TIPS AND HINTS FOR SHARING DATA

Summary

Salesforce provides many flexible options for you to control how records are shared within your org. To specify the objects and tabs that a user can access, assign a profile. To specify the individual records that a user can view and edit, set your org-wide defaults, define a role hierarchy, and create sharing rules.

Objects and Records

A Salesforce org contains objects and records:

- An object is a type of data, such as a contact or a case. It consists of a number of fields, like a spreadsheet with a number of columns.
- A record is a particular instance of an object, such as the contact John Smith, or case #10044. It consists of values for each of the object's fields, like a row in the spreadsheet.

Salesforce provides many flexible options for you to control how records are shared within your org. To specify the objects and tabs that a user can access, assign a profile. To specify the individual records that a user can view and edit, set your org-wide defaults, define a role hierarchy, and create sharing rules.

Granting Access to Objects with Profiles and Permission Sets

The broadest way that you can control data is by specifying the objects that a user can view, edit, and create. You set users' object-level permissions by assigning them a profile and optionally, permission sets. The following standard profiles are available to all orgs:

Profile	Description
Read Only	Can view, but not edit, most standard objects.
Standard User	Can view and edit standard platform objects, but can only view, (not manage) campaigns, and can only create (not review) solutions.
Standard Platform User	Can access the same functionality as the Standard User, but can also use custom apps developed in your org or installed from the AppExchange.
Marketing User	Can access the same functionality as the Standard User, but can also manage campaigns, import leads, create letterheads, create HTML email templates, manage public documents, and update campaign history.
Contract Manager	Can access the same functionality as the Standard User, but can also create, edit, and activate contracts and orders.
Solution Manager	Can access the same functionality as the Standard User, but can also review and publish solutions.
System Administrator	Can create, view, edit, and delete any object, and can also use or customize any functionality that does not require an additional license. For example, administrators cannot manage campaigns unless they also have a Marketing User license.

In Professional, Enterprise, Unlimited, Performance, and Developer Edition orgs, you can use standard profiles, create custom profiles, and create permission sets to fit your business needs.

- To create a custom profile, from Setup, enter *`Profiles`* in the `Quick Find` box, then select **Profiles**, then click **New**.
- To create a permission set, from Setup, enter *`Permission Sets`* in the `Quick Find` box, then select **Permission Sets**, then click **New**.

Last updated: June 1, 2020

Specifying Default Access to Records with Organization-Wide Defaults

Tips for Sharing Records

- Solutions are accessible to all users.
- Salesforce automatically grants sharing access to users above record owners in the hierarchy. To disable this, deselect **Grant Access Using Hierarchies**.
- Forecasts are not affected by sharing settings. Instead, access to forecasts is determined by the role hierarchy. All users can see their own forecasts and those of people below them in the role hierarchy.
- Set price book access from Setup by entering *Sharing Settings* in the Quick Find box and then selecting **Sharing Settings**.

Once you specify object-level permissions in a user's profile or permission sets, you can specify the individual records to which a user has access.

Default access to records is specified with org-wide defaults for objects. To set your org's defaults, from Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings** and edit the org-wide defaults section.

- How do I give all users access to view, edit, delete or transfer any campaign?
  - Set Default Access for campaigns to **Public Full Access**.
- How do I give all users full access to view, edit, or transfer any case?
  - Set Default Access for cases to **Public Read/Write/Transfer**.
- How do I give all users full access to view, edit, or transfer any lead?
  - Set Default Access for leads to **Public Read/Write/Transfer**.
- How do I give all users full access to view and edit any record?
  - Select **Public Read/Write** for all sharing options.
- How do I give all users read access but restrict editing to records they own?
  - Select **Public Read Only** for all sharing options.
- How do I give users read and edit access to all accounts but prevent them from seeing and editing each other's deals?
  - Choose **Public Read/Write** for accounts and **Private** for opportunities.
- If your org-wide default is Public Read Only or Private, create sharing rules to extend access to additional users.
- Set the Opportunity Access on each role to determine whether users can view and edit opportunities they do not own but are related to accounts they do own.

Sharing Records with a Role Hierarchy

Profiles and Roles

Users can be assigned to one profile, one role, and as many permission sets as the org's edition allows. These work together to determine the data a user can view and edit:

- The profile controls a user's object- and field-level permissions, including the apps and tabs that appear when the user logs in. Every user must be assigned to a profile.
- Any permission sets assigned to a user may grant additional object- and field-level permissions.
- The role influences a user's ability to view and edit individual object records through role hierarchy and sharing rules. A user doesn't have to be assigned to a role to use Salesforce.

