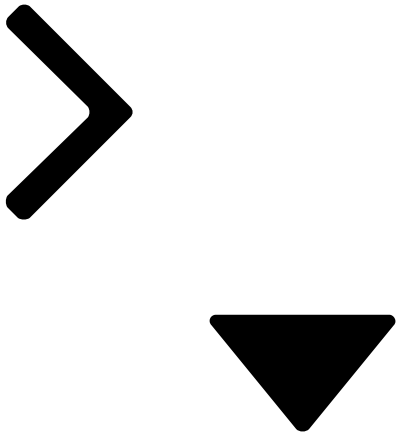
1. Data Security



2. Define Sharing Rules

Define Sharing Rules

Learning Objectives

After completing this unit, you'll be able to:

- Use sharing rules to extend access beyond the role hierarchy structure.
- Create a public group that includes users with different profiles and roles.

Extend Access with Sharing Rules

Your org-wide default sharing settings give you a (relatively restrictive) baseline level of access for each object. If you have org-wide sharing defaults of Public Read Only or Private, you can open access back up for some users with sharing rules. This enables you to make automatic exceptions to your org-wide sharing settings for selected sets of users.

Sharing rules can be based on who owns the record or on the values of fields in the record. For example, use sharing rules to extend sharing access to users in public groups or roles. As with role hierarchies, sharing rules can never be stricter than your org-wide default settings. They just allow greater access for particular users.

Each sharing rule has three components.

Share which records?
You can share records owned by certain users or meeting certain criteria. Criteria-based sharing rules determine what records to share based on field values other than ownership.

With which users?
You can define groups of users by role, by territory, or by defining a public group. A public group is an admin-defined grouping of users that can be used to simplify the creation of sharing rules. Each public group can be a combination of:

- individual users
- roles
- roles and subordinates
- territories
- territories and subordinates
- other public groups

What kind of access?
You can assign either Read-Only or Read/Write access.

Sharing rules work best when they're defined for a particular group of users that you can determine or predict in advance, rather than a set of users that frequently changes. For example, in the Recruiting app, it's important to share every position, candidate, job application, and review with every recruiter. Since recruiters all belong to either the Recruiting Manager or Recruiter roles in the role hierarchy, we can easily use a sharing rule to share those objects with the Recruiting Manager role and its subordinates.

Alternatively, consider another use case from the Recruiting app: interviewers need read access on the candidates and job applications for people they're interviewing. In this case, the set of interviewers is a lot harder to predict in advance—hiring managers might use different sets of interviewers depending on the position for which they're hiring, and the interviewers might come from different groups in the role hierarchy. So, this use case probably shouldn't be handled with sharing rules—the team of interviewers for any given manager is just too hard to predict.

Should we use a sharing rule?

Let's go through the set of required permissions we still want to implement and pick out the ones that work best with sharing rules.

Recruiters need read and update access on every position, candidate, job application, and review record that exists in the app.
Yes. As we discussed previously, it's easy to pick out the group of recruiters in our role hierarchy.

Hiring managers need read and update access on position and job posting records on which they're the hiring manager.
No. It's too hard to predict which positions will be assigned to which hiring manager. We'll need to handle this use case some other way.

Hiring managers need read access on candidate records on which they're the hiring manager.
No. Again, it's too hard to predict which positions will be assigned to which hiring manager.

Hiring managers need read and update access on every job application and review record.
Yes. Since we're not restricting which job applications and reviews a hiring manager gets to read and update, we can easily pick out all of the hiring managers from our role hierarchy and define a sharing rule for them.

Interviewers need read access on the candidate and job application records for people they're interviewing.
No. As we discussed previously, it's hard to predict who will be a member of an interview team for a particular position.

To summarize, here are the key sharing rules we define for the Recruiting app.

Object	Rule Label	Owned by...	Share with...	Access Level
Review	Edit Reviews	Entire Organization	Recruiters and Hiring Managers	Read/Write
Candidate	Edit Candidates	Entire Organization	The role and subordinates of the Recruiting Manager	Read/Write
Position	Edit Positions	The role and subordinates of the Recruiting Manager	The role and subordinates of the Recruiting Manager	Read/Write

