SAP Governance, Risk & Compliance
Access Control 5.3

Post-Installation
→ Enterprise Role Management
→ Part I: Configuration

THE BEST-RUN BUSINESSES RUN SAP™

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 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

2 – Import of Inital System Data
→ Upload Initial Data into ERM

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:

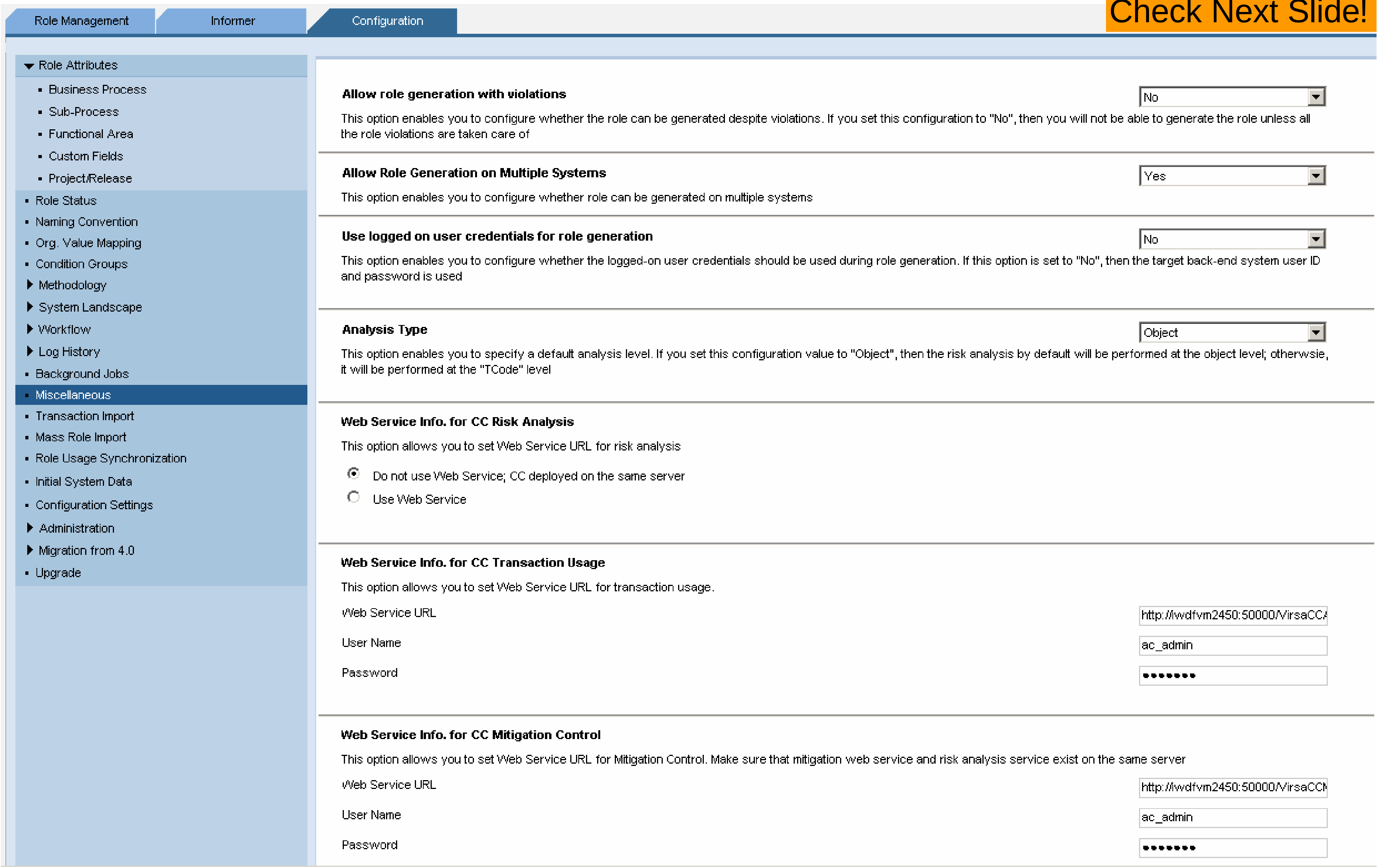
Config. → Role Status

Config. → Methodology

Config. → Configuration Settings

3 – Configuration for RAR & Miscellaneous (1/5)

Check Next Slide!

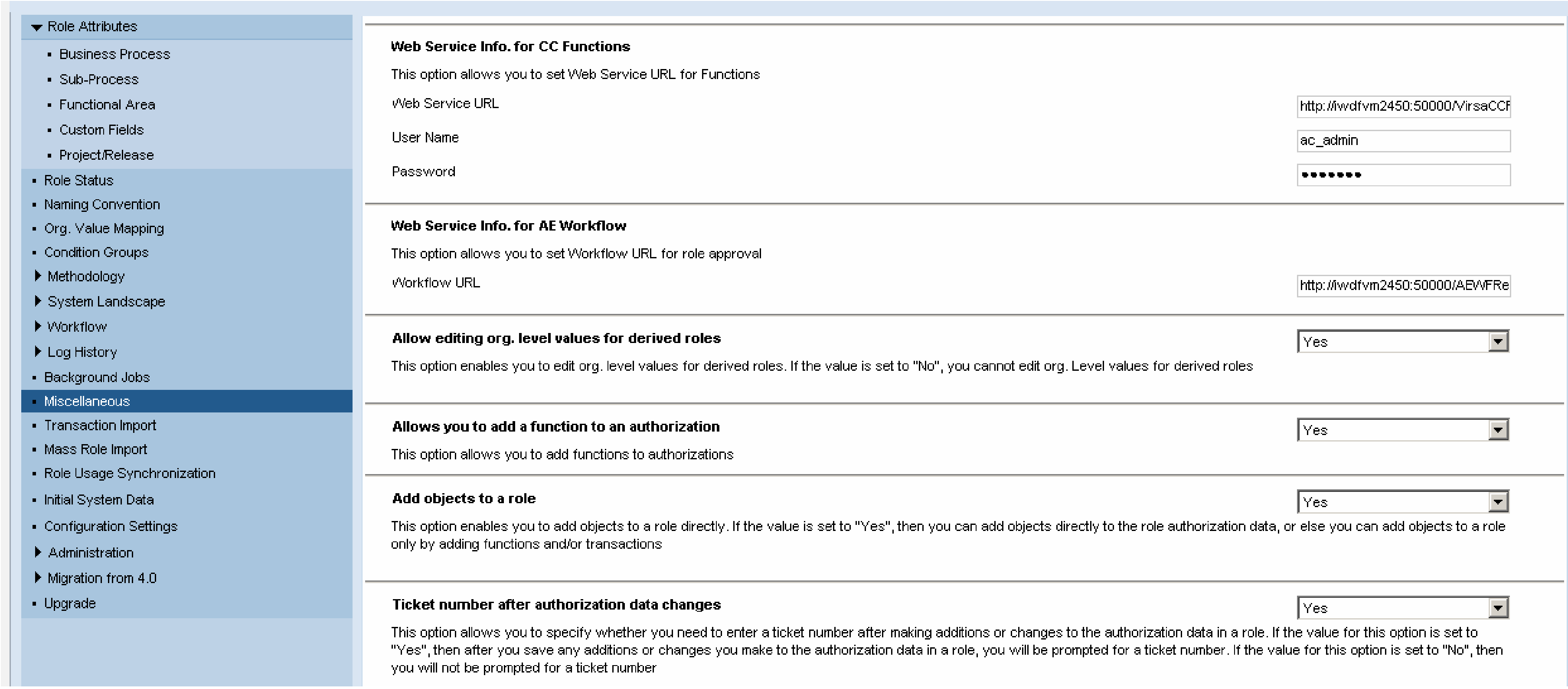


3 – Configuration for RAR & Miscellaneous (2/5)

- 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
    - URL: http://<server>:<port>/VirsaCCActionUsageService/Config1?wsdl&style=document
    - 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)

Check Next Slide!

