



Migration Guide

SAP Access Control from 4.0/5.3 to 10.1

Target Audience

- Technology Consultants
- System Administrators
- Solution Consultants
- Business Process Owners
- Support Specialists

Document version: 1.0 – June 2013



SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

© Copyright 2013 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. SAP AG and its affiliated companies (“SAP Group”) provide these materials for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group 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.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following address:
<http://help.sap.com/grc>

Typographic Conventions

Type Style	Represents
Example Text	Words or characters that appear on the screen. These include field names, screen titles, pushbuttons as well as menu names, paths and options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, titles of graphics and tables
EXAMPLE TEXT	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, names of variables and parameters, source code as well as names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.
EXAMPLE TEXT	Keys on the keyboard, for example, function keys (such as F2) or the ENTER key.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Contents

1. Getting Started	6
1.1 Document History	6
1.2 About this Guide	6
1.3 Audience for this Guide	7
2. Exploring the Technical System Landscape	8
3. Exploring the Data Migration Process	9
4. Understanding the Prerequisites	11
4.1 AC 4.0 to AC 10.1 Prerequisites	11
4.2 AC 5.3 to AC 10.1 Prerequisites	11
4.3 Downloading the Migration Tool	12
4.4 Installing the Migration Tool	13
4.5 Creating the Organization Unit	13
5. Exporting AC 4.0 (RAR/SPM) and AC 5.3 (SPM) Data	13
5.1 Copying Exported Data to the Import Location	15
6. Exporting AC 5.3 (CUP/RAR/ERM) Data	16
6.1 Exploring the Application Features	16
6.2 Starting the Data Export Process	17
6.3 Setting the Data Export Location	18
6.4 Exporting the Configuration and Master Data	18
6.5 Exporting the Transactional Data	22
6.6 Copying Exported Data to the Import Location	25
6.7 Reverting to the Default Configuration (Optional)	25
6.8 Managing Variants (Optional)	25
6.9 Exporting Application Configuration Data Files (Optional)	27
6.10 Uploading an Export Configuration (Optional)	28
7. Importing Data into AC 10.1	29
7.1 Importing the Data	29
7.2 Completing Intra-Migration Tasks	32
7.3 Importing RAR Data	38
7.4 Importing Workflow Data	39
7.5 Importing ERM Repository Data	40
7.6 Importing CUP Repository Data	40
7.7 Importing SPM Data	41
7.8 Importing Workflow Rule Data	42
8. Completing Post-Import Tasks	45
8.1 Activating the GRC_MSMP_CONFIGURATION BC Set	45
8.2 Generating the Rules (AC 4.0 and AC 5.3)	45
8.3 Creating Function Modules (AC 5.3)	46
8.4 Maintaining Workflow Stage Settings (AC 5.3)	47
8.5 Completing Methodology Process Assignments (AC 5.3)	48
9. Validating the Data	49
9.1 Validating RAR Data	49
9.2 Validating ERM Data	50
9.3 Validating Workflow Data	51
9.4 Validating CUP Data	51

10. Supported AC 4.0 Objects.....	52
10.1 Common Configuration.....	52
10.2 Compliance Calibrator (RAR)	52
10.3 Fire Fighter (SPM).....	53
11. Supported AC 5.3 Objects.....	54
11.1 Configuration and Master Data.....	54
11.2 Transactional Data	58
12. Unsupported Objects and Components.....	59

1. Getting Started

This guide is for customers currently using SAP Access Control 4.0 or Access Control 5.3 who need to migrate data to SAP Access Control (AC) 10.1. Access Control data migration offers the following capabilities:

- Data export of Compliance Calibrator (CC) and Firefighter (FF) data from AC 4.0 (ABAP)
- Data export of Superuser Privilege Management (SPM) data from AC 5.3 (ABAP)
- Data export of Compliant User Provisioning (CUP), Risk Analysis & Remediation (RAR), and Enterprise Role Management (ERM) data from AC 5.3 (Java)
- Data import into Access Control 10.1

Note: Access Control 10.0 customers only need to upgrade their software. No data migration is needed. For more information, see the *SAP Access Control 10.0 to 10.1 Upgrade Guide* at <http://help.sap.com/grc-ac>.



AC 10.0 featured a transition to the ABAP platform (from ABAP and Java used with AC 5.3). Therefore, migration of data involves an automated process with certain manual steps.

Only supported data objects are exported. For more information, refer to the following sections: *Supported AC 4.0 Objects* and *Supported AC 5.3 Objects*.

1.1 Document History

Verify you have the latest version of the Migration Guide by checking <http://help.sap.com/grc-ac> before you begin the migration process.

Version	Date	Description
1.0	June 2013	Initial release

1.2 About this Guide

This guide describes how to migrate applicable data from AC 4.0 and AC 5.3 to AC 10.1. The document describes the following:

- Data Migration Process
- Exporting AC 4.0 data
- Exporting AC 5.3 data
- Importing data into AC 10.1
- Supported AC 4.0 and AC 5.3 objects
- Unsupported objects and components

This guide is a stand-alone document. Note the following:

- This guide provides business use cases as examples on how you can use SAP software. These examples are intended to serve as models and might not run the way they are described here in your customer-specific landscape.
- This guide discusses the migration process from AC 4.0 and AC 5.3 to AC 10.1. Any attempt to use this guide for other product versions is not supported.

This guide is *not* intended for the following uses:

- Installing Access Control 10.1. For more information, see the *SAP Access Control 10.1 / Process Control 10.1 / Risk Management 10.1 Installation Guide* at <http://help.sap.com/grc-ac>.
- Upgrading from Access Control 10.0 to 10.1. For more information, see the *SAP Access Control 10.0 to 10.1 Upgrade Guide* at <http://help.sap.com/grc-ac>.

For an overview of the Access Control 10.1 documentation, refer to the *SAP Access Control 10.1 Master Guide* at <http://help.sap.com/grc-ac>.

1.3 Audience for this Guide

This guide is intended for system administrators, solution and technology consultants, business process owners, and support specialists involved in the process of migrating data from AC 4.0 or AC 5.3 to AC 10.1.

This guide requires you to know how to use AC 5.3 Java-based applications, the ABAP-based SPM application, and AC 10.1 ABAP-based applications.

2. Exploring the Technical System Landscape

A Governance, Risk, and Compliance (GRC) 10.1 system landscape consists of the GRC system, Enterprise Portal system, and Adobe Document Server. The GRC system typically integrates with the ERP system to perform services such as Continuous Control Monitoring or Segregation of Duties (SoD) analysis. Optionally, there can be other systems such as the SAP NetWeaver BI system, as well as third-party solutions. For an illustration of the system landscape, refer to the *SAP Access Control 10.1 Master Guide* at <http://help.sap.com/grc-ac>.



Note

Due to a technology shift to the ABAP stack, AC 10.1 does not support the following AC 5.3 interfaces for GRC BI Content integration:

- SAP AC 5.3 BW Data Source, based on Universal Data Connect (UD Connect)
- SAP AC 5.3 data mart.

Access Control 10.1 uses interfaces based on the SAP R/3 BW Data Source Enhancement.

The following diagram illustrates the AC 10.1 migration architecture:

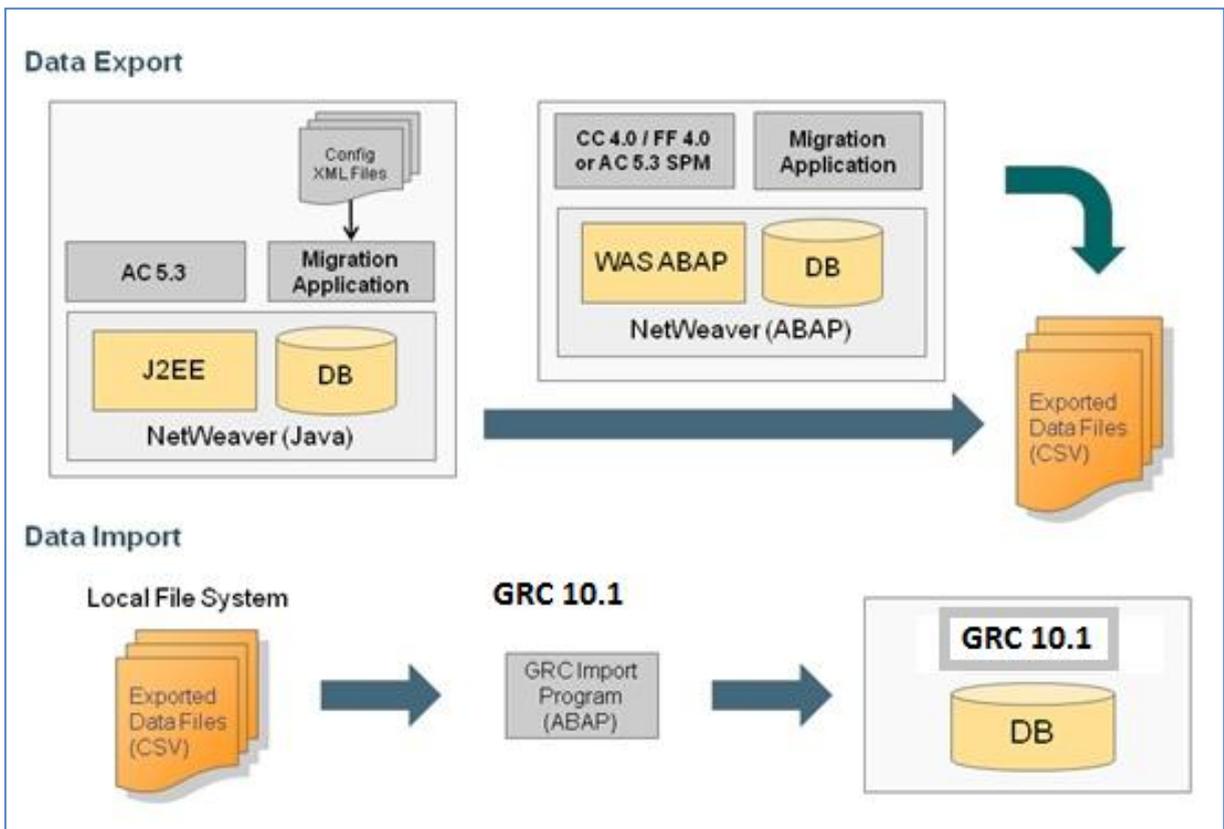


Figure 2-1



Note

If you need to migrate data from all three GRC applications to GRC 10.1, upgrade Process Control and Risk Management first, and then migrate the Access Control data.

3. Exploring the Data Migration Process

This section describes the data migration process from AC 4.0 and AC 5.3 to AC 10.1.

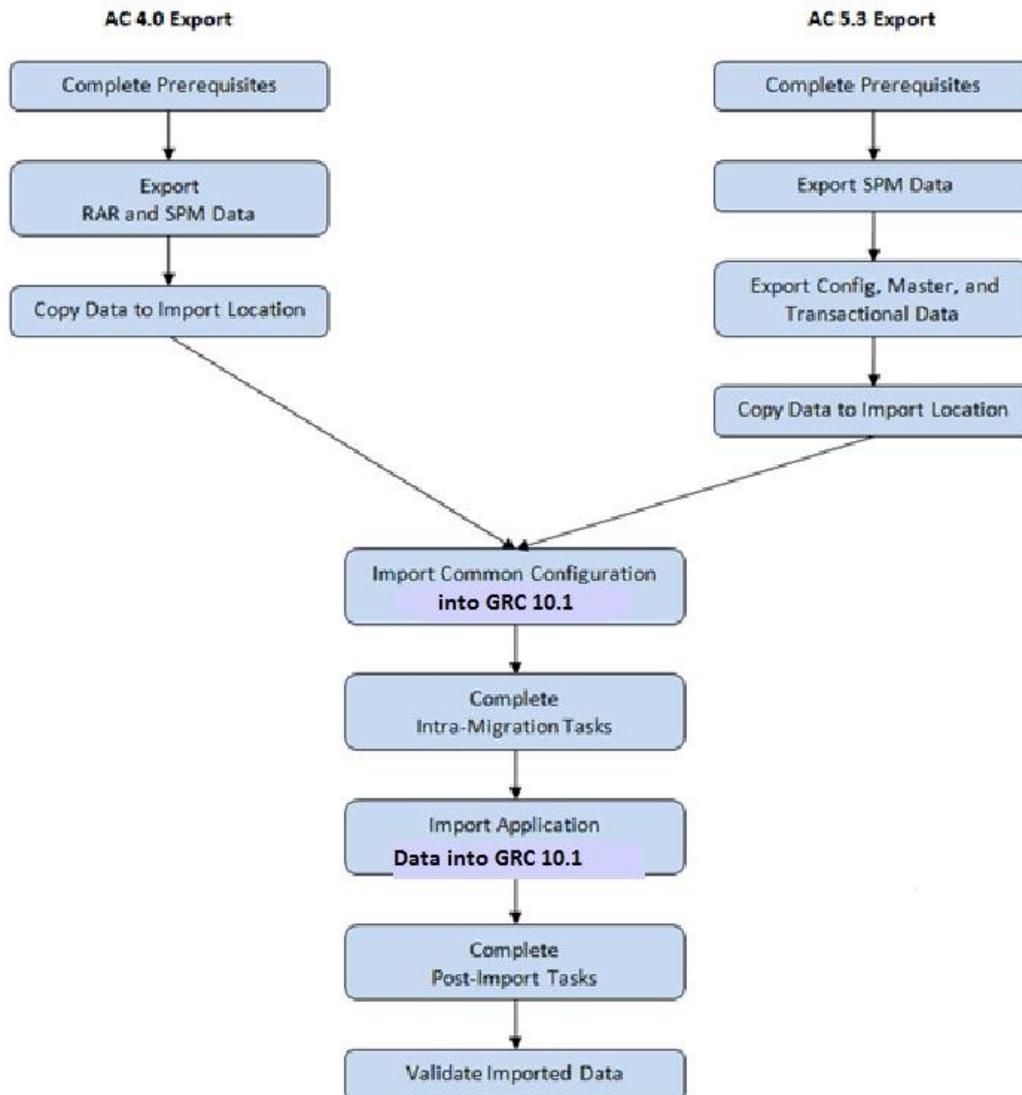


Figure 3-1

The following describes the data migration process:

1. Complete the prerequisites. For more information, see section 4.0 *Understanding the Prerequisites*.
2. Export the RAR and SPM data (AC 4.0) or export the SPM data (AC 5.3), and then copy the exported data to the import location. For more information, see section 5. *Exporting AC 4.0 (RAR/SPM) and AC 5.3 (SPM) Data*.
3. Export the configuration, master, and transactional data (AC 5.3 only). Then copy the exported data to the import location. For more information, see section 6.4 *Exporting the Configuration and Master Data* and section 6.5 *Exporting the Transactional Data*.
4. Import the common configuration data into AC 10.1. For more information, see section 7.1 *Importing the Data*.
5. Complete the intra-migration tasks. For more information, see section 7.2 *Completing Intra-Migration Tasks*.
6. Import the application data into AC 10.1.
7. Complete the post-import tasks. For more information, see section 8. *Completing Post-Import Tasks* *Completing Post-Import Tasks*.
8. Validate the data. For more information, see section 9. *Validating the Data*.

