Getting Started with SalesForce CRM

Security and Data Access in SalesForce CRM

Description:

BISP is committed to provide BEST learning material to the beginners and advance learners. In the same series, we have prepared a complete end-to end Hands-on Beginner's Guide for SalesForce. The document focuses on basic keywords, terminology and definitions one should know before starting SalesForce. Join our professional training program and learn from experts.

History:

Version	Description Change	Author	Publish Date
0.1	Initial Draft	Chandra Prakash Sharma	10th Nov 2013
0.1	Review#1	Amit Sharma	10th Nov 2013

.... 2
Restrict logins.. 3
Login hour restrictions :.. 3
Login Hours :.. 3
Restricting Login IP Addresses :.. 4
Determine Object Access Security.. 6
Viewing the Object Access and Field-Level Security Report :.......................................6
.... 6
Custom Object Security :... 7
Manage record access with the role hierarchy 8
Roles :.. 8
How to Set Rules :... 9
Permission Sets :... 12
Exceptions 14
Manage field-level security 16
For View Field level Security : 17
Manage Field Level Security :... 18

Restrict logins

To help protect your organization's data against unauthorized access, you have several options for setting login restrictions.

Login hour restrictions :

If login hour restrictions are set for the user's profile, any login attempt outside the specified hours is denied. For each profile, you can set the hours when users can log in.

Login Hours :

SalesForce provide to you Login history features, You can set login hours in organization Start or end time .

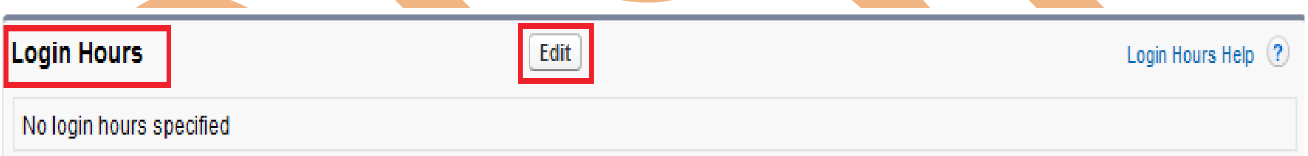
OR

Select the days and hours that users with this profile are allowed to log in. Note that all times are exact times specific to a time zone. Login hours will be applied at those exact times even for users in different time zones.

How to Set Login hours :

Setup > **Mange users** > **Profile** Select profile name (Ex:- Recruiter)(which want do you need).
After then come to down on page there is you can find **Login hours**. see below

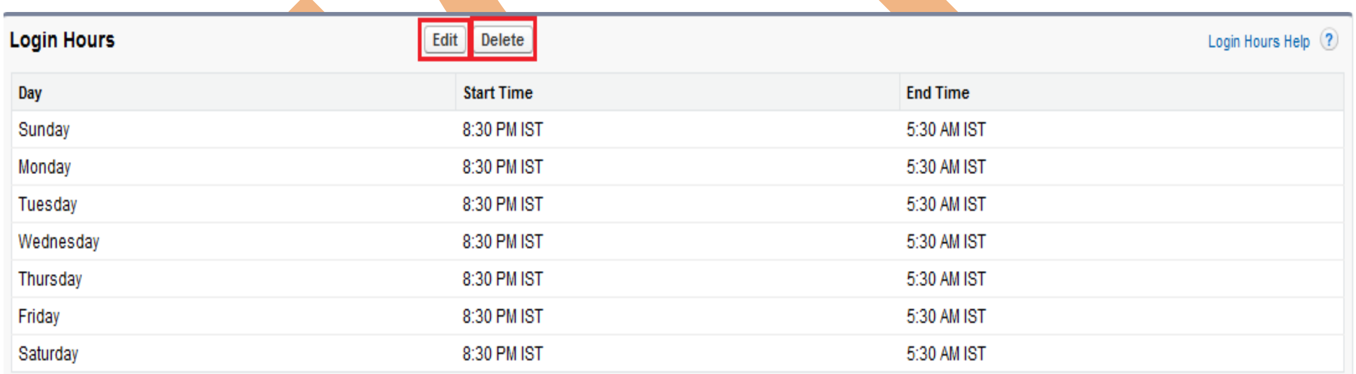
Step 1 :-



After that click on **Edit** button. then you can see new page below.

Step 2 :-
In this page you can set Start or End time by day, After that select login hours click on **Save** button.

After clicking on save button you can see your login hours detail on profile page see below.
There is you can Edit these login hours and also Delete these login hours.



Restricting Login IP Addresses :

User Permissions Needed	
View login IP ranges	View Setup and Configuration
Edit login IP ranges	Manage Users
Delete login IP ranges	Modify All Data

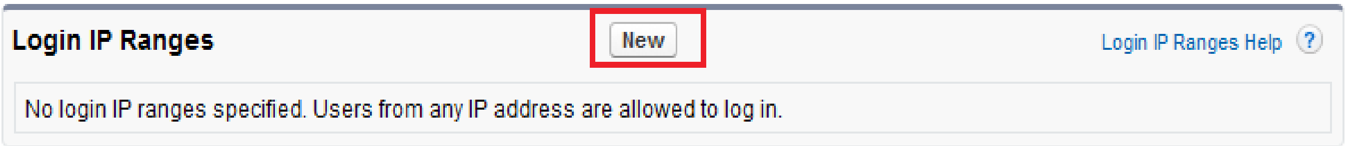
You can control login access on a user's profile by specifying a range of IP addresses. When you define IP address restrictions for a profile, any login from a restricted IP address is denied.

How to Set Login IP Ranges :

Setup > **Mange users** > **Profile** Select profile name (Ex:- Recruiter)(which want do you need).
After then come to down on page there is you can find **Login IP Ranges** . see below

Step 1 :

Click on **New** button for create Login IP Ranges.



Step 2 :

There is you can see two fields, Start IP Address and End IP Address, You can give IP address, which IP address allow to user for login.

