



User Access Review (UAR) Reference Guide

SAP Access Control 12.0

Target Audience

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

Document version: 1.0 – March 2018

**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

© Copyright 2018 SAP AG. All rights reserved.

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.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, 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 are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

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 expressly 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>

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
	Syntax

Contents

Contents

1.	<i>Getting Started</i>	5
1.1	Document History	5
1.2	About this Guide.....	5
1.3	Audience for this Guide.....	6
2.	<i>Introducing User Access Review</i>	7
3.	<i>Participants in the UAR Process</i>	7
4.	<i>Exploring the UAR Process</i>	8
5.	<i>Roles in the UAR</i>	9
5.1	Choosing Role Types in the UAR Process	11
6.	<i>Exploring Process Options</i>	14
6.1	Admin Review.....	14
6.2	Security Stage	14
6.3	Additional Approver Stage	14
7.	<i>Understanding Workflow Stage Configuration</i>	14
7.1	Configuring Email Notification	15
7.2	Setting Reminders	15
7.3	Specifying Escalation	15
8.	<i>Performing Automatic Provisioning</i>	16
9.	<i>Prerequisites</i>	16
9.1	Importing Roles	16
10.	<i>Managing IMG Configurations for UAR</i>	17
12.0	Maintaining Configuration Settings.....	17
10.2	Defining an Email Reminder.....	19
10.3	Specifying the Service Level Agreement	20
11.	<i>Managing Coordinators</i>	21
12.	<i>Managing the UAR Workflow</i>	23
12.1	Managing Workflow Settings for UAR.....	23
13.	<i>Generating Data for UAR</i>	31
14.	<i>Performing an Admin Review</i>	34
14.1	Updating the Workflow for UAR Requests.....	37
15.	<i>Reviewing UAR Requests</i>	38
15.1	Managing UAR Requests	38
15.2	Managing Rejected Users.....	40
15.3	Generating New Requests for Rejected Users	41

1. Getting Started

SAP Access Control (AC) 12.0 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 feature of SAP Access Control automates and documents the periodic decentralized user access review by business managers or role owners.

User Access Review (UAR) 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 an SAP Access Control 12.0 environment. It describes the features, processing options, configuration, and use of the UAR.

1.1 Document History

The UAR Reference Guide is regularly updated on the *SAP Service Marketplace* at service.sap.com/instguides.



Make sure you have the latest version of the UAR Reference Guide by checking the *SAP Service Marketplace* before performing user access reviews.

Version	Date	Description
1.0	March 2018	Initial release

1.2 About this Guide

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



This guide provides business use cases as examples of 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.

The guide discusses UAR for SAP Access Control 12.0. Any attempt to use this guide for other product versions is not supported.

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

UAR in Access Control 12.0 offers the following features:

- An automated process for periodic access review
- Decentralized review of user access
- Workflow of requests for review and approval
- 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
- Support for business roles

The key benefits of the UAR are:

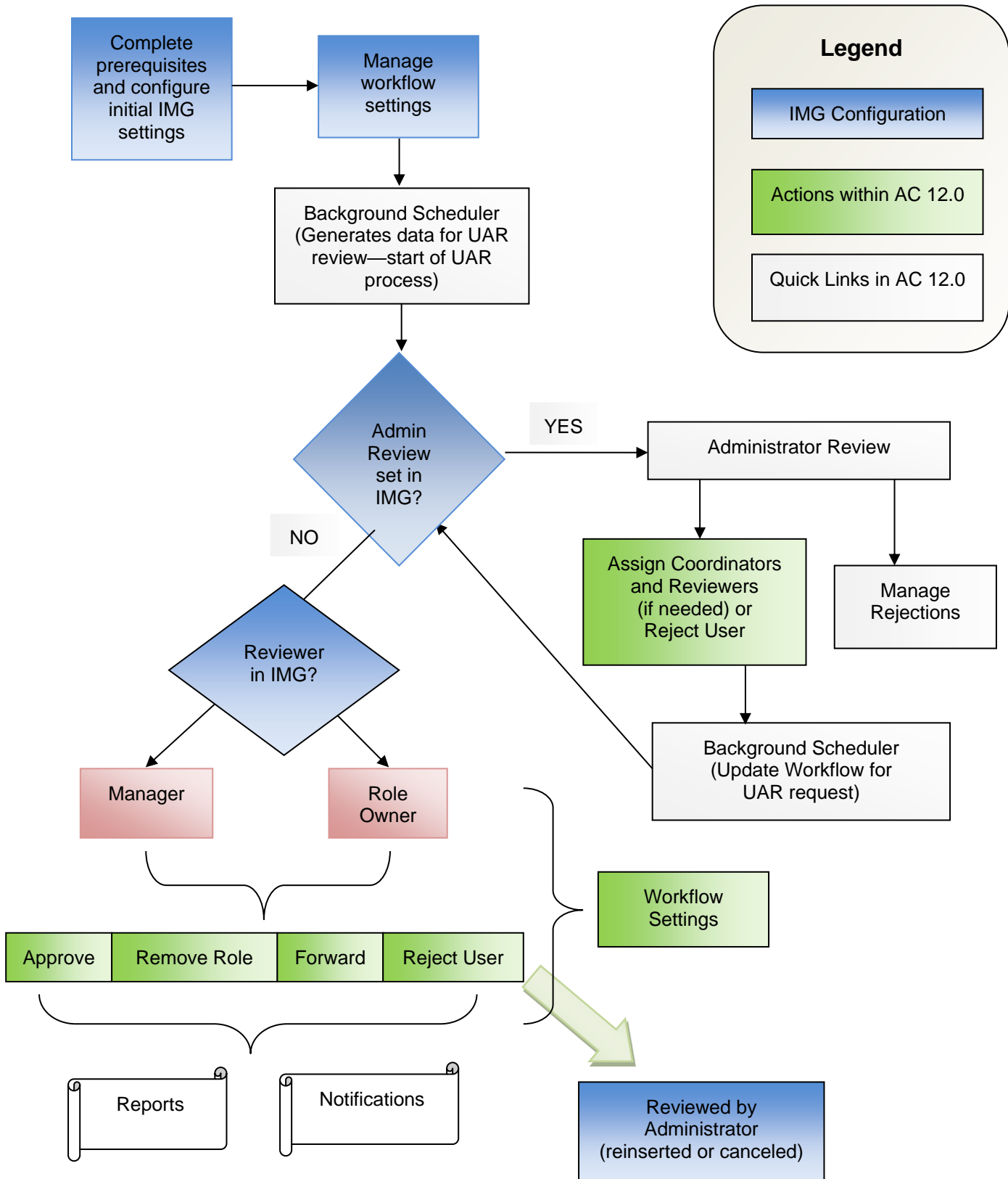
- A streamlined internal control process with collaboration among business managers, internal control, and information technology teams
- Improved efficiency and visibility of the internal control process

3. Participants in the UAR Process

SAP Access Control 12.0 includes the following participants 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 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.

