z/OS 3.2 IBM Education Assistant

Solution Name: zSecure 3.2 (Admin/Audit/Adapters/CICS Tk/Cmd Verifier/Alert), zSCC 1.3

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

July 2025

Agenda

- Trademarks
- Objectives
- Overview
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Multi-Factor Authentication administration
- zSecure Admin Web UI
- Support for RACF enhancements
- Compliance standards
- IBM Theat Detection for z/OS
- Ideas
- Installation & Configuration
- Summary

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 in zSecure 3.2 and Z Security and Compliance Center 1.3

- Currency for z/OS Security Server (and other z/OS elements)
- Extended support for Multi-Factor Authentication administration
- Additional developments in the zSecure Admin web user interface
- Advances in compliance checking
- and more

Notes:

- zSecure 3.2 is **required** for support of z/OS 3.2 (but can also run on z/OS 2.5)
- zSCC 1.3 includes all of zSecure Audit 3.2.
- zSecure CICS Toolkit does not run on the z/OS platform directly.

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)
  - Provides easy interface for RACF administration and reporting
  - Reduces need for green screen skills by allowing web browser interaction
  - Reduces time spent on compliance checking through automation and built-in knowledge

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
  - Report engine: better performance on z15 and above

Upgrade & Coexistence Considerations

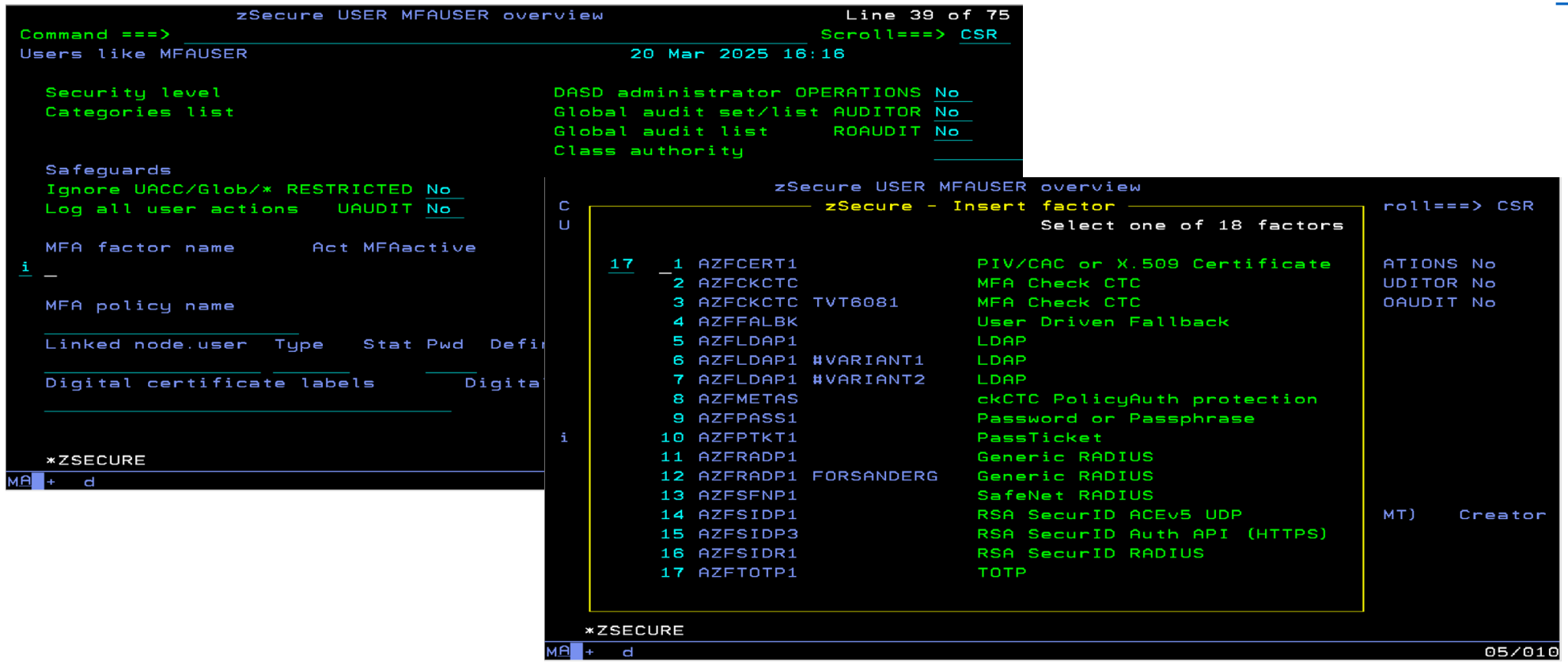
- To exploit this solution, all systems in the Plex must be at the new z/OS level:
  No, runs on any currently supported z/OS release
- As zSecure Command Verifier parses RACF commands in order to determine their conformance to policy, it requires updates whenever new commands or keywords are introduced. When z/OS Security Server puts such updates into the service stream, the required PTFs are usually linked via ++IF REQ.
- A new report engine load module CKR8Z15 is included, while CKR4Z196 is dropped. If you give PROGRAM-controlled access, this might require updates. The option to use a 31-bit report engine has been removed from SE.0.
- There is **no** zSecure Visual 3.2 (5655-ABF, the “Windows UI”).
  End of marketing was announced in December 2024, with the replacement product being zSecure Admin (5655-ABB), which introduced a Web UI in October 2024. Solution packages that included it no longer do, and the solution package with only Admin and Visual (5655-ABH, “Administration”) is no longer there.

Multi-Factor Authentication administration enhancements

MFA administration in zSecure Admin – ISPF UI (1)

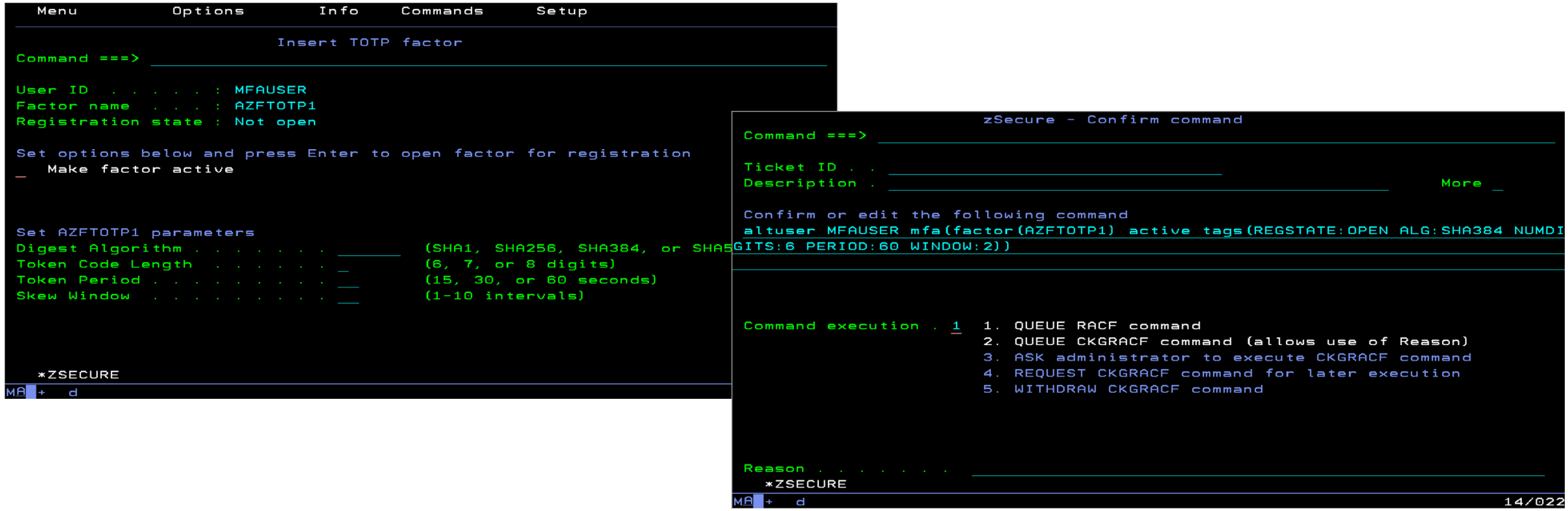
On the detail display of RA.U (RACF administration – User), **I**(nsert)

ZSECURE-I-571



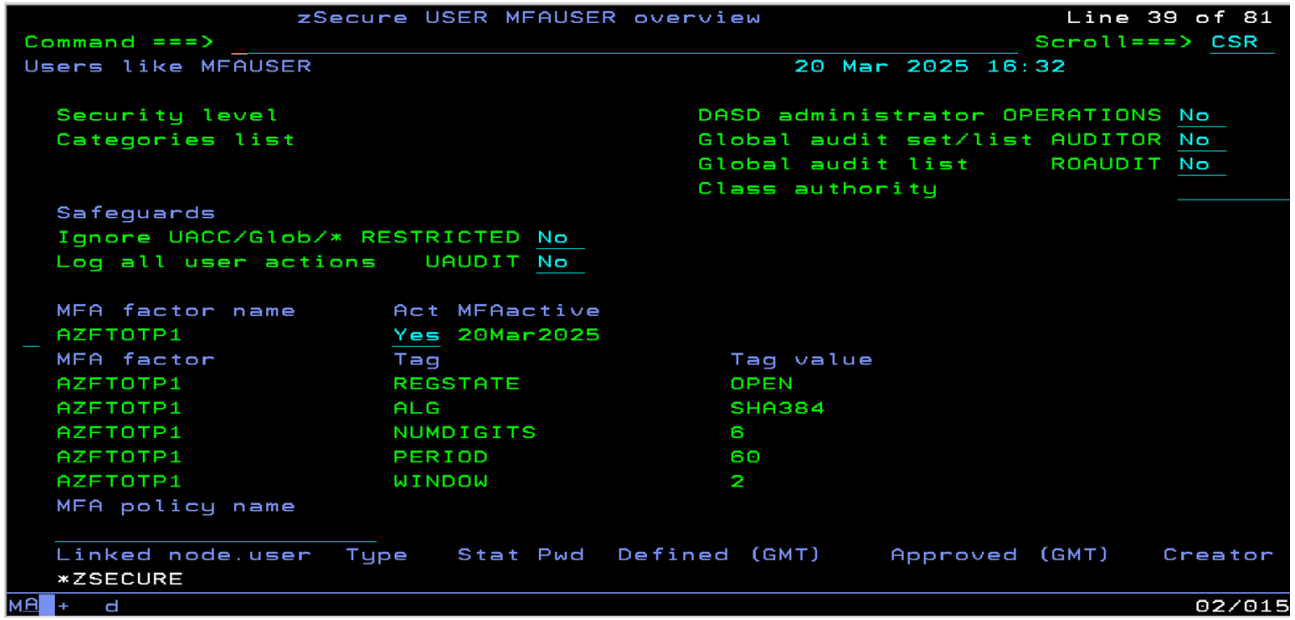
MFA administration in zSecure Admin – ISPF UI (2)

The configuration panel depends on the factor chosen.
In this example, overrides can be specified to the default AZFEXEC configuration.



MFA administration in zSecure Admin – ISPF UI (3)

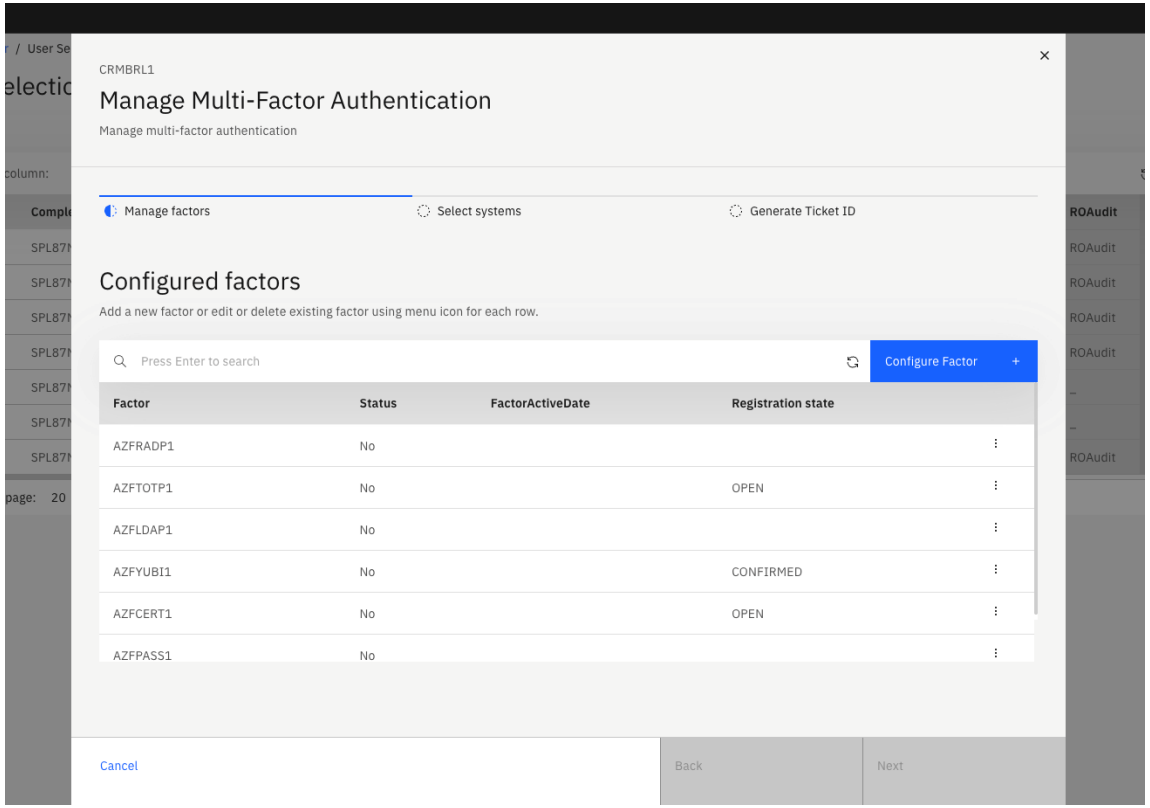
After executing, the **S**(elect) and **D**(elete) actions are also available

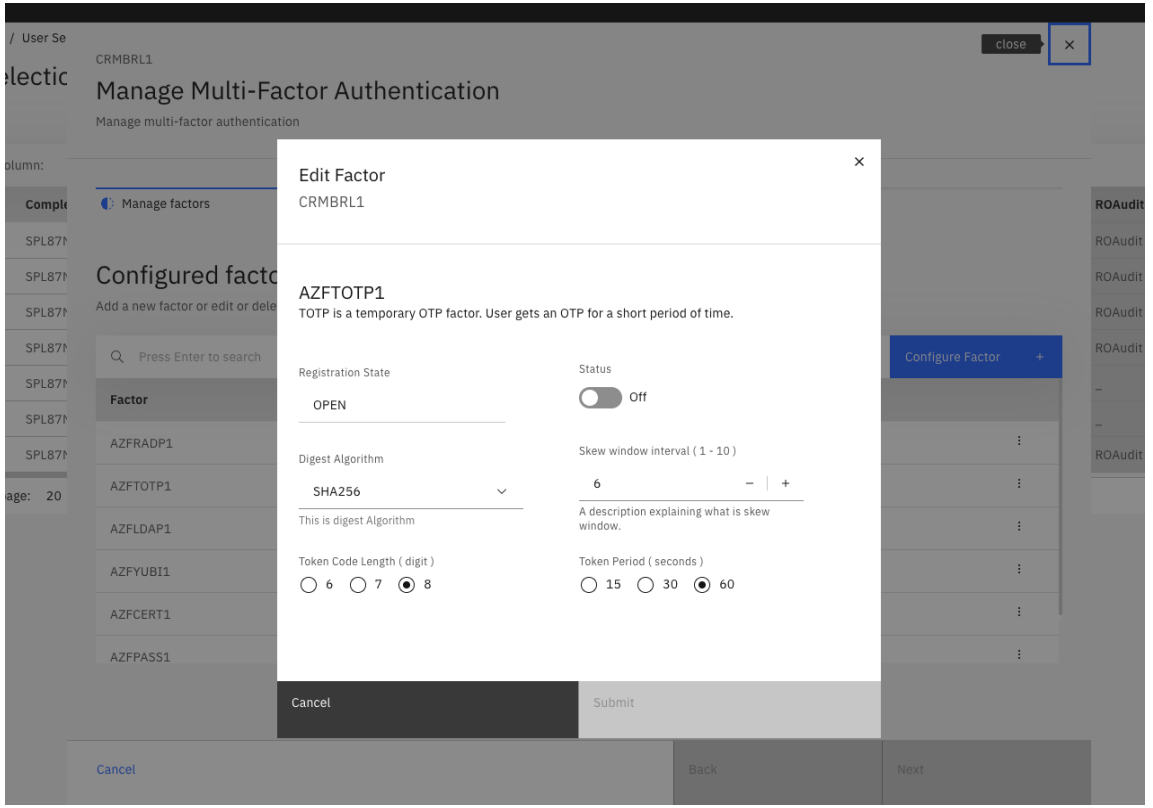


OPEN will become PROVISIONED by registering, that is, by going to https://hostname:6789/AZFTOTP1/GenericStart , logging on with userid and password, and loading the QR code presented into a One Time Password generator such as IBM Verify or Google Authenticator. Afterwards **R**(e-register) will also be available, to go back to OPEN.

