

Cloud application and cloud data security management

Week 8

School of Software

Faculty of Engineering and Information Technology

University of Technology Sydney



SCHOOL OF SOFTWARE

Learning Objectives

- Security of Cloud Objects
- Understand “*Profiles*” and “*Users*”
- Control Access to Objects in Force.com
- Control Access to Fields in Force.com
- Control Access to Records in Force.com
 - Organization-Wide Default
 - Role Hierarchies
 - Sharing Rules
 - Manual Sharing Rules

Security of Cloud Objects

- A cloud application designed on Force.com platform, is a set of collaborating objects, to deliver the desired functionality
- The cloud application (like any other enterprise application) will comprise of sensitive information.
- In order to ensure that only the relevant and authorized persons can see relevant information we need security mechanisms on the Force.com platform
- Force.com platform offers simple-to-configure security mechanisms to regulate access to application and the data comprising it.

Security of Cloud Objects

- Using the security controls (or security mechanisms) provided by Force.com platform, the application owner/application designer can:
 - Control who accesses the application;
 - Control who accesses the objects comprising the application;
 - Control the level of access to the fields within the objects;
 - Control access to records of an object (in terms of who can access the records of a given object)
- We will learn how to use these security controls, to enable fine-grained access to users of your application and application data

How can security of cloud objects be enforced on Force.com platform?

What do you want to control?	Force.com provided security control mechanism
Control access to the user-defined objects on the Force.com platform	Object-level access
Control access to user-defined fields within the objects	Field-level access
Control access to the records of an user-defined objects	(a) Organization-wide defaults for records (b) Role Hierarchies (c) Sharing rules for records (d) Manual Sharing rules to access records

Homework prior to defining security controls

- It is imperative that the application designer/owner has a very clear idea/requirement of:
 - The various (or different) types of “valid users” that will need to access the application and the application data;
 - The level access (to the application data) that each of these “valid users” require.

Case Study

- Consider a web-enabled *Human Resource Management Application* for Company X. Some of the “valid types” of users for this HRM application could be:
- “Head of Area” to keep an account of the performance of employees within his/her department (or area).
 - Should be able to edit all the information of employees under his supervision, except information classified as sensitive, such as Tax File Number, Date of Birth, Salary information, Illness records etc ...;
 - Should not be able to add a new employee, or delete a new employee from the system;
 - The manager should have access to the employment records of only the employees in his area/supervision;
 - Should be able to update the field “*Employment Performance Record*” of each employee under his supervision

Case Study .. Continued

- “Human Resource Staff” to supervise multiple Heads of Areas or Managers
 - They can change the salary of staff under their supervision;
 - They can add new staff or delete existing staff for areas under their supervision only;
 - Have complete access and view of the entire employment records of all staff under their supervision including the Head of Area.
- “Human Resource Manager” to supervise multiple Human Resource Staff
 - Can change the current assignment of Human Resource Staff to areas/units with Company X;
 - They can additionally delete existing Human Resource Staff, or add new Human Resource Staff;
 - Have complete access and view over the employment records of all staff under their supervision including that of Human Resource Staff

Case Study .. Continued

- “Chief Executive Officer”
 - Have complete access and view of the employment records of all staff under his/her supervision including that of Human Resource Manager.
- “Any other user” . This category of users includes employees of Company X, and people outside Company X who will access the information from the HRM system. This type of users can:
 - Can view the name, qualification, email address, extension number etc., of a given employee (say Employee A);
 - Cannot view any other information of the employee (Employee A).

Different “types” of users for the HRM application

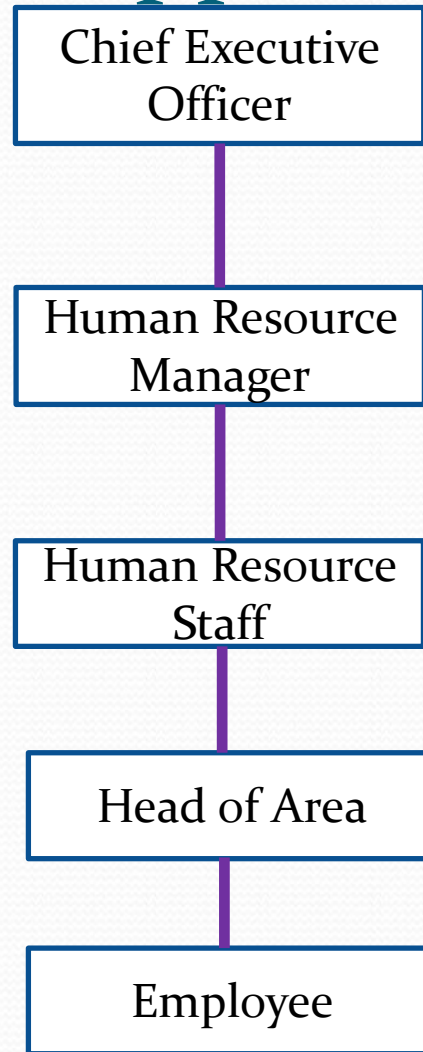


Figure: Organizational hierarchy for Company X and the different types of users requiring access to the HRM application

Table of permissions

- Based on the above, the application designer needs to create a table of permissions
- For each different “type of user”, a corresponding table of permissions needs to be created
- A table of permissions (for a given type of user) manifests:
 - Which objects, should the users of this type have access to?;
 - Which fields within an object, should the users of this type have access to, or should be able to access?;
 - Which records of a given object should the user of this type have access to?.

