

SAP Governance, Risk & Compliance Access Control 5.3

Post-Installation

→ Superuser Privilege Management



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



- 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 Controller
 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

RFC Destination FF_RFC

Remote Logon | Connection Test | Unicode Test |

RFC Destination:

Connection Type: ABAP Connection | Description

Description

Description 1:

Description 2:

Description 3:

Administration | **Technical Settings** | Logon & Security | MDMP & Unicode | Special Options

Target System Settings

Load Balancing Status

Load Balancing: Yes No

Target Host: System Number:

Save to Database as

Save as: Hostname IP Address

Gateway Options

Gateway Host:

Gateway service:

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.

Change Job /VIRSA/ZVFATBAK

Start condition Step Job details Predecessor job Successor job

General data

Job name /VIRSA/ZVFATBAK

Job class C

Status Released

Exec. Target Spool list recipient

Job start		
	Date	Time
Start date	13.04.2007	16:46:51

Job frequency	
Hourly	

Job steps

0000000001 -Steps successfully defined

3 – Create Users



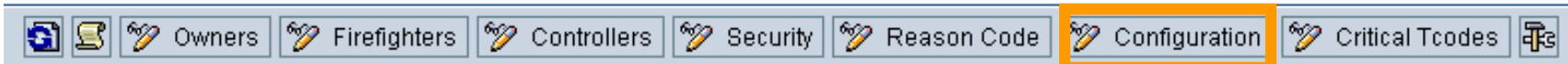
- Create the following users:
 - **SPM Administrator** → Role: /VIRSA/Z_VFAT_ADMINISTRATOR
 - Configuration of Firefighter
 - Assign *Owners* and *Controllers* to Firefighter IDs
 - Maintain *Security Tables*, which requires the knowledge of the passwords of the FireFighterIDs
 - Access to the *Tool 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 /MIRSA/VFAT

Superuser Privilege Management



- In SPM Configuration Table make the following entries

Change View "Configuration": Overview

Configuration	FF Config Parameter Value
Retrieve Change Log	YES
Firefighter Owner Additional Authorization	YES
Firefighter Controller Additional Authorization	YES
Send Log Report Execution Notification Immediately	NO
Send Log Report Execution Notification	NO
Send Firefighter Login Notification Immediately	NO
Send FirefightId Login Notification	NO
Remote Function Call	FF_RFC → RFC Dest you created before!

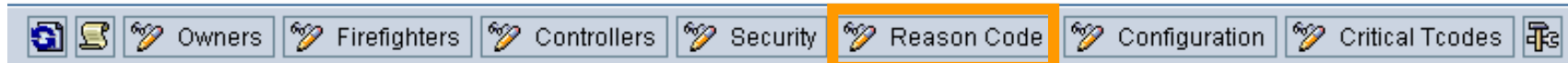
- *Owner Additional Auth. Setting:* Ensures that owners can only manage Firefighter IDs they own.
- *Controler Additional Auth. Setting:* Ensures that controlers can only access log reports of Firefighter IDs they were assigned to.
- Change notification settings, if you want to use email notifications

5 – Create Reason Codes



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

Superuser Privilege Management



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

Change View "Reason Codes": Overview

Table showing Reason Codes with columns: Reason Codes, Description, Active, and a small icon column.

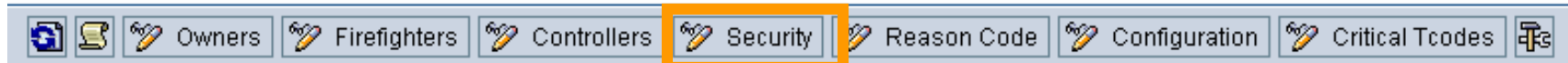
Reason Codes	Description	Active	
HELP DESK TICKET	HELP DESK TICKET	Active	📄
MONTH END CLOSE	MONTH END CLOSE	Active	📄
OPEN CLIENT	OPEN CLIENT	Active	📄
SYSTEM OUTAGE	SYSTEM OUTAGE	Active	📄

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

Superuser Privilege Management



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

New Entries: Overview of Added Entries

Firefight Id	Password	Comments
AC_ADMIN	difficult_password	new Firefighter ID

New Entries: Overview of Added Entries

Firefight Id	Password	Comments
AC_ADMIN	<IQH#s1_%,plx0Msx7aE%?(Qi.hAZwqG.wk%:%y	NEW

