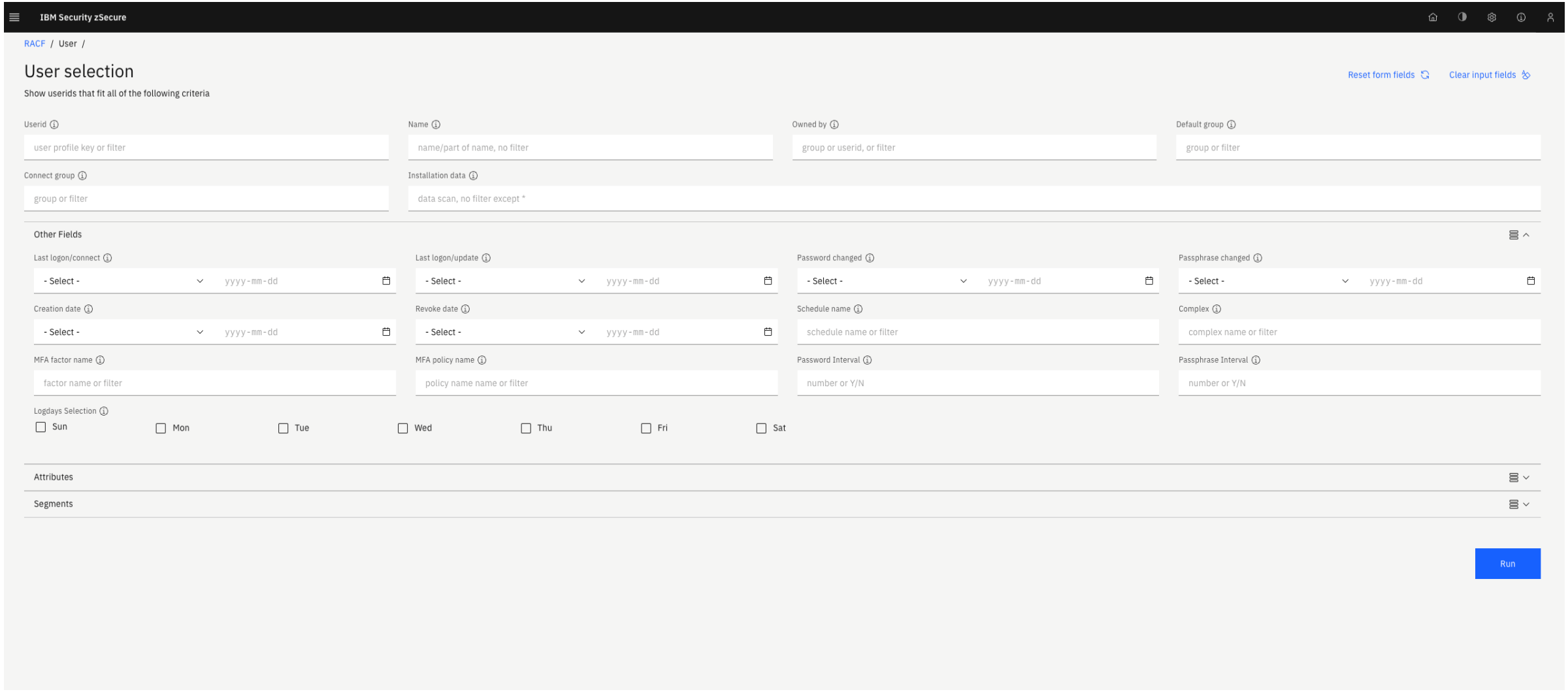
Expanded Drop Down Menu



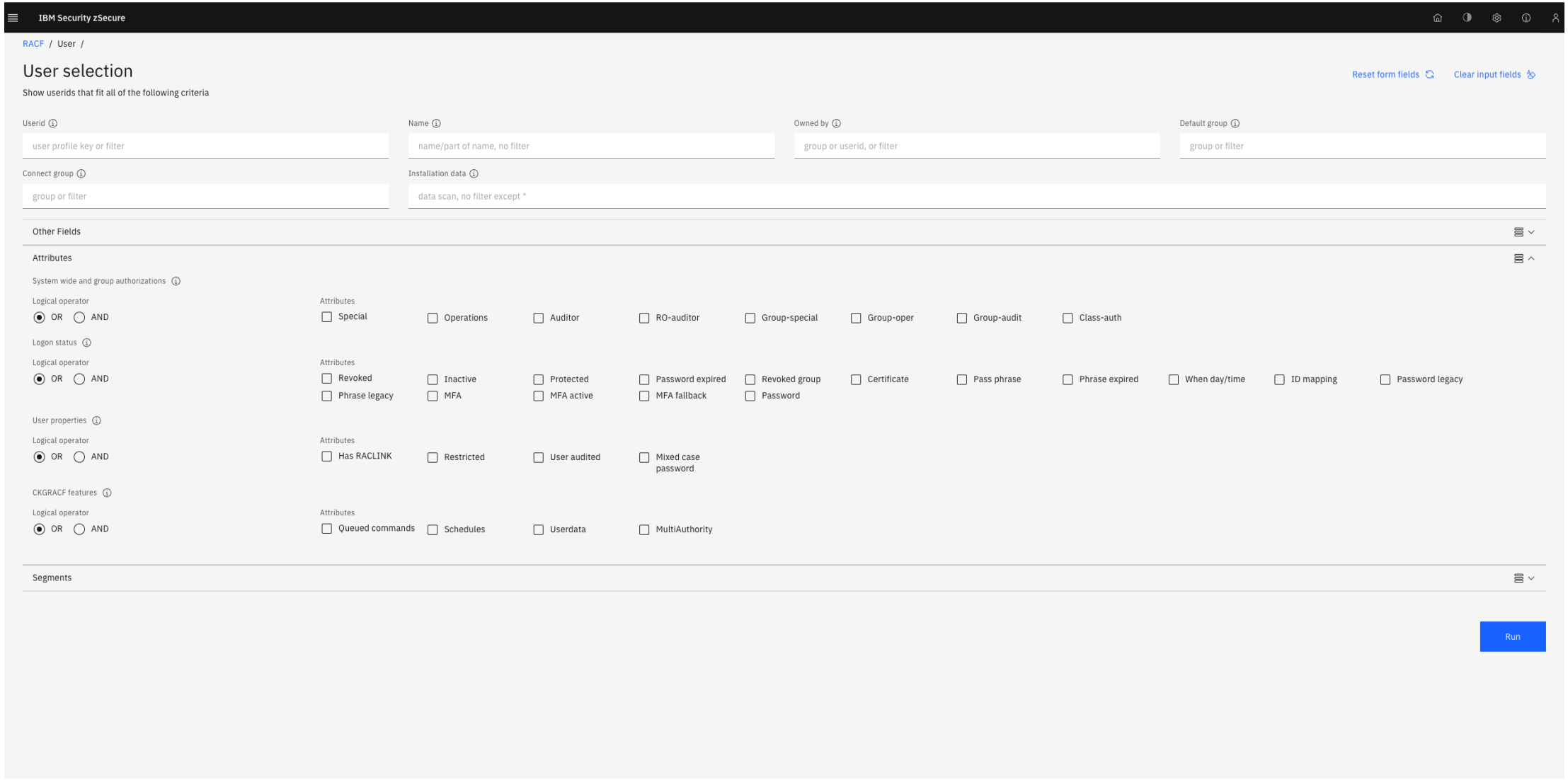
User Selection



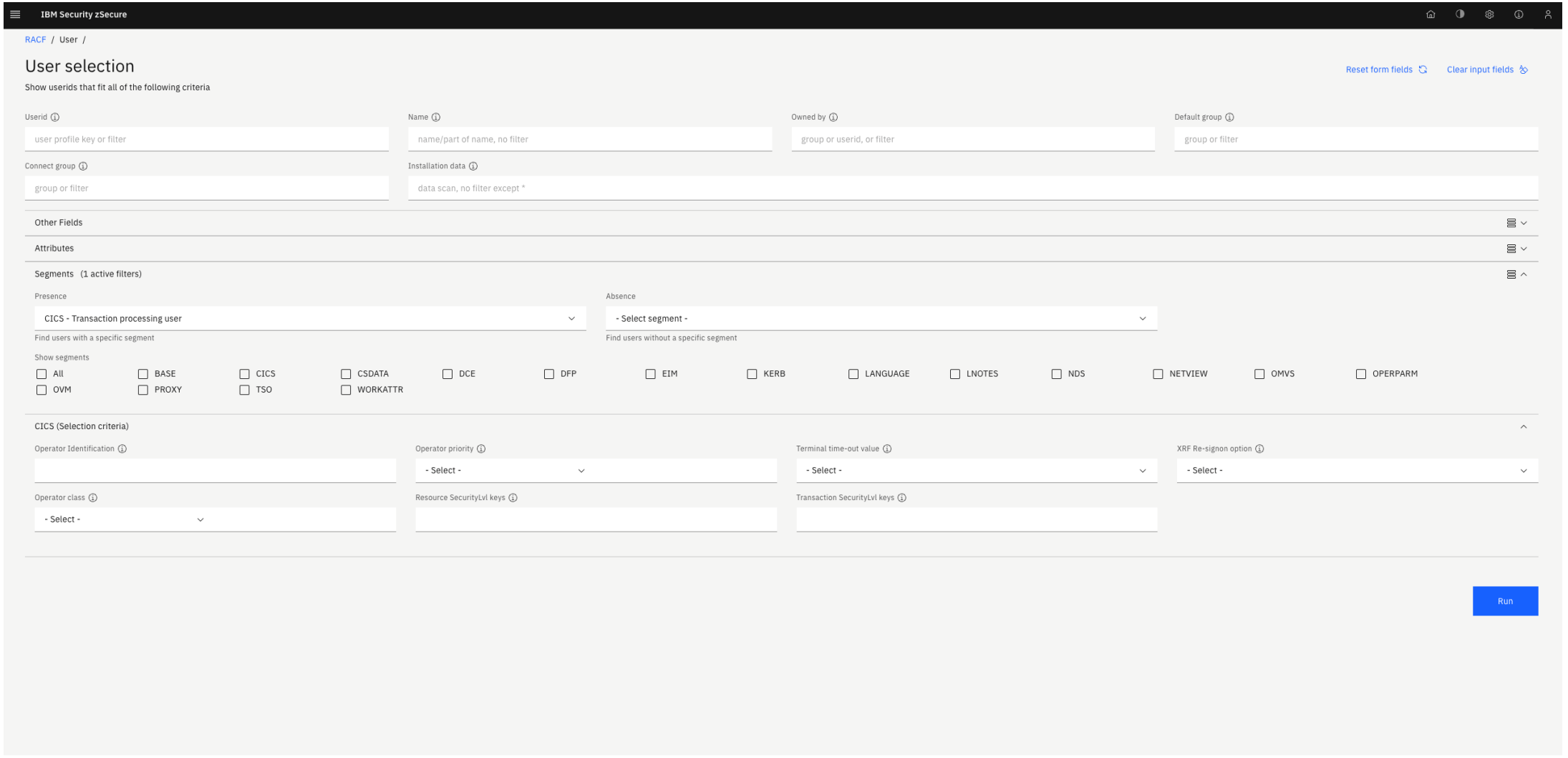
User Selection – Other Fields



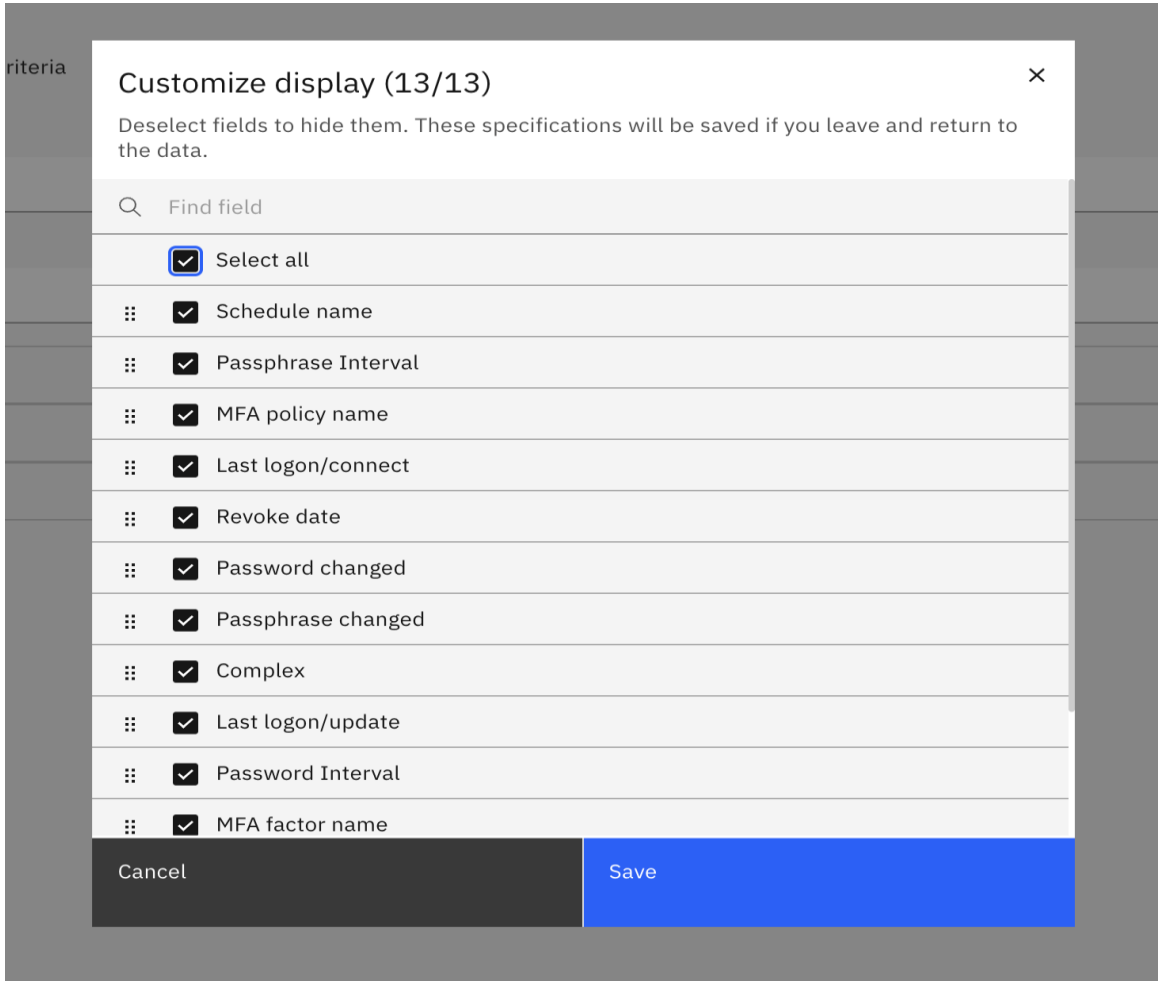
User Selection – Attributes

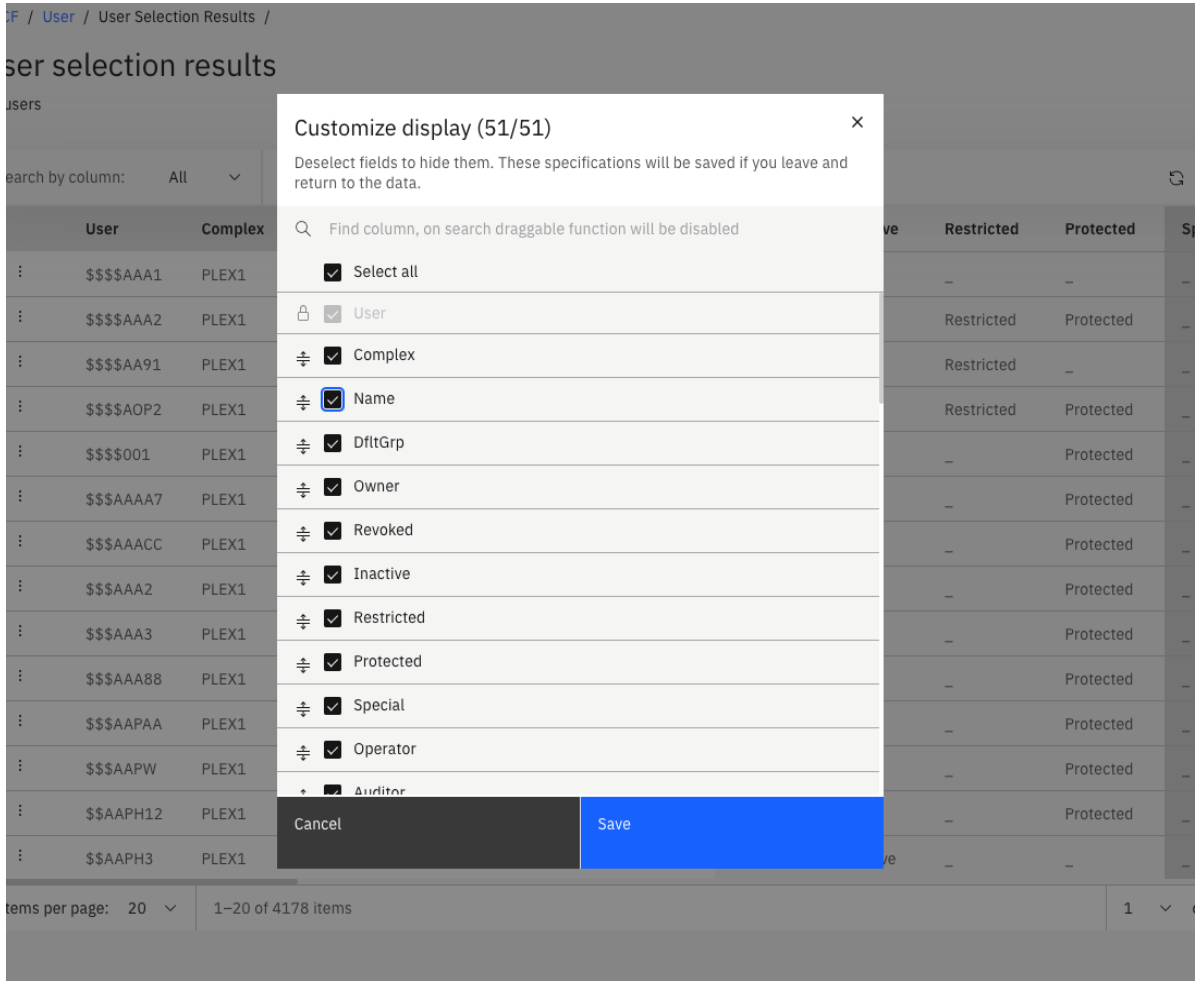


User Selection – Segment selection

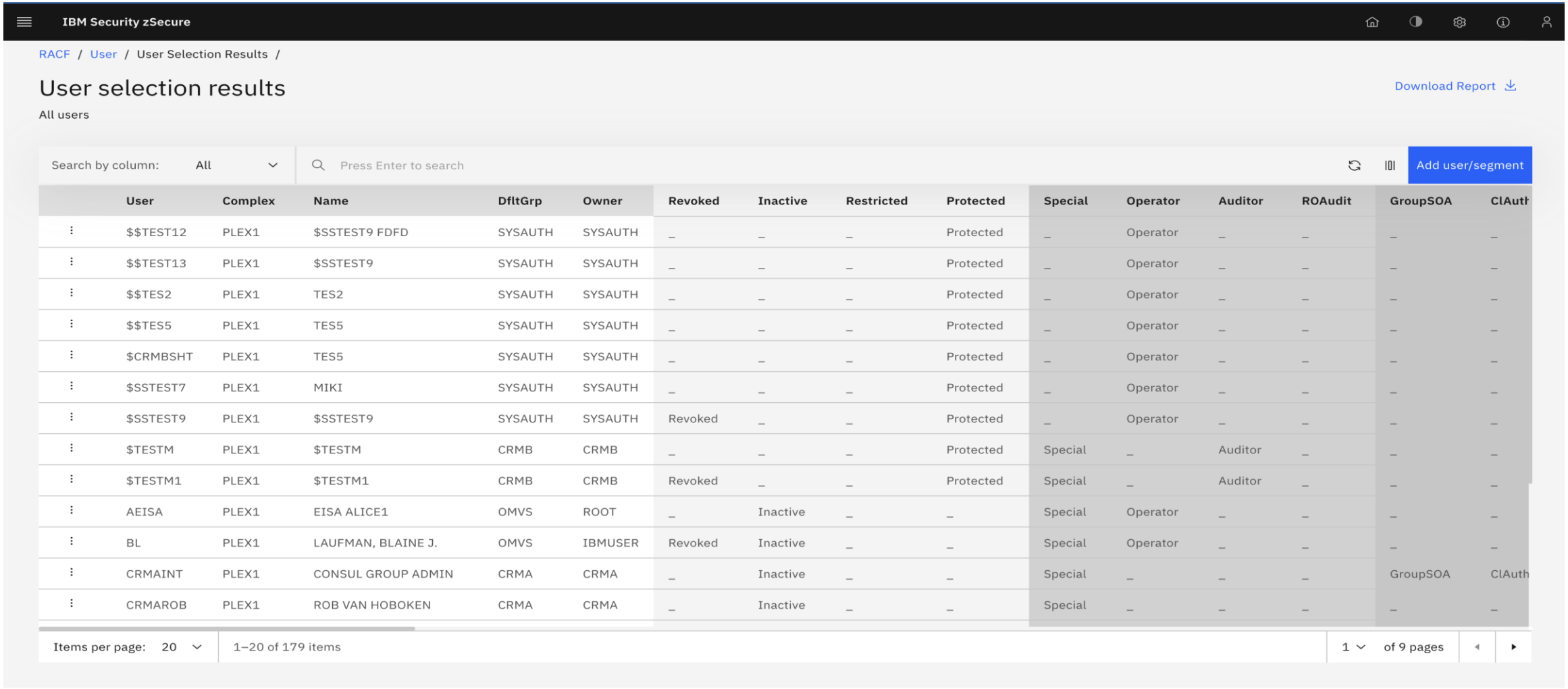


Customization options for fields in selection and selection results pages



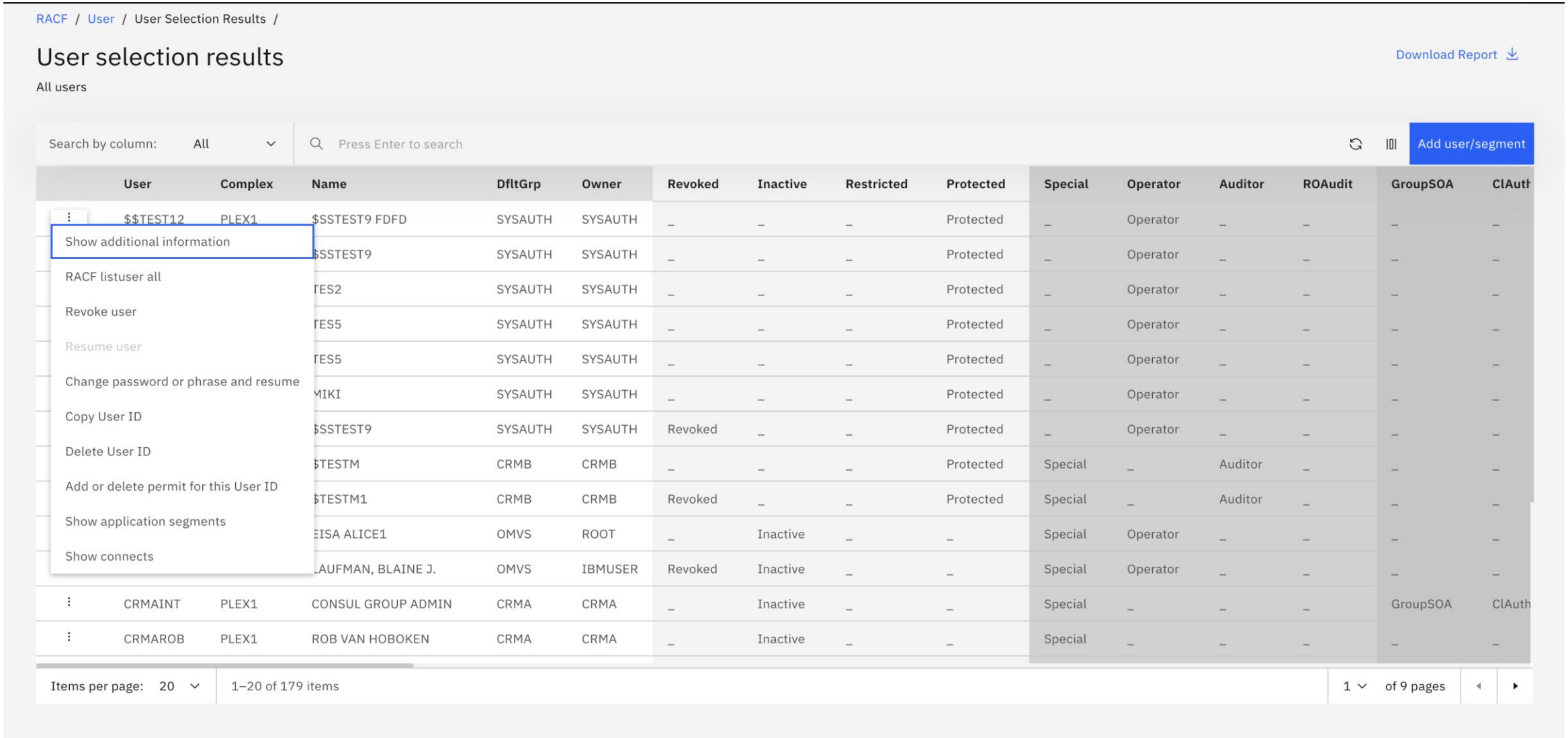


User Selection results – Select Users, Search bar, Search by column



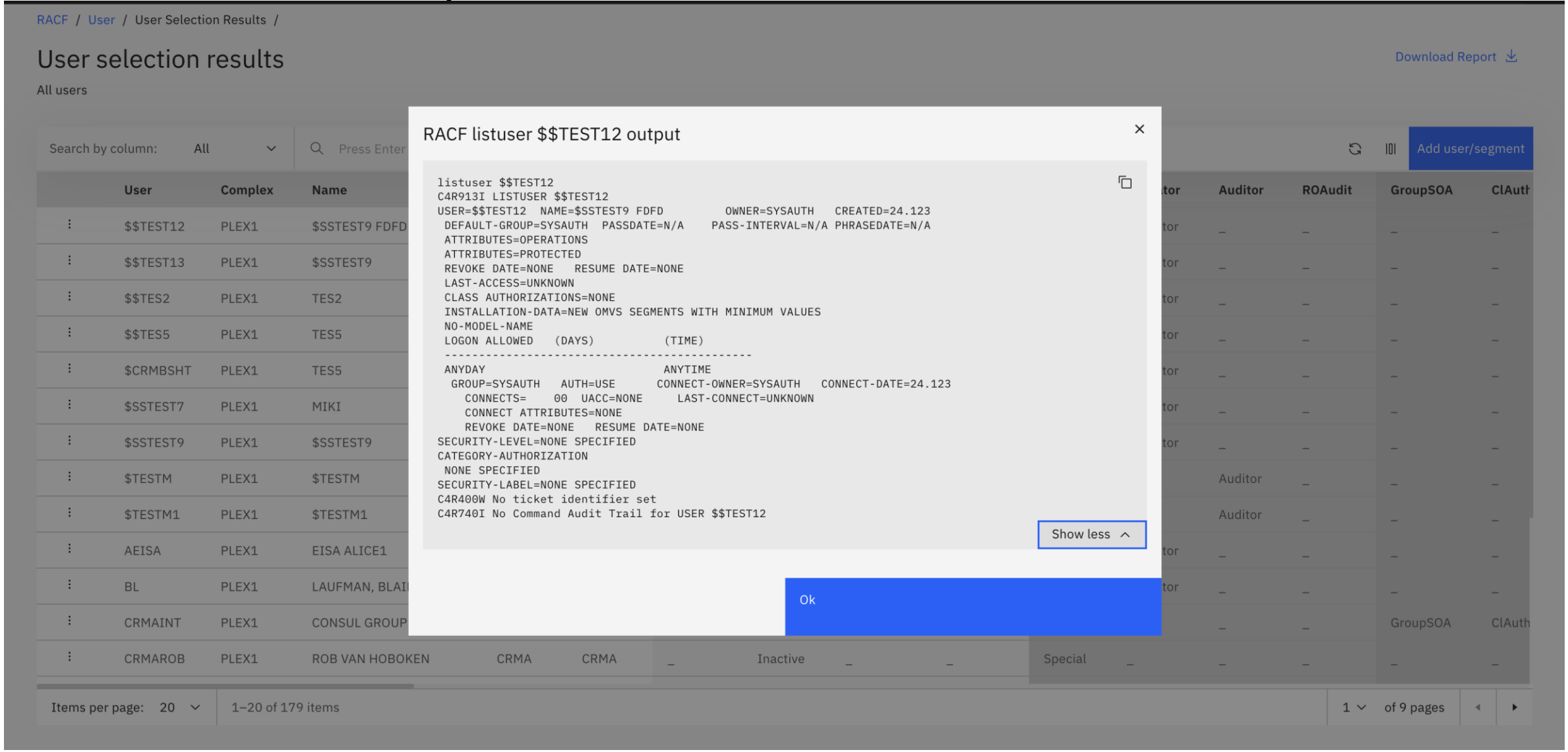
User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth
$$TEST12	PLEX1	$SSTEST9 FDFD	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
$$TEST13	PLEX1	$SSTEST9	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
$$TES2	PLEX1	TES2	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
