SAP Governance, Risk & Compliance
Access Control 5.3

Post-Installation
→ Superuser Privilege Management

Authors – SAP GRC RIG Team

Frank Rambo, SAP GRC RIG, EMEA Region

Frank Bannert, SAP GRC RIG, EMEA Region

- We belong to the GRC Regional Implementation Group (RIG) located in USA, Germany and India
- As recognized experts, our mission is to enable others to successfully implement SAP GRC solutions.
- We ensure:
  - high-adoption rates,
  - 100% customer satisfaction, and customer references.
- We are committed to continuous improvement of GRC products and services

RIG Installation Methodology

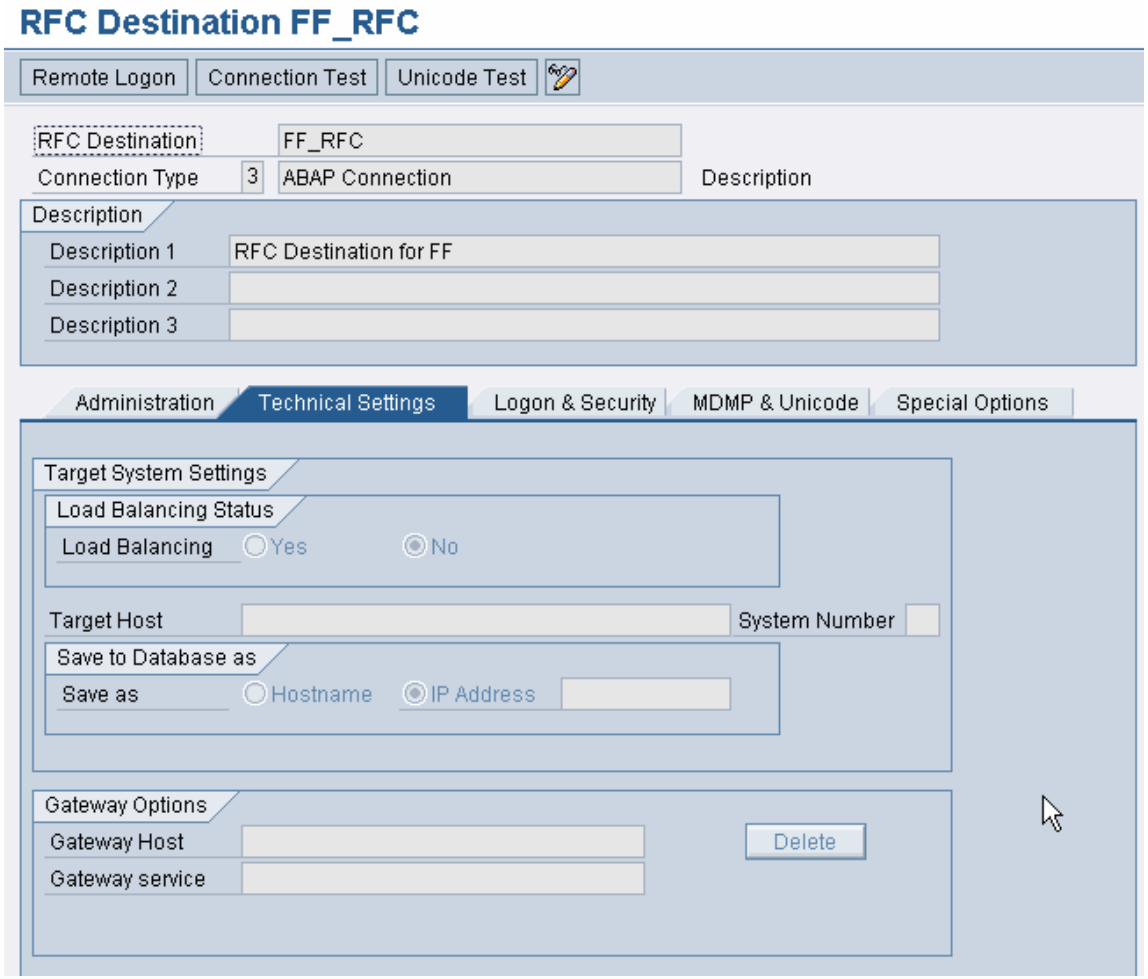
- We recommend the following installation methodology
  1. Install SAP Netweaver AS JAVA 7.0 SP12+
  2. Run Pre-Installation Flash Movie
  3. Deploy Access Control Software (including latest Support Packages)
  4. Run Post-Installation Flash Movies
     a. Post-Installation Risk Analysis and Remediation
     b. **Post-Installation Superuser Privilege Management**
     c. Post-Installation Compliant User Provisioning
     d. Post-Installation Enterprise Role Management
  5. Start Customizing Access Control 5.3 according to customer requirements

Post-Installation Activities Overview
- Superuser Privilege Management -

- Step 1: Configure SPM in each backend
  1. Create RFC Destination in SM59
  2. Schedule Periodic BG Job for Log Report
  3. Create Users
  4. Configure SPM Configuration Table
  5. Create Reason Codes
  6. Convert User IDs into Firefighter IDs
  7. Assign Firefighter IDs to Owners
  8. Assign Firefighter IDs to Firefighter
  9. Assign Firefighter IDs to Controler
  10. Test SPM in SAP Backend System
  11. Test Log Report in Backend System
- Step 2: Configure SPM Frontend Reporting in AC5.3
  12. Create SPM Administrator UME Role
  13. Create JCO in NW for SLD Integration
  14. Create System Connector in SPM Java Frontend
  15. Test SPM Frontend Reporting
- Step 3: Configure SoD Reporting
  16. Change system connector settings in RAR
  17. Start SAP Adapter in RAR
  18. Create TCP/IP RFC Destination
  19. Configure Risk Terminator
  20. Add Connector ID to SPM Configuration
  21. Test SoD Reporting in the SPM Frontend

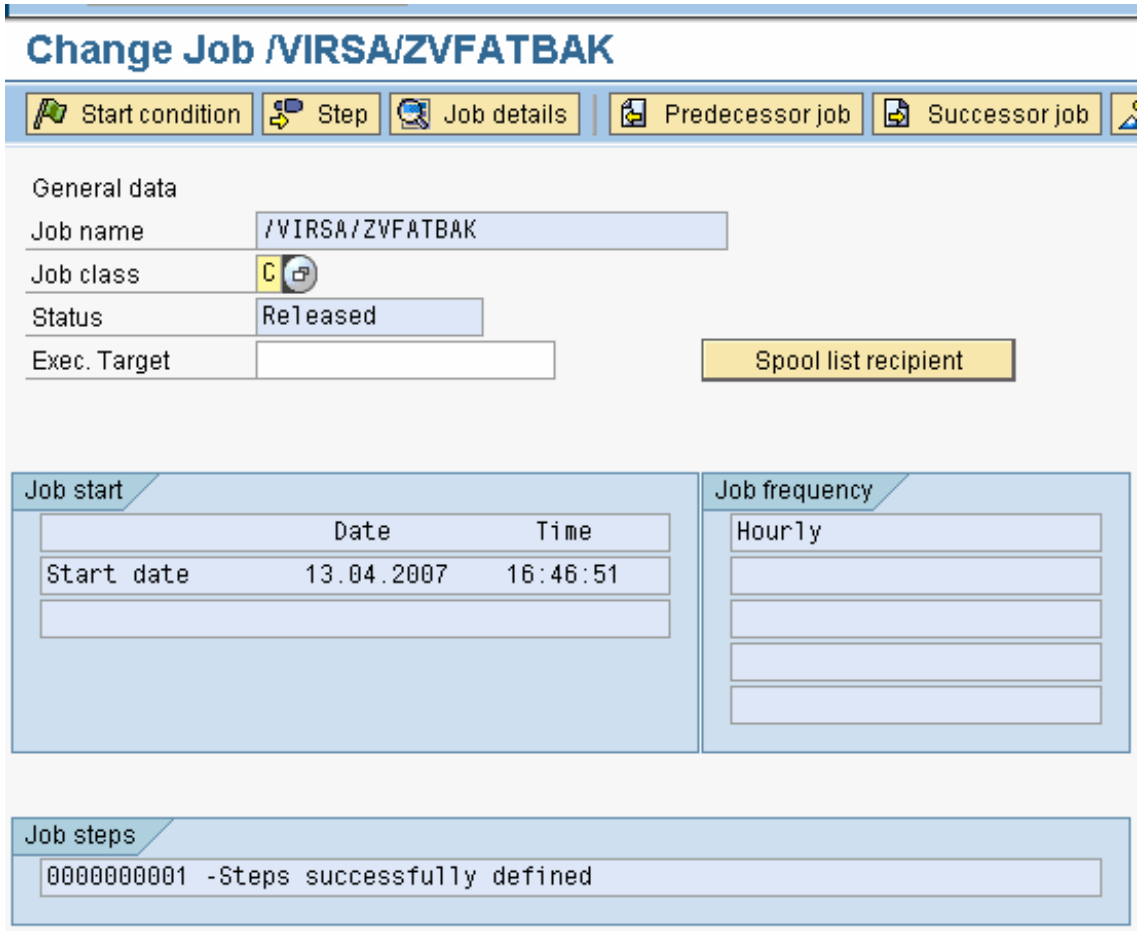
1 – Create RFC Destination in SM59

- Create an RFC destination (ABAP Connection)
- You don‘t need to enter any data into the Logon & Security tab



2 – Schedule Periodic BG Job for Log Report

- Schedule in transaction SM36 a job to run the ABAP report /VIRSA/ZVFATBAK hourly. This report generates the SPM log report.