Note :-

For Single IP Address :

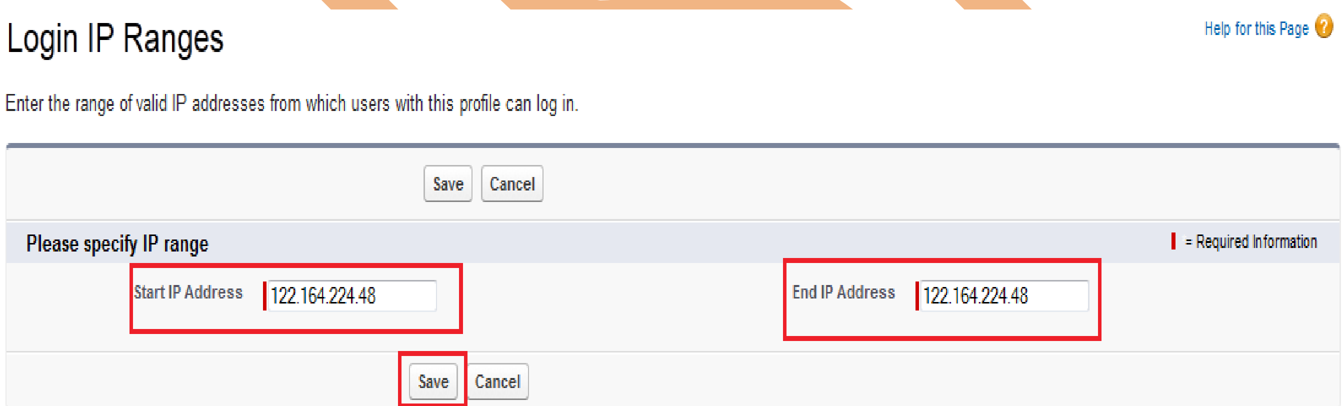
If you want to set single IP address, give this type.

Start IP Address 122.164.224.48	**End IP Address** 122.164.224.48

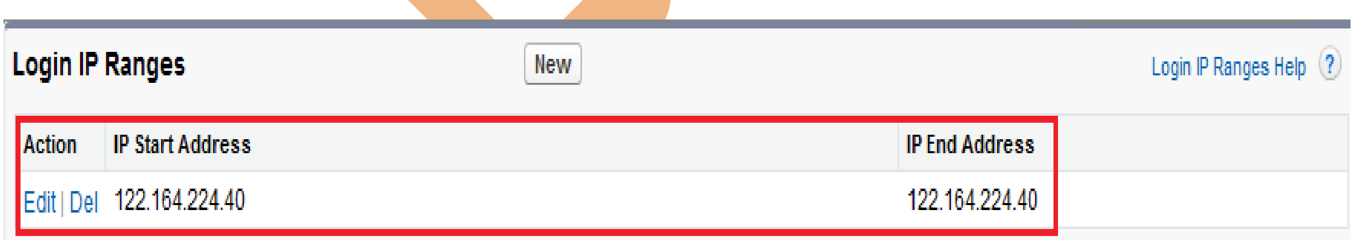
For One to More Range IP Address :

If you want to Set One or More Range IP address, specify like this

Start IP Address 122.164.224.48	**End IP Address** 122.164.224.59



After click save button then you can see your IP address on profile setting page, see below.



Determine Object Access Security

Viewing the Object Access and Field-Level Security Report :

you can also give Field-Level Security in user profile on non-editable page. Scroll down you will find Field-Level security.

Object permissions specify the access that users have to standard and custom objects.

- Create - Users can read and create records.
- Edit - Users can read and update records.
- Read - Users can only view records of this type.
- Delete - Users can read, edit, and delete records.

There is available Standard Field Level Security, Custom Field Level Security, In Standard Field Level Security create permission on create account by SalesForce.com. You can change on Custom Field Level Security Click on View Link then open new page. For Ex :- I have select Candidate Field. you can see below.

Field-Level Security

Standard Field-Level Security

Account	[View]	Lead	[View]
Asset	[View]	Opportunity	[View]
Campaign	[View]	Opportunity Product	[View]
Campaign Member	[View]	Price Book	[View]
Case	[View]	Product	[View]
Contact	[View]	Social Persona	[View]
Contract	[View]	Solution	[View]
Event	[View]	Task	[View]
Idea	[View]	User	[View]

Custom Field-Level Security

Back Office	[View]	ForTesting	[View]
Book	[View]	Job Application	[View]
Candidate	[View]	Job Posting	[View]
Department	[View]	Postion	[View]
Employee	[View]	Review	[View]
Employment website	[View]		

Step 1 :

Click on **Edit** button.

Candidate Field-Level Security for profile

Recruiter

Help for this Page

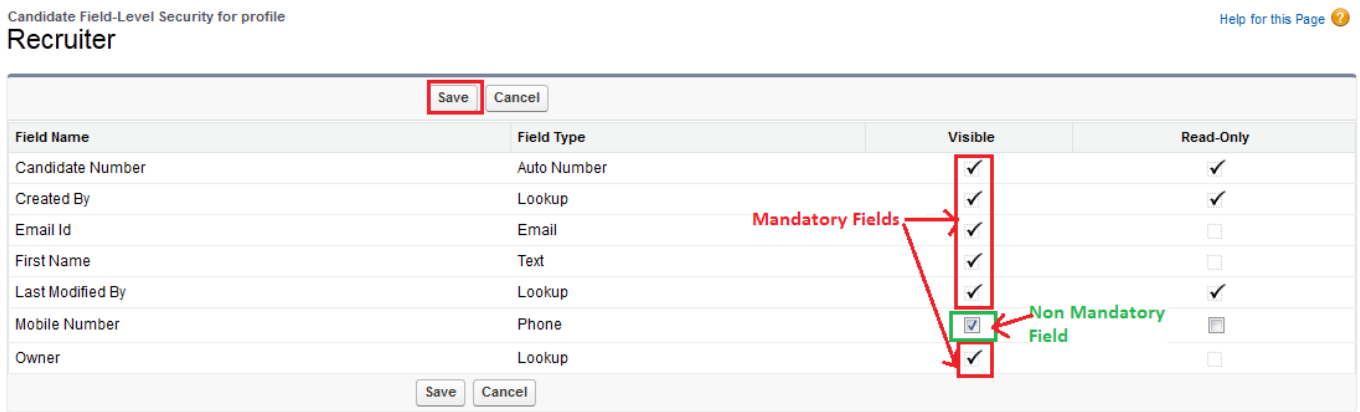
Edit | Back to Profile

Field Name	Field Type	Visible	Read-Only
Candidate Number	Auto Number	✓	✓
Created By	Lookup	✓	✓
Email Id	Email	✓	
First Name	Text	✓	
Last Modified By	Lookup	✓	✓
Mobile Number	Phone	✓	
Owner	Lookup	✓	

Edit | Back to Profile

Step 2 :

There is some check box is not enable, because these check box are Mandatory Fields.
and some check box is visible this check box Non Mandatory field.
In Non Mandatory Field you can provide permission Read-Only, Visible. you can choose it.



