An Integration approach for GRC Access Controls & Identity Management solutions for achieving end to end Compliant provisioning

Applies to:

SAP GRC Access Control 5.3 and Compliant User provisioning

Summary

GRC Access Controls enables the external Identity Management applications and 3rd party/home grown applications to integrate and benefit the value from the real time integrated, end-to-end compliance provisioning solution for current complex environment and adhering to various internal and external regulatory and compliance standards. GRC Access Controls 5.2 and above have developed the compliance provisioning webservices to enable partners to develop the integration scenarios. This document provides more technical details of those webservices and the technical details for configuring the services between SAP GRC and Identity Management or home grown provisioning solutions.

Author(s): Srinivasa Kakkera & Swetta Singh

Company: SAP

Created on: 20 May 20, 2008

Author Bio

Srini Kakkera, Vice President, Development and responsible for product development & Partner Technology Development at SAP GRC. Srini has successfully completed various partner solution integrations with SAP GRC Apps and is actively working on architecture of GRC Compliance Services framework which can be extended for various partner solutions, home grown applications and 3rd party integration applications, which will benefit system integrators, partners, customers, and consultants. Srini has done extensive work in the area of enterprise application architecture, design and development for several years and managing distributed product development teams and established greater track record of releasing successful products into the aggressive market.

Swetta Singh, Architect and Development Manager supporting partner technology development at GRC for various partner technology integration initiatives such as Identity Management, Cisco, Greenlight and others. Swetta has strong architectural and design background and she has been very instrumental in completing the partner integration process and enablement activities.

Table of Contents

1.0 Overview

The GRC application enables the user to define policies or rules, and enforce these policies through the provisioning services.

The web services provided by GRC ensure that the user's provisioned into applications, do not have any risk's associated to the access granted to them.

The solution provides real-time monitoring and proactive enforcement of crucial access policies, such as those which support SOD (segregation of duties).

It anticipates potential SOD conflicts before they arise, and helps prevent any assignment of roles within an application which would compromise the proper segregation of duties. It also allows the customer to simulate changes of roles to determine if those changes would result in a potential risk.

The services enables the user's to provide 'out of policy privilege grants', but ensures that the correct remediation steps are taken to track those privileges.

GRC provides a mechanism to deliver greater governance and control over your environment. Segregation of duty and real time access management can now be a part of a standard provisioning process.

With the exposed services the customer can ensure every provisioning request adheres to company policies and regulatory requirement.

Key Features/ Benefits

Simplifies compliant, enterprise-level role administration

- Single authoritative source for enterprise role definition eliminates offline, manual errors and enforces best practice methodologies
- Technical and business owners use the same, consistent terms to describe the many possible roles within the enterprise.
- Automated risk analysis prevents violations.

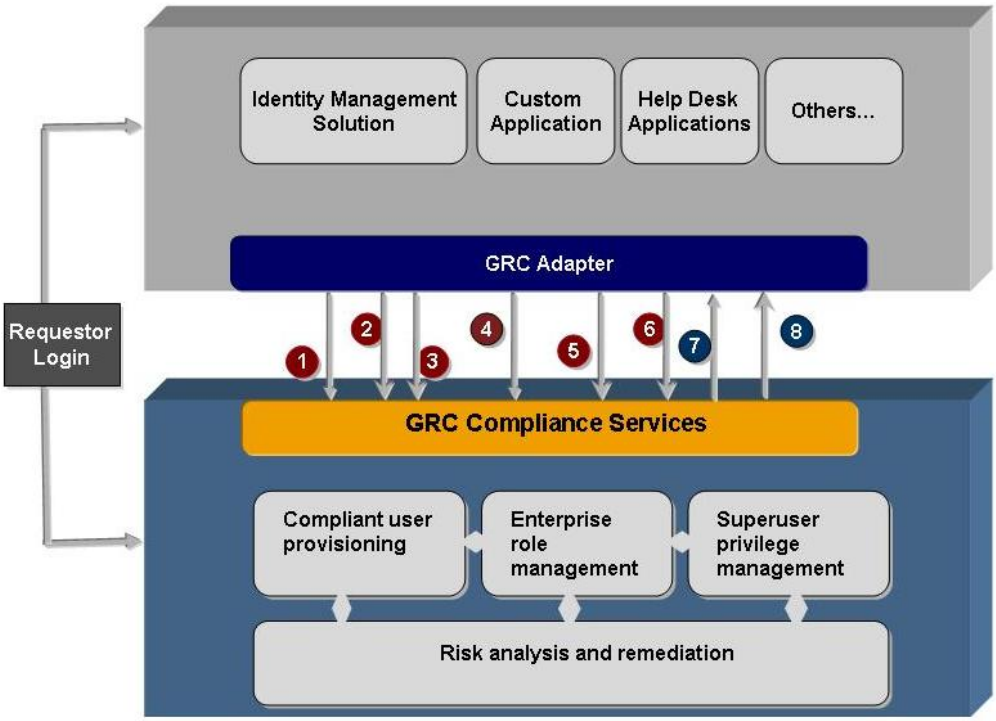
Automated change management empowers business users

