Access Control

Identity Management (IdM)
Implementation Assistance Guide

Janet Tran, Customer Advisory Office
Swetta Singh, Technology
Ankur Baishya, Regional Implementation Group

June 2009
Version 1.0

SAP BusinessObjects

THE BEST-RUN BUSINESSES RUN SAP™

SAP®

Content

Access Control and IdM Integration
Implementation Considerations

- Request submission source
  - From where will the provisioning request be initiated (AC and/or IdM)?
- Provisioning roles
  - Role source: Where will the roles for provisioning be maintained (AC and/or IdM)?
  - The preferred approach is to have one role source for SAP roles.
- Approval workflow
  - Do you want to use approval workflow within AC and/or IdM?
  - Need to consider user notifications from AC and/or IdM.
- Risk analysis
  - The risk analysis web service does not support risk simulation. Risk simulation can only be performed directly in AC.
  - When provisioning new users, the request has to be submitted to AC for risk analysis. IdM can retrieve the result by polling the risk analysis web service with Request ID.
  - When provisioning existing users, risk analysis can be called by IdM.
- Request status and audit trails
  - Consider requirements for request status and audit trails while defining the integration solution. (Web services can only pass certain fields while more details may be viewed natively in AC or IdM.)
- Existing functionality and change control
  - IdM change control policy and it's impact on solution and implementation: Are changes to the current IdM process realistic?

Access Control and IdM Integration
Supported Use Cases

Use Case 1: Single provisioning request workflow in AC

Primarily for customers who would like to have one single workflow for provisioning requests in AC. This solution would result in maintaining non-SAP applications and roles in both IdM and AC.

- End users interface with IdM only.
- Approvers interface with AC for the approval workflow process for both SAP and non-SAP applications.
- SAP and non-SAP applications and roles are maintained in AC.
- Non-SAP applications and roles are also maintained in IdM.
- Provisioning is completed by AC for SAP applications and by IdM (with SPML 1.0 compliant web services) for non-SAP applications.

Use case 2: Separate approval workflows for provisioning to SAP and non-SAP Applications

Primarily for customers who have existing IdM processes and would introduce AC for compliant provisioning to SAP applications. This solution would result in two separate approval workflows (IdM for non-SAP and AC for SAP).

