UAR Reference Guide

SAP® BusinessObjects™ Access Control 10.0

Target Audience

- Technology Consultants
- System Administrators
- Solution Consultants
- Business Process Owner
- Support Specialist

Document version: 1.0 – August 2011

THE BEST-RUN BUSINESSES RUN SAP

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

These materials are subject to change without notice. SAP AG and its affiliated companies ("SAP Group") provide these materials for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following address:
http://service.sap.com/instguides

THE BEST-RUN BUSINESSES RUN SAP SAP®

Typographic Conventions

Type Style	Represents
Example Text	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, titles of graphics and tables
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, names of variables and parameters, source code as well as names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.
EXAMPLE TEXT	Keys on the keyboard, for example, function keys (such as **F2**) or the **ENTER** key.

Icons

Icon	Meaning
⚠	Caution
💬	Example
💡	Note
🧭	Recommendation
SYN	Syntax

Contents

1. Getting Started

GRC 10.0 Access Control (AC) identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. The User Access Review (UAR) feature of Access Control automates and documents the periodic decentralized user access review by business managers or role owners.

User access review provides a workflow-based review and approval process. Business managers and role owners perform periodic reviews of user access, using requests automatically generated by the system based on the organization's internal control policy.

This guide is intended for users who need to perform user access reviews within a GRC Access Control 10.0 environment, and describes details of the system including process options, configuration, and use.

1.1 Document History

Version	Date	Description
1.0	August 2011	Initial release

1.2 About this Guide

This guide describes how to perform user access reviews. This guide is a stand-alone document.

Note the following:

- This guide provides business use cases as examples on how you can use SAP software for your company. These examples are intended to serve only as models and might not necessarily run the way they are described here in your customer-specific landscape.
- This guide discusses UAR for GRC AC 10.0. Any attempt to use this guide for other product versions is not supported.

For an overview of the Access Control 10.0 documentation, refer to the *SAP BusinessObjects Access Control 10.0 Master Guide* on the *SAP Service Marketplace* at service.sap.com/instguides.

1.3 Audience for this Guide

This guide is intended for the following people involved in performing user access reviews:

- Administrators
- User Managers
- Reviewers
- Coordinators

2. Introducing User Access Review

User access review in AC 10.0 offers the following features:

- An automated process for periodic access review
- Decentralized review of user access
- Review and approval workflow for requests
- Automatic role removal, if needed
- Status and history reports to assist in monitoring the review process
- Audit trail and reports for supporting internal and external audits
- Support for back-end systems integrated with Access Control as well as legacy systems

The key benefits of user access review are:

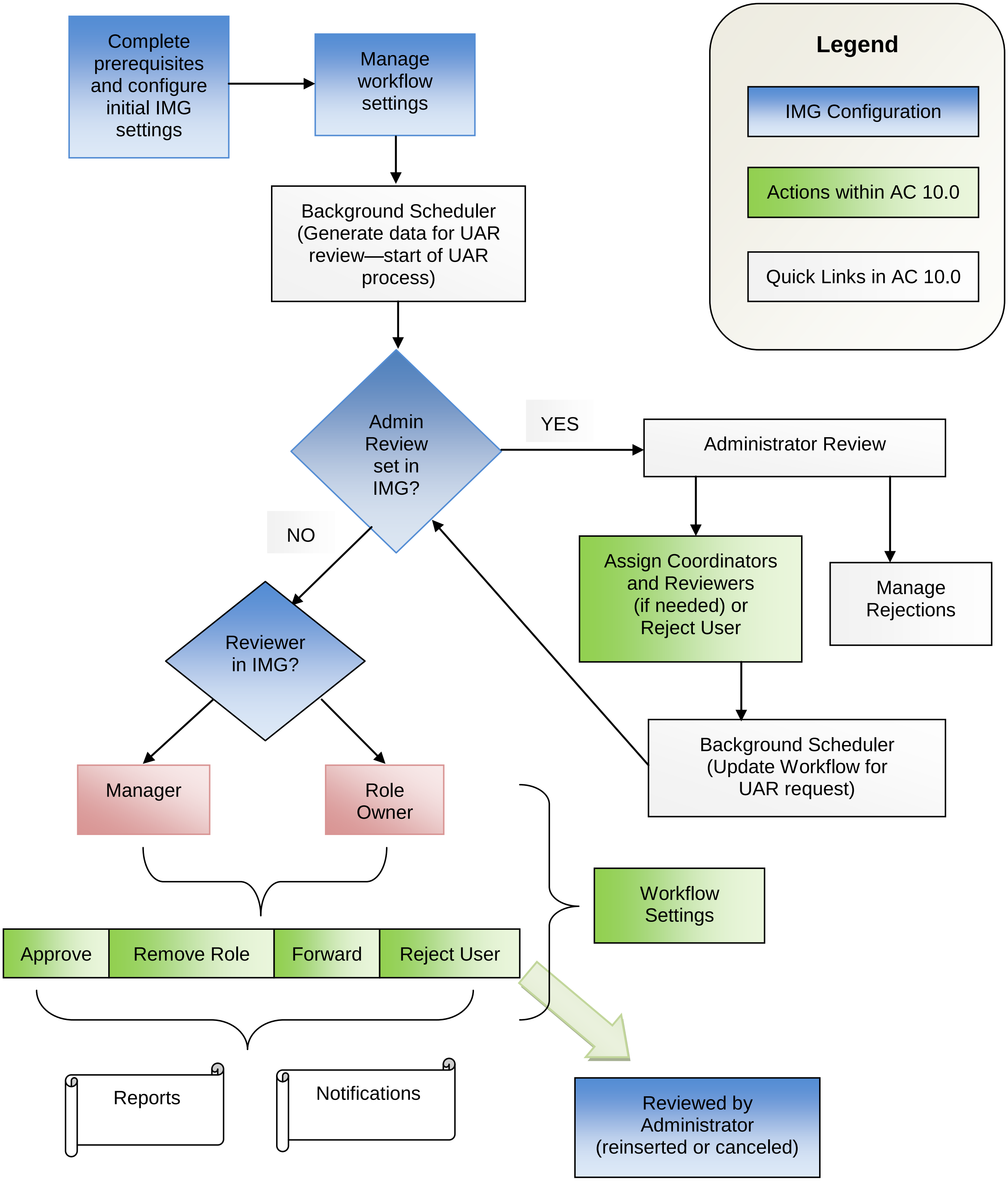
- A streamlined internal control process with collaboration among business managers, internal control, and information technology teams
- Improved efficiency and visibility of the internal control process

2.1 Exploring Roles in the UAR Process

SAP GRC 10.0 includes the following roles that can appear in UAR requests:

- Administrators — Administrators are users with the Admin role assigned for Access Control. Administrators can perform UAR-specific administration tasks, such as cancelling UAR requests and regenerating requests for rejected users. Administrators can also perform admin reviews before generating a workflow for the request.
- User managers — User managers are the direct manager of a user, as defined in the User Details Data Source.
- Reviewers — Reviewers are approvers at the Reviewer stage. A reviewer can be a user’s manager or the role owner.
- Role owners — Role owners are users specified in the business role management master data.
- Coordinators — Coordinators are users assigned to reviewers. Coordinators monitor the UAR process and coordinate activities to ensure that the process is completed in a timely manner.