4. Exploring the UAR Process



5. Roles in the UAR

A role is a set of access privileges and permissions within your IT landscape. The roles assigned to a user determine which business activities the user can perform and which parts of the user interface the user can view. Examples of roles could be Accounts Payable Representative, Project Manager, and Financial Analyst.

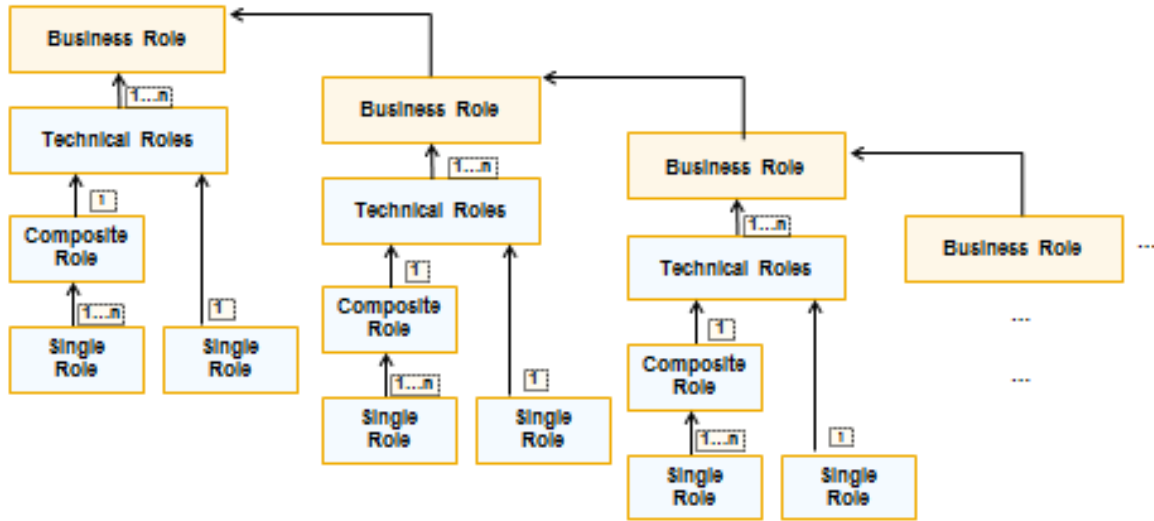
Within SAP Access Control 12.0, users can be assigned various types of roles that are explained below. All users must be assigned at least one role in order to access a system.

Role Types in SAP Access Control 12.0

Role Type	Description
Single Role	Authorization privileges assigned to a single user in one or more systems
Composite Role	Authorization privileges assigned to a grouping of multiple single roles
Derived Role	<p>A role that is created from an existing single role. There are two possible reasons for creating a derived role:</p> <ul style="list-style-type: none"> You want a new role that contains identical menus from your original role, but contains different authorizations for the menu actions You want a new role with the same menu and authorizations as the original role but with different organizational levels
Technical Role	<p>A classification for roles with authorizations associated with them. Technical roles can be single roles, composite roles, or derived roles.</p>
Business Role	<p>A logical grouping for technical and business roles. There are no authorizations assigned to the business role; all authorizations reside in the technical roles that comprise the business role.</p>

The illustration below shows how the different role types relate to one another:

Role Relationships



For more information about roles in SAP, see the SAP Help Portal at help.sap.com. Explore the following topics:

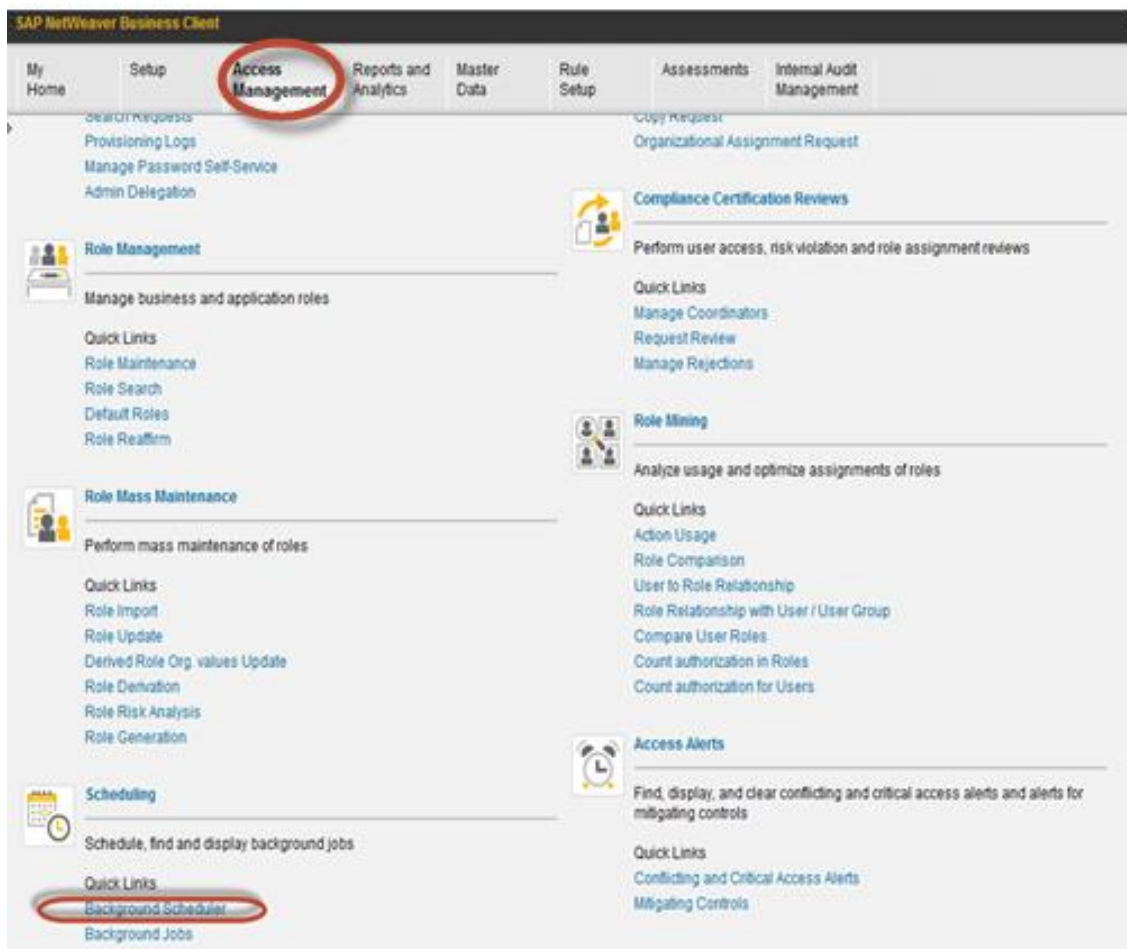
- *Role Maintenance in PFCG*
- *AS ABAP Authorization Concept*