$$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	_	_	_	_	_

User selection results - Action button options

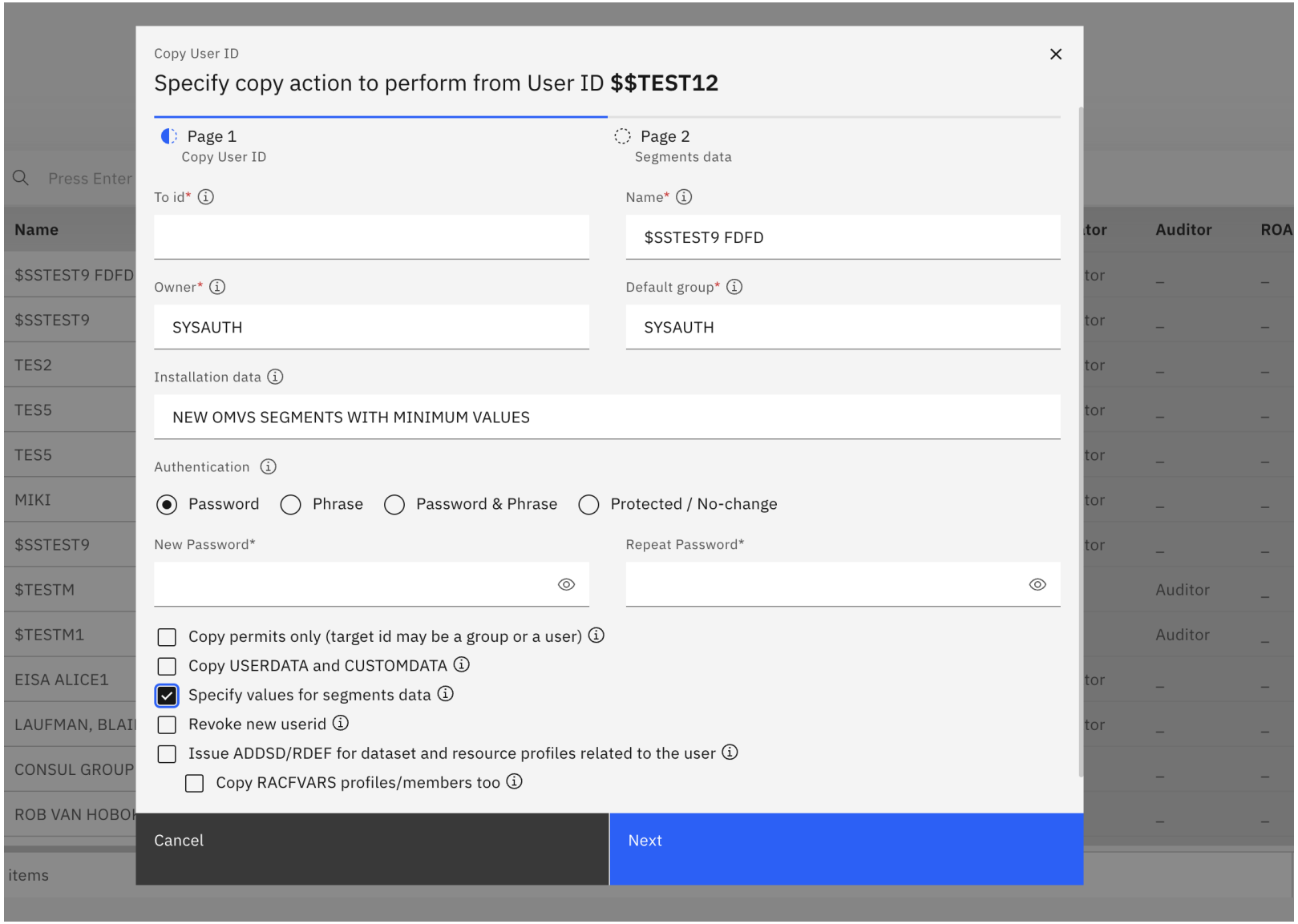


User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth
$$TEST12	PLEX1	$SSTEST9 FDFD	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		$SSTEST9	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		TES2	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		TES5	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		TES5	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		MIKI	SYSAUTH	SYSAUTH	_	_	_	Protected	_	Operator	_	_	_	_
		$SSTEST9	SYSAUTH	SYSAUTH	Revoked	_	_	Protected	_	Operator	_	_	_	_
		$TESTM	CRMB	CRMB	_	_	_	Protected	Special	_	Auditor	_	_	_
		$TESTM1	CRMB	CRMB	Revoked	_	_	Protected	Special	_	Auditor	_	_	_
		EISA ALICE1	OMVS	ROOT	_	Inactive	_	_	Special	Operator	_	_	_	_
		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	_	_	_	_	_