Creating table of permissions (Field level security)

- In order to create table of permissions, the application designer will need to think for the answers of:
 - Does an object have sensitive field information that should be exposed to selected users only?
 - Example: Consider fields such as “Salary information” and “Employment Performance” of an employee A in Company X. These fields are part of employee object.
 - Only the employee A’s manager, the relevant HR staff, HR manager, and CEO should have access to this field. Further employees A’s manager should not be able to change the salary field;
 - All other people (including employees A’s co-workers), should not be able to see this information, but should be able to see general information about employee A, such as employees A’s name, qualification etc....
 - This process of providing access to selected fields in a given object (for a given type of user) is achieved using “*Field Level Security Settings*” on the Force.com platform

Creating table of permissions (Record Level Security)

- In order to create table of permissions, the application designer will need to think for the answers for:
 - Should all the instances of a given object (records) be accessed by all the users?
 - If selective access to records of given object is to be provided, what types of user(s) should be provided the selective access?
 - Example: In the Human Resource Management System, a given HR manager, should have complete control over the employment records, and details of all the employees under his supervision. However, he/she, should not have any access over the employment records and details of other employees who are not under his supervision.
- This process of providing access to selected records of a given object (for a given type of user), is achieved using “*Record Level Security Settings*” on the Force.com platform

Creating “*Permission Table*”

- For “each type of user”, a corresponding *Permission Table* needs to be created.
- The columns in the permission table correspond to the different objects in the application
- The level of access for each type of user needs to be clearly specified.

Permission Table for “Any type of user”

Employee Object (in the HRM application)

Read the employee records (only information such as name, qualification, email address, and extension number)

Permission Table for “Head of Area”

Employee Object (in the HRM application)

Edit employee records under his supervision (except information such as salary information, Tax File Number, Date of Birth, Illness information etc...)

Creating Permission Table

**Permission Table
for “*Human
Resource Manager*”**

Employee Object (in the HRM application)
Edit complete details of employee records (under his supervision only)
Create new employee records
Delete existing employee records

Profile

- Profile is a collection of settings and permissions that determine what a user can do on the Force.com Platform.
- “Profile” on the Force.com platform is used to define and regulate access to a given types of users to:
 - Applications (Developed using Force.com);
 - Object permissions (Object-level permissions);
 - Field-level permissions
- When a new user is created on the Force.com platform, it needs to be assigned to a Profile.
 - All the users assigned to a given profile will have the same access control properties
 - Multiple users can be assigned to a given profile; but a given user can be assigned to one profile only (at a given point in time)

Profile

- The profile assigned to a user (assume user A) determines:
 - The (custom) applications that the user A can access;
 - The objects the user A can view, create, edit, and delete;
 - The tabs that the user A can view in the application;
 - The object fields that the user A can view or edit;
 - The hours during which the user A can log in to the application;
 - The IP addresses from which the user A can log in to the application.

Profile

- Broadly speaking there are two types of profiles on the Force.com platform:
 - Standard (or Force.com defined) profiles. Some of these are:
 - System Administrator Profile;
 - Standard User Profile.
 - Custom (or user-defined) profiles
 - New profile can be created to give access to a different “type of user”.
- The standard profiles include a default set of permissions for all the pre-defined objects on the Force.com platform
- A custom profile can be created by basing it on a standard profile
- When a custom object is created, unless you explicitly assign it to a given profile (standard or custom profile), the users in the corresponding profile cannot see or view the custom object.

Profile - Create Profile and User

- To create a new profile, you need to base it on an existing Force.com defined profile
- Make use of Standard User profile.
- To create a new profile:
 - Setup → Administer → Manage Users → Profiles
- Create a new user
 - Setup → Administer → Manage Users → Users
- Assign profile to a user

Profile – Create New (Custom) Profile

Select: Setup → Administer → Manage Users → Profiles

Profiles

All Profiles ▾ Edit | Delete | Create New View

Click here to create a new profile


New Profile 					A B C D E F G				
<input type="checkbox"/>	Action	Profile Name ↑	User License	Custom					
<input type="checkbox"/>	Edit Clo...	Authenticated Website	Authenticated Website	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Chatter External User	Chatter External	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Chatter Free User	Chatter Free	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Chatter Moderator User	Chatter Free	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Contract Manager	Salesforce	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Del...	Custom: Marketing Profile	Salesforce	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	Edit Del...	Custom: Sales Profile	Salesforce	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	Edit Del...	Custom: Support Profile	Salesforce	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Customer Portal Manager Custom	Customer Portal Manager Custom	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Customer Portal Manager Standard	Customer Portal Manager Standard	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Force.com - Free User	Force.com - Free	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Gold Partner User	Gold Partner	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	High Volume Customer Portal	High Volume Customer Portal	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Del...	Hiring Manager	Salesforce	<input checked="" type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Marketing User	Salesforce	<input type="checkbox"/>					
<input type="checkbox"/>	Edit Clo...	Read Only	Salesforce	<input type="checkbox"/>					
1-23 of 23 ▾ 0 Selected ▾					◀◀ Previous Next ▶▶				

Figure: Profiles in Force.com platform

Profile – Creating New (Custom) Profile

Clone Profile

Enter the name of the new profile.

You must select an existing profile to clone from.

Existing Profile

Standard User

User License

Salesforce

Profile Name

Human Resource Manager

Save

Cancel

Base profile name

New profile name

Figure: Create new profile based on an existing profile and save it

Profile – Edit Profile

Profile

Human Resource Manager

[« Back to List: Profiles](#)

Users with this profile have the permissions and page layouts listed below. Administrators can change a user's profile by editing that user's personal information.

If your organization uses Record Types, use the Edit links in the Record Type Settings section below to make one or more record types available to use.