- The approval workflow provides an easy documentation trail.
- Single-click automatic role creation and role comparison for SAP is possible.

Detailed reporting is audit-ready

- Combines role change history with integrity and security check documentation.

2.0 Web service Description



The web services available as a part of IDM integration are as follows.

From GRC:

1. **Request Submission to GRC** - **SAPGRC_AC_IDM_SUBMITREQUEST**

   The requestor can submit a request to GRC using this service, for compliant provisioning.

   Search Master Data [It is not implemented in the current release]

   This service provides the user the ability to lookup for master data required to submit the request.

   (Example: Functional Area, Priority, Custom Fields, and Request Types etc.)

2. **Select Applications** - **SAPGRC_AC_IDM_SELECTAPPLICATION**

   When the service is called by IDM, it returns a list of application resources configured within GRC to IDM.

   Select Applications (bi-directional)

   This service will return a list of applications configured within IDM.

   [It is not implemented in the current release]

   The information of the application resources configured within IDM is maintained in GRC itself.

3. **Risk Analysis** - **SAPGRC_AC_IDM_RISKANALYSIS**

   The service enables the user to perform Segregation of Duty (SoD) analysis, and returns the possible violations.

4. **Search Roles - SAPGRC_AC_IDM_SEARCHROLES**

   This service enables the user to search for roles before submitting a request to GRC. Additional filtration capabilities are also provided to narrow down the search as a part of this web service.

   - **Role Details** - **SAPGRC_AC_IDM_ROLEDETAILS**

     Detail information of the selected role can be obtained by calling this service.

   Search Roles (bi-directional)

   This service returns the list of roles configured within IDM.

   [It is not implemented in the current release.]

   The IDM roles have to be imported to GRC, which then enables the user to search roles before submitting the request.

5. **Audit Trail (including provisioning logs)** - **SAPGRC_AC_IDM_AUDITTRAIL**

   The Audit log web service will return a comprehensive detail list of audit history.

   It provides the audit history of user provisioning to IDM.

6. **Request Status** - **SAPGRC_AC_IDM_REQUESTSTATUS**

   This service returns the status, and detail request information for the selected request.

From IDM:

7. **Submit Request to IDM** - **SAPGRC_AC_IDM_SUBMITREQUEST_TO_IDM**

   This web service is called by GRC to submit a request to IDM.

   Following are two scenarios when the service will be called.

   - When a user is created or changed in an SAP HR system, a new request will be submitted to IDM to create or remove users and their privileges.

     Example: An event occurs in SAP HR, such as the hiring of a new employee.

     This event will initiate a request to enable the user have some basic privileges to perform the job function for which he/she is hired for.

     The request might consist of both ERP and Non-ERP applications. This will trigger a request being submitted to the IDM system for non-ERP system, while GRC processes the request for the ERP systems in the request.

     The audit logs, and request status can be consolidated into one by calling the ‘Audit Logs’ and ‘Request Status’ web service.

   - When a user requests non-ERP system from the GRC end user form, GRC calls this service to submit a request to IDM.

8. **Audit Trail from IDM - SAPGRC_AC_IDM_AUDITTRAIL_FROM_IDM**

   The Audit log web service will return a comprehensive detail list of audit history.