5.1 Choosing Role Types in the UAR Process

When you perform the UAR, you can decide which types of roles you want to include and at which level the report runs. You can choose to look only at technical roles or you can choose to include business roles in your analysis. If you choose only technical roles, you produce a report at the *technical role level*. If you choose to include business roles, you produce a report at the *business role level*.

You decide at which level to produce the report when you schedule the UAR. The screenshots below show where in the scheduling process you make your choice.

1. From within SAP Access Control, you begin by choosing *Access Management* → *Scheduling* → *Background Scheduler*.



2. On the *Schedules* screen, choose *Create*.

Active Queries

Schedules **Access Management (42)**

Schedules - Access Management

Show Quick Criteria Maintenance Cha

View: [Standard View] Open Create Cancel Delete Print Version Export

Schedule Name	Schedule Activity	Created On	Created By	Changed On	Changed By	Start On
UAR 678799 2	Generates data for access request UAR review	20.09.2014 03:23:11	Jackie Wang	20.09.2014 03:23:11	Jackie Wang	20.09.2014 03:23:11
UAR 1453167 2	Generates data for access request UAR review	20.09.2014 03:19:14	Jackie Wang	20.09.2014 03:19:14	Jackie Wang	20.09.2014 03:19:14
UAR 678799	Generates data for access request UAR review	19.09.2014 19:51:10	Jackie Wang	19.09.2014 19:51:10	Jackie Wang	19.09.2014 19:51:10
UAR 1453167	Generates data for access request UAR review	19.09.2014 19:48:05	Jackie Wang	19.09.2014 19:48:05	Jackie Wang	19.09.2014 19:48:05
UAR Tech Ankush	Generates data for access request UAR review	19.09.2014 01:56:31	Jackie Wang	19.09.2014 01:56:31	Jackie Wang	19.09.2014 01:56:31
UAR All Tech	Generates data for access request UAR review	19.09.2014 01:42:14	Jackie Wang	19.09.2014 01:42:14	Jackie Wang	19.09.2014 01:42:14
UAR Provision	Generates data for access request UAR review	12.09.2014 22:29:25	Jackie Wang	12.09.2014 22:29:25	Jackie Wang	12.09.2014 22:29:25
UAR GUARUA	Generates data for access request UAR review	12.09.2014 20:58:40	Jackie Wang	12.09.2014 20:58:40	Jackie Wang	12.09.2014 20:58:40
UAR_REQ_GEN1	Generates data for access request UAR review	12.09.2014 20:21:03	Ankush Gupta	12.09.2014 20:21:03	Ankush Gupta	12.09.2014 20:21:03
UAR UP SR5	Generates data for access request UAR review	10.09.2014 19:47:46	Jackie Wang	10.09.2014 19:47:46	Jackie Wang	10.09.2014 19:47:46
RA_1	Mass Role Import	09.09.2014 00:39:14	Grishmi Patel	09.09.2014 00:39:14	Grishmi Patel	09.09.2014 00:39:14
UAR SR5 2	Generates data for access request UAR review	06.09.2014 00:56:26	Jackie Wang	06.09.2014 00:56:26	Jackie Wang	06.09.2014 00:56:26
UAR SR5 1	Generates data for access request UAR review	04.09.2014 07:40:13	Jackie Wang	04.09.2014 07:40:13	Jackie Wang	04.09.2014 07:40:13
UAR SR5	Generates data for access request UAR review	04.09.2014 06:17:28	Jackie Wang	04.09.2014 06:17:28	Jackie Wang	04.09.2014 06:17:28
UAR 16	Generates data for access request UAR review	03.09.2014 20:14:25	Grishmi Patel	03.09.2014 20:14:25	Grishmi Patel	03.09.2014 20:14:25

3. On the *Create Scheduler* screen, enter the scheduling details for the UAR job. If you want to include business roles in the analysis, check the box *Generate UAR for Business Roles*.

Scheduler □ ×

Create Schedule

1
Schedule Details

2
Select Variant

3
Review

4
Confirmation

< Previous
Next >
Cancel

* Schedule Name:

* Schedule Activity: Generates data for access request UAR review

* Recurring Plan: Yes No

* Start Immediately: Yes No

* Start Time: HH MM SS i

Generate UAR for Business Roles:



For more information about scheduling the UAR, see the section *Generating Data for UAR* in this reference guide.

6. Exploring Process Options

Access Control 12.0 offers multiple process options that determine the approvers of UAR requests. This section describes the available process options.

6.1 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.

6.1.1 Reviewer Stage

You can specify whether the reviewer stage is addressed by a user's manager or by the role owner.

6.2 Security Stage

You can choose to include a security stage. 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 specified 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.

6.3 Additional Approver Stage

You can choose to include an additional stage with the approver derived by a Custom Approver Determinator (CAD), if required. The fields available in the UAR CAD are:

- Application
- Request type
- Role(s) being reviewed

7. Understanding Workflow Stage Configuration

After deciding on the stages to include in the UAR workflow, you must determine the specific behavior for each stage. These behaviors include the following:

- Email notification
- Reminders
- Escalation

7.1 Configuring Email Notification

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

7.2 Setting Reminders

You must 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 the body content.

7.3 Specifying Escalation

In the details associated with each stage, you specify whether to escalate UAR requests. 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 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.

