

# SAP Governance, Risk & Compliance Access Control 5.3

Post-Installation Slide Deck

→ Compliant User Provisioning



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.

- 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 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

## 2 – Upload Initial 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 screenshot displays the SAP GRC Access Control Compliant User Provisioning interface. The main heading is "SAP GRC Access Control Compliant User Provisioning". The navigation bar includes "My Work", "Informers", and "Configuration". The left sidebar shows a tree view of configuration options, with "Initial System Data" selected. The main content area is titled "Initialize DB" and contains two sections: "Import Data" and "Export Data".

**Import Data**

File Name: C:\51033276\JAVA\WIRAEVAE\_init\_clean\_and\_ Browse.

Insert

Append

Clean and Insert

Import

**Export Data**

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Initial Data	Initial Data
<input type="checkbox"/>	Connector	Connector
<input type="checkbox"/>	Roles	Roles
<input type="checkbox"/>	Workflow Configuration	Workflow Configuration
<input type="checkbox"/>	User Defaults	User Defaults
<input type="checkbox"/>	Hr Triggers	Hr Triggers
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Export

## 2 – Upload Initial Data into CUP (2/2)



- 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*

The screenshot displays the SAP GRC Access Control Compliant User Provisioning interface. The main content area is titled 'Initialize DB' and is divided into two sections: 'Import Data' and 'Export Data'.

**Import Data Section:**

- File Name:** C:\51033276\JAVA\WIRAE\AE\_init\_append\_data.xml (with a 'Browse...' button)
- Options:**  Insert,  Append,  Clean and Insert
- Action:** Import

**Export Data Section:**

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Initial Data	Initial Data
<input type="checkbox"/>	Connector	Connector
<input type="checkbox"/>	Roles	Roles
<input type="checkbox"/>	Workflow Configuration	Workflow Configuration
<input type="checkbox"/>	User Defaults	User Defaults
<input type="checkbox"/>	Hr Triggers	Hr Triggers

**Action:** Export

The left sidebar shows a navigation tree with 'Initial System Data' selected. The top navigation bar includes 'My Work', 'Informers', and 'Configuration' tabs. The top right corner shows 'Welcome Admin Access Controls' and 'Help | About | Logout'.

# 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.

**SAP GRC Access Control**  
Compliant User Provisioning

Welcome Frank Rambo | Help | About | Log Off

My Work | Informer | Configuration

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  
• End User Personalization  
• Support  
• Workflow  
• Request  
• Field Mapping  
• Approvers  
• User Review  
• Change Log  
• Connectors  
• Available Connectors  
• **Create Connectors**  
• Authentication  
• User Data Source  
• HR Trigger  
• Roles  
• Background Jobs

Name\*  
Short Description\*  
Description  
Application\*  
Application Server Host\*  
System Number\*  
Client\*  
User ID\*  
Password\*  
System Language  
Message Server Name\*  
Message Server Group  
Message Server Host  
SAP Version  
HR System\*  
SLD Connector  
Connector Category  
Role  
HR Manager Path

Select  
No  
  
Production  
Back End  
Select

Create Test Connection

# 3 - Create and Test System Connectors (2/3)

## → Select JCo Destination



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

The screenshot shows the SAP GRC Access Control Compliant User Provisioning interface. The main content area displays the 'Connectors' configuration page. A table titled 'Available Connectors' is shown with the following data:

System	Client	Status
<input checked="" type="radio"/> AR1	001	
<input type="radio"/> VIRSAXSR3_01_MODEL	001	
<input type="radio"/> VIRSAXSR3_01_METADATA	001	

The 'AR1' connector is highlighted with an orange border, indicating it is the selected destination. The interface also includes a navigation pane on the left with 'Connectors' expanded, and a 'Select' button at the bottom of the table.



