


Reading Sample

This sample chapter covers the initial configuration of SAP Access Control. It provides step-by-step instructions for quickly checking the add-ons/plugins, activating applications and services, setting up connectors, configuring parameters, configuring multistage multipath (MSMP) workflows, and configuring the email engine for sending and receiving messages. These post-installation steps are usually a one-time requirement and don't require configuring multiple times.

-  **"Post-Installation Steps"**
-  **Contents**
-  **Index**
-  **The Authors**

Raghu Boddu

SAP Access Control The Comprehensive Guide

695 pages | 06/2023 | \$99.95 | ISBN 978-1-4932-2370-1

 www.sap-press.com/5636

Chapter 3

Post-Installation Steps

After installing the SAP Access Control add-on and its plug-in components, the next essential step is to perform the initial configuration. Configuring SAP Access Control is mandatory, as the solution cannot be utilized without configuration. This chapter will guide you through the post-installation process to set up the system for effective use.

This chapter provides post-installation support with step-by-step instructions starting from quickly checking the add-ons/plugin and performing the initial configuration, including activating the applications, setting up the connectors, configuring parameters, configuring multistage multipath (MSMP), etc. Note that post-installation steps are usually a one-time requirement and don't require configuring multiple times (like connector-specific configurations). In this chapter, we'll walk you through the steps for setting up SAP Access Control.

3.1 Quick Checks

Before you proceed further with the configuration, ensure that the following components are installed in your SAP Governance, Risk and compliance (SAP GRC) system:

- SAP NetWeaver 7.52 SPOO: Foundation application layer on SAP GRC system
- GRCFND_A v1200: Add-on installation on the SAP GRC system
- UIGRACO1 100: SAP Fiori UI component on frontend system (optional)
- SAP Enterprise Portal 7.x, versions 7.02 through 7.31 (optional)

The target systems should have the following components:

- GRCPINW v1200 or v1100 (SAP GRC NW PLUGIN), which provides SAP Access Control integration with non-human resources (HR) enterprise resource planning (ERP) functions
- GRCPERP v1100 (SAP GRC 10.1 Plug-in ERP), which provides SAP Access Control integration with HR functions in an ERP and also works for SAP GRC 12.0 solutions too

We recommend using the Software Provisioning Manager (for a new installation) or the Software Update Manager (for a system update) in combination with the maintenance planner to download, install, and update product versions.

3.2 Initial Configuration

Before starting with the configuration, note that configuration tasks are divided into three major phases, as detailed in Table 3.1.

Types of Configurations	Description	When Performed?
Initial configuration	Usually performed during the initial setup of the SAP Access Control system	One time
Connector specific	Can be a repetitive configuration whenever a new system is connected to an SAP Access Control system	When a requirement exists to add a new system to SAP Access Control
Component specific	For configuring the application according to business requirements, using a business requirement document (BRD) or a blueprint document as a base for the configuration	Almost one-time, unless a request arises from the business to change a functionality

Table 3.1 Types of Configuration in SAP Access Control

Since this chapter is specific to post-installation steps, various activities that must be performed as a part of the initial configuration are covered. Subsequent chapters will discuss connector-specific configuration and component specific configurations.

In this section, we'll outline the steps for the initial configuration of the SAP Access Control application, such as activating applications and services, Internet Communication Framework (ICF) services, Internet Communication Manager (ICM) services, business configuration (BC) sets, and SAP-delivered roles; defining business processes and subprocesses; and maintaining plug-in parameters and user exits.

3.2.1 Activating Applications and Services

The first step is activating the application. By default, the SAP Access Control, SAP Process Control, and SAP Risk Management applications are delivered with the GRCFND_A component (GRC Foundation ABAP).

To activate SAP Access Control, follow these steps:

1. Log on to the SAP Access Control system.
2. Execute Transaction SPRO.

3. Navigate to **SAP Reference IMG • Governance, Risk and Compliance • General Settings • Activate Applications In Client**.
4. If the table lacks entries, click the **New Entries** button. Then, add the **GRC-AC** app and select the **Active** checkbox, as shown in Figure 3.1.

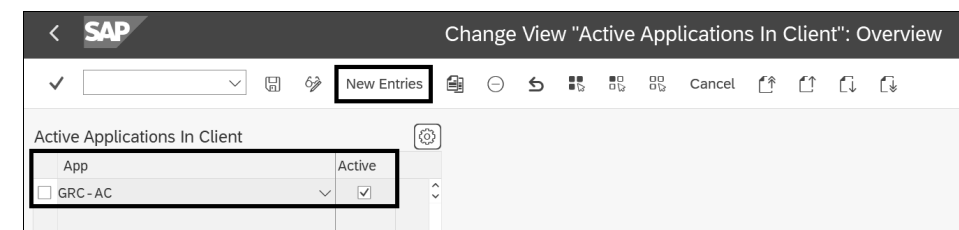


Figure 3.1 Activating Applications in the Client Configuration

5. Click the **Save** button to save the configuration.

With GRCFND_A, only GRC-AC can be utilized without any additional add-ons. To use GRC-PC or GRC-RM, you'll need to install the relevant add-ons/content. Also remember that licensing requirements are different for these applications.

Note

Application activation is a configuration setting in Transaction SPRO that must be captured in a transport request and imported into other systems in the landscape. This approach eliminates the need for administrators to perform the same configuration repetitively because settings are automatically applied to subsequent systems.

3.2.2 Activating Internet Communication Framework Services

The next step is to activate ICF services using Transaction SICF. ICF services include Web Dynpro or Open Data Protocol (OData) components that you must activate. These components are required for your web-based applications to work. Since SAP Access Control uses SAP Business Client screens (HTTP) or SAP Fiori screens (OData), a required step is to activate the respective services. Services related to SAP Access Control are inactive by default after an installation or an upgrade.

The three main ICF service groups that must be activated are **bc**, **public**, and **grc**. To activate these services, follow these steps:

1. Execute Transaction SICF.
2. Right-click the specific service node and click **Activate**, as shown in Figure 3.2.

Virtual Hosts / Services	Documentation	Reference Service
default_host	VIRTUAL DEFAULT HOST	
sap	SAP NAMESPACE; SAP IS OBLIGED NOT TO D...	
option	RESERVED SERVICES AVAILABLE GLOBALLY	
public	PUBLIC SERVICES	
* ap	Application Platform	
* bc	BASIS TREE (BASIS FUNCTIONS)	
* bpcweb	bpc 10.0 restful web services	
* bw	BW	
* bw4	BW4	
* EPM_BPC	EPM BPC	
* es	Enterprise Search	
* grc	SAP GRC (Governance, Risk, and Compliance) C...	
* gw	gateway subnode	
* iwbep	Business Suite Enablement node for Gateway	
* meData	meData synchronization Service	
* opu	OData for SAP Products	
* resources	Handling REST Services from StreamWork	

Figure 3.2 Transaction SICF Service Node Activation

3. When you choose **Activate**, you should see the options/buttons shown in Figure 3.3.

- **Yes**
Will activate only the selected service or node; subnodes are not activated.
- **Yes (with node)**
Will activate the selected service or node along with the services in subnodes, if any.
- **Info**
Shows information about the service.
- **Cancel**
Cancels the operation.

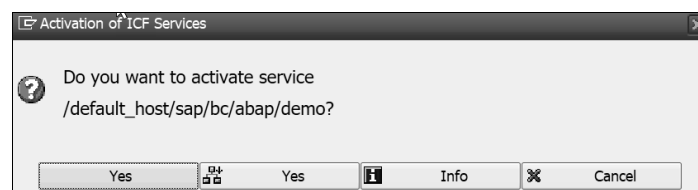


Figure 3.3 ICF Service Activation

4. To activate only the specific node, choose **Yes**. If you choose the second button (**Yes with the node icon**), the entire group will be activated, including the services available in subnodes too. If you have many nodes that need to be activated, we recommend clicking the second button.



Note

Once a service is activated, you can right-click it and choose **Test Service**, as shown in Figure 3.4.

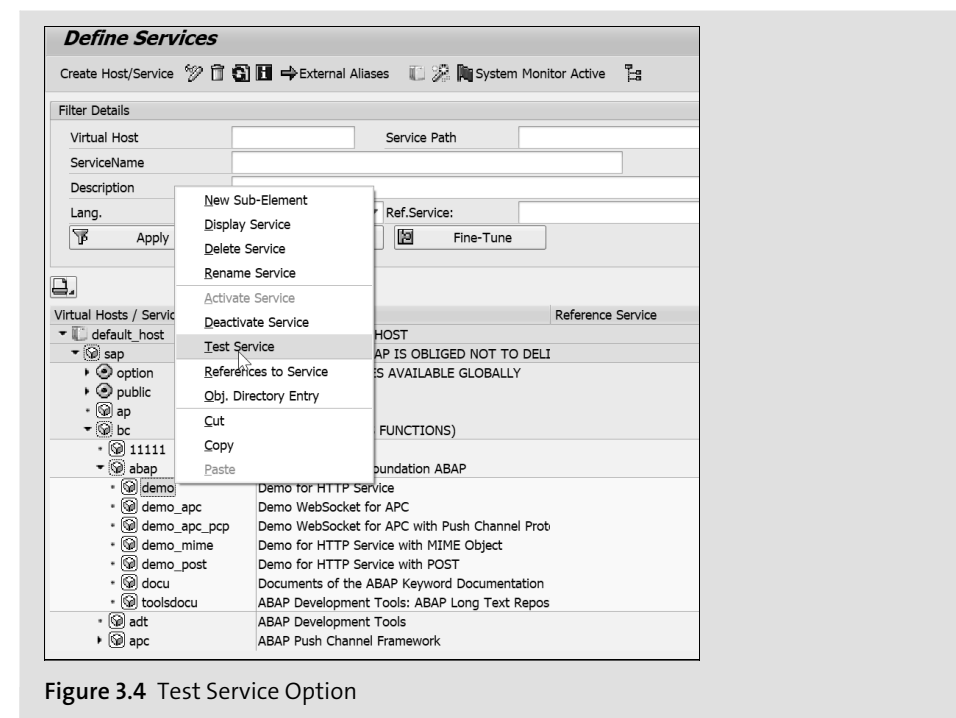


Figure 3.4 Test Service Option

Additionally, services can be deactivated by right-clicking and choosing the **Deactivate Service** option, as shown in Figure 3.5.

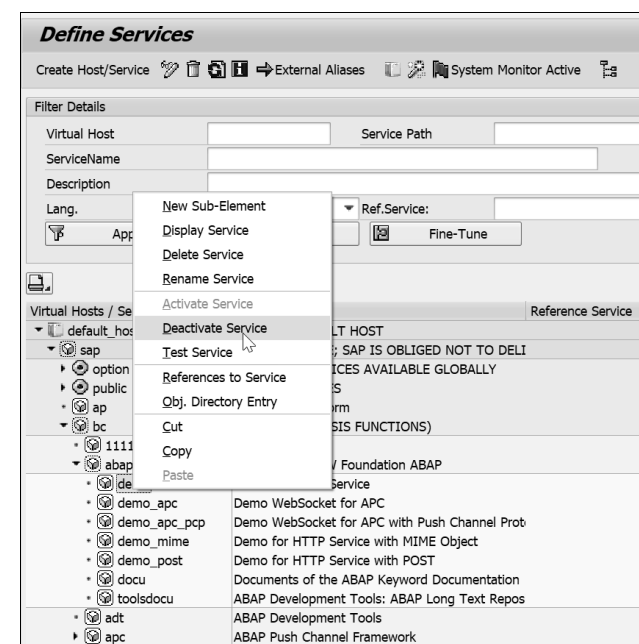


Figure 3.5 Deactivate Service Option

3.2.3 Activating Internet Communication Management Services

ICM is the component of the SAP NetWeaver Application Server that receives and sends web requests in HTTP, HTTPS, and Simple Mail Transfer Protocol (SMTP). During the initial configuration, the required services (i.e., HTTP, HTTPS, and SMTP) can be added manually with a timeout setting of 300 seconds (minimum).

To activate ICM services, follow these steps:

1. Log on to the SAP Access Control system.
2. Execute Transaction SMICM.
3. Click **Go to Menu** and click **Services** or press **Shift+F1**.
4. Click the **Service menu** option and click **Create**.
5. Maintain the **New Service Port** and **Protocol** fields, as well as other details, and click the **Create** button, as shown in Figure 3.6.
6. Once the services (**HTTP**, **HTTPS**, and **SMTP**) are created, you may proceed with the other configuration.

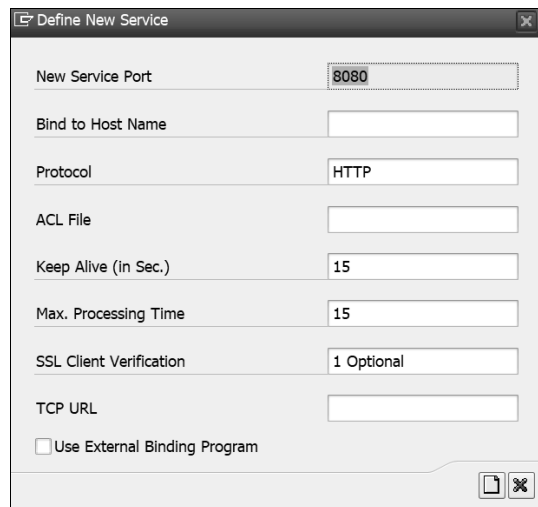


Figure 3.6 Creating a New Service

The services added manually in Transaction SMICM will be automatically deleted during a system restart. Thus, you should add them directly to the RZ10 profile parameters.

To add these parameters, follow these steps:

1. Log on to the SAP Access Control system.
2. Execute Transaction RZ10.
3. Select the **DEFAULT** profile from the **Profile** field.
4. Select the **Extended maintenance** radio button under **Edit Profile**.
5. Click **Change**, as shown in Figure 3.7.

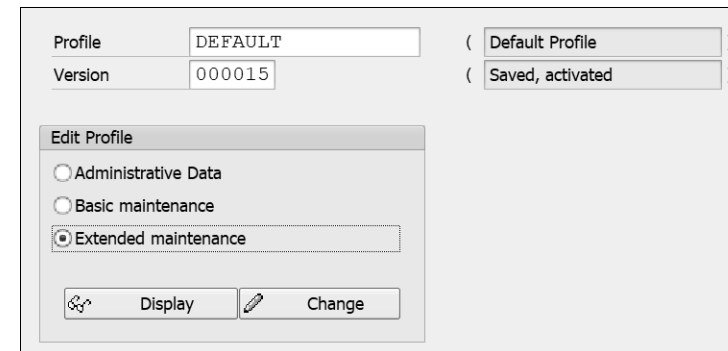


Figure 3.7 RZ10 Profile Parameters

6. Choose **OK** (checkmark icon) when prompted with a warning.
7. Click the **Create Parameter** button.
8. Enter "icm/server_port_0" in the **Parameter name** field or select from the list.
9. In the **Parameter val.** fields, enter "PROT=HTTP," "PORT=<port number>," "TIMEOUT=300," and "PROCTIMEOUT=300," as shown in Figure 3.8.
10. Click **Save** to save these changes.

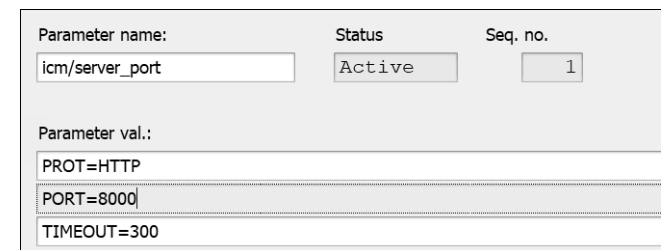


Figure 3.8 Service Entry in RZ10 Profile Parameters

Note

The parameter ICM/SERVER_PORT_<XX> must be added with the right values. For the port number, you may check with your infrastructure management/Basis teams since ports are opened/configured at the networking layer. Additionally, the TIMEOUT and PROCTIMEOUT parameter values should be at least 300 (seconds). However, you can use values greater than 300 as well. You should set this value based on your system resources.

11. Once the parameters are configured, you may need to reboot the SAP Access Control system to activate these changes.



**Note**

The email setup (configured in Transaction SCOT) should also be performed to set up SAP Access Control notifications.

3.2.4 Activating Business Configuration Sets

BC sets are prepackaged snapshots of customization settings that can be used as templates and that can be activated quickly. SAP shares lists of relevant customizations in BC sets. When a BC set is created, the values from the original customizing tables are copied into BC sets. When you activate this BC set in another system, the values stored in the BC set are copied to corresponding customizing tables of the system. This approach makes customization easy.

SAP Access Control 12.0 BC sets start with “GRAC,” and around 30 BC sets are relevant to SAP Access Control. Table 3.2 contains the complete list of available BC sets.

