Post-Installation

→ Enterprise Role Management
→ Part I: Configuration
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 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

   - **Part I: Configuration**
   - **Part II: Testing SAP GRC Default Process**

5. Start Customizing Access Control 5.3 according to customer requirements
Post-Installation Activities
- Enterprise Role Management -

1. Upload UME Roles (→ Refer to Post-Installation Slide Deck for RAR)
2. Initial System Data Import into ERM
3. Configuration of Miscellaneous Settings in ERM
4. Configuration for Compliant User Provisioning
5. System Landscape Definition
6. Run Initial Synchronization Background Jobs
7. Definition of Role Attributes
8. Role Methodology & Condition Groups
9. Definition of Approval Criteria
10. Definition of Naming Conventions
11. Definition of Organizational Value Mapping
Upload the following xml files with Initial System Data:

- *RE_init_clean_and_insert_data.xml* - select the **Clean and Insert** option.
- *RE_init_append_data.xml* - select the **Append** option.
- *RE_init_methodology_data.xml* - select the **Append** option.

This fills data into:
- Config. → Role Status
- Config. → Methodology
- Config. → Configuration Settings
# 3 – Configuration for RAR & Miscellaneous (1/5)

### Role Attributes
- Business Process
- Sub-Process
- Functional Area
- Custom Fields
- Project Metadata
- Role Status
- Naming Convention
- Org Value Mapping
- Condition Groups
- Methodology
- System Landscape
- Workflow
- Log History
- Background Jobs

### Miscellaneous
- Transaction Import
- Mass Role Import
- Role Usage Synchronization
- Initial System Data
- Configuration Settings
- Administration
- Migration from 4.0
- Upgrade

### Allow role generation with violations
This option enables you to configure whether the role can be generated despite violations. If you set this configuration to "No", then you will not be able to generate the role unless all the role violations are taken care of.

| Allow role generation with violations | No |

### Allow Role Generation on Multiple Systems
This option enables you to configure whether a role can be generated on multiple systems.

| Allow Role Generation on Multiple Systems | Yes |

### Use logged on user credentials for role generation
This option enables you to configure whether the logged-on user credentials should be used during role generation. If this option is set to "No", then the target back-end system user ID and password is used.

| Use logged on user credentials for role generation | No |

### Analysis Type
This option enables you to specify a default analysis level. If you set this configuration value to "Object", then the risk analysis by default will be performed at the object level; otherwise, it will be performed at the "Task" level.

| Analysis Type | Object |

### Web Service Info, for CC Risk Analysis
This option allows you to set Web Service URL for risk analysis.

- Do not use Web Service: CC displayed on the same server
- Use Web Service

### Web Service Info, for CC Transaction Usage
This option allows you to set Web Service URL for transaction usage.

<table>
<thead>
<tr>
<th>Web Service URL</th>
<th><a href="http://localhost:2450/servicesOutV1WebSvc.svc">http://localhost:2450/servicesOutV1WebSvc.svc</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>ac_admin</td>
</tr>
<tr>
<td>Password</td>
<td>**********</td>
</tr>
</tbody>
</table>

### Web Service Info, for CC Mitigation Control
This option allows you to set Web Service URL for Mitigation Control. Make sure that mitigation web service and risk analysis service exist on the same server.

<table>
<thead>
<tr>
<th>Web Service URL</th>
<th><a href="http://localhost:2450/servicesOutV1WebSvc.svc">http://localhost:2450/servicesOutV1WebSvc.svc</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>ac_admin</td>
</tr>
<tr>
<td>Password</td>
<td>**********</td>
</tr>
</tbody>
</table>
3 – Configuration for RAR & Miscellaneous (2/5)

- Configuration → Miscellaneous (Check SAP Note 1175227):
  - Allow Role Generation with Violations: **No** (customer selection)
  - Allow Role Generation with Multiple Systems: **Yes**
  - Use Logged-in user credentials for Role Generation: **No** (→ Backend RFC User Logon)
  - Analysis Type: Object (Risk Analysis on object or only transaction level)
  - Web Service Info for CC Risk Analysis
    - EJB Call: Select **Do not use Web Service; Risk Analysis and Remediation deployed on the same server.**
  - Web Service Info for Risk Analysis and Remediation Transaction Usage
    - User Name: <User ID> (with UME Role **VIRSA_CC_ADMINISTRATOR**)
    - Password: <password>
  - Web Service Info for CC Mitigation Control
    - URL: http://<server>:<port>/VirsaCCMitigation5_0Service/Config1?wsdl&style=document
    - User Name: <User ID> (with UME Role **VIRSA_CC_ADMINISTRATOR**)
    - Password: <password>
### 3 – Configuration for RAR & Miscellaneous (3/5)

