



PUBLIC

Document Version: 1H 2025 – 2025-04-04

# Implementing Role-Based Permissions

# Content

<b>1</b>	<b>Introduction to Implementing RBP.</b>	<b>5</b>
<b>2</b>	<b>Implementation Sequence.</b>	<b>6</b>
<b>3</b>	<b>Initial Setup Tasks.</b>	<b>8</b>
3.1	Creating a Super Admin User in Provisioning.	8
3.2	Granting Administrators Access to Role-Based Permissions.	10
3.3	Role-Based Permissions Administrator Access.	11
3.4	Enabling Email Notifications for Large-Size Permission Group or Permission Role Changes.	12
3.5	Enabling Double-Confirmation Messages for Large-Size Permission Changes.	13
3.6	Revoking Administrators Access to RBP.	14
3.7	Granting Yourself and Project Team Members All Permissions.	15
3.8	Refreshing RBP after Changes in Provisioning Configuration.	15
<b>4</b>	<b>Steps for Designing the RBP Configuration.</b>	<b>17</b>
4.1	Checking Available Permissions in a New Customer Instance.	18
4.2	Review Permissions in Existing Customer Instance.	18
4.3	Basic Roles.	18
4.4	Relationships Between Managers and Employees.	20
	Delegate Relationship Assignments.	20
	Hierarchy Depth and User Permissions.	22
4.5	Copying Roles and Groups between Test and Production Systems.	24
4.6	Conducting Tests.	24
<b>5</b>	<b>Role-Based Permissions.</b>	<b>25</b>
5.1	Role-Based Permissions Experience for Administrators.	26
5.2	Permission Groups.	26
	Creating Static Permission Groups.	27
	Adding Individual Members to Static Groups.	29
	Adding Multiple Members to Static Groups.	29
	Removing Members from Static Groups.	30
	Removing Multiple Members from Static Groups.	31
	Creating Dynamic Permission Groups.	32
	Managing Permission Groups.	34
5.3	Creating a Permission Role.	35
5.4	Assigning a Permission Role.	36
5.5	Updating a Permission Role.	38
5.6	Updating a Role Assignment.	39

5.7	Deleting a Permission Role. . . . .	40
5.8	Deleting a Role Assignment. . . . .	41
5.9	Bulk Activating and Deactivating Role Assignments. . . . .	41
5.10	Searching, Sorting, and Filtering Role Assignments. . . . .	42
5.11	Comparing Two Change History Records of a Permission Role. . . . .	43
5.12	Comparing Two Change History Records of A Role Assignment. . . . .	45
5.13	RBP Troubleshooting. . . . .	46
	Searching User Roles and Permissions. . . . .	46
	Comparing Roles. . . . .	47
<b>6</b>	<b>Recommendations and Leading Practices. . . . .</b>	<b>49</b>
6.1	General Leading Practices for RBP. . . . .	49
6.2	Separating RBP Administration Duties. . . . .	51
<b>7</b>	<b>Preparing the Instance. . . . .</b>	<b>53</b>
7.1	Ensuring that Test Instance and Production Instance are In Sync. . . . .	53
7.2	Configuring Fields for Setting up Permission Groups. . . . .	53
	Standard Fields Available to Use as Filters in Permission Groups. . . . .	54
	How Do You Specify Which Fields to Use?. . . . .	55
<b>8</b>	<b>RBP Reports. . . . .</b>	<b>56</b>
8.1	RBP Table Reports. . . . .	56
8.2	Dynamic Group Definition Reports. . . . .	56
8.3	Reporting on Dynamic Group Definition. . . . .	57
<b>9</b>	<b>Transport Role-Based Permissions Configurations to the Production Instance. . . . .</b>	<b>60</b>
9.1	Important Tips for Copying Groups. . . . .	60
9.2	Important Tips for Copying Roles. . . . .	61
<b>10</b>	<b>Using the Check Tool to Solve Issues. . . . .</b>	<b>62</b>
10.1	Benefits of the Check Tool. . . . .	64
10.2	Running Checks. . . . .	64
10.3	Check Types. . . . .	65
10.4	Check Results. . . . .	66
10.5	Creating Technical Support Tickets from the Check Tool. . . . .	67
10.6	Using the Quick Fix Feature. . . . .	68
10.7	Exports. . . . .	69
	Exporting Configuration Information. . . . .	69
	Exporting Check Results. . . . .	70
	Exporting a List of All Checks. . . . .	70
<b>11</b>	<b>Testing Your RBP Configuration. . . . .</b>	<b>72</b>
11.1	Does the Everyone Group Exist?. . . . .	72
11.2	Do Roles Exist Without Groups or Users?. . . . .	72

11.3	Do Roles Exist Without Target Population? . . . . .	73
11.4	Do Group Names Exceed 1000 Characters? . . . . .	73
11.5	Do Target Group Names Exceed 1000 Characters? . . . . .	74
11.6	Does a User Have the Same Permission More Than 30 Times? . . . . .	75
11.7	Does a Role Have More Than 200 Rules? . . . . .	76
11.8	Do All Permission Roles have Consistent Authorizations for Working with Business Rules? . . . . .	77
<b>12</b>	<b>Troubleshooting. . . . .</b>	<b>80</b>
12.1	How Do Permissions Update When User Information Changes? . . . . .	80
12.2	Cross Domain Table Reporting Between the RBP and Employee Central Domains. . . . .	82
12.3	Searching Roles Granted to a User. . . . .	83

# 1 Introduction to Implementing RBP

This content is designed for Professional Services consultants to help them implement Role-Based Permissions (RBP) for customers. It outlines the steps and offers recommendations and best practices.

The following sections outline the individual tasks that comprise the process. If you encounter any issues with permissions, you can find troubleshooting information at the end.

## Note

This implementation content covers all the general aspects of setting up RBP. The implementation handbooks for the individual modules contain additional, module-specific information.

## Related Information

[Change History \[page 87\]](#)

## 2 Implementation Sequence

This table provides an overview of the main steps in their sequential order. We recommend following this sequence.

What you need to do...	Find more information in...
Create a super administrator before you enable RBP.	<a href="#">Creating a Super Admin in Provisioning [page 8]</a>
<div><div> ⓘ Note</div><div>After you have enabled RBP, only super administrators can log in.</div></div>	
Identify those who need permission to manage RBP and grant them RBP administrator access.	<a href="#">Granting Administrators Permissions to RBP [page 10]</a>
<div><div> ⓘ Note</div><div>Only a super administrator can grant RBP administrator access.</div></div>	
Make sure you and your project team members have access to all functions by granting everyone all necessary permissions.	<a href="#">Granting Yourself and Project Team Members All Privileges [page 15]</a>
Design the RBP configuration: <ul style="list-style-type: none"><li>• Identify the modules and functions the customers actually use.</li><li>• Follow leading practices to ensure a smooth transition.</li><li>• Clarify customer requirements. Document the groups, roles, and role assignments in a workbook for easy reference.</li></ul>	<a href="#">Design the RBP Configuration [page 17]</a>
Prepare the test instance: <ul style="list-style-type: none"><li>• Make sure the data on both the test and production instances are in sync.</li><li>• Configure the fields needed for selecting group members.</li></ul>	<a href="#">Ensuring that Test Instance and Production Instance are in Sync [page 53]</a> <a href="#">Configuring Fields for Setting up Permission Groups [page 53]</a>
Create groups in the test instance.	<a href="#">Permission Groups [page 26]</a>
Create roles and assign them to groups in the test instance.	<a href="#">Creating a Permission Role [page 35]</a> <a href="#">Assigning a Permission Role [page 36]</a>
Conduct tests to verify that groups and roles are set up correctly.	<a href="#">Conducting Tests [page 24]</a>

What you need to do...	Find more information in...
<p>Enable RBP reporting to ensure it's ready for customers. Reporting assists in analyzing issues identified during tests.</p> <ul style="list-style-type: none"> <li>• Import standard spreadsheet reports into customer instances.</li> <li>• Enable and set up RBP Table and Story reports.</li> </ul>	<a href="#">RBP Table Reports [page 56]</a>
<p>If you find problems in the tests, analyze the RBP configurations using Check Tool, <i>Role-Based Permissions Troubleshooting Tool</i>, and RBP Table reports.</p>	<a href="#">Using the Check Tool to Solve Issues [page 62]</a> <a href="#">Troubleshooting and FAQ [page 80]</a> <a href="#">RBP Troubleshooting [page 46]</a>
<p>After successful testing, copy the RBP configuration to the production instance.</p>	<a href="#">Transport Role-Based Permissions Configurations to the Production Instance [page 60]</a>

## Related Information

[RBP Troubleshooting \[page 46\]](#)

## 3 Initial Setup Tasks

You can follow the tasks in this guide section to initially set up Role-Based Permissions.

### 3.1 Creating a Super Admin User in Provisioning

Create a super admin user in the Provisioning application, for a specific customer instance, so that you can access the system and grant necessary permissions to other users.

#### Prerequisites

You have Provisioning access to the instance.

##### → Remember




As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

#### Procedure

1. Log into Provisioning and select the company instance you wish to access.
2. Go to ► [Edit Company Settings](#) ► [Company Settings](#) ►.
3. Search or scroll down the page to find the section with "super admin" settings.
4. Provide **all** of the following information.

Setting	Description
Admin Username	Determines both Username and User ID of the super admin user.
Admin Password	Password with which super admin can access your system.
Admin First Name	First name of super admin as it appears in the system.
Admin Last Name	Last name of super admin as it appears in the system.
Admin Email	Email address to which super admin receives notifications.



Setting	Description
Use PWD to log in to SAP SuccessFactors	<p>Once it is checked, the newly created super admin can log into the system using username and password.</p> <div>  <b>Note</b>  This ONLY applies to the instance that has enabled Partial Organization SSO. </div>
Confirmation of customer approval	<p>Provisioning user must check a box confirming that they have received approval from the affected customer for the creation of a super admin user account.</p> <div>  <b>Note</b>  As a Provisioning user, it is your responsibility to obtain this approval before creating a super admin. You cannot proceed without confirming that you have done so. </div>
Customer Email Address	<p>Customer email address that receives notification when the super admin account is created.</p> <div>  <b>Note</b>  This should be the email address of one person who provided the customer approval. You can only send notification to one address.   As a Provisioning user, it is your responsibility to notify the customer and share this information with more people if necessary. </div>

5. Select [Create Admin](#).

#### Note

You can only proceed to create a super admin if you have provided all of the required information. If not, this action is disabled.

6. Save your changes.

## Results

The super admin user account is created and the customer is notified at the email address provided.

## 3.2 Granting Administrators Access to Role-Based Permissions

To grant access to Role-Based Permissions (RBP), you need to log in as a super administrator.

### Context

The [Manage Role-Based Permission Access](#) page allows you to grant user access to both Role-Based Permissions and this page.

### Procedure

1. Log in to your system with administrator credentials. For example, SAP Admin.  
If you don't have super admin credentials, contact Technical Support to have one created for you.
2. Go to [Admin Center](#) and search for [Manage Role-Based Permission Access](#) to grant RBP management access to your super admin or to another admin in your system.

The list of users who have access to RBP in your system is displayed.

3. Select [Add User](#) and use the keyword search to find the user you want to give RBP access to.
4. Select the user's name and choose [Grant Permission](#).
5. Grant access to the user.

RBP Administrator Access	Descriptions
<a href="#">Allow Access to This Page</a>	If selected, the RBP administrator can access this <a href="#">Manage Role-Based Permission Access</a> page.
<a href="#">View Group</a>	If selected, the RBP administrator can view permission groups.
<a href="#">View Role</a>	If selected, the RBP administrator can view permission roles.
<a href="#">Edit Group</a>	If selected, the RBP administrator can edit permission groups.
<a href="#">Edit Role</a>	If selected, the RBP administrator can edit permission roles.

#### Note

We recommend that you grant [View Role](#) and [View Group](#) permissions to RBP administrators so that they can properly use troubleshooting tools such as Role-Based Permissions Troubleshooting Tool, User Role Search, Story reports, and Table reports.

## Results

You've successfully granted administrators access to RBP.

### 3.3 Role-Based Permissions Administrator Access

This topic provides detailed comparison of the [View Group](#), [View Role](#), [Edit Group](#), and [Edit Role](#) access of RBP administrators.

RBP Pages	<a href="#">View Group</a>	<a href="#">View Role</a>	<a href="#">Edit Group</a>	<a href="#">Edit Role</a>
Manage Permission Roles (the legacy RBP)		You can view the list of permission roles.		<ul style="list-style-type: none"><li>You can view, create, edit, delete, and copy permission roles.</li><li>You can edit the <a href="#">RBP-Only</a> column.</li></ul>
Role Details (the legacy RBP)		<ul style="list-style-type: none"><li>You can <b>only</b> view role detail through the view summary action.</li><li>You can't navigate into role detail page.</li></ul>		<ul style="list-style-type: none"><li>You can navigate to the role detail page through the role name link or the <a href="#">Edit</a> action or the <a href="#">Create</a> button.</li><li>You can make changes to the role.</li></ul>
Manage Permission Groups (the legacy RBP)	You can view the list of permission groups.		<ul style="list-style-type: none"><li>You can view, create, edit, and delete permission groups.</li><li>You can edit the <a href="#">RBP-Only</a> column.</li></ul>	
Manage Permission Roles (the latest RBP)		You can view the list of permission roles.		You can view, create, edit, and delete permission roles.

RBP Pages	<a href="#">View Group</a>	<a href="#">View Role</a>	<a href="#">Edit Group</a>	<a href="#">Edit Role</a>
View Role (the latest RBP)		You can view role detail with permissions and assignments.		<ul style="list-style-type: none"> <li>You can view role detail with permissions and assignments.</li> <li>You can navigate to the role detail page through the <a href="#">Edit</a> button.</li> <li>You can add, edit, and delete assignments.</li> </ul>

## 3.4 Enabling Email Notifications for Large-Size Permission Group or Permission Role Changes

For permission role or group changes that impact a large number of employees, you can enable e-mail notifications to alert RBP administrators.

### Prerequisites

You've enabled and customized below email templates under ► [Admin Center](#) ► [Email Notification Templates Settings](#) ►.

- [Role-Based Permission Notification - Role Change](#)
- [Role-Based Permission Notification - Group Change](#)
- [Role-Based Permission Notification - Notification Settings Change](#)

### Context

When counting the number of impacted employees, the system calculates the access population of below relationships of a permission role: [Permission Groups](#), [Managers](#), [HR Managers](#), and [Everyone \(All Employees\)](#).

### Procedure

1. Go to ► [Admin Center](#) ► [Manage Role-Based Permission Access](#) ►.
2. Select [RBP Notification Settings](#).

3. Select [Enable email notification](#).
4. Enter a number between 1 to 99 in the [Threshold for email notification and double-confirmation popup](#) field.
5. Save your changes.

## Results

When an RBP administrator updates a permission role or group that impacts the number of employees you've set, email notifications are sent to all RBP administrators who are selected in the [Notify This User](#) column.

## 3.5 Enabling Double-Confirmation Messages for Large-Size Permission Changes

You can enable double-confirmation messages for large-size permission role or permission group changes.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Role-Based Permission Access](#) ►.
2. Select [RBP Notification Settings](#).
3. Select [Enable double-confirmation popup](#).
4. Enter a number between 1 to 99 in the [Threshold for email notification and double-confirmation popup](#) field.
5. Save your changes.

