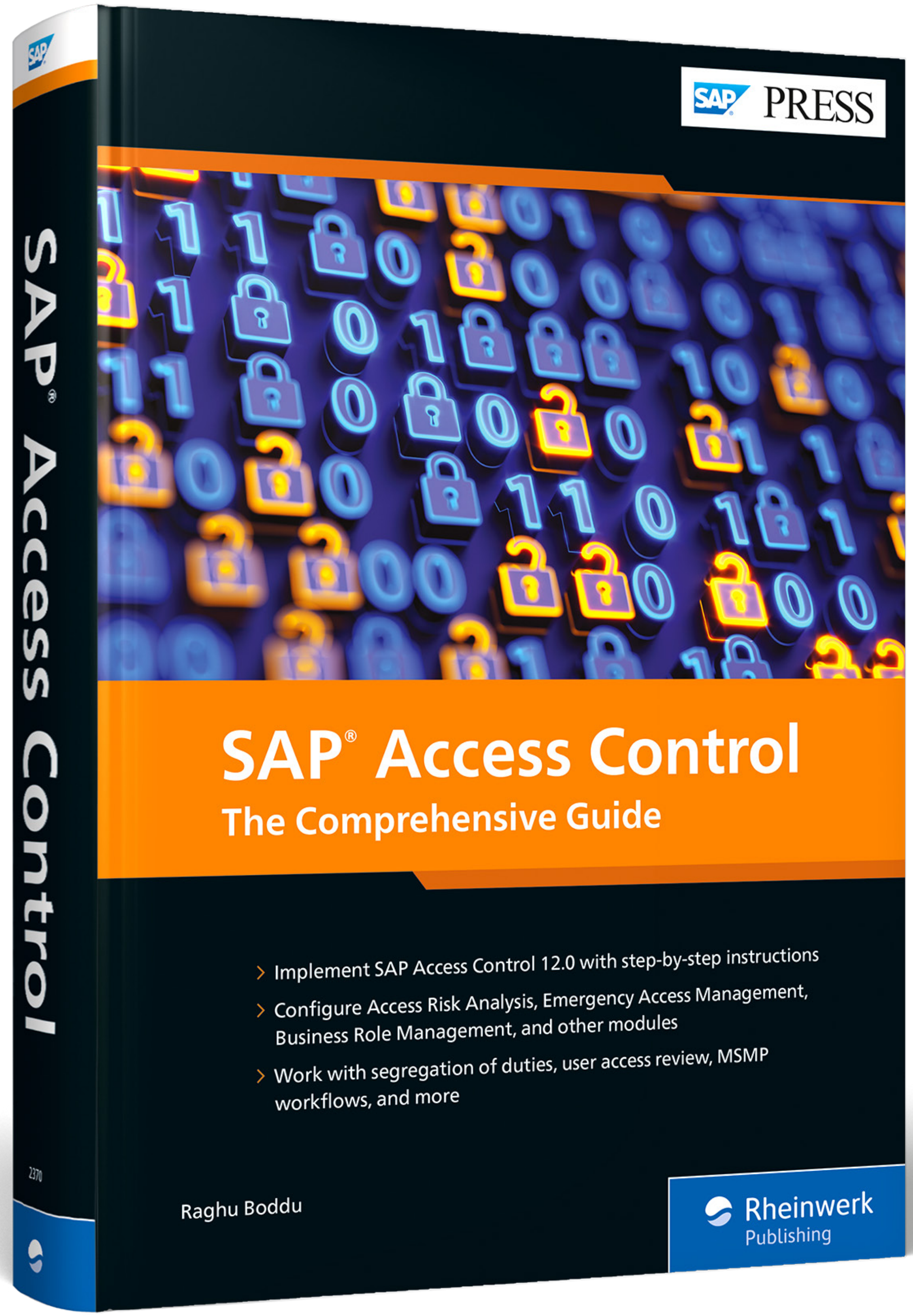


Reading Sample

This sample chapter covers the initial configuration of SAP Access Control. It provides step-by-step instructions for quickly checking the add-ons/plug-ins, 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.

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/plug-ins 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 SP00: Foundation application layer on SAP GRC system
- GRCFND_A v1200: Add-on installation on the SAP GRC system
- UIGRAC01 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
- GRCPIERP 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.

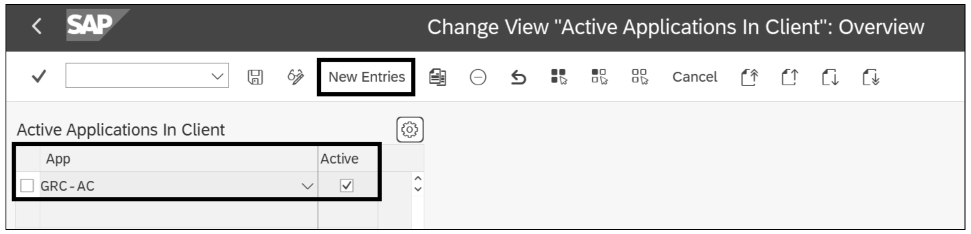
3.2.1 Activating Applications and Services

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.



Active Applications In Client

App	Active
GRC - AC	☑

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

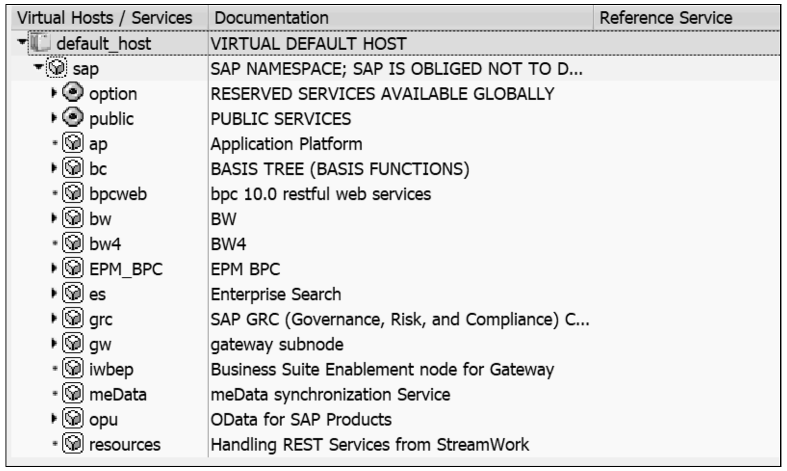
Application activation is a configuration setting in Transaction SPRO that must be captured in a transport request and imported into other systems in the landscape. This approach eliminates the need for administrators to perform the same configuration repetitively because settings are automatically applied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

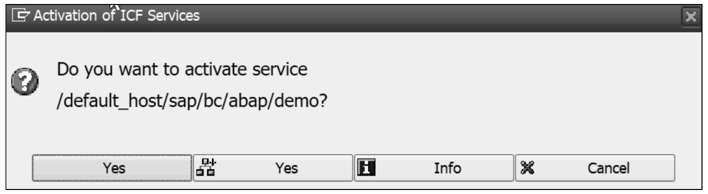
1. Execute Transaction SICF.
2. Right-click the specific service node and click **Activate**, as shown in Figure 3.2.



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.



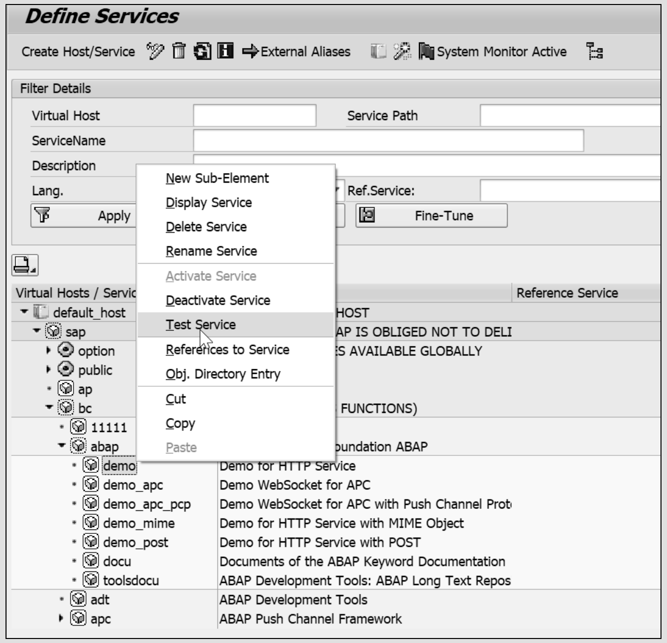
Do you want to activate service
/default_host/sap/bc/abap/demo?

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

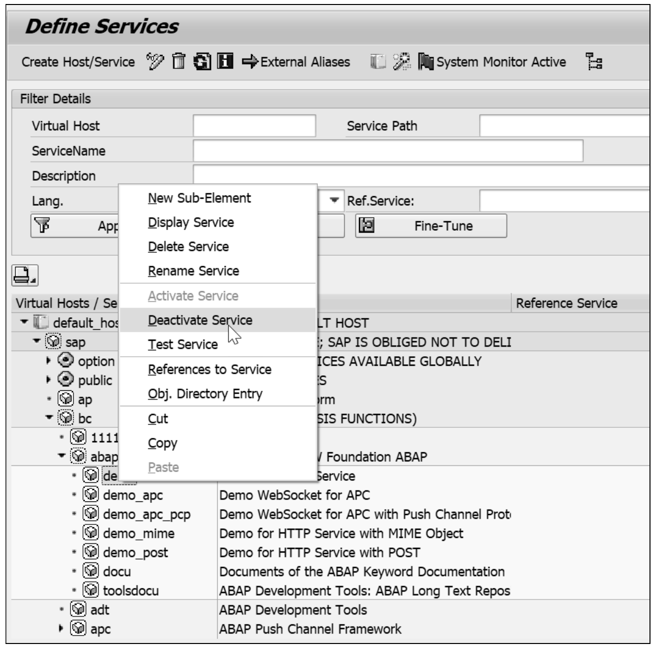
Once a service is activated, you can right-click it and choose **Test Service**, as shown in Figure 3.4.



Virtual Hosts / Servic		Reference Service
default_host	HOST	
sap	AP IS OBLIGED NOT TO DELI	
option	S AVAILABLE GLOBALLY	
public		
ap		
bc	FUNCTIONS)	
11111		
abap	oundation ABAP	
demo	Demo for HTTP Service	
demo_apc	Demo WebSocket for APC	
demo_apc_pcp	Demo WebSocket for APC with Push Channel Prot	
demo_mime	Demo for HTTP Service with MIME Object	
demo_post	Demo for HTTP Service with POST	
docu	Documents of the ABAP Keyword Documentation	
toolsdocu	ABAP Development Tools: ABAP Long Text Repos	
adt	ABAP Development Tools	
apc	ABAP Push Channel Framework	

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.