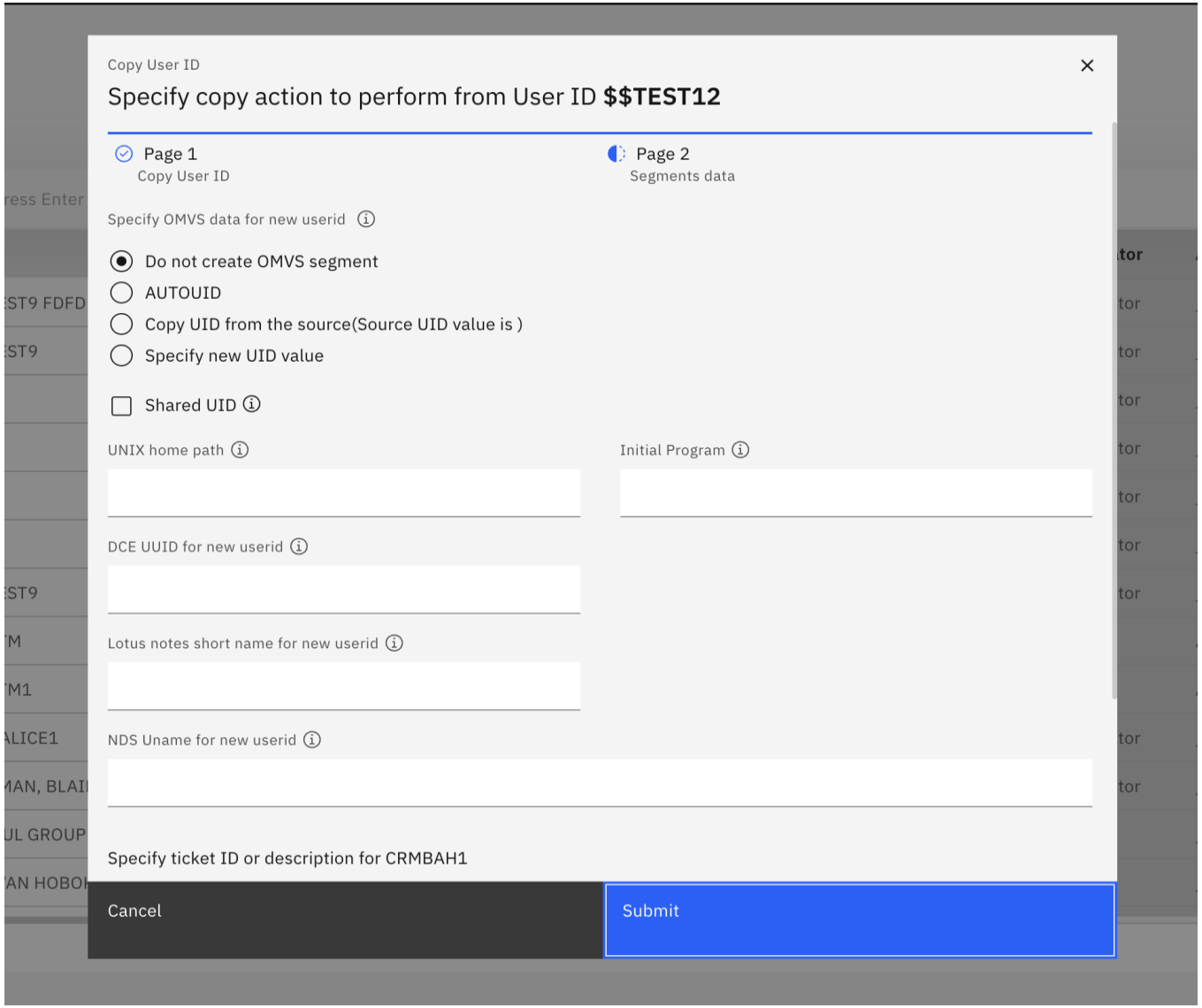
Action example



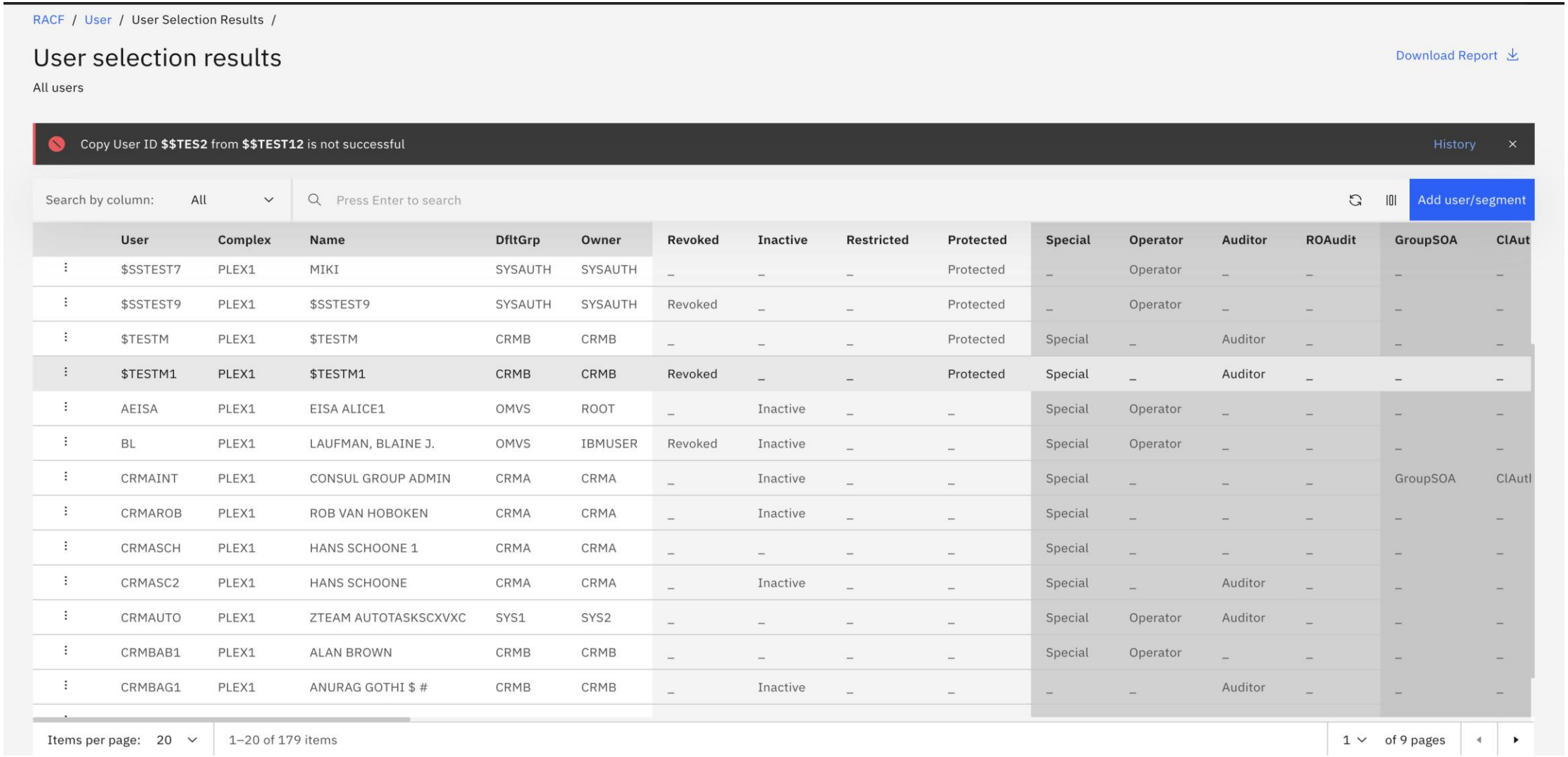
Copy Command



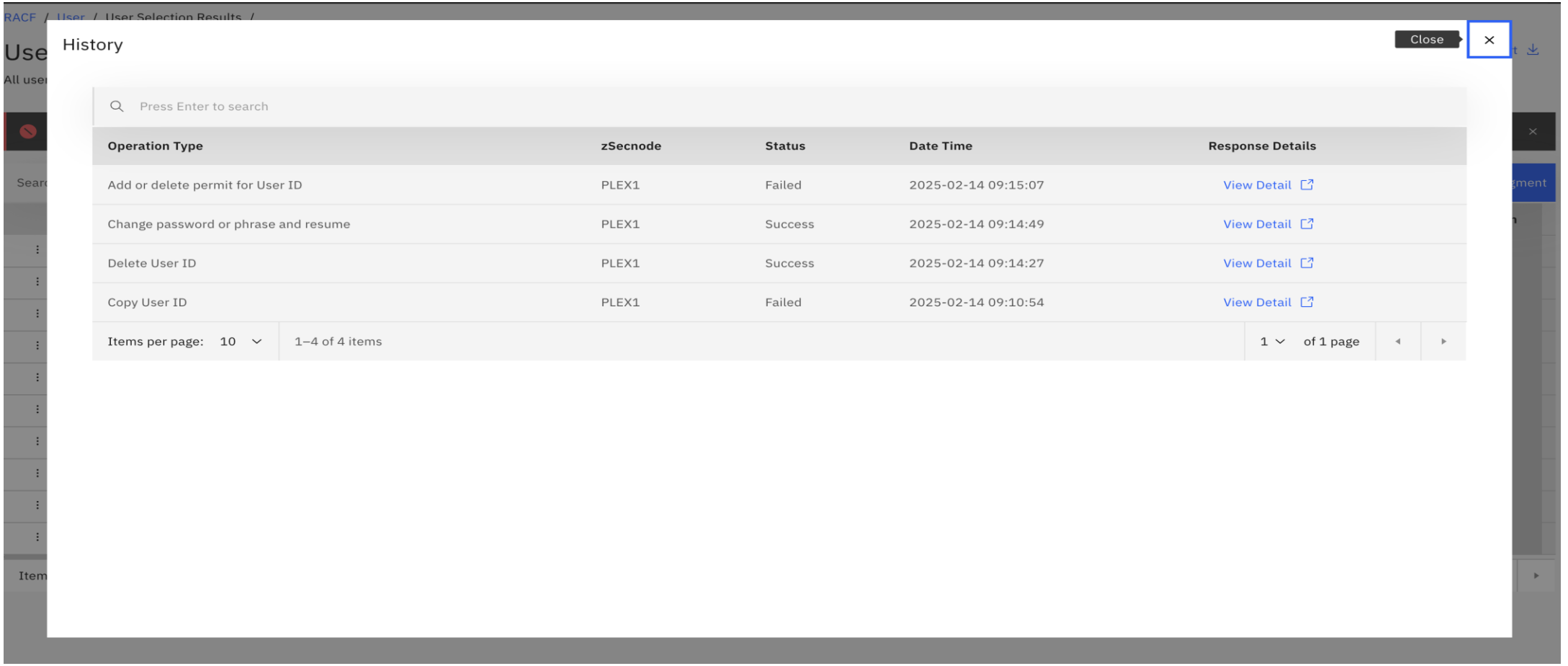
Copy Command – segment data



Copy Command response output

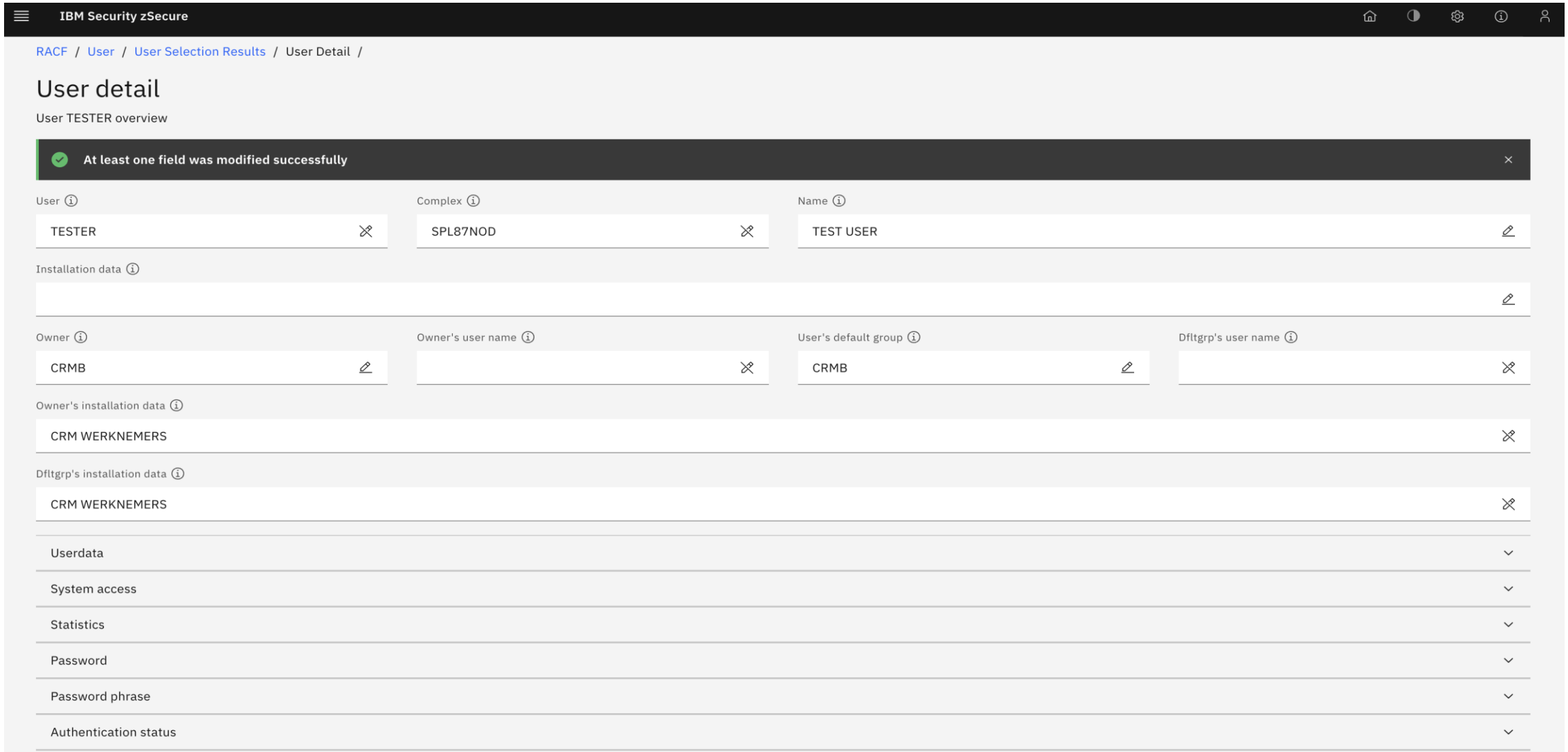


History Tab

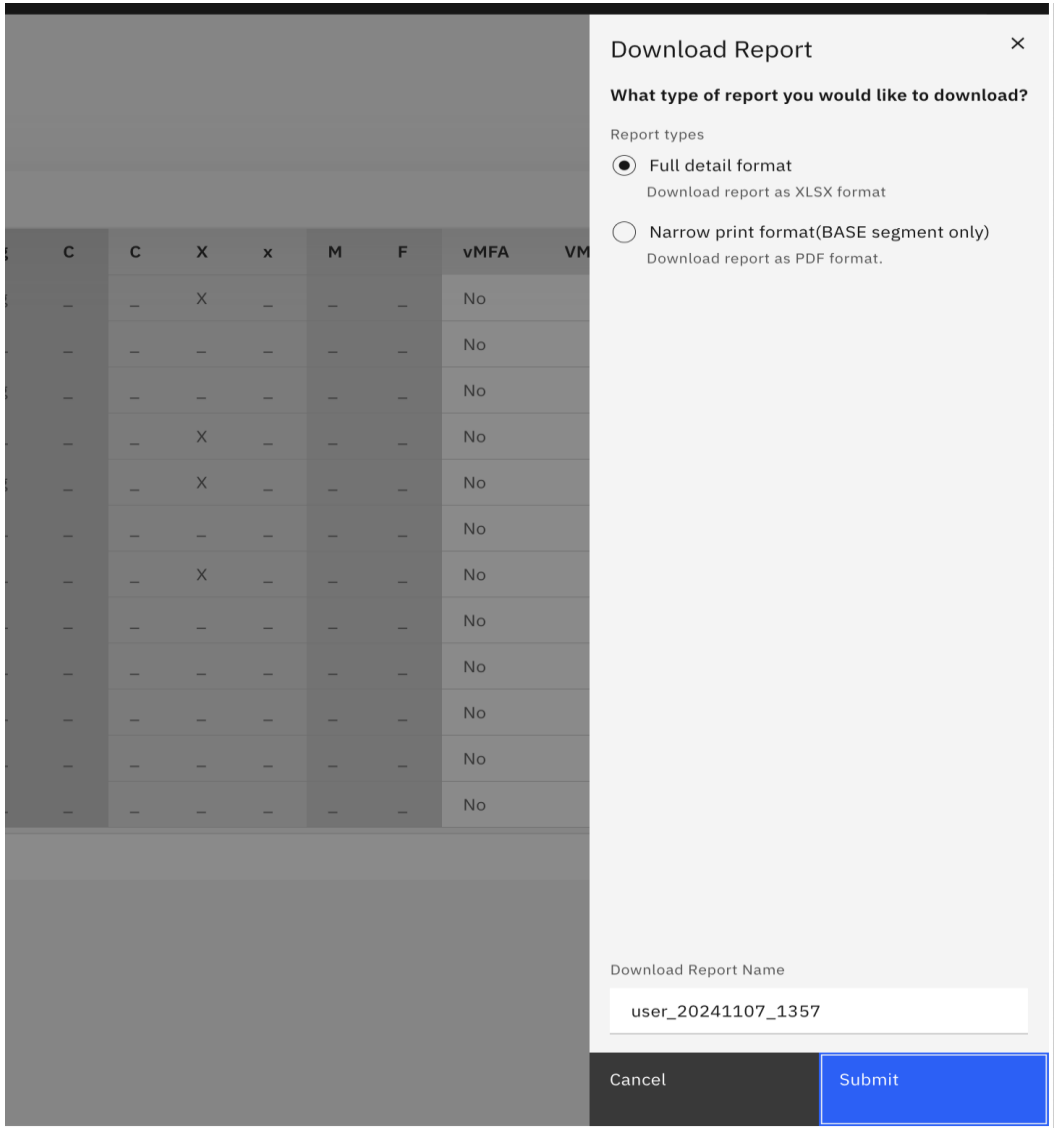


Click on View Detail for more information

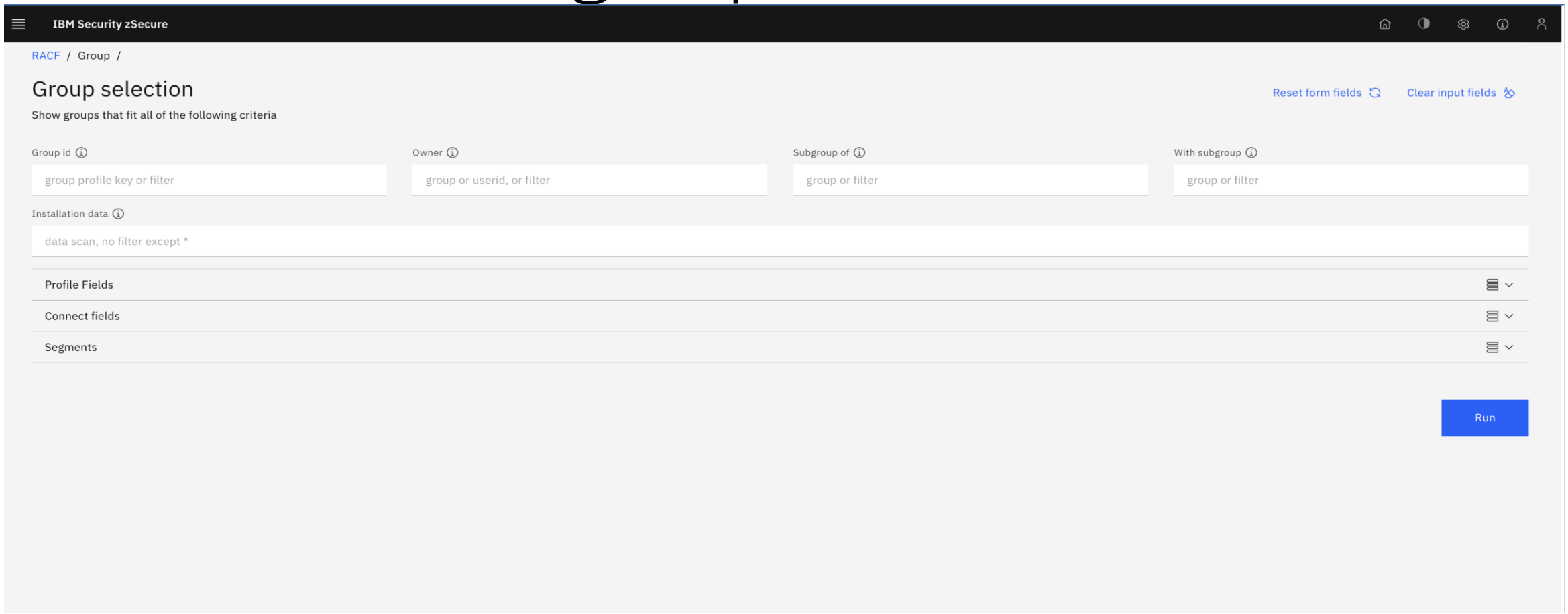
Field Modification on detail page



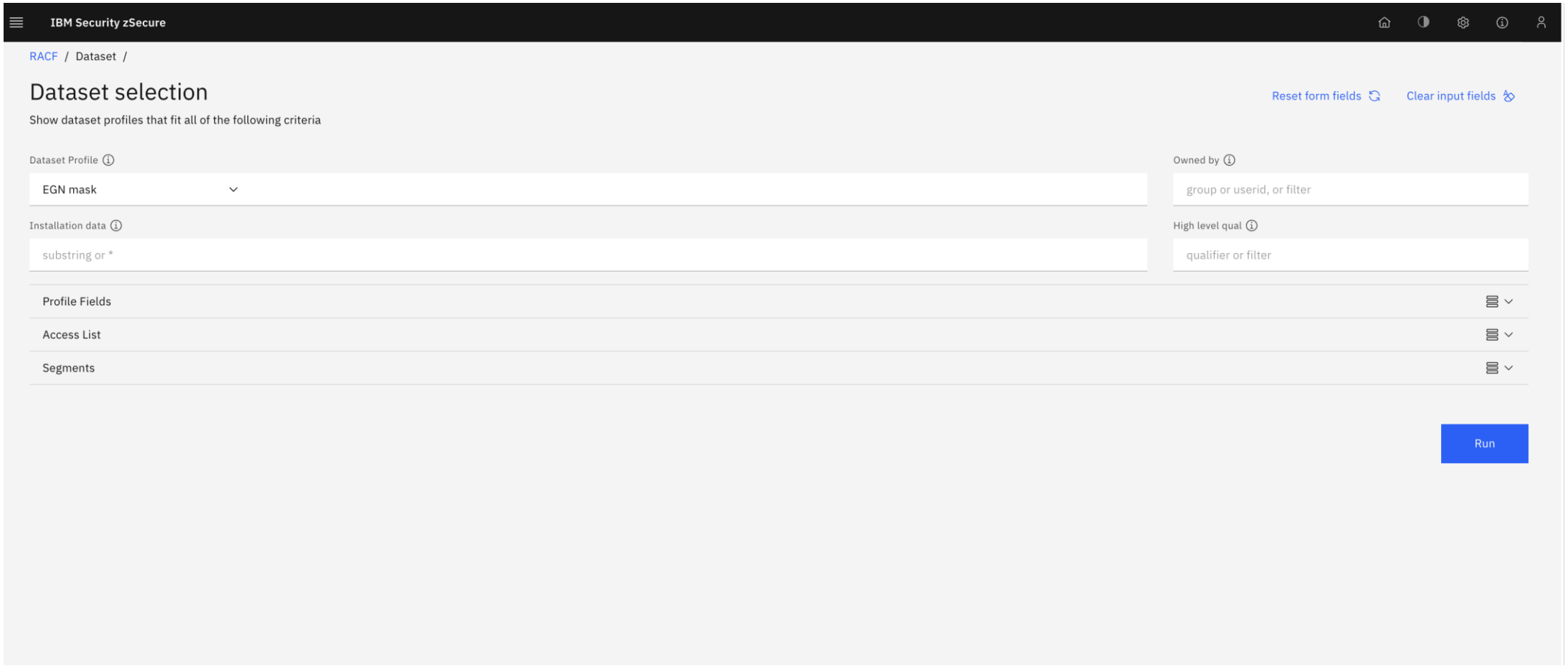
zSecure plugin for z/OSMF – Download report