8. Performing Automatic Provisioning

You decide whether to provision requests automatically at the end of the request's workflow. If your decision is "yes," roles that are marked for removal in the User Access Review are automatically de-provisioned in the target system.

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

9. Prerequisites

You must run the following synchronization job to generate UAR requests.

1. Log on the backend SAP Access Control 12.0 system.
2. From the *SAP Easy Access* screen, choose *Tools* → *Customizing* → *IMG* → *Execute Project*.
3. Choose *SAP Reference IMG* → *Governance, Risk, and Compliance* → *Access Control* → *Synchronization Jobs* → *Repository Object Sync*.

9.1 Importing Roles

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

Procedure

1. Log on to the frontend SAP Access Control 12.0 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.
4. Choose *Next*.
5. 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).
6. Choose *Next*.
7. In *Step 3: Review*, choose a preview option and review the information displayed.
8. Choose *Next*.
9. 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
10. Choose *Submit*.

10. Managing IMG Configurations for UAR

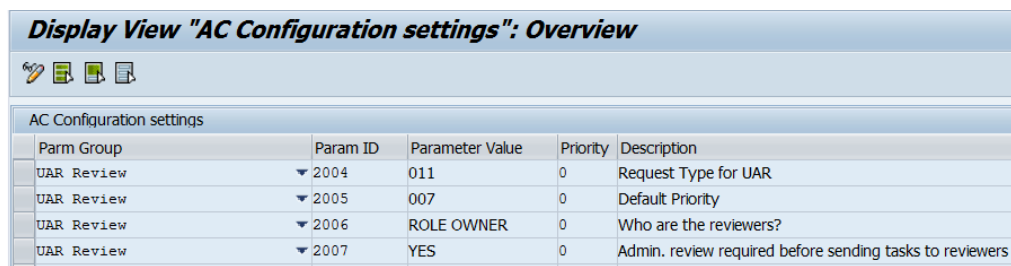
This section describes how to maintain the configuration settings related to UAR and generate the data for UAR.

10.1 Maintaining Configuration Settings

Procedure

1. Log on to the backend SAP Access Control 12.0 system.
2. From the *SAP Easy Access* screen, choose *Tools > Customizing > IMG > Execute Project*.
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.

Display View "AC Configuration settings": Overview



Param Group	Param ID	Parameter Value	Priority	Description
UAR Review	▼ 2004	011	0	Request Type for UAR
UAR Review	▼ 2005	007	0	Default Priority
UAR Review	▼ 2006	ROLE OWNER	0	Who are the reviewers?
UAR Review	▼ 2007	YES	0	Admin. review required before sending tasks to reviewers

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 the user or the role owner for the role can review the UAR request. Parameter 2007 - *Admin review required before sending tasks to reviewers* - can be one of the following:

Parameter 2007 Value	Behavior
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.

The review can be generated by role or user. If you are reviewing by role, you can use Access Control configuration parameter 4019 -- *Do not copy manual role assignment changes during repository sync*. This parameter determines whether you want manual role or profile changes that are done in transaction *SU01 (User Maintenance)* or *SU10 (User Maintenance: Mass Changes)* to be synchronized to the GRC box.

AC Configuration settings			
Parm Group	Param ID	Parameter Value	Description
Access Request Business Role ▼	4019	NO	Do not copy manual role assignment changes during repository sync.

Parameter 4019 Value	Description
NO	If you do want manual role or profile changes that are done in SU01 or SU10 to be synchronized to the GRC box, set the parameter to NO.
YES	If you do not want manual role or profile changes to be synchronized to the GRC repository, set the parameter to YES.



You can maintain the following items in Customizing:

Item	Menu Path
Request Type	<i>Governance, Risk and Compliance > Access Control > User Provisioning > Define Request Type.</i>
Priority	<i>Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Priority Configuration</i>
Number ranges for provisioning requests	<i>Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Number Range Intervals for Provisioning Requests</i>
Rejection reasons	<i>Governance, Risk and Compliance > Access Control > User Provisioning > Maintain Review Rejection Reasons for Provisioning Requests</i>

10.2 Defining an Email Reminder

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

Procedure

1. Log on to the backend SAP Access Control 12.0 system.
2. From the *SAP Easy Access* screen, choose *Tools > Customizing > IMG > Execute Project*.
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.
5. Define the body of the notification message using *General text* as the *Document Class*.
6. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Custom Notification Messages*.
 - The *Notification Messages (Customer) Overview* screen appears.
7. Specify the sender, subject, and attachment of the notification message.
8. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Custom Notification Messages*.
 - The *Notification Messages (Customer) Overview* screen appears.
9. Specify the sender, subject, and attachment of the notification message.

10. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain MSMP Workflows*.
 - The *MSMP Workflow Configuration* screen appears.
11. Select the appropriate *Process ID*, and choose *Step 4: Variables & Templates*.
12. Create a *Notification Template* and map the template to the *Message Class*.
13. Choose *Step 7: Generate Versions* and save. Activate the configuration.
14. Navigate to *Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain Background for E-mail Reminders*.
 - The *Define Background Job* screen appears.
15. Specify the background job information for the notification message.

10.3 Specifying the Service Level Agreement

You can define the service level agreement for UAR requests.

1. Log on to the backend SAP Access Control 12.0 system.
2. From the *SAP Easy Access* screen, choose *Tools > Customizing > IMG > Execute Project*.
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*.

11. Managing Coordinators

This section describes how to manage coordinators for requests.

Procedure

1. Log on to the frontend SAP Access Control 12.0 system.
2. Navigate to *Access Management > Compliance Certification Reviews > Manage Coordinators*.
 - The *Manage Coordinators* screen appears.

