Installation Guide
Document version: 1.7 – 2016-05-26

CUSTOMER

SAP Access Control™, SAP Process Control™, and SAP Risk Management™ 10.1

Typographic Conventions

Table 1

Example	Description
<Example>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your **<User Name>**”.
▸ *Example* ▸ *Example* ▸	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
www.sap.com	Textual cross-references to an internet address
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	• Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. • Cross-references to other documentation or published works
Example	• Output on the screen following a user action, for example, messages • Source code or syntax quoted directly from a program • File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
EXAMPLE	Keys on the keyboard

Document History

Caution

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at the following location: service.sap.com/instguides .

Table 2

Version	Date	Description
1.00	2013-06-14	New content SAP AC 10.1, PC 10.1, RM 10.1 (initial release).
1.2	2013-08-29	Updates to topic *Configuring the SAP NetWeaver Gateway*
1.3	2013-11-15	Updates: ● Added reference to SAP Fiori. to *Introduction* ● SAP NetWeaver version changed from SP02 to SP04 ● Revised Section 6.4: *Configuring the SAP NetWeaver Gateway* ● Revised Sections 3.2, 3.5, 3.6
1.4	2013-12-19	Updates to topic *Configuring the SAP NetWeaver Gateway*
1.5	2014-12-18	Updates to NetWeaver version
1.6	2016-05-03	Removed chapter *Installing the SAP NetWeaver Portal Components*
1.7	2016-05-26	Removed GRCPINW from the required plug-in list for SAP Risk Management.

Content

1 Introduction

SAP Access Control 10.1, Process Control 10.1, and Risk Management 10.1 are part of the SAP solutions for governance, risk, and compliance (GRC).

For more information, see www.sap.com/grc.

SAP Access Control 10.1

SAP Access Control is an enterprise software application that enables organizations to control access and prevent fraud across the enterprise, while minimizing the time and cost of compliance. The application streamlines compliance processes, including access risk analysis and remediation, business role management, access request management, emergency access management, and periodic compliance certifications. SAP Access Control delivers immediate visibility of the current risk situation with real-time data.

SAP Process Control 10.1

SAP Process Control is an enterprise software solution for internal controls management. It enables organizations to document their control environment, test and assess controls, track issues to remediation, and certify and report on the state and quality of internal controls. Using a combination of data forms, automated workflows, certification, and interactive reports, this solution enables members of internal control, audit, and business process teams to manage compliance activities.

SAP Risk Management 10.1

SAP Risk Management is an enterprise software solution that enables organizations to balance business opportunities with financial, legal, and operational risks to minimize the market penalties from high-impact events. The application allows customers to identify these risks and monitor them on a continuous basis. Stakeholders and owners are provided with such tools as analytic dashboards for greater visibility in mitigating risks in their areas of responsibility.

1.1 About this Document

This guide describes how to install SAP solutions for governance, risk, and compliance; that is, SAP Access Control 10.1, SAP Process Control 10.1, and SAP Risk Management 10.1.

1.2 SAP Notes for the Installation

Read the following SAP Notes before you start the installation. These SAP Notes contain the most recent installation information, as well as any corrections to the installation documentation.

Note

Make sure that you have the latest version of each SAP Note, which you can find on SAP Service Marketplace at service.sap.com/notes.

Table 3

SAP Note Number	Title	Description
1855332	Release Strategy for SAP Access Control 10.1	This SAP Note contains information about planning the installation and upgrades of the ABAP add-on.
1814403	WDA: Syntax Error When Activating A Web Dynpro Component	This *mandatory* SAP Note must be applied after you install SAP NetWeaver 7.40 SP02 to make sure that the SAP NetWeaver Business Client (NWBC) is working properly. Caution Apply this note when you *install* or when you *upgrade* to the 10.1 release.
1855403	GRCFND_A V1100 Installation and Upgrade	This SAP Note contains general information about how to install and upgrade SAP solutions for governance, risk, and compliance 10.1.
1855404	GRCPINW V1100 Installation and Upgrade	This SAP Note contains information about planning the installation and upgrading of the SAP NetWeaver Plug–In.
1855405	GRCPIERP V1100 Installation and Upgrade	This SAP Note contains information about planning the installation and upgrading of the SAP GRC ERP Plug–In.
1597627	SAP HANA Connection	This SAP Note contains information about how to set up a second database connection from your system to an SAP HANA system.
1353044	Installation Guide: Crystal Report Adapter	This note contains information about installing a front-end component to integrate SAP Crystal Reports with the Advanced List View (ALV).
1366785	SAP Crystal Reports ALV Integration – Functional Restrictions	This note describes the functional and nonfunctional restrictions of the integration of SAP Crystal Reports into ABAP List Viewer (ALV).

SAP Note Number	Title	Description
1382730	SAP Crystal Reports ALV Integration – Troubleshooting	This note helps you to analyze problems that you might encounter with the integration of SAP Crystal Reports into the Advanced List Viewer ALV.

Read the SAP Notes below if your environment includes more than one component (SAP Access Control, SAP Process Control, or SAP Risk Management) from the SAP solutions for governance, risk, and compliance (GRC).

Table 4

SAP Note Number	Title	Description
1470670	User-defined Fields for RM	The Note describes how to customize user-defined fields in SAP Risk Management.
1505255	Transfer client-specific Customizing for PC/RM	Transfer the client-specific Customizing from the delivery client for SAP Process Control 10.1 and SAP Risk Management 10.1.
1509639	Preparation for Installing GRC-RM 2010	For installation of SAP Risk Management 10.1 or for the upgrade of a production system from SAP Risk Management 3.0 to SAP Risk Management 10.1 ⚠ Caution Review this SAP Note before attempting the installation.
1519164	Create BRF+ application name & ID for Continuous Monitoring	The BRF+ application name must be unique to import BRF+ content from a source system to a target system. The same BRF+ application name and application ID must exist in all environments.
736902	Adobe Credentials	If you want to use Adobe Interactive Forms and you require a credential to complete the configuration, you need this note. The credential is **only** required if you have **interactive forms** (forms in which the user can enter data). For print forms, the credential is not required.

