**Administrators' Handbook**

Document Version: 1.0 – 2013-09-30

**CUSTOMER**

# Role-Based Permissions

# Typographic Conventions

| Type Style | Description |
|---|---|
| *Example* | Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options.<br>Textual cross-references to other documents. |
| **Example** | Emphasized words or expressions. |
| `EXAMPLE` | Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE. |
| `Example` | Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools. |
| **`Example`** | Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation. |
| **`<Example>`** | Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system. |
| `EXAMPLE` | Keys on the keyboard, for example, `F2` or `ENTER`. |

# Document History

| Version | Date | Change |
|---|---|---|
| 1.0 | 2013-09-30 | Initial version |

# Table of Contents

# 1 Introduction

## 1.1 About this Document

This handbook is intended for security administrators to enable them to manage Role-Based Permissions (RBP).

The first chapter familiarizes you with the concept of role-based permissions. The subsequent chapters detail the individual tasks that make up the management of Role-Based Permissions. Finally, you will find troubleshooting information in case problems occur with the permissions.

## 1.2 What are Role-Based Permissions?

Role-Based Permissions (RBP) manage the permissions in the SuccessFactors suite. RBP controls access to the applications and what users can see and edit. It's a suite-wide authorization concept which applies to the majority of modules. You can find details about what is covered by RBP and where other authorization mechanisms apply in the section What´s covered by RBP? [page 9].

> Note
>
> On a single instance, you cannot mix RBP with the old permission framework. If several modules are in use and RBP is mandatory for one, you must configure RBP for all modules.
>
> If multiple instances are used, we recommend as well using either RBP or the old permission framework on all instances. Although it's not a technical limitation - you can have RBP on one instance and the old permission framework on other instances - it's better to go for one solution from a maintenance and governance perspective.

The main elements in RBP are permission roles and permission groups.

### What are 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, or Job Code.

> Example
>
> There might be a permission group called "Human Resources in US" which would list 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 = United States" and "Department = HR".

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 dynamic, 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.

### What are permission roles?

A role is a set of permissions. As such, a permission role controls the access rights an employee or group of employees has to the application or employee data. Role-based permissions allow you to grant a role to a specific employee, a manager, a group, or to all employees in the company. The roles can provide very granular permissions, as this example illustrates:

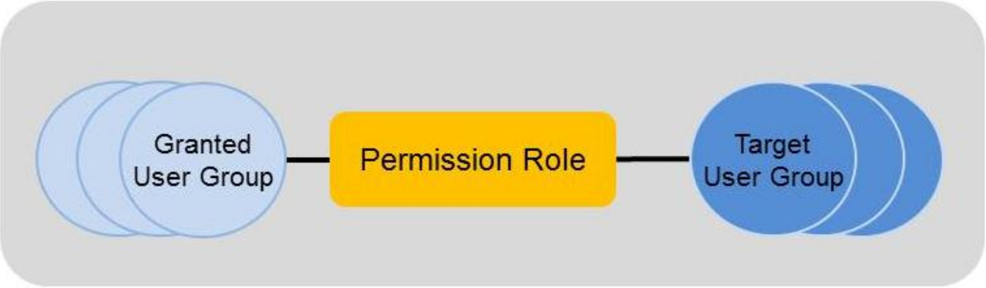
Example

There might be roles like "HR Compensation and Benefits Manager", "HR Manager for Sales", and "HR Learning and Development Manager". While all three are HR managers, their roles have been distinctly carved out– one handling compensation and benefits, another handling the sales team, and the third handling learning and development.

You can have as many permission roles as your company requires.

### How are groups and roles connected?

While roles define what is allowed, the groups define who is allowed to do it (granted users) and for whom (target users). This graphic illustrates the principle:

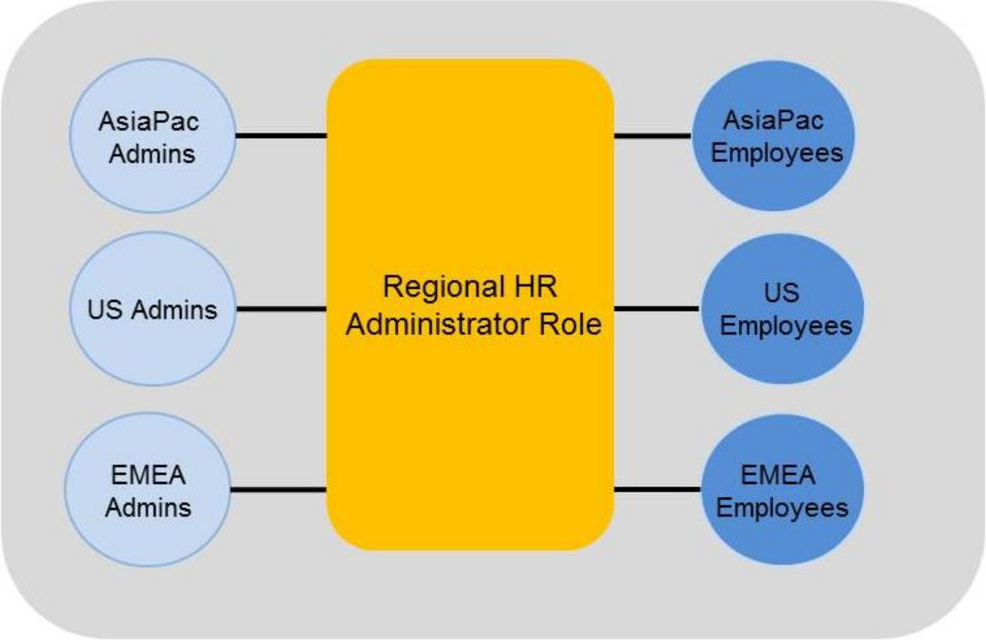


Once a role is defined, you grant the role to one or more groups of users represented by the circles on the left. Then you restrict the granted users to perform the role on target users. For example, you may decide that managers (the left circle) can view dashboards (defined in the role) on their team (the right circle).

You can grant a role to many different user groups which in turn have different target user groups. Thus, you can easily achieve a high degree of granularity.

Example

You could have a "Regional HR Administrator" role and use permission groups to make sure that US Admins are limited to managing employees in the United States, while Europe Admins are limited to managing employees in Europe, or AsiaPac Admins are limited to managing employees in AsiaPac. You would have only a single role called "Regional HR Administrator" and would use groups to control access. Your groups would be "AsiaPac Admins", "US Admins", "Europe Admins", "AsiaPac Employees", "US Employees", and "Europe Employees".



The role-based permission framework allows as many roles in the system as a company requires. At the same time, each role can have a different level of permission granularity.

For detailed information about granting roles, see How can you grant permission roles? [page 26].

### RBP Features

The features of RBP include:

- Administrator definable roles
- Automation of permissions assigned to users
- Definition of user access based on employee attributes, hierarchies and relationships, and exclusion rules
- Auditing of changes to security (who, what, when)
- Copy permission configuration between systems

Note

RBP is approved for organizations with up to 300,000 employees. We will continue to raise this bar in the future.

# 2 Initial Setup Tasks

## 2.1 Granting Permissions to Manage RBP

There are three kinds of admins for each customer instance:

The **Super Administrator** (sometimes referred to as Super User), who is created in your instance by a SuccessFactors support consultant using the provisioning tool, is the only user who is allowed to log in to the system after RBP is first enabled. The Super Admin can grant other users the right to manage Role-Based Permissions. As a Super Admin, grant the permission to manage RBP to yourself and any other administrators you want to allow to manage Role-Based Permissions.

A **Security Admin** is responsible for managing security through roles and permission groups in the role-based permissions.

An **Admin** is any user with access to the Admin Tools.

> i Note
>
> The RBP concept assumes that there are just a few users with access to managing role-based permissions per company. You typically want to keep the number of people able to maintain RBP as limited as possible as permissions management is centrally managed. All of the other administrative tasks can be distributed to many administrators, but managing Role-Based Permissions is intended for a limited set of Security Admins.

To grant the permission to manage Role-Based Permissions:

1. Log on to the instance as Super Admin.
2. Go to *Admin Tools*.
3. In the Manage Employees portlet, select *Set User Permissions*, then choose *Manage Role-Based Permission Access*.

   > i Note
   >
   > Only Super Admins get to see the *Manage Role-Based Permission Access* link when they log in. Security Admins who are not Super Admins cannot see this link.

4. Select *Add User*.
5. Search for and select the employee(s) you'd like to grant permission to.
6. Click *Grant Permission*.

# 3 Managing Role-Based Permissions

Each RBP implementation needs a clear definition of what permissions are needed for the individual user groups. When you define the RBP configuration, you need to take into account your organization's security requirements, the limitations coming from the module coverage of RBP, and best practices which consider maintenance and performance aspects. We recommend that you follow these steps:

1. If this is your first time using Role-Based Permissions in SuccessFactors, get an overview of what permissions can be granted [page 9 ] in your instance depending on the activated modules.
2. Go through the RBP module coverage [page 9] section and evaluate the impact for your RBP implementation.
3. Familiarize yourself with the recommendations and best practices [page 16].
4. See the basic roles [page 18] section to learn about the common roles that are usually created for customers.
5. If you, as recommended, want to create groups and roles on your test instance and then copy them to the production instance, check what requirements regarding data synchronization you have to fulfill [page19].

## 3.1 Checking Available Permissions in Your Instance

Depending on what modules are activated in your instance, different permissions are available to be configured. To find out exactly what permissions can be granted

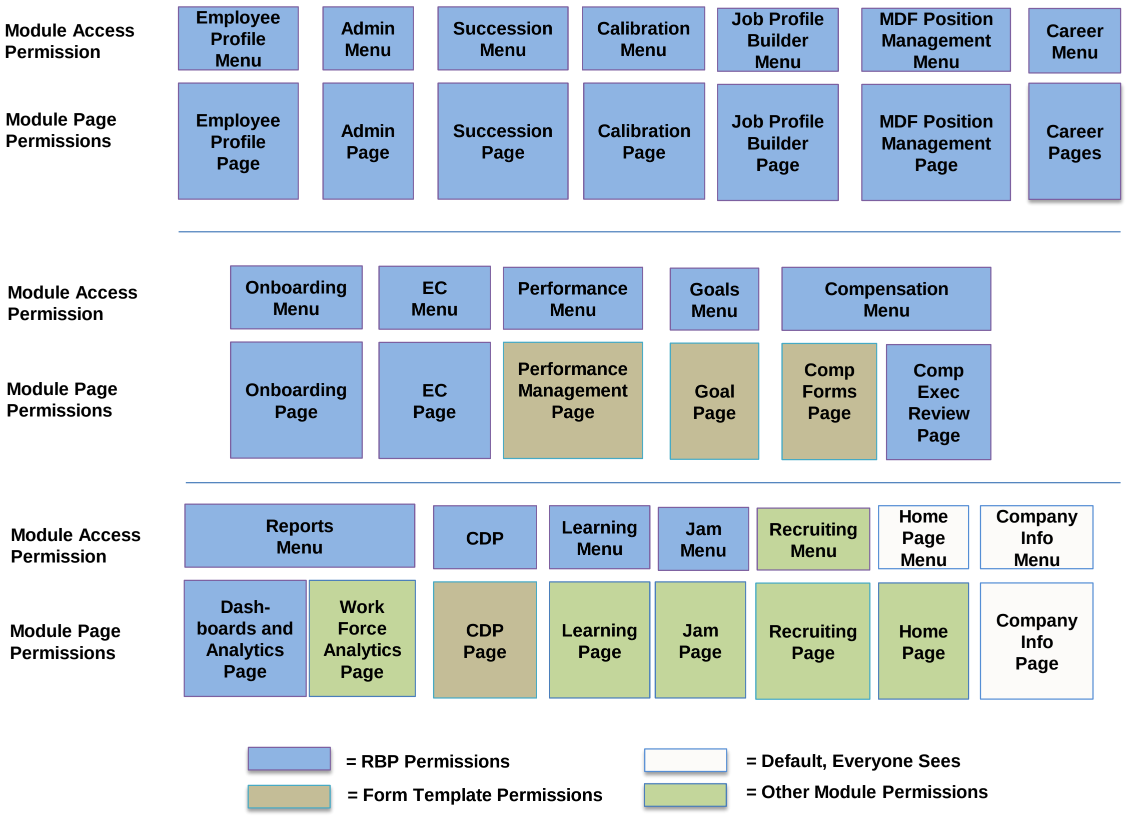
1. Log on to your instance.
2. Go to Administration Tools. In the *Manage Employees* portlet, select Set User *Permissions*.
3. In the *Set User Permissions* section, select *Manage Permission Roles*.
4. Click *Create New.*
5. In section 2 *Permission Settings*, click *Permissions*. On the left you can see the permission categories. If you click on one of these links, you see the detailed permissions on the right.