Note: The naming of the functionality has changed. Refer to the following chart for the updated terms after you migrate your data.

Previous Versions	Access Control 5.3	Access Control 10.0/10.1
Compliance Calibrator (CC)	Risk Analysis & Remediation (RAR)	Access Risk Management (ARA)
Virsa Access Enforcer	Compliant User Provisioning (CUP)	Access Request (ARQ)
Virsa Role Expert	Enterprise Role Management (ERM)	Business Role Management (BRM)
Virsa Firefighter (FF)	Superuser Privilege Management (SPM)	Emergency Access Management (EAM)

4. Understanding the Prerequisites

This section describes the prerequisites for migrating AC 4.0 and AC 5.3 data to AC 10.1.

4.1 AC 4.0 to AC 10.1 Prerequisites

This section describes the prerequisites for migrating AC 4.0 data to AC 10.1.

1. Verify the AC10.1 system is properly installed. This includes the AC 10.1 plug-ins on all back-end systems. For more information, see the *SAP Access Control 10.1 / Process Control 10.1 / Risk Management 10.1 Installation Guide* at <http://help.sap.com/grc-ac>.
2. Verify that the following default configuration parameter is maintained:

Parm Group	Param ID	Description
Emergency Access Management	4000	Application Type

3. Specify a dedicated data export/import directory accessible from both AC 4.0 and AC 10.1 systems.

4.2 AC 5.3 to AC 10.1 Prerequisites

This section describes the prerequisites for migrating AC 5.3 data to AC 10.1.

Procedure

1. Verify the AC10.1 system is properly installed. This includes the AC 10.1 plug-ins on all back-end systems. For more information, see the *SAP Access Control 10.1 / Process Control 10.1 / Risk Management 10.1 Installation Guide* at <http://help.sap.com/grc-ac>.
2. Upgrade the AC 5.x application to AC 5.3 SP 20.
3. Verify that all applicable Business Configuration (BC) sets are activated:

For CUP roles, activate the GRAC_ROLE_MGMT_ROLE_STATUS and GRAC_ROLE_MGMT_METHODODOLOGY BC sets.

For ERM roles, activate the GRAC_ROLE_MGMT_LANDSCAPE BC set.



Note

Do not activate the GRC_MSMP_CONFIGURATION BC set before completing the data migration process. You need to activate this BC set *after* migrating the data.

4. Verify that the following default configuration parameters are maintained:

Parm Group	Param ID	Description
Role Management	3000	Default Business Process
Role Management	3001	Default Subprocess
Role Management	3002	Default Critical Level
Role Management	3003	Default Project Release
Role Management	3004	Default Role Status
Emergency Access Management	4000	Application Type

5. Create all relevant AC 10.1 users on the target system.
 6. Before migrating CUP and ERM data, manually create all AC 5.3 custom fields in AC 10.1 using SAP custom field naming conventions.

In AC 10.1, start field names with x, y, or z. For example if the AC 5.3 custom field name is *location*, use *zlocation* as the new custom field name to preserve the data it contains.



Note

You need to also add the x, y or z prefix during export (using transformations) to the AC 5.3 custom field names to map it to AC 10.1 custom field names.

7. Specify a dedicated data export/import directory accessible from both AC 5.3 and AC 10.1 systems.

4.3 Downloading the Migration Tool

To migrate data from the previous versions of Access Control, you need to download the Migration tool. To do this:

1. Go to the *SAP Software Download Center* at service.sap.com/swdc.
2. Under *Support Packages and Patches* (on the left-hand side), select *Browse our Download Catalog*.
3. Select *SAP Solutions for Governance, Risk, and Compliance*.
4. Select *SAP GRC Access Control*.
5. Underneath that, select *SAP Access Control*.
6. Select *SAP Access Control 10.1*.
7. Select *Entry by Component*.
8. Select *AC Migration Tool*.
9. Select *SAP GRC AC Migration 10.0*. Within this file, you will find the *GRCACMIGxx_x.sca* file. You will deploy this file in your GRC AC 5.3 Java Server.



Note

Although the tool is called Migration 10.0, you will now use it to upgrade your system to Access Control 10.1.

4.4 Installing the Migration Tool

The migration tool is installed using the Software Update Manager (SUM). The previous tool, Java Support Package Manager (JSPM) has been replaced in NetWeaver 7.3 by SUM. For more information about SUM, see the following:

- <https://service.sap.com/instguides> → Other Documentation → Deployment Optimization Option of SUM 10.0.
- <https://scn.sap.com/docs/DOC-25113>

4.5 Creating the Organization Unit

You need to create an Organization Unit to import RAR application data.

Procedure

1. Execute transaction *SPRO*. The *SAP Reference IMG* window appears.
2. To create the root organization, navigate to *Governance, Risk, and Compliance > Shared Master Data Settings > Create Root Orgs Hierarchy*.
3. Choose *Standard Hierarchy View (002)* to display the *Organization View*.
4. Type values in the *Root Organizational Unit* and *Child Organizational Unit* field.
5. Choose *Execute*.
6. Execute */ngrfn_str_change*. The *SAP GRC Change* window appears.
7. Search for the organization name you created earlier to determine the ID number of the organization.



Note

Always use the Child Organizational Unit ID to import RAR application data.

5. Exporting AC 4.0 (RAR/SPM) and AC 5.3 (SPM) Data

This section describes the AC 4.0 and AC 5.3 Data Export Program to export RAR and SPM data from AC 4.0 and SPM data from AC 5.3. The export process formats the data to ensure that it is compatible with corresponding AC 10.1 tables, and creates all files to store the exported data.

Procedure

1. Log on to the backend system (system on which the Access Control 10.1 plug-ins are installed) to update an existing AC 4.0 or AC 5.3 environment.
2. Execute transaction */GRCPI/AC_EXPORT*.

The AC 4.0 and AC 5.3 Data Export program screen appears.

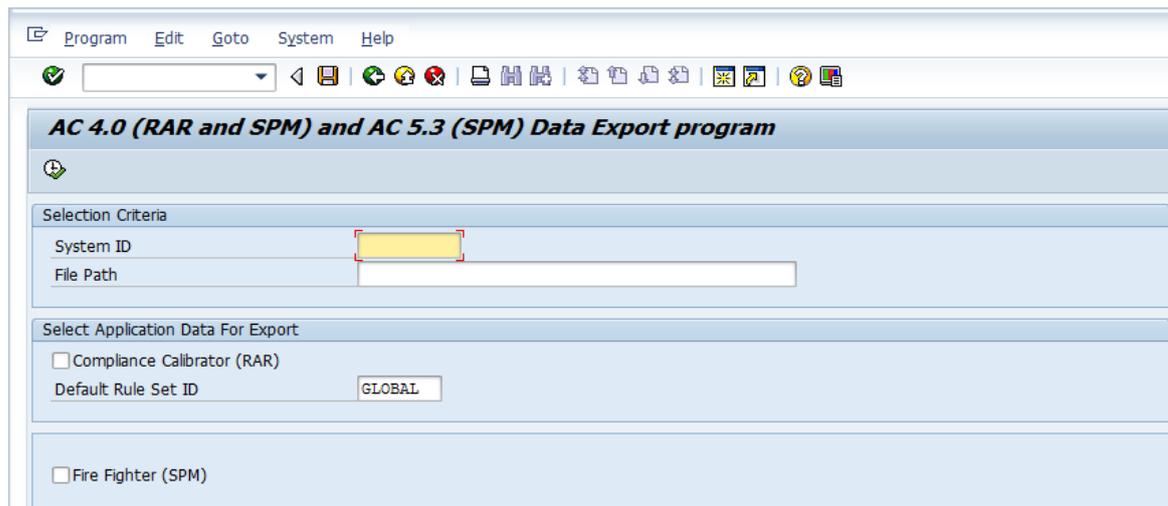


Figure 5-1

3. Enter data in the following fields (all fields are required):

Section	Field	Description
Selection Criteria	System ID	The name of the RFC destination or target connector (that you create using transaction SM59 on the AC 10.1 system).
	File Path	The location of the output file. This must be a local location on the system (not a network folder). Also, the destination folder must have read and write permissions for files to export.
Select Application Data for Export	Compliance Calibrator (RAR)	Select the application: RAR, SPM, or both. You cannot select RAR when exporting AC 5.3 data.
	Fire Fighter (SPM)	
	Default Rule Set ID	A custom name. The default value is GLOBAL.

4. Choose *Execute*.

The program displays the output summary, and creates all files in the location specified in the *File Path* field.

**Note**

When exporting SPM data, the AC 4.0 and AC 5.3 Data Export Program creates a file called OWNERdata.dat. However, the program also creates a similarly-named file for the owner data in the RAR application.

Therefore, you need to import the SPM data in append mode to avoid overwriting the previous application data in the OWNERdata.dat file.

This completes the data export process for AC 4.0. This completes the first step of the data export process for AC 5.3.

5.1 Copying Exported Data to the Import Location

Copy (or FTP) the exported data files to a local folder on the server on which AC 10.1 is deployed.

6. Exporting AC 5.3 (CUP/RAR/ERM) Data

This section describes how to use the Data Export Application, available in SAP solutions for GRC 10.1, to export CUP, RAR, and ERM data from AC 5.3. The export process automatically formats the data to ensure that it is compatible with corresponding AC 10.1 tables, and creates all files to store the exported data.

6.1 Exploring the Application Features

The SAP solutions for GRC Data Export Application enables you to export configuration and master data from AC 5.3, applying filters and transforming the data before exporting, as required. You can also upload a data export configuration, reset the application configuration to default settings, and manage custom filter and transform variants, as necessary. The figure below shows the main screen of the Data Export Application.



Note

Although it is labeled GRC 10.0 Data Export Application, you will now use it to upgrade your system to Access Control 10.1.



Figure 6-1

The data export application features the following principal sections:

- Administration
 - This section allows you to manage customizations and application variants, reset any application customizations, and configure the export location. Specifically, you can do the following:
 - Optionally, upload a configuration file for the export application. This allows you to export custom fields from your AC 5.3 environment.
 - Set the data export location.
 - Reset any custom configurations applied to the application, reverting it back to default settings. You can do this to reset any filters or transformations that you have set.
 - Manage variants (filters and transformation settings) by loading or deleting variants from the application configuration.

- Data Export
 - This section allows you to manage the data to be exported. Specifically, you can do the following:
 - Export AC 5.3 configuration and master data
 - Export AC 5.3 transactional data

- Reports
 - This section enables you to export your customizations of the application, as a data file. Specifically, you can do the following:
 - Export the configuration data
 - Export the master data file
 - Export the transaction data file

6.2 Starting the Data Export Process

This section describes how to start the AC 5.3 data export process.

Procedure

1. Launch the GRC 10.1 Data Export Application using the following URL, where *<servername>* and *<instance>* represent the server name and instance in your environment:

*http://<servername>:5<instance>00/webdynpro/dispatcher/sap.com/grc-acmigapl/
GRC2010Migration*

2. Log on to the application using your user ID and password.

The user ID must be assigned the Administrator role.

6.3 Setting the Data Export Location

This section describes how to specify the location on the local system where the exported files are to be stored.

Procedure

1. In the *Administration* section, click *Configure data export location*.
2. Select the location for the date using the context menu (folder).



The location must be local to the server on which the application is running.

3. Choose *OK*.

6.4 Exporting the Configuration and Master Data

You need to export the AC 5.3 configuration and master data. When exporting the data, you can select the objects you want to export and optionally apply filters and transformations before exporting.

Procedure

1. In the *AC 5.3 Configuration and Master Data Export* section, choose *Data Export*.
2. Select the objects you want to export, and click *Next*.

Optionally, you can select all objects by selecting the corresponding checkbox.