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Service Info. for CC Functions</strong></td>
<td></td>
<td>This option allows you to set Web Service URL for Functions.</td>
</tr>
<tr>
<td><strong>Web Service URL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>cc_admin</td>
<td></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>********</td>
<td></td>
</tr>
<tr>
<td><strong>Web Service Info. for AE Workflow</strong></td>
<td></td>
<td>This option allows you to set Workflow URL for role approval.</td>
</tr>
<tr>
<td><strong>Workflow URL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allow editing org. level values for derived roles</strong></td>
<td></td>
<td>This option enables you to edit org. level values for derived roles. If the value is set to &quot;Yes&quot;, you cannot edit org. Level values for derived roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Allow you to add a function to an authorization</strong></td>
<td></td>
<td>This option allows you to add functions to authorizations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Add objects to a role</strong></td>
<td></td>
<td>This option enables you to add objects to a role directly. If the value is set to &quot;Yes&quot;, then you can add objects directly to the role authorization data, or else you can add objects to a role only by adding functions and/or transactions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ticket number after authorization data changes</strong></td>
<td></td>
<td>This option allows you to specify whether you need to enter a ticket number after making additions or changes to the authorization data in a role. If the value for this option is set to &quot;Yes&quot;, then after you have any additions or changes you make to the authorization data in a role, you will be prompted for a ticket number. If the value for this option is set to &quot;No&quot;, then you will not be prompted for a ticket number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3 – Configuration for RAR & Miscellaneous (4/5)

- Configuration → Miscellaneous:
  - Web Service Info for CC Functions
    - URL: http://<server>:<port>/VirsaCCFunction5_0Service/Config1?wsdl&style=document
    - User Name: <User ID> (with UME Role VIRSA_CC_ADMINISTRATOR)
    - Password: <password>
  - Web Service Info for AE Workflow
    - URL:
      http://<server>:<port>/AEWFRequestSubmissionService_5_2/Config1?wsdl&style=document
    - Allow Editing Org. Level values for derived roles: Yes (customer selection)
    - Allows you to add function to an authorization: Yes
    - Add objects to a role: Yes
    - Ticket number after authorization data changes: Yes (customer selection)
3 – Configuration for RAR & Miscellaneous (5/5)

- Configuration → Miscellaneous:
  - Allow Editing Role Authorizations in PFCG: Yes
  - Upload Directory: <path on AC server for file uploads from ERM> (only temporarily needed when upgrading from RE5.2. In ERM 5.3 all attachments are saved in the database)
  - Log Level: Error (customer selection)
  - Default Language: English (customer selection)
  - Number of concurrent background jobs: 3
  - Allows you to attach files to a role definition
    - This option allows you to attach files to a role: Yes
    - This option allows you to set the file size (in KB): 1000
To enable workflows for role approval, the file `AE_init_append_data_RE.xml` - with Append option - must be uploaded in CUP → Configuration → Initial System Data.
4 – Configuration for CUP (2/8) ➔ Check Request Type for ERM

- In CUP ➔ Configuration ➔ Request Configuration ➔ Request Type
- Check that Request Type *RE_ROLE_APPROVAL* exists
- Make sure it has workflow type *RE*
Check, if a priority `RE_HIGH` for workflow type „RE“ exists

If not, create it accordingly.
Go to CUP → Configuration → Workflow → Initiator and create an initiator

- Workflow type: RE
- Attributes: Request Type = RE Role Approval & Priority = RE_HIGH
Go to CUP → Configuration → Workflow → Custom Approver Determinator

- CAD Type: Web Service
- Workflow Type: RE
- URI: http://<server>:<port>/AEWFCADApproversServiceWS_5_2/Config1?wsdl&style=document
- User Name / Password: User with AC Administrator UME-Roles
4 – Configuration for CUP (6/8)
→ Create a Stage for ERM Role Approval WF

➤ Create at least one stage for ERM approval workflow

➤ Go to CUP → Configuration → Workflow → Stage and create a stage
  ➤ Workflow Type: RE
  ➤ Approver Determinator: ERM_ROLE_APPROVER (created just before)
Create a path for ERM approval workflow

Go to CUP → Configuration → Workflow → Path and create a path

- Workflow Type: RE
- Number of Stages: 1 (but more possible)
- Initiator: ROLE_APPROVAL (created just before)
- Active: Checked
- Stage 1: ERM_ROLE_APPROVER
Go to CUP → Configuration → Miscellaneous

- Exit URI: http://<server>:<port>/AEWFExitServiceWS_5_2/Config1?wsdl&style=document
- User Name: User with AC Administrator UME-Roles
- Password: <password>
- Active: Checked