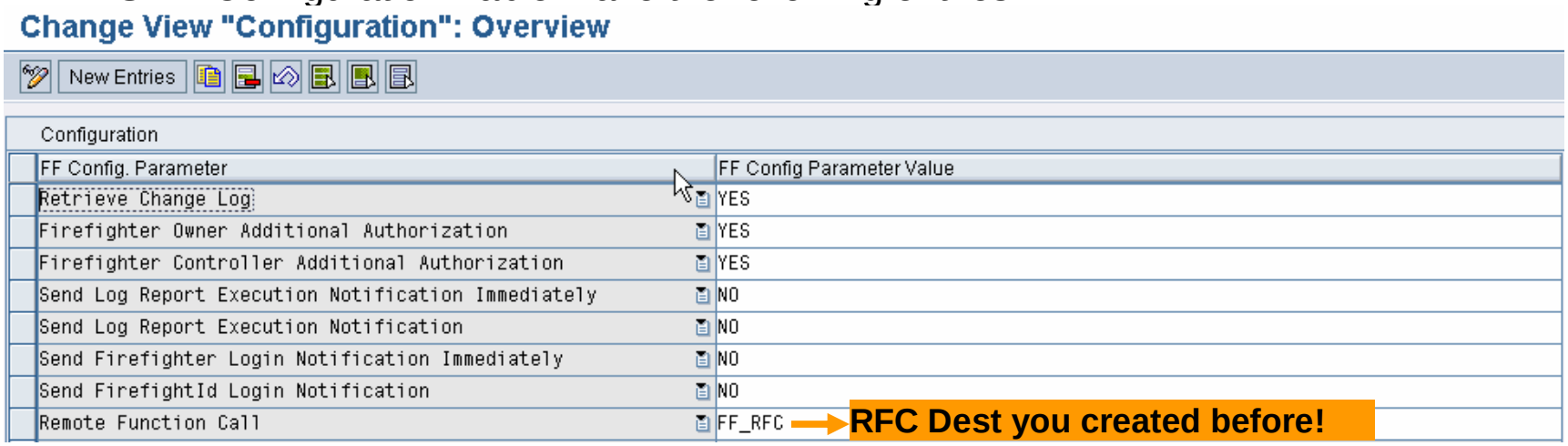
3 – Create Users

- Create the following users:
  - SPM Administrator → Role: /VIRSA/Z_VFAT_ADMINISTRATOR
    - Configuration of Firefighter
    - Assign *Owners* and *Controllers* to Firefighter IDs
    - Maintain *Security Tables*, which requires the knowledge of the passwords of the FireFighterIDs
    - Access to the *Tool Box* containing a number of reports.
  - Owner → /VIRSA/Z_VFAT_ID_OWNER
    - Assign *FireFighterIDs* to *Firefighters*
    - Assign *Controllers* to *FirefighterIDs* they own
  - Controler → /VIRSA/Z_VFAT_ID_OWNER (but with objects GRCFF_0001 & S_TABU_DIS restricted display only!)
    - Check the log report entries the FireFighterIDs they were assigned to.
    - Optionally receive email notifications when a FireFighterID is used.
  - Firefighter ID → Superuser roles (SAP_ALL or „<Module>_ALL“ or other critical roles)
    - Emergency / Superuser ID activated via SPM
  - Firefighter → /VIRSA/Z_VFAT_FIREFIGHTER
    - Regular end user with access to a Firefighter ID in SPM.

4 – Configure SPM Configuration Table

- Logon as SPM Administrator and start transaction /VIRSA/VFAT

- In SPM Configuration Table make the following entries



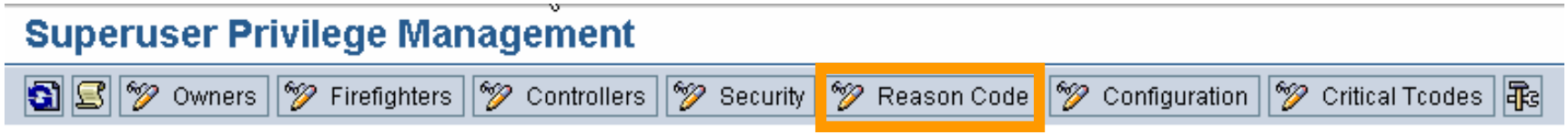
- *Owner Additional Auth. Setting*: Ensures that owners can only manage Firefighter IDs they own.

- *Controler Additional Auth. Setting*: Ensures that controlers can only access log reports of Firefighter IDs they were assigned to.

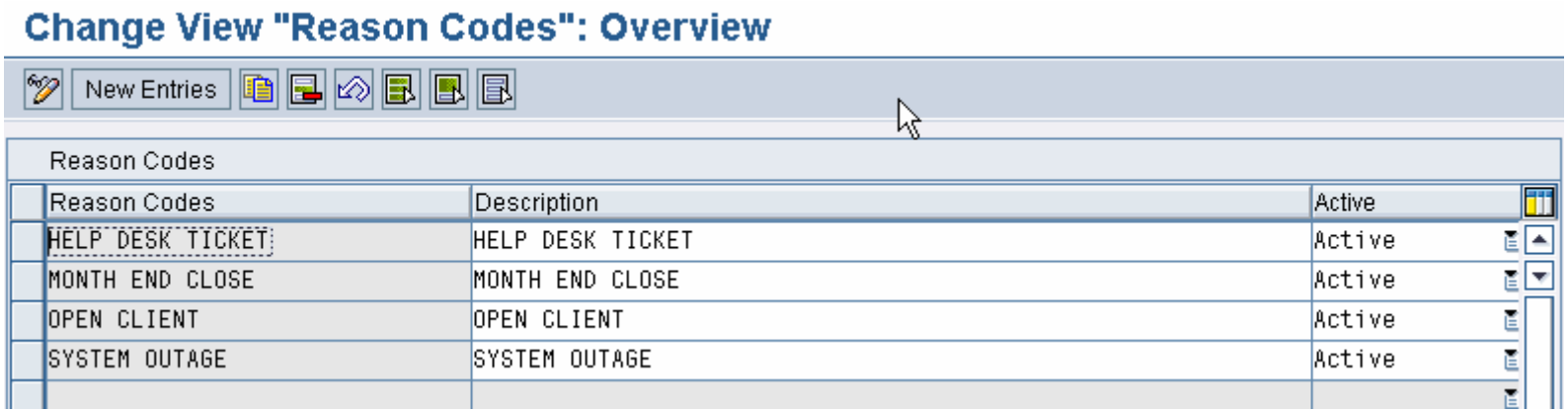
- Change notification settings, if you want to use email notifications

5 – Create Reason Codes

- Logon as SPM Administrator and click in transaction /VIRSA/VFAT on the „Reason Code“ button



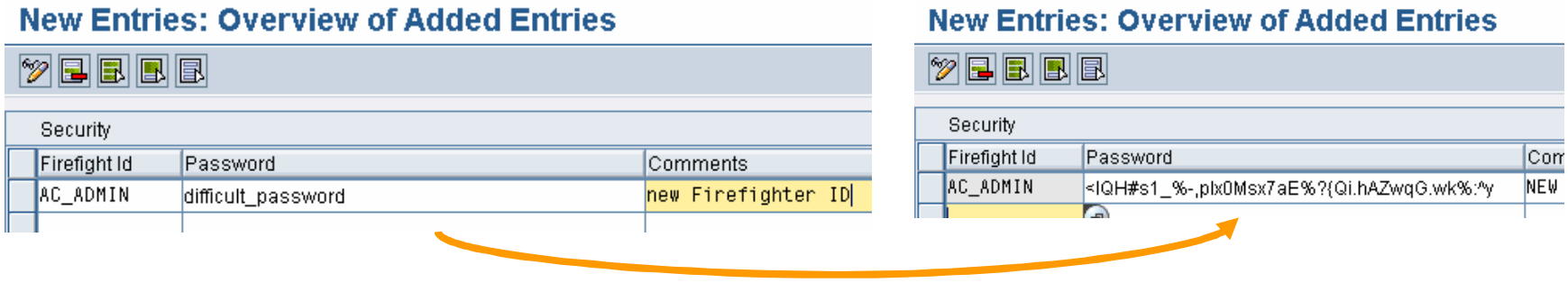
- Then create reason codes which Firefighters will have to select from upon activation of Firefighter IDs that were granted to them.



6 – Convert User IDs into Firefighter IDs: Maintain the Security Table and Apply SAP Note

- Logon as SPM Administrator and click in transaction /VIRSA/VFAT on the „Security“ button

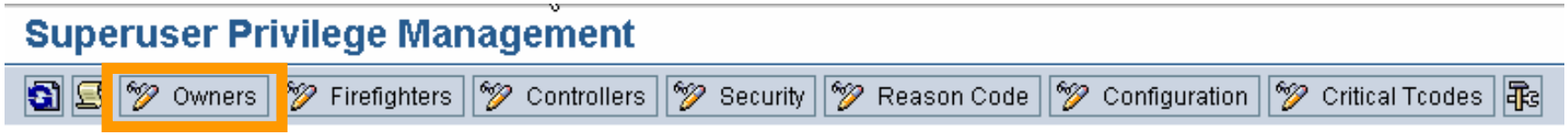
- Then enter the user IDs and their passwords you want to convert into Firefighter IDs. The password will be hashed immediatly. Only Administrators have access to the security table.



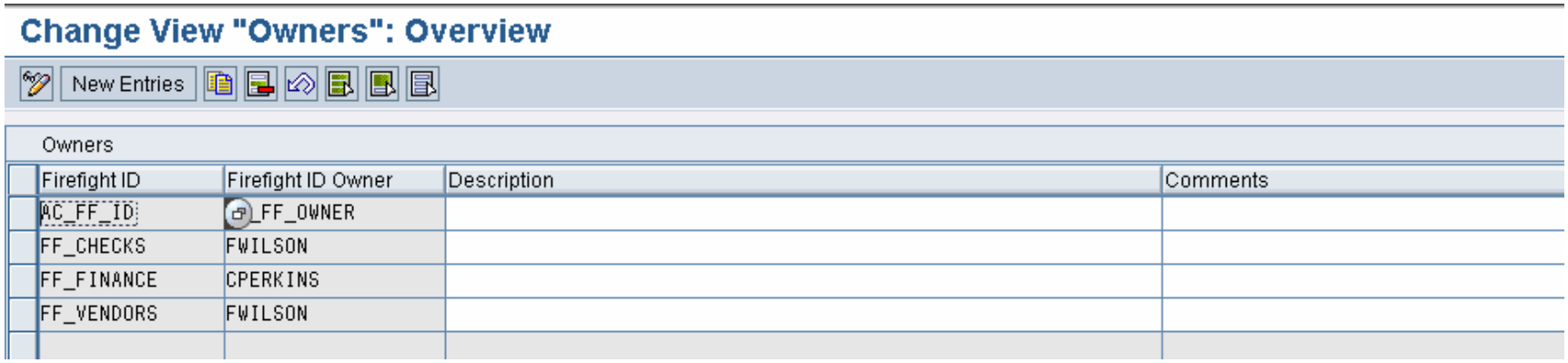
- If you implement SAP note 992200, then Firefighter IDs can‘t logon anymore with their password, but can be accessed only via activation in /VIRSA/ZVFAT

7 – Assign Firefighter IDs to Owners

- Logon as SPM Administrator and click in transaction /VIRSA/VFAT on the „Owners“ button