Virtual Hosts / Se		Reference Service
default_hos	LT HOST	
sap	; SAP IS OBLIGED NOT TO DELI	
option	ICES AVAILABLE GLOBALLY	
public	S	
ap	rm	
bc	SIS FUNCTIONS)	
1111		
abap	/ Foundation ABAP	
de	Service	
demo_apc	Demo WebSocket for APC	
demo_apc_pcp	Demo WebSocket for APC with Push Channel Prot	
demo_mime	Demo for HTTP Service with MIME Object	
demo_post	Demo for HTTP Service with POST	
docu	Documents of the ABAP Keyword Documentation	
toolsdocu	ABAP Development Tools: ABAP Long Text Repos	
adt	ABAP Development Tools	
apc	ABAP Push Channel Framework	

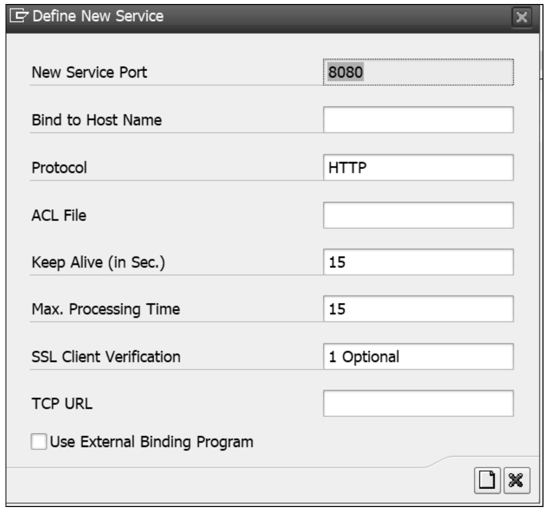
Figure 3.5 Deactivate Service Option

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.



New Service Port	8080
Bind to Host Name	
Protocol	HTTP
ACL File	
Keep Alive (in Sec.)	15
Max. Processing Time	15
SSL Client Verification	1 Optional
TCP URL	

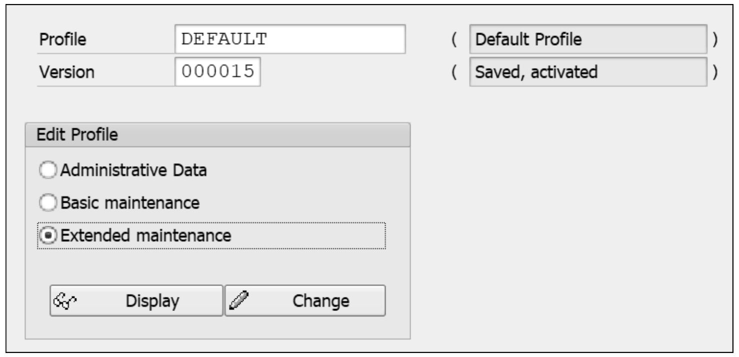
□ Use External Binding Program

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.



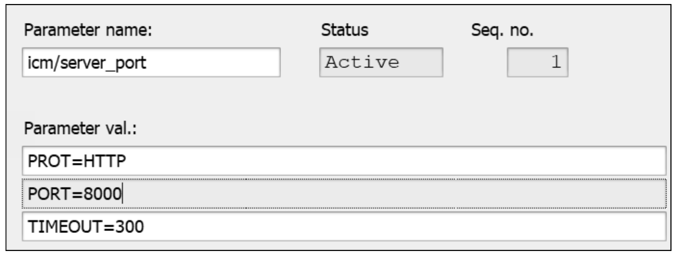
Profile	DEFAULT	(Default Profile)
Version	000015	(Saved, activated)

Edit Profile

○ Administrative Data
○ Basic maintenance
● Extended maintenance

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.



Parameter name:	Status	Seq. no.
icm/server_port	Active	1

Parameter val.:

```
PROT=HTTP
PORT=8000
TIMEOUT=300
```

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_LABLES	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

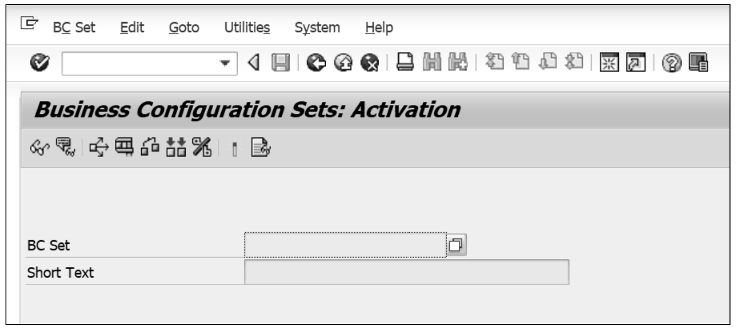
Name of the BC Set	Description
GRAC_RA_RULESET_SAP_APO	BC Set for AC Rules - SAP APO
GRAC_RA_RULESET_SAP_BASIS	BC Set for AC Rules - SAP BASIS
GRAC_RA_RULESET_SAP_CRM	BC Set for AC Rules - SAP CRM
GRAC_RA_RULESET_SAP_ECCS	BC Set for AC Rules - SAP ECCS
GRAC_RA_RULESET_SAP_HANA	BC Set for AC Rules - SAP 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_METHODOLOGY	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.

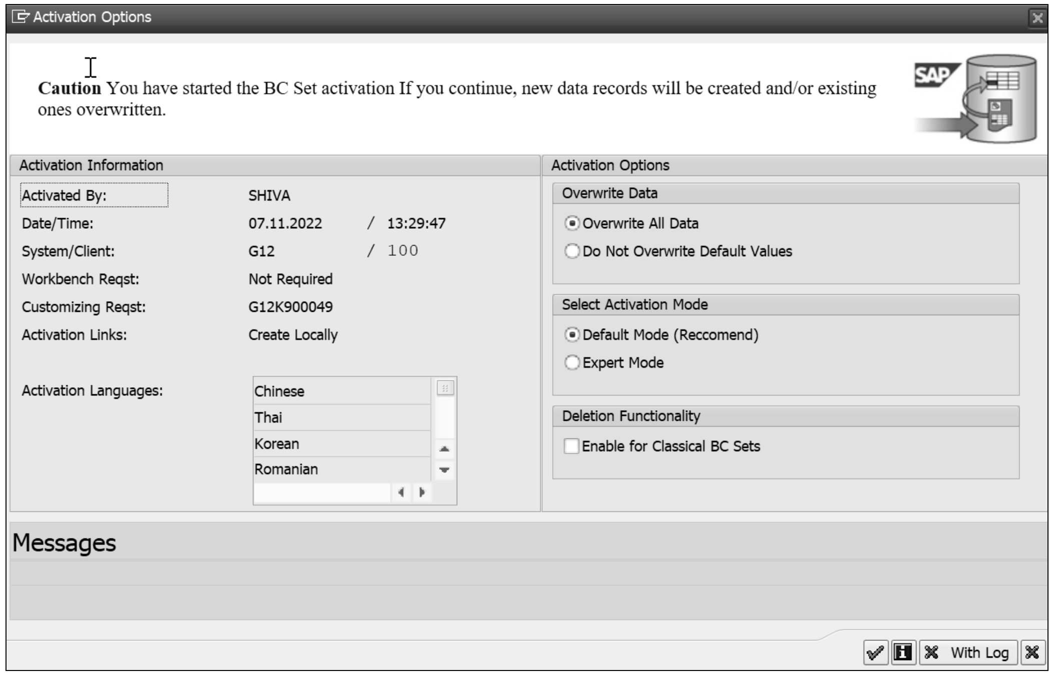


Business Configuration Sets: Activation

BC Set	
Short Text	

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.


Activation Options

Caution You have started the BC Set activation If you continue, new data records will be created and/or existing ones overwritten.

Activation Information

Activated By:	SHIVA	
Date/Time:	07.11.2022	/ 13:29:47
System/Client:	G12	/ 100
Workbench Reqst:	Not Required	
Customizing Reqst:	G12K900049	
Activation Links:	Create Locally	
Activation Languages:	Chinese Thai Korean Romanian	

Activation Options

Overwrite Data
● Overwrite All Data
○ Do Not Overwrite Default Values

Select Activation Mode
● Default Mode (Recommend)
○ Expert Mode

Deletion Functionality
□ Enable for Classical BC Sets

Messages

Figure 3.10 BC Set Activation Options

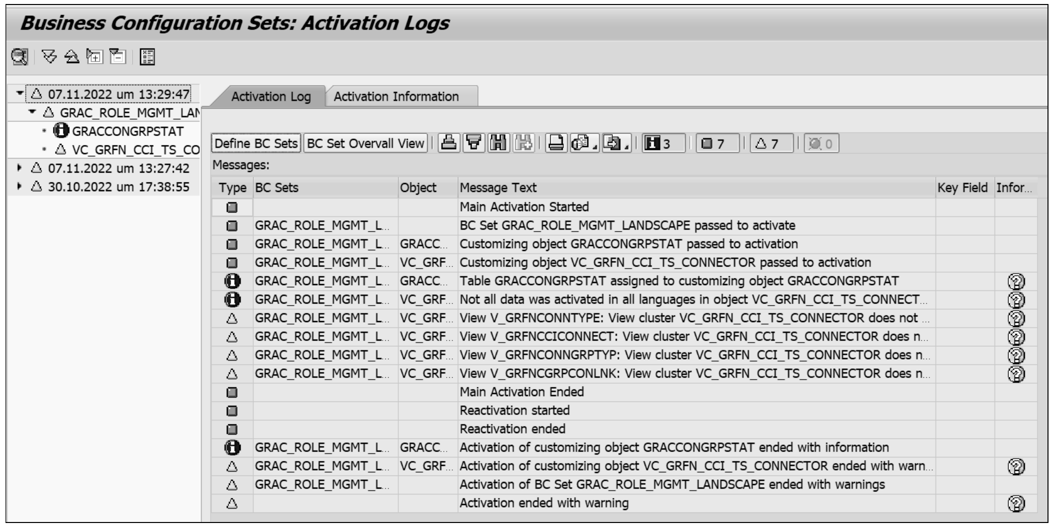
Once activated, activation logs are available that detail information about the activation. Click the **View logs** button or press Ctrl+F2 to verify the logs. In the logs, you may notice various status icons along with descriptions.

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.
ℹ	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.


Business Configuration Sets: Activation Logs

△ 07.11.2022 um 13:29:47
△ GRAC_ROLE_MGMT_LAN
ℹ GRACCONGRPSTAT
△ VC_GRFN_CCI_TS_CO
△ 07.11.2022 um 13:27:42
△ 30.10.2022 um 17:38:55

Messages:

Type	BC Sets	Object	Message Text	Key Field	Infor...
■			Main Activation Started		
■	GRAC_ROLE_MGMT_L...		BC Set GRAC_ROLE_MGMT_LANDSCAPE passed to activate		
■	GRAC_ROLE_MGMT_L...	GRACC...	Customizing object GRACCONGRPSTAT passed to activation		
■	GRAC_ROLE_MGMT_L...	VC_GRF...	Customizing object VC_GRFN_CCI_TS_CONNECTOR passed to activation		
ℹ	GRAC_ROLE_MGMT_L...	GRACC...	Table GRACCONGRPSTAT assigned to customizing object GRACCONGRPSTAT		?
ℹ	GRAC_ROLE_MGMT_L...	VC_GRF...	Not all data was activated in all languages in object VC_GRFN_CCI_TS_CONNECT...		?
△	GRAC_ROLE_MGMT_L...	VC_GRF...	View V_GRFNCONNTYPE: View cluster VC_GRFN_CCI_TS_CONNECTOR does not ...		?
△	GRAC_ROLE_MGMT_L...	VC_GRF...	View V_GRFNCCICONNECT: View cluster VC_GRFN_CCI_TS_CONNECTOR does n...		?
△	GRAC_ROLE_MGMT_L...	VC_GRF...	View V_GRFNCONNGRPTYP: View cluster VC_GRFN_CCI_TS_CONNECTOR does n...		?
△	GRAC_ROLE_MGMT_L...	VC_GRF...	View V_GRFNCGRPCONLNK: View cluster VC_GRFN_CCI_TS_CONNECTOR does n...		?
■			Main Activation Ended		
■			Reactivation started		
■			Reactivation ended		
ℹ	GRAC_ROLE_MGMT_L...	GRACC...	Activation of customizing object GRACCONGRPSTAT ended with information		
△	GRAC_ROLE_MGMT_L...	VC_GRF...	Activation of customizing object VC_GRFN_CCI_TS_CONNECTOR ended with warn...		?
△	GRAC_ROLE_MGMT_L...		Activation of BC Set GRAC_ROLE_MGMT_LANDSCAPE ended with warnings		
△			Activation ended with warning		?