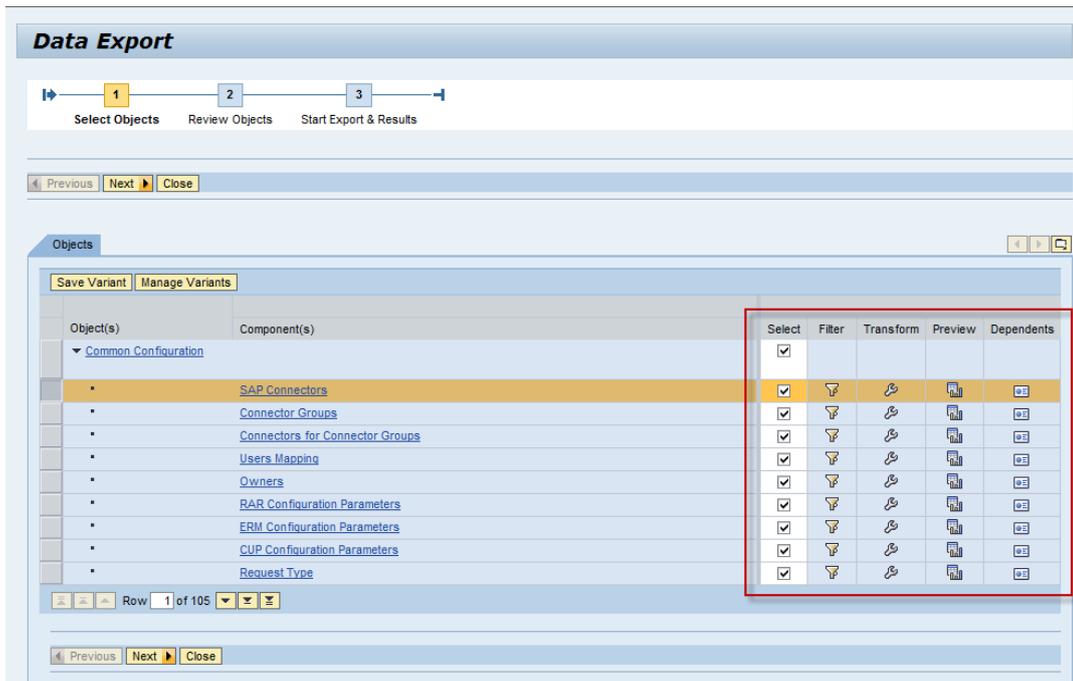


Figure 6-2

3. To preview the data before exporting, choose the preview  icon.



For large data sets, the application displays only the first 500 records. In this case, SAP recommends that you export the files first and preview the data by opening the exported files.

4. To apply a filter, choose the filter icon  to the right of the corresponding object.

Select the *Application*, *Column Name*, *Filter Type*, and *Filter Value*. Select *Copy to Dependents* to copy the filter to dependents of the selected object. Note the following:

- Fields marked with asterisks * are mandatory.
- The Filter Type value can be *Equal to*, *Not equal to*, *In*, *Not in*, *Like*, and *Not like* (in relation to the filter value). *Equal to* performs an exact match, *Like* performs pattern matching using wildcard characters, and *In* compares against a list of values.



Note

You can paste the filter in child objects (dependents) if it applies to key parameters.

5. To modify the existing data, choose the Transform icon  to the right of the corresponding object.

This allows you to remove or change values. For example, you might want to remove data in a description field.

In the *Application* and *Column* fields, choose values using the dropdown menus. In the *Current Value* field, enter the current value for the object; in the *New Value* field, enter the corresponding new value.

Application	Column	Current Value	New Value
RAR			

Figure 6-3

**Note**

In AC 10.1, the maximum length of certain objects (such as Business Subprocess) is shorter than the corresponding object in AC 5.3. You can use the transform option to reduce the length of the data in these objects to comply with AC 10.1.

Also, when transforming an object, you need to manually transform other instances of the object used elsewhere in your environment.

- To view the dependents of a component, choose the Dependents icon  to the left of the corresponding component.

Component Details for SAP Connectors

Component Details

Component Details | Data Source | Target Mapping | **Dependents**

ComponentName	Child
SAP Connectors	Connectors for Connector Groups
SAP Connectors	Function Action
SAP Connectors	Function Permission
SAP Connectors	Mitigation Control Report
SAP Connectors	Critical Roles
SAP Connectors	Critical Profiles
SAP Connectors	Supplement Rule Header
SAP Connectors	Supplement Rule
SAP Connectors	System Users
SAP Connectors	Users Mapping

Row 1 of 10

Close

Figure 6-4

- Review your selection of components, filters, and transformations, and choose *Next*. Uncheck any filters or transformations that you do not want to apply to the component.

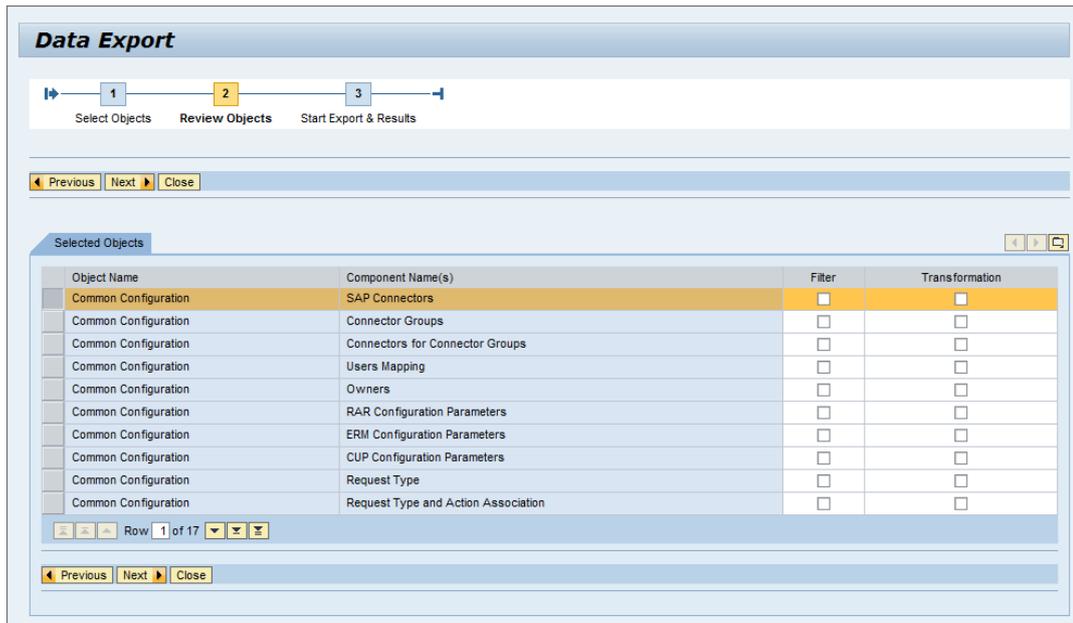


Figure 6-5

8. Perform a final review, and choose *Next*.
9. Choose *Start Export*.

The progress bar shows the percentage of files exported, and the output data appears in the log window.

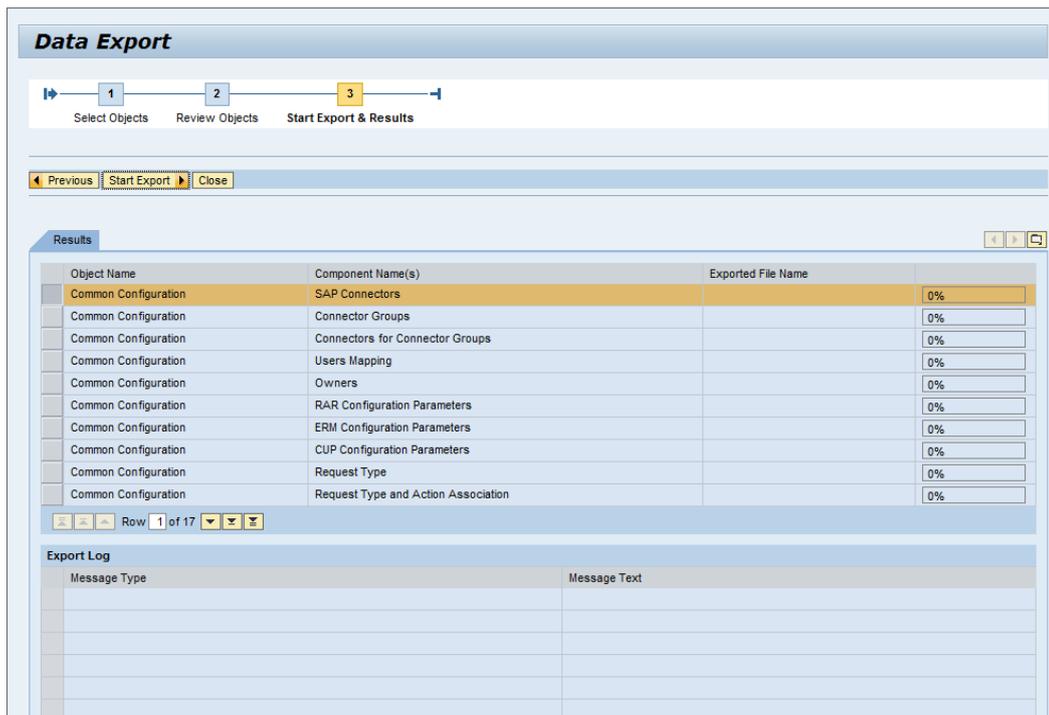


Figure 6-6

The export results are recorded in the *Export Log* table in the bottom pane.

Choose an exported file name, such as *CONNECTORSdata.dat* (for SAP Connectors), to open the exported data. You can also verify the exported data by examining the destination folder or using the export application itself.

If data is not available for any of the components, a *no file created* message appears in the *Export File Name* column (instead of the export file name).

6.5 Exporting the Transactional Data

You can optionally export the AC 5.3 transactional data. When exporting the data, you can select the objects you want to export and optionally apply filters and transformations before exporting.



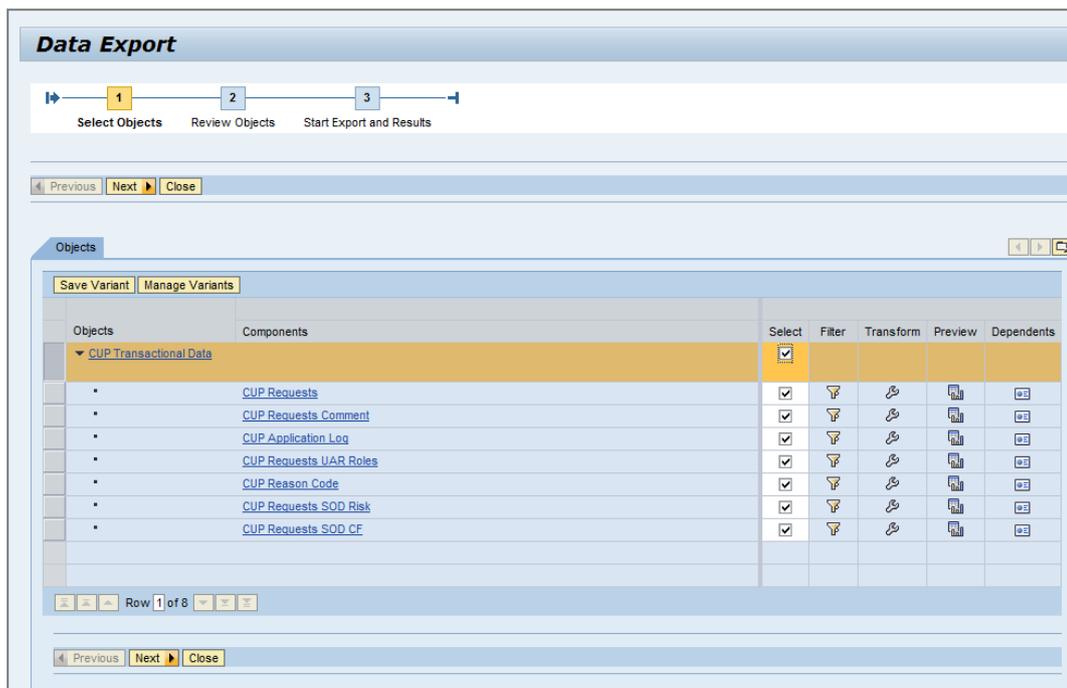
Note

The transactional data is not imported into AC 10.1.

Procedure

1. In the *AC 5.3 Transactional Data Export* section, choose *Data Export*.
2. Select the objects you want to export, and click *Next*.

Optionally, you can select all objects by selecting the corresponding checkbox.



The screenshot shows the 'Data Export' interface. At the top, there is a progress bar with three steps: '1 Select Objects', '2 Review Objects', and '3 Start Export and Results'. Below the progress bar are navigation buttons: 'Previous', 'Next', and 'Close'. The main area is titled 'Objects' and contains a table with columns: 'Objects', 'Components', 'Select', 'Filter', 'Transform', 'Preview', and 'Dependents'. The table lists several objects under the 'CUP Transactional Data' category, each with a checked 'Select' checkbox and icons for 'Filter', 'Transform', 'Preview', and 'Dependents'. At the bottom of the table, there is a 'Row 1 of 8' indicator and another set of 'Previous', 'Next', and 'Close' buttons.

Objects	Components	Select	Filter	Transform	Preview	Dependents
▼ CUP Transactional Data						
•	CUP Requests	<input checked="" type="checkbox"/>				
•	CUP Requests Comment	<input checked="" type="checkbox"/>				
•	CUP Application Log	<input checked="" type="checkbox"/>				
•	CUP Requests UAR Roles	<input checked="" type="checkbox"/>				
•	CUP Reason Code	<input checked="" type="checkbox"/>				
•	CUP Requests SOD Risk	<input checked="" type="checkbox"/>				
•	CUP Requests SOD CF	<input checked="" type="checkbox"/>				

Figure 6-7

3. To preview the data before exporting, choose the preview  icon.



For large data sets, the application displays only the first 500 records. In this case, SAP recommends that you export the files first and preview the data by opening the exported files.