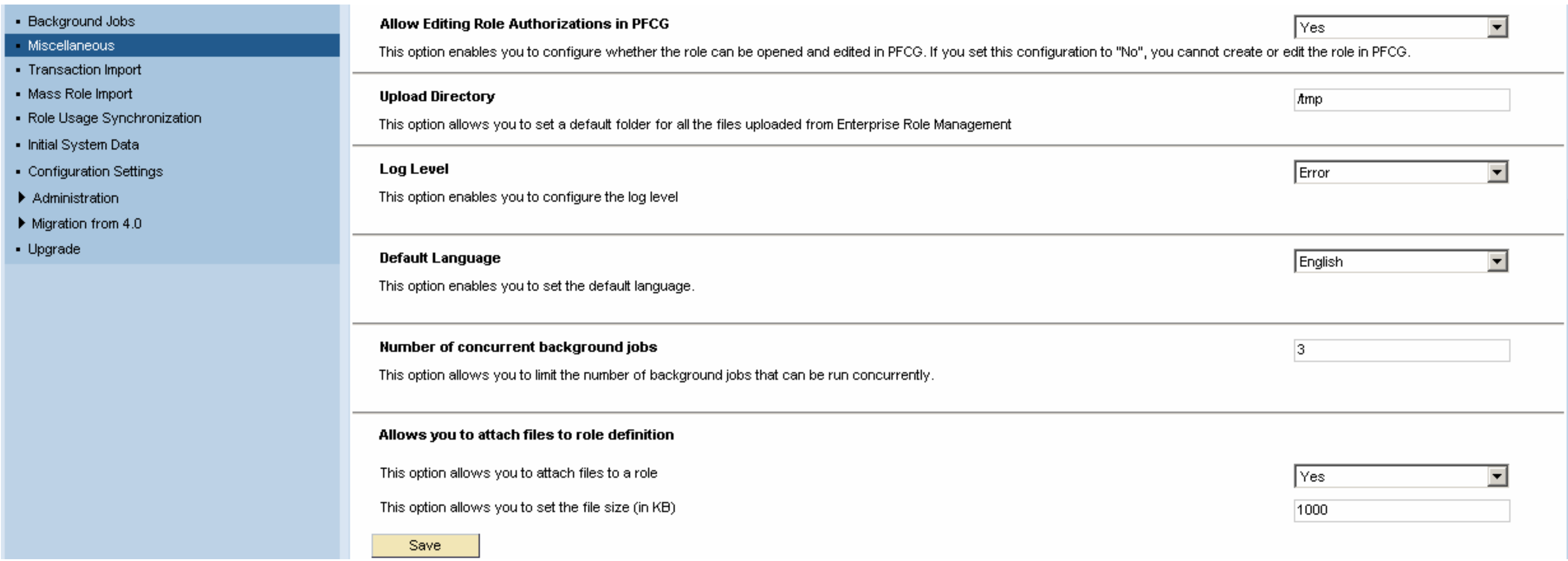


3 – Configuration for RAR & Miscellaneous (4/5)

- 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)

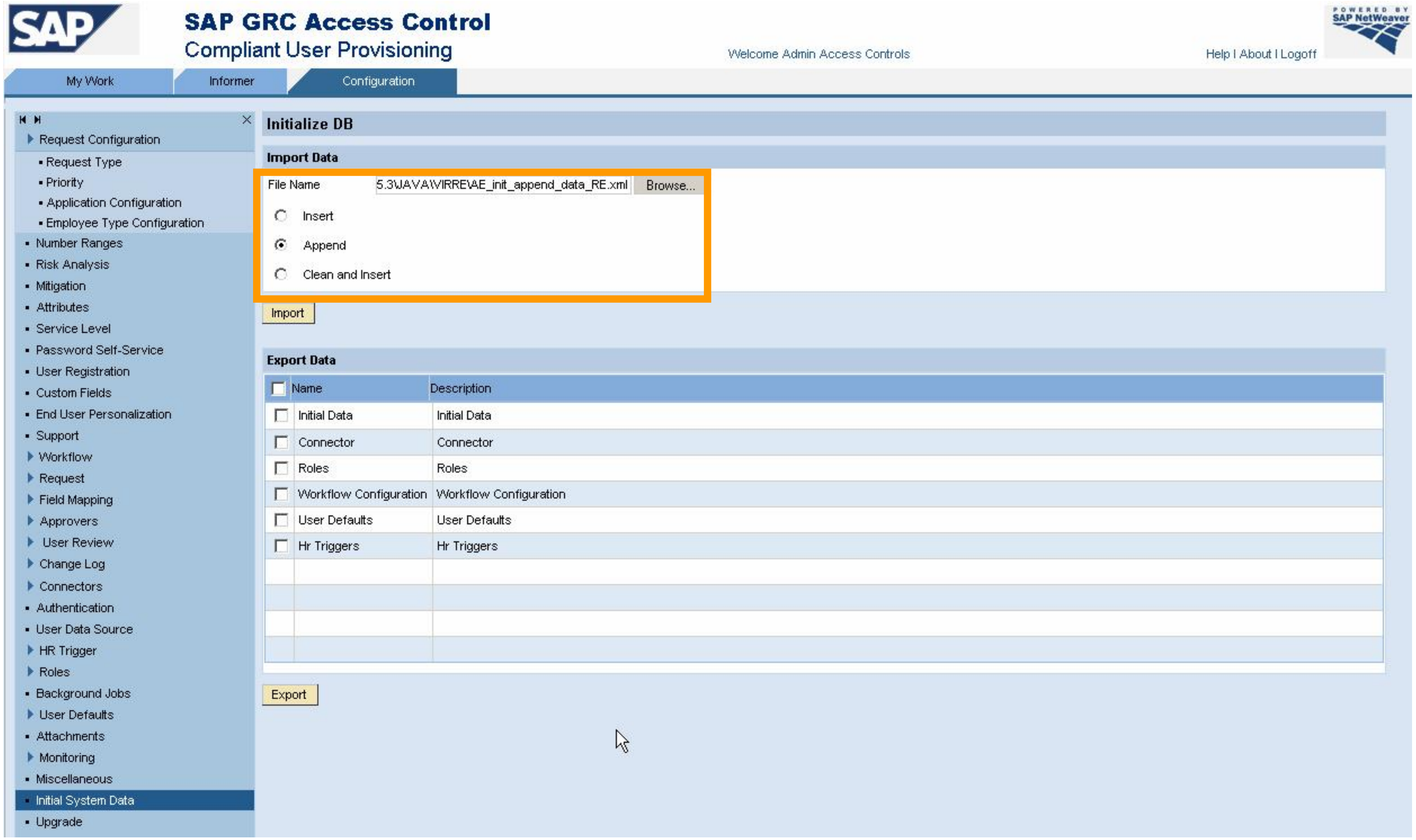
3 – Configuration for RAR & Miscellaneous (5/5)

- 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 attachements 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**



4 – Configuration for CUP (1/8)
→ Upload Initial Data into CUP

➢ To enable workflows for role approval the file *AE_init_append_data_RE.xml* - with **Append** option - must uploaded in **CUP** → Configuration → Initial System Data

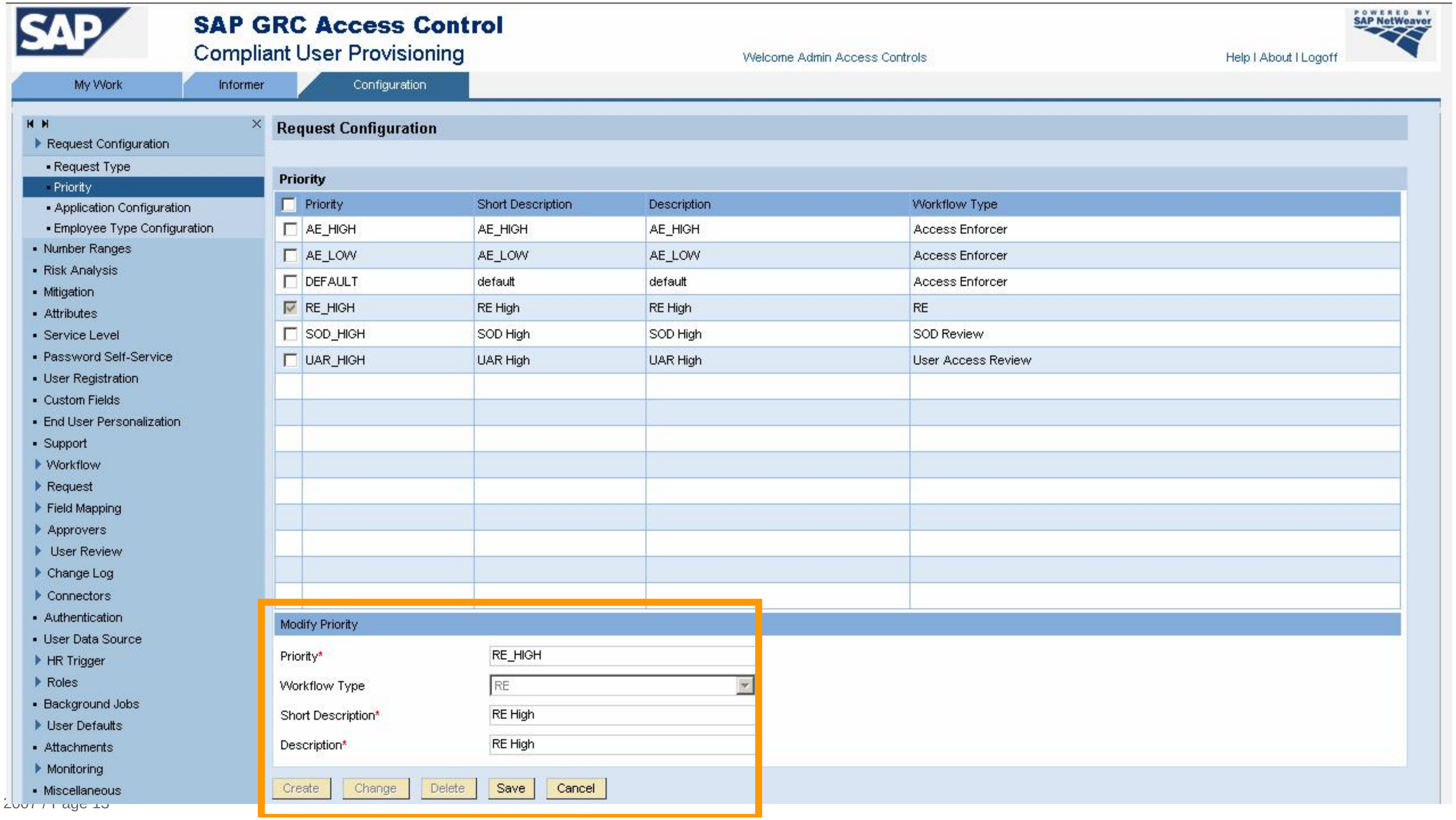


4 – Configuration for CUP (2/8) → Check Request Type for ERM

- In CUP → Configuration →Request Configuration → Request Type
- Check that Request Type *RE_ROLE_APPROVAL* exists
- Make sure it has workflow type *RE*