## 3.2 What's Covered by RBP?

RBP controls the access to most modules. The page permissions (that is, what data and functionality appears on the page) are partly controlled by RBP and partly controlled by other mechanisms, depending on the requirements of the modules.

For some modules it is mandatory to use RBP. If several modules are in use and RBP is mandatory for one, you must configure RBP for all modules. You cannot mix RBP with the old permission framework.
If multiple instances are used we recommend using either RBP or the old permission framework on all instances. Although it's not a technical limitation - you can have RBP on one instance and the old permission framework on other instances - it's better to go for one solution from a maintenance and governance perspective.

The following graphic provides an overview of where RBP is used and where other mechanisms are in place. In the table below, you will find details on RBP coverage for each module.



Module Access Permission

Employee Profile Menu | Admin Menu | Succession Menu | Calibration Menu | Job Profile Builder Menu | MDF Position Management Menu | Career Menu

Module Page Permissions

Employee Profile Page | Admin Page | Succession Page | Calibration Page | Job Profile Builder Page | MDF Position Management Page | Career Pages

Module Access Permission

Onboarding Menu | EC Menu | Performance Menu | Goals Menu | Compensation Menu

Module Page Permissions

Onboarding Page | EC Page | Performance Management Page | Goal Page | Comp Forms Page | Comp Exec Review Page

Module Access Permission

Reports Menu | CDP | Learning Menu | Jam Menu | Recruiting Menu | Home Page Menu | Company Info Menu

Module Page Permissions

Dash-boards and Analytics Page | Work Force Analytics Page | CDP Page | Learning Page | Jam Page | Recruiting Page | Home Page | Company Info Page

🟦 = RBP Permissions

🟫 = Form Template Permissions

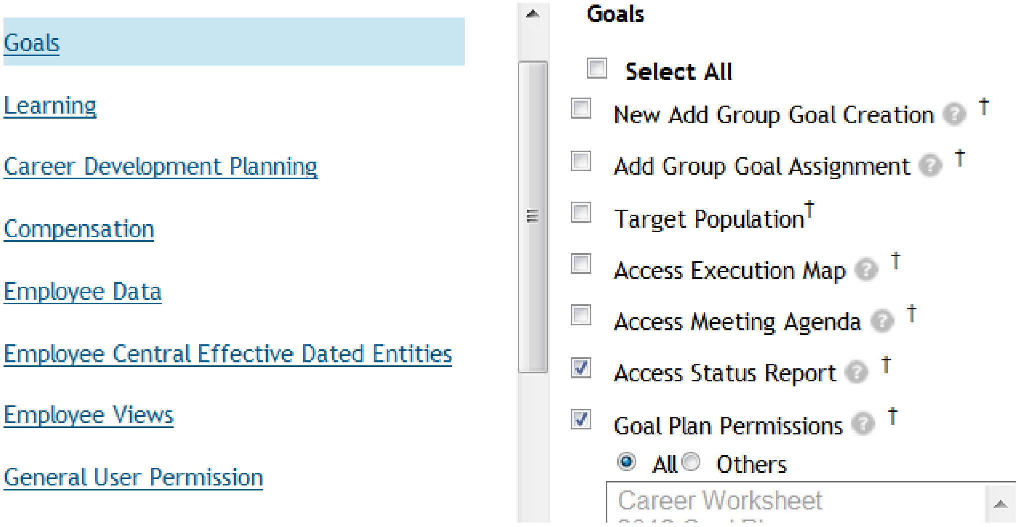
⬜ = Default, Everyone Sees

🟩 = Other Module Permissions

Here are two examples which illustrate how other mechanisms then RBP control access to elements and functions for some modules:

### Goals

For Goals, you set the permission to access the goal plans and some other access permissions in RBP.



Goals

Learning

Career Development Planning

Compensation

Employee Data

Employee Central Effective Dated Entities

Employee Views

General User Permission

Goals

□ Select All

□ New Add Group Goal Creation †

□ Add Group Goal Assignment †

□ Target Population†

□ Access Execution Map †

□ Access Meeting Agenda †

☑ Access Status Report †

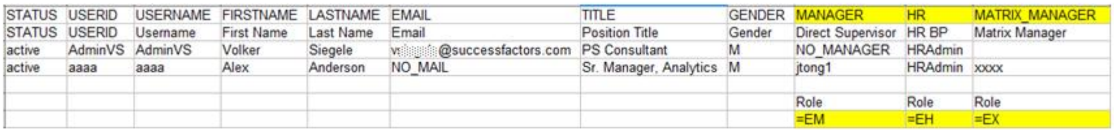
☑ Goal Plan Permissions †

● All ○ Others

Career Worksheet

However, with that, the permissioned users are not allowed to create, edit or cascade goals. These permissions are derived from the custom-specific goal plan xml file. This xml file specifies which roles (such as, employee, manager, HR manager) are allowed to view and edit goals.

In addition, in the employee import file each employee is assigned to a dedicated manager and HR manager. Only the HR manager determined here can see and edit fields in an employee's goal plan. It's a 1:1 relationship. As a consequence, it's not possible to grant multiple HR representatives access to a specific development plan. The following shows an excerpt of such an employee import file:



| STATUS | USERID | USERNAME | FIRSTNAME | LASTNAME | EMAIL | TITLE | GENDER | MANAGER | HR | MATRIX_MANAGER |
|---|---|---|---|---|---|---|---|---|---|---|
| STATUS | USERID | Username | First Name | Last Name | Email | Position Title | Gender | Direct Supervisor | HR BP | Matrix Manager |
| active | AdminVS | AdminVS | Volker | Siegele | v[redacted]@successfactors.com | PS Consultant | M | NO_MANAGER | HRAdmin | |
| active | aaaa | aaaa | Alex | Anderson | NO_MAIL | Sr. Manager, Analytics | M | jtong1 | HRAdmin | xxxx |
| | | | | | | | | | | |
| | | | | | | | | Role | Role | Role |
| | | | | | | | | =EM | =EH | =EX |

### Performance Management

Permissions to access the Performance Management Tab and to create a performance management form are provided in RBP.

Who is involved in each workflow step is defined in a route map. Permissions to do changes, for example rate the performance and potential, is hard coded in the corresponding form xml file. Both the route map and the form xml file use the predefined roles, such as E, EM, and EH. That is, ultimately the role a user has and the relationships defined in the employee import file determine who is allowed to work on performance management forms.

### Details on RBP Module Coverage

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| Admin Tools | ● | Everything within Admin Tools | |
| Calibration | ● | • Access to Calibration tab<br>• Access to employees whom the user will see within | Within Calibration, specific permissions grant read, write, edit, and finalize authorization for individual sessions. |

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| | | Calibration | |
| Career | 🟢 | Access to Careers tab and sub-tabs | Once the Career tabs and sub-tabs are permissioned under RBP, all sub tabs, postings, and so on, are visible. There are no deeper permissions available by RBP, the module, or xml. |
| CDP | 🟡 | User Permissions<br>• Access to development tab<br>• Access to career worksheet tab<br>• Access to development plan template, career worksheet template, learning activity template<br>• Access to Career Development Plan (CDP) Learning Activity Mass Add<br>• Access to development admin permission<br>Administrator Permissions<br>• Access to Import Development Goals<br>• Access to Manage Learning Activity Catalogs<br>• Access to Manage Learning Activity to Competency Mappings<br>• Access to Manage Career Path<br>• Access to Manage User Relationship for Learning Administrator and Educational Representative<br>• Access to Manage Import Learning Activity by Web Service | Permissions within Goal Plans, such as creating, editing, or cascading goals. |
| Company Info | 🔴 | | Company Info menu is visible for everybody |
| Compensation/Variable Pay | 🟡 | • Access to tabs and sub tabs within Compensation and Variable Pay<br>• Permission to read and edit | • Permission within compensation forms<br>• RBP does not apply to compensation plan level |

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| | | executive reviews | |
| Employee Central | 🟢<br>RBP is mandatory | Access to EC and page permissions | |
| Employee Profile | 🟢 | • Access to Employee Profile (Live Profile Access)<br>• Field level permissions to employee data | |
| Goals | 🟡 | • Access to Goal tab<br>• Access to Allow Role to Create Group Goal (Group Goal 2.0)<br>• Access to Allow Role to Assign Add Group Goal 2.0 to other Users<br>• Access to Execution Map under Goal Execution<br>• Access to Meeting Agenda under Goal Execution<br>• Access to Status Report under Goal Execution<br>• Access to Goal Plan(s)<br>• Administrator permissions<br>• Access to Import Goals<br>• Access to Import/Export Goals library<br>• Access to Manage Configuration of Goal Execution | Permissions within Goal Plans, such as creating, editing, or cascading goals. However, for/to whom the employee can create, edit, cascade goals is controlled by the target population of the "Access to Goal Plans" permission item. |
| Home Page | 🔴 | | • Everyone sees the home page<br>• Items visible on the Home Page are based on user's permissions to those individual items/portlets<br>• Administrators can enable or disable out-of-the-box portlets. When an out-of-the-box portlet is enabled, it will appear for all users. Modules control what content will appear in the portlet, so this can be a mix of RBP and non-RBP controls |

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| | | | depending on the portlet. Administrators can add custom portlets and use dynamic groups (outside of RBP) to control who sees the custom portlets. |
| Jam | 🟡 | Access to Jam | Permissions within Jam |
| Job Profile Builder 2.0 | 🟢<br>RBP is mandatory | Access to Job Profile Builder and page permissions | |
| Learning | 🟡 | Access to Learning menu | Permissions within the Learning module |
| MDF Position Management | 🟢<br>RBP is mandatory | Access to MDF Position Management and page permissions | |
| Onboarding | 🟢<br>RBP is mandatory | • For corporate users (that is HR and admins) in 1308 we will pass a group assignment that is created in RBP to onboarding admin. The onboarding admin then reads the group assignment and determines what content in the compliance tool should be exposed to the user.<br>• Page permissions are a mixture of manager discretion and RBP. A manager gives new hires access to some information before their first day on the job. That includes looking at the profiles of their future team, buddies (mentors), and other people the manager recommends. However, RBP controls what data from the selected users the new hires can see. The new hires will not be able to see | Hiring managers automatically gain access to onboarding (it appears in the main menu navigation) if one of their team members is actively being onboarded. This is not through RBP. |

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| | | other people or the whole org of the corporation. | |
| Performance | 🟡 | • Access to Performance tab<br>• Access to Create Forms | Permissions within forms (that is, required fields) |
| Recruiting | 🟡 | • All features under Recruiting Permissions in Permission Settings<br>• Administrator permissions (allows the admin to give the user access to certain links in Admin Tools)<br>• The permission to create forms and the reports permissions are shared with the other modules – both are covered by RBP. | • Recruiting tab<br>• Any user with access to a requisition for any reason has irrevocable access to the Recruiting tab.<br>• Form template permission grants access, but there are also other ways employees may have access. For example, if a form is routed to them, if they are added as an operator to the form, or if certain feature permissions are granted to them |
| Reports Menu – Dashboards & Analytics | 🟡 | Controlled by RBP:<br>• Access to specific dashboards and reports under Analytics<br>• Access to target populations the user will be able to report on<br>Limited RBP control:<br>• For ad hoc reports, the access to specific reporting sub domain schemas is controlled via RBP, but access to specific reports is done via “sharing”, which is not controlled by RBP. Sharing is user based. Though if, for example an RCM report is shared with a user that does not have RCM sub domain schema access, then it will not run. | Cell and field level permissions are not adhered to in ad hoc reports or dashboards, except for Employee Profile (opt-in). |
| Reports Menu – Workforce Analytics | 🟡 | Access to Workforce Analytics is controlled via the “Inform Reports” permission in RBP. | Permission controls within WFA. There is a concept of RBP in WFA but it is a separate RBP permission page within WFA app and does not link through to BizX RBP. |

| Module | Is it covered in RBP? | Controlled by RBP | Not controlled by RBP |
|---|---|---|---|
| Succession | 🟢 | • Access to Succession tab<br>• Access to Succession Org Chart, Succession Planning, Matrix Grid (9-box) and Talent Search<br>• Access to all Succession admin functions, including Succession Management, Position Set-up, Matrix Grid admin tools, Sync Position Model<br>• Beyond access to specific succession features, RBP also controls "target population" for users – which users and what details can be viewed by the logged in user. These include:<br>o Position details of users, which are controlled by position specific permission<br>o Field level details of positions<br>o Ability to view users on search results<br>o Ability to view users on matrix grid reports<br>o Ability to view users on succession org chart and lineage chart | Configuration of the 9 Box and Succession Org Chart. For example, if a client opts to include gender or minority on these as a configuration decision, this will not honor RBP settings that may have excluded visibility of same.<br>The same is true for talent search. RBP limits who shows up, but does not respect field level permissions set up in RBP. |

## 3.3 Recommendations and Best Practices

### 3.3.1 General

When managing Role-Based Permissions in your system, it's crucial that you keep the impact on system performance and the maintenance effort in mind. In addition, it is crucial that you have a governance process in place for further changes. We recommend the following:

- Start with most 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 of the permissions that should be given to everyone. For example, in this role include all of the publically-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 will help 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

  A user should not get the same permission from different roles. If users have multiple roles and get the same permissions from different roles, this slows down the system response time for these users.

