IBM Security Identity Manager
Version 6.0

Integration for SAP Governance, Risk and Compliance Access Control Installation and Configuration Guide

SC27-4414-00

IBM Security Identity Manager
Version 6.0

Integration for SAP Governance, Risk and Compliance Access Control Installation and Configuration Guide

SC27-4414-00

Note
Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 63.

Edition notice

Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.

Preface

About this book

This installation guide provides the basic information that you need to install and configure the IBM® Security Identity Manager Integration for SAP Governance, Risk and Compliance Access Control. SAP Governance, Risk and Compliance Access Control is also called SAP GRC Access Control.

IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

This integration enables compliant user provisioning and risk analysis between IBM Security Identity Manager and the SAP NetWeaver Application Server ABAP by using SAP GRC Access Control.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Identity Manager library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation see the IBM Security Identity Manager Information Center.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm site displays the information center welcome page for this product.

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix A, "Support information," on page 57 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Contents

Figures

Tables

Chapter 1. Integration for SAP GRC Access Control Installation and Configuration Guide

This installation guide provides the basic information that you need to install and configure the IBM Security Identity Manager Integration for SAP GRC Access Control. The Integration for SAP GRC Access Control enables connectivity between the IBM Security Identity Manager server and SAP GRC Access Control.

Overview of the integration

The Integration for SAP GRC Access Control extends the IBM Security Identity Manager SAP NetWeaver Adapter.

In addition to the provisioning capabilities of the SAP NetWeaver Adapter, this integration sends access requests to SAP GRC Access Control for Separation of Duties (SoD) checks. The SAP GRC Access Control result allows a decision to be made on whether to provision the account. The provisioning step can be performed by either the SAP NetWeaver Adapter or by SAP GRC Access Control. The integration contains components that enable IBM Security Identity Manager to integrate with SAP GRC Access Control 5.3, 10.0, or both.

This integration can also invoke the SAP GRC Access Control Risk Analysis web service on role assignments during an access request. It also enables rejected accounts and role assignments to be removed from the access request that was sent to the SAP NetWeaver Adapter.

Architecture of the integration

The integration uses two profiles. The first profile contains SAP NetWeaver Adapter account and service attributes only. This profile does not enable a connection with SAP GRC Access Control. The second profile contains an extended set of account and service attributes necessary to enable interaction between SAP GRC Access Control (version 5.3 or 10.0) and SAP NetWeaver.

This interaction enables IBM Security Identity Manager to coordinate the account compliance checking process in SAP GRC Access Control with the SAP NetWeaver account provisioning process. This profile effectively enables a single account provisioning request to perform two tasks:

1. Submission of an access request to SAP GRC Access Control from IBM Security Identity Manager.
2. Submission of an account provisioning request to SAP NetWeaver from IBM Security Identity Manager, depending whether an approval or rejection is granted for the IBM Security Identity Manager request.

The relationships between components of the adapter are shown in Figure 1 on page 2.

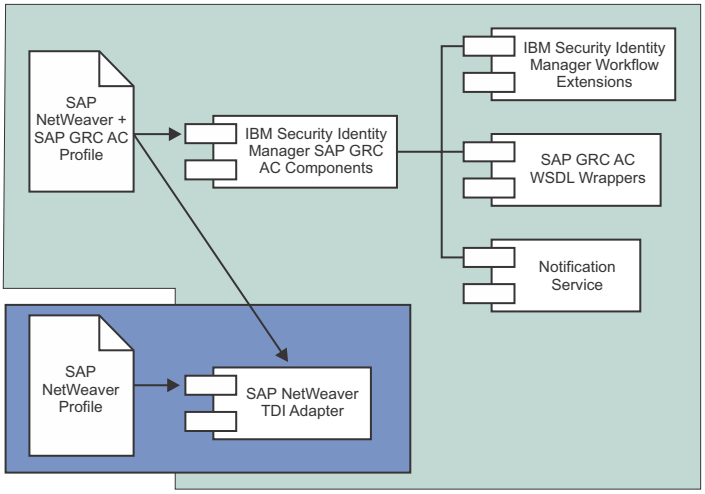


Figure 1. IBM Security Identity Manager SAP NetWeaver Adapter with Integration for SAP GRC Access Control components and relationships

A high level of control is obtained over the provisioning process by configuring IBM Security Identity Manager workflow extensions for SAP GRC Access Control. The IBM Security Identity Manager workflow extensions allow *Add*, *Modify*, *Suspend*, *Restore*, and *Delete* requests to be sent to SAP GRC Access Control. SoD compliance checks are then performed in SAP GRC Access Control before provisioning the account in SAP NetWeaver. The risk analysis and remediation features of SAP GRC Access Control Compliant Provisioning can be used to:

- Modify the request
- Submit an approval
- Submit a rejection
- Cancel the request

In IBM Security Identity Manager workflow, there are two possible modes to configure each type of request. These modes are referred to as **Non-blocking** mode and **Blocking** mode.

In **Non-blocking** mode, SAP GRC Access Control takes control of account provisioning on the target system. Following submission of an access request to SAP GRC Access Control, IBM Security Identity Manager workflow continues execution and does not wait for the result of the request in SAP GRC Access Control. This mode passes the responsibility of provisioning the account in SAP NetWeaver to SAP GRC Access Control.

In **Blocking** mode, IBM Security Identity Manager workflow blocks (or wait/pause) following submission of an access request to SAP GRC Access Control. The workflow continues to block until the result of the request is received from SAP GRC Access Control. A dedicated Notification Service deployed in WebSphere® is responsible for

- Periodically querying SAP GRC Access Control
- Relaying results of completed requests to IBM Security Identity Manager
- Unblocking the relevant IBM Security Identity Manager workflows.

The IBM Security Identity Manager workflow becomes the central point of coordination and auditing for account provisioning. IBM Security Identity Manager

determines whether an account is provisioned in SAP NetWeaver, depending on pre-conditions such as whether the request was approved or rejected in SAP GRC Access Control.

Supported configurations

The integration requires the interaction of several components.

The fundamental components of the integration are:

- An IBM Security Identity Manager Server
- An Tivoli Directory Integrator server
- An IBM Security Identity Manager SAP NetWeaver Adapter
- The Integration for SAP GRC Access Control 5.3 or 10.0

Chapter 2. Planning to install the integration

Installing and configuring the integration involves several steps that must be completed in the appropriate sequence.

Review the pre-installation and installation roadmaps before beginning the installation process.

Preinstallation roadmap

The environment must be prepared following these steps before the integration can be installed.

Table 1. Preinstallation roadmap

What to do	Where to find more information
Verify that the software and hardware requirements for the integration that you want to install have been met.	See "Prerequisites."
Collect the necessary information for the installation and configuration.	See "Installation worksheet for the integration" on page 6.
Obtain the installation software	Download the software from Passport Advantage®. See "Downloading the software" on page 7.

Installation roadmap

The necessary steps here must be completed to install the integration including completing post-installation configuration tasks and verifying the installation.

Table 2. Installation roadmap

What to do	Where to find more information
Install the integration.	See Chapter 3, "Installing the integration," on page 9.
Import the SAP NW GRC profile.	See "Importing the SAP NetWeaver GRC profile into the IBM Security Identity Manager Server" on page 9.
Create a service.	See "Creating an SAP NetWeaver GRC service" on page 9.
Verify the installation.	See "Verifying the SAP GRC AC Workflow components installation" on page 47.
Configure the SAP GRC workflow extensions for the integration.	See Chapter 4, "Installing and configuring SAP GRC Access Control workflow extensions," on page 19.

Prerequisites

Verify that all of the prerequisites are met before installing the Integration for SAP GRC Access Control.

Table 3 identifies hardware, software, and authorization prerequisites to install the Integration for SAP GRC Access Control.

Table 3. Prerequisites to install the integration

Prerequisite	Description
Operating System	The Integration for SAP GRC Access Control can be used on any operating system that is supported by IBM Security Identity Manager.
Network Connectivity	TCP/IP network
System Administrator Authority	The person who completes the Integration for SAP GRC Access Control installation procedure must have system administrator authority.
Tivoli Directory Integrator server	See the IBM Security Identity Manager SAP NetWever adapter release notes for the supported versions.
IBM Security Identity Manager	Version 6.0
IBM Security Identity Manager Adapter (also known as the Dispatcher)	See the IBM Security Identity Manager SAP NetWever adapter release notes for the supported versions.
IBM Websphere Application Server*	WebSphere Application Server 7.0 FixPack 19 (7.0.0.19)
SAP NetWeaver AS ABAP with SAP Basis Component	See the IBM Security Identity Manager SAP NetWever adapter release notes for the supported versions.
SAP JCo	3.0.8
SAP GRC Access Control	5.3, 10.0 FP08

* The minimum WebSphere Application Server FixPacks listed are required to satisfy web service dependencies that the integration has in WebSphere.

Installation worksheet for the integration

The following table identifies the information you need to install the Integration for SAP GRC Access Control.

Table 4. Required information to install the integration

Required information	Description
Administrator account on the managed resource for SAP GRC Access Control 5.3	An administrator account on the managed resource that has the necessary administrative privileges for SAP GRC. The administrator account must have the following assigned role in UME: • AEADMIN
Administrator account on the managed resource for SAP GRC Access Control 10.0	An administrator account on the managed resource that has the necessary administrative privileges for SAP GRC 10.0. The administrator account must have at least the following assigned roles: • SAP_GRC_NWBC • SAP_GRAC_* See the GRC 10.0 Post-installation and Security guides for further information.

Table 4. Required information to install the integration (continued)

Required information	Description
SAP GRC 10.0 Web Service Endpoint creation	Endpoint bindings must be created in the transaction SOAMANAGER under Service Administration – Single Service Configuration - Configurations, for at least the following SAP GRC 10.0 web services: • GRAC_AUDIT_LOGS_WS • GRAC_LOOKUP_WS • GRAC_REQUEST_DETAILS_WS • GRAC_REQUEST_STATUS_WS • GRAC_RISK_ANALYSIS_WITH_NO_WS • GRAC_USER_ACCES_WS After the endpoint binding has been created, the "Calculated Access URL" for the web service is found under the "Transport Settings" tab. This URL is defined on the service form. The service form in the SAP GRC Access Control integration and `SAPNotify.props` make use of these URLs to locate the relevant SAP GRC Access Control 10.0 web service.

Downloading the software

Download the software from your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage.

See the *IBM Security Identity Manager Download Document* for instructions.

Chapter 3. Installing the integration

The following sections contain the information that you need to install and configure the Integration for SAP GRC Access Control.

Importing the SAP NetWeaver GRC profile into the IBM Security Identity Manager Server

An IBM Security Identity Manager integration profile defines the types of resources that the IBM Security Identity Manager Server can manage.

In this case, the profile `SapGRCNWProfile.jar` is used to create a SAP GRC Access Control service on the IBM Security Identity Manager server. The `SapGRCNWProfile.jar` profile must be imported into the IBM Security Identity Manager server.

Before importing the `SapGRCNWProfile.jar` profile, verify that the following conditions are met:

- The IBM Security Identity Manager Server is installed and running.
- You have root or Administrator authority on the IBM Security Identity Manager Server.

1. Log in to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. Import the integration profile by using the **import** feature for your IBM Security Identity Manager product. See the information center or the online help for specific instructions about importing the integration profile.
3. Restart the Dispatcher service.

If an error related to the schema is received when the integration profile is imported, go to the `trace.log` file for information about the error. The `trace.log` file location is specified by the `handler.file.fileDir` property defined in the IBM Security Identity Manager `enRoleLogging.properties` file. The `enRoleLogging.properties` file is installed in the *ITIM_HOME*`/data` directory.

Creating an SAP NetWeaver GRC service

You must define attributes on the SAP GRC SERVICE ATTRIBUTES TAB when you create an SAP NetWeaver GRC service.

If the `SapGRCNWProfile.jar` profile was imported, then an additional SAP GRC Service Attributes tab is displayed that contains the set of the following attributes.

Enable GRC Workflow Extensions
Optional attribute. Flag to indicate whether workflow extensions are configured for either SAP GRC Access Control 5.3 or 10.0. The value of this flag is only used by the "Check GRC Version" workflow extension. It has no effect otherwise.

GRC Version
Optional attribute. The version of SAP GRC Access Control the service is configured against. This attribute can be used in the workflow to determine the path to take if these conditions exist:

- A combination of different SAP GRC Access Control versions exists in the environment.
- The environment is supported by a single IBM Security Identity Manager server instance.

The value of this flag is only used by the "Check GRC Version" workflow extension. It has no effect otherwise.

GRC Admin Id
The SAP GRC Access Control user name with privileges to invoke SAP GRC web services and submit Access Control requests. A value is required if the authentication and security services are enabled on the SAP NetWeaver Application server on which Access Control is deployed.

GRC Password
Password of the SAP GRC Access Control Admin ID.

Access Control Request URL
The URL address of the Access Control Submit Request web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from IBM Security Identity Manager.

For example, the URL for SAP GRC 5.3 might be specified as `http://remotehost:port/SAPGRC_AC_IDM_SUBMITREQUEST/Config1?style=document`

The URL for SAP GRC 10.0 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_user_acces_ws/clientnumber/grac_user_acces_ws/binding?sap-client=clientnumber`

Access Control Look Up URL
The URL address of the Access Control Look Up Request web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from IBM Security Identity Manager.

For example, the URL for SAP GRC Access Control 10.0 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_lookup_ws/clientnumber/grac_lookup_ws/binding?sap-client=clientnumber`

Access Control Risk Analysis URL
The URL address of the Access Control Risk Analysis Request with Request ID web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from IBM Security Identity Manager.

For example, the URL for SAP GRC Access Control 10.0 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_risk_analysis_with_no_ws/clientnumber/grac_risk_analysis_with_no_ws/binding?sap-client=clientnumber`

Access Control Request Details URL
The attribute for Update Account Attribute Request. The URL address of the Access Control Request Details web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from IBM Security Identity Manager.

For example, the URL for SAP GRC Access Control 10.0 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_request_details_ws/clientnumber/grac_request_details_ws/binding?sap-client=clientnumber`

System Identifier
The system identifier is the SAP connector name defined in Access Control to enable provisioning directly to the target SAP ABAP server from SAP GRC Access Control. This system identifier is also supplied to SAP GRC Access Control on a request submission in the account role data.

