

Sharing Setting

Salesforce allows you to configure sharing settings to control how records are accessed and shared within your organization. These settings are crucial for maintaining data security and privacy. Salesforce provides a variety of tools and mechanisms to define and enforce sharing rules, such as:

Organization-Wide Default (OWD) Settings:

These settings define the default level of access for all objects within your Salesforce org.

OWD settings include Private, Public Read-Only, Public Read/Write, and Controlled by Parent.

OWD settings can be configured for each standard and custom object.

Role Hierarchy:

Salesforce uses a role hierarchy to determine record access.

Users at higher levels in the hierarchy have greater access to records owned by or shared with users lower in the hierarchy.

The role hierarchy is often used in combination with OWD settings to grant different levels of access.

Profiles and Permission Sets:

Profiles and permission sets allow administrators to specify object-level and field-level permissions for users.

Profiles are typically used to grant general object and field access, while permission sets can be used to extend those permissions to specific users.

Sharing Rules:

Sharing rules are used to extend access to records for users who meet specific criteria.

They can be used to grant read-only or read-write access to records owned by other users.

Manual Sharing:

Administrators and record owners can manually share specific records with other users or groups.

Creating Sharing settings

1. Go to setup >> type users in quick find box >> select Sharing Settings >> click Edit.
2. Change the OWD setting of the Service records Object to private as shown in fig.

The screenshot shows the 'Sharing Settings' page in Salesforce Setup. The 'Service records' object is highlighted with a red box, and its OWD (Owner Write Default) is set to 'Private'. The 'Save' button is also highlighted with a red box.

Object	Private	Public Read/Write	Public Read/Write	Public Read/Write
Work Plan Template	Private	Private	Private	Private
Work Step Template	Private	Private	Private	Private
Work Type	Private	Private	Private	Private
Work Type Group	Public Read/Write	Private	Private	Private
Appointment	Public Read/Write	Private	Private	Private
Billing details and feedback	Public Read/Write	Private	Private	Private
Customer Details	Public Read/Write	Private	Private	Private
Environment	Public Read/Write	Private	Private	Private
Laptop	Public Read/Write	Private	Private	Private
Service records	Private	Private	Private	Private
SessionData	Public Read/Write	Private	Private	Private

User Visibility Settings

Portal User Visibility ☐ Site User Visibility ☐



Other Settings

Standard Report Visibility ☒ Manual User Record Sharing ☐ Manager Groups ☐

Minimize the number of roles created, which improves performance by cutting down processing loads ☒ Grant site users access to related cases ☒ Secure guest user record access ☐ Require permission to view record names in lookup fields ☐

Save **Cancel**

3. Click on save and refresh.
4. Scroll down a bit, Click new on Service records sharing Rules.
- 5.

Service records Sharing Rules   [Service records Sharing Rules Help](#)


No sharing rules specified.


6. Give the Label name as “ Sharing setting”
7. Rule name is auto populated.
8. In step 3 : Select which records to be shared, members of “ Roles ”
>> “ Sales person”
9. In step 4: share with, select “ Roles ” >> “ Manager ”
10. In step 5 : Change the access level to “ Read / write ”.
11. Click on save.

SETUP
Sharing Settings

You can use sharing rules only to grant model access to data, not to restrict access.

Step 1: Rule Name I = Required Information

Label 


Rule Name 

Description


Step 2: Select your rule type

Rule Type ☒ Based on record owner ☐ Based on criteria

Step 3: Select which records to be shared

Service records: owned by members of 

Step 4: Select the users to share with

Share with 

Step 5: Select the level of access for the users

Access Level 