Name of the BC Set	Description
GRAC_ACCESS_REQUEST_APPL_MAPPING	BC Set for Access Request - Application Function mapping
GRAC_ACCESS_REQUEST_EUP	BC Set for Access Request - End User Personalization
GRAC_ACCESS_REQUEST_PRIORITY	BC Set for Access Request - Priority
GRAC_ACCESS_REQUEST_REQ_TYPE	BC Set for Access Request - Request Type
GRAC_DT_REQUEST_DISPLAY_SECTIONS	Simplified Access Request Display Sections
GRAC_DT_REQUEST_FIELD_LABELS	Simplified Access Request Field Labels
GRAC_DT_REQUEST_PAGE_SETTINGS	Simplified Access Request Page Settings
GRAC_RA_RULESET_COMMON	Rule Set for Common rules
GRAC_RA_RULESET_ISU_COMMON	ISU Ruleset Common
GRAC_RA_RULESET_JDE	BC Set for AC Rules for JDE
GRAC_RA_RULESET_ORACLE	BC Set for AC Rules for ORACLE
GRAC_RA_RULESET_PSOFT	BC Set for AC Rules for PeopleSoft
GRAC_RA_RULESET_S4HANA_ALL	S4HANA and Fiori Apps Both
GRAC_RA_RULESET_S4HANA_CORE	S4HANA Core Ruleset
GRAC_RA_RULESET_S4HANA_FIORI	S4HANA Ruleset for Fiori Apps Only

Table 3.2 BC Sets for SAP Access Control 12.0

Name of the BC Set	Description
GRAC_RA_RULESET_SAP_APO	BC Set for AC Rules - SAP APO
GRAC_RA_RULESET_SAP_BASIS	BC Set for AC Rules - SAP BASIS
GRAC_RA_RULESET_SAP_CRM	BC Set for AC Rules - SAP CRM
GRAC_RA_RULESET_SAP_ECCS	BC Set for AC Rules - SAP ECCS
GRAC_RA_RULESET_SAP_HANA	BC Set for AC Rules - SAP HANA
GRAC_RA_RULESET_SAP_HR	BC Set for AC Rules for SAP HR
GRAC_RA_RULESET_SAP_ISU	SAP IS-Utilities Rule Set
GRAC_RA_RULESET_SAP_NHR	BC Set for SAP R3 less HR BASIS
GRAC_RA_RULESET_SAP_R3	BC Set for AC Rules for SAP R3
GRAC_RA_RULESET_SAP_SRM	BC Set for AC Rules for SAP SRM
GRAC_ROLE_MGMT_LANDSCAPE	BC Set for Business Roles Landscape
GRAC_ROLE_MGMT_METHODODOLOGY	BC Set for Role Management Methodology Process and Steps
GRAC_ROLE_MGMT_PRE_REQ_TYPE	BC Set for Role Management Pre-Requisite Types
GRAC_ROLE_MGMT_ROLE_STATUS	BC Set for Role Management Role Status
GRAC_ROLE_MGMT_SENTVITY	BC Set for Role Management Sensitivity Level
GRAC_ROLE_SEARCH_CONFIGURATION	Role Search Attributes Configuration
GRC_MSMP_CONFIGURATION	BC Set for MSMP Workflow Configuration
GRAC_SPM_CRITICALITY_LEVEL	Criticality Level

Table 3.2 BC Sets for SAP Access Control 12.0 (Cont.)

Note

You may find other BC sets in the list. However, only the BC sets that start with “GRAC” are relevant for SAP Access Control.

You are not required to activate all the BC sets. For example, if you’re not connecting to a JD Edwards system, you can skip the activation of the GRAC_RA_RULESET_JDE BC set. While activating ruleset-related BC sets, you should consult all the stakeholders and activate only the relevant BC sets.

A BC set can be activated via Transaction SCPR20. Enter the **BC Set** name (or select from the list) and click the **Activate** button or press **[F7]**, as shown in Figure 3.9.

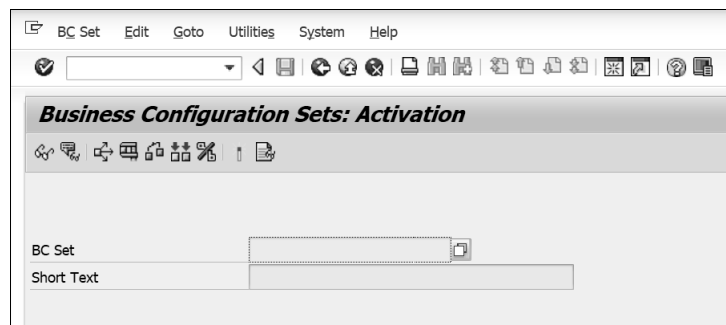


Figure 3.9 BC Set Activation

On the **Activation Options** screen, select the **Overwrite All Data** radio button under the **Overwrite Data** heading. Choosing this option will overwrite previous activations. If you're activating a specific BC set for the first time, you may choose any of these options. Further, choose the **Default mode (Recommended)** radio button under the **Select Activation Mode** heading and click **Execute**. Figure 3.10 shows the options for BC set activation.

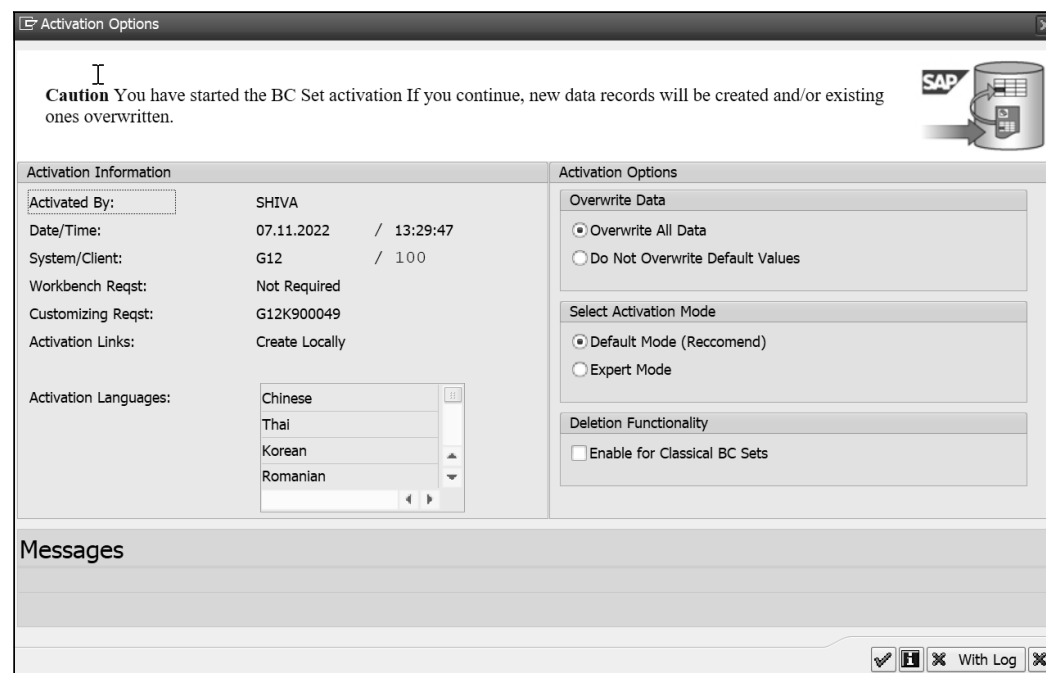


Figure 3.10 BC Set Activation Options

Once activated, activation logs are available that detail information about the activation. Click the **View logs** button or press **Ctrl+F2** to verify the logs. In the logs, you may notice various status icons along with descriptions.

Table 3.3 lists the icons you'll see in the logs and the purpose of each.

Icon	Color	Purpose
	Green	Activation is successful; no issues have arisen.
	Yellow	Activation is successful but with warnings.
	Red	Activation is unsuccessful.
	Information	Additional information to review exists.

Table 3.3 BC Set Activation Status Color Codes

A line item with a red icon/entry means that an issue with the activation has arisen. We recommend you identify the issue, resolve it, and proceed further. Note that the activation remains incomplete until the activation returns all green/all yellow log entries. Line items in yellow can be reviewed, but they are not the showstoppers. Figure 3.11 shows an activation log with various activation codes.

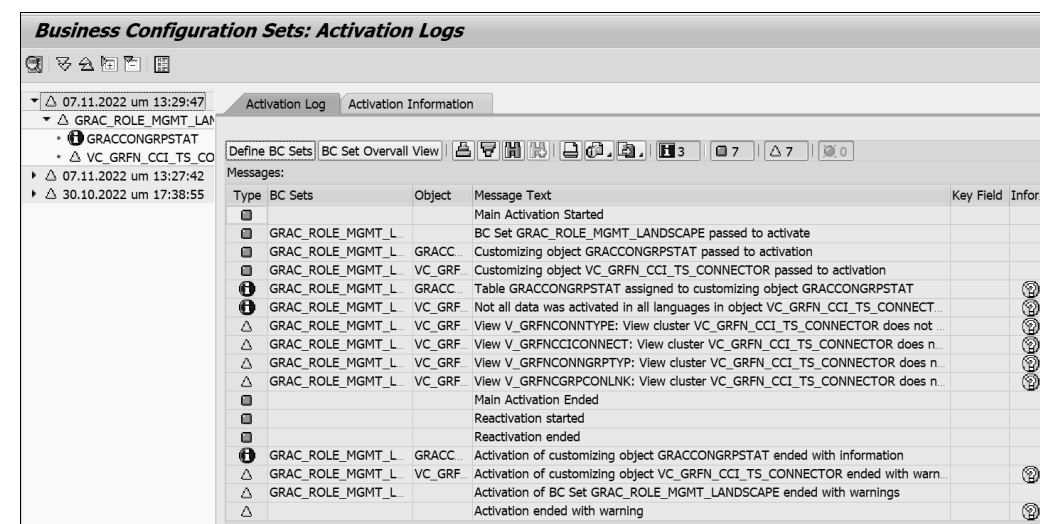


Figure 3.11 BC Set Activation Log

The other buttons on the **Business Configuration Sets: Activation Logs** screen can be used as required. Table 3.4 describes the functionalities of each button.



Button	Shortcut	Icons	Functionality
Overall View	F6		Shows information about the BC set, including tables and configurations that it will update.
Display Documentation	Ctrl + F1		Displays the associated documentation.
Where-used List	Ctrl + F6		Displays the other BC sets where the current BC set is used.
Consistency Check	Shift + F1		Consistency check to validate the BC set; provides an overview of the consistency among objects, what can be activated, and any potential issues.
Key conflict check	Ctrl + Shift + F12		Checks if any key conflicts with the BC set exist.
Compare with customizing table	Ctrl + F9		Compares BC sets with customizing tables.
BC Set/BC Set Comparison	Ctrl + F7		Can be used to compare two BC sets. This tool is useful when you're not sure which BC set to activate.
Activate BC Set	F7		This option will activate the BC set and fill in the customization tables with the respective data.
Activation Logs	Ctrl + F2		Shows the logs of both previous and current activations.

Table 3.4 Additional Options for BC Set Activation

However, you can capture the activation in a transport request or activate them individually in the respective systems. When BC sets are activated in the development system, configuration settings are automatically carried out and saved in transport requests. (You'll need authorization to create/capture changes in transport requests.) Transport requests resulting from the BC set activation are then imported into the quality assurance or production system.

Note

You must activate each BC set separately.

**3.2.5 Maintaining Plug-In Parameters**

Once the plug-in components are installed, namely, the non-HR component GRCPINW and the optional HR component GRCPERP, the next step is maintaining the plug-in parameters. Make sure you maintain the parameters listed in Table 3.5 in each plug-in system.

Parameter	Parameter Description	What to Maintain?
1000	Maintain Plug-in Connector	The local Remote Function Call (RFC) connection (i.e., the RFC created for the plug-in system)
1001	Maintain GRC Connector	The RFC connection created for the SAP Access Control system

Table 3.5 Plug-In System Parameters for SAP GRC and Plug-In Connectors

Note

You might need to maintain additional parameters related to the SAP Access Control components. More details about these parameters are provided in the various component chapters.

**3.2.6 Maintaining Plug-In (User Exit) Settings**

You'll also need to maintain user exits to enable the risk terminator option. User exit settings are required to utilize the risk terminator in role maintenance (Transaction PFCG) and user management (Transactions SU01, SU10, and SU12). The risk terminator enables real-time risk analysis while making changes to role authorizations or role assignments in a plug-in system.






To maintain these user exists settings, follow these steps:

1. Log on to the plug-in (backend SAP ERP or SAP S/4HANA) system.
2. Execute Transaction SPRO.
3. Navigate to **SAP Reference IMG • Governance, Risk and Compliance (Plug-In) • Access Control • Maintain User Exists for Plug-In Systems**.
4. Click the **New Entries** button and add the user exists listed in Table 3.6, as shown in Figure 3.12.

Name	Value to Set	Text
SAP_AFTER_PROF_GEN	/GRCP1/GRIA_AFTER_PROF_GEN	Function Module PRGN_EXIT_AFTER_PROFGEN (Default)
SAP_BEFORE_PROF_GEN	/GRCP1/GRIA_BEFORE_PROF_GEN	Function Module PRGN_EXIT_BEFORE_PROFGEN (Default)
SAP_EXIT_USERS_SAVE	/GRCP1/GRIA_EXIT_USERS_SAVE	Function Module PRGN_EXIT_USERS_SAVE (Default)
SAP_SINGLE_USERPROF	/GRCP1/GRIA_SINGLE_USERPROFS	NO (default), YES or X will make it so that the system does not display the SAP menu on the easy access screen (refer to SAP Note 380029 for more information)

Table 3.6 User Exit Parameters and Values

Change View "Set Values for the Session Manager / Profile Generator":

New Entries     

Set Values for the Session Manager / Profile Generator		
Name	Value to be set	Text
SAP_AFTER_PROF_GEN	/GRCP1/GRIA_AFTER_PROF_GEN	Function Module PRGN_EXIT_AFTER_PROFGEN (Default)
SAP_BEFORE_PROF_GEN	/GRCP1/GRIA_BEFORE_PROF_GEN	Function Module PRGN_EXIT_BEFORE_PROFGEN (Default)
SAP_EXIT_USERS_SAVE	/GRCP1/GRIA_EXIT_USERS_SAVE	Function Module PRGN_EXIT_USERS_SAVE (Default)
SAP_GRC_COLL_ROLE	/GRCP1/GRIA_SINGLE_USERPROFS	
SAP_SINGLE_USERPROF	/GRCP1/GRIA_SINGLE_USERPROFS	Function Module PRGN_EXIT_SINGLE_USERPROF (Default)

Figure 3.12 User Exit Entries for Risk Terminator

5. Click **Save** once all the user exit entries are maintained.



Note

This configuration can be skipped if the risk terminator is not configured. The risk terminator is an optional configuration. Risk terminator configuration is detailed in Chapter 5, Section 5.9.

3.2.7 Activating SAP-Delivered Roles

For SAP Access Control, the roles listed in Table 3.7 are delivered with the SAP Access Control component. These roles can be utilized directly, or you may copy them into Z/Y namespace roles.

Role Name	Purpose of the Role
SAP_GRAC_ACCESS_APPROVER	Provides the ability to approve access requests in SAP Access Control. All approvers (i.e., managers, role owners, risk owners, etc.) should have this role assigned.
SAP_GRAC_ACCESS_REQUEST_ADMIN	Provides authorization to administer the access request configuration. An SAP Access Control admin should have access to this role.
SAP_GRAC_ACCESS_REQUESTER	Provides end users the ability to access the access request page.
SAP_GRAC_ALERTS	Provides authorization to generate, clear, and delete segregation of duties (SoD) alerts.
SAP_GRAC_ALL	Provides super admin authorization to maintain the SAP Access Control application.
SAP_GRAC_BASE	Provides base access to utilize the SAP Access Control application. Should be assigned to all SAP Access Control users.
SAP_GRAC_CONTROL_APPROVER	Provides authorization to create mitigation controls, approve and assign mitigation controls, and review alerts. Users with this role can also perform risk analysis.
SAP_GRAC_CONTROL_MONITOR	Provides authorization to assign a mitigation control to a risk and perform risk analysis.
SAP_GRAC_CONTROL_OWNER	Provides authorization to create and manage mitigation controls.
SAP_GRAC_DISPLAY_ALL	Provides authorization to access all SAP Access Control objects. This role can be assigned to provide display-only access, for example, for auditors who need to validate SAP Access Control objects.
SAP_GRAC_END_USER	Provides authorization to access the end user home page. Assigning this role will limit the authorization to specific work items in the SAP Business Client page. This role is assigned to SAP Access Control guest users (such as EUHOME, etc.).
SAP_GRAC_FUNCTIONAL_APPROVER	Provides authorization to approve a function for workflow.
SAP_GRAC_NWBC	Provides authorization to view the SAP Access Control information architecture in SAP Business Client. Usually assigned to all the users in the SAP Access Control system.

Table 3.7 SAP Standard Roles and Their Purposes

Role Name	Purpose of the Role
SAP_GRAC_REPORTS	Provides authorization to execute all the SAP Access Control reports under the Reports & Analytics tab. Usually assigned to the key business teams.
SAP_GRAC_RISK_ANALYSIS	Provides authorization to perform risk analysis at both the user level and the role level. Usually assigned to the key users such as business process owners, line managers, etc.
SAP_GRAC_RISK_OWNER	Provides authorization to maintain risks and perform risk analysis.
SAP_GRAC_ROLE_MGMT_ADMIN	Provides authorizations to maintain Business Role Management component configurations. Usually assigned to administrators.
SAP_GRAC_ROLE_MTMT_DESIGNER	Provides authorization to design roles using the Business Role Management component.
SAP_GRAC_ROLE_MGMT_ROLE_OWNER	Provides authorization to act as a role owner for various roles in Business Role Management. The role owner can be either a content approver or an assignment approver. In Business Role Management, the approval goes to the respective owner. However, the role owner should also have the access approver role if the workflow has the role owner stage.
SAP_GRAC_ROLE_MGMT_USER	Provides authorization to roles as a role management business user.
SAP_GRAC_RULE_SETUP	Provides the ability to define access rules. Users with this access can define functions and risks and generate rulesets.
SAP_GRAC_SETUP	Provides the ability to set up the SAP Access Control application.
SAP_GRAC_SPM_FFID	Helps to identify firefighter IDs (FFIDs). During owner and controller maintenance, the FFIDs with this role will be pulled automatically. Further, this role should be maintained in parameter 4010 (FFID role name).
SAP_GRAC_SUPER_USER_MGMT_ADMIN	Provides the ability to administer the Emergency Access Management application. Users with access to this role can assign owners and controllers, create reason codes, generate logs, etc.
SAP_GRAC_SUPER_USER_MGMT_CNTLRL	Provides Emergency Access Management controller authorization. Users with this role can review the logs generated based on the review settings.

Table 3.7 SAP Standard Roles and Their Purposes (Cont.)

Role Name	Purpose of the Role
SAP_GRAC_SUPER_USER_MGMT_OWNER	This role provides the ability to manage FFIDs as an FFID owner. Firefighter owners can assign IDs to firefighters and controllers.
SAP_GRAC_SUPER_USER_MGMT_USER	This role provides authorization to access FFIDs assigned to the users. Users with this access can go to the Emergency Access Management launchpad.