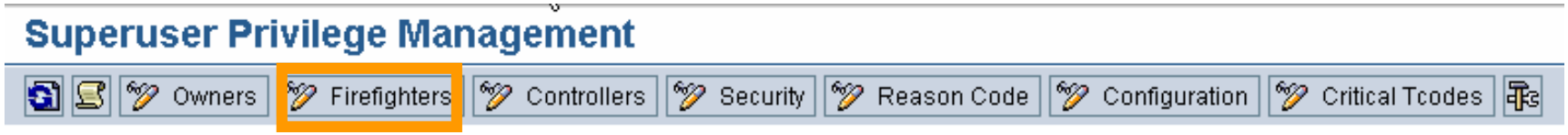


- Then assign to each Firefighter ID one or multiple (new in AC5.3) Owners

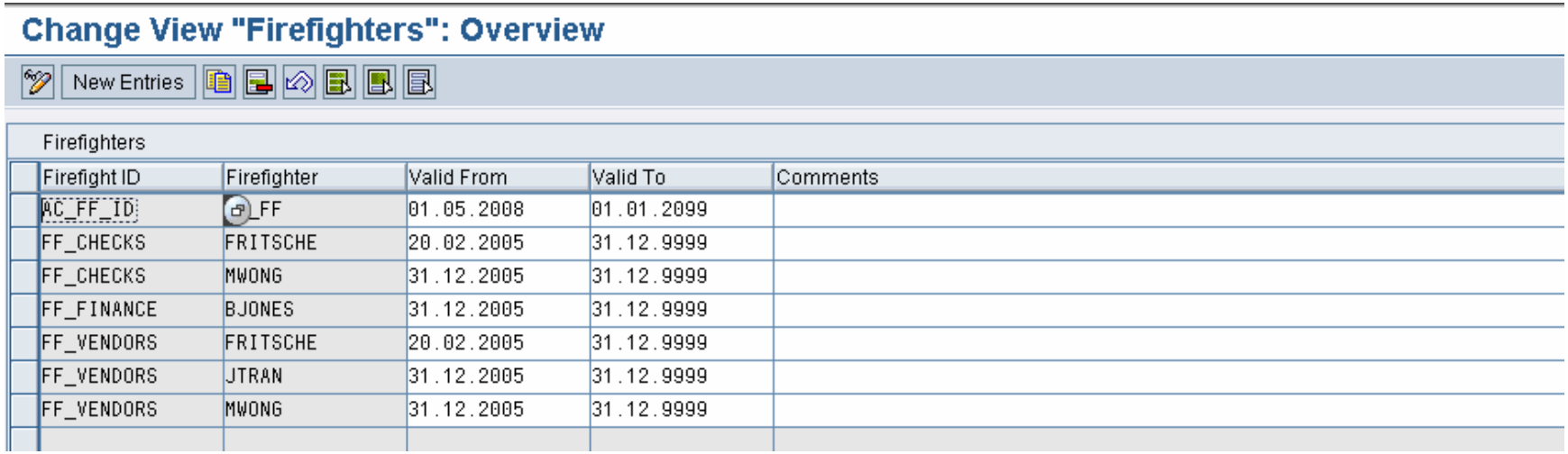


8 – Assign Firefighter IDs to Firefighter

- Logon as Owner (or Administrator) and click in transaction /VIRSA/VFAT on the „Firefighter“ button



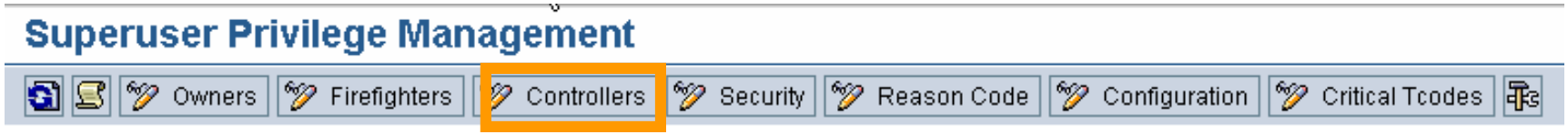
- Then assign Firefighter IDs to Firefighters (end users with access to SPN)



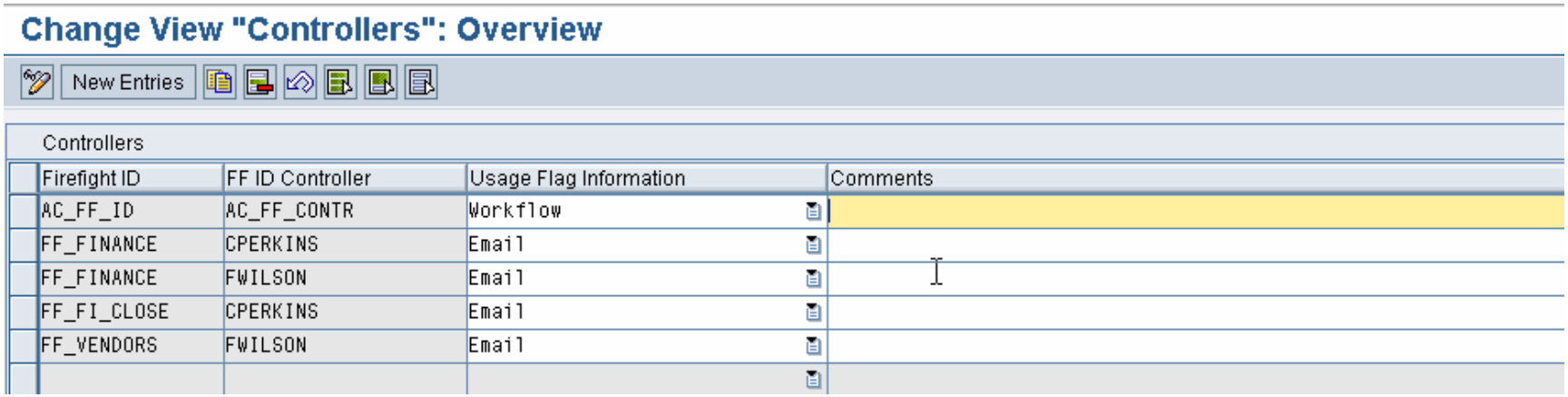
Firefight ID	Firefighter	Valid From	Valid To	Comments
AC_FF_ID	_FF	01.05.2008	01.01.2099	
FF_CHECKS	FRITSCHE	20.02.2005	31.12.9999	
FF_CHECKS	MWONG	31.12.2005	31.12.9999	
FF_FINANCE	BJONES	31.12.2005	31.12.9999	
FF_VENDORS	FRITSCHE	20.02.2005	31.12.9999	
FF_VENDORS	JTRAN	31.12.2005	31.12.9999	
FF_VENDORS	MWONG	31.12.2005	31.12.9999	

9 – Assign Firefighter IDs to Controllers

- Logon as Owner (or Administrator) and click in transaction /VIRSA/VFAT on the „Controllers“ button



- Then assign Firefighter IDs to Controllers. This allows Owners to delegate the monitoring or auditing of Firefighter activities to Controllers.



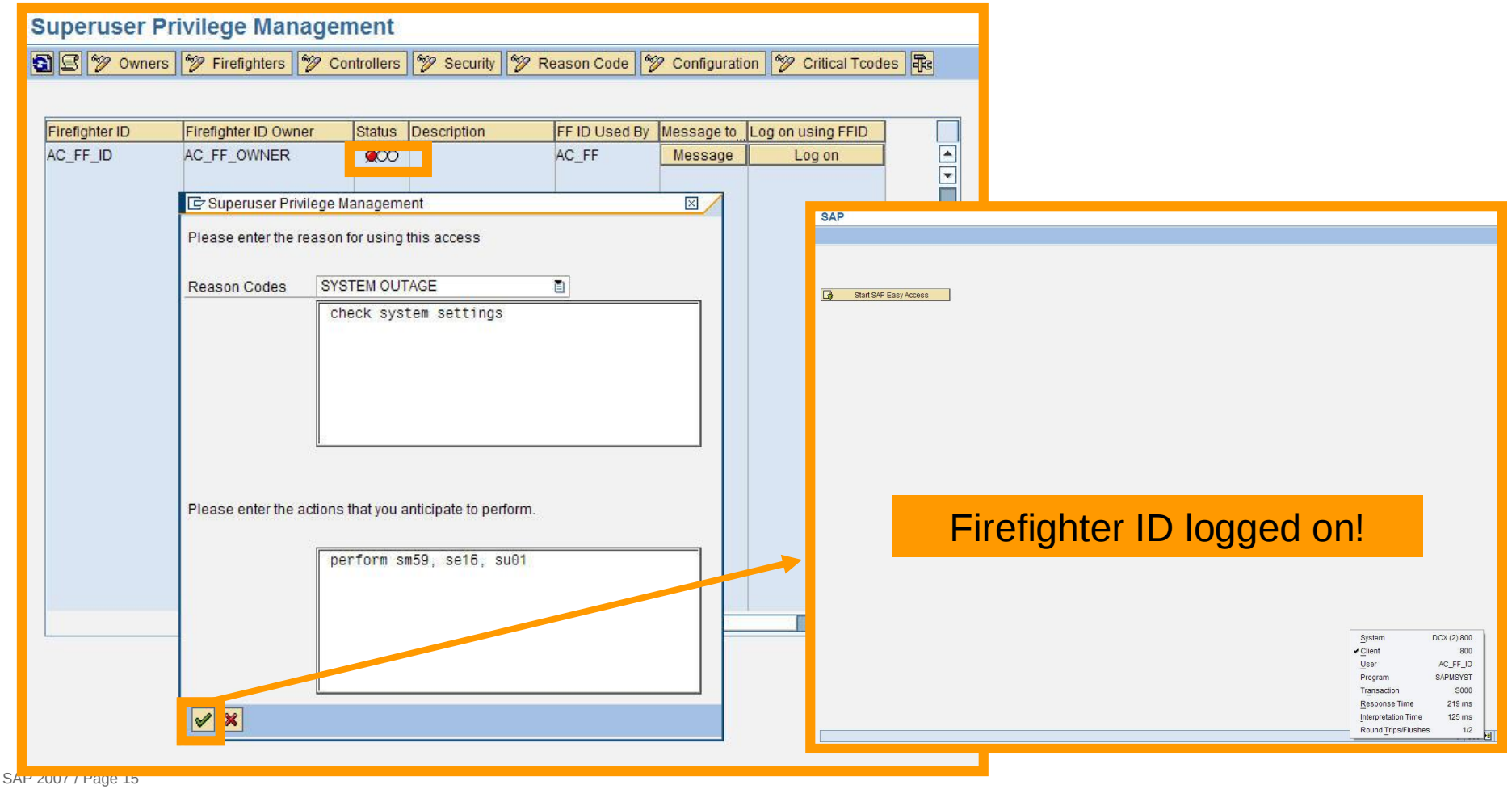
10 – Test SPM in SAP Backend System (1/2)

- Logon as Firefighter and start transaction /VIRSA/VFAT

- As long as the status is green the Firefighter ID is not in use and you can logon with it.

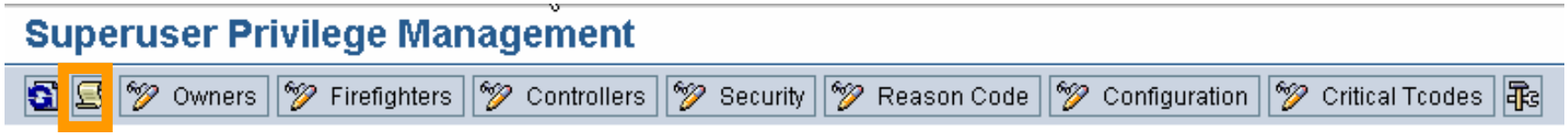
10 – Test SPM in SAP Backend System (2/2)

- Provide reason code and list actions (free text) you want to perform for later reference. Note that the status has turned red. This means that the Firefighter ID is not available for no one else as of this point in time.