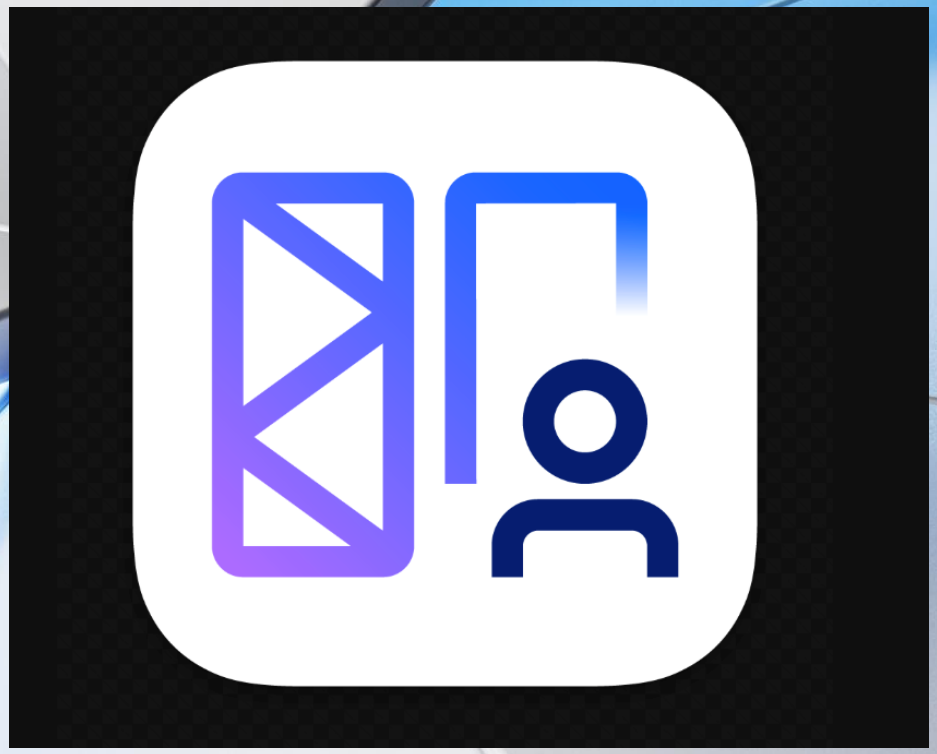
MFA administration in zSecure Admin – Web UI

- In the Web UI it looks like this (subject to further adjustments):





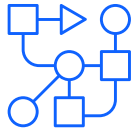
zSecure Admin Web UI



New icon

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.



Simplified management

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

Secure administration

14

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.

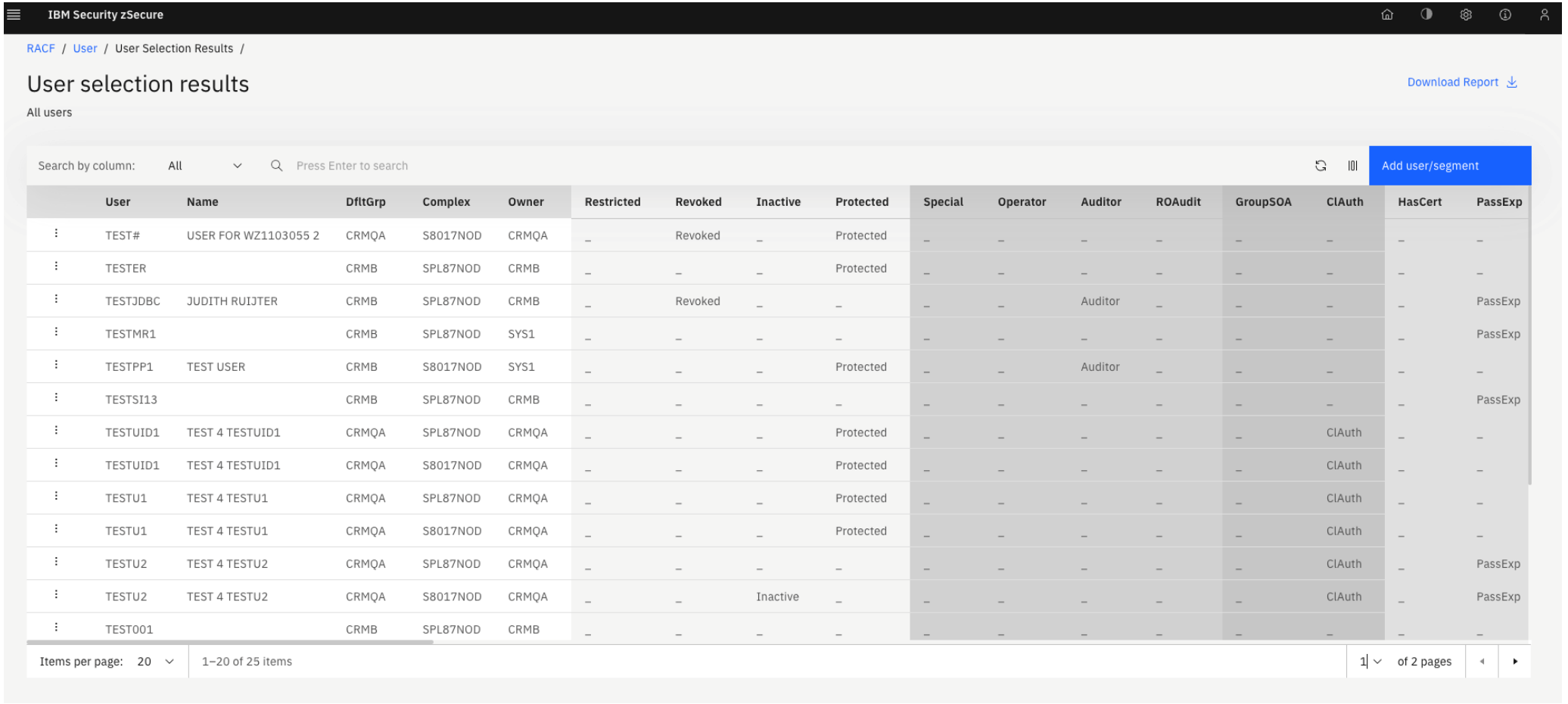
Modern design

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

Web user interface – selection results (1)

ZSS-1133

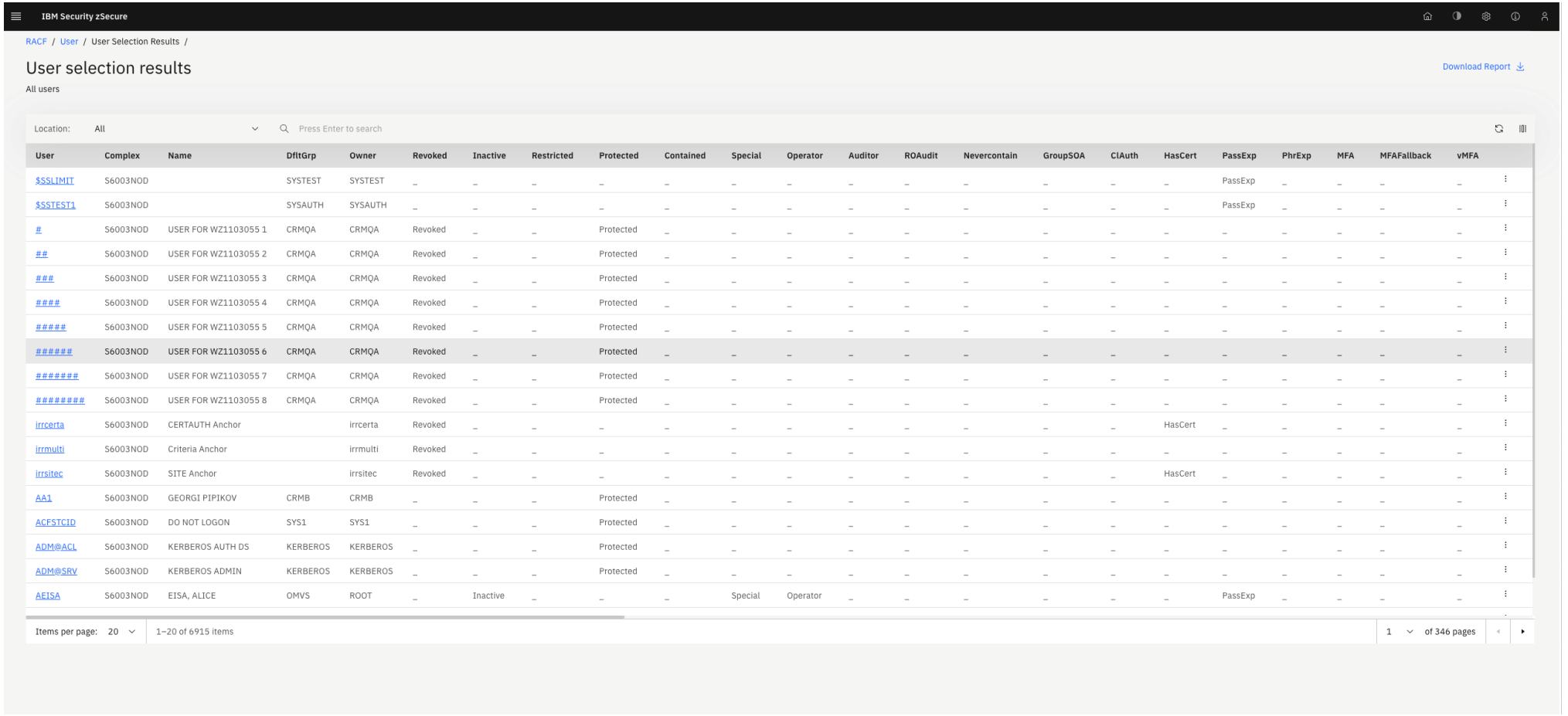
Redesigned for better user experience; before:



	User	Name	DfltGrp	Complex	Owner	Restricted	Revoked	Inactive	Protected	Special	Operator	Auditor	ROAudit	GroupSOA	ClAuth	HasCert	PassExp
⋮	TEST#	USER FOR WZ1103055 2	CRMQA	S8017NOD	CRMQA	_	Revoked	_	Protected	_	_	_	_	_	_	_	_
⋮	TESTER		CRMB	SPL87NOD	CRMB	_	_	_	Protected	_	_	_	_	_	_	_	_
⋮	TESTJDBC	JUDITH RUIJTER	CRMB	SPL87NOD	CRMB	_	Revoked	_	_	_	_	Auditor	_	_	_	_	PassExp
⋮	TESTMR1		CRMB	SPL87NOD	SYS1	_	_	_	_	_	_	_	_	_	_	_	PassExp
⋮	TESTPP1	TEST USER	CRMB	S8017NOD	SYS1	_	_	_	Protected	_	_	Auditor	_	_	_	_	_
⋮	TESTSI13		CRMB	SPL87NOD	CRMB	_	_	_	_	_	_	_	_	_	_	_	PassExp
⋮	TESTUID1	TEST 4 TESTUID1	CRMQA	SPL87NOD	CRMQA	_	_	_	Protected	_	_	_	_	_	ClAuth	_	_
⋮	TESTUID1	TEST 4 TESTUID1	CRMQA	S8017NOD	CRMQA	_	_	_	Protected	_	_	_	_	_	ClAuth	_	_
⋮	TESTU1	TEST 4 TESTU1	CRMQA	SPL87NOD	CRMQA	_	_	_	Protected	_	_	_	_	_	ClAuth	_	_
⋮	TESTU1	TEST 4 TESTU1	CRMQA	S8017NOD	CRMQA	_	_	_	Protected	_	_	_	_	_	ClAuth	_	_
⋮	TESTU2	TEST 4 TESTU2	CRMQA	SPL87NOD	CRMQA	_	_	_	_	_	_	_	_	_	ClAuth	_	PassExp
⋮	TESTU2	TEST 4 TESTU2	CRMQA	S8017NOD	CRMQA	_	_	Inactive	_	_	_	_	_	_	ClAuth	_	PassExp
⋮	TEST001		CRMB	SPL87NOD	CRMB	_	_	_	_	_	_	_	_	_	_	_	_

Web user interface – selection results (2)