## Results

When RBP administrators try to save the permission role or group changes that impact the percentage of employees you've set, a double-confirmation popup displays.

## 3.6 Revoking Administrators Access to RBP

As a super administrator of Role-Based Permissions, you can revoke the administrator access of others.

### Prerequisites

You can access the [Manage Role-Based Permission Access](#) page.

### Procedure

1. Go to ► [Admin Center](#) ► [Set User Permissions](#) ► [Manage Role-Based Permission Access](#) ►.

A list of Role-Based Permission administrators displays.

2. Select the users that you want to delete.

If you delete the administrators from the page, they can't grant permissions to others or access the [Manage Role-Based Permission Access](#) page anymore. If you want to prevent administrators from accessing this page but keep their rights to grant permissions, you can deselect the [Allow Access to This Page](#) column instead.

3. Click the [Delete User](#) button.

#### ⓘ Note

You can't delete yourself from the page or deselect the [Allow Access to This Page](#) column for yourself. But you can remove your [Role-Based Permission Admin](#) permission.

### Results

You've successfully revoked the administrator access of the selected users.

## 3.7 Granting Yourself and Project Team Members All Permissions

You can use groups to grant yourself and other project members access permissions.

### Context

You and other project team members require access to all modules and data.

### Procedure

1. Create a group, for example "System Admins All Modules", then assign all relevant admin users to this group.
2. Create a role, for example, "System Admin All Modules", add all available permissions to it, and grant this role to the just created group with the target population of everyone.

### Related Information

[Grant Permission Roles](#)  
[Creating Permission Roles](#)

## 3.8 Refreshing RBP after Changes in Provisioning Configuration

Once RBP is enabled, changes to settings in Provisioning don't immediately appear to RBP permissions settings. You need to refresh RBP.

You can refresh RBP in the following ways. The first option is highly recommended.

#### → Remember

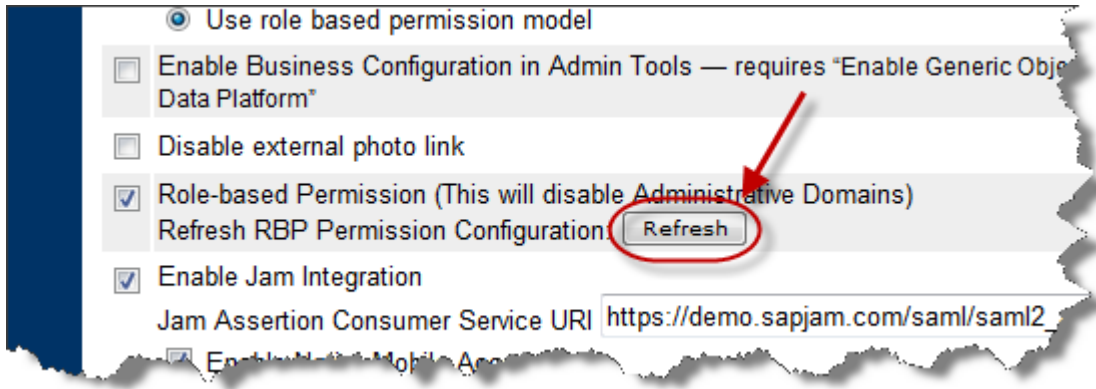
As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

- (Recommended) Enable the [Enable Refresh Framework](#) option in Provisioning. When this option is enabled, RBP changes are updated in near real time, and there's no need for you to refresh RBP in other ways.

#### 📌 Note

If [Enable Refresh Framework](#) is enabled in your system, don't disable it.

- (Recommended) You can now trigger a [Refresh RBP Model](#) job to refresh RBP permission list under ► [Admin Center](#) ► [Scheduled Job Manager](#) . It's a one-time job. For this job type, you need to wait for one job to finish before starting another.
- In Provisioning, under [Company Settings](#), click [Refresh](#) next to [Refresh RBP Permission Configuration](#). This triggers a real time refresh of the RBP permissions to become aware of the features you've enabled.



- Export and re-import the Succession Data Model. This action triggers a real time refresh of the RBP permissions to become aware of the new features you've enabled.
- Wait 24 hours, and the system automatically refreshes RBP.




# 4 Steps for Designing the RBP Configuration

Each implementation project needs a clear definition of what permissions are needed for the individual user groups. To define this configuration, you should consider the customer's requirements and the leading practices considering maintenance and performance aspects.

## Context

We recommend that you follow these steps:

## Procedure

1. For new customers or customers who have RBP enabled, you can start out by reviewing the available permissions based on the modules that are deployed in the customer's instance. [Checking Available Permissions in a New Customer Instance \[page 18\]](#)
2. If you're migrating a customer instance from a non-RBP system to an RBP enabled system, start by reviewing the permissions settings in the non-RBP instance. [Review Permissions in Existing Customer Instance \[page 18\]](#)
3. Familiarize yourself with the recommendations and leading practices. [Recommendations and Leading Practices \[page 49\]](#)
4. See the basic roles section to learn about the common roles that are created for customers. [Basic Roles \[page 18\]](#)
5. Conduct requirements sessions with the customer to clarify their needs. Ask them to determine the appropriate roles, what permissions those roles require, and who would be granted those roles.
6. Create a workbook that lists the groups, roles, and what permissions they contain, and the mapping of roles to groups. For defining these, it's useful to have a good understanding of how you can grant roles to groups ([Creating a Permission Role \[page 35\]](#)), especially how you can use relationships ([Relationships Between Managers and Employees \[page 20\]](#)).
7. Typically, the workbook functions as a statement of work for your project. That is, it doesn't contain the complete RBP setup, but only the limited number of groups and roles you set up. The remainder should then be configured by the customers themselves to familiarize them with RBP as much as possible. This way you can ensure they're autonomous and ready to manage RBP after you leave the project. As a guideline, we suggest that you set up a maximum of 10 roles. If you have access to Product Information Central, you can download a sample workbook: [sample workbook](#) .

## 4.1 Checking Available Permissions in a New Customer Instance

When setting up RBP in your system for the first time, it's important to understand the permission structure that is already deployed.

### Context

Depending on what modules are activated in your system, different permissions are available to be configured. Follow the steps to find out exactly what permissions can be granted:

### Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The latest [Manage Permission Roles](#) page displays.
2. Choose [Create](#).  
The [Create Role](#) wizard displays.
3. Provide information in the [Basic Information](#) step.
4. Go to step 2 [Add Permissions](#). On the left, you can see the permission categories. If you click on one of these categories, you see the detailed permissions on the right.

## 4.2 Review Permissions in Existing Customer Instance

If you migrate a customer instance from the old permission framework to RBP, create a security permissions report to review what permissions are set.

Log on to the customer instance and select ► [Admin Tools](#) ► [Set User Permissions](#) ► [Security Permissions Report](#) ►.

## 4.3 Basic Roles

Some roles in general exist in each company, for example, Managers and HR Manager. These roles tend to have similar permissions. We have listed the most common roles below along with their typical permissions. You could use these to start the requirements discussions with your customers. Even before the requirements session you could proactively configure these roles to give users access to the system to test the configuration. These roles do

not require specific groups. Therefore it is possible to create them before you have created any groups. However, in larger organizations some roles might be split up in more specific roles. For example, they do not have a single manager role, but one manager role for each region because in each region they are allowed to see different data.

Role Name	Includes the following permissions...
Login	<ul style="list-style-type: none"> <li>Login permission</li> </ul> <p>To have the login permission in a separate role allows the admin to turn the system on and off as needed (for maintenance, for example) without going into any other roles. This can also be useful if a global organization wants to release the system to a specific population (for example, in specific country) at different time. Additionally, the login permission should be included in the "System Admin All Modules" role to make sure that they are not locked out either.</p>
All users (what any user can do and see for all other users)	<ul style="list-style-type: none"> <li>Data any user can see about any other user</li> <li>Access to goal and development plan</li> <li>Careers tab permission</li> <li>Permission to navigate within the org chart</li> <li>Mobile access, if necessary</li> </ul>
Employee self (what users can do and see for themselves)	<ul style="list-style-type: none"> <li>Data users can see about themselves (like employment data or personal info)</li> <li>What background sections they can maintain and edit for themselves</li> <li>Permission to create forms for themselves (depending on the culture)</li> </ul>
Managers (permissions granted to users who have at least one direct report defining what they can do and see for their direct reports)	<ul style="list-style-type: none"> <li>What data managers can see about their reports</li> <li>Permission to create forms for their reports</li> <li>Permission to create job requests</li> <li>Permissions to manage compensation for their reports, if necessary</li> <li>Permission to use succession and succession org chart</li> </ul>
HR (permissions granted to HR staff)	<ul style="list-style-type: none"> <li>What data HR can see and maintain for their scope</li> <li>Permissions to create forms depending on the culture</li> <li>Permission to use succession, calibration and so on</li> <li>Permission to search for candidates or use talent search</li> </ul>
System Admin All Modules (permissions granted to customer admins)	<ul style="list-style-type: none"> <li>Permissions to do and see everything for everybody</li> </ul>
Local Administrators	<ul style="list-style-type: none"> <li>Limited administration rights, for example, upload employee data, create performance forms</li> </ul>

## 4.4 Relationships Between Managers and Employees

There are relationships that can be specified through employee fields, and managed through tools, like the employee data.

**General Relationship Types:** Hierarchical relationships are characterized by a reporting line between the granted user and the target user. These are relationships between employees and their managers, and employees and their second managers or alternate managers. Non-hierarchical relationships on the other hand are single-level relationships. These include the relationship of an employee to the HR manager, the matrix manager and custom manager. While each employee can have only one Manager, one Second Manager and one HR Manager, they can have multiple Matrix Managers and Custom Managers.

**Employee Central Only:** If employees have global assignments (that is, a job in another country/region), they have both a home manager and a host manager. In addition, they have a home HR manager and a host HR manager. All managers need to have access to both the home jobs of the employees as well as to the host jobs of the employees. This is covered by the following additional relationship types for global assignments:

General Relationship Types	Employee Central Only: Relationship Types for Global Assignments
Manager	Home Managers
Second/Alternate Manager	Home HR Managers
HR Manager	Host Managers
Matrix Manager	Host HR Managers
Custom Manager	
Managers (Internal Hire)	

### 4.4.1 Delegate Relationship Assignments

As a delegator you can assign delegates to perform actions on your behalf that affects other employees in your organization.

As a manager, you can use the [Delegate A](#) and [Delegate B](#) relationship roles to assign permissions to up to two individuals for each role, allowing them to act as your delegates. The delegate users you assign, can access your direct and indirect reports and can perform tasks that have been permitted to you, while acting as your delegates. You can assign up to two delegates per delegate role and each delegate can be given separate tasks or permissions to cover different functional or regional areas.

#### 📌 Note

You must configure [Delegate](#) relationship type in the Employee Central Picklist. After you've configured your delegates, you'll see the option to give permissions to this relationship type in your system. For more information about how to configure picklists, see the topic [Picklist Configuration for Employee Status and Job Relationship Type](#).

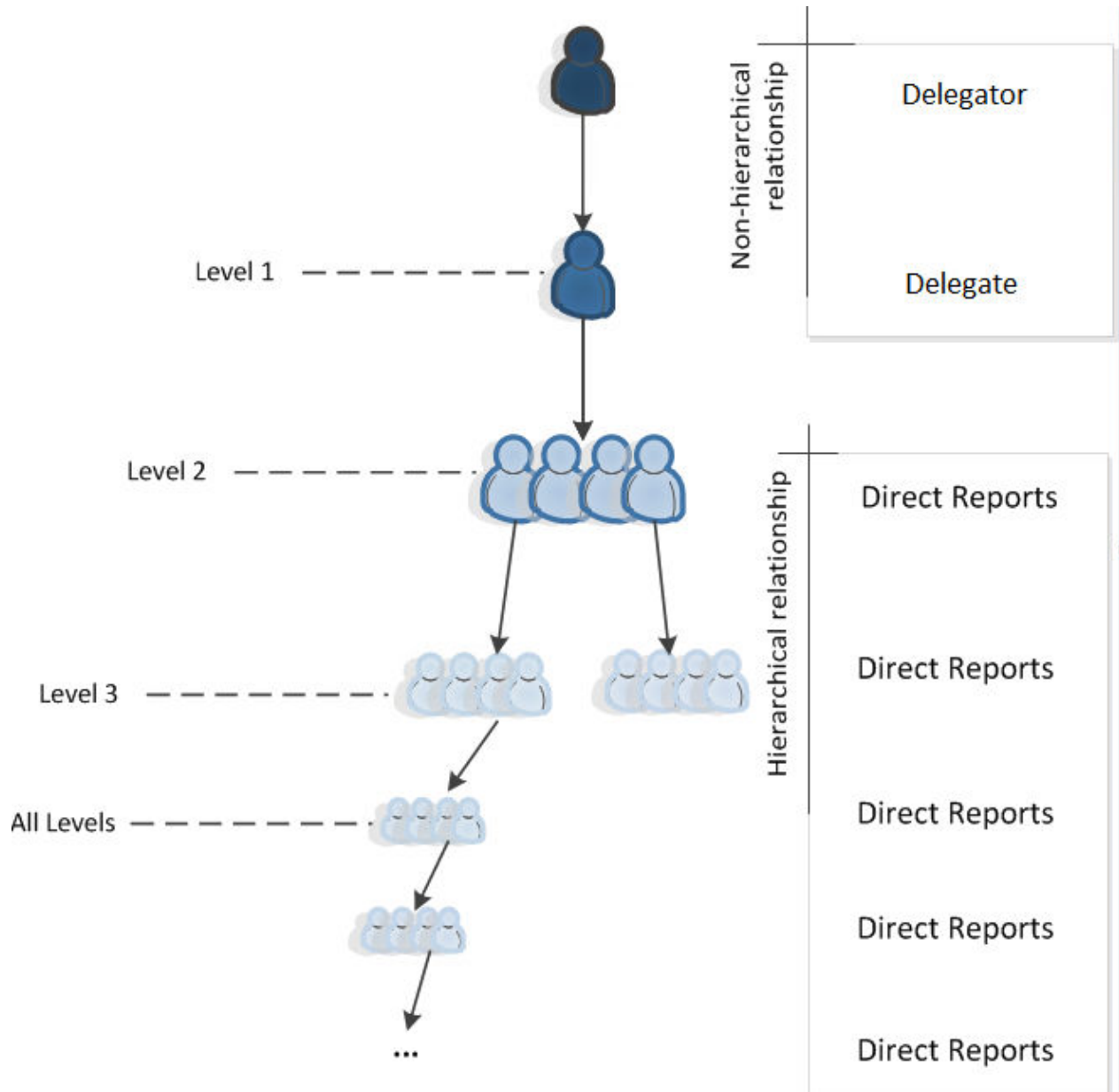
## Why would I want to use delegates?

You might use a delegate when you want to assign delegates permissions in different functional areas.

You can also assign permissions to delegates that separate functionality according to locations.

If delegate relationship has been defined in Employee Central picklists, you can grant a permission role to delegates. When a manager delegates his or her tasks to two delegates, delegate A and delegate B, the manager's direct reports are the target population of delegate A and delegate B. If the manager, delegate A, and delegate B are in the same permission roles, delegate A and delegate B will have the same permissions. The manager's direct reports are the target populations of the delegate A and delegate B for the permissions that require a target. However, this delegate relationship can't be used in non-user-based permissions. For example, even if delegate A and delegate B has the same ► [Miscellaneous Permissions](#) ► [Position](#) ► permission as the manager, delegate A and delegate B can't view the current state of the position or view its history because the [Position](#) permission isn't user-based.