[Login IP Ranges \[0\]](#) | [Enabled Apex Class Access \[0\]](#) | [Enabled Visualforce Page Access \[0\]](#)

Profile Detail

[Edit](#) [Clone](#) [Delete](#) [View Users](#)

Name	Human Resource Manager		
User License	Salesforce	Custom Profile	<input checked="" type="checkbox"/>
Description			
Created By	Farookh Hussain, 1/04/2012 1:26 PM		Modified By Farookh Hussain, 1/04/2012 1:26 PM

Console Settings

Console Layout [\[Edit \]](#)

Page Layouts

Standard Object Layouts

Home Page Layout	DE Default [View Assignment]	Event	Event Layout [View Assignment]
------------------	---------------------------------------------------	-------	---------------------------------------------------------------------

[Click here to edit a profile](#)

Assign application access to profile

PROFILE EDIT

Human Resource Manager

Set the permissions and page layouts for this profile.

Select “visible” if you wish the users assigned to this profile to have access to this application

Profile Edit

Name
Human Resource Manage

User License
Salesforce

Description

Custom Profile ☒

Custom App Settings

	Visible	Default		Visible	Default
Call Center	<input checked="" type="checkbox"/>	<input type="radio"/>	Recruiting App	<input checked="" type="checkbox"/>	<input type="radio"/>
Community	<input checked="" type="checkbox"/>	<input type="radio"/>	Sales	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>
Farookh's Application	<input type="checkbox"/>	<input type="radio"/>	Salesforce Chatter	<input checked="" type="checkbox"/>	<input type="radio"/>
HR Management Application	<input checked="" type="checkbox"/>	<input type="radio"/>	Sample Console	<input type="checkbox"/>	<input type="radio"/>
Marketing	<input checked="" type="checkbox"/>	<input type="radio"/>	Site.com	<input checked="" type="checkbox"/>	<input type="radio"/>

Assigning tab access control to profiles

Standard Tab Settings

Home	Default On	Forecasts	Tab Hidden
Accounts	Default On	Groups	Default On
Answers	Default On	Ideas	Default On
Campaigns	Default On	Leads	Default On
Cases	Default On	Opportunities	Default On
Chatter	Default On	People	Default On
Console	Tab Hidden	Portals	Tab Hidden
Contacts	Default On	Products	Default On
Contracts	Default On	Profile	Default On
Dashboards	Default On	Reports	Default On
Data.com	Default Off	Site.com	Default On
Documents	Default On	Solutions	Default On
Files	Default On		

Custom Tab Settings

Candidates	Default On	Job Applications	Default On
Customer Records	Tab Hidden	Job Postings	Default On
Employee	Default On	Positions	Default On
Employment Website	Tab Hidden		
	Default Off		
	Default On		

Assign access control for users of this profile to custom and standard objects

Assigning tab access control to profiles



- Three levels of access control can be assigned to objects from a given profile page



Access control on the object	What does it mean?
Tab Hidden	The object will be completely hidden from the users assigned to this profile
Default Off	The object will be made available to the profile's users; but it will be hidden from the user's page; the user will have to select "All Tabs" to view this object.
Default On	The object will be made available to the profile's users on top of user's page.

Profile and Custom Objects

- When defining a profile you can specify the level and type of access to each user-defined object

Custom Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All 	Modify All 
Candidates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer Records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employee	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employment Website	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All 	Modify All 
Job Applications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Job Postings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Positions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reviews	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Assign level and type of access to each standard object while defining a profile

Objects and Access control

- There are different types of access control properties that you may specify on objects when defining a profile (depending on your requirements)
- The “*permissions table*” can used to determine and specify level of access

Types of access control on objects

Level of access control	What does it mean?
Read	Users assigned to this profile can read <u>all</u> the records of this object
Create	Users assigned to this profile can create new records corresponding to this object
Edit	Users assigned to this profile can edit the records of this object
Delete	Users assigned to this profile can delete the records of this object

Field-level access control

- Using object-level access control, one can regulate access to objects as a whole:
 - Give access to objects (as a whole), to selected profiles (and hence users assigned to that profile); (or)
 - Restrict access to objects (as a whole), to selected profiles (and hence users assigned to that profile).
- Cannot regulate or specify access to individual fields within an object
 - Example: Using object-level access control, we cannot enforce that the Head of Area(s) in Company X should not be able to access and view sensitive information such as Tax File Number, Illness information of the employees under their supervision.
- Field Level access control (or field-level security), can be used to regulate and manage control to individual fields in an object (such as the Employee object in this case)

Field-level access control

- Field level security controls determine whether a given profile's users' can view, edit or delete the value of a given field within an object.
- Permission tables specify restricted field access on different objects (for different types of users).
- The field-level access control for custom and standard objects can be specified by choosing the following:
 - Setup → Administer → Manage Users → Profiles
 - Select the profile for which you intend to assign field-level controls

Field-level access control

Select: Setup → Administer → Manage Users → Profiles

Change field settings for standard objects by clicking here

Field-Level Security			
Standard Field-Level Security			
Account	[View]	Lead	[View]
Asset	[View]	Opportunity	[View]
Campaign	[View]	Opportunity Product	[View]
Campaign Member	[View]	Product	[View]
Case	[View]	Social Persona	[View]
Contact	[View]	Solution	[View]
Contract	[View]	Task	[View]
Event	[View]	User	[View]
Idea	[View]		
Custom Field-Level Security			
Candidate	[View]	Job Application	[View]
Customer	[View]	Job Posting	[View]
Customer Record	[View]	Position	[View]
Employee	[View]	Review	[View]
Employment Website	[View]		

Change field settings for custom objects by clicking here

Field-level access control

Employee Field-Level Security for profile
Standard User

[Help for this page](#)

<div>Save Cancel</div>			
Field Name	Field Type	Visible	Read-Only
Created By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Date of Birth	Date	<input type="checkbox"/>	<input type="checkbox"/>
Email Address	Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Employee Name	Text	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Extension Number	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Illness Records	Rich Text Area	<input type="checkbox"/>	<input type="checkbox"/>
Last Modified By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Name	Text Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Owner	Lookup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Qualification	Text Area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Salary	Number	<input type="checkbox"/>	<input type="checkbox"/>
Tax File Number	Number	<input type="checkbox"/>	<input type="checkbox"/>
<div>Save Cancel</div>			