   It enables GRC to retrieve the audit Logs from IDM (for non-ERP provisioning).

** All messages returned by the web service will consist of a response object comprising of, Message Type, Message Code, and Message Description.

2.1 Release Date

Sl. No.	Web service name	Availability
1.	Submit Request to GRC **SAPGRC_AC_IDM_SUBMITREQUEST**	Q3 07 (AC 5.2 SP 4)
2.	Select Application **SAPGRC_AC_IDM_SELECTAPPLICATION**	Q3 07 (AC 5.2 SP 4)
3.	Risk Analysis **SAPGRC_AC_IDM_RISKANALYSIS**	Q3 07 (AC 5.2 SP 4)
4.	Search Roles, Role Details **SAPGRC_AC_IDM_SEARCHROLES,** **SAPGRC_AC_IDM_ROLEDETAILS**	Q1 08 (AC 5.3)
5.	Audit Logs **SAPGRC_AC_IDM_AUDITTRAIL**	Q3 07 (AC 5.2 SP 4)
6.	Request Status **SAPGRC_AC_IDM_REQUESTSTATUS**	Q1 08 (AC 5.3)
7.	Submit Request to IDM **SAPGRC_AC_IDM_SUBMITREQUEST_TO_IDM**	Q1 08 (AC 5.3)
8.	Audit Logs from IDM **SAPGRC_AC_IDM_AUDITTRAIL_FROM_IDM**	Q1 08 (AC 5.3)

3.0 Technical Definition

3.1 Request Submission to GRC

Description

The submit request web service is called by IDM to submit a request in GRC.

Input parameters

Field	Search	Optional
1. Request Type	yes	no
2. Priority (default HIGH)	yes	no
3. Applications	yes	no
4. { User Info } (Fetch other details from selected data source)	yes	no
a. User ID		
b. User Name (First Name and Last Name)		
c. Email		
d. Telephone Number		
e. Department		
f. Location		
g. Company		
h. Employee Type (NEW incase of NEW Request)		
i. Valid From Date		
j. Valid To Date		
5. {Requestor }	yes	yes
a. Requestor ID (default ADMIN)		
b. Requestor Email		
c. Requestor Name		
d. Telephone Number		
6. {Manager}	yes	
a. Manager Id (Fetch from Datasource System else set as ADMIN)		
b. Manager name (First Name and Last Name)		
c. Manager Email (Fetch from Datasource System else set as ADMIN Email)		
7. Request Reason		yes
9. {Roles}	yes	yes
a. System ID		
b. Role ID		
c. Action		
d. Company		
e. Valid From		
f. Valid To		
10.. {Custom Fields }	yes	yes
a. Field Name	yes	
b. Value	yes	

**Note:

- Consider AE system configuration for form customization, when extracting values from the web service submission (get more info on this use case).validation to add the default values.
- Attachments are not supported.

Output parameters

Field
Request Number
Status

3.2 Select Applications

Description

Select Application service provided by GRC:

The list of applications to which the user can be provisioned via GRC is returned by calling the 'Select Application' web service.

Select Application service provided by IDM:

This service is called by GRC to get the list of applications configured within IDM.

The user can lookup based on the following two parameters.

- System Category: The systems are categorized into Production, Non-Production, QA etc. system.
- System Type: The type of application denotes whether the application is an SAP application, or any other system.

Select Applications (bi-directional)

The list of the applications resources configured within IDM is maintained in the GRC itself.

The administrator needs to configure the application(s) to which the user can be provisioned before submitting the request.

Input parameters

Field	**Search**	**Optional**
1. System Type	no	yes
2. Application Type	no	yes
3. Locale	no	yes

Output parameters

Field
List
System Id
System Description
System Category

3.3 Risk Analysis

Description

The user can use this service to perform the SoD (Segregation of Duty) Analysis.

For the selected roles, the user can check if assigning them would result in any possible risk in the system.