2.2 Exploring the UAR Process


Complete prerequisites and configure initial IMG settings
Manage workflow settings
Background Scheduler (Generate data for UAR review—start of UAR process)
Legend
IMG Configuration
Actions within AC 10.0
Quick Links in AC 10.0
Admin Review set in IMG?
YES
Administrator Review
NO
Assign Coordinators and Reviewers (if needed) or Reject User
Manage Rejections
Reviewer in IMG?
Background Scheduler (Update Workflow for UAR request)
Manager
Role Owner
Workflow Settings
Approve
Remove Role
Forward
Reject User
Reports
Notifications
Reviewed by Administrator (reinserted or canceled)

2.3 Exploring Process Options

AC 10.0 offers multiple process options that determine the approvers of UAR requests. This section describes the available process options.

2.3.1 Admin Review

You have the option to enable an admin review, which provides administrators an opportunity to validate request data after requests are generated (by the UAR Load Data job) but prior to generating workflow tasks (by the UAR Update Workflow job).

If the reviewer information is incorrect or missing, administrators can modify the data prior to generating workflow tasks and notifications. The administrator can also delete requests, as required.

2.3.2 Reviewer Stage

You can specify whether the reviewer stage is addressed by a user’s manager or by the role owner, as appropriate.

2.3.3 Security Stage

You can choose to include a security stage, if required. Note that a security stage is mandatory if you do not have automatic provisioning enabled, though you might want to include the stage even when automatic provisioning is enabled so that security personnel can ensure accurate data prior to provisioning.

If a security stage is included in the approval workflow, you must decide whether security personnel are able to modify the direction previously noted by an approver. For example, a security team member might decide to retain basic roles that have been inappropriately marked for removal by an approver.

2.4 Understanding Workflow Stage Configuration

After deciding on the stages to include in the UAR workflow, you need to determine the specific behavior for each stage to reflect your review process. These behaviors include the following:

- Email notification
- Reminders
- Escalation

2.4.1 Configuring Email Notification

You need to determine the content of email notifications to be sent to approvers at each stage. You also need to determine the recipients, as well as the content of the notification header and the email body.

2.4.2 Setting Reminders

You need to decide whether to send reminders to reviewers who have not completed their portion of the request by the date specified in configuration. You can specify the interval of reminder notifications (in days), the reminder notification header, and body content.

2.4.3 Specifying Escalation

You need to specify whether to escalate UAR requests in the details associated with each stage. Escalation is based on the time spent in a particular stage. If a reviewer does not complete a review of a request according to the date parameter defined in the configuration, the request is escalated. Escalation of a request appears in the audit trail of the request.

You also need to specify whether escalation automatically removes access that is not approved by a certain date.

2.5 Performing Automatic Provisioning

You need to decide whether to automatically provision requests at the end of the request’s workflow. If so, roles that are marked for removal in the user access review are automatically de-provisioned in the target system.

If you choose not to automatically provision, you need to include a security stage in the workflow to allow the security team to modify access according to the review.

3. Prerequisites

You need to run the following synchronization jobs (in the order listed) to generate UAR requests:

Job	Description
GRAC_ROLEREP_ROLE_SYNC	Synchronizes all roles in the repository.
GRAC_ROLEREP_USER_SYNC	Synchronizes all users, and roles used by these users.
GRAC_ACTION_USAGE_SYNC	Retrieves the action usage for users.
GRAC_ROLE_USAGE_SYNC	Retrieves the role usage.

3.1 Importing Roles

You can import multiple roles from systems that support plug-ins.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Role Mass Maintenance* > *Role Import*. The *Role Import* screen appears.
3. In *Step 1: Define Criteria*, specify the role type, import source, and other parameters for importing multiple roles, and choose the *Next* pushbutton.
4. In *Step 2: Select Role Data*, specify information for the role attribute source and the role authorization source (such as the location of the attribute and authorization files), and choose the Next pushbutton.
5. In *Step 3: Review*, choose a preview option, review the information displayed, and choose the Next pushbutton.
6. In *Step 4: Schedule*, schedule the job to run in the background at a specified time or choose to run the job in the foreground, and choose the *Submit* pushbutton.

4. Managing IMG Configurations for UAR

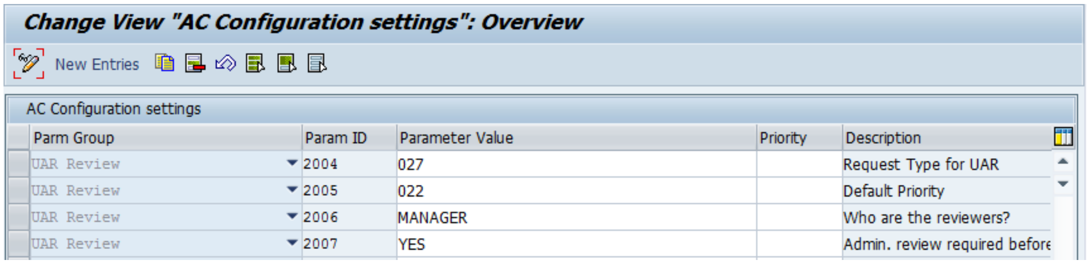
This section describes how to maintain the configuration settings related to UAR, define email reminders, and set service level agreements.

4.1 Maintaining Configuration Settings

This section describes how to maintain the configuration settings related to UAR.

Procedure

1. Log on to the backend GRC Access Control 10.0 system.
2. Enter transaction SPRO.
3. Choose the *SAP Reference IMG* button.
4. Navigate to *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings*. The *AC Configuration Settings Overview* screen appears.



Change View "AC Configuration settings": Overview

AC Configuration settings

Parm Group	Param ID	Parameter Value	Priority	Description
UAR Review	2004	027		Request Type for UAR
UAR Review	2005	022		Default Priority
UAR Review	2006	MANAGER		Who are the reviewers?
UAR Review	2007	YES		Admin. review required before

You can specify the following fields:

Column	Description
Param Group	The parameter group, in this case, UAR Review.
Param ID	The specific parameter identifier.
Parameter Value	The value of the parameter.
Priority	The parameter priority.
Description	A description of the parameter.

The manager of a user or the role owner for a role can review corresponding UAR requests. In addition, the *Admin review required before sending tasks to reviewers* setting can be one of the following:

- YES — The request is sent to the administrator before it is generated for the manager or role owner to review.
- NO — The request bypasses administrator review and is directly generated and sent to the reviewer.

⚠

If the user does not have a manager, or the role owner does not have an owner, selecting *NO* for the *Admin review required* setting results in no workflow being generated for the request.

Additionally, the role owner or manager must have an assigned coordinator, otherwise the request is not sent to a reviewer. You can configure this mapping using *Access Management > Manage Coordinators* in the SAP NetWeaver Business Client.

Note the following:

- You can maintain the request type using the *Governance, Risk and Compliance > Access Control > User Provisioning > Define Request Type* Customizing activity.
- You can maintain the priority using the *Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Priority Configuration* Customizing activity.
- You can maintain the number ranges for provisioning requests using the *Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Number Range Intervals for Provisioning Requests* Customizing activity.
- You can maintain the rejection reasons using the *Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Review Rejection Reasons for Provisioning Requests* Customizing activity.

4.2 Defining an Email Reminder

You can optionally define whether notifications are sent for UAR requests.

Procedure

1. Log on to the backend GRC Access Control 10.0 system.
2. Enter transaction SPRO.
3. Choose the *SAP Reference IMG* button.

4. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Text for Custom Notification Messages*. The *Documentation Maintenance* screen appears.

   Define the body of the notification message using *General text* as the *Document Class*.

5. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Custom Notification Messages*. The *Notification Messages (Customer) Overview* screen appears.

   Specify the sender, subject, and attachment of the notification message.

6. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain MSMP Workflows*. The *MSMP Workflow Configuration* screen appears.

   Select the appropriate *Process ID*, and choose *Step 4: Variables & Templates*. Create a *Notification Template* and map the template to the *Message Class*. Choose *Step 7: Generate Versions* and save and activate the configuration.

7. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Background for E-mail Reminders*. The *Define Background Job* screen appears.

   Specify the background job information for the notification message.

4.3 Specifying the Service Level Agreement

You can define the service level agreement for UAR requests.

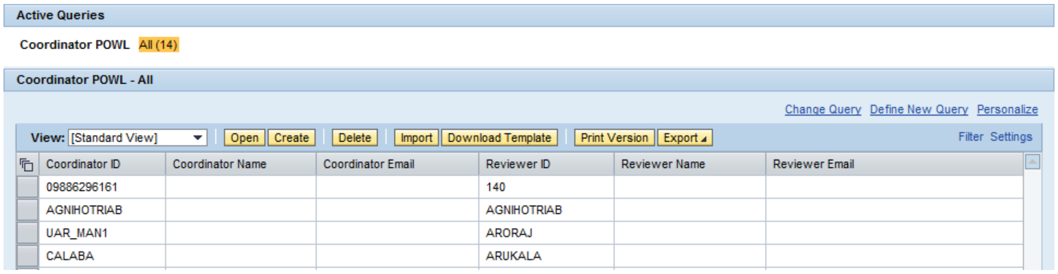
1. Log on to the backend GRC Access Control 10.0 system.
2. Enter transaction SPRO.
3. Choose the *SAP Reference IMG* button.
4. Navigate to *Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Service Level Agreements*. The *Service Line Agreement Overview* screen appears.
5. Create a new Service Level Agreement using *SAP_GRAC_USER_ACCESS_REVIEW* as the *Process ID*.

5. Managing Coordinators

This section describes how to manage coordinators for requests.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Compliance Certification Reviews* > *Manage Coordinators*. The *Manage Coordinators* screen appears.



Active Queries

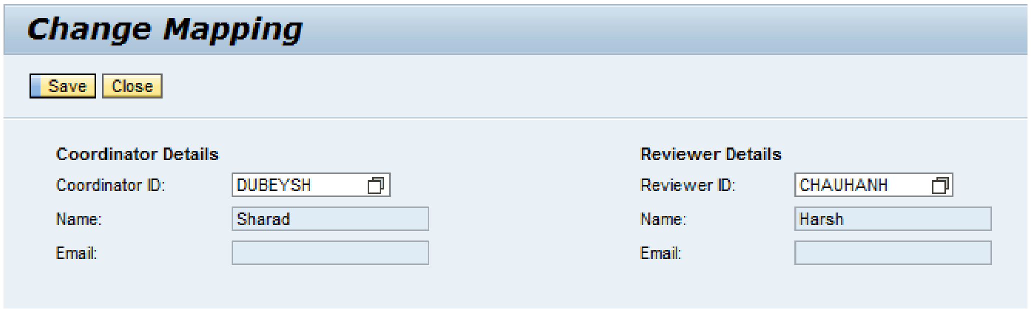
Coordinator POWL All (14)

Coordinator POWL - All

Coordinator ID	Coordinator Name	Coordinator Email	Reviewer ID	Reviewer Name	Reviewer Email
09886296161			140		
AGNIHOTRIAB			AGNIHOTRIAB		
UAR_MAN1			ARORAJ		
CALABA			ARUKALA		

3. To change a coordinator-to-reviewer mapping, choose the *Open* pushbutton. The *Change Mapping* screen appears.

   Modifying the settings, as required, and choose the *Save* pushbutton.



Change Mapping

Coordinator Details

Coordinator ID: DUBEYSH

Name: Sharad

Email:

Reviewer Details

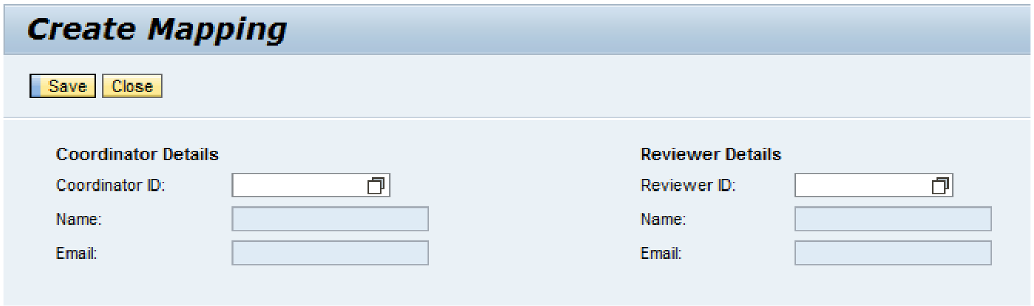
Reviewer ID: CHAUHANH

Name: Harsh

Email:

4. To delete a coordinator-to-reviewer mapping, select the mapping you want to delete, and choose the *Delete* pushbutton. A confirmation dialog box appears. Choose *Yes*.

5. To create a new coordinator-to-reviewer mapping, choose the *Create* pushbutton. The *Create Mapping* screen appears



.

6. In the *Coordinator ID* field, type or select the appropriate value.
7. In the *Reviewer ID* field, type or select the appropriate value.
8. Choose the *Save* pushbutton.
9. Choose the *Close* pushbutton. The mapping appears in the table on the *Manage Coordinators* screen.
10. Run the *Update UAR workflow* job to generate the UAR requests. This step is mandatory only if you are generating requests after an admin review.

6. Managing the UAR Workflow

This section describes how to manage workflow settings for UAR and how to update the workflow for UAR requests.

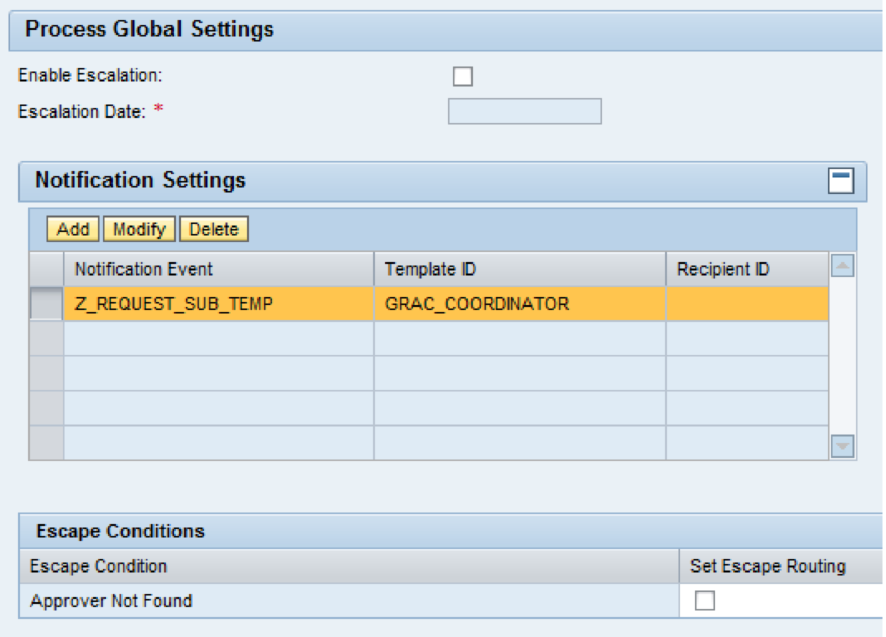
6.1 Managing Workflow Settings for UAR

This section describes how to manage workflow settings for UAR.