Table 3.7 SAP Standard Roles and Their Purposes (Cont.)

These SAP-delivered roles can be used directly by generating profiles. Profiles can be generated individually using Transaction PFCG or en masse using Transaction SUPC, as shown in Figure 3.13.

Roles: Mass generation of profiles

Which roles do you want to output?

Roles with Non-Current Profiles
 Also Roles to Be Compared
 Also Roles with no Authorization Data
 All Roles
 Roles with Current Profiles for New Generation

Additional restrictions

Role: SAP_GRAC_DISPLA.. to [] **Multiple Option**

Last changed by: [] to []

Presentation in the list

Display Data When Created and Changed
 Display Role Texts

Generate all profiles to be generated?

Generate automatically

Figure 3.13 Transaction SUPC: Generating Mass Roles

To generate roles en masse, follow these steps:

1. Execute Transaction SUPC.
2. Choose the **All Roles** radio button under the **Which roles do you want to output?** heading.
3. Under **Additional restrictions**, for the **Role** selection, enter the individual role name, or click the **Multiple Option** button and paste all the roles listed in Table 3.7.
4. Select the **Generate automatically** checkbox under the **Generate all profiles to be generated?**
5. Click **Execute**.

As an alternative, standard roles can be copied into Z or Y roles. Since in SAP you cannot copy roles en masse, you'll need to copy roles individually.

To complete this task, follow these steps:

1. Log on to SAP Access Control.
2. Execute Transaction PFCG.
3. On the **Role Maintenance** screen, for the **Role** field, enter the name of the role to be copied or select it by pressing **F4**.
4. Press **Enter** to confirm that the role exists.
5. Click the **Copy** button or press **Shift + F11**, as shown in Figure 3.14.

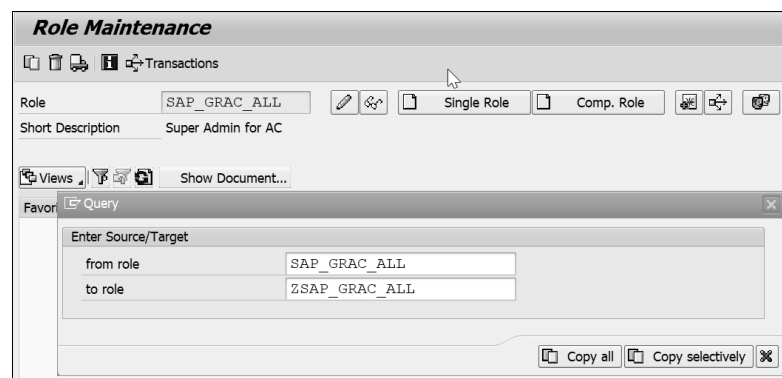


Figure 3.14 Copying a Role

6. In the **Query** popup window, enter a new role name.
7. Once the role has been copied, you'll be returned to the original **Role Maintenance** screen where you'll see the name of your new role.

The new role now can be changed to meet your business requirements and saved. Changes must be captured in a transport request to further move them to your quality and production environments.

3.2.8 Defining Business Processes and Subprocesses

As a part of the initial configuration, you must set up business processes, subprocesses, and functional areas. These independent elements are used in multiple scenarios by all components of SAP Access Control.

To set up the business subprocess, you must create the business process first by following these steps:

1. Execute Transaction SPRO.
2. Navigate to **SAP Reference IMG • Governance, Risk and Compliance • Access Control • Maintain Business Process and Subprocesses**.

3. Click the **New Entries** button and, as shown in Figure 3.15, add values to the **Business Process** and **Business Process Description** columns.

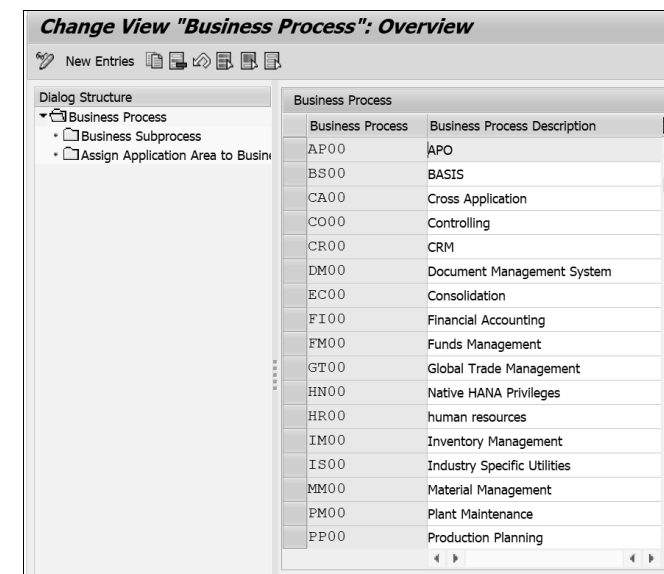


Figure 3.15 Creating a Business Process

4. Once business processes are created, to add a business subprocess, select a business process and double-click **Business Subprocess**.
5. Click the **New Entries** button and add values to the **Subprocess** and **Description** columns, as shown in Figure 3.16.

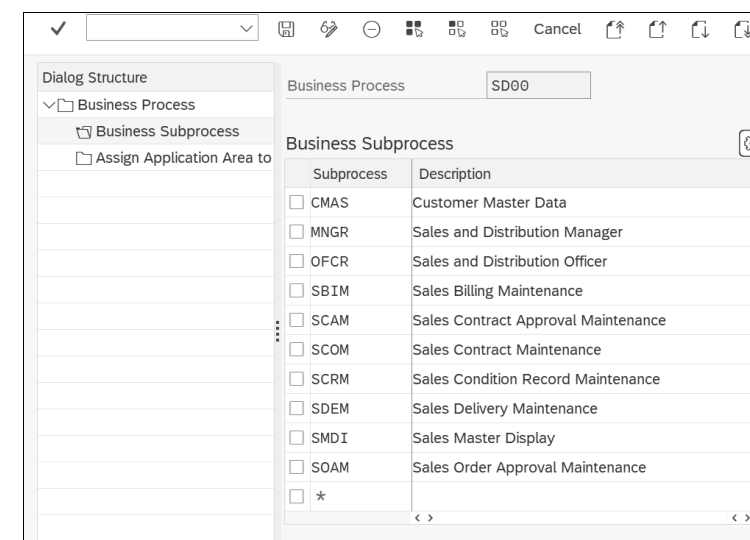


Figure 3.16 Business Subprocesses

6. These steps must be repeated to define all the necessary business subprocesses for all your business processes.

3.3 Multistage Multipath Workflow Initial Configuration

Once the basic configuration is performed, the other major configuration task is to set up MSMP workflows. Before starting with the MSMP workflow configuration, make sure that you've met the following prerequisites:

- The WF-BATCH user is available with the necessary authorizations.
- Background work processes should be increased to accommodate the background jobs that are required.

The WF-BATCH user can be created as a SYSTEM type user with following authorizations:

- Profile SAP_ALL
- Profile SAP_NEW
- Role SAP_BC_BMT_WFM_SERV_USER
- Authorization objects S_RFC, S_RFCACL and S_RFC_TT

If the authorization objects are not available in any of the standard roles, you should create a custom Z or Y role and assign it to the WF-BATCH user. This user ID will be utilized in the next set of configurations.

The next step is to ensure that there are sufficient background work processes. Check the available work processes in RZ10 profile parameters. The parameter RDISP/WP_NO_BTC should be maintained with the correct value.

In this section, we'll provide step-by-step instructions for configuring MSMP workflows in SAP Access Control. Topics include automated workflow configuration, classifying workflow tasks as general tasks, scheduling workflow background jobs, customizing tasks specific to your needs, activating event linkages, assigning agents to tasks, and defining number ranges for access requests. By following these instructions, you can ensure a successful configuration of MSMP workflows in SAP Access Control.



Note

We highly recommend you consult the Basis team before changing parameter values since the configuration depends on many other parameters. Once the parameter is maintained correctly, the next step is to proceed with the automatic workflow configuration.

3.3.1 Performing Automatic Workflow Configuration

Automatic workflow configuration is a great tool for carrying out the activities necessary for setting up the workflow automatically. It shows the current status of each step

and guides an administrator to set up the configuration in the right order. Automatic workflow customizing is made up of several areas. Each area features a status icon for administrators to easily understand the pending activities. By default, these items will be displayed in red, and upon customization, they will be updated with a checkmark (v).

To perform the automatic workflow configuration, log on to SAP Access Control, execute Transaction SPRO, and navigate to **SAP Reference IMG • Governance, Risk and Control • General Settings • Workflow • Perform Automatic Workflow Customizing** option, as shown in Figure 3.17. Alternatively, execute Transaction SWU3.

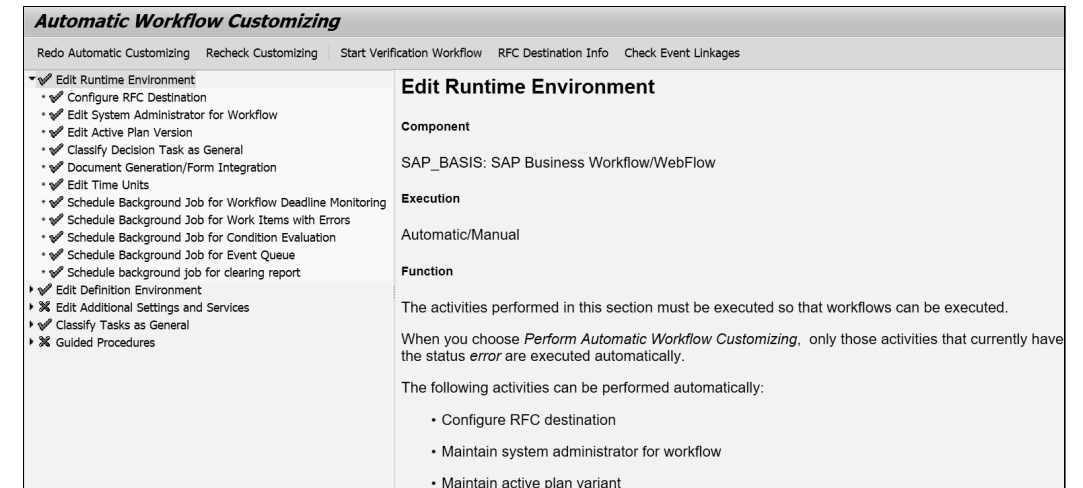


Figure 3.17 Automatic Workflow Customizing

The **Automatic Workflow Customizing** screen will have five event sets, namely, the following:

- **Edit Runtime Environment**
In this set, all activities are executed that are necessary for the execution of workflows.
- **Edit Definition Environment**
In this set, activities are executed that are necessary for the smooth modeling of workflows.
- **Edit Additional Settings and Services**
In this set, you'll find activities that are needed for specific special functions of a workflow.
- **Classify Tasks as General**
This set is used to define tasks that are not specific to any particular workflow. When tasks are classified as general, they can be used in any workflow, making it easier to create new workflows and manage tasks across multiple workflows. This option allows administrators to create a set of reusable tasks for numerous workflows, instead of creating new tasks each time a new workflow is created.

■ Guided Procedures

This set involves executing process templates on the SAP Business Workflow engine. For this task, the address of the SAP Gateway server must be specified for the guided procedures runtime to establish a connection. Standard tasks for process templates can be either predefined or generated to correspond with guided procedure activities, with predefined tasks declared in task group TG77200003.

Right-click an event and choose **Redo Automatic Customizing**, as shown in Figure 3.18.

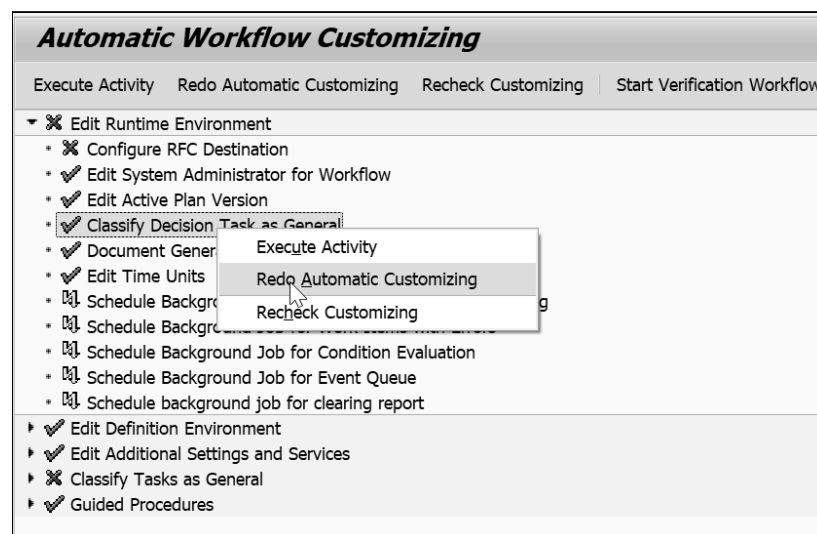


Figure 3.18 Performing Automatic Customization

If required to maintain any values, the right side of the screen will guide you through the requirements. Once the configuration is set, the event option will be displayed with a green checkmark .

The **Configure RFC Destination** and **Edit System Administrator for Workflow** events under **Edit Runtime Environment** require manual input. In this configuration, you may need to create a logical destination for use by the MSMP workflow. If automatic customization cannot create an RFC destination, make sure you follow these steps:

1. Log on to SAP Access Control.
2. Execute Transaction SM59.
3. Click **Create**.
4. In the **RFC Destination** field, enter "WORKFLOW_LOCAL_<Client>."
5. In the **Connection Type** field, enter "L" (**Logical Destination**).
6. Maintain the **Description 1** field, as shown in Figure 3.19.
7. Now, go to the **Logon & Security** tab.

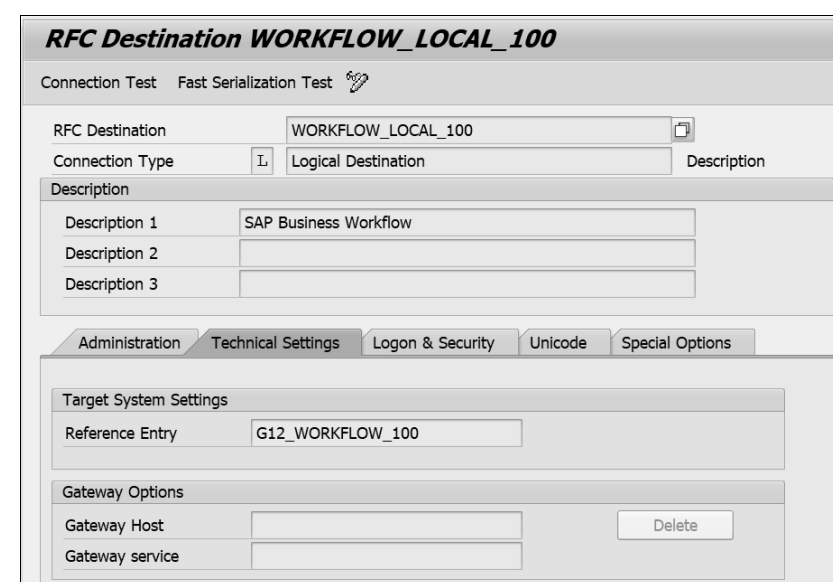


Figure 3.19 RFC Destination Definition

8. Enter a client number in the **Client** field, Then, for the **User name** field, enter "WF-BATCH" and, for the **PW Status** (password status) field, enter "is initial," as shown in Figure 3.20.

9. Click **Save**.

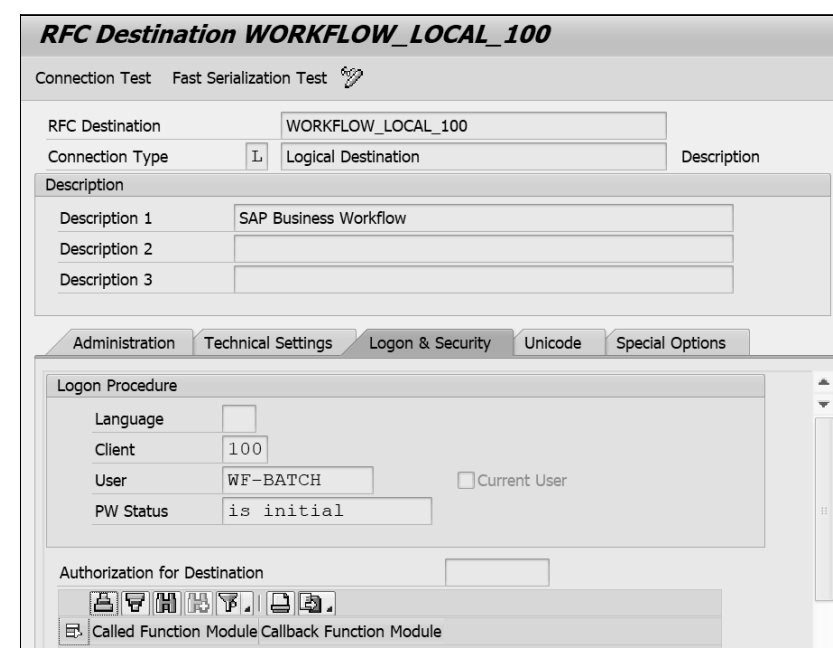


Figure 3.20 Logon & Security Tab: WF-BATCH User Update

Alternatively, clicking the **Setup Destination** button will invoke the RFC maintenance screen automatically.

Once the RFC is set up, right-click **Configure RFC Destination** and choose **Execute Activity**. The **Check and Configure RFC Destination** window will open, as shown in Figure 3.21.