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 GRCPIERP, 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

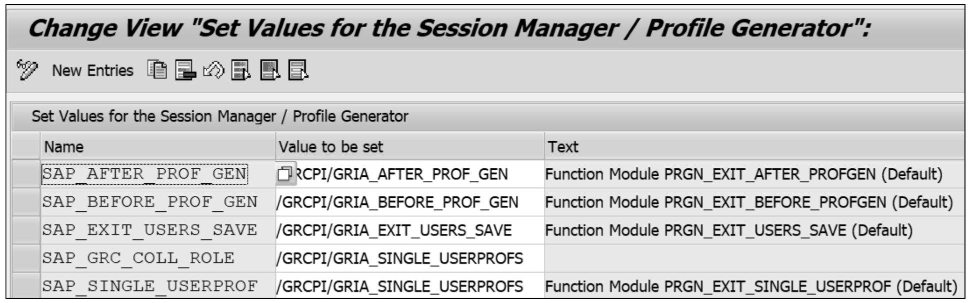
You'll also need to maintain user exits to enable the risk terminator option. User exit settings are required to utilize the risk terminator in role maintenance (Transaction PFCG) and user management (Transactions SU01, SU10, and SU12). The risk terminator enables real-time risk analysis while making 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	/GRCPI/GRIA_AFTER_PROF_GEN	**Function Module PRGN_EXIT_AFTER_PROFGEN (Default)**
SAP_BEFORE_PROF_GEN	/GRCPI/GRIA_BEFORE_PROF_GEN	**Function Module PRGN_EXIT_BEFORE_PROFGEN (Default)**
SAP_EXIT_USERS_SAVE	/GRCPI/GRIA_EXIT_USERS_SAVE	**Function Module PRGN_EXIT_USERS_SAVE (Default)**
SAP_SINGLE_USERPROF	/GRCPI/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":

Set Values for the Session Manager / Profile Generator

Name	Value to be set	Text
SAP_AFTER_PROF_GEN	RCPI/GRIA_AFTER_PROF_GEN	Function Module PRGN_EXIT_AFTER_PROFGEN (Default)
SAP_BEFORE_PROF_GEN	/GRCPI/GRIA_BEFORE_PROF_GEN	Function Module PRGN_EXIT_BEFORE_PROFGEN (Default)
SAP_EXIT_USERS_SAVE	/GRCPI/GRIA_EXIT_USERS_SAVE	Function Module PRGN_EXIT_USERS_SAVE (Default)
SAP_GRC_COLL_ROLE	/GRCPI/GRIA_SINGLE_USERPROFS	
SAP_SINGLE_USERPROF	/GRCPI/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

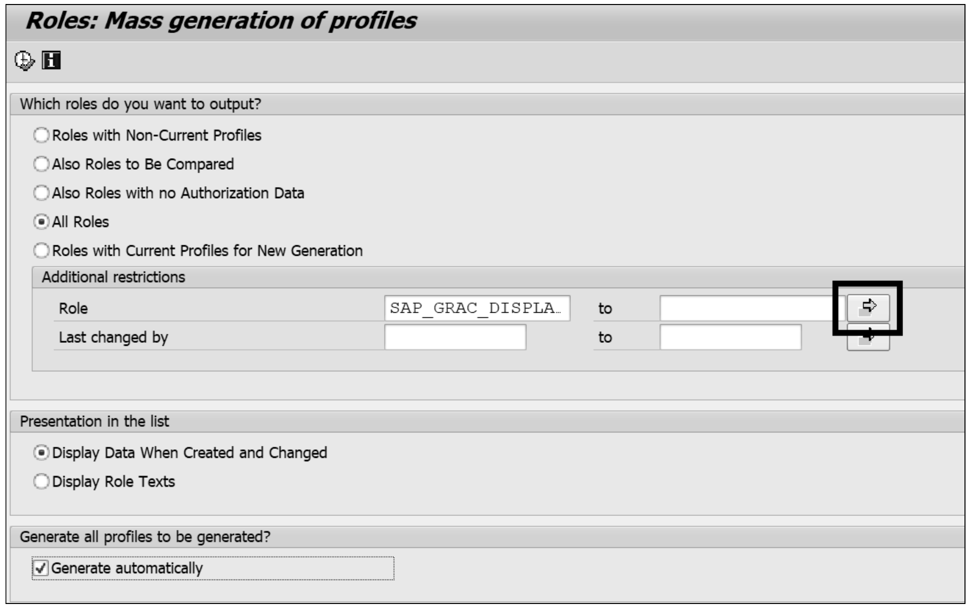
Role Name	Purpose of the Role
SAP_GRAC_REPORTS	Provides authorization to execute all the SAP Access Control reports under the **Reports & Analytics** tab. Usually assigned to the key business teams.
SAP_GRAC_RISK_ANALYSIS	Provides authorization to perform risk analysis at both the user level and the 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_CNTLR	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
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

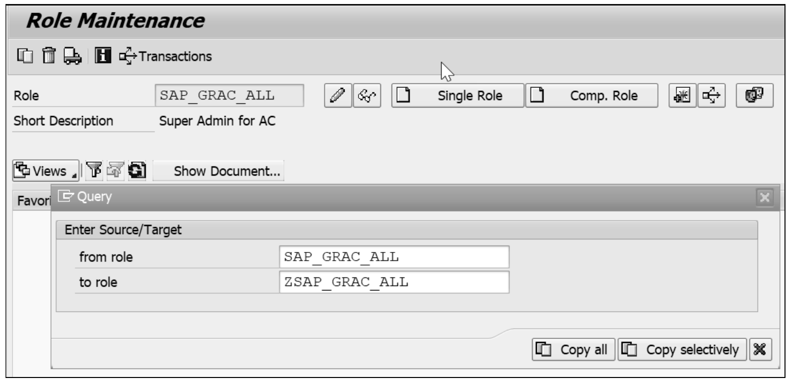
To generate roles en masse, follow these steps:

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.



Role: SAP_GRAC_ALL
Short Description: Super Admin for AC

Enter Source/Target
from role: SAP_GRAC_ALL
to role: ZSAP_GRAC_ALL

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.

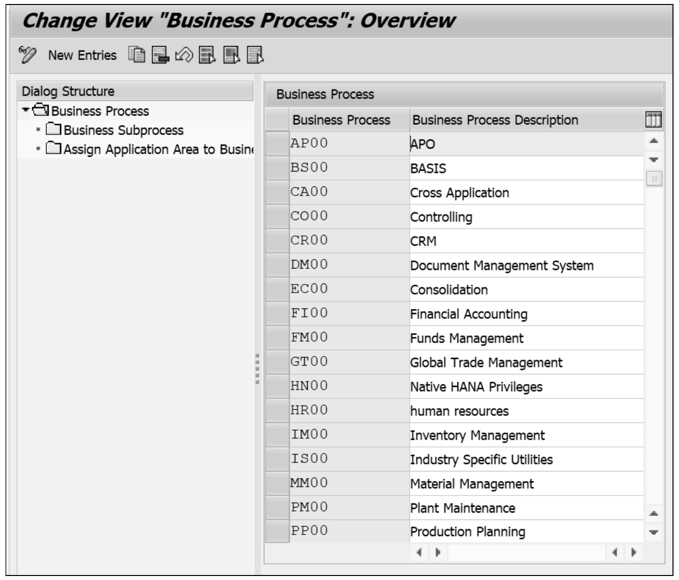
3.2.8 Defining Business Processes and Subprocesses

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.

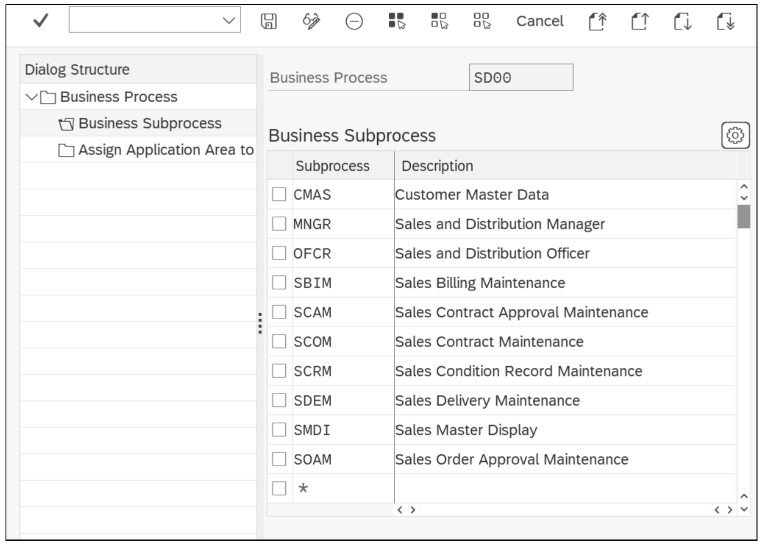

Change View "Business Process": Overview
New Entries
Dialog Structure
Business Process
Business Subprocess
Assign Application Area to Busin

Business Process

Business Process	Business Process Description
AP00	APO
BS00	BASIS
CA00	Cross Application
CO00	Controlling
CR00	CRM
DM00	Document Management System
EC00	Consolidation
FI00	Financial Accounting
FM00	Funds Management
GT00	Global Trade Management
HN00	Native HANA Privileges
HR00	human resources
IM00	Inventory Management
IS00	Industry Specific Utilities
MM00	Material Management
PM00	Plant Maintenance
PP00	Production Planning

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.