1.3 SAP Fiori Apps

For more information regarding SAP Fiori apps, see SAP Fiori for SAP Access Control 10.1 help.sap.com/grc-ac .

2 Planning

Perform the following planning steps before you start the installation.

Procedure

1. Consult the master guides to determine the software components and supporting systems that you want to run either an SAP Access Control 10.1 only landscape or a multiple componentSAP goverance, risk, and complicance (GRC) 10.1 solution landscape. Each component has its own master guide in its own section of the SAP GRC help:
   - For the SAP Access Control 10.1 component, consult the *SAP Access Control 10.1 Master Guide* at help.sap.com/grc-ac > *Installation and Migration Information*
   - For the SAP Process Control 10.1 component, consult the *SAP Process Control 10.1 Master Guide* at help.sap.com/pc > *Installation and Upgrade Information*
   - For the SAP Risk Management 10.1 component, consult the *SAP Risk Management 10.1 Master Guide* at help.sap.com/rm > *Installation and Migration Information*
2. Download and check the relevant SAP Notes listed in this document.
3. Before you begin your installation, make sure that SAP NetWeaver 7.40 SP05 (ABAP) is properly installed and configured as described later in this guide. This step is *mandatory.*

   > Note
   >
   > SAP Access Control, SAP Process Control, and SAP Risk Management 10.1 run on SAP NetWeaver 740 SP05 (on non-HANA or HANA databases).

4. SAP Access Control and SAP Process Control require that you install plug-ins for your ERP system as directed in this guide.

   > Note
   >
   > If you want to manage access for HANA, you must install the HANA plug-in. For more information, see the section of this guide called *Installing the SAP HANA Plug-In.*

5. If you want to use the SAP NetWeaver Portal, which is not required if you use the SAP NetWeaver Business Client (NWBC), install the following programs according to the directions in this guide:
   - GRCPIERP Portal Plug-In
   - GRC_POR_1000 (this replaces NWBC)
6. If you want to use the document search feature in SAP Process Control and SAP Risk Management (only), install `TREX`, by following the directions in this guide.
7. If you want to use Adobe Document Services, install SAP NetWeaver Java as directed in this guide.

Note

To enable printing from SAP software, download the Adobe Document Services license. For more information, see the SAP Library at help.sap.com and search on *Licensing Adobe Document Services*. Also see SAP Note 736902, *Adobe Credentials*.

8. If you plan to use Simplified Access Control, ensure that your browser is HTML5 and CSS3 compliant. Examples of such browsers include Internet Explorer 9, Chrome, and Firefox.
9. Take all applicable security measures. For more information, see the *SAP AC/PC/RM 10.1 Security Guide* at help.sap.com/grc. Select the desired product and then select *Security Information*.

3 Installing the Components

This chapter discusses the various software and tools that you may use in your installation.

3.1 Preparing to Install SAP Solutions for Governance, Risk, and Compliance (GRC) 10.1

Install SAP solutions for governance, risk, and compliance (GRC) 10.1 on a standalone system as opposed to installing them along with an SAP Business Suite or with any SAP Business Suite components such as ERP, SCM, CRM, OR SRM.

3.2 Software Update Manager (SUM)

Software Update Manager (SUM) is an installer that replaces JAVA Service Program Manager (JSPM). SUM is now the only supported JAVA installation tool; JSPM is no longer supported.

For more information about Software Update Manager, see the following:

- https://service.sap.com/instguides ▸ *Other Documentation* ▸ *Deployment Optimization Option of SUM 10.0* ◂.
- scn.sap.com/docs/DOC-25113

3.3 SAP NetWeaver Components

Depending on your landscape configuration, the following SAP NetWeaver components are available to install:

Table 5

Component	Details
Support Package Manager (SPAM) 7.40 or higher	N/A
SAP Basis	7.40 SP05
SAP ABA Cross Application Component	7.40 SP05
SAP_GWFND SAP - Gateway Foundation 7.40	7.40 SP05
SAP User Interface Technology 7.40	7.40 SP06
PI_BASIS – Basis Plug-In	7.40 SP05
SAP BW – SAP Business Warehouse	7.40 SP05

Component	Details
GRCFND_A – GRC Foundation ABAP V1100	N/A
DMIS 2010_1_700	2010_1_700 SP06 (or latest)
(Optional) SAP NetWeaver Application Server Java for Adobe Document Services	SAP NetWeaver Java is required to use Adobe Document Services. It must be available in the system landscape, but does not need to be installed on the same system as the SAP GRC 10.1 applications. You must create and activate the following JCo destinations: ● WD_ALV_METADATA_DEST ● WD_ALV_MODELDATA_DEST It is essential to create Adobe Credentials; see SAP Note 736902, *Adobe Credentials*. If problems occur in forms processing, see SAP Note 944221 for more details about troubleshooting. For more information, see the following Web page:www.sdn.sap.com/irj/sdn/adobe.
BI Java Usage Type (part of the SAP NetWeaver Java stack) to enable the printing of PDFs from Process Control reports and Risk Management reports.	BI Java Usage Type must be installed on the same system as the Adobe Document Services. For more information, see SAP Note1533060 *WD ABAP ALV - create print version*.
Standalone Engine	TREX 7.10 (revision 53 or higher) TREX 7.25 SP24 (SAP HANA)

Note

If you use SAP Process Control 10.1 Policy Survey PDFs, be sure to upgrade to the latest version of Adobe Reader.

3.4 Java Components

The Java components, SAP GRC Portal, and SAP GRC Portal Plug-Ins are supported on all SAP NetWeaver releases from 7.02 to 7.40. See the software compatibility matrix later in this document to determine the versions of SAP NetWeaver, SAP GRC Portal Content, and SAP GRC Portal Plug-Ins that work together.

Note

The 10.0 version of the Java components is used with the SAP GRC 10.1 system.