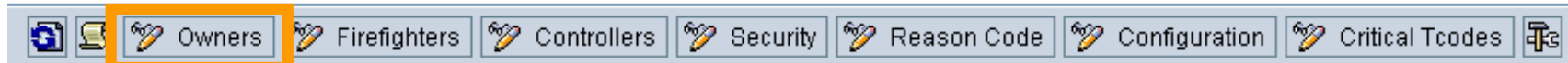
- If you implement SAP note 992200, then Firefighter IDs can't logon anymore with their password, but can be accessed only via activation in /VIRSA/ZVFAT

7 – Assign Firefighter IDs to Owners



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

Superuser Privilege Management



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

Change View "Owners": Overview

Firefight ID	Firefight ID Owner	Description	Comments
AC_FF_ID	_FF_OWNER		
FF_CHECKS	FWILSON		
FF_FINANCE	CPERKINS		
FF_VENDORS	FWILSON		

8 – Assign Firefighter IDs to Firefighter



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

Superuser Privilege Management



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

Change View "Firefighters": Overview

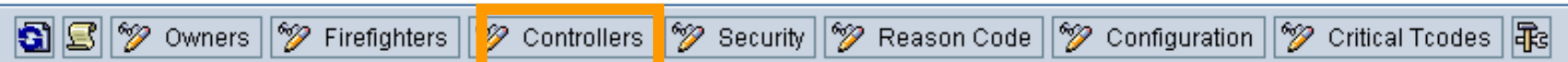
Firefight ID	Firefighter	Valid From	Valid To	Comments
AC_FF_ID	FF	01.05.2008	01.01.2099	
FF_CHECKS	FRITSCH	20.02.2005	31.12.9999	
FF_CHECKS	MWONG	31.12.2005	31.12.9999	
FF_FINANCE	BJONES	31.12.2005	31.12.9999	
FF_VENDORS	FRITSCH	20.02.2005	31.12.9999	
FF_VENDORS	JTRAN	31.12.2005	31.12.9999	
FF_VENDORS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

Superuser Privilege Management



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

Change View "Controllers": Overview

Firefight ID	FF ID Controller	Usage Flag Information	Comments
AC_FF_ID	AC_FF_CONTR	Workflow	
FF_FINANCE	CPERKINS	Email	
FF_FINANCE	FWILSON	Email	
FF_FI_CLOSE	CPERKINS	Email	
FF_VENDORS	FWILSON	Email	

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



- Logon as Firefighter and start transaction /MIRSA/VFAT

Superuser Privilege Management

Firefighter ID	Firefighter ID Owner	Status	Description	FF ID Used By	Message to	Log on user
AC_FF_ID	AC_FF_OWNER				Message	Log on

- 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.

The screenshot displays the SAP Superuser Privilege Management (SPM) interface. At the top, there is a navigation bar with icons for Owners, Firefighters, Controllers, Security, Reason Code, Configuration, and Critical Tcodes. Below this is a table with the following columns: Firefighter ID, Firefighter ID Owner, Status, Description, FF ID Used By, Message to, and Log on using FFID. The first row shows AC_FF_ID as the Firefighter ID, AC_FF_OWNER as the owner, a red status icon, and AC_FF as the FF ID Used By. A dialog box titled 'Superuser Privilege Management' is open, prompting the user to enter a reason for using this access. The 'Reason Codes' field contains 'SYSTEM OUTAGE' and the 'Please enter the actions that you anticipate to perform' field contains 'perform sm59, se16, su01'. An orange arrow points from the bottom of this dialog box to a separate window titled 'SAP' which displays 'Start SAP Easy Access' and a status box that says 'Firefighter ID logged on!'. In the bottom right corner of the SAP window, a system status box shows the following information:

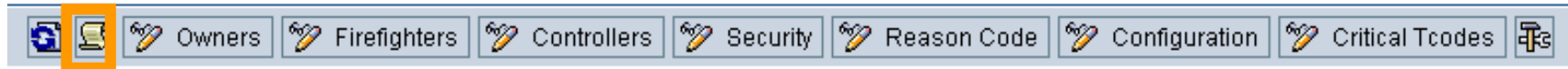
System	DCX (2) 800
Client	800
User	AC_FF_ID
Program	SAPMSYST
Transaction	S000
Response Time	219 ms
Interpretation Time	125 ms
Round Trips/Flashes	1/2

11 - Test Log Report in Backend System



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

Superuser Privilege Management



- 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.

