SAP Governance, Risk & Compliance
Access Control 5.3

Post-Installation Slide Deck
→ Compliant User Provisioning

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 are committed to the continuous improvement of GRC products and services, taking the product from validation to customer deployment.

➢ We ensure
  ➢ Field readiness,
  ➢ high customer satisfaction, and
  ➢ customer references.

RIG Installation Methodology

> We recommend the following installation methodology

1. Install SAP Netweaver AS JAVA 7.0 SP12+
2. Run Pre-Installation Presentation
3. Deploy Access Control Software (including latest Support Packages)
4. Run Post-Installation Presentations (also available as Flash Movie)
   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
- Compliant User Provisioning -

1. Upload UME Roles (→ Refer to Post-Installation Slide Deck for RAR)

2. Upload Initial Configuration Data

3. Create and Test System Connectors

4. Configure User Data Source & User Details Source

5. Optionally Configure Authentication System

6. Configure SMTP Server for Workflow Email Notications (Optional)

7. Configure Risk Analysis and Mitigation

8. Configure Miscellaneous Settings

9. Define Number Ranges for Request Numbering

10. Create Role Attributes

11. Upload Roles from SAP Backend Systems via Spreadsheet

2 – Upload Inital Data into CUP (1/2)

> Upload two initial data files in xml format. The first file is called
> *AE_init_clean_and_insert_data.xml*

> The second one is *AE_init_append_data.xml*

> There is a third file required when using the SoD or UAR Review features: *AE_init_append_data_ForSODUARReview.xml*

➢ Make sure you have already created a JCo in the Web Dynpro Content Administrator as described in *Post-Installation Slide Deck – SPM* page 17-21

➢ Click on the magnifying glass.

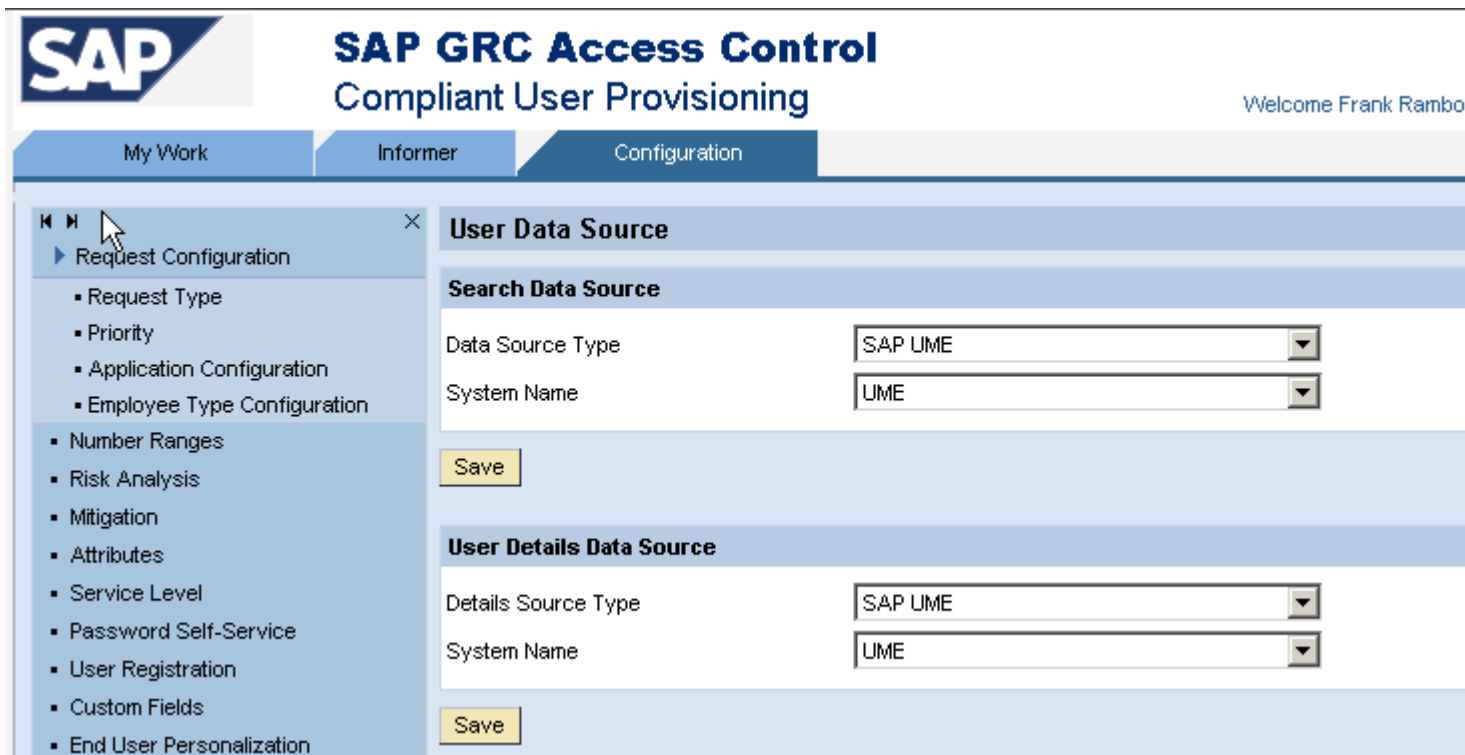> Select the JCo destination that corresponds to the RAR system connector pointing to your SAP backend system.