Procedure

1. Log on to the backend GRC Access Control 10.0 system.
2. Enter transaction SPRO.
3. Choose the *SAP Reference IMG* pushbutton.
4. Navigate to *Governance, Risk and Compliance* > *Access Control* > *Workflow for Access Control* > *Maintain MSMP Workflows*.
5. To configure the global escalation settings and escape conditions, select the SAP_GRAC_USER_ACCESS_REVIEW process ID, and choose the *Display/Change* pushbutton to toggle to change mode.

   Configure the settings, as required.



Process Global Settings

Enable Escalation: □

Escalation Date: *

Notification Settings

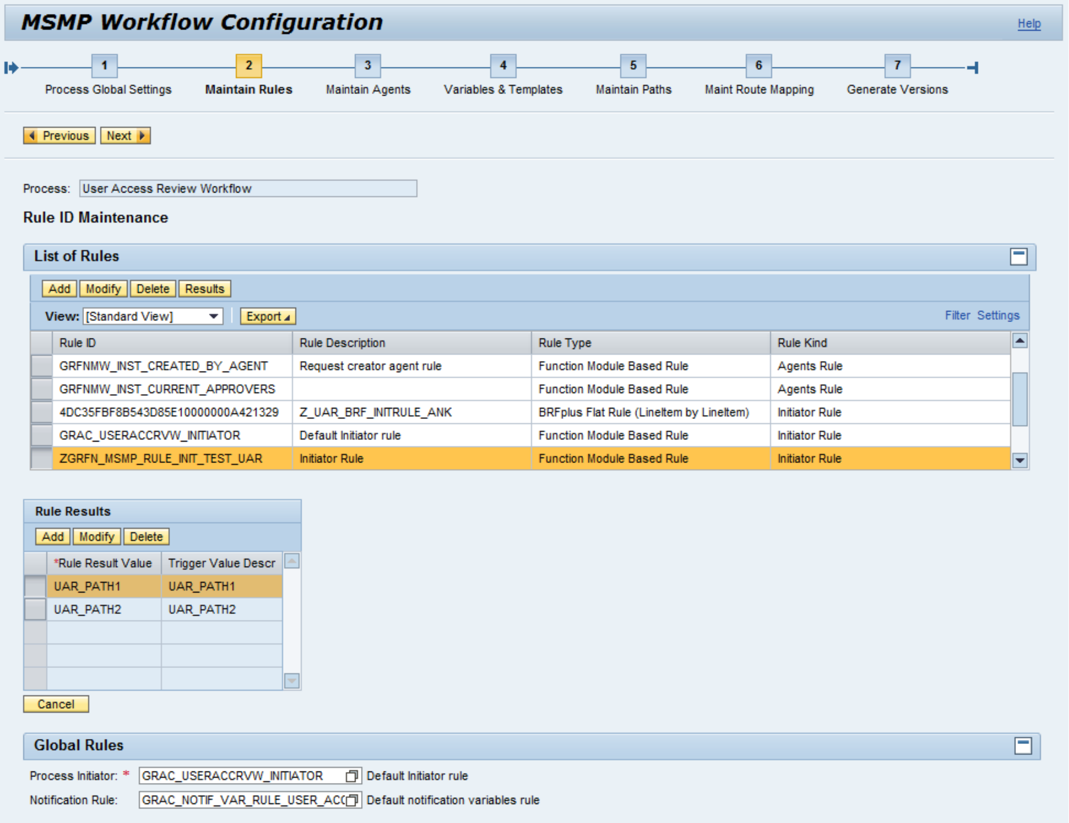
Notification Event	Template ID	Recipient ID
Z_REQUEST_SUB_TEMP	GRAC_COORDINATOR	

Escape Conditions

Escape Condition	Set Escape Routing
Approver Not Found	□

6. Choose the *Next* pushbutton. The *Maintain Rules* step appears.
7. Configure and maintain the rules, as required.

   You can configure the Function Module, BRF plus, ABAP Class, and BRF plusFlat rules to utilize in the Process ID. The rules can be for an initiator, routing, agent, or notification variables.



MSMP Workflow Configuration

Process: User Access Review Workflow

Rule ID Maintenance

List of Rules

View: [Standard View]

Rule ID	Rule Description	Rule Type	Rule Kind
GRFNMW_INST_CREATED_BY_AGENT	Request creator agent rule	Function Module Based Rule	Agents Rule
GRFNMW_INST_CURRENT_APPROVERS		Function Module Based Rule	Agents Rule
4DC35FBF8B543D85E10000000A421329	Z_UAR_BRF_INITRULE_ANK	BRFplus Flat Rule (LineItem by LineItem)	Initiator Rule
GRAC_USERACCRVW_INITIATOR	Default Initiator rule	Function Module Based Rule	Initiator Rule
ZGRFN_MSMP_RULE_INIT_TEST_UAR	Initiator Rule	Function Module Based Rule	Initiator Rule

Rule Results

*Rule Result Value	Trigger Value Descr
UAR_PATH1	UAR_PATH1
UAR_PATH2	UAR_PATH2

Global Rules

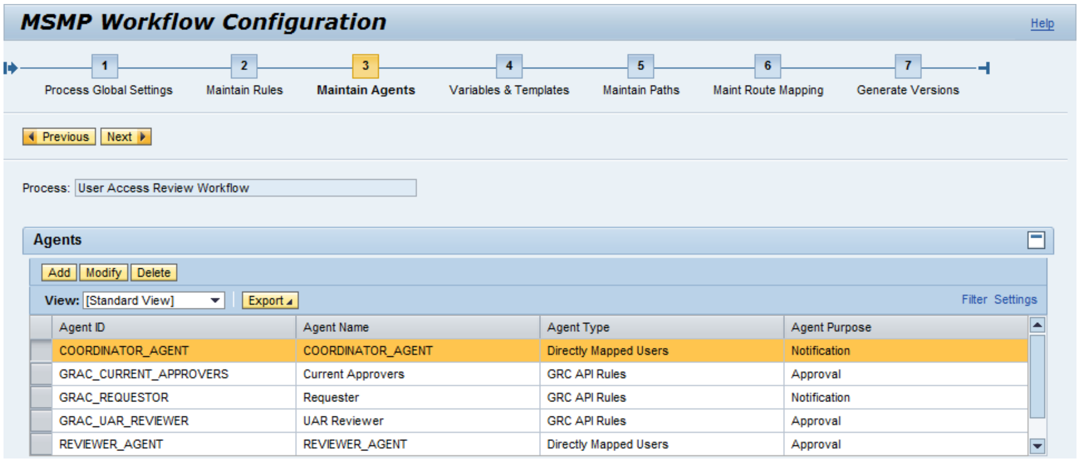
Process Initiator: * GRAC_USERACCRVW_INITIATOR Default Initiator rule

Notification Rule: GRAC_NOTIF_VAR_RULE_USER_ACC Default notification variables rule

Select a rule, and configure the *Rule Results*, as appropriate. You can also configure the *Global Rules* by specifying the *Process Initiator* and the *Notification Rule* for the process.

8. Choose the *Next* pushbutton. The *Maintain Agents* step appears.

   You can define agents for workflow stages, either for notification or approval.