Log Report

Download [Download Icon] [Refresh Icon]

FFID	Owner	Firefighter ID	Firefighter	Session Date	Session Time	Reason Code
Date		Time	Server Name	Transaction		Report Name
Tcode	Time	Change Document	Table	Field Text	Old Value	
AC_FF_OWNER	AC_FF_ID	AC_FF	02.05.2008	13:25:12	SYSTEM	OUTAGE
AC_FF_OWNER	AC_FF_ID	AC_FF	02.05.2008	13:27:54	SYSTEM	OUTAGE
AC_FF_OWNER	AC_FF_ID	AC_FF	02.05.2008	15:42:05	MONIT	END CLOSE
AC_FF_OWNER	AC_FF_ID	AC_FF	06.05.2008	14:33:24	HELP	DESK TICKET
AC_FF_OWNER	AC_FF_ID	AC_FF	06.05.2008	15:22:27	HELP	DESK TICKET
06.05.2008	15:22:42	dcxtdc00_DCX_50			RFC	
06.05.2008	15:22:47	dcxtdc00_DCX_50	SU01		RFC	Us
15:23:55		BC0100000621930000008322	ADR2			New record Created.
15:23:55		BC0100000621930000008322	ADRP	Language Key		
15:23:55		BC0100000621930000008322	ADRP	First name	Frank	
15:23:55		BC0100000621930000008322	ADRU			New record Created.
15:23:55		D029517				

Log Report

Please enter the reason for using this access:

Reason Code: HELP DESK TICKET

New in AC5.3: Reason Code Reporting!

Please enter the actions that you anticipate to perform.

SU01 - add a role

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

Welcome Admin Access Controls Help Log Off

Identity Management | Import | Configuration | Consistency Check

Role successfully created

Search

Search Criteria Role All Data Sources Go

Select All Deselect All Create Role Delete Export

Type	Name	Description	Data Source
	FF_ADMIN	Admin Role for AC53 FireFighter	UME Database

Row 1 of 1

Details of Role FF_ADMIN

Modify

General Information | Assigned Groups | Assigned Users | Assigned Actions | User Mapping for System Access

Assigned Actions

Type	Service / Application	Name
	FF	ReasonActivityReport
	FF	TranUsageReport
	FF	ViewReportsTab
	FF	ViewConfigurationTab
	FF	ConfChangeRoleLogReport

Row 1 of 11

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!

The screenshot shows the SAP GRC Access Control Launchpad interface. At the top, it says "SAP GRC Access Control" and "Welcome Rambo, Frank". There are three main components visible: "Risk Analysis and Remediation", "Enterprise Role Management", and "Compliant User Provisioning".

Two callout boxes highlight the "Superuser Privilege Management" link:

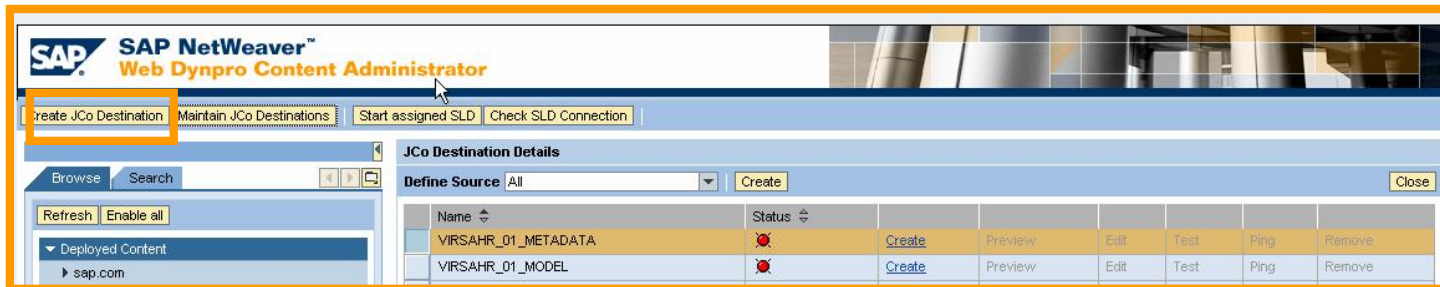
- The top callout box points to the link and says: **← UME User with no SPM Role**
- The bottom callout box points to the link and says: **← UME User with SPM Role**

