Profiles and Permission Sets

Profiles and permission sets provide object-level security by determining what types of data users see and whether they can edit, create, or delete records.

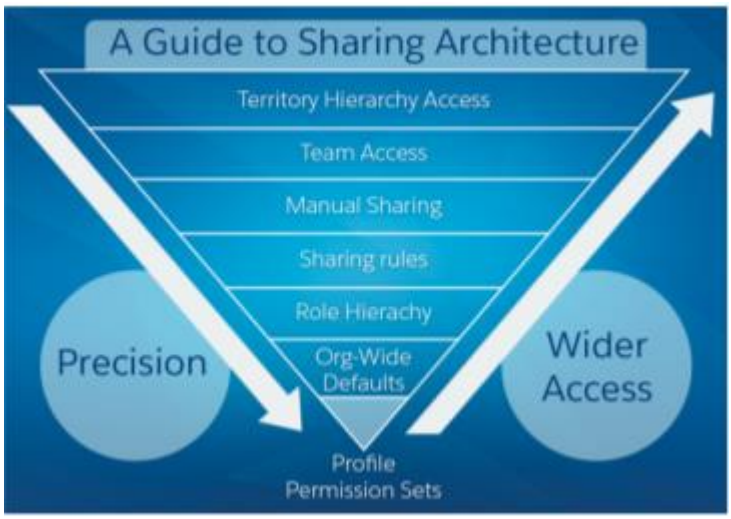
For each object, the “View All” and “Modify All” permissions ignore sharing rules and settings, allowing administrators to quickly grant access to records associated with a given object across the organization.

Record Ownership and Queues

If the owner’s profile has Create and Read permission on an object, but not Edit or Delete permission, the owner can create a record for the object and see the new record. However, the owner won't be able to edit or delete the record.

Users higher in a hierarchy (role or territory) inherit the same data access as their subordinates for standard objects. Managers gain as much access as their subordinates. If the subordinate has read-only access, so will the manager. This access applies to records owned by users, as well as records shared with them.

Queues help you prioritize, distribute, and assign records to teams who share workloads. Queue members and users higher in a role hierarchy can access queues.



Organization-Wide Defaults

Organization-wide defaults are the only way to restrict user access to a record.

For custom objects only, use the Grant Access Using Hierarchies setting, which if unchecked (default is checked), prevents managers from inheriting access. This setting is found in the organization-wide default settings.

Organization-wide default settings can be changed from one setting to another (private to controlled by parent, then back to private); however, these changes require sharing recalculation and depending on volume could result in very long processing times.

Role Hierarchy

A role hierarchy represents a level of data access that a user or group of users needs. The role hierarchy ensures that managers always have access to the same data as their employees, regardless of the organization-wide default settings.

Public Groups: A public group (not Chatter group) is a collection of individual users, roles, territories, and so on, that all have a function in common.

Sharing Rules

Ownership-based Sharing Rules Ownership-based sharing rules allow for exceptions to organization-wide default settings and the role hierarchy that give additional users access to records they do not own. Ownership-based sharing rules are based on the record owner only.

Criteria-based sharing rules provide access to records based on the record's field values (criteria). If the criteria are met (one or many field values), then a share record is created for the rule. Record ownership is not a consideration.

Manual Sharing

Record owners can use manual sharing to give read and edit permissions to users who would not have access to the record any other way. Although manual sharing is not automated like organization-wide sharing settings, role hierarchies, or sharing rules, it gives record owners the flexibility to share particular records with users that need to see them.

Manual sharing is removed when the record owner changes or when the sharing access granted does not grant additional access beyond the object's organization-wide sharing default access level. This also applies to manual shares created programmatically. Only manual share records can be created on standard objects.

Manual share records are defined as share records with the row cause set to manual share.

Team

A team is a group of users that work together on an account, sales opportunity, or case. Record owners can build a team for each record that they own. The record owner adds team members and specifies the access level each team member has to the record. Some team members can have read-only access, while others have read/write.

The team object is not a first-class object. You can't create custom fields, validations rules, or triggers for teams.

Territory Hierarchy

The territory hierarchy is a single dimensional, additional hierarchy which can be structured by business units or any kind of segmentation in a hierarchical structure. When territory management is enabled, you must manage both the role hierarchy and territory hierarchy. Territories exist only on Account, Opportunity and master/detail children of Accounts and Opportunities. As a best practice, keep the territory hierarchy to no more than 10 levels of branches in the hierarchy.