SECURITY FEATURES

Licenses: License provides a set of features that can be accessible by the user within the Organization.

While adding the users in the Organization, each user should be associated with a License.

Salesforce provides the various types of Licenses as below.

1. Salesforce License/ Standard License / Full License (2)

This is a full license, which grants the permissions on all the features available inside the Organization.

2. Salesforce Platform License (3)

It grants the access on the platform features (i.e., custom features) such as Custom Apps, Tabs, Objects, Fields along with 5 Standard Objects Account, Contact, Document, Task and Event.

3. Chatter Free License (5,000)

It will grant the access on "Chatter Feed" hence the users can communicate with other users inside the Organization by using "Chatter Feed".

4. Customer Community License (5)

It will grant the access on community portals to the users like Customer Community and Partner Community etc.

We can verify all the available licenses inside the Organization as below.

Click on Setup menu.

1. Search for the option "Company Information" in Quick find box.
2. Go to "User Licenses" section.
3. View the available licenses in the Organization.

All the licenses information will get stored inside the User License object.

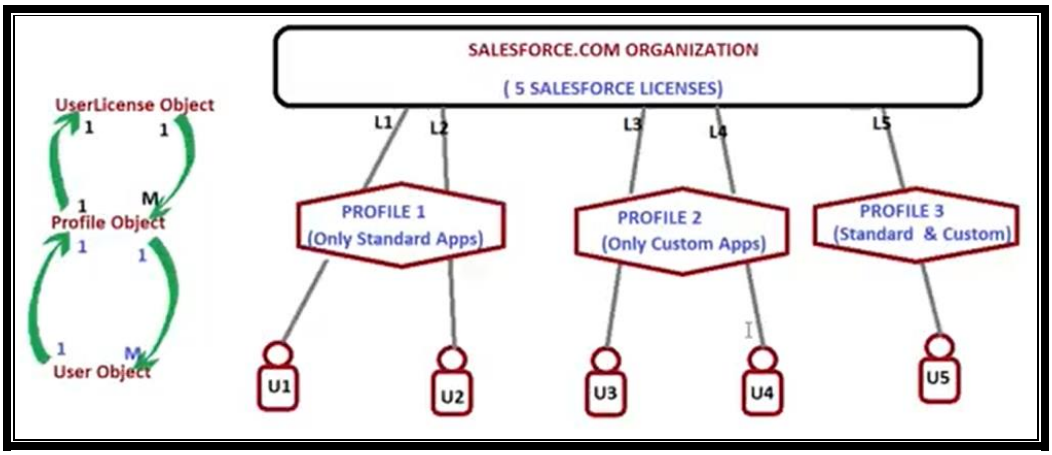
Profiles

Profile is a component which acts as the mediator between the "User and Organization".

Profile contains a set of permissions can be assigned to one or more users inside the Organization.

By using profiles, we can grant the permissions on Applications, Objects, Tabs, Fields, Page Layouts, Apex Classes, VF Pages, Session Settings, Password Policies, login IP ranges, login hours, System permissions, custom permissions, custom metadata types, external data sources, communities etc.

A User should be always associated with a "Profile". The same profile can be assigned to multiple users.



Salesforce provides the below 2 types of profiles.

1. Standard Profiles: These are the readymade profiles given by Salesforce by default.

Standard Profiles are editable up to some extent and Standard Profiles can't be removable.

2. Custom Profiles: The developer/administrator, can create a custom profile by cloning an existing one.

Custom Profiles are fully editable and removable from the organization.

It is always recommended to Assign the Custom Profiles to the Users.

All the profiles information will reside inside the Profile object.

Each profile should be associated with a license type. For one license type we can create multiple profiles.

Click on "Setup" menu.

1. Search for the option "Profiles" in Quick find box.

2. Go to the "Profiles" section.

3. View the Profiles.

4. Click on "New" button.

5. Select the Existing Profile from "Picklist".

6. Enter the "New Profile Name" in textbox.

7. Click on "Save" button.

Available Licenses in the organization

Salesforce License: 1

Platform License: 3

Create the below 2 Profiles:

i. Salesforce Licensed Profile:

Existing Profile Name: Standard User Profile

New Profile Name: DL Salesforce Profile

ii. Platform Licensed Profile:

Existing Profile Name: Standard Platform User

New Profile Name: DL Platform Profile

User Management: User is a person, who can login into our organization and can access the applications and data.