13 - Create JCo in NW for SLD Integration

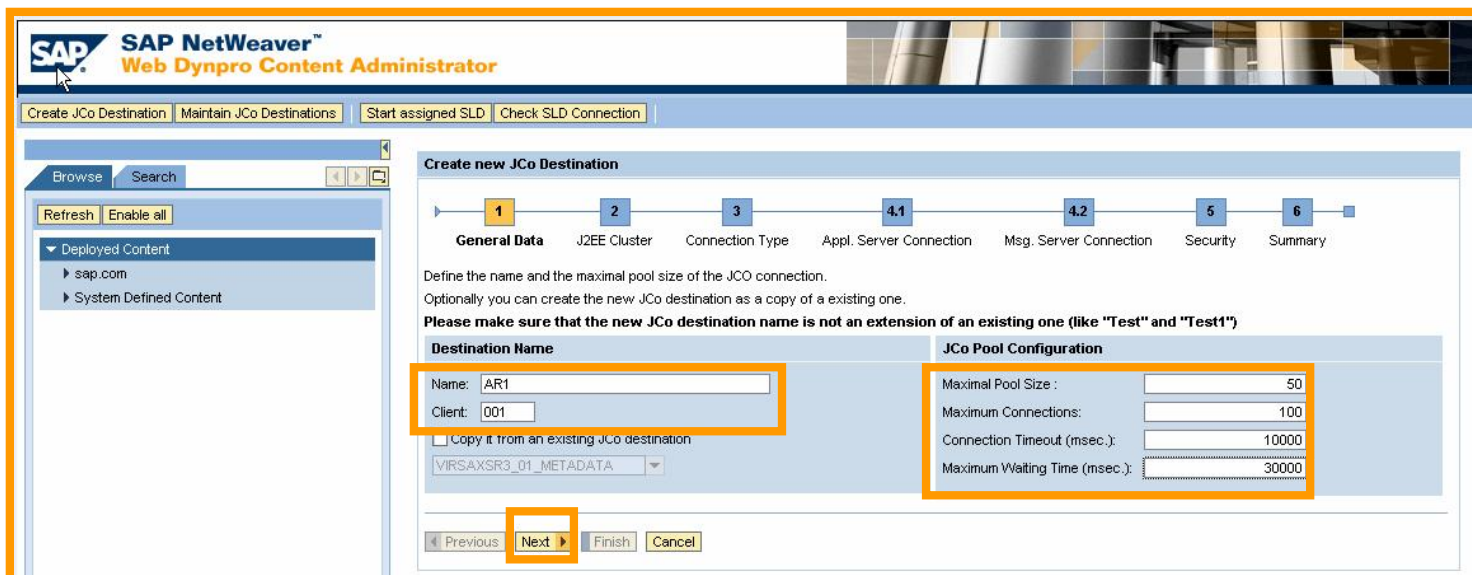
→ Destination Name = RAR Connector ID



- 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*

The screenshot shows the 'Create new JCo Destination' wizard in SAP NetWeaver. The progress bar indicates that step 2, 'J2EE Cluster', is the current step. The 'Use local J2EE engine' checkbox is checked, and the dropdown menu shows 'JA1 on grc-rig-03'. The 'Next' button is highlighted with an orange box.

The screenshot shows the 'Create new JCo Destination' wizard in SAP NetWeaver. The progress bar indicates that step 3, 'Connection Type', is the current step. The 'Data Type' section has 'Application Data' selected with a radio button. The 'Destination Type' section has 'Load-balanced Connection (recommended)' selected. The 'Next' button is highlighted with an orange box.

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.

SAP NetWeaver™
Web Dynpro Content Administrator

Create JCo Destination | Maintain JCo Destinations | Start assigned SLD | Check SLD Connection

Browse Search

Refresh Enable all

Deployed Content
▶ sap.com
▶ System Defined Content

Create new JCo Destination

1 General Data 2 J2EE Cluster 3 Connection Type 4.1 Appl. Server Connection **4.2 Msg. Server Connection** 5 Security 6 Summary

Define the message server, system name and the logon group used by the JCo connection.

Message Server: AR1_grc-rig-03

System Name: AR1

Logon Group: SPACE

Use SAP Router

SAP Router String:

Previous Next Finish Cancel

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.