- Limit the number of groups and roles

  In general, keep the number of groups and roles as low as possible. This will both reduce the maintenance effort and ease the troubleshooting in case of any issues. Remember, that you can grant a role to multiple groups, so you do not have to duplicate roles just to assign them to different groups.

  From a performance point of view, we recommend a maximum of 1000 dynamic permission groups. Dynamic groups are based on rules in contrast to static groups which contain named users. These static groups do not count against the 1000 recommendation. Note that this is not a hard limit, it is a guidance recommendation. The system will allow you to exceed 1000 dynamic groups, but the consequences of exceeding 1000 dynamic groups will be to reduce system performance.

- Naming Conventions

  Agree on a naming convention for groups and roles. This makes the maintenance much easier, especially for large implementations. For groups, you could for example use the prefixes "Granted:" and "Target:"

- Meaningful Group Names, Role Names, and Role Descriptions

  Meaningful group and role names and role descriptions help you to identify the correct groups and roles later during maintenance and troubleshooting. The role descriptions should state clearly the purpose of the role and not just repeat the role name.
  Additionally, it could be helpful to maintain a change log in the role description field. It should include the change, the date, and who made and approved the change. The "View change history" function also delivers this information; however, looking up the description field is much quicker.

- Governance
  It's key that you define a governance on RBP. You should define how changes to RBP will be handled in the future: Who should be able to make changes? How can a change be requested, who needs to review it and needs to be involved in deciding whether to make the change or not?
  This is especially important in large organizations where the departments tend to be separated from each other. If one department requests a change, this might also have an impact on other departments, so all parties need to agree on it.

  You may also want to introduce the concept of separation of duties for the administration of RBP. How to achieve this is described in the next chapter.

### 3.3.2 Special Requirement: Separation of Duties in RBP Administration

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.

Role-Based Permission 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.

In summary, you can achieve Separation of Duties with the following process:

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.

## 3.4 Basic Roles

Some roles in general exist in each company, like, 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.

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 | • Login permission<br>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 (see below) to make sure that they are not locked out either. |
| All users (what any user can | • Data any user can see about any other user |

| Role Name | Includes the following permissions... |
|---|---|
| do and see for all other users) | • Access to goal and development plan<br>• Careers tab permission<br>• Permission to navigate within the org chart<br>• Mobile access, if necessary |
| Employee self (what users can do and see for themselves) | • Data users can see about themselves (like employment data or personal info)<br>• What background sections they can maintain / edit for themselves<br>• Permission to create forms for themselves (depending on the culture) |
| Managers (permissions granted to users who have at least one direct report defining what they can do and see for their direct reports) | • What data managers can see about their reports<br>• Permission to create forms for their reports<br>• Permission to create job requests<br>• Probably permissions to manage compensation for their reports<br>• Permission to use succession and succession org chart |
| HR (permissions granted to HR staff) | • What data HR can see / maintain for their scope<br>• Permissions to create forms depending on the culture<br>• Permission to use succession, calibration and so on<br>• Permission to search for candidates or use talent search |
| System Admin All Modules (permissions granted to customer admins) | • Permissions to do/see everything for everybody |
| Local Administrators | • Limited administration rights, for example, upload employee data, create performance forms |

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

When you configure RBP, it is common to make changes first on the test instance. Only after successful testing you copy the configuration to the production instance. As roles are depended on the system configuration (for example, which fields, forms or reports are enabled), and groups are dependent on the employees and their data it is very 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 would 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 will need 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 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.

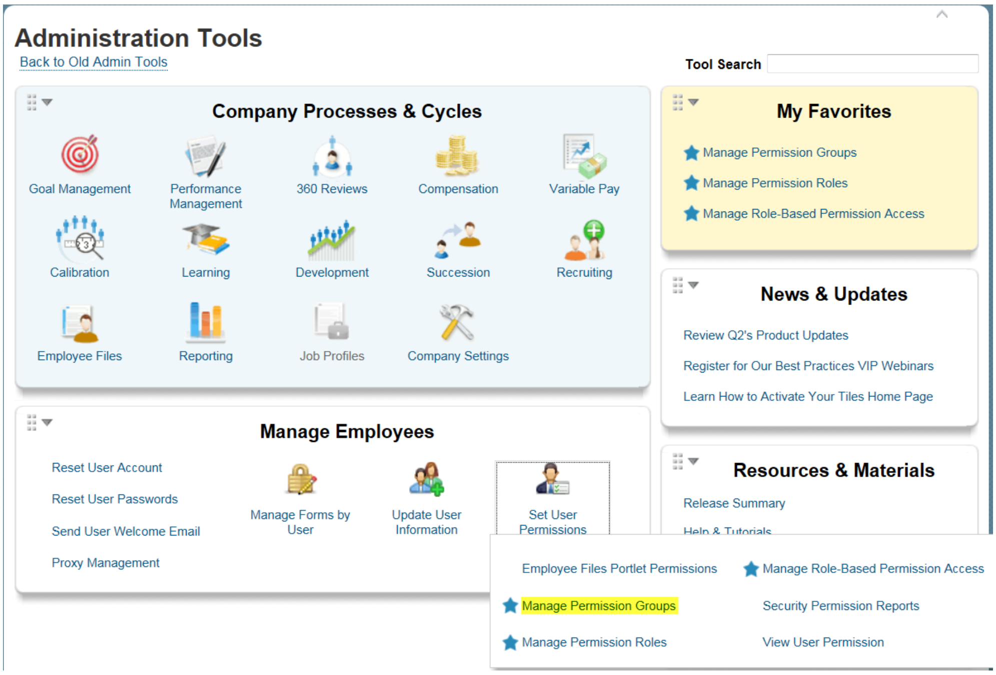
Depending on how much is out of sync, you may need to have the production instance copied to the test instance (possibly using the instance sync tool) or you may be able to work around it.

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.

# 4 Setting up Groups and Roles

## 4.1 How do you create a permission group?

1. Go to Administration Tools. In the *Manage Employees* portlet, select *Set User Permissions*.
2. In the Set User Permissions section, select *Manage Permission Groups*.

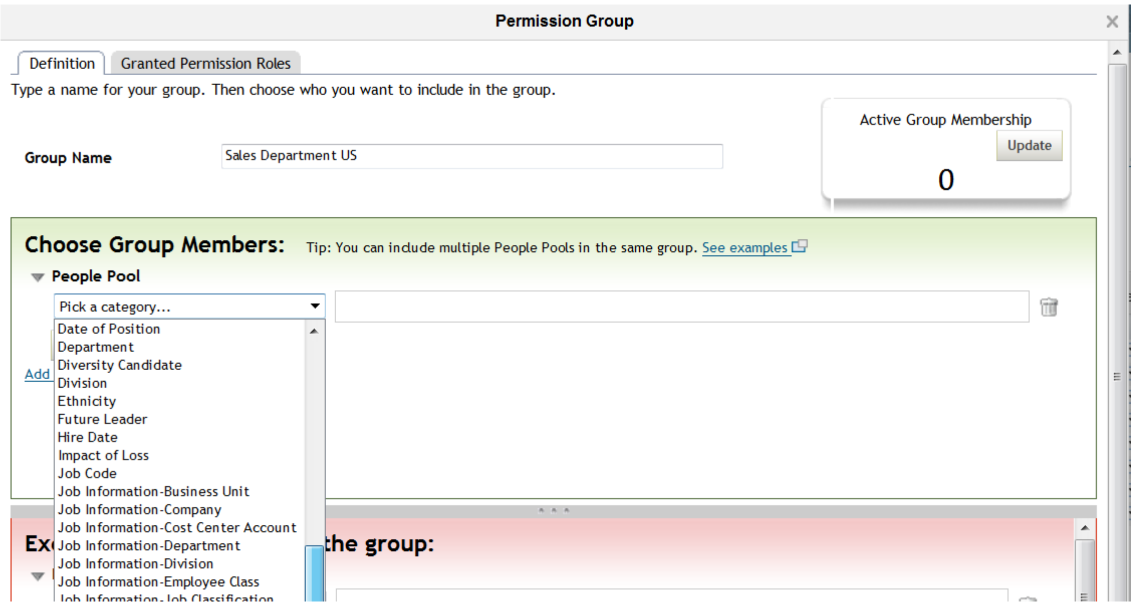


The *Manage Permission Groups* page opens.

3. Click the *Create New* button to create a new Permission Group.

   The *Permission Group* page opens.

4. In the Group Name field, provide a name for your Permission Group.
5. In the *Choose Group Members* section, click the *Pick a Category* dropdown menu and select a category.



Permission Group

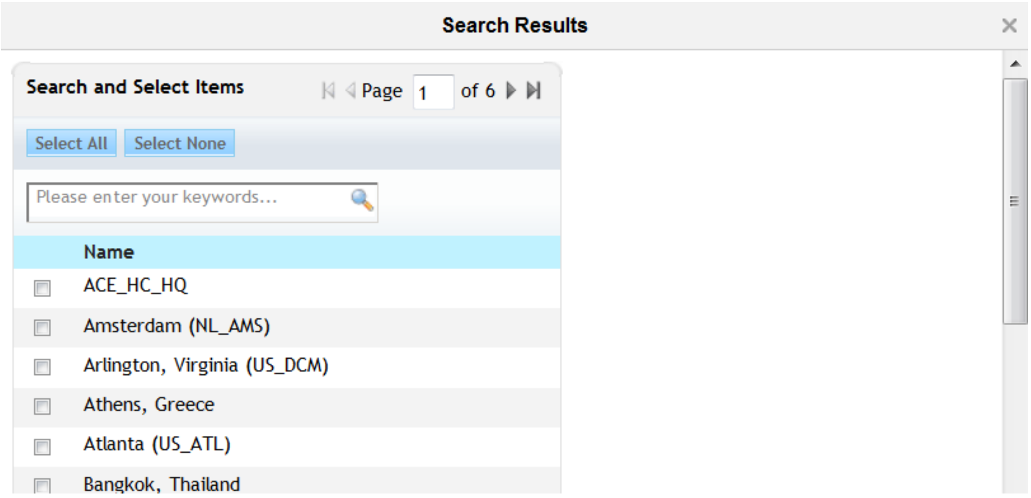
Type a name for your group. Then choose who you want to include in the group.

Group Name: Sales Department US

Active Group Membership: 0

Choose Group Members: Tip: You can include multiple People Pools in the same group. See examples

6. A search screen opens where you can either enter a search term or click the magnifying glass, which will display all values available.

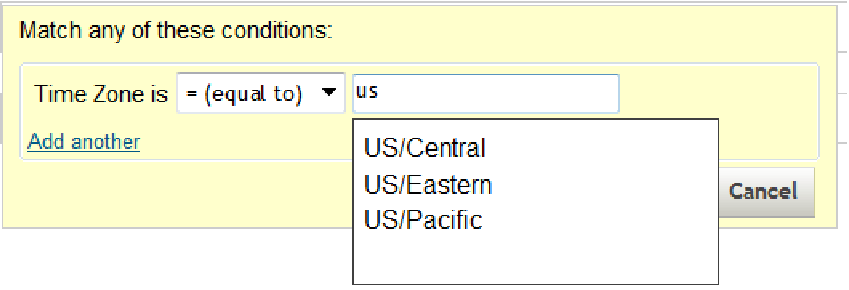


Search Results

Search and Select Items

| | Name |
|---|---|
| □ | ACE_HC_HQ |
| □ | Amsterdam (NL_AMS) |
| □ | Arlington, Virginia (US_DCM) |
| □ | Athens, Greece |
| □ | Atlanta (US_ATL) |
| □ | Bangkok, Thailand |

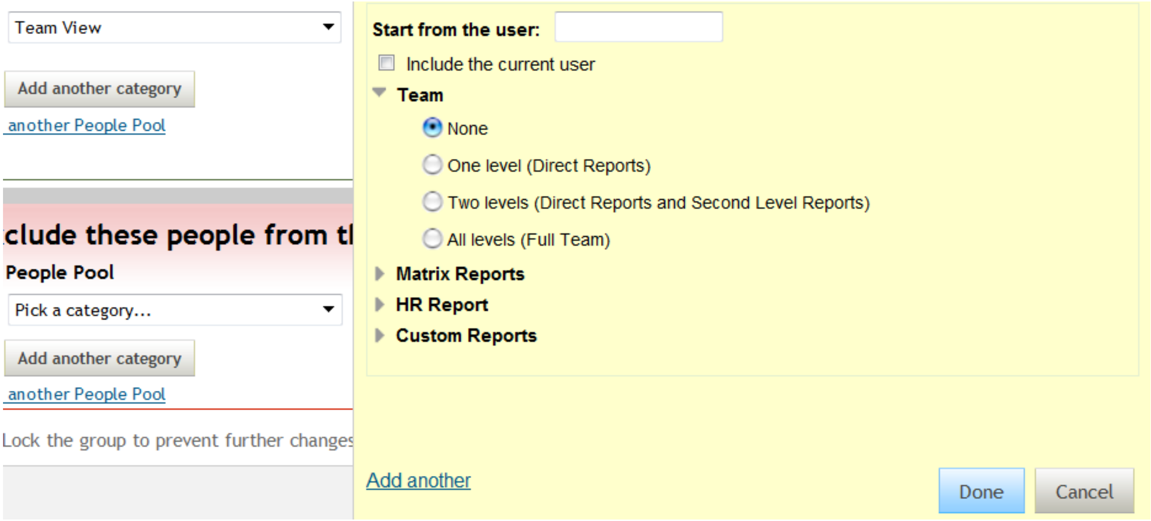
For some categories, a smaller pop-up appears where you can enter values. The following screenshot shows this pop up for the Time Zone.