4. To apply a filter, choose the filter icon  to the right of the corresponding object.

Select the *Application*, *Column Name*, *Filter Type*, and *Filter Value*. Select *Copy to Dependents* to copy the filter to dependents of the selected object. Note the following:

- Fields marked with asterisks * are mandatory.
- The Filter Type value can be *Equal to*, *Not equal to*, *In*, *Not in*, *Like*, and *Not like* (in relation to the filter value). *Equal to* performs an exact match, *Like* performs pattern matching using wildcard characters, and *In* compares against a list of values.



Note

You can paste the filter in child objects (dependents) if it applies to key parameters.

5. To modify the existing data, choose the Transform icon  to the right of the corresponding object.

This allows you to remove or change values. For example, you might want to remove data in a description field. In the *Application* and *Column* fields, choose values using the dropdown menus.

In the *Current Value* field, enter the current value for the object. In the *New Value* field, enter the corresponding new value.

6. To view the dependents of a component, choose the Dependents icon  to the left of the corresponding component.
7. Review your selection of components, filters, and transformations, and choose *Next*.

Clear any filters or transformations that you do not want to apply to the component.

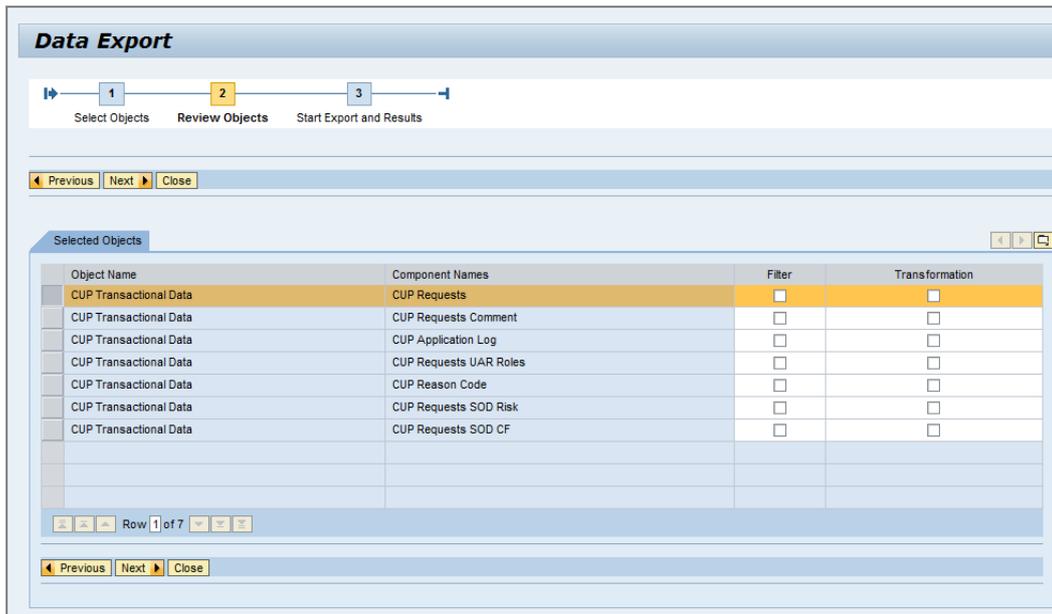


Figure 6-8

8. Perform a final review, and choose *Next*.
9. Choose *Start Export*.

The progress bar shows the percentage of files exported, and the output data appears in the log window.

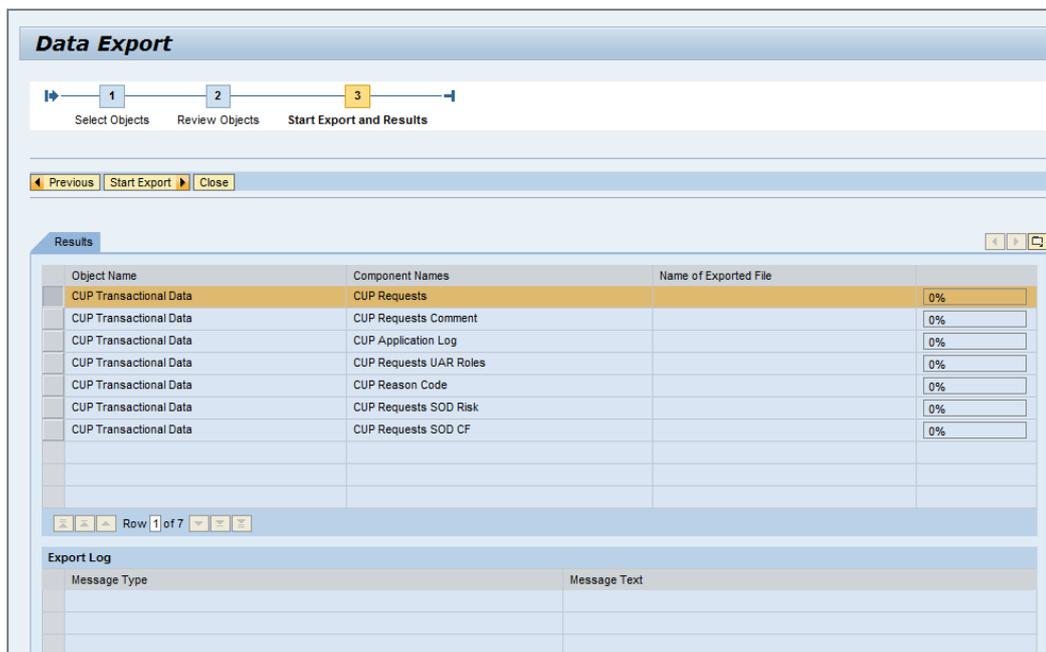


Figure 6-9

The export results are recorded in the *Export Log* table in the bottom pane.

You have now completed the AC 5.3 data export process.

6.6 Copying Exported Data to the Import Location

Copy (or FTP) the exported data files to a local folder on the server on which AC 10.1 is deployed.

6.7 Reverting to the Default Configuration (Optional)

You can reset the application to the default configuration, removing any filters or transformations that you have defined. This is an optional step and not required to complete the export process.

Procedure

1. In the *Administration* section, choose *Reset data export configuration*.
2. Select the options you want reset.
3. Chose *OK*.



Figure 6-10

6.8 Managing Variants (Optional)

You can save your filter and transformation settings as a variant for later use. This allows you to save and view specific data exports that you performed earlier. You can further manage these variants, loading and deleting them.

Procedure

To save a variant

1. When selecting objects while performing a *Data Export* operation, define filters and data transformations.

- Choose *Save Variants*. The *Save Variant* dialog appears.

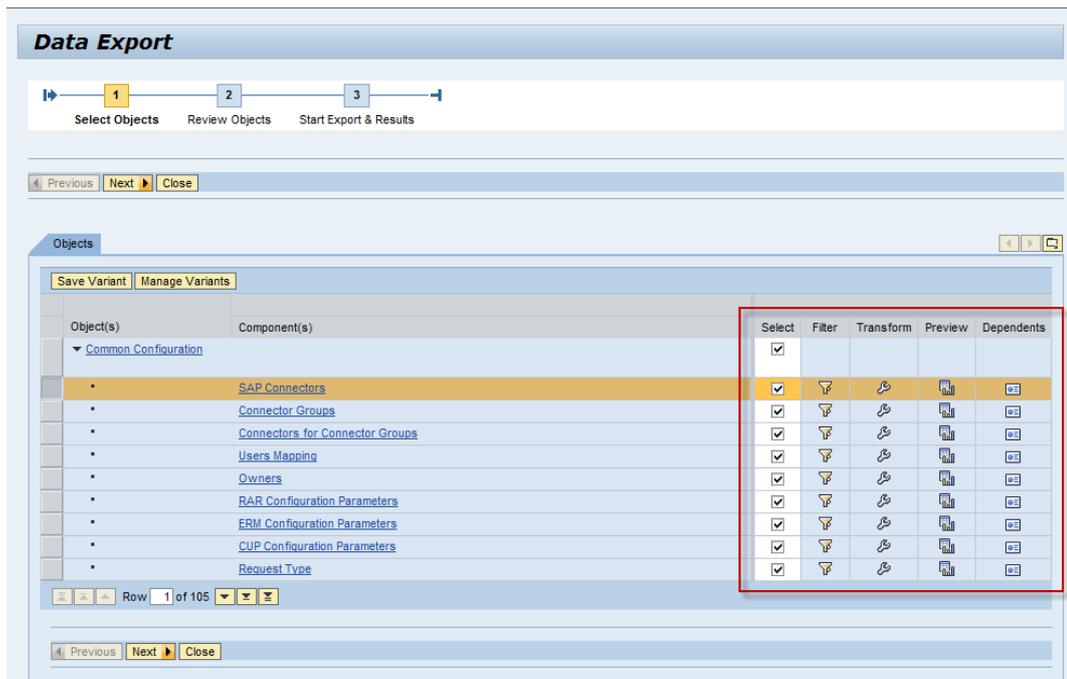


Figure 6-11

- In the *Variant Name* field, enter a unique name.
- In the *Description* field, enter a description of the filters and transformations being saved.
- Choose *Save*.

To load or delete a variant

- In the *Administration* section, choose *Manage Variants*.
- To load a variant, select a variant and choose *Load*.



Note

Loading a variant removes your current data export location configuration. You need to specify the location again immediately after loading a variant. For more information, see [6.3 Setting the Data Export Location](#).

- To remove a variant, select the variant and choose *Delete*.

Variant Name	Variant Description
--------------	---------------------

Figure 6-12

6.9 Exporting Application Configuration Data Files (Optional)

You can optionally create an XML-formatted file containing the filters and transformation configuration. This is not required to complete the data export process.

Procedure

1. In the *Reports* section, choose *Export Configuration Data*, *Export Master Data File*, or *Export Transaction Data File*.
2. Choose the tab corresponding to the data you want to export.



The data is exported as an (.xls) excel file.

3. Choose *Export*.

The following shows the *Export Configuration Data* screen.

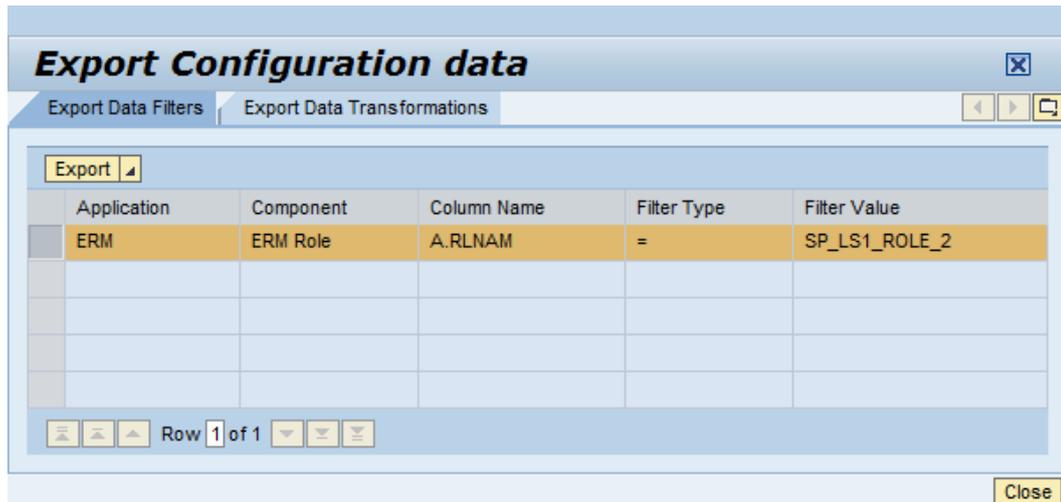


Figure 6-13

6.10 Uploading an Export Configuration (Optional)

You can upload an export configuration into the application, if required.



This is an optional step and not required to complete the data export process. The application comes with a default configuration.

Procedure

1. In the *Administration* section, choose *Upload data export configuration*.
2. Enter the file path for the XML-based configuration, or choose *Browse* to browse to the file location.
3. Choose *OK*.

7. Importing Data into AC 10.1

This section describes how to use the SAP solutions for GRC 10.1 Data Import Application to import data into Access Control 10.1.