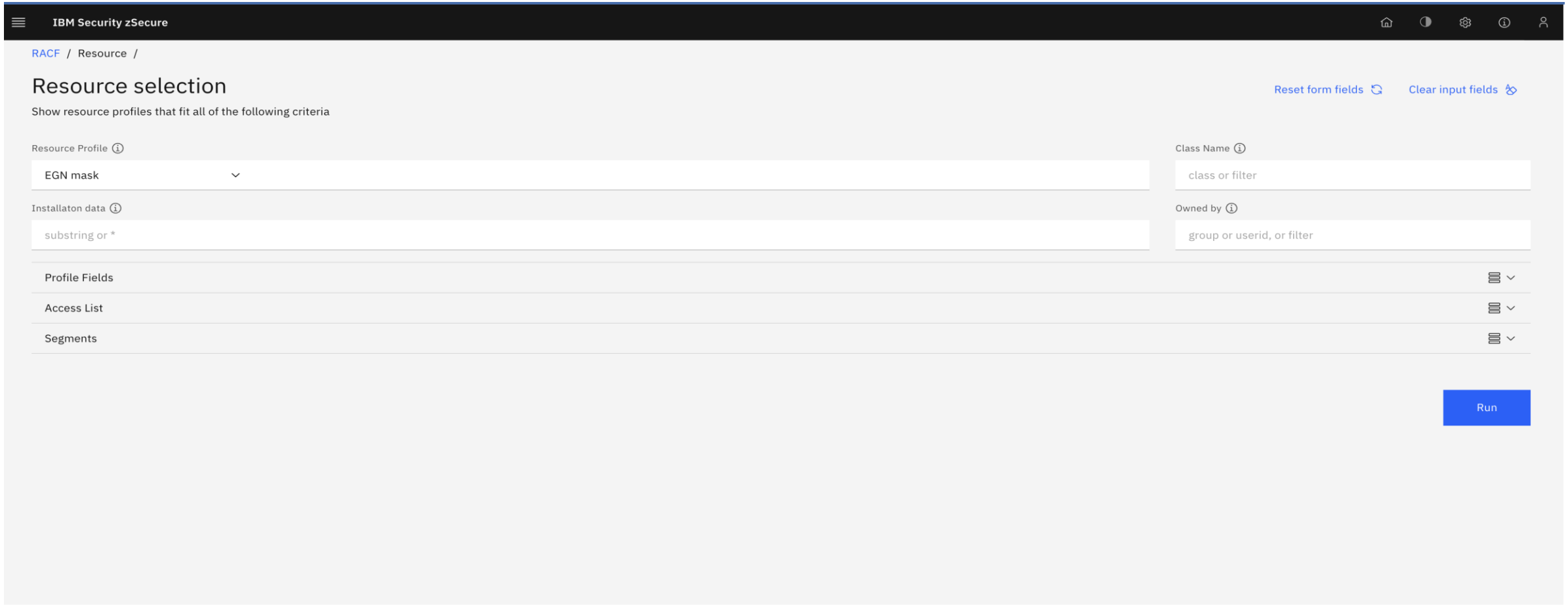
RACF.GROUP – group selection



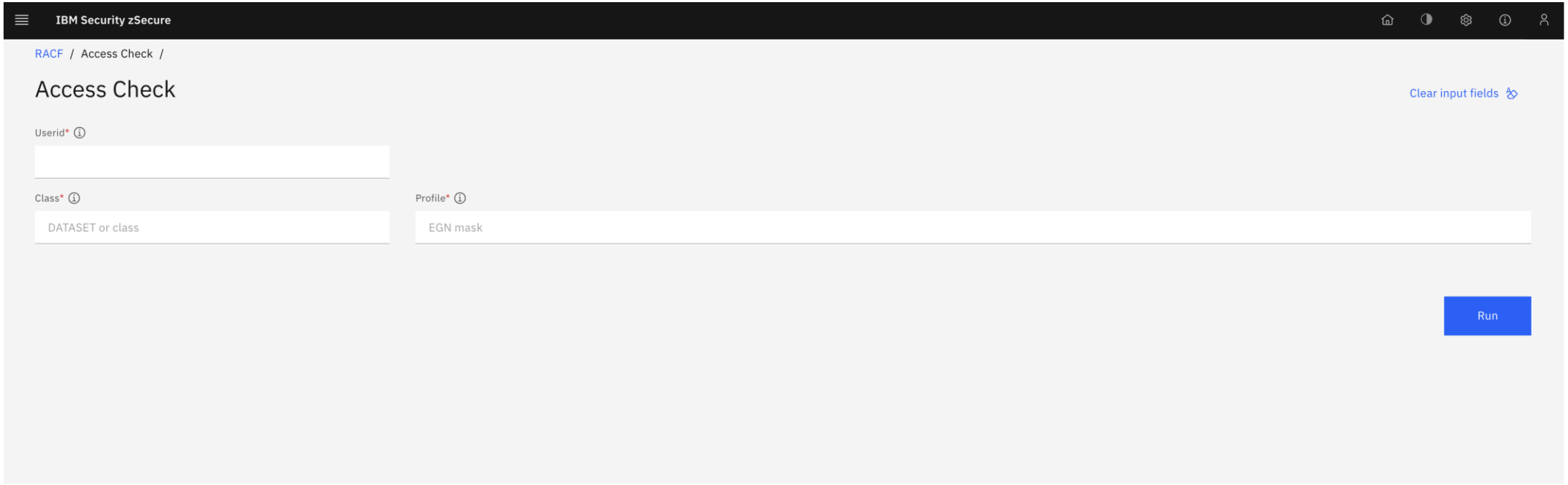
RACF.DATASET – dataset selection



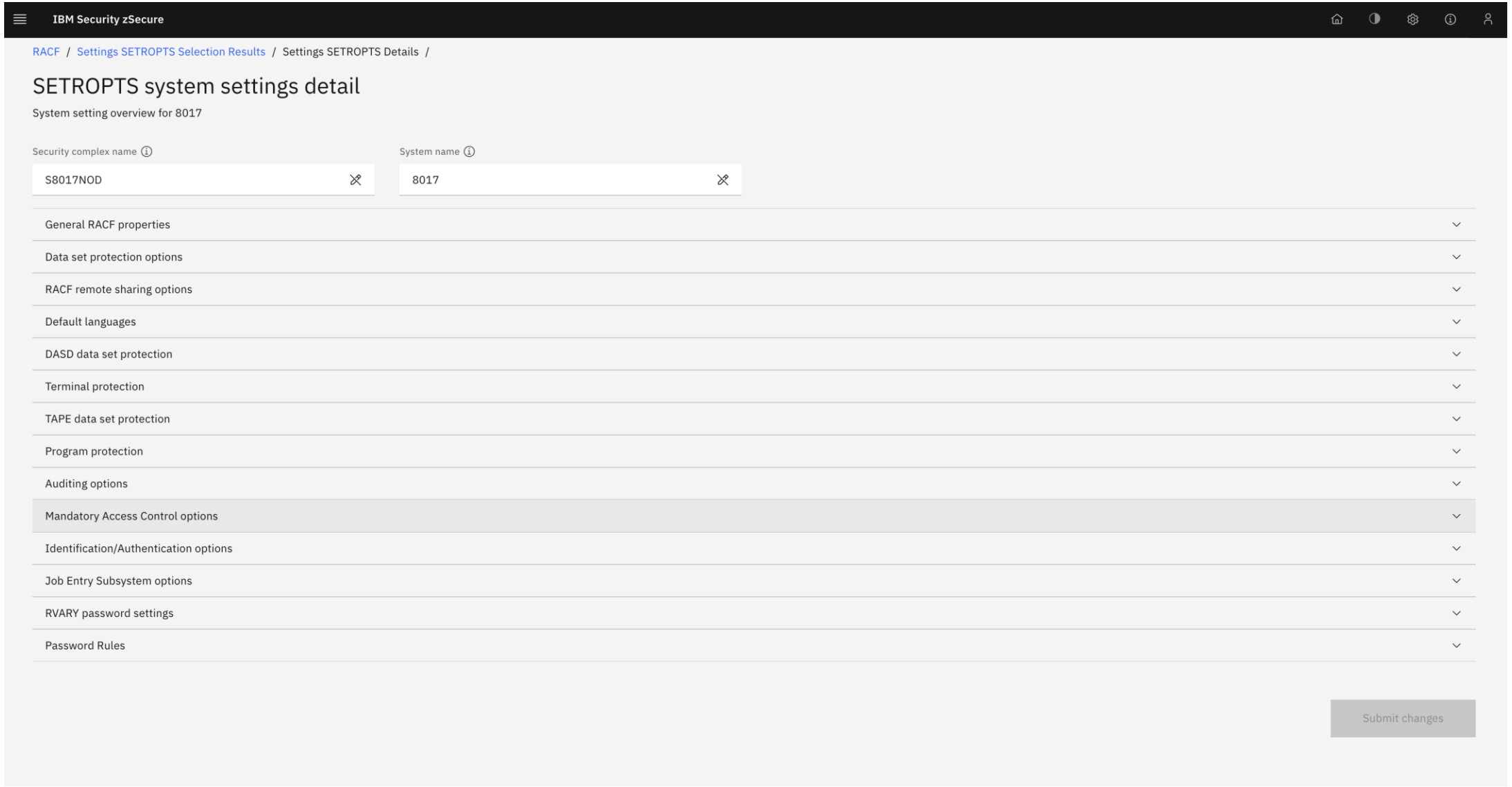
RACF.RESOURCE – resource selection



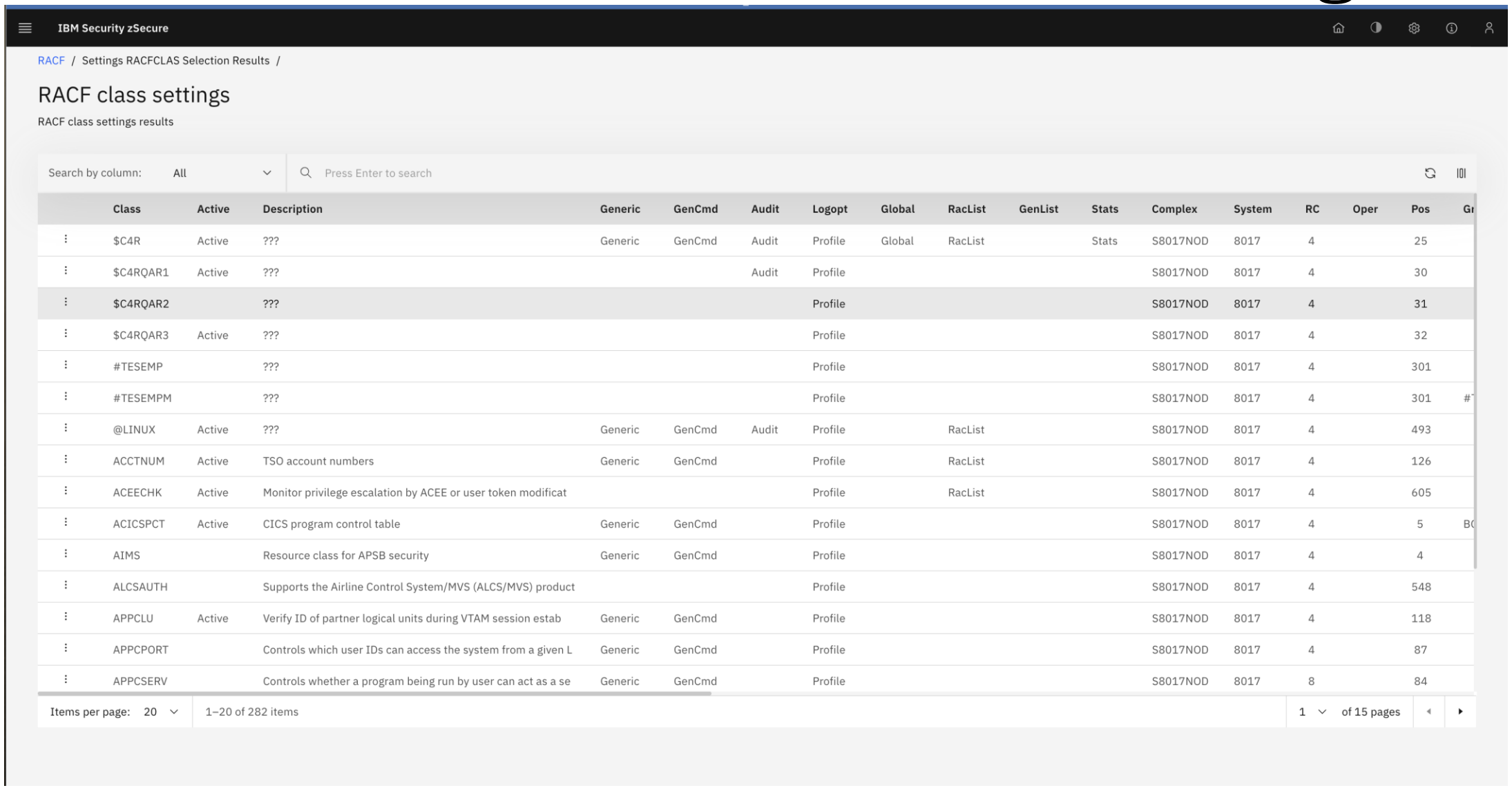
RACF.Access Check



RACF.SETTINGS – SETROPTS

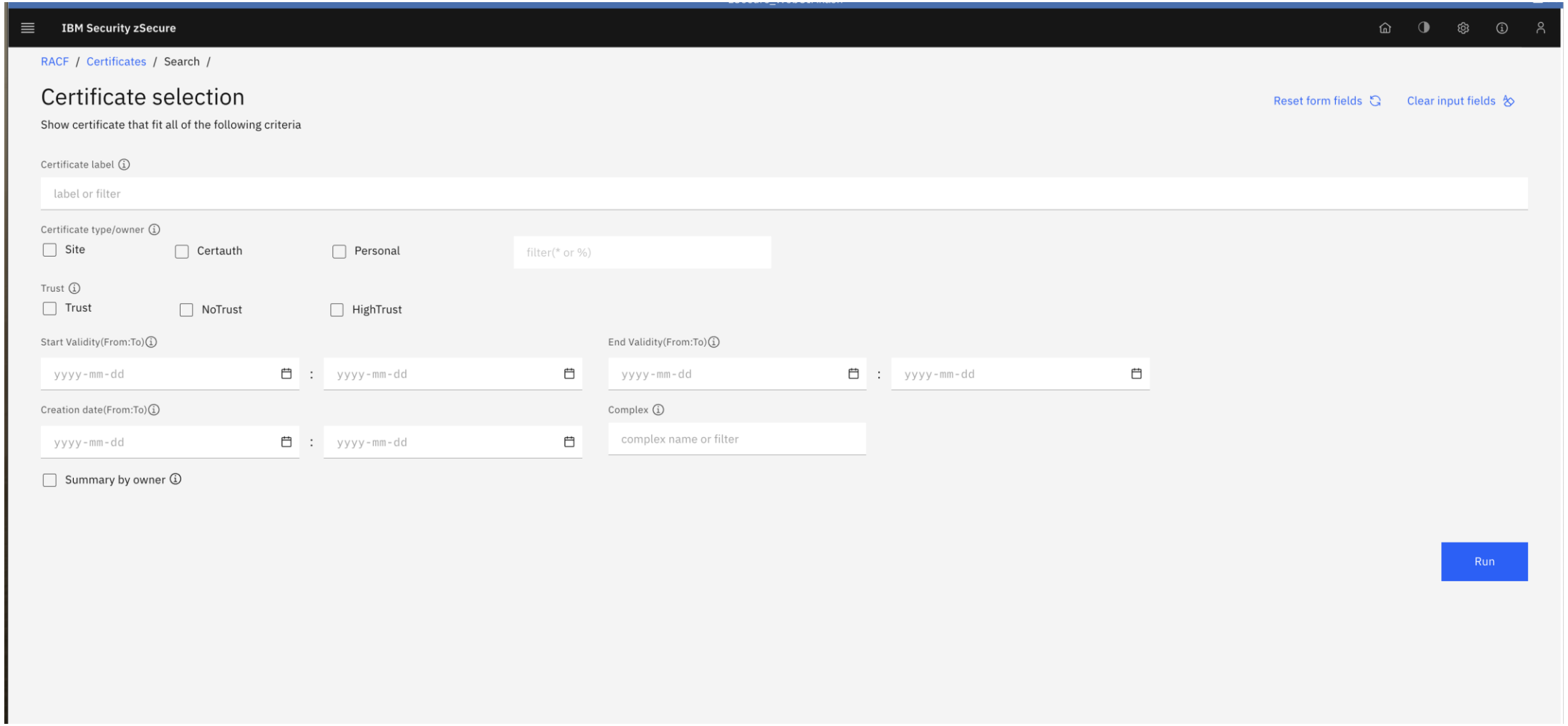


RACF.SETTINGS – RACF class settings

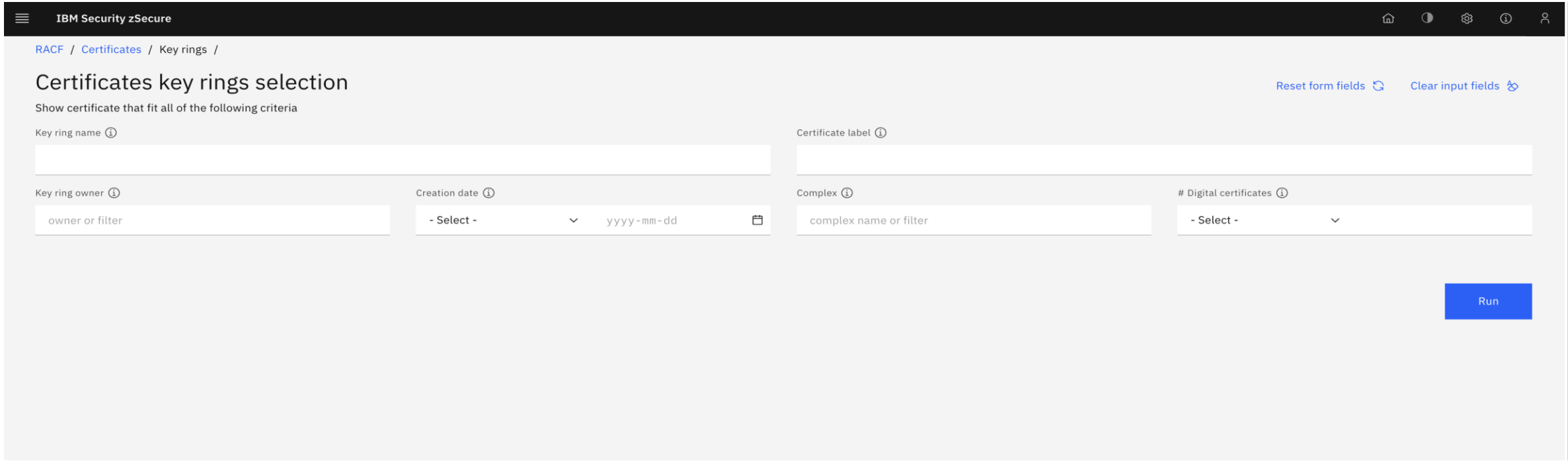


Class	Active	Description	Generic	GenCmd	Audit	Logopt	Global	RacList	GenList	Stats	Complex	System	RC	Oper	Pos	Gr
$C4R	Active	???	Generic	GenCmd	Audit	Profile	Global	RacList		Stats	S8017NOD	8017	4		25	
$C4RQAR1	Active	???			Audit	Profile					S8017NOD	8017	4		30	
$C4RQAR2		???				Profile					S8017NOD	8017	4		31	
$C4RQAR3	Active	???				Profile					S8017NOD	8017	4		32	
#TESEMP		???				Profile					S8017NOD	8017	4		301	
#TESEMPM		???				Profile					S8017NOD	8017	4		301	#T
@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	BC
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	
APPCPORT		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	

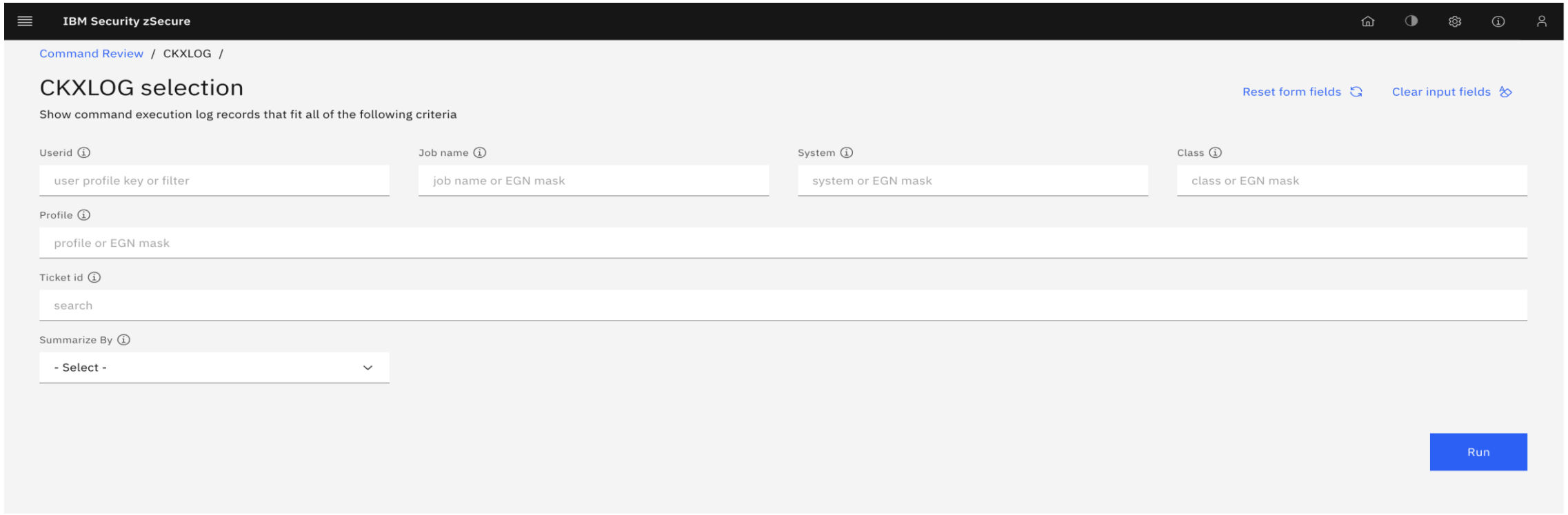
RACF.CERTIFICATES – Certificate selection