Match any of these conditions:

Time Zone is = (equal to) us

If you select the "Team View" category, you can use hierarchical relationships to specify the group, as you can see in this screenshot:



Team View

Start from the user:

☐ Include the current user

Team

● None

○ One level (Direct Reports)

○ Two levels (Direct Reports and Second Level Reports)

○ All levels (Full Team)

This allows you to apply rules such as "everybody in Carla Grant's team, all levels deep".

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.

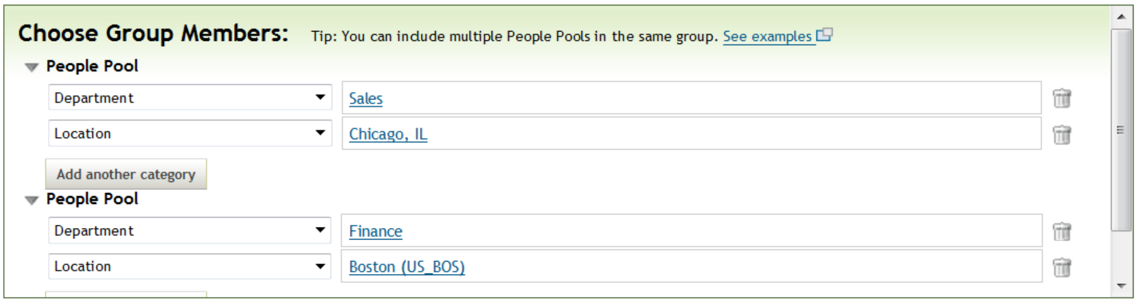
   ### Example

   You want to create a group of sales employees working in the US. Then you choose the category Department and select "Sales". You add a second category "Country" and select "USA".

9. Complex group definitions may require you to use multiple people pools. If you use two or more people pools, this 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.



Choose Group Members: Tip: You can include multiple People Pools in the same group. See examples

People Pool

| | |
|---|---|
| Department | Sales |
| Location | Chicago, IL |

People Pool

| | |
|---|---|
| Department | Finance |
| Location | Boston (US_BOS) |

Note

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

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. Click *Done* to complete the process.

## 4.2 How do you create a permission role?

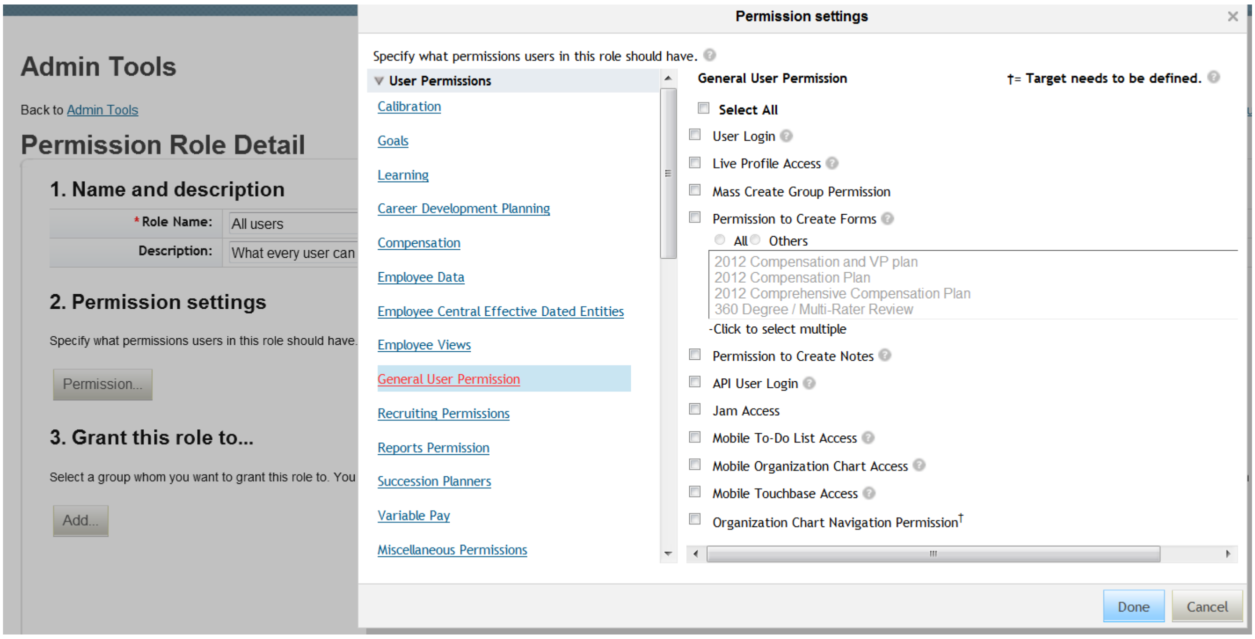
1. Go to Administration Tools.
2. In the *Manage Employees* portlet, select *Set User Permissions*.
3. In the *Set User Permissions* section, select *Manage Permission Roles*.

   The Permission Role List page opens.
4. To add a Permission Role, click the *Create New* button.

   The Permission Role Detail page opens.
5. In the *Role Name* field, type a name describing of what the role allows you to do.
6. In the *Description* field provide a statement describing what the role allows an employee to do. Add a note about when the role was created and by whom.
7. In the *Permission Settings* section, click the *Permission* button to specify the permission you want to assign to the role.

   The *Permission Settings* window opens.
8. On the left side of the page, you'll see the different permission categories. Click a permission category to reveal the different permissions.

   The list of permissions associated with this category is displayed.



Admin Tools

Back to Admin Tools

Permission Role Detail

1. Name and description

| | |
|---|---|
| * Role Name: | All users |
| Description: | What every user can |

2. Permission settings

Specify what permissions users in this role should have.

Permission...

3. Grant this role to...

Select a group whom you want to grant this role to. You

Add...

**Permission settings**

Specify what permissions users in this role should have.

User Permissions

- Calibration
- Goals
- Learning
- Career Development Planning
- Compensation
- Employee Data
- Employee Central Effective Dated Entities
- Employee Views
- General User Permission
- Recruiting Permissions
- Reports Permission
- Succession Planners
- Variable Pay
- Miscellaneous Permissions

General User Permission

†= Target needs to be defined.

□ Select All

□ User Login

□ Live Profile Access

□ Mass Create Group Permission

□ Permission to Create Forms

○ All ○ Others

2012 Compensation and VP plan<br>
2012 Compensation Plan<br>
2012 Comprehensive Compensation Plan<br>
360 Degree / Multi-Rater Review

-Click to select multiple

□ Permission to Create Notes

□ API User Login

□ Jam Access

□ Mobile To-Do List Access

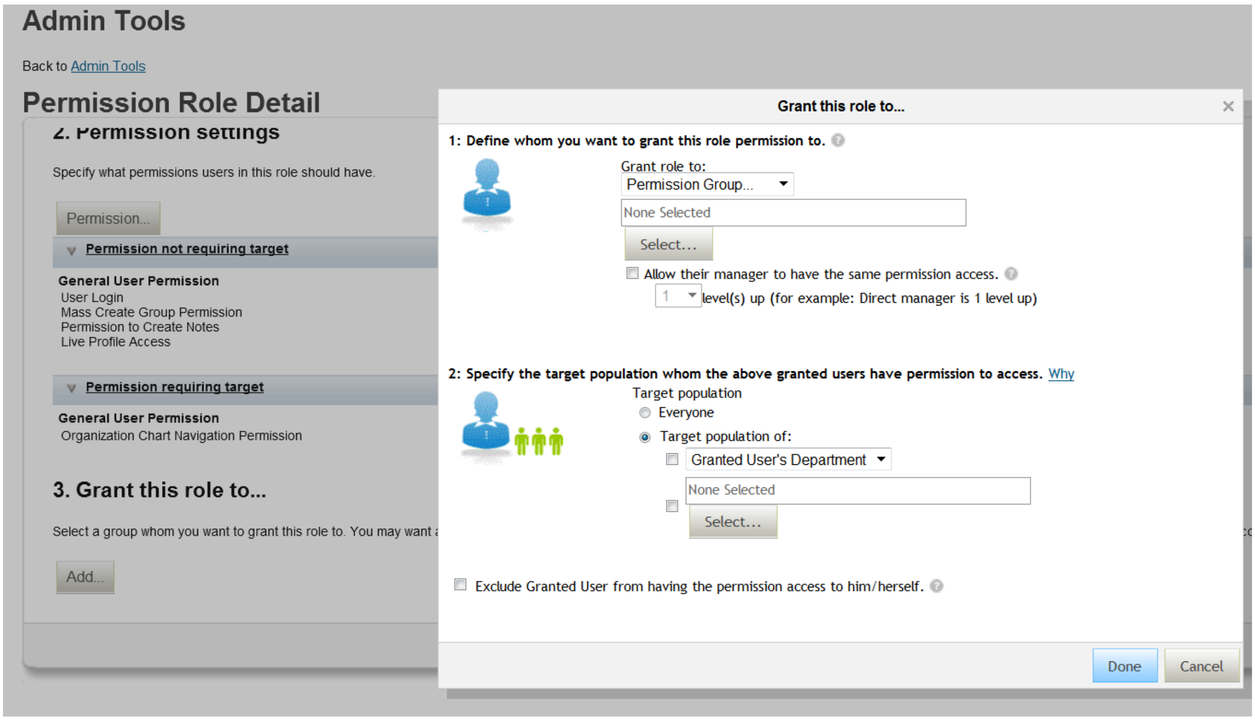
□ Mobile Organization Chart Access

□ Mobile Touchbase Access

□ Organization Chart Navigation Permission†

Done Cancel

9. Select the checkboxes next to the permissions you'd like to grant to the role.
10. Click the *Done* button when you finish marking your selections.
11. In the *Grant this role to* section, click the *Add* button to select the employees to be granted this permission. The *Grant this role* to page opens.



Admin Tools

Back to Admin Tools

Permission Role Detail

2. Permission settings

Specify what permissions users in this role should have.

Permission...

Permission not requiring target

General User Permission<br>
User Login<br>
Mass Create Group Permission<br>
Permission to Create Notes<br>
Live Profile Access

Permission requiring target

General User Permission<br>
Organization Chart Navigation Permission

3. Grant this role to...

Select a group whom you want to grant this role to. You may want

Add...

**Grant this role to...**

1: Define whom you want to grant this role permission to.

Grant role to: Permission Group...

None Selected

Select...

□ Allow their manager to have the same permission access.

1 level(s) up (for example: Direct manager is 1 level up)

2: Specify the target population whom the above granted users have permission to access. Why

Target population

○ Everyone

● Target population of:

□ Granted User's Department

□ None Selected

Select...

□ Exclude Granted User from having the permission access to him/herself.

Done Cancel

12. Grant the permissions and specify the target population. For a detailed description, see the section How can you grant permission roles? [page 26].

13. For some permissions, it might be necessary to exclude the granted users from applying the permissions on themselves. For this, select *Exclude Granted User from having the permission access to him/herself*.

    Example

    If the role grants permission to edit the salary, you want to prevent the members of this permission group to be able to edit their own salary as well.