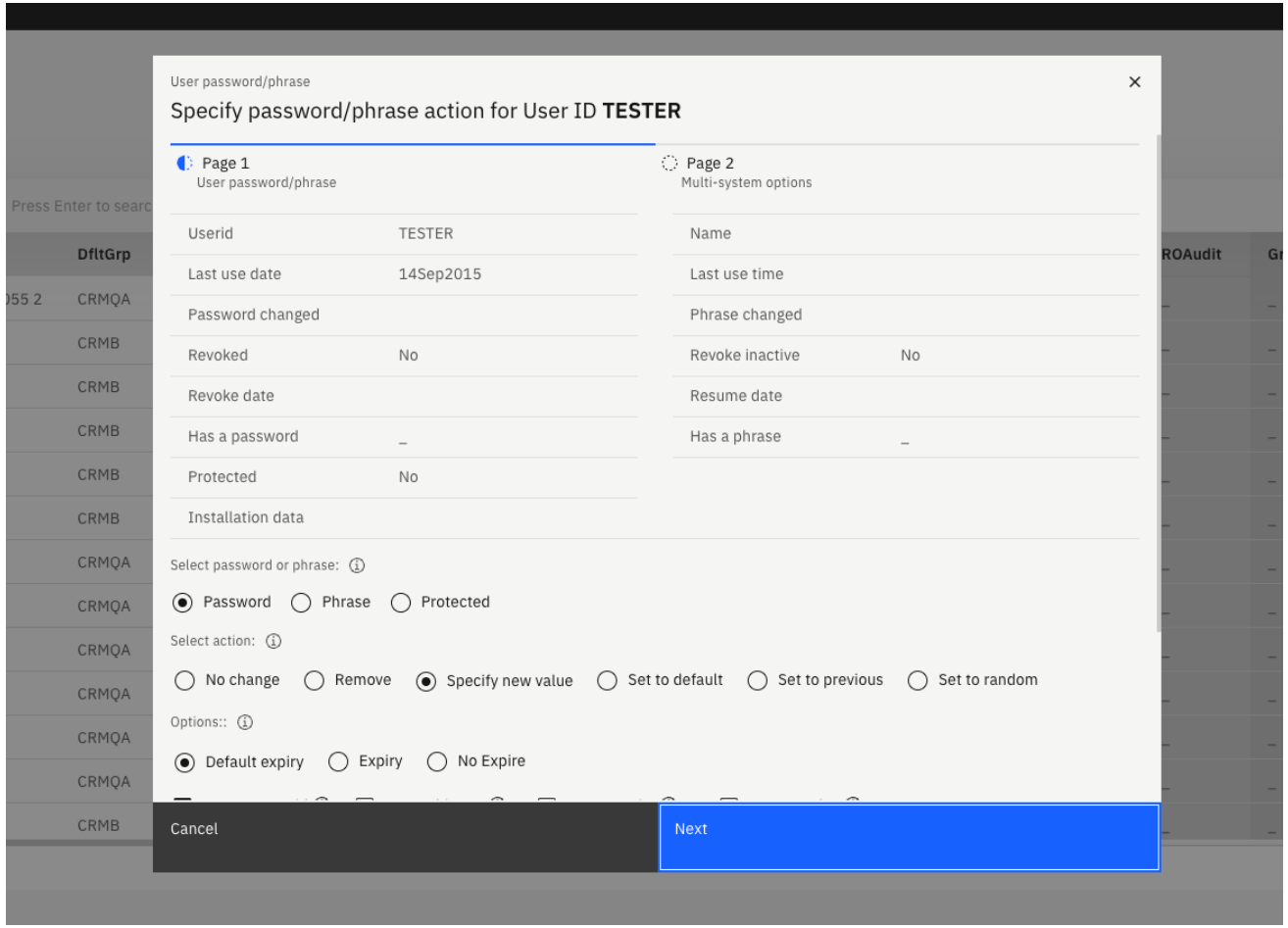
Redesigned for better user experience; after:



User	Complex	Name	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Contained	Special	Operator	Auditor	ROAudit	Nevercontain	GroupSOA	ClAuth	HasCert	PassExp	PhrExp	MFA	MFAFallback	vMFA
$SSLIMIT	S6003NOD		SYSTEST	SYSTEST	_	_	_	_	_	_	_	_	_	_	_	_	_	PassExp	_	_	_	_
$SSTEST1	S6003NOD		SYSAUTH	SYSAUTH	_	_	_	_	_	_	_	_	_	_	_	_	_	PassExp	_	_	_	_
#	S6003NOD	USER FOR WZ1103055 1	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
##	S6003NOD	USER FOR WZ1103055 2	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
###	S6003NOD	USER FOR WZ1103055 3	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
####	S6003NOD	USER FOR WZ1103055 4	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
#####	S6003NOD	USER FOR WZ1103055 5	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
######	S6003NOD	USER FOR WZ1103055 6	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
#######	S6003NOD	USER FOR WZ1103055 7	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
########	S6003NOD	USER FOR WZ1103055 8	CRMQA	CRMQA	Revoked	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
irrcerta	S6003NOD	CERTAUTH Anchor		irrcerta	Revoked	_	_	_	_	_	_	_	_	_	_	_	HasCert	_	_	_	_	_
irrmulti	S6003NOD	Criteria Anchor		irrmulti	Revoked	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
irrsitec	S6003NOD	SITE Anchor		irrsitec	Revoked	_	_	_	_	_	_	_	_	_	_	_	HasCert	_	_	_	_	_
AA1	S6003NOD	GEORGI PIPIKOV	CRMB	CRMB	_	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
ACFSTCID	S6003NOD	DO NOT LOGON	SYS1	SYS1	_	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
ADM@ACL	S6003NOD	KERBEROS AUTH DS	KERBEROS	KERBEROS	_	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
ADM@SRV	S6003NOD	KERBEROS ADMIN	KERBEROS	KERBEROS	_	_	_	Protected	_	_	_	_	_	_	_	_	_	_	_	_	_	_
AEISA	S6003NOD	EISA, ALICE	OMVS	ROOT	_	Inactive	_	_	_	Special	Operator	_	_	_	_	_	_	PassExp	_	_	_	_

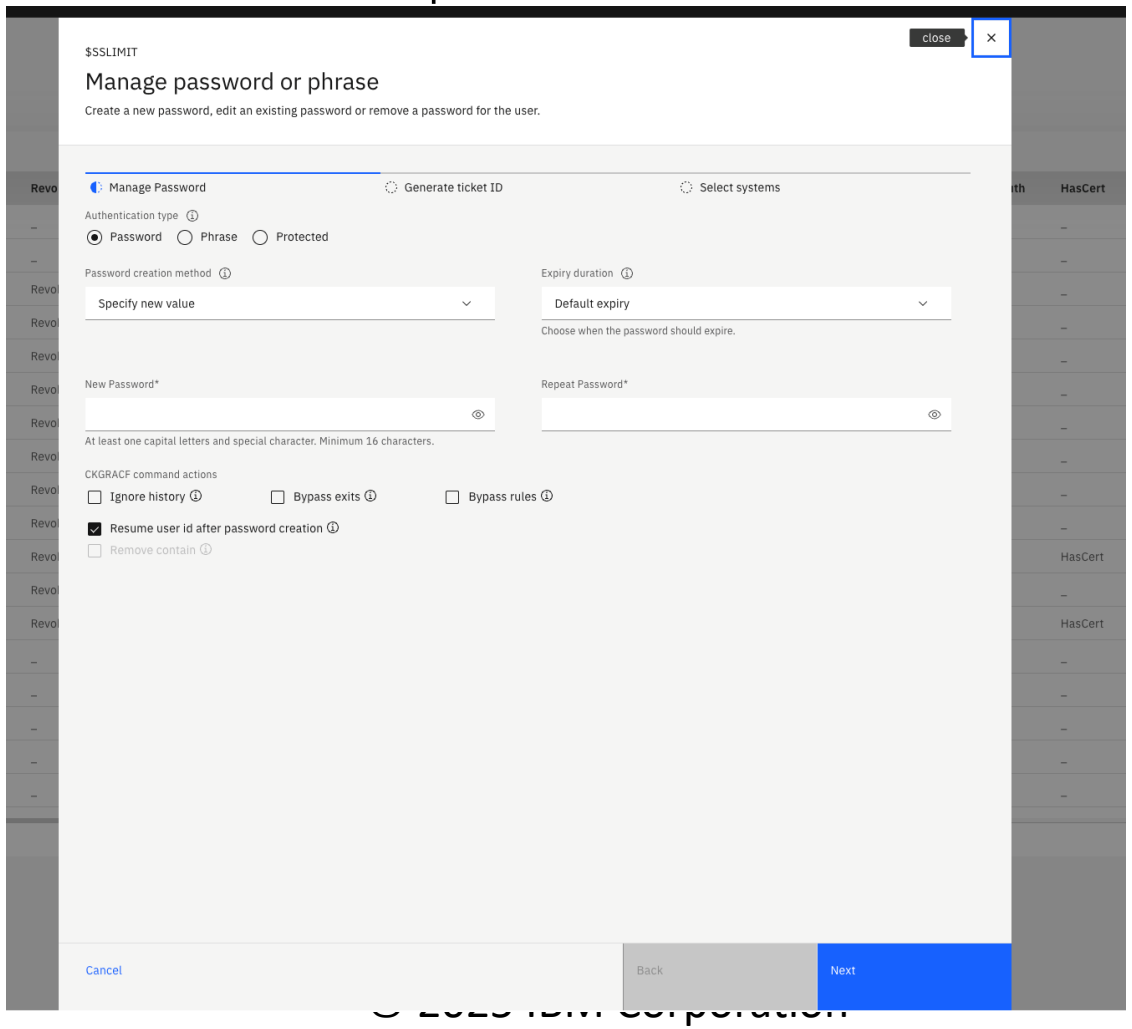
Web user interface – line commands (1)

Redesigning for better user experience; before:



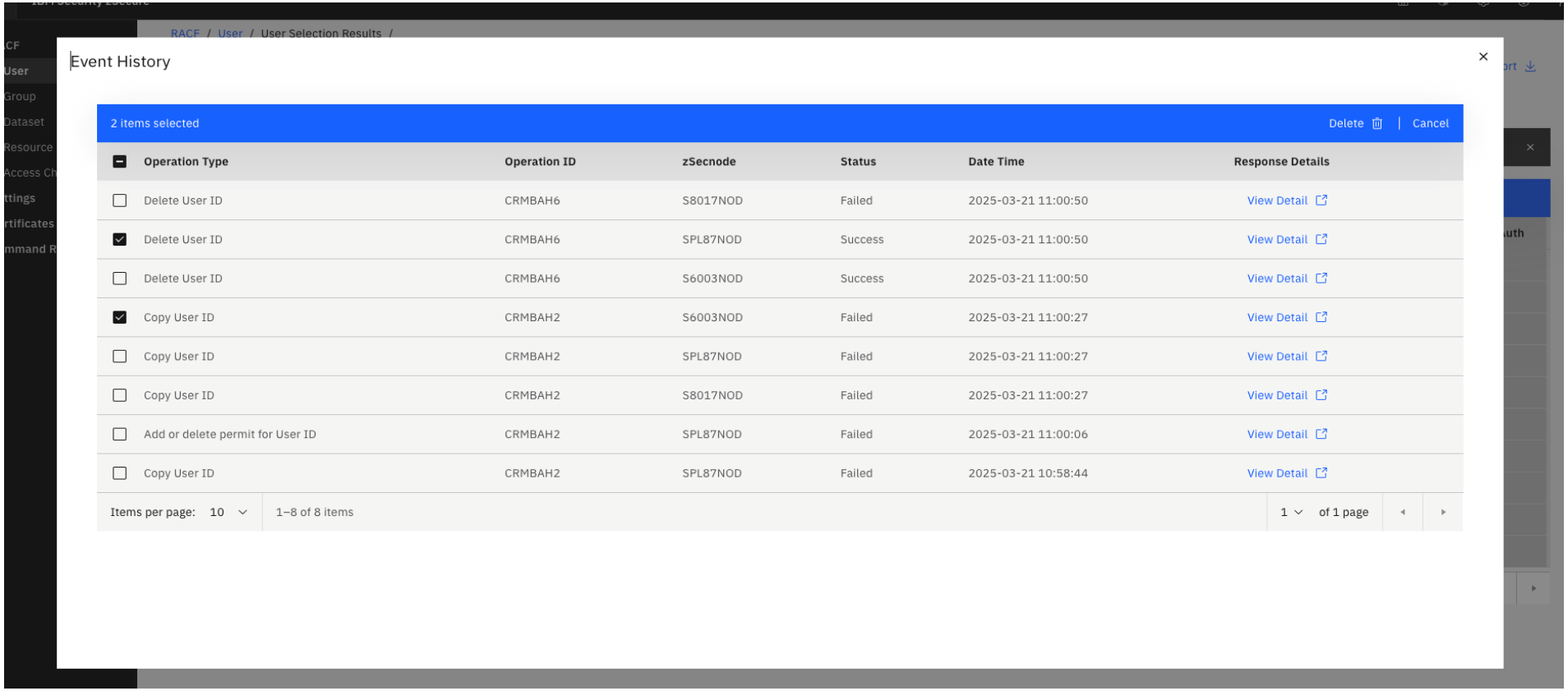
Web user interface – line commands (2)

Redesigning for better user experience; after:



Web user interface – history tab

History is now persistent across sessions, and adds detail such as target ID:



It is possible to delete some or all entries.

Support for RACF enhancements

Data Set Encryption (1)

DFSMS provides Tape Data Set Access Method Encyption
RACF provides support for setting a granular encryption policy
zSecure provides support for easy administration of RACF.

New RACF template field ENCTYPES available in CARLa, with alias ENCRYPTTYPES (the RACF command keyword).

Shown in RA.D (RACF administration – DATASET) in the DFP segment.
Overtype, COPY, RECREATE, MERGE support in zSecure Admin.
SMF: keyword formatted in RACF command in zSecure Audit (and Adapters/zSCC).

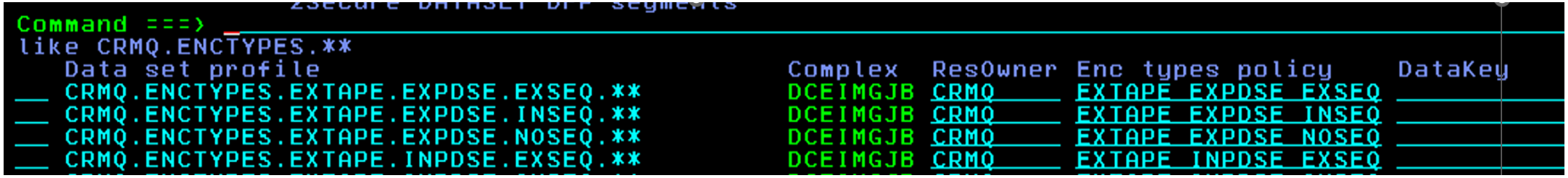
zSecure Command Verifier: C4R.DATASET.DFP.ENCRYPTTYPES.*profile* policy profiles to control keyword use

Back-ported to z/OS 2.5 and 3.1. Already available.
zSecure PTF numbers included in RACF presentation.

zSecure technote: https://www.ibm.com/support/pages/node/7182342

Data Set Encryption (2)

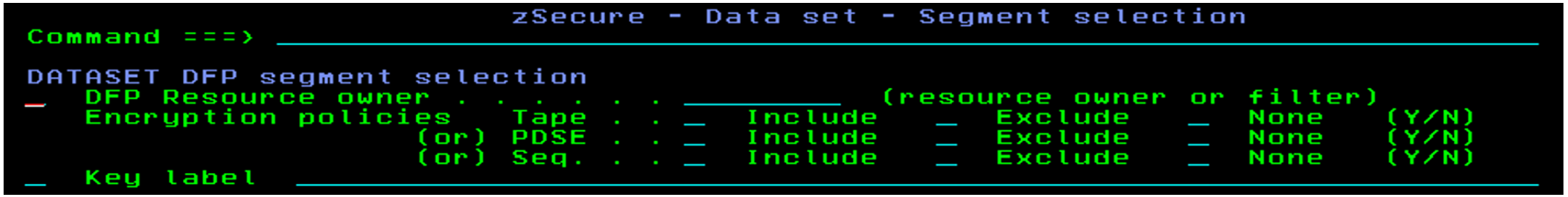
In the ISPF UI, the field value is shown as a string (on both display levels):



"*encrypt*TAPE *encrypt*PDSE *encrypt*SEQ" (within quotes), where *encrypt* is either IN, EX, or NO:

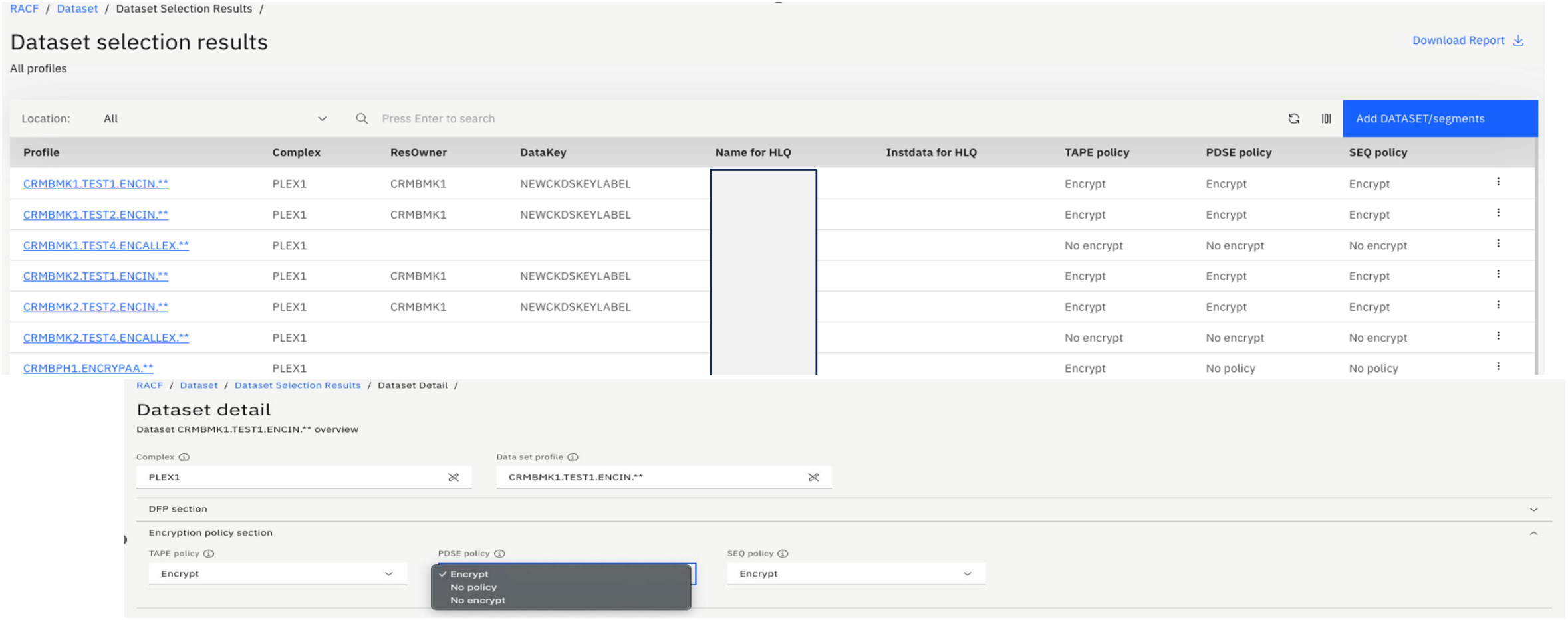
- IN – Include the data set type for encryption.
- EX – Exclude the data set type from encryption.
- NO – When determining encryption eligibility, ENCTYPES is not considered for this data set type. This is the default behavior.

And in the UI selection is done like this:



Data Set Encryption

In the Web UI, the field is shown like this:



Extend JWT support (“IDT3”) (1/2)

RACF provides support for additional Identity Tokens
zSecure provides support for easy administration of RACF.

New RACF template fields IDTLABP and IDTKIDP available in CARLa, with aliases SIGLABELPRIMARY and SIGKIDPRIMARY (the RACF command keywords).

Shown in RA.R (RACF administration – RESOURCE) in the IDTPARMS segment.
Overtype, COPY, RECREATE, MERGE support in zSecure Admin.
SMF: formatted in RACF command in zSecure Audit (and Adapters/zSCC).
SMF: new CARLa fields IDT_SIGNATURE_EVALUATOR, KEY_IDENTIFIER, and SIGNATURE_ALGORITHM for data in new relocate section 443 (SMF 80-1).

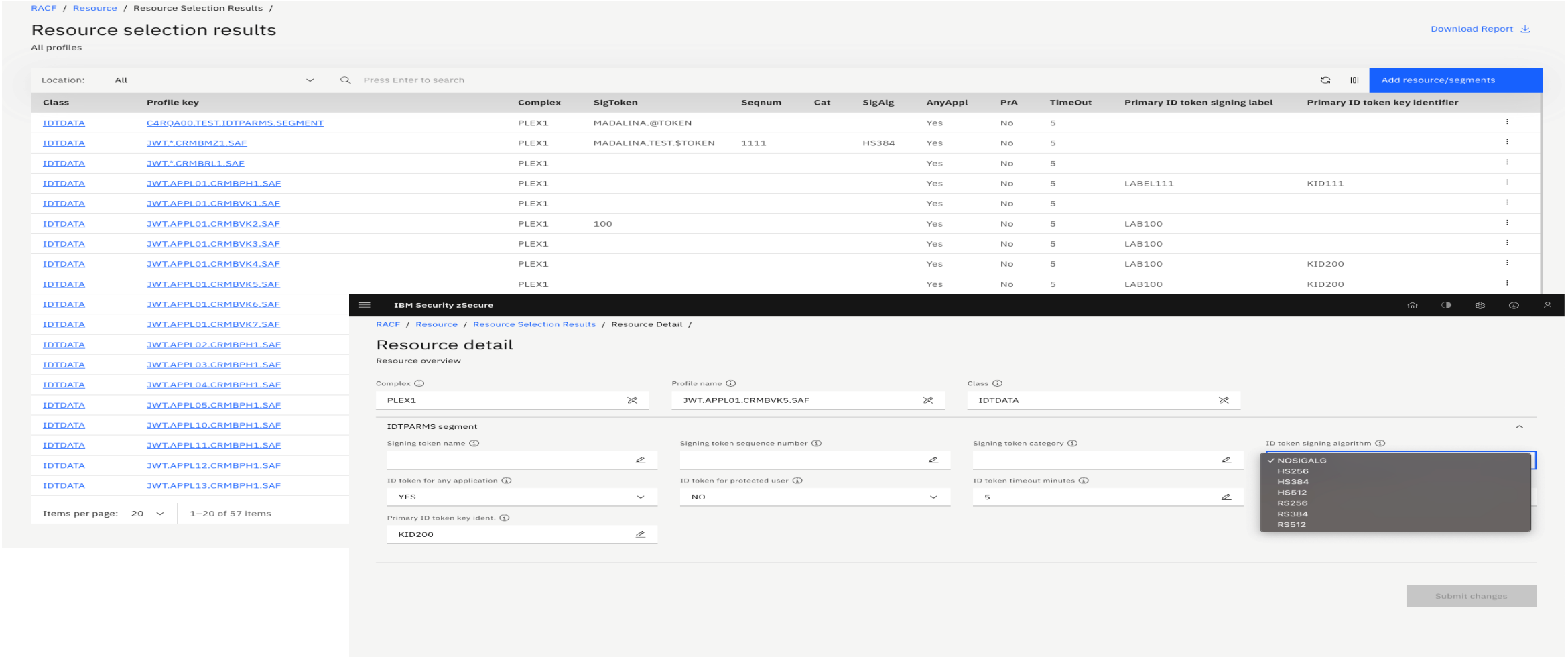
zSecure Command Verifier recognizes the keywords.

Back-ported to 3.1. zSecure APARs: OA67545 (HCKR310) OA67546 (HC4R310)

zSecure FMID	zSecure PTF	RACF FMID	RACF PTF
HCKR310	UJ96690	HRF77E0	UJ96699
HC4R310	UJ96691	HRF77E0	UJ96699

Extend JWT support (“IDT3”) (2/2)

In the Web UI, the support looks like this:



RACF User Quarantine (CONTAIN) (1)

RACF provides support for quarantining a user
zSecure provides support for easy administration of RACF.

RACF user IDs can be CONTAINed (stronger than revoke).
Keywords CONTAIN, NOCONTAIN, NEVERCONTAIN, ALLOWCONTAIN.
Flags shown in RA.U (RACF administration – USER), etc., zSecure CICS Toolkit, and CKGRACF output.

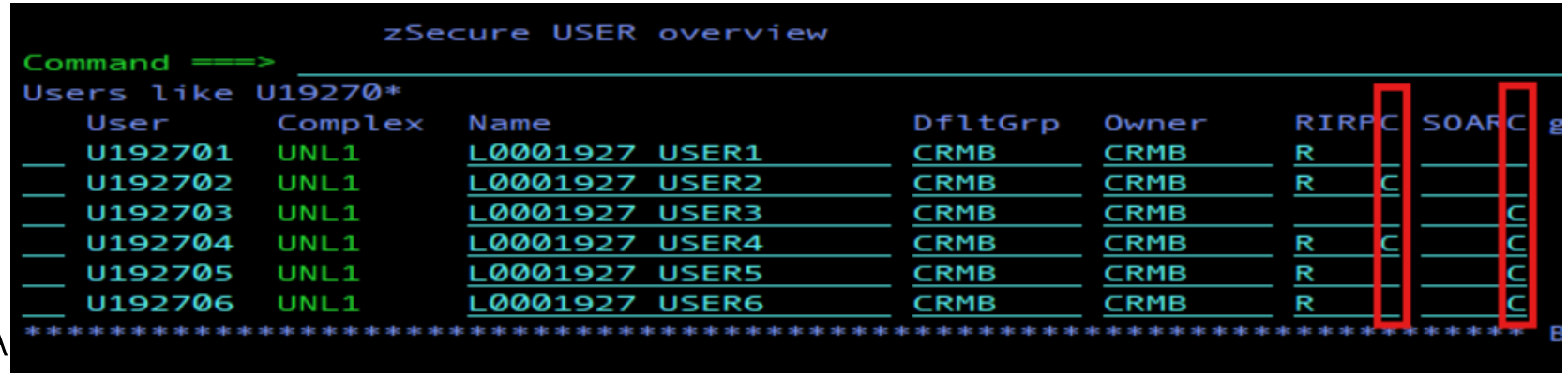
COPY/RECREATE/MERGE will copy NEVERCONTAIN but not CONTAINED.
RA.U P(assword) command extended with ALTUSER RESUME NOCONTAIN.
SMF formats keywords, and supports CONTAIN event, with details.
Alerts for CONTAIN event and setting NEVERCONTAIN property (zSecure Alert)

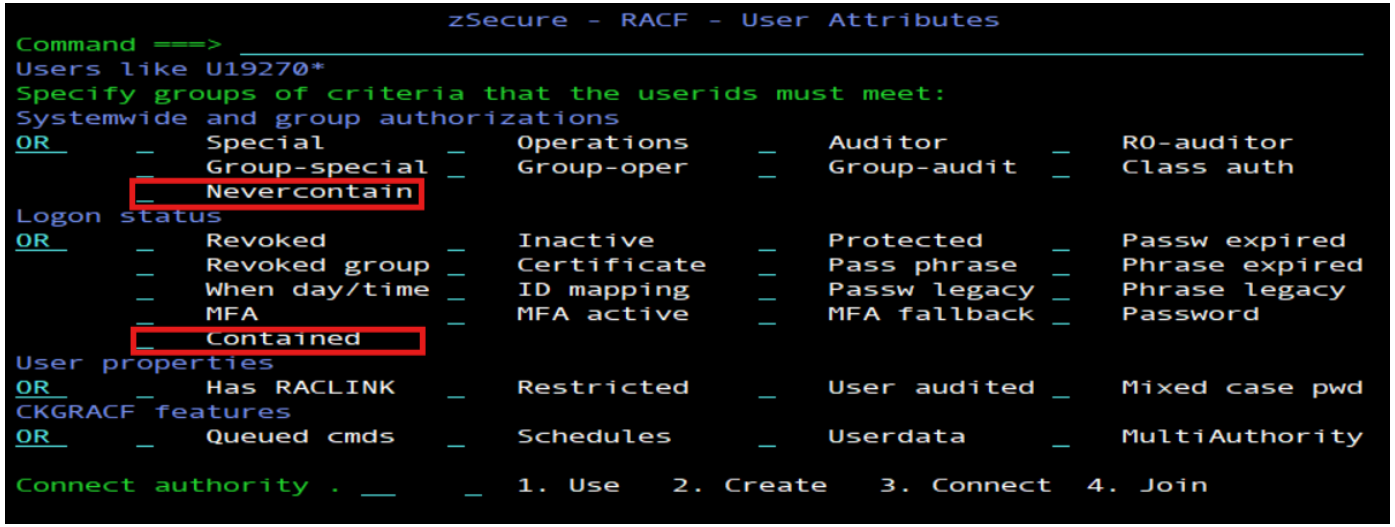
zSecure Command Verifier supports the keywords

RACF User Quarantine (CONTAIN) (2)

In the ISPF UI, the flags are shown like this:

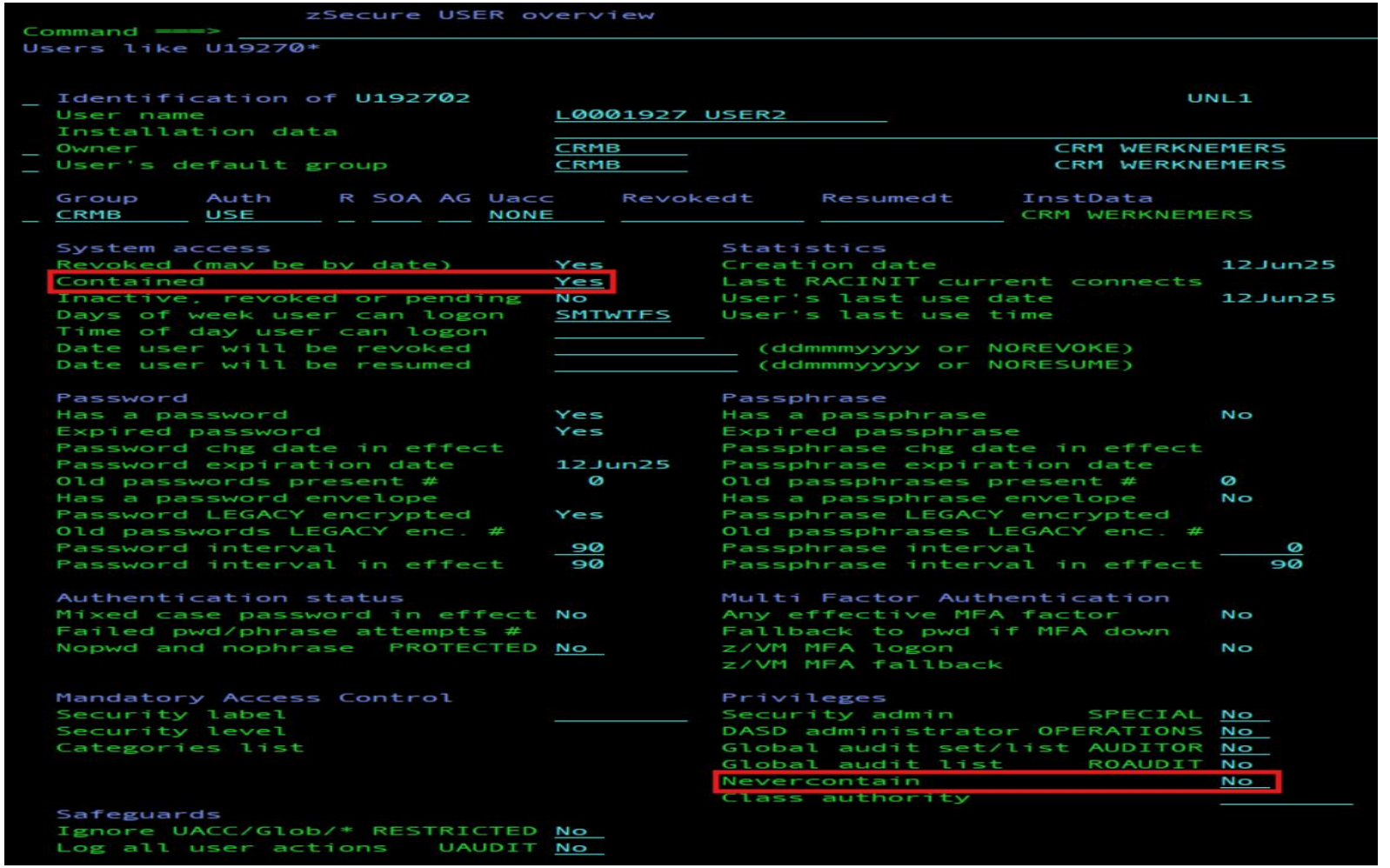
A





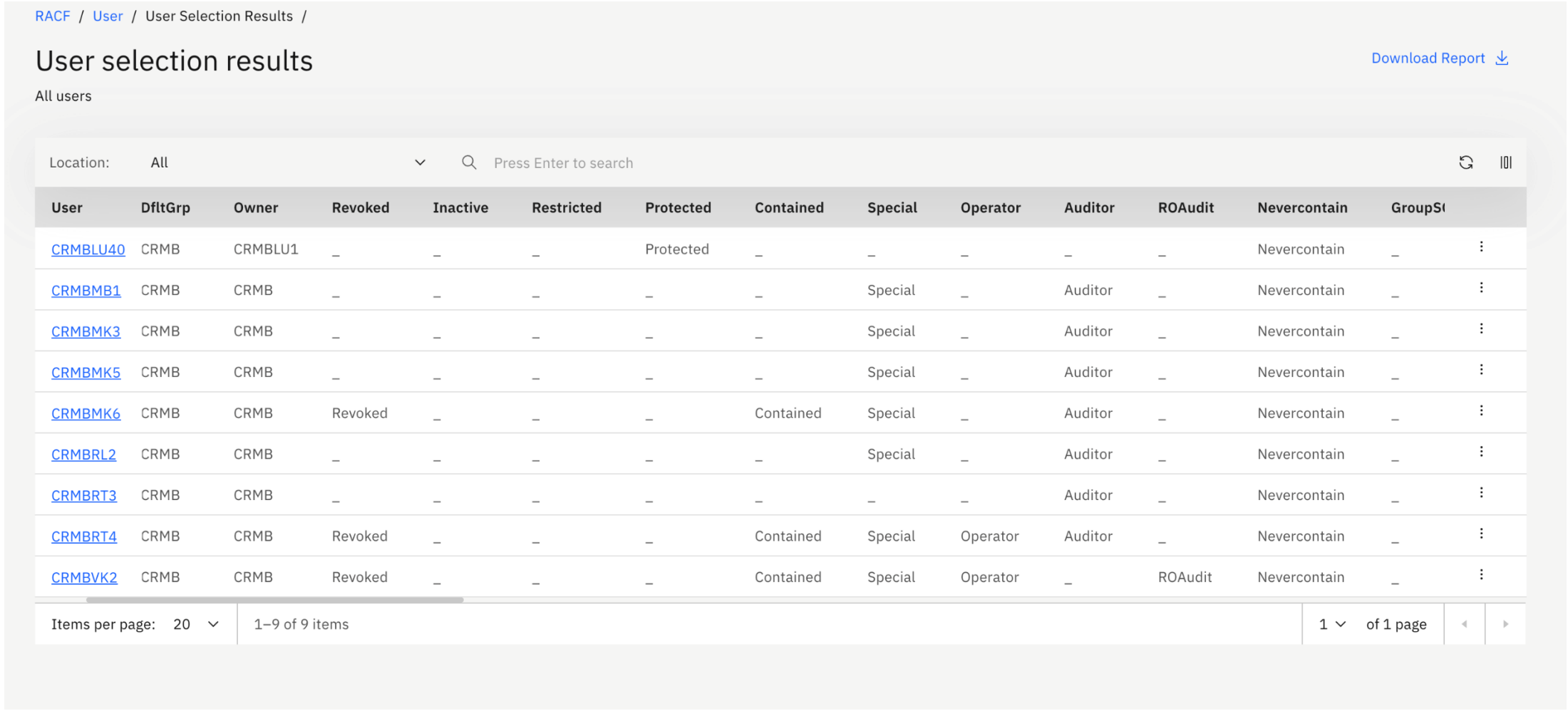
RACF User Quarantine (CONTAIN) (3)

User detail display:



RACF User Quarantine (CONTAIN) (4)

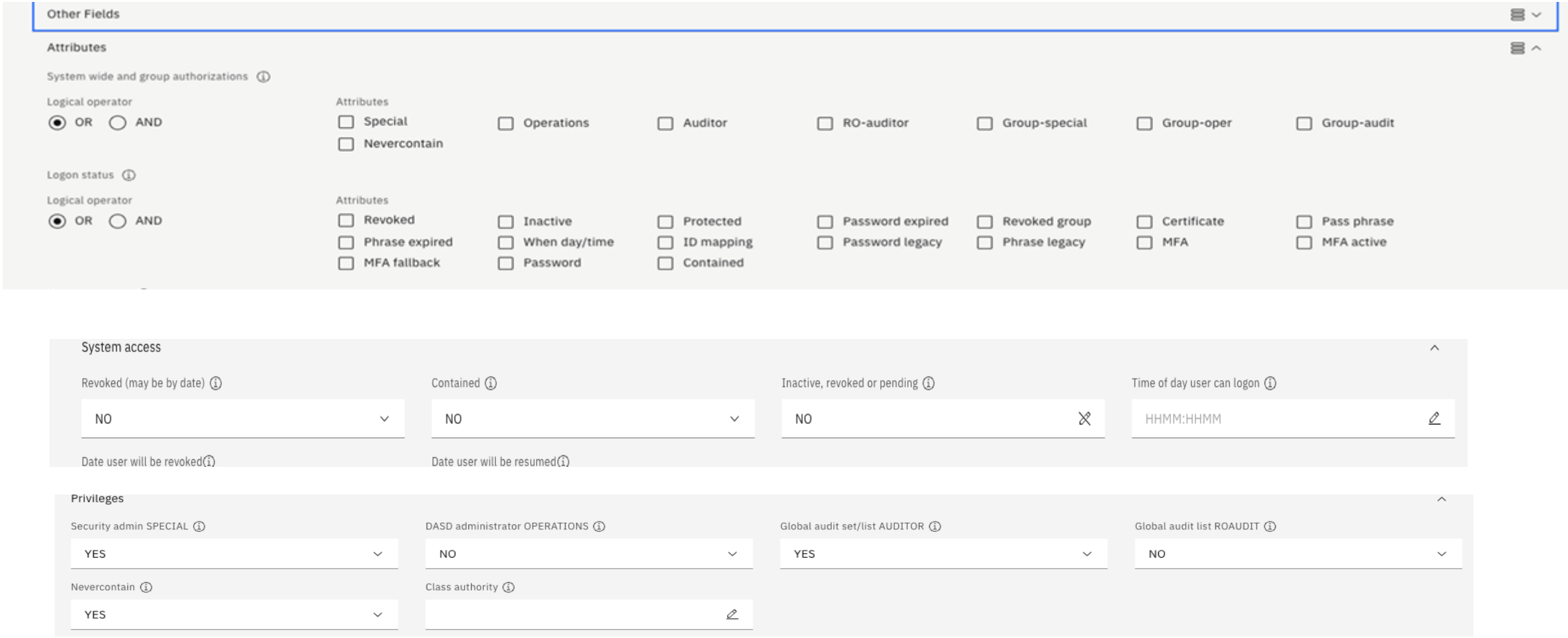
Web UI USER overview:



User	DfltGrp	Owner	Revoked	Inactive	Restricted	Protected	Contained	Special	Operator	Auditor	ROAudit	Nevercontain	GroupS(
CRMBLU40	CRMB	CRMBLU1	_	_	_	Protected	_	_	_	_	_	Nevercontain	_
CRMBMB1	CRMB	CRMB	_	_	_	_	_	Special	_	Auditor	_	Nevercontain	_
CRMBMK3	CRMB	CRMB	_	_	_	_	_	Special	_	Auditor	_	Nevercontain	_
CRMBMK5	CRMB	CRMB	_	_	_	_	_	Special	_	Auditor	_	Nevercontain	_
CRMBMK6	CRMB	CRMB	Revoked	_	_	_	Contained	Special	_	Auditor	_	Nevercontain	_
CRMBRL2	CRMB	CRMB	_	_	_	_	_	Special	_	Auditor	_	Nevercontain	_
CRMBRT3	CRMB	CRMB	_	_	_	_	_	_	_	Auditor	_	Nevercontain	_
CRMBRT4	CRMB	CRMB	Revoked	_	_	_	Contained	Special	Operator	Auditor	_	Nevercontain	_
CRMBVK2	CRMB	CRMB	Revoked	_	_	_	Contained	Special	Operator	_	ROAudit	Nevercontain	_

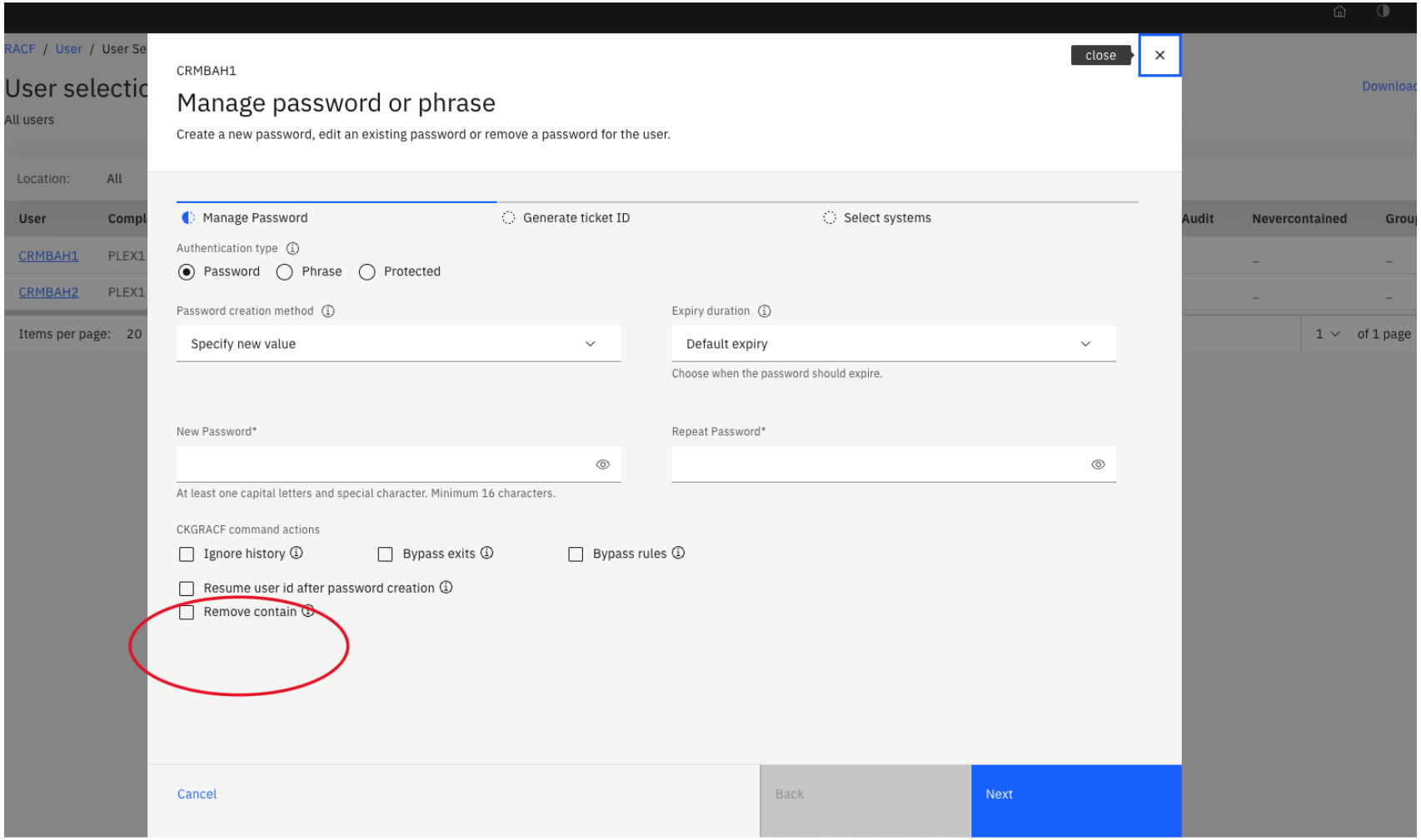
RACF User Quarantine (CONTAIN) (5)

Web UI selection:



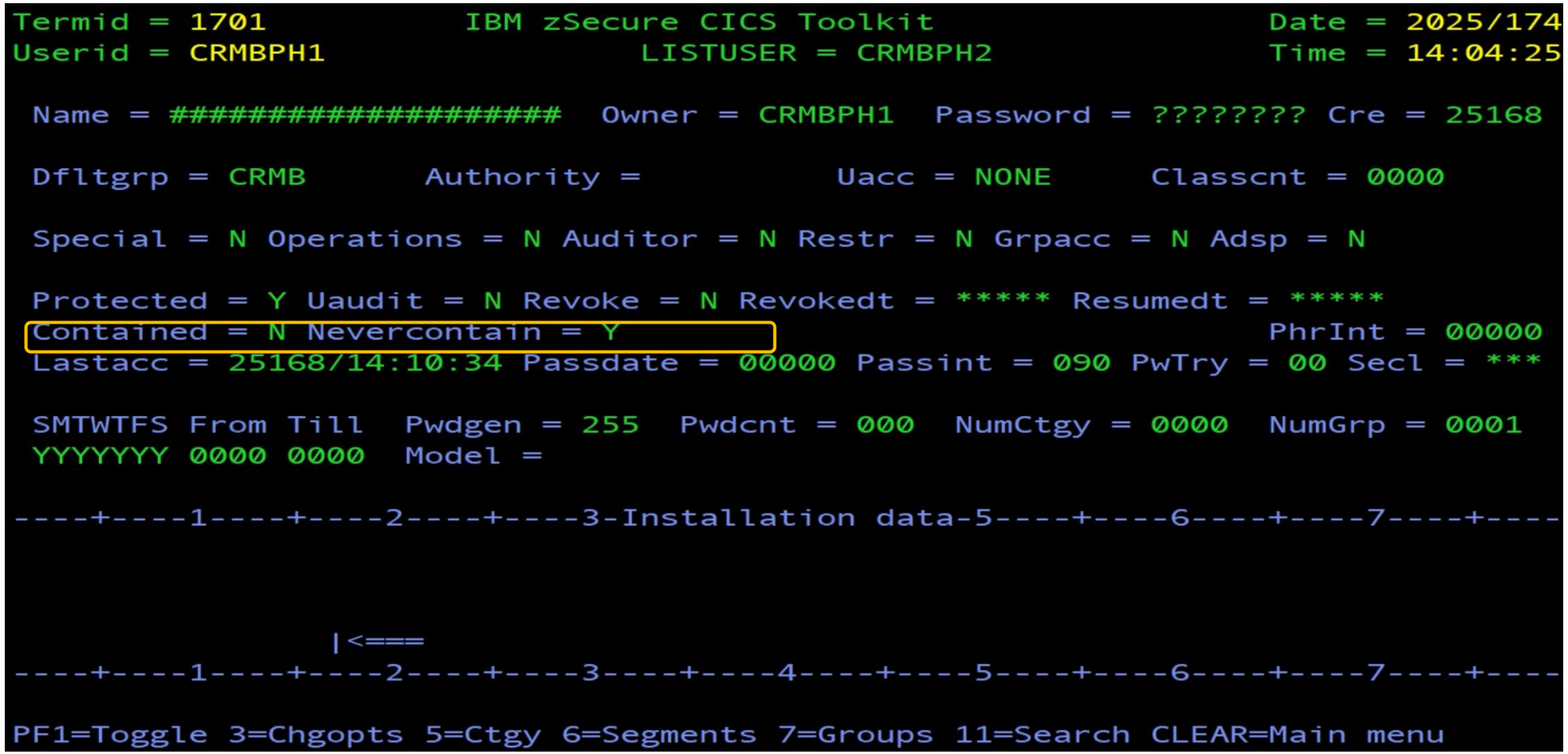
RACF User Quarantine (CONTAIN) (6)

In order to RESUME a user, CONTAIN cannot remain set.