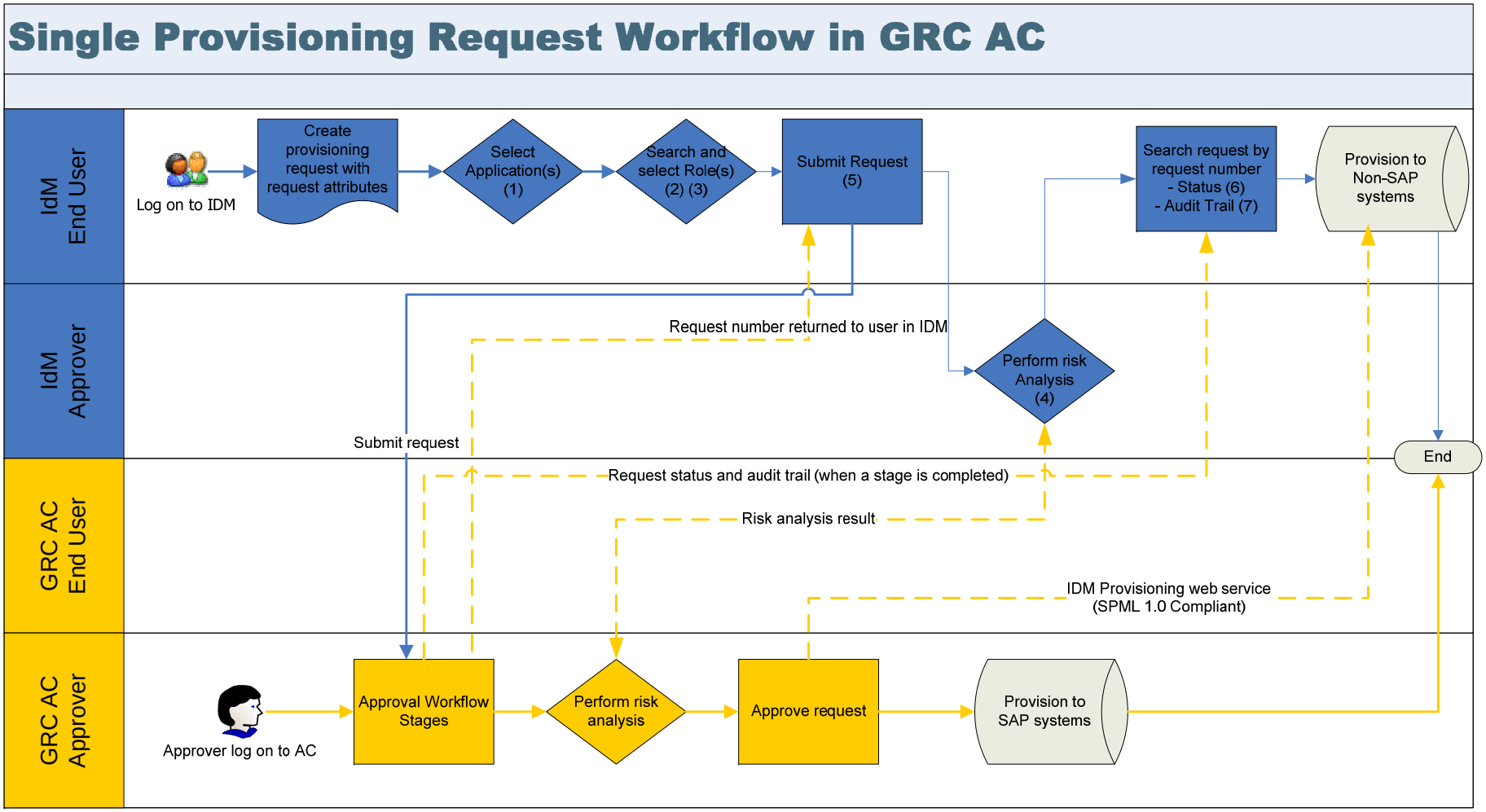
- End users interface with IdM only.
- Approvers interface with AC for the approval workflow process for SAP applications.
- Approvers interface with IdM for the approval workflow process for non-SAP applications.
- SAP applications and roles are maintained in AC
- Non-SAP applications and roles are maintained in IdM.
- Provisioning is completed by AC for SAP applications and completed directly from IdM for non-SAP applications.

Use case 3: Leveraging IdM for Provisioning to non-SAP Applications only

Primarily for customers who wants to use AC as the main interface for both end users and approvers and ONLY leverage IdM web service integration to provision to non-SAP applications from AC. This solution would result in maintaining non-SAP applications and roles in both IdM and AC.

- End users and approvers interface with AC only.
- SAP and non-SAP applications and roles are maintained in AC.
- Non-SAP applications and roles are also maintained in IdM.
- Provisioning is completed by AC for SAP applications and by IdM (with SPML 1.0 compliant web services) for non-SAP applications.

Use Case 1: Single Provisioning Request
High Level Illustration



Web Services Utilized:
(1) SAPGRC_AC_IDM_SELECTAPPLICATION
(2) SAPGRC_AC_IDM_SEARCHROLES
(3) SAPGRC_AC_IDM_ROLEDETAILS
(4) SAPGRC_AC_IDM_RISKANALYSIS (No simulation)
(5) SAPGRC_AC_IDM_SUBMITREQUEST
(6) SAPGRC_AC_IDM_REQUESTSTATUS
(7) SAPGRC_AC_IDM_AUDITTRAIL

Use Case 1: Single Provisioning Request Workflow in AC

End user creates and submits request with application(s) and role(s) selected from IdM. Request submitted to AC approval workflow and provisioned from AC to SAP and/or non-SAP applications.