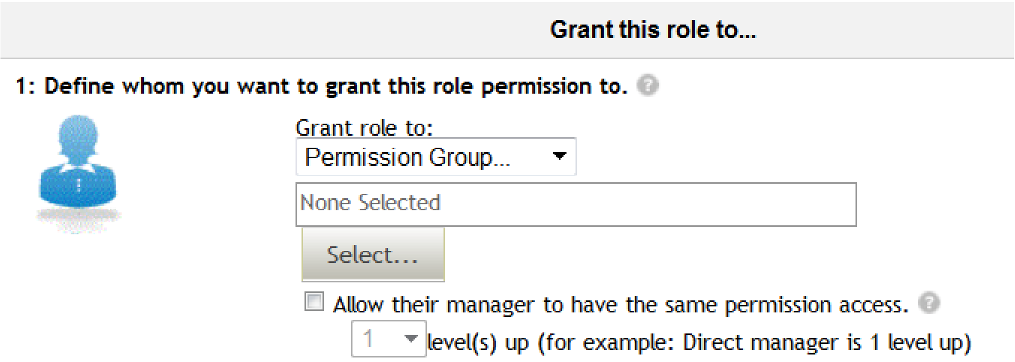
14. Click the *Done* button to assign this role to the defined users. You are taken back to the *Permission Role Detail* page.
15. Click the *Save Changes* button to complete creating the role.

Once this role is successfully created, the new role will be listed on the Permission Role List page.

## 4.3 How can you grant permission roles?

You can grant a permission role to everyone, or to a subset of employees determined by permission groups or relationships.

- Permission groups: You assign a permission role to a defined group of users. However, relationships can also play a role here as you can define that the granted user's managers have the same permissions. You can also define how many levels up in the hierarchy you want this permission to be granted.



Grant this role to...

1: Define whom you want to grant this role permission to.

Grant role to: Permission Group...

None Selected

□ Allow their manager to have the same permission access.

1 level(s) up (for example: Direct manager is 1 level up)

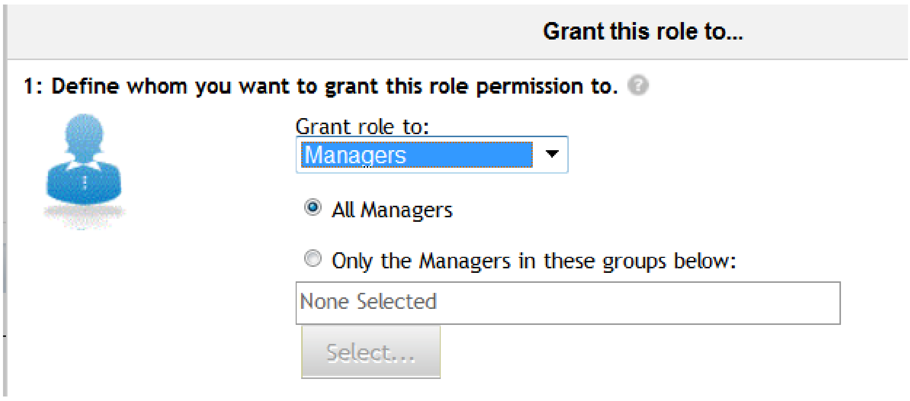
Note

If you allow the respective managers to have the same permissions, this may have a negative impact on the performance. The hierarchy then has to be checked whenever such a manager tries to access an element which was permissioned this way.

Note

If you want to grant a role to a named user, you first have to create a group and add the user to this group. Then you can grant the role to the just created group.

- In the second case, you use relationships (for example, manager -employee relationship) derived from the job relationship object. These relationships can be hierarchical or non-hierarchical. You can find more information in the following chapter Using Relationships to Grant Permissions [page 27]



Grant this role to...

1: Define whom you want to grant this role permission to.

Grant role to: Managers

● All Managers

○ Only the Managers in these groups below:

None Selected

Depending on the permissions included in the role, you might also have to define the target population. Not all permissions require you to define a target population. For example, if the permission includes just the access to an application (such as the Learning Access Permission), there is no need to add a target group. For each permission it's indicated on the screen by a "t" whether it needs a target population. Target populations can also be groups or can be derived from relationships.

## 4.3.1 Using Relationships to Grant Permissions

### General Relationship Types

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

- Manager
- Second/Alternate Manager
- HR Manager
- Matrix Manager
- Custom Manager

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: Relationship Types for Global Assignments

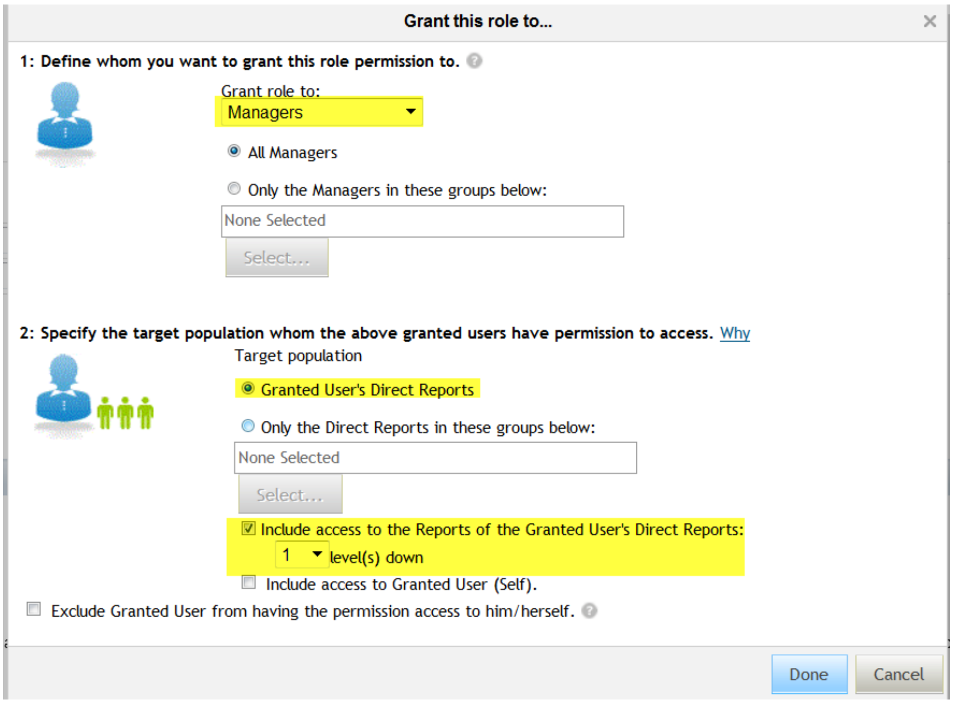
If employees have global assignments (that is, a job in another country), they have both a home manager and a host manager. In addition, they have a home HR manager and a host HR manager. All managers need to have access to both the home jobs of the employees as well as to the host jobs of the employees.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

- Home Managers

- Home HR Managers
- Host Managers
- Host HR Managers

## 4.3.2 Specifying the Hierarchy Depth

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.



Grant this role to...

1: Define whom you want to grant this role permission to.

Grant role to: Managers

● All Managers

○ Only the Managers in these groups below:

None Selected

Select...

2: Specify the target population whom the above granted users have permission to access. Why

Target population

● Granted User's Direct Reports

○ Only the Direct Reports in these groups below:

None Selected

Select...

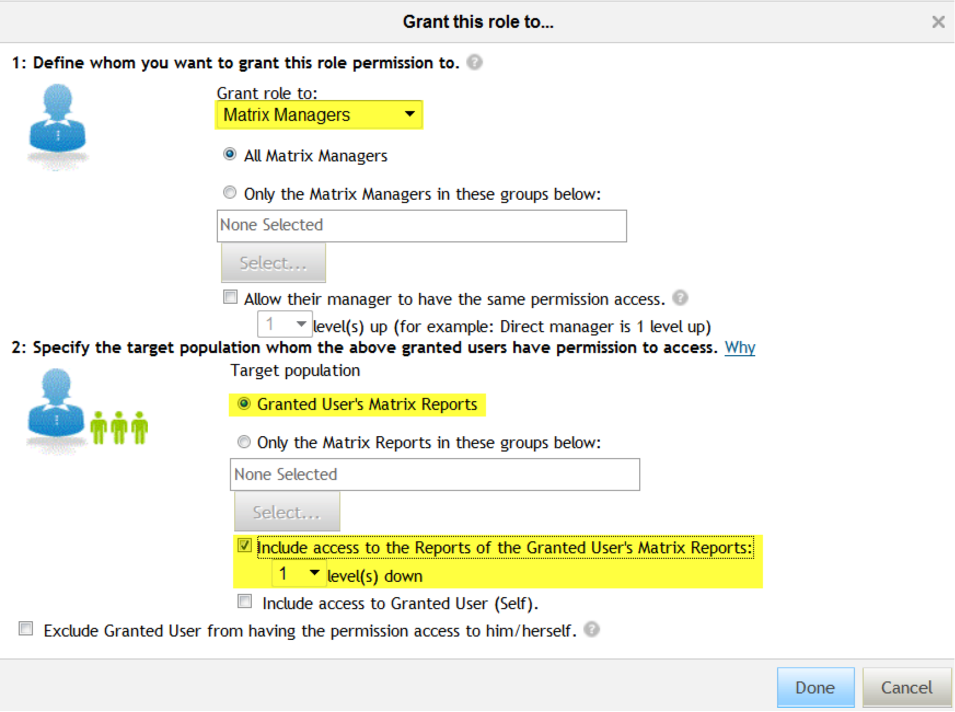
☑ Include access to the Reports of the Granted User's Direct Reports:

1 level(s) down

□ Include access to Granted User (Self).

□ Exclude Granted User from having the permission access to him/herself.

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.



Grant this role to...

1: Define whom you want to grant this role permission to.

Grant role to:

Matrix Managers

● All Matrix Managers

○ Only the Matrix Managers in these groups below:

None Selected

□ Allow their manager to have the same permission access.

1 level(s) up (for example: Direct manager is 1 level up)

2: Specify the target population whom the above granted users have permission to access. Why

Target population

● Granted User's Matrix Reports

○ Only the Matrix Reports in these groups below:

None Selected

☑ Include access to the Reports of the Granted User's Matrix Reports:

1 level(s) down

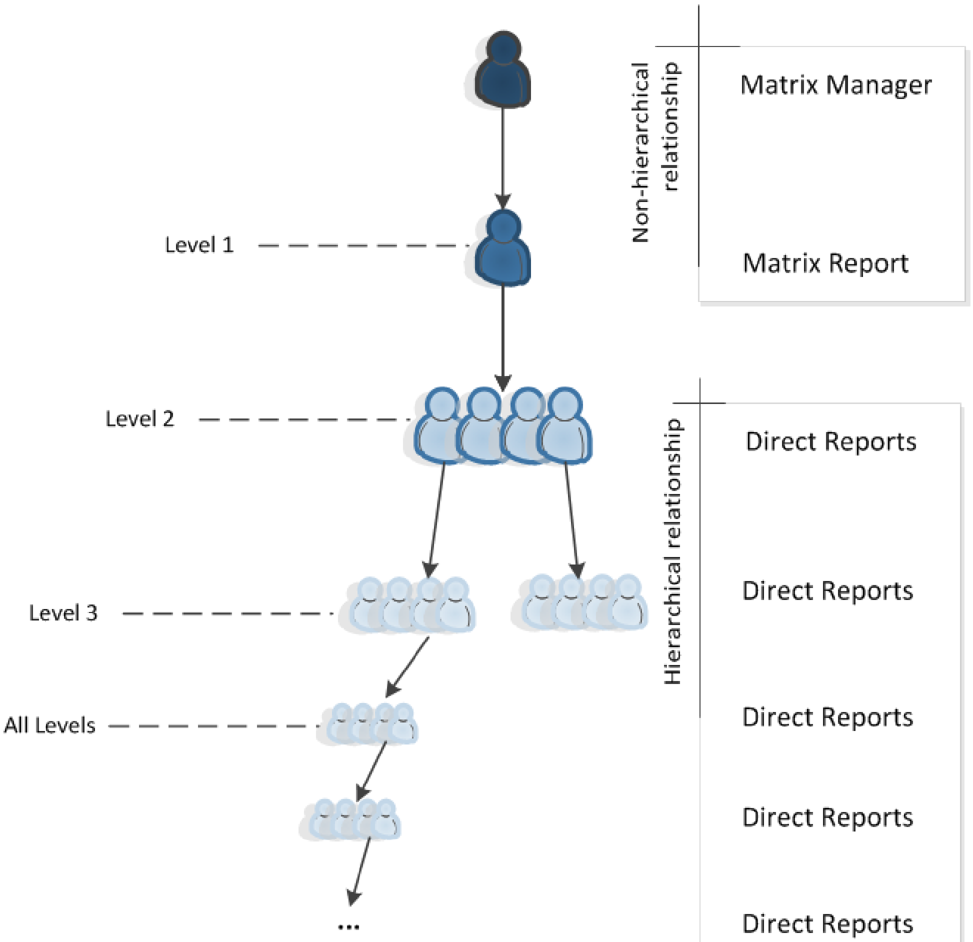
□ Include access to Granted User (Self).