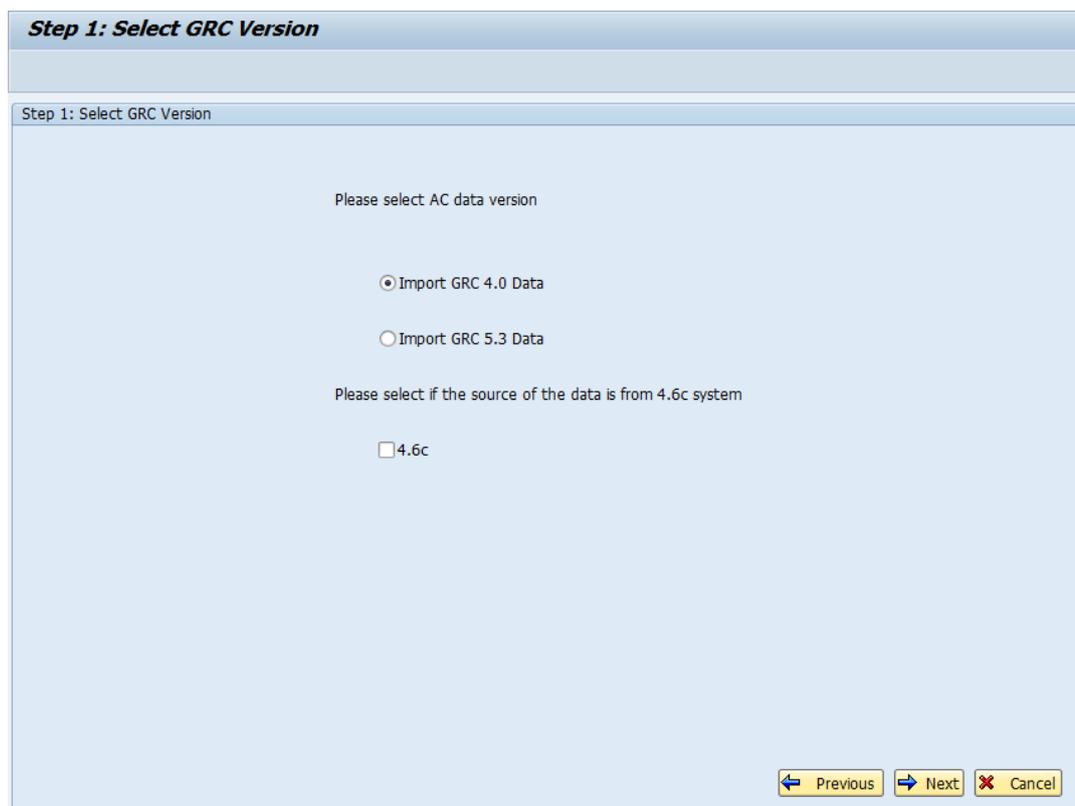
7.1 Importing the Data

You can use the SAP solutions for GRC 10.1 Data Import Application to import the following data:

- Common configuration data
- RAR data (including Risk, Mitigation Control, Org Rule, and Business Unit data)
- Workflow data
- ERM Repository data
- CUP Repository data
- SPM data

Procedure

1. Log on to the SAP Access Control system.
2. Execute transaction *GRAC_DATA_MIGRATION*. The welcome screen appears.
3. Choose *Start Process* to start the import process.
4. Select the system from which to import the data, and click *Next*.



Step 1: Select GRC Version

Step 1: Select GRC Version

Please select AC data version

Import GRC 4.0 Data

Import GRC 5.3 Data

Please select if the source of the data is from 4.6c system

4.6c

← Previous Next → ✕ Cancel

Figure 7-1



Note

If you are importing data from a 4.6C system, select the 4.6C check box.

A screen appears allowing you to import the configuration data.

5. Enter the location for the configuration data from the previous system. Use UNIX-style directory names, such as /AC_MIGRATION, on both UNIX and Windows-based systems.



The folder must contain files from the previously-specified system.



You can skip this step if you have already imported the configuration data.

6. Choose *Get Files*. The configuration-related files for the system you selected earlier appears.
7. Choose the files to import by selecting the corresponding boxes to the left of the files.



Files might be dependent, therefore, you need to select the parent file when selecting a dependent to import.

Step 2: Import Configuration

Step 2: Import Configuration Data

Import Location: /cf2/ac0301 Get Files

Process Name	File Name	Append Data
RAR Configuration Parameters	/cf2/ac0301/RARC�FGPARAMdata.dat	<input type="checkbox"/>
Owners	/cf2/ac0301/OWNERSdata.dat	<input type="checkbox"/>
Users Mapping	/cf2/ac0301/GRACUSERMAPdata.dat	<input type="checkbox"/>
Request Type	/cf2/ac0301/GRACREQTYPEdata.dat	<input type="checkbox"/>
Request Type	/cf2/ac0301/GRACREQTYPETdata.dat	<input type="checkbox"/>
Request Type and Action Association	/cf2/ac0301/GRACREQTYPACTdata.dat	<input type="checkbox"/>
Priority	/cf2/ac0301/GRACPRIORITYdata.dat	<input type="checkbox"/>
Priority	/cf2/ac0301/GRACPRIORITYTdata.dat	<input type="checkbox"/>
Functional Area	/cf2/ac0301/GRACFUNCTAREAdata.dat	<input type="checkbox"/>
Functional Area	/cf2/ac0301/GRACFUNCTAREATdata.dat	<input type="checkbox"/>
Employee Type	/cf2/ac0301/GRACEMPTYPEdata.dat	<input type="checkbox"/>
Employee Type	/cf2/ac0301/GRACEMPTYPETdata.dat	<input type="checkbox"/>
Critical Level	/cf2/ac0301/GRACCRITLVLdata.dat	<input type="checkbox"/>
Critical Level	/cf2/ac0301/GRACCRITLVLTdata.dat	<input type="checkbox"/>
Company	/cf2/ac0301/GRACCOMPANYdata.dat	<input type="checkbox"/>
Company	/cf2/ac0301/GRACCOMPANYTdata.dat	<input type="checkbox"/>

Navigation icons: Previous, Submit, Skip, Cancel

Figure 7-2

8. Choose *Submit*.
9. Choose *Import* to import the configuration data.

The results appear at the bottom of the screen.

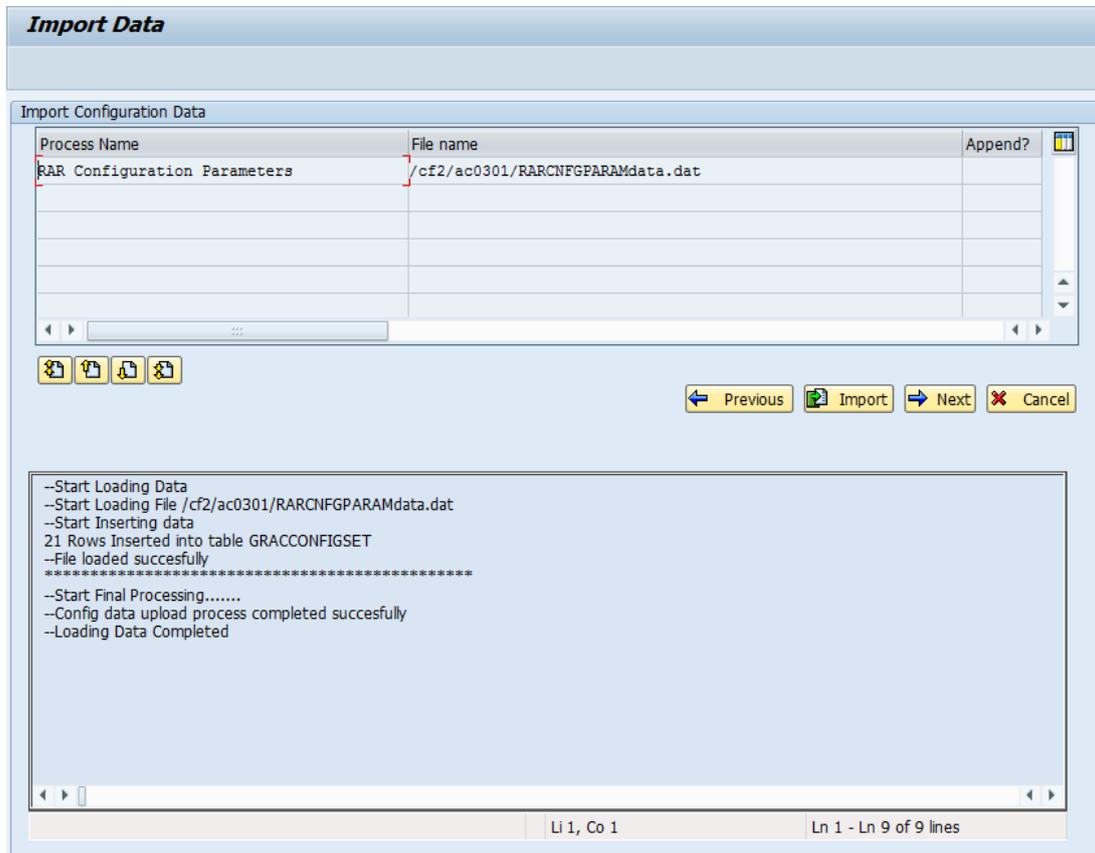


Figure 7-3

10. Choose *Next*.

The *Select Process Type* screen appears.

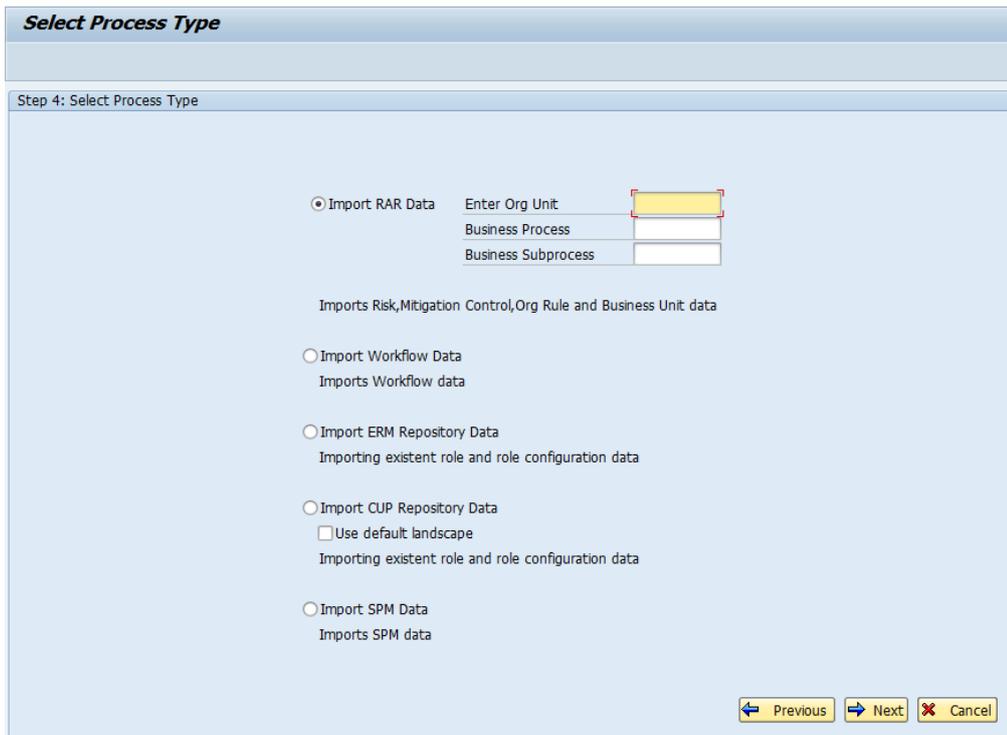


Figure 7-4

7.2 Completing Intra-Migration Tasks

You need to complete the following tasks before importing the RAR, Workflow, ERM, CUP, and SPM application data.

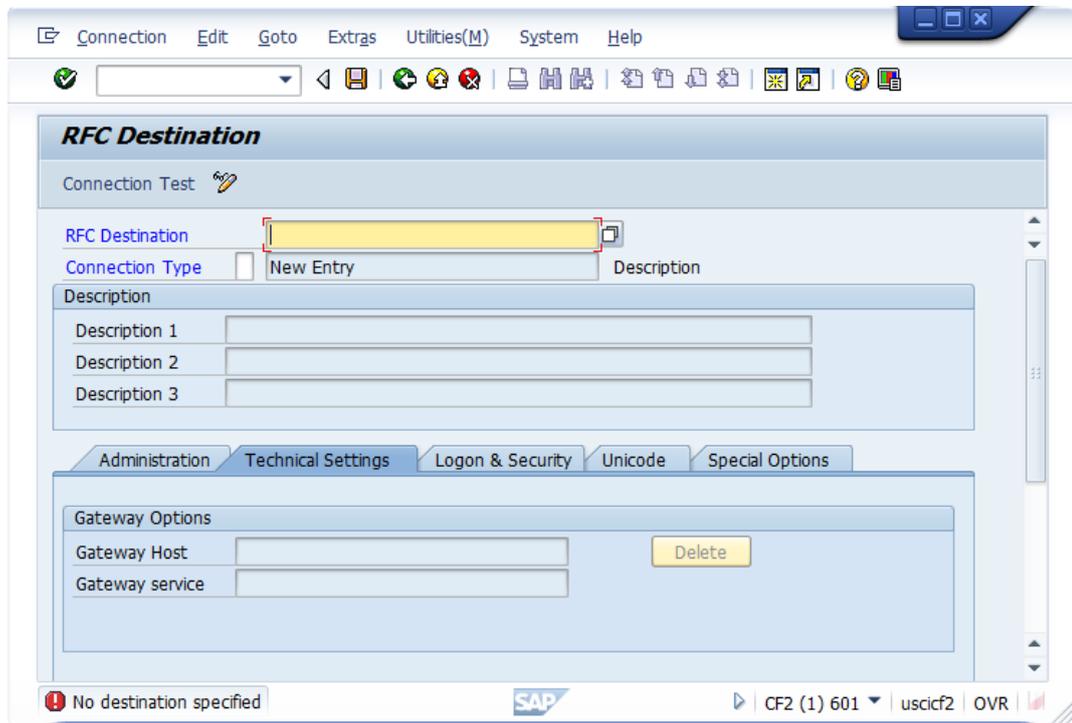
- Maintain connectors and connector groups
- Perform repository synchronization for all defined connectors
- Maintain configuration settings
- Import roles for defined connectors (CUP Roles only)
- Create prerequisites (CUP Roles only)

7.2.1 Maintaining Connectors and Connector Groups

The migration process does not support non-SAP connectors and non-SAP systems for RAR and CUP application data. Similarly, the migration process does not support non-SAP landscapes and enterprises for ERM data. You need to manually maintain these connectors and connector groups after importing the common configuration using IMG.