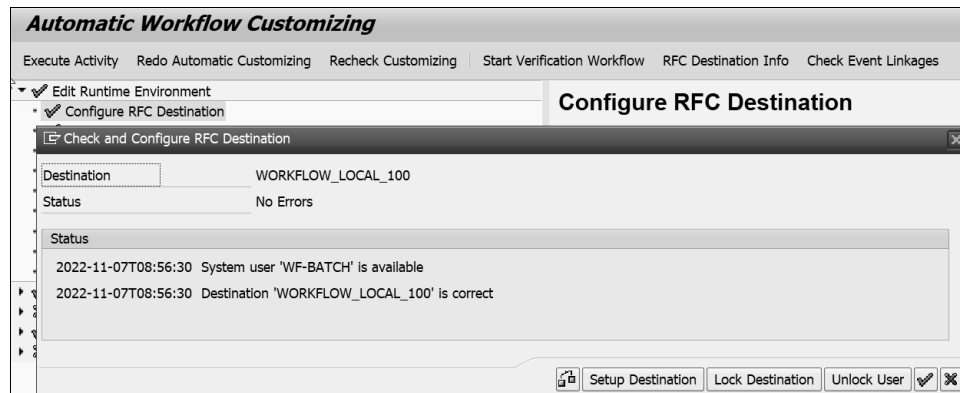


Figure 3.21 Configuring an RFC Destination

The **Status** of user WF-BATCH should be available, and the **Destination** should be correct. If any other message is shown, we recommend fixing the issue before moving forward. Click **OK** or the green checkmark to complete the RFC destination configuration. The next step is to update user WF-BATCH in the **Edit System Administrator for Workflow** step.

The next sequence of steps is self-configurable. Right-click each workflow event and choose **Execute Activity**. You can schedule the necessary background jobs for the workflow system and activate the plan version, as shown in Figure 3.22.

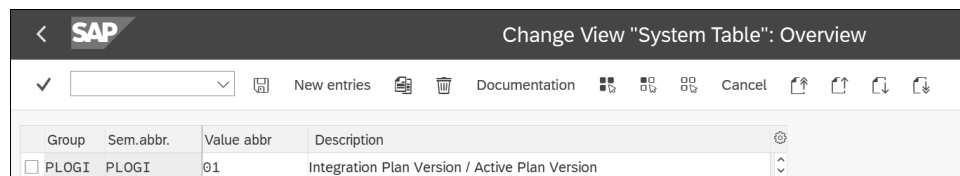


Figure 3.22 Plan Version Configuration

You can only have one plan version in the **Active** status. All the workflow components utilize the active or integrated plan version. If **Execute Activity** is used, 01 is set as the active plan version automatically.



Note

The **Guided Procedures** option might be in red since it requires SAP Process Control components. In this case, the current system does not have the SAP Process Control component, and you can skip activating it.

3.3.2 Testing Automatic Workflows

To test automatic workflows, execute Transaction SWU3 and click the **Start Verification Workflow** button (if needed accept the event linkage activation), as shown in Figure 3.23. Then, go to the inbox to check if your validation workflow was properly launched.

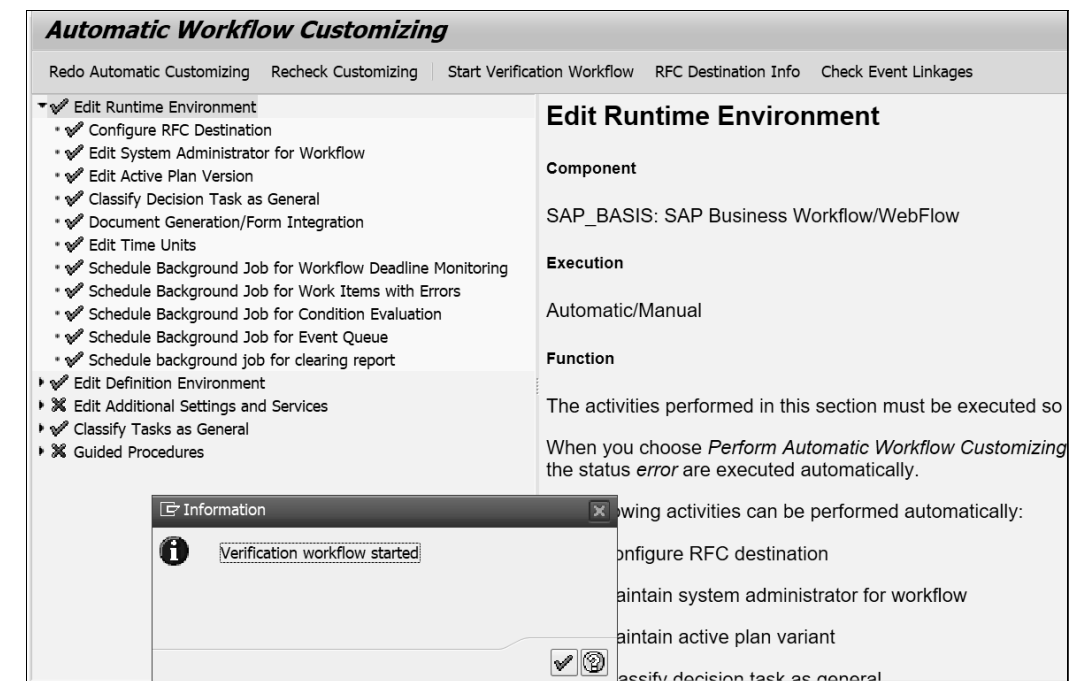


Figure 3.23 Automatic Workflow Verification Started

3.3.3 Classifying Workflow Tasks as General

General workflow tasks must be managed using the **Classify Tasks as General** option. General decision task and other tasks used in predelivered SAP workflows must be classified as *general tasks*:

- The following are the general tasks for processing documents:
 - TS70008298
 - TS71007944
 - TS71007945
 - TS71007946
 - TS71007954
- The following are the general tasks for processing forms:
 - TS70008112
 - TS70008113

- TS70008114
- TS70008115

To change these settings, select a task and click on the **Attributes...** button, as shown in Figure 3.24.

Tasks of an Application Component: Assign Agents					
Name	ID	General or Background Task	Task Version	Assigned as of	Assigned until
Governance, Risk and Compliance GRC					
Execute Task Plan	TS 76300001	Background task		01.01.1900	Unlimited
Notify Employee If Rejecte	TS 76300008	General Task		01.01.1900	Unlimited
Assign Temporary Authori	TS 76300009	Background task		01.01.1900	Unlimited
Notify Approver and Relat	TS 76300011	General Task		01.01.1900	Unlimited
User Decision of Change R	TS 76300013	General Task		01.01.1900	Unlimited
Notify Employee If Approv	TS 76300014	General Task		01.01.1900	Unlimited

Figure 3.24 Maintain Agent Assignment

For decision tasks that are generic in nature, you must declare them as general tasks. By default, these tasks do not have any agents assigned to them. An important step is assigning standard agents to each task.

3.3.4 Scheduling Workflow Background Jobs

The options under **Perform Automatic Workflow Customization** involve scheduling the required MSMP workflow jobs, listed in Table 3.8.

Job	Jobs Scheduled
Missed Deadlines	SWWDHEX, RSWWDHEX
Work Items with Errors	SWWERRE, RSWWERRE
Condition Evaluation	SWWCOND: Work item rule monitoring
Event Queue	Will be scheduled automatically with the RFC destination.
Clearing Report	SWWCLEAR: Clearing tasks in the workflow system
Deadline for Update of Shared Memory of Container Factory	SWFSLSDLEX, RSWFSLSDLEX: This deadline ensures that a job is started regularly that updates the buffer on all application servers. This requirement enables the buffering of definition enhancements of SAP Business Workflow containers in shared memory. You can change the interval of this job using Transaction SWPA.

Table 3.8 Jobs for MSMP Workflows

Note

You must successfully configure the RFC destinations to proceed.



We recommend specifying a time interval for these jobs. The time interval used in automatic customizing is usually 3 minutes. However, this value can be changed according to your requirements. This value depends on the number of requests being created, the workflow items being triggered, and so on. Each time a job is executed, the background job checks whether new deadlines were met since the last run.

3.3.5 Performing Task-Specific Customizing

Once the automatic workflow customization is completed, the next step is to perform task-specific customization by following these steps:

1. Execute Transaction SPRO and navigate to **SAP Reference IMG • Governance, Risk and Control • General Settings • Workflow • Perform Task-Specific Customizing**.
2. On the **Task Customizing Overview** screen, expand the **GRC** node.
3. Click the **Assign Agents** link to the right of the **GRC-AC** node, as shown in Figure 3.25.

Task Customizing Overview			
Application Component Abbreviati...	Application Component Description	Agent Assignment	Event Linkage
SAP Application Components			
AP	Application Platform		
BC	Basis Components		
BI	Business Intelligence solutions		
EPM	Enterprise Performance Management		
BNS	Business Network Solutions		
BW	SAP Business Warehouse		
CA	Cross-Application Components	Assign Agents	Activate event linking
EP	Enterprise Portal		
CEC	Customer Engagement and Commerce		
CRM	Customer Relationship Management		
EIM	Enterprise information management soluti		
FIN	Financials		
FS	Financial Services		
GRC	Governance, Risk and Compliance	Assign Agents	Activate event linking
GRC-ACP	GRC Access Control Plug-In		
GRC-PCP	GRC Process Control Plug-in		
GRC-RM	GRC Risk Management	Assign Agents	Activate event linking
GRC-AC	Access Control	Assign Agents	Activate event linking
GRC-SPC	Process Controls	Assign Agents	Activate event linking
GRC-AC	Access Control	Assign Agents	Activate event linking
/CPMB/KP11000001	/CPMB/KP1100		
HAN	SAP HANA		
KM	Knowledge Management		
MOB-UIA	UI5 Content		
MOB	Business Mobile		
SCM	Supply Chain Management		
PI M	Product Lifecycle Management		

Figure 3.25 Performing Task-Specific Customizing

4. Select each task from the list that are listed as **General** and click the **Attributes...** button. Select **General Task** from the list and ensure that the **Classification** dropdown list is set to **Not classified**. Click the **Transfer** button once changed, as shown in Figure 3.26.

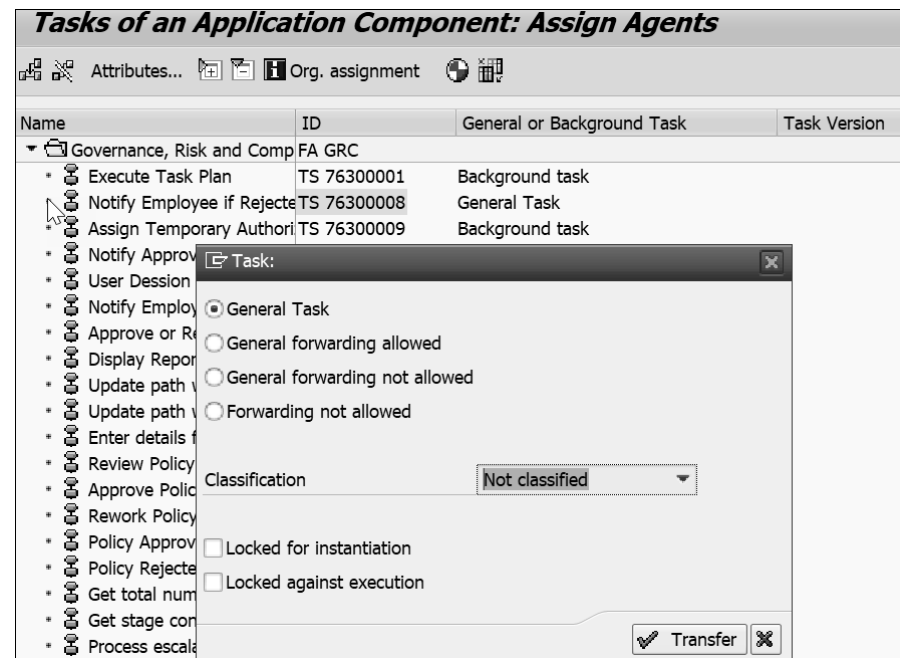


Figure 3.26 Changing a Task into a General Task



Note

If no folders are visible below the GRC folder, run report RS_APPL_REFRESH using Transaction SE38 or SA38.

3.3.6 Activating Event Linkages

Upon completion of agent assignment, proceed with activating the event linkage. On the same screen, click the **Activate Event Linkage** option. Maintain an event linkage using the **Perform task specific customization** option for all workflow step (WS) line items. Click the **Properties** icon and select the **No Errors** option in the **Linkage status** dropdown list, select the **Event linkage activated** checkbox, and select the **Do not change linkage** option from the **Error feedback** dropdown list, as shown in Figure 3.27.

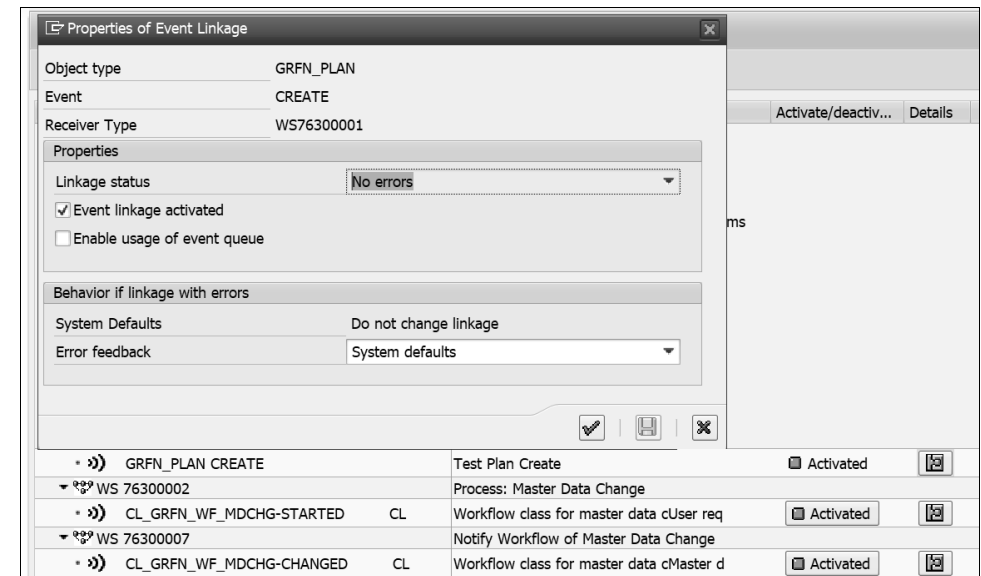


Figure 3.27 Activating an Event Linkage

Make sure you activate all workflow step items.

Note

Task-specific customizing for SAP Access Control is *not* available if you have the GRCPERP and GRCPINW plug-ins installed in your system. In this case, execute Transaction SWE2 and maintain all the ABAP class line items, as shown in in Figure 3.28, by double-clicking on each line in change mode.

The screenshot shows the "Change View 'Event Type Linkages': Overview" table. The table has the following columns: Object Category, Obj. Type, Event, Receiver Type, Type linkage a..., Enable event ..., and Status. The table contains 20 rows of data, each representing an event type linkage. The "Status" column for all rows is "No errors".

Object Category	Obj. Type	Event	Receiver Type	Type linkage a...	Enable event ...	Status
ABAP Class	CL_GRAC_ACCESS_APPROVA	START	WS76300016	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_ACCESS_REQUEST	CANCEL	WS76300056	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_ACCESS_REQUEST	START	WS76300056	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW	CANCEL	WS76300082	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW	START	WS76300031	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW	START	WS76300082	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_CONTROL_ASSGN	CANCEL	WS76300087	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_CONTROL_ASSGN	START	WS76300087	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_FF_REVIEW_WF	START	WS76300107	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_FUNC_MAINT_WF	CANCEL	WS76300084	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_FUNC_MAINT_WF	START	WS76300084	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_MITIGATION_CNT	CANCEL	WS76300088	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_MITIGATION_CNT	START	WS76300088	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_RISK_MAINT_WF	CANCEL	WS76300085	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_RISK_MAINT_WF	START	WS76300085	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_RISK_REVIEW_WF	CANCEL	WS76300081	✓	<input type="checkbox"/>	No errors
ABAP Class	CL_GRAC_RISK_REVIEW_WF	START	WS76300081	✓	<input type="checkbox"/>	No errors

Figure 3.28 Event Type Linkages

In the event linkage settings, enable the **Linkage Activated** checkbox, change the **Behavior Upon Error Feedback** dropdown list to **Do not change linkage**, and change the **Receiver Status** to **No errors**, as shown in Figure 3.29. Then, click **Save**.

Figure 3.29 Maintaining a Linkage

3.3.7 Performing Task-Specific Customizing with Plug-Ins (Assigning Agents)

From Transaction PFTC, the **Standard Tasks & Workflow Templates** should be maintained, as follows:

1. Execute Transaction PFTC.
2. Select **Standard task** from the **Task type** dropdown list.
3. Enter the task number in the **Task** field, as shown in Figure 3.30.

Figure 3.30 Transaction PFTC: Maintaining a Task

4. Click the **Display** icon in the menu bar.
5. Navigate to **Additional data • Agent assignment • Maintain**, as shown in Figure 3.31.

Figure 3.31 Transaction PFTC: Agent Assignment

6. Click the **Attributes...** button and change the setting to **General Task** and change **Classification** to **Not classified**, as shown in Figure 3.32.

Figure 3.32 Transaction PFTC: Attribute

7. Click the **Transfer** button.
8. Repeat these steps for all the standard tasks and workflow templates listed in Table 3.9 and Table 3.10.

Standard Tasks	Task Number
Display Approval Webdynpro Application	TS 76307918
Display Role Approval App	TS 76307944
User Access Review Approval task	TS 76307964
Role Approval UI task	TS 76307966
GRAC Read Stage	TS 76307967
GRAC Read Stage	TS 76308011
GRAC Display Approval for AR	TS 76308013
Access Request Approval Dialog	TS 76308021
Access Request Approval Dialog	TS 76308026
SPM Audit Review Approval	TS 76308028
RAR Rule for Function Approval	TS 76308029
Display Approval Webdynpro Application	TS 76308031
Display Approval Webdynpro RAR Risk	TS 76308038
Display Approval Webdynpro Application	TS 76308047
Role assignment dialog step	TS 76308056
Control Assignment approval dialog	TS 76308057

Table 3.9 Task-Specific Tasks Related to SAP Access Control Workflows

Workflow Templates	Template Number
Access Request Approval Workflow	WS 76300056
User Access Review Workflow	WS 76300082
Function Approval Workflow	WS 76300084
Mitigation Control Maintenance	WS 76300088
Risk Approval Workflow	WS 76300085
SOD Risk Review Workflow	WS 76300081

Table 3.10 Templates Related to SAP Access Control Workflows

Workflow Templates	Template Number
Role Approval Workflow	WS 76300080
Fire Fighter Log Report Review WF	WS 76300089
Control Assignment Approval Workflow	WS 76300087
Role Assignment Review Workflow	WS 76300086
Firefighter Review Workflow	WS 76300107

Table 3.10 Templates Related to SAP Access Control Workflows (Cont.)