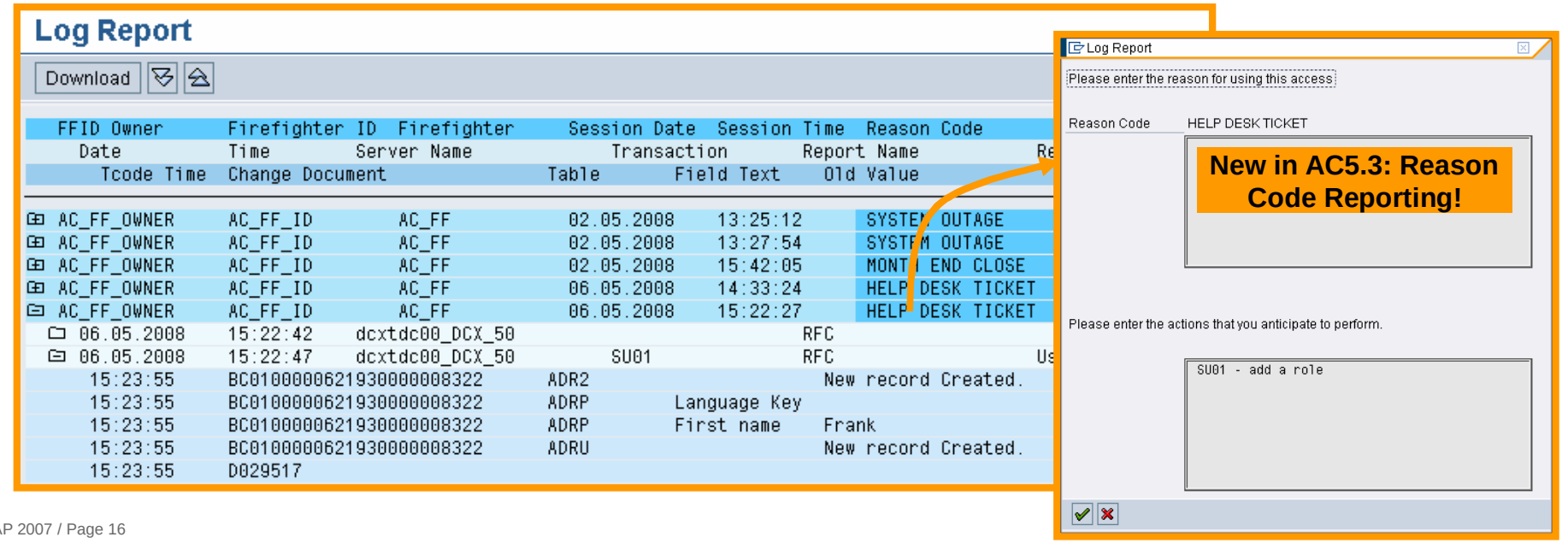


11 - Test Log Report in Backend System

- Logon as Controler (or Administrator) and click in transaction /VIRSA/VFAT on the „Log Report“ icon. Make sure that the bg job in (2) has run in the meantime!

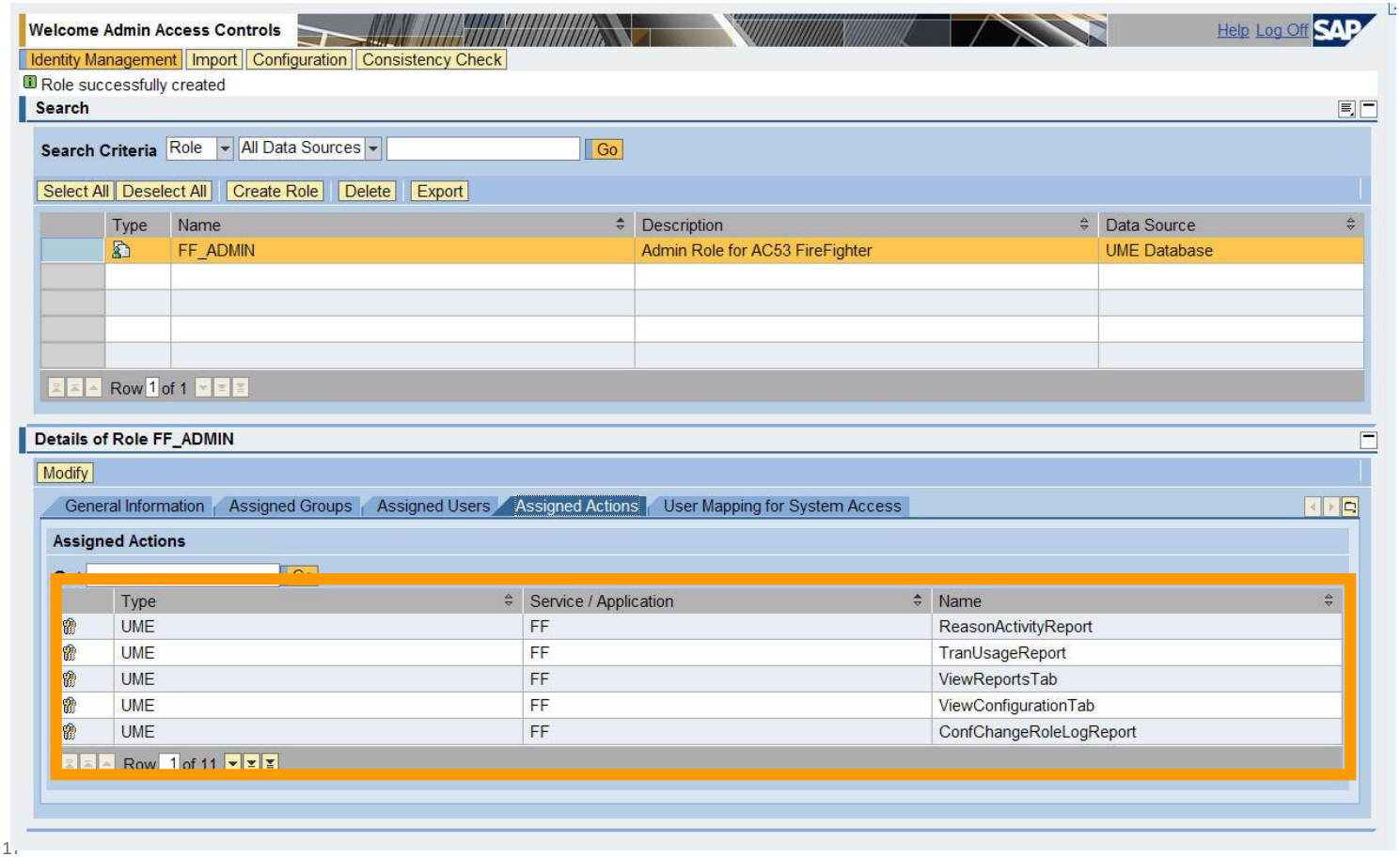


- After you made your selection the log report appears. It should list all relevant details as displayed below: Firefighter, Firefighter ID, logon time stamp, transaction or report name and details of change documents, if created by SAP system.



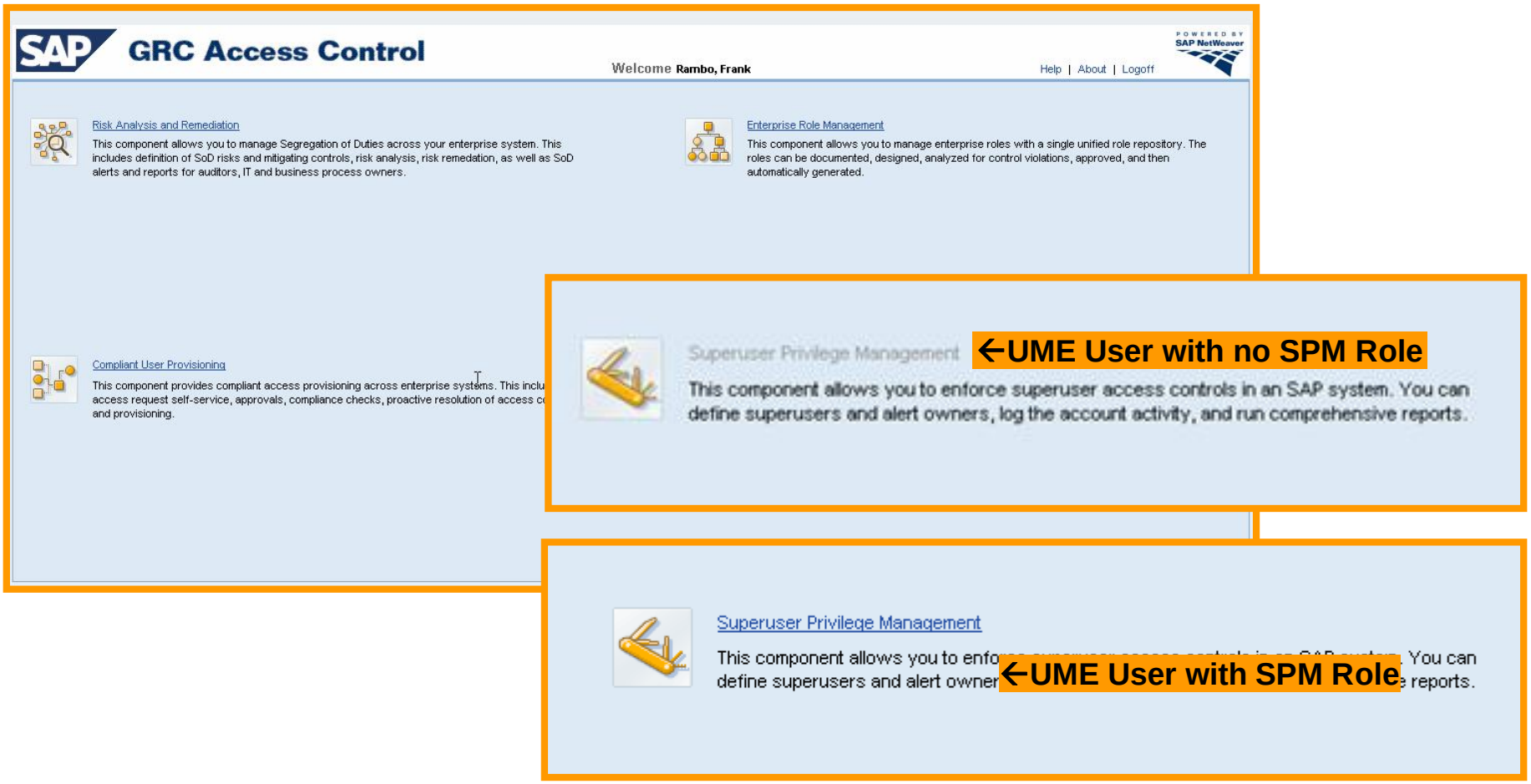
12 – Create SPM Administrator UME Role (1/2)

- Step 2 starts now: Configure SPM Frontend Reporting in AC5.3
- In UME of AC5.3 application server create a UME Role for SPM administrators and assign all UME Actions of Service / Application “FF” that were shipped by SAP



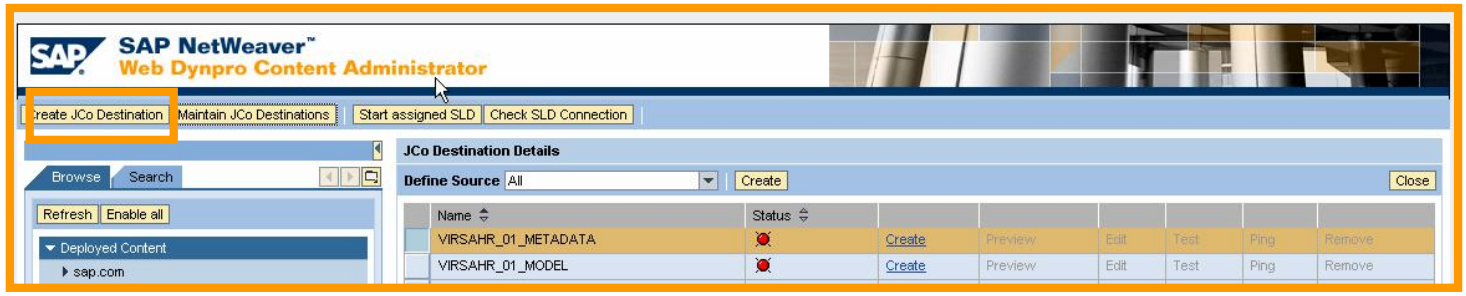
12 – Create SPM Administrator UME Role (2/2)

- Only UME users with roles that contain „FF“ UME Actions will find an active link to Superuser Privilege Management in the Launchpad!