Procedure

1. Execute transaction *SPRO* and choose *SAP Reference IMG*. The *SAP Reference IMG* window appears.
2. Navigate to *Governance, Risk and Compliance > Common Component Settings > Integration Framework*, and choose *Create Connectors*. The *Configuration of RFC Connections* screen appears.
3. Select *Create*. The *RFC Destination* screen appears.



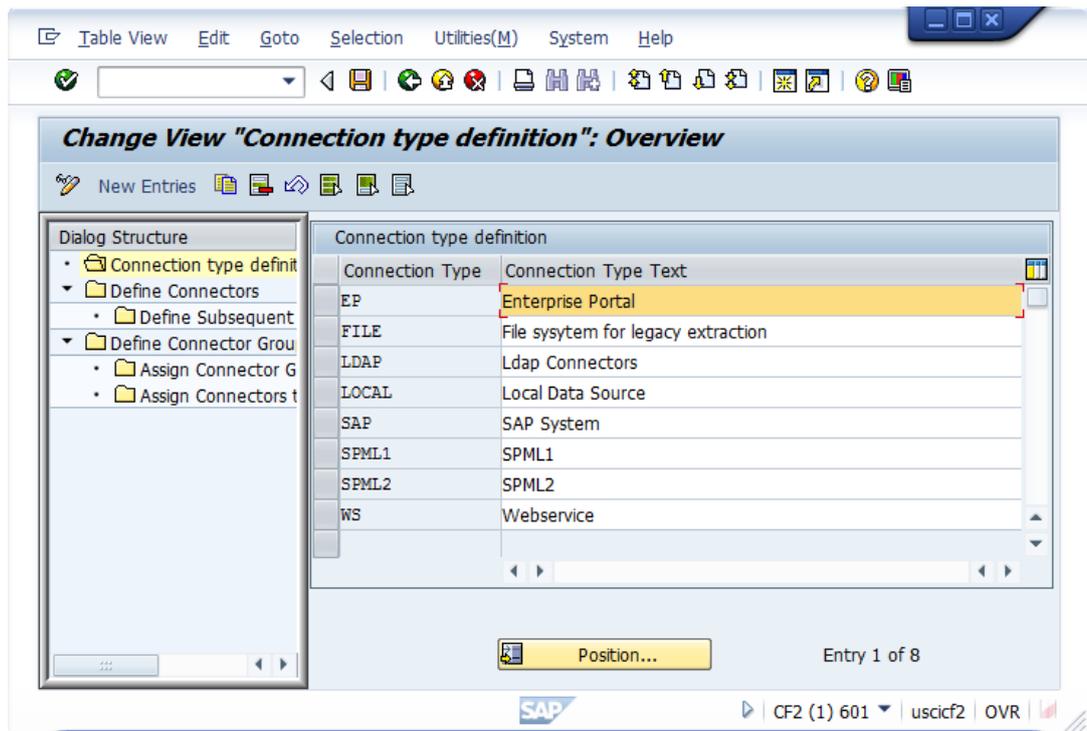
4. Specify the connector details, and select *Save*.

You can optionally test the connector and remotely log on to target system.

Note

The migration process does not support the passwords of migrated connectors. You need to manually maintain these passwords to use the migrated connectors.

In *Governance, Risk and Compliance > Common Component Settings > Integration Framework*, choose *Maintain Connectors and Connection Types*. The *Connection type definition* screen appears.



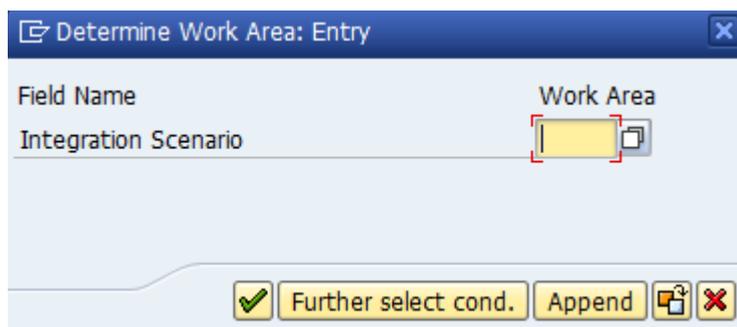
5. Choose *Define Connectors*, and define the connector.
6. Choose *Define Connector Groups*, and define the connector group.
7. In *Assign Connector Groups to Group Types*, assign the group type to the group, and assign the connector to the connector group in *Assign Connectors to Connector Group*.



Note

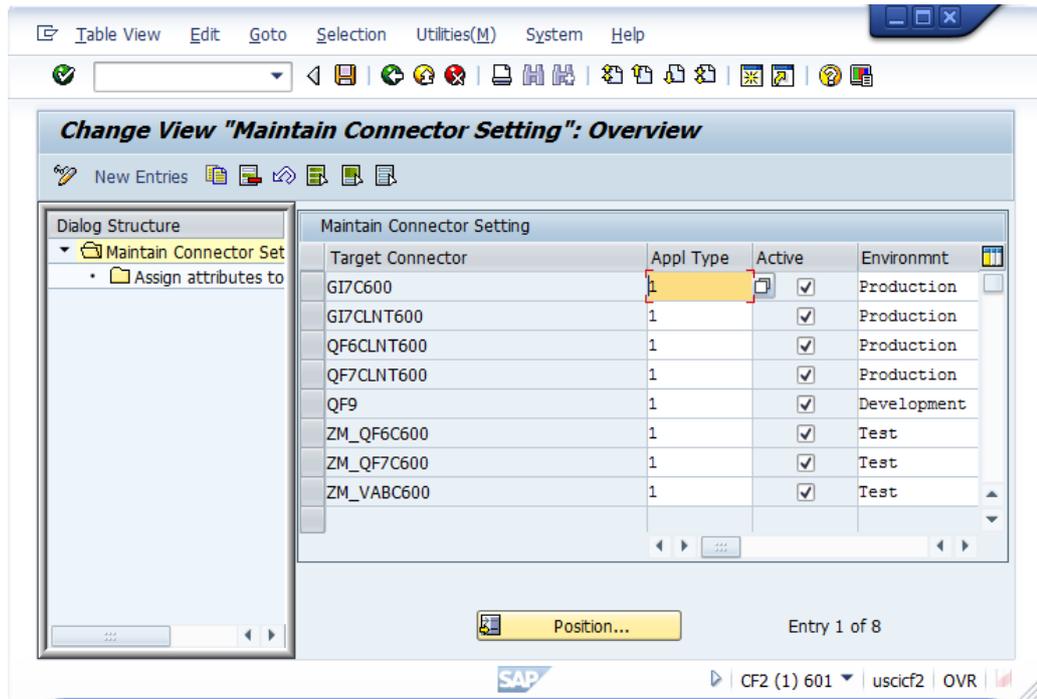
ERM Groups do not have any visible connection type. Only connectors are visible. You cannot assign a connector to more than one ERM Group/Landscape.

8. In *Governance, Risk and Compliance > Common Component Settings > Integration Framework*, choose *Maintain Connection Settings*. The *Determine Work Area* dialog appears.



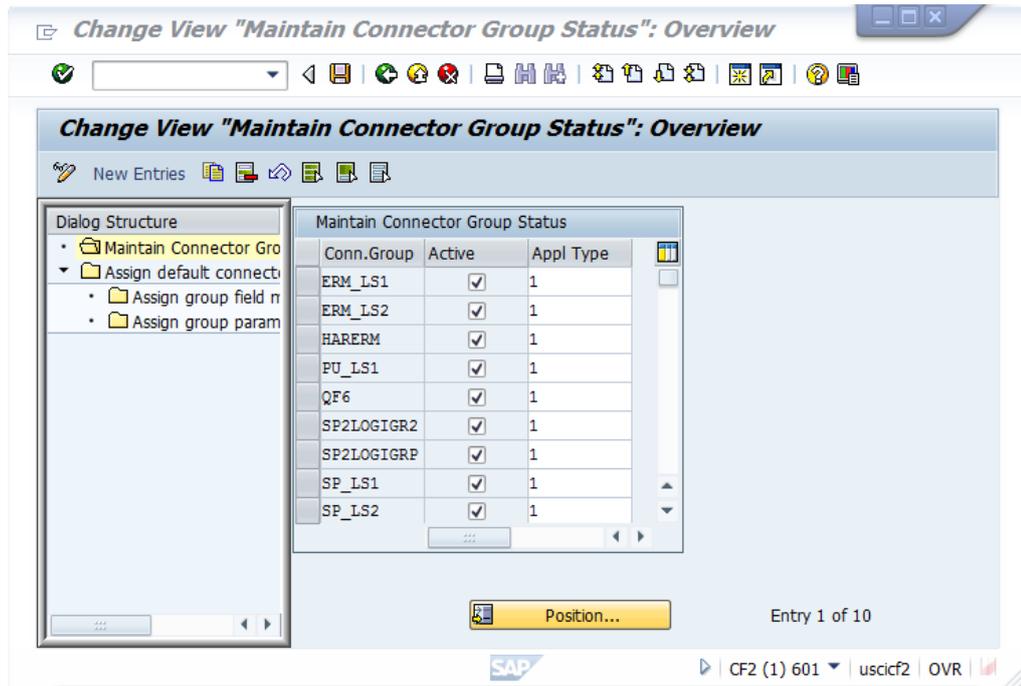
Associate connectors to the related integration scenarios.

- In *Governance, Risk and Compliance > Access Control > Maintain Connector Settings*. The *Maintain Connector Setting* screen appears.



Maintain the connector settings.

- In *Governance, Risk and Compliance > Access Control > Maintain Mapping for Actions and Connector Groups*. The *Maintain Connector Group Status* screen appears.



- Assign the application type to the connector group, and activate it. Assign actions for the defined connectors, and assign the default connector for each action (for each connector group).



Note

You need to maintain connector settings, assign actions to connectors, and define default connectors for each action for SAP connectors as well (using steps 9, 10, and 11 in this procedure).

7.2.2 Performing Repository Synchronization

After you have complete maintaining the connectors and connector groups, you need to perform repository synchronization.



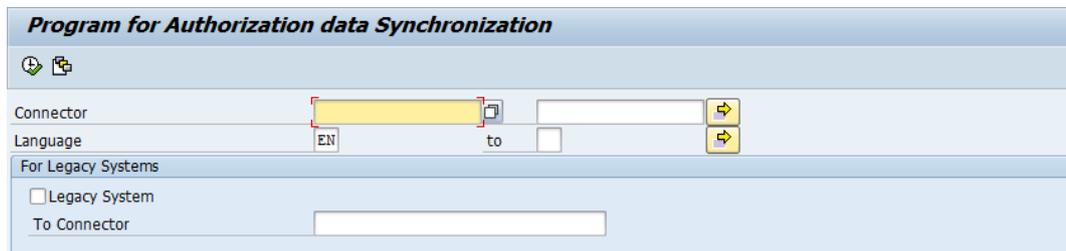
Note

SAP recommends running the repository synchronizations in the background (*Program > Execute in Background* or press F9).

7.2.2.1 Performing Authorization Synchronization

Procedure

- Execute transaction *SPRO* and choose *SAP Reference IMG*. The *SAP Reference IMG* window appears.
- Navigate to *Governance, Risk and Compliance > Access Control > Synchronization Jobs*, and choose *Authorization Synch*. The *Authorization Data Synchronization* screen appears.



- Type values in the *Connector* and *Language* fields, and run the authorization sync.

7.2.2.2 Performing Profile, Role, and User Synchronization

Procedure

1. Execute transaction *SPRO* and choose *SAP Reference IMG*. The *SAP Reference IMG* window appears.
2. Navigate to *Governance, Risk and Compliance > Access Control > Synchronization Jobs*, and choose *Repository Object Synch*. The *Repository Object Synchronization* screen appears.

Repository Object (Profile, Role & User) Synchronization

Select Sync Job

- Profile
- Role
- User

Connector to

Language to

Incremental Sync Mode
 Full Sync Mode

For Legacy Systems

Legacy System
To Connector

3. Select the objects (Profile, Role, and User) you want to synchronize.
4. Type values in the *Connector* and *Language* fields, and run the repository object sync.



Note

You can run Profile Sync, Role Sync, and User Sync jobs either in incremental or full sync mode.

7.2.3 Maintaining Configuration Settings

The migration process does not support all configuration settings. Check the configuration settings in AC 10.1 to verify that the imported configuration matches your business scenario.

7.2.4 Importing Roles for Defined Connectors (CUP Roles Only)

Since AC 5.3 CUP Roles do not maintain either parent-child or master-derived role relationships, you need to import CUP roles from the back-end systems to bring these relationships into AC 10.1.

Procedure

- Execute transaction *GRAC_ROLE_MASS_IMPRT* to import roles to AC 10.1 for all defined connectors.

7.2.5 Creating Prerequisites (CUP Roles Only)

You need to maintain the prerequisites in the IMG before importing the application data.



Note

This procedure is required for CUP roles only.

Procedure

1. Execute transaction *SPRO* and choose *SAP Reference IMG*. The *SAP Reference IMG* window appears.
2. Navigate to *Governance, Risk and Compliance > Access Control > Role Management*.
3. Choose *Define Prerequisite Types*.
4. Choose *Define Role Prerequisites* to define the prerequisites.
5. Verify that the names that appear match the Verification/Training System name in AC 5.3.

7.3 Importing RAR Data

You can continue the data import process to import the RAR data.

Procedure

1. On the *Select Process Type* screen, select *Import RAR Data*.
2. In the *Enter Org Unit* field, enter the organization unit. This is a mandatory field.

This is the Organization Unit you created in section 4.3, Creating the Organization Unit. When importing RAR data, AC 5.3 business units are migrated as AC 10.1 organizations.