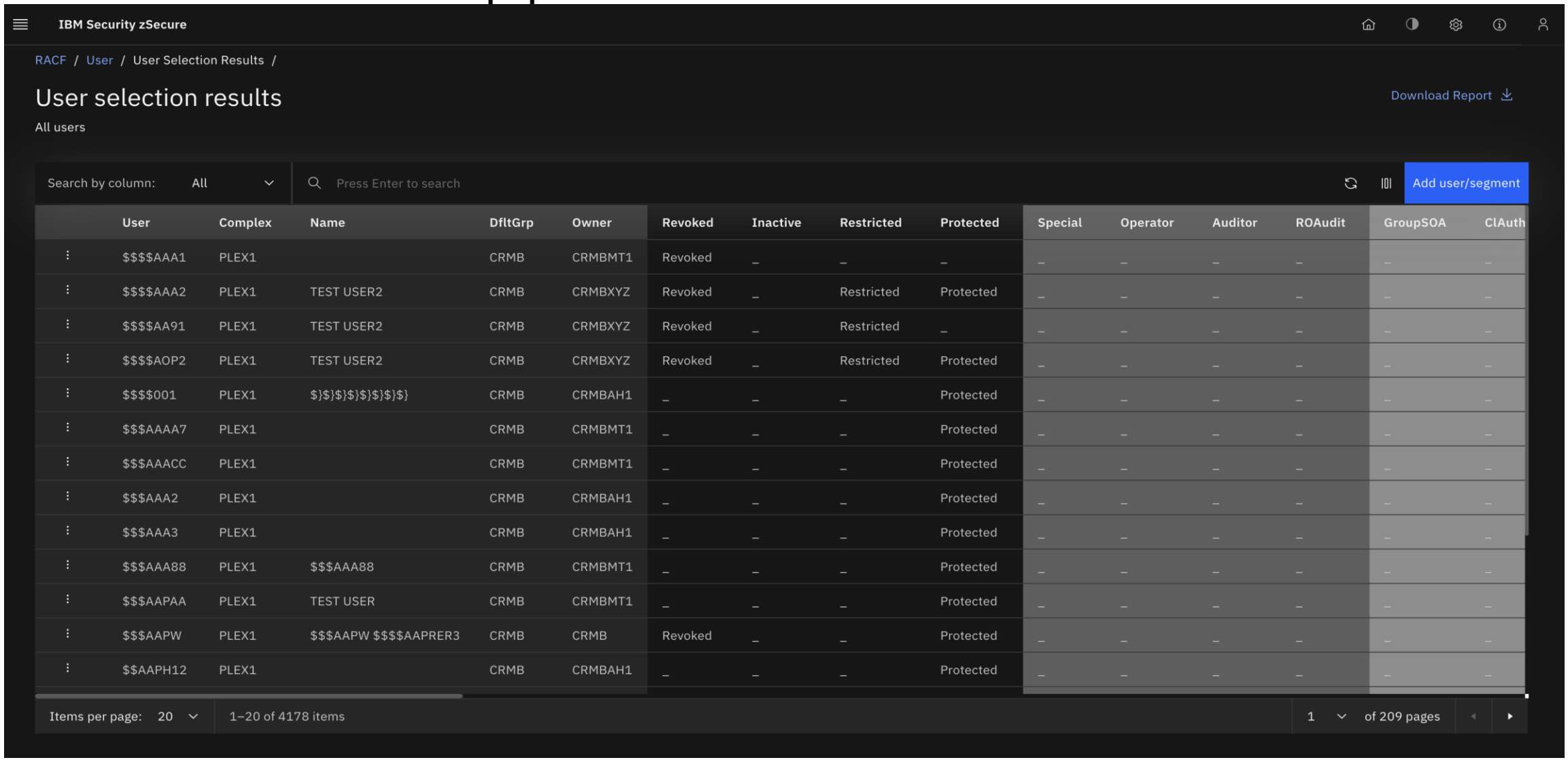
RACF.CERTIFICATES – Key rings



RACF.CKXLOG – Command Review CKXLOG

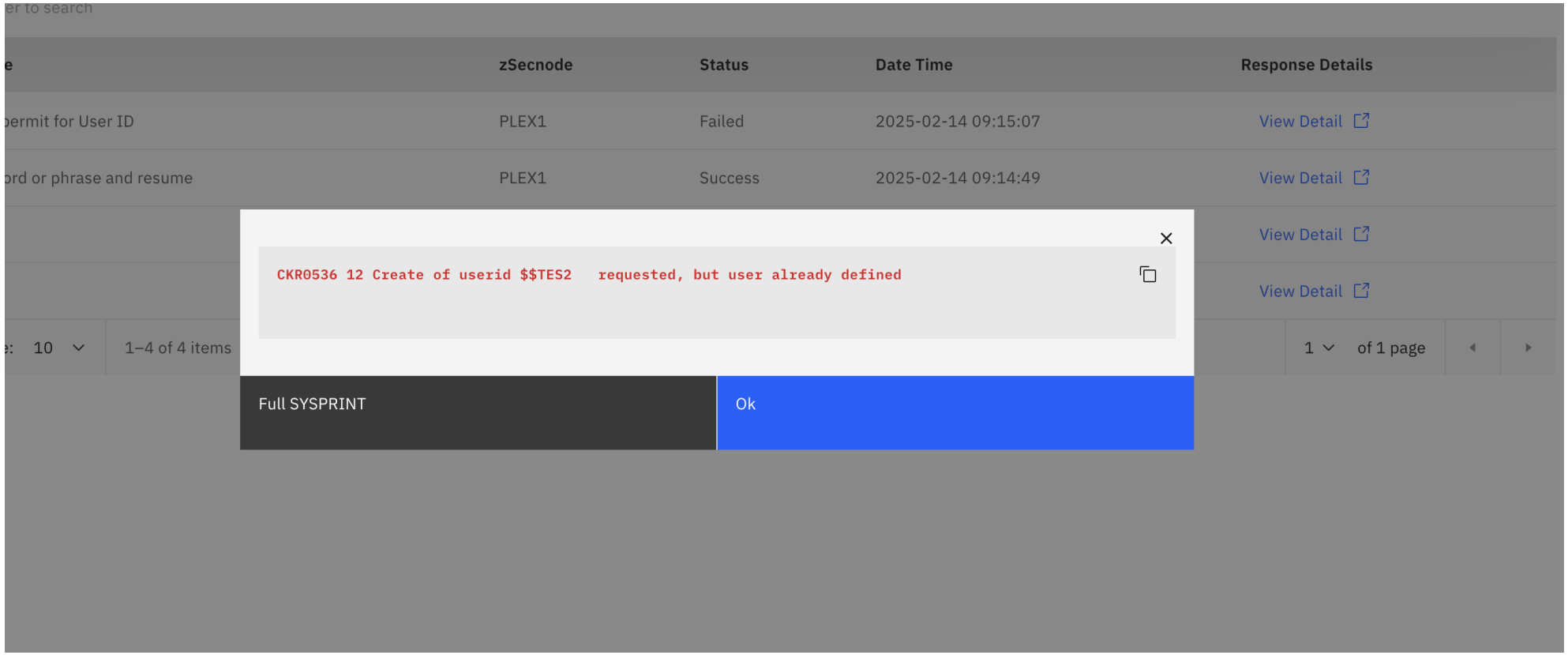


Dark theme support



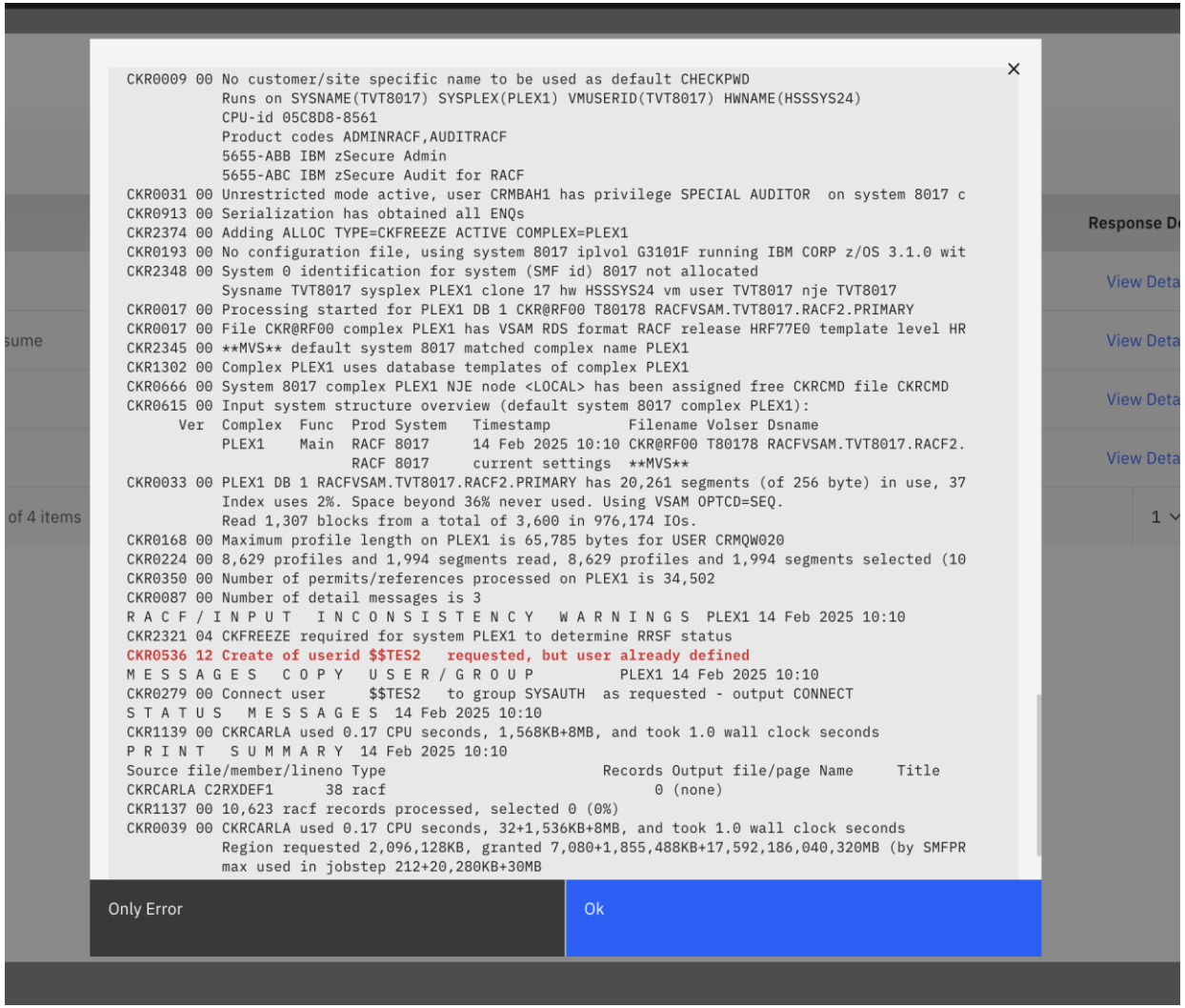
SHOWLOG

Web UI – failed COPY



Click on View Detail for more information

Web UI - Copy output (Full SYSPRINT)



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 ******************************
```

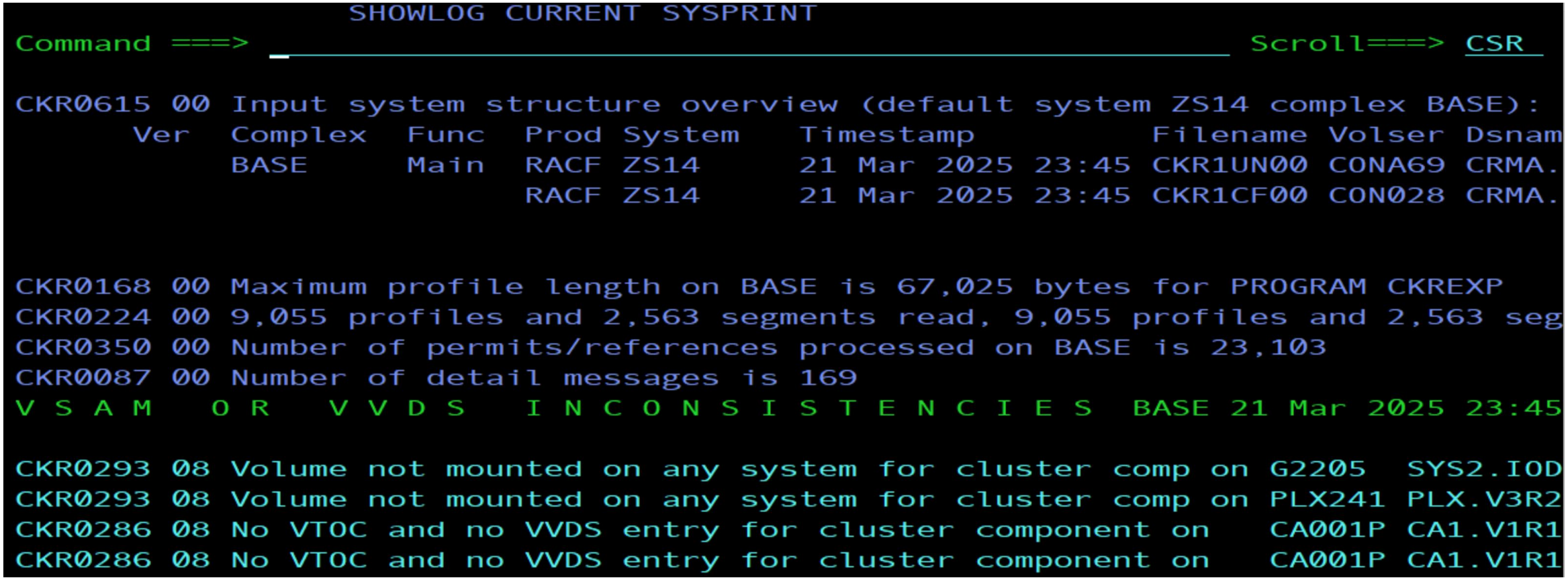
RESET and FIND 12 10 lets you navigate to

```
                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



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	*fieldname*	*owner.userid*
GROUP	*fieldname*	*owner.group*
DATASET	*fieldname*	*hlq.rest-of-profile*
General Resource	*fieldname*	*profile*

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 Security Standards Council

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

CIS Center for Internet Security®

CIS Benchmarks™

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]

CIS Center for Internet Security®

CIS Benchmarks™

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)

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 Products STIG:

- Release and version differs per product

z/OS STIG v9.03

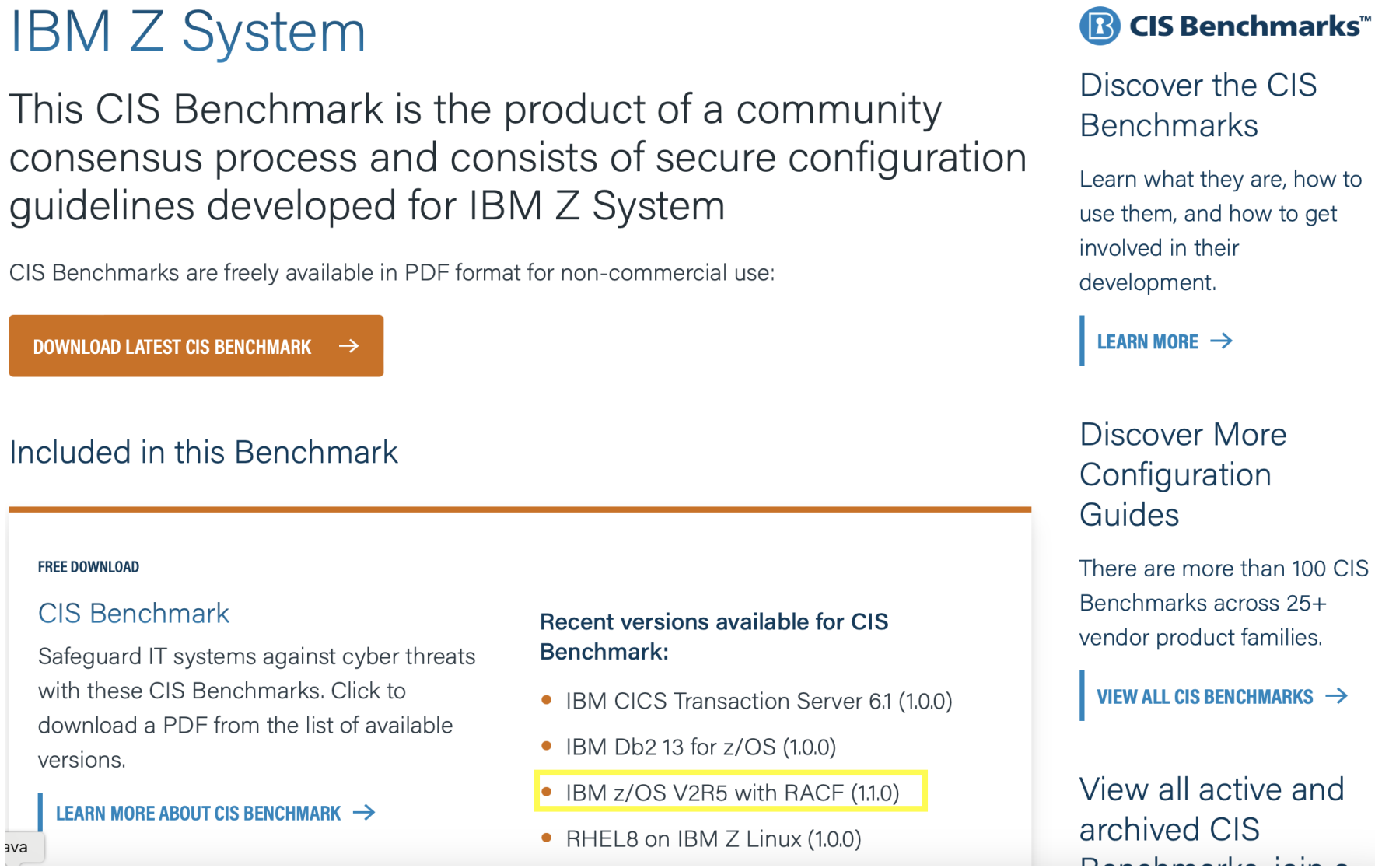
	ACF2 z/OS	RACF z/OS	TSS z/OS
Total	221	217	226
Ready	204	205	73
Missing	17	12	164
%	92%	94%	32%

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 →

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)

CIS Benchmarks™

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

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

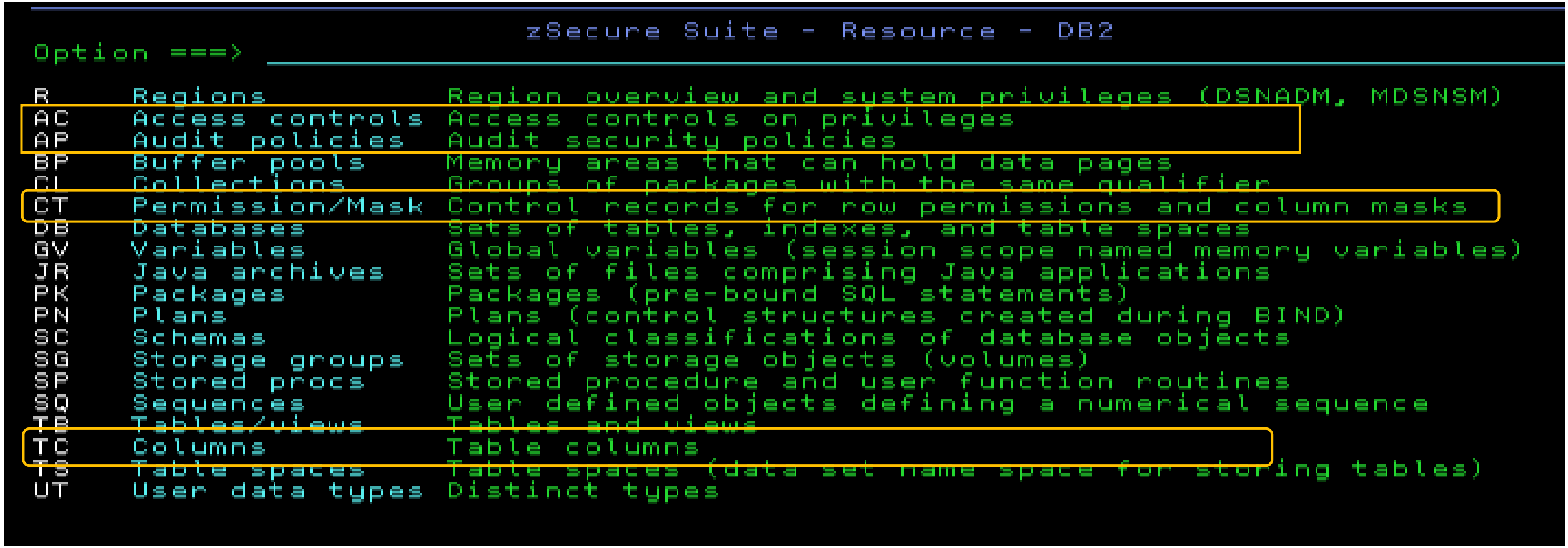
In order to build the controls, several new Db2 report types have been added.

In RE.D (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

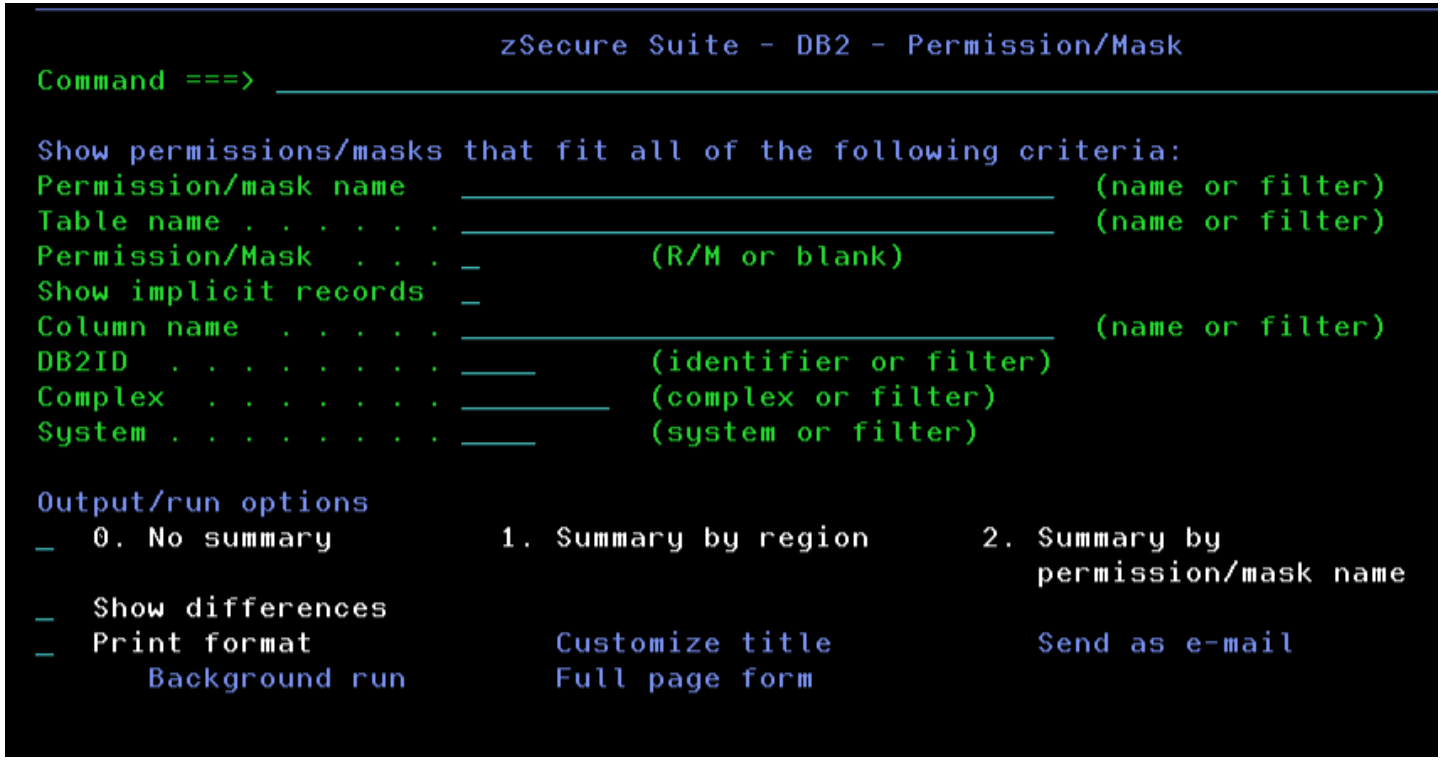
Note that TC and AP are only available with a zSCC entitlement

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

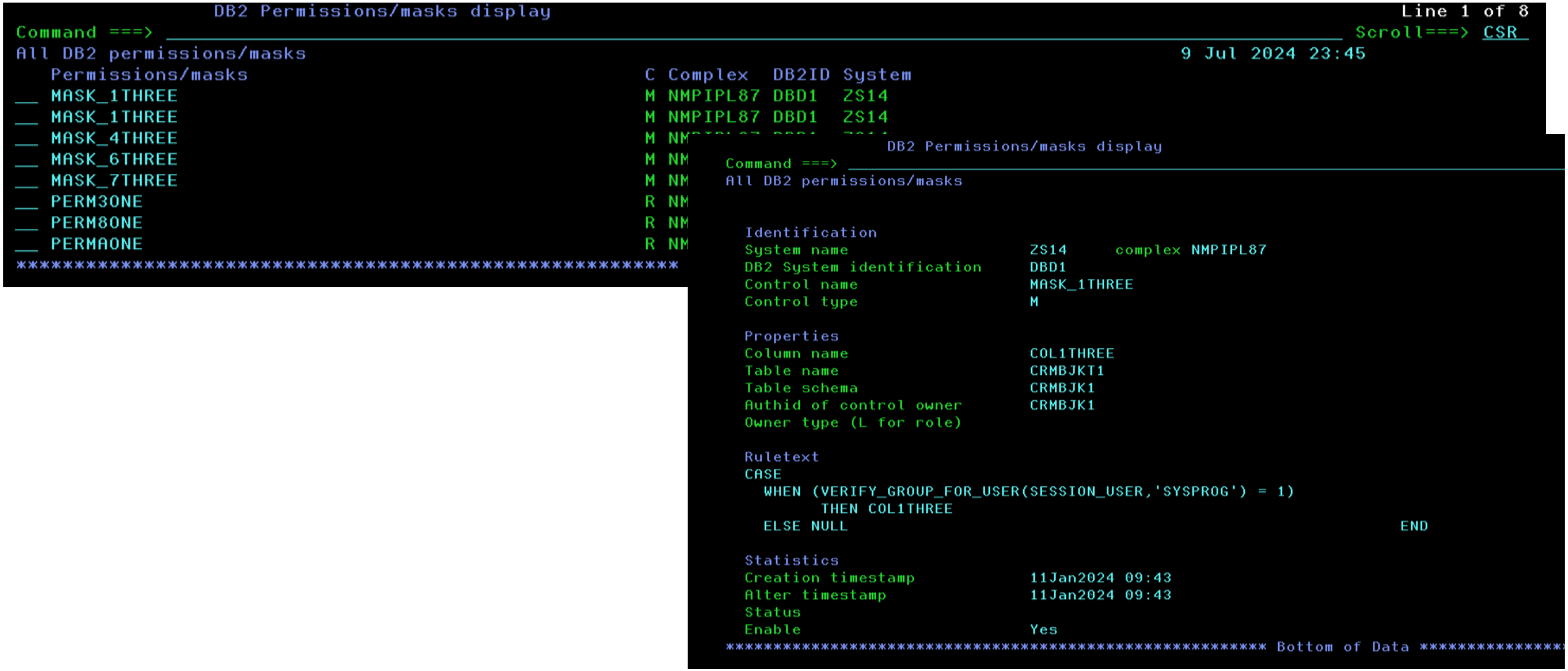


Report type DB2_CONTROL (1)