Business Process: SD00

Business Subprocess

Subprocess	Description
□ CMAS	Customer Master Data
□ MNGR	Sales and Distribution Manager
□ OFCR	Sales and Distribution Officer
□ SBIM	Sales Billing Maintenance
□ SCAM	Sales Contract Approval Maintenance
□ SCOM	Sales Contract Maintenance
□ SCRM	Sales Condition Record Maintenance
□ SDEM	Sales Delivery Maintenance
□ SMDI	Sales Master Display
□ SOAM	Sales Order Approval Maintenance
□ *	

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

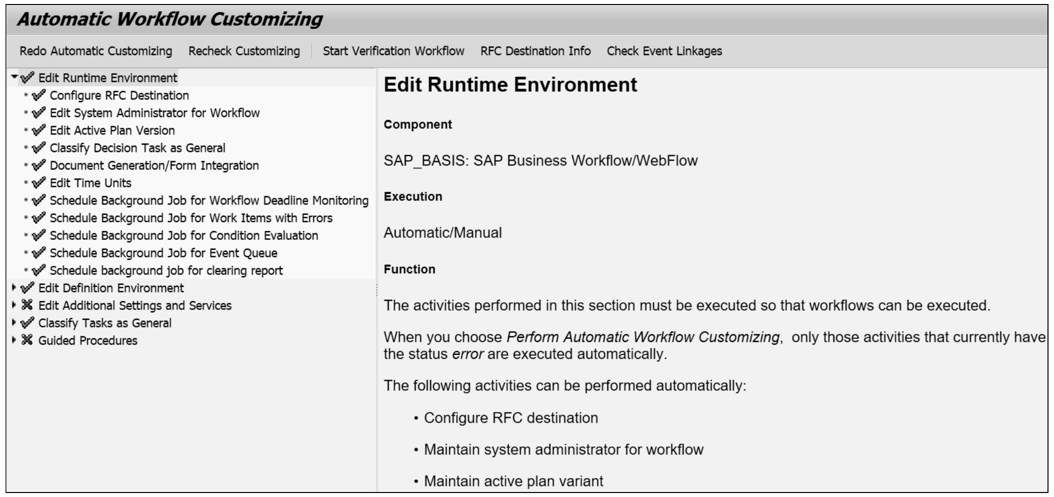
We highly recommend you consult the Basis team before changing parameter values since the configuration depends on many other parameters. Once the parameter is maintained correctly, the next step is to proceed with the automatic workflow configuration.

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 (√).

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.


Automatic Workflow Customizing
Redo Automatic Customizing
Recheck Customizing
Start Verification Workflow
RFC Destination Info
Check Event Linkages
✓ Edit Runtime Environment
✓ Configure RFC Destination
✓ Edit System Administrator for Workflow
✓ Edit Active Plan Version
✓ Classify Decision Task as General
✓ Document Generation/Form Integration
✓ Edit Time Units
✓ Schedule Background Job for Workflow Deadline Monitoring
✓ Schedule Background Job for Work Items with Errors
✓ Schedule Background Job for Condition Evaluation
✓ Schedule Background Job for Event Queue
✓ Schedule background job for clearing report
✓ Edit Definition Environment
✗ Edit Additional Settings and Services
✓ Classify Tasks as General
✗ Guided Procedures

Edit Runtime Environment

Component

SAP_BASIS: SAP Business Workflow/WebFlow

Execution

Automatic/Manual

Function

The activities performed in this section must be executed so that workflows can be executed.

When you choose *Perform Automatic Workflow Customizing*, only those activities that currently have the status *error* are executed automatically.

The following activities can be performed automatically:

- Configure RFC destination
- Maintain system administrator for workflow
- Maintain active plan variant

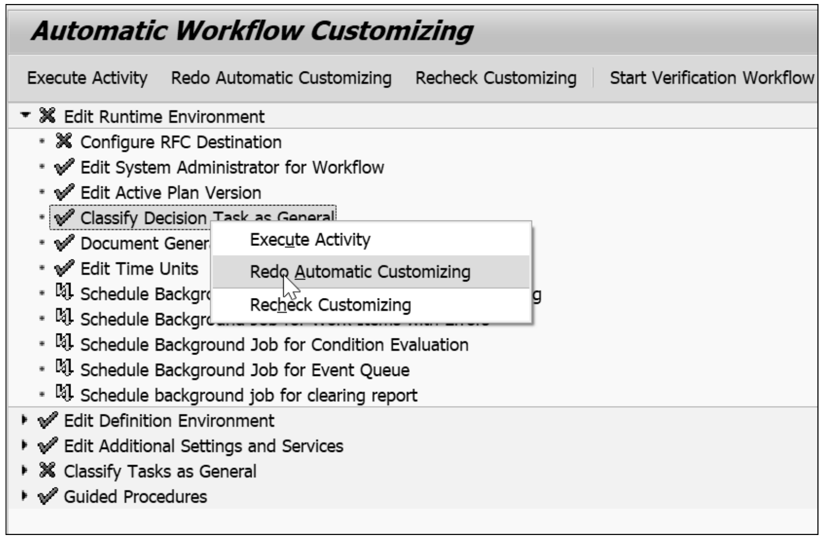
Figure 3.17 Automatic Workflow Customizing

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.



Automatic Workflow Customizing

Execute Activity | Redo Automatic Customizing | Recheck Customizing | Start Verification Workflow

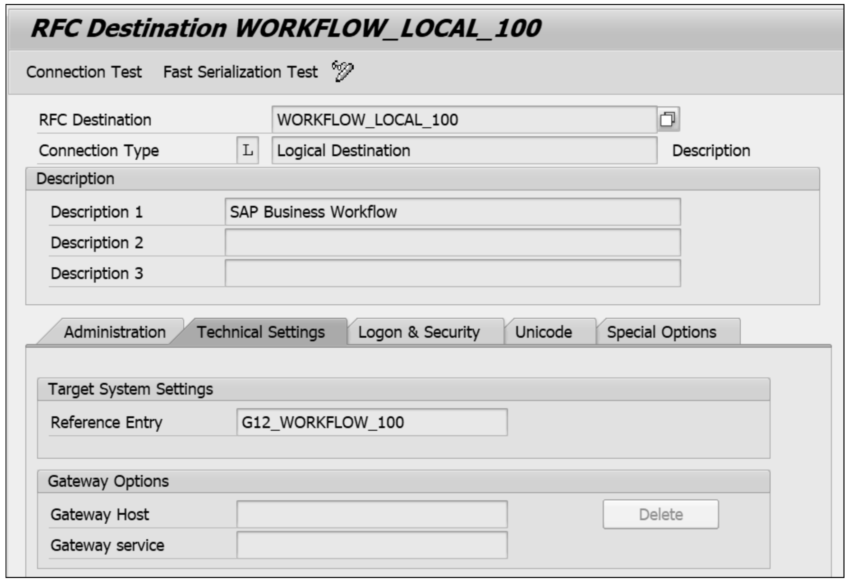
- ✗ Edit Runtime Environment
  - ✗ Configure RFC Destination
  - ✓ Edit System Administrator for Workflow
  - ✓ Edit Active Plan Version
  - ✓ Classify Decision Task as General
  - ✓ Document Gener
  - ✓ Edit Time Units
  - Schedule Backgr g
  - Schedule Backgr
  - Schedule Background Job for Condition Evaluation
  - Schedule Background Job for Event Queue
  - Schedule background job for clearing report
- ✓ Edit Definition Environment
- ✓ Edit Additional Settings and Services
- ✗ Classify Tasks as General
- ✓ Guided Procedures

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.



RFC Destination WORKFLOW_LOCAL_100

Connection Test | Fast Serialization Test

RFC Destination	WORKFLOW_LOCAL_100
Connection Type	L Logical Destination

Description

Description 1	SAP Business Workflow
Description 2	
Description 3	

Administration | Technical Settings | Logon & Security | Unicode | Special Options

Target System Settings

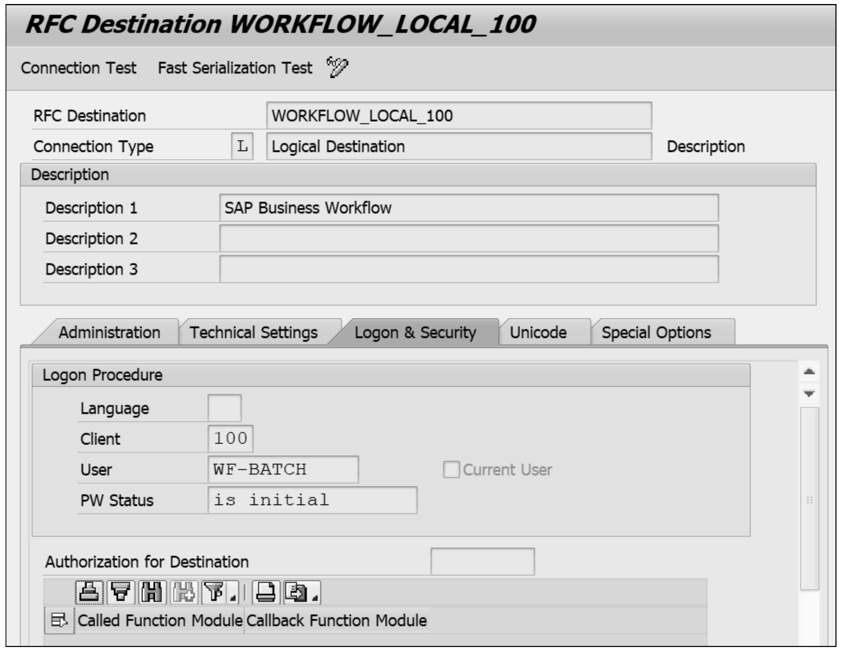
Reference Entry	G12_WORKFLOW_100

Gateway Options

Gateway Host	
Gateway service	

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.**



RFC Destination WORKFLOW_LOCAL_100

Connection Test | Fast Serialization Test

RFC Destination	WORKFLOW_LOCAL_100
Connection Type	L Logical Destination

Description

Description 1	SAP Business Workflow
Description 2	
Description 3	

Administration | Technical Settings | Logon & Security | Unicode | Special Options

Logon Procedure

Language	
Client	100
User	WF-BATCH
PW Status	is initial

□ Current User

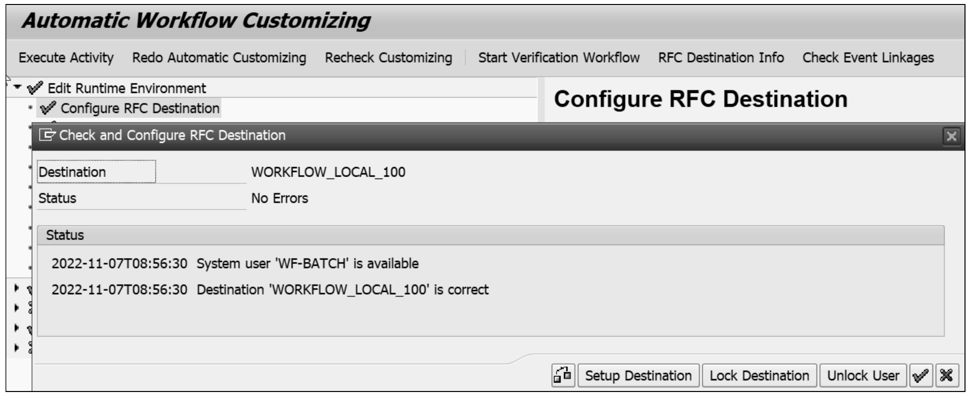
Authorization for Destination

Called Function Module | Callback Function Module

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.