Input parameters

Field	**Search**	**Optional**
1. Locale		yes
2. Request Id (optional when searching by user id and system)		no
3. User Id		yes
4. System		no

Output parameters

Field
TCodeDetails
Role Description
System
Tcode Description
Tcode ID
Risk Details

Org Rule Details
Risk
Risk Description
Risk Level
System
Tcodes
Violation Count
Risk Analysis Results
Critical Tcode

Note: the default configuration options configured within AE will be considered for Risk Analysis.

3.4 Search Role

Description

The user retrieves the list of roles in the selected application, by calling this web service.

Role filter feature is provided to narrow down the search. The various filter parameters supported are as follows.

- Application: Enter the application that has the given role information.
- Access Type: Select the criteria by which the role is to be searched.
  - Roles: This option enables to search by Role Name/ Description.
  - Transaction: With this option, roles can be searched by Transaction Code (Transaction Code: Enter the exact transaction code of the searched role).
  - Create Account Like: This enables the user to create a role or account that is similar to an existing account.
    - User ID: When the 'Access Type' selected is 'Create Account Like', the user id of a user is entered to which the authorization of the new account should resemble.
- Business Process: Enter the business process for the searched role.
- Sub Process: Enter the sub process for the searched role.
- Role Name: Enter the role name of the searched role.
- Role Description: Enter the description of the searched role.
- Functional Area: enter the functional area of the searched role.
- Company: Enter the company to which the searched role belongs.

Input Parameters

Field	Search	Optional
1. Application	yes	no
2. Access Type [Role, Transaction, 'Create Account Like']	no	no
3. Business Process	yes	yes
4. Sub Process (sub process for the selected Business Process)	yes	yes
5. Role/Profile Name		yes
6. Role/Profile description		yes
7. Functional Area	yes	yes
8. Company	yes	yes
9. Transaction Code (*Applicable for 'Transaction' only)		yes
10. { User Info } (*Applicable for 'Create Account Like' only)	yes	yes
a. User ID		
b. User Name (First Name and Last Name)		
11.Locale		yes
12. Hit Count (default100)	no	yes

Output Parameters

Field
List
Application
Role Name
Role Type
Role Description
Valid From
Valid To
Lead Owner

Role Details

Description

The detail description of the selected role can be viewed by calling 'Role Details' web service.

Input Parameters

Field	Search	Optional
1. Role/Profile Name	*yes*	yes
2. System		
3. Locale		

Output Parameters

Field
Role Name
Role Type
Role Description
Detail Description
Business Process
Sub Process
Critical level
Reaffirm Period
Last reaffirm Date
List
System
List
Role Approver
Alternate Approver
List
Functional Area
List

Company
List
Functional Area and Company Approver
List
Transaction Code

3.5 Audit Trail

Description

Audit Logs service provided by GRC:

This service provides the request approval history at anytime. It returns the request details such as, when the request was created, who submitted the request, which approvers approved the request. All the provisioning service activity performed within GRC is logged in the audit trail.

Audit Logs service provided by IDM:

This service returns the provisioning actions performed within IDM.

Note: The current integration will provide a separate section within GRC Audit Logs to display the audit history provided by IDM for non-ERP application provisioning.

Input parameters

Field	Search	Optional
1. Request Id		yes
2. { User Info } (Fetch other details from selected Application)	yes	yes
a. User ID		
b. User Name (First Name and Last Name)		
3. From Date		yes
4. To Date		yes
5. Action		yes
6. Locale		yes

Output parameters

Field
Priority
Status
Create Date
Request Id
Submitted By
Requested By
Request History{List}
Request History entity{ List}
Path
Stage
Id
Description
Display String
User Id
Request Id
Action Date
Action Value
{Action Definition}
Name
Message Code
Dependent Id
Provisioned user Id

3.6 Request Status

Description

Request Status service provided by GRC:

This service enables the user to check the status of a request processed within GRC, along with the request details.

Request Status service provided by IDM:

This service returns the status of the request within IDM.