Field Name	Field Type	Visible	Read-Only
Candidate Number	Auto Number	✓	✓
Created By	Lookup	✓	✓
Email Id	Email	✓	
First Name	Text	✓	
Last Modified By	Lookup	✓	✓
Mobile Number	Phone	☑	☐
Owner	Lookup	✓	

Custom Object Security :

In SalesForce many security settings work together so you can control access to your custom objects with flexibility.
Set custom object security following levels :
Tab, Object, Records, Relationship, Fields
Tab - Display the custom tab for suitable users based on their user profiles.
Object - Set the access users have to create, read, edit, and delete records for each object.
Records - Set the default sharing model for all your users.
Relationship - For objects on the detail side of a master-detail relationship, specify the sharing access that users must have to the master record in order to create, edit, or delete records.
Fields - Set the level of access users have to fields on your custom object page layout.

Custom objects with no master-detail relationship :

Action	Required Privileges
Create a record	"Create" permission. The user must have the tab displayed to create a new record from the Create New drop-down list in the sidebar.
View a record	"Read" permission and Public Read Only or Public Read/Write sharing model if not the record owner.
Edit a record	"Edit" permission and Public Read/Write sharing model if not the record owner.
Delete a record	"Delete" permission and must be the record owner or above the record owner in the role hierarchy.

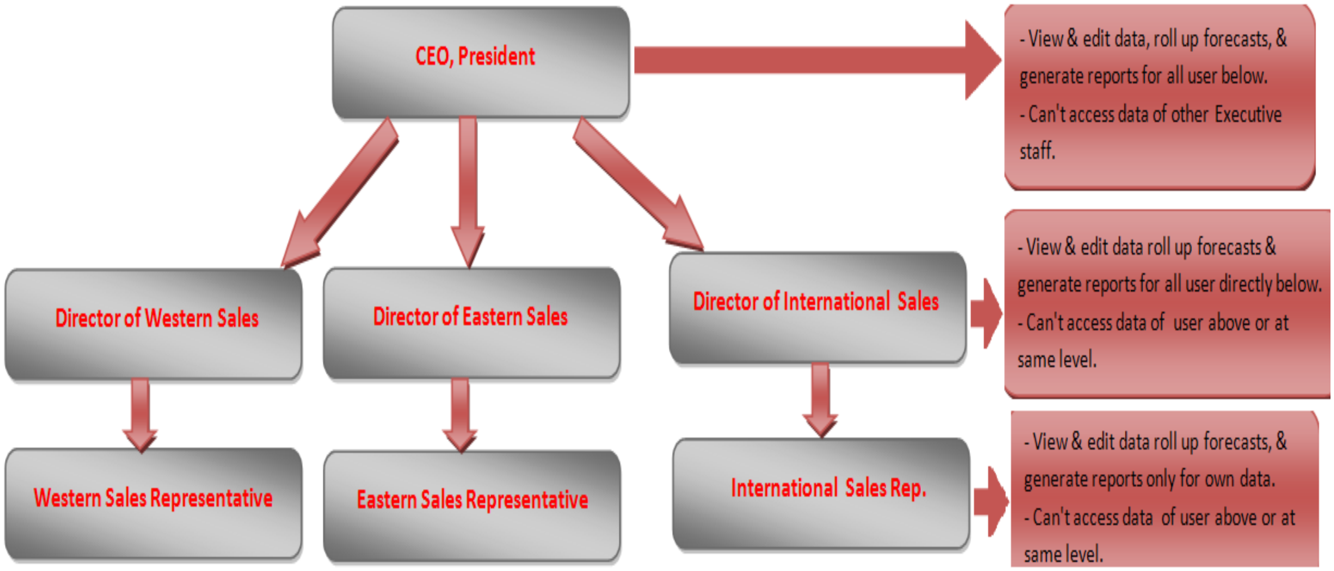
The following requirements apply to custom objects that have a master-detail relationship with a standard or custom object:

Action	Required Privileges
Create a record	"Create" permission and either read or read/write access to the related master record, depending on the value of the `Sharing Setting` attribute of the master-detail relationship field on the detail object.
View a record	"Read" permission and read access to the related master record. If the record has two master records in a many-to-many relationship, the user must have read access to both master records.
Edit a record	"Edit" permission and either read or read/write access to the related master record, depending on the value of the `Sharing Setting` attribute of the master-detail relationship field on the detail object.
Delete a record	"Delete" permission and either read or read/write access to the related master record, depending on the value of the `Sharing Setting` attribute of the master-detail relationship field on the detail object. When a user deletes a record that has related custom object records, all related custom object records are deleted regardless of whether the user has delete permission to the custom object.

Manage record access with the role hierarchy

Roles :

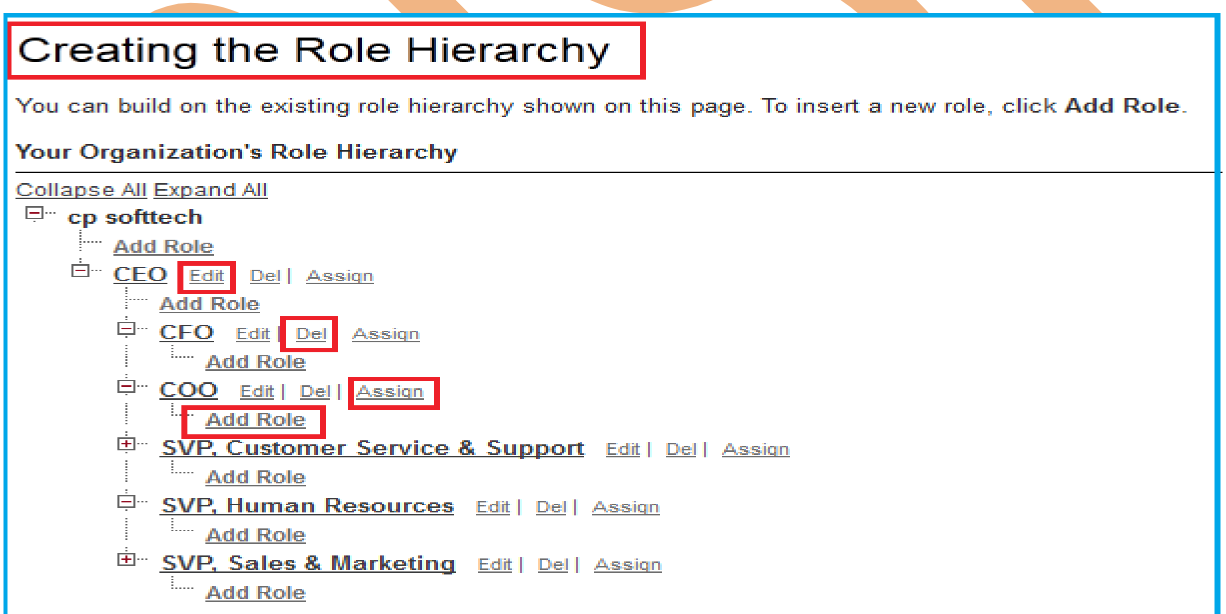
By using SalesForce.com you can Set in your organization Roles. Roles are one of the ways you can control access to records. Set up your Role Hierarchy to control how your organization reports on and accesses data.