Detail Logging
Optional attribute. Flag to enable SAP GRC request debugging trace output. For SAP GRC Access Control 5.3, this option writes a log file called `grcextension.log` to the location specified by the Java™ system property **`user.home`**. For SAP GRC Access Control 10.0, this option enables the IBM Security Identity Manager trace log file for the workflow extension component.

Note: The IBM Security Identity Manager logging level must be set to DEBUG_MIN.

Adapter attributes and object classes

After the GRC profile is installed, the integration supports a standard set of attributes that contains attributes from the NetWeaver adapter in addition to attributes required for SAP GRC Access Control.

The following table lists the standard attributes supported for SAP GRC Access Control, in addition to the SAP NetWeaver attributes that are listed in the *Adapter for SAP NetWeaver Installation and Configuration Guide*.

The following table shows the SAP GRC Access Control attributes used by requests sent to the SAP GRC Access Control 5.3 or 10.0. The set of attributes between SAP GRC Access Control versions is different as indicated in Table 3.

The list of SAP GRC Access Control service form attributes can be found in Table 5 on page 12.

Table 5. Supported SAP GRC AC service attributes

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for SAP GRC Access Control 5.3 Request	Required for SAP GRC Access Control 10.0 Request
Enable GRC Workflow Extensions	ersapgrcenabled	Optional attribute. Indicates whether SAP GRC Access Control workflow extensions have been configured	String	Yes	Yes
GRC Version	ersapgrcversion	Optional attribute. The version of SAP GRC Access Control the service has been configured against. Used when there is a combination of different version of SAP GRC Access Control needs to be supported in the a single server instance.	String	Yes	Yes
GRC Admin Id	ersapgrcsubmitrequestuid	User ID of the SAP GRC Access Control Administrator	String	Yes	Yes
GRC Password	ersapgrcabappwd	Password of the SAP GRC Access Control Administrator	String	Yes	Yes
System Identifier	ersapgrcsystemid	System identifier	String	Yes	Yes
Access Control Request URL	ersapgrcsubmitrequesturl	The URL address of the Access Control Submit Request Web service	String	Yes	Yes
Access Control Look Up URL	ersapgrclookupurl	The URL address of the Access Control Look Up Request web service	String	No	Yes

Table 5. Supported SAP GRC AC service attributes (continued)

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for SAP GRC Access Control 5.3 Request	Required for SAP GRC Access Control 10.0 Request
Access Control Risk Analysis URL	ersapgrcriskanalysisurl	The URL address of the Access Control Risk Analysis Request web service	String	No	Yes, If using Risk Analysis workflow extension
Access Control Request Detail URL	ersapgrcrequestdetailsurl	The URL address of the Request Detail web service	String	No	Yes, If using Update Account Attribute workflow extension
Detail Logging	ersapgrcdebug	Flag to enable GRC request debugging trace output	String	No	No

Note: a GRC request contains values of several attributes that are supplied from the SAP NetWeaver account form tabs such as Given name, Surname, Email address, and Role. The list of SAP GRC and NetWeaver account form attribute values that are forwarded onto a GRC request are found in Table 6.

Table 6. Supported SAP GRC/NetWeaver account attributes

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 Request
Priority	ersapgrcpriority	Request Priority. The value must match the identifier of a configured AC priority.	String	Yes	Yes
Location	ersapgrclocation	The work location of the user to be provisioned.	String	No	No
Employee Type	ersapgrcemployeetype	Type of employee. This attribute value must match configuration in AC.	String	No	No

Table 6. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 Request
Requestor ID	ersapgrcrequesteruid	User name of the requester.	String	Yes	If Requestor ID is not defined, SAP GRC Access Control 10.0 will default it to the SAP GRC Access Control Admin ID defined on the service form as the requestor.
Requestor First Name	ersapgrcrequesterfirstname	Given name of the requester.	String	Yes	No
Requestor Last Name	ersapgrcrequesterlastname	Surname of the requester.	String	Yes	No
Requestor Email	ersapgrcrequesteremail	The email address of the requester.	String	Yes	Yes
Requestor Telephone	ersapgrcrequestertelephone	Telephone number of the requester.	String	No	No
Manager ID	ersapgrcmanageruid	User name of the employees manager. This attribute value must match the user ID of a user in the AC authentication data source.	String	Yes	If Manager is configure as one of the approver in GRC 10.0, this attribute is required.
Manager First Name	ersapgrcmanagerfirstname	Given name of the employees manager.	String	No	No
Manager Last Name	ersapgrcmanagerlastname	Surname of the employees manager.	String	No	No
Manager Email	ersapgrcmanageremail	Email address of the employees manager.	String	No	No

Table 6. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 Request
Manager Telephone	ersapgrcmanagertelephone	Telephone number of the employees manager.	String	No	No
Locale	ersapgrclocale	Locale of the employee. For example, EN, DE, US.	String	No	No
Request Reason	ersapgrcrequestreason	The reason for the AC request.	String	Yes	Yes
Organization Unit	ersapgrcorgunit	Organization Unit	String	No	No
Business Process	ersapgrcbusprocess	Business Process. This attribute value must match the configuration in AC.	String	Yes	Yes
Functional Area	ersapgrcfunctionalarea	Functional Area	String	No	No
Personnel Area	ersapgrcpersonnelarea	Personnel Area	String	No	No
Employee Job	ersapgrcemployeejob	Job of Employee	String	No	No
Employee Position	ersapgrcemployeeposition	Position of Employee	String	No	No
Request Due Date	ersapgrcrequestduedate	Due Date of the request	Date	No	No
Request Item Comments	ersapgrcreqitemcomment	Comments on the request item	String	No	No
Custom Fields	ersapgrccustomfields	Custom fields that are configured in AC. This attribute is a multi-valued attribute that must be supplied in the format: "<custom field name>|<custom field value>" It must match a configured custom field in AC.	Key/Value Pair String	No	No
Given Name	ersapnwgivenname	Given name of the user.	String	Yes	Yes
Surname	ersapnwsurname	Surname of the user.	String	Yes	Yes

Table 6. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 Request
Email Address	ersapnwemailaddress	The value of the "primary email address" given in the Communication tab. For more information about the format for providing email addresses, see the email section under Special Attributes.	String	Yes	Yes
Company	ersapnwcompany	Represents the identifier of a company configured in AC. The value must match a “Company ID” configured in AC role attributes. This value is set as the value for company in both the AC request and all requested roles for the request.	String	No	No
Department	ersapnwdepartment	Represents the department of the user to be provisioned.	String	No	No
Function	ersapnwfunction	Represents the department of the user to be provisioned. The value must match a “Functional Area” configured in AC role attributes.	String	No	No

Table 6. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Identity Manager Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 Request
Role	ersapnwagrname	Multi-valued attribute that contains the proposed group of roles to be provisioned for the account. The request uses the values supplied for system ID, company, role name, start date, and end date in the role data. CUA client names are not used as the system ID in the role data.	Custom Data Type	Yes	Yes
CUA Systems	ersapnwcuasystem	Connector name for CUA clients.	String	No	Yes

There are constraints imposed by SAP GRC AC for a successful request submission, such as attribute values that match pre-configured values in SAP GRC AC. The attributes that have values that must match values in SAP GRC AC are listed in Table 7.

Table 7. Attributes with required data in SAP GRC AC 10.0

Attribute Name	Details
Role	All roles that exist on an SAP GRC AC request are inspected. Therefore all roles that exist in the target SAP NetWeaver system must also exist in SAP GRC AC 10.0.
CUA Systems	The value must match the connector name of a configured SAP Client.
Priority	The value must match the identifier of a configured AC priority. If the priority codes in SAP GRC AC are different from the supported defaults `006=HIGH, 007=LOW, 008=MEDIUM` then the **`ersapgrcpriority`** form element on the account form must be edited to match the configured priorities. To customize the adapter profile, see the *IBM Security Identity Manager SAP NetWeaver Adapter Installation and Configuration Guide*.
Employee Type	This attribute value must match configuration in AC.
System Identifier	The attribute value must match the name of a connector that is configured in SAP GRC AC 10.0.
Manager ID	This attribute value must match the user ID of a user in the AC authentication data source.
Function	The value must match a "Functional Area" configured in AC.
Business Process	This attribute value must match the business process configuration in AC.

Chapter 4. Installing and configuring SAP GRC Access Control workflow extensions

The following sections describe the steps to be performed to install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Identity Manager.

There are slightly different procedures to follow depending on which target system you want to support.

Support SAP GRC Access Control 5.3 only

1. "Installing SAP GRC Access Control 5.3 workflow extensions"
2. "Configuring SAP GRC Access Control 5.3 workflow extensions" on page 22
3. "Log file locations for workflow extensions" on page 38
4. "Installing and configuring the notification component for SAP GRC Access Control 5.3" on page 25

Support SAP GRC Access Control 10.0 only

1. "Installing SAP GRC Access Control 10.0 workflow extensions" on page 27
2. "Configuring SAP GRC Access Control 10.0 workflow extensions" on page 29
3. "Log file locations for workflow extensions" on page 38
4. "Installing and configuring the notification component for SAP GRC Access Control 10.0" on page 36

Support SAP NetWeaver, SAP GRC Access Control 5.3, and SAP GRC Access Control 10.0

1. "Installing SAP GRC Access Control 5.3 workflow extensions"
2. "Installing SAP GRC Access Control 10.0 workflow extensions" on page 27
3. "Log file locations for workflow extensions" on page 38
4. "Configuring workflow extensions to concurrently support SAP GRC Access Control 5.3, SAP GRC Access Control 10.0, and SAP NetWeaver" on page 39
5. "Installing and configuring the notification component for SAP GRC Access Control 5.3" on page 25
6. "Installing and configuring the notification component for SAP GRC Access Control 10.0" on page 36

Installing SAP GRC Access Control 5.3 workflow extensions

Follow these steps to install the workflow extensions.

1. Edit the `workflowextensions.xml` file under the `ITIM_HOME/data` directory to add a workflow extension. Add the following workflow extension:

   Note: This sample is provided as part of the installation package as `workflow\grc53\GRC53WorkflowExtensions.xml`. After modifications to

workflowextensions.xml are complete, open it with an Internet browser to make sure there are no XML syntax errors in the file.

```
<ACTIVITY ACTIVITYID="SAPGRCNonblockingAddRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="nonblockingSAPGRCAddRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRCBlockingAddRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="blockingSAPGRCAddRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRCNonblockingModifyRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="nonblockingSAPGRCModifyRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRCBlockingModifyRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="blockingSAPGRCModifyRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRCNonblockingDeleteRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="nonblockingSAPGRCDeleteRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRCBlockingDeleteRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
```

```
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="blockingSAPGRCDeleteRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRCNonblockingSuspendRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="nonblockingSAPGRCSuspendRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRCBlockingSuspendRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="blockingSAPGRCSuspendRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRCNonblockingRestoreRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="nonblockingSAPGRCRestoreRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRCBlockingRestoreRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc53.wfe.SapGRCApplicationExtension"
   METHOD_NAME="blockingSAPGRCRestoreRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
```

2. Copy `workflow\grc53\SAPGRC53Workflow.jar` from the installation package to the appropriate directory:

   ```
   WEBSPHERE_HOME\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME
   \ITIM.ear\app_web.war\WEB-INF\lib
   ```

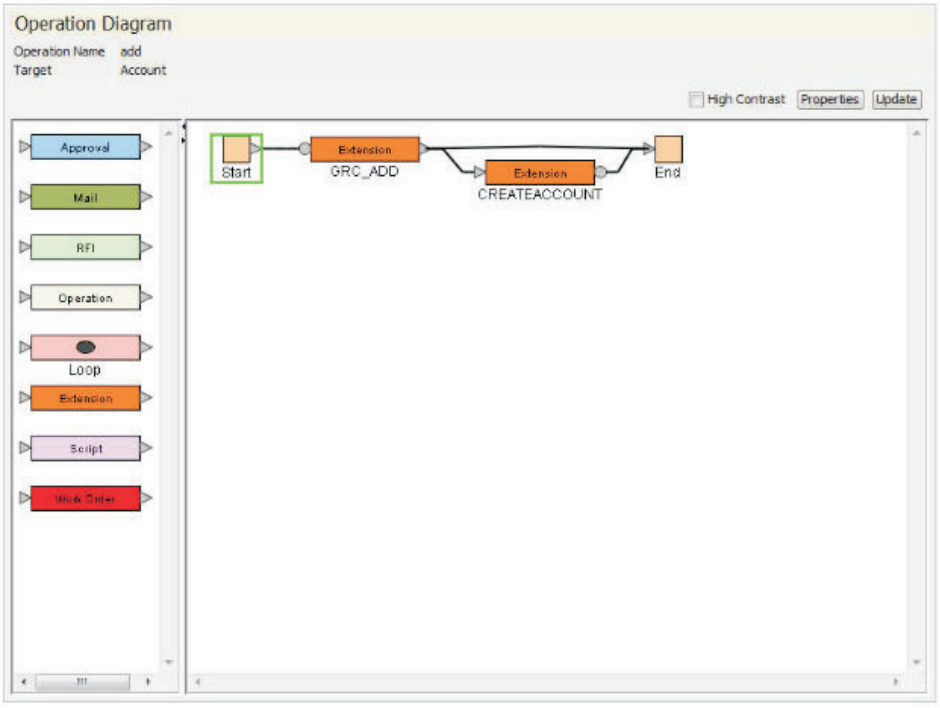
   If the directory does not exist, create a new one.

3. Restart the IBM Security Identity Manager application from the WebSphere console, or restart the WebSphere server itself. After a successful restart, continue with configuration.