### Workflow Types

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Short Description</th>
<th>Exit URI</th>
<th>User Name</th>
<th>Password</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE</td>
<td>Access Enforcer</td>
<td>Access Enforcer</td>
<td></td>
<td>ac_admin</td>
<td>**********</td>
<td>✔️</td>
</tr>
<tr>
<td>MITCTR</td>
<td>This is a workflow type for creating Mitigation Control</td>
<td>Mitigation Control</td>
<td>http://&lt;server&gt;:&lt;port&gt;/wdfwvr2450.wdf.sap.corp:50000</td>
<td>ac_admin</td>
<td>**********</td>
<td>✔️</td>
</tr>
<tr>
<td>MITOBJ</td>
<td>This is a workflow type for creating Mitigation Object</td>
<td>Mitigation Object</td>
<td>http://&lt;server&gt;:&lt;port&gt;/wdfwvr2450.wdf.sap.corp:50000</td>
<td>ac_admin</td>
<td>**********</td>
<td>✔️</td>
</tr>
<tr>
<td>RISK</td>
<td>This is a workflow type for creating Risk</td>
<td>Risk</td>
<td>http://&lt;server&gt;:&lt;port&gt;/wdfwvr2450.wdf.sap.corp:50000</td>
<td>ac_admin</td>
<td>**********</td>
<td>✔️</td>
</tr>
<tr>
<td>RROLE_RPM</td>
<td>Role Reassign</td>
<td>Role Reassign</td>
<td>http://&lt;server&gt;:&lt;port&gt;/wdfwvr2450.wdf.sap.corp:50000</td>
<td>ac_admin</td>
<td>**********</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Create for each backend system a System in ERM → Configuration → System Landscape → Systems.

Make sure you have already created JCo destination in Netweaver stack with correct naming as explained in *Post-Installation Slide Deck – SPM* page 17-21.

Select System Type SAP and check SLD Connector checkbox and click on magnifying glass to select JCo from SLD.
Maintain manually the following fields: Application Server Host, System Number – otherwise the profile generator won’t be started correctly – and SAP Version.

Now, maintain the remaining empty mandatory fields Password, Message Server name with arbitrary dummy values. They are directly read from SLD.

Click on “Test Connection” and save.
First create a System Landscape for each backend system landscape you want to create/maintain/generate roles for.

Then assign systems to it – normally the DEV and PRD backend – here in the example we only have a DEV called AR1. Then Associate Actions (next slide).
Per backend system landscape you have to assign to two different Actions:

- **Role Risk Analysis** → Assigned to PRD, because risks are defined with respect to the productive systems. In the example below we had only one system available.

- **Role Generation** → Assigned DEV, because roles still need to undergo their usual testing, which starts in DEV (unit tests), then continues in QA (integration test) etc.
6 – Run Initial Synchronization Background Jobs

- There are three types of (static) background jobs:
  - **Org Value Sync**: Synchronizes the organizational values in Enterprise Role Management with the SAP ERP backend system → Takes 2 min.
  - **Transaction/Object/Field Sync**: Synchronizes the Transaction, Object, and Field values with the SAP backend system → Takes on slow hardware up to 5 hours!
  - **Activity Sync**: Synchronizes Activity field values → Takes 5 min.

- We recommend running these jobs in sequential order. So, wait until a job has completed before you start the next one.
Go to ERM → Configuration → Role Attributes → Business Processes and create business processes you want to use as role attributes.

Then create Sub-Processes you want to use as role attributes.
Definition of Role Attributes (2/3)

→ Map Sub-Processes to Business Processes

- Return to ERM → Configuration → Role Attributes → Business Processes and click on Process Mapping to map Sub-Processes to Business Processes
Go to ERM → Configuration → Role Attributes → Functional Areas and create Functional Areas you want to use as role attributes.

Optionally you can create custom fields to have additional role attributes available.

Also, you can create project or release attributes for your roles.
There is already a pre-defined **Methodology Process** available in ERM.

We recommend using this process for first tests.

Then you can create one or **Multiple Methodology** processes according to your business requirements.

If you create multiple **Methodology Processes**, then you need to create **Condition Groups** and assign one or multiple **Condition Groups** to each **Methodology Process**. However, you cannot assign the same **Condition Group** to multiple **Methodology Processes**.

A **Condition Group** is a set of role attributes. Once the role attributes are defined for a new role and match a **Condition Group** the system will apply the corresponding **Methodology Process** for further creation steps of this role.
Approval Criteria are stored as Groups and are used to determine role approver based on the role attributes.

In the example we determine role approver based on the role attribute Business Process and map to our BP *Procure to Pay (PR)* the responsible approvers. However, you could any combination of role attributes to determine role approvers from.
Assign approvers to each business process
The result is a list of business processes, each one assigned with an approver and optionally an alternate approver. In our example the list has only one item.

To these approvers CUP will send approval requests in the role approval step of the methodology process to.
Create naming Conventions for single, composite & derived roles as well as for profile in your different system landscapes and determine whether the naming convention shall be enforced (recommended).
Create an example Organizational Value Mapping to have it later available to test the role derivation feature. However, as of AC 5.3 you can also derive roles without org value mappings.

The idea here is that a primary organizational level exists, which other organizational levels in the same business context depend from.

Example: A Company may have a business unit for central European region having company codes 1000 to 2000. The org level *Purchasing Org.* depends on the values of CC: Purch. Org. 1000 belongs to the range 1000 – 2000 of CCs. It can be mapped to these values.