	User-Based RBP Permissions	Non-User-Based RBP Permissions
Description	Permission to the data of a user. The target population of the permission can be grouped as a user list. It can be RBP permissions or some of the MDF permissions.	MDF objects that are categorized in the <a href="#">Permission requiring MDF object target</a> section.
Example	The <a href="#">Personal Information</a> permission controls access to the personal information data of a user.	The ► <a href="#">Miscellaneous Permissions</a> ► <a href="#">Payment Information Detail</a> ► permission.



## 4.4.2 Hierarchy Depth and User Permissions

Understand how to use hierarchy depth when assigning permissions to your users.

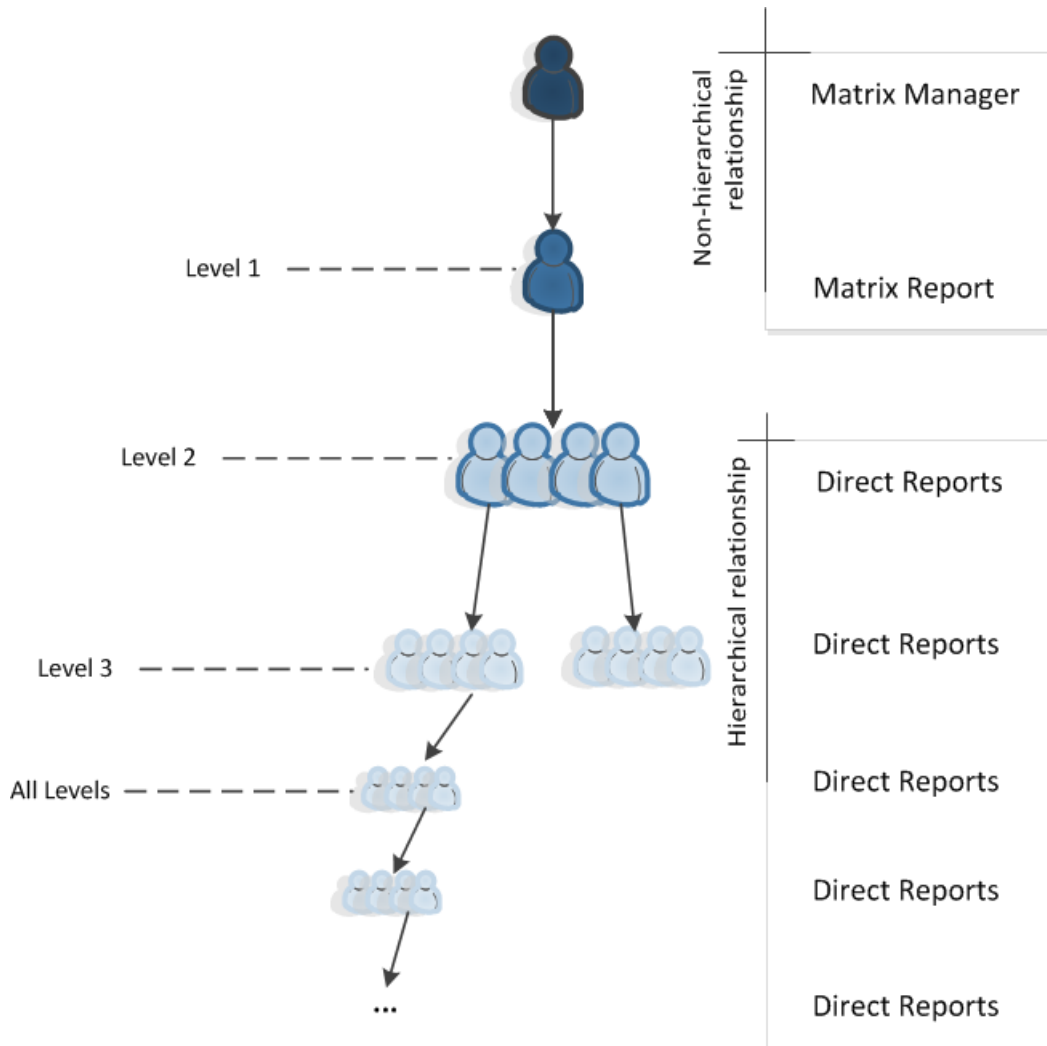
When granting permissions using hierarchical relationships, you can specify how many levels down to go in the hierarchy for the target population. For example, you can indicate that Managers can see performance ratings on their direct reports (1 level deep), or allow it to go deeper into their team, that is 2 levels down or all levels.

When granting permissions to non-hierarchical relationships (HR, Matrix and Custom Managers), you can follow this non-hierarchical relationship for only one level. Beyond the first level, you can cross over to the standard manager hierarchy if desired to go deeper.

For example, using the Matrix Manager relationship, you can use hierarchical depth to accomplish the following:

- 1 Level Deep: Matrix Managers can view ratings information for their Matrix Reports.
- 2 Levels Deep: Matrix Managers can view ratings information for their Matrix Reports and the Direct Reports of their Matrix Reports.
- All Levels Deep: Matrix Managers can view ratings information for their Matrix Reports (1 level deep) and the Direct Reports, all levels deep of the manager hierarchy of their Matrix Reports.

The following graphic illustrates the different hierarchical depths you can specify when you use the Matrix Manager relationship:



## 4.5 Copying Roles and Groups between Test and Production Systems

When you configure RBP, it's common to make changes first on the test instance. Only after successful testing you copy the configuration to the production instance.

Permission roles are dependent on the system configuration, for example, fields, forms, or reports in your system. Permission groups are dependent on the employees and their data. It's important that test instance and production instance contain the same system configuration and employee data.

To make sure that test and production instance are in sync:

- Ensure that your employee data file is synchronized between your test and production systems.
- Consider if there are data changes coming that could affect the ability to permission correctly (for example organizational restructures). If so, you need to have that data available in the test instance if you want to permission it now. In addition, the data needs to be in the production instance by the time the permissions are ready to be copied to the production instance.
- Consider if there are system configuration differences between your test and production systems. For example, are there more features enabled in the production instance than in the test instance? Compare the data models to make sure the instances match. You can ignore the permissions sections of the data models at this point that don't apply in RBP systems. Only check for data elements.

Depending on how much is out of sync, you can either have the production instance copied to the test instance by using the instance sync tool or work around it.

If it's not possible to update the test instance with productive data for data protection reasons, you must at least make sure that all elements actually exist in the test instance. Otherwise, it isn't possible to fully implement RBP on the test instance so that it can then be copied to the production instance.

## 4.6 Conducting Tests

After you have set up all groups and roles and granted the roles, test the permissions thoroughly to find out whether the employees have access to everything they need.

You can only conduct reliable tests if the data is complete in the test instance. Roles which require dedicated groups cannot be tested otherwise. If the data is not there to populate the granted users group or the target users group, the tests will fail. The easiest way would be to update the test instance with production data. However, if this is not possible due to data protection reasons, a set of real sample data is required to conduct valid testing.

Testing roles which do not require specific groups but make use of relationships is easier. You just need test users for all hierarchy levels, like manager, HR Manager, and employee. Double check the hierarchy, then log on as a specific test user and double check the permissions.



## 5 Role-Based Permissions

Role-Based Permissions (RBP) is a security model that allows you to restrict and grant access to your SAP SuccessFactors HCM suite. RBP controls access to the applications that employees can see and edit. This is a suite-wide authorization model that applies to the majority of the SAP SuccessFactors products.

Here's an example of the *Create Role* wizard:

[Admin Center](#) / [Manage Permission Roles](#) / [Create Role](#)

### Create Role

1 Basic Information — 2 **Add Permissions** — 3 Preview

#### 2. Add Permissions

Specify what permissions users of this role should have.

**User Permissions**

- Goals
- Career Development Planning
- Talent Search Field
- Succession Planners**
- Learning
- Employee Central Effective Date...
- Employee Central - Compensati...
- Employee Central Import Entities
- Employee Widgets
- Employee Views
- Manage Document Generation T...

#### Succession Planners

★=Access period can be defined at the granting rule level. †=Target needs to be defined. \*+=Target criteria need to be defined.

☐ Select All

<input type="checkbox"/> Succession Org Chart Permission	Allow role to access the succession organizational chart an...
<input type="checkbox"/> Succession Approval Permission †	Allow role to approve successors nominated to Succession ...
<input type="checkbox"/> Succession Management and Matrix Report Permissions †	The target population assigned to this permission will contr...
<input type="checkbox"/> Succession Planning Permission †	Allow role to nominate successors for an incumbent.
<input type="checkbox"/> Talent Search Access	Allow role to access Talent Search
<input type="checkbox"/> Talent Search Export Permission	Allow role to export Talent Search results. The fields in the ...
<input type="checkbox"/> Matrix Report Permission	Allow role to access the Matrix Report

### Supported Features

- RBP-only permission roles and permission groups are also supported. RBP-only indicates that the permission role or permission group is only accessible for RBP administrators for permission-related features. Other features, such as home page, can't reuse this role or group.
- All four permission types are supported, including on-off permissions, parent-child permissions, all-other permissions, and permissions with actions.
- Compensation and MDF permissions are supported.
- Target criteria, data blocking, and tree security permissions are supported.
- Printing permission roles and role assignments are supported.

## 5.1 Role-Based Permissions Experience for Administrators

As an RBP administrator, you see a simplified administration page using Role-Based Permissions.

Before we dive into Role-Based Permissions, here're four concepts you want to know.

- **Permission role:** a set of permissions
- **Access population:** users who are granted the permissions
- **Target population:** users whose data can be accessed or managed by an access population
- **Role assignment:** a relationship between a role and its access population and target population

To understand the concepts of RBP, consider an administrator named Carla Grant whose job requires this administrator to edit the personal data of employees in Canada. The permission role for Carla includes a set of permissions that give Carla write access to Canadian employees' personal data. Carla is one of the administrators in the access population because Carla is granted permissions to edit Canadian Employees' data. Employees working in Canada are the target population because Carla can access their data and manage them. The role assignment is what Carla can do to access or manage Canadian Employees: as a simple example, add, edit, and delete.

You can use Role-Based Permissions to create permission roles, define access population, define target population, and manage roles and role assignments.

## 5.2 Permission Groups

Permission groups are used to define groups of employees who share specific attributes. You can use various attributes to select the group members, for example a user's department, country/region, or job code. Permission groups can be dynamic or static. Dynamic permission groups support employee and onboarder user types, while static permission groups support only employee user type.

### ❖ Example

There might be a permission group called "Human Resources in US", which lists all US-based employees who work in the HR department. To define this group, you would specify that users must match the selection criteria "Country/Region = United States" and "Department = HR".

### 📌 Note

The attributes or selection criteria that are available for defining groups are configurable.

In RBP, you can assign permission roles to permission groups. In addition, you use groups to define the target population a granted user has access to.

### ❖ Example

The group "Human Resources in US" might have access to the group "US Employees".

Groups configured with criteria other than specific user names are called **dynamic** (as opposed to **static**), which means that the assignment of employees into and out of a group is automated. For example, a group of

granted users can be “All employees in the Sales department”. As employees are transferred into and out of the sales department, their permissions will automatically adjust. This automation will save you time and money. This is especially beneficial for large organizations that need higher levels of administrative efficiency.

## 5.2.1 Creating Static Permission Groups

Static permission groups are created and modified by adding individual user names to a group using an excel spreadsheet. They store a static list of users instead of a list based on dynamically generated criteria. Changing user information does not modify group members, you must redefine group members by importing an updated spreadsheet.

### Procedure

1. In the *Admin Center*, search for *Manage Permission Groups*.
2. Click *Import Static Groups* to create or modify a group.
3. Select between *Full Replace* or *Delta Replace*.

A full replace, creates or entirely replaces a group, while a delta replace adds members to an already existing group.

**Import Static Group**

The Import Static Group page lets you add or modify static groups by uploading a static group data file. You can download a blank CSV template to see the file format. Please note the character encoding of the file should be Unicode(UTF-8). You can use a full replacement import. Or you can add or remove users of a static permission group using delta replacement import. After completing importing, you will receive an email and the group will display in the list by refreshing.

**Choose File:**  No file chosen

[Download a blank CSV template](#)

**Import Type**

☒ Full Replace

☐ Delta Replace

4. Download a blank CSV template after you've chosen an import type. The *Full Replace* template has two column headers, *GROUPNAME* and *USERID*. The *Delta Replace* has an additional *Action* column.
5. For each user that you add to a group, add the group name to the *GROUPNAME* column and user's ID to the *USERID* column.

#### Note

For new users, you can create user IDs in the upload file.

### Note

Character encoding of your file should be Unicode (UTF-8). The maximum file size is 20MB. If your import file exceeds 20MB, you can either split the file into several smaller files or request Professional Services to modify the system configuration file.

6. Select the file with your data by clicking [Choose File](#).
7. Click [Validate File](#) to validate file format, file size, etc.
8. If the validation is successful, click [Upload](#) to import the static permission groups.

If your file has errors, they display at the top of the [Import Static Group](#) window.

### Note

For one group type, a maximum of two jobs can run at the same time.

## Results

After the upload completes, the system sends you a notification with success or error messages. Successfully created groups display in the group list after refreshing your system.

Subject: Static Group Import Notification

Please be advised that static group import process has been finished.

Total rows in the static group import file: 7  
Successful: 1; Failed: 6

Static group import job reported error(s). You need to fix the following error(s) and re-import if necessary:

Row 5: Column number is not consistent with headers.  
Row 3: USERID asadasdad does not exist in system.  
Row 6: Duplicate row.  
Row 2: Empty in GROUPNAME column.  
Row 7: GROUPNAME HR Group is an existing dynamic group.  
Row 8: Length of GROUPNAME exceeds 100 bytes.

-----  
PerformanceManager  
Copyright 2003 SuccessFactors, Inc. All rights reserved.

This message was sent by the PerformanceManager application.  
For questions about this application, please contact the technical support personnel.

## 5.2.2 Adding Individual Members to Static Groups

You can add members to a static group in your system or by importing an excel file to your system.

### Procedure

1. In the [Admin Center](#), search for [Manage Permission Groups](#).
2. Click the name of the static group you're updating.

The [Permission Group](#) screen displays.

3. To add a user to a static group, click [Add User](#).
4. Search for the users you'd like to add to the group.

Entering keywords in the search field displays user names.

5. Select each user you want to add to the group.

Each user you select automatically displays in the right pane.

6. Click [Done](#).

The users you selected are added to the group immediately.

## 5.2.3 Adding Multiple Members to Static Groups

Instead of opening static groups one by one to add members, you can add multiple members to several static groups all at once with a CSV file.

### Procedure

1. Go to ► [Admin Center](#) ► [Set User Permissions](#) ► [Manage Permission Groups](#) ►.
2. Click [Import Static Groups](#).

The [Import Static Group](#) popup displays.

3. Choose [Delta Replace](#).
4. Click [Download a blank CSV template](#).

A CSV template for delta replacement is downloaded.

5. Fill in the CSV file.

Column Head	Description
GROUPNAME	Fill in the names of the static groups that you want to add members to.

Column Head	Description
USERID	You can choose to provide either USERID or ASSIGNMENTID of employees.
ASSIGNMENTID	You can choose to provide either USERID or ASSIGNMENTID of employees.
ACTION	ADD

6. Save the file.
7. Go back to the [Import Static Group](#) popup and upload the CSV file that you've prepared.
8. Click [Validate File](#).