Process: User Access Review Workflow

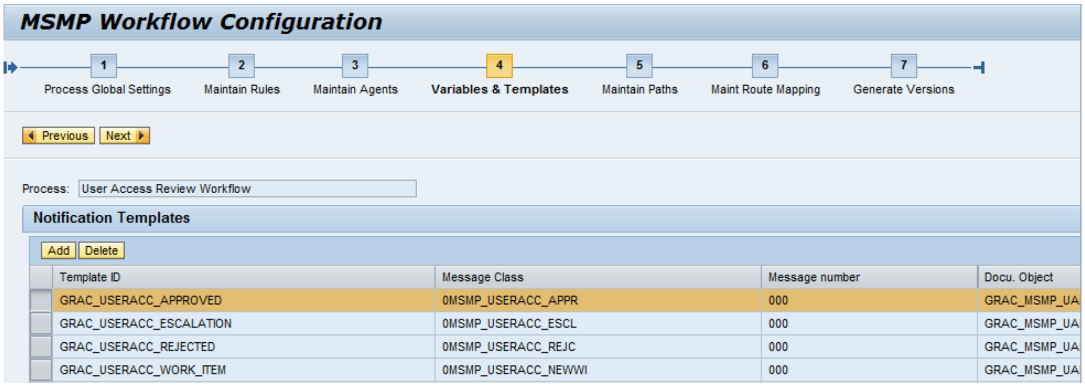
View: [Standard View]

Agent ID	Agent Name	Agent Type	Agent Purpose
COORDINATOR_AGENT	COORDINATOR_AGENT	Directly Mapped Users	Notification
GRAC_CURRENT_APPROVERS	Current Approvers	GRC API Rules	Approval
GRAC_REQUESTOR	Requester	GRC API Rules	Notification
GRAC_UAR_REVIEWER	UAR Reviewer	GRC API Rules	Approval
REVIEWER_AGENT	REVIEWER_AGENT	Directly Mapped Users	Approval

The following table lists the agent types:

Agent Type	Description
Directly Mapped Users	Approvers are selected from the Approver definition.
PFCG Roles	Users with a specific role are selected.
PFCG User Groups	Approvers are selected from PFCG User Groups assigned to users (SU01 Groups tab).
GRC API Rules	Approvers are selected from the associated function module (FM) or BRF+ rules.

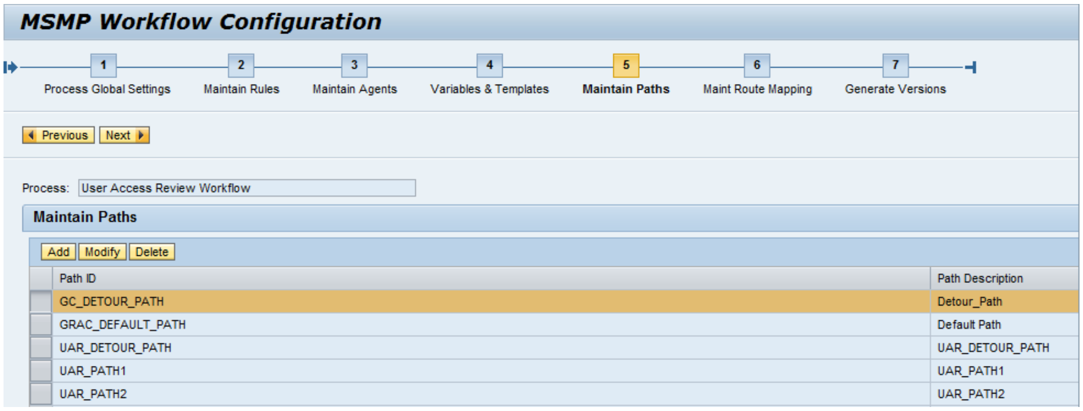
9. Choose the *Next* pushbutton. The *Variables & Templates* step appears.
10. Maintain the notification templates and variables, as required.



Process: User Access Review Workflow

Template ID	Message Class	Message number	Docu. Object
GRAC_USERACC_APPROVED	0MSMP_USERACC_APPR	000	GRAC_MSMP_UA
GRAC_USERACC_ESCALATION	0MSMP_USERACC_ESCL	000	GRAC_MSMP_UA
GRAC_USERACC_REJECTED	0MSMP_USERACC_REJC	000	GRAC_MSMP_UA
GRAC_USERACC_WORK_ITEM	0MSMP_USERACC_NEWWI	000	GRAC_MSMP_UA

11. Choose the *Next* pushbutton. The *Maintain Paths* step appears.
12. Choose the *Add* or *Modify* pushbutton, and enter values in the *Path ID* and *Path Description* fields.

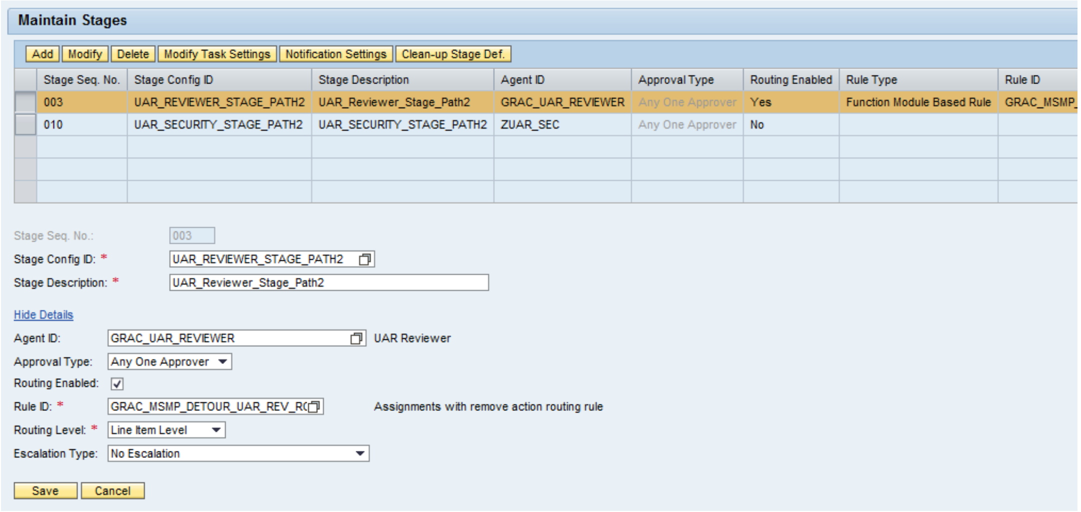


Process: User Access Review Workflow

Maintain Paths

Path ID	Path Description
GC_DETOUR_PATH	Detour_Path
GRAC_DEFAULT_PATH	Default Path
UAR_DETOUR_PATH	UAR_DETOUR_PATH
UAR_PATH1	UAR_PATH1
UAR_PATH2	UAR_PATH2

Select a path, and choose either the *Add* or *Modify* pushbuttons in the *Maintain Stages* section to define the path stages.