# 3 - Create and Test System Connectors (3/3)

## → Maintain Mandatory Fields with Dummies

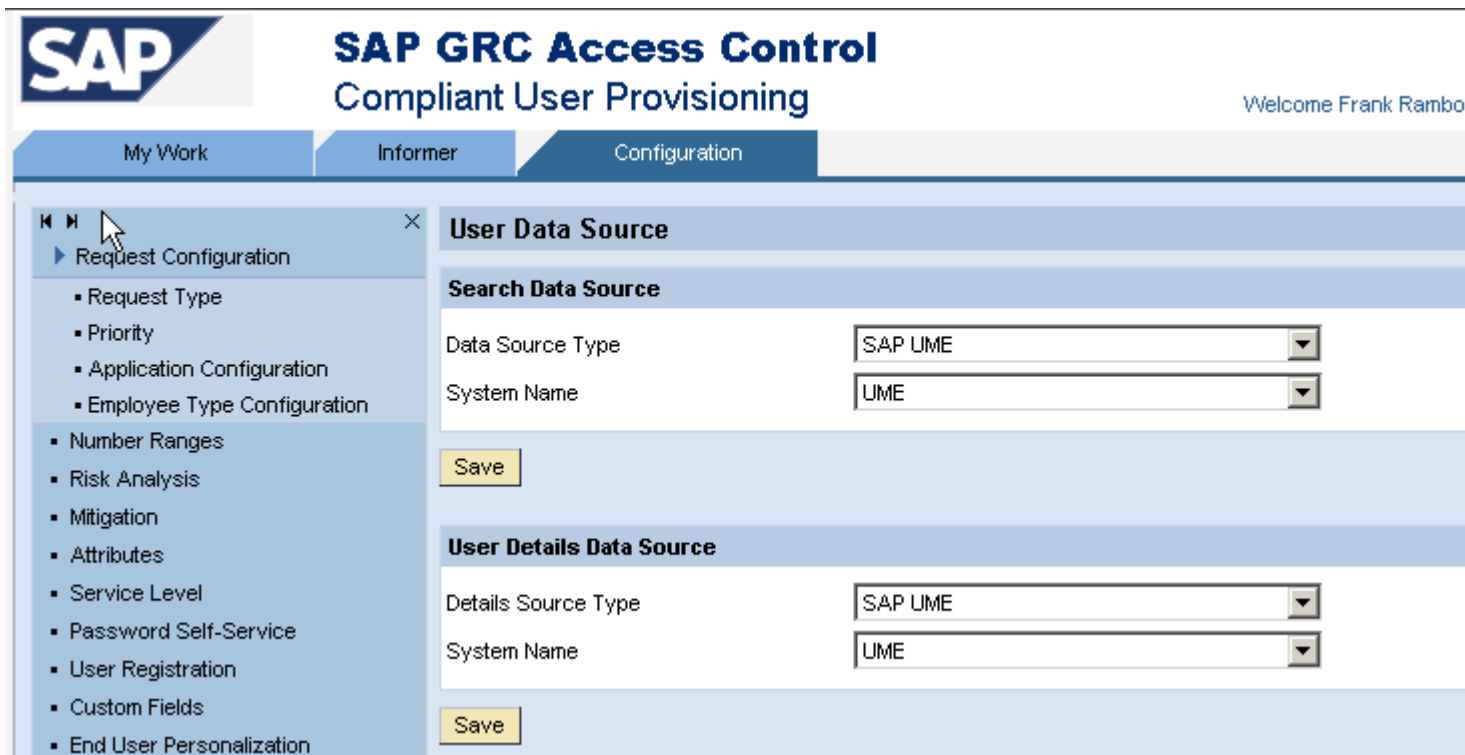


- Maintain the highlighted fields with arbitrary dummy entries and enter a *Short Description* and a *Description*. Finally click on *Test Connection* to verify.

The screenshot displays the SAP GRC Access Control interface for configuring a system connector. The left pane shows the 'Connectors' section with 'Create Connectors' selected. The right pane shows the 'Connectors' configuration form with a 'Connection Successful' message. Arrows indicate the flow of data from the left pane to the right pane.

Field	Value
Name*	AR1
Short Description*	[Highlighted]
Description	[Highlighted]
Application*	AR1
Application Server Host*	[Highlighted]
System Number*	[Highlighted]
Client*	001
User ID*	webuser
Password*	[Highlighted]
System Language	EN
Message Server Name*	[Highlighted]
Message Server Group	SPACE
Message Server Host	grc-rig-03
SAP Version	Select
HR System*	No
SLD Connector	<input checked="" type="checkbox"/>
Connector Category	Production
Role	Back End
HR Manager Path	Select

- **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.



The screenshot shows the SAP GRC Access Control Compliant User Provisioning interface. The top navigation bar includes 'My Work', 'Informer', and 'Configuration'. The main content area is titled 'User Data Source' and contains two sections: 'Search Data Source' and 'User Details Data Source'. Both sections have dropdown menus for 'Data Source Type' (set to 'SAP UME') and 'System Name' (set to 'UME'), along with a 'Save' button.