The *Business Process*, and *Business Subprocess* fields, used with mitigation controls, are optional and can be left blank.

3. Choose *Next*.
4. In the *Import Location* field, enter the location of the exported data, and choose *Get Files*.
5. Choose the files to import by selecting the corresponding boxes to the left of the files.

Alternatively, you can choose the *Select All Files* button.



Choosing *Append Data* adds to existing data in the target location. If you do not choose *Append Data*, the data in the target location is overwritten.

6. Choose *Submit* after completing the selection.
7. Review your selections and choose *Import*.

The application displays the import logs in the bottom pane. After the import process completes, choose *Previous* to return to the *Select Process Type* screen; choose *Cancel* to close the application.



Note

The AC 5.3 Mitigation Control *Short Description* field gets populated in the AC 10.1 Mitigation Control *Name* field (which is limited to 40 characters). The complete AC 5.3 Mitigation Control *Short Description* and *Description* data gets populated in the AC 10.1 Mitigation Control *Description* field in the following format: Short Description – Description.

After migrating the RAR risks, you need to generate Rules for the risks to run the risk analysis.

7.4 Importing Workflow Data

You can continue the data import process to import the Workflow data.

Procedure

1. On the *Select Process Type* screen, select *Import Workflow Data*.
2. In the *Import Location* field, enter the location of the exported data, and choose *Get Files*.
3. Choose the files to import by selecting the corresponding boxes to the left of the files.

Alternatively, you can choose the *Select All Files* button.



Choosing *Append Data* adds to existing data in the target location. If you do not choose *Append Data*, the data in the target location is overwritten.

4. Choose *Submit* after completing the selection.
5. Review your selections and choose *Import*.

The application displays the import logs in the bottom pane. After the import process

completes, choose *Previous* to return to the *Select Process Type* screen; choose *Cancel* to close the application.

7.5 Importing ERM Repository Data

You can continue the data import process to import the ERM Repository data.

Procedure

1. On the *Select Process Type* screen, select *Import ERM Repository Data*.
2. In the *Import Location* field, enter the location of the exported data, and choose *Get Files*.
3. Choose the files to import by selecting the corresponding boxes to the left of the files.

Alternatively, you can choose the *Select All Files* button.



Choosing *Append Data* adds to existing data in the target location. If you do not choose *Append Data*, the data in the target location is overwritten.

4. Choose *Submit* after completing the selection.
5. Review your selections and choose *Import*.

The application displays the import logs in the bottom pane. After the import process completes, choose *Previous* to return to the *Select Process Type* screen; choose *Cancel* to close the application.

7.6 Importing CUP Repository Data

You can continue the data import process to import the CUP Repository data.



Note

If the AC 5.3 CUP Roles do not have a defined system (or have a system that is not associated with a landscape in AC 10.1), the system creates the roles under the default landscape

Procedure

1. On the *Select Process Type* screen, select *Import CUP Repository Data*.
2. Optionally, choose the *Use default landscape* checkbox.

CUP Roles in AC 5.3 do not have an associated landscape. Choosing the *Use default landscape* checkbox causes the SAP solutions for GRC 10.1 Data Import Application to group all systems associated with AC 5.3 CUP Roles into the default landscape, creating the corresponding role-to-landscape association in AC 10.1.

**Note**

Choose this option only if you have not already configured your landscape structure.

3. In the *Import Location* field, enter the location of the exported data, and choose *Get Files*.
4. Choose the files to import by selecting the corresponding boxes to the left of the files.

Alternatively, you can choose the *Select All Files* button.



Choosing *Append Data* adds to existing data in the target location. If you do not choose *Append Data*, the data in the target location is overwritten.

5. Choose *Submit* after completing the selection.
6. Review your selections and choose *Import*.

The application displays the import logs in the bottom pane. After the import process completes, choose *Previous* to return to the *Select Process Type* screen; choose *Cancel* to close the application.

7.7 Importing SPM Data

You can continue the data import process to import the SPM data.

Procedure

1. On the *Select Process Type* screen, select *Import SPM Data*.
2. In the *Import Location* field, enter the location of the exported data, and choose *Get Files*.
3. Choose the files to import by selecting the corresponding boxes to the left of the files.

Alternatively, you can choose the *Select All Files* button.



Choosing *Append Data* adds to existing data in the target location. If you do not choose *Append Data*, the data in the target location is overwritten.

4. Choose *Submit* after completing the selection.
5. Review your selections and choose *Import*.

The application displays the import logs in the bottom pane. After the import process completes, choose *Previous* to return to the *Select Process Type* screen; choose *Cancel* to close the application.

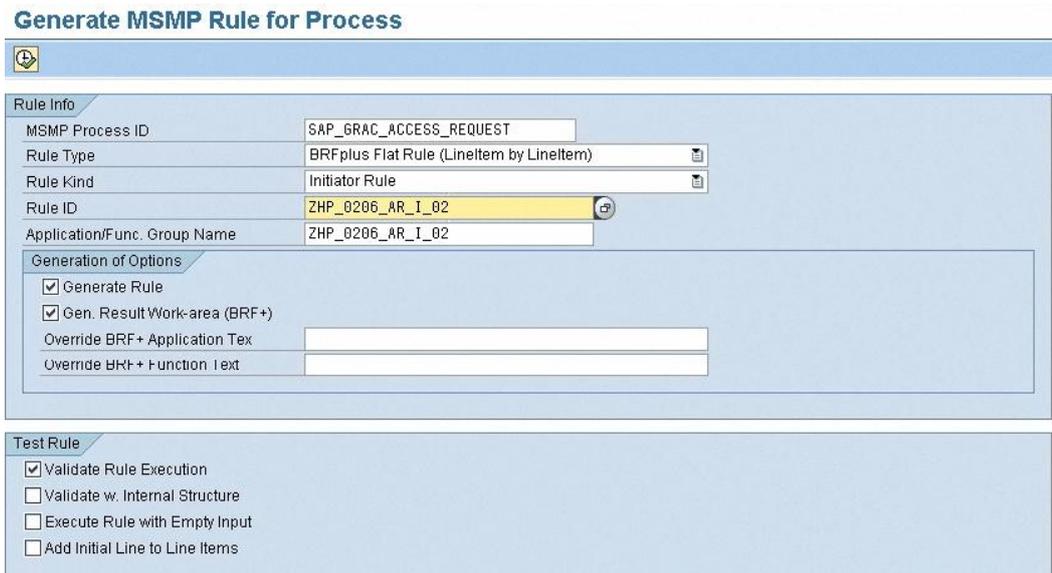
7.8 Importing Workflow Rule Data

You need to import the workflow rule data exported earlier from AC 5.3.

Procedure

To import the initiator rules:

1. Execute transaction *GRFNMW_DEV_RULES*. The *Generate MSMP Rule for Process* screen appears.



Generate MSMP Rule for Process

Rule Info

MSMP Process ID	SAP_GRAC_ACCESS_REQUEST
Rule Type	BRFplus Flat Rule (LineItem by LineItem)
Rule Kind	Initiator Rule
Rule ID	ZHP_0206_AR_I_02
Application/Func. Group Name	ZHP_0206_AR_I_02

Generation of Options

Generate Rule

Gen. Result Work-area (BRF+)

Override BRF+ Application Text:

Override BRF+ Function Text:

Test Rule

Validate Rule Execution

Validate w. Internal Structure

Execute Rule with Empty Input

Add Initial Line to Line Items

2. Enter the following data in the corresponding fields:

In the *MSMP Process ID* field, enter the corresponding process ID, from among the following: *SAP_GRAC_ACCESS_REQUEST*, *SAP_GRAC_SOD_RISK_REVIEW*, or *SAP_GRAC_USER_ACCESS_REVIEW*.

In the *Rule Type* field, enter *BRFplus Flat Rule (LineItem by LineItem)*.

In the *Rule Kind* field, choose *Initiator Rule*.

Type values in the *Rule ID* and *Application/Func. Group Name* fields. Start the values using the letter Z, for example, *ZHP_0206_AR_I_02*.

3. Choose *Execute*. The *Display logs* screen appears.

- Execute transaction `GRAC_WF_MIG`. The *Migrate Initiators and CAD* screen appears.

Migrate Workflow Initiator and CAD rules	
Initiator/CAD File Location	d:\acmigration
MSMP Process ID	SAP_GRAC_ACCESS_REQUEST
Application/Func. Group Name	ZHP_0206_AR_I_02
<input checked="" type="radio"/> Initiators Rule <input type="radio"/> Agent Rule	
Initiators Rule ID	ZHP_0206_AR_I_02

- Enter the following data in the corresponding fields:

Select the *Initiators Rule* radio button.

In the *Initiator/CAD File Location* field, enter the data location.

In the *MSMP Process ID* field, enter the corresponding process ID, from among the following: `SAP_GRAC_ACCESS_REQUEST`, `SAP_GRAC_SOD_RISK_REVIEW`, or `SAP_GRAC_USER_ACCESS_REVIEW`.

In the *Application/Func. Group Name* field, enter the value you specified in Step 2.

In the *Initiators Rules ID* field, enter the value you specified in Step 2.

- Choose *Execute*. The *Initiators Rules Migration* screen appears.
- Choose *Upload*. The *Display logs* screen appears.

To import CAD/agent rules:

- Execute transaction `GRFNMW_DEV_RULES`. The *Generate MSMP Rule for Process* screen appears.
- Enter the following data in the corresponding fields:

In the *MSMP Process ID* field, enter the corresponding process ID, from among the following: `SAP_GRAC_ACCESS_REQUEST`, `SAP_GRAC_SOD_RISK_REVIEW`, or `SAP_GRAC_USER_ACCESS_REVIEW`.

In the *Rule Type* field, enter *BRFplus Flat Rule (LineItem by LineItem)*.

In the *Rule Kind* field, choose *Agents Rule*.

Type values in the *Rule ID* and *Application/Func. Group Name* fields. You will use the *Rule ID* in the *Approvers Rules ID* field in Step 9.

- Choose *Execute*. The *Display logs* screen appears.
- Execute transaction `GRFNMW_DEV_RULES`. The *Generate MSMP Rule for Process* screen appears.

5. Enter the following data in the corresponding fields:

In the *MSMP Process ID* field, enter the corresponding process ID, from among the following: *SAP_GRAC_ACCESS_REQUEST*, *SAP_GRAC_SOD_RISK_REVIEW*, or *SAP_GRAC_USER_ACCESS_REVIEW*.

In the *Rule Type* field, enter *BRFplus Flat Rule (LineItem by LineItem)*.

In the *Rule Kind* field, choose *Agents Rule*.

Type values in the *Rule ID* and *Application/Func. Group Name* fields. In the *Application/Func. Group Name* field, use the same value that you specified in Step 3. You will use the *Rule ID* in the *Alternate Approvers Rules ID* field in Step 9.

6. Choose *Execute*. The *Display logs* screen appears.
7. Execute transaction *GRAC_WF_MIG*. The *Migrate Initiator and CAD* screen appears.
8. Enter the following data in the corresponding fields:

Select the *Agent Rule* radio button.

In the *Initiator/CAD File Location* field, enter the data location.

In the *MSMP Process ID* field, enter the corresponding process ID, from among the following: *SAP_GRAC_ACCESS_REQUEST*, *SAP_GRAC_SOD_RISK_REVIEW*, or *SAP_GRAC_USER_ACCESS_REVIEW*.

In the *Application/Func. Group Name* field, enter the value you specified in Step 3.

In the *Approvers Rules ID* field, enter the value you specified in Step 3.

In the *Alternate Approvers Rule ID* field, enter the value you specified in Step 6.

9. Choose *Execute*. The *Agents Rules Migration* screen appears.

Agent rules available for migration are automatically selected. You can modify the selection, as required.

10. Choose *Upload*. The *Display logs* screen appears.
11. Execute transaction *BRF+* to verify the uploaded data.

You need to activate the initiator and agent rules after uploading.



Note

For initiators, conditions containing an OR operator between different attributes or an AND operator between the same attribute, are not migrated.

Similarly, in the case of CAD, conditions of type *Webservice* are not migrated.

Also, the entire initiator/CAD condition is not migrated in cases when the data is invalid, an attribute is not mapped, or a custom field is not found.

8. Completing Post-Import Tasks

You need to complete certain tasks after importing the application data. Specifically, you need complete the following tasks:

- Activate GRC_MSMP_CONFIGURATION BC set
- Generate the rules
- Create function modules
- Maintain workflow stage settings
- Complete methodology process assignments

8.1 Activating the GRC_MSMP_CONFIGURATION BC Set

After you have completed the data migration process, you need to activate the GRC_MSMP_CONFIGURATION BC set.

8.2 Generating the Rules (AC 4.0 and AC 5.3)

After you have migrated the RAR risks, you need to generate the rules before running a risk analysis.

Procedure

1. Using AC 10.1, navigate to *Rule Setup > Access Risks*.
2. Select the risk for which you need to generate rules, and choose *Generate Rules*.

You can generate the rules either in the foreground or the background.

Alternatively, you can generate multiple rules using the IMG configuration. In this case, use transaction *SPRO* > navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Access Risk Analysis > Generate SoD Rules*. Select the range of SoD risks that you want to generate rules for, and choose *Execute*.

8.3 Creating Function Modules (AC 5.3)

Attributes/conditions for AC 5.3 CAD/Initiators are not transferred during the migration process. This means that you need to manually create the Function Module to specify the attributes/conditions for Workflow CAD/Initiators.

The procedure in this section describes how to create a Function Module for an Initiator Rule.



Note

Depending on your requirements, you can create a single Function Module for all initiator conditions (of AC 5.3 initiators and their respective rule result values).