How to Set Rules :

Click **Setup** > **Manage user** > **Rules** then click on **Set Up Rules** button . see below.

There you can see that your organization role hierarchy , here you can Edit role , Delete Role and Add Role.



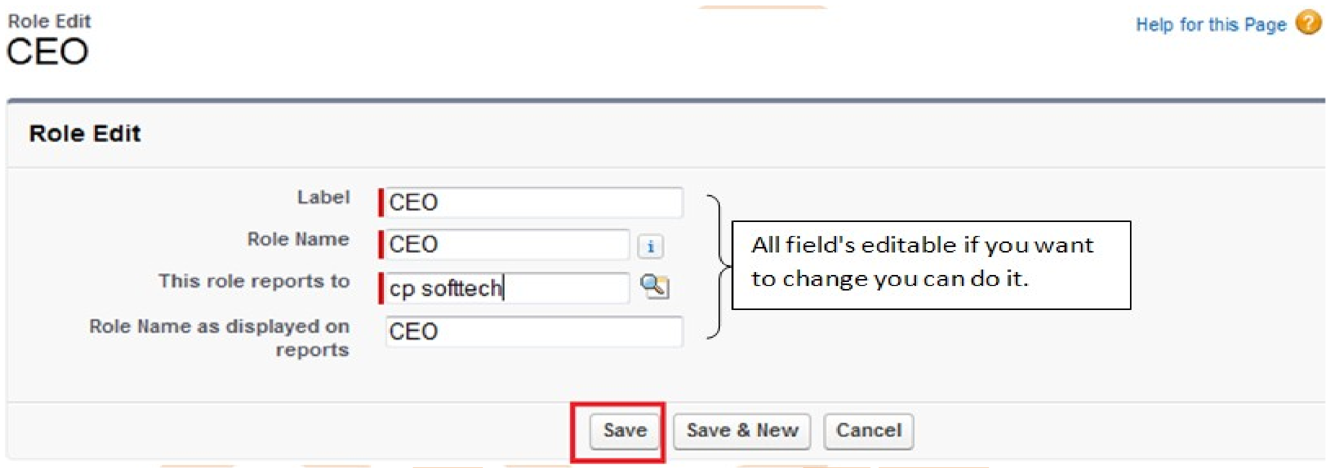
Edit Role :

Step 1 :

Click on Edit link for Editing role.

Step 2 :

if you need to change field's name you can do it. after that click on **Save** button.



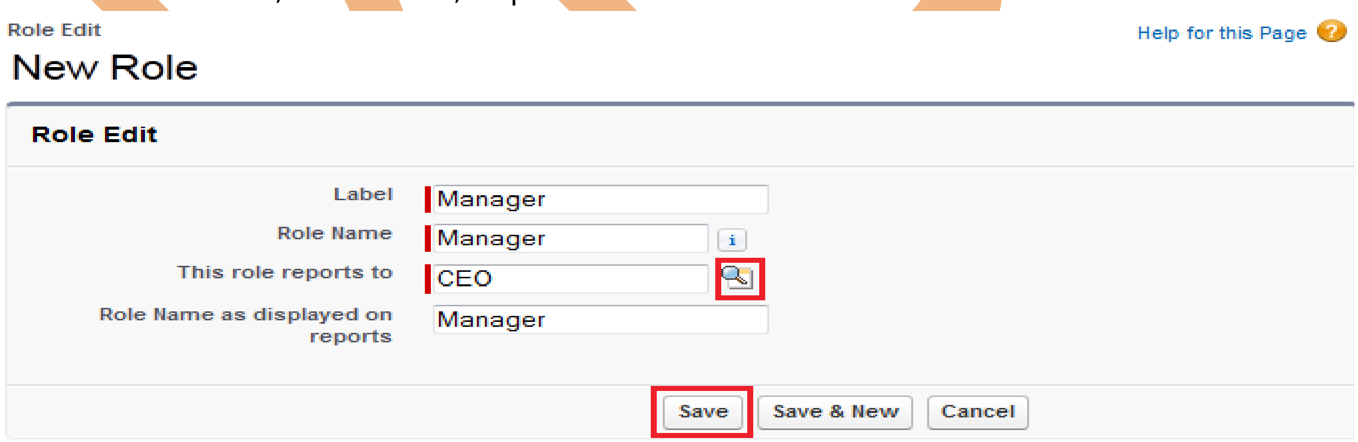
Add Role :

Step 1 :

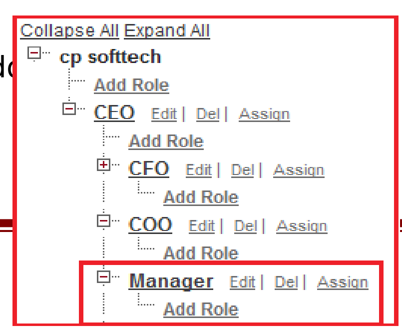
Click on Add Role link for Editing role.

Step 2 :

Fill all field's Label, Role Name, Report to then click on **Save** button.



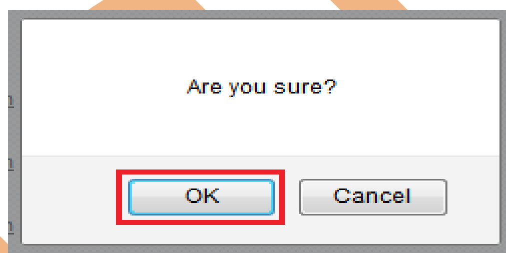
After that you can see the Role Hierarchy list Manager is add



Delete Role :

By using **Delete** link you can delete Role in hierarchy.

Click on Del link button you can get conformation Message click ok button you can delete Role.