9. The last step in workflow configuration is to activate workflow templates using Transaction SWDD (Workflow Builder). The workflow builder is a graphical and an alphanumeric view and also a tree-like display of a workflow definition, as shown in Figure 3.33.

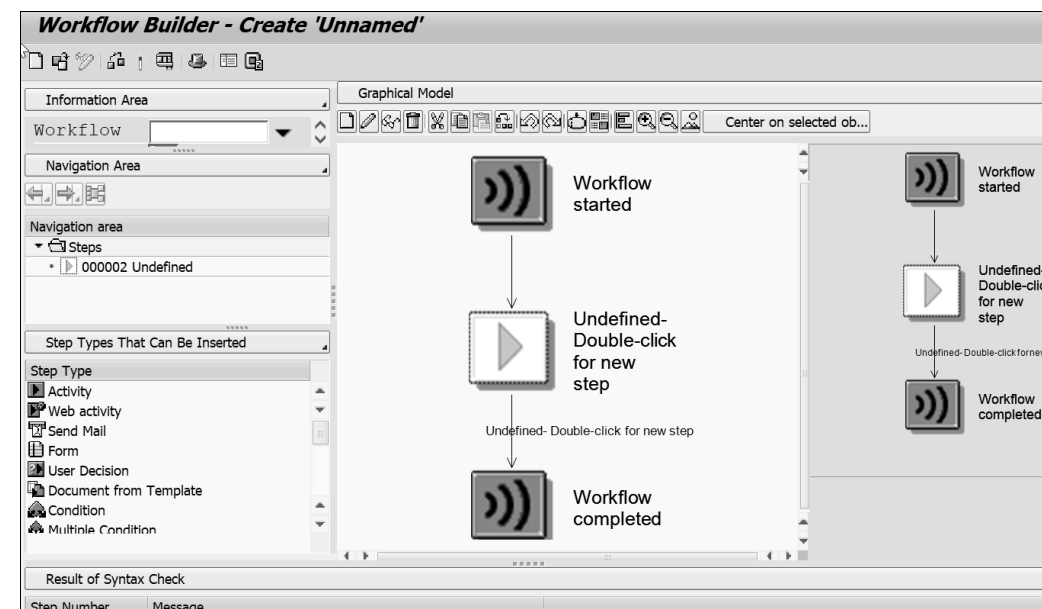


Figure 3.33 Workflow Builder

10. In the **Information Area**, in the **Workflow** field, enter the workflow step number, as listed in Table 3.10. Click the **Activate** button to activate the template.
11. Repeat the steps for all the workflow step templates.

3.3.8 Defining Number Ranges for Access Requests

Every request in SAP Access Control is identified by a unique number, and thus number ranges are important to maintain.

To set up an active number range, follow these steps:

1. Log on to SAP Access Control system.
2. Execute Transaction SPRO.
3. Navigate to **SAP Reference IMG • Governance, Risk and Compliance • Access Control • User Provisioning**.
4. Click **Define** and select the **Maintain Number Range Intervals for Provisioning Requests** option.
5. Enter "GRACREQNO" and maintain the number range, as shown in Figure 3.34.

Figure 3.34 GRACREQNO Number Range



Note

SAP Access Control allows you to create multiple request number ranges. However, only one number range can be active.

6. To maintain the interval, click on **Change**, as shown in Figure 3.35.

Figure 3.35 Editing an Interval

7. On this screen, maintain the **From** number and **To** number, as shown in Figure 3.36.

No	From No.	To Number	NR Status	Ext
01	0000000001	0999999999	83	<input type="checkbox"/>

Figure 3.36 Changing an Interval

8. Once the number range is defined, you should define the number range for provisioning requests. Execute Transaction SPRO and navigate to **SAP Reference IMG • Governance, Risk and Compliance • Access Control • User Provisioning**. Then, activate the desired number range by selecting the **Active** radio button, as shown in Figure 3.37.

Object	No	From number	To number	Current Number	Active
GRACREQNO	01	0000000001	0999999999	896	<input type="radio"/>
GRACREQNO	02	2020000001	2020999999	2020000941	<input checked="" type="radio"/>

Figure 3.37 Activating Number Ranges

3.4 Setting Up Common Parameters

Parameters define the way the application should function. Parameters are classified into two types:

- Common parameters
- Component-specific parameters

Common parameters should be maintained either with the default values or maintained with the desired values.

Some common parameter groups include the following:

- **Change Log**
The parameters in the change log group will be displayed for every critical activity. Thus, for example, risk creation, modification, etc. can be identified from the change logs easily. From an audit point of view, we highly recommend to enabling the change logs.
- **Workflow**
These parameters enable/disable workflow for the Access Risk Analysis component. Access Risk Analysis utilizes four workflows:

- Risk maintenance
- Function maintenance
- Mitigation control maintenance
- Mitigation control assignment

Additionally, this parameter group includes parameters related to workflow-related settings.

■ Performance

The parameters in this group will help to optimize the performance of the system. Settings related to mass risk analysis, sync etc., can be defined using the parameters in this group.

■ Access Controls - General Settings

The parameters in this group relate to all the components of SAP Access Control.

The parameters in each group are listed in Table 3.11.

Parameter Group	Parameter ID	Description
Change Log	1001	When set to Yes , the Access Risk Analysis function change log is enabled.
Change Log	1002	When set to Yes , the Access Risk Analysis risk change log is enabled.
Change Log	1003	This parameter will enable the organization rule log.
Change Log	1004	This parameter will enable the supplementary rule log.
Change Log	1005	Setting this parameter to Yes will enable the critical role change log.
Change Log	1006	Setting this parameter to Yes will enable the critical profile log.
Change Log	1007	Setting this parameter to Yes will enable the ruleset change log.
Change Log	1008	Setting this parameter to Yes will enable the role change log.
Workflow	1061	This parameter can be used to enable or disable the mitigating control maintenance workflow.
Workflow	1062	This parameter can be used to enable or disable the mitigation assignment workflow.
Workflow	1063	Setting this parameter to Yes will enable the risk maintenance workflow.

Table 3.11 Common Parameters Related to SAP Access Control

Parameter Group	Parameter ID	Description
Workflow	1064	Setting this parameter to Yes will enable the function maintenance workflow.
Workflow	1101	When this value is set to Yes , a request will be created for risk approval.
Workflow	1102	Update request for risk approval.
Workflow	1103	Delete request for risk approval.
Workflow	1104	Create request for function approval.
Workflow	1105	Update request for function approval.
Workflow	1106	Delete request for function approval.
Workflow	1107	Create request for mitigation assignment approval.
Workflow	1108	Update request for mitigation assignment approval.
Workflow	1109	Delete request for mitigation assignment approval.
Workflow	1110	Default workflow request priority for updating and creating risks.
Workflow	1111	Default workflow request priority for creating and updating functions.
Workflow	1112	Default workflow request priority for mitigation control assignments.
Workflow	1113	Maintain the user ID from which the emails should be triggered for the SAP Access Control requests, typically, WF-BATCH.
Workflow	2051	Enable user ID validation in access request against search data sources.
Workflow	3022	Request type for role approval.
Workflow	3023	Priority for role approval.
Performance	1120	Batch size for batch risk analysis.
Performance	1121	Batch size for user sync.
Performance	1122	Batch size for role sync.
Performance	1123	Batch size for profile sync.

Table 3.11 Common Parameters Related to SAP Access Control (Cont.)

Parameter Group	Parameter ID	Description
Performance	2050	Enable real-time Lightweight Directory Access Protocol (LDAP) search for access request users.
Access Controls - General Settings	2401	Allowed extensions for attachments in a comma-separated list (for instance, .docx or .pdf). This list will help to avoid SQL injections.
Access Controls - General Settings	2402	Display change delegation link for delegated user if only SAP Access Control application is active.

Table 3.11 Common Parameters Related to SAP Access Control (Cont.)

3.5 Email Configuration

SAP Access Control utilizes the default SAP email engine for sending and receiving messages. However, similar to SAP ERP and SAP S/4HANA, an external email infrastructure is required to set up the mail configuration. Figure 3.38 shows an overview of how SMTP within SAP communicates with the external SMTP server.

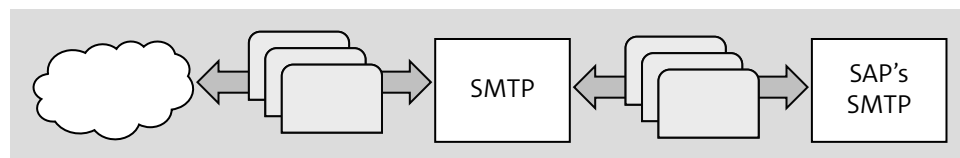


Figure 3.38 SAP SMTP Communication Channel with External SMTP

An external SMTP server acts as a SMTP server between SAP and the receiver. This server is the email server used to send emails. You can use the official SMTP server of your enterprise (i.e., sap.com).

Since SAP Access Control uses workflows, you must set up the email configuration. We'll cover the following high-level steps in greater detail in the following sections:

1. Open the port for SMTP.
2. Maintain the RZ10 profile parameters for the SMTP service or maintain it in Transaction SMICM.
3. Create a system user for receiving emails.
4. Configure the SMTP service.
5. Configure the SMTP server and the outbound and inbound flows.
6. Set up SMTP jobs.

3.5.1 Opening a Simple Mail Transfer Protocol Port

SMTP is the basic standard that mail servers use to send email to one another across the Internet. SMTP email relies on domain names and Internet addresses to know where to send messages. However, these network addresses use specific *port numbers*. The first step in configuring the SMTP service is to open the port number. Your IT infrastructure team should be contacted to open the port and assign it to the SMTP service.

3.5.2 Maintaining RZ10 Profile Parameters for the Simple Mail Transfer Protocol Service

The ICM parameter for SMTP should be added to the RZ10 profile parameters by following these steps:

1. Execute Transaction RZ10.
2. Choose **Instance profile** from the available profiles and select the **Extended maintenance** radio button under **Edit Profile**, as shown in Figure 3.39.

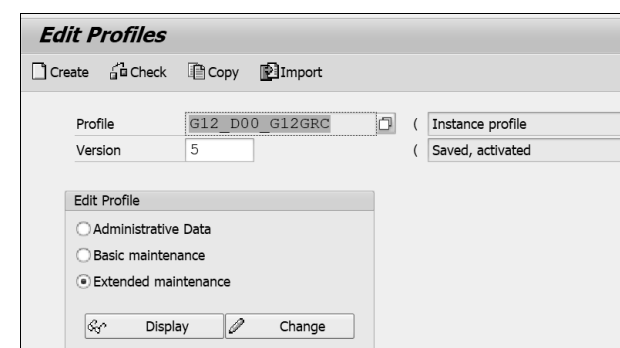


Figure 3.39 Profile Maintenance

3. Click the **New Entries** button.
4. Add an entry for SMTP. The parameter to be added is "icm/server_port_<no>" with value "PROT=SMTP, PORT=<port no which is opened for SMTP>, TIMEOUT=<time out value>, PROCTIMEOUT=<Process Timeout value>". An example is shown in Figure 3.40.

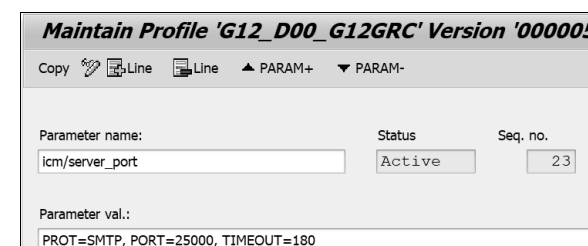


Figure 3.40 ICM Configuration for an SMTP Port

- Click **Save** to save these changes to the instance profile.
- If prompted to activate the profile, click **Yes**, and the activation information screen will be displayed.

**Note**

It is required to restart the SAP system to load the profile parameter values. As an alternative, to proceed with the configuration, the ports can be configured in the Transaction SMICM. Refer to Section 3.2.3 to add the SMTP protocol as well.

3.5.3 Creating a System User for Receiving Emails

For SMTP communication purposes, a dedicated ID is required. Create one user ID of the system type by following these steps:

- Execute Transaction SU01.
- Enter a user ID of the system type in the **User** field (e.g., "SMTPUSER").
- Under the **Profiles** tab, assign the profile **S_A.SCON** from Transaction SU01, as shown in Figure 3.41.

The screenshot shows the SAP 'Maintain Users' transaction (SU01) in the 'Address' tab. The user ID is 'SMTPUSER'. Below the tabs, the 'Assigned Authorization Profiles' section is visible, showing a table with one entry: Profile 'S_A.SCON' and Type 'Text' with the description 'SAPconnect: All Auth. RFC User / SAPphone: Centr. Arch.'.

Profile	Type	Text
S_A.SCON	Text	SAPconnect: All Auth. RFC User / SAPphone: Centr. Arch.

Figure 3.41 SMTPUSER ID with Profile Assignment

**Note**

You may assign additional authorizations as required.

- Click the **Save** icon to save the user ID.
- Make sure all users in the SAP Access Control system have an email address assigned under the **Address** tab, as shown in Figure 3.42.

The screenshot shows the SAP 'Maintain Users' transaction (SU01) in the 'Address' tab. The user ID is 'SMTPUSER'. The 'Communication' section is visible, showing fields for Telephone, Mobile Phone, Fax, and E-Mail Address (raghu@togglenow.com).

Figure 3.42 Transaction SU01: Address Data Screen for a User

3.5.4 Configuring the Simple Mail Transfer Protocol Service

To configure the SMTP service, follow these steps:

- Execute Transaction SICF.
- Click the **Services** icon.
- Find the **SAPconnect** service, as shown in Figure 3.43.

Virtual Hosts / Services	Documentation
default_host	VIRTUAL DEFAULT HOST
SAPconnect	SAPCONNECT (E)SMTP

Figure 3.43 SAP Connect Service

- Right-click the **SAPconnect** service and choose **Display SMTP host**.
- Click the **Edit** button.
- Check that the virtual SMTP server is configured, as shown in Figure 3.44.

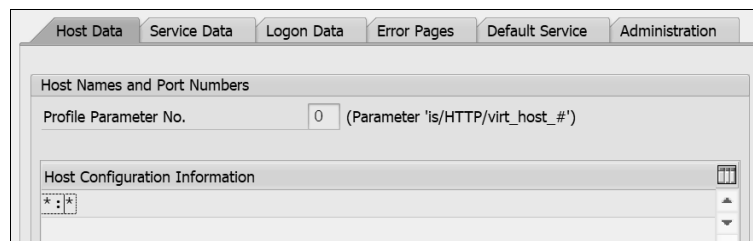


Figure 3.44 Checking the SMTP Configuration under the Host Data Tab

**Note**

The value of the **Profile Parameter No.** field must be the same as the value maintained in RZ10 profile parameter IS/HTTP/VIRT_HOST_#.

- Click the **Logon Data** tab and maintain the **Client**, **User**, and **Password** fields, using the **SMTPUSER** ID created in the previous step, as shown in Figure 3.45.

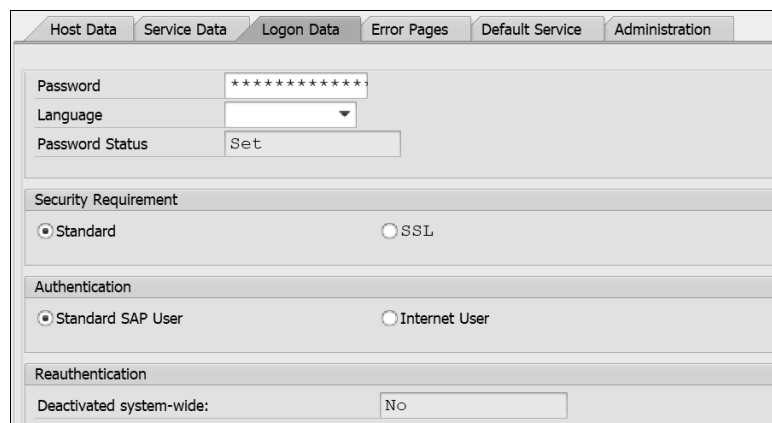


Figure 3.45 Logon Data Maintenance

- Select the **Handler List** tab. In the **Handler** column, make sure that class **CL SMTP_EXT_SAPCONNECT** has been maintained, as shown in Figure 3.46.

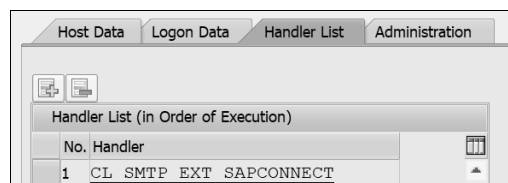


Figure 3.46 SMTP Class Handler

- Click **Save** to save these changes and then right-click the **SAPconnect** service again and select **Activate SMTP Host** to activate the service, as shown in Figure 3.47.

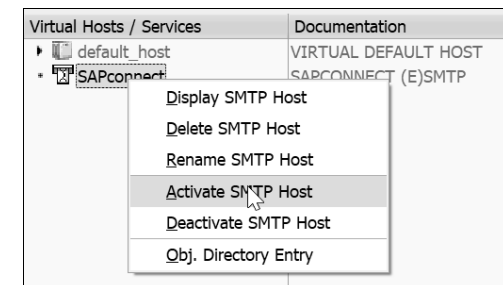


Figure 3.47 Activation of SMTP Host from Transaction SICF

3.5.5 Configuring the Simple Mail Transfer Protocol Server Inbound/Outbound Flow

Once the SICF service is activated successfully, the next step is to configure the SMTP server and outbound and inbound flow by following these steps:

- Log on to SAP Access Control system.
- Execute Transaction SCOT.
- Click **Settings • Default domain** or press **Ctrl+Shift+F9** to set the default domain, as shown in Figure 3.48.