□ Exclude Granted User from having the permission access to him/herself.

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

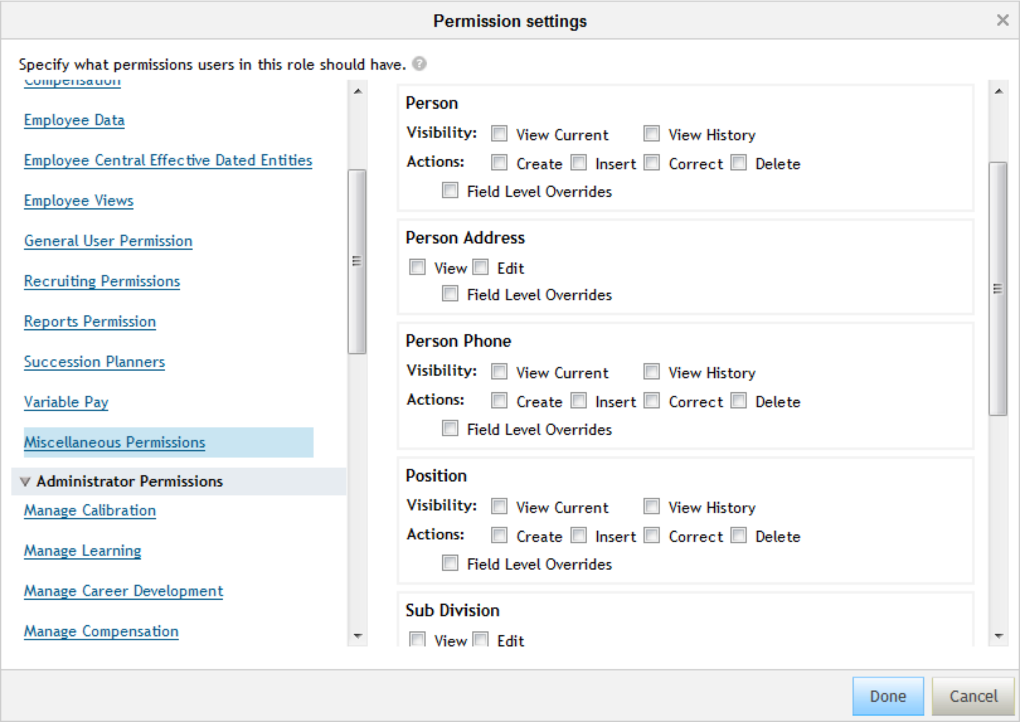
- 1 Level Deep: Matrix Managers can view ratings information for their Matrix Reports.
- 2 Levels Deep: Matrix Managers can view ratings information for their Matrix Reports and the Direct Reports of their Matrix Reports.
- All Levels Deep: Matrix Managers can view ratings information for their Matrix 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:


Matrix Manager
Non-hierarchical relationship
Level 1
Matrix Report
Level 2
Direct Reports
Hierarchical relationship
Level 3
Direct Reports
All Levels
Direct Reports
Direct Reports
Direct Reports
...

## 4.4 Granting Permissions for MDF Objects

You can grant permissions for viewing or editing generic objects which are part of the Meta Data Framework (MDF). These objects, such as "Position", "Time", or "Absence", appear under *Miscellaneous Permissions* when you create permission roles.



Permission settings

Specify what permissions users in this role should have.

Compensation

Employee Data

Employee Central Effective Dated Entities

Employee Views

General User Permission

Recruiting Permissions

Reports Permission

Succession Planners

Variable Pay

Miscellaneous Permissions

▼ Administrator Permissions

Manage Calibration

Manage Learning

Manage Career Development

Manage Compensation

Person

Visibility: □ View Current □ View History

Actions: □ Create □ Insert □ Correct □ Delete

□ Field Level Overrides

Person Address

□ View □ Edit

□ Field Level Overrides

Person Phone

Visibility: □ View Current □ View History

Actions: □ Create □ Insert □ Correct □ Delete

□ Field Level Overrides

Position

Visibility: □ View Current □ View History

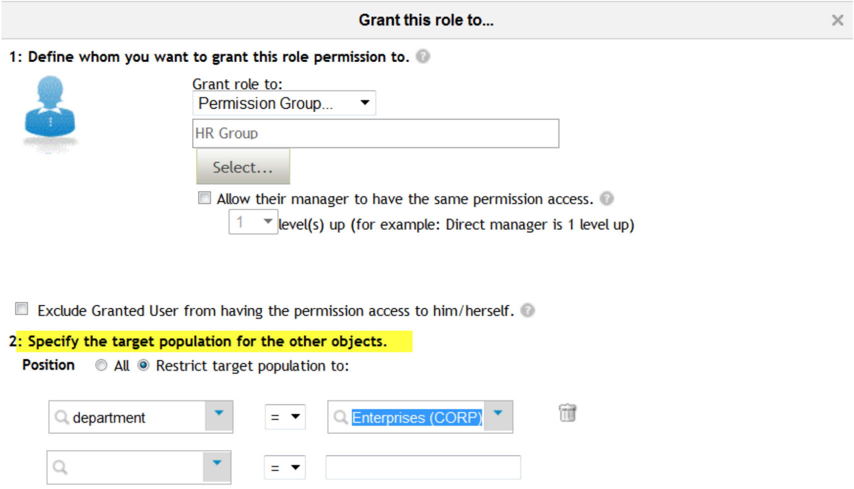
Actions: □ Create □ Insert □ Correct □ Delete

□ Field Level Overrides

Sub Division

□ View □ Edit

Whenever you select to add permissions for a generic object to a permission role, you have to define a target population for this object. For this, the "Specify the target population for the other objects" section appears on the "Grant this role to..." screen. The target population in this context is made up of the specific objects that may be accessed. When you grant the role to the permissioned users, you use various selection criteria to specify the specific objects.



Grant this role to...

1: Define whom you want to grant this role permission to.

Grant role to: Permission Group...

HR Group

□ Allow their manager to have the same permission access.

1 level(s) up (for example: Direct manager is 1 level up)

□ Exclude Granted User from having the permission access to him/herself.

2: Specify the target population for the other objects.

Position ○ All ● Restrict target population to:

department = Enterprises (CORP)

=

Example

You grant the permission to edit positions. As target population for this permission, you define the finance department. The permissioned users are then allowed to change positions in the finance department only. If you would choose *All*, the users could change all positions.

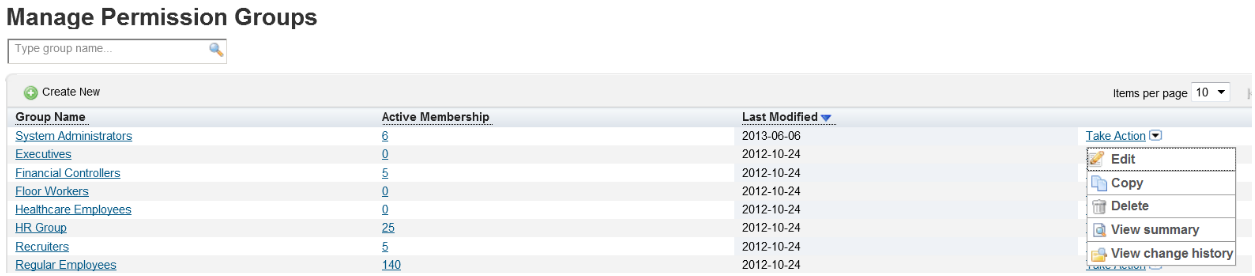
## 4.5 Further actions on permission groups

You can edit, copy, or delete permission groups and also view a summary of a permission group and its change history.

Note

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

1. Go to *Administration Tools*. In the *Manage Employees* portlet, select *Set User Permissions*.
2. In the *Set User Permissions* section, select *Manage Permission Groups*. The *Manage Permission Groups* page opens.
3. Click *Take Action* next to the Permission Group you want to modify.
4. Choose the desired action.



Manage Permission Groups

Type group name...

Create New

Items per page 10

| Group Name | Active Membership | Last Modified | |
|---|---|---|---|
| System Administrators | 6 | 2013-06-06 | Take Action |
| Executives | 0 | 2012-10-24 | |
| Financial Controllers | 5 | 2012-10-24 | |
| Floor Workers | 0 | 2012-10-24 | |
| Healthcare Employees | 0 | 2012-10-24 | |
| HR Group | 25 | 2012-10-24 | |
| Recruiters | 5 | 2012-10-24 | |
| Regular Employees | 140 | 2012-10-24 | |

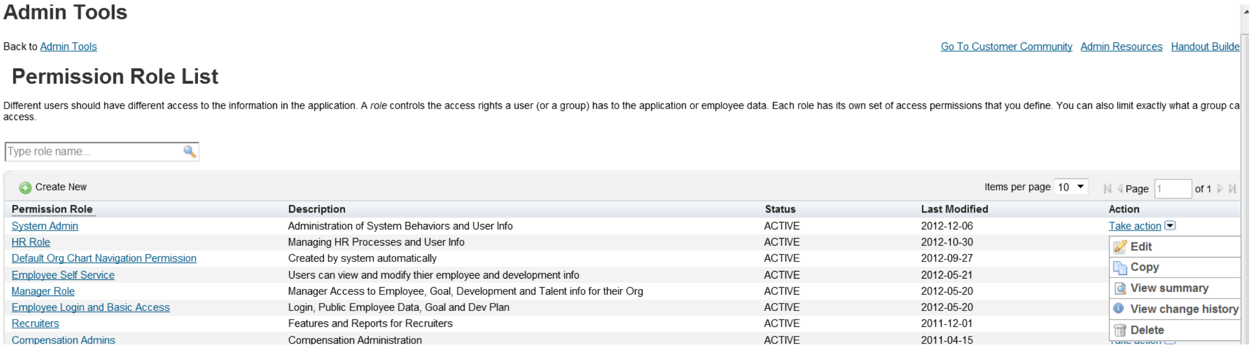
## 4.6 Further Actions on Permission Roles

You can edit, copy, or delete a role and also view a summary of a permission role and its change history.

Note

When copying a role, only the permissions get copied over. You will need to manually grant employees access to this new role.

1. Go to *Administration Tools*. In the *Manage Employees* portlet, select *Set User Permissions*.
2. In the *Set User Permissions* section, select *Manage Permission Roles*. The Permission Role List page opens displaying a list of permission roles in the system.
3. Click the *Take Action* next to the role you'd like to work on.
4. Choose the desired action.



## Admin Tools

Back to Admin Tools

Go To Customer Community   Admin Resources   Handout Builde

## Permission Role List

Different users should have different access to the information in the application. A *role* controls the access rights a user (or a group) has to the application or employee data. Each role has its own set of access permissions that you define. You can also limit exactly what a group ca access.

Type role name...

Create New

Items per page 10   Page 1 of 1

| Permission Role | Description | Status | Last Modified | Action |
|---|---|---|---|---|
| System Admin | Administration of System Behaviors and User Info | ACTIVE | 2012-12-06 | Take action |
| HR Role | Managing HR Processes and User Info | ACTIVE | 2012-10-30 | |
| Default Org Chart Navigation Permission | Created by system automatically | ACTIVE | 2012-09-27 | |
| Employee Self Service | Users can view and modify thier employee and development info | ACTIVE | 2012-05-21 | |
| Manager Role | Manager Access to Employee, Goal, Development and Talent info for their Org | ACTIVE | 2012-05-20 | |
| Employee Login and Basic Access | Login, Public Employee Data, Goal and Dev Plan | ACTIVE | 2012-05-20 | |
| Recruiters | Features and Reports for Recruiters | ACTIVE | 2011-12-01 | |
| Compensation Admins | Compensation Administration | ACTIVE | 2011-04-15 | Take action |

# 5 Testing and Copying the RBP Configuration

## 5.1 Conducting Tests

After you have set up 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.

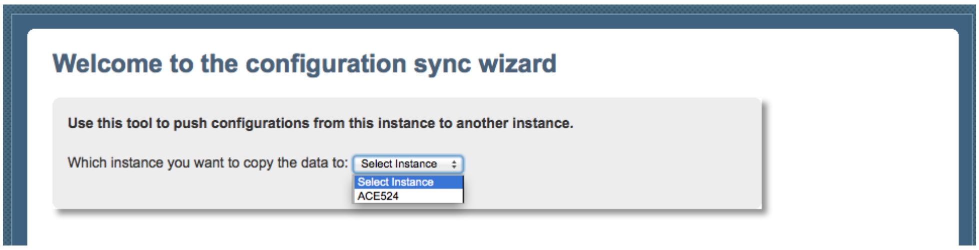
Testing roles which do not require specific groups but make use of relationships is easier. You just need test users for all hierarchy levels, like manager, HR Manager, and employee. Double check the hierarchy, then log on as a specific test user and double check the permissions.