RACF User Quarantine (CONTAIN) (7)

Updated zSecure CICS Toolkit screen (display only):



RACDCERT multiple altnames

RACF provides support for multiple altnames in certificates
zSecure provides support for easy administration of RACF.

RACDCERT GENCERT adds keywords like ADOMAIN in addition to DOMAIN, etc.

RA.5 (RACF administration – certificates) will be updated to allow multiple altnames to be specified and generate the right RACF commands.

SMF data for these new specifications will be formatted appropriately.

====

New keyword PBE on RACDCERT EXPORT
to specify whether the new algorithm is needed when the export format is either PKCS12DER or PKCS12B64. The only acceptable values for this keyword are AES and TDES.

RA.5 line command EX updated
SMF command support

RACF CSDATA fields in RA.*x* selection and overview displays

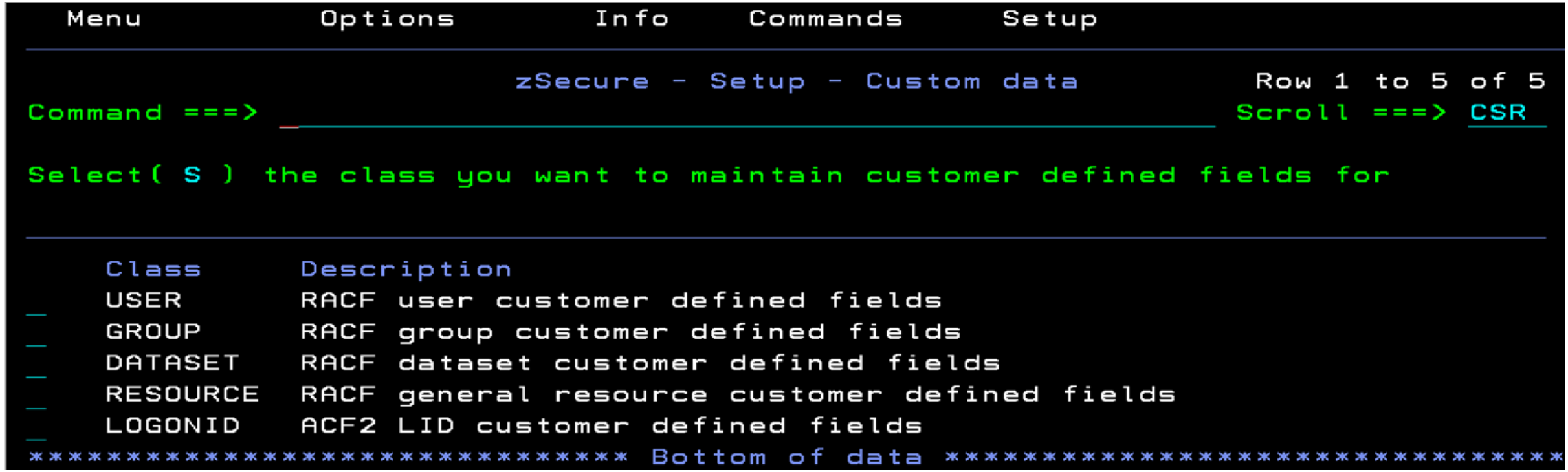
Custom data support

The SE.6 Instdata option allowed defining substrings from installation data to display with the various profile displays.

This now becomes a Custom data option where you can add custom data fields to those profile displays.

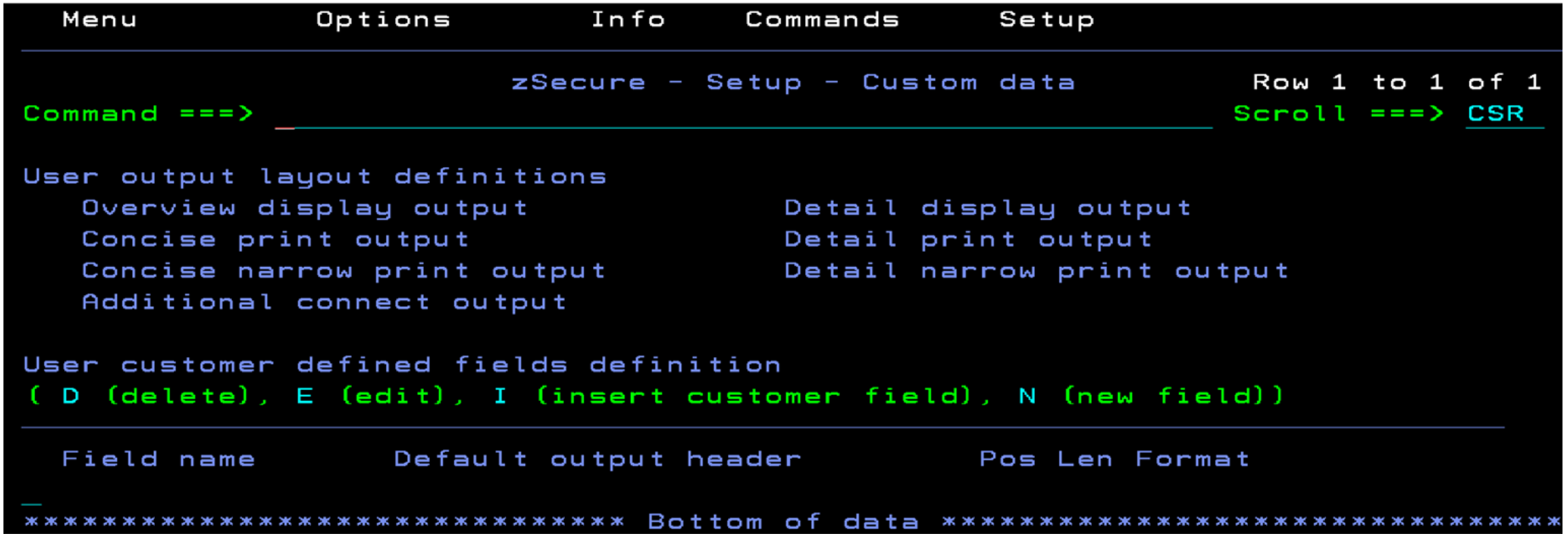
- Underlying, there have been substantial updates to the engine support for DEFINE statements, where the target can more often be another DEFINE.

SE.6 extended custom data fields customization



- Put an **S** in front of **USER**

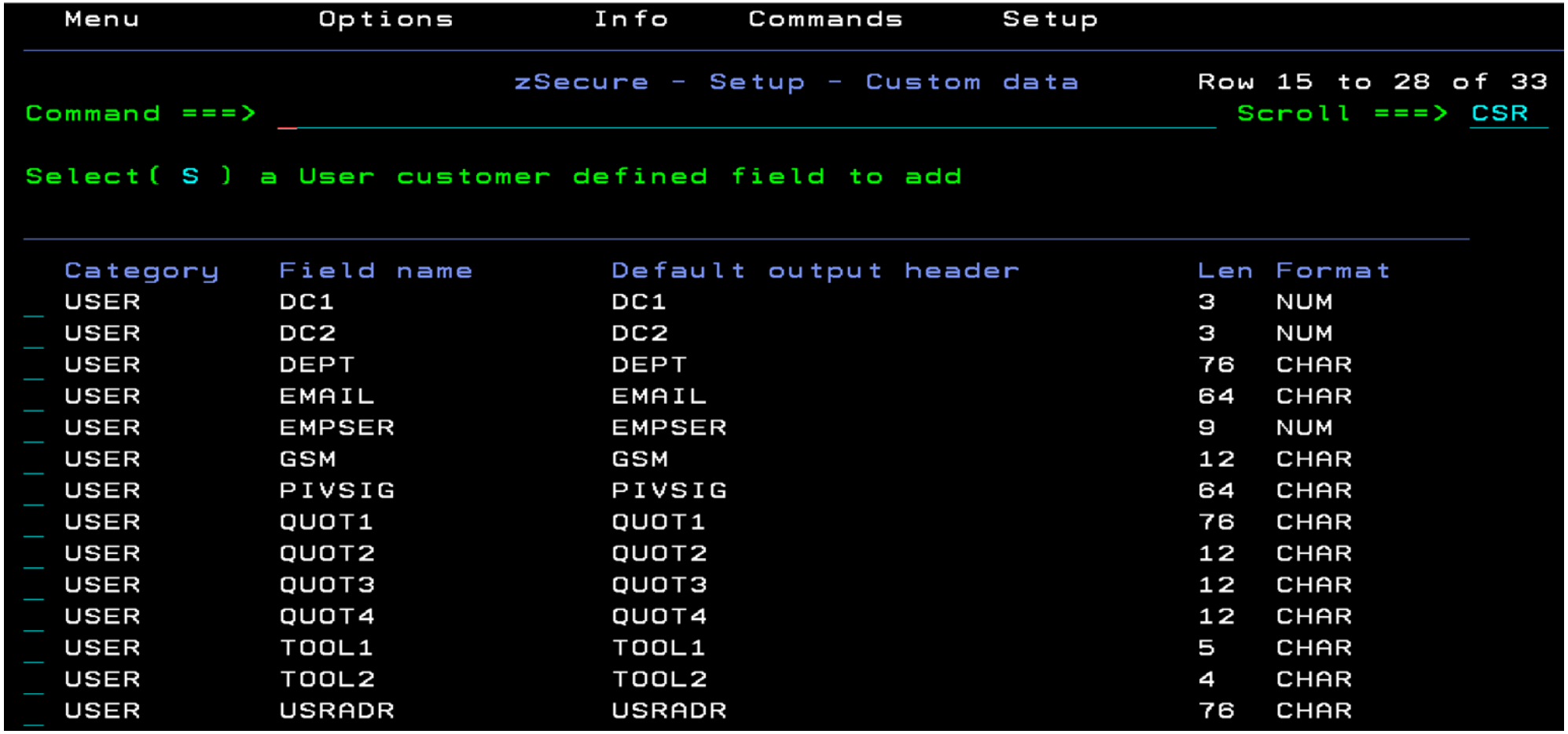
SE.6 - Add fields to USER display



- Put an **I** below **Field name** to add a field definition

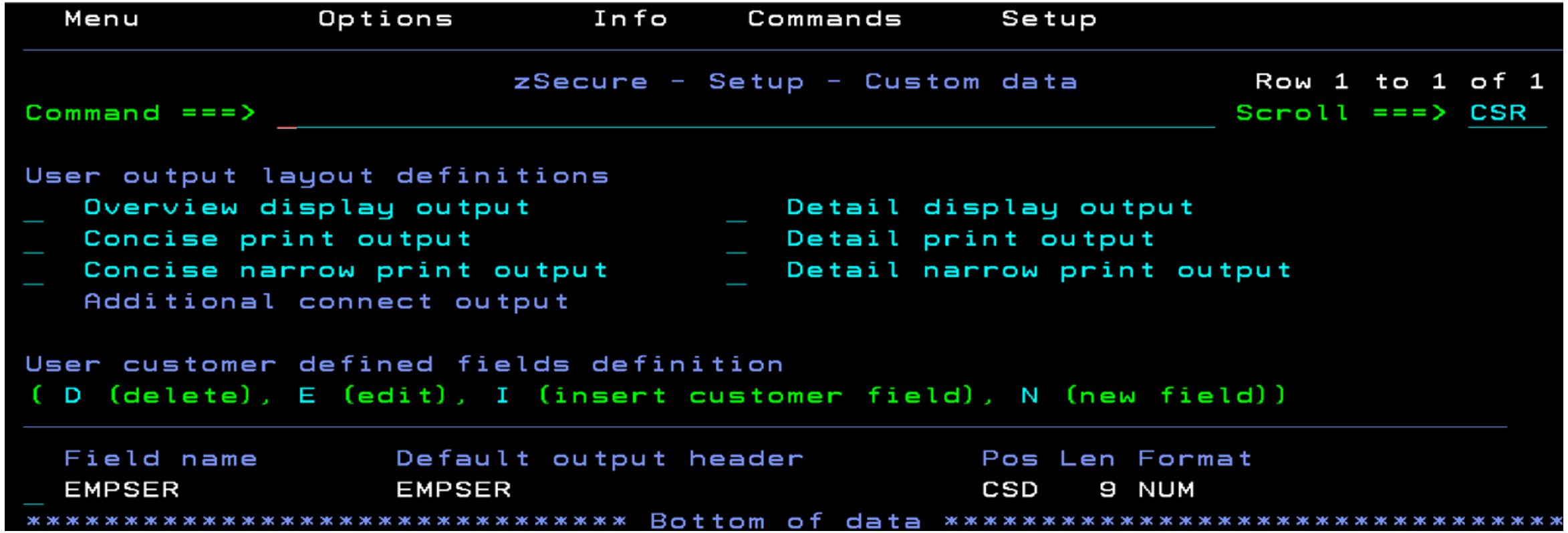
SE.6 - Adding custom fields

- Put an **S** in front of **EMPSER**



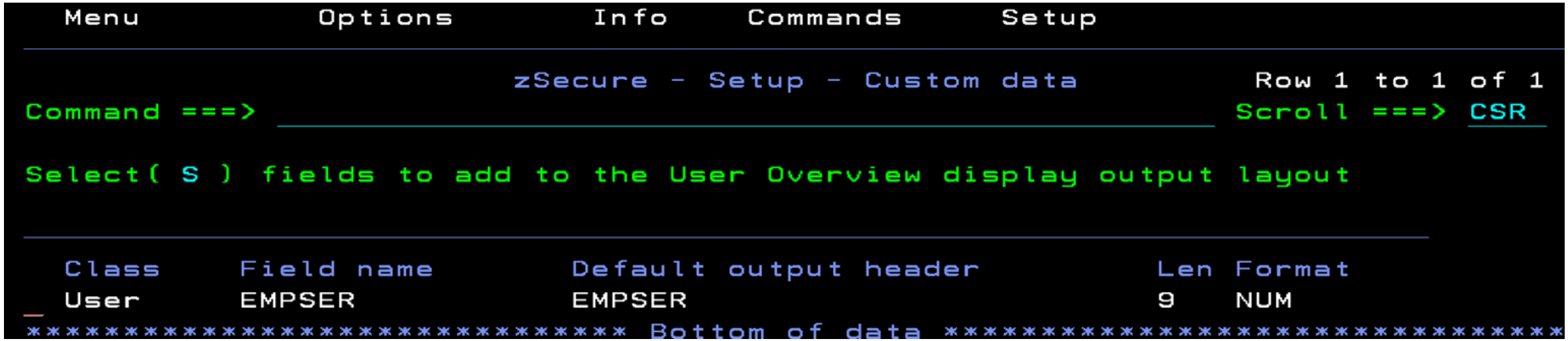
Press **PF3** when done adding fields

SE.6 - Adding custom fields to USER display layouts (1)