SAP NetWeaver™ Web Dynpro Content Administrator

Create JCo Destination | Maintain JCo Destinations | Start assigned SLD | Check SLD Connection

Browse | Search

Refresh | Enable all

Deployed Content

- ▶ sap.com
- ▶ System Defined Content

Create new JCo Destination

1 General Data | 2 J2EE Cluster | 3 Connection Type | 4.1 Appl. Server Connection | 4.2 Msg. Server Connection | **5 Security** | 6 Summary

Define the required authentication method and (optionally) the parameters needed for a secure network communication (SNC).

Define the used authentication method and (optionally) the parameters needed for a secure network connection (SNC).

User Authentication

Used Method: User / Password
Name: webuser
Password:
Confirm Password:
Language: English

Secure Network Connection (SNC)

SNC Mode: Off
SNC Partner Name:
SNC Security Level:
SNC Name:
SNC Library Path:

Previous | **Next** | Finish | Cancel

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



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

SAP NetWeaver™ Web Dynpro Content Administrator

Create JCo Destination | Maintain JCo Destinations | Start assigned SLD | Check SLD Connection

Create new JCo Destination

1 General Data | 2 J2EE Cluster | 3 Connection Type | 4.1 Appl. Server Connection | 4.2 Msg. Server Connection | 5 Security | 6 Summary

You defined the following JCO connection:

General Security Connection

General Data

Name: AR1
Client: 001
J2EE Cluster Name: JA1 on grc-rig-03

JCo Pool Configuration

Maximum Pool Size: 50
Maximum Connections: 100
Connection Timeout (msec.): 10,000
Maximum Waiting Time (msec.): 30,000

Previous Finish Cancel

SAP NetWeaver™ Web Dynpro Content Administrator

Create JCo Destination | Maintain JCo Destinations | Start assigned SLD | Check SLD Connection

JCo Destination Details

Define Source: All Create Close

Name	Status	Create	Preview	Edit	Test	Ping	Remove
AR1	🟢	Create	Preview	Edit	Test	Ping	Remove
VIRSAHR_01_METADATA	🔴	Create	Preview	Edit	Test	Ping	Remove
VIRSAHR_01_MODEL	🔴	Create	Preview	Edit	Test	Ping	Remove
VIRSAHR_02_METADATA	🔴	Create	Preview	Edit	Test	Ping	Remove
VIRSAHR_02_MODEL	🔴	Create	Preview	Edit	Test	Ping	Remove