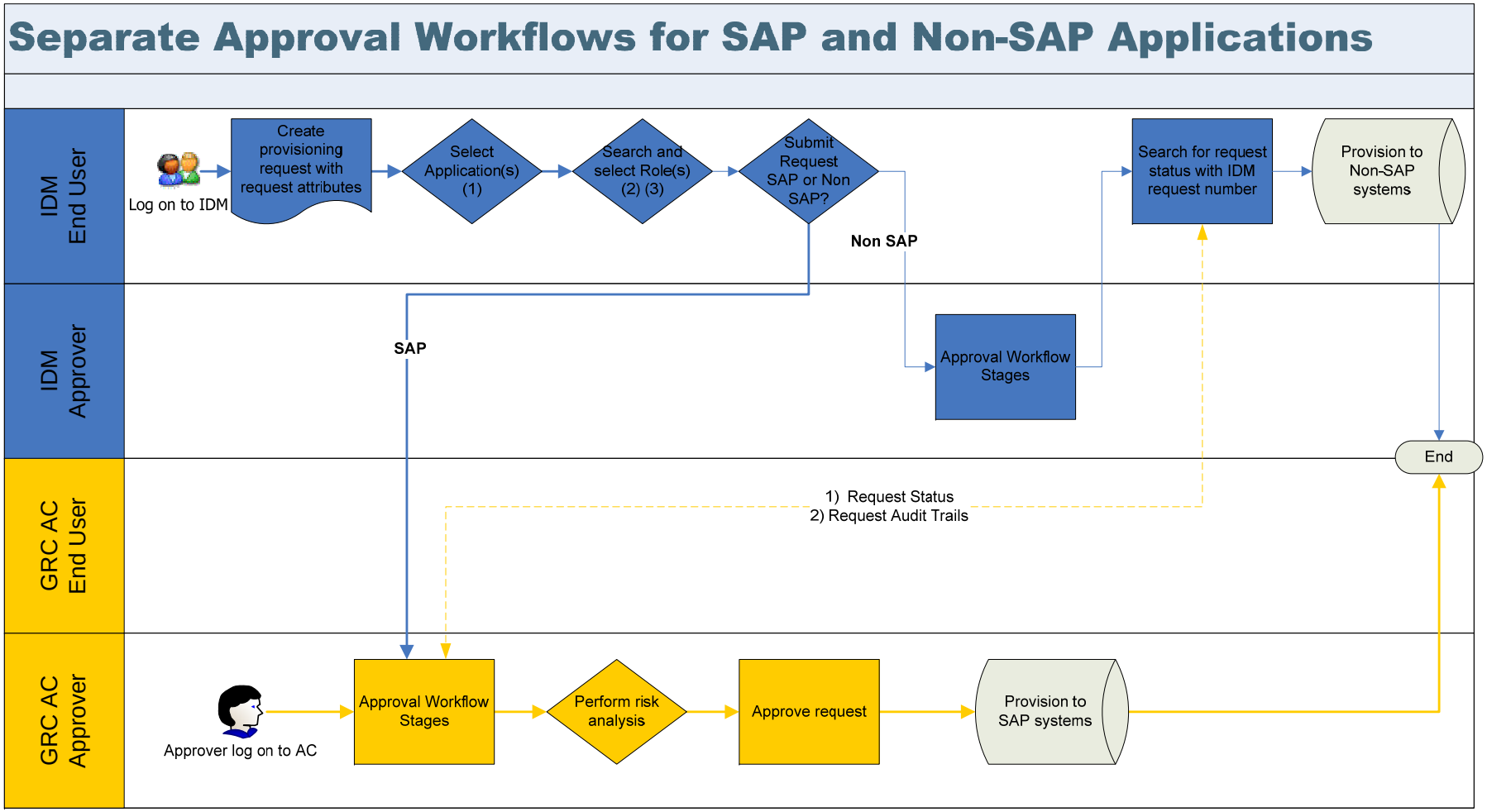
1) IdM – End user logs into IdM.
2) IdM – End user creates request.
3) IdM – End user selects application(s). (IdM calls the SAPGRC_AC_IDM_SELECTAPPLICATION web service.)
4) IdM – End user selects role(s) and view role details. (IdM calls the SAPGRC_AC_IDM_SEARCHROLES and SAPGRC_AC_IDM_ROLEDETAILS web services.)
   - If role mapping functionality is configured in CUP, the web service will present all roles (main and dependent roles) if search criteria are met.
   - If role default functionality is configured in CUP, the request attributes submitted from the web service will determine the default roles based on configured standard default role functionality for CUP.
5) IdM – End user submits request (IdM calls the SAPGRC_AC_IDM_SUBMITREQUEST web service.)
6) IdM – User receives system confirmation message “Request # submitted successfully”
7) AC – Request submitted into workflow approval stages.
8) IdM – End user performs risk analysis and risk analysis result is returned from AC – Optional step (IdM calls the SAPGRC_AC_IDM_RISKANALYSIS web service.)
9) AC – Approvers log into AC to run risk analysis (if required) and approve request.
10) AC – If approved, roles are provisioned to end user from AC to ERP for SAP. (For non-SAP applications with SPML 1.0 compliant provisioning web service, auto provisioning can be done by calling the IdM provisioning web service from AC.)
11) IdM – End user searches for his/her request in IdM to view status. (IdM calls the SAPGRC_AC_IDM_REQUESTSTATUS web service. This service can be called immediately per request or by batch to update request status for IdM requests.)
12) IdM – End user searches for request audit trail in IdM (IdM calls the SAPGRC_AC_IDM_AUDITTRAIL web service.)