Coordinator ID	Coordinator Name	Coordinator Email	Reviewer ID	Reviewer Name	Reviewer Email
ADITHEVENKA	ADITHEVENKA		ADITHEVENKA	ADITHEVENKA	
CHINNATHAMBI	CHINNATHAMBI		ADITHEVENKA	ADITHEVENKA	
ADITHEVENKA	ADITHEVENKA		CHINNATHAMBI	CHINNATHAMBI	
CHINNATHAMBI	CHINNATHAMBI		PULIVENKATA	PULIVENKATA	

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

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

Change Mapping

Save Close

Coordinator Details

Coordinator ID: ABBOT

Name: Nayan Abbot

Email:

Reviewer Details

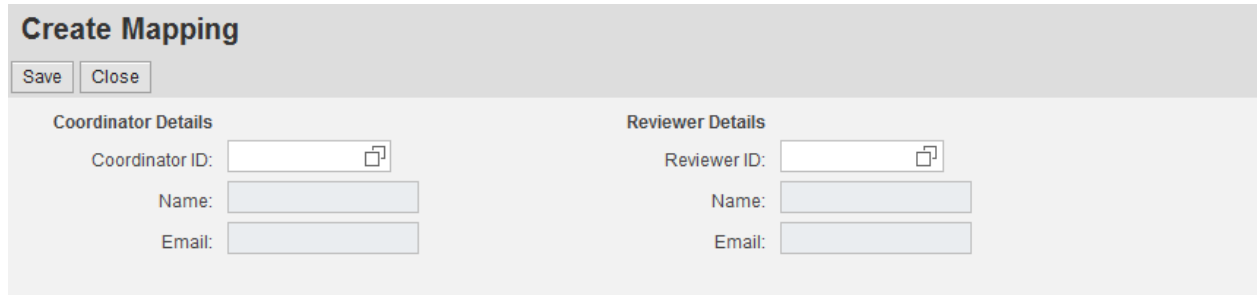
Reviewer ID: ADITHEVENKA

Name: ADITHEVENKA

Email: AMAN@SAP.COM

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*.


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



Create Mapping

Save Close


Coordinator Details

Coordinator ID: 

Name:

Email:

Reviewer Details

Reviewer ID: 

Name:

Email:

- In the *Coordinator ID* field, type or select the appropriate value.
- In the *Reviewer ID* field, type or select the appropriate value.
- Choose the *Save* pushbutton.
- Choose the *Close* pushbutton. The mapping appears in the table on the *Manage Coordinators* screen.
- 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.

12. Managing the UAR Workflow

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

12.1 Managing Workflow Settings for UAR

This section describes manage workflow settings for UAR.

Procedure

1. Log on to the backend SAP Access Control 12.0 system.
2. From the *SAP Easy Access* screen, choose *Tools > Customizing > IMG > Execute Project*.
3. Choose the *SAP Reference IMG* button.
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.

The screenshot displays the 'Process Global Settings' configuration page. It includes sections for 'Enable Escalation', 'Notification Settings', and 'Escape Conditions'.

Process Global Settings

Enable Escalation:
Escalation Date: *

Notification Settings

Buttons: Add, Modify, Delete

Notification Event	Template ID	Recipient ID

Escape Conditions

Escape Condition	Set Escape Routing
Approver Not Found	<input type="checkbox"/>

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: Step 2 of 7 (Maintain Rules)

Process: User Access Review Workflow

Rule ID Maintenance

List of Rules

Rule ID	Rule Description	Rule Type	Rule Kind
GRAC_MSMP_REVIWER_AGENT	Reviewer agent rule	Function Module Based Rule	Agents Rule
GRFNMW_INST_CREATED_BY_AGENT	Request creator agent rule	Function Module Based Rule	Agents Rule
GRFNMW_INST_CURRENT_APPROVERS	Current Approvers	Function Module Based Rule	Agents Rule
GRAC_USERACCRVW_INITIATOR	Default Initiator rule	Function Module Based Rule	Initiator Rule
GRAC_MSMP_DETOUTR_UAR_REV_ROLE	Assignments with remove action routing rule	Function Module Based Rule	Routing Rule

Global Rules

Process Initiator: * GRAC_USERACCRVW_INITIATO [?] Default Initiator rule

Notification Rule: GRAC_NOTIF_VAR_RULE_USER [?] 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.

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

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

MSMP Workflow Configuration: Step 3 of 7 (Maintain Agents)

< Previous Next >

1 2 **3** 4 5 6 7
 Process Global Settings Maintain Rules **Maintain Agents** Variables & Templates Maintain Paths Maint Route Mapping Generate Versions

Process:

Agents

Add Modify Delete

View: [Standard View] Export

Agent ID	Agent Name	Agent Type	Agent Purpose
GRAC_CURRENT_APPROVERS	Current Approvers	GRC API Rules	Notification
GRAC_REQUESTOR	Requester	GRC API Rules	Notification
GRAC_UAR_REVIEWER	UAR Reviewer	GRC API Rules	Approval

The following table lists the agent types:

Agent Type	Description
Directly Mapped Users	Approvers selected from the Approver definition.
PFCG Roles	Users with a specific role are selected.
PFCG User Groups	Approvers selected from PFCG User Groups assigned to users (SU01 Groups tab).
SAP API Rules	Approvers 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.

MSMP Workflow Configuration: Step 4 of 7 (Variables & Templates)

← Previous Next →

1 2 3 4 5 6 7
 Process Global Settings Maintain Rules Maintain Agents Variables & Templates Maintain Paths Maint Route Mapping Generate Versions

Process: User Access Review Workflow

Notification Templates

Template ID	Message Class	Message number	Docu. Object	Owner
GRAC_USERACC_APPROVED	OMSMP_USERACC_APPR	000	GRAC_MSMP_UAR_APPROVED	SAP
GRAC_USERACC_ESCALATION	OMSMP_USERACC_ESCL	000	GRAC_MSMP_UAR_ESCALATION	SAP
GRAC_USERACC_REJECTED	OMSMP_USERACC_REJC	000	GRAC_MSMP_UAR_REJECTED	SAP
GRAC_USERACC_WORK_ITEM	OMSMP_USERACC_NEWWI	000	GRAC_MSMP_UAR_NEWWORKITM	SAP

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.

MSMP Workflow Configuration: Step 5 of 7 (Maintain Paths)

← Previous Next →

1 2 3 4 5 6 7
 Process Global Settings Maintain Rules Maintain Agents Variables & Templates Maintain Paths Maint Route Mapping Generate Versions

Process: User Access Review Workflow

Maintain Paths

Path ID	Path Description
GRAC_DEFAULT_PATH	Default Path

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	Routing Level	Escalation Type	Escalation Time Mins	Escalation Agent
001	GRAC_DEFAULT_STAGE	Default stage			No					0	

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 <i>Any One Approver</i> or <i>All Approvers</i>
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Escalate to Specified Agent — Requires you to maintain the <i>Escalation Time Mins</i> and <i>Escalation Agent</i> 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 <i>Escalation Time Mins</i> 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 Mines	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. Use this dialog to specify the actions that an approver can perform at the selected stage.