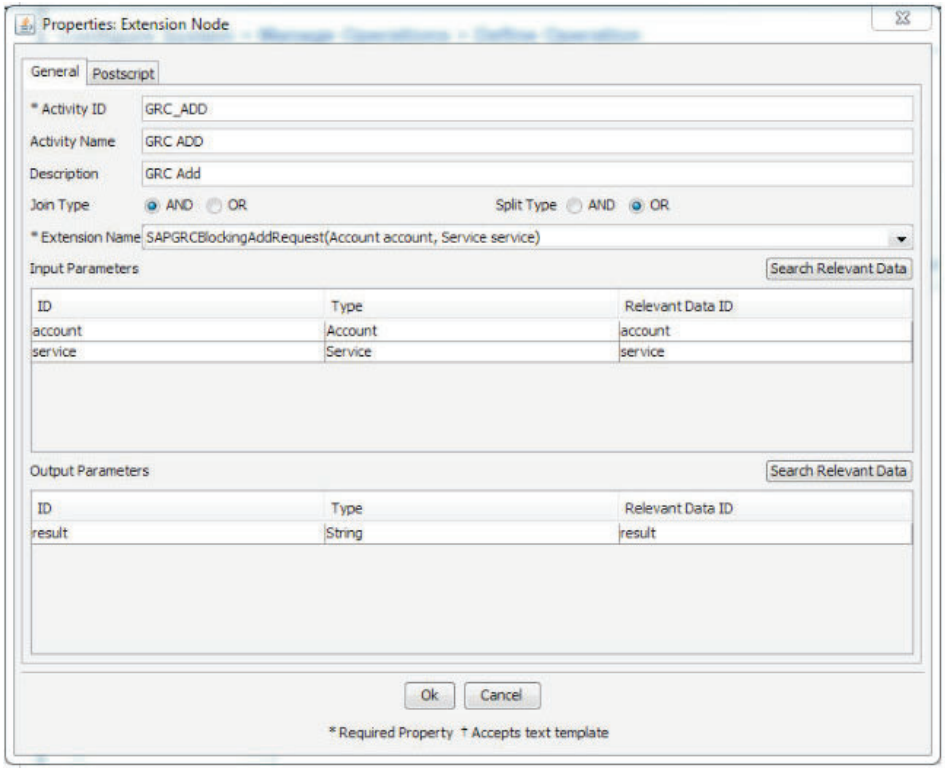
Configuring SAP GRC Access Control 5.3 workflow extensions

Define workflow extensions for the existing SAP GRC NetWeaver account type.

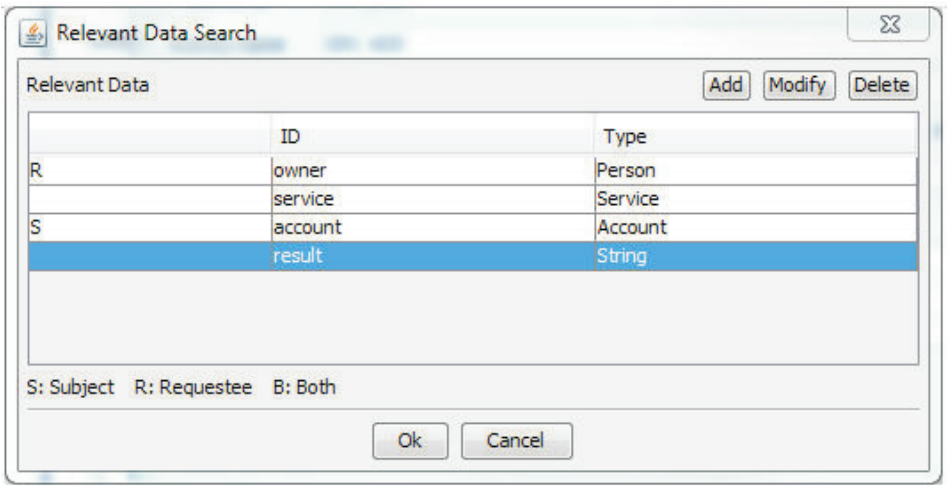
1. Log on to IBM Security Identity Manager.
   a. Select **Configure System > Manager Operations**.
   b. For the **Operation Level**, select **Entity level**.
   c. Select **Account** as the **Entity type**.
   d. Select **SAP GRC NetWeaver Account** as the type of account to be configured with the GRC workflow extension.
2. Click the **Add** button to create an add operation if it doesn't already exist. The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



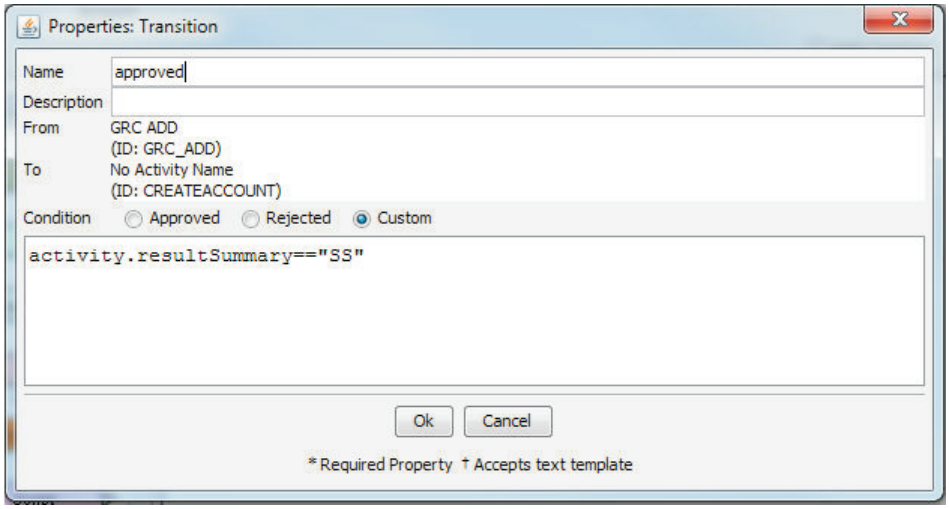
3. Remove the transition line from the **Start** node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **Start** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRCBlockingAddRequest** and fill in the **Activity ID** with **GRC_ADD**. Set the **Activity Name** to **GRC ADD**.



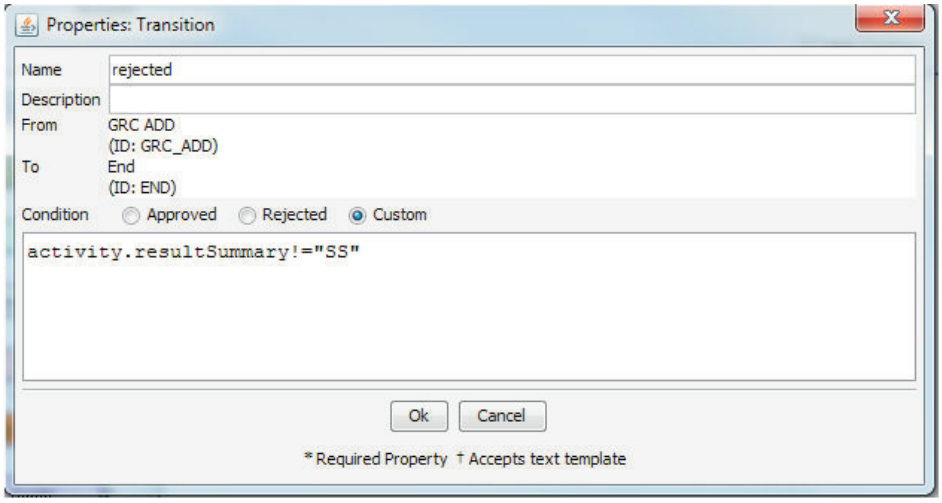
7. Select **OR** for the **Split Type**.
8. Click **Ok** and attach the transitions to the newly-added extension.
9. Click the **Properties** button.
10. Click the **Add** button next to Relevant Data.
11. Create a new **result** Relevant Data. Enter result in the **ID** field. Ensure that the **Type** is String and leave **Default Value** as blank. Click **Ok** to finish.



12. Double-click on the transition connecting the newly-added extension to the **CRETEACCOUNT** extension node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **Ok** to close the transition properties window.



13. Double-click on the transition connecting the newly-added extension to the **END** node and key in the condition `activity.resultSummary!="SS"`. Name the transition "rejected". Click **Ok** to close the transition properties window.
14. Click **Update** and then click **OK** to close the Operations window.



15. Repeat Steps 2 to 14 above for delete, modify, suspend and restore operations, replacing the type of workflow extension to be invoked as needed.

    NOTE: When configuring the properties of the newly-added extension nodes (see Step 6) for these operations, the following values are suggested:

Table 8. SAP GRC Access Control 5.3 Workflow Extension Options

Blocking Operations	**ActivityID**	**Extension Name**
ADD	GRC_ADD	SAPGRCBlockingAddRequest
DELETE	GRC_DELETE	SAPGRCBlockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRCBlockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRCBlockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRCBlockingSuspendRequest
Non-Blocking Operations	**ActivityID**	**Extension Name**

Table 8. SAP GRC Access Control 5.3 Workflow Extension Options (continued)

Blocking Operations	ActivityID	Extension Name
ADD	GRC_ADD	SAPGRCNonblockingAddRequest
DELETE	GRC_DELETE	SAPGRCNonblockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRCNonblockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRCNonblockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRCNonblockingSuspendRequest

Installing and configuring the notification component for SAP GRC Access Control 5.3

Install the workflow notification component for SAP GRC Access Control 5.3.

1. If the `SAPGRC53Workflow.jar` file does not exist for SAP GRC Access Control 5.3, copy it from the installation package `\workflow\grc53\SAPGRC53Workflow.jar` to the directory:

   WEBSPHERE_HOME`\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\ITIM.ear\app_web.war\WEB-INF\lib`

   If the `\WEB-INF\lib` directory does not exist, create one.
2. Copy the `jaas_login_was.conf`, `runNotifierWAS7`, and `SAPNotify.props` files from the installation packages `workflow\grc53\notifier` to a directory on the IBM Security Identity Manager server.

   Use the `runNotifierWAS7.sh` file for UNIX systems or the `runNotifierWAS7.bat` file for Windows systems.
3. Edit the `runNotifierWAS7` script and update the following variables to match your environment:

APP_SRV_HOME	The location of the IBM Security Identity Manager server, including the profile name. For example, `c:\Program Files\IBM\WebSphere\AppServer\profiles\server1`
JAVA_HOME	The location of the root directory of a JAVA. For example: `c:\Program Files\IBM\WebSphere\AppServer\java`
ITIM_HOME	The location on the IBM Security Identity Manager installation, not the IBM Security Identity Manager deployed ear. For example, `c:\Program Files\IBM\itim`
APP_SRV_CELL	Name of the WebSphere cell that the IBM Security Identity Manager application is deployed on. This attribute is required to find the `SAPGRCWorkflow.jar` file.
WFE_HOME	The location of the `SAPGRCWorkflow.jar` file.

4. Edit the `SAPNotify.props` file and provide the correct value for each of these attributes.

GRCNotifyURL	This attribute is the URL to the SAP GRC Access Control 5.3 Request Status WebService. For example, the URL might be: `http://sapgrc53:50100/SAPGRC_AC_IDM_REQUESTSTATUS/Config1?style=document`
GRCUserName	An administration user ID used to access the SAP GRC Access Control system.
GRCPassword	The password for the Administrator user name.
itim.user	An IBM Security Identity Manager user with administration privileges.
itim.pswd	The password for the IBM Security Identity Manager user
itim.home	Path to the IBM Security Identity Manager server directory. For example, the path might be: `C:/Program Files/IBM/itim`

apps.context.factory	This attribute is the context to get access to the IBM Security Identity Manager server. Use the default value com.ibm.itim.apps.impl.websphere.WebSpherePlatformContextFactory, unless otherwise instructed by an IBM representative.
isim.authentication.factory.classname	This attribute is the authentication factory class name. For IBM Security Identity Manager 6.0. Use the default value com.ibm.tivoli.auth.ISIM6AuthenticationFactory ,unless otherwise instructed by an IBM representative.
isim.jaas.logincontextname	This attribute is the JAAS login context name. The default value is used if no value is defined. For IBM Security Identity Manager 6.0, the default value is WSLogin.
enrole.appServer.realm	This attribute is the application server realm name. The default value is defined in the *ISIM_HOME*\data\ enrole.properties file.

5. Validate the configuration by running **runNotifierWAS7** from the command line. The following two lines are displayed on the command line:

   ```
   Starting Notifier
   .....
   Stopping Notifier
   ```

   The notification service updates all relevant workflows in IBM Security Identity Manager to either "APPROVED_SUCCESS" or "APPROVED_REJECTED" if:

   - There is a request in SAP GRC that was closed, either "Approved," "Rejected," or "Cancelled".
   - The request has a matching SAP GRC Access Control request ID for an IBM Security Identity Manager workflow currently in the PENDING state.

6. Edit the logging.properties file in the JAVA_HOME lib directory to enable more or less logging. For example,*WAS_HOME*\java\jre\lib\logging.properties

   This log file contains the jlog configuration. By adding the following line the logging level can be increased:

   ```
   com.ibm.tivoli.sapgrc53.level=ALL
   ```

   The console handler might also need to be increased to allow for the output of all logging:

   ```
   java.util.logging.ConsoleHandler.level=ALL
   ```

   Logging might be disabled. This disablement might be required when running the notifier as a scheduled task. To turn logging off, set the following values:

   ```
   java.util.loging.ConsoleHandler.level=NONE
   com.ibm.tivoli.sapgrc53.level=NONE
   ```

7. If security is enabled on WebSphere, import the WebSphere key into the IBM Security Identity Manager keystore. The IBM Security Identity Manager keystore file and its password are defined in the *ISIM_HOME*\data\ enrole.properties file, look for the **enrole.encryption.keystore** and **enrole.encryption.password**:

   a. Navigate to the *WAS_HOME*\bin directory.
   b. Launch the ikeyman.bat file from C:\Program Files\IBM\WebSphere\ AppServer\bin.
   c. Select **Key Data File** > **Open**.
   d. Select Key database type **PKCS12** and then browse to the keystore file in *WAS_HOME*\config\cells\iqint17aNode01Cell\nodes\iqint17aNode01\key.p12
   e. Enter the keystore password WebAS.
   f. Select **Export** to export the key to a temp directory C:\temp\default.p12.
   g. Enter password WebAS.
   h. Select **Key Data File** > **Open**.

i. Select Key database type **JCEKS** and then browse to the IBM Security Identity Manager keystore.

j. Enter the keystore password.

k. Select **Import** to import the key from `C:\temp\default.p12` into the IBM Security Identity Manager keystore and save it.