User can be either an Employee/Partner/Customer/End User.

While adding the users, each user should be associated with a License and a Profile.

i. Creating New User:

To add new user, follow the below steps

Step 1: Create a User Record, by filling up all the details.

Click on "Setup" menu.

i. Search for the option "Users" in Quick find box.

ii. Click on "New" button.

iii. Enter the User Details.

iv. Select the "License" from the Picklist.

v. Select the "Profile Name" from the Picklist.

vi. Click on "Save" button.

Observation: It will add the new user to the organization, and will send the user activation details to the User Email Id.

Step 2: Activate the User Account.

Open the Email received from Salesforce.

1. Click on "Verify Account" button.

2. Enter the Password, Confirm Password, Security Question and Answer.

3. Click on Change Password button.

Observation: It will activate the user and will re-direct to user account.

Create the below 4 Users:

1. Development User ---> Salesforce License (devuser@dl.com)

2. Manager User---> Platform License (mnguser@dl.com)

3. Customer User---> Platform License (cususer@dl.com)

4. Testing User---> Platform License (tsetuser@dl.com)

ii. Edit the user details: Once the user has been added to the organization, we can modify the user details at any point of time.

Go to the Users.

1. Click on edit link in the user record to be edited.
2. Make the required changes in the user record.
3. Click on "Save" button.

Observation: User record will get updated with the new details.

iii. Reset the User Password: By default, Salesforce allows maximum of 10 Invalid Login Attempts. If the user tries to login after 10 invalid login attempts, the Account gets locked.

We can reset the user Password by contacting the System Administrator.

Go to the Users.

i. Select the Checkboxes for the Required Users to Reset the Password.

ii. Click on "Reset Password" button.

Observation: It will generate a separate Reset Password Link for each user and will send to the user's email id automatically.

iii. Prevent the User from Login.

a. De-Activate the User
b. Freeze/Unfreeze the User.

iv. Login Access Policies: Configure from Login access policies

v. Prevent Force Re-Login After Login as a User: Configure from Session Settings

vi. Expire All User Passwords: Configure from Expire All Passwords

vii. View Setup Audit Trials

Role Hierarchy

Role Hierarchy makes the sub-ordinates records to be visible to the manager by default.

By default, Salesforce provides a set of roles that can be assigned to the users.

We can configure the Role Hierarchy based on the requirement and we can assign the roles to the required users.

A User should be associated with only one role. But a role can be assigned to multiple users.

All the Roles information will reside inside the User Role object.

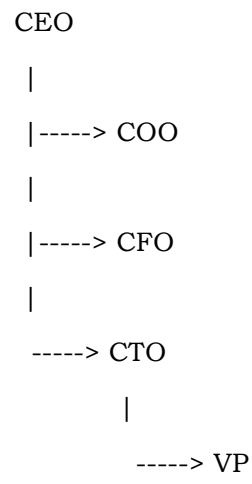
Click on "Setup" menu.

1. Search for the option "Roles" in Quick find box.

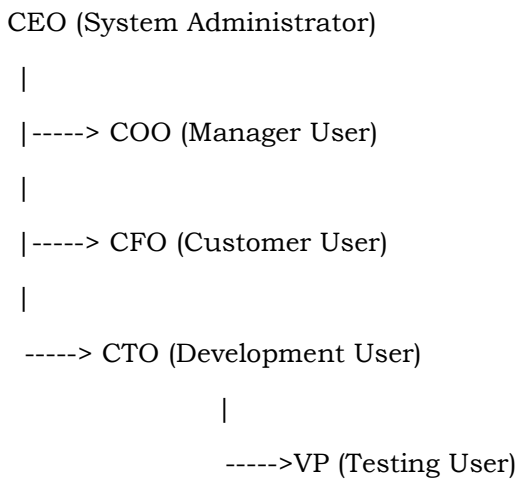
2. Click on "Continue" button.