MSMP Workflow Configuration: Step 5 of 7 (Maintain Paths)

Process Global Settings | Maintain Rules | Maintain Agents

Maintain Stages

Stage Seq. No.	Stage Config ID	Stage Descri...	Agent ID
001	GRAC_DEFA...	Default stage	

Stage Seq. No.: 001
 * Stage Config ID: GRAC_DEFAULT_STAGE
 * Stage Description: Default stage

Hide Details

Agent ID:
 Approval Type:
 Routing Enabled:
 * Rule ID:
 * Routing Level:
 Escalation Type: Use Defaults

Stage Definition

Stage Details

Stage Config ID: GRAC_DEFAULT_STAGE
 * Agent ID: GRAC_UAR_REVIEWER
 * Approval Type: Any One Approver
 Routing Enabled:
 Escalation Type: No Escalation

Task Settings

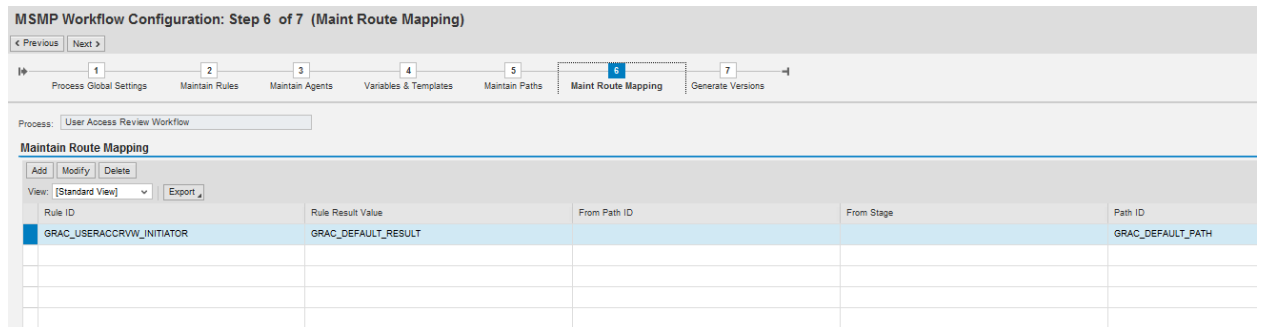
RT Config Change OK: Change Request Det:
 Email Group: Comments Mandatory:
 Reroute: Forward Allowed:
 Display Review Scrn: Approval Type:
 Reject Users: Reaffirm Approve:

Save Cancel

Task Settings	Description
RT Config Change OK	Runtime Configuration Change OK – Use configuration changes available at runtime.
Email Group	Note: The application does not use this field. We provide it only for backward compatibility.
Reroute	Allows approvers to reroute the request to a previous stage as an alternative to rejecting the request. Note: The approval workflow is comprised of stages and paths. For a standard approver, the application does not display the reroute option in the first stage, because there is no previous stage. For an administrator, the reroute option is available for all the stages because the administrator can send the request to different paths.
Display Review Scrn	Select to show the <i>Review Screen</i> .
Reject Users	Approvers receive e-mails informing

	them that a request requires their attention. Such e-mails include a link that opens the user provisioning screen.
Change Request Det	Allows approvers to change the content of requests
Comments Mandatory	Requires approvers to enter comments when approving or rejecting a request.
Forward Allowed	Allows approvers to forward requests to another approver.
Approval Type	Allows approvers to approve requests for the following levels: Request Approvers have the authority to approve all roles in a request. For example, security approvers can approve any role relevant to a request. Role Approvers can approve only those roles that belong to them. System and Role Approvers have the authority to approve systems and roles.
Reaffirm Approve	Requires approvers to confirm their identities before approving requests.

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



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.
16. The *Generate Versions* step appears.
17. 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 Generate* pushbutton to activate versions.



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

13. Generating Data for UAR

You need to execute a job to retrieve the user-to-role relationship and role usage data 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 SAP Access Control 12.0 system.
2. Navigate to *Access Management > Scheduling > Background Scheduler*.
3. Choose the *Create* pushbutton. The *Schedule Details* step appears.

11:18:25 AM 9/22/2014

Scheduler

Create Schedule

1 2 3 4
Schedule Details Select Variant Review Confirmation

< Previous Next > Cancel

* Schedule Name: UAR Review 2014

* Schedule Activity: Generates data for access request UAR review

* Recurring Plan: Yes No

* Start Immediately: Yes No

* Start Time: 22.09.2014 HH 20 MM 17 SS 34

Generate UAR for Business Roles:

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. In the *Generate UAR for Business Roles*, check the box if you want to include business roles.
10. Choose the *Next* pushbutton. The *Select Variant* step appears.



The application ignores the *Connector id* parameter if you select business roles for processing.

11. Specify the selection criteria or choose a saved variant, as appropriate. You can save the selection criteria as a new variant, if required.
12. Choose the *Next* pushbutton.
 - a. The *Review* step appears displaying a summary of the scheduled job.

13. Review the summary, and choose the *Finish* pushbutton.
14. 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 later.
Completed	The job has completed.
Terminated	The job was terminated by the administrator.
Error	An error was detected with the job.



If the Admin Review option (parameter 2007) is set to *No*, the MSMP workflow begins at this point.

14. 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.



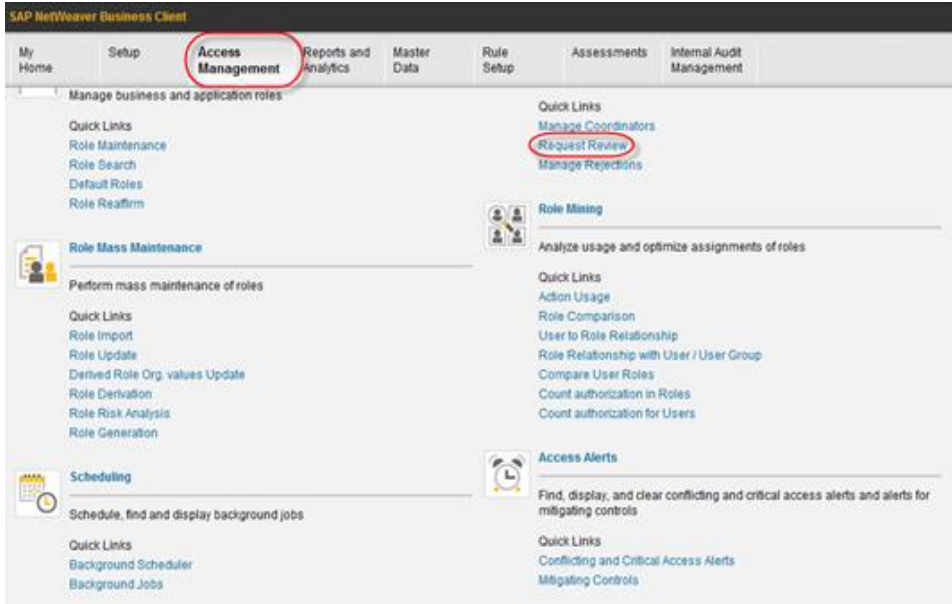
This step is not applicable in cases when the Admin review setting is set to NO in the *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings* Customizing activity.

