

# Access Elevation

Marco Egli, October 2023



## Table of Contents

Rational for Access Elevation	03
Elevated Access Management	04

# Rational for Access Elevation

- Reduce Timeframe where user has highest privileges
- Automated Reporting over high privileged groups
- Remove high access for software installation in Production as only needed in Maintenance

# Elevated Access Management

- ISPF based
- Maximum elevation time is 2 hours
- RITM number required for elevation
- Automatic removal process every hour
- Per RACF environment (according to RRSF synch setup)

# Elevated Access Management – ISPF application – request access

If this field is empty when one hits enter, it offers a list of available groups for elevation.

If this field is empty your userid will be used by default.

Maximum duration for the elevation is 2 hours.

RITM number must be provided as evidence that the elevation is used for a task that requires that elevated access.

```
Elevated Access Management
Option ==> 1
blank Display group
1 Request access
2 Refresh connect group(s)
Enter selection values below:
Group . . . . . ACCELUSS (blank for selection list, * to Refresh all)
User id . . . . . SRZOEG (leave blank for yourself)
Duration . . . . . 2 hrs (max 2 hours)
Request ticket . RITM12345678 (e.g., RITM00000000)
```

# Elevated Access Management – ISPF application – show current elevations

Add a group name or select one when the group name is empty.

```
Elevated Access Management
Option ==> _____
blank Display group
1 Request access
2 Refresh connect group(s)

Enter selection values below:
Group . . . . . ACCELUSS      (blank for selection list, * to Refresh all)
User id . . . . . _____ (leave blank for yourself)
Duration . . . . . ___ hrs   (max 2 hours)
Request ticket . _____ (e.g., RITM00000000)
```

Confirmation by hitting enter shows all current active elevations.



Displays the list of all current elevated users from the selected group.

```
Elevated Access Management
Option ==> _____

Group status for ACCELUSS

$ User      Name      Ticket      Hr Asked by Start      Status
_ SRZOEGLI MARCO  RITM12345678 2 SRZOEGLI 02Sep2020 15:03 Active
***** Bottom of data *****
```

# Elevated Access Management – zSecure – show current elevations

- zSecure shows the queued commands that triggered the RACF group connect (red box).
- zSecure shows the queued command that will be executed by the hourly scheduled Job (blue box).

```
Identification
RACF group name ACCELUSS
Superior group $RAK_____ STRUCTURAL OWNER GROUP FOR APPLICATION RACF(STANDARD PREFIX RAK) - NO AUTHORIZATIONS PERMITTED FOR THIS GROUP
Owner $RAK_____ STRUCTURAL OWNER GROUP FOR APPLICATION RACF(STANDARD PREFIX RAK) - NO AUTHORIZATIONS PERMITTED FOR THIS GROUP
Security Class PRIVILEGED_____
Install Data ACCESS ELEVATION TESTING - USER

User/Grp Auth R SOA AG Uacc Revokedt Resumedt Name RI DfltGrp InstData
SRZDEG USE - - - NONE - - EGLI MARCO USRUSR 501333332

Safeguards
Terminal use authorization No
Universal access authority NONE
Data set model profile name

Statistics
Creation date 10Jun20
Universal group No

UsrNm Flg UsrData
$C4RAINS 00 A,20162/0552,SRZDEG,00
$C4RAOWN 00 A,20162/0552,SRZDEG,00
$C4RASPG 00 A,20162/0552,SRZDEG,00

Timed commands waiting for execution
Queued command (PR): CMD AT 03Sep2020 REASON('RITH12345678 HRS(2)') REMOVE SRZDEG OWNER(ACCELUSS) GROUP(ACCELUSS); pending reverse by SRZDEG at 2 Sep 2020

Commands that have been executed
Queued command (X): CMD AT 02Sep2020 FOR 1 REASON('RITH12345678 HRS(2)') CONNECT SRZDEG GROUP(ACCELUSS); request by SRZDEG at 2 Sep 2020 15:03; executed by
```

## Elevated Access Management – Successful access request

- A successful requests with the details from the previous slide will result
  - in a WTO

```
14000000 CH01MSYS 20246 15:03:44.89 T0788850 00000090 +SR-ACCESS-ELEVATION FOR SRZOEK TO ACCELUSS FOR 2H SRZOEK  
00000000 CH01MSYS 00015 15 00 50 00 00788850 00000090 TWT014T TWT014T REQUEST FOR STRUCTURE CVC000 USV01 BCL 774
```

- in a E-Mail Alert



The screenshot shows an email alert with the following content:

**SR-ACCESS-ELEVATION FOR SRZOEK TO ACCELUSS**

To  Marco Egli

Retention Policy SR-DPT-DeleteAll-35YR (3 years, 6 months)

---

User SRZOEK requested elevated access to ACCEL USS USER.  
A temporary connection to ACCELUSS was made for 2 hour(s).  
Request ticket RITM12345678, see <http://go/snow/RITM12345678>



## Elevated Access Management – Hourly Clean-up Job

- An hourly scheduled Job will execute all the queued commands as shown on the zSecure Panel for a selected elevation group.

```
CKG105I 00 NO SYSTEM ATTACHED  
Parm: REFRESH GROUP ACCELUSS  
  
CKG106I 00 Starting command: CKGRACF REFRESH GROUP ACCELUSS  
Input: CKGINPDC STORAGE INPUT AREA  
  
1 |CMD AT 03Sep2020 REASON('RITM12345678 HRS(2)') REMOVE SRZDEG OWNER(ACCELUSS) GROUP(ACCELUSS)  
REMOVE SRZDEG OWNER(ACCELUSS) GROUP(ACCELUSS)  
C4R913I REMOVE SRZDEG OWNER(ACCELUSS) GROUP(ACCELUSS)  
CKG111I 00 Highest result code was 0  
BOTTOM OF LIST
```

## Elevated Access Management – Important note

- Only Groups in the RACFVARS Profile &ACCELEV can be used for elevation.
- Elevation to such a privileged group can only be requested by specified groups.
- All based on zSecure (Command Verifier) with profiles in CL(XFACILIT)
  - CKG.CMD.CMD.REQ.CONNECT|REMOVE
  - CKG.SCP.G.INFRA.\$RAK.RAKPUSSA
  - CKG.SCP.ID.RAKPUSSA.\* -> only permit here the group that shall be able to elevate
  - C4R.CONNECT.ID.&ACCELEV.=RACUID
- Own written solution just because zSecure offers only calendar day elevations
  - Vote for idea to support hour granularity: [ZSECURE-I-247](#)

”

You do not lose  
access, you will have  
it for a limited time.



Any questions?



# Legal notice

©2020 Swiss Re. All rights reserved. You may use this presentation for private or internal purposes but note that any copyright or other proprietary notices must not be removed. You are not permitted to create any modifications or derivative works of this presentation, or to use it for commercial or other public purposes, without the prior written permission of Swiss Re.

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.