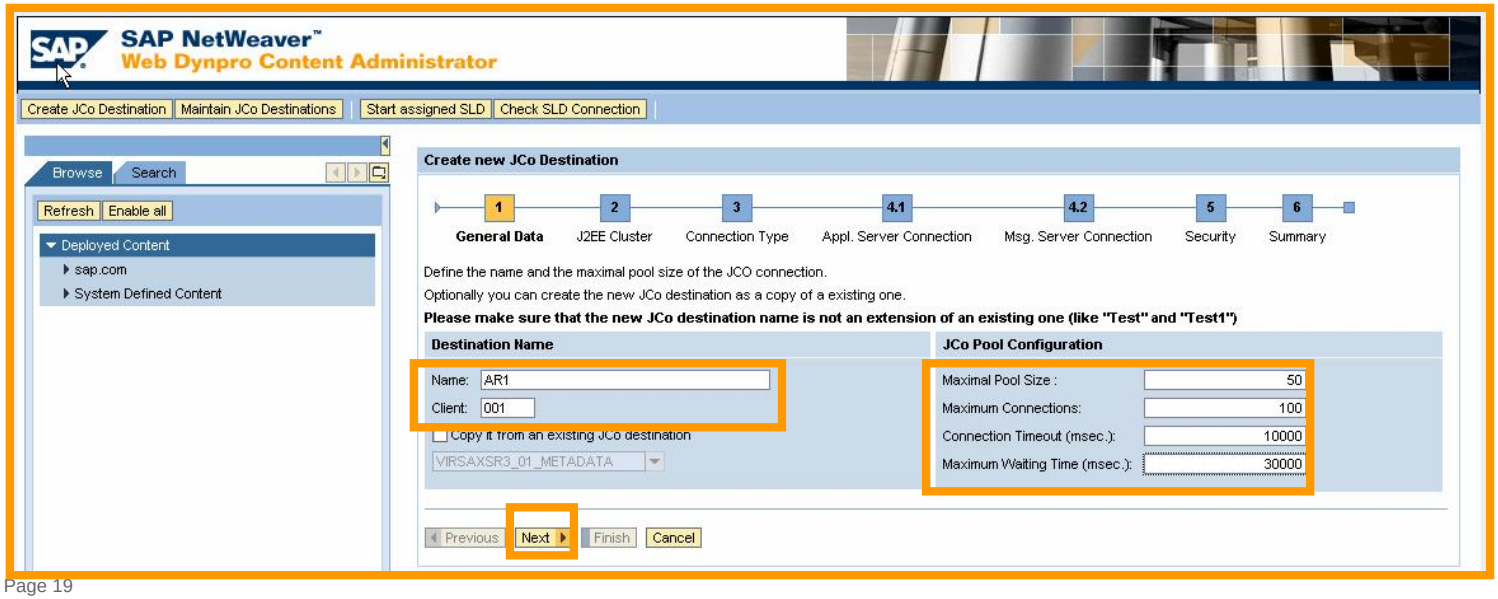


13 - Create JCO in NW for SLD Integration → Destination Name = RAR Connector ID

- Go http://<server>:<port> → Web Dynpro → Content Administrator

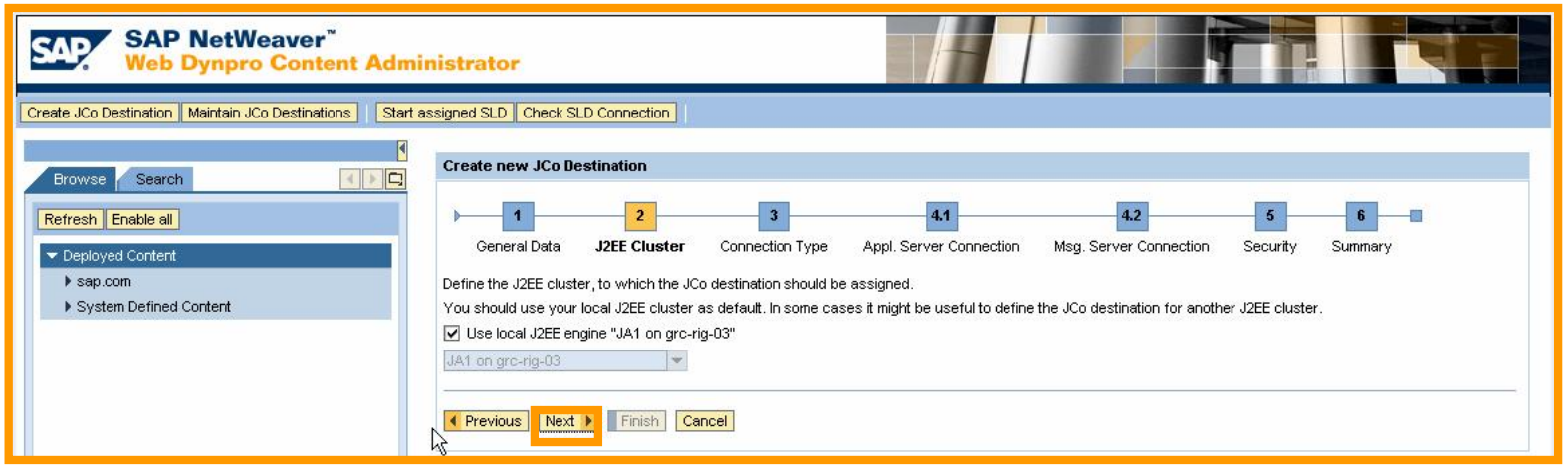


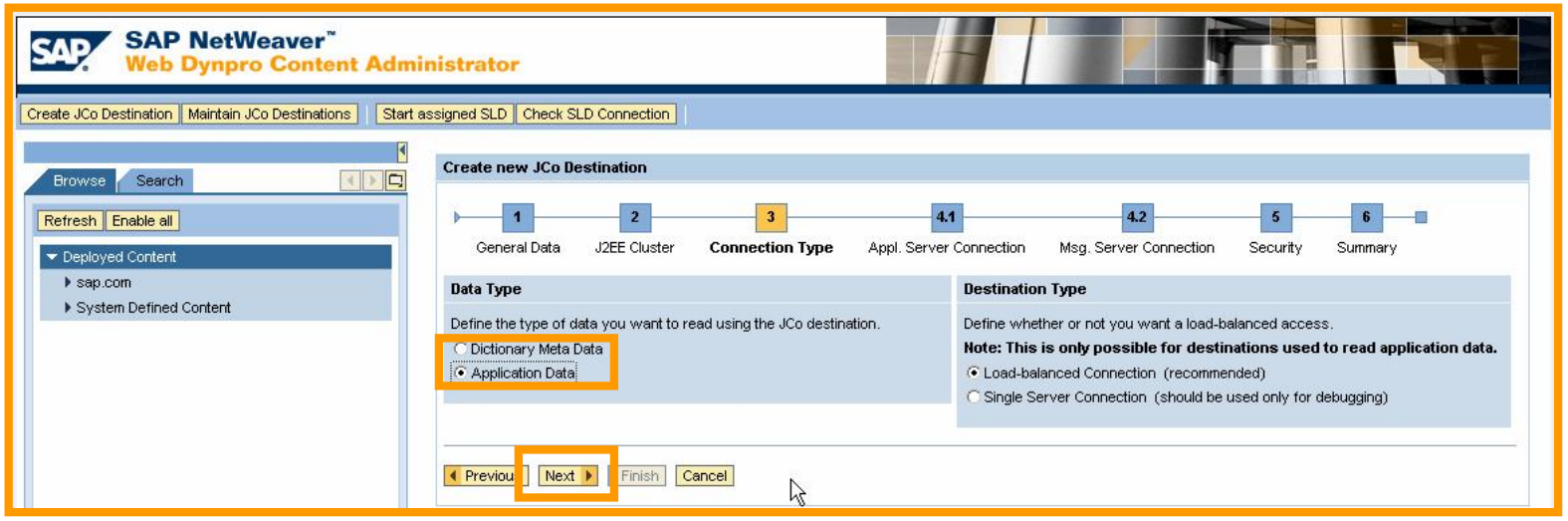
- Click on Create JCo Destination and **use as Destination Name the Connector ID you‘re using in RAR (Field „System“)** for the same SAP backend system. Also set correct JCo Pool parameters



13 - Create JCO in NW for SLD Integration → Connection Type = Application Data

- Confirm the next screen with *Next*, then select *Application Data* and click *Next*