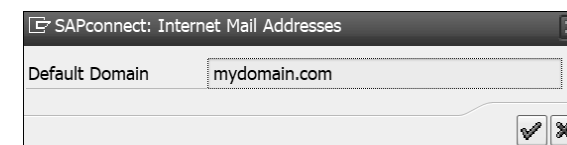


Figure 3.48 Default Domain Maintenance

Note

Ensure that the domain maintained on this screen matches the email domain of the users (as maintained in Transaction SU01, under the **Address** tab).

- Click **OK**.
- Set up the outgoing SMTP server, as shown in Figure 3.49. Enter "SMTP" in the **Node** field, provide a description, and maintain the **Mail Host** and **Mail Post** fields. Click **OK**.

Note

The **Mail Host** and **Mail Port** fields must be maintained.

The screenshot shows the 'SAPconnect: General Node Data of Node' dialog box. It has three main sections:

- General information:** Node: SMTP, Description: Mail Server, Maximum waiting time for repeat send attempt procedure: Hours/minutes: / 5, Node in use.
- SMTP Connection:** Mail Host: myexternalsmtpserver.com, Mail Port: 25, Security: Do not use TLS, Settings button.
- Supported address types:** Fax (Set), Internet (Set), Pager (SMS) (Set).

At the bottom, there is a 'Last changed by' field and a date field, and a toolbar with icons for OK, Cancel, and Help.

Figure 3.49 SMTP Outgoing Configuration

6. Select the **Internet** checkbox and click the **Set** icon to set the address type.
7. In the address areas, insert the valid format of email addresses. When you enter “*” the node will accept every email address.

3.5.6 Setting Up Simple Mail Transfer Protocol Jobs

Now, the node is configured to accept outgoing emails. What is missing is a job that picks up the emails from the outgoing queue and sends them.

To create a job that will send the queued messages, follow these steps:

1. Click the **Job** menu and choose **Create** or press **Ctrl + F8**.
2. Enter the **Job name** and click **OK** .
3. Select **SAP&CONNECTALL** or **SAP&CONNECTINT** for sending internet email.
4. Click **Start immediately** to start the job to run immediately. Alternatively, the job can be scheduled to run at defined intervals. Click the **Schedule** button and schedule a job. The recommended interval is 1 minute.

3.6 Summary

SAP Access Control is a powerful solution that can help your organization ensure compliance with regulations and internal policies related to access control. However, a critical task is to configure the solution correctly to achieve the desired results.

In this chapter on post-installation steps, all the initial configuration steps are outlined, such as activating applications, services, BC sets, maintaining parameters, and plug-in settings. By leveraging standard features like MSMP and BRFplus, many manual and complex processes can be simplified, and audit gaps and issues can be addressed. By carefully analyzing your business requirements, your organization can achieve a clean and planned design that aligns with its objectives.

Note that individual solutions must be enabled for each system connected to SAP Access Control. This process is referred to as *common configuration*, and the steps are detailed in the next chapter. Once the post-installation configuration is successfully completed, your organization can move forward with SAP Access Control’s common configuration.

Contents

Preface	19
1 Introduction to Governance, Risk and Compliance	25
1.1 Why Use Governance, Risk and Compliance Solutions?	25
1.2 Introduction to SAP Access Control	29
1.3 Architecture and Landscape	31
1.3.1 Architecture	32
1.3.2 Landscape	33
1.4 Key Capabilities, Supported Systems, and Integration	34
1.4.1 Key Capabilities	34
1.4.2 Supported Systems	36
1.5 Cloud Integration	37
1.6 Summary	39
2 Prerequisites	41
2.1 Checking License Agreements and Licensing Requirements	41
2.1.1 Creating an SAP GRC Solutions System in SAP Support Portal	42
2.1.2 Generating and Applying an SAP GRC Solutions License	43
2.1.3 Identify the User License Requirements	44
2.2 System Sizing	45
2.3 System Time Zone Check	47
2.4 Component and Plug-In Requirements	48
2.4.1 Components	48
2.4.2 Plug-Ins	49
2.5 Summary	50

3	Post-Installation Steps	51
3.1	Quick Checks	51
3.2	Initial Configuration	52
3.2.1	Activating Applications and Services	52
3.2.2	Activating Internet Communication Framework Services	53
3.2.3	Activating Internet Communication Management Services	56
3.2.4	Activating Business Configuration Sets	58
3.2.5	Maintaining Plug-In Parameters	63
3.2.6	Maintaining Plug-In (User Exit) Settings	63
3.2.7	Activating SAP-Delivered Roles	64
3.2.8	Defining Business Processes and Subprocesses	68
3.3	Multistage Multipath Workflow Initial Configuration	70
3.3.1	Performing Automatic Workflow Configuration	70
3.3.2	Testing Automatic Workflows	75
3.3.3	Classifying Workflow Tasks as General	75
3.3.4	Scheduling Workflow Background Jobs	76
3.3.5	Performing Task-Specific Customizing	77
3.3.6	Activating Event Linkages	78
3.3.7	Performing Task-Specific Customizing with Plug-Ins (Assigning Agents)	80
3.3.8	Defining Number Ranges for Access Requests	84
3.4	Setting Up Common Parameters	85
3.5	Email Configuration	88
3.5.1	Opening a Simple Mail Transfer Protocol Port	89
3.5.2	Maintaining RZ10 Profile Parameters for the Simple Mail Transfer Protocol Service	89
3.5.3	Creating a System User for Receiving Emails	90
3.5.4	Configuring the Simple Mail Transfer Protocol Service	91
3.5.5	Configuring the Simple Mail Transfer Protocol Server Inbound/Outbound Flow	93
3.5.6	Setting Up Simple Mail Transfer Protocol Jobs	94
3.6	Summary	95
4	Common Configurations	97
4.1	Configuring Remote Function Call Destinations	97
4.1.1	Connecting an SAP NetWeaver System	98
4.1.2	Connecting an SAP HANA Database	101
4.1.3	Connecting an SAP Enterprise Portal System	113

4.2	Maintaining Connectors and Connection Types	116
4.2.1	Creating Connection Types and Connectors	116
4.2.2	Defining Connector Groups	118
4.2.3	Assigning Connectors to Connector Groups	119
4.3	Maintaining Connection Settings	119
4.4	Maintaining Connector Settings	123
4.5	Maintaining Configuration Settings	124
4.6	Maintaining Mapping for Actions and Connector Groups	127
4.7	Configuring Data Sources	129
4.7.1	Data Source Configuration	129
4.7.2	Setting Up an HR Connection	131
4.7.3	Setting Up a LDAP Connection	132
4.8	Setting Up Background Synchronization Jobs	137
4.8.1	Authorization Sync	137
4.8.2	Repository Object Sync	138
4.8.3	Action Usage Sync	139
4.8.4	Role Usage Sync	139
4.8.5	Superuser Privilege Management Log Sync	139
4.8.6	Batch Risk Analysis	140
4.8.7	Alert Generation	142
4.8.8	Generate Rules	143
4.8.9	Email Reminders	143
4.8.10	Emergency Access Management Master Data Sync	144
4.8.11	Fetch IDM Schema	144
4.9	Distributing Jobs for Parallel Processing	145
4.9.1	Setting Up Background Work Processes	145
4.9.2	Maintaining Parameters for Parallel Processing	146
4.9.3	Distributing Jobs for Parallel Processing	146
4.10	Summary	147
5	Access Risk Analysis	149
5.1	Introduction to Access Risk Analysis	149
5.1.1	Why Use an Access Risk Analysis Solution?	150
5.1.2	Evolution of Access Risk Analysis	151
5.1.3	Terminology	153
5.1.4	Definitions	155

5.2	Setting Up Access Risk Analysis	157
5.2.1	Configuring Parameters	158
5.2.2	Setting Up Rulesets	176
5.2.3	Synchronization Jobs	191
5.2.4	Setting Up Batch Risk Analysis	192
5.2.5	Setting Up Risk Owners, Mitigation Control Owners, and Controllers	192
5.3	Setting Up Workflows for Access Risk Analysis	196
5.4	Maintaining Custom User Groups	197
5.5	Maintaining Master User ID Mappings	199
5.6	Working with Access Risk Analysis	200
5.6.1	Performing Risk Analysis	201
5.6.2	Risk Simulation	211
5.7	Working with Mitigation Controls	216
5.7.1	Configuring Mitigating Control	216
5.7.2	Applying Mitigations	221
5.8	Setting Up Alerts	224
5.9	Configuring the Risk Terminator	228
5.10	Reports and Analytics	230
5.11	Summary	231
6	Emergency Access Management	233
6.1	Introduction to Emergency Access Management	233
6.1.1	Why Use an Emergency Access Management Solution?	234
6.1.2	Advantages and Business Benefits	235
6.2	Configuring Emergency Access Management	235
6.2.1	Setting Up Parameters	236
6.2.2	Setting Up Transaction SPRO Configuration in SAP Access Control	242
6.2.3	Setting Up Transaction SPRO Configuration in Your Backend (Plug-In) System	243
6.2.4	Setting Up Notification Templates	244
6.2.5	Setting Up Reason Codes	249
6.3	Maintaining Emergency Access Management Access Control Owners	250
6.3.1	Users in Emergency Access Management	250
6.3.2	Assigning the Firefighter Owner to a Firefighter ID	251
6.3.3	Assigning the Firefighter Controller to a Firefighter ID	252
6.3.4	Assigning Firefighter IDs to Firefighters	254

6.4	Activating Multistage Multipath for Emergency Access Management	254
6.5	ID-Based and Role-Based Emergency Access Management	264
6.5.1	Centralized Emergency Access Management	265
6.5.2	Decentralized Emergency Access Management	265
6.5.3	Role-Based Emergency Access Management	266
6.6	Setting Up Emergency Access Management Jobs	268
6.7	Emergency Access Management Log Synchronization	269
6.8	Working with Firefighter IDs	269
6.8.1	Using Firefighter IDs in a Centralized Environment	270
6.8.2	Using Firefighter IDs in a Decentralized Environment	271
6.9	Firefighter ID Report Execution	271
6.10	Emergency Access Management Log Reviews	273
6.11	Emergency Access Management Log Types and Details	273
6.12	Summary	274
7	Access Request Management	275
7.1	Introduction to Access Request Management	275
7.1.1	Why Use an Access Request Management Solution?	275
7.1.2	Advantages and Business Benefits	277
7.2	Setting Up Access Request Management	280
7.2.1	Activating Business Configuration Sets	280
7.2.2	Setting Up Parameters	281
7.2.3	Setting Up a Number Range for Access Requests	298
7.2.4	Setting Up an Access Request Workflow	300
7.2.5	Maintaining Provisioning Settings	301
7.2.6	Defining Request Types	304
7.2.7	Maintaining End User Personalization	305
7.2.8	Setting Up Default Roles	308
7.2.9	Maintaining User Defaults	309
7.2.10	Setting Up Templates	311
7.2.11	Defining Service Level Agreements	313
7.3	Using Access Request Management	316
7.3.1	Raising Requests	316
7.3.2	Approving a Request	330
7.3.3	Administration Activity for Requests	333
7.3.4	Searching Requests	333

7.3.5	Provisioning Logs	336
7.3.6	Managing Password Self-Service	337
7.3.7	Delegating Requests	338
7.3.8	Working with Requests	340
7.4	Summary	341
8	Business Role Management	343
8.1	Introduction to Business Role Management	343
8.1.1	Why Use a Business Role Management Solution?	344
8.1.2	Advantages and Business Benefits	344
8.1.3	Terminology	345
8.2	Setting Up Business Role Management	346
8.2.1	Setting Up Connectors and Connector Groups	346
8.2.2	Maintaining Connection Settings	347
8.2.3	Maintaining Mapping for Actions and Connector Groups	347
8.2.4	Activating Business Configuration Sets	349
8.2.5	Maintaining Configuration Settings	349
8.2.6	Defining Role Owners	357
8.2.7	Maintaining Role Type Settings	363
8.2.8	Specifying Naming Conventions	366
8.2.9	Defining Other Role Attributes	368
8.2.10	Maintaining Organizational Level Mapping	372
8.2.11	Maintaining Role Prerequisites	374
8.2.12	Setting Up Role Methodologies	376
8.3	Maintaining Multistage Multipath Workflows	382
8.4	Working with Roles	382
8.4.1	Define Role	383
8.4.2	Maintain Authorizations	383
8.4.3	Derive Role	384
8.4.4	Analyze Access Risks	386
8.4.5	Request Approval	386
8.4.6	Generate Roles	387
8.4.7	Maintain Test Cases	388
8.5	Role Mass Maintenance	389
8.5.1	Role Import	389
8.5.2	Role Mass Update	392
8.5.3	Derived Role Organizational Value Update	393
8.5.4	Role Derivation	395
8.5.5	Role Generation	396

8.6	Role Recertification	397
8.7	Role Management Reports	398
8.8	Summary	399
9	Periodic Reviews	401
9.1	User Access Review	402
9.1.1	Performing User Access Review Configuration	402
9.1.2	Configuring User Access Review Workflows	407
9.1.3	Validating Role Methodology	417
9.1.4	Generating Data for User Access Review	418
9.1.5	Admin Reviews	422
9.1.6	Triggering User Access Review Workflows	423
9.1.7	Updating the Workflow for User Access Review Requests	423
9.1.8	Performing User Access Reviews	424
9.2	Segregation of Duties Risk Review	428
9.2.1	Performing Segregation of Duties Risk Review Configuration	428
9.2.2	Scheduling Synchronization Jobs	432
9.2.3	Setting Up and Managing Coordinators	434
9.2.4	Verifying Risk Owners	434
9.2.5	Generating Data for Segregation of Duties Risk Reviews	436
9.2.6	Admin Reviews	437
9.2.7	Updating the Workflow for Segregation of Duties Risk Reviews	437
9.2.8	Performing Segregation of Duties Risk Reviews	438
9.3	Firefighter ID Review	440
9.3.1	Multistage Multipath Configuration	441
9.3.2	Setting Up Notification Templates	441
9.3.3	Generating Data for Firefighter ID Reviews	442
9.3.4	Reviewing Firefighter ID Requests	443
9.4	Summary	443
10	End User Home Page	445
10.1	End User Home Page Services	445
10.2	Implementation	446
10.2.1	Prerequisites	446
10.2.2	Activating the End User Home Page Services	449
10.2.3	Using End User Home Page	452

10.3 Advantages for End User Licenses	454
10.4 Password Self-Service, Access Request Creation, and Managing Access Control Information	454
10.4.1 Password Self-Service	454
10.4.2 Name Change Self-Service	462
10.4.3 Access Request Creation	464
10.5 Summary	466
11 Multistage Multipath Workflows	467
11.1 Introduction to Multistage Multipath Workflows	467
11.1.1 What Is a Workflow?	468
11.1.2 Terminology	471
11.2 Process Global Settings	472
11.2.1 Workflow Process Definitions	473
11.2.2 Global Settings	475
11.2.3 Notification Settings	475
11.2.4 Escape Conditions	476
11.3 Maintaining Rules and Rule Results	477
11.3.1 Rule Kinds	477
11.3.2 Rule Types	478
11.4 Maintaining Agents	479
11.4.1 Agent Types	479
11.4.2 Directly Mapped Users	480
11.4.3 PFCG Roles	482
11.4.4 PFCG User Groups	483
11.4.5 GRC API Rules	484
11.5 Setting Up Notification Variables and Templates	485
11.6 Maintaining Paths	492
11.6.1 Working with Approval Paths	492
11.6.2 Approval Types	494
11.6.3 Routing Enabled (Detour Conditions)	494
11.6.4 Escalation Types	495
11.7 Setting Up Notifications: Definition	502
11.8 Maintaining a Route Mapping	504
11.9 Generating Versions	506

11.10 Troubleshooting Multistage Multipath Issues	507
11.10.1 Transaction GRFNMW_GEN_VERSION	507
11.10.2 Transaction GRFNMW_CN_VERA	508
11.10.3 Transaction GRFNMW_CONFIGURE	508
11.10.4 Transaction GRFNMW_DBGMONITOR_WD	510
11.10.5 Transaction GRFNMW_DEBUG_MSG	511
11.10.6 Transaction GRFNMW_DEBUG	511
11.10.7 Transaction GRFNMW_DEV_CONFIG	513
11.10.8 Transaction GRFNMW_MONITOR	513
11.10.9 Transaction SLG1	514
11.11 Summary	515
12 BRFPplus: Business Rule Framework	517
12.1 Introduction and Activation	517
12.2 Generating Multistage Multipath Rules for Processes	521
12.3 Understanding BRFPplus Scenarios	523
12.3.1 Creating a BRFPplus Initiator-Based Rule	523
12.3.2 Creating a BRFPplus Agent-Based Rule	529
12.4 Creating a BRFPplus Routing-Based Rule	537
12.4.1 Creating a Data Object	538
12.4.2 Creating a Procedure Call	540
12.4.3 Creating a Table Operation	543
12.4.4 Creating a Decision Table	544
12.4.5 Creating a Ruleset	547
12.5 Transporting a BRFPplus Application	550
12.6 Summary	554
13 SAP Fiori for SAP Access Control	555
13.1 Introduction	555
13.1.1 SAP Fiori Architecture	556
13.1.2 Deployment Options	558
13.1.3 Terminology	561
13.1.4 Types of SAP Fiori Apps	562