➢ Maintain the highlighted fields with arbitrary dummy entries and enter a *Short Description* and a *Description.* Finally click on *Test Connection* to verify.

4 – Set User Data Source & User Details Sources

> **One** User Data Source & **Multiple** User Details Sources are supported

> Select from SAP(-HR), UME, LDAP, SAPEP, JDE, Oracle, Peoplesoft

> Make sure you have created the corresponding system connectors.

5 – Optionally Configure Authentication System for Requester Authentication

> If you want the requesters to authenticate first (recommended) before they can create a request in CUP, select your authentication system, for example UME of the AC5.3 server. Make sure you have created the corresponding system connector.

6 – Configure SMTP Server for Workflow Email Notications (Optional)

- ➢ In case you want to receive emails for workflows you can configure this optionally

- ➢ Go to Configuration → Workflow → SMTP Server

- ➢ Enter the SMTP server

- ➢ Choose an optional sender ID (otherwise a standard one will be used)

- ➢ Note: as of AC 5.3 <u>SP6 and higher</u> two additional fields appear
  - ➢ Application URL
  - ➢ Redirection URL
  - ➢ These URLs are used for SPNego redirection and the (application) URL of a Portal in case this applies to your system landscape
  - ➢ See also SAP Note 1252589

- ➢ See also next slide

6 – Configure SMTP Server for Workflow Email Notications (Optional)

> Configure Risk Analysis according to your requirements (next slide)

7 – Configure Risk Analysis and Mitigation (2/4) → Risk Analysis Configuration

- Configuration → Risk Analysis → Options:
  - Risk Analysis Type: Select *Permission Level*
  - Consider Mitigation Control: To start leave unchecked and revise later

- Configuration → Risk Analysis → Select Risk Analysis and Remediation Version:
  - Version: 5.3 Web Services
  - URI: http://<server>:<port>/VirsaCCRiskAnalysisService/Config1?wsdl&style=document
  - User Name: <admin user id with UME role VIRSA_CC_ADMINISTRATOR
  - Password: <admin password>
  - Perfrom Org. Rule Analysis: To start leave unchecked and revise later

- Configuration → Risk Analysis → Risk Analysis On Request Submission:
  - Perform Risk Analysis On Request: No

> Configure Mitigation according to your requirements (next slide)

> The flag „Allow Approvers …" allows approvers to approve requests containing risks. If it is unflagged all risks must be remediated or mitigated before approval.

SAP

SAP GRC Access Control
Compliant User Provisioning

Welcome Admin Access Controls

| My Work | Informer | Configuration | |

Mitigation

✓ Successfully saved Mitigation Configuration.

Select Options

Allow Approvers to Approve Access Despite any Conflicts	☐
Default Duration (Days) for the Mitigation Control	365
Mitigation URI	CCMitigation5_0Service/Config1?style=document
Risk Search URI	VirsaCCRisk5_0Service/Config1?style=document
Org. Rule Search URI	CCOrgRules5_3Service/Config1?style=document
Function Search URI	CCFunction5_0Service/Config1?style=document

Save

Left navigation:
- ▶ Request Configuration
  - Request Type
  - Priority
  - Application Configuration
  - Employee Type Configuration
- Number Ranges
- Risk Analysis
- **Mitigation**
- Attributes
- Service Level
- Password Self-Service
- User Registration
- Custom Fields

➢ Configuration → Mitigation

   ➢ Allow approvers to approve access despite any conflicts: Checked, revise later

   ➢ Default Duration (in days) for Mitigation Control: 30

   ➢ Mitigation URI:
   http://<server>:<port>/VirsaCCMitigation5_0Service/Config1?wsdl&style=document

   ➢ Risk Analysis URI:
   http://<server>:<port>/VirsaCCRisk5_0Service/Config1?wsdl&style=document

   ➢ Org. Rule Search URI:
   http://<server>:<port>/VirsaCCOrgRules5_3Service/Config1?wsdl&style=document

   ➢ Function Search URI:
   http://<server>:<port>/VirsaCCFunction5_0Service/Config1?wsdl&style=document

8 – Configure Miscellaneous Settings (1/2)

> Note that the required workflow settings depend which of the integration scenarios you want to use:

> Integration with RAR: Approval for creation/changes to risks, mitigation control objects and assignment of mitigation controls to users

> Integration with ERM: Role Approval

> Specific CUP features that require configuration: SOD and UAR Review, Role Reaffirm