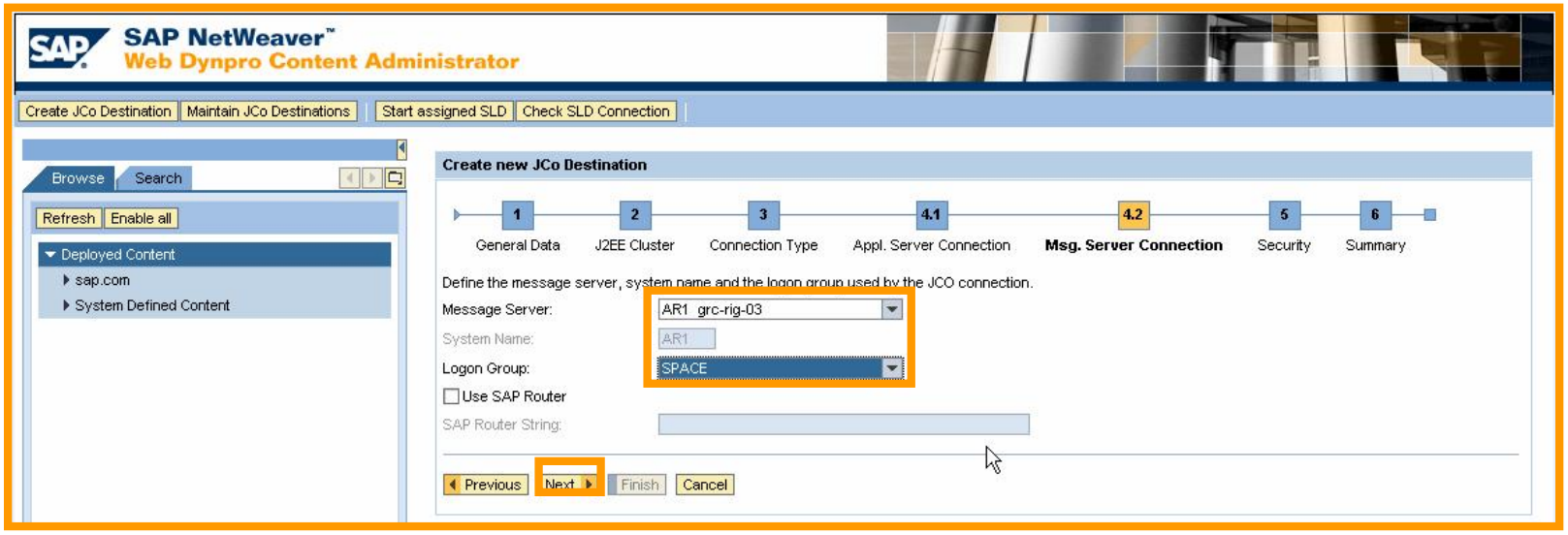




13 - Create JCO in NW for SLD Integration → Connection Type = Application Data

- Choose Message Server and Logon Group

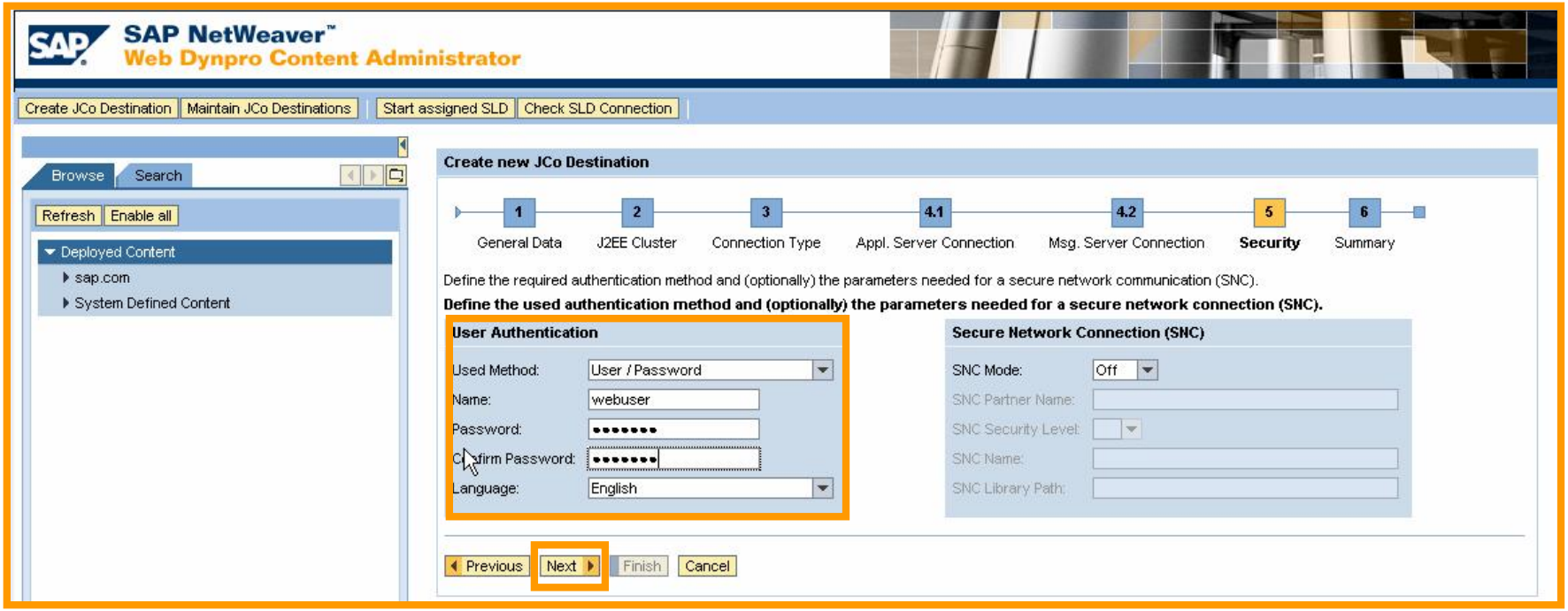
- SAP Router Strings can be configured here as well. This may be required in outsourcing scenarios where AC Java Frontend and SAP Backends belong to different networks.



13 - Create JCO in NW for SLD Integration → Security Settings

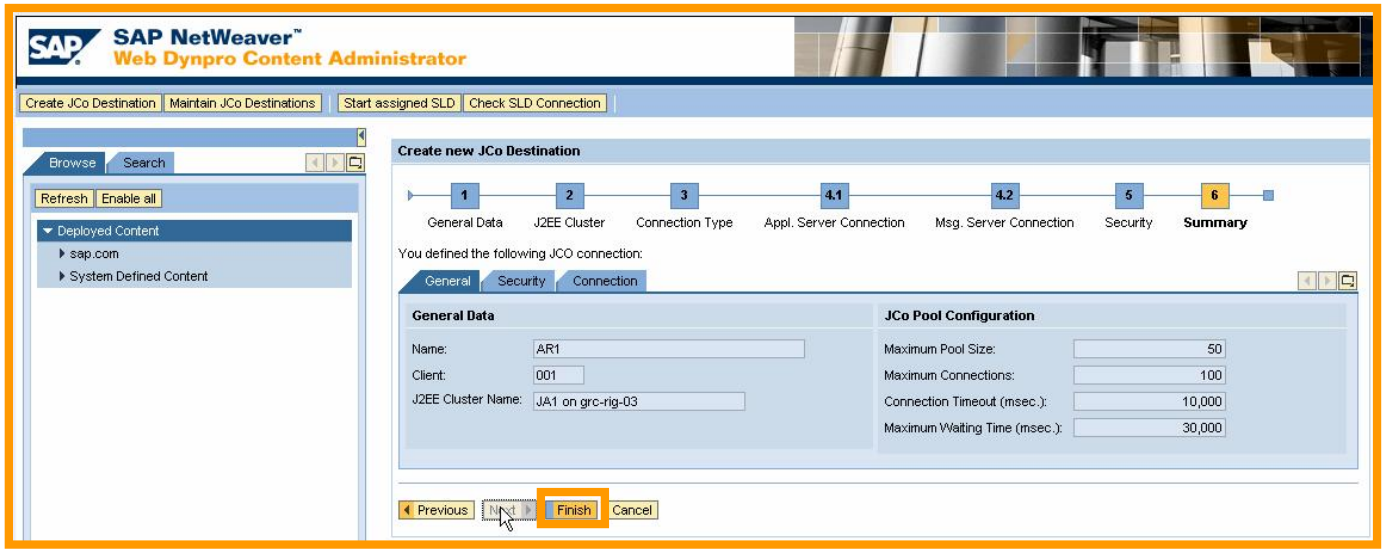
- Provide userID and password of RFC user you have already created for RAR in the backend.

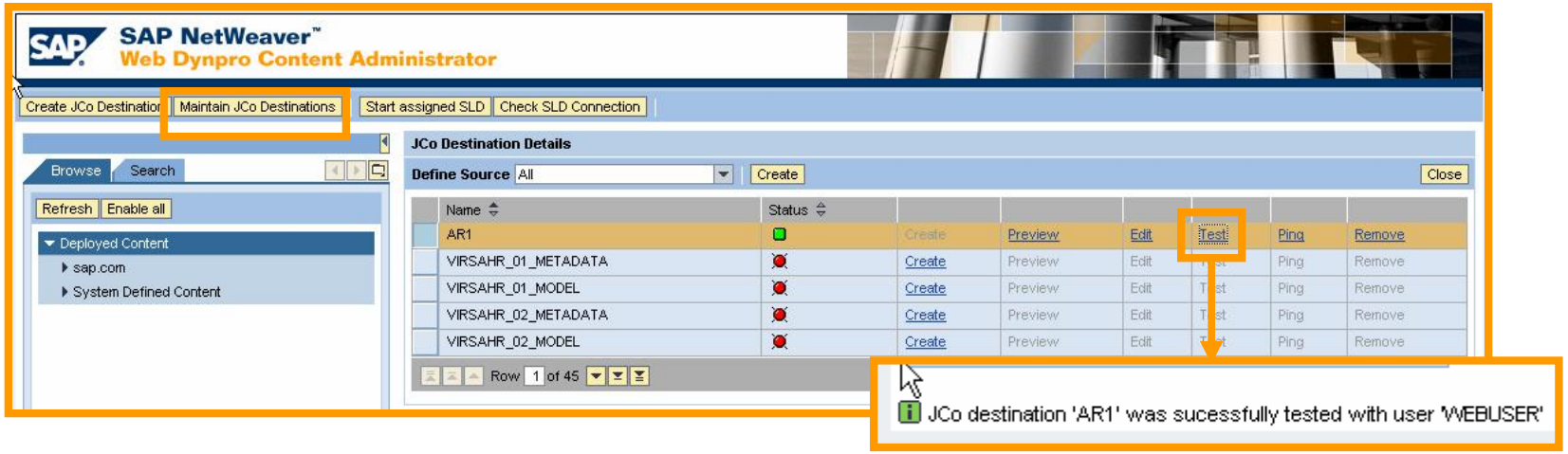
- SNC encryption (transport layer) can be activated here, too. This may be required for high security environments where all communication between AC Java Frontend and SAP Backend has to be encrypted (for example for CUP password transmission). For more details refer to SAP Netweaver Documentation.



