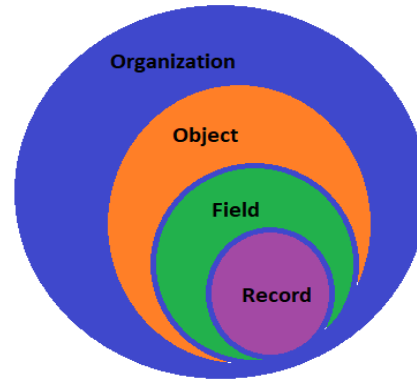


SESSION 17

SECURITY AND SHARING SETTINGS

There are 3 levels of security can be set within salesforce org to secure the data of object. They are

1. Object Level Security
2. Field Level Security
3. Record Level Security



LEVEL 1: OBJECT LEVEL SECURITY

This has been controlled in two ways such as Profile and Permission Sets.

1. Profile

It is used to set permissions to be assigned to users.

Object permissions specify the type of access that users have to objects. They are

Permission	Description
Read (R)	Users can only view records of this type.
Create (C)	Users can read and create records.
Edit (E)	Users can read and update records.
Delete (D)	Users can read, edit, and delete records.
View All	Users can view all records associated with this object, regardless of sharing settings.
Modify All	Users can read, edit, delete, transfer, and approve all records associated with this object, regardless of sharing settings.

Scenario: Pravin has joined Capital info Corporation as Sales Manager would need access to below custom objects.

Profile	Training__c	Contact	Department	Employee	Project	Trainee
Sales	R	R	R	CRE	CRE	CRE

Create a custom profile 'Sales' with required object permissions and assign to user Pravin

Step 1 : Setup -> Administer -> Manager Users -> Profiles

Step 2: Object Permissions
Standard Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Contacts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Custom Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Departments	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employees	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Projects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 3: Assign to user Pravin

User Edit
Pravin Jana

User Edit Save Save & New Cancel

General Information

First Name: Pravin	Role: Sales Manager
Last Name: Jana	User License: Salesforce Platform
Alias: pjana	Profile: Standard Platform User ▼
Email: vkranjithkrishnan@gmail.c	Active: Accountant
Username: pravin.jana@ranjithbatch1i	Marketing User: Sales
	Standard Platform User

2. Permission Set

It consists of permissions to be assigned to users addiitonally further to profile permissions. More than one permission set can be assigned to users.

Scenario:

Among the sales managers, only Pravin requires create and edit permission to Training objects.

Step 1: Setup -> Administer -> Manager Users -> Permission Sets

Step 2: Go to Object Setting section and enable as below

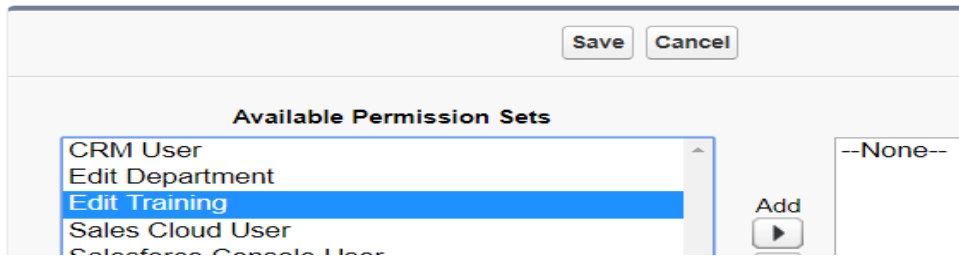
Trainings Edit

Object Permissions

Permission Name	Enabled
Read	<input checked="" type="checkbox"/>
Create	<input checked="" type="checkbox"/>
Edit	<input checked="" type="checkbox"/>
Delete	<input type="checkbox"/>

Step 3: GO to user page and section 'Permission Set Assignments' and choose the created permission set.

Permission Set Assignments
Pravin Jana



LEVEL 2: FIELD LEVEL SECURITY

This is controller below the respective objects in **profile** or **permission sets**.

Scenario: Pravin can read/edit all the fields in the training object but not the Course Fee.

Step 1: Go to Pravin's profile and under **Field Level Security** section.

Field-Level Security	
Standard Field-Level Security	
Account	[View]
Asset	[View]
Asset Relationship	[View]
Campaign Member	[View]
Coaching	[View]
Contact	[View]
Course	[View]
Course Fee	[View]

Step 2: Go to custom object 'Traininig' then do the below changes

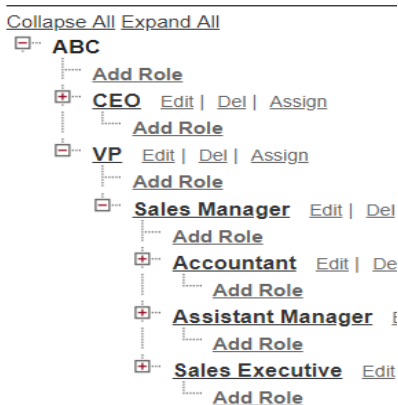
Training Field-Level Security for profile Sales			
Field Name	Field Type	Read Access	Edit Access
Active	Checkbox	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Availability	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Course Duration	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Course End Date	Date/Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Course Fee	Currency	<input type="checkbox"/>	<input type="checkbox"/>

