



TIPS & HINTS FOR SHARING DATA

Salesforce provides many flexible options for you to control how records are shared within your organization. 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 organization-wide defaults, define a role hierarchy, and create sharing rules.

Granting Access to Objects with Profiles

The broadest way that you can control data is by specifying the objects that a user can view, edit, and create in Salesforce. You set a user's object-level permissions by assigning him or her a profile on the User Edit page. Salesforce provides the following standard profiles to all organizations:

- ◆ *Read Only*. Can view, but not edit, most objects.
- ◆ *Standard User*. Can view and edit core platform objects, but can only view, (not manage) campaigns, and can only create (not review) solutions.
- ◆ *Standard AppExchange User*. Can access the same functionality as the Standard User, but can also use custom apps developed in your organization 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, activate, and approve contracts.
- ◆ *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 Enterprise, Unlimited, and Developer Edition organizations, you can use any of the standard profiles or you can create custom profiles to better fit your business needs. To create a custom profile, click **Setup | Manage Users | Profiles**.

Objects and Records

In Salesforce there are 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.

Specifying Default Access to Records with Organization-Wide Defaults

Once object-level access has been specified with a user's profile, you can specify the individual records to which a user has access by setting record-level permissions. Default record-level permissions for accounts, activities, assets, calendars, cases, contacts, contracts, leads, opportunities, price books, and custom objects are specified with organization-wide defaults. To set your organization's defaults, click **Setup | Security Controls | Sharing Settings** and edit the organization-wide defaults section.

- How do I give all users full access to view, edit, or transfer any case?
 - ◆ Set **Default Case Access** 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 organization-wide default is Public Read Only or Private, create sharing rules to extend access to accounts, cases, leads, opportunities, or custom objects.
- Set the **Opportunity Access** field on each role to determine whether users can view and edit opportunities they don't own that are associated with accounts they do own.

Tips for Sharing Records

- Solutions are accessible to all users.
- Campaigns are not affected by the sharing model; all users can view campaigns and only marketing users can edit them.
- Forecasts are not affected by the sharing model. 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 in **Setup | Security Controls | Sharing Settings**.



Sharing Records with a Role Hierarchy

Once you have defined your organization-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, regardless of the default settings.

To define your organization's role hierarchy, click **Setup | Manage Users | Roles**.

Remember:

- Role hierarchies do not 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.
- The tree and list views show roles in relation to one another. Use either of them when defining a new hierarchy. The sorted list view is alphabetized. Use this view when you know the name of an existing role, but are not sure how it fits in the hierarchy.

Profiles and Roles

Users can be assigned to one profile and one role. Both work together to determine the data a user can view and edit:

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

Sharing Records with Sharing Rules

Sharing rules extend the access specified by organization-wide defaults and the role hierarchy. Below 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.
 - ◆ Choose a **Private** sharing model. Create a sharing rule that gives the Western Sales Team read and write access to all accounts and opportunities 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 opportunities in one industry: petroleum.
 - ◆ Within a **Private** sharing model, create a public group that includes two users: Bob and Dave, the engineers for petroleum. Create an opportunity sharing rule that allows your new public group to access opportunity records owned by the users in the petroleum group. This rule may look like:

To define sharing rules, click **Setup | Security Controls | Sharing Settings**.

Share with

- **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

Types of Sharing Rules

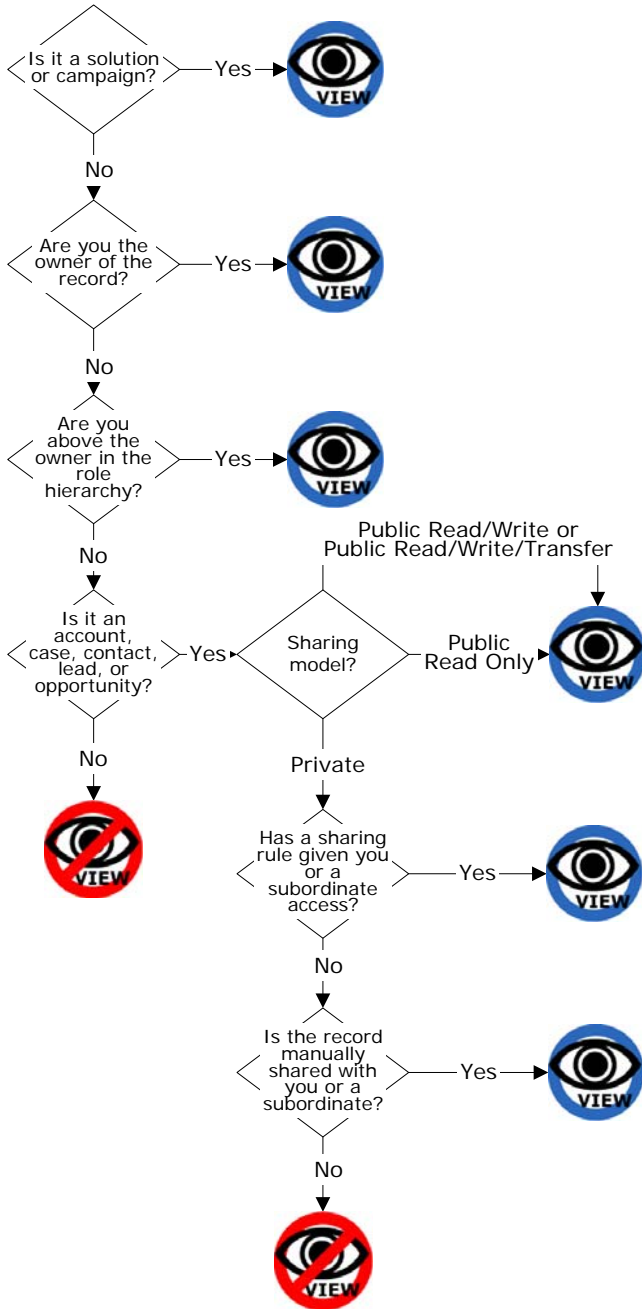
- Account sharing rules grant access to accounts and their associated records, including opportunities and cases.
- Opportunity sharing rules grant access to opportunities. They also give read access to the associated account if users do not already have access.
- Case sharing rules grant access to cases. Additionally, Salesforce automatically grants access to the associated account.
- Lead and custom object sharing rules grant access to leads and custom objects, respectively.