3.5 Downloading SAP Solutions for Governance, Risk, and Compliance 10.1

Procedure

1. Go to the SAP Software Distribution Center on SAP Service Marketplace at service.sap.com/swdc.
2. Download the following SAP GRC 10.1 applications and install them using the Software Update Manager (SUM) or transactions SAINT or SPAM.

Table 6

Application	Path
SAP Access Control	▶ *Software Downloads* › *Installations and Upgrades* › *A - Z Index* › *G* › *SAP GRC Access Control* › *SAP Access Control* › *SAP Access Control 10.1* ◀
SAP Process Control	▶ *Software Downloads* › *Installations and Upgrades* › *A - Z Index* › *P* › *SAP Process Control* › *SAP Process Control 10.1* ◀
SAP Risk Management	▶ *Software Downloads* › *Installations and Upgrades* › *A - Z Index* › *R* › *SAP Risk Management* › *SAP Risk Management 10.1* ◀

3.6 Installing HR and Non-HR Plug-Ins

GRCPINW and GRCPIERP Plug-Ins are used as indicated in the table below. The subsequent table gives instructions on how to download these Plug-Ins.

Table 7

Plug-In	Use
GRCPINW	This Plug-In is used for non-HR functions in SAP Access Control. In SAP Process Control, it is used for Continuous Monitoring (required if you use the ABAP Report, Configurable and Programmed Sub-Scenarios).
GRCPIERP	This Plug-In is used for HR functions in SAP Access Control and SAP Process Control.

Procedure

Follow the steps below to download the SAP GRC 10.1 Plug-Ins.

1. Go to the SAP Software Distribution Center on SAP Service Marketplace at https://service.sap.com/swdc.
2. Download SAP GRC 10.1 plug-ins and install them using SUM or transactions SAINT or SPAM.

   Use the paths in the table below.

Table 8

Application	Path
SAP Access Control	*Software Downloads › Installations and Upgrades › A - Z Index › G › SAP GRC Access Control › SAP Access Control › SAP Access Control 10.1*
SAP Process Control	*Software Downloads › Installations and Upgrades › A - Z Index › P › SAP Process Control › SAP Process Control 10.1*
SAP Risk Management	*Software Downloads › Installations and Upgrades › A - Z Index › R › SAP Risk Management › SAP Risk Management 10.1*

3.7 Installing the SAP HANA Plug-In

Install the following Plug-In if you are using the SAP HANA database:

Table 9

Technical name	HCO_GRC_PI
Software Component Version	SAP GRC 10.1 Plug-In SAP HANA

Procedure

You download this plug-in as follows:

1. Go to service.sap.com/swdc.
2. Choose *Software Downloads › Installations and Upgrades › A - Z Index › G › SAP GRC Access Control › SAP Access Control › SAP Access Control 10.1 › Installation*
3. Select the HCO_GRC_PI download object.

More Information

For more information, see SAP Note 1597627 SAP HANA Connection.

4 Installing TREX (Optional)

You can install the standalone version of TREX if you want to use Enterprise Search for document search in SAP Process Control 10.1 and SAP Risk Management 10.1.

Note

TREX is not an option in SAP Access Control 10.1 only environments.

Procedure

1. To install the latest TREX version, see the Master Guide at service.sap.com/installnw74 *SAP NetWeaver 7.4* Installation - Standalone Engines and Clients →Master Guide.
2. For more information, see the following SAP Notes:

Table 10

SAP Note Number	Title
1249465	*How to install TREX for Embedded Search*
1164532	*Limitations*
1266024	*Sizing TREX for Embedded Search*
1269011	*Additional TREX instance for Embedded Search*

5 Post-Installation

After downloading and installing the files described in the previous sections, configure the product by following the post-installation sections in the order that they are presented.

5.1 Client Copy

Client copy is not required in SAP Access Control 10.1 only environments.

For more information, see SAP Note 2290499.

5.2 Activating the Applications in Clients

After the installation is complete and the SAP solutions for governance, risk, and compliance (GRC) 10.1 are in place, you must activate them in each client.

Procedure

Complete the following steps to activate the applications:

1. Open the SAP Reference IMG iby going to *Tools* > *Customizing* > *IMG* > *Execute Project (transaction SPRO)*.
2. Display the SAP Reference IMG.
3. Choose *Governance, Risk, and Compliance* > *General Settings* > *Activate Applications in Client*.
4. Execute *Activate Applications in Client*.
5. Activate an application component:by following the steps below:
    1. Choose the *New Entries* pushbutton.
    2. Select an application component from the dropdown list.
    3. In the *Active* column, select the check box for each application that you want to use.

    The application component activation is now complete.

1. Choose the *New Entries* pushbutton.
2. Select an application component from the dropdown list.
3. In the *Active* column, select the check box for each application that you want to use.

The application component activation is now complete.

5.3 Checking SAP ICF Services

Specific Internet Communication Framework (ICF) SAP Services, and SAP GRC services need to be activated. They are inactive by default after an installation or an upgrade. Check that all the relevant services are active.

For more information about activating these services, see SAP Note 1088717, *Active services for Web Dynpro ABAP in transaction SICF*.

Procedure

1. Activate each of the following ICF service nodes:
   - `/sap/public/bc`
   - `/sap/public/bc/icons`
   - `/sap/public/bc/icons_rtl`
   - `/sap/public/bc/its`
   - `/sap/public/bc/pictograms`
   - `/sap/public/bc/ur`
   - `/sap/public/bc/webdynpro`
   - `/sap/public/bc/webdynpro/mimes`
   - `/sap/public/bc/webdynpro/adobeChallenge`
   - `/sap/public/bc/webdynpro/ssr`
   - `/sap/public/bc/webicons`
   - `/sap/public/myssocntl`

   > Note
   >
   > You can also activate all ICF services within:
   > - `/sap/public`
   > - `/sap/bc`
   > - `/sap/grc` – for Access Control 10.1 only environments

2. Activate all GRAC, GRPC, and GRRM services.
3. Activate all services under `/sap/bc/webdynpro/sap`.

5.4 Configuring the SAP NetWeaver Gateway

In order to use some of the new functionality in SAP Access Control 10.1, such as the *Remediation View* in SAP Access Risk Analysis, an SAP NetWeaver Gateway connection must be established. Follow these steps to maintain or verify the connector.