8. After confirming that the configuration is correct, place the **runNotifierWAS7** script into a scheduled task so that it runs on a regular basis. On Windows systems, use the Windows scheduler to schedule the task. On Linux or UNIX systems, use the **crontab** command. Contact your system administrator to set up these tasks.

Installing SAP GRC Access Control 10.0 workflow extensions

Follow these steps to install the workflow extensions.

1. Edit the `workflowextensions.xml` file under the *ISIM_HOME*`/data` directory to add a workflow extension.

   Note: This sample is provided as part of the installation package as `workflow\grc10\GRC10workflowExtensions.xml`. To avoid confusion with the SAP GRC Access Control 5.3 workflow extensions the SAP GRC Access Control 10.0 workflow extensions exist in different packages. They were also given different names to ensure that the correct code is executed after invoking the extension. For example, if the `SAPGRC53Workflow.jar` file was mistakenly installed in WebSphere but the SAP GRC Access Control 10.0 workflow extensions are invoked, an error is displayed. The error informs the user that the SAP GRC Access Control 10.0 workflow extension could not be found. After the SAP GRC Access Control 10.0 workflow extensions are added to `workflowextensions.xml`, do the following actions:

   a. Open the file with a browser.

   b. Check that the file does not contain any XML syntax errors.

   c. Add the following SAP GRC Access Control 10.0 workflow extensions:

```
<ACTIVITY ACTIVITYID="SAPGRC10NonblockingAddRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="nonblockingSAPGRC10AddRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRC10BlockingAddRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="blockingSAPGRC10AddRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10NonblockingModifyRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="nonblockingSAPGRC10ModifyRequestExtension" />
```

```
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRC10BlockingModifyRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="blockingSAPGRC10ModifyRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10NonblockingDeleteRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="nonblockingSAPGRC10DeleteRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRC10BlockingDeleteRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="blockingSAPGRC10DeleteRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10NonblockingSuspendRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="nonblockingSAPGRC10SuspendRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRC10BlockingSuspendRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="blockingSAPGRC10SuspendRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10NonblockingRestoreRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="nonblockingSAPGRC10RestoreRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
```

```
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>
<ACTIVITY ACTIVITYID="SAPGRC10BlockingRestoreRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="blockingSAPGRC10RestoreRequestExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10RiskAnalysisRequest" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="SAPGRC10RiskAnalysisExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="riskDetail" RELEVANT_DATA_ID="riskDetail" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="checkGRCVersion" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="checkGRCVersion" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="Entity" TYPE="Account" />
  <OUT_PARAMETERS PARAM_ID="grcVersion" RELEVANT_DATA_ID="grcVersion" TYPE="String" />
 </PARAMETERS>
</ACTIVITY>

<ACTIVITY ACTIVITYID="SAPGRC10UpdateAccountAttributesExtension" LIMIT="0">
 <IMPLEMENTATION_TYPE>
  <APPLICATION
   CLASS_NAME="com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension"
   METHOD_NAME="SAPGRC10UpdateAccountAttributesExtension" />
 </IMPLEMENTATION_TYPE>
 <PARAMETERS>
  <IN_PARAMETERS PARAM_ID="account" RELEVANT_DATA_ID="account" TYPE="Account" />
  <IN_PARAMETERS PARAM_ID="service" RELEVANT_DATA_ID="service" TYPE="Service" />
  <OUT_PARAMETERS PARAM_ID="result" RELEVANT_DATA_ID="result" TYPE="String" />
  <OUT_PARAMETERS PARAM_ID="output" RELEVANT_DATA_ID="account" TYPE="Account" />
 </PARAMETERS>
</ACTIVITY>
```

2. Copy `workflow\grc10\SAPGRC10Workflow.jar` from the installation package to the appropriate directory: `WEBSPHERE_HOME\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME \ITIM.ear\app_web.war\WEB-INF\lib`

   If the directory does not exist, create a new one.
3. Restart the IBM Security Identity Manager application from the WebSphere console, or restart the WebSphere server itself. After a successful restart, continue with configuration.

Configuring SAP GRC Access Control 10.0 workflow extensions

SAP GRC Access Control 10.0 workflow extensions support three different SAP GRC operations: *Access Request*, *Risk Analysis* and *Update Account Attributes*.

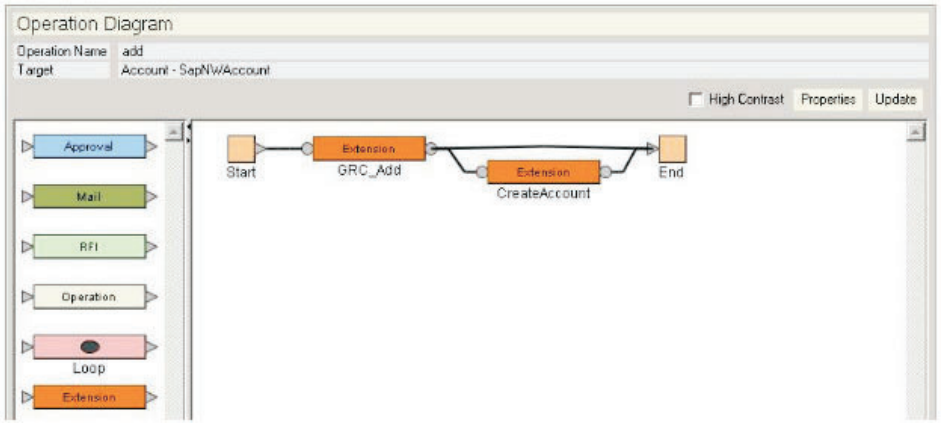
This section provides detail steps on how to configure these workflow extensions using the Add operation as an example.

- "Configuring Access Request workflow extension"
- "Configuring Risk Analysis workflow extension" on page 32
- "Configuring Update Account Attributes workflow extension" on page 35

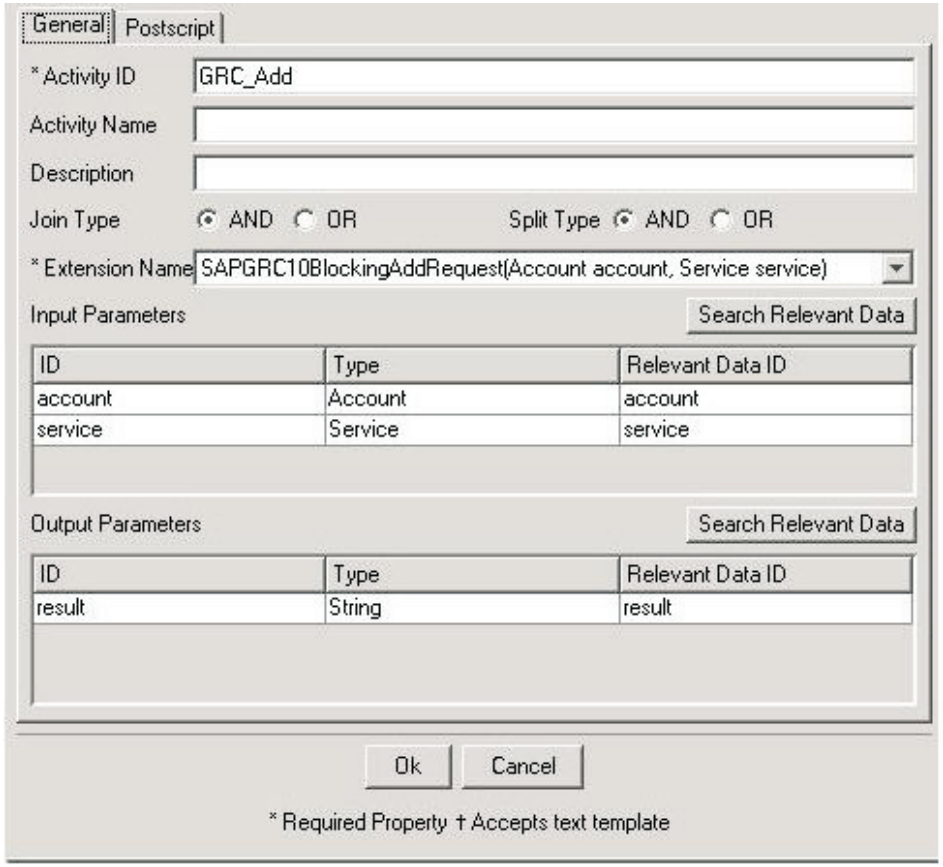
Configuring Access Request workflow extension

Define Access Request workflow extensions for the existing SAP GRC NetWeaver account type.

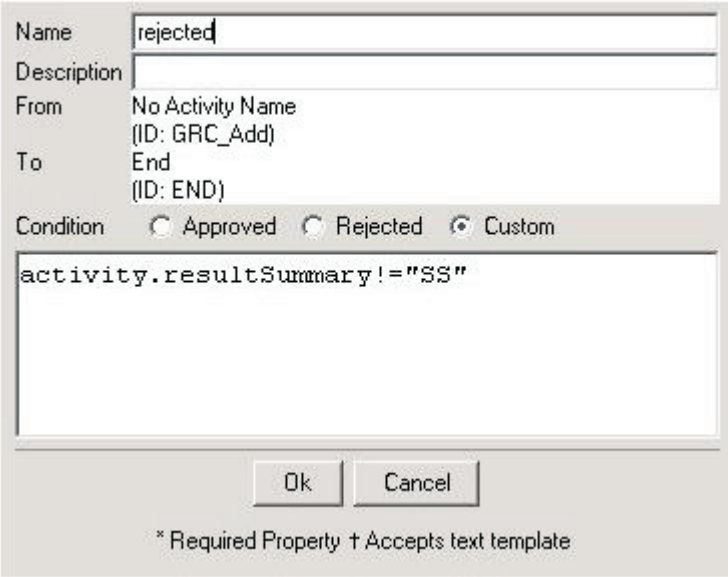
1. Log on to IBM Security Identity Manager.
   a. Select **Configure System** > **Manager Operations**.
   b. For the **Operation Level**, select **Entity level**.
   c. Select **Account** as the **Entity type**.
   d. Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click the **Add** button to create an add operation if it doesn't already exist. The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



3. Remove the transition line from the **Start** node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **Start** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRC10BlockingAddRequest** and fill in the **Activity ID** with **GRC_ADD**. Set the **Activity Name** to **GRC ADD**.
7. Select **OR** for the **Split Type**.



8. Click **Ok** and attach the transitions to the newly-added extension.
9. Click the **Properties** button.
10. Click the **Add** button next to Relevant Data.
11. Create a new **result** Relevant Data. Enter result in the ID field. Ensure that the **Type** is String and leave **Default Value** as blank. Click **Ok** to finish.
12. Double-click the transition connecting the newly-added extension to the **CREATEACCOUNT** extension node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **Ok** to close the transition properties window.
13. Double-click the transition connecting the newly-added extension to the **END** node and key in the condition `activity.resultSummary!="SS"`. Name the transition "rejected". Click **Ok** to close the transition properties window.



14. Click Update and then click **Ok** to close the Operations window.
15. Repeat Steps 2 to 12 for delete, modify, suspend, and restore operations.

    Note: When configuring the properties of the newly-added extension nodes (see Step 6) for these operations, the following values can be used:

Table 9. SAP GRC Access Control 10.0 Workflow Extension Options

Blocking Operations	**ActivityID**	**Extension Name**
ADD	GRC_ADD	SAPGRC10BlockingAddRequest
DELETE	GRC_DELETE	SAPGRC10BlockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRC10BlockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRC10BlockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRC10BlockingSuspendRequest
Non-Blocking Operations	**ActivityID**	**Extension Name**
ADD	GRC_ADD	SAPGRC10NonblockingAddRequest
DELETE	GRC_DELETE	SAPGRC10NonblockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRC10NonblockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRC10NonblockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRC10NonblockingSuspendRequest

Configuring Risk Analysis workflow extension

This workflow extension allows IBM Security Identity Manager to send a risk analysis request that will be performed for a specific access request ID to SAP GRC Access Control 10.0.

The risk analysis result is recorded by IBM Security Identity Manager workflow as a string output parameter named"riskDetail". Risk results returned from SAP GRC Access Control are indicated by a '#' character. Each risk consists of a number of name-value pairs. These name-value pairs are separated by a '|' character. The risk

name and its value are separated by a ':' character. If the value is multi-valued, then the set of values is enclosed by '[ ]' characters, and each value in the set is separated by a ',' character.