LEVEL 3: RECORD LEVEL SECURITY

Pravin can only read/edit the records owned by him as per Object and Field Level. But as the role hierarchy he will be able to read/edit records owned by his sub-ordinates. For example, the role hierarchy in his Org (Setup -> Administer -> Manage Users -> Roles)

1. Roles

Your Organization's Role Hierarchy



User assigned as below

<pre> graph TD Ranjith((Ranjith)) --- Pravin((Pravin)) Pravin --- David((David)) Pravin --- Wilson((Wilson)) Pravin --- Raj((Raj)) style Ranjith fill:#fff,stroke:#000,stroke-width:2px style Pravin fill:#fff,stroke:#000,stroke-width:2px style David fill:#fff,stroke:#000,stroke-width:2px style Wilson fill:#fff,stroke:#000,stroke-width:2px style Raj fill:#fff,stroke:#000,stroke-width:2px </pre>	<p>Users at any role level can view, edit, and report on all data that's owned by or shared with users below them in their role hierarchy, unless your org's sharing model for an object specifies otherwise.</p> <p>Here, the user in the role CEO (Ranjith) can see/edit records owned by or shared with user in the role - Sales Manager (Pravin).</p> <p>Similarly the user Pravin can see/edit the records owned by or shared with user in the role - Sales Executive, Accountant or Assistant Manager. There are 3 users existing under Sales Managers.</p> <p>Hence to prevent role based sharing for custom objects? Un-check the option "Grant Access Using Hierarchies" option for that object here Setup -> Adminster -> Security Controls When disabled, only the record owner and users who are granted access by the organization-wide defaults receive access to the object's records.</p>
--	---

2. Organization Wide Default

This is used to set the level of access that each user can have on others data.

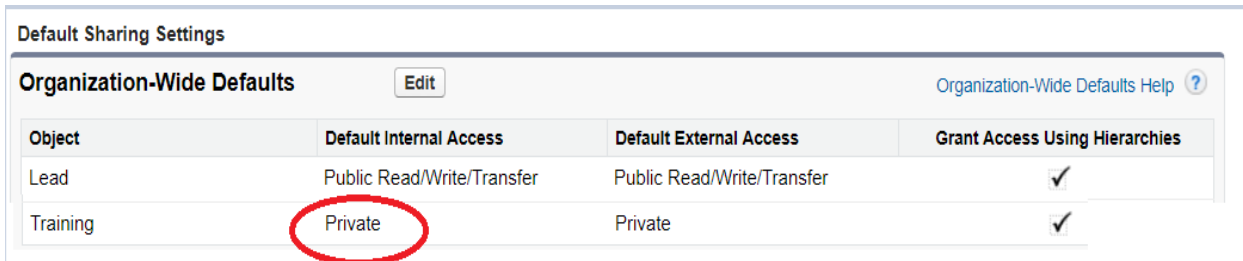
There are 5 levels of access we can set as below

OWD Default Access	Purpose
Private	Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records. For example, if Tom is the owner of an account, and he is assigned to the role of Western Sales, reporting to Carol (who is in the role of VP of Western Region Sales), then Carol can also view, edit, and report on Tom's accounts.
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. For example, Sara is the owner of ABC Corp. Sara is also in the role Western Sales, Field Description reporting to Carol, who is in the role of VP of Western Region Sales. Sara and Carol have full read/write access to ABC Corp. Tom (another Western Sales Rep) can also view and report on ABC Corp, but cannot edit it. Public
Public Read/Write	All users can view, edit, and report on all records. For example, if Tom is the owner of Trident Inc., all other users can view, edit, and report on the Trident account. However, only Tom can alter the sharing settings or delete the Trident account.
Public Read/Write/Transfer	All users can view, edit, transfer, and report on all records. Only available for cases or leads. For example, if Alice is the owner of ACME case number 100, all other users can view, edit, transfer ownership, and report on that case. But only Alice can delete or change the sharing on case 100.
Public Full Access	All users can view, edit, transfer, delete, and report on all records. Only available for campaigns. For example, if Ben is the owner of a campaign, all other users can view, edit, transfer, or delete that campaign.

Scenario:

Restrict read/edit access to all users in the org for training object.

Set OWD as Private: Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.



Default Sharing Settings

Organization-Wide Defaults Edit Organization-Wide Defaults Help ?

Object	Default Internal Access	Default External Access	Grant Access Using Hierarchies
Lead	Public Read/Write/Transfer	Public Read/Write/Transfer	✓
Training	Private	Private	✓

3. Sharing Rules

The feature called 'Sharing rule' helps to grant the records under Private or Public Read Only model to Users through Public Groups, Roles, and Roles & Sub-ordinates. Sharing rule can be based on record ownership or other criteria.