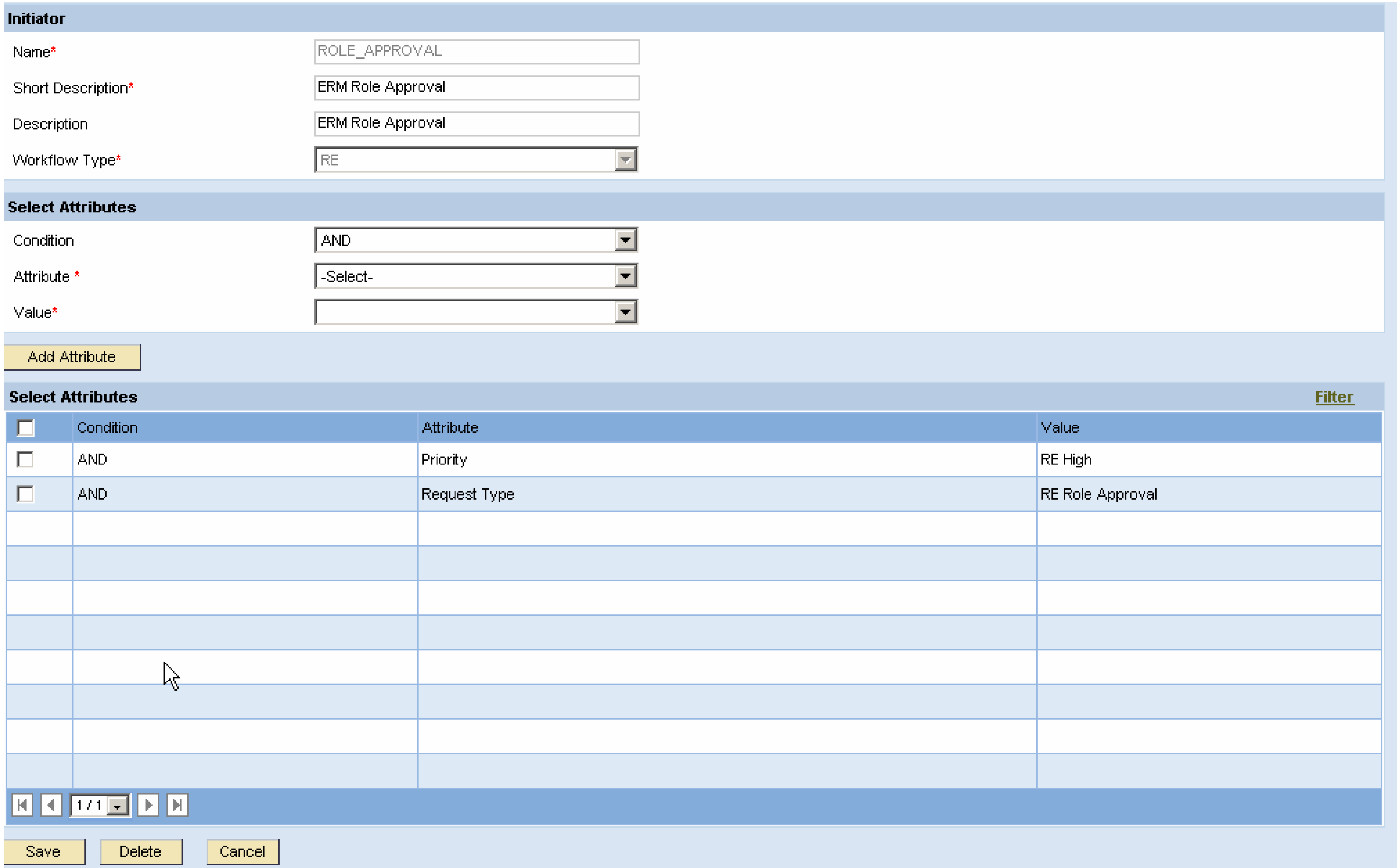
4 – Configuration for CUP (3/8)
→ Check, if Priority for ERM exists

- Check, if a priority *RE_HIGH* for workflow type „*RE*“ exists
- If not, create it accordingly.



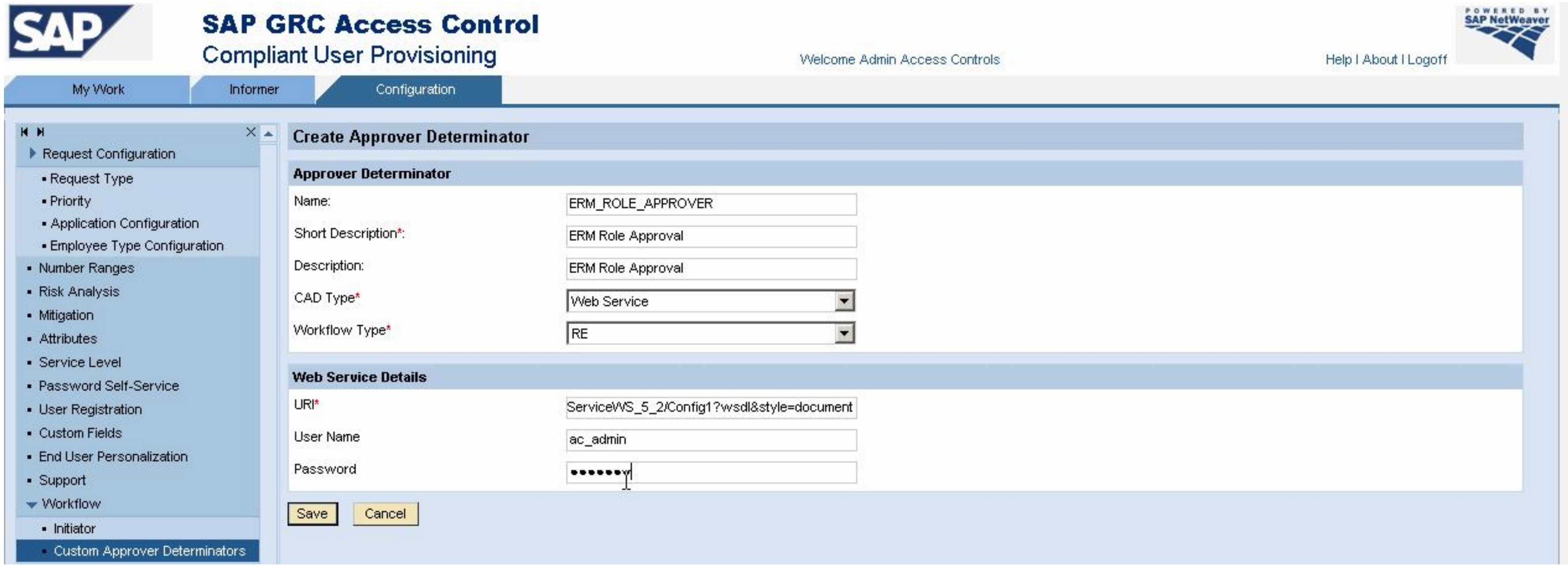
4 – Configuration for CUP (4/8)
→ Create a workflow initiator for ERM

- Go to CUP → Configuration → Workflow → Initiator and create an initiator
  - Workflow type: RE
  - Attributes: Request Type = RE Role Approval & Priority = RE_HIGH