13 - Create JCO in NW for SLD Integration → Finish & Test

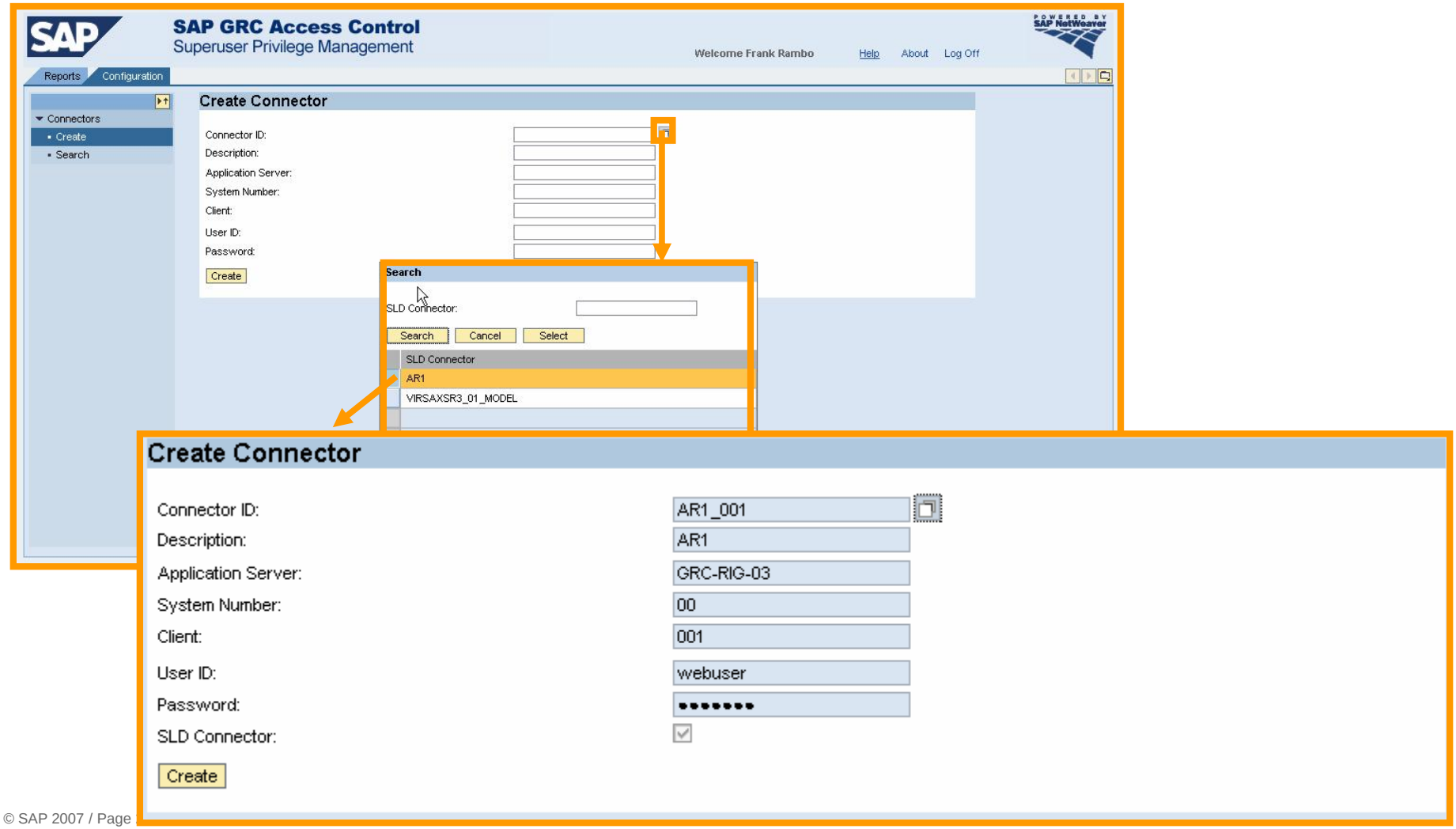
- Click on *Finish.* It is always a good idea to test the connection!





14 – Create System Connector in SPM Java Frontend

- Create a system connector in SPM → Configuration → Connectors → Create and select SLD connector from list.



15 - Test SPM Frontend Reporting

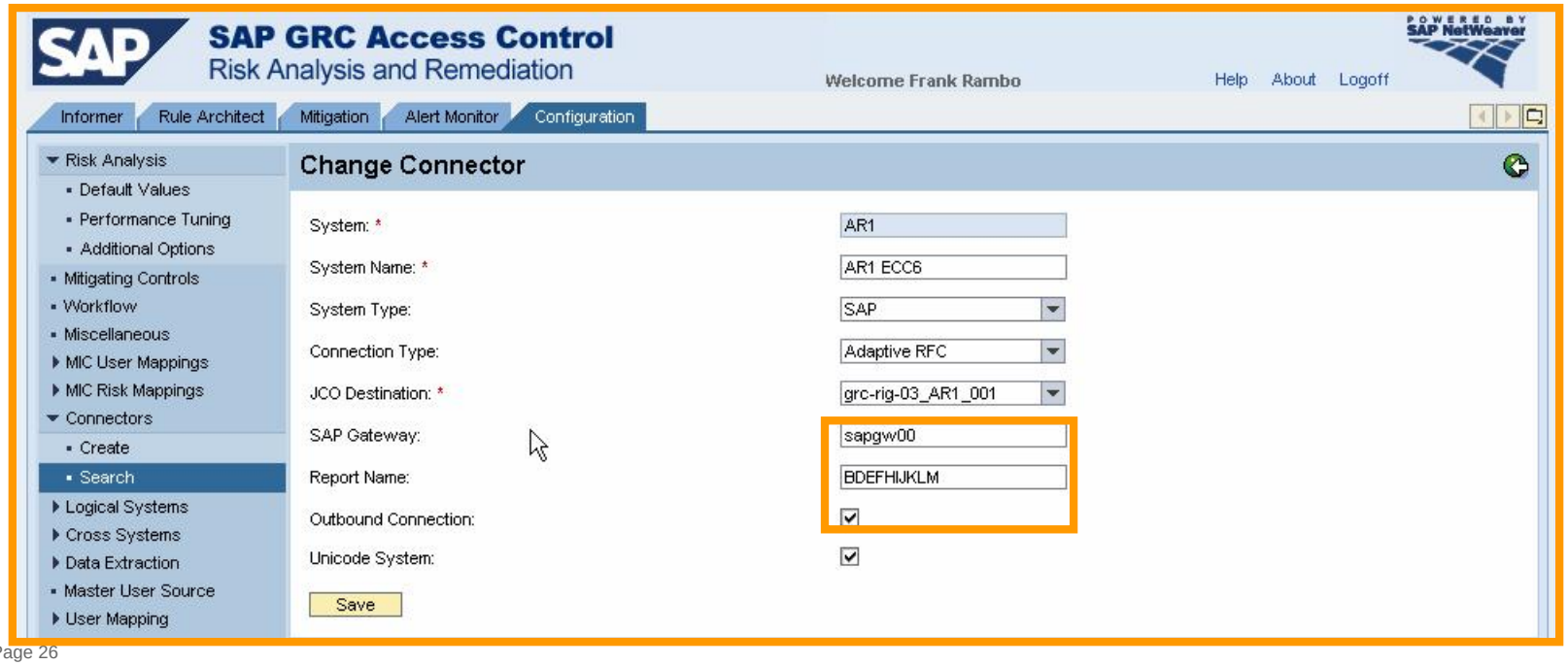
- Test the access to the SPM reports generated in each of your backend systems

16 - Change system connector settings in RAR

- Step 3 starts now: Configure SoD Reporting for SPM as explained in SAP notes 1055976 and 1060673.

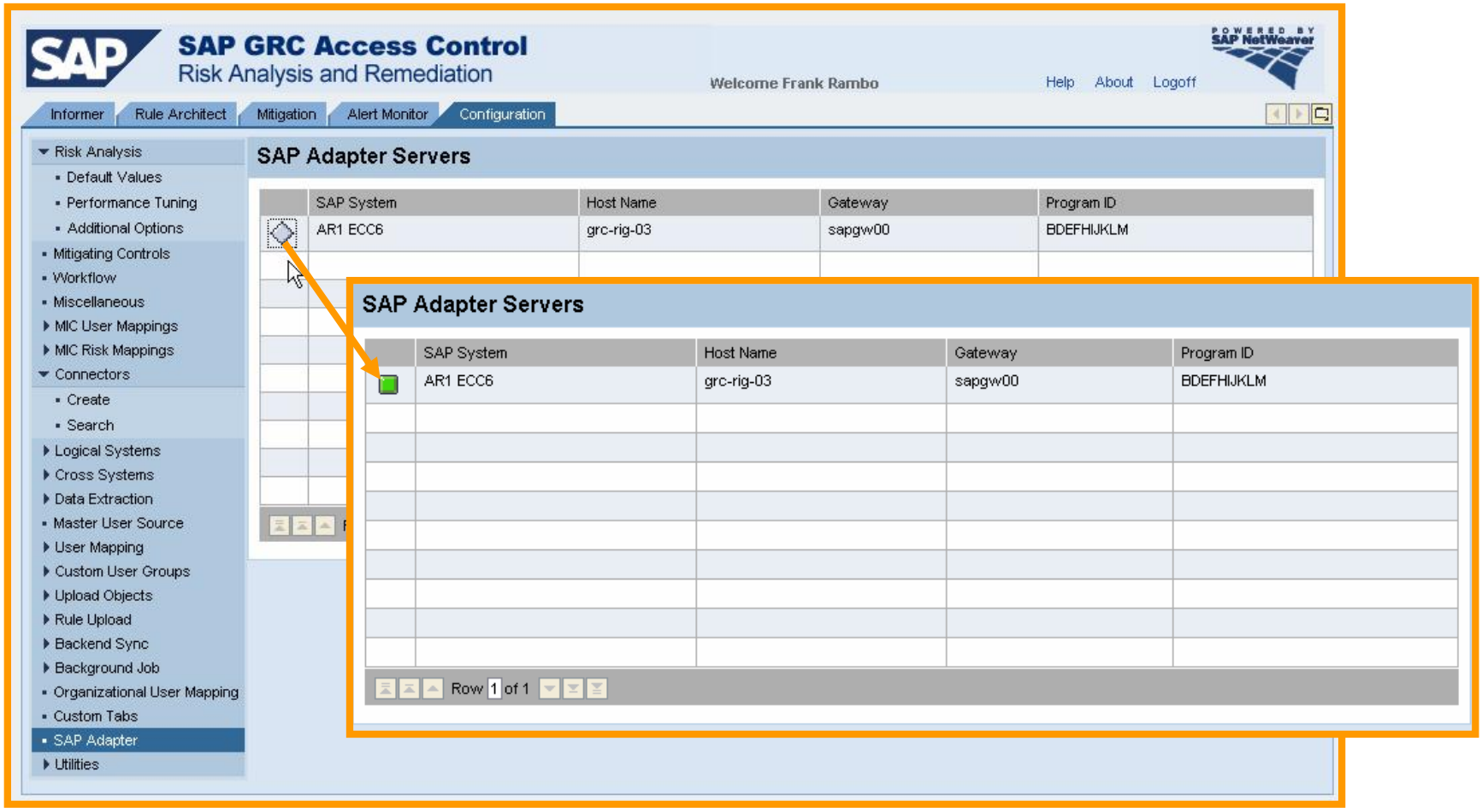
- In RAR → Configuration → Connectors add / change for each backend connector settings as displayed below

- In some instances usage of Risk Terminator comes up with an error unless a specific naming for *Report Name* & corresponding RFC destination (Task 17) is used as documented in SAP Note 1145048. The report name *BDEFHIJKLM* has been chosen arbitrarily and should be chosen differently for each backend system your are connecting to.