Use Case 2: Separate Approval Workflows for Provisioning to SAP and non-SAP Applications

End user creates and submits request with SAP and non-SAP application(s) and role(s) selected from IdM. Request for SAP applications is submitted to AC approval workflow and provisioned from AC. Request for non-SAP applications is submitted to IdM approval workflow and provisioned directly from IdM.

1) IdM – End user logs into IdM.
2) IdM – End user creates user provisioning request for SAP and/or non-SAP applications.
3) IdM – End user selects application(s).
   - For SAP applications, IdM calls the SAPGRC_AC_IDM_SELECTAPPLICATION web service.
   - For non-SAP applications, end user selects applications maintained natively in IdM.
4) IdM – End user selects role(s) and views role details.
   - For SAP applications – IdM calls the SAPGRC_AC_IDM_SEARCHROLES and SAPGRC_AC_IDM_ROLEDETAILS web services.
     - If role mapping functionality is configured in CUP, the web service will present all roles (main & dependents) if search criteria are met.
     - If role default functionality is configured in CUP, the request attributes submitted from the web service will determine the default roles based on configured standard default role functionality for CUP.
   - For non-SAP applications, end user selects roles maintained natively in from IdM.
5) IdM – End user submits request. (IdM must be configured to route SAP applications to AC web service and non-SAP applications to IdM approval workflow).
   - For SAP applications, IdM calls the SAPGRC_AC_IDM_SUBMITREQUEST web service.
   - For non-SAP applications, IdM will route the request directly to IdM workflow.
6) IdM – End user receives system confirmation message from IdM “Request # submitted successfully”.
7) AC – Request for SAP applications submitted into workflow approval stages. (AC returns Request Number to IdM for internal system reconciliation.)
8) AC – Approver logs into AC to run risk analysis (if required) and approves request.
9) AC – Once approved, roles are provisioned to end user from AC to ERP for SAP. (AC returns Request Status and Audit Trail to IdM for internal system reconciliation.)
10) IdM – End user searches for request in IdM to view status. (IdM calls the SAPGRC_AC_IDM_REQUESTSTATUS web service. This service can be called immediately per request or by batch to update request status for requests in IdM).
11) IdM – End user searches for request audit trail in IdM. (IdM calls the SAPGRC_AC_IDM_AUDITTRAIL web service.)