## 5.2 Copying RBP Configuration to Production Instance

After the tests are complete and you solved all issues, you copy the RBP configuration to the production instance. You can do this in Admin tools using the Instance Sync tool. You may need to ask SuccessFactors to enable this tool for your test and production systems.

1. Grant the permission to use the Instance Sync tool to the appropriate role:
   1. Log on to the instance and choose *Admin Tools*.
   2. Choose *Set User Permissions* → *Manage Permission Roles*.
   3. Select the role which will be responsible for synching data between instances and choose *Take action* → *Edit*.
   4. Under *Permission Settings* click *Permissions...*
   5. Click *Data Management* and select *Sync RBP Permission Roles* and *Sync RBP Permission Groups*.
   6. Log out and back in.
2. Copy roles and groups:
   1. Choose *Admin Tools* → *Synchronize Instance Configurations*.

      The configuration sync wizard starts.

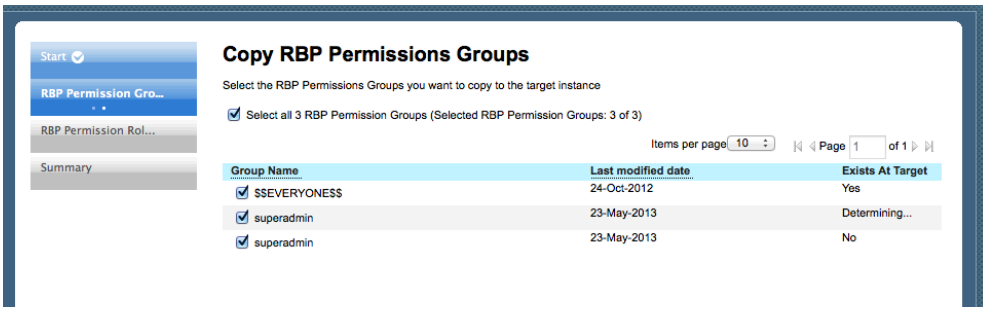


Welcome to the configuration sync wizard

Use this tool to push configurations from this instance to another instance.

Which instance you want to copy the data to: Select Instance

2. Follow the wizard to select the target instance, and the groups and roles to be copied.



Copy RBP Permissions Groups

Select the RBP Permissions Groups you want to copy to the target instance

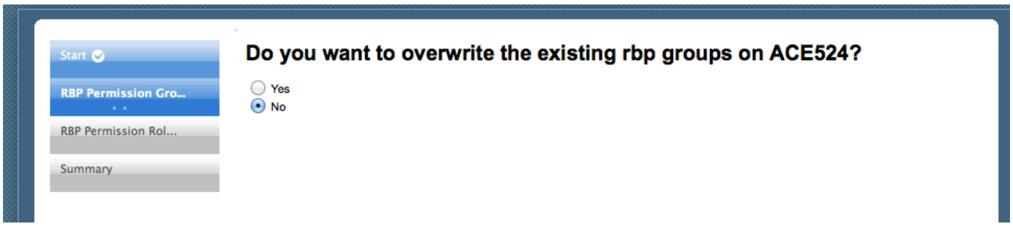
☑ Select all 3 RBP Permission Groups (Selected RBP Permission Groups: 3 of 3)

Items per page 10 | Page 1 of 1

| Group Name | Last modified date | Exists At Target |
|---|---|---|
| ☑ $$EVERYONE$$ | 24-Oct-2012 | Yes |
| ☑ superadmin | 23-May-2013 | Determining... |
| ☑ superadmin | 23-May-2013 | No |

Tips for copying 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.



Do you want to overwrite the existing rbp groups on ACE524?

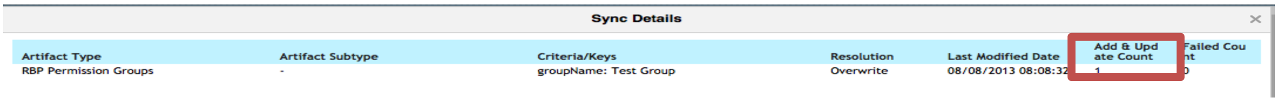
○ Yes
● No

Tips for copying 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

3. Choose *Test Sync* and evaluate the results of the test run.

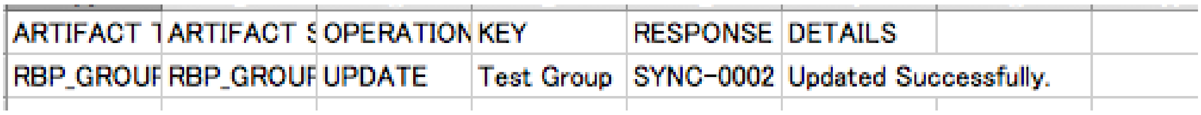
If the sync was successful, you will see in the UI that the *Add & Update Count* has been updated with the number of groups copied.



Sync Details

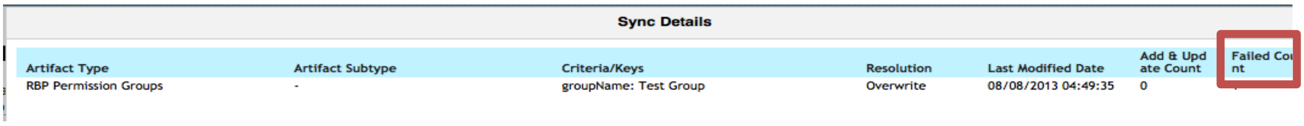
| Artifact Type | Artifact Subtype | Criteria/Keys | Resolution | Last Modified Date | Add & Update Count | Failed Count |
|---|---|---|---|---|---|---|
| RBP Permission Groups | - | groupName: Test Group | Overwrite | 08/08/2013 08:08:32 | 1 | 0 |

In the download report you will see a success message.



| ARTIFACT T | ARTIFACT S | OPERATION | KEY | RESPONSE | DETAILS |
|---|---|---|---|---|---|
| RBP_GROUF | RBP_GROUF | UPDATE | Test Group | SYNC-0002 | Updated Successfully. |

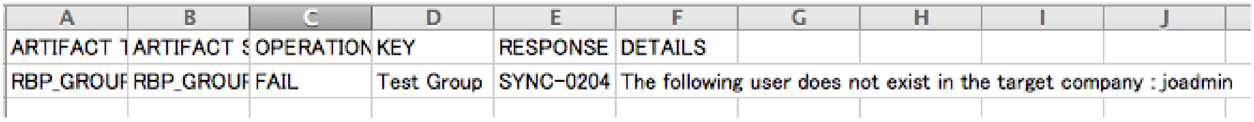
If the sync was not successful, you will see in the UI that the *Failed Count* has been updated.



Sync Details

| Artifact Type | Artifact Subtype | Criteria/Keys | Resolution | Last Modified Date | Add & Update Count | Failed Count |
|---|---|---|---|---|---|---|
| RBP Permission Groups | - | groupName: Test Group | Overwrite | 08/08/2013 04:49:35 | 0 | |

In the downloaded report, you will see the reason for the failure - for example, that the user does not exist in the target instance.



| A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|
| ARTIFACT T | ARTIFACT S | OPERATION | KEY | RESPONSE | DETAILS | | | | |
| RBP_GROUF | RBP_GROUF | FAIL | Test Group | SYNC-0204 | The following user does not exist in the target company : joadmin | | | | |

4. If the test run was successful, then choose *Run Sync Now* to actually copy the groups and roles.

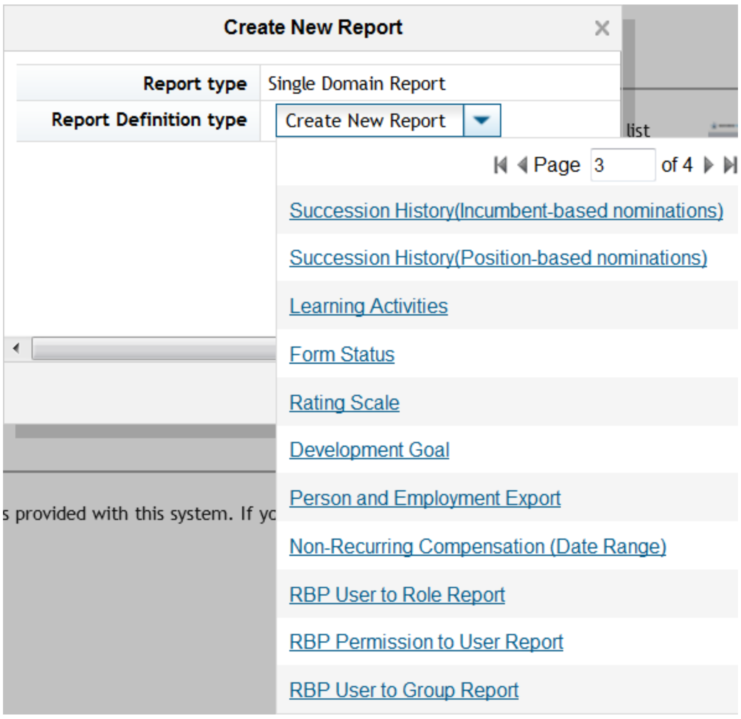
# 6 Reporting on your Permissions Configuration

## 6.1 Setting up Ad Hoc Reports

The *RBP Permission to User report* is useful for auditing purposes as well as for troubleshooting, for example, to find out why a user can see a specific field or element. We recommend setting up this report in two different ways: one report with all permissions, and one report with a filter for a single permission.

**To set up the report with all permissions:**

1. Go to the *Reporting* page in Analytics and choose *Create New Report*.
2. Select the *RBP Permission to User Report*.



Create New Report

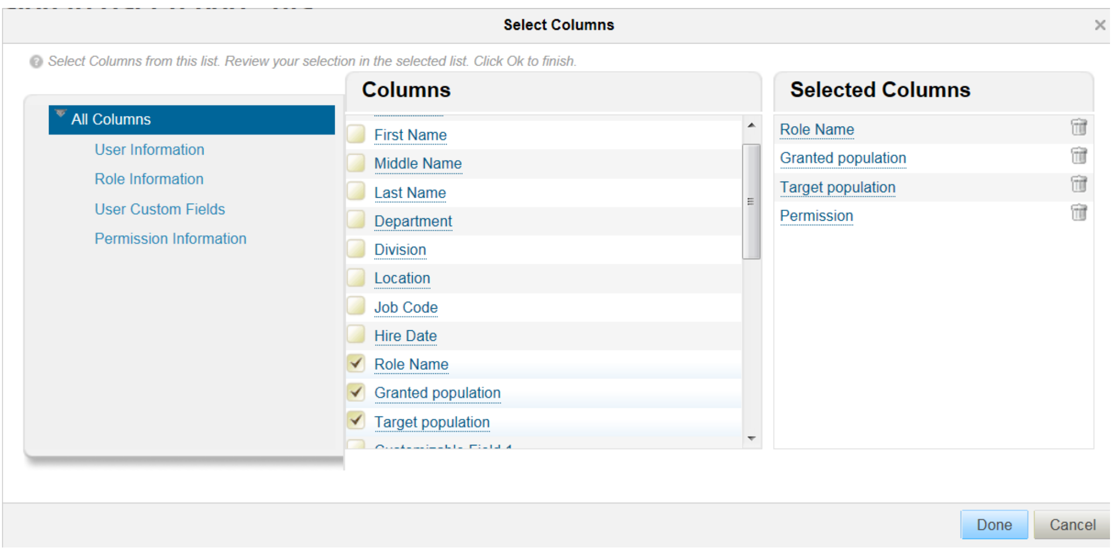
Report type: Single Domain Report

Report Definition type: Create New Report

Page 3 of 4

- Succession History(Incumbent-based nominations)
- Succession History(Position-based nominations)
- Learning Activities
- Form Status
- Rating Scale
- Development Goal
- Person and Employment Export
- Non-Recurring Compensation (Date Range)
- RBP User to Role Report
- RBP Permission to User Report
- RBP User to Group Report

3. Define the report by selecting the columns desired. Select Role Name, Granted Population, Target Population and Permission.

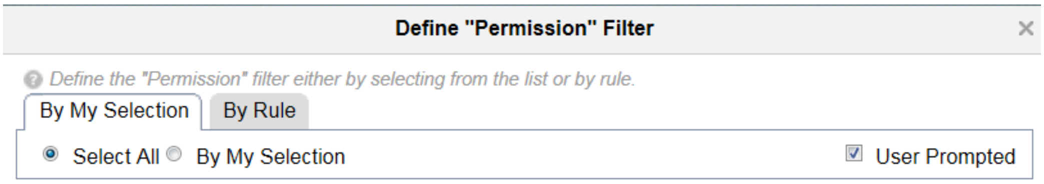


Select Columns from this list. Review your selection in the selected list. Click Ok to finish.