13.2 SAP Fiori Configuration	564
13.2.1 Prerequisites	565
13.2.2 Activate SAP Gateway	566
13.2.3 Setting Up Remote Function Call Connections	566
13.2.4 Setting Up System Aliases	568
13.2.5 Activating SICF Services	573
13.2.6 System Alias Mapping	574
13.2.7 Maintaining Aliases: SAP Gateway Routing Configuration	576
13.2.8 Replicating the SAP GRC Technical Catalog	577
13.2.9 Types of Users and Authorizations	579
13.3 Working with SAP Fiori Apps	581
13.4 Troubleshooting SAP Fiori App Issues	583
13.4.1 Cache Issues	584
13.4.2 Reference Lost Errors	585
13.4.3 Verifying Error Logs	585
13.4.4 Troubleshooting Core Data Services Authorization Issues	586
13.5 Summary	586
14 HR Triggers	587
14.1 Introduction to HR Triggers	587
14.2 Configuring HR Triggers	588
14.2.1 Maintaining Parameters in the Plug-In System	589
14.2.2 Activating Plug-Ins	589
14.2.3 Assigning Connectors to an Integration Scenario	590
14.2.4 Maintaining Data Source Configuration	590
14.2.5 Defining Request Types	591
14.2.6 Maintaining Action IDs and Systems for HR Triggers	592
14.2.7 Creating BRFplus Applications for HR Triggers	594
14.2.8 Maintaining BRFplus Function IDs	609
14.3 Troubleshooting HR Trigger Issues with Debugging	610
14.4 Summary	612

15 Enhancements and Developments	613
15.1 Enhancements	613
15.1.1 Notification Template Enhancements	614
15.1.2 Adding Licensing Category Custom Field in Access Request Form	619
15.1.3 Deactivate Unused Risk Analysis Types in Access Request Form	626
15.1.4 Limit Number of Line Items in the Access Request Form	629
15.1.5 Assign User Group in the Logon Data Tab	631
15.1.6 Changing Menu Tab Order in Access Request Form	632
15.1.7 Customize Role Search Screen in Access Request Form	636
15.2 Custom Developments	637
15.2.1 Cancel Pending Requests Automatically for Departed Users	638
15.2.2 Route Log Review for Critical Firefighter IDs to Critical Review Path	647
15.2.3 Restrict Manager ID to Only Numeric Values in Access Request Form	659
15.2.4 Restrict Contract User ID Role Assignment Validity to Six Months	664
15.2.5 Managing Your Mitigating Controls	670
15.3 Summary	680
The Author	681
Index	683

Index

\$Temp package 552

A

ABAP List Viewer (ALV) 241
Access control owners 194
 assignment 195
Access forms 469
Access Request app 327
Access request form 318
 add licensing category field 619
 default values 309
 menu tab order 632
 number of line items 629
 role search screen 636
 simplified 297, 324
 unused risk analysis types 626
Access Request Management 36, 275, 587
 BC sets 280
 benefits 277
 integration 278
 overview 275
 raise requests 316
 request flow 276
 set up 280
 use 316
Access requests 317–318, 464
 administration 335
 administrators 333
 approve 330
 audit log 334
 cancel instance 336
 copy 321
 delegation 338, 340
 instance status 334
 multiple users 328
 number ranges 84
 open 334
 raise 317
 raise from Transaction NWBC 318
 roles 283
 routing rule 539
 SAP Fiori app 327
 search 333
 simplified 324
 template-based 325
 training verification 291
 validation 294
 work with 340

Access Risk Analysis 35, 149
 evolution 151
 function IDs in roles 351
 overview 149
 reports and analytics 231
 set up 157
 terminology 153
 use 201
 workflows 197
Account validation 303
Action IDs 592, 600
Actions 127, 154, 156, 562
 assign 128
 mapping 347
Action usage sync 139
Activation 52
Administrator reviews 406, 422
Administrators 429, 510
Agent IDs 535
Agent rules 477
Agents 300, 471
 maintain 479
 types 480
Alerts 28, 225
 comments 228
 events 226
 generation 142
 messages 227
 review 227
Analysis 202
Analytical apps 563
API rules 484
Application layer 32
Application programming interfaces (APIs) ... 101
Approval levels 498
Approvals 386, 470
Approval types 494
Approver agents 477
Approver groups 481
Approvers 330
Architecture 32
Assignments 500
Attributes 290
Auditing 345, 470
Authorizations 65, 101, 211, 579
 checks 161
 maintain 383
Authorization sync 137

Authorization sync job	192	Business Object Repository (BOR)	575
Automatic workflows	70	Business processes	68, 154, 219
<i>events</i>	71	<i>default</i>	350
<i>test</i>	75	Business Role Management	36, 126, 343
B		<i>advantages</i>	344
Background work processes	145	<i>configuration</i>	349
Batch email reminders	143	<i>delete roles</i>	352
Batch risk analysis	140, 145, 155, 193, 432–433	<i>mass management</i>	389
<i>maintain excluded objects</i>	141	<i>master data</i>	405
BC sets	58	<i>overview</i>	343
<i>Access Request Management</i>	280	<i>reports</i>	398
<i>Access Risk Analysis</i>	176	<i>roles</i>	66
<i>activate</i>	59, 349	<i>terminology</i>	345
<i>activation logs</i>	61	Business roles	293, 346, 419
<i>activation options</i>	60	<i>assignment</i>	294
<i>Business Role Management</i>	349	Business workplaces	471
<i>functions</i>	61	C	
<i>list</i>	58	Catalogs	561
Benchmark testing	45	Change logs	85–86, 125, 158
Binding types	539	Cloud integration	37
BRFplus	517	Common configuration	97
<i>agent-based rule</i>	529	Companies	371
<i>event mode</i>	531	Compliance	27
<i>initiator-based rules</i>	523	<i>phases</i>	34
<i>modes</i>	518	<i>recertification</i>	35
<i>routing-based rule</i>	537	<i>reviews</i>	36
<i>rule creation log</i>	530	Components	48
<i>rule log</i>	527	Condition groups	362, 379
<i>rule results</i>	534	<i>assign to BRFplus functions</i>	381
<i>scenarios</i>	523	<i>IDs</i>	379
<i>terminology</i>	518	<i>role owners</i>	362
BRFplus applications	526	Conditions	258
<i>activate</i>	554	Conflict check	62
<i>create</i>	594–595	Connection types	116
<i>development packages</i>	551	Connector groups	118, 347, 631
<i>functions</i>	596	<i>define</i>	118
<i>make transportable</i>	552	<i>mapping</i>	127, 347
<i>role types</i>	379	Connectors	97, 116–117, 242, 346
<i>transporting</i>	550	<i>assign to groups</i>	119
BRFplus functions	359, 377, 609	<i>assign to integration scenarios</i>	119
<i>mapping</i>	609	<i>multiple</i>	121
BRFplus rules	260, 494, 522, 588, 611	<i>settings</i>	123
<i>create</i>	255, 359	Consistency check	62
<i>custom</i>	505	Continuous monitoring	202
<i>firefighter log review</i>	651	Contractor IDs	664
<i>ID</i>	657	Controllers	239
<i>trigger values</i>	505	Coordinators	416, 429
Browser cache	584	<i>activities</i>	417
Business catalogs	561, 578, 585	<i>review mapping</i>	416
<i>roles</i>	579	<i>set up</i>	434

Core data services (CDS)	173	Emergency Access Management (Cont.)	
Custom developments	637	<i>decentralized</i>	265
<i>cancel pending requests</i>	638	<i>ID-based</i>	240, 264
<i>manage mitigating controls</i>	670	<i>ID-based vs role-based</i>	237
<i>restrict contract user ID</i>	664	<i>log reviews</i>	273
<i>restrict manager ID</i>	659	<i>log synchronization</i>	269
<i>route log review</i>	647	<i>log sync job</i>	269
Custom fields	623	<i>log types</i>	273
D		<i>master data sync</i>	144
Database layer	33	<i>master data sync job</i>	269
Database lookup	533	<i>overview</i>	233
Data binding	597	<i>role-based</i>	266
Data breaches	26	<i>roles</i>	66
Data objects	538, 597	<i>set up jobs</i>	268
<i>result</i>	542	<i>users</i>	250
<i>table</i>	539	End rules	468
Data sources	129	End user home page	445
<i>configure</i>	590	<i>activating services</i>	449
<i>user authentication</i>	130	<i>end user verification</i>	446
<i>user details</i>	130, 591	<i>guest user</i>	448
Data synchronization	172, 192	<i>implementation</i>	446
Data types	620	<i>logon page</i>	447
Decision tables	360, 379, 523, 525, 600	<i>prerequisites</i>	446
<i>add conditions</i>	546	<i>raise request</i>	317
<i>condition column</i>	602	<i>services</i>	445
<i>create</i>	257, 544, 600, 655	<i>SSO</i>	452
<i>definition</i>	545, 602	<i>use</i>	452
<i>details</i>	601	End user personalization	305, 319, 499
Delete account request type	638	<i>definition</i>	307
Delivery units	101–102	<i>field properties</i>	306
Deprovision roles	430	<i>fields</i>	306
Detour paths	492	<i>ID</i>	306
Detours	477	<i>ID in template</i>	307
Directly mapped users	480	<i>templates</i>	305
Document storage	469	Enhancements	613
E		<i>change menu tab order</i>	632
Email	88	<i>customize role search screen</i>	636
<i>content</i>	679	<i>deactivate unused risk analysis types</i>	626
<i>jobs</i>	94	<i>licensing category</i>	619
<i>notifications</i>	680	<i>limit number of line items</i>	629
<i>system users</i>	90	<i>notification templates</i>	614
<i>templates</i>	245	<i>user groups on Logon Data tab</i>	631
Emergency Access Management	35, 125, 233	Enron	152
<i>benefits</i>	235	Error logs	585
<i>centralized</i>	265	Escalations	409
<i>configure</i>	235	Escalation types	495
<i>configure role-based</i>	266	Escape paths	476

F

Factsheets	563
Fetch IDM schema	144
FFID reviews	401, 440
<i>generate data</i>	442
<i>notification templates</i>	441
<i>review requests</i>	443
Field-based configuration	624
Firefighter admins	251
Firefighter controller log review	139
Firefighter controllers	251, 271
FFIDs	252
Firefighter IDs (FFIDs)	66, 234, 251
<i>assignment</i>	255
<i>centralized environment</i>	270
<i>decentralized environment</i>	271
<i>designate as critical</i>	647
<i>function module</i>	648
<i>per user</i>	242
<i>report execution</i>	271
<i>work with</i>	269
Firefighter log review	240, 651
Firefighter owners	250
FFID	251
<i>role</i>	252
Firefighters	251
FFIDs	254
<i>roles</i>	267
Firefighter workflow sync job	269
Functional areas	372
Function groups	649, 667
Function modules	541
Functions	154, 181, 526, 596
ID	182

G

Generate rules	143
Global escalation	475
GLOBAL ruleset	149, 178
<i>copy</i>	186
Governance and compliance require- ments	27
GRC_POR	113
GRCFND_A	41, 49
GRCPERP	33, 36, 49, 79
GRCPINW	33, 49, 79
Group field mapping	128
Groups	582

H

HCO_GRC_PI	49, 102
HR triggers	587
<i>activate plug-ins</i>	589
<i>BRFplus applications</i>	594
<i>configure</i>	588
<i>data source</i>	590
<i>debug</i>	611
<i>integration scenarios</i>	590
<i>objects</i>	594
<i>overview</i>	587
<i>plug-in system</i>	589
<i>troubleshooting</i>	610
Human resources (HR)	131
connector	131

I

ICF services	53, 573
<i>activate</i>	54
<i>deactivate</i>	55
<i>test</i>	54
ICM services	56
Identity Authentication service	37
Indirect assignments	323
Industry 4.0	26
Initiator rules	477, 523
Initiators	468
Integration	36
Integration framework	116
Integration layer	33
Integration scenarios	120, 347
<i>maintain classes</i>	122

J

Jobs	421
<i>error</i>	421
<i>statuses</i>	421

L

Landscape	33
LDAP group	196–197
License agreements	41
License keys	42–43
Licenses	454
Lightweight Directory Access Protocol (LDAP)	113, 126, 404, 452, 664
connector	132
connector	133

Lightweight Directory Access Protocol (LDAP)
(Cont.)

<i>create services</i>	134
<i>default connector</i>	134
<i>mapping</i>	135
<i>test connection</i>	136
Logical connector	113
Logical ports	115, 118
Loops	604
<i>assign a rule</i>	606
<i>definition</i>	604

M

Maker-checker concept	202
Manager IDs	660
Manual provisioning	502
Mass notifications	600
Master user ID mapping	200
Measures	217
Menu tab order	635
Message classes	248, 413
Metadata	572
MIME repository	617
Mitigating controls	670
Mitigation	202
Mitigation approvers	193
Mitigation control monitors	154
Mitigation control owners	154
Mitigation controls	154, 159, 208, 282
<i>advantages</i>	208
<i>apply</i>	222
<i>configuration</i>	217
<i>create</i>	220
<i>mass upload</i>	223
<i>reports</i>	161
<i>Risk Analysis screen</i>	222
<i>Transaction NWBC</i>	222
<i>working with</i>	217
Mitigation monitors	194
Model user	320
Monitor batch risk analysis	141
Monitoring users	44
MSMP	
<i>configuration</i>	441
<i>Emergency Access Management</i>	254
<i>process ID</i>	170
<i>process IDs</i>	255
<i>rule</i>	260
MSMP workflows	255, 300, 467, 588
<i>add rule</i>	527
<i>approaches</i>	468

MSMP workflows (Cont.)

<i>automated approach</i>	468
<i>debugging</i>	511
<i>escape conditions</i>	476
<i>fragmented approach</i>	469
<i>general tasks</i>	75
<i>global settings</i>	472
<i>initial configuration</i>	70
<i>maintain</i>	382
<i>maintain rules</i>	478
<i>notification settings</i>	475
<i>overview</i>	467
<i>process definitions</i>	473
<i>process IDs</i>	475
<i>RFC destination</i>	72
<i>roles</i>	472
<i>rules</i>	477, 521
<i>schedule background jobs</i>	76
<i>sequence of operations</i>	468
<i>set up</i>	408
<i>standard tasks</i>	82
<i>statistics</i>	513
<i>task-specific customizing</i>	77
<i>templates</i>	82
<i>terminology</i>	471
<i>troubleshooting</i>	507
My Profile page	465
<i>options</i>	465

N

Name change self-service	462
<i>failed authentication</i>	463
<i>user authentication</i>	463
Notification agents	477
Notifications	502
<i>add</i>	503
<i>cleanup stage definitions</i>	503
<i>set up</i>	502
Notifications events	245
Notification templates	244, 441, 485, 614
<i>add file</i>	619
<i>add HTML content</i>	614
<i>add to document object</i>	489
<i>create</i>	247, 488
<i>custom</i>	488
<i>customize</i>	247
<i>email</i>	410
<i>email body content</i>	488
<i>hide recipient</i>	490
<i>message class</i>	490
<i>modify</i>	410, 486

Notification templates (Cont.)	Parameters (Cont.)
<i>SoD</i> 431	1031 165
<i>stage level</i> 414	1032 165
<i>subject line</i> 249, 412, 490	1033 166
Notification variables ... 246, 411, 413, 485–486	1034 166
<i>rules</i> 477	1035 166
Number ranges 84, 298, 300	1036 166
<i>provisioning requests</i> 85	1037 166
O	1038 166
OData 244, 556	1039 166
OData services 579	1046 167
Organizational assignment requests 323	1047 176
Organizational level mapping 372	1048 167
Organizational rules 189	1049 176
<i>definition</i> 190	1050 167
<i>mitigation</i> 190	1051 168
Organizational units 218	1052 168
Overview pages 563–564	1053 168
Owner group 195	1054 168
P	1055 167
Parallel processing 145	1061 169
<i>distributing jobs</i> 146	1062 169
<i>parameters</i> 146	1063 169
Parameters 85, 125, 158, 236, 310	1064 169
1001 158	1071 281
1002 159	1072 281
1003 159	1074 282
1004 159	1075 282
1005 159	1080 174
1006 159	1081 174
1007 159	1082 174
1008 159	1083 174
1011 160	1084 174
1012 160	1085 174
1013 161	1086 175
1014 161	1087 175
1015 161	1088 175
1016 162	1101 169
1021 162	1102 170
1022 162	1103 170
1023 163	1104 170
1024 163	1105 170
1025 164	1106 170
1026 164	1107 170
1027 165	1108 170
1028 165	1109 170
1029 165	1110 170
1030 165	1111 171
	1112 171
	1113 171
	1115 171
	1120 172

Parameters (Cont.)	Parameters (Cont.)
1121 172	2064 406
1122 172	2065 407
1123 172	3000 350
1124 172	3001 350
1125 173	3002 350
1126 173	3003 350
1127 173	3004 350
1128 171	3005 351
1302 289	3006 351
2004 403	3007 351
2005 404	3008 352
2006 404	3009 352
2007 406, 422	3010 352
2008 406, 424	3011 353
2009 289	3012 353
2010 289	3013 353
2011 290	3014 353
2012 290	3015 354
2013 290	3016 354
2014 291	3017 354
2015 291	3018 354
2016 430	3019 354
2017 430	3020 354
2018 430	3021 355
2019 430	3022 171
2020 430	3023 171
2023 430	3024 355
2024 292	3025 355
2031 283	3026 355
2032 283	3027 355
2033 283	3028 356
2034 283	3029 356
2035 283	3030 356
2036 284	3040 356
2037 284	3041 356
2038 284	3042 357
2039 285	3043 357
2040 285	4000 237
2042 285	4001 237
2043 286	4002 238
2044 286	4003 238
2045 286	4004 238
2046 287	4005 238
2047 288	4006 238
2048 288	4007 238
2050 173	4008 239
2051 171	4009 239
2060 173	4010 240
2061 173	4011 293
2062 406	4012 240
2063 406	4013 240