This section describes how administrators can review a request if parameter *2007 Admin review required before sending tasks to reviewers* - is set to YES. This is done in Customizing under *Governance, Risk and Compliance > Access Control > Maintain Configuration Settings*.

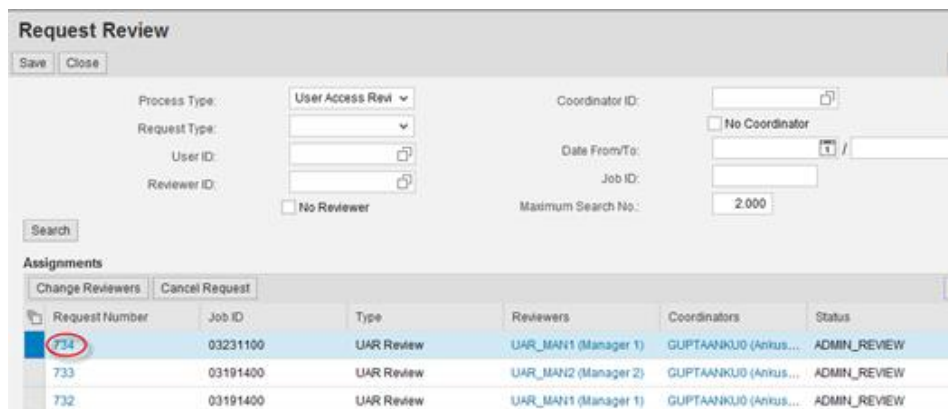
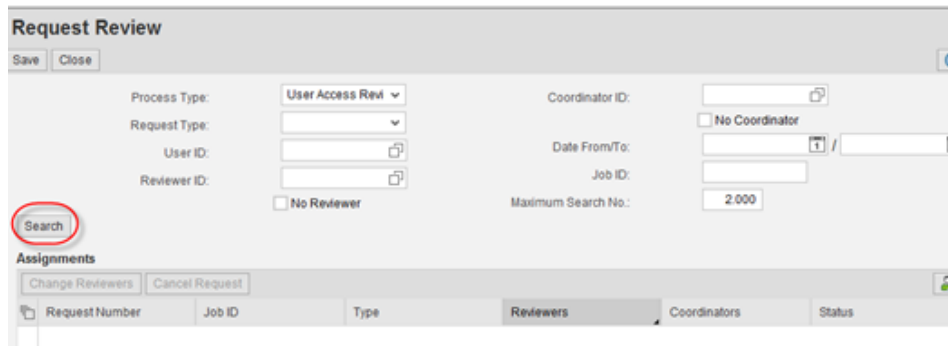
In this case, administrators can also add reviewers and coordinators, if they are not defined for the role or user.

Procedure

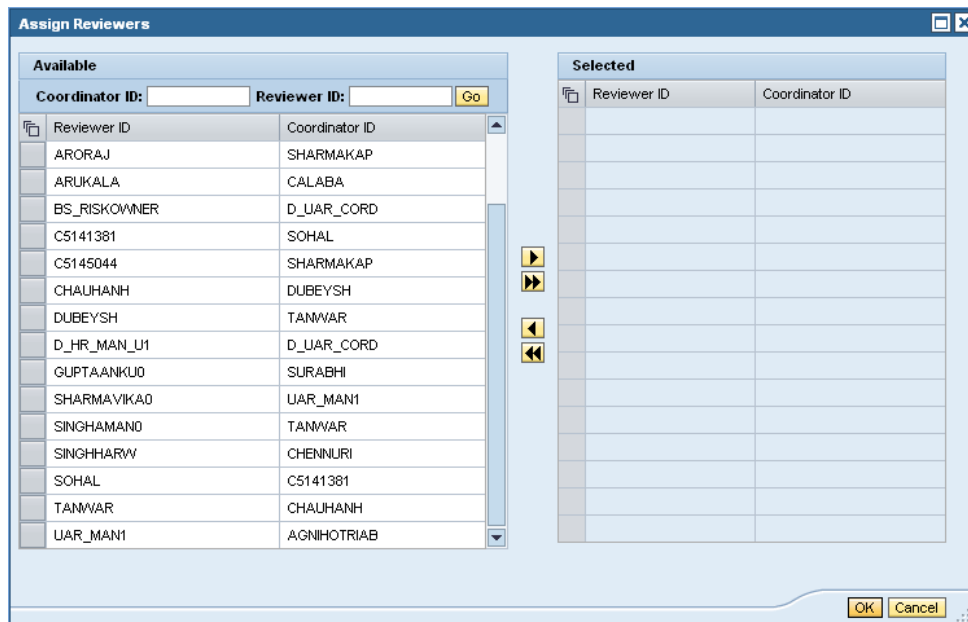
1. Log on to the frontend SAP Access Control 12.0 system.
2. Navigate to *Access Management > Compliance Certification Reviews > Request Review*.



3. The *Request Review* screen appears.



4. To change reviewers, select an assignment and choose the *Change Reviewers* pushbutton.
The *Assign Reviewers* dialog box appears.
5. Select one more reviewers and coordinators from the *Available* list, and choose the right-arrow pushbutton to move the entry to the *Selected* list. After assigning the reviewers and coordinators, choose *OK*.



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.

6. To cancel a request, select an assignment and choose the *Cancel Request* pushbutton.
 - a. A confirmation dialog box appears.
7. Choose *Yes* to mark the users as rejected for request regeneration; choose *No* to cancel the request from this review.
Choose the *Save* pushbutton.