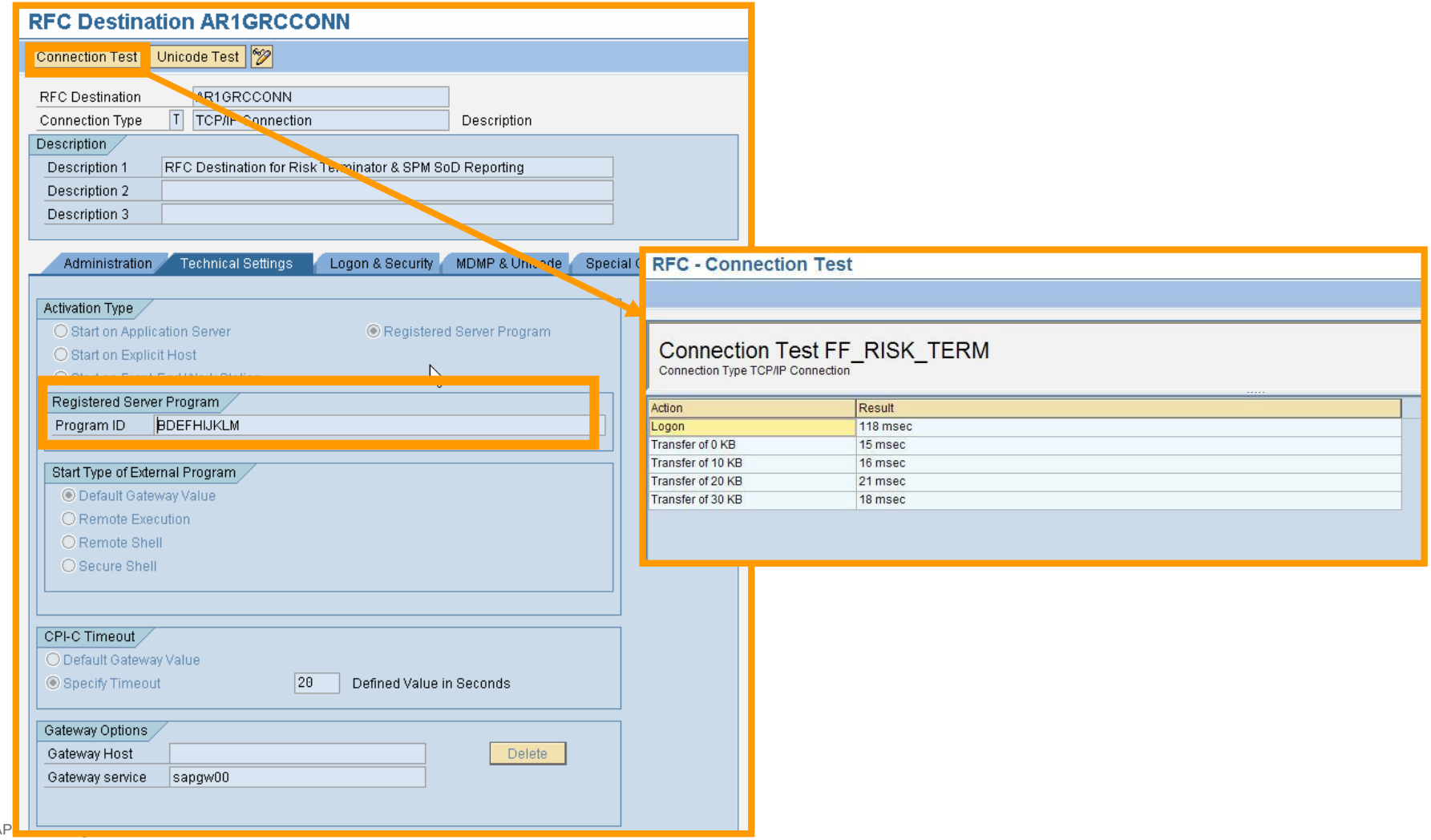
17 – Start SAP Adapters for each SAP Backend

- Click on the grey diamond icon to start SAP Adapter



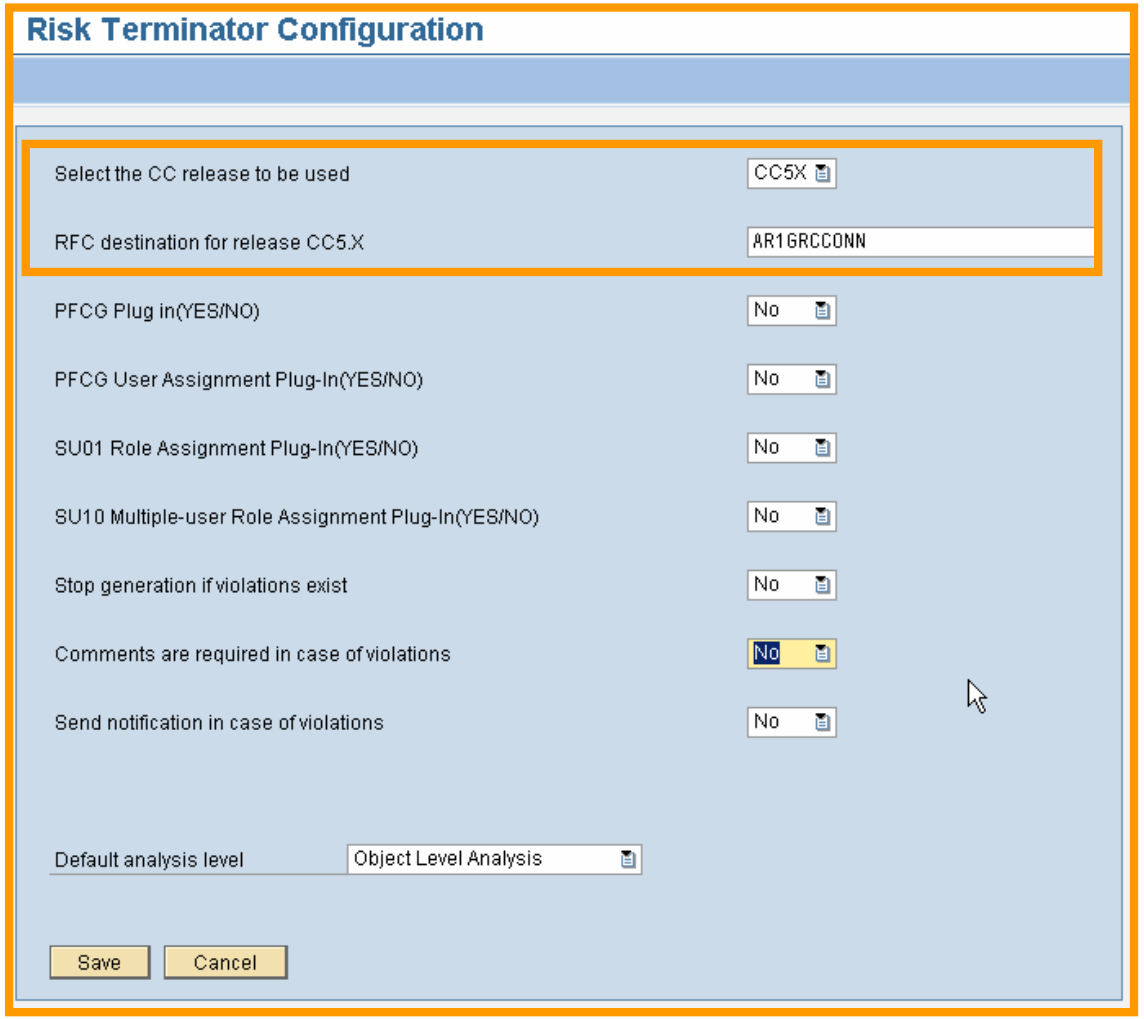
18 – Create TCP/IP RFC Destination in each SAP Backend and Test Connection

- In SM59 create a RFC connection of type TCP/IP and enter as Program ID *BDEFHIJKLM.* Then perform a connection test.



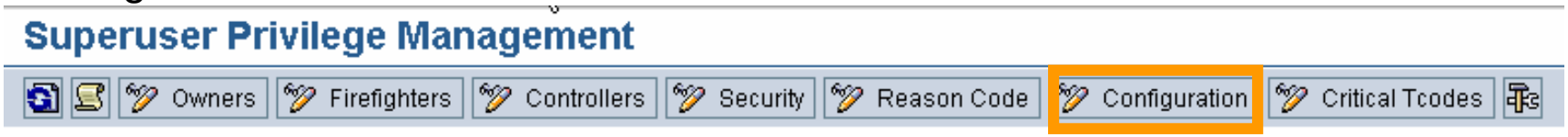
19 – Configure Risk Terminator in each SAP Backend

- Start transaction /VIRSA/ZRTCNFG and enter the name of the RFC connection created in (17). Also select „CC5X“ as CC release to be used

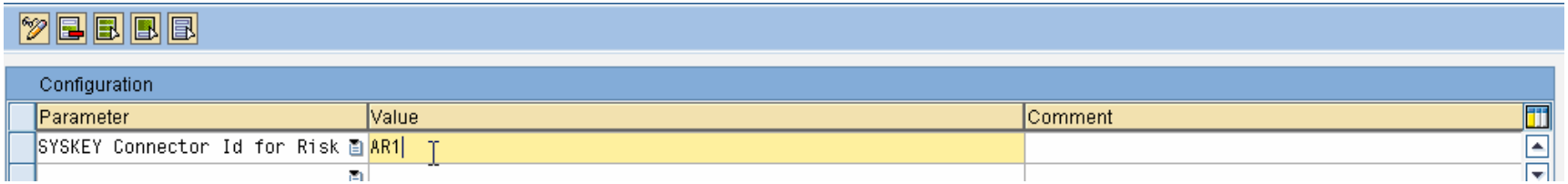


20 – Add Connector ID to SPM Configuration

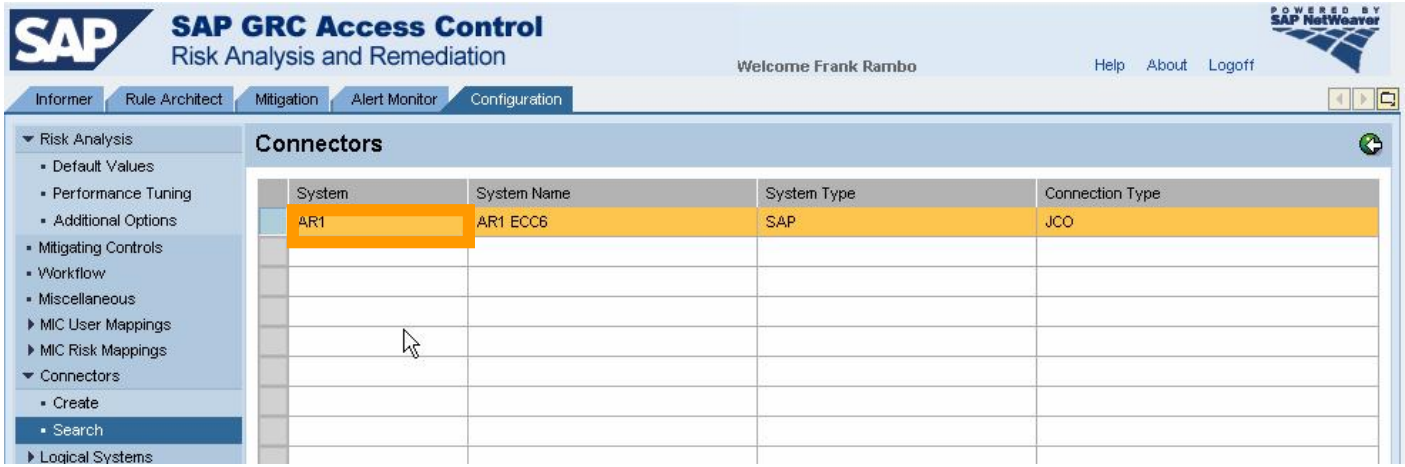
- Logon as SPM Administrator and start transaction /VIRSA/VFAT



- In SPM Configuration Table make the following additional entry



- Make sure that the Connector ID coincides with the field „System“ defined as connector in RAR.



21 – Test SoD Reporting in the SPM Frontend

- Test SoD Reports in your SPM Frontend

- It should show up as displayed below once you made your selection

Copyright 2008 SAP AG
All rights reserved