- 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

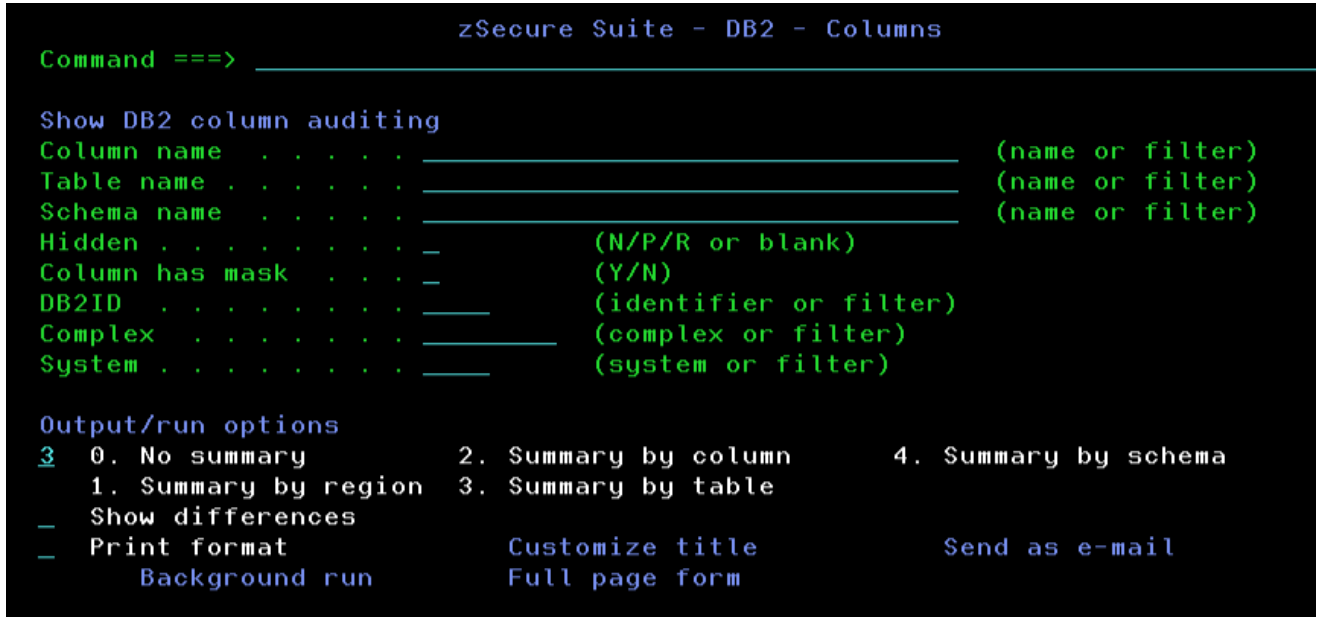


Report type DB2_CONTROL (2)



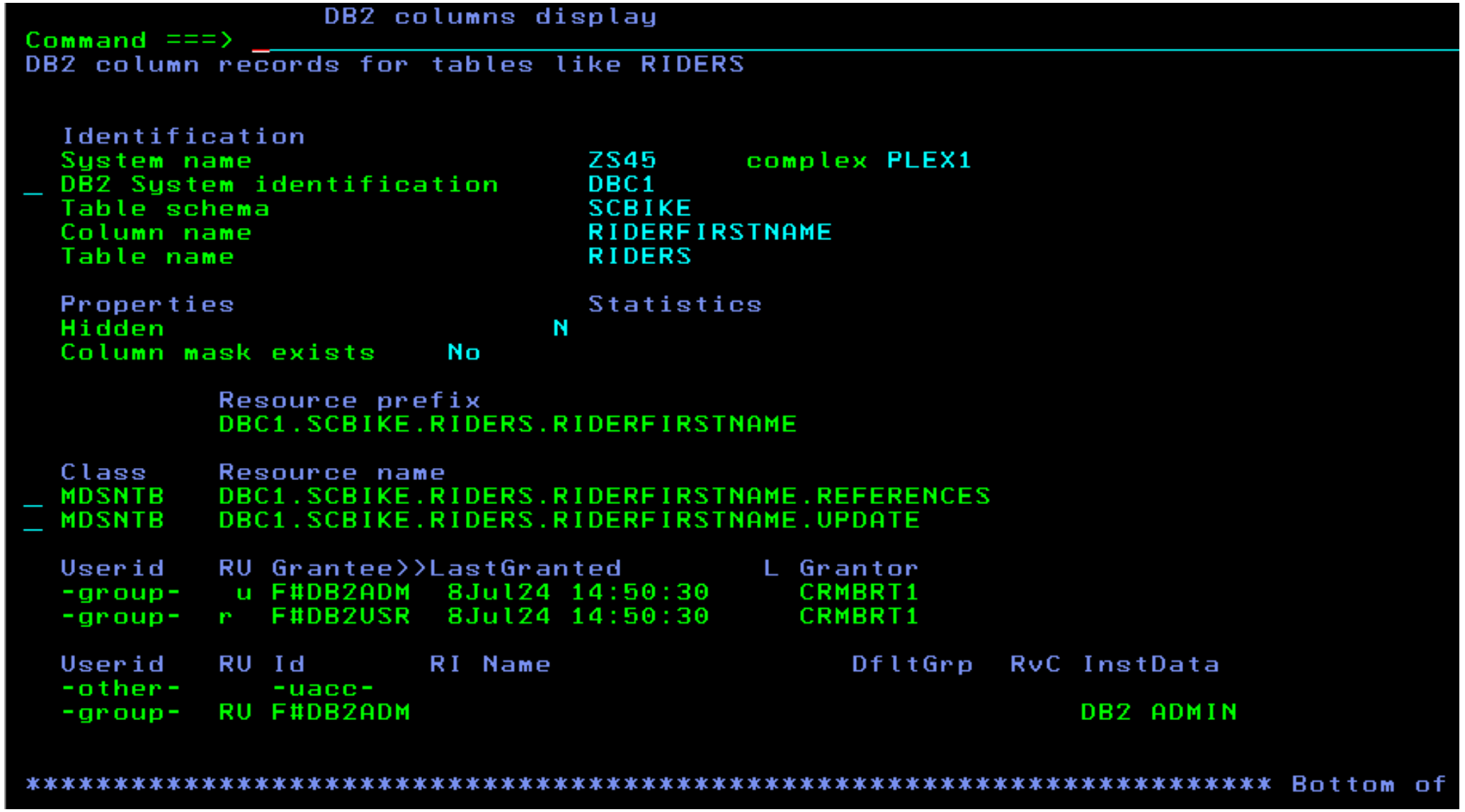
Report type DB2_COLUMN

- 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

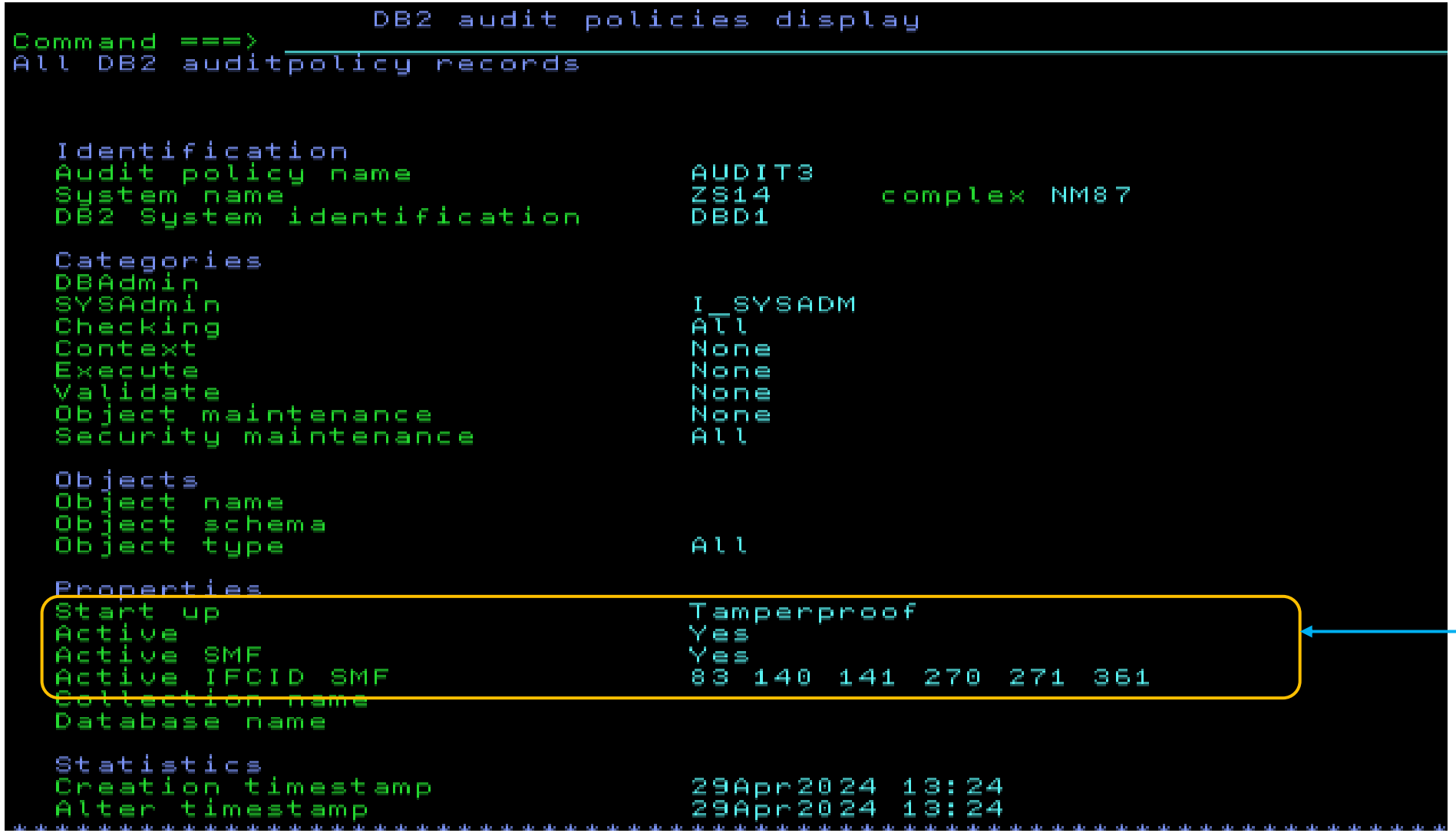


Report type DB2_AUDITPOLICY

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

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

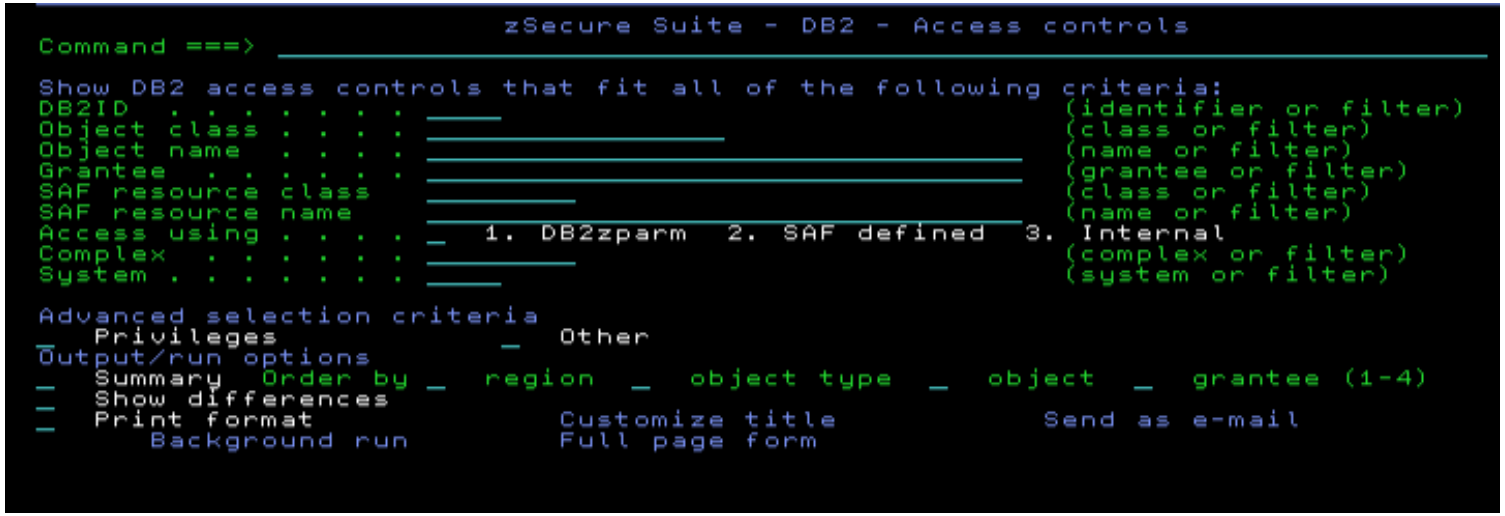
RE.D.AP Db2 Audit Policy Detail



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

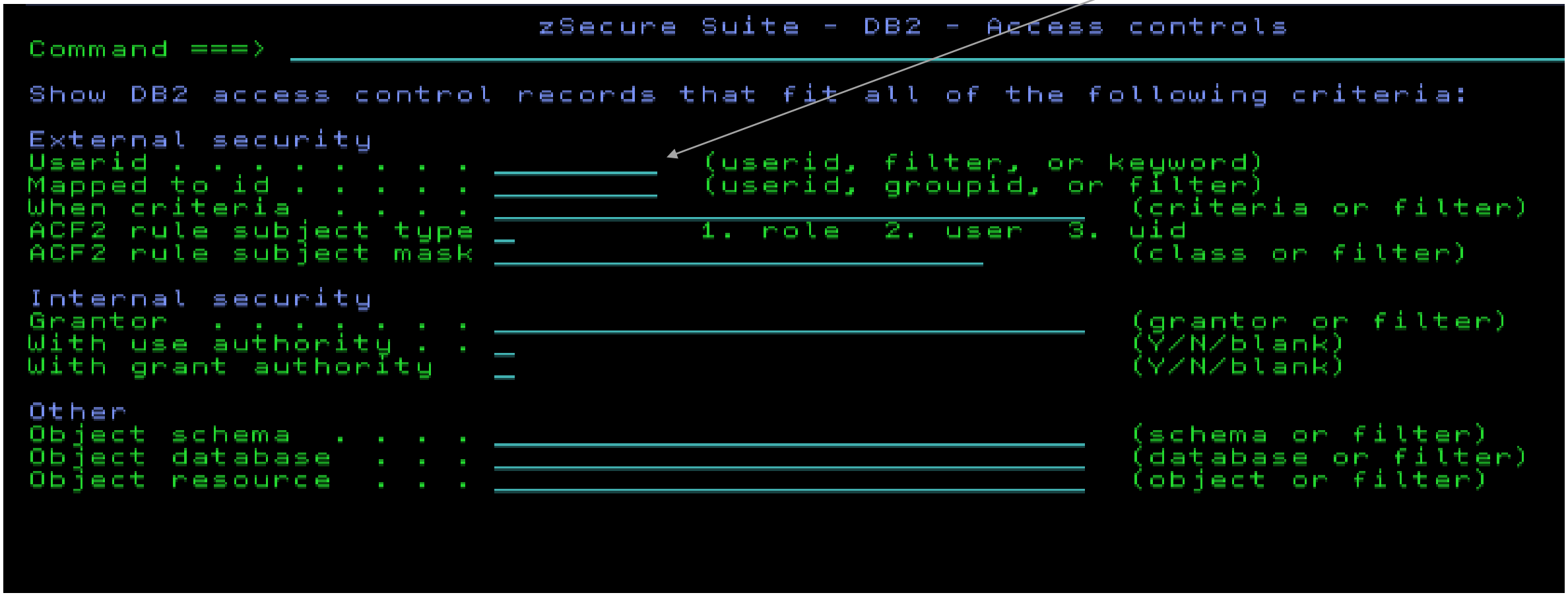
- Shows Db2 objects that have an access list either through Db2 internal security or through the standard Db2 external access control module DSNX@XAC.
- CARLa sample CKADQDP
- Entitled for zSecure Audit and zSCC
- Has been in the CARLa engine since zSecure 2.3.1
- Exploitation CIS benchmark for DB2 in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



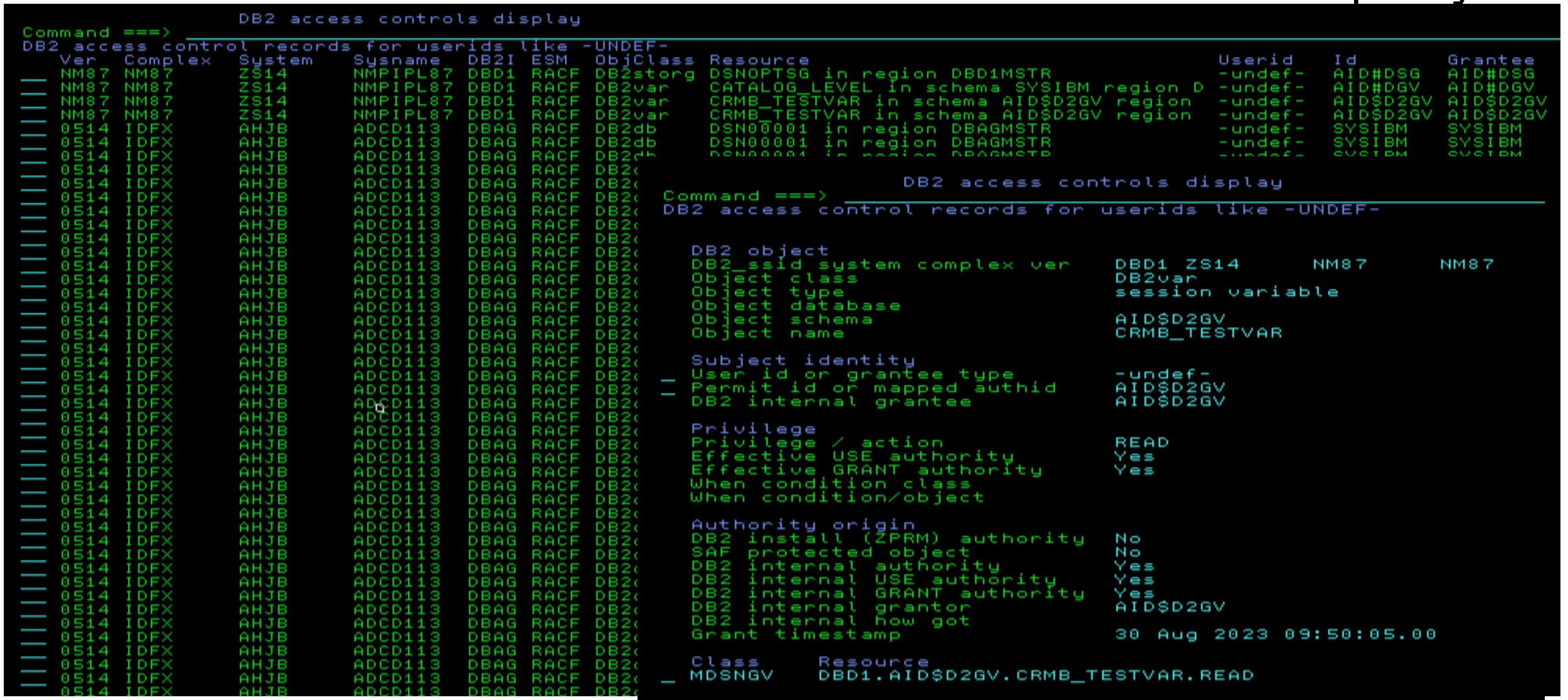
RE.D.AC Db2 Access Control - Privileges

RE.D.AC Db2 Access Control - Other

For example, request -undef-



RE.D.AC Db2 Access Control – results display



Report types ACF2_DB2_RULE / _RULELINE

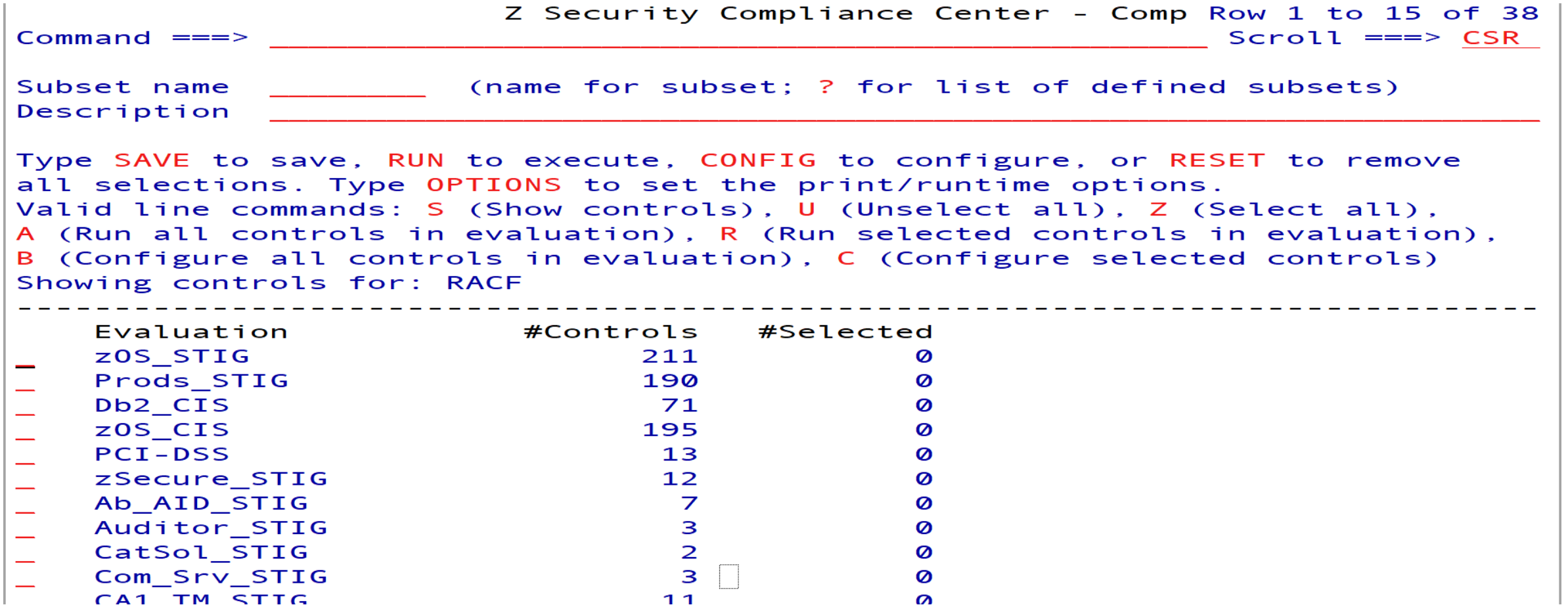
- Shows rules from ACF2/DB2 product
- Support ACF2/DB2 add-on product to ACF2
- Entitled for zSCC
- Shipped in engine in October 2024