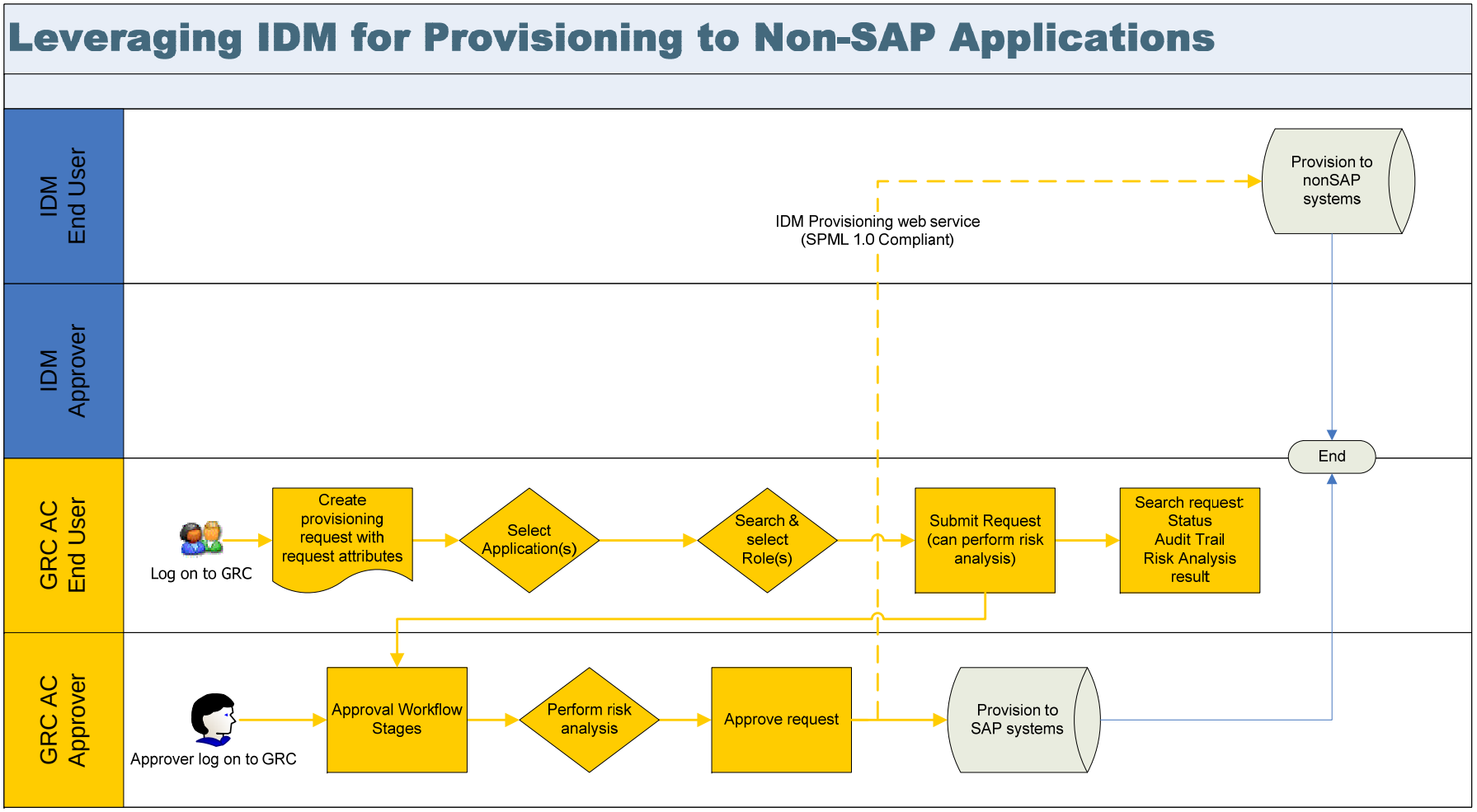
Use Case 2: Separate Approval Workflows
High Level Illustration



Web Services:
(1) SAPGRC_AC_IDM_SELECTAPPLICATION
(2) SAPGRC_AC_IDM_SEARCHROLES
(3) SAPGRC_AC_IDM_ROLEDETAILS
(4) SAPGRC_AC_IDM_RISKANALYSIS (No simulation)
(5) SAPGRC_AC_IDM_SUBMITREQUEST
(6) SAPGRC_AC_IDM_REQUESTSTATUS
(7) SAPGRC_AC_IDM_AUDITTRAIL

Note:
1) GRC AC returns Request Number to IDM for internal system reconciliation. Utilizes web services (5).
2) GRC AC returns Request Status and Audit Trail to IDM for internal system reconciliation. Utilizes web services (6) and (7).

Use Case 3: Leveraging IdM for non-SAP Apps
High Level Illustration



Use Case 3: Leveraging IdM for Provisioning to non-SAP Applications

End user creates and submits request with SAP and non-SAP application(s) and role(s) selected from AC. Request goes through approval workflow and is provisioned from AC to SAP and/or non-SAP applications.

1) AC – End user logs into AC.
2) AC – End user creates request.
3) AC – End user selects SAP and/or non-SAP application(s).
4) AC – End user selects role(s) and views role details.
5) AC – End user submits request.
6) AC – User receives system confirmation message “Request # submitted successfully”.
7) AC – Request is submitted into workflow approval stages.
8) AC – Approver logs into AC to run risk analysis (if required) and approves request.
9) AC – If approved, roles are provisioned to end users as follow:
   - For SAP applications, provisioning is completed directly from AC.
   - For non-SAP applications, the request is sent to IdM (with SPML 1.0 compliant web service) via web service and provisioning is completed by the IdM system.