3. Setup the Role Hierarchy based on the need.

4. Assign the Roles to the required users.



Once the Role Hierarchy has been configured, assign the Roles to the users as below.



OWD (Organization Wide Defaults):

OWD Options are used to describe the level of access of the record inside the Organization i.e., it decides which record should be visible to which user inside the Organization.

Once the OWD option has been assigned for an object, the same option will be applicable to all users inside the organization.

Salesforce provides the below OWD options.

1. Private

2. Public Read Only

3. Public Read/Write

4. Public Read/Write/Transfer

5. Public Full Access

6. No Access

7. View Only

8. Use

9. Controlled by Parent

1. Private, Public Read Only and Public Read/Write options will be applicable for all Standard and Custom Objects of Salesforce except the Price Book object.

2. Public Read/Write/Transfer option will be Applicable for only Lead and Case Objects in Salesforce.

3. Public Full Access Option will be applicable only for Campaign object.

4. No Access, View Only and Use options will be applicable only for "Price Book" object.

5. Controlled by Parent option will be applicable only for Child Objects associated with "Master-Detail" association.

Click on "Setup" menu.

1. Search for the option "Sharing Settings" link.

2. Go to the "Organization Wide Defaults" section.

3. Click on "Edit" button.

4. Select the "OWD Option" for the object, from the Picklist.

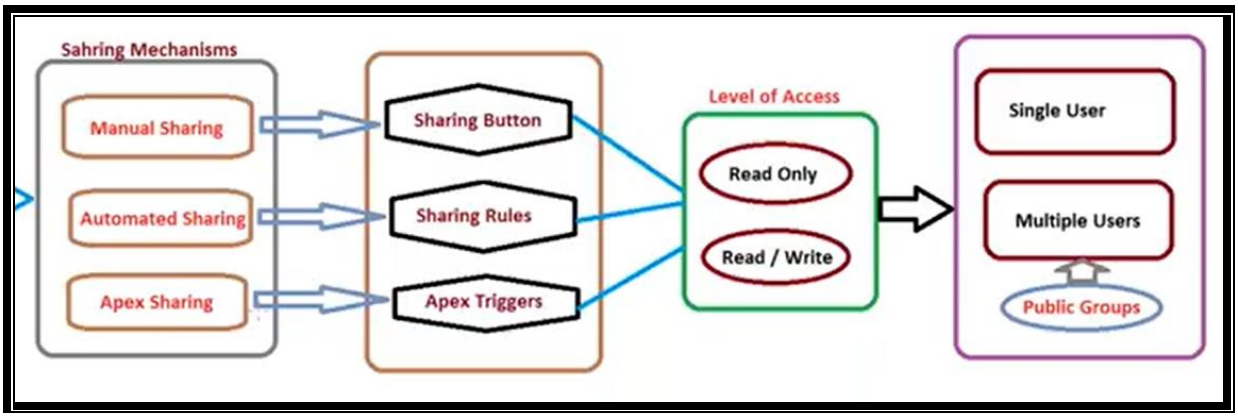
5. Click on "Save" button.

Private: When the Object's OWD has been assigned as Private, if any of the user creates a record inside the Object, the record will be visible only to the Record Owner and his Manager based on the Role Hierarchy.

Other users (i.e., Siblings and Sub-Ordinates) will not be able to access the records.

To make the records to be visible to the other users inside the Organization, we have to use Sharing feature.

By using Sharing feature, we can share the record to either one/more users with the required level of access based on the need.



Manual Sharing: In this approach, we can share the records to one/more users with the required level of access by using "Sharing" button.

Drawback: If a greater number of records to be shared to the multiple users, it takes more time.

While sharing the record to the users, we can grant the below access levels.

1. Read-only: Grants only "Read Permission" on the record.

2. Read/Write: Grants both "Read and Edit" permissions on the record to the users.

Use Case: Create an account record by login into "Development User Account" and share the record to "Customer User" with Read Only access.