4. Click *Done* and save the report.

**To set up the report with a filter for permissions:**

1. Follow the steps 1- 3 of the above procedure.
2. Click *Filters* and then click *Refine Criteria*.
3. Choose *Permission* as filter.
4. On the *By My Selection* tab, choose *Select All* and mark the checkbox *User Prompted*.



Define the "Permission" filter either by selecting from the list or by rule.

● Select All ○ By My Selection ☑ User Prompted

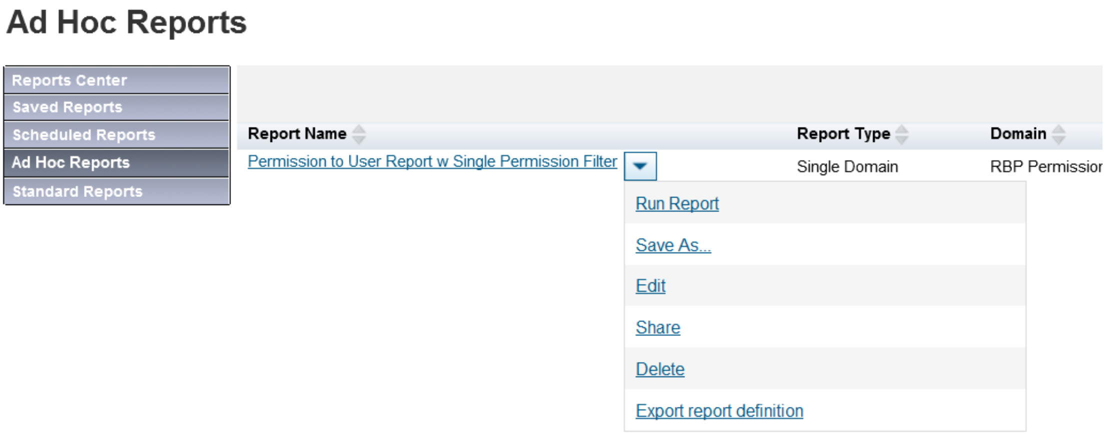
5. Click *Done* and save your changes.

When users run this report, they can specify a permission to be filtered for. This helps identify how a certain permission was granted to a user.

## 6.2 Running an Ad Hoc Report

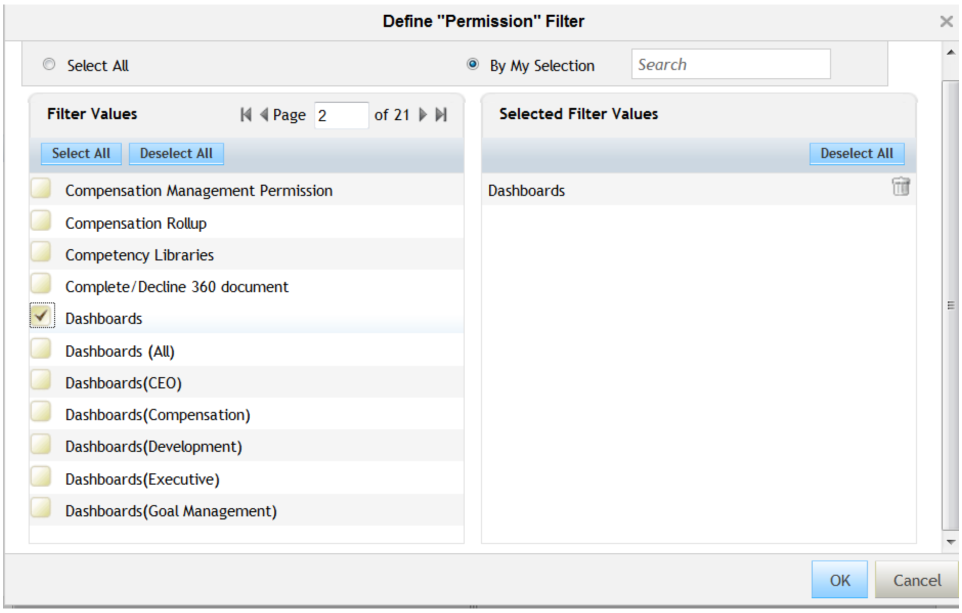
To run the *RBP Permission to User Report* with the Single Permission Filter, follow these steps:

1. Go to the *Reporting* page in Analytics and choose Ad Hoc Reports.
2. Open the menu next to the report name and choose *Run Report*.



| Report Name | Report Type | Domain |
|---|---|---|
| Permission to User Report w Single Permission Filter | Single Domain | RBP Permissior |

3. On the *Execute Permission to User...* screen, open the *Take Action* menu and choose *Edit*.
4. Choose *By My Selection* and select the permission you are interested in.

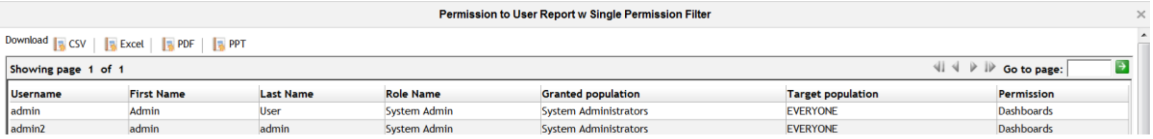


○ Select All ● By My Selection

- □ Compensation Management Permission
- □ Compensation Rollup
- □ Competency Libraries
- □ Complete/Decline 360 document
- ☑ Dashboards
- □ Dashboards (All)
- □ Dashboards(CEO)
- □ Dashboards(Compensation)
- □ Dashboards(Development)
- □ Dashboards(Executive)
- □ Dashboards(Goal Management)

Selected Filter Values: Dashboards

5. Click *OK* and then *Generate Report*.
6. In the report, you can now see exactly to which role(s) the permission is granted.



Permission to User Report w Single Permission Filter

Showing page 1 of 1

| Username | First Name | Last Name | Role Name | Granted population | Target population | Permission |
|---|---|---|---|---|---|---|
| admin | Admin | User | System Admin | System Administrators | EVERYONE | Dashboards |
| admin2 | admin | admin | System Admin | System Administrators | EVERYONE | Dashboards |

# 7 Troubleshooting

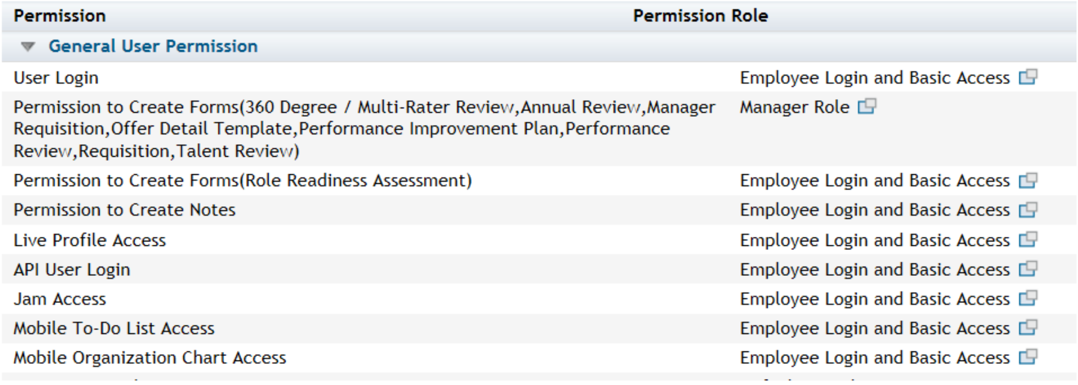
If you find that users have access to applications or data they should not have, we recommend the following steps:

1. Run the *View User Permission report* to determine how - through which role - the permission was granted to the employees. For details see How can you check the permissions assigned to a user? [page 41]
2. If that does not clarify how/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. For details see Running an Ad Hoc Report [page 38].

## 7.1 How can you check the permissions assigned to a user?

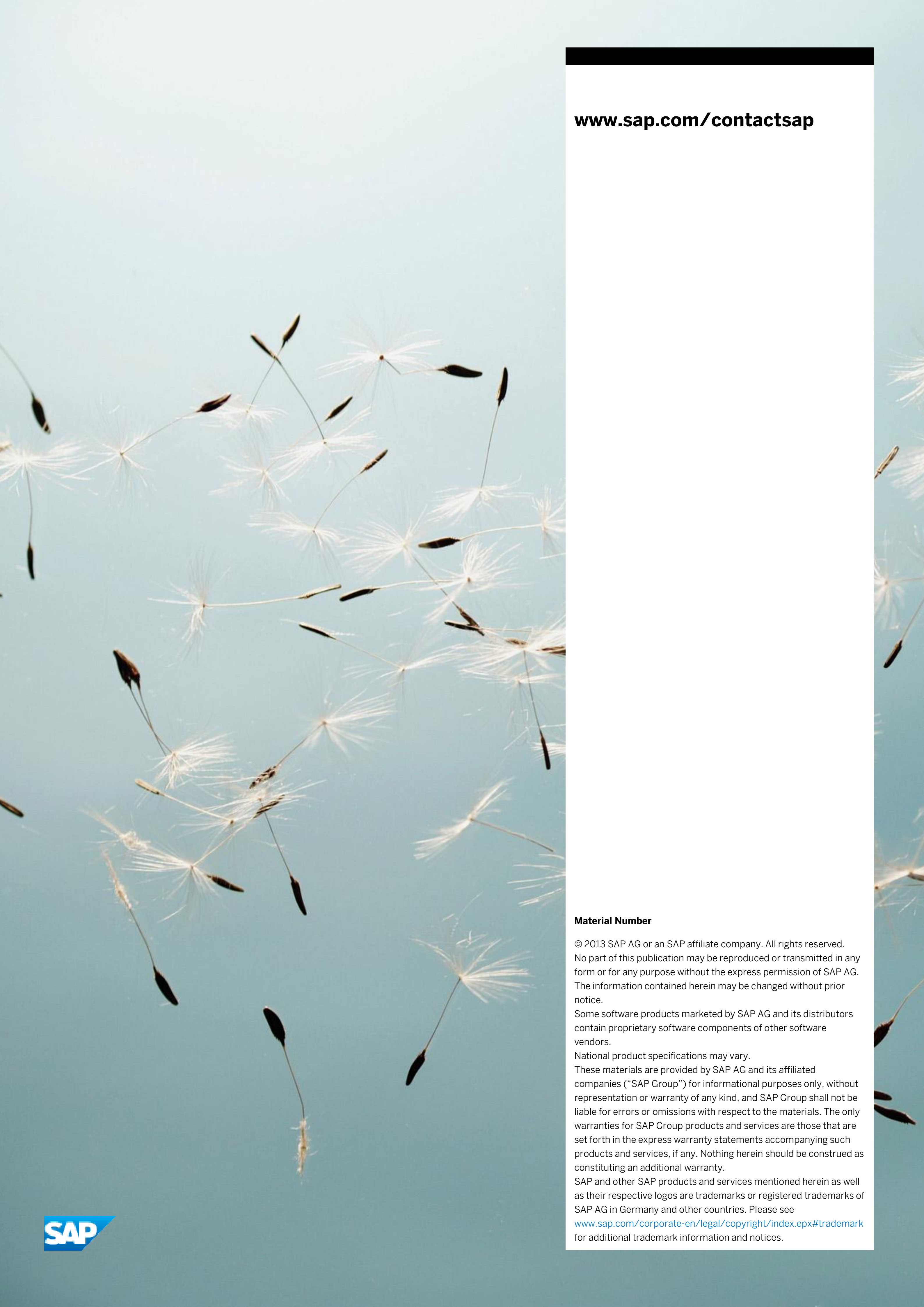
1. Go to Administration Tools.
2. In the *Manage Employees* portlet, select *Set User Permissions*.
3. In the *Set User Permissions* section, select *View User Permissions*.
4. In the Advanced Search, enter the user name.
5. Click *View Permission* next to the user name.

   A list of permissions is displayed along with the roles that grant those permissions.



| Permission | Permission Role |
|---|---|
| ▼ General User Permission | |
| User Login | Employee Login and Basic Access |
| Permission to Create Forms(360 Degree / Multi-Rater Review,Annual Review,Manager Requisition,Offer Detail Template,Performance Improvement Plan,Performance Review,Requisition,Talent Review) | Manager Role |
| Permission to Create Forms(Role Readiness Assessment) | Employee Login and Basic Access |
| Permission to Create Notes | Employee Login and Basic Access |
| Live Profile Access | Employee Login and Basic Access |
| API User Login | Employee Login and Basic Access |
| Jam Access | Employee Login and Basic Access |
| Mobile To-Do List Access | Employee Login and Basic Access |
| Mobile Organization Chart Access | Employee Login and Basic Access |

6. To learn more about the roles, click the pop-up window icon next to any role name.



**www.sap.com/contactsap**

**Material Number**