A message displays at the top of the [Import Static Group](#) popup to inform you whether there's any format issue in the CSV file.

9. If there are no issues found in the validation phase, choose the CSV file again and click [Upload](#).
10. Click [Cancel](#) to dismiss the Import Static Group popup.

## Results

You have successfully added members to the static groups with a CSV file. You receive an email about the details.

## Next Steps

Refresh the Manage Permission Groups page to double check the active membership of the static groups that you've updated.

## 5.2.4 Removing Members from Static Groups

Although you add members to a static group using a spreadsheet, you can remove static group members using the system.

### Procedure

1. In the [Admin Center](#), search for [Manage Permission Groups](#).
2. Click the name of the static group you're updating.  
The [Permission Group](#) screen displays.
3. Select the users that you want to remove from the group.
4. Click [Delete](#).

The list of users updates immediately.

5. Click [Close](#).

## Results

Removed members will no longer have access to the tasks or data of the group.

## 5.2.5 Removing Multiple Members from Static Groups

Instead of opening static groups one by one to remove members, you can remove multiple members from several static groups all at once with a CSV file.

### Procedure

1. Go to ► [Admin Center](#) ► [Set User Permissions](#) ► [Manage Permission Groups](#) ►.
  2. Click [Import Static Groups](#).
- The [Import Static Group](#) popup displays.
3. Choose [Delta Replace](#).
  4. Click [Download a blank CSV template](#).

A CSV template for delta replacement is downloaded.

5. Fill in the CSV file.

Column Head	Description
GROUPNAME	Fill in the names of the static groups that you want to remove members from.
USERID	You can choose to provide either USERID or ASSIGNMENTID of employees.
ASSIGNMENTID	You can choose to provide either USERID or ASSIGNMENTID of employees.
ACTION	REMOVE

6. Save the file.
7. Go back to the [Import Static Group](#) popup and upload the CSV file that you've prepared.
8. Click [Validate File](#).

A message displays at the top of the [Import Static Group](#) popup to inform you whether there's any format issue in the CSV file.

9. If there are no issues found in the validation phase, choose the CSV file again and click [Upload](#).
10. Click [Cancel](#) to dismiss the Import Static Group popup.

## Results

You have successfully removed members from the static groups with a CSV file. You receive an email about the details.

## Next Steps

Refresh the Manage Permission Groups page to double check the active membership of the static groups that you've updated.

## 5.2.6 Creating Dynamic Permission Groups

Dynamic permission groups are generated automatically when the attributes of employees match the group selection criteria. Administrators can create and manage dynamic permission groups for both employees and external users.

## Procedure

1. In the *Admin Center*, search for *Manage Permission Groups*.
2. Click *Create New* to create a new permission group.

The *Permission Group* page opens.

3. Enter a name for your permission group in the *Group Name* field.
4. Choose a *User Type* for your group.

The available user types vary depending on how your system is configured. Possible values may include:

- *Employee* (default)
- *External Learning User*

### Note

The External Learning User option is only available if you have Learning enabled in your system.

- Alumni
- External Onboarding User

When defining a dynamic group for an external learning user, you can identify an **External Source Channel** to complete the criteria for inclusion. This allows external learning users to be defined based on the source of origin. The external source channel is only available to SAP SuccessFactors Learning customers. The **External Learning User** must be enabled in *Provisioning* for external learner and external source channel to be available.



### → Remember


As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

### → Tip

When defining *External Learning User* groups in your system, it is recommended that you do not create more than 50 groups.

5. Choose the group selection criteria from the *People Pool*, in the *Choose Group Members* section.

Depending on the complexity of your permission group selection criteria, you can choose multiple people pools.

6. In the *Search Results* screen, enter a search term or click the  *search*, to display all available values.

For some categories, a smaller pop-up window appears where you can enter additional values or information, such as *Time Zone* settings. If you select the *Team View* category, you can use hierarchical relationships to specify the group. This allows you to apply rules such as: everybody in Carla Grant's team, all levels deep.

### 📌 Note

When you search employees with the *User* category, the search results in the dropdown display only employee names. When you search employees with the *Team View* category, the search results in the dropdown display employee names, employee titles, and locations.

7. Make your selection and click *Done*.
8. If you want to add another condition for defining the people pool, click *Add another category* and choose a category and item. If you use two or more categories, this functions as an **AND** operation, that is, only users are selected who meet all selection criteria.

### 🔗 Example

If you want to create a group of sales employees working in the US, you would need to choose the category Department and select Sales. You add a second category Country/Region and select United States.

9. Complex group definitions may require you to use multiple people pools. If you use two or more people pools, these people pools functions as an **OR** operation, that is, all users are selected who fulfill the selection criteria of at least one pool.

Click *Add another People Pool* and then add categories and items.

### 🔗 Example

You have two different offices: An office in Chicago and an office in Boston. Each office has a Sales team and a Finance team. You only want to include Sales employees from the Chicago office and Finance employees from the Boston office. You'll need to create two separate pools then.

### 📌 Note

The number of people pools in a group is limited to four.

10. If there are employees you'd like to exclude from the Permission Group definition, select them in the *Exclude these people from the group* section.

11. If you want to prevent the group being updated automatically when new employees match the selection criteria, click [Lock group](#).
12. (Optional) Choose [Update](#) in the [Active Group Membership](#) box to see how many users match the criteria. Click the number to see the detail list.

The active group membership number isn't updated automatically when you modify the dynamic group definition.

13. Choose [Done](#) to complete the process.

## 5.2.7 Managing Permission Groups

You can manage static or dynamic permission groups. You can also mark a permission group as RBP-only, which means the group can be only used in Role-Based Permissions. If a permission group isn't RBP-only, it can also be used in other modules, for example, on home page. For dynamic groups, you can also view the group's change history.

### Context

#### ⓘ Note

You can only delete a permission group if it has no associated role.

### Procedure

1. Go to the [Admin Center](#) [Tools](#) and search for **Manage Permission Groups**.
2. In the [Manage Permission Groups](#) screen, click the [Take Action](#) dropdown menu next to the permission group you want to modify.
  - You can see delete and view summary of static groups.
  - You can edit, copy, delete, view summary, and view change history of dynamic groups.

#### ⓘ Note

You can only see the most recent 1000 changes in the View change history view. If you want to see more than the last 1000 changes, use the Change Audit report.

3. Choose the desired action.

## 5.3 Creating a Permission Role

Role-Based Permissions use permission roles to group a set of permissions.

### Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) permission.

### Procedure

1. Go to [Admin Center](#) > [Manage Permission Roles](#).

The [Manage Permission Roles](#) page displays.

2. Choose [Create](#).

The [Create Role](#) wizard displays.

3. Input information by following the wizard steps as listed.

Wizard Steps	Actions
Basic Information	<p>Provide a role name. This is a required field. The maximum length is 255 bytes.</p> <p>Provide a description. The maximum length is 4000 bytes.</p> <p>Select a user type from the drop-down. Three user types are supported: <a href="#">Employee</a>, <a href="#">External Onboarding User</a>, <a href="#">External Learner</a>, and <a href="#">Alumni</a>.</p> <p>If you want to prevent other modules from using this role, select <a href="#">RBP-Only</a>.</p>
Add Permissions	<p>Choose a permission category from the left panel. A list of permissions of the category displays on the right panel for your selection.</p> <div><p>→ Tip</p><ol style="list-style-type: none"><li>1. To make navigation easier, select the <a href="#">Sort By Ascending</a> check box in the left panel. This arranges the permission categories in ascending order.</li><li>2. Click the <a href="#">Enter Full Screen</a> button to expand the Add Permissions section.</li><li>3. If the number of field-level overrides for a permission category exceeds 20, these overrides appear in "view" mode. You can select <a href="#">Edit</a> next to the permission to switch to "edit" mode.</li></ol></div>
Preview	Double check the information that you've defined.

4. Save your changes.

A success message displays.

5. Choose [OK](#) to assign the role or choose [Not Now](#) to go back to the [Manage Permission Roles](#) page.

## Results

You've successfully created a new permission role.

## 5.4 Assigning a Permission Role

A role assignment is a relationship between a role and its access population and target population. You can use the [Add Role Assignment](#) page to assign permissions to a group of users and define whose data those users can access.

### Prerequisites

You're in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) and [View Group](#) permissions.

### Context

After creating a permission role, choose [OK](#) on the [Success](#) popup to continue to assign the role. You can also add role assignments in the [Manage Permission Roles](#) page or the [Role Assignments](#) page.

### Procedure

1. Go to [Admin Center](#) [Manage Permission Roles](#).
- The [Manage Permission Roles](#) page displays.
2. Choose [Add Role Assignment](#) for the permission role that you want to assign.
- The [Assign Role Assignment for](#) wizard displays.
3. Input information by following the wizard steps as listed.

Wizard Steps	Actions
Basic Information	Provide a role assignment name. It's a required field. The maximum length is 255 bytes. Provide a description. The maximum length is 4000 bytes.

Wizard Steps	Actions
	<p>Select a user type for the target population.</p> <p>Optionally, you can set the effective duration of the role.</p> <p>Choose a status for the role assignment. If you enable effective duration, the <a href="#">Status</a> field is hidden.</p> <p>In an Employee role assignment, if Alumni Experience is enabled in your instance, you can specify Alumni as the target population by selecting <a href="#">Alumni</a> in the <a href="#">Target Population User Type</a> dropdown in the <a href="#">1. Basic Information</a> step.</p>
Grant Access to	<p>Select all or groups of users.</p> <p>For Alumni roles, user type <a href="#">Alumni</a> is selected in this step.</p> <p>(Optional) You can also grant the same access to managers of the users in those groups.</p> <div data-bbox="841 646 1435 814"> <p><b>Note</b></p> <p>When you search for a group, input the beginning of the group name in the group search field and click "Enter".</p> </div>
Define a Target Population	<p>Select everyone or a subset of employees.</p> <p>To select a subset of employees, use permission groups, filters such as <a href="#">Granted User's Location</a>, or both.</p> <p>(Optional) You can exclude the granted users from having the same access to themselves.</p> <p>In an Alumni role assignment, the target population is always the granted users themselves.</p>
Define Target Criteria	<p>(Optional) For permission roles that require target criteria, choose <a href="#">Restrict Target Criteria to:</a> and select the <a href="#">value help</a> icon to add your target criteria.</p>
Define Data Blocking	<p>(Optional) For permission roles that require data blocking, choose <a href="#">Restricted</a>, and enter the number of months (0 to 999) for which the role has access to the historical data.</p> <ul style="list-style-type: none"> <li>The system always uses the current date to calculate the authorization period, so if you enter "12", the role will have access to historical data up to 12 months prior to today's date.</li> <li>If you enter "0", the role has no historical access at all. That is, the role can't see anything older than today.</li> <li>The system always uses the time zone of the signed-in user to calculate the period.</li> </ul>
Define Tree Security	<p>(Optional) For permission roles that require tree security, define the view of the dimension that's accessible to the user.</p> <div data-bbox="841 1560 1435 1707"> <p><b>Note</b></p> <p>Tree security permissions are only for instances that have enabled Workforce Analytics (WFA).</p> </div> <ul style="list-style-type: none"> <li>Tree security rules can be <a href="#">Include</a> or <a href="#">Exclude</a> rules. Include rules specifically identify the nodes of the tree that are accessible, whereas Exclude rules specify access to all nodes except those identified.</li> <li>Specify the target tree security permissions applicable to each Structural Dimension, which the granted users</li> </ul>

Wizard Steps	Actions								
	<p>have permission to access. While specifying, you can choose from the following:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><i>All</i></td><td>To allow the user to see the entire dimension. If needed, you can choose <i>Drill to Detail</i> to allow users to view applicable underlying series of data.</td></tr> <tr> <td><i>Hidden</i></td><td>If the granted users don't require access to the dimension.</td></tr> <tr> <td><i>Restricted</i></td><td>If users only require access to specific dimensions.</td></tr> </table>	Option	Description	<i>All</i>	To allow the user to see the entire dimension. If needed, you can choose <i>Drill to Detail</i> to allow users to view applicable underlying series of data.	<i>Hidden</i>	If the granted users don't require access to the dimension.	<i>Restricted</i>	If users only require access to specific dimensions.
Option	Description								
<i>All</i>	To allow the user to see the entire dimension. If needed, you can choose <i>Drill to Detail</i> to allow users to view applicable underlying series of data.								
<i>Hidden</i>	If the granted users don't require access to the dimension.								
<i>Restricted</i>	If users only require access to specific dimensions.								
<b>Preview</b>	Double check the information that you've defined.								

4. Save your changes.

A success message displays.

## Results

You've successfully created a role assignment.

## Related Information

[Tree Security Rules](#)

## 5.5 Updating a Permission Role

You can update details of a permission role, except for its user type.

## Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) permissions.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The [Manage Permission Roles](#) page displays.
2. Choose [Edit](#) of the permission role that you want to update.  
The edit role wizard displays.
3. Update the changes you want.
4. Save your changes.

## Results

You've successfully updated the permission role.

## 5.6 Updating a Role Assignment

You can update details of a role assignment.

## Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) and [View Group](#) permissions.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The [Manage Permission Roles](#) page displays.
2. Choose a permission role.  
The [Permissions](#) and [Assignments](#) tabs display.
3. Go to the [Assignments](#) tab.  
The assignment list of the permission role shows.
4. Choose the [Edit](#) button of the role assignment you want to update.  
The edit role assignment wizard displays.
5. Update the changes you want.
6. Save your changes.

## Results

You've successfully updated the role assignment.

### Note

After you **create** or **delete** role assignments, the system updates the last modified date of the permission roles accordingly. However, when you **update** role assignments, the last modified date of the permission roles remains unchanged.

## 5.7 Deleting a Permission Role

You can delete permission roles that you no longer need. If you delete a permission role, all its role assignments are deleted as well.

### Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) permission.

### Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The [Manage Permission Roles](#) page displays.
2. Choose [Delete](#) in the [Actions](#) column of the permission role you want to delete.  
A double confirmation message shows.
3. Choose [Delete](#).

## Results

You've successfully deleted the permission role.



## 5.8 Deleting a Role Assignment

You can delete role assignments that you no longer need.

### Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) and [View Group](#) permissions.

### Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The [Manage Permission Roles](#) page displays.
2. Choose a permission role.  
The [Permissions](#) and [Assignments](#) tabs display.
3. Go to the [Assignments](#) tab.  
The assignment list of the permission role shows.
4. Choose the [Delete](#) button of the role assignment you want to delete.  
A double-confirmation message displays.
5. Choose [Delete](#).

### Results

You've successfully deleted the role assignment.

## 5.9 Bulk Activating and Deactivating Role Assignments

You can activate and deactivate multiple role assignments of a permission role at the same time.

### Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [Edit Role](#) and [View Group](#) permissions.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ►.  
The [Manage Permission Roles](#) page displays.
2. Choose a permission role.  
The [Permissions](#) and [Assignments](#) tabs display.
3. Go to the [Assignments](#) tab.  
The assignment list of the permission role shows.
4. Select the role assignments you want to activate or deactivate.

### Note

You can select up to 30 role assignments. This limit is to ensure optimal system performance, especially in systems that have enabled double-confirmation messages for large-size permission role or permission group changes. See *Enabling Double-Confirmation Messages for Large-Size Permission Changes* in *Related Information*.

5. Choose [Activate](#) or [Deactivate](#).

## Results

You've successfully activated or deactivated multiple role assignments of the permission role.