1. Login into the "Development User" account.

2. Click on "Accounts" Tab.

3. Create an Account Record with the required details.

4. Go to the Record Detail Page.

5. Click on "Sharing" button.

6. Select the User Type to Share (Ex: User)

7. Select the User Names, to be get Shared. (Ex: Customer User)

8. Select the "Account Access Level" as "Read Only".

9. Select the "Opportunity Access Level" as "Read Only".

10. Select the Case Access Level "Read Only".

11. Click on "Save" button.

Testing Process:

1. Login into "Customer" User.
2. Click on "Accounts" tab.

Observation: It should display the Account Record to the User with "Read Only" access.

Negative Testing:

1. Open the Record.

2. Click on "Delete / Edit" button.

Observation: It should show the Message "Insufficient Privileges".

Use Case: Share the Above record to the "Testing User" with "Read/Write" permissions.

Public Groups: Instead of sharing records to the multiple users separately, share the records to the public group by adding the users in to the group.

We can create one/more Public Groups inside the Organization.

All the Public Groups Information will get resides inside the "Group" object.

All the Public Group Members information will get resides inside the "Group Member" object.

While sharing the record to the Public Group, whatever the access has been granted, the same level of access will be applicable to all the users inside the group.

Use Case: Configure a Public Group with the name "Hyderabad Sales Group" and add the "Customer User and Manager User" as the Group Members.

Click on "Setup" menu.

1. Search for the option "Public Group" in Quick Find box.

2. Click on "New" button.

3. Enter the Public Group Label and Name.

4. Unselect the Checkbox Grant Access using Hierarchies.

5. Select the Group Members by using "Add / Remove" button.

6. Click on "Save" button.

Use Case: Create an Account Record by login into the "Development User" Account and share the record to "Hyderabad Sales Group" with "Read/Write" access.

Automated Sharing: While sharing the records manually to the required users, if the number of records to be shared are more, it takes more time.

To Share the records to the required users automatically, use Sharing Rules.

Sharing Rules are used to share the record to either one or more users dynamically at runtime based on the specified conditions.

Through Sharing Rules, we can share the record to either a "Public Group/Role/Roles & Subordinates".

Salesforce provides 2 types of Sharing Rules

1. Owner-Based Sharing Rules: In this approach, based on the record owner we can share the record to the required users.

2. Criteria-Based Sharing Rules: In this approach, we can share the records to the required people if the record meets the specified conditions.

Sharing Rules always fire "After Insert" and "After Update" the record inside the object.

We can create one/more Sharing Rules per an object.

Use Case: Configure a Sharing Rule, to share the Account Records to the "Hyderabad Sales Group" with "Read Only" Access if the record meets the below conditions.

1. Account: Rating = 'Hot'

2. Account: Customer Priority = 'High'

3. Account: Industry = 'Finance'

4. Account: Active = 'Yes'

Click on "Setup" menu.

1. Search for the option "Sharing Settings" link.

2. Go to the "Sharing Rules" Section.

3. Go to the section "Account Sharing Rules".

4. Click on "New" button.

5. Enter the Sharing Rule Label and Description.

6. Select the "Active" Checkbox, to make the Rule Active.

7. Select the Sharing Rule Type as "Criteria-Based Sharing Rule".

8. Select the Rule Conditions.

    i. Account: Rating = 'Hot'

    ii. Account: Customer Priority = 'High'

    iii. Account: Industry = 'Insurance'

    iv. Account: Active = 'Yes'

9. Select the "Share With" from the Picklist, and Select "Public Groups".

    9.1. Select the Public Group, to whom the record gets Shared.

10. Select the "Level of Access" as "Read Only".

11. Click on "Save" button.

Governor Limits

An object can have maximum of 300 Sharing Rules including both Owner-Based and Criteria-Based sharing rules.

i. We can have maximum of 50 Criteria-Based Sharing Rules.

ii. We can create maximum of 250 Owner-Based Sharing Rules.

Public Read Only: When the Object's OWD has been assigned as Public Read Only, if the user creates a record in the object, then record will be visible to all the users inside the Organization.

The Record Owner and his Manager will have the complete access on the Record whereas the other users inside the Organization will have "Read Only" access. They cannot edit, delete and share the record to other users.

Public Read/Write: When the Object's OWD has been assigned as "Public Read/Write" and if the User creates a record in the object, then record will be visible to all the Users inside the Organization.

