**What is a user?**

 A user is anyone who logs in to Salesforce. Users are employees at your company, such as sales reps, managers, and IT specialists, who need access to the company's records.

Every user in Salesforce has a user account. The user account identifies the user, and the user account settings determine what features and records the user can access. Each user account contains at least the following:

* Username
* Email Address
* User's First and Last Name
* License
* Profile
* Role (optional)

## Key Terms

**Usernames**

Each user has both a username and an email address. The username must be formatted like an email address and must be unique across all Salesforce organizations. It can be the user's email address, so long as it is unique.

**User Licenses**

A user license determines which features the user can access in Salesforce. For example, you can allow users access to standard Salesforce features and Chatter with the standard Salesforce license. But, if you want to grant a user access to only some features in Salesforce, you have a host of licenses to choose from. For example, if you have to grant a user access to Chatter without allowing them to see any data in Salesforce, you can give them a Chatter Free license.

**Profiles**

Profiles determine what users can do in Salesforce. They come with a set of permissions which grant access to particular objects, fields, tabs, and records. Each user can have only one profile. Select profiles based on a user’s job function (the Standard User profile is the best choice for most users). Don’t give a user a profile with more access than the user needs to do their job. You can grant access to more items the user needs with a permission set.

**Roles**

Roles determine what users can see in Salesforce based on where they are located in the role hierarchy. Users at the top of the hierarchy can see all the data owned by users below them. Users at lower levels can't see data owned by users above them, or in other branches, unless sharing rules grant them access. Roles are optional but each user can have only one.

If you have an org with many users, you may find it easier to assign roles when adding users. However, you can set up a role hierarchy and assign roles to users at any time. Roles are only available in Professional, Enterprise, Unlimited, Performance, and Developer editions of Salesforce.

**Alias**

An alias is a short name to identify the user on list pages, reports, or other places where their entire name doesn't fit. By default, the alias is the first letter of the user's first name and the first four letters of their last name

**Guidelines for Adding Users**

You have many options for adding users and many tools at your disposal in Salesforce. Here are some guidelines to help you get started.

* **Username**: Each user must have a username that is unique across *all* Salesforce organizations (not just yours).
* **Username Format**: Users must have a username in the format of an email address (that is, jdoe@domain.com), but they don't have to use a real email address. (They can use their email address if they wish as long as their email address is unique across all Salesforce orgs.)
* **Email**: Users can have the same email address across organizations.
* **Passwords**: Users must change their password the first time they log in.
* **Login Link**: Users can only use the login link in the sign–up email once. If a user follows the link and does not set a password, you (the admin) have to reset their password before they can log in.

## Add Users

To add users:

1. From Setup, enter Users in the Quick Find box, then select **Users**.
2. Click **New User** to add a single user or click **Add Multiple Users** to add up to 10 users at a time.
3. Enter each user's name, email address, and a unique username in the form of an email address. By default, the username is the same as the email address, but you can overwrite this.
4. Select the user license you want to associate with the users you create (the license determines which profiles are available for each user).
5. Select a profile.
6. Select **Generate passwords and notify user via email** to email a login name and temporary password to each new user.
7. Click **Save**.

**Levels of Data Access**

You can configure access to data in Salesforce at four main levels.

**Organization**

At the highest level, you can secure access to your organization by maintaining a list of authorized users, setting password policies, and limiting login access to certain hours and certain locations.

**Objects**

Object–level security provides the simplest way to control which users have access to which data. By setting permissions on a particular type of object, you can prevent a group of users from creating, viewing, editing, or deleting any records of that object. For example, you can use object permissions to ensure that interviewers can view positions and job applications but not edit or delete them.

**Fields**

You can use field–level security to restrict access to certain fields, even for objects a user has access to. For example, you can make the salary field in a position object invisible to interviewers but visible to hiring managers and recruiters.

**Records**

To control data with greater precision, you can allow particular users to view an object, but then restrict the individual object records they're allowed to see. For example, record–level access allows interviewers to see and edit their own reviews, without exposing the reviews of other interviewers. You can manage record–level access in the following ways.

* ***Organization–wide defaults*** specify the default level of access users have to each others' records. You use organization–wide sharing settings to lock down your data to the most restrictive level, and then use the other sharing tools to selectively give access to other users. For example, you can give all employees access to an object called Candidate to allow anyone to add a candidate to the database. But you can restrict access to Positions so that anyone can see the jobs available but only the employees with the proper permissions can edit them.
* ***Role hierarchies*** open up access to those higher in the hierarchy so they inherit access to all records owned by users below them in the hierarchy. Role hierarchies don't have to match your organization chart exactly. Instead, each role in the hierarchy represents a level of data access that a user or group of users needs. For example, you can restrict access to Candidates by setting the organization–wide default to Private, but allow recruiters to view and edit the candidate records that they own. Recruiters can't see candidate records they don't own because recruiters are all at the same level in the role hierarchy. However, hiring managers can be given read/write access to all candidate records because they are at a higher level in the role hierarchy than recruiters.
* ***Sharing rules*** enable you to make automatic exceptions to organization–wide defaults for particular groups of users, to give them access to records they don't own or can't normally see. Sharing rules, like role hierarchies, are only used to give more users access to records—they can't be stricter than your organization–wide default settings. For example, you can allow all employees to view Positions, but use sharing rules to grant full editing access to employees in a role or group called Hiring Managers.
* ***Manual sharing*** allows owners of particular records to share them with other users. Although manual sharing isn't automated like organization–wide sharing settings, role hierarchies, or sharing rules, it can be useful in some situations, for example, if a recruiter going on vacation needs to temporarily assign ownership of a job application to another employee.

## Organization–Wide Sharing Defaults

These are the defaults that specify the baseline level of access that the most restricted user should have. You can use organization–wide defaults to lock down your data to this most restrictive level, and then use other record–level security and sharing tools (role hierarchies, sharing rules, and manual sharing) to open up the data to other users who need to access it.

| **Field** | **Description** |
| --- | --- |
| Private | Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records. |
| Public Read Only | All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records. |
| Public Read/Write | All users can view, edit, and report on all records. |
| Controlled by Parent | A user can perform an action (such as view, edit, or delete) on a contact based on whether he or she can perform that same action on the record associated with it. |

In environments where you've set the organization–wide sharing setting for an object as Private or Public Read Only, you can grant users more access to records by setting up a role hierarchy or defining sharing rules. However, you can only use sharing rules to grant more access—they cannot be used to restrict access to records beyond what was originally specified with the organization–wide sharing defaults.

## Set Organization-Wide Sharing Defaults

Now that you’ve read about org-wide defaults, you’re ready to set some.

1. From Setup, enter Sharing Settings in the Quick Find box, then select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use.
4. To allow employees at higher levels in the role hierarchy to access records automatically, select **Grant Access Using Hierarchies** for any custom object that does not have default access of Controlled by Parent.

By default, Salesforce uses hierarchies, like a role hierarchy, to automatically grant record access to users above the record owner in the hierarchy. Setting an object to Private makes those records visible only to record owners and users above them in the role hierarchy. If you want to disable access to records for users above the record owner in the hierarchy for custom objects, use the **Grant Access Using Hierarchies** checkbox. If you deselect this checkbox for a custom object, you restrict record access to only the record owner and users granted access by the organization–wide defaults.

If you deselect **Grant Access Using Hierarchies**, users that are higher in the role hierarchy don't receive automatic access. However, some users can still access records they don't own by default—such as users with the "View All" and "Modify All" object permissions and the "View All Data" and "Modify All Data" system permissions.