## Related Information

[Enabling Double-Confirmation Messages for Large-Size Permission Changes \[page 13\]](#)

## 5.10 Searching, Sorting, and Filtering Role Assignments

If a permission role has many role assignments, you can search, sort, and filter role assignments easily.

## Prerequisites

You are in the [Manage Role-Based Permission Access](#) list and assigned the [View Role](#) and [View Group](#) permissions.

## Procedure

1. Go to  [Admin Center](#) > [Manage Permission Roles](#) .

The [Manage Permission Roles](#) page displays.

2. Choose a permission role.

The [Permissions](#) and [Assignments](#) tabs display.

3. Go to the [Assignments](#) tab.

The assignment list of the permission role shows.

4. Use the search box, the  [Sort](#) icon, or the  [Filter](#) icon on the [Assignments](#) tab to narrow down your search.

Function	Description
<b>Search</b>	In the search box, you can enter a role assignment ID, name, or description. Note that if you search by assignment ID, the search result is a strict match.
<b>Sort</b>	<p>You can sort role assignments by <a href="#">ID</a>, <a href="#">Name</a>, or <a href="#">Last Modified</a> in ascending or descending order.</p> <ul style="list-style-type: none"><li>• Choose <a href="#">OK</a> to apply your sorting criteria.</li><li>• Choose <a href="#">Reset</a> on the upper right hand of the popup to reset your changes.</li><li>• Choose <a href="#">Close</a> to close the popup without applying your sorting criteria to the role assignment table.</li></ul>
<b>Filter</b>	You can filter role assignments by role assignment ID, name, description, status, last modified date, access population, and target population.

### Note

For [Permission Group Name](#) field in both the [Access Population](#) and [Target Population](#) sections, you can either choose to enter a group name, or select the [Everyone](#) option. If you enter a group name and also select [Everyone](#), the system returns results matching [Everyone](#) and the group name you entered.

- Choose [OK](#) to apply your filtering criteria.
- Choose [Reset](#) on the upper right hand of the popup to reset your changes.
- Choose [Close](#) to close the popup without applying your filtering criteria to the role assignment table.

## 5.11 Comparing Two Change History Records of a Permission Role

You can check the change history of a permission role. You can also compare two versions of a permission role to check which permissions or role assignments were added or removed.

## Context

When you add or remove permissions or role assignments of a permission role, a change record of the permission role is created.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ► [\[select a permission role\]](#) ► [View History](#) ►. Or, you can go into the role details page and choose the [View History](#) button.

The role history page displays. There are two tabs, [Role](#) and [Role Assignment](#), in this page.

2. Go to the [Role](#) tab.
3. Select two records from the role history list.
4. Choose [Compare](#).

## Results

Changes between the two versions are highlighted in the [Permissions](#) and [Assignments](#) subtabs. The strikethrough texts highlighted in red are removed permissions or assignments, and the underlined texts highlighted in green are newly added permissions or assignments.

### Note

*Comparison of MDF permissions is not supported.*

### Note

The [Assignments](#) subtab displays only the ID, the latest name and the latest description of a role assignment. To view more changed details of a role assignment, such as access population, target population, and target criteria, you can go to the [Role Assignment](#) tab.

## Next Steps

- Choose [Show All](#) to see all the permission details and assignments, changed or not.
- Choose [Show Difference](#) to see only the changed permissions and assignments.

## Related Information

[Comparing Two Change History Records of A Role Assignment \[page 45\]](#)

## 5.12 Comparing Two Change History Records of A Role Assignment

You can check the change history of a role assignment. You can also compare two versions of a role assignment to view the changed details.

### Context

When you add, remove, or edit a role assignment for a permission role, a change record of the role assignment is created.

### Procedure

1. Go to ► [Admin Center](#) ► [Manage Permission Roles](#) ► [\[select a permission role\]](#) ► [View History](#) ►. Or, you can go into the role details page and choose the [View History](#) button.  
The role history page displays. There are two tabs, [Role](#) and [Role Assignment](#), in this page.
2. Go to the [Role Assignment](#) tab.
3. Select a role assignment from the [Role Assignment](#) dropdown.  
A list of change records appears for the selected role assignment.
4. Select two records from the role assignment history list.
5. Choose [Compare](#).

### Results

Changes between the two versions are highlighted, including the changes in access population, target population, target criteria, data blocking, and tree security.

The strikethrough texts highlighted in red indicates removed details. The underlined texts highlighted in green are newly added details.

#### ❗ Note

Comparison of MDF permissions in [Target Criteria](#), [Data Blocking](#), and [Tree Security](#) is not supported.

### Next Steps

- Choose [Show All](#) to see all details about the role assignment, changed or not.

- Choose [Show Difference](#) to see only the changed details of the role assignment.

## 5.13 RBP Troubleshooting

You can use [RBP Troubleshooting](#) to better prevent, diagnose, and fix RBP issues.

Here are the details of the [RBP Troubleshooting](#):

- [User Role and Permission Search](#) allows you to search for and compare permission roles and user permissions. You're able to search for the roles and permissions of a single user. Alternatively, you can search for and compare the roles and permissions of two users.

### Note

The system supports searching for employees, external learners, and onboardees. It also supports MDF permissions.

- [Compare Roles](#) allows you to search for permissions of a role, or compare the permissions of two roles.

### 5.13.1 Searching User Roles and Permissions

You can use the [User Role and Permission Search](#) tab of the [RBP Troubleshooting](#) to know the permission roles and permissions of a user, or compare search and compare the roles and permissions of two users.

## Prerequisites

You have at least RBP administrator [View Role](#) and [View Group](#) access.

## Procedure

1. Go to ► [Admin Center](#) ► [RBP Troubleshooting](#) ►.
2. Go to the [User Role and Permission Search](#) tab.
3. Input users in the access user field.  
Input a single user into the [Access User 1](#) field to search for that user's permissions and roles. Input users into both the [Access User 1](#) and [Access User 2](#) fields to compare the permissions and roles of the two users.
4. Choose [Search](#).

## Results

Permissions and roles of the user or users are displayed in the [Result](#) table. You can click role names to check role details.

## Next Steps

If you are comparing permissions and roles of two users, you have two options to view the results.

- Choose [Show All](#) to see all permissions and roles of the two users.
- Choose [Show Difference](#) to see only the different permissions and roles of the two users.

## 5.13.2 Comparing Roles

You can use the [Compare Roles](#) tab of the [RBP Troubleshooting](#) to know the permissions in a role, or compare permissions of two roles.

## Prerequisites

You have at least RBP administrator [View Role](#) and [View Group](#) access.

## Procedure

1. Go to ► [Admin Center](#) ► [RBP Troubleshooting](#) ►.
2. Go to [Compare Roles](#) tab.
3. Select roles in the search fields.  
Input a single role into the [Role 1](#) field to search for permissions of the role. Input roles into both the [Role 1](#) and [Role 2](#) fields to compare the permissions of the two roles.
4. Choose [Search](#).

## Results

Permissions of the role or roles are displayed in the [Result](#) table.

## Next Steps

If you are comparing two roles, you have two options to view the results.

- Choose [Show All](#) to see all permissions of the two roles.
- Choose [Show Difference](#) to see only the different permissions of the two roles.



## 6 Recommendations and Leading Practices

You can find recommendations and leading practices of planning RBP setup for customers.

### 6.1 General Leading Practices for RBP

When planning the RBP setup for the customer, it's crucial that you keep the impact on system performance and the maintenance effort in mind. In addition, it's crucial to agree on a governance process for further changes. We recommend the following:

---

#### Organize Permission Groups and Permission Roles

##### **Start with generic roles**

We recommend starting with the most generic role such as an "All Employees Role", and casting the net as wide as possible to include all permissions that should be given to everyone. For example, in this role include all of the publicly viewable fields in the Employee Profile.

---

##### **Avoid redundancy**

For additional roles, work on an exception basis and include only the unique extra permissions that the role should have beyond other roles. This practice helps reduce the number of roles in the system, which will both be easier to maintain, and will help improve system performance.

---

##### **No overlap between roles**

Users shouldn't receive the same permission from different roles. If users have multiple roles that grant the same permissions, it can slow down the system's response time for them.


---

	<p><b>Reduce the complexity and number of groups and roles</b></p> <p>In general, keep the number of groups and roles as low as possible. This approach reduces maintenance efforts and eases troubleshooting in case of issues. Remember, you can grant a role to multiple groups, so there's no need to duplicate roles just to assign them to different groups.</p> <p>For example, dynamic groups (with people pools using HRIS elements) and roles with level-up and level-down settings increase complexity. Systems with many complex groups and roles take longer for authorization configuration changes to take effect.</p>
Naming Conventions	<p>Agree on naming conventions for groups and roles to simplify maintenance, especially in large implementations. For groups, consider using prefixes like "Granted:" and "Target:".</p>
Meaningful Group Names, Role Names, and Role Descriptions	<p>Meaningful group and role names, along with clear role descriptions, help customers identify the correct groups and roles during maintenance and troubleshooting. Role descriptions should clearly state the purpose of the role, rather than just repeating the role name. Encourage customers to maintain a change log in the role description field. This log should include the change, the date, and who made and approved the change. While the "View change history" function provides this information, checking the description field is quicker.</p>
Governance	<p>It's crucial for customers to define governance on RBP early in the project. They should establish how to handle changes to RBP: Who can make changes? How can someone request a change? Who needs to review and decide on the change? These questions are especially important in large organizations where departments often operate independently. If one department requests a change, it might impact others, so all parties need to agree.</p> <p>Some customers may want to introduce the concept of separation of duties for administering RBP. The "Special Requirement: Separation of Duties in RBP Administration" topic describes how to achieve this.</p>
Run the RBP Check Tool	<p>The Check Tool section in this guide offers information on running RBP checks and maintaining good system performance. This tool generates a report that highlights all potential risks associated with specific RBP configuration settings.</p>

## RBP Guardrails

The RBP refresh framework for regular updates is fundamental for most customers.

- Total group number: fewer than 7,000 groups
- Role assignments associated with a role: 200 (We have a check tool for this.)
- Total role number: 30 roles
- Total role assignments: recommend not exceeding 6,000

If you have a complex system with many users that exceed the previous recommendations, contact SAP Technical Support. See details in <https://me.sap.com/notes/3545847> .

## Related Information

[Using the Check Tool to Solve Issues \[page 62\]](#)

## 6.2 Separating RBP Administration Duties

You may require the capability to separate duties such that one group of administrators can define the permission roles, while a different group of administrators can assign the roles to users. This requirement is also known as the “four eyes principle”, meaning that at least two persons (four eyes) are required in order for a permission to ultimately be assigned to a user.

### Context

Role-Based Permissions can allow for separation of duties by virtue of its ability to automatically assign a role to users based on attributes about the user. One group of administrators set up the roles and the attribute-based group definitions. Another group of administrators manages the employee profile data by assigning specific values to individual users for a specific custom field. When the employees' values match a role assignment, the role is granted to the user.

### Procedure

1. You create a Global Security Administrators group which has access to RBP. These global security administrators define the roles and create groups based on values available in the custom field "Access Rights". They assign the roles to the appropriate groups

2. You create a separate group of administrators and allow them to edit the values in the user profile for the custom field "Access Rights". These administrators do not need access to RBP. Instead, the administrators control the assignment of users via criteria defined in employee profile.

## 7 Preparing the Instance

### 7.1 Ensuring that Test Instance and Production Instance are In Sync

When you implement and configure RBP, you do this first on the test instance. Only after successful testing you copy the configuration to the production instance. For this reason, it is very important that test instance and production instance contain the same data.

To make sure that test and production instance are in sync:

- Request the client to refresh the employee data file in the test instance with production data.
- Ask the client if there are data changes coming that would affect the ability to permission correctly (for example organizational restructures). If so, they need to have that data available in the test instance if they want to permission it now. In addition, the data will need to be in the production instance by the time the permissions are ready to be copied to the production instance.
- Compare the Provisioning to see if there are more features enabled in the production instance than in the test instance. Compare the data models to make sure the instances match. You can ignore the permissions sections of the data models at this point which do not apply in RBP systems. Only check for data elements.

#### → Remember

As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

Depending on how much is out of sync, you may advise the client to have the production instance copied to the test instance (possibly using the instance sync tool) or you may be able to work around it.

If, for data protection reasons, it is not possible to update the test instance with productive data, you must at least make sure that all elements actually exist in the test instance. Otherwise it is not possible to fully implement RBP on the test instance so that it can then be copied to the production instance.

### 7.2 Configuring Fields for Setting up Permission Groups

When you create groups, you select the group members according to specific selection criteria. You can configure which selection criteria should show up on the screen where you define permission groups.

## 7.2.1 Standard Fields Available to Use as Filters in Permission Groups

The fields that can be used when defining permission groups are the standard fields listed below, as well as any of the HRIS fields when Employee Central is enabled.

To add the fields as filters in dynamic permission groups, use either Succession Data Model or Business Configuration UI. For more information, see [Related Information](#).

Standard Fields allowed as filters in Permission Groups

benchStrength	custom12	keyPosition
citizenship	custom13	location
city	custom14	married
country	custom15	minority
custom01	dateOfBirth	nationality
custom02	dateOfPosition	newToPosition
custom03	department	reasonForLeaving
custom04	division	riskOfLoss
custom05	ethnicity	state
custom06	External Source Channel (Only available if Learning is enabled.)	Team View
custom07		timeZone
custom08	futureLeader	title
custom09	gender	username
custom10	hireDate	zipCode
custom11	impactOfLoss	jobLevel
	jobCode	

---

### Related Information

[Creating and Using Dynamic Group Filters in Business Configuration UI](#)

[How Do You Specify Which Fields to Use? \[page 55\]](#)

[Configuring Standard and HRIS Elements for Dynamic Group Filters](#)

## 7.2.2 How Do You Specify Which Fields to Use?

You can specify which fields appear for defining permission groups. You can do so by editing the `<permission-group-filter>` subelement of the `<dg-filters>` element in the Succession Data Model. The `<dg-filters>` tag means “Dynamic Groups Filters”. Here is an example XML snippet and a description of these XML tags.

### ⚠ Caution

If you don't specify any fields in the `<dg-filters>` XML configuration, then RBP defaults to display all of the possible fields listed in [Standard Fields Available to Use as Filters in Permission Groups \[page 54\]](#). By specifying the fields, you replace the standard filters with your own list. If you specify an unsupported field with `<standard-element-ref>`, the field doesn't display in the RBP Permission Groups UI.

### → Recommendation

For large organizations (above 100,000 employees), it helps performance to limit the number of fields used to define groups. At the least, if a customer doesn't intend to use all available fields, remove those fields that you're sure aren't needed.

Example XML snippet:

```
<dg-filters>
  <my-filter>
    <standard-element-ref refid="department"/>
    <standard-element-ref refid="location"/>
  </my-filter>
  <permission-group-filter>
    <standard-element-ref refid="division"/>
    <standard-element-ref refid="custom05"/>
    <standard-element-ref refid="custom06"/>
    <standard-element-ref refid="custom01"/>
  </permission-group-filter>
</dg-filters>
```

The XML tags above work as follows:

The `<dg-filters>` tag has two subtags, `<my-filter>` and `<permission-group-filter>`:

- `<permission-group-filter>`  
Used to specify the fields that can appear in the RBP Permission Groups UI.  
You specify fields here by adding `<standard-element-ref>` or `<hris-element-ref>` sub elements (if Employee Central is enabled). In Employee Central, the allowable HRIS fields are documented here at: [Implementing Employee Central Core](#).
- `<my-filter>`  
Used to specify the fields used in the My Groups feature, which is a separate, unrelated feature. Contact your SAP SuccessFactors representative for more information.