Parameters (Cont.)	
4014	240
4015	240
4016	293
4017	241
4018	241
4019	294
4020	241
4021	241
4022	294
4023	294
4025	241
4026	242
4027	242
4100	244
5001	159
5021	294
5022	295
5023	295
5024	295
5026	295
5027	296
5028	297
5031	298
5032	298
5033	242
6002	173
groups	85, 125
Passwords	303
Password self-service	337, 454
<i>admin-defined questions</i>	458
<i>challenge response</i>	457
<i>data sources</i>	462
<i>disable verification</i>	456
<i>document template</i>	460
<i>enable</i>	455
<i>global configuration</i>	455
<i>HR system</i>	461
<i>HR system settings</i>	456
<i>notification</i>	460
<i>reset password</i>	459
<i>security questions</i>	458
Paths	408, 471, 536, 549
<i>approval</i>	492
<i>approval options</i>	497
<i>comments</i>	499
<i>create</i>	493
<i>maintain</i>	492
<i>new roles</i>	496
Payment Card Industry (PCI)	25
Pending requests	646
Performance	87
Periodic reviews	401, 471
Permission-level risks	180
Permission levels	626
Permissions	154, 157
PFCG roles	482
PFCG user groups	483
Plug-ins	49, 63, 243
Port numbers	89
Post-installation configuration	51
Prerequisites	41
Presentation layer	32
Procedure calls	540
<i>definition</i>	541
<i>parameters</i>	541
Process initiator	262, 528
Project and product release names	369
Provisioning	295, 470
<i>automatic</i>	302
<i>individual systems</i>	303
<i>logs</i>	336
<i>manual</i>	302
<i>settings</i>	301
<i>type</i>	302

Q

Queued Remote Function Call (qRFC)	589
------------------------------------	-----

R

Reason codes	249–250
Rejection levels	501
Remediation	202
Reminders	414
<i>time periods</i>	415
<i>values</i>	415
Remote Function Calls (RFCs)	33, 97, 588
<i>connection</i>	100
<i>connection test</i>	100
<i>destination</i>	98
<i>setting up connections</i>	566–567
Reports	398
<i>GRAC_DELETE_REPORT_SPOOL</i>	168
<i>GRFN_CHECK_CDF</i>	623
<i>management dashboard</i>	176
<i>RS_APPL_REFRESH</i>	78
Repository object sync	138
Repository object sync job	192
Repository workspaces	104
<i>create</i>	105
<i>objects</i>	106

Request types	259, 304, 524, 591
<i>create</i>	592
<i>default</i>	591
<i>disable</i>	304
Rerouting	497
RESTful APIs	557
Result data objects	599
Result rules	258
Reviewers	429
Risk analysis	125, 162, 281, 470
<i>additional criteria</i>	207
<i>background</i>	167
<i>criteria</i>	203
<i>custom groups</i>	199
<i>detail</i>	205
<i>executive summary</i>	206
<i>format</i>	204
<i>management summary</i>	205
<i>objects</i>	211
<i>online vs offline</i>	155
<i>perform</i>	202
<i>permission-level</i>	180
<i>profile level</i>	210
<i>role level</i>	209
<i>spool</i>	167
<i>summary report</i>	204
<i>types</i>	156, 626
<i>user level</i>	203
<i>views</i>	206
Risk assessments	501
Risk management	435
Risk mitigation	125
Risk owners	154, 184, 193, 429
<i>verify</i>	434
Risk recognition	201
Risks	153, 181, 550
<i>create</i>	183
<i>modify</i>	185
<i>rulesets</i>	184
<i>types</i>	183
<i>violation types</i>	157
Risk simulation	212
<i>criteria</i>	213
<i>HR object level</i>	216
<i>profile level</i>	215
<i>role level</i>	214
<i>user level</i>	212
Risk terminator	126, 174
<i>configure</i>	229
<i>role assignment</i>	230
<i>user exits</i>	229
Risk Terminator Log report	230
Role administrators	354
<i>default approvers</i>	363
Role attributes	367, 390
<i>define</i>	368
Role-level risk analysis	386
Role mapping	291
Role methodology	346, 356, 376, 417
<i>BRFplus functions</i>	377
<i>default</i>	376
<i>mapping</i>	381
<i>steps</i>	376
Role owner assignment	405
Role owners	345
<i>authorizations</i>	358
<i>create</i>	358
<i>default</i>	359
<i>define</i>	357
Role prerequisites	374
<i>maintain</i>	375
<i>types</i>	374
Role repository	346
Roles	64, 382
<i>add default</i>	308
<i>assignment</i>	303
<i>child/parent</i>	291
<i>comments</i>	284
<i>copy</i>	68
<i>criticality level</i>	371
<i>default</i>	289, 308
<i>define</i>	383
<i>derive</i>	384, 395
<i>generate</i>	387, 396
<i>generate en masse</i>	67
<i>import</i>	389, 391
<i>mass update</i>	392
<i>provisioning</i>	286
<i>recertification</i>	397
<i>search</i>	285
<i>search display format</i>	287
<i>sensitivity</i>	369
<i>status</i>	350, 370
<i>update derived roles</i>	393
<i>update scheduling</i>	393
Role search	636
Role selection	283
Role types	
<i>deactivate</i>	364
<i>labels</i>	365
<i>maintain</i>	363
<i>maximum length</i>	366
<i>naming conventions</i>	366
Role usage synchronization	139
Route mapping	528, 536, 549, 658
<i>maintain</i>	504
Routing conditions	494
Routing levels	495

Routing rules 477, 537
 Rule IDs 537, 549
 Rule kinds 471, 477, 519
 Rules 185, 602
 condition 605
 create 605
 definition 603
 generate 179
 results 528
 Rulesets 176, 181, 518, 547, 607
 create 185, 607
 creation 548
 custom 186
 enable 608
 insert rules 608
 upload 187
 Rule types 471, 478, 520
 RZ10 profile parameters 56, 70, 92

S

SAP_PI_GRC 109
 SAP_UI 49
 SAP Application Performance Standard (SAPS) 45
 SAP Ariba 37
 SAP Audit Management 30
 SAP BTP cockpit 37
 SAP Business Client 32, 53
 SAP Business Integrity Screening 30
 SAP Business Technology Platform (SAP BTP) 557
 SAP Business Workflow
 engine 72
 SAP Cloud Identity Access Governance ... 37, 127
 SAP Cloud Identity Access Governance
 bridge 38
 SAP Concur 37
 SAP Enterprise Portal 32, 49, 113, 115, 118, 144
 integrate 113
 SAP ERP HCM 131
 SAP Fieldglass 37
 SAP Fiori 32, 53, 244, 555
 app types 562
 architecture 556
 benefits 560
 cache issues 584
 CDS 586
 central hub deployment 558, 571
 client 557
 configuration 564

SAP Fiori (Cont.)
 deployment options 558
 embedded deployment 558
 overview 555
 prerequisites 565
 raise requests 327
 reference lost errors 585
 terminology 561
 troubleshooting 583
 working with apps 581
 SAP Fiori apps reference library 562
 SAP Fiori Cloud 560
 SAP Fiori launchpad 327, 562
 SAP Gateway 72, 558
 activate 566
 embedded 559
 hub 560
 routing configuration 576
 SAP GRC solutions 25, 29, 31, 41
 technical content 577
 SAP GUI 32, 556–557
 SAP HANA 109
 development perspective 104
 integration API 104
 plug-in 101–102
 SAP HANA database 101, 110
 connection 101
 connect to SAP GRC 111
 test connection 111
 SAP HANA Studio 102
 errors 109
 SAP Identity Management 36, 294, 357
 SAP Information Lifecycle 127
 SAP NetWeaver 32, 42
 connect 98
 SAP One Support Launchpad 101
 SAP Process Control 29
 SAP Regulation Management by
 Greenlight 30
 SAP Risk Management 30
 SAP Software Change Registration (SSCR) ... 662
 SAP SuccessFactors 37, 131
 SAP SuccessFactors Employee Central 200
 SAPUI5 32
 SAP Web IDE 557
 Sarbanes-Oxley (SOX) 25, 30, 150
 Title 1 152
 Title 2 152
 Title 3 153
 Title 4 153
 Secure Sockets Layer (SSL) 568

Securities and Exchange Commission (SEC) 152
 Segregation of duties (SoD) 25, 150, 537
 reviews 126
 Semantic objects 562
 Service level agreements (SLAs) 313, 470
 due date 315
 IDs 314
 service levels 315
 trigger actions 316
 type 314
 Service Provisioning Markup Language (SPML) 113
 Simulation 534
 Sizing 45
 exercise 46
 scenarios 46
 SMTP server 88
 inbound/outbound flow 93
 SMTP service configuration 91
 SoD reviews 401, 428
 actions 438
 admin review 437
 configuration 428
 generate data 436
 generate new requests 439
 manage rejections 439
 notification templates 431
 number of requests 436
 perform 438
 review requests 438
 schedule 440
 set up parameters 429
 set up workflows 431
 update workflow 437
 Spool files 168
 Spool type 125
 SQL editor 108
 connect to database 108
 Stages 409, 471, 549
 add 409, 493
 define 493
 stage-level definitions 496
 Standard operating procedures (SOPs) 614
 add to emails 617
 Structures 622
 update 623
 Subprocesses 68, 154, 219
 default 350
 Subscenarios 120
 Superuser privilege management log
 sync 139

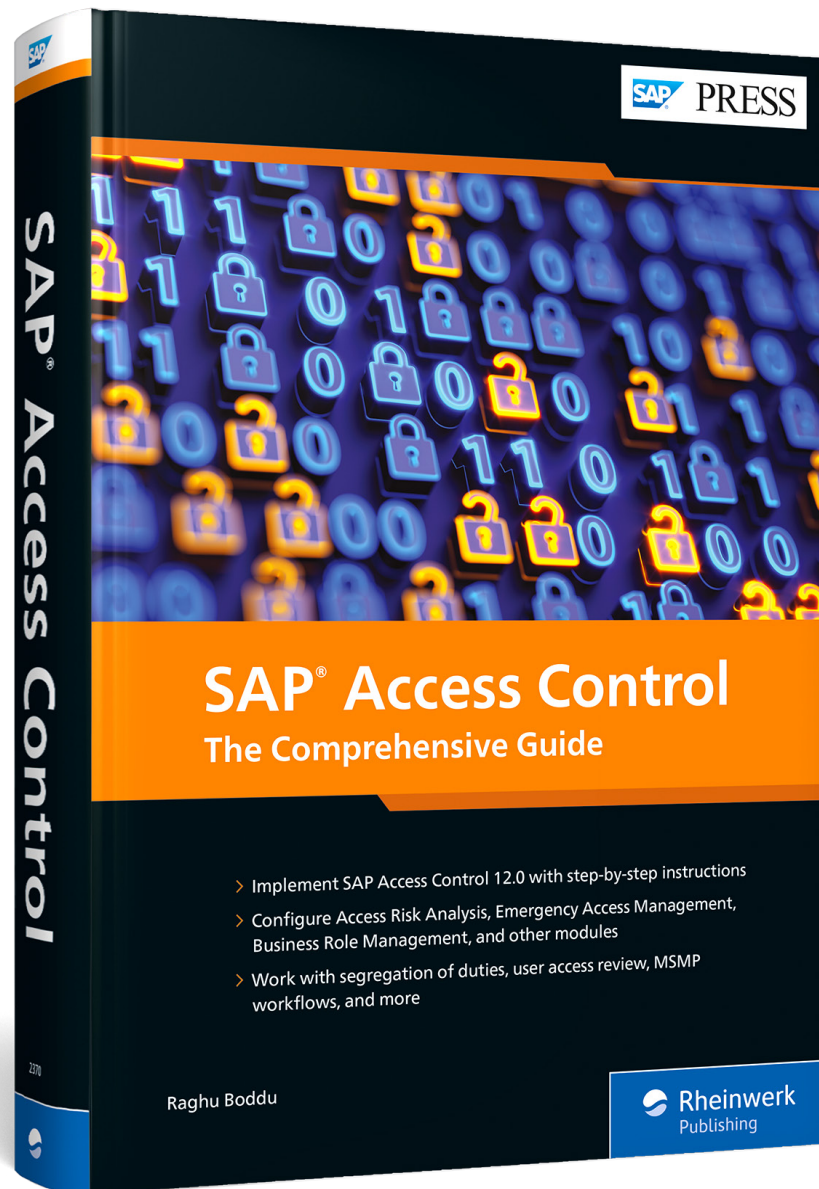
Supplementary rules 190
 create 190
 definition 191
 Supported systems 36
 Synchronization jobs 137, 192
 schedule 407, 432
 System administrators 44
 System aliases 568, 570
 create 575
 mapping 574
 System audits 28
 System users 133

T

Table DB_LOOKUP 533
 Table operations 543, 546
 Boolean setting 544
 definition 543
 Tabstrip control 634
 Target connectors 121
 Target mappings 561
 Target system 575
 TCP/IP connection 132
 Technical catalog 561
 Technical roles 293
 Templates 311
 create 311
 request details 313
 use 312
 Temporary tables 539
 Termination requests 600
 Test cases 388
 Ticket numbers 356
 Time zones 47
 Top expression 259, 362, 526, 653
 Training certification 126
 Training verification 293
 Transaction
 /IWBEP/ERROR_LOG 585
 /IWFND/CACHE_CLEANUP 584
 /IWFND/MAINT_SERVICE 569
 /N/GRCPI/GRIA_EAM 240, 254, 271
 /N/IWFND/ERROR_LOG 583
 /N/IWFND/MAINT_SERVICE 583
 /N/UI2/FLP 327, 332, 562
 /N/UI2/FLPD_CUST 581
 /UI2/FLPD_CUST 562, 578–579
 /UI2/GW_SYS_ALIAS 574
 ALL1 168, 512
 BRFplus 521, 530, 595, 651
 DBCO 111

Transaction (Cont.)		Transaction (Cont.) (Cont.)	
FKO2	189	SUPC	67
GRAC_ACT_USAGE_SYNC	139	SWDD	83
GRAC_AUTH_SYNC	137	SWE2	79
GRAC_BATCH_RA	155	SWU3	71, 75
GRAC_EAM	254	VA31	180
GRAC_GEN_ERM_BRFRULE	378	Transactional apps	562
GRAC_REP_OBJ_SYNC	138	Transport layer	551
GRFNMW_CN_VERA	508	Transport requests	117, 485, 529, 553, 596
GRFNMW_CONFIGURE	508, 629	Trigger values	259
GRFNMW_CONFIGURE_WD	245–246, 260, 412, 442, 481, 493, 527, 534, 548, 615, 657	U	
GRFNMW_DBGMONITOR_WD	510	UIGRAC01	49
Transaction (Cont.)		UIGRC001	49
GRFNMW_DEBUG	511	User access reviews	126–127, 401
GRFNMW_DEBUG_MSG	511	<i>actions</i>	425
GRFNMW_DEV_CONFIG	513	<i>configuration</i>	402
GRFNMW_DEV_RULES	522, 530, 537	<i>configuration parameters</i>	403
GRFNMW_GEN_VERSION	506–507	<i>features</i>	402
GRFNMW_MONITOR	513	<i>generate data</i>	418
LDAP	133, 135	<i>generating new requests</i>	427
LPCONFIG	115	<i>managing rejections</i>	426
MIGO	180	<i>perform</i>	424
NWBC	405, 416–417, 648	<i>priority</i>	404
PFCG	67, 582	<i>recurring plan</i>	418
PFTC	80, 441	<i>rejecting requests</i>	426
RZ10	56, 89, 145	<i>Request Review screen</i>	423
SA38	47	<i>reviewing requests</i>	424
SACM	586	<i>schedule</i>	421
SCOT	249, 491	<i>triggering workflows</i>	423
SCPR20	59, 177, 281, 349	<i>updating workflows</i>	423
SE11	620, 622–623	<i>variants</i>	419
SE16	413	<i>workflows</i>	407
SE21	550	User assignments	296
SE37	47, 484, 610, 648, 667	User authentication source	448
SE38	111, 142, 623	User data type	131
SE61	247, 355, 431, 487, 615, 678	User defaults	309
SE80	617	User exits	63
SICF	53, 450, 452, 520, 573, 619	<i>parameters</i>	63
SLG1	159, 421, 514, 610	User groups	295, 310
SLICENSE	43–44	<i>add users</i>	199
SM19	238	<i>assign</i>	631
SM30	490, 575	<i>custom</i>	198
SM37	178, 415	User license requirements	44
SM59	98, 100, 113, 132, 567	User management engine (UME)	113
SMICM	56, 167	User managers	404, 429
SPRO_ADMIN	537	User profiles	285
SQVI	406	Users	579
SU01	90, 195, 416		
SU24	137		
SUGR	195, 483		

V		Workflow builder	83
Variants	419	Workflows	86, 125, 169, 197
Versions	506	Work Inbox	330
Violations	191	Work Inbox app	330, 332
Virsa Systems	30	Work items	471
W		Z	
Web Dynpro application	659	Z enhancements	660
Web services-based connectors	122		
Where-used list	62		



Raghu Boddu

SAP Access Control The Comprehensive Guide

695 pages | 06/2023 | \$99.95 | ISBN 978-1-4932-2370-1

 www.sap-press.com/5636



Raghu Boddu is a seasoned expert with more than 25 years of experience in the SAP security and Governance, Risk and Compliance (GRC) industry. He is well-known in the community for his ability to solve complex problems with simple solutions and is highly sought after for his expertise in risk and fraud management.

Raghu has led numerous successful projects throughout his career, including the implementation of comprehensive security and risk management programs using SAP GRC solutions for Fortune 500 companies. He has also contributed to the development of innovative software solutions for use cases such as firefighter log review automation, protecting SAP systems from identity and data theft, and many more, that have helped organizations secure their SAP systems and streamline their GRC processes.

In addition to his extensive industry experience, Raghu holds several certifications including Certified Fraud Examiner (CFE), Certified Information Systems Auditor (CISA), and Certified Data Privacy Solutions Engineer (CDPSE). He has also served on the board of the Hyderabad Chapter of ISACA.

Raghu currently heads ToggleNow Software Solutions and leads their GRC innovation practice. Raghu enjoys sharing his knowledge and expertise through speaking engagements, blog posts, and mentorship programs. He is passionate about helping others succeed in the industry and is dedicated to advancing the SAP security and GRC field.

We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.