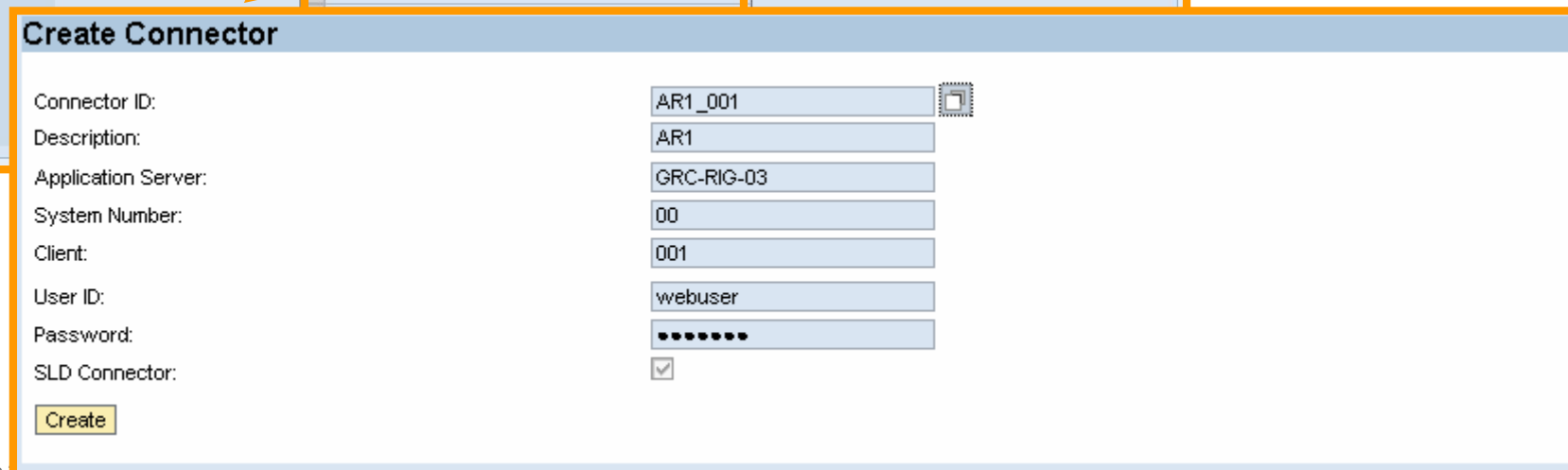
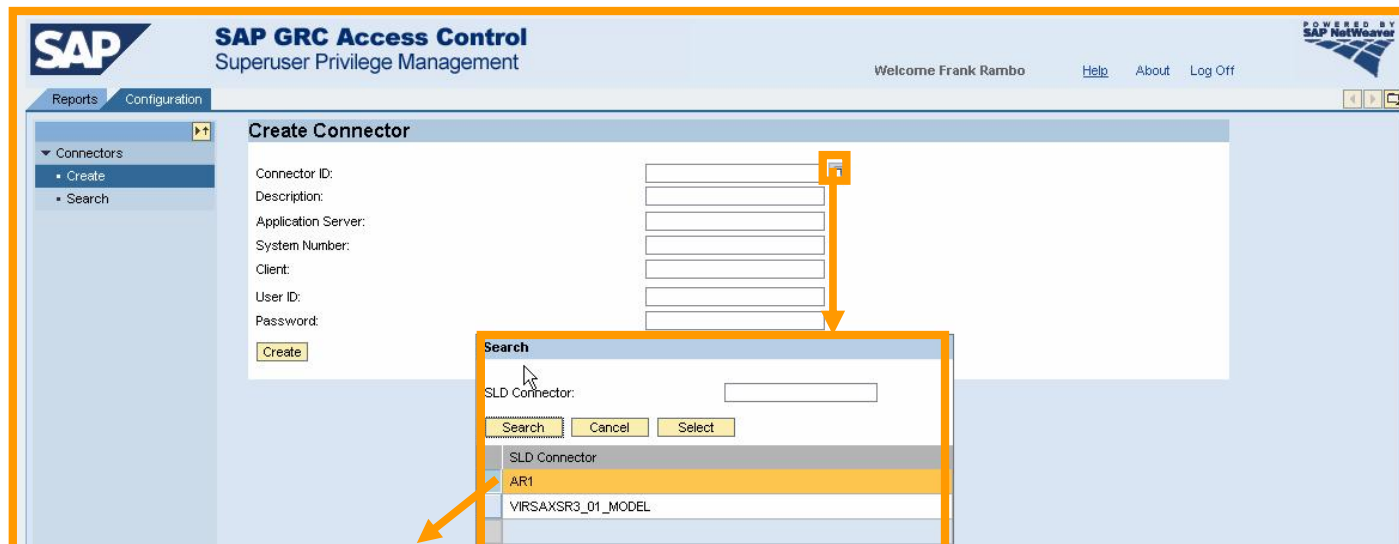
Row 1 of 45

📄 JCo destination 'AR1' was successfully tested with user 'WEBUSER'

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

SAP GRC Access Control
Superuser Privilege Management

Welcome Frank Rambo | Help | About | Log Off

Reports | Configuration

Log Report

System : AR1_001
Reason Code : All
Firefighter ID : All
Firefighter ID Owner : All
Firefighter : All
Date : All
Time : All
Transaction : All

Firefighter ID: FFID | Firefighter: ID40302 | Firefighter ID Owner: FFOwner
Session Date: 6/17/08 | Session Time: 20:50:00 | Reason Code: HELP DESK TICKET

Transaction	Report Name	Server	Date	Time
SMEN	SAPLSMTR_NAVIGATION	grc-rig-03_AR1_00	6/17/08	20:53:05

Firefighter ID: FFID | Firefighter: ID40302 | Firefighter ID Owner: FFOwner
Session Date: 6/17/08 | Session Time: 22:29:02 | Reason Code: HELP DESK TICKET

Transaction	Report Name	Server	Date	Time
SMEN	SAPLSMTR_NAVIGATION	grc-rig-03_AR1_00	6/17/08	22:29:46
PFCG	SAPLPRGN_TREE	grc-rig-03_AR1_00	6/17/08	22:33:07
SU01	RSM13000	grc-rig-03_AR1_00	6/17/08	22:34:32
SESSION_MANAGER	SAPLSMTR_NAVIGATION	grc-rig-03_AR1_00	12/10/07	13:38:21
MIRSA/VFAT	MIRSA/ZVFAT	grc-rig-03_AR1_00	12/10/07	13:38:23