Automatic Workflow Customizing
Execute Activity
Redo Automatic Customizing
Recheck Customizing
Start Verification Workflow
RFC Destination Info
Check Event Linkages
Edit Runtime Environment
Configure RFC Destination
Configure RFC Destination
Check and Configure RFC Destination
Setup Destination
Lock Destination
Unlock User

Destination WORKFLOW_LOCAL_100

Status No Errors

Status

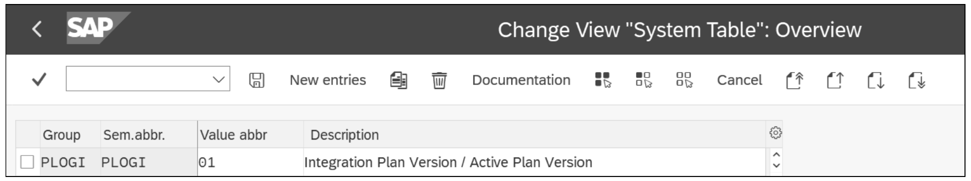
2022-11-07T08:56:30 System user 'WF-BATCH' is available

2022-11-07T08:56:30 Destination 'WORKFLOW_LOCAL_100' is correct

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 recommending 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.



	Group	Sem.abbr.	Value abbr	Description
□	PLOGI	PLOGI	01	Integration Plan Version / Active Plan Version

Figure 3.22 Plan Version Configuration

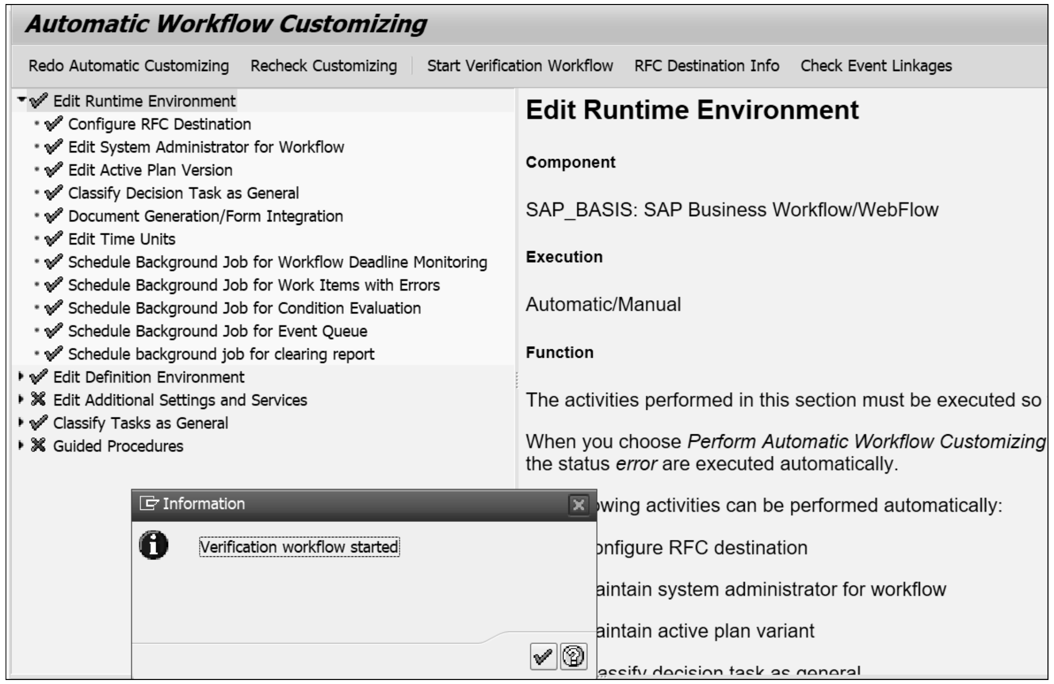
You can only have one plan version in the **Active** status. All the workflow components utilize the active or integrated plan version. If **Execute Activity** is used, **01** is set as the active plan version automatically.

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.


Automatic Workflow Customizing
Redo Automatic Customizing
Recheck Customizing
Start Verification Workflow
RFC Destination Info
Check Event Linkages
Information

✓ Edit Runtime Environment
- ✓ Configure RFC Destination
- ✓ Edit System Administrator for Workflow
- ✓ Edit Active Plan Version
- ✓ Classify Decision Task as General
- ✓ Document Generation/Form Integration
- ✓ Edit Time Units
- ✓ Schedule Background Job for Workflow Deadline Monitoring
- ✓ Schedule Background Job for Work Items with Errors
- ✓ Schedule Background Job for Condition Evaluation
- ✓ Schedule Background Job for Event Queue
- ✓ Schedule background job for clearing report

✓ Edit Definition Environment
✖ Edit Additional Settings and Services
✓ Classify Tasks as General
✖ Guided Procedures

Edit Runtime Environment

Component

SAP_BASIS: SAP Business Workflow/WebFlow

Execution

Automatic/Manual

Function

The activities performed in this section must be executed so

When you choose *Perform Automatic Workflow Customizing* the status *error* are executed automatically.

owing activities can be performed automatically:

onfigure RFC destination

aintain system administrator for workflow

aintain active plan variant

assify decision task as general

Verification workflow started

Figure 3.23 Automatic Workflow Verification Started

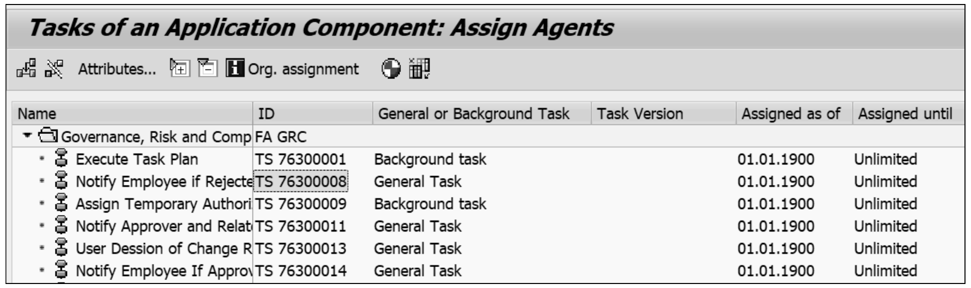
3.3.3 Classifying Workflow Tasks as General

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 Comp	FA 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 Dession 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

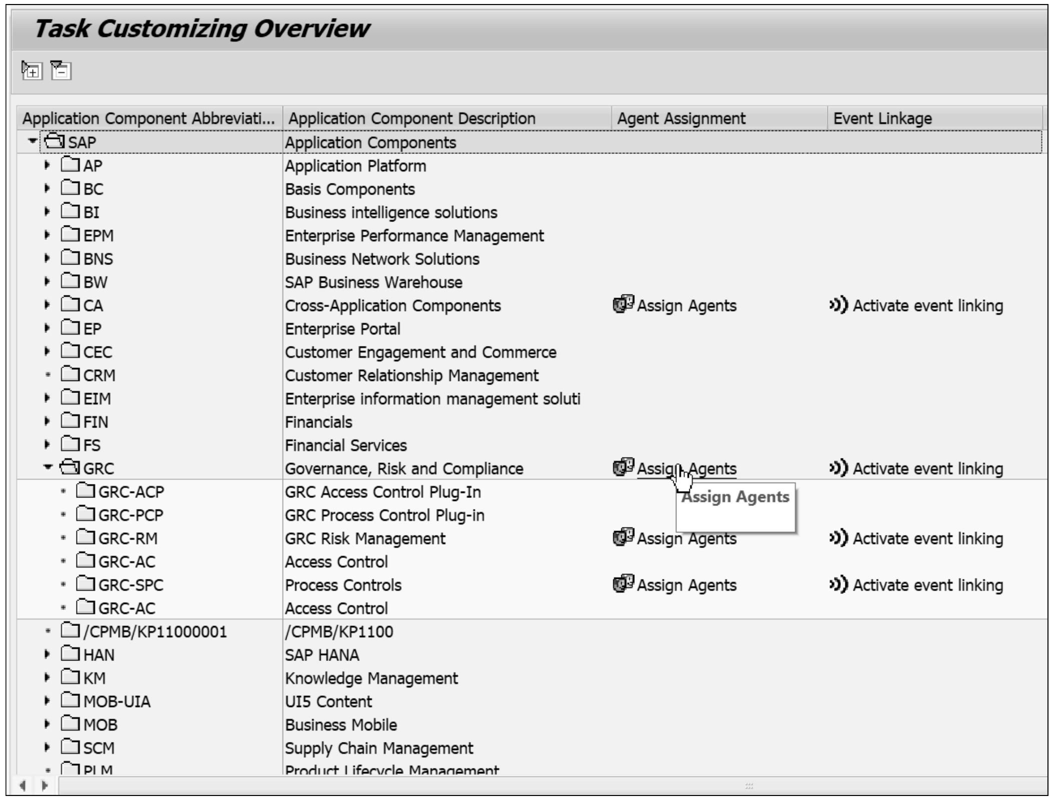
> **Note**
> You must successfully configure the RFC destinations to proceed.

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:

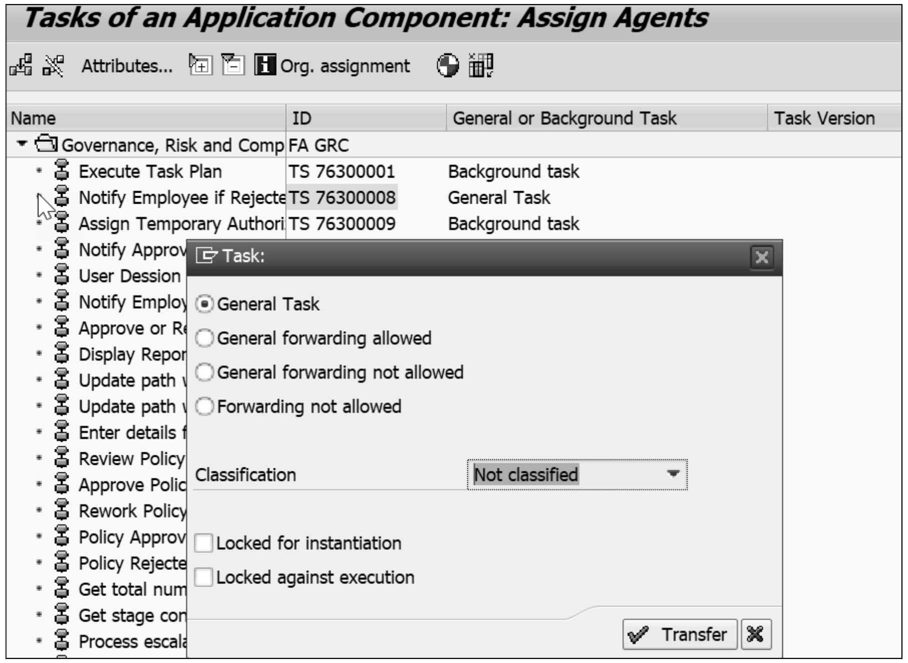
1. Execute Transaction SPRO and navigate to **SAP Reference IMG • Governance, Risk and Control • General Settings • Workflow • Perform Task-Specific Customizing**.
2. On the **Task Customizing Overview** screen, expand the **GRC** node.
3. Click the **Assign Agents** link to the right of the **GRC-AC** 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		
GRC-SPC	Process Controls	Assign Agents	Activate event linking
GRC-AC	Access Control		
/CPMB/KP11000001	/CPMB/KP1100		
HAN	SAP HANA		
KM	Knowledge Management		
MOB-UIA	UI5 Content		
MOB	Business Mobile		
SCM	Supply Chain Management		
PLM	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.