Timeline for Web Service Availability

Web services available as of:

- SAP BusinessObjects Access Control 5.2 SP04+
  1. Select Application
  2. Submit Request to AC
  3. Risk Analysis
  4. Audit Logs
- SAP BusinessObjects Access Control 5.3
  5. Search Roles
  6. Role Details
  7. Submit Request to IdM
  8. Request Status
  9. Audit Log from IdM

Inbound (from IdM to AC) Web Services

1. Select Application **SAPGRC_AC_IDM_SELECTAPPLICATION**

   This Web service returns a list of resources that are configured within Access Control.

2. Search Roles **SAPGRC_AC_IDM_SEARCHROLES**

   This Web service enables you to search for roles before submitting a request to Access Control. To refine your search, you can use a filtration function.

3. Role Details **SAPGRC_AC_IDM_ROLEDETAILS**

   This Web service provides detailed information about the selected role.

4. Submit Request **SAPGRC_AC_IDM_SUBMITREQUEST**

   You call this Web service from the IdM system for compliant provisioning by Access Control

5. Risk Analysis **SAPGRC_AC_IDM_RISKANALYSIS**

   This Web service enables you to perform risk analysis. It returns any possible risk violations.

6. Audit Trail (includes the Provisioning Log Web service) **SAPGRC_AC_IDM_AUDITTRAIL**

   This Web service returns a comprehensive audit history. It enables IdM to retrieve an audit log from Access Control (for ERP provisioning) as well as provide an audit history of user provisioning to Access Control.

7. Request Status **SAPGRC_AC_IDM_REQUESTSTATUS**

   This Web service returns the status and detailed request information for the selected request.

Outbound (from AC to IdM) Web services

1. Submit Request (to IdM) **SAPGRC_AC_IDM_SUBMITREQUEST_TO_IDM**

   This Web service enables you to submit a request to IdM for non-ERP provisioning as well as when user information is new or changed in an HR system and privileges need adjusting.

2. Audit Trail (includes the Provisioning Log Web service) **SAPGRC_AC_IDM_AUDITTRAIL_FROM_IDM**

   This Web service returns a comprehensive audit history. It enables Access Control to retrieve the audit log from IdM (for non-ERP provisioning) as well as an audit history of user provisioning to IdM.

   Note: For more detailed information on AC / IdM web services, see the Access Control and Identity Manager Integration section of the Access Control 5.3 Configuration Guide.

IdM Integration
Supported Versions and Web Services

1.NetWeaver IDM

- Version: SAP NW IdM 7.0 SP02 and later is compatible with AC 5.3 SP02 and later
- Supported AC 5.3 Web Services: All available AC 5.3 IdM Web services in AC.
- The integration framework can be downloaded at https://www.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/b0196981-09d0-2b10-1b96-9b488d34a317
- The How-to-guide can be downloaded at https://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/b0da2dba-0480-2b10-a7ae-f055ab6e9355

2.IBM TIM

- Version
  - 4.6 Adapter available for TIM 4.6 and TIM 5.0 – supports AC 5.1 and 5.2
  - 5.0.2 Integration framework for TIM 4.6 and 5.0 – supports AC 5.3 SP06 and later

    Limitation: If the 4.6 adapter is used with the TIM 5.0 version, all new features in TIM 5.0 will not be available.
- Supported AC Web services:
  - Both TIM 4.6 and TIM 5.0 support the following Web services in AC:
    - Select Application (**SAPGRC_AC_IDM_SELECTAPPLICATION**)
    - Submit Request (**SAPGRC_AC_IDM_SUBMITREQUEST**)
- Where to download the integration framework to integrate with AC:
  - For the ITIM adapter information and download, please contact your IBM TIM account representative.

IdM Integration
Supported Versions and Web Services

3. SUN IDM

- Version
  - Virsa adapter available for SUN IDM 7.x and 8.x – supports AC 5.1 and 5.2
  - SUN IdM Integration framework available for IdM 8.1 – supports AC 5.3.
- Supported AC Web services – All available IdM web services in AC.
- Where to download the integration framework to integrate with AC:
  - The integration framework package for IdM 7.x and 8.x are only available by a direct Sun IdM-BU request.