Firefighter ID: FFID1 | Firefighter: AC_ADMIN | Firefighter ID Owner: D029517
Session Date: 7/9/08 | Session Time: 03:29:40 | Reason Code: HELP DESK TICKET

Transaction	Report Name	Server	Date	Time
SU01	SAPMSUU0	grc-rig-03_AR1_00	7/9/08	03:29:57

Firefighter ID: FFID1 | Firefighter: AC_ADMIN | Firefighter ID Owner: D029517
Session Date: 7/9/08 | Session Time: 04:32:25 | Reason Code: MONTH END CLOSE

Transaction	Report Name	Server	Date	Time
SU01	SAPMSUU0	grc-rig-03_AR1_00	7/9/08	04:32:46
PFCG	SAPLPRGN_TREE	grc-rig-03_AR1_00	7/9/08	04:33:00

Firefighter ID: FFID1 | Firefighter: AC_ADMIN | Firefighter ID Owner: D029517
Session Date: 7/9/08 | Session Time: 05:30:15 | Reason Code: SYSTEM OUTAGE

Transaction	Report Name	Server	Date	Time
SU01	SAPMSUU0	grc-rig-03_AR1_00	7/9/08	05:30:19

No. of Rows per Page: 10

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 you are connecting to.

The screenshot displays the 'Change Connector' configuration page in SAP GRC Access Control. The page is titled 'SAP GRC Access Control Risk Analysis and Remediation' and includes a navigation menu with options like 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', and 'Configuration'. The 'Configuration' tab is active, and the 'Connectors' section is expanded. The 'Change Connector' form contains the following fields:

System: *	AR1
System Name: *	AR1 ECC6
System Type:	SAP
Connection Type:	Adaptive RFC
JCO Destination: *	grc-rig-03_AR1_001
SAP Gateway:	sapgw00
Report Name:	BDEFHIJKLM
Outbound Connection:	<input checked="" type="checkbox"/>
Unicode System:	<input checked="" type="checkbox"/>

A 'Save' button is located at the bottom of the form. The 'Report Name' field is highlighted with an orange box.

17 – Start SAP Adapters for each SAP Backend



- Click on the grey diamond icon to start SAP Adapter

The screenshot shows the SAP GRC Access Control Configuration interface. The main content area is titled "SAP Adapter Servers" and contains a table with the following data:

SAP System	Host Name	Gateway	Program ID
AR1 ECC6	grc-rig-03	sapgw00	BDEFHIJKLM

An orange arrow points to a grey diamond icon in the first row of the table, indicating the action to start the SAP Adapter. A zoomed-in view of the table is overlaid on the right, showing a green square icon in the first row, which is the result of clicking the diamond icon.

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.

The screenshot displays the SAP SM59 interface for configuring an RFC destination. The main window is titled "RFC Destination AR1GRCCONN". It shows the "Connection Test" tab selected, with the "Connection Type" set to "TCP/IP Connection". The "Description" field contains "RFC Destination for Risk Terminator & SPM SoD Reporting". The "Registered Server Program" section is highlighted with an orange box, showing the "Program ID" as "BDEFHIJKLM". The "Start Type of External Program" is set to "Default Gateway Value". The "CPI-C Timeout" is set to "Specify Timeout" with a value of "20". The "Gateway Options" section shows the "Gateway Host" and "Gateway service" as "sappgw00".

An inset window titled "RFC - Connection Test" shows the results of a connection test for "Connection Test FF_RISK_TERM". The test results are as follows:

Action	Result
Logon	118 msec
Transfer of 0 KB	15 msec
Transfer of 10 KB	16 msec
Transfer of 20 KB	21 msec
Transfer of 30 KB	18 msec

19 – Configure Risk Terminator in each SAP Backend



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

Risk Terminator Configuration

Select the CC release to be used	CC5X
RFC destination for release CC5X	AR16RCCONN
PFCG Plug in(YES/NO)	No
PFCG User Assignment Plug-In(YES/NO)	No
SU01 Role Assignment Plug-In(YES/NO)	No
SU10 Multiple-user Role Assignment Plug-In(YES/NO)	No
Stop generation if violations exist	No
Comments are required in case of violations	No
Send notification in case of violations	No
Default analysis level	Object Level Analysis