# 8 RBP Reports

## 8.1 RBP Table Reports

Use Table reports to understand an RBP configuration.

Reports help to troubleshoot and understand the permissions that have been configured. RBP Table reports are an aggregate of all the RBP data in your system. You can access this information and share it using the following output formats: PDF, Excel, PPT, and CSV.

- RBP User to Role Report
- RBP Permission to User Report
- RBP User to Group Report
- Permission Roles Report

### Related Information

[Using Table Reports](#)

## 8.2 Dynamic Group Definition Reports

The *Dynamic Group Definition Report* displays the *Include* and *Exclude People Pool* criteria that you've used to define your dynamic permission groups.

In addition to *People Pool* data, the report displays your dynamic group names, each groups total number of members, and the last modified date. When you run the report, a CSV file is created in the destination folder. You can use this CSV file to extract specific information regarding your permission group definition.

Since the *Dynamic Group Definition Report* displays the dynamic permission group criteria that's defined in your RBP implementation, you may find it useful to run this report for frequent compliance needs or for more frequent edits to your group creation criteria.

When you select to activate the *Enable Dynamic Group Definition Report*, this action begins the process of syncing the Employee Central (EC) data that you use to define your permission groups. If you use EC data for permission group definition, any changes you make to your data will take effect the following day, for reporting, after the data has completed the sync process.

#### → Tip

The Employee Central data sync occurs everyday, therefore, if you do not plan to run this report daily, you may consider disabling the Dynamic Group Definition Report until you need to run a report. Doing so ensures that you are not using your resources, daily, to sync your EC data.



## 8.3 Reporting on Dynamic Group Definition

The report for *Dynamic Group Definition* is accessible through the *Integration Center*.

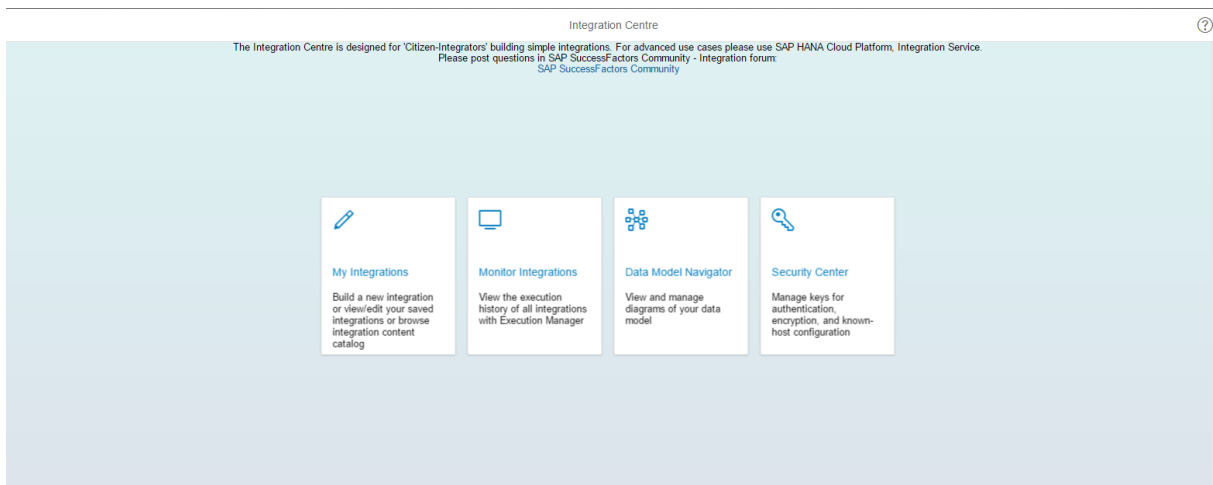
### Context

The *Enable Dynamic Group Definition Report* must be enabled by selecting it from the *Platform Feature Settings* page. To enable this report, log in as a Super Admin. Go to the ► *Admin Center* ► *Platform Feature Settings* ► page.

### Procedure

1. From the *Admin Center*, search for **Integration Center**.
2. On the landing page of the *Integration Center*, click *My Integrations*.

On the *My Integrations* page, you'll see an overview of existing integrations from the *My Integrations* page. In addition to the *Name* and *Description*, *Last Modified* and *Actions* column, it now includes information from the *Execution Manager* such as error/warning/success icons along with subtotals and a *Last Run* column with runtime and version. Clicking on the last run date opens the latest job log in the *Execution Manager*. The *My Integrations* page also includes a *Refresh* button so that you can get the latest status of the job.



Landing Page

3. Click ► *+Create* ► *Scheduled Simple File Output Integration* ►.
4. In the *Search Entity* field, search for **DynamicGroupDefinition**.
5. Select the **DynamicGroupDefinition** entity and select the *People Pool* criteria that you want to include in the report.




When you run the report, the fields you select will populate the spreadsheet.

6. Select to enable *group (to DynamicGroup)* if you want to limit the report to group entity information.
7. Click *Select*.


8. From the *Options* tab:
  - a. Enter a name for your integration.
  - a. Select **csv** for the *Output File Type*.
  - b. Select **Simple Header** in the *Header Type*.

9. Click *Next*.

You'll see the *Configure Fields* screen.

10. Add fields to your report by selecting  **+Add**  **+Add Field** , from the *Configure Fields* screen.
11. Select *Advanced Sorting* and then select the field you want to sort your report by from the screen, from the *Filter and Sort*.
12. Click *Next*.
13. Configure the following *Destination Settings*:

Field	Description
<b>SFTP Server Host Address</b>	Enter the address of the SFTP server, the folder and file information, and the credentials needed to write the file to the destination folder
<b>Port</b>	<p>You can edit the SFTP port. By default, the port is set to 22. You should change it only if your security requirements make a different SFTP port necessary. The port must be between 0 and 65535.</p> <p>Only encrypted SFTP/port 22 file transfer protocol is supported. Integration Center does not support data to be transmitted on the public internet FTP/port 21 channel because this would expose your sensitive data to the public internet.</p> <div> <p>→ Recommendation</p> <p>Work with your corporate IT to allow traffic only from the SAP SuccessFactors data center internet (IP) address range. This technique prevents access from any location other than locations whose addresses are included in your company's allowlist. To be able to connect to your allowlisted server, your corporate IT needs to add the SAP SuccessFactors data center IP address to the allowlist.</p> </div>
<b>SFTP User Name</b>	Your SFTP server must be available from the public internet; otherwise, it will not be available from the SAP SuccessFactors data centers. If your firewall blocks all external access (or allowlisted access that does not include the SAP SuccessFactors IP addresses), your SFTP server will not be available.
<b>SFTP Password</b>	The <i>SFTP Password</i> field supports alphanumeric characters that are case-sensitive. This field does not support special character (+) and non-ascii characters.
<b>File Name Prefix</b>	Template to be used for the file name, including the file extension.

Field	Description
	<div>  <b>Note</b>            Integration Center does not support blank space and any other special character other than '_' (underscore) in the file name.         </div>
<b>File Extension</b>	Select CSV as the extension for the file, excluding the period.
<b>File Folder</b>	Enter the name of the folder to which the file is written.

14. Pick a frequency for your report, from the [Scheduling](#) screen.

15. Click [Set Schedule](#), from the [Review and Run](#) screen.

You can review each component that you've configured for the report.

## Results

When the report is completed, the CSV file will be available in the file location that you specified. For further information about each step in the [Integration Center](#) when running the [Dynamic Group Definition Report](#), review the Integration Center document linked in the Related Information section.

## Related Information

[Integration Center](#)

## 9 Transport Role-Based Permissions Configurations to the Production Instance

After completing the tests and resolving all issues, transport the RBP configurations to the production instance.

Access the [Configuration Transport Center](#) tool in the [Admin Center](#). This tool allows you to copy permission groups and permission roles across data centers. See details in *Related Information*.

### Preparation for Transporting Role-Based Permissions Groups and Roles

Ensure the following data match between source and target instances:

- RBP Permission Roles
- RBP Permission Groups
- MDF Picklists
- MDF Object Definitions
- MDF Rules
- Data Model

### Related Information

[Configuration Transport Center](#)

### 9.1 Important Tips for Copying Groups

Here are a few important tips for copying permission groups:

- The user (username) who created the group in the source instance must also be a user in the target instance for the sync of the groups to be successful.
- You are asked if you want to overwrite the existing groups in the target instance. If you choose not to overwrite and there is a group in the target instance with the same name, the group will not copy to target instance.

## 9.2 Important Tips for Copying Roles




Here are a few important tips for coping permission roles:

- To successfully copy roles, you first have to sync all attached groups with the target instance.
- Templates, families, roles, picklists and further data associated with the roles in the source instance need to exist in the target instance for roles to be successful

# 10 Using the Check Tool to Solve Issues


Get an overview of potential problems and errors in your configuration that you can try to solve yourself before you contact Technical Support about an issue.

## Prerequisites

- You've enabled the Metadata Framework.
- You have the following  [Administrator Permissions](#)  [Check Tool](#)  permissions:
  - [Access Check Tool](#) authorizes users to access the tool.
  - [Allow Configuration Export](#) authorizes users to attach configuration information to a ticket.
  - [Allow Check Tool Quick Fix](#) authorizes users to run quick fixes for the checks that have this feature. A quick fix can be used to immediately correct any issues found by that check.

For more information about role-based permissions, refer to [List of Role-Based Permissions](#).

### → Tip

Refer to [Guided Answers for the Check Tool](#)  for a guided navigation through the available check tool checks and more information on each check.

## Context

The check tool provides an overview of the issues found in the system. New checks that are being added in a new release go through a first initial run to return a result. After the initial run, checks are run on a regular basis (at least monthly). We recommend you open the check tool after you upgrade to a new release to see whether issues have been found by new checks.

In addition to these runs performed by the system, you can also run individual checks after you make changes to the system, for example, after updating data models or picklists. For more information, refer to the application-specific documentation.

## Procedure

1. Go to  [Admin Center](#)  [Check Tool](#) .

The [Check Tool](#) page opens displaying the results of the first tab **System Health**.

2. Depending on the check type of the check you're interested in, select the corresponding tab.

Tab	Description
<a href="#">System Health</a>	<p>Displays configuration checks that have returned errors or warnings after the last run. We recommend you solve these in a timely manner.</p> <p>To display all checks, select all result types in the <a href="#">Result Type</a> search filter and select <a href="#">Go</a>.</p>
<a href="#">Migration</a>	<p>Displays the migrations that are still pending, either because the check tool couldn't automatically migrate all issues or because new issues have been found after the last run. We recommend you solve these in a timely manner.</p> <p>To display all checks, turn on the <a href="#">Show completed migrations also</a> search filter and select <a href="#">Go</a>.</p>
<a href="#">Validation</a>	<p>Displays a list of all validation checks.</p> <div> <p><b>Note</b></p> <p>Validation checks require one or more parameters for execution, therefore we can't run these checks automatically. You need to enter input parameters and run the corresponding check manually to get results.</p> </div>

3. To solve a check that returned issues, select it.

The detail view opens to the right side of the screen with more information on the check and on how to solve the issue.

4. Evaluate the results and resolve the issues. If the check provides a quick fix that you can use to immediately correct issues found during a check run, select the [Quick Fix](#) button.
5. If you encounter an error you can't resolve, contact Technical Support by creating a ticket.

## Next Steps

To verify that you've solved the underlying issue, select the checkbox for the corresponding checks and choose [Run Checks](#). You can also wait until the next automatic run to see if the issue has been solved.

### Note

If the check you selected requires one or more prechecks (checks that need to be run successfully first), the prechecks are run first even if you haven't selected them.

## Related Information

[Running Checks \[page 64\]](#)

## 10.1 Benefits of the Check Tool

The SAP SuccessFactors check tool helps you identify and resolve issues when your system doesn't work as you expect.

If your SAP SuccessFactors applications are behaving in unexpected ways, it is likely that it has a configuration or data conflict: you have some data that is inconsistent or a configuration error. The check tool quickly identifies these types of problems so that you can avoid support tickets. You might still need to create a support ticket if the problem is severe, but even in severe cases, the check tool can save you time because it can export the results of the check and your configuration for Technical Support. The support engineer, therefore, can identify the issue more quickly.

When you open the check tool, you see:

- A list of issues in your configuration or data and the severity of each issue.
- A solution or recommendation to address the issue.

## 10.2 Running Checks

Trigger the execution of individual checks to find potential issues in the system, or to check if an issue has been solved in the meantime.

### Prerequisites

- You've enabled the Metadata Framework.
- You have the following [Administrator Permissions](#) > [Check Tool](#) permissions:
  - [Access Check Tool](#)
  - [Allow Configuration Export](#)
  - [Allow Check Tool Quick Fix](#)

### Context

In addition to the job runs performed automatically by the system, you can also run individual checks. For example:

- You want to check whether the issue has been solved.
- You want to run a check as a prerequisite or post-step of a task. For example, you made changes to the system (such as updating data models or picklists), and you want to verify that your changes didn't cause any new issues. For more information, refer to the application-specific documentation.



- Validation checks need to be run manually as they require input parameters.

## Procedure

1. Go to ► [Admin Center](#) ► [Check Tool](#) ►.

The [Check Tool](#) page opens displaying the results of the first tab [System Health](#).

2. Depending on the check type of the check you want to perform, select the corresponding tab.

A list of checks is displayed in the results table according to the predefined selection criteria.

3. **Optional:** If the check you're searching for is not listed in the results table, adjust the selection criteria and choose [Go](#).

You get a list of checks that fulfill the selection criteria you've entered.

4. Select the corresponding checks, and choose [Run Checks](#) from the top right of the results table.

### ⓘ Note

Please note that, for checks on the [Validation](#) tab, you can only select one row at a time. Execution of multiple checks at once is not possible.

Also, for validation checks you need to enter the required input parameters when running a check.

### ⓘ Note

If the check you selected requires one or more prechecks (checks that need to be run successfully first), the prechecks are run first even if you haven't selected them.

The [Results](#) column displays any issues found.

## Next Steps

Investigate and solve the underlying issue.

## 10.3 Check Types

Overview of the different check types and their purpose.

The check type groups those checks that have a common purpose. On the [Check Tool](#) page, each tab represents a check type.

Check Type	Description	Automatic Job Runs
System Health	<p>Checks that run without parameters and check configuration and data issues that need to be fixed.</p> <p>The predefined selection criteria displays only those that have returned errors or warnings after the last run. We recommend you solve these in a timely manner.</p> <p>To display all checks, select all result types in the <b>Result Type</b> search filter and select <a href="#">Go</a>.</p>	<ul style="list-style-type: none"> <li>• Automatic initial run at the beginning of a new release</li> <li>• Periodic runs (usually monthly)</li> </ul>
Migration	<p>Checks that perform an automatic migration of features.</p> <p>When you open the page, only pending migrations are displayed. To display also the completed migrations, turn on the <a href="#">Show completed migrations also</a> search filter and select <a href="#">Go</a>.</p>	<ul style="list-style-type: none"> <li>• Automatic initial run at the beginning of a new release</li> <li>• Periodic runs (usually monthly)</li> </ul>
Validation	<p>Checks which need one or more parameters for execution, for example:</p> <ul style="list-style-type: none"> <li>• A specific template</li> <li>• A specific user</li> <li>• A specific time frame</li> </ul> <p>Validation checks can be triggered by single selection and choosing the <a href="#">Run</a> button. A popup appears with input fields for the parameters. Execution of multiple checks at once is not possible.</p>	Only triggered through user

## 10.4 Check Results

After you run checks in the check tool, it returns the results of the checks so that you can resolve the issues found.