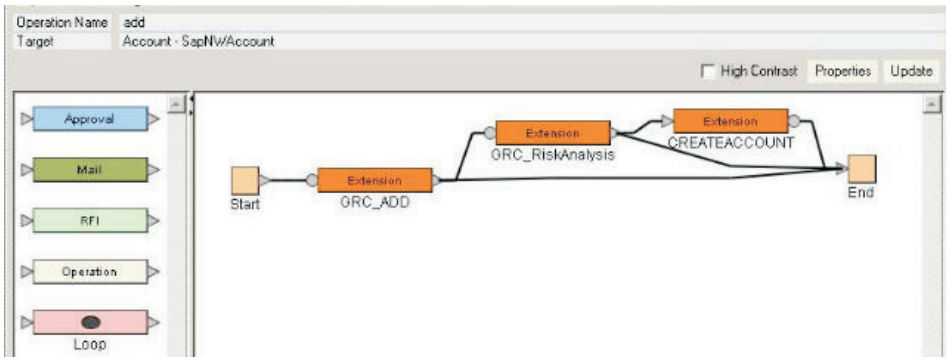
An example of the riskDetail returned to IBM Security Identity Manager workflow looks like:

```
#Risk Number:1|Risk Id:B009|Risk Description:Basis Table Maintenance &
System Administration|Risk Level:High|System Name:GC7CLNT001|User
Id:AC102509|Role List:[SAP_XI_ADMINISTRATOR_ABAP, SAP_XI_CONFIGURATOR,
SAP_XI_BPE_ADMINISTRATOR_ABAP, SAP_XI_ADMINISTRATOR]|Action List:[SXMB_ADM,
SM30, SM12, SXMB_ADM_BPE, SM59]|
```

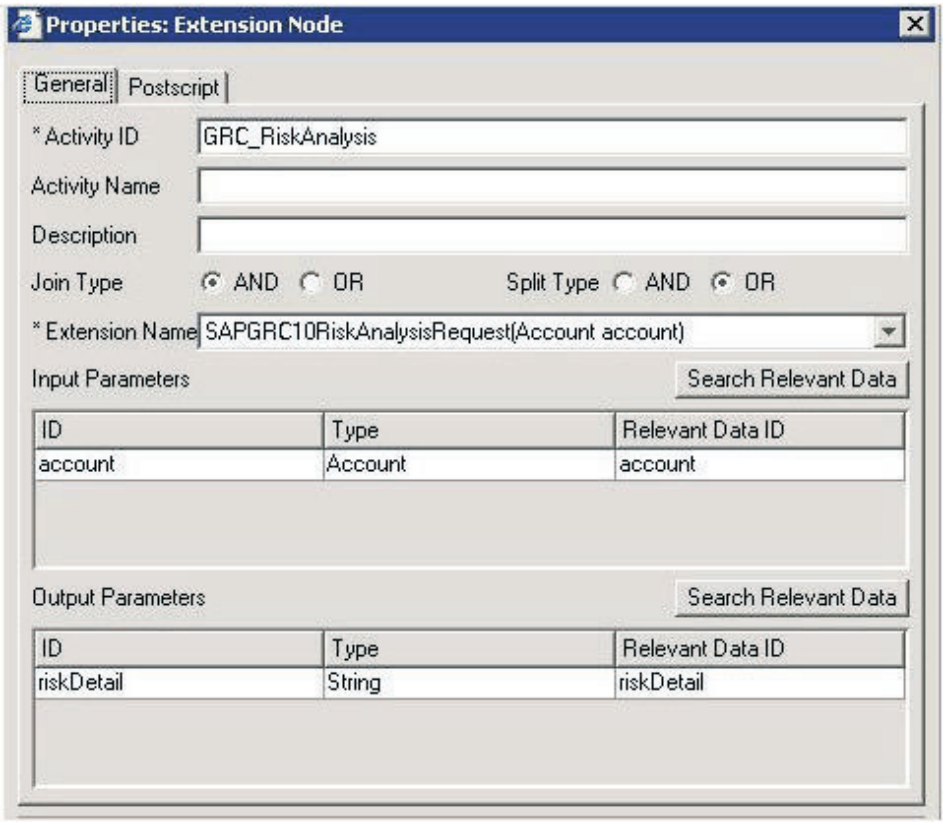
If necessary, the output parameter can be parsed in IBM Security Identity Manager workflow to catch risk violations that have been detected by SAP GRC Access Control 10.0. Detail on how to parse the riskDetail output parameter is out-of-scope of this guide.

Define Risk Analysis workflow extensions for the existing SAP GRC NetWeaver account type.

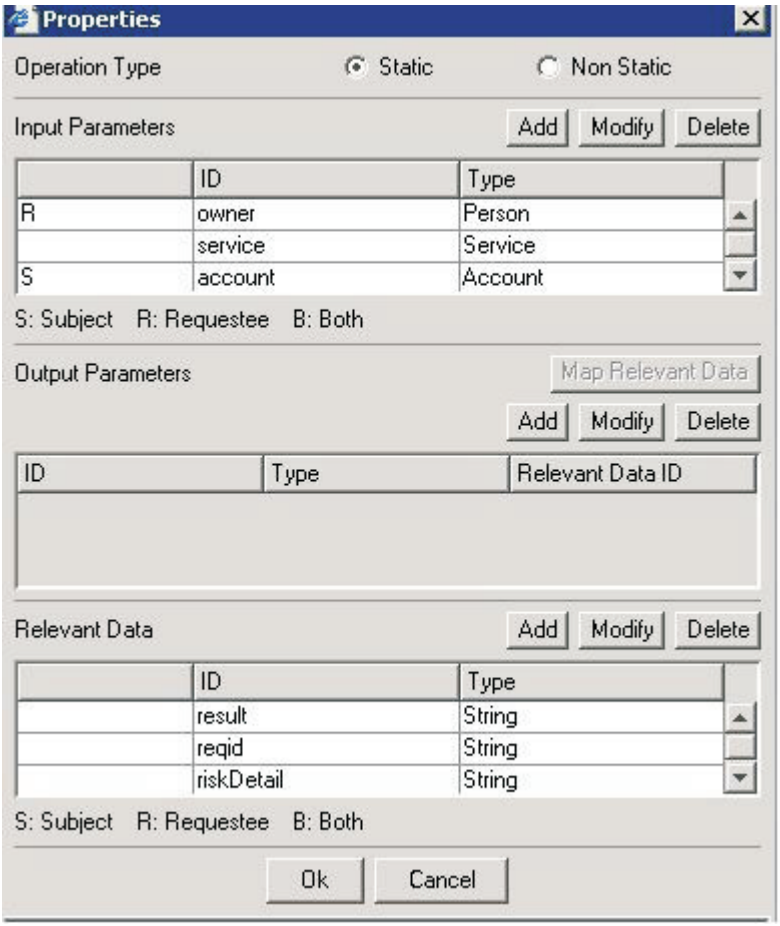
1. Log on to IBM Security Identity Manager.
   a. Select **Configure System > Manager Operations**.
   b. For the **Operation Level**, select **Entity level**.
   c. Select **Account** as the **Entity type**.
   d. Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click the **Add** button to create an add operation if it doesn't already exist. The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



3. Remove the transition line from the **GRC_ADD** extension node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **GRC_ADD** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRC10RiskAnalysisRequest** and fill in the **Activity ID** with **GRC_RiskAnalysis**. Set the **Activity Name** to **GRC RiskAnalysis**.
7. Select **OR** for the **Split Type**.
8. Click **Ok** and attach the transitions to the newly-added extension.



9. Click the **Properties** button.
10. Click the **Add** button next to Relevant Data.
11. Create a new **reqid** Relevant Data. Enter **reqid** in the **ID** field. Ensure that the **Type** is String and leave **Default Value** as blank. Click **Ok** to finish.



12. Create a new **riskDetail** Relevant Data. Enter **riskDetail** in the **ID** field. Ensure that the **Type** is String and leave **Default Value** as blank. Click **Ok** to finish.
13. Double-click on the transition connecting the newly-added extension to the **CREATEACCOUNT** extension node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **Ok** to close the transition properties window.
14. Double-click on the transition connecting the newly-added extension to the **END** node and key in the condition `activity.resultSummary!="SS"`. Name the transition "rejected". Click **Ok** to close the transition properties window.
15. Click **Update** and then click **OK** to close the Operations window.
16. Repeat Steps 2 to 14 above for another operation when risk analysis is applicable.

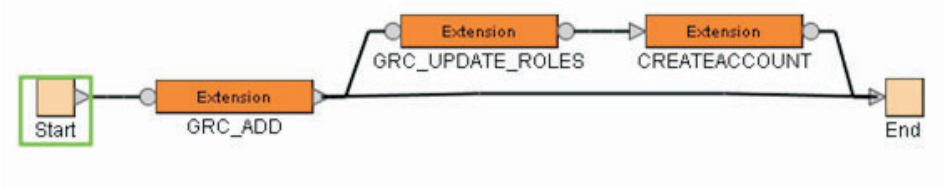
Configuring Update Account Attributes workflow extension

This workflow extension compares the list of roles on an approved request returned by SAP GRC Access Control 10.0 with the list of roles requested by IBM Security Identity Manager.

If the status of a role is not “approved”, then the role is assumed to have been rejected in SAP GRC AC 10.0. The extension then removes the rejected roles from the request in IBM Security Identity Manager. The same behavior applies to rejection of account assignments. This workflow extension should be executed before the account is provisioned in SAP NetWeaver.

Define Update Account Attribute workflow extensions for the existing SAP GRC NetWeaver account type.

1. Log on to IBM Security Identity Manager.
   a. Select **Configure System > Manager Operations**.
   b. For the **Operation Level**, select **Entity level**.
   c. Select **Account** as the **Entity type**.
   d. Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click the **Add** button to create an add operation if it doesn't already exist. The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



3. Remove the transition line from the **GRC_ADD** extension node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **GRC_ADD** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Set the **ActivityId** to **GRC_UPDATE_ACCOUNT** and **ExtensionName** as **SAPGRC10UpdateAccountAttributesExtension(Account account, Service service)**.
7. Click **Ok** to save and close the popup window.
8. Connect the **GRC_UPDATE_ACCOUNT** extension node to the **End** node with a transition line and enter the following condition:

   ```
   activity.resultSummary!="SS"
   ```

9. Click **Update** and then click **OK** to close the Operations window.
10. Repeat Steps 2 to 7 above for another operation when update account attributes is applicable.

Installing and configuring the notification component for SAP GRC Access Control 10.0

Install the notification component for SAP GRC Access Control 10.0.

1. If the `SAPGRC10Workflow.jar` file does not exist for SAP GRC Access Control 10.0, copy it from the installation package `\workflow\grc10\SAPGRC10Workflow.jar` to the directory: *`WEBSPHERE_HOME`*`\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\ITIM.ear\app_web.war\WEB-INF\lib`

   If the `\WEB-INF\lib` directory does not exist, create one.
2. Copy the `jaas_login_was.conf`, `runNotifierWAS7.[bat|sh]`, and `SAPNotify.props` files from the installation packages `workflow\grc10\notifier` to a directory on the IBM Security Identity Manager server.

   Use the `runNotifierWAS7.sh` file for UNIX systems or the `runNotifierWAS7.bat` file for Windows systems.
3. Edit the **`runNotifierWAS7`** script and update the following variables to match your environment:

APP_SRV_HOME	The location of the IBM Security Identity Manager server, including the profile name. For example: `c:\Program Files\IBM\WebSphere\AppServer\profiles\server1`
JAVA_HOME	The location of the root directory of a JAVA installation. For example, `c:\Program Files\IBM\WebSphere\AppServer\java`
ITIM_HOME	The location on the IBM Security Identity Manager installation, not the ITIM deployed ear. For example: `c:\Program Files\IBM\itim`
APP_SRV_CELL	Name of the WebSphere cell that the IBM Security Identity Manager application is deployed on. This attribute is required to find the `SAPGRC10Workflow.jar` file.
WFE_HOME	The location of the `SAPGRC10Workflow.jar` file.

4. Edit the `SAPNotify.props` file and provide the correct value for each of the attributes.

GRCNotifyURL	This attribute is the URL to the SAP GRC Access Control 10.0 Audit Logs Web Service. For example, the URL could resemble: `http://`*`remotehost`*`:`*`port`*`/sap/bc/srt/rfc/sap/grac_audit_logs_ws/`*`client_number`*`/grac_audit_logs_ws/binding?sap-client=`*`client_number`*
GRCUserName	An administration or user ID used to access the SAP GRC Access Control system.
GRCPassword	The password for the Administrator user name.
itim.user	An IBM Security Identity Manager user with administration privileges.
itim.pswd	The password for the IBM Security Identity Manager user.
itim.home	Path to the IBM Security Identity Manager server directory. For example, the path might be: `C:/Program Files/IBM/itim`
apps.context.factory	This attribute is the context to get access to the IBM Security Identity Manager server. Use the default value `com.ibm.itim.apps.impl.websphere.WebSpherePlatformContextFactory`, unless otherwise instructed by an IBM representative.
`isim.authentication.factory.classname`	This attribute is the authentication factory class name. For IBM Security Identity Manager 6.0. Use the default value `com.ibm.tivoli.auth.ISIM6AuthenticationFactory` ,unless otherwise instructed by an IBM representative.
isim.jaas.logincontextname	This attribute is the JAAS login context name. The default value is used if no value is defined. For IBM Security Identity Manager 6.0, the default value is `WSLogin`.
enrole.appServer.realm	This attribute is the application server realm name. The default value is defined in the *`ISIM_HOME`*`\data\ enrole.properties` file.

5. Validate the configuration by running **runNotifierWAS7** from the command line. The following two lines are displayed on the command line:

```
Starting Notifier
......
Stopping Notifier
```

The notification service updates all relevant workflows in IBM Security Identity Manager to either "APPROVED_SUCCESS" or "APPROVED_REJECTED" if:

- There is a request in SAP GRC that was closed, either "Approved," "Rejected," or "Cancelled".
- The request has a matching SAP GRC Access Control request ID for an IBM Security Identity Manager workflow currently in the PENDING state.

6. Edit the `logging.properties` file in the JAVA_HOME lib directory to enable more or less logging. For example, *`WAS_HOME`*`\java\jre\lib\logging.properties`

This log file contains the jlog configuration. By adding the following line the logging level can be increased:

```
com.ibm.tivoli.sapgrc10.level=ALL
```

The console handler might also need to be increased to allow for the output of all logging:

```
java.util.logging.ConsoleHandler.level=ALL
```

7. Logging might be disabled. This disablement might be required when running the notifier as a scheduled task. To turn logging off, set the following values:

   ```
   java.util.loging.ConsoleHandler.level=NONE
   com.ibm.tivoli.sapgrc10.level=NONE
   ```

8. If security is enabled on WebSphere, import the WebSphere key into the IBM Security Identity Manager keystore. The IBM Security Identity Manager keystore file and its password are defined in the *ISIM_HOME*\data\ enrole.properties file, look for the **enrole.encryption.keystore** and **enrole.encryption.password**:
   a. Navigate to the *WAS_HOME*\bin directory.
   b. Launch the ikeyman.bat file from C:\Program Files\IBM\WebSphere\ AppServer\bin.
   c. Select **Key Data File** > **Open**.
   d. Select Key database type **PKCS12** and then browse to the keystore file in *WAS_HOME*\config\cells\iqint17aNode01Cell\nodes\iqint17aNode01\key.p12
   e. Enter the keystore password WebAS.
   f. Select **Export** to export the key to a temp directory C:\temp\default.p12.
   g. Enter password WebAS.
   h. Select **Key Data File** > **Open**.
   i. Select Key database type **JCEKS** and then browse to the IBM Security Identity Manager keystore.
   j. Enter the keystore password.
   k. Select **Import** to import the key from C:\temp\default.p12 into the IBM Security Identity Manager keystore and save it.
9. After confirming that the configuration is correct, place the **runNotifierWAS7** script into a scheduled task so that it runs on a regular basis. On Windows systems, use the Windows scheduler to schedule the task. On Linux or UNIX systems, use the **crontab** command. Contact your system administrator to set up these tasks.