Procedure

1. Logon to an SAP NetWeaver system and access the SAP Reference IMG as follows: from the SAP Easy Access menu, choose *Tools* > *Customizing* > *IMG* > *Execute Project (transaction SPRO)*.
2. Choose *SAP Reference IMG* > *SAP NetWeaver* > *Gateway* > *OData Channel* > *Configuration* > *Connection Settings* > *SAP NetWeaver Gateway to SAP System*.
3. Choose *Manage RFC Destinations* and create an RFC (communication) destination that points to the system itself.

> ⚠ Caution
>
> Be sure to specify the proper RFC Type, client, and user information using the naming convention:
>
> <**System SID**>CLNT<**Client Number**>; for example, **GD1CLNT200**.

4. If you are using Single-Signon, choose *Define Trust for SAP Business Systems*. Complete the fields with the information you provided in the Step 3.

> Note
>
> This step *only* applies if you are using Single-Signon.

5. Choose *Manage SAP System Aliases* to create the system alias for the RFC destination that you created in Step 3.
6. Choose *New Entries* and enter the following values:

Table 11

Field Name	What You Enter
SAP System Alias	Enter the name of the RFC destination that you created in Step 3.
Description	Enter a description that is meaningful to your installation.
RFC Destination	Enter the name of the RFC destination that you created in Step 3.
Software Version	Choose the value DEFAULT from the drop down list.

7. *Save* your entries.
8. If required, choose *Activate or Deactivate SAP NetWeaver Gateway* to activate the SAP NetWeaver Gateway Services.
9. Choose *SAP NetWeaver* > *Gateway* > *OData Channel* > *Administration* > *General Settings*.
10. Choose *Activate and Maintain Services*. The system displays a list of all the services that have been created in the backend system.
11. Click to select the *Technical Service* GRAC_GW_VIOLSUMM_REM_SRV.
12. In the *System Aliases* section (bottom right-hand corner), click *Add System Alias*.
13. Enter **GRAC_GW_VIOLSUMM_REM_SRV_0001** as the *Service Doc. Identifier*.
14. For the *SAP System Alias*, enter the system alias name that you created in Step 6.
15. Click the check box for *Default System*.
16. *Save* your entries.

17. On the *Activate and Maintain Services* screen, in the ICF Node section (bottom left-hand corner), verify that the traffic light in front of the ICF Node is green. If it is not, click the ICF Node field and select *Activate* from the ICF Node dropdown menu.
18. If required, *Save* your settings.
19. You may need to perform additional activations depending on what has already been activated in your environment. To do so, on the *Activate and Maintain Services* screen, repeat steps 11 through 18 for the following services:

Table 12

Technical Service Name	External Service Name	Service Doc Identifier
/IWFND/SG_MED_CATALOG	CATALOGSERVICE	/IWFND/SG_MED_CATALOG_0001
/IWFND/SG_USER_SERVICE	USERSERVICE	/IWFND/SG_USER_SERVICE_000

> Note
>
> This step is optional. It may not be required in some environments where the services have already been activated.

More Information

For more information, see the SAP Help portal at help.sap.com and search for: *SAP NetWeaver Gateway Developer Guide*. Then choose *OData Channel* > *Basic Features* > *Service Life-Cycle* > *Activate and Maintain Services*.

5.5 Maintaining System Data

Complete the Add-On Product Version in your system data application so that customer support can see which SAP solutions for governance, risk, and compliance (GRC) applications are implemented in your environment.

For more information, see SAP Note 1313108, *System Data Maintenance for GRC Process Control*.

Procedure

1. Go to SAP Service Marketplace at service.sap.com. Locate the System Data application in the *Support Portal* under *Data Administration*.
2. Use one of the search functions provided to select an installed SAP system.
3. On the *System* tab, scroll down to the *Add-On Product Version* section.
4. Insert a line.
5. Select the SAP Access Control 10.1 support package, SAP Process Control 10.1 application support package, or the SAP Risk Management 10.1 application support package from the list.
6. Save your changes.
7. Repeat this procedure for all SAP systems.

Activating Crystal Reports

To use the Crystal Reports function, activate the flag *Allow Crystal Reports* in Customizing under ▶ *SAP NetWeaver* › *Application Server* › *SAP List Viewer (ALV)* › *Maintain Web Dynpro ABAP-Specific Settings* ◀.

5.6 Maintaining Plug-in Settings

Once you install the plug-in components, Non-HR (GRCPINW), and, optionally, HR (GRCPIERP), you must maintain the plug-in user exit and configuration settings.

Procedure

In the IMG activity below, you maintain the user exit settings that are required to run Risk Terminator in Role Maintenance (transaction PFCG). Risk Terminator enables real time risk analysis while making changes to role authorizations or role assignments in the Plug-In system.

1. Open the SAP Reference IMG from ▶ *Tools* › *Customizing* › *IMG* › *Execute Project (transaction SPRO)* ◀.
2. Display the SAP Reference IMG.
3. Open ▶ *Governance, Risk, and Compliance (Plug-In)* › *Access Control* ◀.
4. Maintain the necessary IMG activities for your system according to the instructions in the IMG documentation that is located at the left of each of the following IMG nodes:
   - *Maintain User Exits for Plug-in Systems*
   - *Maintain Plug-in Configuration Settings*

6 Customizing with Business Configuration (BC) Sets

You activate Business Configuration (BC) sets after the software is installed. BC sets are delivered implementation toolsets that simplify the Customizing process. You need to activate some or all of the BC sets that are delivered with SAP solutions for governance, risk, and compliance 10.1.

See the following sections in this guide for the specific BC sets for SAP Access Control, SAP Process Control, and SAP Risk Management 10.1.