4. Novell IDM

- Version
  - Novell Compliance Management Platform 1.0's Identity Management 3 driver supports AC 5.3.
- Supported AC Web services:
  - Novell Identity Management 3 driver supports the following Web services from AC:
    - Select Application (**SAPGRC_AC_IDM_SELECTAPPLICATION**)
    - Submit Request (**SAPGRC_AC_IDM_SUBMITREQUEST**)
    - Request Status (**SAPGRC_AC_IDM_REQUESTSTATUS)**
    - Audit Trail **(SAPGRC_AC_IDM_AUDITTRAIL)**
    - Search Roles **(SAPGRC_AC_IDM_SEARCHROLES)**
    - Role Details **(SAPGRC_AC_IDM_ROLEDETAILS)**
    - Risk Analysis **(SAPGRC_AC_IDM_RISKANALYSIS)**
- Where to download the driver to integrate with AC:
  - For the Novell Identity Management 3 driver information and download, please contact your Novell account representative.

Installation and Configuration

IdM

1. SAP Netweaver IdM
   - https://www.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/b0196981-09d0-2b10-1b96-9b488d34a317 and https://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/b0da2dba-0480-2b10-a7ae-f055ab6e9355
2. IBM, SUN, Novell – IdM Adapter/Driver Installation
   - Installation guide for adapter/driver provided by individual IdM vendor.

GRC Access Control 5.3

1. IdM connector configuration
   - Sample IdM connector field mapping screens provided in the following slides.
2. Link to AC 5.3 Configuration Guide:
   - http://help.sap.com → Click on SAP Business User on left hand panel → GRC Solutions → SAP GRC Access Control → Open → Master, Installation, Upgrade, Operations, and Configuration Guides

You will need proper authorization to access these Documents from the Service Marketplace.*

GRC Access Control 5.3
Configuration for NW IdM Connector

Connectors

IDM

Name*	MV_IDM_CONN
Short Description*	MV_IDM_CONN
Description	MV_IDM_CONN
Web Services URI*	http://nwdemo2450.wdf.sap.corp:50000/nwids/
User ID*	superuser
Password*	••••••••••••••••••••
System Language	
Connector Category	Production

Note: PROV_CALL = async; for asynchronous requests and = sync; for synchronous requests.

Parameter Name	Parameter Value
APPROVER_ID	requestuserid
ASSIGN_ROLES:OC	MX_PERSON
AUDIT_SEARCH_ATTRIBUTE	requestid
AUDIT_SEARCH_OPERATION	operation=auditlog
AUDIT_TYPE	auditlogs
CHANGE_USER:OC	MX_PERSON
CREATE_USER:OC	MX_PERSON
DATE	timestamp
DELETE_USER:OC	MX_PERSON
LOCK_USER:OC	MX_PERSON
LOCK_USER:islocked	true
OPERATION	requestoperation
PROV_CALL	async
REQUESTED_BY	requestuserid
REQUEST_ID	requestid
REQUEST_STATUS	operationstatus
ROLE	privilege
SCHEMA_ID	default
SEARCH_CRITERIA	searchBase
UNLOCK_USER:OC	MX_PERSON
UNLOCK_USER:islocked	false
USER_ID	requestuserid

NetWeaver IDM Connector
Parameter Names and Values

Parameter Name (AC Parameter)	Parameter Value (NW IDM Parameter)
APPROVER_ID	requesteduserid
ASSIGN_ROLES:OC	MX_PERSON
AUDIT_SEARCH_ATTRIBUTE	requestid
AUDIT_SEARCH_OPERATION	operation=auditlog
AUDIT_TYPE	auditlogs
CHANGE_USER:OC	MX_PERSON
CREATE_USER:OC	MX_PERSON
DATE	timestamp
DELETE_USER:OC	MX_PERSON
LOCK_USER:OC	MX_PERSON
LOCK_USER:islocked	TRUE
OPERATION	requestoperation
PROV_CALL	sync
REQUESTED_BY	requestuserid
REQUEST_ID	requestid
REQUEST_STATUS	operationstatus
ROLE	privilege
SCHEMA_ID	default
SEARCH_CRITERIA	searchBase
UNLOCK_USER:OC	MX_PERSON
UNLOCK_USER:islocked	FALSE
USER_ID	requestuserid