Log file locations for workflow extensions

The log file locations for SAP GRC Access Control are different for versions 5.3 and 10.0. You must take an additional action to enable logging for SAP GRC Access Control 10.0.

SAP GRC Access Control 5.3
The logging for the workflow extensions is in the user.home\ grcextension.log file.

SAP GRC Access Control 10.0
The logging for the workflow extensions is in the IBM Security Identity Manager trace.log file.

To enable logging for the extensions, modify the settings in the enRoleLogging.properties file in the *ISIM_HOME*\data\ directory to:

```
logger.trace.com.ibm.tivoli.sapgrc10.wfe.SapGRCApplicationExtension.level=DEBUG_MAX
logger.trace.com.ibm.itim.workflowextensions.AccountExtensions.level=DEBUG_MAX
```

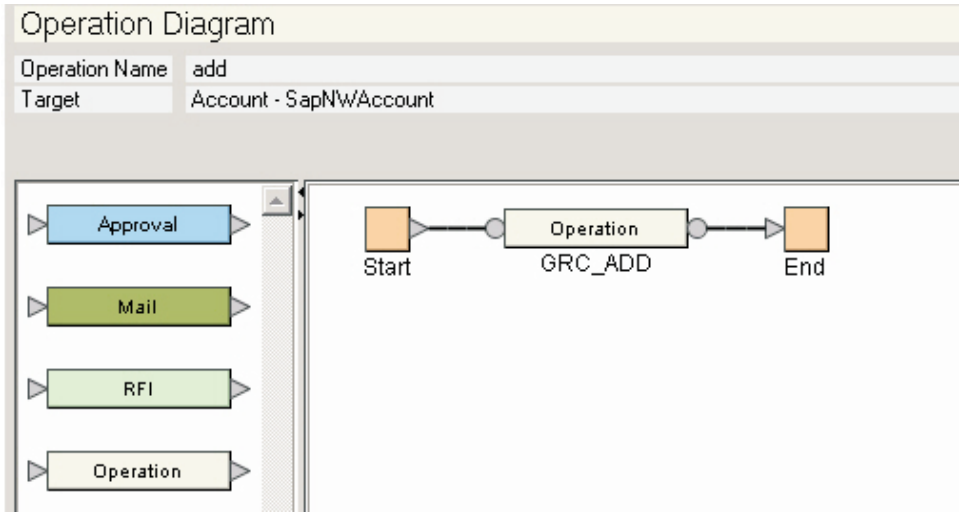
Configuring workflow extensions to concurrently support SAP GRC Access Control 5.3, SAP GRC Access Control 10.0, and SAP NetWeaver

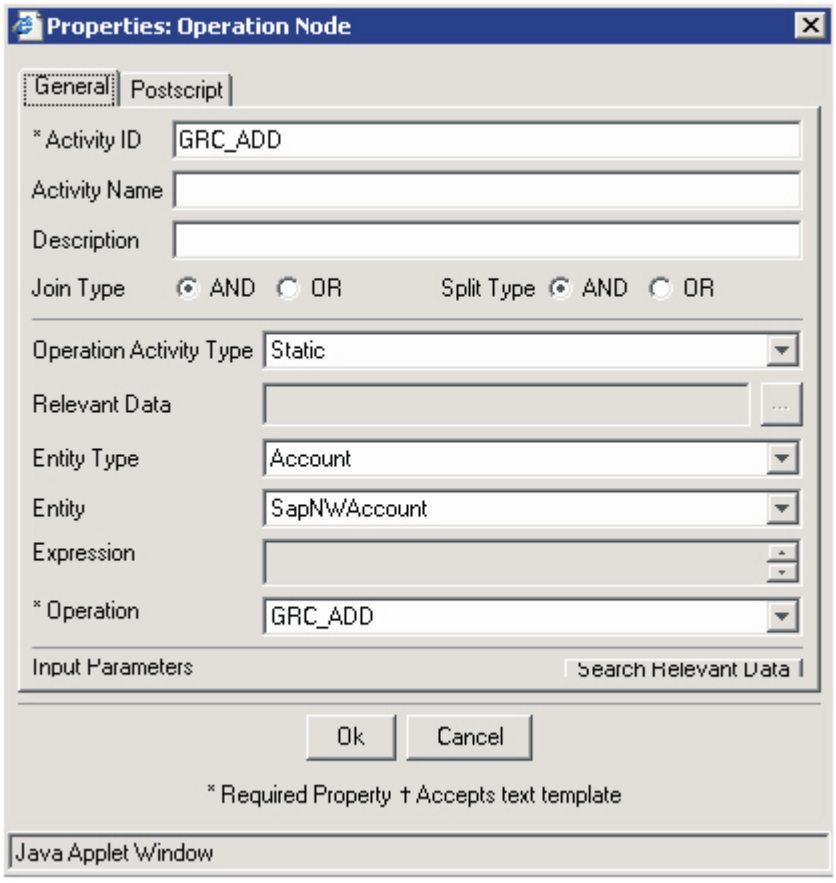
To support SAP GRC Access Control 5.3, SAP GRC Access Control 10.0 and non-GRC managed SAP NetWeaver resources in a single IBM Security Identity Manager server instance, a sub-process needs to be created to neatly encapsulate these operations.

The control flow path in the sub-process is determined by the value given to the GRC Version attribute on the service form.

Define Access Request workflow extensions for the existing SAP GRC NetWeaver account type.

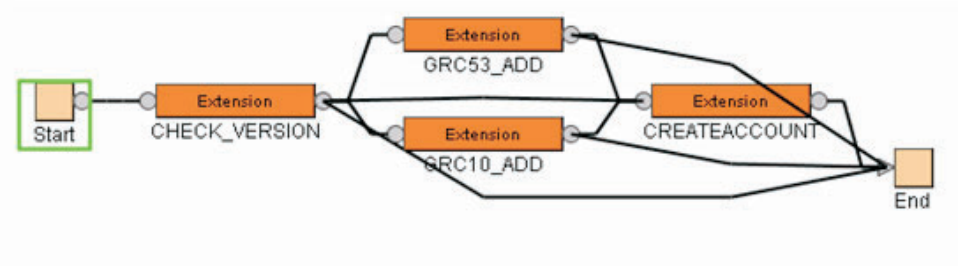
1. Log on to Tivoli Identity Manager.
   a. Select **Configure System > Manage Operations**.
   b. For the **Operation Level**, select **Entity level**.
   c. Select **Account** as the **Entity type**.
   d. Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. To simplify the layout of the workflow extension for this operation, the SAP GRC Access Control workflow configuration should be created as a sub-process and referenced to by an operation node.





The following steps will use the Add operation as an example to show how to configure a GRC_ADD operation node to support the Add operation when different SAP GRC Access Control versions need to be supported in a single server instance.

3. Click the **Add** button to create a **GRC_ADD** operation. The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



4. Add all the required Input Parameters and Relevant Data.
   a. Click the **Properties** button to add the following attributes.

Table 10. Input parameters

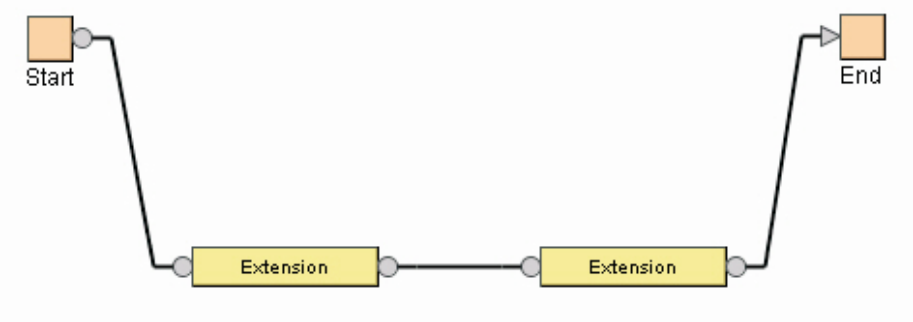
ID	Description	Context	Type
owner	Owner	Requestee	Person
service	Service	N/A	Service
account	Account	Subject	Account

Table 11. Relevant data

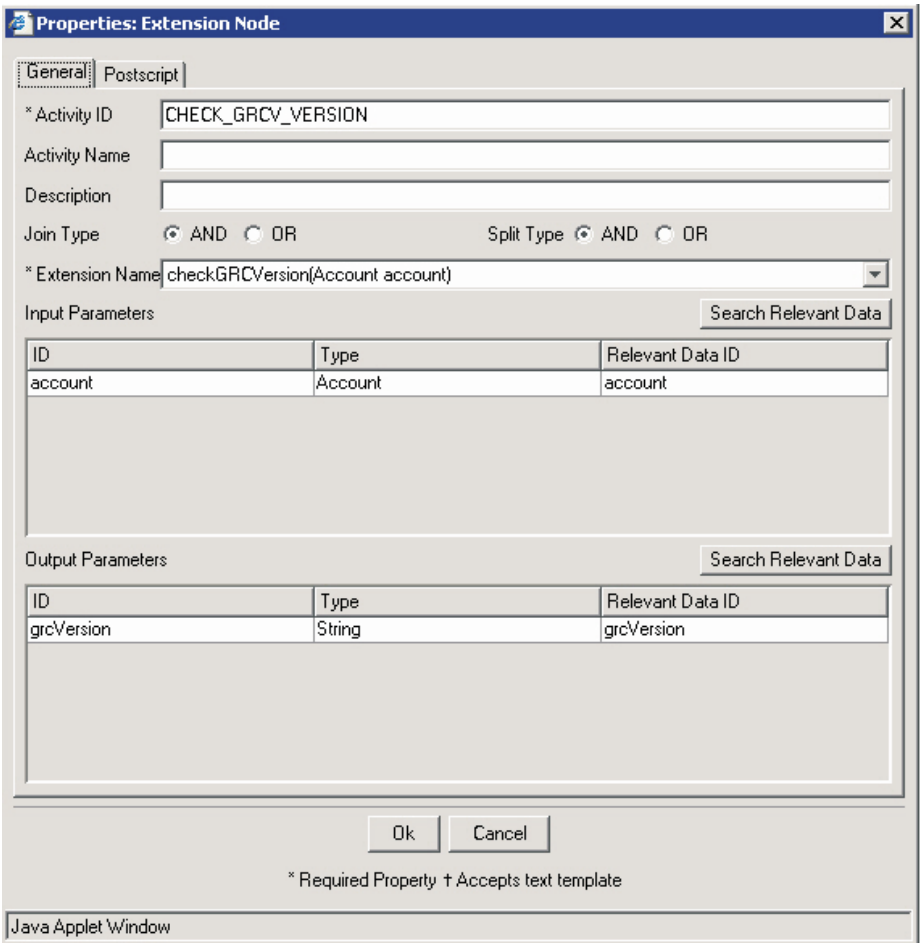
ID	Type
grcVersion	String
result	String
reqid	String
riskDetail	String

b. Click **Ok** to save.

5. Add nodes to support SAP NetWeaver only.
   a. Select two Extension nodes, connect them together from Start to End as following:



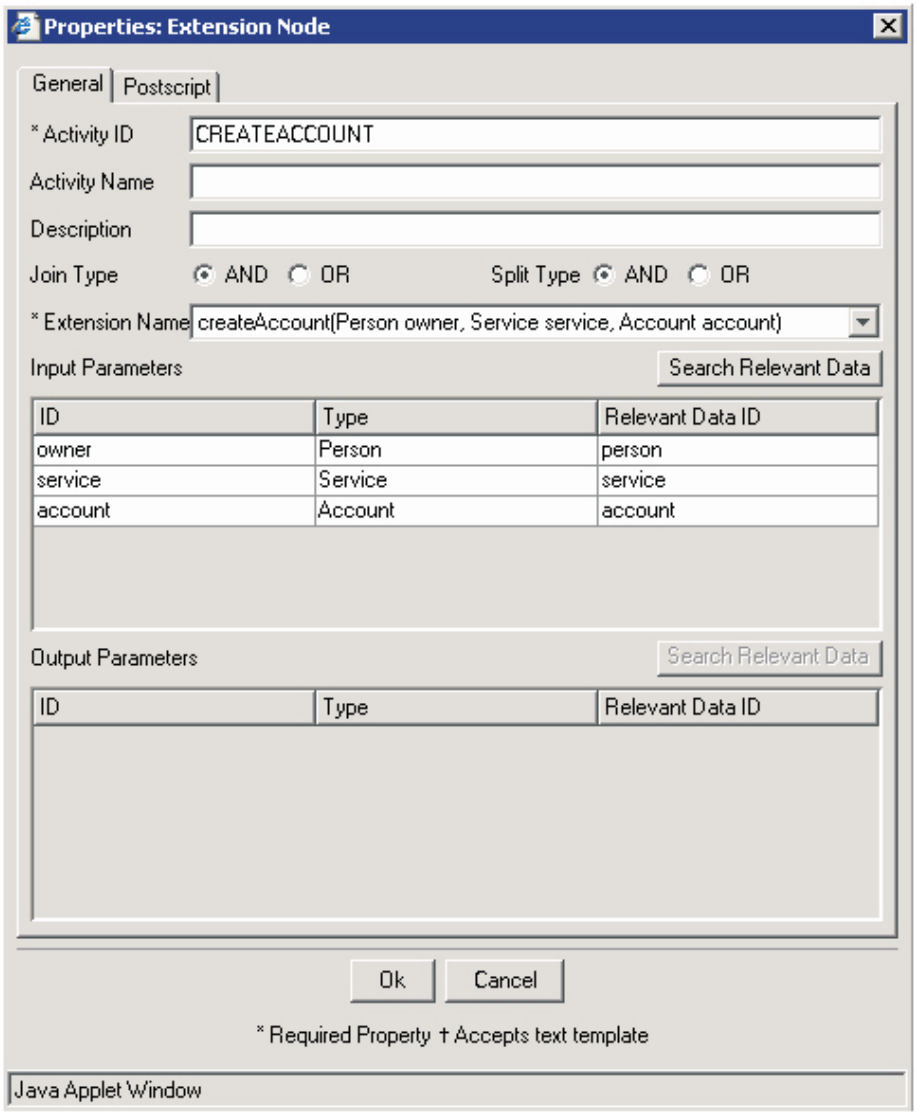
   b. Double click the first extension, set the **ActivityID** to **CHECK_GRC_VERSION** and **ExtensionName** as **checkGRCVersion(Account account)**.
   c. Click the **Search Relevant Data** button to find the relevant data for the Input Parameters and the Output Parameters.



d. Click **Ok** to save and close the popup window.