**SAP GRC Access Control**  
Compliant User Provisioning

Welcome Frank Rambo

My Work | Informer | Configuration

**User Data Source**

**Search Data Source**

Data Source Type: SAP UME  
System Name: UME

Save

**User Details Data Source**

Details Source Type: SAP UME  
System Name: UME

Save

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
- End User Personalization

# 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.

The screenshot shows the SAP GRC Access Control interface. The main title is "SAP GRC Access Control Compliant User Provisioning". The navigation bar includes "My Work", "Informer", and "Configuration". The left sidebar lists various configuration options, with "Authentication" selected. The main content area is titled "Authentication System" and displays a success message: "Requestor Authentication System successfully saved." Below this, the "Access Requestors" section is highlighted with an orange border. It contains two dropdown menus: "Authentication System" set to "SAP UME" and "System Name" set to "UME". A checkbox labeled "End User Verification Required" is checked. A "Save" button is located below the form fields.

## 6 – Configure SMTP Server for Workflow Email Notifications (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 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

Welcome Dominic Yow-Sin-Cheung

My Work

Informer

Configuration

⏪ ⏩

✕ ▲

- ▶ Request Configuration
  - Number Ranges
  - Risk Analysis
  - Mitigation
  - Attributes
  - Service Level
  - Self Service
  - User Registration
  - Custom Fields
  - End User Personalization
  - Support
- ▼ Workflow
  - Initiator
  - Custom Approver Determinators
  - Stage
  - Path
  - Detour/Fork
  - Email Reminder
  - Escape Route
  - Auto Provisioning
  - CUA System
  - SMTP Server

### SMTP Server

#### Enter Email Server Name

Email Server Name\*

#### Enter Email Notification Sender

System Email ID

#### Application URL

Application URL

Redirection URL

Save

Cancel

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

## → Risk Analysis



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

The screenshot shows the SAP GRC Access Control Configuration interface. The main header includes the SAP logo, the text "SAP GRC Access Control Compliant User Provisioning", the user name "Welcome Frank Rambo", and a "Help | About | Log Off" link. The navigation bar has tabs for "My Work", "Informer", and "Configuration". A left-hand navigation menu lists various configuration areas, with "Risk Analysis" selected. The main content area is titled "Risk Analysis" and displays a green success message: "Successfully saved Risk Analysis Configuration." Below this, there are three sections for configuration:

- Select Options:** Includes a dropdown for "Default Analysis Type" (set to "Permission Level") and a checkbox for "Consider Mitigation Controls" (unchecked). A "Save" button is present.
- Select Risk Analysis and Remediation Version:** Includes a dropdown for "Version" (set to "5.3 Web Service"), a text field for "URI" (set to "http://grc-rig-03.pal.sap.corp:50100/VirsaCCRis"), a text field for "User Name" (set to "ac\_admin"), a password field, and a checkbox for "Perform Org. Rule Analysis" (unchecked). A "Save" button is present.
- Risk Analysis On Request Submission:** Includes a dropdown for "Perform Risk Analysis on Request" (set to "No"). A "Save" button is partially visible at the bottom.

## 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>
  - 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

# 7 – Configure Risk Analysis and Mitigation (3/4)

## → Mitigation



- 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.

The screenshot shows the SAP GRC Access Control interface. The main header displays the SAP logo, the title "SAP GRC Access Control Compliant User Provisioning", and a welcome message "Welcome Admin Access Controls". The navigation bar includes "My Work", "Informer", and "Configuration". A left-hand menu lists various configuration options, with "Mitigation" selected. The main content area shows a confirmation message "Successfully saved Mitigation Configuration." followed by a "Select Options" section. This section contains several configuration fields: "Allow Approvers to Approve Access Despite any Conflicts" (checkbox), "Default Duration (Days) for the Mitigation Control" (text input with value 365), "Mitigation URI" (text input with value /CCMitigation5\_0Service/Config1?style=document), "Risk Search URI" (text input with value /irsaccRisk5\_0Service/Config1?style=document), "Org. Rule Search URI" (text input with value /CCOrgRules5\_3Service/Config1?style=document), and "Function Search URI" (text input with value /CCFunction5\_0Service/Config1?style=document). A "Save" button is located at the bottom of the configuration area.