Miscellaneous Configuration

Parameters

Language*	English
Log Level*	ERROR
Cache Job Time Interval in Seconds*	5 [Note: Need to Restart the Server]
Background Job Time Interval In Minutes*	1 [Note: Need to Restart the Server]

[Save] [Refresh Cache]

Workflow Types

Name	Description	Short Description	Exit URI	User Name	Password	Active
AE	Compliant User Provisioning	CUP				☑
MITICTRL	This is a workflow type for creatin	Mitigation Control	http://nwdemo2450.wdf.sap.corp:	ac_admin	••••••••••••••••••••	☑
MITIOBJ	This is a workflow type for creatin	Mitigation Control Assignment	http://nwdemo2450.wdf.sap.corp:	ac_admin	••••••••••••••••••••	☑
RE	Enterprise Role Management	ERM	http://nwdemo2450.wdf.sap.corp:	ac_admin	••••••••••••••••••••	☑
RISK	This is a workflow type for creatin	Risk	http://nwdemo2450.wdf.sap.corp:	ac_admin	••••••••••••••••••••	☑
ROLE_RFM	Role Reaffirm	Role Reaffirm				☑
SOD_REVIEW	SOD Review	SOD Review				☑
UAR_REVIEW	User Access Review	User Access Review				☑

[Save]

8 – Configure Miscellaneous Settings (2/2)

- Configuration → Miscellaneous
  - Parameters
    - Language: English (for example)
    - Log Level: Error (change, if needed for troubleshooting)
    - Cache Job Time interval in seconds: 5
    - Background Job Time Intervals in Minutes: 1
  - Workflow Types
    - AE: Checked
    - MITICTRL URL http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document, Checked[1]
    - MITIOBJ URL http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document , Checked[1]
    - RE http://<server>:<port>/AEWFExitServiceWS_5_2/Config1?wsdl&style=document , Checked
    - RISK URL http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document , Checked[1]
    - ROLE_RFM: Checked
    - SOD_REVIEW: Checked
    - UAR_REVIEW: Checked

- Configuration → Attachments
  - Only needed, if you want to allow for attachements sent with requests.
  - Folder: <Folder name on server to store attachements>

---

[1] These workflow types appear only after import of AE_init_append_data_CC.xml (refer to post-installation slide deck RAR page 44).

9 – Define Number Ranges for Request Numbering

> Without Number Ranges, no request can be submitted!

> You need to define a number range and activate it.

> Before importing roles we recommend creating role attributes.

> Maintain Role Attributes in Configuration → Roles → Attributes

> Company

Role Attribute		
Company		
☐ Company ID*	Short Description*	Description
☐ SAP	SAP	SAP

> Functional Area

Role Attribute		
Functional Area		
☐ Name*	Short Description*	Description
☐ FI	Financial	Financial
☐ PR	Purchasing	Purchasing

> Application Area

Role Attribute			
Application Area			
☐ Name*	Short Description*	Description	System
☐ ERP	ERP ECC 6.0	ERP ECC 6.0	DCX

> Business Process

> Note: if you plan to integrate with Risk Analysis and Remediation (RAR) you should choose two-character values for the name like in RAR

Role Attribute

Business Process

	Name*	Short Description*	Description	Owner / Approver	Alternate Approver	Application Area
☐	PR	Procure to Pay	Procure to Pay	GRC_ADMIN	D043805	ERP
☐	SD	Oder to Cash	Oder to Cash	GRC_ADMIN	D043805	ERP

> Business Sub-Process

Role Attribute

Business Sub-Process

	Name*	Short Description*	Description	Business Process
☐	PR01	Vendor Master Maintenance	Vendor Master Maintenance	Procure to Pay
☐	PR02	Production Order Processing	Production Order Processing	Procure to Pay
☐	PR03	Service Master Maintenance	Service Master Maintenance	Procure to Pay
☐	PR04	PO Approval	PO Approval	Procure to Pay
☐	SD01	Customer Master Data	Customer Master Data	Order to Cash
☐	SD02	Delivery Processing	Delivery Processing	Order to Cash
☐	SD03	Sales Rabates	Sales Rabates	Order to Cash
☐	SD04	Sales Document Release	Sales Document Release	Order to Cash

> Functional Area and Company is optional

11 – Upload Roles from SAP Backend Systems via Spreadsheet (1/2)

> We recommend to upload roles from your backend systems via spreadsheet

> This way you upload only the roles you need within CUP and can maintain role attributes more conveniently in the spreadsheet rather than maintaining each role after role import in CUP manually.

> The role attribute used in the spreadsheet must be created prior to upload

> Upload roles in Configuration → Roles → Import

Next Steps

> Now you are ready to create workflows in Compliant User Provisioning

> Before you do this in the system, we advice designing them first as flow charts on paper and involving all stakeholders in this phase.

> Also cater for exceptions like „no approver defined", or „auto-provisioning failed" to handle error situations. Include „Detour" and „Escape Routes" to handle error situations in your workflows!

Copyright 2009 SAP AG
All rights reserved