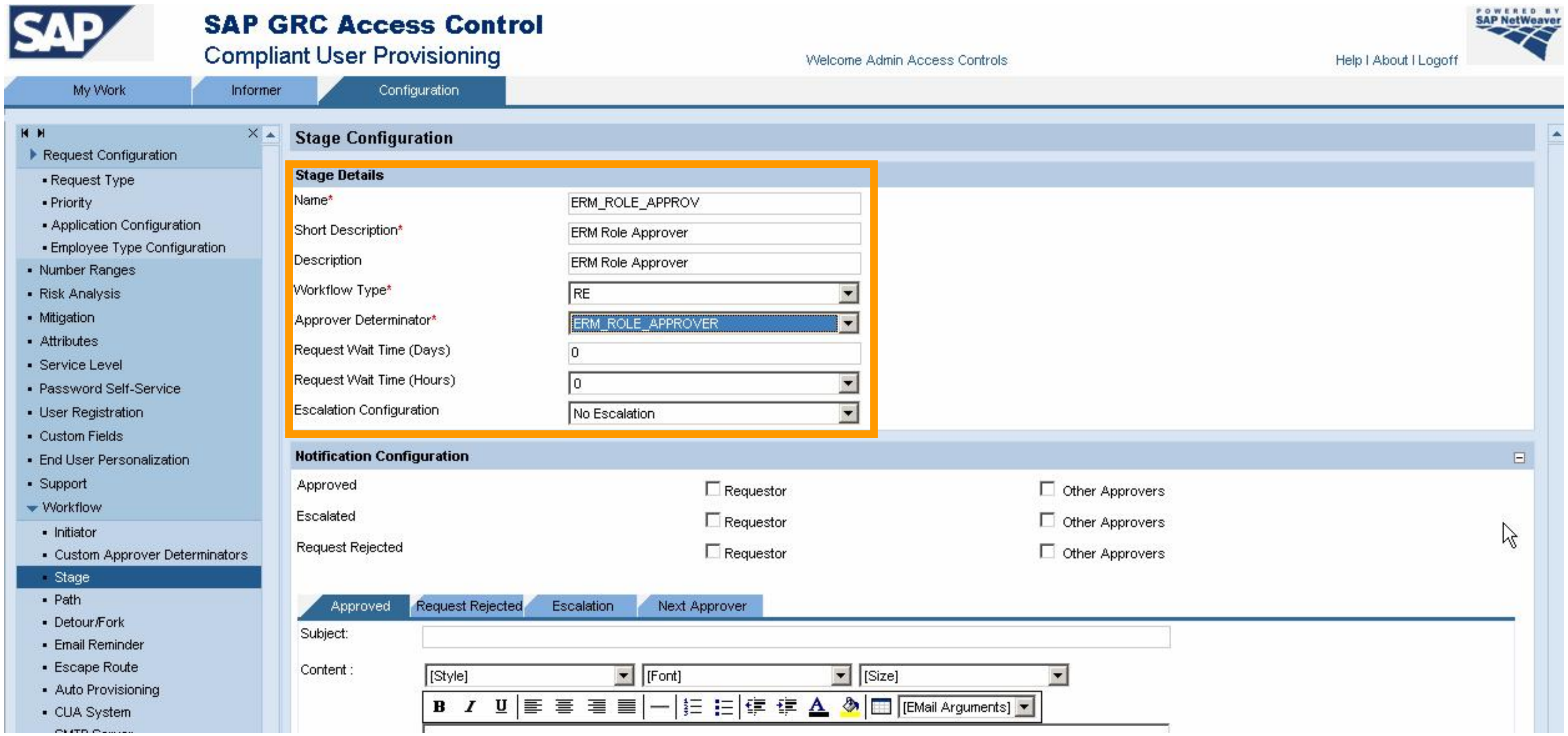
4 – Configuration for CUP (5/8) → Create a CAD for ERM

- 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



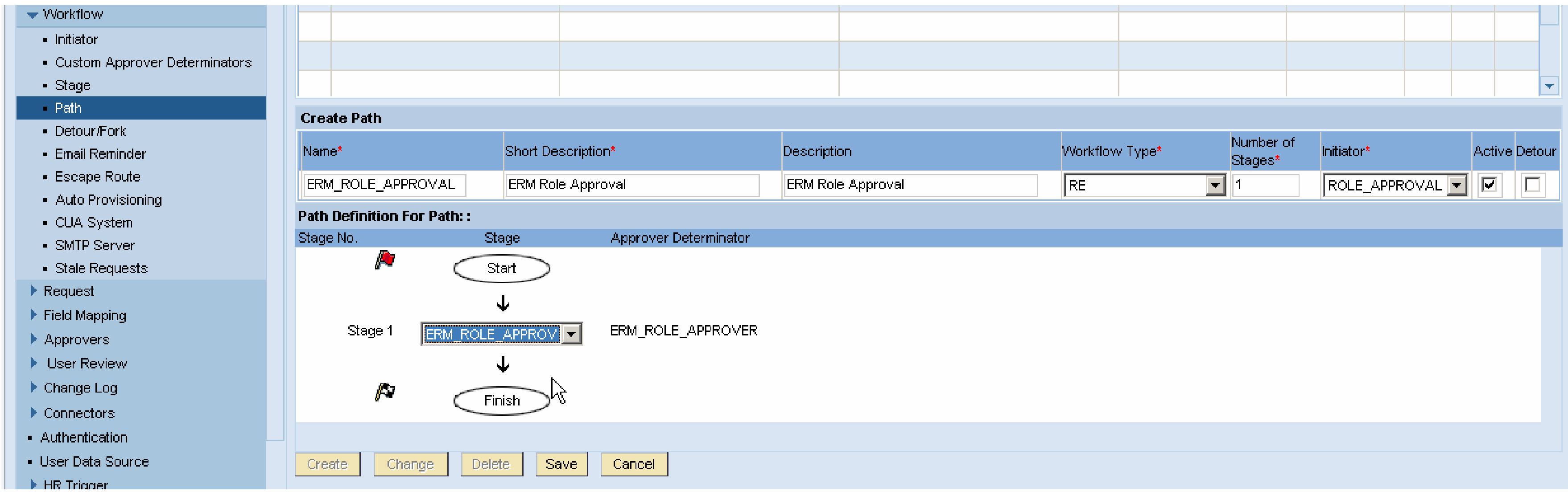
4 – Configuration for CUP (6/8) → Create a Stage for ERM Role Approval WF

- Create at least one stage for ERM approval workflow
- Go to CUP → Configuration → Workflow → Stage and create a stage
  - Worklow Type: RE
  - Approver Determinator: ERM_ROLE_APPROVER (created just before)



4 – Configuration for CUP (7/8)
→ Create a Path for ERM Role Approval WF

- Create a path for ERM approval workflow
- Go to CUP → Configuration → Workflow → Path and create a path
  - Worklow Type: RE
  - Number of Stages: 1 (but more possible)
  - Initiator: ROLE_APPROVAL (created just before)
  - Active: Checked
  - Stage 1: ERM_ROLE_APPROVER



4 – Configuration for CUP (8/8)
→ Configure Exit Web Service

- 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

Name	Description	Short Description	Exit URI	User Name	Password	Active
AE	Access Enforcer	Access Enforcer				☑
MITICTRL	This is a workflow type for creatin	Mitigation Control	http://iwdfvm2450.wdf.sap.corp:5	ac_admin	••••••••••••••••••••	☑
MITIOBJ	This is a workflow type for creatin	Mitigation Object	http://iwdfvm2450.wdf.sap.corp:5	ac_admin	••••••••••••••••••••	☑
RE	Role Expert	RE	/iwdfvm2450.wdf.sap.corp:50000	ac_admin	••••••••••••••••••••	☑
RISK	This is a workflow type for creatin	Risk	http://iwdfvm2450.wdf.sap.corp:5	ac_admin	••••••••••••••••••••	☑
ROLE_RFM	Role Reaffirm	Role Reaffirm				☑
SOD_REVIEW	SOD Review	SOD Review	http://iwdfvm2450.wdf.sap.corp:5	ac_admin	••••••••••••••••••••	☑
UAR_REVIEW	User Access Review	User Access Review	http://iwdfvm2450.wdf.sap.corp:5	ac_admin	••••••••••••••••••••	☑

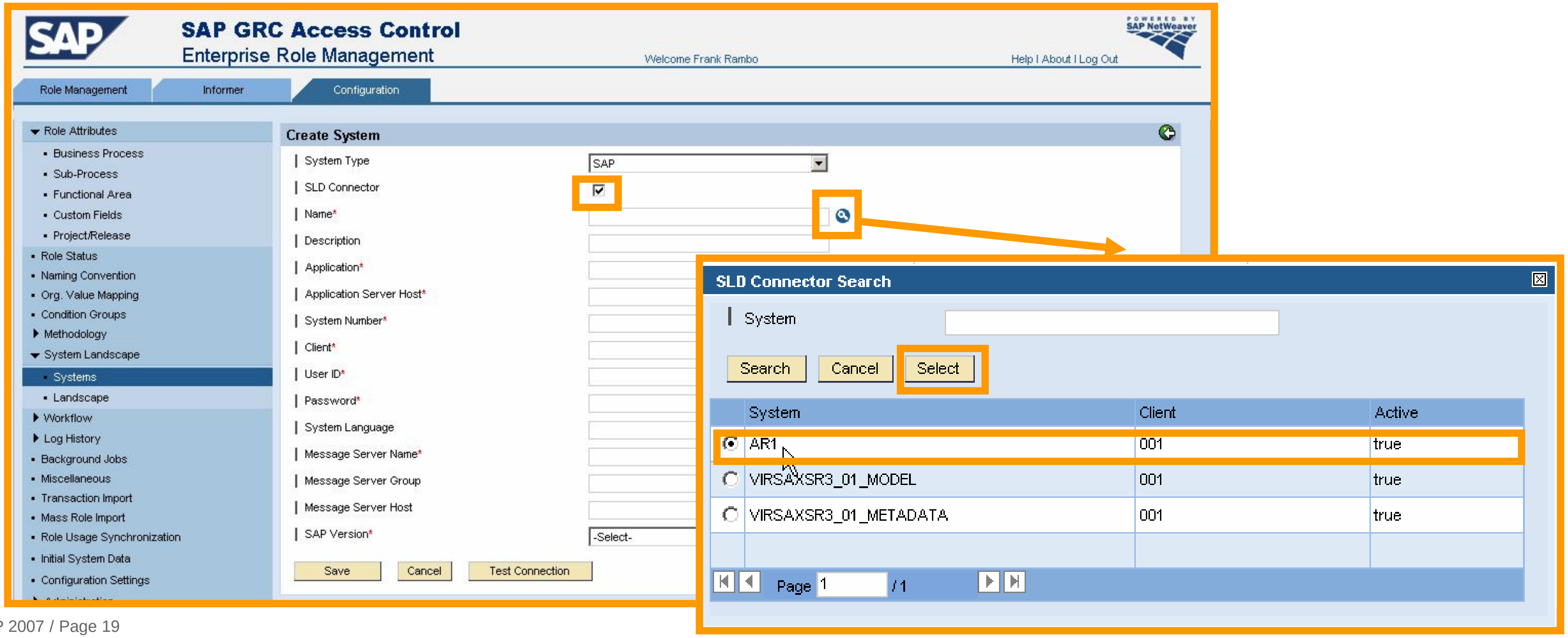
Save

5 – System Landscape Definition (1/4) → Create Systems with SLD Integration

- 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.