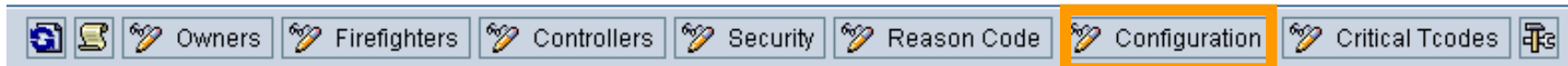
Save Cancel

20 – Add Connector ID to SPM Configuration



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

Superuser Privilege Management



- In SPM Configuration Table make the following additional entry

Parameter	Value	Comment
SYSKEY Connector Id for Risk	AR1	

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

SAP GRC Access Control - Risk Analysis and Remediation

Welcome Frank Rambo

Navigation: Informer, Rule Architect, Mitigation, Alert Monitor, Configuration

Connectors Table:

System	System Name	System Type	Connection Type
AR1	AR1 ECC6	SAP	JCO

21 – Test SoD Reporting in the SPM Frontend



- Test SoD Reports in your SPM Frontend

SAP GRC Access Control
Superuser Privilege Management

Welcome Admin Access Controls [Help](#) [About](#) [Logout](#)

Reports Configuration

• User Reports
• Role Reports

Superuser Privilege Management Reports

- [Log Summary Report](#)
This report provides Firefighter usage lists by Firefighter ID, Firefighter ID Owner, or Firefighter.
- [Transaction Usage Report](#)
This reports transactions which were executed during the firefighting session. You have the option to report only critical transaction usage.
- [Log Report](#)
This reports usage details from the Firefighter Session.
- [Configuration Change Log Report](#)
This report lists the changes made to the Firefighter configuration.
- [Reason / Activity Report](#)
This report lists the reasons and expected activity as entered by the firefighter when initiating a firefighting session. You can generate reports by Reason Code, Firefighter ID, Firefighter ID Owner, or Session Date.
- [Invalid Firefighter IDs, Controllers or Owners Report](#)
This report lists IDs defined in Superuser Privilege Management that no longer valid because they have expired, have been deleted, or are locked.
- [SoD Violations Report](#)
This reports whether a firefighter has violated a Segregation of Duties rule as defined in Risk Remediation and Analysis.

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

SAP GRC Access Control
Superuser Privilege Management

Welcome Admin Access Controls [Help](#) [About](#) [Logout](#)

Reports Configuration

• User Reports
• Role Reports

SoD Violations Report

System :DCX
Firefighter ID Owner :All
Firefighter :AC_FF
Date :5/6/2008

Firefighter:AC_FF **Risk:P008001**

Transaction	Date
FK01	5/6/08
ME21	5/6/08



- > No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.
- > Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.
- > SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned and associated logos displayed are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.
- > The information in this document is proprietary to SAP. This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
- > SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
- > The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages
- > Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.
- > Einige von der SAP AG und deren Vertriebspartnern vertriebene Softwareprodukte können Softwarekomponenten umfassen, die Eigentum anderer Softwarehersteller sind.
- > SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge und andere in diesem Dokument erwähnte SAP-Produkte und Services sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und in mehreren anderen Ländern weltweit. Alle anderen in diesem Dokument erwähnten Namen von Produkten und Services sowie die damit verbundenen Firmenlogos sind Marken der jeweiligen Unternehmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.
- > Die in diesem Dokument enthaltenen Informationen sind Eigentum von SAP. Dieses Dokument ist eine Vorabversion und unterliegt nicht Ihrer Lizenzvereinbarung oder einer anderen Vereinbarung mit SAP. Dieses Dokument enthält nur vorgesehene Strategien, Entwicklungen und Funktionen des SAP®-Produkts und ist für SAP nicht bindend, einen bestimmten Geschäftsweg, eine Produktstrategie bzw. -entwicklung einzuschlagen. SAP übernimmt keine Verantwortung für Fehler oder Auslassungen in diesen Materialien. SAP garantiert nicht die Richtigkeit oder Vollständigkeit der Informationen, Texte, Grafiken, Links oder anderer in diesen Materialien enthaltenen Elemente. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u. a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung der geltenden Rechts.
- > SAP übernimmt keine Haftung für Schäden jeglicher Art, einschließlich und ohne Einschränkung für direkte, spezielle, indirekte oder Folgeschäden im Zusammenhang mit der Verwendung dieser Unterlagen. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.
- > Die gesetzliche Haftung bei Personenschäden oder die Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.
- > Alle Rechte vorbehalten.