Note

For SAP Access Control 10.1 only environments, you only activate the SAP Access Control BC Sets.

Caution

You can activate a BC set *only* if that client is *not a production client*. When you activate the BC set, all data in the BC set is transferred into the corresponding tables and any existing entries are overwritten.

Recommendation

Always consult with the functional experts for your application before activating any of the BC sets.

See *SAP Solution Manager* for information about Customizing activities at service.sap.com/solutionmanager.

For more information about BC sets, see help.sap.com/nw70 > *Application Help* > *SAP NetWeaver* > *SAP NetWeaver by Key Capability* > *Solution Life Cycle Management by Key Capability* > *Customizing* > *Business Configuration Sets (BC-SETS)*

6.1 Activating BC Sets

Procedure

1. From the SAP Easy Access screen, choose *Tools* > *Customizing* > *IMG* > *Execute Project* > *SAP Reference IMG*
2. Choose *Existing BC Sets* from the toolbar in the *Implementation Guide* to identify all of the IMG activities that have BC sets.
3. Select one of these IMG activities and choose the *BC Sets for Activity* button.

   The system displays the contents of the BC set in a new window.
4. To activate this BC set, choose the pull-down menu *Go to* > *Activation Transaction* .
5. Select the icon for *Activate BC Set* (or use **F7**).

   The *Activation Options* screen opens.
6. Choose *Continue*.

A completion message appears: *Activation successfully completed*. If a yellow informational message appears, choose *Enter* and then the completion message appears.

Note

A message with a **yellow** background is only a warning and you can proceed. A message with a **red** background is an error message and you must resolve the error. If you receive a Basis error message with a red background, contact your system administrator.

Caution

The following information *does not apply*when activating BC sets in SAP Access Control 10.1 *only* environments.

Caution

When activating the BC set tables that begin with `GRPC-ATTR-*`, errors may appear in the *Progress* column.

7. You must activate the following five BC sets *twice*:
   - `GRPC-ATTR-CTRL_OBJ_CATEGORY`
   - `GRPC-ATTR-CTRL_GROUP`
   - `BC_SET_RISK_LEVEL_MATRIX`
   - `GRFN-PNS-FDA`
   - `GRFN-PNS-SOX`

Note

You can ignore the following error messages during first-time activation:

Table 13

#	Message
1	`GRPC-ATTR-CTRL_GROUP VC_GRPCATTR Table/View V_GRPCATTRVALUE2: higher-level entry for & missing`
2	`GRPC-ATTR-CTRL_GROUP VC_GRPCATTR Entry xxxx xxxx does not exist in GRPCATTRVALUE (check entry).`
3	`GRFN-PNS-FDA Entry FDA does not exist in GRPC_MCF_REGCONF (check entry).`
4	`GRFN-PNS-SOX Entry SOX does not exist in GRPC_MCF_REGCONF (check entry).`

Second-time activation may produce warning messages that can safely be accepted if no error message occurs.

6.2 SAP Access Control BC Sets

The following tables list the BC sets for SAP Access Control 10.1 categorized by type. BC sets marked with an asterisk (*) indicate that you can also activate them in Customizing.

➡ Recommendation

Always consult with the SAP Access Control functional experts before activating the BC sets for rules such as *Segregation of Duties (SoD)*to determine which rule sets are relevant for your implementation.

Table 14

BC Set	BC Set Name
Specific to Access Risk Analysis	
GRAC_RA_RULESET_COMMON	SoD Rules Set
GRAC_RA_RULESET_JDE	JDE Rules Set
GRAC_RA_RULESET_ORACLE	ORACLE Rules Set
GRAC_RA_RULESET_PSOFT	PSOFT Rules Set
GRAC_RA_RULESET_SAP_APO	JDE Rules Set
GRAC_RA_RULESET_SAP_BASIS	SAP BASIS Rules Set
GRAC_RA_RULESET_SAP_CRM	SAP CRM Rules Set
GRAC_RA_RULESET_SAP_ECCS	SAP ECCS Rules Set
GRAC_RA_RULESET_SAP_HR	SAP HR Rules Set
GRAC_RA_RULESET_SAP_NHR	SAP R/3 less HR Basis Rules Set
GRAC_RA_RULESET_SAP_R3	SAP R/3 AC Rules Set
GRAC_RA_RULESET_SAP_SRM	SAP SRM Rules Set
Specific to Access Request Management	
GRAC_ACCESS_REQUEST_REQ_TYPE*	Request Type
GRAC_ACCESS_REQUEST_EUP*	EUP (Note: Only the value **EU ID 999** is valid for this BC set.)
GRAC_ACCESS_REQUEST_APPL_MAPPING*	Mapping BRF Function IDs and AC Applications
GRAC_ACCESS_REQUEST_PRIORITY*	Request Priority
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
Specific to Business Role Management	
GRAC_ROLE_MGMT_SENTIVITY*	Sensitivity
GRAC_ROLE_MGMT_METHODOLOGY*	Methodology Process and Steps
GRAC_ROLE_MGMT_ROLE_STATUS*	Role Status
GRAC_ROLE_MGMT_PRE_REQ_TYPE*	Prerequisite Types

BC Set	BC Set Name
GRAC_ROLE_SEARCH_COFIGURATION	Role Search Configuration for Access Request
Specific to Superuser Management	
GRAC_SPM_CRITICALITY_LEVEL*	Criticality Levels
Specific to Workflow	
GRC_MSMP_CONFIGURATION*	MSMP Workflow Configuration Rules Set

6.3 SAP Process Control BC Sets

You need to activate the following BC sets (categorized by type) that are delivered with SAP Process Control 10.1:

Table 15

BC Set	Name
SAP Process Control-specific generic BC sets	
GRPC-AGENTSLOTC-GLOBAL	Global Roles to Receive Tasks in Workflow
GRPC-ROLE-CROSS-REG	Role Assignment for PC Cross Regulation Roles
GRPC-SCOPE-MAT-ANA-FREQ	Scoping Materiality Analysis Frequency
GRPC-SCOPE-IMPACT-LEVEL	Impact Levels
BC_SET_PROBABILITY_LEVEL_ID	Maintain Probability Level ID
BC_SET_RISK_LEVEL_MATRIX	Maintain Risk Level Matrix Note Before activating this BC set, first activate BC_SET_PROBABILITY_LEVEL_ID.
GRPC-SCOPE-CNTL-RISK-FACTOR	Control Risk Factor
GRPC-SCOPE-CNTL-RATE-RNG	Control Rating Range
GRPC-SCOPE-LVL-EVID-VAL	Level of Evidence Value
GRPC-SCOPE-LVL-EVID	Level of Evidence
BCSET-GRRM-GRRMVRISKOPPLVL	Maintain Risk and Opportunity Levels
GRPC-BP-ATTR-VALUE	Business Process Attribute Values
GRPC-ATTR-ASSERTION	Financial Assertions
GRPC-ATTR-CATEGORY	Control Category
GRPC-ATTR-CTRL_FREQUENCY	Frequency of Control Operation

BC Set	Name
GRPC-ATTR-CTRL_GROUP	Control Group and Subgroup
GRPC-ATTR-CTRL_OBJ_CATEGORY	Control Objective Category and Control Type
GRPC-ATTR-IELC-FREQ	Indirect Entity-Level Control Operation Frequency
GRPC-ATTR-INDUSTRY	Industry
GRPC-ATTR-NATURE	Nature of Control
GRPC-ATTR-PURPOSE	Control Purpose
GRPC-ATTR-RELEVANCE	Control Relevance
GRPC-ATTR-RISK_IMPACT	Qualitative Risk Impact
GRPC-ATTR-SAMPLE_METHOD	GRPC: Add New Sampling Method to BC Set
GRPC-ATTR-SCHED_FREQUENCY	Scheduling Frequency
GRPC-ATTR-SIGNIFICANCE	Control Significance
GRPC-ATTR-TEST_TECH	Test Technique
GRPC-ATTR-TRANSTYPE	Transaction Type
GRPC-RPTRES-SOX	User Responsible for Reporting Entity- SOX
GRPC-RPTRES-FDA	User Responsible for Reporting Entity- FDA
GRPC-RESP-USER-SOX-UPG	Upgrade-BC Set of SOX Agent Determination Rules
GRPC-RESP-USER-FDA-UPG	Upgrade-BC Set of FDA Responsible Person
SAP Process Control FDA-specific BC sets for FDA regulations	
GRFN-PNS-FDA	Plan Usage – FDA Note Before activating this BC set, first activate GRPC-MCF-FDA.
GRPC-AGENTSLOTC-FDA	FDA Roles to Receive Tasks in Workflow
GRPC-MCF-FDA	Regulation/Policy – FDA
GRPC-ROLE-FDA	Roles for Regulation/Policy FDA Note Before activating this BC set, first activate GRPC-MCF-FDA.
SAP Process Control BC sets for SOX regulations:	
GRFN-PNS-SOX	Plan Usage – SOX

BC Set	Name
	Note Before activating this BC set, first activate GRPC-MCF-SOX.
GRPC-AGENTSLOTC-SOX	SOX Roles to Receive Tasks in Workflow
GRPC-MCF-SOX	Regulation/Policy – SOX
GRPC-ROLE-SOX	Roles for Regulation/Policy SOX Note Before activating this BC set, first activate GRPC-MCF-SOX.

Note

The following BC sets must be activated *twice*:

- GRPC-ATTR-CTRL_OBJ_CATEGORY (Control Objective Category and Control Type)
- GRPC-ATTR-CTRL_GROUP (Control Group and Subgroup)

6.4 Shared BC Sets (SAP Process Control and SAP Risk Management)

You need to activate the following BC sets that are delivered with SAP Process Control 10.1 and SAP Risk Management 10.1

Table 16

BC Set	Description
GRFN-AHISS-CAPA-REG-CRS	Enable CAPA by Regulation Type for Cross Regulation Entities
GRFN-AHISS-OBJECT	Enable Ad Hoc Issues by Object Type
GRFN-AHISS-SOURCE	Maintain Ad Hoc Issue Sources
GRFN-AHISS-SOURCE-ENTITY	Assign Ad Hoc Issue Sources to Entity Types
GRFN-ALLOW-CREATE-LOCAL-CTRL	Maintain Possibility to Add Local Controls to Local Subprocess
GRFN-POLICY-ACKN-OPTION	Define acknowledgment option
GRFN-POLICY-APPROVAL	Define Policy Approvals
GRFN-POLICY-CATEGORY	Maintain Policy Categories
GRPC-AMF-MENUITEM-UPGRADE	BC Set of AMF menu items for upgrade customers

BC Set	Description
	(for upgrade customers only) Note This BC set must be activated twice.
GRFN-WORKFLOW-NOTIFICATION	Maintain Workflow Notifications
GRPC-FREQUENCY	Timeframe Frequencies
GRPC-TIMEFRAME	Timeframes
BC_SET_BENEFIT_CATEGORY	Maintain Benefit Category
GRPC-RISK-DRIVER-CATEGORY	Driver Category of Risk Attributes
GRPC-RISK-IMPACT-CATEGORY	Impact Category of Risk Attributes
BCSET-GRRM-GRFNV_DEC_SETUP	Define Probability and Maximum Score
BCSET-GRRM-GRRMVRISKOPPLVL	Maintain Risk and Opportunity Levels
BC-SET_RISK_PRIORITY_ID	Maintain Risk Priority ID

Note

If you are using Internal Audit Management functionality, ensure that the following BC Sets are activated:

- BCSET-GRRM-GRFNV_DEC_SETUP
- BCSET-GRRM-GRRMVRISKOPLVL
- BC-SET_RISK_PRIORITY_ID

These BC sets are used by the audit risk rating function of Internal Audit Management when setting risk score, risk level, and risk priority for an auditable entity.