Maintain Stages

Stage Seq. No.	Stage Config ID	Stage Description	Agent ID	Approval Type	Routing Enabled	Rule Type	Rule ID
003	UAR_REVIEWER_STAGE_PATH2	UAR_Reviewer_Stage_Path2	GRAC_UAR_REVIEWER	Any One Approver	Yes	Function Module Based Rule	GRAC_MSMP_
010	UAR_SECURITY_STAGE_PATH2	UAR_SECURITY_STAGE_PATH2	ZUAR_SEC	Any One Approver	No		

Stage Seq. No.: 003

Stage Config ID: * UAR_REVIEWER_STAGE_PATH2

Stage Description: * UAR_Reviewer_Stage_Path2

Agent ID: GRAC_UAR_REVIEWER UAR Reviewer

Approval Type: Any One Approver

Routing Enabled: ☑

Rule ID: * GRAC_MSMP_DETOUR_UAR_REV_R(Assignments with remove action routing rule

Routing Level: * Line Item Level

Escalation Type: No Escalation

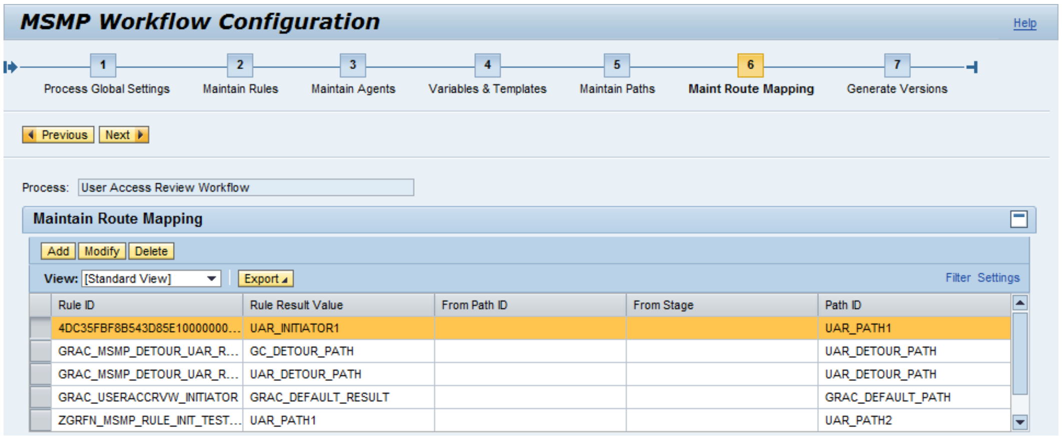
You can specify the following fields when configuring the stages:

Column	Description
Stage Seq. No.	A three-digit character sequence number.
Stage Config ID	The name of the configuration.
Stage Description	A description of the stage purpose.
Agent ID	The logical approver ID.
Approval Type	Either *Any One Approver* or *All Approvers*.
Routing Enabled	(Optional) Determines an optional detour route. If enabled, you need to specify the following fields: Rule Type, Rule ID, and Routing Level.
Rule ID	The ID of the selected detour routing.
Routing Level	The routing level, from among the following: • Stage Level (routing applies to the entire stage) • Line Item Level (routing applies to the failed line items)
Escalation Type Different from global escalation, as defined above	(Optional) Determines how the escalation should be handled for this stage, from among the following: • Escalate to Specified Agent — Requires you to maintain the *Escalation Time Mins* and *Escalation Agent* fields. • Use Defaults — Uses the default escalation setting. • Skip to Next Stage — Escalates the request to the next stage, after the specified time. Requires an entry for the Escalation Time Mins field. • No Escalation — The request will not escalate. • Deactivate, lock and move to next stage • Deactivate and move to next stage • Lock and move to next stage
Escalation Time Mins	Determines how long a request should be idle before the escalation process begins.
Escalation Agent	The agent ID that determines the approvers for escalation.

13. Select a path in the *Maintain Paths* table, select a stage in the *Maintain Stages* table, and choose the *Modify Task Settings* pushbutton. The *Stage Definition* dialog appears.

    You can use this dialog to specify the actions that an approver can perform at the selected stage.

14. Choose the *Next* pushbutton. The *Maint Route Mapping* step appears.



Process: User Access Review Workflow

Maintain Route Mapping

View: [Standard View]

Rule ID	Rule Result Value	From Path ID	From Stage	Path ID
4DC35FBF8B543D85E10000000...	UAR_INITIATOR1			UAR_PATH1
GRAC_MSMP_DETOUR_UAR_R...	GC_DETOUR_PATH			UAR_DETOUR_PATH
GRAC_MSMP_DETOUR_UAR_R...	UAR_DETOUR_PATH			UAR_DETOUR_PATH
GRAC_USERACCRVW_INITIATOR	GRAC_DEFAULT_RESULT			GRAC_DEFAULT_PATH
ZGRFN_MSMP_RULE_INIT_TEST...	UAR_PATH1			UAR_PATH2

Map the logical path (initiator) to an actual path, using the following columns:

Column	Description
Rule ID	The ID of the router.
Rule Result Value	The result value returned by the rule.
Path ID	The path to be started.

15. Choose the *Next* pushbutton. The *Generate Versions* step appears.
16. Choose the *Save* pushbutton.

    The application saves your changes.

    Choose the *Save/Simulate* pushbutton to save your changes and run a simulation to check for errors. Alternatively, choose the *Activate* pushbutton to activate the workflow.

⚠

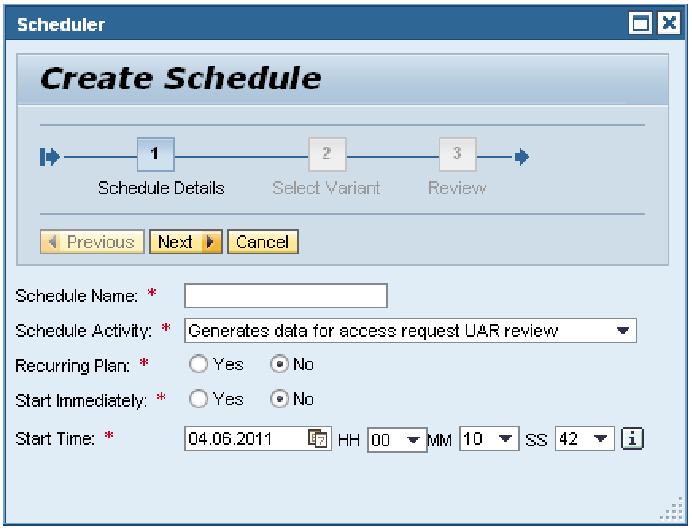
Changes in the workflow are not reflected in requests generated prior to the change. Only requests generated after the change reflect your changes.

7. Generating Data for UAR

You need to execute a job to retrieve the user-to-role relationship and role usage data from BRM, as well as create user access review requests. This section describes how to generate data for UAR by creating a schedule using the *Background Scheduler*.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Scheduling* > *Background Scheduler*.
3. Choose the *Create* pushbutton. The *Schedule Details* step appears.