Tasks of an Application Component: Assign Agents

Name	ID	General or Background Task	Task Version
Governance, Risk and Comp	FA GRC		
Execute Task Plan	TS 76300001	Background task	
Notify Employee if Rejecte	TS 76300008	General Task	
Assign Temporary Authori	TS 76300009	Background task	
Notify Approv			
User Dession			
Notify Employ			
Approve or R			
Display Repor			
Update path			
Update path			
Enter details			
Review Policy			
Approve Polic			
Rework Policy			
Policy Approv			
Policy Rejecte			
Get total num			
Get stage cor			
Process escala			

Task:

● General Task
○ General forwarding allowed
○ General forwarding not allowed
○ Forwarding not allowed

Classification: Not classified

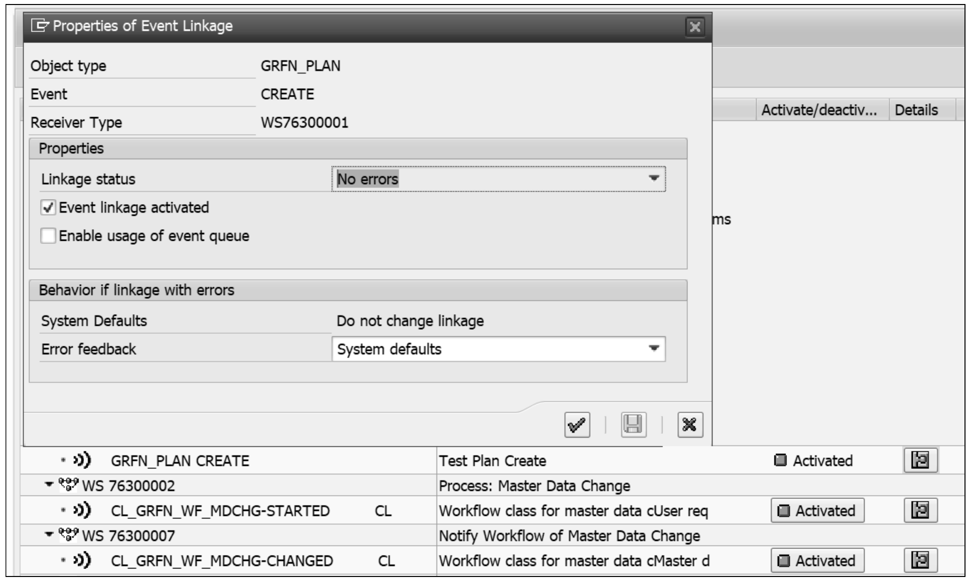
□ Locked for instantiation
□ Locked against execution

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.



Properties of Event Linkage

Object type: GRFN_PLAN
Event: CREATE
Receiver Type: WS76300001

Properties
Linkage status: No errors
☑ Event linkage activated
□ Enable usage of event queue

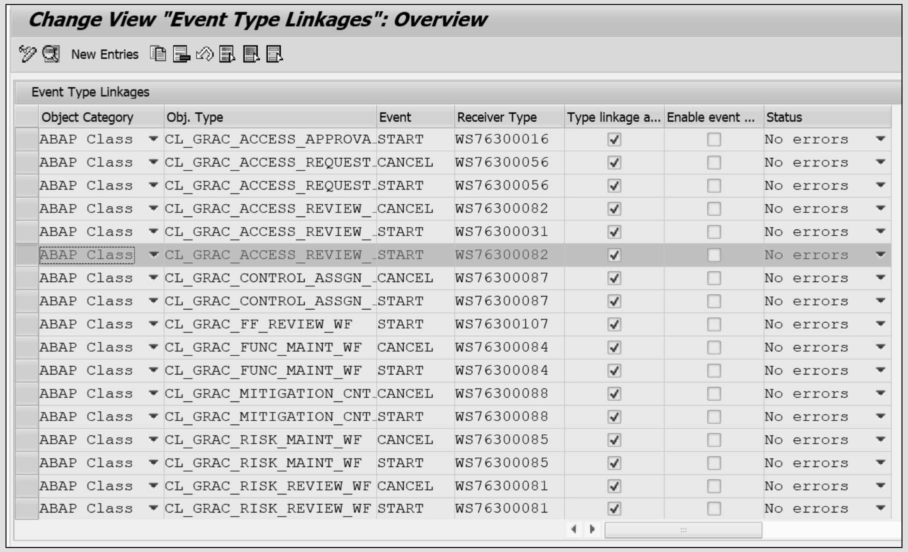
Behavior if linkage with errors
System Defaults: Do not change linkage
Error feedback: System defaults

			Activate/deactiv...	Details
GRFN_PLAN CREATE		Test Plan Create	Activated	
WS 76300002		Process: Master Data Change		
CL_GRFN_WF_MDCHG-STARTED	CL	Workflow class for master data cUser req	Activated	
WS 76300007		Notify Workflow of Master Data Change		
CL_GRFN_WF_MDCHG-CHANGED	CL	Workflow class for master data cMaster d	Activated	

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 GRCPIERP 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.



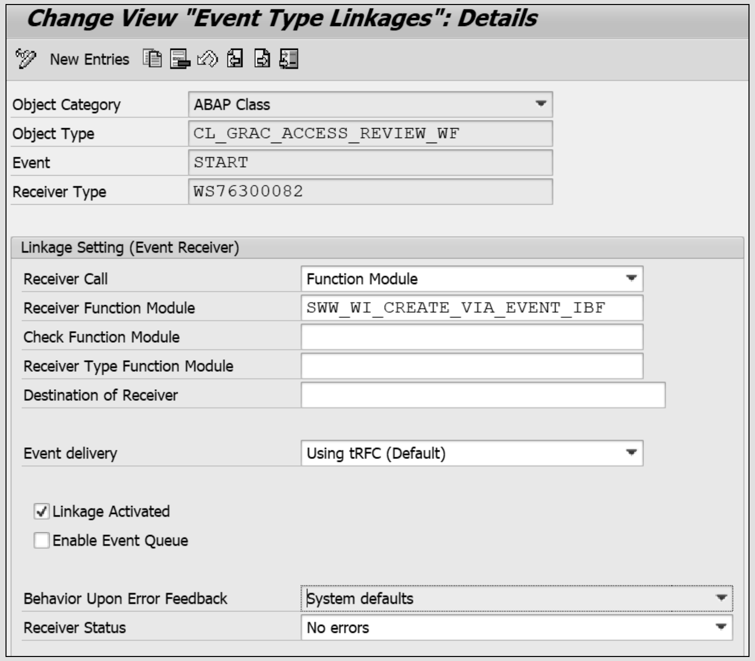
Change View "Event Type Linkages": Overview

Event Type Linkages

Object Category	Obj. Type	Event	Receiver Type	Type linkage a...	Enable event ...	Status
ABAP Class	CL_GRAC_ACCESS_APPROVA…	START	WS76300016	☑	□	No errors
ABAP Class	CL_GRAC_ACCESS_REQUEST…	CANCEL	WS76300056	☑	□	No errors
ABAP Class	CL_GRAC_ACCESS_REQUEST…	START	WS76300056	☑	□	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW_…	CANCEL	WS76300082	☑	□	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW_…	START	WS76300031	☑	□	No errors
ABAP Class	CL_GRAC_ACCESS_REVIEW_…	START	WS76300082	☑	□	No errors
ABAP Class	CL_GRAC_CONTROL_ASSGN_…	CANCEL	WS76300087	☑	□	No errors
ABAP Class	CL_GRAC_CONTROL_ASSGN_…	START	WS76300087	☑	□	No errors
ABAP Class	CL_GRAC_FF_REVIEW_WF	START	WS76300107	☑	□	No errors
ABAP Class	CL_GRAC_FUNC_MAINT_WF	CANCEL	WS76300084	☑	□	No errors
ABAP Class	CL_GRAC_FUNC_MAINT_WF	START	WS76300084	☑	□	No errors
ABAP Class	CL_GRAC_MITIGATION_CNT…	CANCEL	WS76300088	☑	□	No errors
ABAP Class	CL_GRAC_MITIGATION_CNT…	START	WS76300088	☑	□	No errors
ABAP Class	CL_GRAC_RISK_MAINT_WF	CANCEL	WS76300085	☑	□	No errors
ABAP Class	CL_GRAC_RISK_MAINT_WF	START	WS76300085	☑	□	No errors
ABAP Class	CL_GRAC_RISK_REVIEW_WF	CANCEL	WS76300081	☑	□	No errors
ABAP Class	CL_GRAC_RISK_REVIEW_WF	START	WS76300081	☑	□	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**.



Change View "Event Type Linkages": Details

Object Category: ABAP Class
Object Type: CL_GRAC_ACCESS_REVIEW_WF
Event: START
Receiver Type: WS76300082

Linkage Setting (Event Receiver)

Receiver Call: Function Module
Receiver Function Module: SWW_WI_CREATE_VIA_EVENT_IBF
Check Function Module:
Receiver Type Function Module:
Destination of Receiver:

Event delivery: Using tRFC (Default)

☑ Linkage Activated
☐ Enable Event Queue

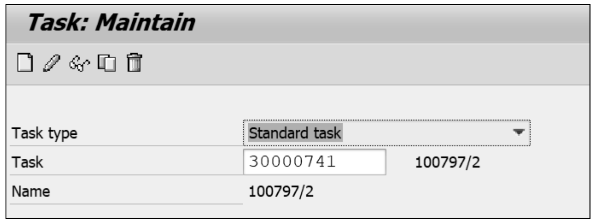
Behavior Upon Error Feedback: System defaults
Receiver Status: No errors

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.