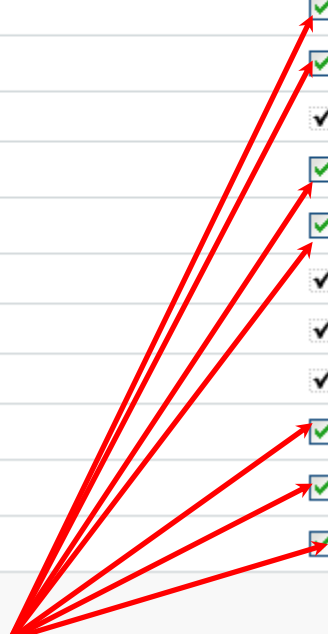
Fields of an object (in this case the employee object)

Rule 1: If both “Visible” and “Read-Only” boxes are selected then this field will be “Read Only” for users of this profile

Field-level access control

Employee Field-Level Security for profile
Human Resource Manager [Help](#)

Field Name	Field Type	Visible	Read-Only
Created By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Date of Birth	Date	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address	Email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Name	Text	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Extension Number	Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Illness Records	Rich Text Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Last Modified By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Name	Text Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Owner	Lookup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Qualification	Text Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Salary	Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Tax File Number	Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Rule 2: If only “Visible” is selected then this field is editable for users of this profile

Field-level access control

Employee Field-Level Security for profile
Standard User

[Help for this f](#)

<div>Save Cancel</div>			
Field Name	Field Type	Visible	Read-Only
Created By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Date of Birth	Date	<input type="checkbox"/>	<input type="checkbox"/>
Email Address	Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Employee Name	Text	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Extension Number	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Illness Records	Rich Text Area	<input type="checkbox"/>	<input type="checkbox"/>
Last Modified By	Lookup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Name	Text Area	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Owner	Lookup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Qualification	Text Area	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Salary	Number	<input type="checkbox"/>	<input type="checkbox"/>
Tax File Number	Number	<input type="checkbox"/>	<input type="checkbox"/>
<div>Save Cancel</div>			

Fields of an object

Rule 3: If neither box is selected then this field is hidden from the users of this profile

Record-level access controls

- Record-level access controls specify and regulate access to records of a given object
- Using *object-level access control*, access to objects (including creation, deletion or modification) as a whole can be specified using profiles.
- *Field-level access controls* build on top of object-level access controls to specify exceptions of access to fields within an object
- *Record-level access controls* build on top of object-level, and field-level access controls, to specify exceptions of access to records of the object.

Object-level and record-level access control

- If you restrict access to an object from a given profile (such as hiding it completely), the corresponding users' will not be able to view any of the records (or instances) of that object.
- If you give access to an object from a given profile (using object-level settings) such as “Read” or “Edit”; it **does not** necessarily imply that the users of this profile will be able to read or edit every instance of that object on the Force.com platform
- Using record-level settings, we can assign access or restrict access to specific set of records of a given object (by individual users or to profiles).
- The permissions on a record are always evaluated according to a combination of
 - Object-level permissions; and
 - Record-level permissions.

Record-level access control

- Four types of record-level access control measures:
 - Organization-Wide Defaults
 - Role Hierarchies
 - Sharing Rules
 - Manual Sharing

Organization-Wide Defaults

- Organization-wide defaults specify the baseline level of access that the most restricted user should have for the records of a given object
- Using organization-wide defaults the access to records of a given object is locked down to the most restrictive level
- Other record level security settings (*role hierarchies*', *sharing rules*', and *manual sharing rules*'), can be used to provide exceptions to the organization-wide defaults.

Organization-Wide Defaults for Objects

- Private
 - Only the record owner can view and edit the records of the object.
- Public Read Only
 - All users can view the object, but only the record owner can edit the records of the object.
- Public Read/Write
 - All users can view and edit the records of the object

Determining the Organization-Wide Default

- To determine the organization-wide default, the following questions need to be asked for each object:
 - **Question 1**: Who is the most restricted user of this object?
 - **Question 2**: Is there ever going to be an instance of this object that this user shouldn't be allowed to view?
 - **Question 3**: Is there ever going to be an instance of this object that this user shouldn't be allowed to edit?
- Based on our answers to these questions, we can determine the sharing model (organization-wide default) for this object