Schedule Name: *

Schedule Activity: * Generates data for access request UAR review

Recurring Plan: * ○ Yes ● No

Start Immediately: * ○ Yes ● No

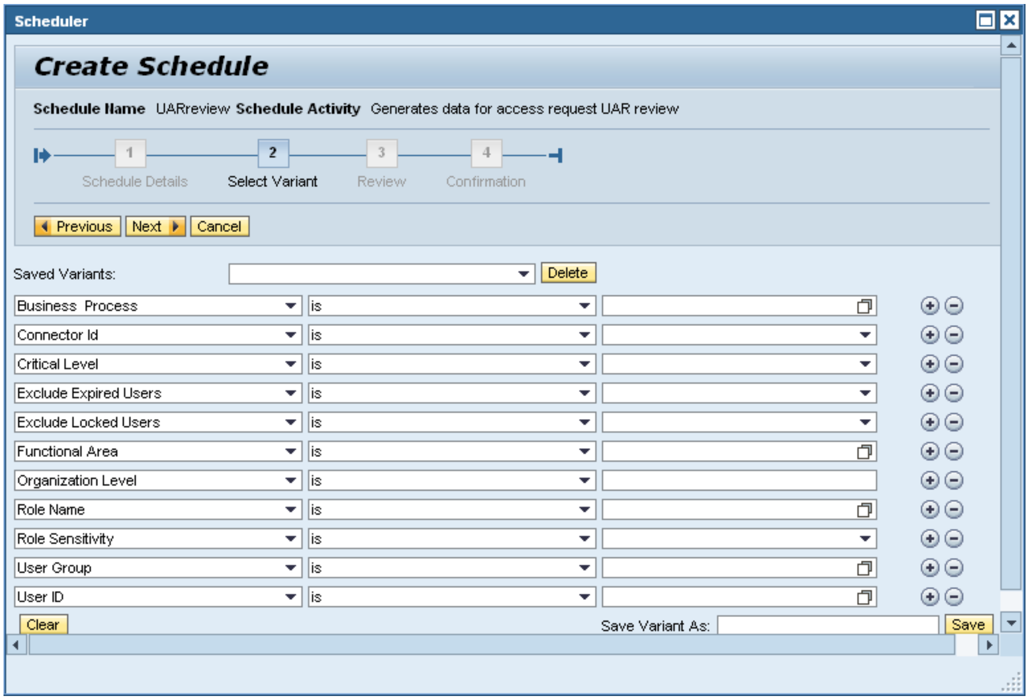
Start Time: * 04.06.2011 HH 00 MM 10 SS 42

4. In the *Schedule Name* field, type the name of the UAR job.
5. In the Schedule Activity field, select *Generates data for access request UAR review* using the drop-down list.
6. In the *Recurring Plan* field, choose whether to schedule the job to recur.

   If you choose *Yes*, you need to specify the recurring date and time range, along with the frequency and recurrence interval.

7. In the *Start Immediately* field, choose whether to start the job immediately.
8. In the *Start Time* field, specify the date and time for the job to start.

9. Choose the *Next* pushbutton. The *Select Variant* step appears.



Create Schedule

Schedule Name UARreview **Schedule Activity** Generates data for access request UAR review

Saved Variants:

Save Variant As:

Business Process	is	
Connector Id	is	
Critical Level	is	
Exclude Expired Users	is	
Exclude Locked Users	is	
Functional Area	is	
Organization Level	is	
Role Name	is	
Role Sensitivity	is	
User Group	is	
User ID	is	

10. Specify the selection criteria or choose a saved variant, as appropriate.

    You can save the selection criteria as a new variant, if required.

11. Choose the *Next* pushbutton.

    The *Review* step appears displaying a summary of the scheduled job.

12. Review the summary, and choose the *Finish* pushbutton.
13. Choose the *Close* pushbutton.

    The scheduled job appears in the table with one of the following statuses:

Status	Description
Planning	The job is either currently working on the request, or the job is scheduled to start at a later time.
Completed	The job has completed.
Terminated	The job was terminated by the administrator.
Error	An error was detected with the job.

Note that if the Admin Review option is set to *No*, the MSMP workflow begins at this point.

7.1.1 Managing Role Assignment and Usage Data

Note the following when managing role usage data to ensure that the required data is used by the UAR process:

- The role usage job appends existing data in the table.
- The BRM data populated by the role usage synchronization job (or by the manual upload of role usage information) is not the data reported in the *BRM User to Role Relationship* report.

8. Performing an Admin Review

Administrators can evaluate requests to ensure completeness and accuracy of the request information prior to sending workflow items to reviewers. If the requests are incomplete or inaccurate, administrators can do the following:

- Cancel the current UAR requests
- Maintain user-to-manager relationships in the User Details Data Source
- Generate new requests

This section describes how administrators can review a request if the *Admin review required before sending tasks to reviewers* parameter is set to *YES* in the *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings* Customizing activity.

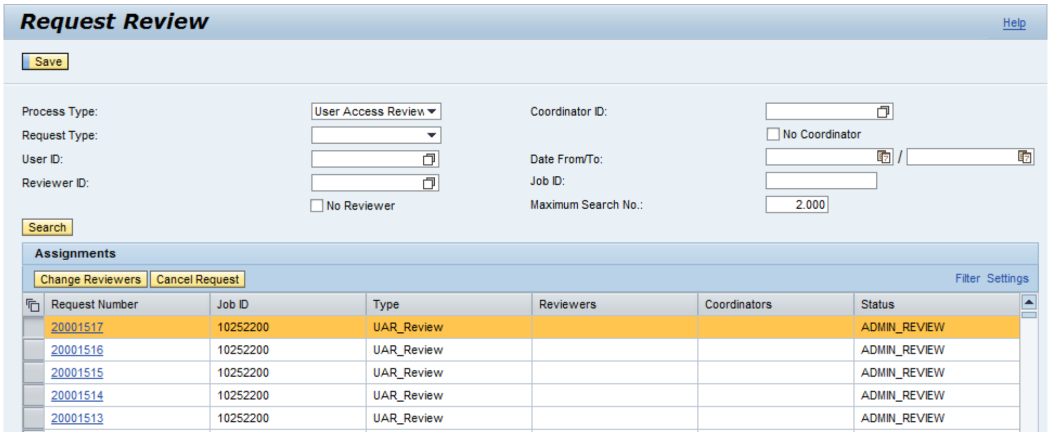
In this case, administrators can also add reviewers and coordinators, if they are not defined for the role or user.

⚠

This step is not applicable in cases when the *Admin review* setting is set to NO in the *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings* Customizing activity.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management > Compliance Certification Reviews > Request Review*. The *Request Review* screen appears.



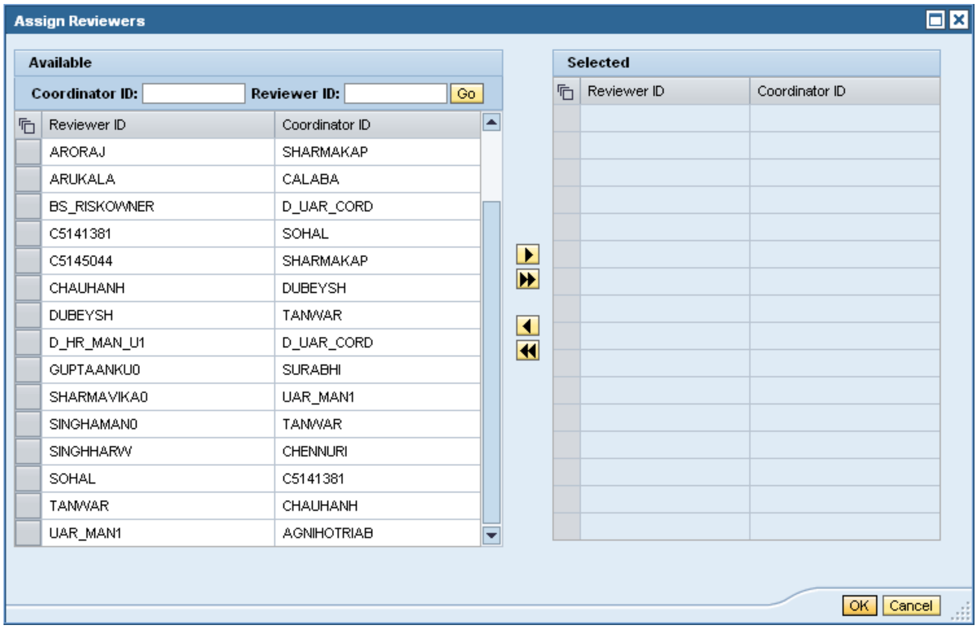
Process Type: User Access Review
Request Type:
User ID:
Reviewer ID:
□ No Reviewer
Coordinator ID:
□ No Coordinator
Date From/To: /
Job ID:
Maximum Search No.: 2.000