The results of a check are displayed in the [Result](#) column. If you run the checks multiple times to see how you're resolving issues, you can select a previous result from the [History](#) dropdown list.

### Note

To display the [History](#) dropdown list, select a check. On the details screen that opens on the right side of the page, expand the header. The [History](#) dropdown list is directly below the check title.

## Possible Results of Check Tool

Result	Action
No issues found	If the tool can't find issues, you see a green check mark in the <a href="#">Result</a> column.
Issues found	<p>If the tool finds issues, it reports the number of issues and a yellow warning icon or a red alarm icon.</p> <ul style="list-style-type: none"><li>• The yellow icon indicates a low severity issue. The system proposes a solution.</li><li>• The red icon indicates a high severity issue. You must take action, which could include creating a support ticket.</li></ul>
Pending migrations	If the tool finds pending migrations that need to be completed by the user, you can see a yellow warning icon or a red alarm icon in the <a href="#">Status</a> column on the <a href="#">Migration</a> tab.
Completed	If the tool finds no issues with migration, or the migration has already been completed, you see a green check mark in the <a href="#">Status</a> column on the <a href="#">Migration</a> tab.

### Note

- Select the [Export Results](#) button to download the check results. Ensure you run the check before exporting the check results. If not you can view only the first 100 check results.
- The downloaded check result table can display a maximum number of 10,000 rows.

## Related Information

[Creating Technical Support Tickets from the Check Tool \[page 67\]](#)

## 10.5 Creating Technical Support Tickets from the Check Tool

When the check tool reports a serious issue that you can't solve, you might need to contact Technical Support. You can create a support ticket from within the check tool.

### Prerequisites

You've run the check tool. You can find the check tool by going to ► [Admin Center](#) ► [Check Tool](#) ►. You create the ticket from the details page of the tool.

## Procedure

1. Select the check you can't solve.

The detail view opens to the right side of the screen with more information on the check and on how to solve the issue.

2. On the [Result](#) tab, scroll down to the results table to look for the errors you want to report on.

You usually contact Technical Support for high severity issues not low severity issues.

3. On the [Check Information](#) tab, under [Need Assistance?](#), copy the component ID.

For example, LOD-SF-EC is the component ID for Employee Central.

4. Create a customer case in the relevant category.
5. When you create the ticket, paste the component ID into the ticket.

## 10.6 Using the Quick Fix Feature

The check tool includes a quick fix feature that you can use to immediately correct issues found during a check run.

### Prerequisites

The checks you want to solve with a quick fix have run and provide a check result with error or warning.

## Procedure

1. Go to ► [Admin Center](#) ► [Check Tool](#) .

The **Check Tool** page opens.

2. Select the check you want to fix.

The details screen opens on the right side of the page with more information about the check. If the check includes a quick fix, the [Quick Fix](#) button is displayed on the [Result](#) tab, under [Proposed Solution](#).

3. Choose [Quick Fix](#) to start fixing the issue.

A third screen opens to the right side, with step 1, called [Select Correction](#), that shows one or more corrections for the issue.

4. Select the correction you want to carry out and choose [Step 2](#) to proceed to [Final Approval](#).

In the [Final Approval](#) step, you can opt to change your mind and not carry out the fix.

5. If you want to proceed, choose [Step 3](#).

The system confirms that the fix is now running.

6. Choose [Close](#) to complete the procedure.

After a short time, the system runs the check again to verify that the fix has run correctly.

## 10.7 Exports

### 10.7.1 Exporting Configuration Information

Export the configuration information from your system and attach it to the Support ticket created from the check tool. This information can help Support identify the issue of a check you can't solve yourself.

#### Prerequisites

You have the [Administrator Permissions](#) > [Check Tool](#) > [Allow Configuration Export](#) permission.

#### Context

##### ⚠ Restriction

Export of configuration information is supported only in the following applications:

- Payroll Information
- Position Management
- Time Off
- Time Sheet

#### Procedure

1. Go to [Admin Center](#) > [Check Tool](#).

The [Check Tool](#) page opens with a list of all applications for which you can use the check tool..

2. Select the corresponding application.

If the application has the export configuration feature enabled, you can see an information message at the bottom of the page with a link.

3. Choose the [Export Configuration](#) link in the information message.

## Results

The system downloads a file with the configuration information for the application you've selected.

## Next Steps

Attach the downloaded file to the Support ticket you created from the check tool.

## 10.7.2 Exporting Check Results

After you run checks in the check tool, you can export the results.

### Context

- Ensure you run the check before exporting the check results. If you don't do this, you can view only the first 100 check results.
- The downloaded check result table can display a maximum number of 10,000 rows.

### Procedure

On the [Result](#) tab, select the [Export Results](#) button to download the check results.

## 10.7.3 Exporting a List of All Checks

Get an overview of all checks available in the system by exporting a CSV file.

### Procedure

1. Go to [Admin Center](#) > [Check Tool](#) .

The [Check Tool](#) page opens.

2. In the top-right corner, select [Export all checks](#).

A CSV file with all checks available in the system is downloaded, including check descriptions and application area.

#### 📌 Note

The list includes also checks that you can't access from the user interface if you don't have the corresponding applications set up, or if you lack the required permissions.

# 11 Testing Your RBP Configuration

## 11.1 Does the Everyone Group Exist?

The [CheckEveryoneGroup](#) test validates that the Everyone group exists.

The Everyone group includes all employees in your system and is automatically created when your super admin enables RBP. If the Everyone group isn't created in your system, you might encounter errors when trying to create groups for other users. The [CheckEveryoneGroup](#) test confirms that the Everyone group exists.

When you run this check and the result is true, the [Result](#) section of the Check Tool displays the names of the [User Types](#) that don't have the Everyone group. These names may include either the Employee or External Learner user types.

Check ID	Check Name	Recommended Solution
CheckEveryoneGroup	Verify if the Everyone Group Exists	When you enable Role-Based Permissions (RBP) in your system, it automatically creates the Everyone group. To re-trigger this automatic creation, disable RBP and then enable it again.

## 11.2 Do Roles Exist Without Groups or Users?

The [CheckRoleRuleAccessGroupUser](#) test validates if your system contains roles that exist without access permission users or groups.

In your system, each role must contain access users or groups. When users or groups haven't been assigned to a role, runtime exceptions occur. These exceptions can happen whenever the system tries to run access permissions.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the names of the roles that don't have access users or groups assigned to the role.



Check ID	Check Name	Recommended Solution
CheckRoleRuleAccessGroupUser	Verify if Roles Exist that are not Associated with Access Permission Groups or Users	<p>Choose any of the following solutions if you have errors in your system after running this check.</p> <p>Associate Permission groups or users that you want to grant this permission role to.</p> <p>Deactivate the role assignments that aren't currently associated with any permission groups or users.</p> <p>Delete any role assignments that aren't associated with permission groups or users.</p>

## 11.3 Do Roles Exist Without Target Population?

The [CheckRoleRuleTargetGroup](#) test validates if there are any roles in your system where target population hasn't been defined.

Roles in your system include some permissions that need a defined target population and others that don't. For permissions needing a target group, you must define one for the role. If you don't, you might encounter errors when the system tries to calculate target group permissions.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the names of the roles that do not have target groups assigned to the role.

Check ID	Check Name	Recommended Solution
CheckRoleRuleTargetGroup	Verify if Roles Exist Without Target Population Defined.	<p>Choose any of the following proposed recommendations for the roles listed in Results section:</p> <p>Specify the target population for whom granted users have permission to access.</p> <p>Deactivate the role assignments that aren't currently associated with any target population.</p> <p>Delete the role assignments that aren't associated with a target population.</p>

## 11.4 Do Group Names Exceed 1000 Characters?

The [CheckAccessGroupNameLength](#) test validates if the total length of access group names that are associated with a rule exceeds 1000 characters.

When associating role assignments with roles, ensure that each role assignment doesn't exceed 1,000 characters. A role assignment can include several groups, and a role can have multiple role assignments. However, the total

character count for group names in each role assignment must stay under 1,000. Group names exceeding this limit might cause errors or slow down your system.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the names of the roles that contain 1000 or more characters in total length.

Check ID	Check Name	Recommended Solution
CheckAccessGroupNameLength	Verify if the Access Group Names Associated with a Rule Exceeds 1000 Characters.	<p>Choose any of the following solutions if you have errors in your system after running this check.</p> <p>For each role in the Results section, review the highlighted role assignments.</p> <p>Create a new access group that includes all the access groups associated with a role assignment. Or condense the current access groups into fewer access groups.</p> <p>Replace the current access groups with the newly created access group.</p> <p>You can also rename the associated access groups so that the total number of characters doesn't exceed 1000.</p>

## 11.5 Do Target Group Names Exceed 1000 Characters?

The [CheckTargetGroupNameLength](#) test validates if the total length of target group names that are associated with a role assignment exceeds 1000 characters for a role.

When you associate role assignments to your roles, it's important that you don't exceed 1000 characters for each role assignment. While a role assignment can contain several groups and a role can contain several role assignments, each role assignment must not contain 1000 characters or more target group name characters, meaning the names of your target groups for each role assignment must not exceed 1000 characters. Target groups with 1000 or more characters may cause errors in your system.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the names of the roles that contain target group names with 1000 or more characters in total length.

Check ID	Check Name	Recommended Solution
CheckTargetGroupNameLength	Verify if the target group names associated with a rule exceeds 1000 characters	<p>Choose any of the following solutions if you have errors in your system after running this check.</p> <p>Create a new target group that includes all the target groups associated with a role assignment.</p> <p>Or condense the current target groups into fewer target groups.</p> <p>Replace the current target groups with the newly created target group.</p> <p>You can also rename the associated target groups so that the total number of characters doesn't exceed 1000.</p>

## 11.6 Does a User Have the Same Permission More Than 30 Times?

The [CheckUserPermissions](#) test verifies if there are employees in your system who have been granted the same permission more than 30 times.

When employees in your system are granted with the same permission multiple times by granting them roles that contain duplicated permissions, it may cause your system some issues, such as system slowdowns or errors.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the user names, permission names, the number of times the user has been granted the permission, and the role names associated with the permission. Additionally, by clicking the user names, you can review more records that are associated with each user.

Check ID	Check Name	Recommended Solution
CheckUserPermissions	Verify if a user has been granted the same permission more than 30 times	<p>Execute any of the following solutions if you have errors in your system after running this check.</p> <ul style="list-style-type: none"> <li>• Determine roles defining the Permission Basic Roles first including the most common settings for all users. This is expected to be the Role Everyone, Employee, Manager, HR and Administrator. If a permission has been granted to everyone, it never needs to be repeated again in another role. A user in multiple groups gets the combined permissions of all groups they are a member of.</li> <li>• For additional roles, work on an exception basis and include only the unique extra permissions that the role should have beyond other roles.</li> <li>• Avoid Duplication of permissions across roles.</li> </ul>

## 11.7 Does a Role Have More Than 200 Rules?

The [CheckRulePerRole](#) test validates if there are more than 200 rules associated with a role.

Rules, or role assignments, are defined when you assign access groups and target groups to a role. While you might have several rules defined for one role, it's important to ensure that the number of rules for a role doesn't exceed 200. That means, ensure that each row that defines access and target groups doesn't exceed 200 rules. When defining group access rules for the roles in your system, it's most efficient to break up rules otherwise, you may experience issues in your system.

When you run this check, if the result is true, the [Result](#) section of the Check Tool displays the role name and the number of rules associated with the role.

Check ID	Check Name	Recommended Solution
CheckRulePerRole	Verify if the number of rules associated with a role exceeds 200	<p>Choose any of the following solutions if you have errors in your system after running this check.</p> <p>Minimize the number of rules by combining them into fewer role assignments and then re-associate to the role.</p> <p>In case you have specific needs and you are not able to combine the role assignments, split them in different new permission roles that do not exceed 50.</p>

## 11.8 Do All Permission Roles have Consistent Authorizations for Working with Business Rules?

The [PermissionRolesHaveConsistentAuthorizationsForRules](#) check validates if all permission roles have consistent authorizations for working with business rules.

Check ID	Check Name	Recommended Solution
PermissionRolesHaveConsistentAuthorizationsForRules	All Permission Roles have Consistent Authorizations for Working with Business Rules	<p>If you find the following error in your system after running this check:</p> <ul style="list-style-type: none"> <li>"We couldn't check the permission roles."</li> </ul> <p>go to <a href="#">Admin Center</a> &gt; <a href="#">Configure Object Definitions</a> and ensure that both <a href="#">Secured</a> and <a href="#">CREATE Respects Target Criteria</a> are set to <a href="#">Yes</a> for the rule object.</p> <p>Refer to <i>Permissions for Business Rules</i> in the Related Information section.</p>

Check ID	Check Name	Recommended Solution
		<p>If you find the following error in your system after running this check:</p> <ul style="list-style-type: none"> <li>"Metadata Framework permission "Configure Object permission" is not granted."</li> </ul> <p>select the role name in the result list. This takes you to the <a href="#">Manage Permission Roles</a> UI, where you can assign the <a href="#">Configure Business Rules</a> permission. Instead of clicking on a role name, you can also navigate go to <a href="#">Admin Center</a> &gt; <a href="#">Manage Permission Roles</a> &gt; <a href="#">Administrator Permissions</a> &gt; <a href="#">Metadata Framework</a> and assign the <a href="#">Configure Business Rules</a> permission. Refer to <i>Permissions for Business Rules</i> in the Related Information section on how to set up the permissions.</p> <hr/> <p>If you find the following errors in your system after running this check:</p> <ul style="list-style-type: none"> <li>"Neither the view nor the edit permission is configured for the rule object."</li> <li>"View/Edit permission is not correctly configured for the rule object." (For example, the user has only <a href="#">View Current</a> of the View permissions, or <a href="#">Correct</a> of the Edit permission.)</li> </ul> <p>select the role name in the result list. This takes you to the <a href="#">Manage Permission Roles</a> UI, where you can configure the permissions consistently. Alternatively, go to <a href="#">Admin Center</a> &gt; <a href="#">Manage Permission Roles</a>. Refer to <i>Permissions for Business Rules</i> in the Related Information section on how to set up the permissions.</p>

### Note

This check doesn't have a quick fix. The check runs asynchronously and might take some time until completion.

## Related Information

[Permissions for Business Rules](#)

# 12 Troubleshooting

## Context

If you find that users have access to applications or data they shouldn't have, we recommend the following steps:

## Procedure

1. Use [RBP Troubleshooting](#) tool to check how - through which role - the permission was granted to the employees.
2. If that does not clarify how or why they have that permission or creates concern about where else this permission is visible, then use the RBP Permission to User Report with the Single Permission Filter to validate what other groups have access to this permission.

## Related Information

[RBP Troubleshooting \[page 46\]](#)

[RBP Table Reports \[page 56\]](#)

## 12.1 How Do Permissions Update When User Information Changes?

Role-based permissions refresh periodically to propagate any changes to your dynamic groups or to the permission roles in your system. These changes occur when employees are hired, employees change departments, and during integration scenarios.