Flowchart for determining the Organization-Wide default

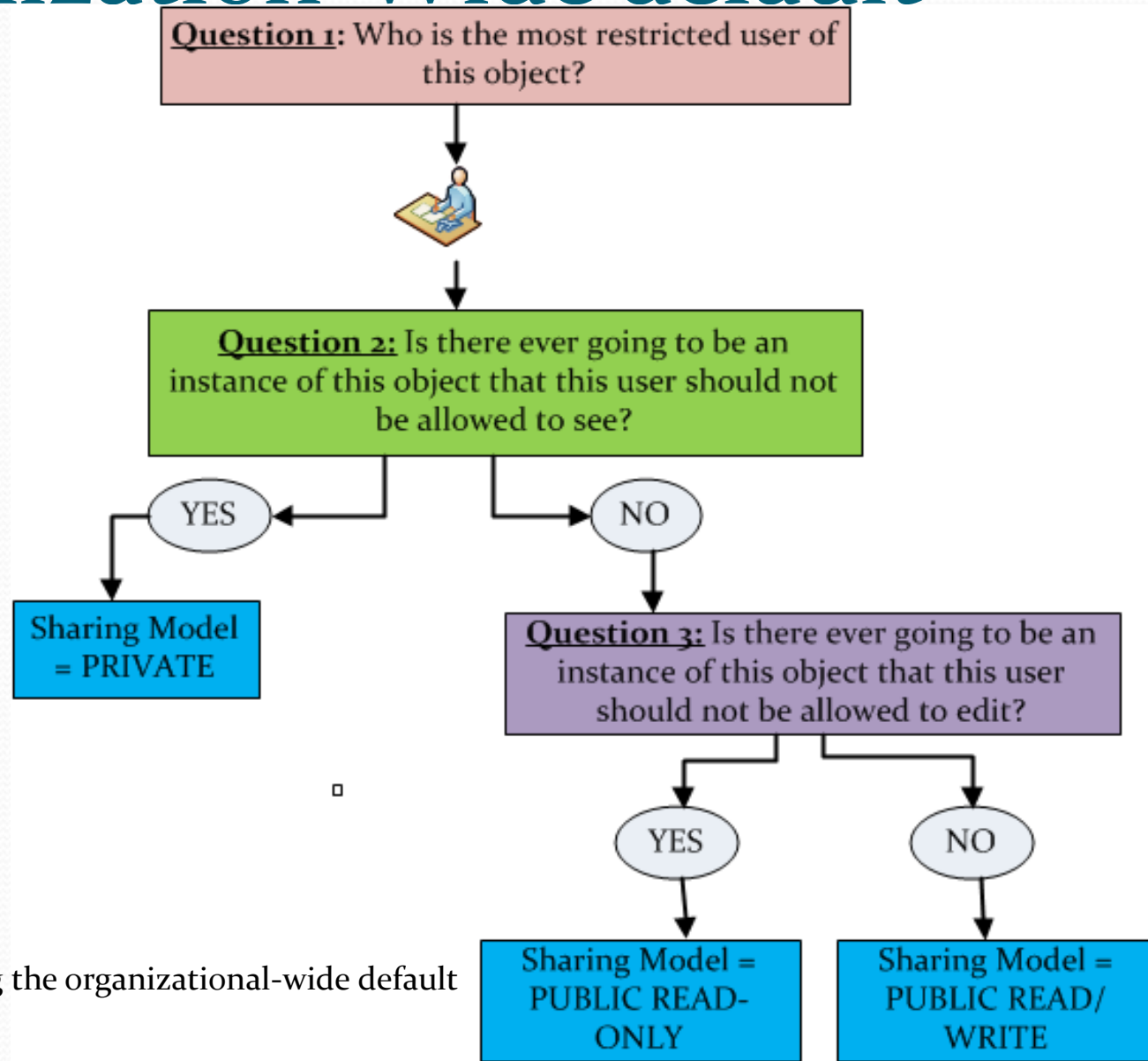


Figure: Flowchart for determining the organizational-wide default

Example of determining the organization-wide default

- Determine the organization-wide default for the “Employee” Object in the HRM application
 - **Question 1:** Who is the most restricted user of this object?
 - Answer: General Public Users, and the co-workers of company X
 - **Question 2:** Is there ever going to be an instance of this object that this user shouldn't be allowed to see?
 - Answer: No
 - **Question 3:** Is there ever going to be an instance of this object that this user shouldn't be allowed to edit?
 - Answer: Yes
- Based on the answers to these questions, the organization-wide default for this object should be “PUBLIC READ ONLY”

Specifying Organization-Wide defaults on the Force.com platform

- In order to specify Organization-Wide defaults on the Force.com platform select
 - Setup → Administer → Security Controls → Sharing Settings
 - In the Organization Wide Defaults area select “Edit”
 - Specify the organization wide default for the object.

Specifying Organization-Wide defaults

Select: Setup → Administer → Security Controls → Sharing Settings

Edit your organization-wide sharing defaults below. Changing these defaults will cause all sharing rules to be recalculated. This can take some time and resources depending on the amount of data in your organization.

SaveCancel

Object	Default Access	Grant Access Using Hierarchies
Lead	Public Read/Write/Transfer	<input type="checkbox"/>
Account, Contract and Asset	Public Read/Write	<input type="checkbox"/>
Contact	Controlled by Parent	<input type="checkbox"/>
Opportunity	Public Read/Write	<input type="checkbox"/>
Case	Public Read/Write/Transfer	<input type="checkbox"/>
Campaign	Public Full Access	<input type="checkbox"/>
Activity	Private	<input type="checkbox"/>
Calendar	Hide Details and Add Events	<input type="checkbox"/>
Price Book	Use	<input type="checkbox"/>
Candidate	Private	<input checked="" type="checkbox"/>
Customer	Public Read/Write	<input checked="" type="checkbox"/>
Customer Record	Public Read/Write	<input checked="" type="checkbox"/>
Employee	Public Read/Write	<input checked="" type="checkbox"/>
Employment Website	Private	<input checked="" type="checkbox"/>
Job Application	Public Read Only	<input checked="" type="checkbox"/>
Position	Public Read Only	<input checked="" type="checkbox"/>

Select the object, and specify the organization-wide default for the object

Role Hierarchies

- The first mechanism to share access to records is by “*Role Hierarchies*”
- Role Hierarchies can be used to ensure that, a user with a given “*organizational role*” *automatically* has access to all the records that users assigned to role(s) below him have.