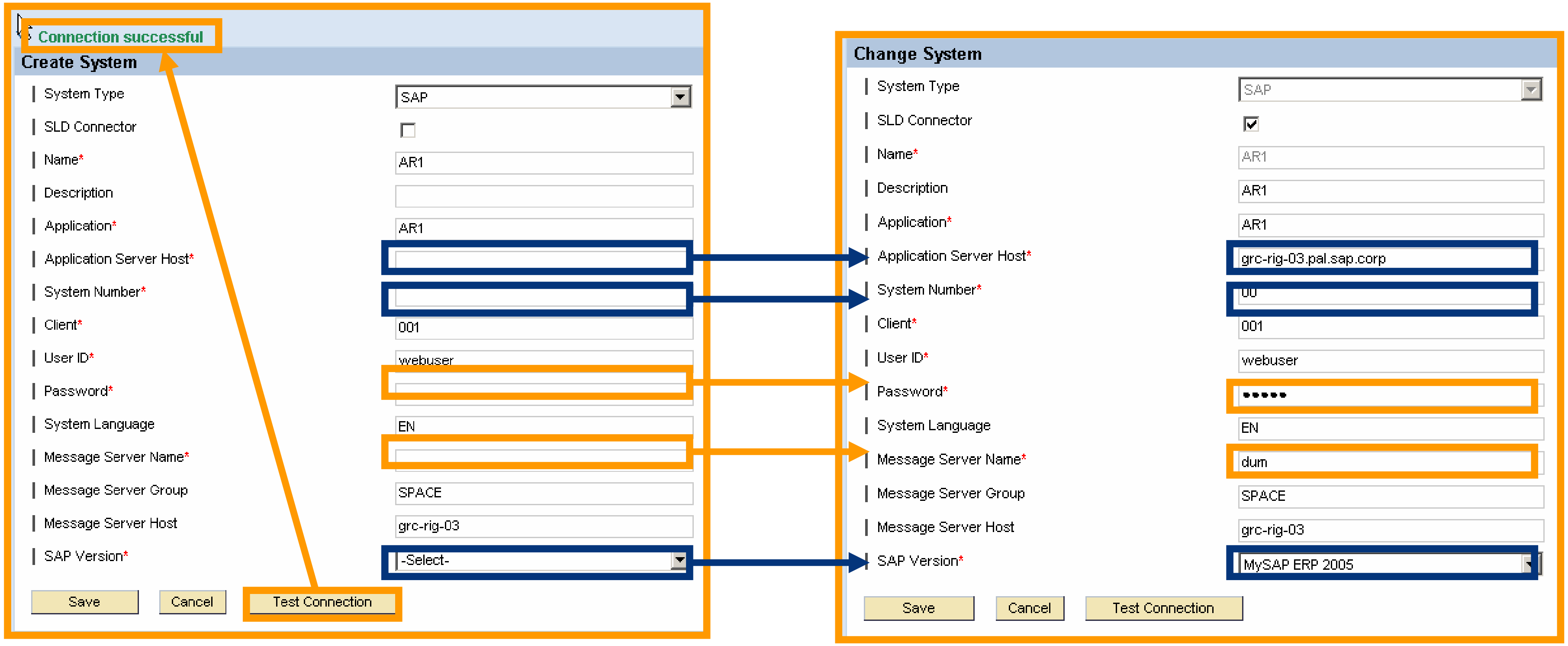


5 – System Landscape Definition (2/4)
→ Test Connection and Fill-In Dummy Values

- 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.

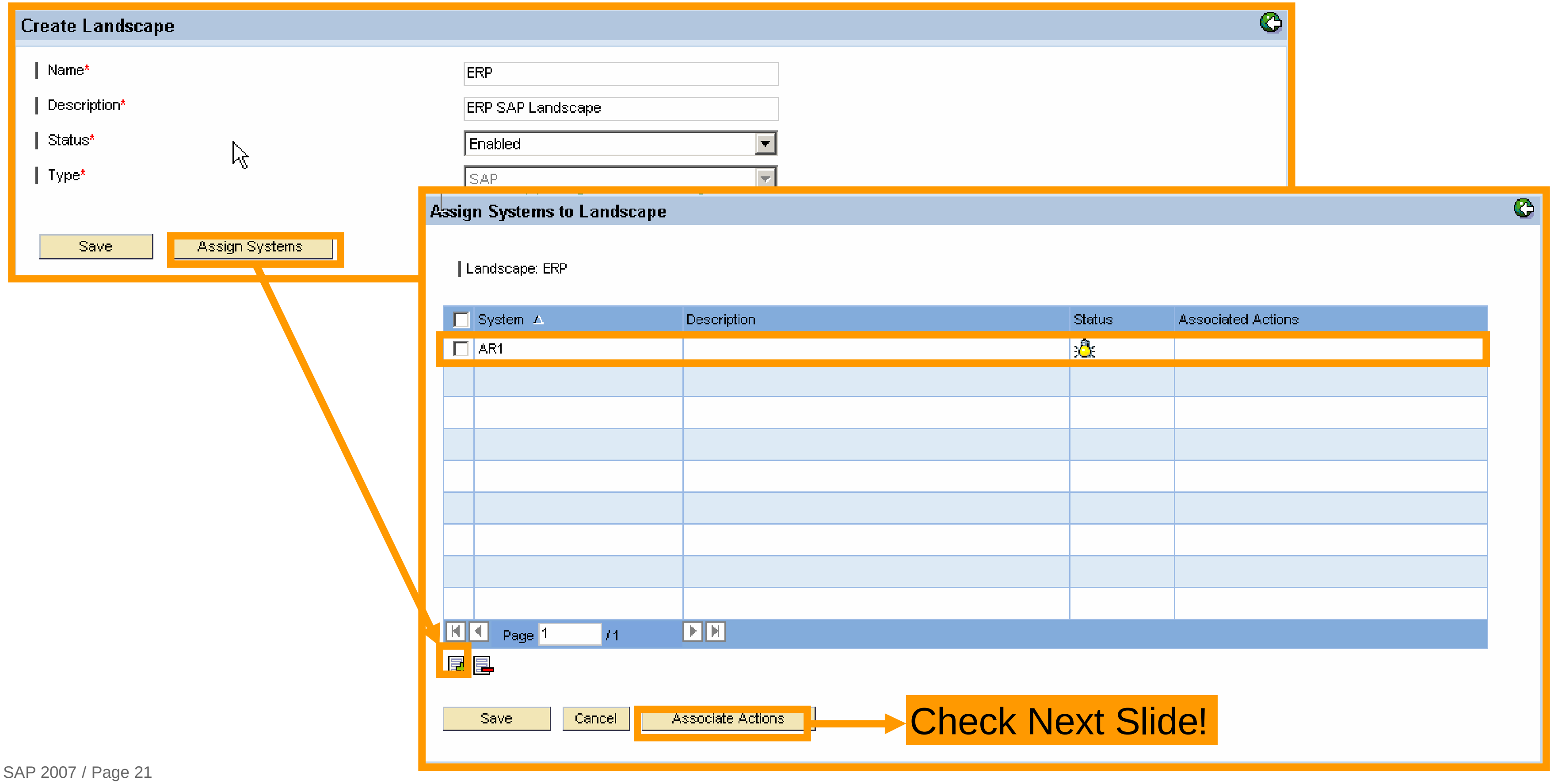
- Click on "Test Connection" and save.