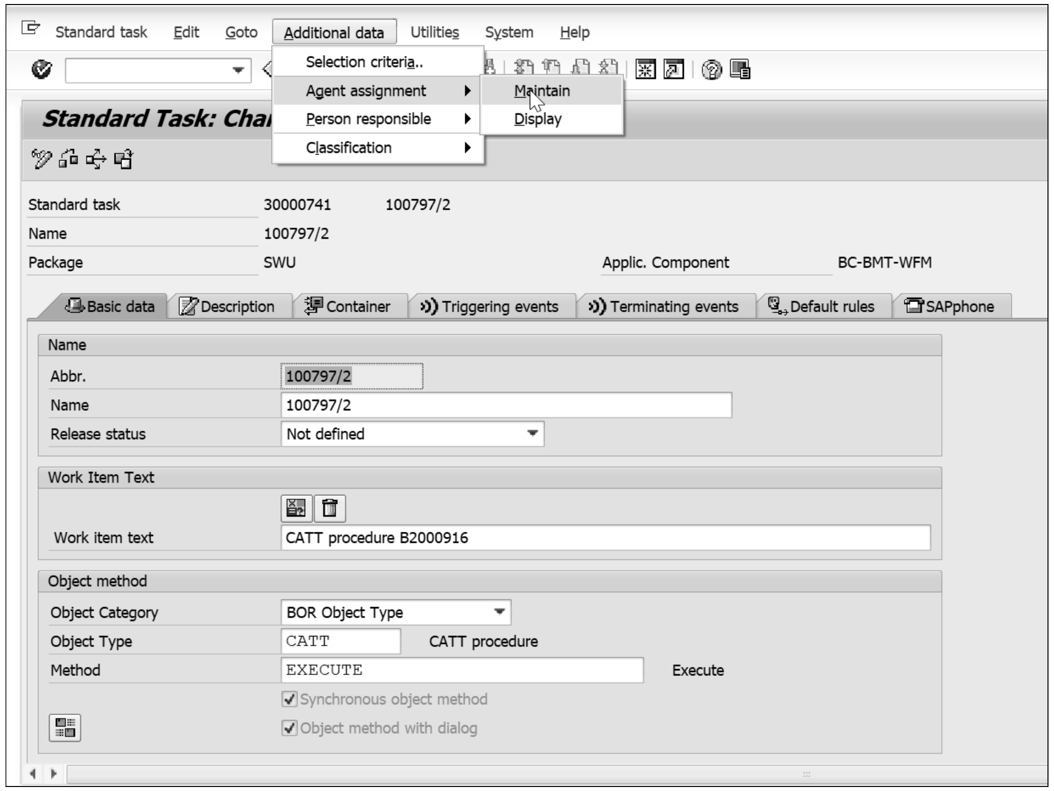


Task: Maintain

Task type: Standard task
Task: 30000741 100797/2
Name: 100797/2

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.



Standard task: 30000741 100797/2
Name: 100797/2
Package: SWU
Applic. Component: BC-BMT-WFM

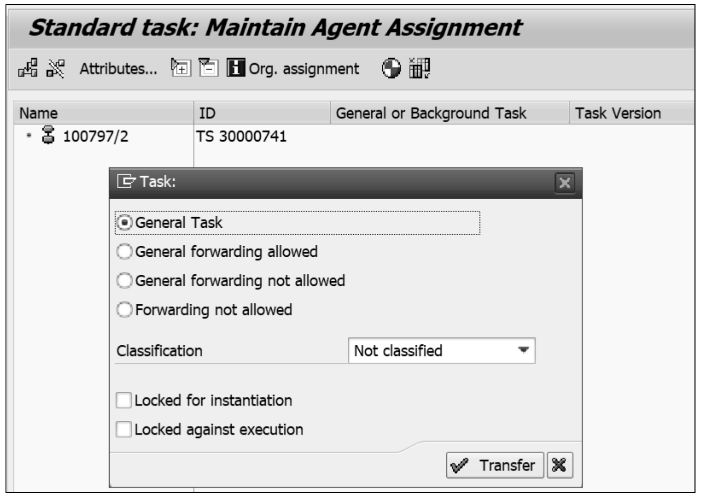
Name
Abbr.: 100797/2
Name: 100797/2
Release status: Not defined

Work Item Text
Work item text: CATT procedure B2000916

Object method
Object Category: BOR Object Type
Object Type: CATT CATT procedure
Method: EXECUTE Execute
☑ Synchronous object method
☑ Object method with dialog

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.



Standard task: Maintain Agent Assignment

Name	ID	General or Background Task	Task Version
100797/2	TS 30000741		

Task:

● General Task
○ General forwarding allowed
○ General forwarding not allowed
○ Forwarding not allowed

Classification: Not classified

☐ Locked for instantiation
☐ Locked against execution

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.

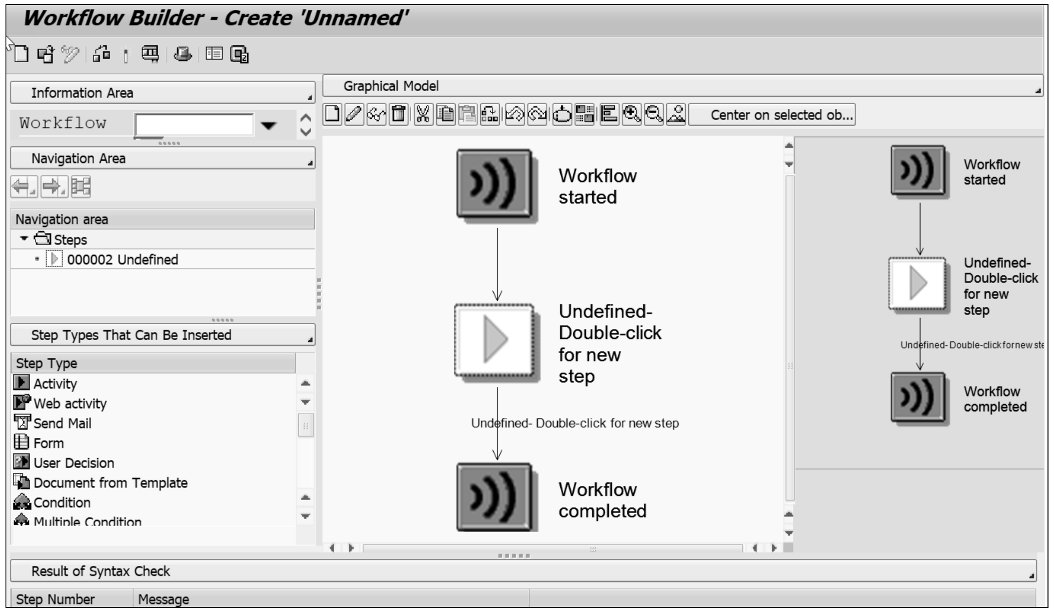


Figure 3.33 Workflow Builder

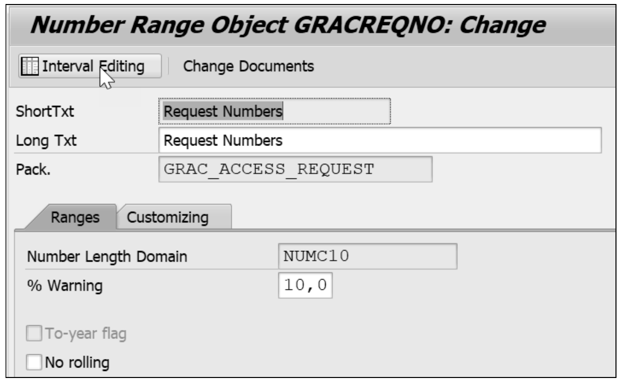
10. In the **Information Area**, in the **Workflow** field, enter the workflow step number, as listed in Table 3.10. Click the **Activate** button to activate the template.
11. Repeat the steps for all the workflow step templates.

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.



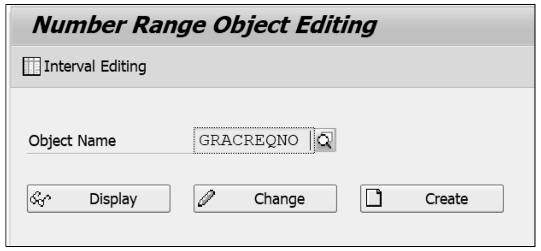
Number Range Object GRACREQNO: Change

ShortTxt: Request Numbers
Long Txt: Request Numbers
Pack.: GRAC_ACCESS_REQUEST
Number Length Domain: NUMC10
% Warning: 10,0
□ To-year flag
□ No rolling

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.

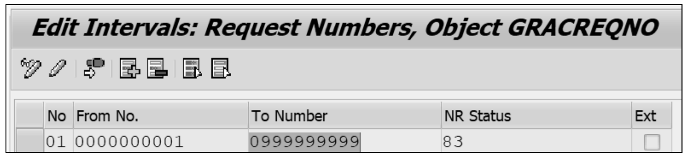


Number Range Object Editing

Object Name: GRACREQNO

Figure 3.35 Editing an Interval

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

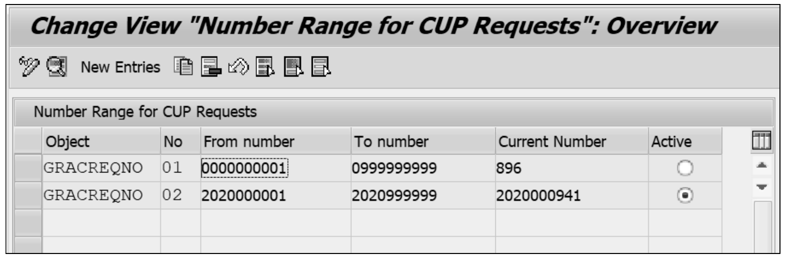


Edit Intervals: Request Numbers, Object GRACREQNO

No	From No.	To Number	NR Status	Ext
01	0000000001	0999999999	83	□

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.



Change View "Number Range for CUP Requests": Overview

Number Range for CUP Requests

Object	No	From number	To number	Current Number	Active
GRACREQNO	01	0000000001	0999999999	896	○
GRACREQNO	02	2020000001	2020999999	2020000941	●

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.
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

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.

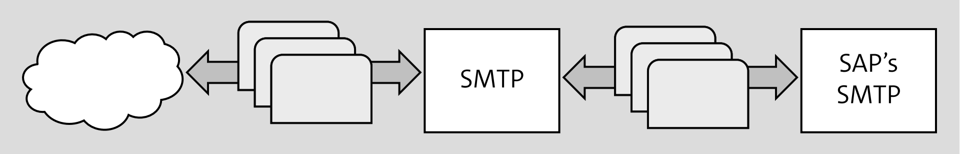


Figure 3.38 SAP SMTP Communication Channel with External SMTP

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.

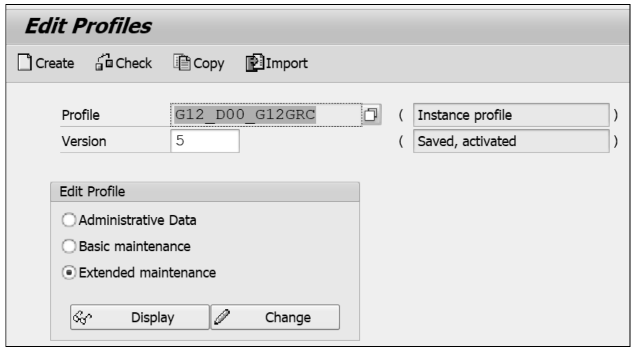
3.5.1 Opening a Simple Mail Transfer Protocol Port

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.

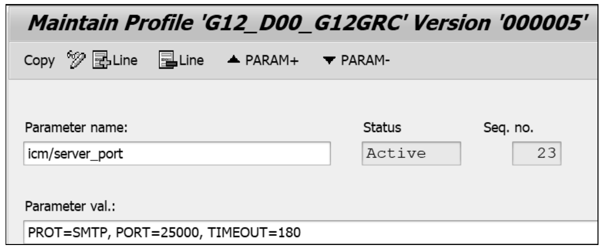


Profile: G12_D00_G12GRC (Instance profile)
Version: 5 (Saved, activated)

Edit Profile
○ Administrative Data
○ Basic maintenance
● Extended maintenance

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 in Figure 3.40.