6.5 SAP Risk Management BC Sets

You need to activate the following BC sets that are delivered with SAP Risk Management 10.1:

Table 17

BC Set	Name
BC_SET_ANALYSIS_PROFILE	Maintain Analysis Profile
BC-SET_ACTIVITY_TYPES	Maintain Activity Types
BC_SET_BENEFIT_CATEGORY	Maintain Benefit Category
BC_SET_DEFINE_CATEGORIES_POWL	Maintain Categories for POWL
BC_SET_DEFINE_THREE_POINT_ANALYS	Define Three Point Analysis
BC_SET_DRIVER_CATEGORY	Maintain Driver Category

BC Set	Name
BC_SET_IMPACT_CATEGORY	Maintain Impact Category
BC_SET_IMPACT_LEVEL	Impact and Risk Levels
BC-SET_INFLUENCE_STRENGTH	Define Influence Strength
BC_SET_MAINTAIN_DEFAULT_QUERY	Maintain Default Query for POWL
BC-SET_MAINTAIN_OPP_RESP_TYPES	Maintain Opportunity Response Types
BC_SET_MAINTAIN_USER_RESP	Maintain Users Responsible for Entity
BC_SET_OBJECTIVE_CATEGORIES	Maintain Objective Category
BC_SET_PROBABILITY_LEVEL_ID	Maintain Probability Level ID
BC_SET_PROBABILITY_LEVEL_MATRIX	Maintain Probability Level Matrix
BC-SET_RESPONSE_EFFECTIVENESS	Maintain Response Effectiveness
BC-SET_RESPONSE_TYPE	Maintain Response Type
BC_SET_RISK_APETITE	Maintain Risk Appetite
BC_SET_RISK_LEVEL	Impact and Risk Levels
BC_SET_RISK_LEVEL_MATRIX	Maintain Risk Level Matrix
BC_SET_RISK_PRIORITY_MATRIX	Maintain Risk Priority Matrix
BC_SET_ROLES	BC Set for Roles
BC_SET_SPEED_OF_ONSET	Maintain Speed of Onset
BC-SET_LOSS_MATRIX_COLORS	Incident Loss Color Matrix
BC_SET_UNIT_MEASURE	Maintain Units of Measures
BC-SET_RISK_RESPONSE_TYPE	Maintain Risk Response Type Combination
BCSET-GRRM-GRFNV_POLICYTYPE	Maintain Response Relevance for Policy Types
BCSET-GRRM-GRRMVPOLICYRESP	Link Policy Status and Response Completeness

7 SAP Enterprise Portal Configuration

7.1 Creating a System Connection with the SAP Enterprise Portal

For information about how to create an SAP Enterprise Portal system connection for SAP Access Control 10.1, SAP Process Control 10.1, and SAP Risk Management 10.1, follow the path: help.sap.com/nw70 › *Application Help* › *SAP Library* › *SAP NetWeaver* › *SAP NetWeaver by Key Capability* › *People Integration by Key Capability* › *Portal* › *Portal Administration Guide* › *Super Administration* › *Pre-configured Roles* › *Administration Roles* › *Workset: System Administration*

For optimum display of the portal, choose the relevant portal configuration required depending on your license configuration. Select portal configuration for SAP Access Control 10.1-only license users or for SAP solutions for governance, risk, and compliance (GRC) multiple application license users (AC10.1 + PC10.1 + RM10.1 or any combination of two applications).

> Note
>
> SAP provides a set of sample roles that include the recommended authorizations. You can create your own PFCG roles or copy the sample roles to your customer namespace and then modify them as needed.
>
> For more information about the delivered roles for, see the Security Guide for SAP Access Control 10.1 / SAP Process Control 10.1 / SAP Risk Management 10.1 at help.sap.com/grc. Choose your application, then choose *Security Information* › *Security Guide*.

7.2 Portal Configuration for SAP Access Control 10.1- Only Licensed Users

The list below contains the system and portal aliases roles that you configure if you only have SAP Access Control 10.1 in your system landscape.

- **System Aliases**:
  - The system alias must use `SAP-GRC`, `SAP-GRC-AC`, and SAP_GRC.
- **Portal Roles**:
  - Assign the role `GRC ACCESS CONTROL` to users.
  - Assign the role `ERP COMMON` to everyone in the user group.

7.3 Portal Configuration for SAP Solutions for GRC- Licensed Users

If your system landscape contains more than one GRC component (SAP Access Control 10.1, SAP Process Control 10.1, or SAP Risk Management 10.1), you configure the system aliases and portal roles as follows:

System Aliases

Table 18

GRC Component	System Alias Configuration
If SAP Access Control 10.1 is activated:	The system alias must use SAP-GRC, SAP-GRC-AC, and SAP_GRC.
If SAP Process Control 10.1 is activated:	The system alias must use SAP-GRCand SAP-GRC-PC, and SAP_GRC
If SAP Risk Management 10.1 is activated:	The system alias must use SAP-GRC and SAP-GRC-RM, and SAP_GRC.

Portal Roles

Table 19

Assign to	Role Name
User	GRC SUITE
Everyone in the user group	ERP COMMON
User, if needed	GRC Internal Audit Management

Note

For SAP Access Control 10.1 only environments, you must assign the GRC Access Control role to at least one user.

7.4 Creating the Initial User in the ABAP System

SAP solutions for governance, risk, and compliance (GRC) 10.1 uses various roles to interface with the SAP system. This section explains how to create your initial ABAP system user for SAP Access Control 10.1, SAP Process Control 10.1, and SAP Risk Management 10.1.

Note

This section uses the delivered roles as examples only. As you complete the procedure, you must replace the delivered roles with equivalent roles in your customer namespace.

Procedure

SAP Access Control 10.1

To create an initial user in the ABAP system for SAP Access Control 10.1:

1. Assign all SAP Access Control users the role `SAP_GRAC_BASE` so they can access the SAP Access Control 10.1 applications.
2. Assign the role `SAP_GRAC_ALL` to the user who will perform Customizing. This role is the power user role. It gives the designated user the ability to see and do everything without being assigned to a specific SAP Access Control role. This role is typically assigned to the user who creates the organization structures and assigns the business roles to all the other users.