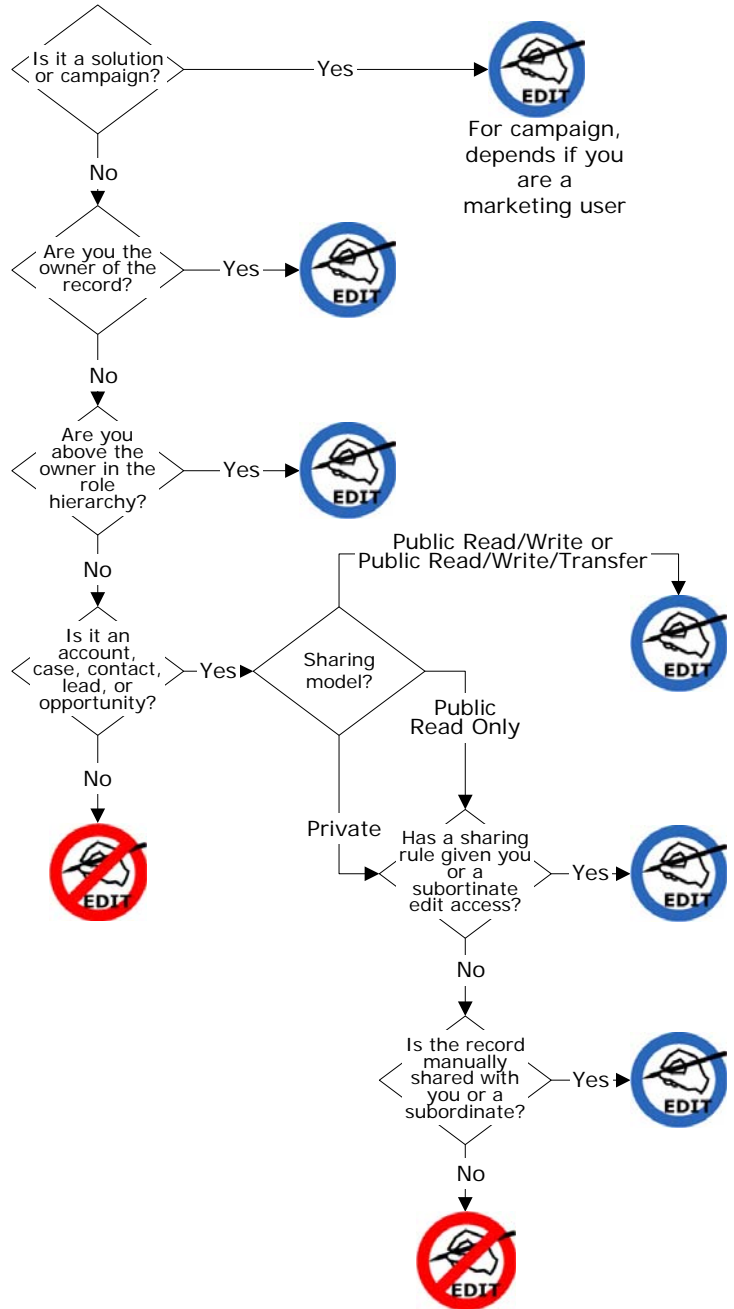
The Big Picture for Sharing Records


Many security options work together to determine whether users can view or edit a record. This flow chart helps you visualize how users are affected by the different security options you implement.

Can you **view** a record?



Can you **edit** a record?



 All of these icons assume you have the correct permission in your profile.