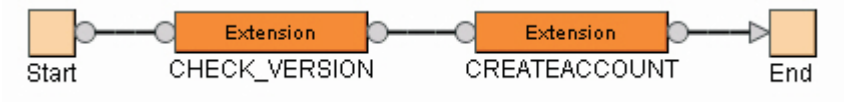
e. Double click the second extension, set the **ActivityID** to **CREATEACCOUNT** and **ExtensionName** as the default **createAccount(Person owner, Service service, Account account)**.

f. Click the **Search Relevant Data** button to find the relevant data for the Input Parameters.



g. Click **Ok** to save and close the popup window.

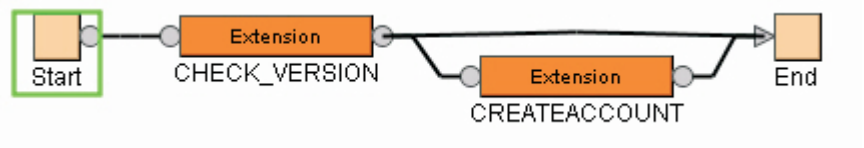
h. Click the **Update** button. The workflow extension should look similar to the following screen capture.



i. Double click the transition line between the two extension nodes to enter the following condition: `grcVersion.get()=="na"`

   If the output parameter **grcVersion** string returns a value of **na**, that means the **Enable GRC workflow configuration** option is not enabled on the service form.

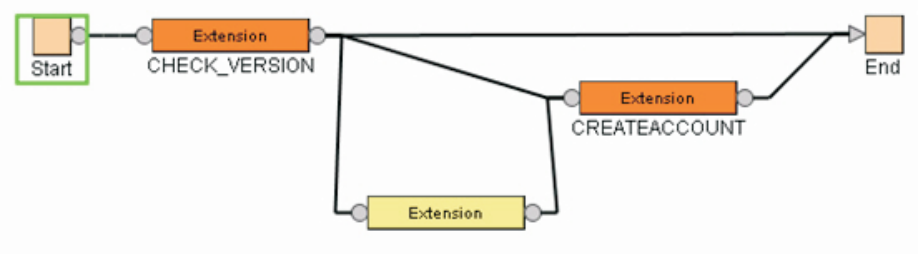
j. To ensure that workflow is invoked correctly, use a transition line to connect the first extension node to the End node and enter the following condition:
```
(grcVersion.get() != "10.0") &&(grcVersion.get() != "5.3")
&&(grcVersion.get() != "na")
```



k. Click **Update** to save the current configuration.

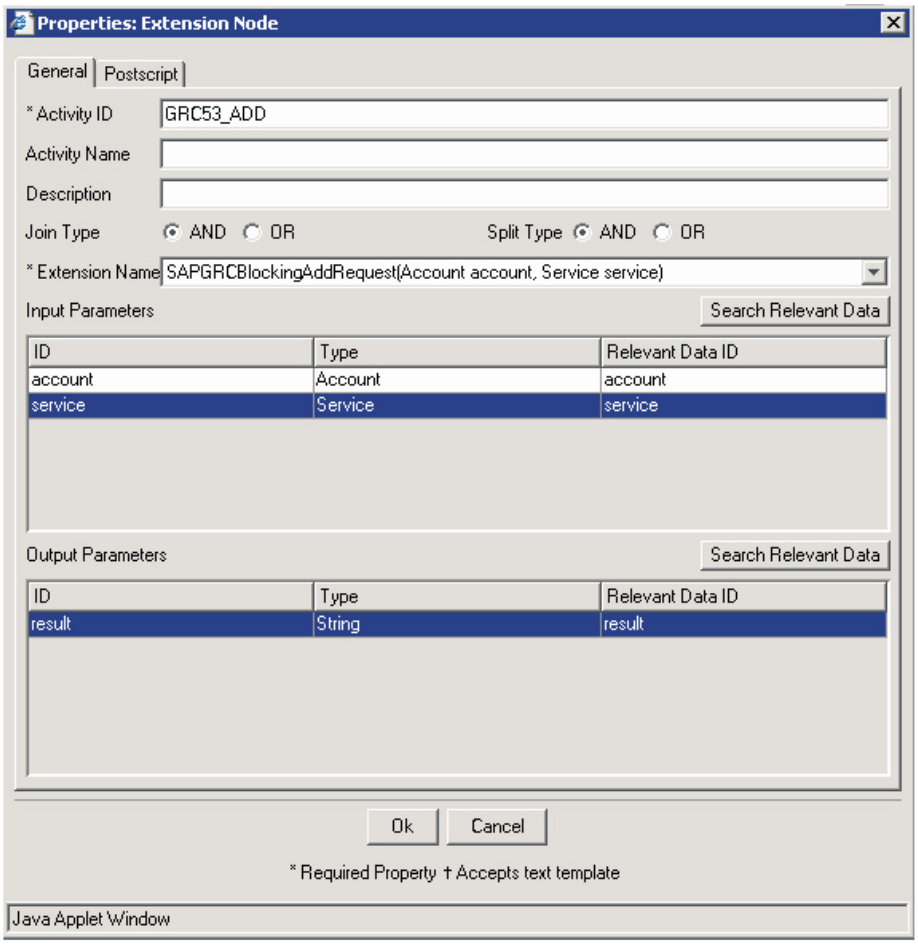
6. Add nodes to support SAP GRC Access Control 5.3.

a. Select one Extension node and connect it to the existing extensions as shown in the following screen capture:



b. Double click this extension to set the **ActivityID** to **GRC53_ADD** and **ExtensionName** to **SAPGRCBlockingAddRequest(Account account, Service service)**.

c. Click the **Search Relevant Data** button to find the relevant data for the Input Parameters and the Output Parameters.



d. Click **Ok** to save and close the popup window.

e. Double click the transition line between the **CHECK_GRC_VERSION** extension node and **GRC53_ADD** extension node to enter the following condition: `grcVersion.get()=="5.3"`.

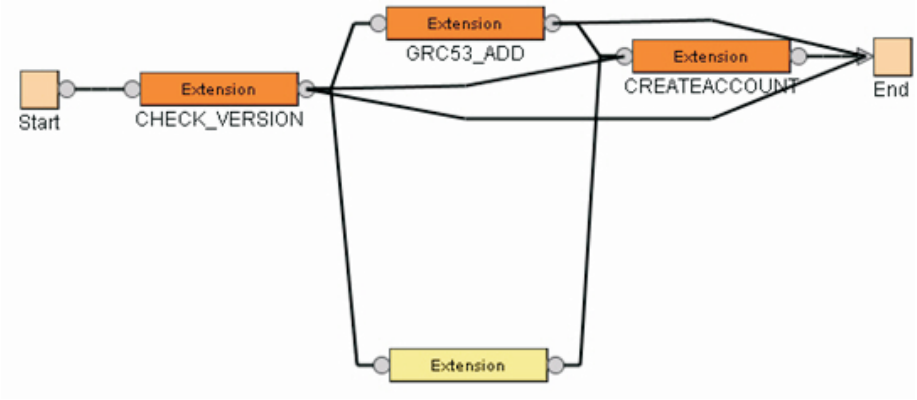
f. Connect the **GRC53_ADD** extension node to the **End** node with a transition line and enter the following condition: `activity.resultSummary!="SS"`

g. Click the **Update** button. The workflow extension should look similar to the following screen capture:

h. Click **Update** to save the current configuration.

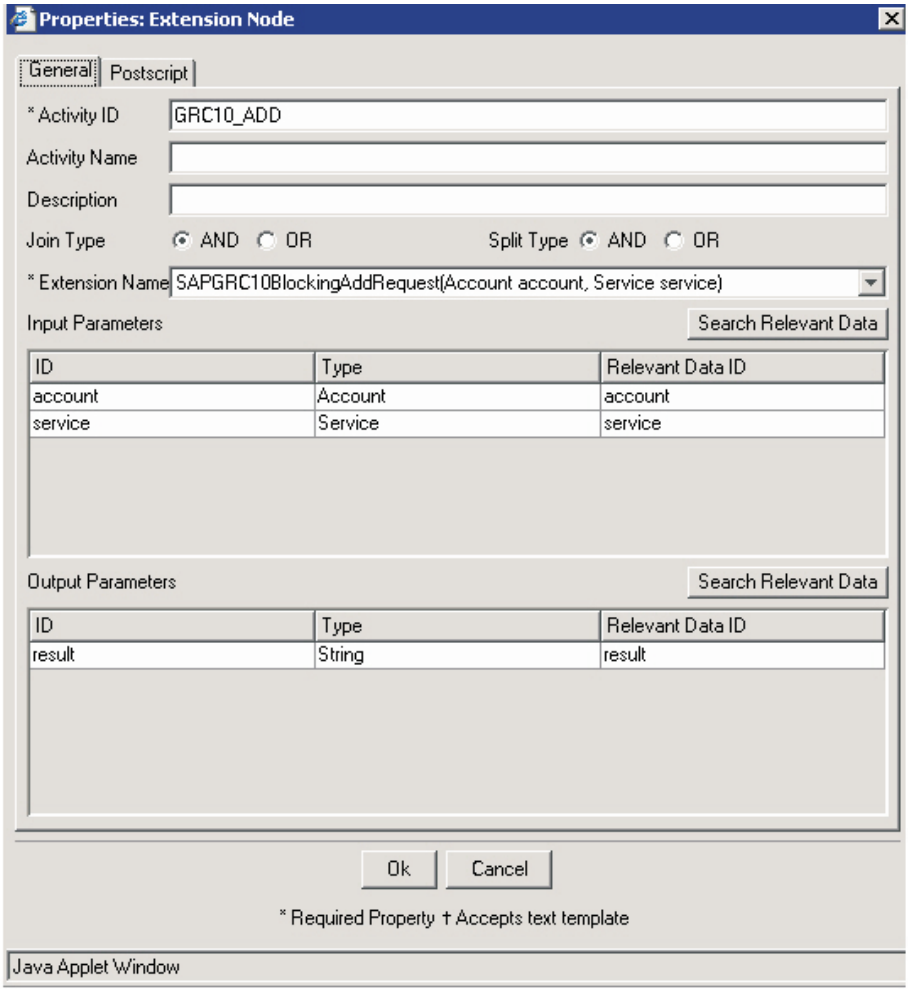
7. Add nodes to support SAP GRC Access Control 10.0.

a. Select one Extension node and connect it to the existing extensions as shown in the following screen capture:



b. Double click this extension to set the **ActivityID** to **GRC10_ADD** and **ExtensionName** to **SAPGRC10BlockingAddRequest(Account account, Service service)**.

c. Click the **Search Relevant Data** button to find the relevant data for the Input Parameters and the Output Parameters.

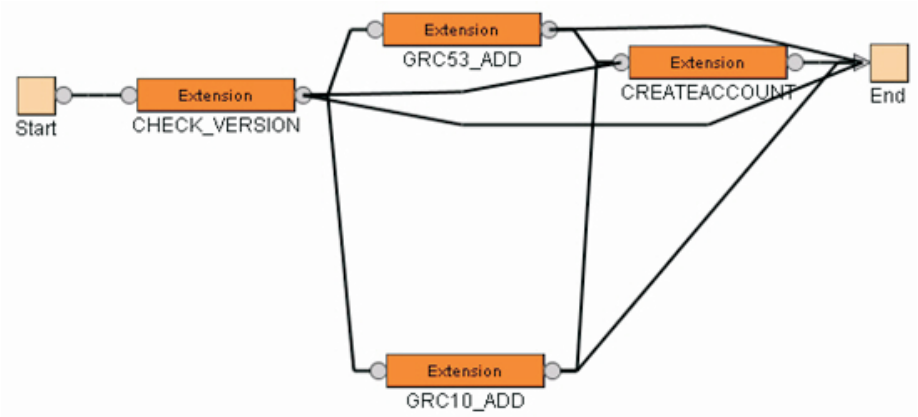


d. Click **Ok** to save and close the popup window.

e. Double click the transition line between the **CHECK_GRC_VERSION** extension node and **GRC10_ADD** extension node to enter the following condition: `grcVersion.get()=="10.0"`.

f. Connect the **GRC10_ADD** extension node to the **End** node with a transition line and enter the following condition: `activity.resultSummary!="SS"`

g. Click the **Update** button. The workflow extension should look similar to the following:



h. Click **Update** to save the current configuration.

8. SAP GRC Access Control 10.0 workflow extensions also support RiskAnalysis and UpdateAttributes workflow extensions. See "Configuring Access Request workflow extension" on page 30 and "Configuring Update Account Attributes workflow extension" on page 35 for details.

Verifying the SAP GRC AC Workflow components installation

If the integration is installed correctly, these components exist on the IBM Security Identity Manager server.

Table 12. SAP GRC Access Control Workflow and Notification components

Directory	Workflow component
WAS_HOME\AppServer\profiles*APP_SERVER*\installedApps*NodeCell*\ITIM.ear\	SAPGRC53Workflow.jar
app_web.war\WEB-INF\lib	SAPGRC10Workflow.jar
Notification_Component_HOME	jaas_login_was.conf runNotifierWAS7.bat runNotifierWAS7.sh SAPNotify.props
ITIM_HOME\data	workflowextensions.xml

Configuring reconciliation for the SAP NetWeaver adapter with SAP GRC Access Control integration

Due to limitations in the SAP GRC Access Control reconciliation capability, the adapter uses the SAP ABAP server as an account repository for reconciliation process.