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



### ➤ 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\*    
Log Level\*    
Cache Job Time Interval in Seconds\*  [Note: Need to Restart the Server]  
Background Job Time Interval In Minutes\*  [Note: Need to Restart the Server]

**Workflow Types**

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



## ➤ 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<sup>1</sup>
- MITIOBJ URL `http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document` , Checked<sup>1</sup>
- RE `http://<server>:<port>/AEWFExitServiceWS_5_2/Config1?wsdl&style=document` , Checked
- RISK URL `http://<server>:<port>/VirsaCCWFExitService5_2Service/Config1?wsdl&style=document` , Checked<sup>1</sup>
- 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>

---

<sup>1</sup> These workflow types appear only after import of AE\_init\_append\_data\_CC.xml (refer to post-installation slide deck RAR page 44).



# 10 – Create Role Attributes (1/3)

## → Overview



- Before importing roles we recommend creating role attributes.
- Maintain Role Attributes in Configuration → Roles → Attributes

Role Attribute	
	<b>Company</b>
	<b>Functional Area</b>
	<b>Application Area</b>
	<b>Business Process</b>
	<b>Business Sub-Process</b>
	<b>Functional Area and Company</b>

# 10 – Create Role Attributes (2/3)

→ Company, Funct. Area, Application Area



## ➤ Company

Role Attribute		
Company		
<input type="checkbox"/> Company ID*	Short Description*	Description
<input type="checkbox"/> SAP	SAP	SAP

## ➤ Functional Area

Role Attribute		
Functional Area		
<input type="checkbox"/> Name*	Short Description*	Description
<input type="checkbox"/> FI	Financial	Financial
<input type="checkbox"/> PR	Purchasing	Purchasing

## ➤ Application Area

Role Attribute			
Application Area			
<input type="checkbox"/> Name*	Short Description*	Description	System
<input type="checkbox"/> ERP	ERP ECC 6.0	ERP ECC 6.0	DCX

# 10 – Create Role Attributes (3/3)

## → Business Process, Business Sub-Process



### ➤ 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						
<input type="checkbox"/> Name*	Short Description*	Description	Owner / Approver	Alternate Approver	Application Area	
<input type="checkbox"/> PR	Procure to Pay	Procure to Pay	GRC_ADMIN	D043805	ERP	
<input type="checkbox"/> SD	Order to Cash	Order to Cash	GRC_ADMIN	D043805	ERP	

### ➤ Business Sub-Process

Role Attribute				
Business Sub-Process				
<input type="checkbox"/> Name*	Short Description*	Description	Business Process	
<input type="checkbox"/> PR01	Vendor Master Maintenance	Vendor Master Maintenance	Procure to Pay	
<input type="checkbox"/> PR02	Production Order Processing	Production Order Processing	Procure to Pay	
<input type="checkbox"/> PR03	Service Master Maintenance	Service Master Maintenance	Procure to Pay	
<input type="checkbox"/> PR04	PO Approval	PO Approval	Procure to Pay	
<input type="checkbox"/> SD01	Customer Master Data	Customer Master Data	Order to Cash	
<input type="checkbox"/> SD02	Delivery Processing	Delivery Processing	Order to Cash	
<input type="checkbox"/> SD03	Sales Rabates	Sales Rabates	Order to Cash	
<input type="checkbox"/> 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



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



➤ Upload roles in Configuration → Roles → Import

The screenshot displays the SAP GRC Access Control Compliant User Provisioning interface. The top navigation bar includes the SAP logo, the product name "SAP GRC Access Control Compliant User Provisioning", a welcome message "Welcome Admin Access Controls", and a "Help | About | Logoff" link. Below the navigation bar, there are three tabs: "My Work", "Informer", and "Configuration". The left sidebar contains a tree view of configuration options, with "Roles" expanded to show "Import Roles". The main content area is titled "Import Roles" and contains the following fields and options:

- System:** ERP-DCX (dropdown menu)
- Role Source:** Back End (dropdown menu)
- Last Synch Date:** 05/02/2008 (text input with calendar icon)
- Radio buttons:**
  - All Roles
  - All Roles Except SAP Predefined Roles
  - Selected Roles
- Role Name:** (text input field)
- From File:** em Landscape\RIG53\_DCX\_selected\_roles.xls (text input with "Browse..." button)
- Buttons:** "Download Template" (yellow button)
- Overwrite Existing Roles
- Import:** (yellow button)

- 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!



- > 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 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.