Define a Public Group

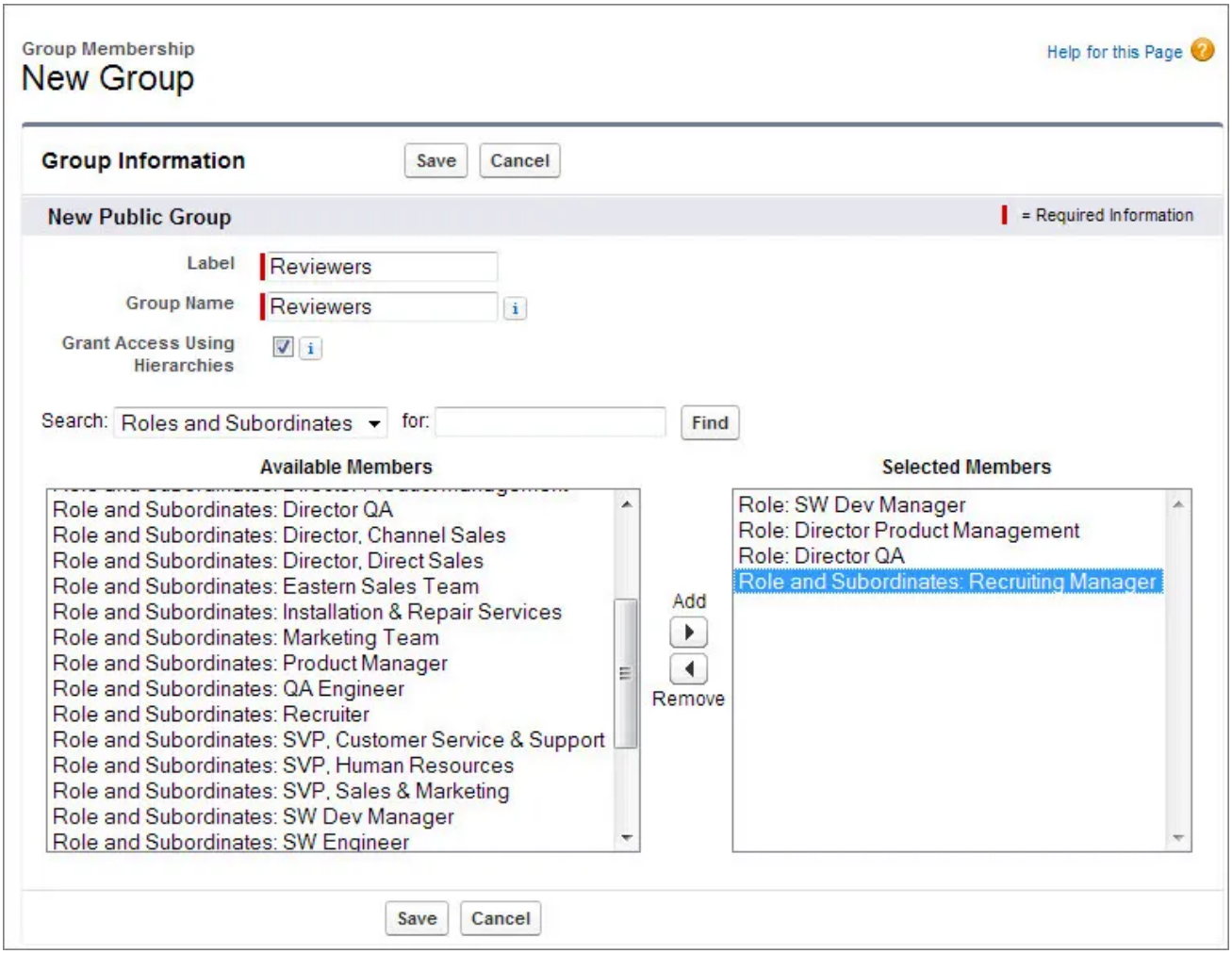
Before creating a sharing rule, it's important to set up the appropriate public group. A public group is a collection of individual users, other groups, individual roles or territories, and/or roles or territories with their subordinates that all have a function in

common. For example, users with the Recruiter profile as well as users in the SW Dev Manager role both review job applications.

Using a public group when defining a sharing rule makes the rule easier to create and, more important, easier to understand later, especially if it's one of many sharing rules that you're trying to maintain in a large organization. Create a public group if you want to define a sharing rule that encompasses more than one or two groups or roles, or any individual.

Looking at the required permissions that we want to implement, there are just two objects that need a public group for their sharing rules: Job Application and Review. The good news is that we can cover these objects in a single group because the Review object is on the detail side of a master-detail relationship, so it inherits the sharing settings we apply to the Job Application object. Since both recruiters and hiring managers need read and update access to job applications and reviews, we can define a public group called Reviewers that includes both recruiters and hiring managers.

1. In Setup, use the Quick Find box to find **Public Groups**.
2. Click **New**.



   The New Public Group page allows you to choose other public groups, individual roles, individual roles including the roles' subordinates, or individual users.
3. Give your rule the label `Reviewers` .

   The **Group Name** text box populates automatically when you click it. This is the unique name used by the API and managed packages.
4. In the **Search** drop-down list, choose Roles.
5. In the **Available Members** list, select SW Dev Manager, Director Product Management, and Director QA, then click **Add**.
6. Go back up to the **Search** drop-down list, and this time choose Role and Subordinates.
7. In the **Available Members** list, select Recruiting Manager, click **Add**, and save.

Once you've defined your group, you can use it to define sharing rules.

Define a Sharing Rule

Let's use the public group we've created to define a sharing rule for review records. You can define a sharing rule for a single public group, role, or territory. You can also define a sharing rule for a role plus its subordinates or for a territory plus its subordinates.

There is already one default public group that encompasses every user in your organization.

1. In Setup, use the Quick Find box to find **Sharing Settings**. This is the same page used to define org-wide defaults.
2. In the **Manage sharing settings for** drop-down list, choose Job Application.
   Choosing an object in this drop-down list allows you to focus in on the org-wide defaults and sharing rules for a single object at a time rather than looking at all of them in a long page—a useful thing if you've got a large org with multiple custom objects. Let's use this Sharing Rules related list to create a sharing rule that applies to both the Job Application and the Review objects.
3. In the Job Application Sharing Rules area, click **New** and give your rule the label `Review Records` .
   The **Rule Name** text box populates automatically when you click it.
4. For the rule type, make sure **Based on record owner** is selected.
5. For **Select which records to be shared**, select Public Groups, then choose Entire Organization.
6. For **Select users to share with**, select Public Groups, then choose Reviewers.
7. For **Select the level of access for the users**, select Read/Write, then save.

We just created a rule that shares reviews written and owned by any member of the org with all recruiters and hiring managers. Since reviewers and hiring managers all need to read and update reviews, we handled everyone with a single sharing rule and a public group.

Resources

- Sharing Rules
- Sharing Rule Categories
- Sharing Considerations

Assessment Complete!

+500 points

Data Security
100%
Progress: 100%
Retake this Challenge
View more modules