The Record Owner and his Manager will have the complete access on the Record whereas the other users inside the organization will only have Read/Write access.

Public Read/Write/Transfer: By using this option, we can transfer the Record Ownership from one user to another user/Queue.

Upon transferring the Ownership, the old owner will lose the access on the record and the new owner will get the full access on the record.

We can Transfer the Record Ownership as below.

Click on the Required Object Tab

1. Open any of the Account Record.
2. Go to the "Account Owner Field".
3. Click on "Change Owner" link.
4. Select the "User" to Transfer the Record.
5. Select the Checkbox to transfer the Related "Opportunities and Cases".
6. Click on "Change Owner" button.

Observation: It will transfer the Record Ownership to new user automatically by default.

While transferring the ownership for lead and case records, the owner can be a User/Queue.

Queue: Queue is a location where all the pending records wait to get processed.

Queue contains 2 parts.

1. Queue Supporting Objects: It describes the various object records the queue can hold inside it.

Queue will support the following objects.

Lead, Case, Order, Feedback, Feedback Question, Feedback Question Set, Feedback Request, Feedback Template, performance cycle, Goal, Metric, Macro, Knowledge Article Version, User Provisioning request etc. + All Custom Objects.

2. Queue Members: It describes the users who can access the Queue Records.

While placing the record inside the queue, all the queue members will receive an Email Notification.

The record will wait inside the queue until any of the queue member accepts it.

Once if any of the member accepts the record, it will transfer the Record Ownership from "Queue" to "Accepted Member" automatically.

We can create one or more Queues inside the Organization.

Click on Setup menu.

i. Search for the Option "Queues".

ii. Click on "New" button.

Use Case: Configure a Queue "Hyderabad Sales Queue" by adding the lead Object as the supporting object and "Development User" as the queue member.

ASSIGNMENT RULES

Record ownership can be transferred to the required user/queue either manually or automatically using Assignment Rules.

Assignment Rules are used to transfer the lead/case records to the required user/queue dynamically at run time based on the specified conditions.

Assignment Rules will fire after performing the insert and update operations on the records.

Salesforce provides two types of Assignment Rules.

i. **Lead Assignment Rules**: Used to transfer the lead records to the user/queue at runtime based on the business requirement.

We can create one/more lead Assignment Rules in the organization, but only one rule must be in the active state at a time.

ii. **Case Assignment Rules**: Used to transfer the case records to the user/queue at runtime based on the business requirement.

We can create one/more case Assignment Rules in the organization, but only one rule must be in the active state at a time.

Use Case: Configure a lead assignment rule to transfer the lead records to the required queue based on the specified conditions as below.

Lead city name	**Transfer to**
City= Hyderabad …….	Hyderabad Sales queue
City= Bangalore …….	Bangalore Sales queue
City= Mumbai …….	Mumbai Sales queue
City= Chennai …….	Chennai Sales queue
City= Kochi …….	Kochi Sales queue

Step i: Create the required queues by selecting the supporting object as lead and development user as the queue member.

Step ii: Configure the assignment rule.

Step iii. Test the assignment rule.

Use Case: Configure a case assignment rule to transfer the case records to the required queue based on the specified conditions as below.

Case Priority Transfer to

Priority= High ……. Tier 1 Service queue

Priority= Medium …… Tier 2 Service queue

Priority= Low …… Tier 3 Service queue

Step i: Create the required queues by selecting the supporting object as case and development user as the queue member.

Step ii: Configure the case assignment rule.

Step iii. Test the assignment rule.

ONLINE LEADS/WEB TO LEAD

Using this feature, we can capture leads from company/organization website.

Whenever a new lead record is submitted online from website, the record will be sent to the salesforce server, which will insert the record in the lead object through a webservice.

Once the record is inserted successfully, the lead assignment rule fires and will transfer the record to the queue based on the specified rule entries.

Once the queue member accepts the record, the record ownership will be transferred from the queue to the queue member.

Implementation Steps

Step i: Enable web to lead feature inside the organization.

Step ii: Create web to lead form.

Step iii. Test the HTML form.

Observation: It will create a new lead record inside the object and the lead assignment rule will fire automatically, will transfer the record to the associated queue.