The Workflow Initiator imported from AC 5.3 requires you to create a Function Module in AC 10.1 for each corresponding initiator. In AC 10.1, Initiator conditions and their respective rule result values are declared in Initiator Rules, which are Function Module-based rules.

After migration, the AC 5.3 Initiator maps to two configuration areas: Rule ID and Rule Result Value. The AC 5.3 initiator rule conditions (attributes and their values) are not, however, mapped to AC 10.1.

You need to manually declare these conditions in the Function Module.

Procedure

1. Execute transaction SE37.
2. Create function module `Z_Initiator_SP_INI1` by copying it from `GRAC_AR_INITIATOR`.



Note

Use the custom Function Group.

Create the function module with the same conditions as in AC 5.3 and with the rule result value for the name of the corresponding initiator.



Note

In AC 10.1, the Req Type has the numeric value that you need for the function module. For example, `SP_REQ_CREATE_USER_DESC` is represented by 16. You can determine this using transaction `SPRO > SAP Reference IMG > Governance, Risk, and Compliance > Access Control > User Provisioning > Define Request Type`.

3. After creating `Z_Initiator_SP_INI1`, activate it and maintain the workflow using MSMP.
4. After the initiator is activated, maintain the initiator using the global settings (using the process id for the workflow).
5. Complete the remaining required steps for configuring a workflow.

8.4 Maintaining Workflow Stage Settings (AC 5.3)

In certain cases, you need to map CUP Stage Escalation settings to corresponding AC 10.1 Workflow Stage settings.

In AC 5.3, the CUP Stage Escalation configuration consists of the following four entities:

1. No Escalation
2. Forward to next stage
3. Forward to Administrator
4. Forward to Alternate Approver.

In contrast, AC 10.1 Workflow Stage settings consist of the following three entities:

- No Escalation
- Skip to Next Stage
- Escalate to Specified Agent.

The following table shows the mapping between the AC 5.3 and AC 10.1 settings, and whether manual steps are required to complete the migration:

AC 5.3 Escalation Configuration	AC 10.1 Escalation Type	Manual Step Required
No Escalation	No Escalation	No
Forward to next stage	Skip to Next Stage	No
Forward to Administrator	Escalate to Specified Agent	Yes
Forward to Alternate Approver	Escalate to Specified Agent	Yes

Procedure

To migrate AC 5.3 Forward to Administrator settings:

1. Create an Agent (for example, ADMIN) with *Approval* as the *Agent Purpose* setting and *Directly Mapped Users* as the *Agent Type* setting.
2. Create an Approver Group ID and add the AC 5.3 Administrator ID to the *Approver User ID*.
3. As part of the *Stage Definition*, specify the Agent ID (for example, ADMIN) in the *Escalation Agent* field.

To migrate AC 5.3 Forward to Alternate Approver settings

1. Create an Agent (for example, ALTRAPPVR) with *Approval* as the *Agent Purpose* setting and GRAC_MSMP_AR_ROLE_ALT_APPR as the *Agent Type* setting.
2. As part of the *Stage Definition*, specify the Agent ID (for example, ALTRAPPVR) in the *Escalation Agent* field.

8.5 Completing Methodology Process Assignments (AC 5.3)

Imported CUP Roles imported from back-end systems and AC 5.3 do not get an assigned methodology process. As a result, these roles are not editable.

You therefore need to assign the methodology process for these roles, as described in this section.



Note

The procedure described in this section applies the default methodology.

Procedure

1. In AC 10.1, choose *Access Management > Role Mass Maintenance > Role Update*.
2. Select all migrated CUP roles, and choose *Next*.
3. Choose *All Attributes* in the *Attributes* field, choose *Update* in the *Action* field, and choose *Next*.
4. Choose *Reapply role methodology*, and choose *Next*.
5. Schedule the job to run in the background, and choose *Submit*.

9. Validating the Data

You can manually validate the AC 4.0 or AC 5.3 to AC 10.1 data migration by examining the corresponding areas in the application. This section describes how to validate the following application data.

- RAR data
- ERM data
- Workflow data
- CUP data

9.1 Validating RAR Data

This section describes how to manually validate the RAR application data migration.

Procedure

To validate the functions:

- In AC 4.0 or AC 5.3, choose *Rule Architect > Functions* to display the functions.
- In AC 10.1, choose *Setup > Access Rule Maintenance > Functions* to display the functions.

To validate function actions:

- In AC 4.0, select the function and choose *Display/Change*.
- In AC 5.3, select the function and choose *Change*.
- In AC 10.1, select the function and choose *Open*.

To validate function permissions:

- In AC 4.0, select the function, choose *Display/Change*, and choose the *Business View* tab.
- In AC 5.3, select the function, choose *Change*, and choose the *Permissions* tab.
- In AC 10.1, select the function, choose *Open*, and choose the *Permission* tab.

To validate the risks:

- In AC 4.0 or AC 5.3, choose *Rule Architect > Risks* to display the risks.
- In AC 10.1, choose *Setup > Access Rule Maintenance > Access Risks* to display the risks.

To validate specific risks:

- In AC 4.0, select the risk and choose *Display/Change*.
- In AC 5.3, select the risk and choose *Change*.
- In AC 10.1, select the risk and choose *Open*.

To validate mitigating controls:

- In AC 4.0 or AC 5.3, choose *Mitigation > Mitigating Controls* to display the mitigating controls.
- In AC 10.1, choose *Setup > Mitigating Controls > Mitigating Controls* or *Master Data > Mitigating Controls > Mitigating Controls* to display the corresponding mitigating controls.

To validate specific mitigating controls:

- In AC 5.3, select the mitigating control and choose *Change*.
- In AC 10.1, choose the link for the mitigating control.

To validate mitigated users:

- In AC 4.0, choose *Mitigation > Mitigated User* to display the mitigated users.
- In AC 10.1, choose *Access Management > Mitigated Access > Mitigated Users* to display the corresponding mitigated users.

To validate connectors:

- In AC 5.3, choose *Configuration > Connectors* to display the connectors.
- For AC 10.1, execute transaction SM59 or navigate to *SPRO > SAP Reference IMG > Governance, Risk and Compliance > Common Component Settings > Integration Framework > Create Connectors* to display the corresponding connectors.

9.2 Validating ERM Data

This section describes how to manually validate the ERM application data migration.



Note

The migration process only populates ERM Role Risk Analysis data in AC 10.1 if the rule has been generated for the particular role risk in AC 10.1.

Procedure

To validate the roles:

- In AC 5.3, choose *Role Management > Role* to display the roles.
- In AC 10.1, choose *Access Management > Role Management > Role Maintenance* to display the corresponding roles.

To validate specific roles:

- In AC 5.3, select the role and choose *Change*.
- In AC 10.1, select the role and choose *Open*.

9.3 Validating Workflow Data

This section describes how to manually validate the Workflow data migration.

Procedure

To validate workflow initiators:

- In AC 5.3, choose *CUP > Configuration > Workflow > Initiators* to display the workflow initiators.
- For AC 10.1, use transaction *SPRO > navigate to SAP Reference IMG > Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain MSMP Workflows*.

In the browser window that opens, choose *Next*. Then select *Maintain Rules* to display the corresponding workflow initiators.



Note

After migration, the Rule ID is populated with *Z_Initiator_Name-of-5.3-initiator* and the Rule Result Value is populated with *Name-of-5.3-initiator*. For example, in the case of *SP_INI1*, the Rule ID becomes *Z_Initiator_SP_INI1* and the Rule Result Value becomes *SP_INI1*.

To validate workflow paths:

- In AC 5.3, choose *CUP > Configuration > Workflow > Paths* to display the workflow paths.
- For AC 10.1, use transaction *SPRO > navigate to SAP Reference IMG > Governance, Risk and Compliance > Access Control > Workflow for Access Control > Maintain MSMP Workflows*.

In the browser window that opens, choose *Next* and choose *Maintain Paths* to display the corresponding workflow paths.

9.4 Validating CUP Data

This section describes how to manually validate the CUP application data migration.

Procedure

To validate the roles:

- In AC 5.3, choose *Configuration > Roles* to display the roles.
- In AC 10.1, choose *Access Management > Role Management > Role Maintenance* to display the corresponding roles.

To validate specific roles:

- In AC 5.3, select the role and choose *Change*.
- In AC 10.1, select the role and choose *Open*.

10. Supported AC 4.0 Objects

This section lists the AC 4.0 objects supported in the data migration process.

10.1 Common Configuration

This section outlines the common configuration, which includes all applicable configuration information from AC applications.

Category	Object
Common Configuration	Owners
	Business Process

10.2 Compliance Calibrator (RAR)

Category	Object
SOD Rules	Rule Set
	Function
	Function Action
	Function Permission
	Risk
	Risk Rule Set
	Risk Description
	Risk Objective
Business Units	Business Unit
	Business Unit Owners
Mitigation Controls	Mitigation Control
	Mitigation Control Description
	Mitigation Control Risk ID and Rule ID
	Mitigation Control Monitor
	Mitigation Control Report
	Mitigation Control Users
	Mitigation Control Roles
	Mitigation Control Profiles
Mitigation Control HR Objects	
Critical Roles and Profiles	Critical Roles
	Critical Profiles
Organization Rules	Organization Rule Header
	Organization Rule
Supplemental Rules	Supplement Rule Header
	Supplement Rule

10.3 Fire Fighter (SPM)

Category	Object
SPM	Fire Fighter User Based
	Fire Fighter User Based Description
	Fire Fighter Object
	Fire Fighter Object Description
	Fire Fighter Owner
	Fire Fighter Owner Description
	Fire Fighter Controller
	Fire Fighter Controller Description

11. Supported AC 5.3 Objects

This section lists the AC 5.3 objects supported in the data migration process.

11.1 Configuration and Master Data

This section outlines the AC 5.3 configuration and master data supported in the data migration process.

11.1.1 Configuration Data

This section outlines the configuration data supported in the data migration process.

Object	Component
Common Configuration	SAP Connectors
	Connector Groups
	Connectors for Connector Groups
	Users Mapping
	Owners
	RAR Configuration Parameters
	ERM Configuration Parameters
	CUP Configuration Parameters
	Request Type
	Request Type and Action Association
	Business Process
	Business Subprocess
	Critical Level
	Functional Area
	Company
	Priority
Employee Type	

11.1.2 Master Data

This section outlines the master data supported in the data migration process.

11.1.2.1 Compliance Calibrator (RAR)

Object	Component
SOD Rules	Rule Set
	Function
	Function Action
	Function Permission
	Risk
	Risk Rule Set
	Risk Description
	Risk Objective
	Risk Owners
Business Units	Business Unit
	Business Unit Owners
Mitigation Controls	Mitigation Control
	Mitigation Control Description
	Mitigation Control Risk ID and Rule ID
	Mitigation Control Monitor
	Mitigation Control Report
	Mitigation Control Users
	Mitigation Control Users and Org Rules
	Mitigation Control Roles
	Mitigation Control Profiles
	Mitigation Control HR Objects
Critical Roles and Profiles	Critical Roles
	Critical Profiles
Organization Rules	Organization Rule Header
	Organization Rule
Supplemental Rules	Supplement Rule Header
	Supplement Rule

11.1.2.2 Fire Fighter (SPM)

Object	Component
SPM	Fire Fighter User Based and Role Based
	Fire Fighter User Based and Role Based Description
	Fire Fighter Object
	Fire Fighter Object Description
	Fire Fighter Owner
	Fire Fighter Owner Description
	Fire Fighter Controller
	Fire Fighter Controller Description
	Fire Fighter Reason Code
	Fire Fighter Reason Code Description

11.1.2.3 Workflow (CUP)

Object	Component
Workflow	Workflow Type
	Workflow Initiator
	Workflow Stage
	Workflow Stage Actions
	Workflow Stage Role
	Workflow Stage Escalations
	Workflow Path
	Workflow Path Stages
	Workflow Approvers
	Workflow CAD

11.1.2.4 Role Repository (ERM)

Object	Component
ERM Roles Repository	Project Release
	Role Status
	Org Value Mapping Main
	Org Value Mapping Detail
	Methodology
	Methodology Actions
	Methodology Steps
	Methodology Steps Description
	Methodology Process Step Assignment
	Methodology and Conditional Group
	Naming Convention
	Naming Convention Position
	ERM Role
	ERM Role Archive
	Role Text
	Role Detail Description
	Role Approver
	Role Function Area
	Role Function
	Role Action
	Role Permission
	Role Permission Authorization
	Role Global Org Fields
	Role Field Value
	Role Org Level Information
	Role Step
	Composite Role
	Derived Role
Role Test Results	
Role Test Results Description	
Role Custom Fields	

11.1.2.5 Role Repository (CUP)

Object	Component
CUP Roles Repository	Role Company
	Role Custom Fields
	Role Default
	Role Reaffirm
	CUP Role
	CUP Role Text
	Role Approvers
	Role Mapping
	Role Verification Systems
	CUP Role Function Area
	CUP Role Systems

11.2 Transactional Data

This section outlines the AC 5.3 transactional data supported in the data migration process.

Object	Component
CUP Transactional Data	CUP Requests
	CUP Requests Comment

12. Unsupported Objects and Components

The following objects and components are not supported as part of the AC 4.0 and AC 5.3 to SAP solutions for GRC 10.1 data migration process:

- Non-SAP type connectors
- Condition groups and approval criteria
- HR triggers
- User defaults
- Password Self Service
- Number ranges
- Service Level Agreement and Provisioning
- Attachments
- Detour paths
- Web Service-type CAD, and CADs without conditional approvers



You can continue to access historic transactional data using AC 5.3.