SAP Governance, Risk & Compliance
Access Control 5.3

Post-Installation Slide Deck
→ Compliant User Provisioning
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
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 Notifications (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
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`
3 – Create and Test System Connectors (1/3)

Create Connectors with SLD Integration

- 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.
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.
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 SP6 and higher 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 Notifications (Optional)

SAP GRC Access Control
Compliant User Provisioning

SMTP Server

Enter Email Server Name

Email Server Name: iwdfvm2070.wdf.sap.corp

Enter Email Notification Sender

☐ System Email ID

Application URL


Save  Cancel
7 – Configure Risk Analysis and Mitigation (1/4)

→ Risk Analysis

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
  - User Name: `<admin user id with UME role VIRSA_CC_ADMINISTRATOR`
  - Password: `<admin password>`
  - Perform 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.
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:
- Function Search URI:
  http://<server>:<port>/VirsaCCFunction5_0Service/Config1?wsdl&style=document
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
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
    - MITIOBJ URL http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document, Checked
    - RE http://<server>:/AEWFExitServiceWS_5_2/Config1?wsdl&style=document, Checked
    - RISK URL http://<server>:/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document, Checked
    - ROLE_RFM: Checked
    - SOD_REVIEW: Checked
    - UAR_REVIEW: Checked

- Configuration ➔ Attachements
  - 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
## 10 – Create Role Attributes (2/3)

### Company, Funct. Area, Application Area

#### Company

<table>
<thead>
<tr>
<th>Role Attribute</th>
<th>Company</th>
<th>Company ID</th>
<th>Short Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SAP</td>
<td>SAP</td>
<td>SAP</td>
</tr>
</tbody>
</table>

#### Functional Area

<table>
<thead>
<tr>
<th>Role Attribute</th>
<th>Functional Area</th>
<th>Name</th>
<th>Short Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>FI</td>
<td>Financial</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR</td>
<td>Purchasing</td>
<td>Purchasing</td>
</tr>
</tbody>
</table>

#### Application Area

<table>
<thead>
<tr>
<th>Role Attribute</th>
<th>Application Area</th>
<th>Name</th>
<th>Short Description</th>
<th>Description</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ERP</td>
<td>ERP ECC 6.0</td>
<td>ERP ECC 6.0</td>
<td>DCX</td>
</tr>
</tbody>
</table>
10 – Create Role Attributes (3/3)

- **Business Process**

- **Business Sub-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.

- **Functional Area and Company is optional**
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.
11 – Upload Roles from SAP Backend Systems via Spreadsheet (2/2)

- 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!