Note: We can send email notification automatically to the leads captured online from website by using a feature Lead Auto Response Rules.

WEB TO CASE

Using this feature, we can capture cases from company/organization website.

Whenever a new case record is submitted online from website, the record will be sent to the salesforce server, which will insert the record in the case object through a webservice.

Once the record is inserted successfully, the case assignment rule fires and will transfer the record to the queue based on the specified rule entries.

Once the queue member accepts the record, the record ownership will be transferred from the queue to the queue member.

Implementation Steps

Step i: Enable web to case feature inside the organization.

Step ii: Create web to case form.

Step iii. Test the HTML form.

Observation: It will create a new case record inside the object and the case assignment rule will fire automatically, will transfer the record to the associated queue.

Note: We can send email notification automatically to the case captured online from website by using a feature Case Auto Response Rules.

PROFILE

Use Case: Configure a profile level permission on application to the development user.

For each tab salesforce provides the below three settings

i. Default ON: It will show the tab on the tab bar by default.
ii. Default OFF: It will not show the tab on the tab bar by default.
iii. Tab Hidden: No access for the tab to the profile user.

Use Case: Configure the below tab settings for the development user profile grant the access only on one application to the development user.

Leads- Default OFF

Cases: Default OFF

Opportunities: Tab Hidden

Use Case: Configure the below object level permissions to the development user profile.

Account: Create, Read, Edit

Lead: Create, Read

Campaign: Read, Create, Edit, Delete

Hiring Manager: Read, Create

We can restrict the field visibilty in the object to the profile user.

Use Case: Configure the profile permissions to the development user to restrict the visibility of the following fields in the account object.

Rating

Annual Revenue

Account Website

Industry

We can configure different page layouts to the profile users.

General/Administrative/System/Custom Permissions

Author Apex Permission: Grants permission to the profile users to create apex classes to implement custom business logic.

Bulk API Hard Delete: Allows us to remove the records from the object permanently without moving to the Reyclebin.

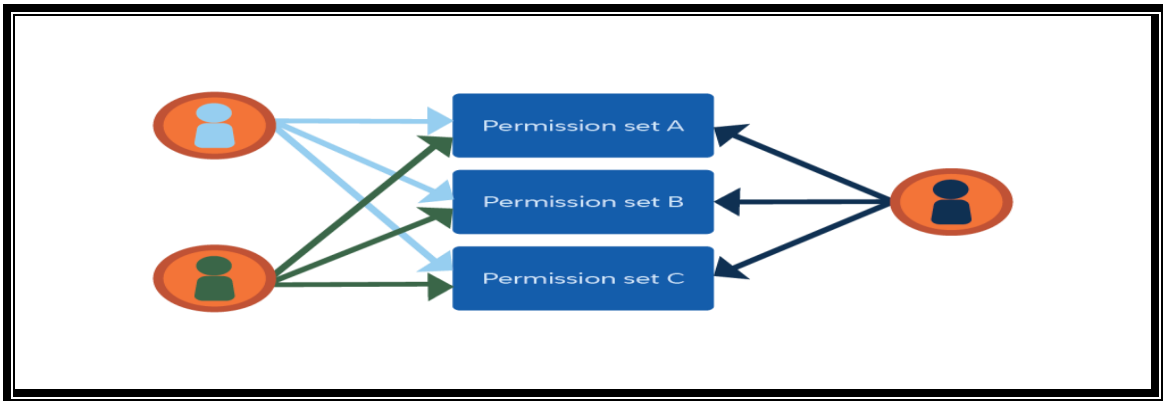
Login Hours allows to configure the business hours. We can also configure the holidays from Setup---> Holidays from quick find box.

Permission Sets

Allows to exend permission on the various features to the users who are at same profile i.e., users under same profile can be granted more permissions.

Can grant permission on all features which profile can grant, except login hours and login IP ranges.

While creating user, profile is mandatory but permission set is optional.



One user can be assigned with multiple permission sets and one permission set can be assigned to muliple users. i.e., between user and permission set there is many-many association which can be acheived using juncion object, permission set assignment.

Profile level settings can Overwrite the OWD Settings and Permission Sets can overwrite the profile level settings.