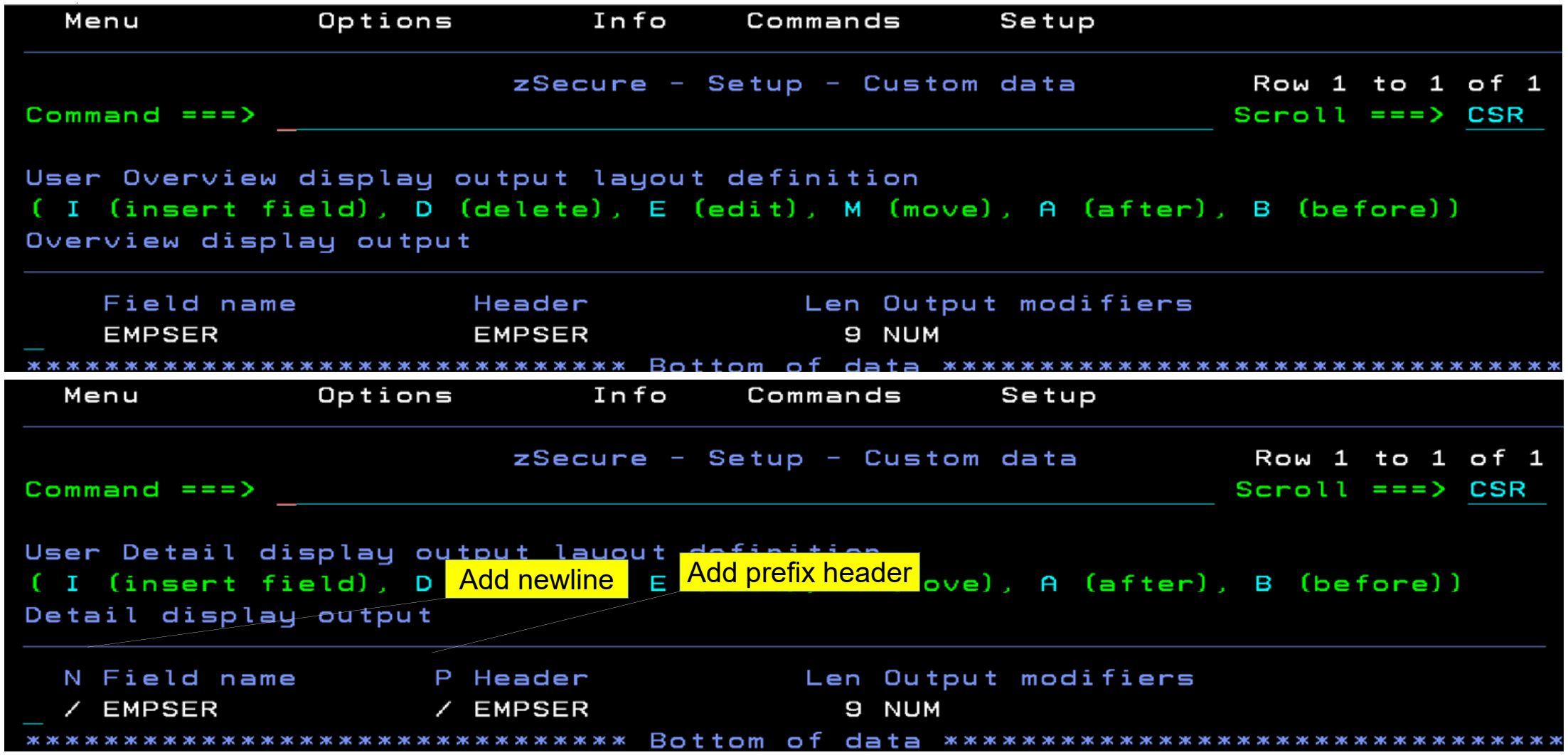
Put a **/** before **Overview display output** and **Detail display output**

SE.6 - Adding custom fields to USER display layouts (2)



Put an **S** before the EMPSER field

SE.6 overview and detail for USER layout



RA.U overview and detail enriched

```
                  zSecure USER CRMBRL1 overview                    Line 1 of 1
Command ===>                                                  Scroll===> CSR
Users like CRMBRL1                                    7 Jul 2025 23:45
   User      ClAut Link #Cert #Maps PEPEM AG Pri EMPSER    Home directory
__ CRMBRL1    _    0    1      3      1 P P M __   10 50294788 /home/CRMBRL1
********************************* Bottom of Data ********************************
```

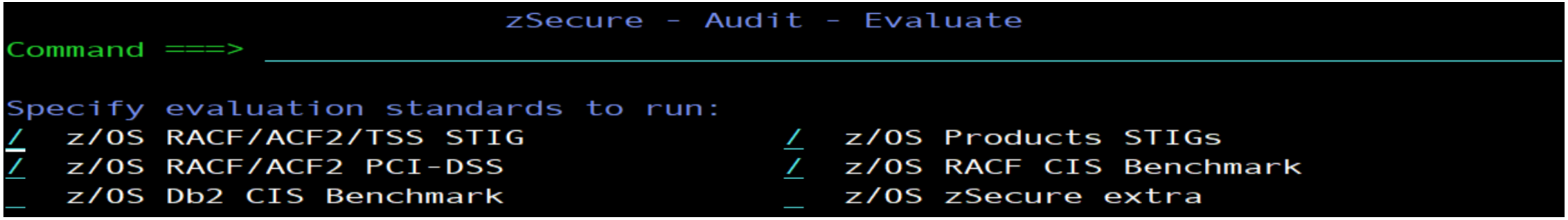
```
                  zSecure USER CRMBRL1 overview                   Line 1 of 201
Command ===>                                                  Scroll===> CSR
Users like CRMBRL1                                    7 Jul 2025 23:45


_ Identification of CRMBRL1                                          NMPIPL87
  User name                          RONALD VAN DER LAAN
  EMPSER                             50294788
_ Owner                              CRMB                  CRM WERKNEMERS
_ User's default group               CRMB                  CRM WERKNEMERS

  Group    Auth     R SOA AG Uacc     Revokedt     Resumedt     DEPT
_ #TEST2   USE      _ SOA   NONE                                
_ CRMB     USE      _ SOA   NONE                                TEST
```

Group custom data

Compliance standards

Compliance standards - ISPF

In the ISPF UI, standards can be found under AU.R (Rule-based audit)



The most important ones are the Security Technical Implementation Guides and Center for Internet Security benchmarks.
Current STIG levels are 9.4 (z/OS) and variable 6.*x*/7.*x* (Products).
Current CIS levels are 1.1 (RACF) and 1.0 (Db2).
Coverage for RACF is 90% or more (and increasing), ACF2 close behind.

Every quarter a STIG update is released (usually a few weeks after the Defense Information Systems Agency publishes their newest releases).

The Db2 CIS Benchmark requires a zSCC entitlement.

New Db2 report types

Underlying report types **DB2_CONTEXT** and **DB2_ROLE**:

- Objects with their authids from Db2 SYSCONTEXT, SYSCONTEXTAUTHIDS, and SYSCTXTTRUSTATTRS, resp. objects from Db2 SYSROLES
- Sample CARLa members CKCDQDZ and CKCDQDI
- These require a zSCC entitlement
- Not added to the UI yet

DB2_CONTEXT

Record and detail level displays:

```
Command ===>            DB2 context display                                                                                          Scroll===>
                                                                                                                         13 Jul 2025 23:45
   Complex   System   DB2I Count
   NMPIPL87 ZS14      DBD1        15
   DB2I Trusted context    SysAuthid    O Definer   D Default role Dflt sec lab Ena AlP AuP Encrypt   Encrypt created Created          Altered           Remarks
__ DBD1 CRMBCTX1           CRMBJK1      L CRMBJK2     CRMBROLE                   Yes No  No                            6Feb2025 07:34   6Feb2025 07:34
__ DBD1 DB2CTXGR           DB2            CRMBJK2                                Yes No  No  HIGH     13Feb2025 09:11 13Feb2025 09:11  13Feb2025 09:11
__ DBD1 TRUSTCN1           AUTHID1      L CRMBJK2     ROLE1                      Yes No  No                            5Feb2025 12:10   5Feb2025 12:10
__ DBD1 TRUSTCN2           AUTHID2      L CRMBJK2     ROLE2                      Yes No  No                            5Feb2025 12:10   5Feb2025 12:10
__ DBD1 TRUSTCN3           AUTHID3      L CRMBJK2     ROLE3                      No  No  No                            5Feb2025 12:10   5Feb2025 12:10
__ DBD1 TRUSTCN4           AUTHID4        CRMBJK2     ROLE4                      Yes No  No  HIGH      5Feb2025 12:10  5Feb2025 12:10   5Feb2025 12:10
__ DBD1 TRUSTCN5           AUTHID5      L CRMBJK2     CRMBROLE     LABEL5        Yes No  No                            5Feb2025 12:10   5Feb2025 12:10
__ DBD1 TRUSTCN6           AUTHID6      L CRMBROLE L  ROLE1                      Yes No  No                            6Feb2025 07:39   6Feb2025 07:39
__ DBD1 TRUSTCN7           AUTHID7        CRMBJK2                                Yes No  No                           12Feb2025 14:56  12Feb2025 14:56
__ DBD1 TRUSTCN88          AUTHID88       CRMBJK2                                Yes No  No  HIGH      7May2025 11:14  7May2025 11:14   7May2025 11:35
__ DBD1 TRUSTCN89          AUTHID89       CRMBJK2                                Yes No  No  HIGH      7May2025 11:12  7May2025 11:12   7May2025 11:12
__ DBD1 TRUSTCN8           AUTHID8        CRMBJK2                                Yes No  No  HIGH      7May2025 11:10  7May2025 11:10   7May2025 11:10
__ DBD1 TRUSTCN9           AUTHID9        CRMBJK2                                Yes No  No                            7May2025 11:10   7May2025 11:10
__ DBD1 TRUSTCNA           AUTHIDA        CRMBJK2                                Yes No  No                            7May2025 11:12   7May2025 11:12
__ DBD1 TRUSTCNB           AUTHIDB        CRMBJK2                                Yes No  No                            7May2025 11:14   7May2025 11:14
****************************************************************************** Bottom of Data ******************************************************************************
```

```
Command ===>           DB2 context display                                                                                          Line 1 of 21
                                                                                                                                     Scroll===> CSR
                                                                                                                   13 Jul 2025 23:45


  AUTHID    AAu AUTHID Role          Authid Seclabel          Authid creation timestamp           Authid creation timestamp DB2         Authid List
  &CRMBJK5  Yes ROLE2                LABEL88                    7 May 2025 11:35:13.00            2025-05-07-11.35.13                   CRMBJK5
  &CRMBJK4  Yes ROLE2                                           7 May 2025 11:35:13.00            2025-05-07-11.35.13                   CRMBJK4
  &CRMBJK3  Yes ROLE2                                           7 May 2025 11:35:13.00            2025-05-07-11.35.13                   CRMBJK3
  &SYSPROG  Yes ROLE2                                           7 May 2025 11:35:13.00            2025-05-07-11.35.13                   CRMBNAI CRMBSRU CRMBJK99
  &DB2CTX   Yes ROLE3                                           7 May 2025 11:14:33.00            2025-05-07-11.14.33                   CRMBJKA CRMBJKB

  IP address   IP address creation timestamp       IP address creation timestamp DB2
  9.88.7.4      7 May 2025 11:14:33.00             2025-05-07-11.14.33
  9.88.7.5      7 May 2025 11:14:33.00             2025-05-07-11.14.33
  9.88.7.6      7 May 2025 11:14:33.00             2025-05-07-11.14.33

  Jobname      Jobname creation timestamp          Jobname creation timestamp DB2


  SERVAUTH     SERVAUTH creation timestamp         SERVAUTH creation timestamp DB2
  SERVCN6M      7 May 2025 11:14:33.00             2025-05-07-11.14.33
  SERVCN6L      7 May 2025 11:14:33.00             2025-05-07-11.14.33
  SERVCN6K      7 May 2025 11:14:33.00             2025-05-07-11.14.33
****************************************************************************** Bottom of Data ******************************************************************************
```

DB2_ROLE

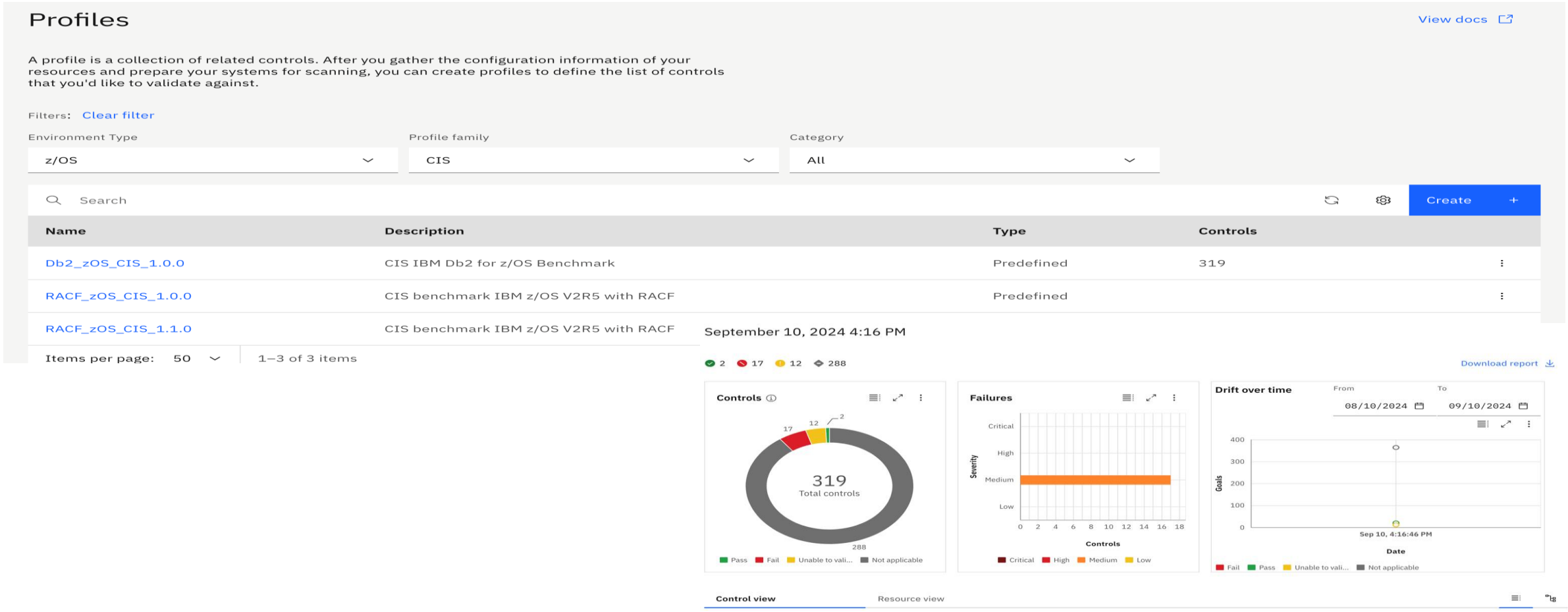
Record and detail level displays:

```
                    DB2 roles display
Command ===>

   System    DB2I Count
   ZS14      DBD1          7
   Role                                Complex   Created           System
___ CRMBROLE                           NMPIPL87 12Jan2024 11:24 ZS14
___ ROLE1                              NMPIPL87  5Feb2025 11:57 ZS14
___ ROLE2                              NMPIPL87  5Feb2025 11:57 ZS14
___ ROLE3                              NMPIPL87  5Feb2025 11:57 ZS14
___ ROLE4                              NMPIPL87  5Feb2025 11:57 ZS14
___ ROLE5                              NMPIPL87  5Feb2025 11:57 ZS14
___ ROLEMC1                            NMPIPL87 23May2025 15:13 ZS14
********************************************************************** Bottom of Data **
```

```
                    DB2 roles display
Command ===>


  DB2 object
  DB2 ssid system complex ver    DBD1 ZS14      NMPIPL87

  Role
  Role name                      ROLE4

  Role attributes
  Authid of role definer         CRMBJK2
  Definer type (L for role)
  Remarks

  Statistics
  Creation timestamp              5Feb2025 11:57
  Release created                Db2 13
********************************************************************** Bottom of Data **
```

Compliance standards – zSCC dashboard

IBM Z Security and Compliance Center provides a compliance dashboard.