   > **Note**
   >
   > The role does not contain the authorizations for Workflow Customizing, Case Management, or web services activation. For these authorizations, use the role `SAP_GRAC_SETUP`.

   > **Caution**
   >
   > Assign the `SAP_GRAC_ALL` role carefully, since a user assigned to this role can make pervasive changes.
   >
   > For more information on the `SAP_GRAC_ALL` role and its authorizations, see the *SAP AC/PC/RM 10.1 Security Guide* at: help.sap.com/grc › *Access Control* › *Security Information* › *Security Guide* .

3. Using transaction `SU01`, create a user.
4. If this user needs to receive workflow notifications via e-mail, on the *Address* data tab, assign an e-mail address and a *Comm. Meth* of *E-Mail* to the user.
5. On the *Roles* tab, assign the roles `SAP_GRAC_BASE` and `SAP_GRAC_ALL` to this user.
6. This user can now use transaction `SPRO` to complete the Customizing configuration including such steps as activating the Business Configuration (BC) sets and assigning roles to other users

   .

SAP Process Control 10.1 and SAP Risk Management 10.1

To create initial users in the ABAP systems for SAP Process Control 10.1 and SAP Risk Management 10.1 follow the steps below:

1. Assign all SAP Process Control and SAP Risk Management users to the role `SAP_GRC_FN_BASE` to allow them to access the SAP Process Control or SAP Risk Management applications.
2. Assign the `SAP_GRC_FN_ALL` role to the user doing the Customizing of the product. This role is the power user role. It gives the designated user the ability to see and do everything without being assigned to a specific SAP Process Control or SAP Risk Management role. This role is typically assigned to the person who creates the organization structures and assigns business roles to all the other users. It contains all of the authorizations from the role `SAP_GRC_FN_BUSINESS_USER` in addition to the following authorizations:
   - Administrative functions in the SAP Process Control Implementation Guide (IMG), and the SAP Risk Management IMG
   - Structure setup in expert mode
   - Data upload for structure setup
   - Customizing table maintenance for SAP Process Control and SAP Risk Management 10.1
   - Initiation of role assignment procedures

The role does not contain the authorizations for Workflow Customizing, Case Management, or web services activation. For these authorizations, use the role `SAP_GRC_SPC_SETUP`.

> ⚠ Caution
>
> Assign the `SAP_GRC_FN_ALL` carefully, since a user assigned to this role can make pervasive changes.
>
> For more information about the `SAP_GRC_FN_ALL` role and its authorizations, see the *SAP AC/PC/RM 10.1 Security Guide* at: help.sap.com/grc > *choose your product* > *Security Information* > *Security Guide*.

3. Using transaction `SU01`, create a user.
4. If this user needs to receive workflow notifications via e-mail, on the *Address* data tab, assign an e-mail address and a *Comm. Meth* of *E-Mail* to the user.
5. On the *Roles* tab, assign the roles `SAP_GRC_FN_BASE` and `SAP_GRC_FN_ALL` to this user.

This user can now use transaction `SPRO` to complete the Customizing configuration steps such as activating the BC sets and assigning roles to other users.

7.5 Creating the Initial User in the SAP NetWeaver Portal

The navigation tabs and work centers for SAP Access Control 10.1, SAP Process Control 10., and SAP Risk Management 10.1 are defined in the portal roles that are maintained in the SAP GRC portal package.

After creating the portal user, the portal administrator must assign to that user the SAP GRC 10.1 portal roles. These portal roles enable the user to see the SAP GRC navigation and work centers tabs.

> i Note
>
> This section uses the delivered roles as examples As you complete the procedure, you must replace the delivered roles with equivalent roles in your customer namespace.

Procedure

SAP Access Control 10.1

1. Log on as the portal user administrator and access the *User Administration* function.
2. If a user has already been created by the `User Management Engine(UME)` that is connected to the SAP GRC ABAP system, you do not need to create a user in the portal system.

   If a user has not been created by the `User Management Engine(UME)`, create a new portal user and assign the SAP GRC ABAP system to the user in the *User Mapping for System Access* tab, along with a mapped user ID and password.
3. Go to the *Assigned Roles* tab and assign the role *GRC Suite* (name: `pcd:portal_content/com.sap.pct/com.sap.grc.grac/com.sap.grc.ac.roles/com.sap.grc.ac.Role_All`) to the user who has the power user role `SAP_GRAC_ALL` in the ABAP system. This role enables the power user to view the work centers.

SAP Process Control 10.1 and SAP Risk Management 10.1

1. Log on as the portal user administrator and access the *User Administration* function.

2. If a user has already been created by the `User Management Engine (UME)` that is connected to the SAP GRC ABAP system, you do not need to create a user in the portal system.

   If a user has not been created by the UME, create a new portal user and assign the SAP GRC ABAP system to the user in the*User Mapping for System Access* tab, along with a mapped user ID and password.
3. Go to the *Assigned Roles* tab and assign the role*GRC Suite* (name: `pcd:portal_content/($installedpath$)/com.sap.grc.GRC_Suite/com.sap.grc.GRC_Suite_Role/com.sap.grc.GRC)` to the user who has the power user role `SAP_GRC_ALL` in the ABAP system. This role enables the power user to view the work centers.

More Information

For more information about the visibility of work centers, see the *SAP AC/PC/RM 10.1 Security Guide* at ▸ help.sap.com/grc ▸ *choose your product* ▸ *Security Information* ▸ *Security Guide* ◂.

This information is based on the technologies delivered by SAP NetWeaver Portal. For more information, see the *Portal Security Guide* athelp.sap.com/saphelp_spm21_bw/helpdata/en/5c/429f00a14aa54195b1c63ae1512d10/frameset.htm .

www.sap.com

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.