

[1. Data Security](#)[2. Control Access to the Org](#)

Control Access to the Org

Learning Objectives

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

- Create, view, and manage users.
- Set password policies.
- Limit the IP addresses from which users can log in.
- Limit the times at which users can log in.

Control Access to the Organization

When you ensure that only employees who meet certain criteria can log in to Salesforce, you're protecting your data at the broadest level. You do this by managing authorized users, setting password policies, and limiting when and where users can log in.

Manage Users

Every Salesforce user is identified by a username, a password, and a single profile. Together with other settings, the profile determines what tasks users can perform, what data they see, and what they can do with the data.

To view and manage the users in your org, use the Quick Find box in Setup to find **Users**. The user list shows all the users in your org.

Create a User

You can create users—even multiple users—in just a few clicks. It's as simple as entering a username, alias, and email, and selecting a role, license, and profile. Many more options are available, of course, but that's all you need to get started.

Salesforce auto-generates a password and notifies new users immediately. Users can change or add to their own personal information after they log in.

1. Use the Quick Find box to find **Users** | **Users** in Setup.
2. Click **New User**.

Or you can click **Add Multiple Users** to add up to ten users at a time.

3. Enter the 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.
4. Select the user license this user will have.
The license determines which profiles are available for each user.
5. Select a profile, which specifies the user's minimum permissions and access settings.
6. Select the option to generate a new password and notify the user, then save.

Longer is usually better, within reason.

b. How complex do you want your passwords?

You can require alphabetical, numeric, uppercase, lowercase, or special characters.

c. How many days is a password valid?

d. How many times can someone try to log in with invalid credentials before being locked out?

3. Choose what to do about forgotten passwords and locked accounts.

4. Click **Save**.

Whitelist Trusted IP Ranges for the Org

The first time you log in to Salesforce, the IP address is cached in your browser. Anytime you log in from a different IP address, you will be asked to verify your identity, typically by entering a verification code. You can bypass this step for trusted IP ranges. For example, suppose that your users should be able to log in without entering a verification code whenever they are in the office.

1. From Setup, in the Quick Find box, enter **Network Access**, then select **Network Access**.
2. Click **New**.
3. Enter the start and end point of the range of trusted IP addresses, and click **Save**.

If you have an address outside this range, you aren't excluded from logging in. You simply have to verify your identity by entering a verification code.

Restrict Login Access by IP Address Using Profiles

By default, Salesforce doesn't restrict locations for login access. If you do nothing, users can log in from any IP address. You can restrict where users can log in from using profiles. For example, suppose that certain users shouldn't be able to log in if they're using an IP address outside of the office.

1. From Setup, in the Quick Find box, enter **Profiles**, then select **Profiles**.
2. Select a profile and click its name.
3. Click **IP Ranges**. If you don't have Enhanced Profile Interface enabled, scroll down to the Login IP Range related list.
4. Click **New**.

Login IP Ranges

[Help for this Page](#) ?

Enter the range of valid IP addresses from which users with this profile can log in.

5. Enter the start and end point of the range of trusted IP addresses, and click **Save**.

Now all users with this profile who are outside the trusted range can't log in. When using profile IP ranges, there are no verification codes to worry about - a user is either in or out.

Restrict Login Access by Time

For each profile, you can specify the hours when users can log in. For example, if you decide your call center employees really only need to look at customer data while they're taking phone calls nine to five, you can make it so they can't log in during evenings and weekends.

1. In Setup, use the Quick Find box to find **Profiles**.
2. Click the profile you want to change.
3. Under **Login Hours**, click **Edit**.
4. Set the days and hours when users with this profile can log in to the organization.
 - o To allow users to log in at any time, click **Clear all times**.
 - o To prohibit users from using the system on a specific day, set the start and end times to the same value.

**Note**

If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

Resources

- [Licenses Overview](#)
- [Control Login Access](#)
- [Set Login Restrictions](#)
- [Delegate Administrative Duties](#)

Assessment Complete!

+500 points



Data Security

100%

Progress: 100%

Retake this Challenge

[View more modules](#)