IBM Z Security and Compliance Center

IBM Z Security and Compliance Center 1.3

This product is to some extent built on zSecure Audit 3.2 infrastructure.
The STIG and CIS standard evaluations are “sent over” to the dashboard.

In addition to the FMIDs provided from ShopZ, container images are provided to install under RedHat OpenShift or zCX.

The product follows a “continuous delivery” model.

zSCC – March 2025 update

Custom Goals for Indepent Software Vendors and Users

- ISVs can now define their own subtypes for SMF 1154 (z/OS compliance evidence) and surface evidence in zSCC through the Common Data Provider component, and create goals associated to their subtype for z/OS based environments. Creating new goals support is also provided for existing users of zSCC (privileged users).

IBM Concert integration

- An automated OSCAL feed of zSCC compliance evaluation results is sent to IBM Concert

IBM Threat Detection for z/OS

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

SMF 83-8 is the “anomaly detected” record from TDz.

The z/OS Compliance Integration Manager [3.2] component of zSCC 1.3 now writes SMF 83-8 recording activity into SMF 1154-97 records.

This recording activity is shown in the EV(ents) menu (zSecure Audit/zSCC).

Ideas

CL/SuperSession SMF support

CL/Supersession writes multiple events into a single SMF record, that with current CARLa support cannot really be extracted. ZAUDIT-I-263

zSecure Audit (and Adapters/zSCC) adds support to process these SMF records (“creating multiple records from a single record”).

Add appropriate selection capabilities in the UI. Menu option EV.A.S.

- Back-ported to zSecure 3.1. Available. PTF UJ97479.

  Technote https://supportcontent.ibm.com/support/pages/zsecure-audit-31-added-smf-record-support-zsecure-carla-ibm-clsupersession

Display Command Audit Trail in zSecure Admin

zSecure Command Verifier puts audit data into updated RACF profiles.

This information is stored in USRDATA fields, but zSecure Admin does not format the data in a readable fashion.

This $C4R-data will now be formatted in the same format as it would be shown with LISTUSER etc.

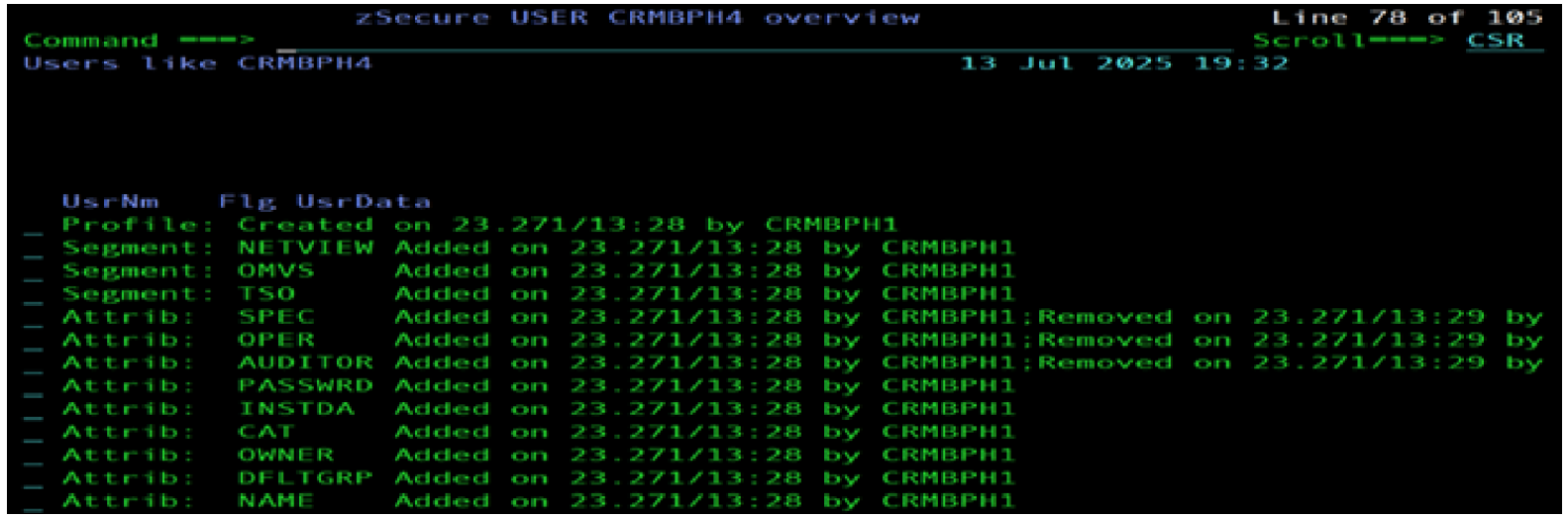
[ZSECURE-I-53](#)

[ZSECURE-I-60](#)

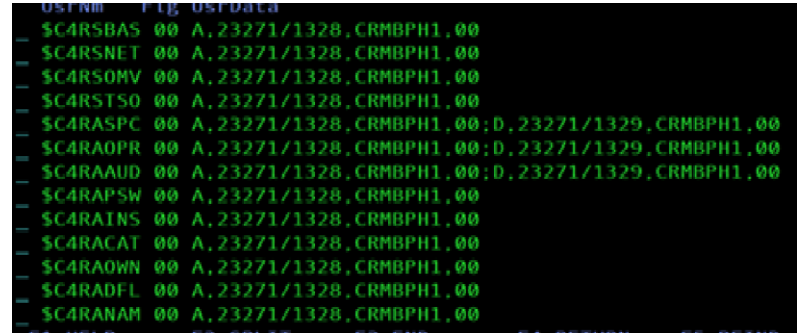
[ZSECURE-I-132](#)

[ZSECURE-I-236](#)

[ZSECURE-I-425](#)



Old layout:



Other Ideas

ZSECURE-I-272 Access Monitor: select on Profile Owner for DATASET/RESOURCE

ZSECURE-I-567 Show complete installation data for connections and subgroups in RA.U/G

ZAUDIT-I-388 Explain impact of message CKR1403

ZSECURE-I-581 Option to select on physical UNIX attributes as opposed to effective ones in RE.U.F

ZSECURE-I-579 Resource Copy panel for wide screen (62x160)

ZAUDIT-I-328 Lookup of DB2 fields to RACF

ZALERT-I-93 Alert on buffer pool resources (BP0) under ACF2 option for Db2.
Also alert on granting Db2 admin privileges.

Subject: Alert: SYSADM Authority granted by CRMBRT1

```
Alert: SYSADM Authority granted by  CRMBRT1
ACF2 for Db2 command used to grant SYSADM Authority

   Alert id        2618
   Date and time   20Mar2025 21:15:36.79
   Type            SYS
   DB2ID           RENB
   Rule entry      UID(CRMB    CRMBRT2) PREVENT
   Rule entry      UID(CRMB    CRMBRT4) LOG
   Rule entry      UID(CRMB    CRMBRT5) ALLOW
   User            CRMBRT1  RENE VAN T TE Z
   Job name        CRMBRT1
   System id       ZS49
```

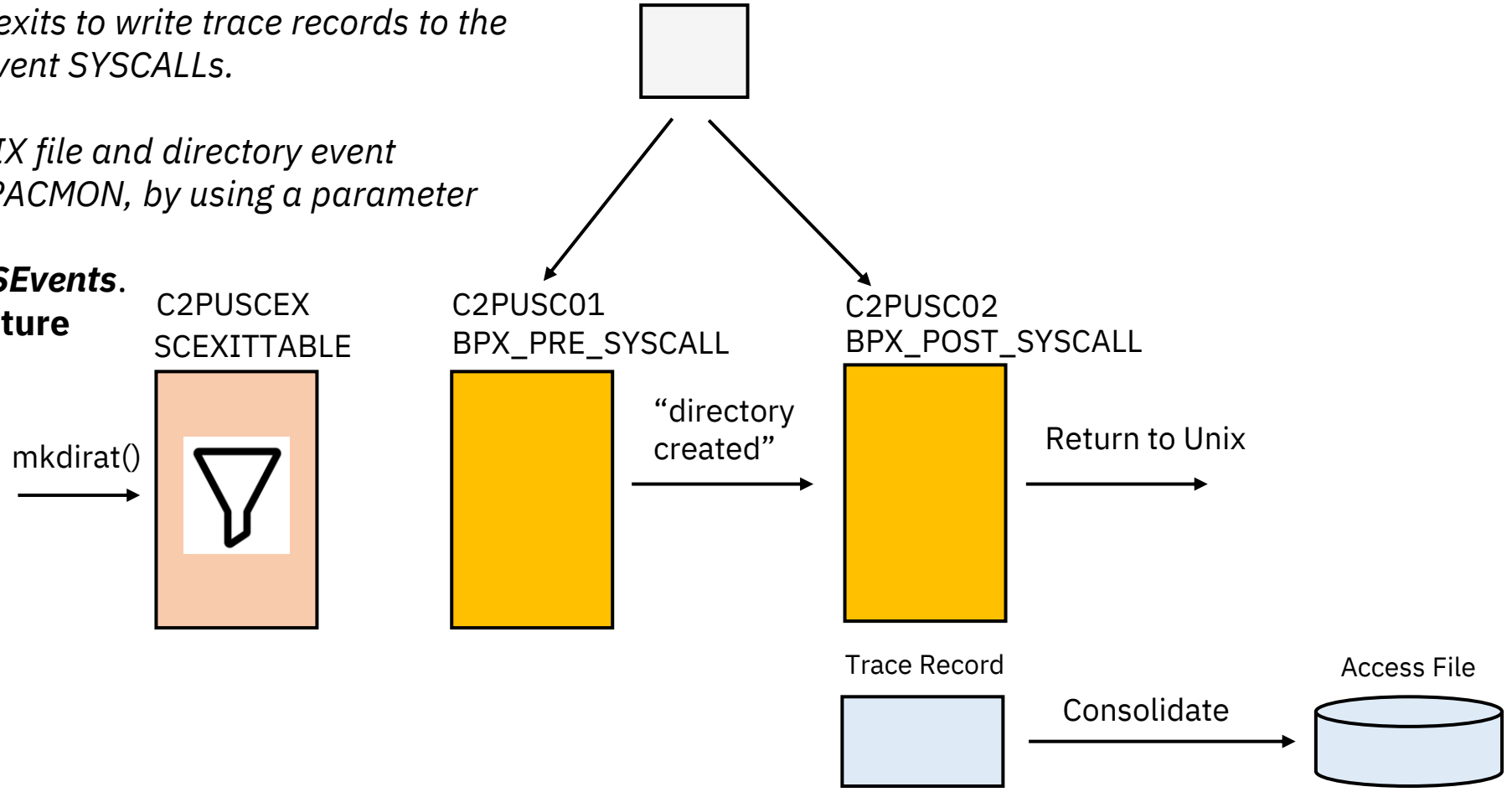
Access Monitor – UNIX

Access Monitor – capturing UNIX events

Access Monitor uses the BPX_PRE_SYSCALL and BPX_POST_SYSCALL exits to write trace records to the AM buffers, not to prevent SYSCALLs.

To start collecting UNIX file and directory event information, start C2PACMON, by using a parameter file with

***OPTION CaptureUSSEvents*.**
DIAGNOSE USSCapture



971	93 Unix	ZS17	mkdirat	15	0	/home/crmbph1/dir41

Access Monitor – new UNIX syscalls

Example SCEXITTABLE

A substantial set of syscalls has been added of the form *at(), for example, openat(), mkdirat() etc.

These take a file descriptor and a relative pathname.

```
VIEW       CRMA.D.ZSSDEV.$BASE.SCKRSAMP(C2PUSCEX) - 01.17
Command ===>
000018 /* 250618 3.2.0 PH  L0001649: Add new unix syscalls
000019 /*************************************************
000020 BPX1ACC    /* access             */
000021 BPX1ATM    /* attach_execmvs     */
000022 BPX1ATX    /* attach_exec        */
000023 BPX1CHA    /* chaudit            */
000024 BPX1CHD    /* chdir              */
000025 BPX1CHM    /* chmod              */
000026 BPX1CHO    /* chown              */
000027 BPX1CHR    /* chattr             */
000028 BPX1CMA    /* fchmodat           */
000029 BPX1COA    /* fchownat           */
000030 BPX1CRT    /* chroot             */
000031 BPX1EXC    /* exec               */
000032 BPX1EXM    /* execmvs            */
000033 BPX1EXT    /* extlink_np         */
000034 BPX1FAA    /* faccessat          */
000035 BPX1FCD    /* fchdir             */
000036 BPX1FSA    /* fstatat            */
```

The BPX1 prefix is for 31-bit calls; 64-bit calls use BPX4.
You need to specify only one form--both calls are captured.

TYPE=ACCESS field UNIX_EVENT

Validation

Installation & Configuration

- The zSecure 3.2 base level will be provided
  - This includes a file in the SCKRPAX data set that contains the z/OSMF plug-in that is the zSecure Admin Web UI
- Be aware that the 31-bit version CKR4Z196 of the engine is no longer there. Instead, there is now a CKR8Z15 that should work better for z15 and up.
- For zSCC 1.3, container images need to be obtained separately, per the memo distributed via ShopZ

Summary

- zSecure 3.2 is required for full support of z/OS 3.2. Incremental updates will be made in a number of code drops.
- zSecure Visual is reaching end of marketing. The future of RACF administration is a Web UI that is being developed as part of zSecure Admin. Design iterations are in full swing, this is a good time to chime in.
- RACF and z/OS currency support are core business for zSecure.
- For zSCC and zSecure Audit compliance standards are quite important.