Parameter name: icm/server_port
Status: Active
Seq. no.: 23
Parameter val.: PROT=SMTP, PORT=25000, TIMEOUT=180

Figure 3.40 ICM Configuration for an SMTP Port

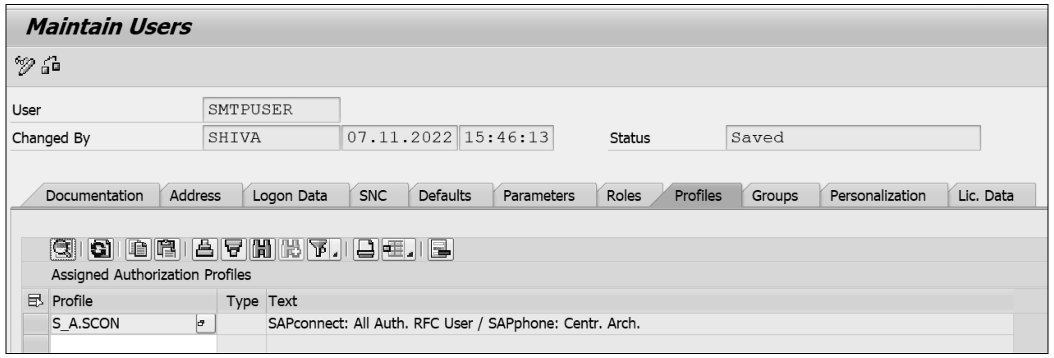
5. Click **Save** to save these changes to the instance profile.
6. If prompted to activate the profile, click **Yes**, and the activation information screen will be displayed.

> **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:

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



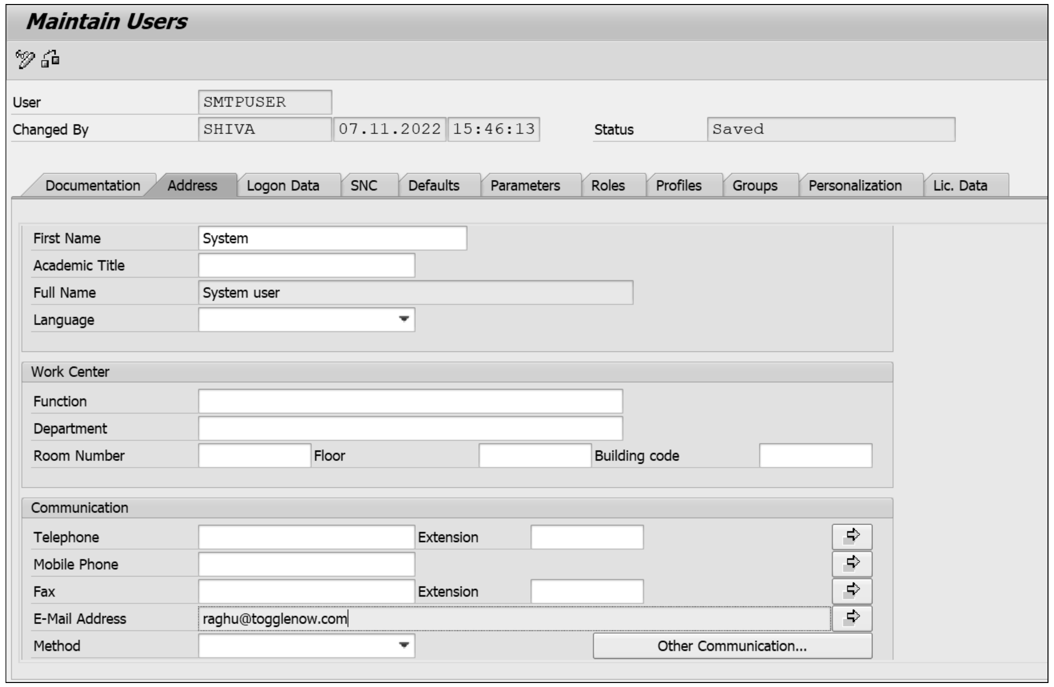
User: SMTPUSER
Changed By: SHIVA 07.11.2022 15:46:13 Status: Saved

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

Figure 3.41 SMTPUSER ID with Profile Assignment

> **Note**
>
> You may assign additional authorizations as required.

4. Click the **Save** icon to save the user ID.
5. 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.



User: SMTPUSER
Changed By: SHIVA 07.11.2022 15:46:13 Status: Saved

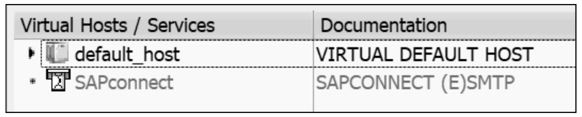
First Name: System
Full Name: System user
E-Mail Address: raghu@togglenow.com

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:

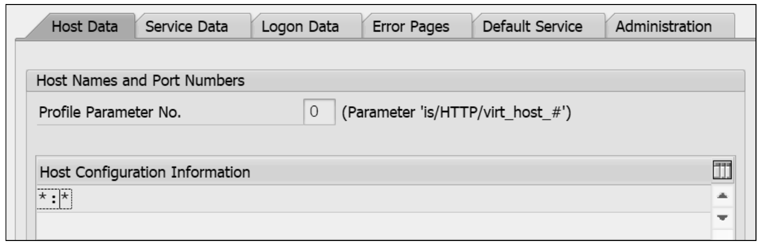
1. Execute Transaction SICF.
2. Click the **Services** icon.
3. Find the **SAPconnect** service, as shown in Figure 3.43.



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

Figure 3.43 SAP Connect Service

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



Host Names and Port Numbers

Profile Parameter No. 0 (Parameter 'is/HTTP/virt_host_#')

Host Configuration Information

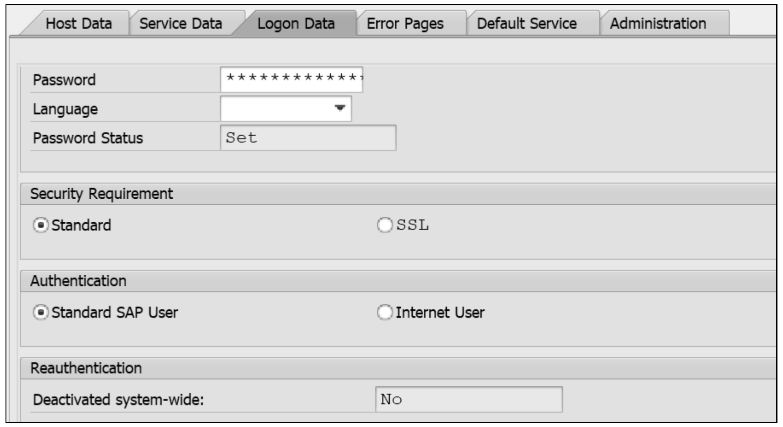
:

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_#`.

7. 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.



Password: *************

Language:

Password Status: Set

Security Requirement

● Standard ○ SSL

Authentication

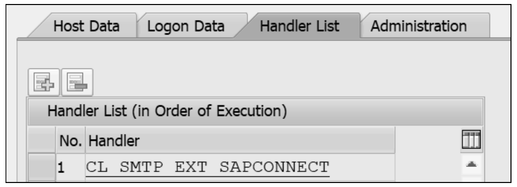
● Standard SAP User ○ Internet User

Reauthentication

Deactivated system-wide: No

Figure 3.45 Logon Data Maintenance

8. 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.

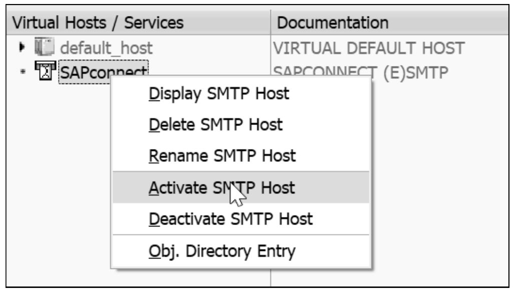


Handler List (in Order of Execution)

No.	Handler
1	CL_SMTP_EXT_SAPCONNECT

Figure 3.46 SMTP Class Handler

9. 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.



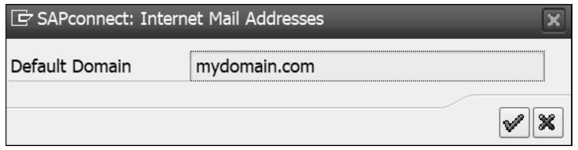
Virtual Hosts / Services	Documentation
default_host	VIRTUAL DEFAULT HOST
SAPconnect	SAPCONNECT (E)SMTP

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:

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



SAPconnect: Internet Mail Addresses

Default Domain: mydomain.com

Figure 3.48 Default Domain Maintenance

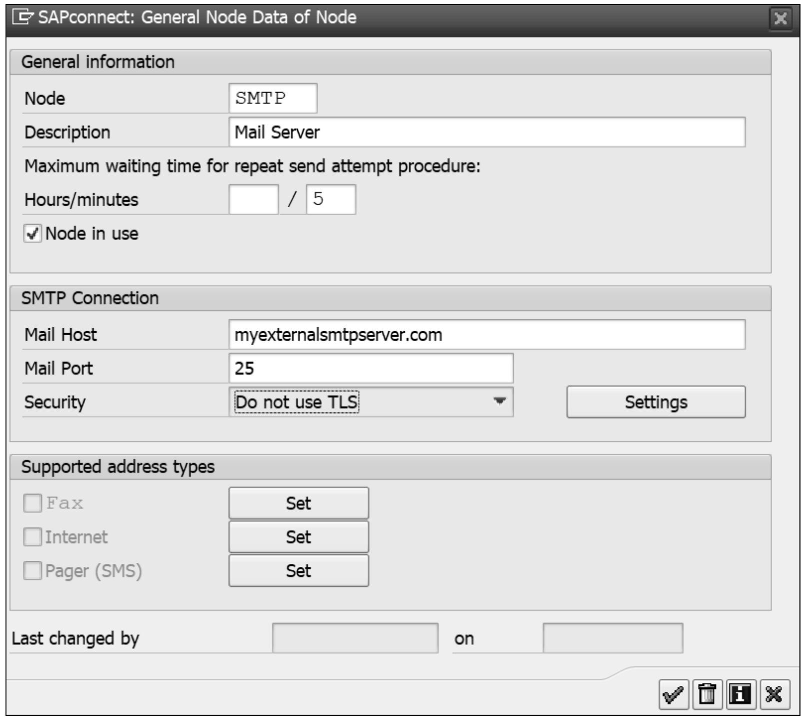
Note

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

4. Click **OK** ✓.
5. 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.



SAPconnect: General Node Data of Node

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

Supported address types

□ Fax	Set
□ Internet	Set
□ Pager (SMS)	Set

Last changed by on

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

8 Business Role Management 343

9 Periodic Reviews 401

10 End User Home Page 445

11 Multistage Multipath Workflows 467

12 BRFplus: Business Rule Framework 517

13 SAP Fiori for SAP Access Control 555

Index

SAP PRESS
SAP® Access Control
The Comprehensive Guide
Implement SAP Access Control 12.0 with step-by-step instructions
Configure Access Risk Analysis, Emergency Access Management, Business Role Management, and other modules
Work with segregation of duties, user access review, MSMP workflows, and more
Raghu Boddu
Rheinwerk Publishing

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.

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