Field Mappings for NW IdM

AC Field	Application Field
Email Address - STANDARD	mail
User FName - STANDARD	sn
User ID - STANDARD	requestuserid
User LName - STANDARD	givenname

GRC Access Control 5.3
Configuration for SUN IdM Connector

Connectors

IDM

Name*	SUN_LDAP
Short Description*	SUN_LDAP
Description	SUN_LDAP
Web Services URI*	http://10.48.122.157:8080/idm/servlet/rpcrouter2
User ID*	configurator
Password*	••••••••••••••••••••
System Language	
Connector Category	Production

Note: PROV_CALL = async; for asynchronous requests and = sync; for synchronous requests.

Parameter Name	Parameter Value
ASSIGN_ROLES:OC	BasicUser
AUDIT_TYPE	statusrequest
CHANGE_USER:OC	BasicUser
CREATE_USER:OC	BasicUser
CREATE_USER:options.AllowPasswordGenerat	true
CREATE_USER:options.onlyResourcesUserPass	true
CREATE_USER:resources	LDAP
DELETE_USER:OC	BasicUser
LOCK_USER:EXT	disableUser
PROV_CALL	async
RESET_PASSWORD:EXT	resetUserPassword
RESET_PASSWORD:accounts	LDAP
ROLE	roles
SCHEMA_ID	standard
SEARCH_CRITERIA	identifier
SEARCH_PASSWORD:EXT	launchProcess
SEARCH_PASSWORD:process	SPML Decrypt Password
UNLOCK_USER:EXT	enableUser

SUN IdM Connector
Parameter Names and Values

Parameter Name (AC Parameter)	Parameter Value (SUN IDM Parameter)
ASSIGN_ROLES:OC	BasicUser
AUDIT_TYPE	statusrequest
CHANGE_USER:OC	BasicUser
CREATE_USER:OC	BasicUser
CREATE_USER:options.AllowPasswordGeneration	true
CREATE_USER:options.onlyResourcesUserPasswordRequired	true
CREATE_USER:resources	<Application name>
DELETE_USER:OC	BasicUser
LOCK_USER:Ext	disableUser
PROV_CALL	sync
RESET_PASSWORD:EXT	resetUserPassword
RESET_PASSWORD:accounts	<Application name>
ROLE	roles
SCHEMA_ID	standard
SEARCH_CRITERIA	identifier
SEARCH_PASSWORD:EXT	launchProcess
SEARCH_PROCESS:process	SPML Decrypt Password
UNLOCK_USER:EXT	enableUser

Field Mappings for SUN IdM

AC Field	Application Field
Email Address - STANDARD	email
User FName - STANDARD	firstname
User ID - STANDARD	accountId
User LName - STANDARD	lastname

Production Support
AC and IdM Support

Depending on system error logs, the following areas are supported.

1. Supported by SAP BusinessObjects AC
   - AC IdM Web Services
   - AC standard configuration
   - AC workflow configuration
   - AC IdM connector configuration

2. Supported by IdM vendor
   - Adapter installation & configuration
   - IdM standard configuration
   - IdM workflow configuration
   - IdM provisioning web service
   - IdM connector configuration

Production Support
Issue Reporting and Resolution

If an issue is found specifically with:

- SUN IdM → Contact SUN Support.
- Tivoli IdM → Contact IBM Support.
- Novell IdM → Contact Novell Support.
- NW IdM → Log a CSS Message with component BC-IDM in the SAP Support Portal. Include all relevant documentation for replication of the issue.
- AC Web Services → Log a CSS Message with component GRC-SAC-SAE in the SAP Support Portal. Include all relevant documentation for replication of the issue.

Documentation Feedback

Your feedback is very valuable and will enable us to improve our documents. Please take a few moments to complete our feedback form. Any information you submit will be kept secure and confidential.

You can access the feedback form at:
http://www.surveymonkey.com/s.aspx?sm=stdoYUlaABrbKUBpE95Y9g_3d_3d

Copyright 2009 SAP AG
All Rights Reserved

SAP BusinessObjects