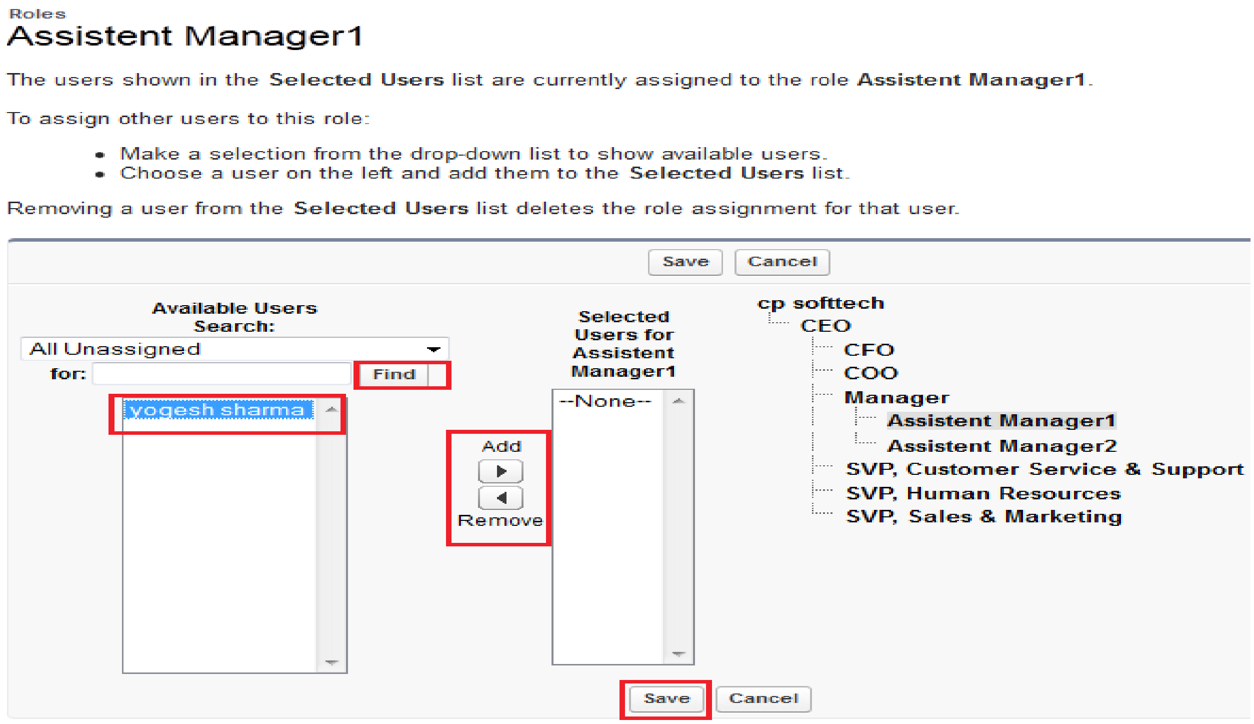


Assign Role :

First you can click on **Assign** link .

Then select user name, After then select user name click on **Add** button, Then click on **Save** button.

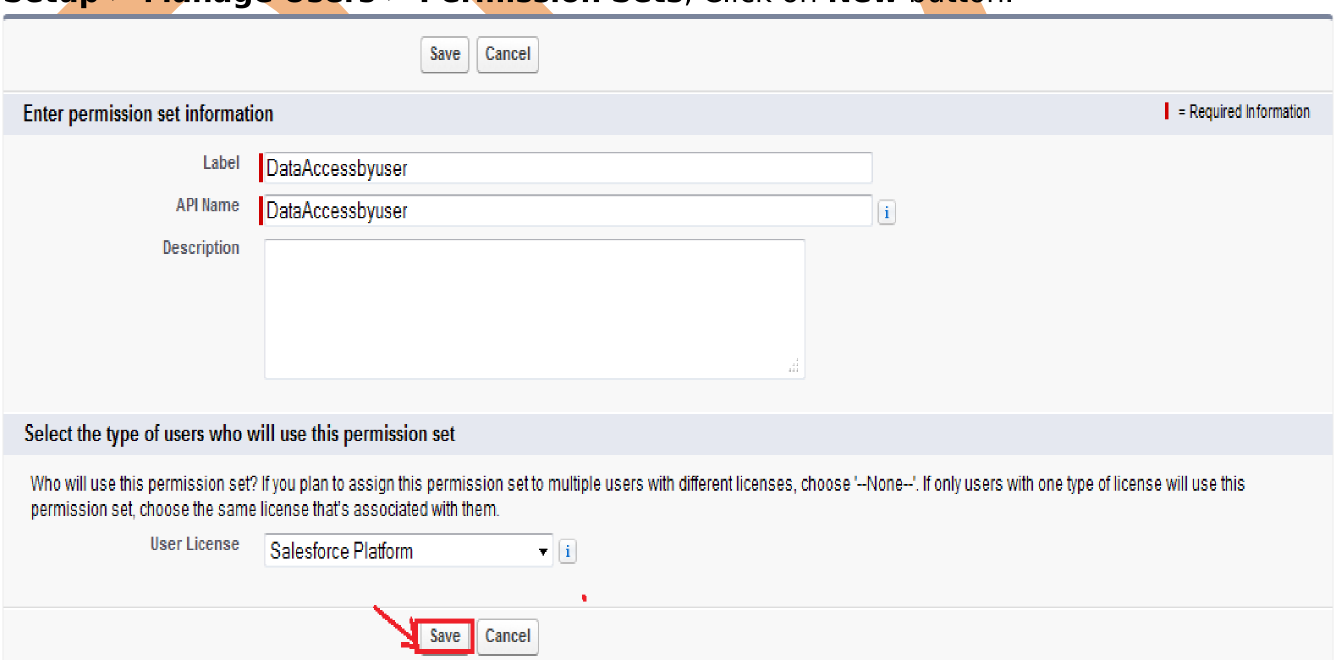
You can also Find user in available users.s