Example of a hierarchy

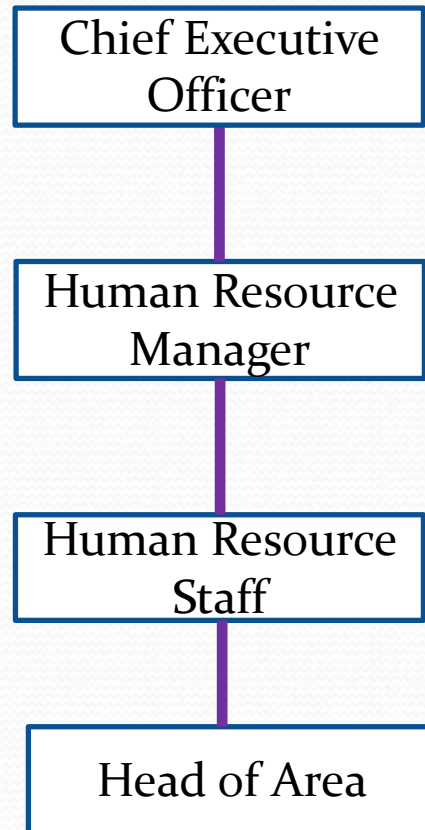


Figure: Example Role Hierarchy for Company X

Role Hierarchies vs. Profile

- Profiles are used to regulate object-level access control, and field-level access control
- In contrast to profiles, role hierarchies are used to regulate access to records of a given object.
- The organization-wide default mechanism restricts access to records of a given object to that of the most restricted user
 - The role hierarchies build on top of the organization-wide defaults, to expose selected records of a given object to selected users depending on their *role in the organization*.

Specifying Role Hierarchies on Force.com

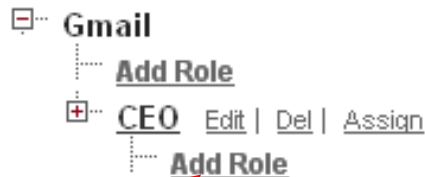
- In order to specify role hierarchy on the Force.com platform select
- Setup → Administer → Manage Users → Roles

Creating the Role Hierarchy

You can build on the existing role hierarchy shown on this page. To insert a new role, click **Add Role**.

Your Organization's Role Hierarchy

[Collapse All](#) [Expand All](#)





You can then define additional roles below the role of the Chief Executive Officer

You can then assign actual users to this role

Defining a new role

Role Edit
New Role

Role Edit

Label	<input type="text" value="Employee"/>
Role Name	<input type="text" value="Employee"/> 
This role reports to	<input type="text" value="Head of Area"/> 
Role Name as displayed on reports	<input type="text" value="Employee"/>

Specify the title of the role here

Who do the users of this role report to?

The title that should be used for this role for reporting

Role Hierarchies on Force.com platform

Creating the Role Hierarchy

You can build on the existing role hierarchy shown on this page. To insert a new role, click **Add Role**.

Your Organization's Role Hierarchy

[Collapse All](#) [Expand All](#)



Figure: Implementing role hierarchy for Company X

Assigning users to roles

You can assign existing users on the Force.com platform to this newly defined role

You can create new users and assign them to this newly defined role

Role
Employee

Below is the list of users assigned to this role. Click Edit to modify the role name. Click Assign Users to Role to assign existing users to this role. Click New User to create a new user for this role.


Hierarchy: [Gmail](#) » [CEO](#) » [Human Resource Manager](#) » [Human Resource Staff](#) » [Head of Area](#) » [Employee](#)

[Users in Employee Role \(0\)](#)

Role Detail

EditDelete

Label	Employee	Role Name	Employee
This role reports to	Head of Area	Role Name as displayed on reports	Employee
Modified By	Farookh Hussain , 2/04/2012 5:22 PM	Sharing Groups	Role, Role and Subordinates
Customer Portal Role	<input type="checkbox"/>		

 **Users in Employee Role**

Assign Users to RoleNew User

[Users in Employee Role](#)

Assigning users to roles

Roles

Human Resource Staff

The users shown in the **Selected Users** list are currently assigned to the role **Human Resource Staff**

To assign other users to this role:

- Make a selection from the drop-down list to show available users.
- Choose a user on the left and add them to the **Selected Users** list.

Removing a user from the **Selected Users** list deletes the role assignment for that user.

Save Cancel

Available Users

All Users

Farookh Hussain

Selected Users for Human Resource Staff

--None--

Add

Remove

Gmail

CEO

Human Resource Manager

Human Resource Staff

Head of Area

Employee

Step 1: Select the existing user from the Force.com platform that you wish to assign to this role

Step 2: Add the selected users that you wish to add to this role

Step 3: You may wish to remove some existing users from this role

Step 4: Save the users assigned or deleted from this role

Implementing the role hierarchy

System Overview **New!**

Personal Setup

▶ My Personal Information

▶ Email

▶ Import

▶ Desktop Integration

▶ My Chatter Settings

▶ My Social Accounts and Contacts **New!**

App Setup

▶ Customize

▶ Create

▶ Develop

▶ Deploy

Schema Builder

Installed Packages

AppExchange Marketplace

Critical Updates

Administration Setup

▶ Manage Users

▶ Company Profile

■ Security Controls

Sharing Settings

Field Accessibility

Password Policies

Session Settings

SaveCancel

Object	Default Access	Grant Access Using Hierarchies
Lead	Public Read/Write/Transfer	<input checked="" type="checkbox"/>
Account, Contract and Asset	Public Read/Write	<input checked="" type="checkbox"/>
Contact	Controlled by Parent	<input checked="" type="checkbox"/>
Opportunity	Public Read/Write	<input checked="" type="checkbox"/>
Case	Public Read/Write/Transfer	<input checked="" type="checkbox"/>
Campaign	Public Full Access	<input checked="" type="checkbox"/>
Activity	Private	<input checked="" type="checkbox"/>
Calendar	Hide Details and Add Events	<input checked="" type="checkbox"/>
Price Book	Use	<input checked="" type="checkbox"/>
Candidate	Private	<input type="checkbox"/>
Customer	Public Read/Write	<input type="checkbox"/>
Customer Record	Public Read/Write	<input type="checkbox"/>
Employee	Public Read/Write	<input checked="" type="checkbox"/>
Employment Website	Public Read Only	<input type="checkbox"/>
Job Application	Private	<input type="checkbox"/>
Position	Public Read Only	<input checked="" type="checkbox"/>