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)



CIS IBM Db2 for z/OS Benchmark (1.0.0)

or OPTIONS to set the print/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

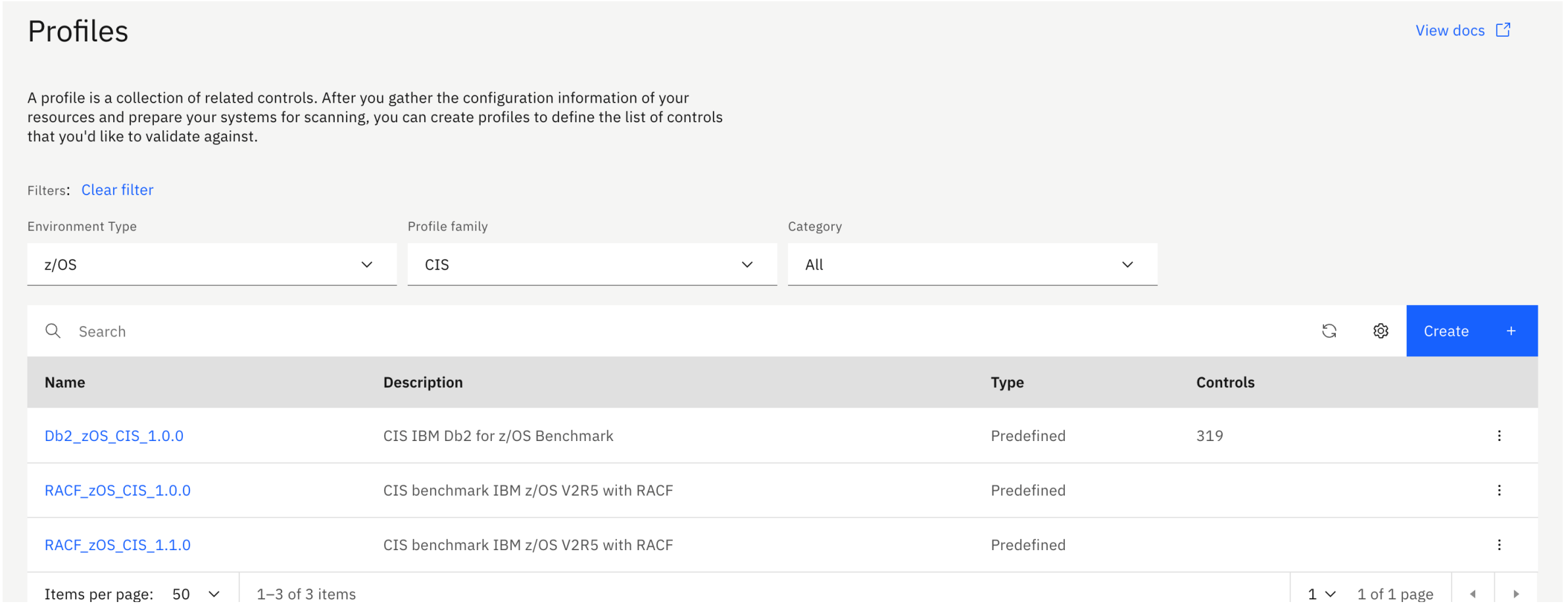
STIG for z/OS ACF2

8.12,8.13,8.14,8.15,9.01,9.02,9.03

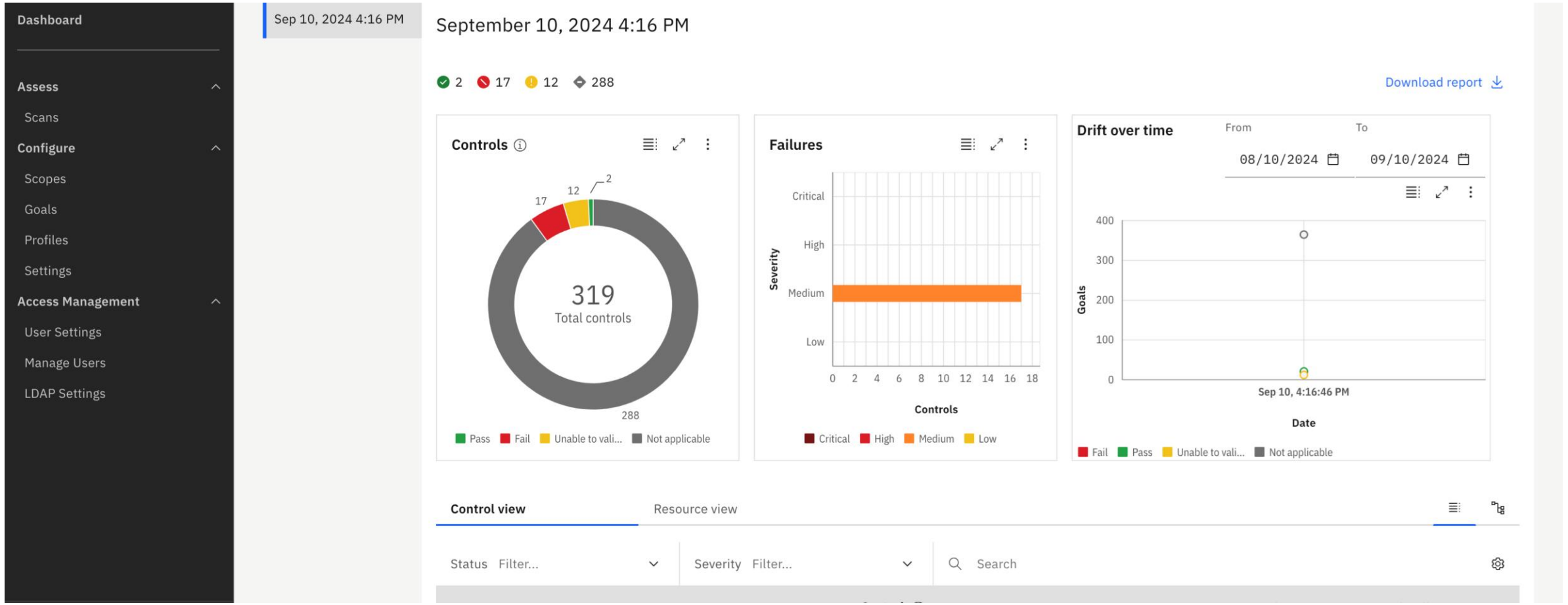
z/OS with RACF CIS Benchmark 1.0.0, 1.1.0

z/OS Db2 CIS Benchmark version 1.0.0
(*Only with zSCC license*)

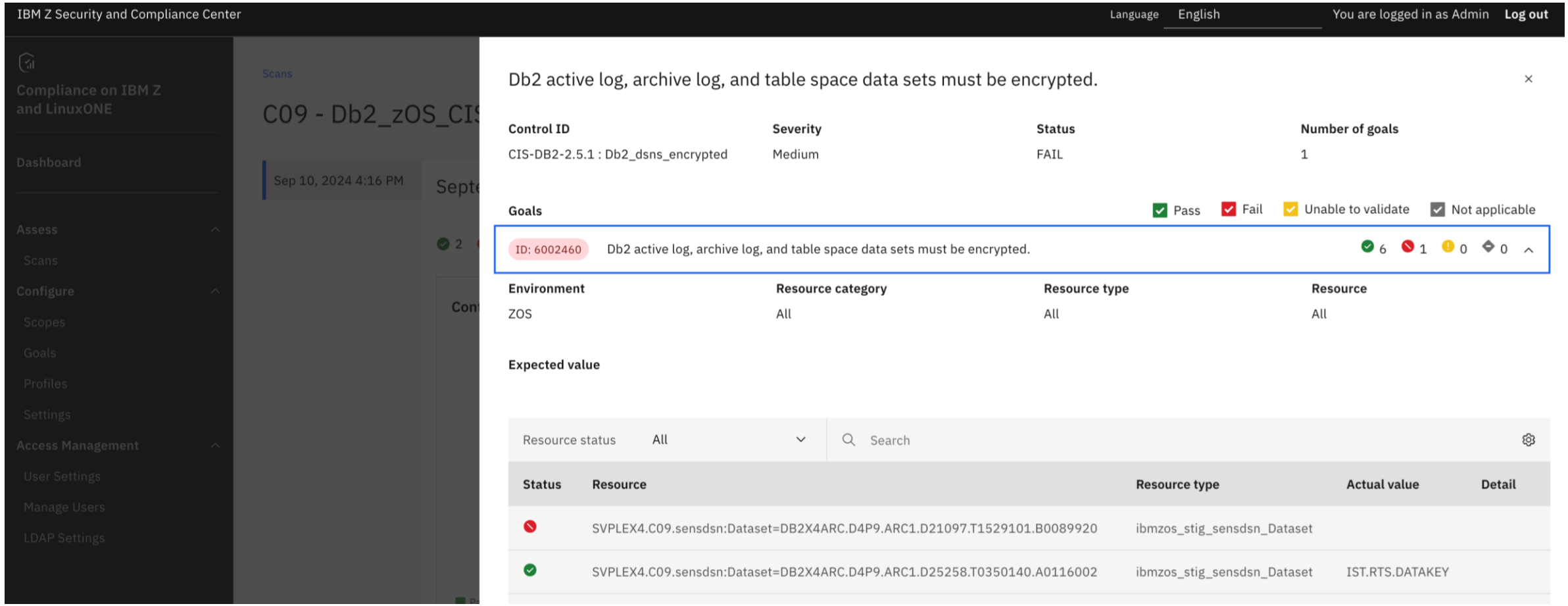
CIS IBM Db2 for z/OS – dashboard: Profiles



CIS IBM Db2 for z/OS - dashboard: Scans



CIS IBM Db2 for z/OS – dashboard: Results



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.

Enter F

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

```
_ Unit of Work Id:    USIBMWZ.TEC2TOR1.C30C1EF64A6C
_ Tracking token:     BAQ.1.TECPLEX.TEC2.2020-11-02T14:22:17.247495
```

to see

```
                Tracking token event                                  5 s elapsed, 0.8 s CPU
Command ===> ____________________________________________________________ Scroll===> CSR
                                                          2Nov20 10:22 to  2Nov20 10:22
   Date/time event     Description
__  2Nov20 10:22:17.24 KENISHI CICS transaction TEC2AOR1 CSMI
__  2Nov20 10:22:17.24 KENISHI CICS transaction TEC2TOR1 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

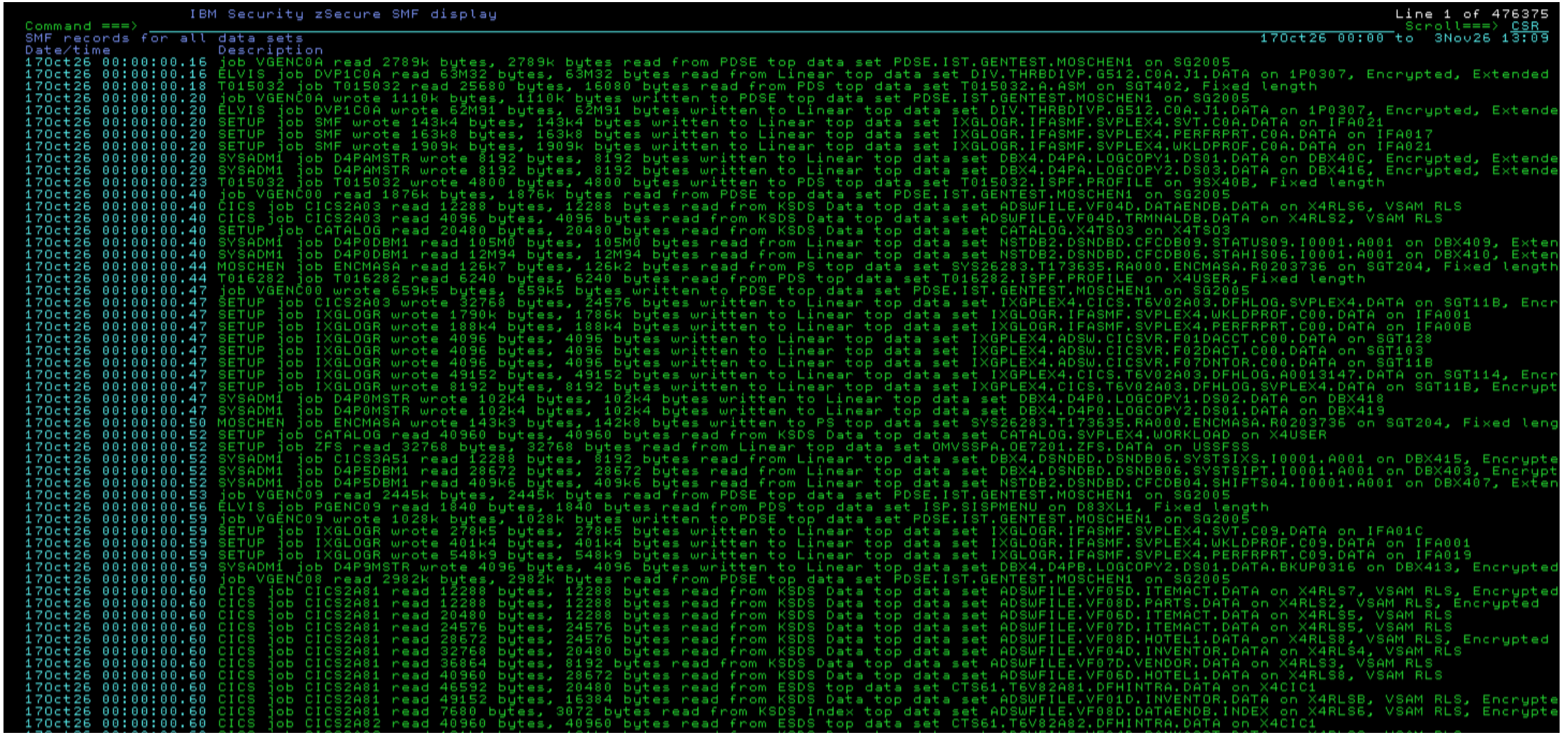
DFSMS determines top job and data set activity in 5 seconds intervals

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



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

- New type=SMF fields
- Existing fields populated
- Entitled in zSecure Audit, zSCC, and zSecure Alert

- BYTES_READ
  BYTES_WRITTEN
- JOBNAME
  USER
  DSN
  VOLSER

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

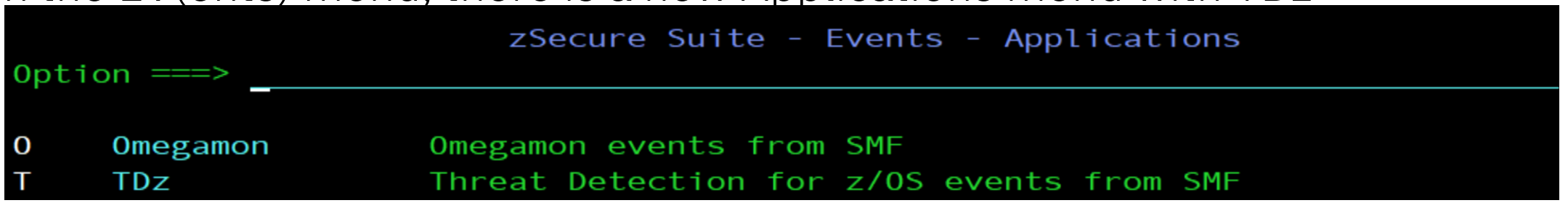
- Entitled in zSecure Audit, zSCC, and zSecure Alert

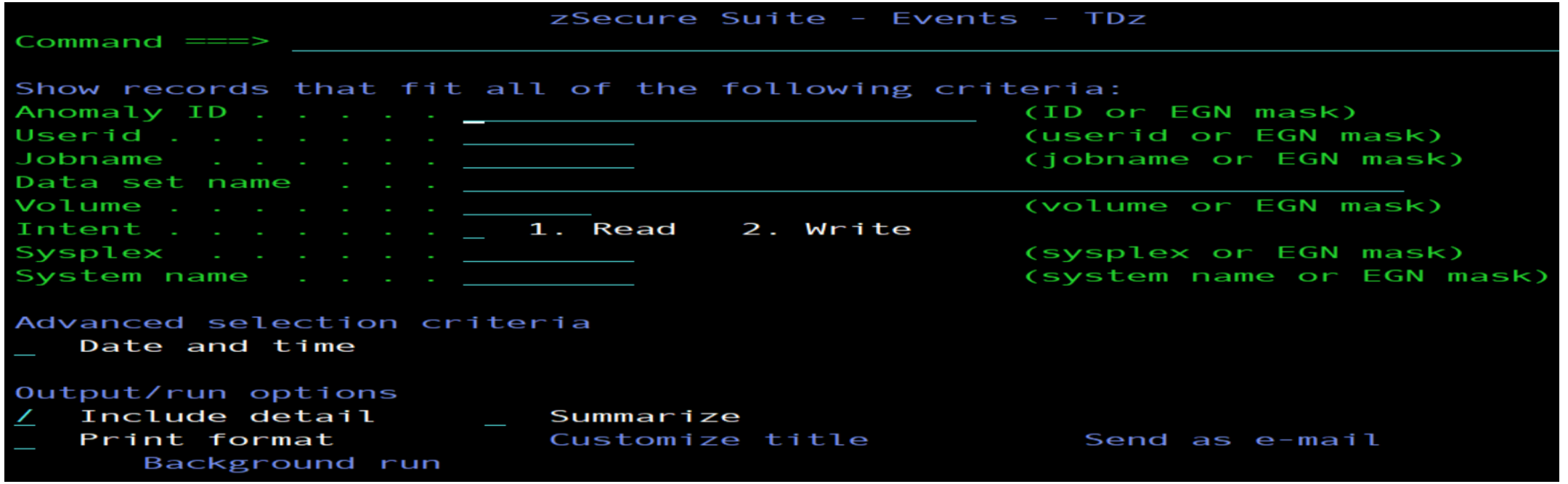
- ANOMALY_ID
  DATASET_ACTIVITY
  AGGR_DATASET_SIZE

- SYSPLEX
  SYSNAME
  JOBNAME
  USER
  DSN
  VOLSER
  BYTES_WRITTEN
  BYTES_READ

EV.A.T – events from Threat Detection

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

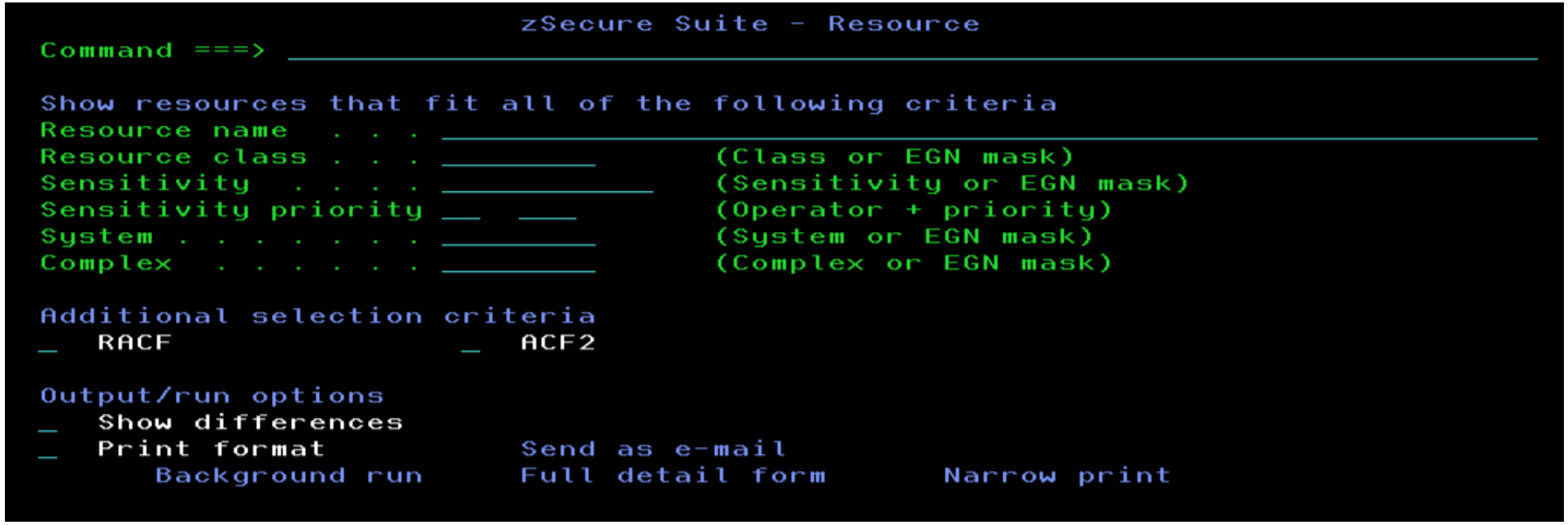


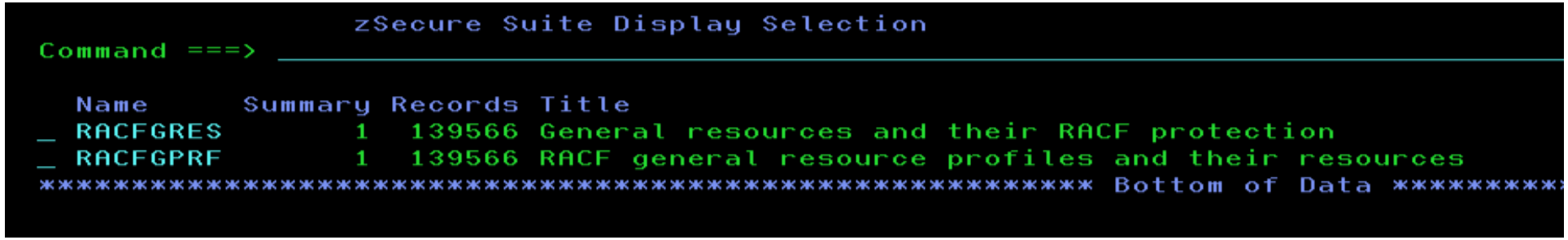


Report type RESOURCE

Report type RESOURCE

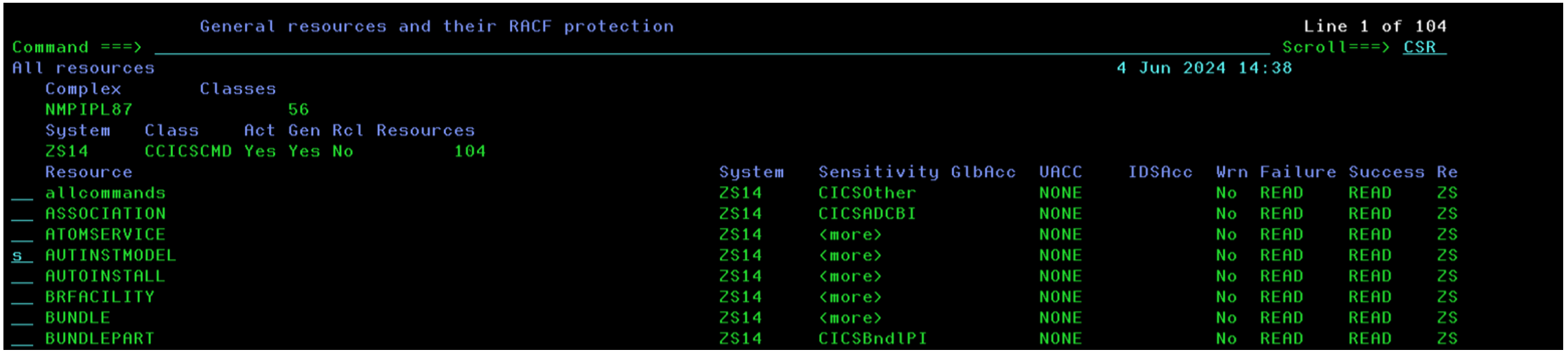
The report type was added in 2012, but now there is a menu option RE.R





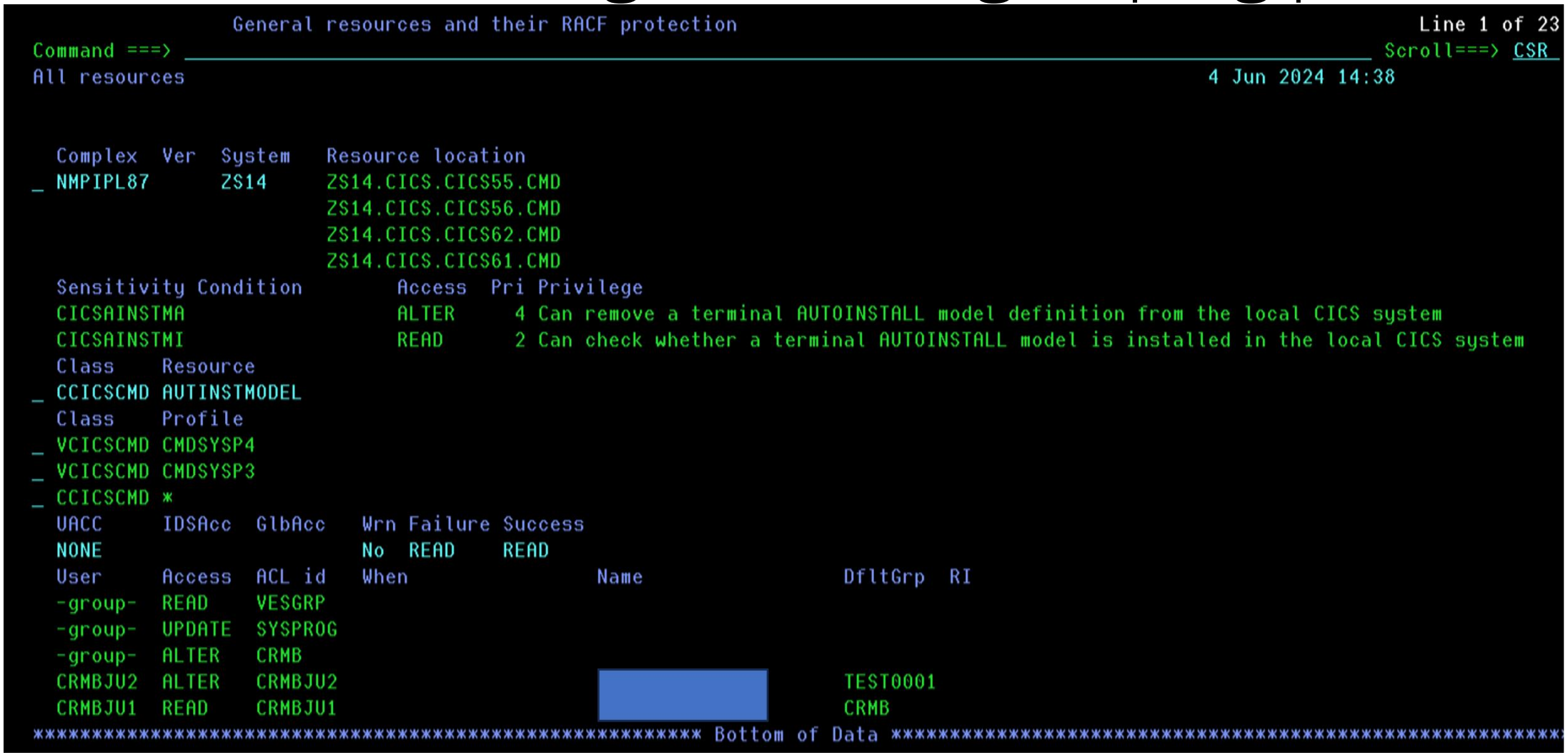
Report type RESOURCE – class, resource