### What's the Refresh Framework?

When changes to your employees' information occur in your SAP SuccessFactors HCM suite such as, job title changes, hiring of new employees, or giving additional responsibilities to employees, your role-based permissions security platform runs an automated process that propagates these changes in your system. The changes affect



the permission roles that employees have access to and the permission groups they belong to. The Refresh Framework handles this automated process in your system. Depending on the size of your organization, you may have a high number of user changes or you could have a relatively low number of user changes in your system. The refresh framework uses two types of refresh jobs to handle these scenarios.

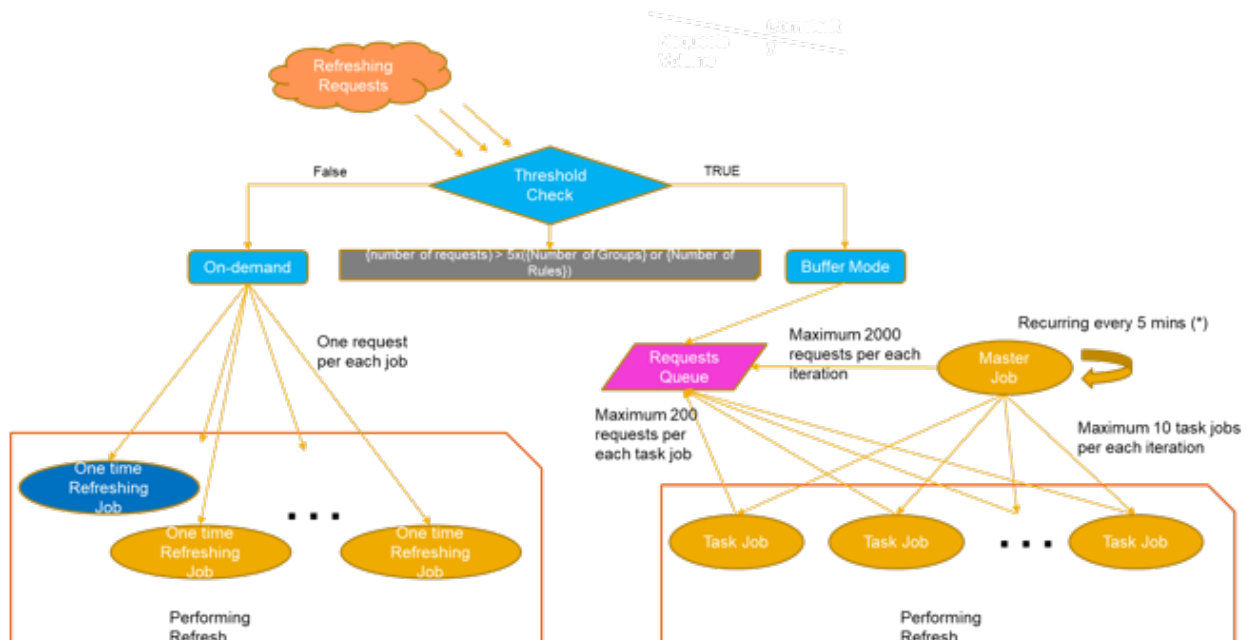
Refresh Type	Description
On-demand mode (Previously called Real-Time Refresh)	When changes to user information occur infrequently, each update action triggers its own refresh job.
Buffer mode	When there's a high frequency of user information changes, the framework buffers the refresh request for 5 minutes. Since the refresh requests are always based on the same set of groups and roles, buffering the request helps to avoid those duplicated refresh actions that occur within that 5-minute timeframe.

## How Does the Refresh Framework Work?

The Refresh Framework consists of two types of refresh jobs: the **on-demand mode** and **buffer mode**. The refresh framework automatically adjusts between buffer mode and on-demand mode, based on the actual refresh work load.

When the workload is light, the framework enables the on-demand job. This is the refresh mode you're most familiar with as you may currently use it for each refresh request. For example, an API call to change one user causes a refresh on all user groups.

When the workload is heavy, on-demand mode is disabled and buffer mode is enabled. That means requests within the next 5 minutes will buffer and reschedule tasks based on the buffer refresh request.



(\*) Since 1908, the master job will be on-demand scheduled when buffer mode is activated

### 📌 Note

If your company has scheduled a background job to refresh RBP regularly, the scheduled job remains effective and RBP refresh follows the defined interval. The Refresh Framework doesn't take effect even if you stop the background job. If you wish to start using the Refresh Framework in your company, contact Technical Support.

## What Are the Benefits to Using the Refresh Framework?

The Refresh Framework automatically switches between two refresh types depending on the workload detected. If infrequent user information changes occur, your RBP roles and groups are immediately refreshed. If frequent user information changes are detected, the buffer mode helps to reduce duplicate requests by collecting delta changes and processing them in one refresh request. As a result, you experience improved system stability and better RBP refresh performance. With the buffer mode enabled, you notice little delay.

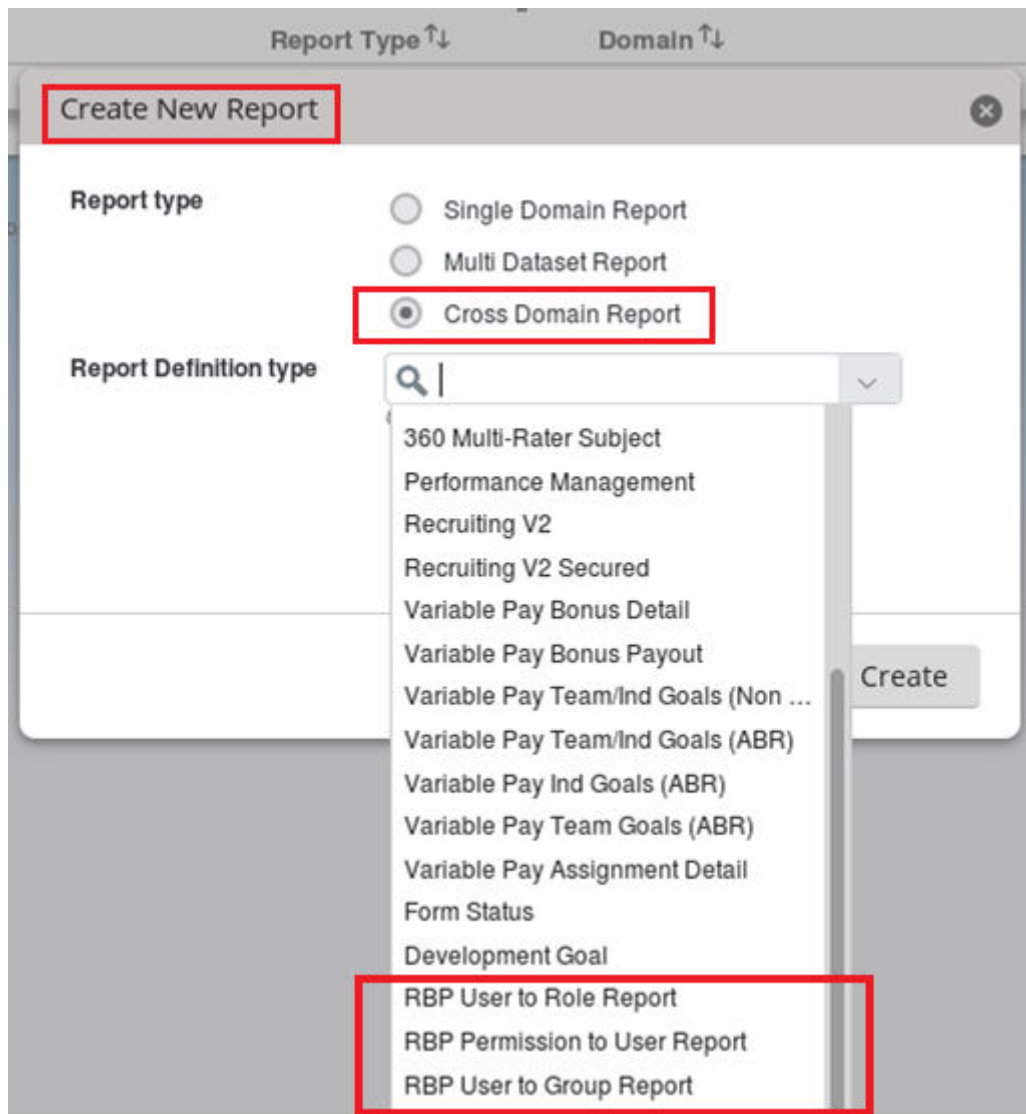
## My Organization Uses Scheduled Jobs, Are We Impacted by the Refresh Framework?

No. If your organization uses Scheduled Jobs, the Refresh Framework **doesn't** impact your system.

## 12.2 Cross Domain Table Reporting Between the RBP and Employee Central Domains

The cross domain Table report capability allows administrators to run reports between the Role-Based Permission (RBP) domain and Employee Central (EC) domain. RBP reports are included in the drop-down menu when selecting the Cross Domain Report Definition types.

Administrators can create Cross Domain Reports to join RBP and Employee Central data. *Person and Employment* is the EC domain information that is included and the tables are joined using the *user\_sys\_id* key.



## 12.3 Searching Roles Granted to a User

User Role Search can search the roles granted to specific users for a specific permission and a target user. When some users get some permissions on some target users that shouldn't be granted, the administrator can use this tool to find which role grants the permission so they can update the permission settings.

- This tool doesn't support MDF RBP permission as search criteria.
- This tool doesn't support permissions under the Growth Portfolio category.
- This tool doesn't support Inactive Internal User or TBH user to be selected as Target User.
- This tool doesn't support External User.

1. Go to Administration Tools.
2. In the Manage Employees block, select Set User Permissions.

3. In the Set User Permissions section, select User Role Search.
4. In the Selection session of the tool, enter Access Users. You can select at most 2 access users.
5. Select a permission category and one permission. If the permission needs target population, you can optionally select one target user.

## Admin Tools

[Back to Admin Tools](#)

### User Role Search

Use this page to search specific roles granted to users. Users can select at most 2 access users, 1 permission and 1 or none target users. The : grant this permission and target user to the access users. If the target user field is empty, the search result will not consider target user. On the r the selected access user and target user will be highlighted in the "Grant this role to ..." session.

#### Selection

Access Users

Permission Category

Manage User

Permission

Set User Status

Target User(optional)

Search Roles

6. Click Search Roles Button. The search result displays all roles that grant this permission and target user to the access users. If the target user field is empty, the search result won't consider target user. If a result you expect to see isn't showing up, it may be because there are back-end update jobs still running.

### Result

**User:** cgrant

**Role:** Set User Status testing

**User:** jessie\_admin

**Role:** Set User Status testing

- On the Result section, you can click the role name to see role details. On the role details page, the access and target populations are highlighted in the [Grant this role to...](#)

### Role name: Set User Status testing (last modified by wliu, 2015-01-15)

This role has the following permissions:

▼ Permission requiring target
Manage User
• Set User Status

Groups / Users granted with role permission access and their targets:

Group/User granted with role permission	Target population	Object Name	Criteria
Everyone	Department - sales		

section.

## How can you compare permission roles?

You can use User Role Search to quickly search for and compare permission roles assigned to specified users in role-based permissions.

- Go to Administration Tools.
- In the Manage Employees block, select Set User Permissions.
- In the Set User Permissions section, select User Role Search.
- In the Selection session of the tool, enter the Access Users whose roles you're comparing.
- Click Search Roles Button. The search result displays which roles, if any, grant the specified permission to either user. In the following example, you can see that both of the selected access users have permission to view address data.

[Back to Admin Tools](#)

#### User Role Search

Use this page to search specific roles granted to users. Users can select at most 2 access users, 1 permission and 1 or none target users. The search result will display all roles that grant this permission and target user to the access users. If the target user field is empty, the search result will not consider target user. On the role detail page, the grant rules that grant the selected access user and target user will be highlighted in the "Grant this role to ..." session.

**Selection**

Access Users

cgrant\_jreed

Permission Category

Employee Data

Permission

Business Phone(View)

Target User(optional)

click to add users

Search Roles

**Result**

User: cgrant

User: jreed

Role: All Employees

Role: All Employees

Manager Role

Admin

- If a user doesn't have the specified permission, it's indicated as "no result." In the following example, you can see that the user "cgrant" has permission to view "Impact of Loss" data, due to her roles as a manager and

administrator. The user "jreed" isn't assigned to any role that allows him to view this information.

Back to [Admin Tools](#)

User Role Search

Use this page to search specific roles granted to users. Users can select at most 2 access users, 1 permission and 1 or none target users. The search result will display all roles that grant this permission and target user to the access users. If the target user field is empty, the search result will not consider target user. On the role detail page, the grant rules that grant the selected access user and target user will be highlighted in the "Grant this role to ..." session.

Selection

Access Users

cgrant\_jreed

Permission Category

Employee Data

Permission

Impact of Loss(View)

Target User(optional)

click to add users

Search Roles

Result

User: cgrant

User: jreed

Role: Manager Role

Role: No result

Admin

7. You can also specify one target user, to see whether either of the two access users has the specified permission for the specified target. In the following example, you can see that although both user "cgrant" and user "dsharp" are managers, only user "cgrant" has permission to view "Impact of Loss" data for user "vstokes". It's because, in this example, the manager role has a target permission group of "All Direct Reports" and "vstokes" is a direct report of "cgrant".

Admin Tools

Back to [Admin Tools](#)

User Role Search

Use this page to search specific roles granted to users. Users can select at most 2 access users, 1 permission and 1 or none target users. The search result will display all roles that grant this permission and target user to the access users. If the target user field is empty, the search result will not consider target user. On the role detail page, the grant rules that grant the selected access user and target user will be highlighted in the "Grant this role to ..." session.

Selection

Access Users

cgrant\_dsharp

Permission Category

Employee Data

Permission

Impact of Loss(View)

Target User(optional)

vstokes

Search Roles

Result

User: cgrant

User: dsharp

Role: Manager Role

Role: No result

Admin

# Change History

Learn about changes to the documentation for Implementing Role-Based Permissions in recent releases.

## <1H 2025>

Type of Change	Description	More Info
Changed	The <a href="#">CheckRulePerRole</a> check now verifies if the number of rules associated with a role exceeds 200 instead of 100.	<a href="#">Does a Role Have More Than 200 Rules? [page 76]</a>
Changed	We removed content on legacy Role-Based Permissions.	
Changed	Updated information on transporting Role-Based Permissions configurations using <a href="#">Configuration Transport Center</a> .	<a href="#">Transport Role-Based Permissions Configurations to the Production Instance [page 60]</a>
Added	Added tips on <a href="#">Sort By Ascending</a> button, the <a href="#">Enter Full Screen</a> button, and the view and edit modes of field-level overrides.	<a href="#">Creating a Permission Role [page 35]</a>

## <2H 2024>



Type of Change	Description	More Info
Changed	We subdivided Role-Based Permissions administrator access into view and edit accesses. <a href="#">Role-Based Permission Admin (View)</a> is split into <a href="#">View Group</a> and <a href="#">View Role</a> , while <a href="#">Role-Based Permission Admin (Edit)</a> is split into <a href="#">Edit Group</a> and <a href="#">Edit Role</a> .	<a href="#">Granting Administrators Access to Role-Based Permissions [page 10]</a> <a href="#">Role-Based Permissions Administrator Access [page 11]</a>

# Important Disclaimers and Legal Information

## Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

## Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

## Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

## Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

## Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.





© 2025 SAP SE or an SAP affiliate company. 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 SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

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 or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP 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.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.