As result, all attributes that are specific to SAP GRC Access Control will be lost during reconciliation because the SAP AS ABAP server will not recognize them. To avoid losing values of SAP GRC Access Control-specific attributes, the reconciliation operation must exclude all of the SAP GRC Access Control-specific attributes listed in Table 6 on page 13.

Chapter 5. Upgrading the integration

You can upgrade the Integration for SAP GRC Access Control to support SAP GRC Access Control 10.0 or 5.3.

Upgrade to support SAP GRC Access Control 10.0

To upgrade the integration to support SAP GRC Access Control 10.0, you must perform several tasks.

Follow these steps:

- "Importing the profile"
- "Creating an SAP NetWeaver GRC service"
- "Installing the SAP GRC Access Control 10.0 workflow extensions"
- "Configuring the SAP GRC Access Control 10.0 workflow extension" on page 50

Importing the profile

Obtain the `SapGRCNWProfile.jar` profile from the installation package and import the profile into IBM Security Identity Manager.

Creating an SAP NetWeaver GRC service

After the `SapGRCNWProfile.jar` has been imported into IBM Security Identity Manager successfully, update the attributes under the SAP GRC Service Attributes tab on the service form.

See "Creating an SAP NetWeaver GRC service" on page 9 for details on how to create a service and how to define those attributes on the SAP GRC Service Attributes tab.

To support the difference version of SAP GRC Access Control with the same profile, the * which used to indicate mandatory account attributes has been removed from the account form as these attributes are not necessary required for SAP GRC Access Control 10.0 support. Refer to Table 5 for full reference of supported account attributes.

Installing the SAP GRC Access Control 10.0 workflow extensions

Follow these steps to install the SAP GRC Access Control 10.0 workflow extension.

1. Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to add a workflow extension. For more information, see "Installing SAP GRC Access Control 10.0 workflow extensions" on page 27.
2. Copy `workflow\grc10\SAPGRC10Workflow.jar` from the installation package to the appropriate directory: *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`

   If the directory does not exist, create one.
3. Restart the IBM Security Identity Manager application from the WebSphere console, or restart the WebSphere server itself. After a successful restart, continue with configuration.

Configuring the SAP GRC Access Control 10.0 workflow extension

The SAP GRC Access Control 10.0 workflow extensions support Access Request, Risk Analysis and Update Account Attributes features by configuring the IBM Security Identity Manager workflow extension.

For more information, see "Configuring SAP GRC Access Control 10.0 workflow extensions" on page 29.

Upgrade to support SAP GRC Access Control 5.3 support

To upgrade the adapter to support SAP GRC Access Control 5.3, you must perform several tasks.

- "Import the profile"
- "Creating a SAP NetWeaver GRC service"
- "Installing SAP GRC Access Control 5.3 workflow extension"
- "Configuring SAP GRC Access Control 5.3 workflow extension" on page 51

Import the profile

Obtain the `SapGRCNWProfile.jar` profile from the installation package and import the profile into IBM Security Identity Manager.

Creating a SAP NetWeaver GRC service

After the `SapGRCNWProfile.jar` has been imported into IBM Security Identity Manager successfully, update the attributes under the SAP GRC Service Attributes tab on the service form.

See "Creating an SAP NetWeaver GRC service" on page 9 for details on how to create a service and how to define those attributes on the SAP GRC Service Attributes tab.

To support the difference version of SAP GRC AC with the same profile, the * which used to indicate mandatory account attributes has been removed from the account form as these attributes are not necessary required for SAP GRC Access Control 10.0 support. Refer to Table 5 for full reference of supported account attributes.

Installing SAP GRC Access Control 5.3 workflow extension

The workflow extension JAR file for SAP GRC Access Control 5.3 is renamed. You must perform two actions, if the SAP GRC Access Control 5.3 notification component is already configured before installing and configuring the new component.

1. Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to remove all SAP GRC Access Control 5.3 extensions.
2. Delete the `SAPGRCWorkflow.jar` file from the appropriate directory where it is installed: *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`

To install the new SAP GRC Access Control 5.3 workflow extension:

1. Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to add a workflow extension. See "Installing SAP GRC Access Control 5.3 workflow extensions" on page 19 for details.

2. Copy workflow\grc53\SAPGRC53Workflow.jar file from the installation package to the appropriate directory: *WEBSPHERE_HOME*\AppServer\profiles*SERVER_NAME*\installedApps*NODE_NAME*\ITIM.ear\app_web.war\WEB-INF\lib

   If the directory does not exist, create one.
3. Restart the IBM Security Identity Manager application from the WebSphere console, or restart the WebSphere server itself. After a successful restart, continue with configuration.

Configuring SAP GRC Access Control 5.3 workflow extension

The SAP GRC Access Control 5.3 workflow extensions support only the Access Request feature by configuring the IBM Security Identity Manager workflow extension.

See "Configuring SAP GRC Access Control 5.3 workflow extensions" on page 22 for details.

Installing and configuring SAP GRC Access Control 5.3 notification component

The workflow extension JAR file for SAP GRC Access Control 5.3 is renamed. You must perform two actions, if the SAP GRC Access Control 5.3 notification component is already configured before installing and configuring the new component.

1. Delete the SAPGRCWorkflow.jar file from the appropriate directory where it is installed: *WEBSPHERE_HOME*\AppServer\profiles*SERVER_NAME*\installedApps*NODE_NAME*\ITIM.ear\app_web.war\WEB-INF\lib
2. Delete the runNotifierWAS7 script.

For more information, see "Installing and configuring the notification component for SAP GRC Access Control 10.0" on page 36.

Chapter 6. Uninstalling the Integration for SAP GRC Access Control

To uninstall the integration you must remove the SAP GRC Access Control workflow extensions from IBM Security Identity Manager.

1. Log on to IBM Security Identity Manager, navigate to **Configure System** > **Manage Operations**. Remove the SAP GRC Access Control workflow extension configuration for the add, delete, modify, restore, and suspend operations for the SAP GRC NetWeaver Account type.
2. Delete `SAPGRC53Workflow.jar` or `SAPGRC10Workflow.jar` from the following directory *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`
3. Remove the following SAP GRC Access Control workflow activity from the *ITIM_HOME*`\data\workflowextensions.xml`
   - If using SAP GRC Access Control 5.3:

     ```
     SAPGRCNonblockingAddRequest
     SAPGRCBlockingAddRequest
     SAPGRCNonblockingModifyRequest
     SAPGRCBlockingModifyRequest
     SAPGRCNonblockingDeleteRequest
     SAPGRCBlockingDeleteRequest
     SAPGRCNonblockingSuspendRequest
     SAPGRCBlockingSuspendRequest
     SAPGRCNonblockingRestoreRequest
     SAPGRCBlockingRestoreRequest
     ```

   - If using SAP GRC Access Control 10.0:

     ```
     SAPGRC10NonblockingAddRequest
     SAPGRC10BlockingAddRequest
     SAPGRC10NonblockingModifyRequest
     SAPGRC10BlockingModifyRequest
     SAPGRC10NonblockingDeleteRequest
     SAPGRC10BlockingDeleteRequest
     SAPGRC10NonblockingSuspendRequest
     SAPGRC10BlockingSuspendRequest
     SAPGRC10NonblockingRestoreRequest
     SAPGRC10BlockingRestoreRequest
     SAPGRC10RiskAnalysisRequest
     SAPGRC10UpdateAccountAttributesExtension
     checkGRCVersion
     ```

4. Restart WebSphere Application Server.

To remove the SAP GRC Access Control workflow notification component:

1. Log on to IBM Security Identity Manager server.
2. Remove the following notification configuration files from *ITIM_HOME*`\bin` or the directory where it was installed.
   - `jaas_login_was.conf`
   - `runNotifierWAS7.bat` or `runNotifierWAS7.sh`
   - `SAPNotify.props`

Chapter 7. Runtime Problems

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Error messages	Problem descriptions
Workflow Activity Status Failed CTGIMA407E A configured workflow activity expected to receive 1 parameters, but 0 parameters were received for <workflow_name> workflow that was processing the <activity_name> activity.	If no further information is supplied in IBM Security Identity Manager request details, enable the 'Detail Logging' option on the SAP GRC Service Attributes tab then inspect the IBM Security Identity Manager trace.log file for the root cause. Possible reasons include; incorrect SAP GRC Access Control username/password, SAP GRC Access Control user is unauthorized, Access Control Submit Request URL is incorrect, IBM Security Identity Manager workflow is incorrectly configured, or SAP GRC Access Control rejected the request due to invalid data supplied on the request.
GRC Request failed : This is the message received from SAP GRC V10: ' msgNo= , msgType= , msgStatement= . '	Incorrect URL for the relevant SAP GRC Access Control 10.0 web service has been specified so no error message was returned by the SAP GRC Access Control web service call. Revise the SAP GRC Service Attributes Tab on the service form to correct the relevant URL.
Risk Analysis returns ERROR when no risk results are found. GRC Request failed : This is the message received from SAP GRC V10: ' msgNo=4 , msgType=ERROR , msgStatement=Invalid input or no data found for given input data. . '	This message is returned by the SAP GRC Access Control 10.0 risk analysis web service when no risk results are found. It receives no special handling by the IBM Security Identity Manager Adapter for SAP GRC Access Control 10.0. For more information on the problem see SAP Note “1692553 - Risk Analysis web service output is wrong when no risks”.
GRC Request failed. This is the message received from SAP GRC V10: ' msgNo=4 , msgType=ERROR , msgStatement=Invalid Item Name. . '	Indicates invalid configuration of either the SAP GRC Access Control connector (System Identifier) referenced on the IBM Security Identity Manager service form, or one or more of the roles specified on the request have not been imported correctly into IBM Security Identity Manager 10.0.
Activity status terminated.	Inspect IBM Security Identity Manager *trace.log*. Potential cause is IBM Security Identity Manager workflow misconfiguration such as missing relevant data.
Notification Failed SEVERE: File Not Found Exception during Connection: [java.io.FileNotFoundException: SAPNotify.props (The system cannot find the file specified.)]	`SAPNotify.props` file is missing. The `SAPNotify.props` file needs to be existed in the same location where the notifier script is being executed.
Notification Failed SEVERE: File Not Found Exception during Connection: [java.io.FileNotFoundException: \data\enRole.properties (The system cannot find the path specified.)]	Cannot locate the `enRole.properties` file. Define itim.home in the `SAPNotify.props` file. For example `itim.home=C:/Program Files/IBM/itim`
Notification Failed SEVERE: A value for the property itim.user was not found in SAPNotify.props	The user name to login to the Identity Manager server is missing. Define itim_user in the `SAPNotify.props` file.

Error messages	Problem descriptions
Notification Failed SEVERE: A value for the property itim.pswd was not found in SAPNotify.props	The password for the Identity Manager user is missing. Define itim_pswd in the `SAPNotify.props` file
Notification Failed SEVERE: A value for the property GRCUserName was not found in SAPNotify.props	The user name to login to SAP GRC Access Control system is missing. Define GRCUserName in the `SAPNotify.props` file.
Notification Failed SEVERE: A value for the property GRCPassword was not found in SAPNotify.props	The password for the SAP GRC Access Control user is missing. Define GRCPassword in the `SAPNotify.props` file.
Notification Failed SEVERE: A value for the property GRCStatusURL was not found in SAPNotify.props	The SAP GRC Access Control 10 Audit Logs Web Service URL is missing. Define the correct URL for the audit logs web service in the `SAPNotify.props` file. For example: `http://sapgrc10:8000/sap/bc/srt/ rfc/sap/ grac_audit_logs_ws/001/ grac_audit_logs_ws/ binding?sap-client=001`
Notification Failed SEVERE: Exception occurred during request lookup [(500) SRT: Unexpected failure in SOAP processing occurred: ("No Web service configuration for this access path: "/sap/bc/srt/rfc/sap/grac_audit_log_ws/001/ grac_aud"")]	Incorrect web service URL has been defined in the `SAPNotify.props` file. Verify the URL for the GRCNotifyURL property.
Notification Failed SEVERE: WSWS3938E: The message is enclos ebServicesFault faultCode: HTTP faultString: (401) Unauthorized faultActor: http://10.150.22.7:8000 faultDetail: null: WSWS3192E: Error: return code: (401) Unauthorized	Incorrect SAP GRC Access Control user password has been defined in the `SAPNotify.props` file. Verify the GRCPassword property.
Notification Failed SEVERE: Login Exception during Connection: [com.ibm.itim.apps.ITIMFailedLoginException: The information used to login is not correct.] com.ibm.itim.apps.ITIMFailedLoginException: The information used to login is not correct.	Incorrect Identity Manager user password has been defined in the `SAPNotify.props` file. Verify the itim.pswd property.
GRC Request failed : This message is received from SAP GRC V10: `' msgNo=4 , msgType=ERROR, msgStatement=Invalid request initiation system. .'`	An incorrect value has been supplied for the System Identifier on the GRC Service Attributes. Revise the value and correct the System Identifier to match the name of the relevant SAP connector in GRC 10.0.
GRC Request failed : `msgNo=, msgType= , msgStatement=Primary email address on the Communications tab is not in the correct format.`	The email address on the Communications tab needs to be input using a particular syntax. For more information about this format consult the “Special Attributes” section in the *SAP NetWeaver Adapter Installation and Configuration Guide*. The GRC 10.0 integration inserts the standard email address into the user information **email address** field as required by the GRAC_USER_ACCES_WS web service.

Appendix A. Support information

Use the following options to obtain support for IBM products:

- "Searching knowledge bases"
- "Obtaining a product fix" on page 58
- "Contacting IBM Support" on page 58

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for IBM Security Identity Manager. However, sometimes you need to look beyond the information center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

   Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Obtaining a product fix

A product fix might be available to resolve your problem.

About this task

You can get fixes by following these steps:

Procedure

1. Obtain the tools required to get the fix. You can obtain product fixes from the *Fix Central Site*. See http://www.ibm.com/support/fixcentral/.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.

Contacting IBM Support

IBM Support assists you with product defects.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

About this task

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
b. Open ISA.
c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix B. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager Information Center, and its related publications, are accessible.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for additional navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to utilize more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

Appendix C. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

Printed in USA

SC27-4414-00