```
                General resources and their RACF protection                    Line 1 of 56
Command ===> ____________________________________________________________ Scroll===> CSR
All resources                                                  4 Jun 2024 14:38
   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
```



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

Detail - contributing member/grouping profiles



New data set sensitivity types

Non-VSAM	VSAM:
• AccMonData • CEF Carla • zSecFreeze • SMFadapters • DB2 ArchLog • DB2 Drivers • zSCC Parm	• DB2 ActLog • DB2 SysCtlg • DB2 TbSpace

New sensitivity types for CSFSERV resources

Senstype	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, arhive 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, arhive 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, arhive 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 cryptohgraphic 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]

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-tiggelman/2019/12/01/ibm-security-zsecure-administration-auditing-and-c

- Hardware Dependencies
  - None, except as possibly implied by z/OS releases in support

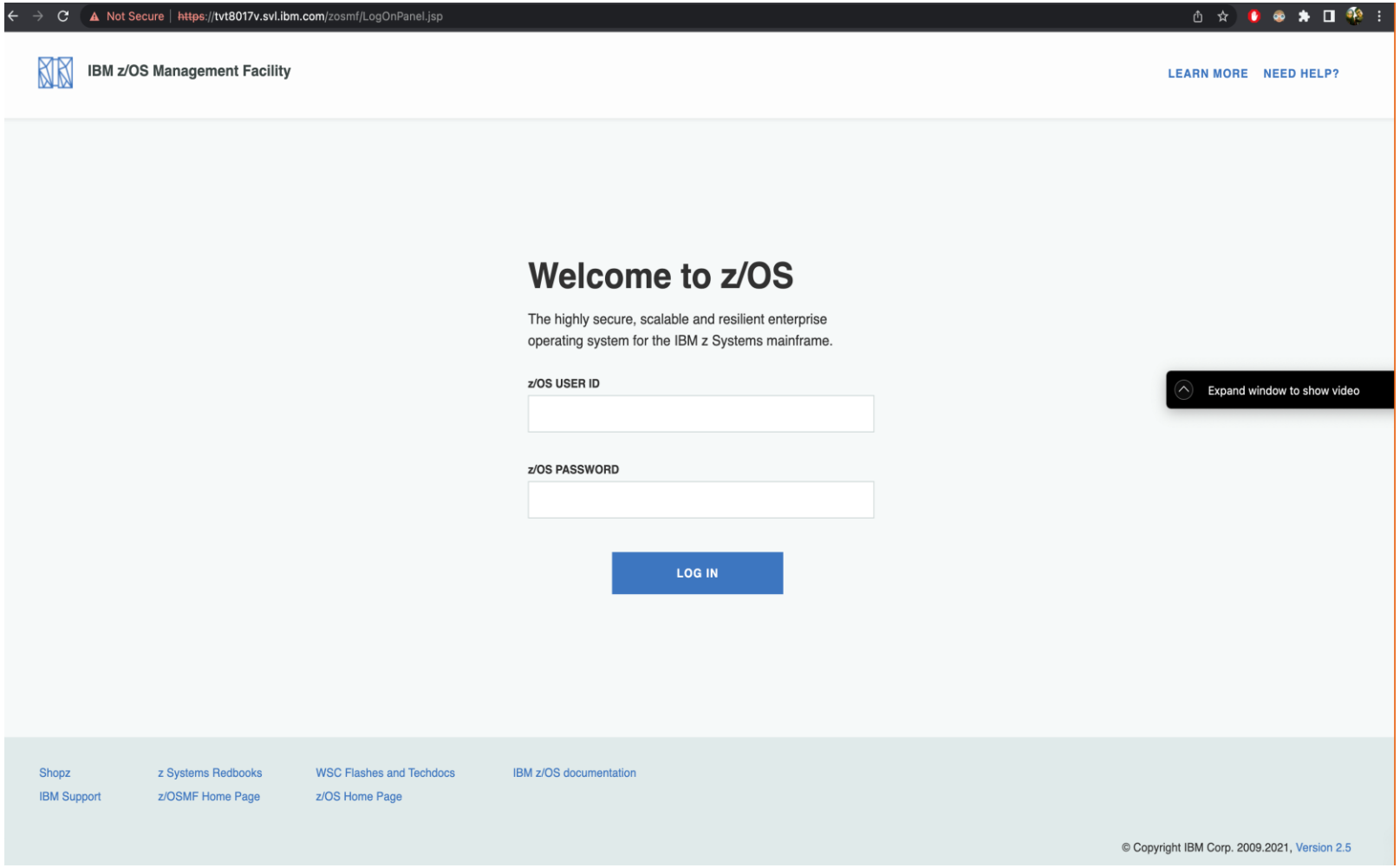
Upgrade & Coexistence Considerations

- 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.

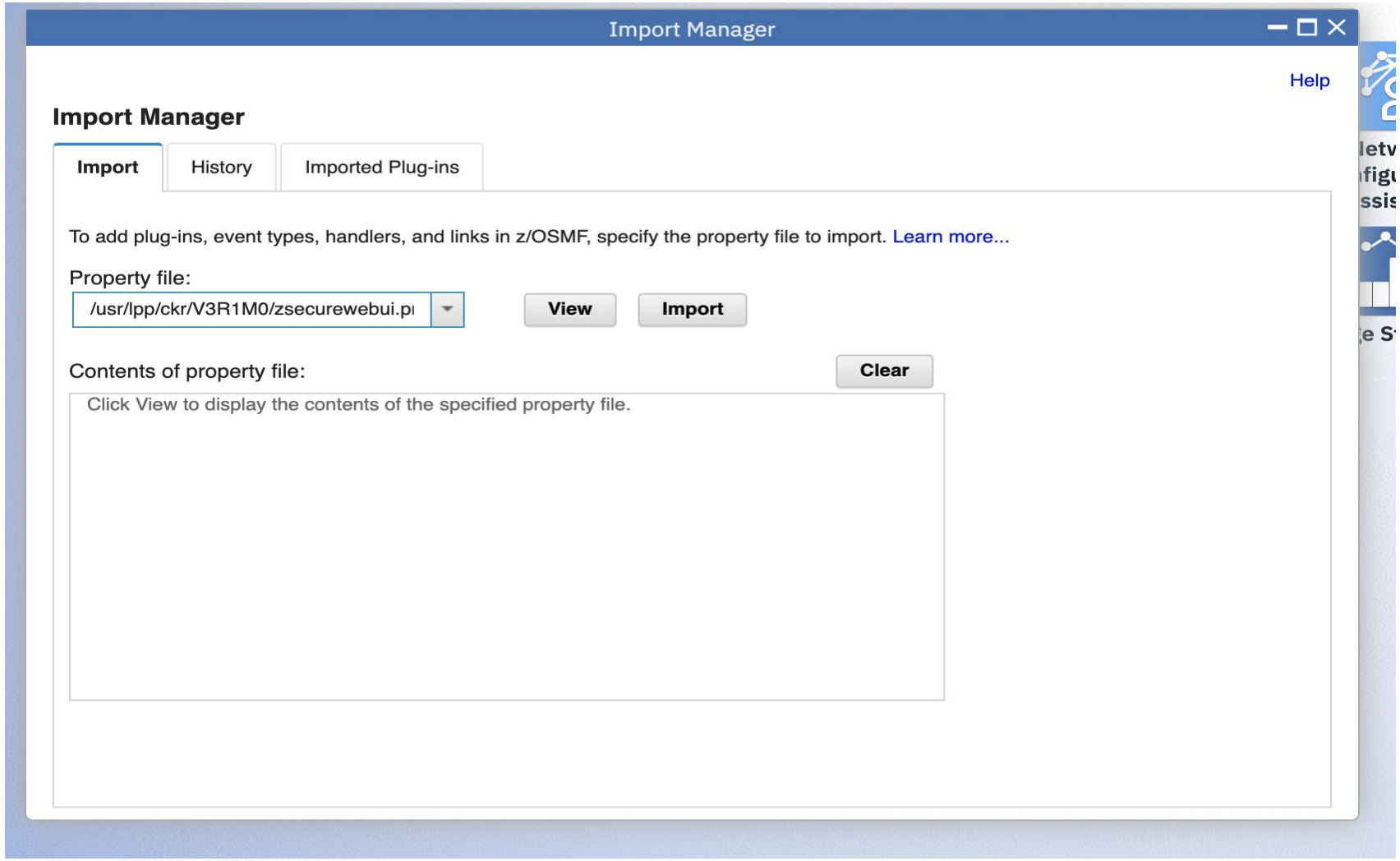


Installation & Configuration

- 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.

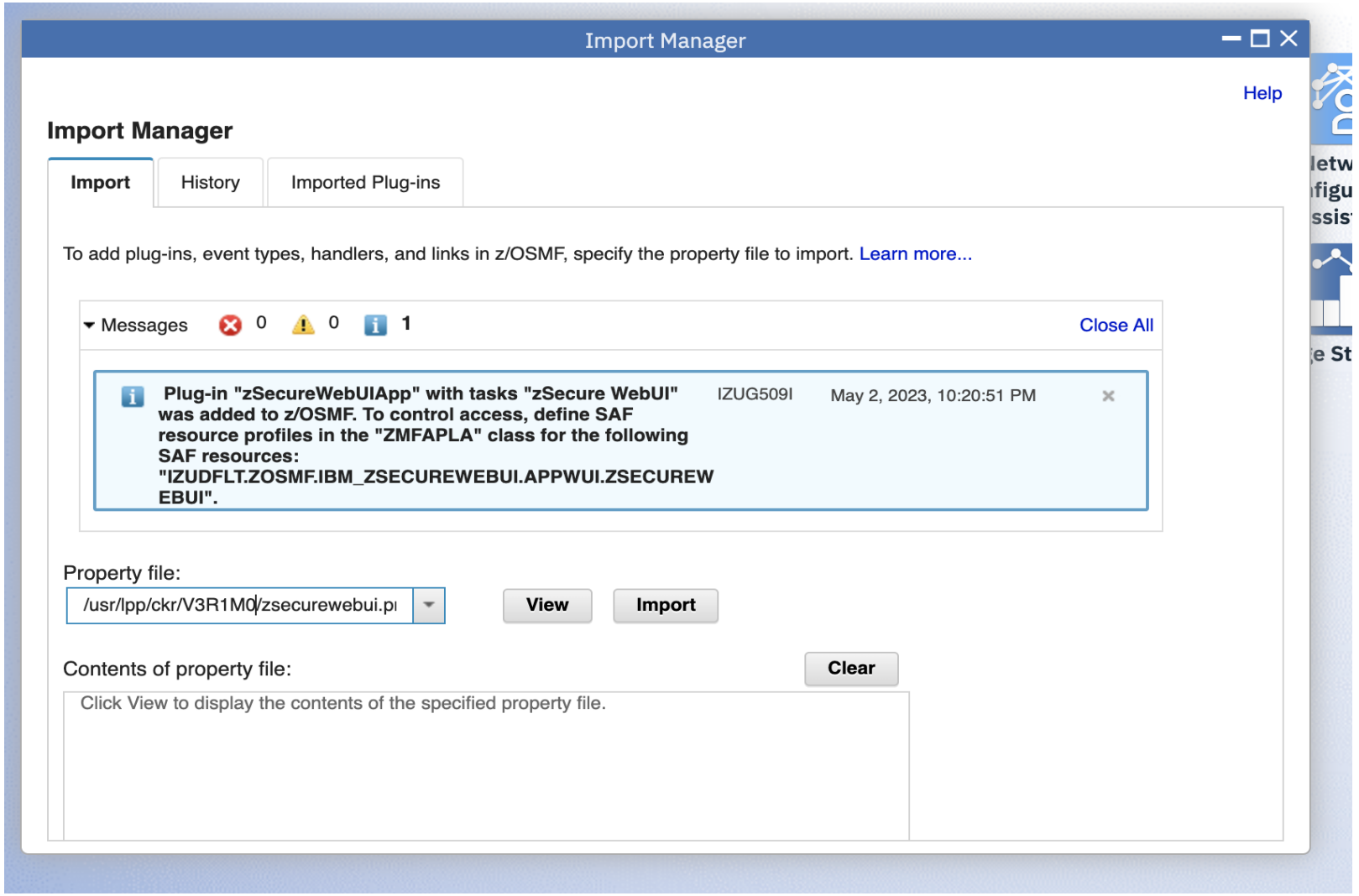
zSecure plug-in for z/OSMF (Installation) (1)

- 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.

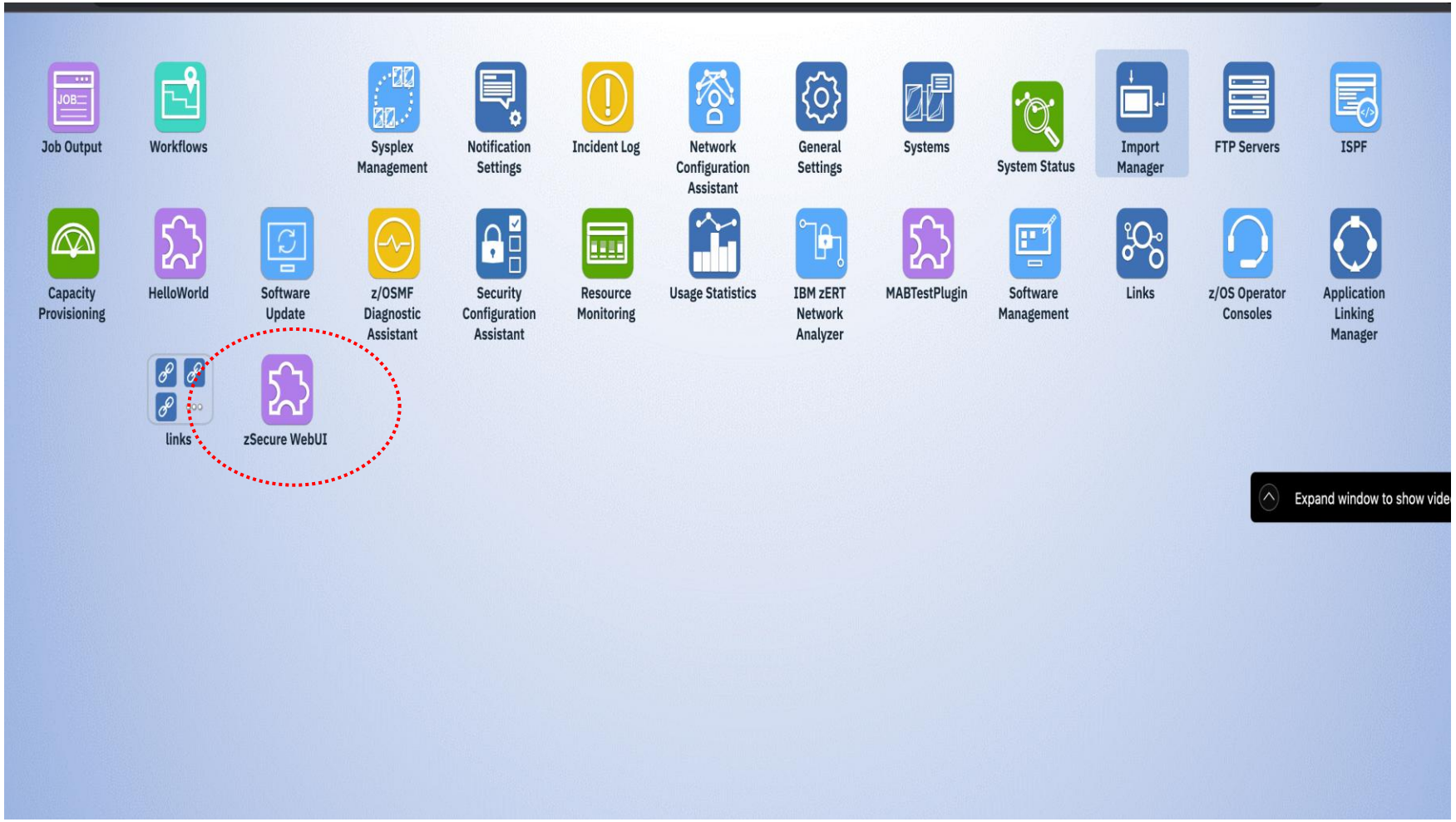


zSecure plug-in for z/OSMF (Authorization)

- 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