Once you have defined your org-wide defaults, use a role hierarchy to ensure that managers can view and edit the same records their employees can. Users at any given role level are always able to view, edit, and report on all data owned by or shared with users below them in the hierarchy, unless an object's settings specify ignoring the hierarchies.

To define your org's role hierarchy, from Setup, enter *Roles* in the Quick Find box, then select **Roles**. Role hierarchies don't need to match your org chart exactly. Instead, each role in the hierarchy should represent a level of data access that a user or group of users needs.

Sharing Groups

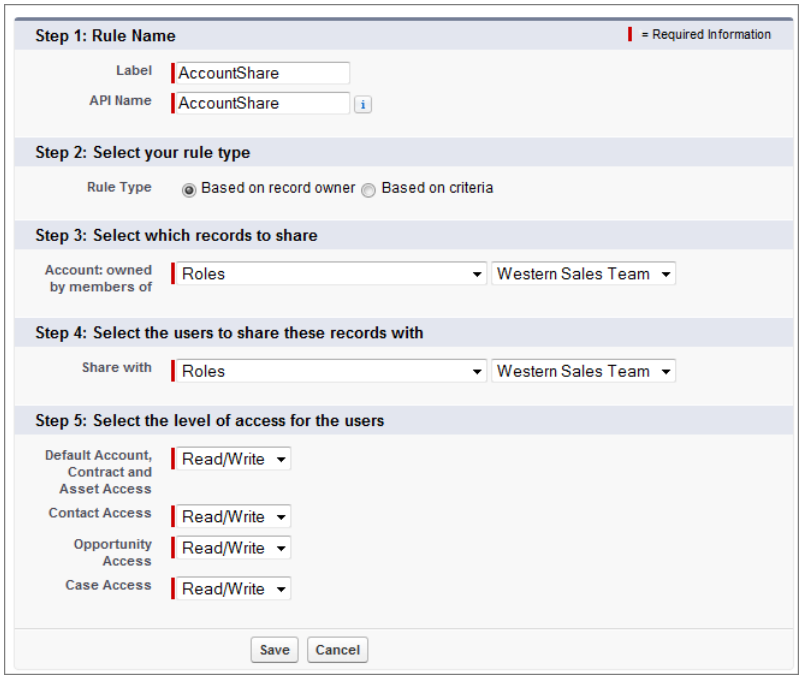
The most common groups for sharing records with are:

- **Public Groups**—to give access to any group you have created. A public group can include users, members of a role, members of a role and subordinates, or other public groups.
- **Roles**—to give access to the members of a role in the role hierarchy
- **Roles and Subordinates**—to give access to the members of a role including their subordinates

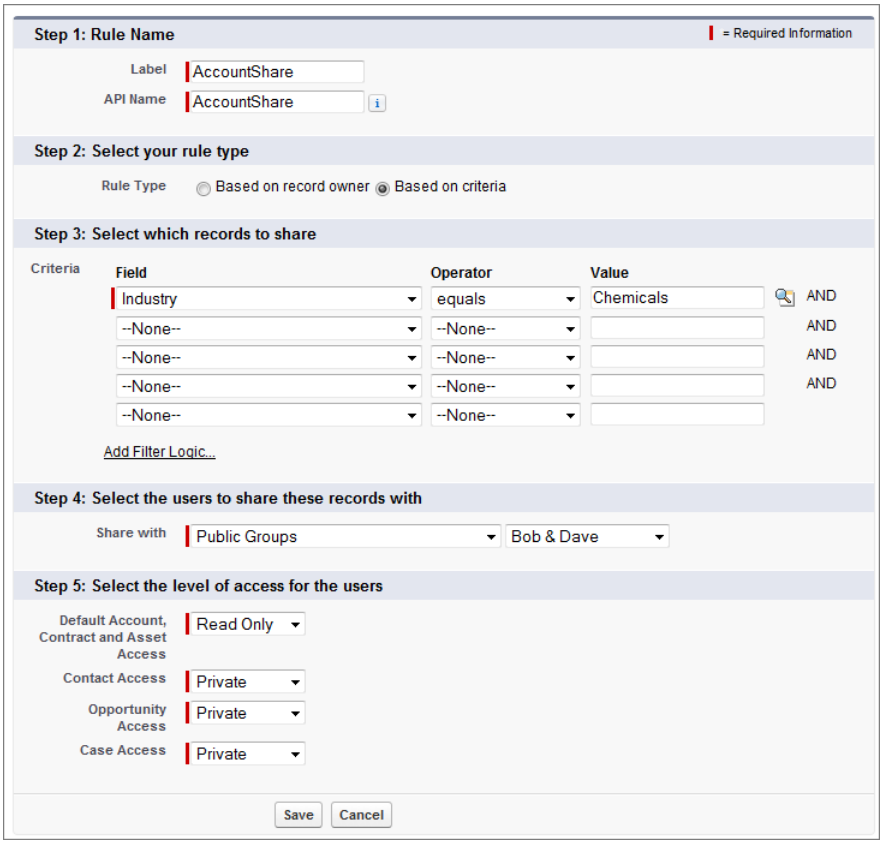
Sharing Records with Sharing Rules

Sharing rules extend the access specified by org-wide defaults and the role hierarchy. Sharing rules are typically based on record ownership, or in some cases, other criteria. To define sharing rules, from Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings**, then in a sharing rules related list, click **New**. Following are a few common scenarios and their solutions using sharing rules:

- Your company has two sales divisions: Eastern and Western. The Western sales reps want to share all account and opportunity records with their colleagues within their division. The Eastern sales division prefers to keep data private. For this example, you can choose a **Private** org-wide default for accounts and contacts. Then create a sharing rule that gives the Western Sales Team read and write access to all accounts, contacts, opportunities, and cases owned by members of that role. This rule may look like:



- Your company sells to many different industries. Two of your engineers need to know the details of accounts in one industry: chemicals. With a **Private** sharing org-wide default setting for accounts, create a public group that includes two users: Bob and Dave, the engineers for chemicals. Create an account sharing rule based on criteria that allows this group read-only access to account records in which the Industry field equals Chemicals. This rule may look like:



Types of Sharing Rules

Type	Based On	Set Default Sharing Access For
Account sharing rules	Account owner or other criteria, including account record types or field values	Accounts and their associated contracts, opportunities, cases, and optionally, contacts and orders
Account territory sharing rules (Not available with Enterprise Territory Management)	Territory assignment	Accounts and their associated cases, contacts, contracts, and opportunities
Asset sharing rules	Asset owner or other criteria, including asset record types or field values	Individual assets
Campaign sharing rules	Campaign owner or other criteria, including campaign record types or field values	Individual campaigns

Type	Based On	Set Default Sharing Access For
Case sharing rules	Case owner or other criteria, including case record types or field values	Individual cases and associated accounts
Contact sharing rules	Contact owner or other criteria, including contact record types or field values	Individual contacts and associated accounts
Custom object sharing rules	Custom object owner or other criteria, including custom object record types or field values	Individual custom object records
Data privacy sharing rules	Data privacy record owner or other criteria, including field values. Data privacy records are based on the Individual object.	Individual data privacy records
Flow interview sharing rules	Flow interview owner or other criteria, such as the pause reason	Individual flow interviews
Lead sharing rules	Lead owner or other criteria, including lead record types or field values	Individual leads
Location sharing rules	Location owner or other criteria	Individual locations
Opportunity sharing rules	Opportunity owner or other criteria, including opportunity record types or field values	Individual opportunities and their associated accounts
Order sharing rules	Order owner or other criteria, including order record types or field values	Individual orders
Product item sharing rules	Product item owner or other criteria	Individual product items
Product request sharing rules	Product request owner only; criteria-based sharing rules aren't available	Individual product requests
Product transfer sharing rules	Product transfer owner only; criteria-based sharing rules aren't available	Individual product transfers
Return order sharing rules	Return order owner or other criteria	Individual return orders
Service appointment sharing rules	Service appointment owner or other criteria	Individual service appointments

Type	Based On	Set Default Sharing Access For
Service contract sharing rules	Service contract owner only; criteria-based sharing rules aren't available	Individual service contracts
Service crew sharing rules	Service crew owner only; criteria-based sharing rules aren't available	Individual service crews
Service resource sharing rules	Service resource owner or other criteria	Individual service resources
Service territory sharing rules	Service territory owner or other criteria	Individual service territories
Shipment sharing rules	Shipment owner only; criteria-based sharing rules aren't available	Individual shipments
Time sheet sharing rules	Time sheet owner only; criteria-based sharing rules aren't available	Individual time sheets
User sharing rules	Group membership or other criteria, including username and whether the user is active	Individual users
User provisioning request sharing rules	User provisioning request owner, only; criteria-based sharing rules aren't available	Individual user provisioning requests
Work order sharing rules	Work order owner or other criteria, including work order record types or field values	Individual work orders
Work type sharing rules	Work type owner or other criteria	Individual work types

The Big Picture for Sharing Records

Many security options work together to determine whether users can view or edit a record. Use org-wide sharing settings to lock down your data to the most restrictive level, and use record-level security and sharing tools—such as roles, sharing rules, and manual sharing—to give access to other users.

See *A Guide to Sharing Architecture* for data accessibility components, sample sharing model use cases and customer sharing solutions, and troubleshooting guidelines.