SaveCancel

Check “grant access using hierarchies” for relevant objects

Sharing Rules

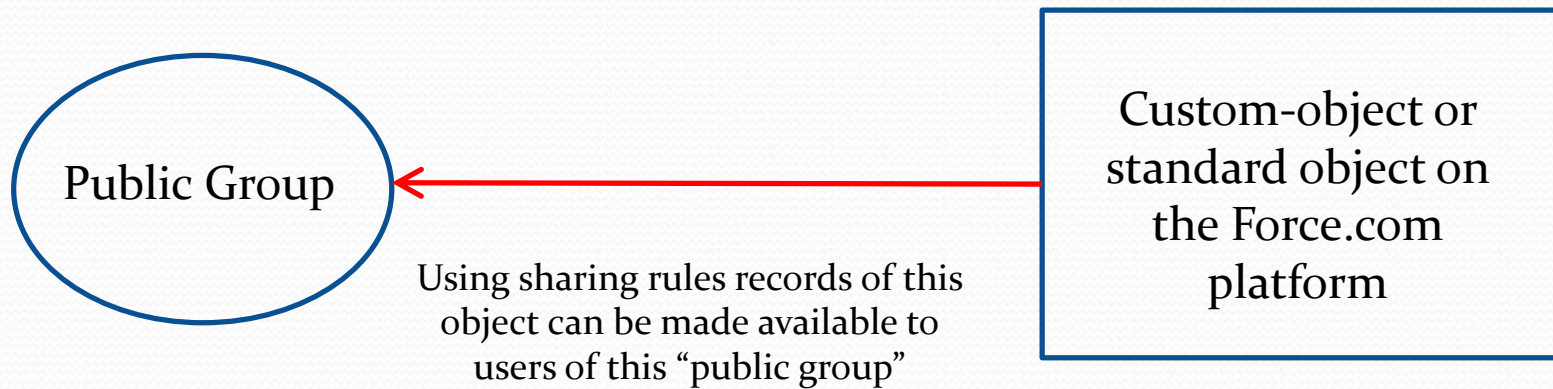
- Sharing rules allow the application owner to make automatic exceptions to organization-wide defaults for particular groups of users
- Using the sharing rules, we can make up additional groups (termed as “*public groups*”)
- **Important**: Sharing rules can be used to open up record access to more users than that specified by the organization-wide default. Sharing rules cannot be more stricter than the organization-wide defaults.

Sharing Rules

- A public group is defined as:
 - a) a collection of individual users;
 - b) a collection of roles, and/or roles with their subordinates;
 - c) any collection of (a) or (b), above that need access to a certain set of records

Sharing Rules

- Sharing rules:
 - Are always specified against the records of a given object
 - Specified for a public group



Defining a public group on the Force.com platform

- In order to specify Sharing Rules on the Force.com platform click, we first need to define a public group. To define a public group select the following:
- Setup → Administer → Manage Users → Public Groups

Group Membership
New Group

Group Information Save Cancel

New Public Group

Label

Group Name i

Grant Access Using Hierarchies ☒ i

Search: Public Groups ▼ for: Find

Available Public Groups Selected Members

Group: Roles None--

Roles and Subordinates

Users

Add

Step 1: Specify the name of the public group

Step 2: Public groups can be defined as any combination of

- (a) Roles
- (b) Users
- (c) Existing Public Groups
- (d) Roles and their subordinates

Specifying sharing rules

- Sharing rules can only be specified against records of a given object(s)
- To specify a sharing rule
 - Setup → Administer → Security Controls → Sharing Settings
 - Select the object on which the sharing rule is to be defined

Specifying sharing rules (Step 1 and Step 2)

Setup

Employee Sharing Rule

Use sharing rules to make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: "Roles and subordinates" includes all users in a role, and the roles below that role.

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

Step 1: Specify the name of the sharing rule

Step 1: Rule Name

Label

Rule Name

Step 2: Select your rule type

Rule Type

☒ Based on record owner ☐ Based on criteria

Step 3: Select which records to share

Employee: owned by members of

Step 4: Select the users to share these records with

Share with

Step 5: Select the level of access for the users

Access Level

Save

Cancel

Step 2: You may choose to permit access to the members of this public group based on

- (a) The owner of the record
- (b) Certain pre-defined criteria

Specifying sharing rules (Step 3)

Setup

Employee Sharing Rule

Use sharing rules to make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: "Roles and subordinates" includes all users in a role, and the roles below that role.

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

Step 3: You may choose to permit access to the members of this public group to selected records of this object, which match the specified criteria

Step 1: Rule Name

Label

Rule Name

i

Step 2: Select your rule type

Rule Type

☐ Based on record owner

☒ Based on criteria

Step 3: Select which records to share

Criteria	Field	Operator	Value	
	Name	--None--		AND
	--None--	--None--		AND
	Created By ID	--None--		AND
	Date of Birth	--None--		AND
	Email Address	--None--		AND
	Employee Name	--None--		AND
	Extension Number	--None--		
	Last Modified By ID	--None--		
	Name			
	Owner ID			
	Qualification			
	Salary			
	Tax File Number			

Step 4: Select the users to share with

Specifying sharing rules (Step 3)

Setup

Employee Sharing Rule

Use sharing rules to make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: "Roles and subordinates" includes all users in a role, and the roles below that role.

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

Step 3: You may choose to permit access to the members of this public group to selected records of this object depending on the ownership of the records

Step 1: Rule Name

Label

Rule Name

i

Step 2: Select your rule type

Rule Type

☒ Based on record owner ☐ Based on criteria

Step 3: Select which records to share

Employee: owned by members of

Roles

Public Groups

Roles

Roles and Subordinates

-- -- Select One -- --

Step 4: Select the users to

Share with

Public Groups

-- -- Select One -- --

Step 5: Select the level of access for the users

Access Level

Read Only

Save

Cancel

Specifying sharing rules (Step 4)

Setup

Employee Sharing Rule

Use sharing rules to make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: "Roles and subordinates" includes all users in a role, and the roles below that role.