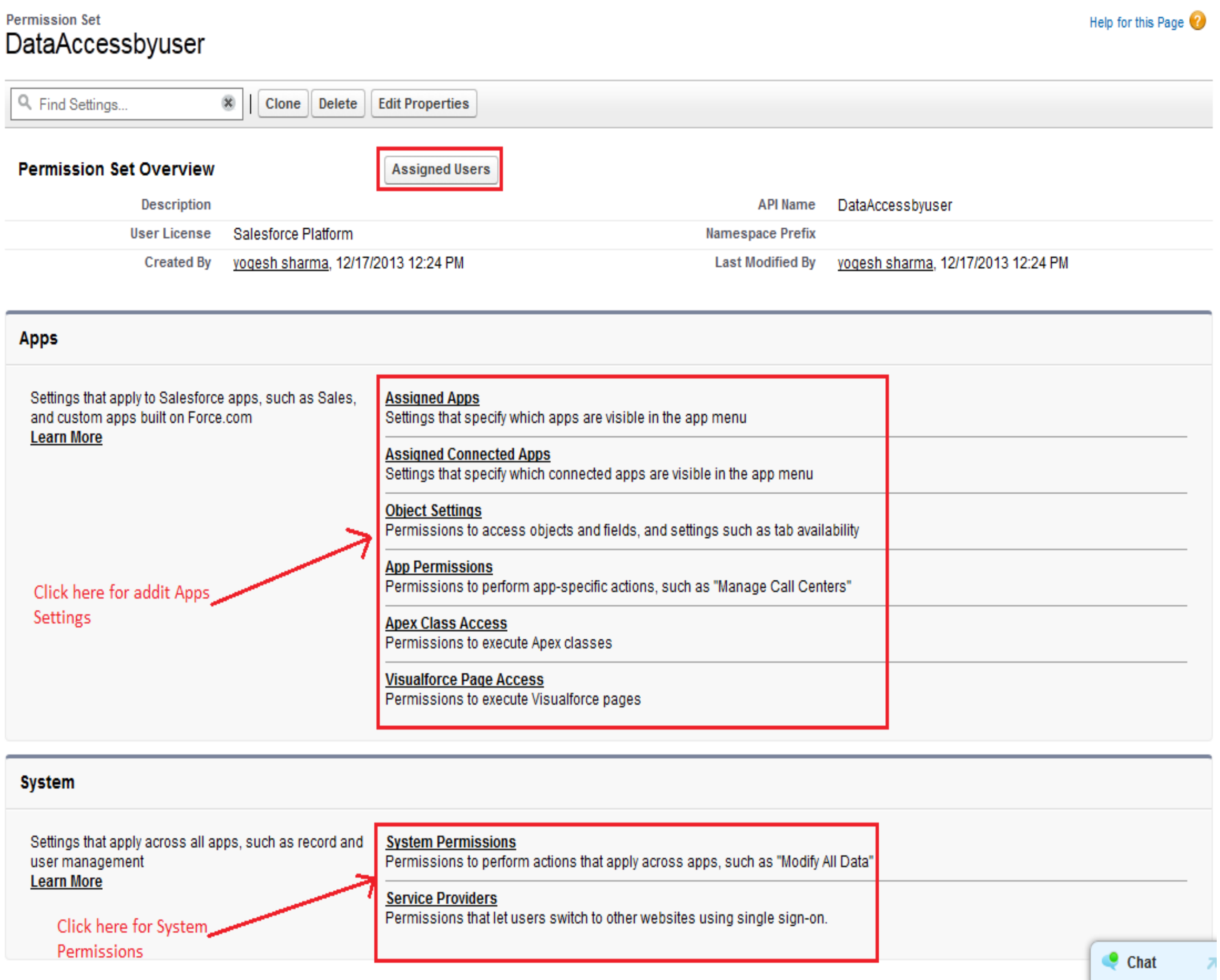


Permission Sets :

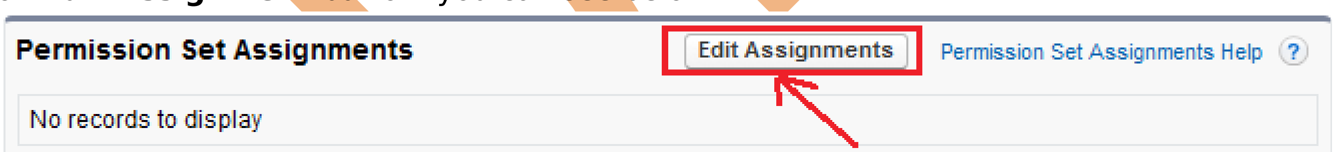
How to Set Permission :

Setup > **Manage Users** > **Permission Sets**, Click on **New** button.





After that click on Users.
Setup > **Manage Users** > **User**, click on **New** User or if want to update existing user profile click on user profile after that **select Permission Set Assignments** and click on **Edit Assignment** button. you can see below.



After that select user permissions, then assign user permissions then click on Save button. you can see below .

Exceptions

An exception is a problem that arises during the execution of a program. An exception can occur for many different reasons.

An exception denotes an error that disrupts the normal flow of code execution. You can use Apex built-in exceptions or create custom exceptions. All exceptions have common methods.

All exceptions support built-in methods for returning the error message and exception type. In addition to the standard exception class, there are several different types of exceptions.

Exception	Description
AsyncException	Any problem with an asynchronous operation, such as failing to enqueue an asynchronous call.
CalloutException	Any problem with a Web service operation, such as failing to make a callout to an external system.
DmlException	Problem with a DML statement, such as an insert statement missing a required field on a record.
EmailException	Problem with email, such as failure to deliver. For more information, see Outbound Email.
InvalidParameterValueException	Problem with a URL. This is generally used with VisualForce pages. For more information on VisualForce.
JSONException	Problem with JSON serialization and deserialization operations. For more information, methods of System.JSON, System.JSONParser, and System.JSONGenerator.
ListException	Problem with a list, such as attempting to access an index that is out of bounds.
MathException	Problem with a mathematical operation, such as dividing by zero.

NoAccessException	Problem with unauthorized access, such as trying to access an sObject that the current user does not have access to. This is generally used with VisualForce pages.
NoDataFoundException	Problem with data that does not exist, such as trying to access an sObject that has been deleted. This is generally used with VisualForce pages.
NoSuchElementException	Used specifically by the Iteratornext method. This exception is thrown if you try to access items beyond the end of the list. Ex:- if iterator.hasNext() == false and you call iterator.next(), this exception is thrown.
NullPointerException	Problem with dereferencing null, such as in the following code: String s; s.toLowerCase();
QueryException	Problem with SOQL queries, such as assigning a query that returns no records or more than one record to a singleton sObject variable.
RequiredFeatureMissing	A Chatter feature is required for code that has been deployed to an organization that does not have Chatter enabled.
SearchException	Any problem with SOSL queries executed with SOAP APIsearch() call, for example, when the searchString parameter contains less than two characters.
SecurityException	Any problem with static methods in the Crypto utility class. For more information, see Crypto Class.
SerializationException	Problem with the serialization of data. This is generally used with VisualForce pages.
SObjectException	Problem with sObject records, such as attempting to change a field in an update statement that can only be changed during insert.
StringException	Problem with Strings, such as a String that is exceeding your heap size.
TypeException	Problem with type conversions, such as attempting to convert the String 'a' to an Integer using the valueOf method.
VisualforceException	Problem with a VisualForce page.
XmlException	Problem with the XmlStream classes, such as failing to read or write XML.