5 – System Landscape Definition (3/4)
→ Create System Landscape

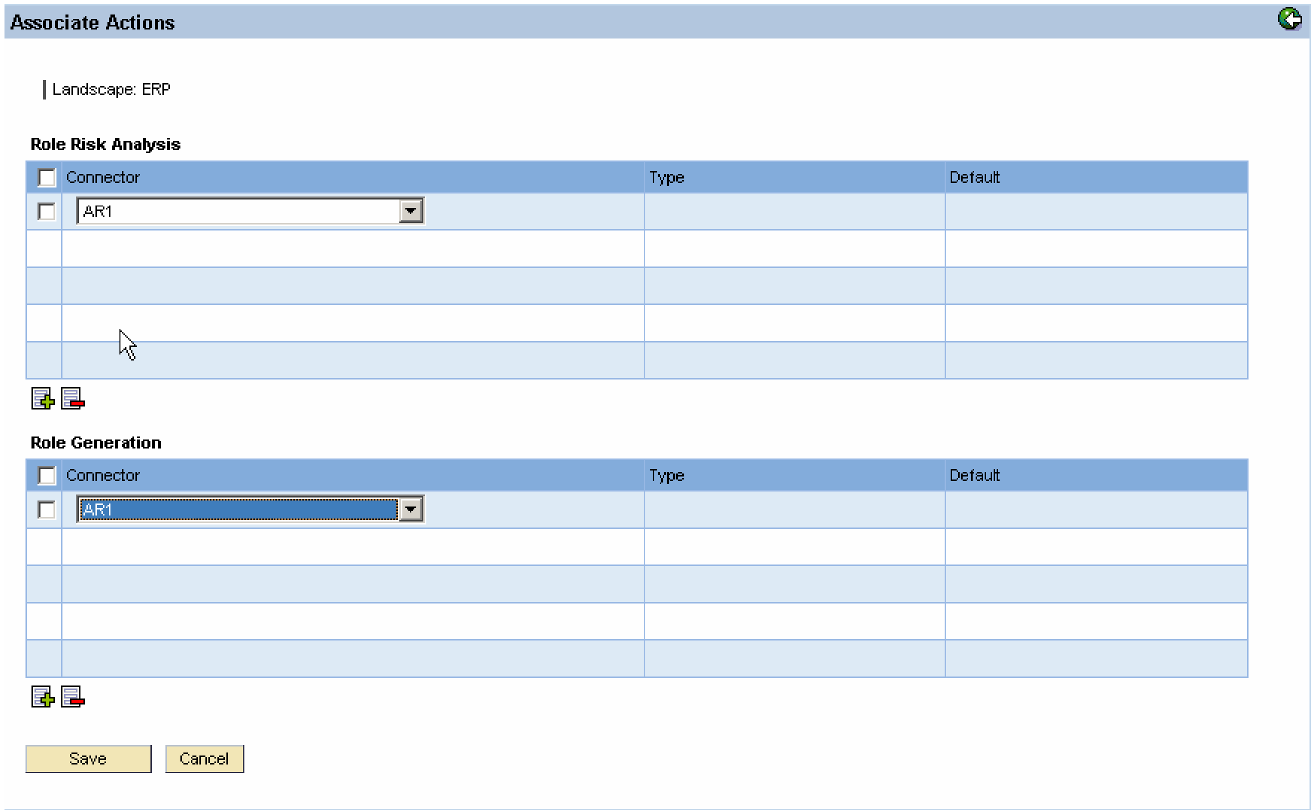
- First create a System Landscape for each backend system landscape you want to create/maintain/generate roles for.

- 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)



5 – System Landscape Definition (4/4) → Assign Systems to Actions

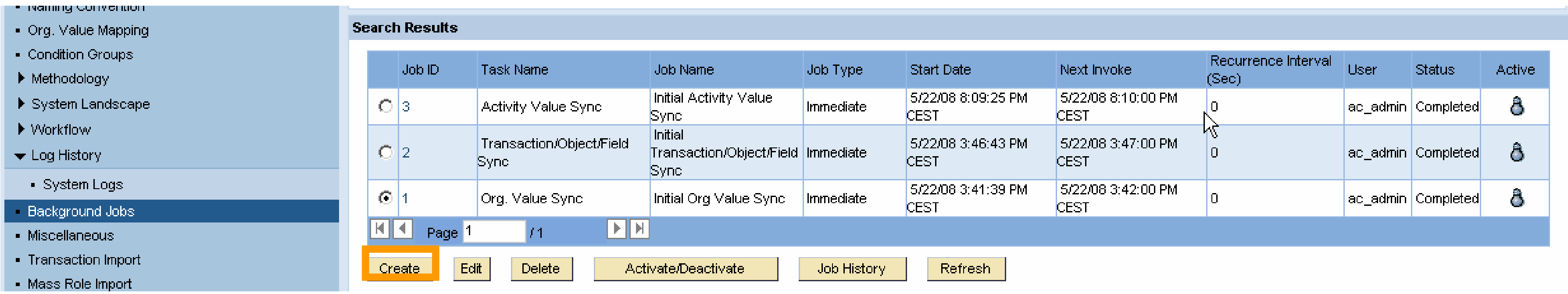
- Per backend system landscape you have to assign to two different Actions:
  - **Role Risk Analysis →** Assigned to PRD, because risks are defined with respect to the productive systems. In the example below we had only one system available.
  - **Role Generation →** Assigned DEV, because roles still 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

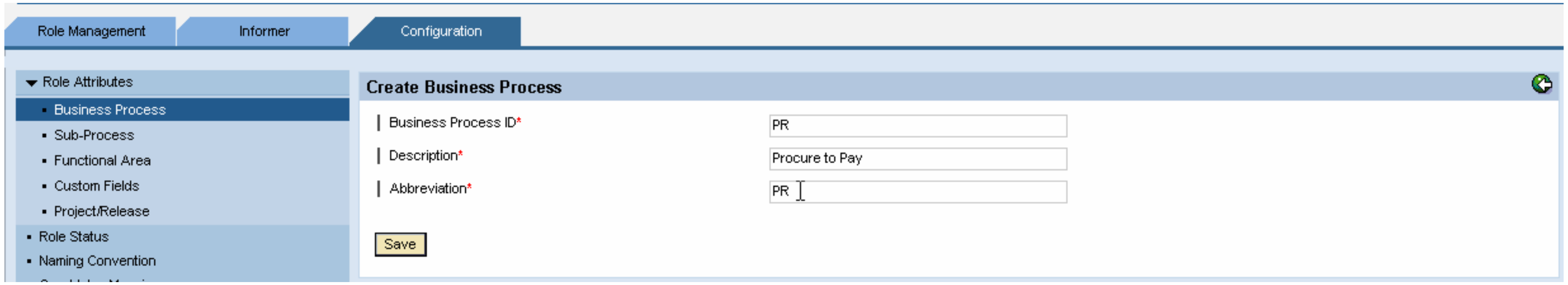
- There are three types of (static) background jobs:
  - **Org Value Sync:** Synchronizes the organizational values in Enterprise Role Management with the SAP ERP backend system → Takes 2 min.
  - **Transaction/Object/Field Sync:** Synchronizes the Transaction, Object, and Field values with the SAP backend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

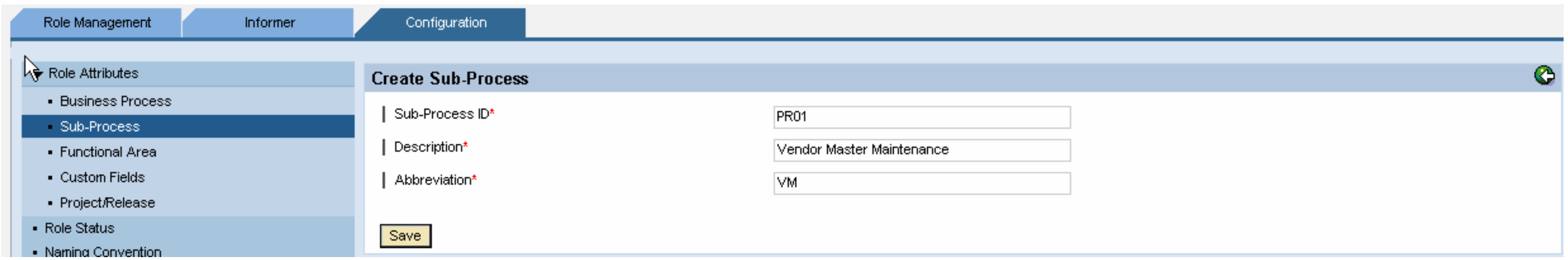


7 – Definition of Role Attributes (1/3)
→ Business Processes & Sub-Processes

- ➢ Go to ERM → Configuration → Role Attributes → Business Processes and create business processes you want to use as role attributes