Assignments

Request Number	Job ID	Type	Reviewers	Coordinators	Status
20001517	10252200	UAR_Review			ADMIN_REVIEW
20001516	10252200	UAR_Review			ADMIN_REVIEW
20001515	10252200	UAR_Review			ADMIN_REVIEW
20001514	10252200	UAR_Review			ADMIN_REVIEW
20001513	10252200	UAR_Review			ADMIN_REVIEW

3. Search for a request by specifying the criteria, including the *Process Type* and *Request Type*, among other criteria, and choose the *Search* pushbutton.
4. To change reviewers, select an assignment and choose the *Change Reviewers* pushbutton. The *Assign Reviewers* dialog box appears.

   Select one more reviewers and coordinators from the *Available* list, and choose the right-arrow pushbutton to move the entries to the *Selected* list. After assigning the reviewers and coordinators, choose *OK*.



Reviewer ID	Coordinator ID
ARORAJ	SHARMAKAP
ARUKALA	CALABA
BS_RISKOWNER	D_UAR_CORD
C5141381	SOHAL
C5145044	SHARMAKAP
CHAUHANH	DUBEYSH
DUBEYSH	TANWAR
D_HR_MAN_U1	D_UAR_CORD
GUPTAANKU0	SURABHI
SHARMAVIKA0	UAR_MAN1
SINGHAMAN0	TANWAR
SINGHHARW	CHENNURI
SOHAL	C5141381
TANWAR	CHAUHANH
UAR_MAN1	AGNIHOTRIAB

Note that coordinators are for reporting purposes only; coordinators cannot take any action. For example, if a reviewer does not take action for a request, the coordinator is notified, depending on the configuration settings.

5. To cancel a request, select an assignment and choose the *Cancel Request* pushbutton.

   A confirmation dialog box appears. Choose *Yes* to mark the users as rejected for request regeneration; choose *No* to cancel the request from this review.

6. Choose the *Save* pushbutton.

8.1 Updating the Workflow for UAR Requests

After you have generated the data for UAR and completed the admin review, as appropriate, you can execute the *Update Workflow for UAR request* job to send the workflow tasks to reviewers.

> This step is not applicable in cases when the *Admin review* setting is set to NO in the *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings* Customizing activity.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Scheduling* > *Background Scheduler*.
3. Choose the *Create* pushbutton. The *Schedule Details* step appears.
4. In the *Schedule Name* field, type the name of the UAR job.
5. In the Schedule Activity field, select *Update Workflow for UAR request* using the drop-down list.
6. In the *Recurring Plan* field, choose whether to schedule the job to recur.

   If you choose *Yes*, you need to specify the recurring date and time range, along with the frequency and recurrence interval.

7. In the *Start Immediately* field, choose whether to start the job immediately.
8. In the *Start Time* field, specify the date and time for the job to start.
9. Choose the *Next* pushbutton. The *Select Variant* step appears.
10. Choose the *Finish* pushbutton.

Note that if the Admin Review option is set to *Yes*, the MSMP workflow begins at this point.

9. Reviewing UAR Requests

After you update the request workflow, the request follows the workflow path and is routed to the appropriate reviewer.

9.1 Managing UAR Requests

This section describes how to manage UAR requests. After a request is generated, it is sent to the reviewer's *Work Inbox*.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *My Home* > *Work Inbox* > *Work Inbox*.

   Requests appear in your work inbox and email inbox (if your email address is configured in the system).

   Alternatively, administrators can access requests by navigating to *Access Management* > *Access Requests Administration* > *Search Requests*.

3. Open a request.

   You can perform the following tasks:

Task	Description
Approve	Approves the request (the role is not removed).
Remove Role	Removes the role (from the user).
Forward	Forwards the request to another reviewer with a note.
Reject User/Role	Rejects the user or role (based on the *Reviewers* setting in the *Governance, Risk and Compliance* > *Access Control* > *Maintain Configuration Settings* Customizing activity).
Reason	Specifies the reason for the rejection. You can maintain the rejection reasons using the *Governance, Risk, and Compliance* > *User Provisioning* > *Maintain Review Rejection Reasons* Customizing activity.
Add Comment	Adds a comment to the review request.

A user’s manager may reject users for whom they are no longer responsible during UAR approver review. After being rejected, users can then be included in new requests, if required. Rejected users are also visible in the *UAR History* report and the *User Review Status* report.

Note that the *Reject User* option is not relevant for the reviewer stage if the reviewer is the role owner. The Role Owner review screen does not include the option to reject a user, but does include options to approve or remove access.

4. Choose the *Submit* pushbutton to submit the request.

   You can also view the Audit Log, attach a file, or view and edit comments by switching tabs within the *User Access Review* screen.

⚠

After submitting the review request by choosing the *Submit* pushbutton, you cannot make any further changes to the request (as it moves to the next stage).

9.2 Managing Rejected Users

Authorized users can search for rejected users, view search results, sort the results by user, and generate review requests. Authorized users can also cancel review request generation for those requests that have not been completed.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Compliance Certification Reviews* > *Manage Rejections*. The *Manage Rejections* screen appears.
3. Specify the search criteria and choose the *Search* pushbutton. The rejected users appear in the *Result* table.
4. To select users for UAR request generation, select the corresponding rejection and choose the *Generate Requests* pushbutton.

   This marks the user for inclusion in a new UAR request when the *UAR Review Process Rejected* background job is executed.

   Before generating requests for rejected users, make sure the users have the correct reviewer information. This prevents incorrect information from entering the request cycle again. For example, if the reviewer information is stored in an LDAP data source and is incorrect, it must be updated in the LDAP data source so that new requests are generated with the correct reviewer name.

   Note that if the Admin Review option is set to *Yes*, the administrator can choose to modify the reviewer/coordinator information to correct the reviewer information. The system generates a request for users without a manager in the data source when the reviewer is set as the manager.

5. To cancel request generation, select the corresponding rejections and choose the *Cancel Generation* pushbutton.

   For example, you can cancel the request generation for all users with a request status of *To Generate*. Note that after the request status is *In Process*, the background job has already started and the request cannot be cancelled.

9.2.1 Generating New Requests for Rejected Users

You can generate new requests for rejected users, as required.

Procedure

1. Log on to the frontend GRC Access Control 10.0 system.
2. Navigate to *Access Management* > *Scheduling* > *Background Scheduler*.
3. Choose the *Create* pushbutton. The *Schedule Details* step appears.
4. In the *Schedule Name* field, type the name of the UAR job.
5. In the Schedule Activity field, select *Generates new request for UAR rejected request* using the drop-down list.
6. In the *Recurring Plan* field, choose whether to schedule the job to recur.

   If you choose *Yes*, you need to specify the recurring date and time range, along with the frequency and recurrence interval.

7. In the *Start Immediately* field, choose whether to start the job immediately.
8. In the *Start Time* field, specify the date and time for the job to start.
9. Choose the *Next* pushbutton. The *Select Variant* step appears.
10. Choose the *Finish* pushbutton.