14.1 Updating the Workflow for UAR Requests

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



This step is not applicable in cases when the *Admin review* setting (parameter 2007) is set to NO in the Governance, Risk and Compliance > Access Control > Maintain Configuration Settings Customizing activity.

Procedure

1. Log on to the frontend SAP Access Control 12.0 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.



If the *Admin Review* option (parameter 2007) is set to *Yes*, the MSMP workflow begins at this point.

15. Reviewing UAR Requests

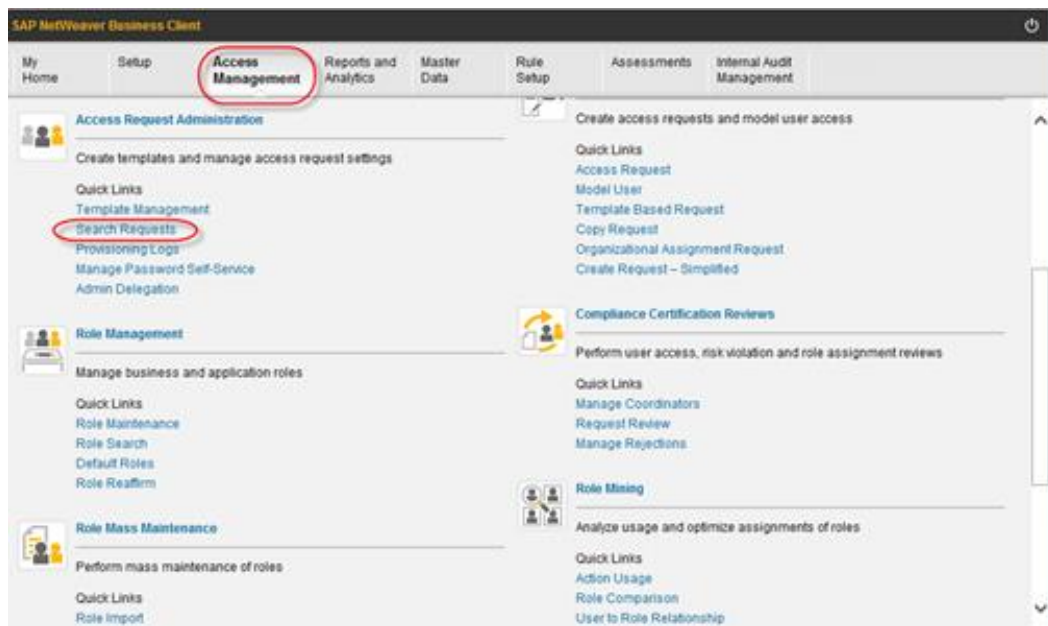
After you update the request workflow, the request follows the workflow path and is routed to the appropriate reviewer.

15.1 Managing UAR Requests

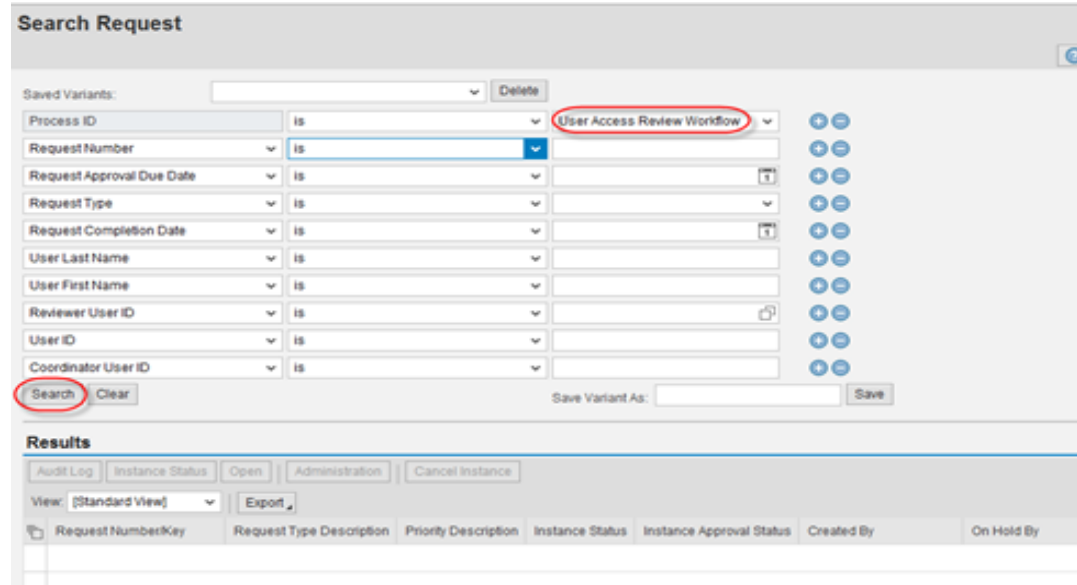
After a request is generated, it is sent to the reviewer's *Work Inbox*.

Procedure

1. Log on to the frontend SAP Access Control 12.0 system.
2. Navigate to *My Home > Work Inbox > Work Inbox*.
 - a. Requests appear in your work inbox and email inbox (if your email address is configured in the system).
 - b. Alternatively, administrators can access requests by navigating to *Access Management > Access Requests Administration > Search Requests*.
 - c. Search for a request by specifying the criteria, including the *Process Type* and *Request Type*, among other criteria, and choose the *Search* pushbutton.
 - d. A second way to find requests uses the *Search Requests* path:



- e. Enter the Process ID *User Access Review Workflow*



- 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	Reject the user or role (based on the <i>Reviewers</i> setting in the <i>Governance, Risk and Compliance > Access Control > Maintain Configuration Settings</i> Customizing activity).
Reason	The reason for the rejection. You can maintain the rejection reasons using the <i>Governance, Risk, and Compliance > User Provisioning > Maintain Review Rejection Reasons</i> 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 on new requests. Rejected users are also visible in the UAR History report and the User Review Status report.

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 the 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, you cannot make any further changes to the request (as it moves to the next stage).

15.2 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 SAP Access Control 12.0 system.
2. Navigate to *Access Management > Compliance Certification Reviews > Manage Rejections*.
 - a. The *Manage Rejections* screen appears.
3. Specify the search criteria and choose the *Search* pushbutton.
 - a. 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 (parameter 2007) 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 .After the request status is *In Process*, the background job has already started and the request cannot be cancelled.

15.3 Generating New Requests for Rejected Users

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

Procedure

1. Log on to the frontend SAP Access Control 12.0 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.