Common Exception Methods :

Name	Return Type	Description
getCause	Exception	Returns the cause of the exception as an exception object.
getLineNumber	Integer	Returns the line number from where the exception

		was thrown.
getMessage	String	Returns the error message that displays for the user.
getStackTraceString	String	Returns the stack trace as a string.
getTypeName	String	Returns the type of exception, such as DmlException, ListException, MathException, and so on.
initCause	void	Sets the cause for this exception, if one has not already been set.
setMessage	void	Sets the error message that displays for the user.

EmailException and DMLException Methods :

Name	Return Type	Description
getDmlFieldNames	String []	Returns the names of the field or fields that caused the error described by the ith failed row.
getDmlFields	Schema.sObjectField []	Returns the field token or tokens for the field or fields that caused the error described by the ith failed row. For more information on field tokens, see Dynamic Apex.
getDmlId	String	Returns the ID of the failed record that caused the error described by the ith failed row.
getDmlIndex	Integer	Returns the original row position of the ith failed row.
getDmlMessage	String	Returns the user message for the ith failed row.
getDmlStatusCode	String	Deprecated. Use getDmlType instead. Returns the Apex failure code for the ith failed row.
getDmlType	System.StatusCode	Returns the value of the System.StatusCode enum.
getNumDml	Integer	Returns the number of failed rows for DML exceptions.

Manage field-level security

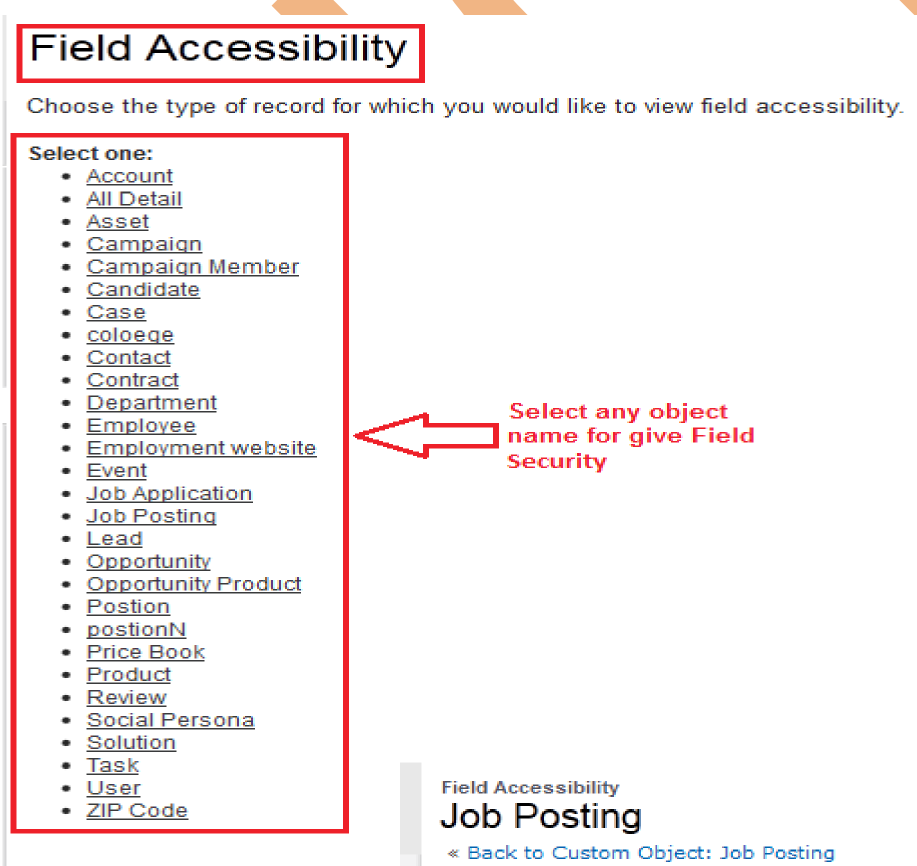
SalesForce.com provide many sections, following sections describe the characteristics and behaviors of page layouts, mini page layouts, and field-level security.

Administrators restrict users' access to view and edit specific following fields :

- Detail and edit pages.
- Related lists.
- List views.
- Reports.
- Connect Offline.
- Email and mail merge templates.
- Custom links.
- The partner portal.
- The SalesForce Customer Portal.
- Synchronized data.
- Imported data.

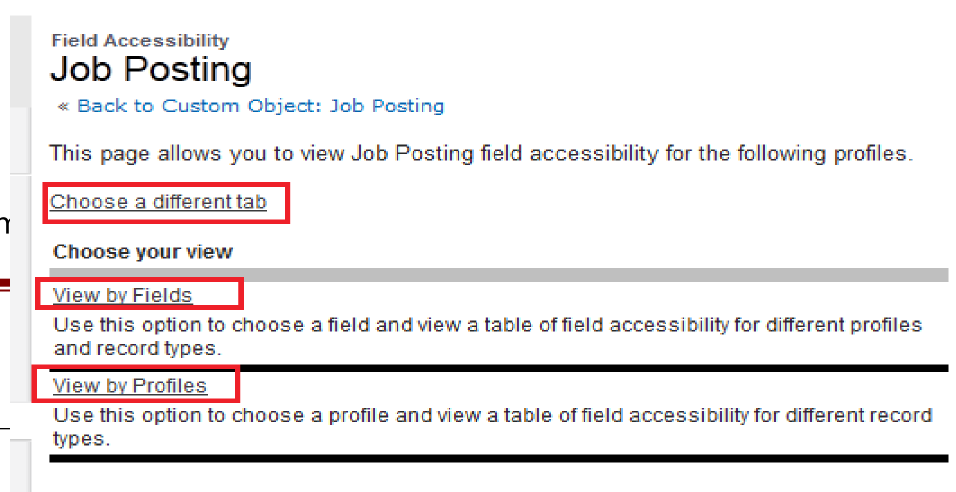
For View Field level Security :

Setup > **Customize** > **user Page Layout**, after that choose any object to apply Field Security.