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

Step 4: Specify the name of the public group who should have access to the records

Step 1: Rule Name

Label

Rule Name

i

Step 2: Select your rule type

Rule Type

☒ Based on record owner ☐ Based on criteria

Step 3: Select which records to share

Employee: owned by members of

Public Groups

-- -- Select One -- --

Step 4: Select the users to share these records with

Share with

Public Groups

All Internal Users
-- -- Select One -- --
All Internal Users
Executive Group
Reviewers

Step 5: Select the level of access for the users

Access Level

Read Only

Save

Cancel

Specifying sharing rules (Step 5)

Setup

Employee Sharing Rule

Use sharing rules to make automatic exceptions to your organization-wide sharing settings for defined sets of users.

Note: "Roles and subordinates" includes all users in a role, and the roles below that role.

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

Step 5: Specify the level of access to the records.

Step 1: Rule Name

Label

Rule Name



Step 2: Select your rule type

Rule Type

☒ Based on record owner ☐ Based on criteria

Step 3: Select which records to share

Employee: owned by members of



Step 4: Select the users to share these records with

Share with



Step 5: Select the level of access for the users

Access Level

Read Only

Read Only

Read/Write

Save

Cancel

Manual Sharing Rules


- Manual Sharing rules
 - Allow the application designer to share an individual record of an object; (and)
 - Are very helpful when it is very hard or impossible to define a consistent group of users who would need access to a particular set of records.
 - **Example:**
 - Interviewers in Company X need access to the complete information of the persons applying for a given job;
 - Any person in Company X may be asked to perform an interview;
 - The persons carrying out an interview for a given candidate (say candidate A), might not necessarily be the same as that for another candidate;
 - In such cases we make use of manual sharing rules to allow selected user access to a given record;

Specifying Manual Sharing Rules

- Manual Sharing rules
 - Are always specified against a single record
 - Specified for given user(s) only.
- To specify a manual sharing rule, select the record on which the manual sharing rule is to be defined

Specifying Manual Sharing Rules (Step 1 and Step 2)

Step 1: Select the record that you wish to share


 **Position**
CEO

[« Back to List: Profiles](#)

[Open Activities \[0\]](#) | [Activity History \[0\]](#) | [Notes & Attachments \[0\]](#) | [Job Applications \[1\]](#) | [Employment Websites \[0\]](#)

Position Detail

[Edit](#) [Delete](#) [Clone](#) [Sharing](#)

Position Title	CEO	Owner	 Farookh Hussain [Change]
Status	Open-Approved	Location	
Type	Full Time	Open Date	
Functional Area	Human Resource	Close Date	
Job Level	HR-200	Hire By	28/04/2012
Travel Required	<input checked="" type="checkbox"/>	Created By	Farookh Hussain , 29/01/2012 6:30 PM
Hiring Manager	Farookh Hussain		

▼ **Compensation**

Min Pay	\$400.00	Max Pay	\$40,000.00
----------------	----------	----------------	-------------

▼ **Job Description**

Job Description	All that the CEO requires
Responsibilities	All that the CEO requires
Skills Required	All that the CEO requires
Educational Requirements	All that the CEO requires

▼ **Required Languages**

Step 2: Select “Sharing” to specify the manual sharing rule

Specifying Manual Sharing Rules (Step 3)



[Help for this Page](#)

This page lists the users, groups, roles, and territories that have sharing access to **CEO**. Click **Expand List** to view all users who have access to it.

View: [Edit](#) | [Create New View](#)

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other **All**

User and Group Sharing

Add

Expand List

[User and Group Sharing Help](#)


Action	Type	Name ↑	Access Level	Reason
	User	Farookh Hussain	Full Access	Owner

Explanation of Access Levels

- Full Access - User can view, edit, delete, and transfer the record. User can also extend sharing access to other users.
- Read/Write - User can view and edit the record, and add associated records, notes, and attachments to it.
- Read Only - User can view the record, and add associated records to it. They cannot edit the record or add notes or attachments.
- Private - User cannot access the record in any way.

Step 3: Select “Add” to specify manual sharing rule

Specifying Manual Sharing Rules (Step 4)

 **New Sharing**

Position: Specify the sharing for this record. You can share this record and its related data with ind users in a particular role plus all of the users in roles below that role.

Individual sharing can only be used to grant wider access to data, not to restrict access.

New Sharing Save Cancel

Sharing Information

Search: Users for: Find

User: Public Groups
Roles
Roles and Subordinates
Users

Share With --None--

Add
Remove

Access Level Read/Write

Step 4: Select the user(s), roles, or public groups with whom you wish to share the record.

Specifying Manual Sharing Rules (Step 5 and Step 6)



CEO New Sharing

Position: Specify the sharing for this record. You can share this record and its related data with users in a particular role plus all of the users in roles below that role.

Individual sharing can only be used to grant wider access to data, not to restrict access.

New Sharing

Save

Cancel

Sharing Information

Search: for:

Available

All Internal Users
Group: Reviewers

Share With

Group: Executive Group

Add



Remove



Access Level

Read/Write



Save

Cancel

Step 5(a): You may add the users, roles or public groups who should have access to this record.

Step 5(b): You may remove the existing users, roles or public groups who have access to this record.

Step 6: Specify the level of access that these users should have on this record.

Summary

- Need for securing cloud objects
- Profiles
- Object-level access control
- Field-level access control
- Record-level access control
 - Organization-Wide Default
 - Role Hierarchies
 - Sharing Rules
 - Manual Sharing Rules



Reading

Books

1. McGuire, C., Roth, C., Carroll, D., and Tran, N. (2013), Force.com Fundamentals: An Introduction – Chapter 7