** Request Id, User first name, User last name, Created On –to, Status, Locale

Input parameters

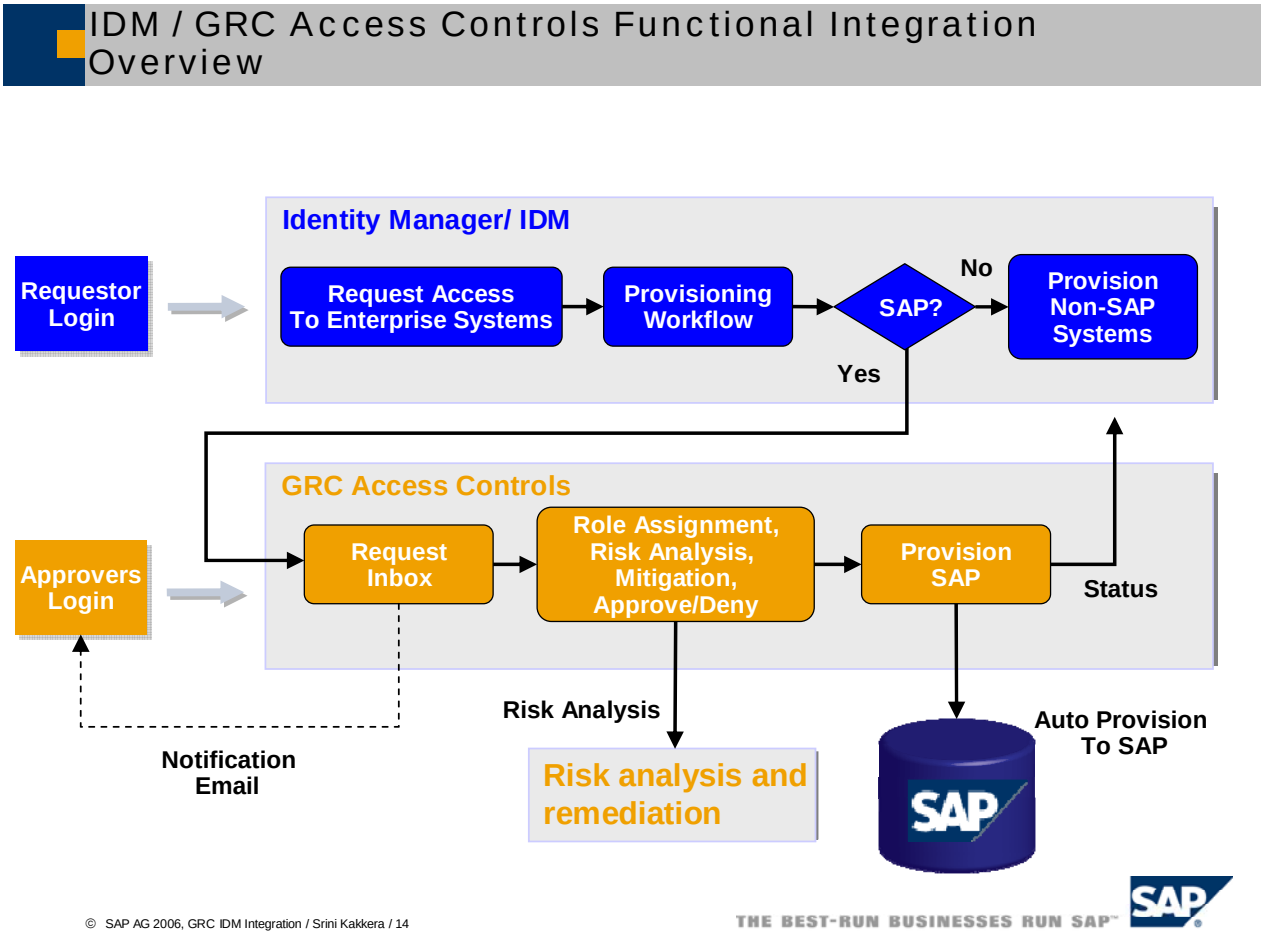
Field	Search	Optional
Request Id		yes
Locale		yes

Output parameters

Field
Request Status
Request Id
Status
Approval Due Date
User Name
Stage

Related Content

See the following image which illustrates the simple use case reference on the provisioning scenario between Identity Management and Access Controls.



For more information on GRC product related topics and articles, please access it from Reference 1

For attending the training class or looking for RKT material, you can access Reference 2

Copyright