Owner-Based Sharing Rules

An owner-based sharing rule opens access to records owned by certain users.

Criteria-Based Sharing Rules

A criteria-based sharing rule determines with whom to share records based on field values.

Scenario: Only Sales Manager can read/edit the training records which is in progress.

Setup -> Administer -> Security Controls -> Sharing Settings

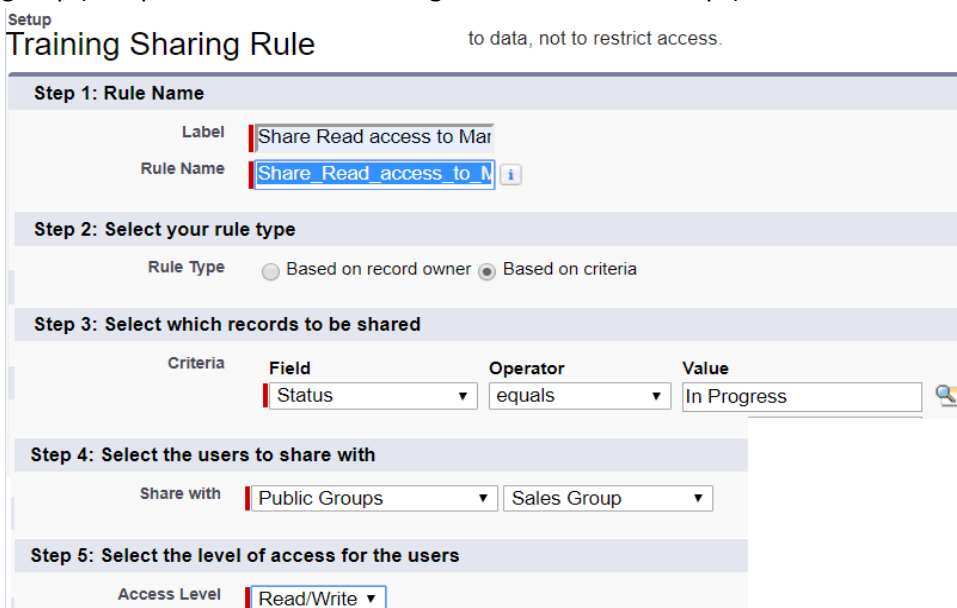
Step 1: Click New under related list for the object.

Step 2: Choose the rule type as based on criteria

Step 3: Choose criteria from the field of the object ((Field = 'Status').

Step 4: To whom the records need to be shared.

Note: Before you come to this step, the sales users needs to be grouped as one group using feature called public group (Setup -> Administer -> Manage Users -> Public Groups).



Setup Training Sharing Rule to data, not to restrict access.

Step 1: Rule Name

Label: Share Read access to Mar
Rule Name: Share Read access to M

Step 2: Select your rule type

Rule Type: Based on record owner Based on criteria

Step 3: Select which records to be shared

Criteria	Field	Operator	Value
	Status	equals	In Progress

Step 4: Select the users to share with

Share with: Public Groups, Sales Group

Step 5: Select the level of access for the users

Access Level: Read/Write

Scenario:

Records owned by Sales Executive should be viewable by Accountant.
This is an example scenario to share based on ownership

The screenshot shows a five-step configuration process for a sharing rule:

- Step 1: Rule Name**
 - Label: Share Read access to Mar
 - Rule Name: Share_Read_access_to_Mar
 - Description: (empty)
- Step 2: Select your rule type**
 - Rule Type: Based on record owner Based on criteria
- Step 3: Select which records to be shared**
 - Training: owned by members of: Public Groups (dropdown) | --- Select One --- (dropdown)
- Step 4: Select the users to share with**
 - Share with: Public Groups (dropdown) | --- Select One --- (dropdown)
- Step 5: Select the level of access for the users**
 - Access Level: Read Only (dropdown)

4. Manual Sharing (This is available ONLY in classic)

You can use this manual sharing option to give specific other users access to an individual record on demand. Sometimes, granting access to one record includes access to all its associated records. **For example**, if you grant another user access to an account, the user automatically has access to all the opportunities and cases associated with that account.

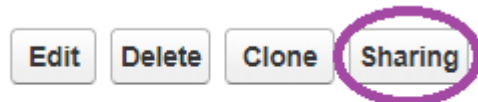
This can be done using **Sharing** button displayed on record detail pages.

Scenario:

Pravin would like to share his training record to another user in the org with read access.

Step 1: Go to detail page of the record to be shared

Training Detail



Training No TRN-005

Step 2: Click on Add button and share with necessary users | public Group | Roles | Roles & Sub-Ordinates.

The screenshot shows a table titled "User and Group Sharing" with an "Add" button circled in purple. The table lists the following entries:

Action	Type	Name ↑	Access Level
	User	Jana Pravin	Full Access
	Public Group	Sales Group	Read Only
	Public Group	VP	Read/Write

Note: This button will appear only if the OWD is private or public read-only because otherwise (say public read/write), you wouldn't need it.