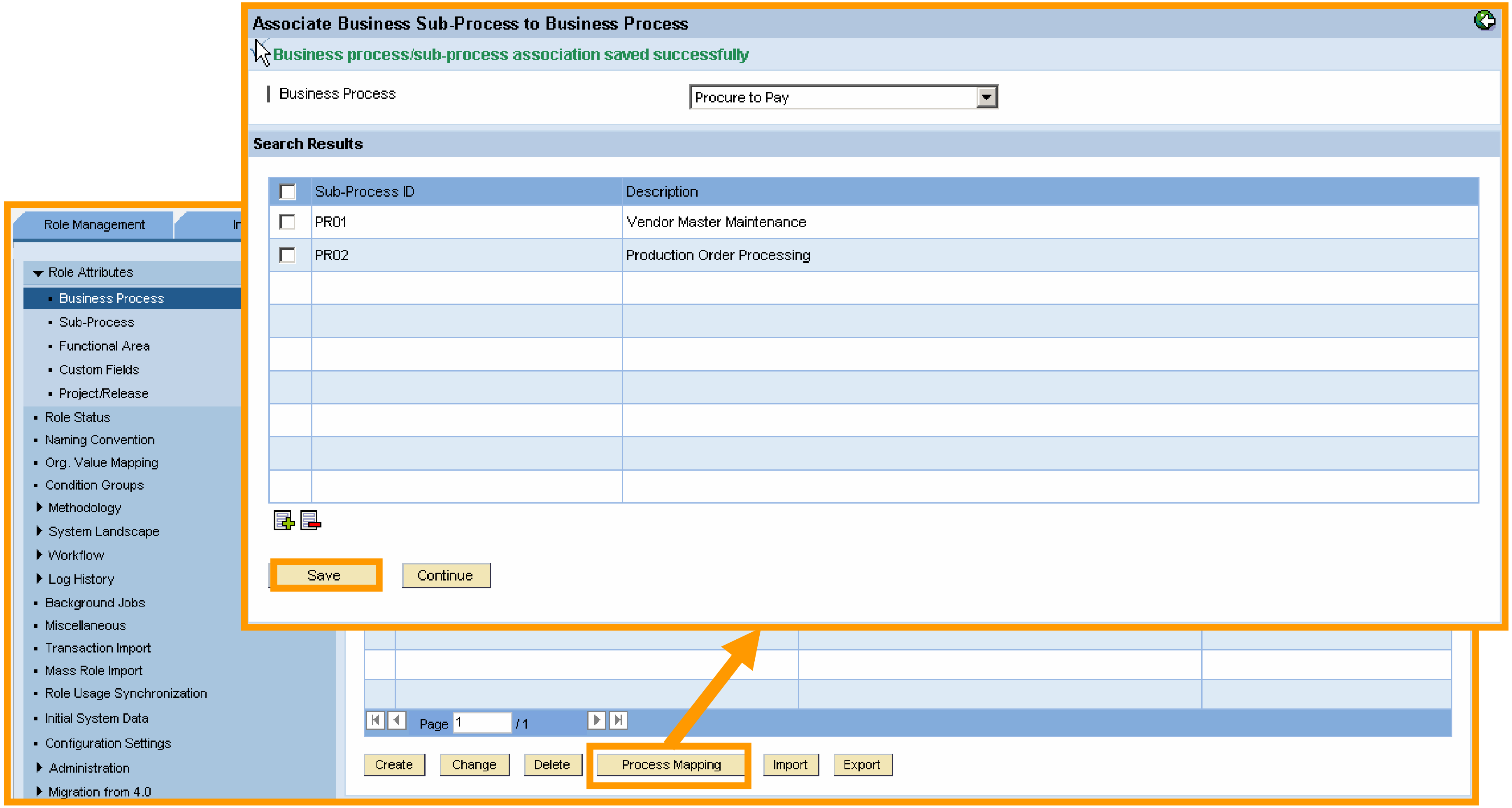


- ➢ Then create Sub-Processes you want to use as role attributes



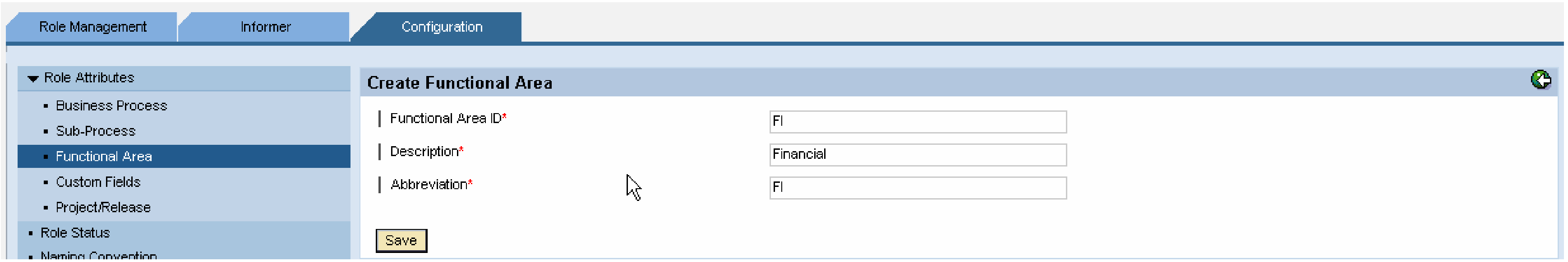
Definition of Role Attributes (2/3) → Map Sub-Processes to Business Processes

- Return to ERM → Configuration → Role Attributes → Business Processes and click on Process Mapping to map Sub-Processes to Business Processes



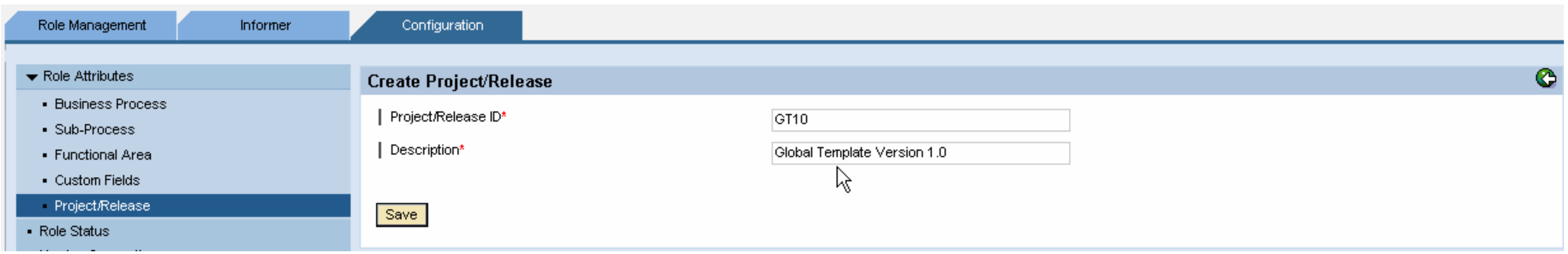
7 – Definition of Role Attributes (3/3) → Functional Areas, Custom Fields & More

- 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 you roles



8 – Role Methodology & Condition Groups

SAP

- There is already a pre-defined **Methodology Process** available in ERM.

Process

	Process	Description	Status	Default
☐	VIRSA DEFAULT PROCESS	Default process provided by Virsa		

- We recommend using this process for first tests.

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

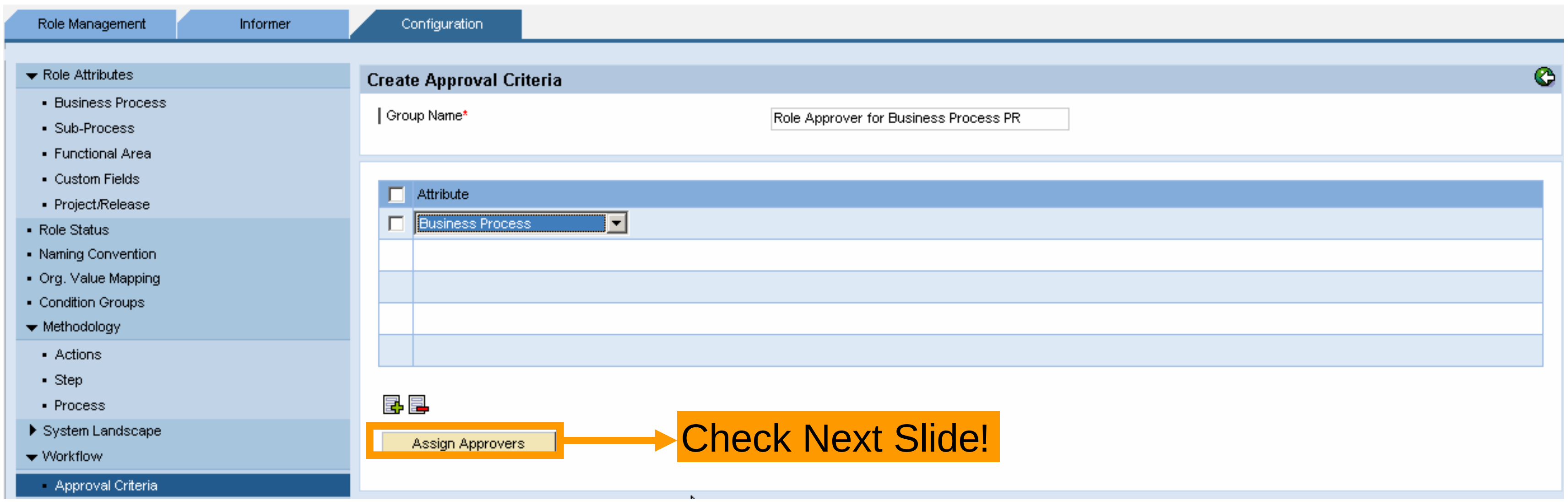
- If you create multiple **Methodoly Processes**, then you need to create **Condition Groups** and assign one or multiple **Condition Groups** to each **Methodology Process**. However, you cannot assign the same Condition Group to multiple **Methodology Processes**.

- 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.

9 – Definition of Approval Criteria (1/3)