Step 1 :

Choose any link for perform

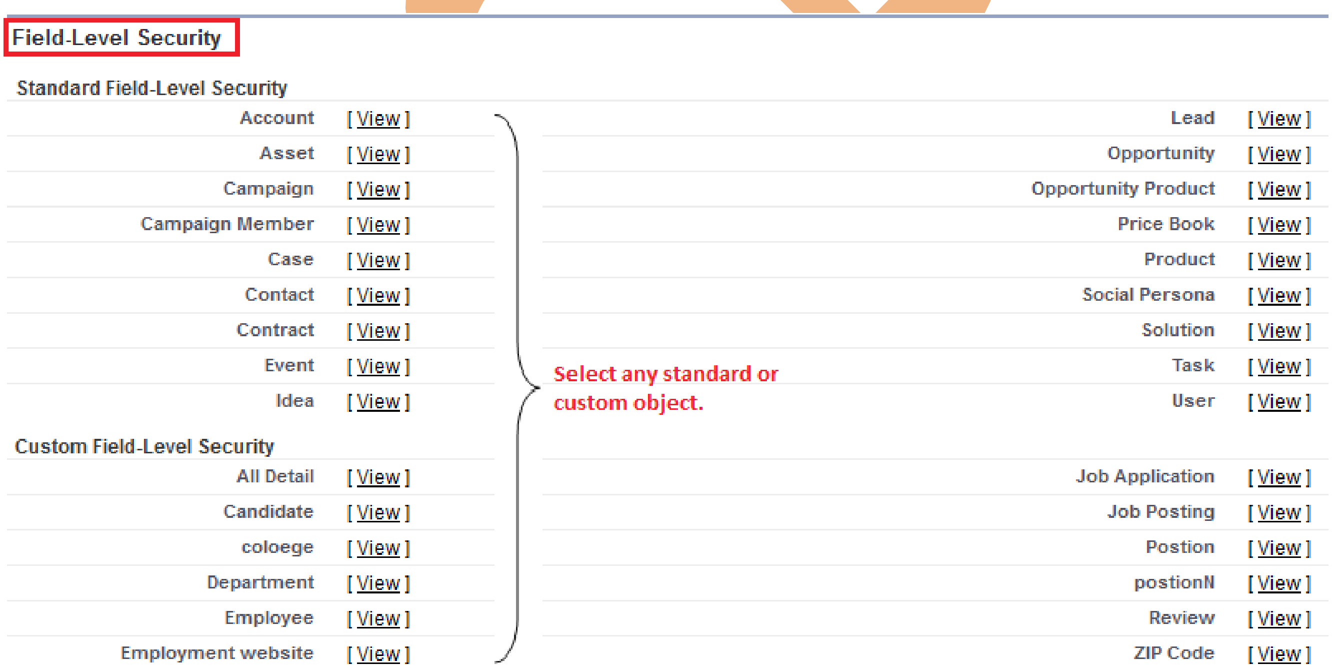


action.

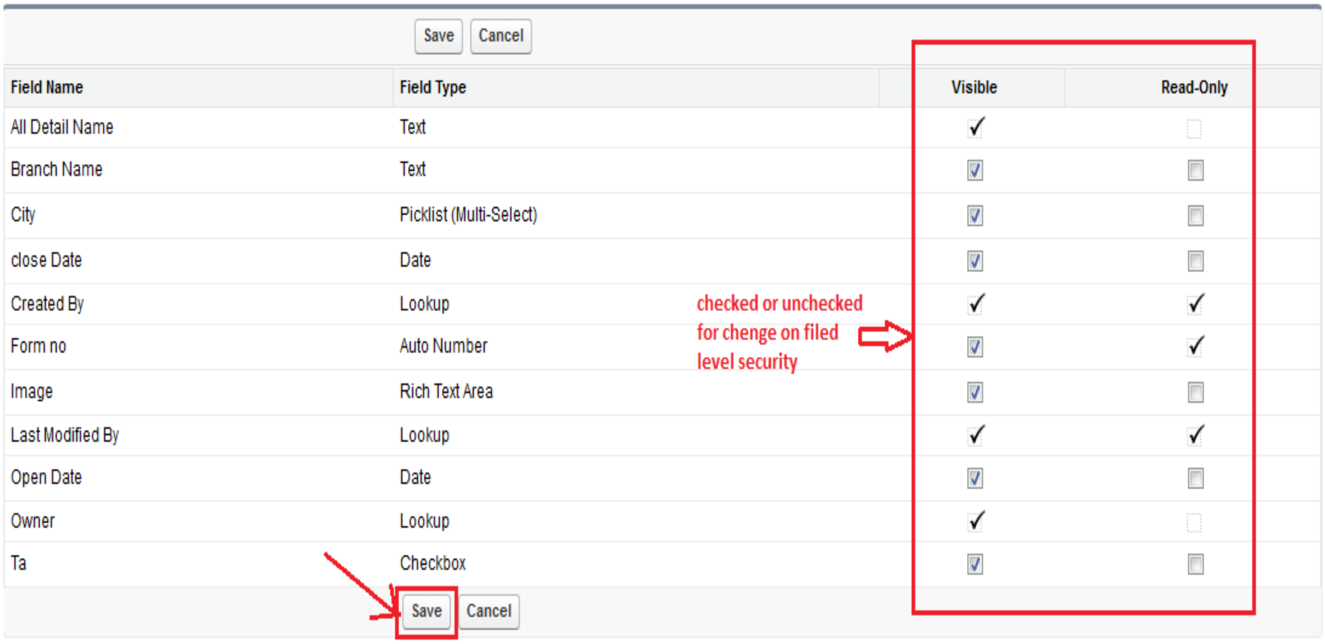
Select any link and see Filed level security .

Manage Field Level Security :

Setup > **Manage user** > **Profile**, Select any profile then go to down and you can see **Field level security** , click on any filed . you can see below.



Step 1 : click on Edit button.
Step 2 : check or uncheck check box for Field level security after that click on **Save** button.



Save Cancel

Field Name	Field Type	Visible	Read-Only
All Detail Name	Text	✓	
Branch Name	Text	✓	
City	Picklist (Multi-Select)	✓	
close Date	Date	✓	
Created By	Lookup	✓	✓
Form no	Auto Number	✓	✓
Image	Rich Text Area	✓	
Last Modified By	Lookup	✓	✓
Open Date	Date	✓	
Owner	Lookup	✓	
Ta	Checkbox	✓	

Save Cancel