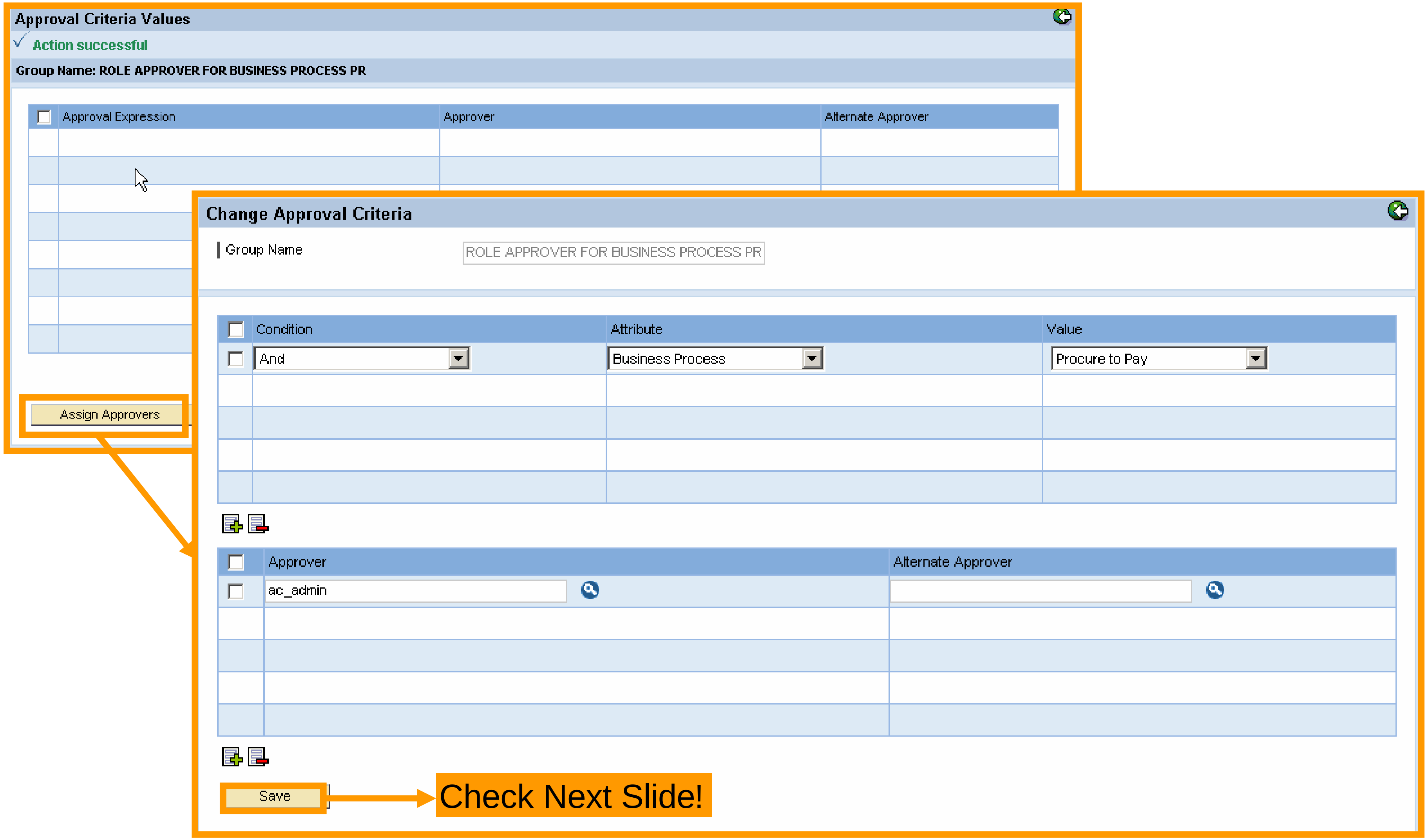
- Approval Criteria are stored as Groups and are used to determine role approver based on the role attributes.

- 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.



9 – Definition of Approval Criteria (2/3)

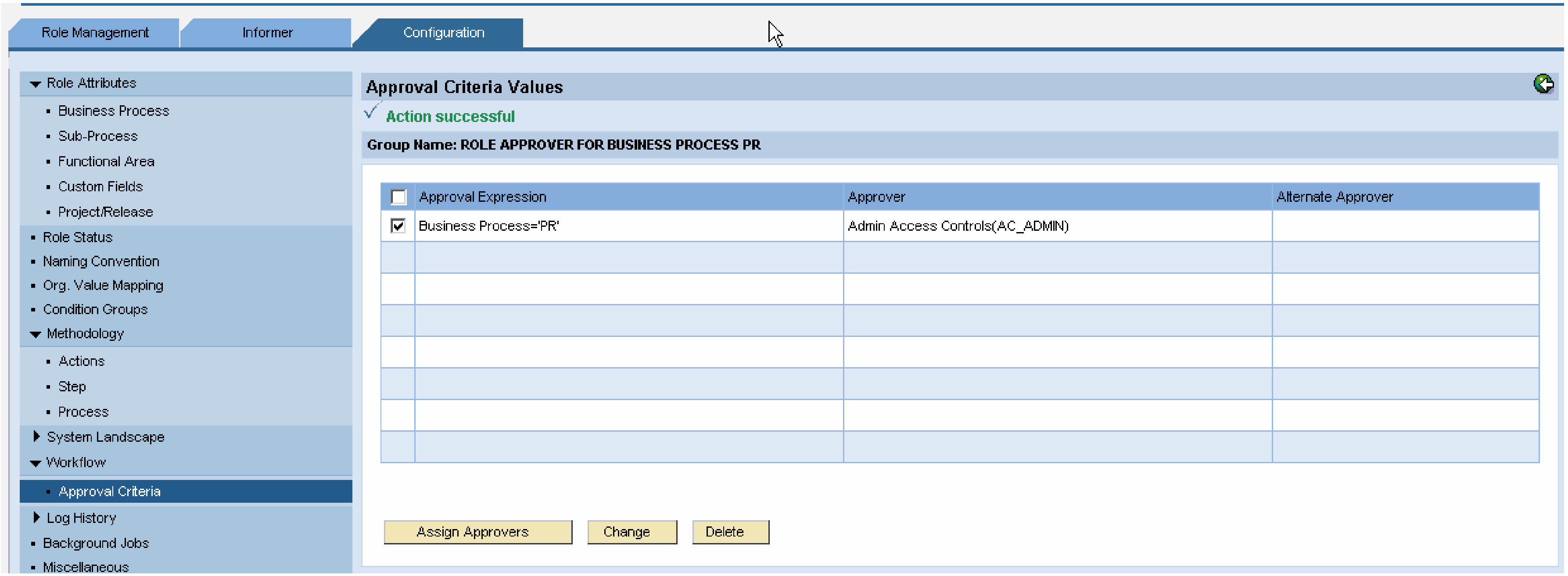
- Assign approvers to each business process



9 – Definition of Approval Criteria (3/3)

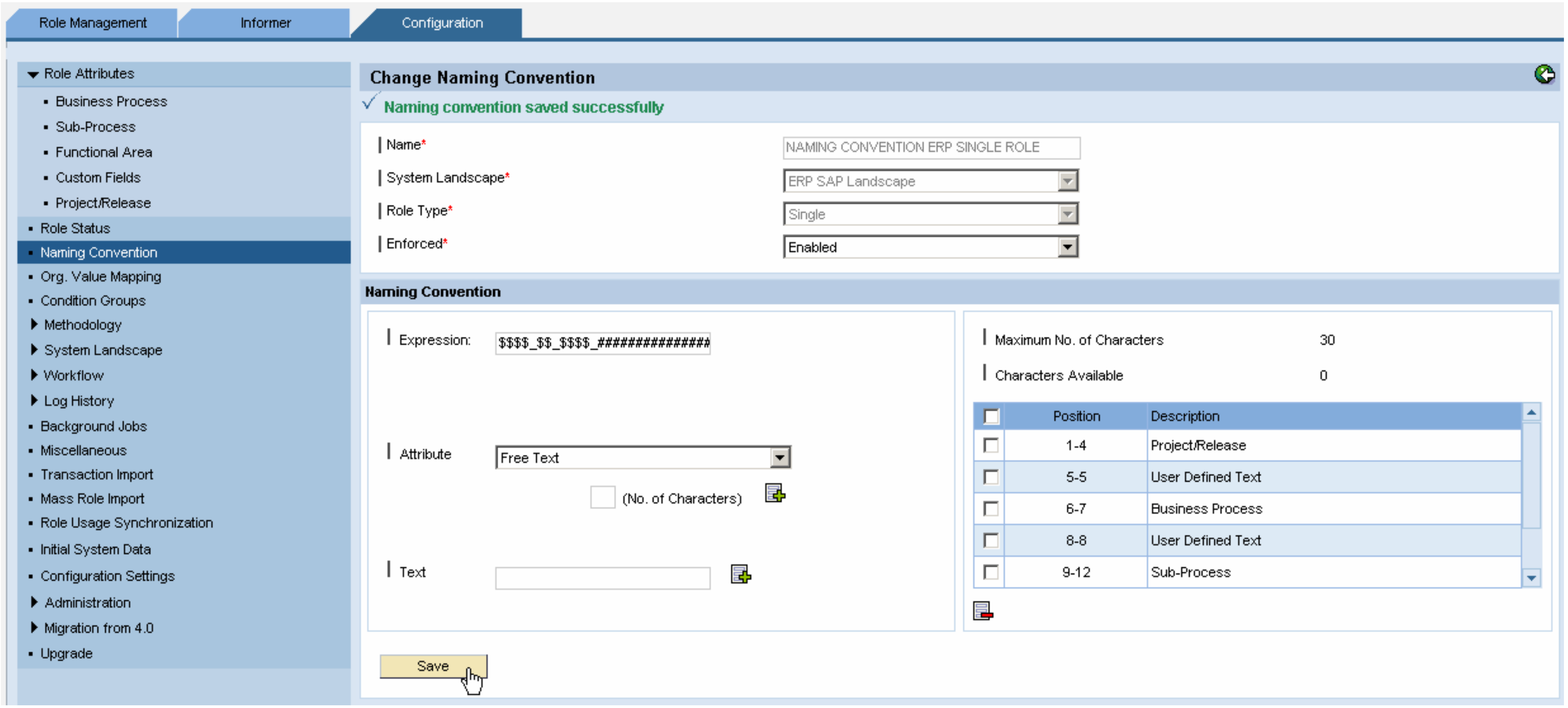
➢ The result is a list of business processes, each one assigned with a approver and optionally an alternate approver. In our example the list has only one item.

➢ To these approvers CUP will send approval requests in the role approval step of the methodology process to.



10 – Definition of Naming Conventions

➢ Create naming Conventions for single, composite & derived roles as well as for pofile in your different system landscapes and determine whether the naming convention shall be enforced (recommended).



11 – Definition of Organization Value Mapping

- 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.