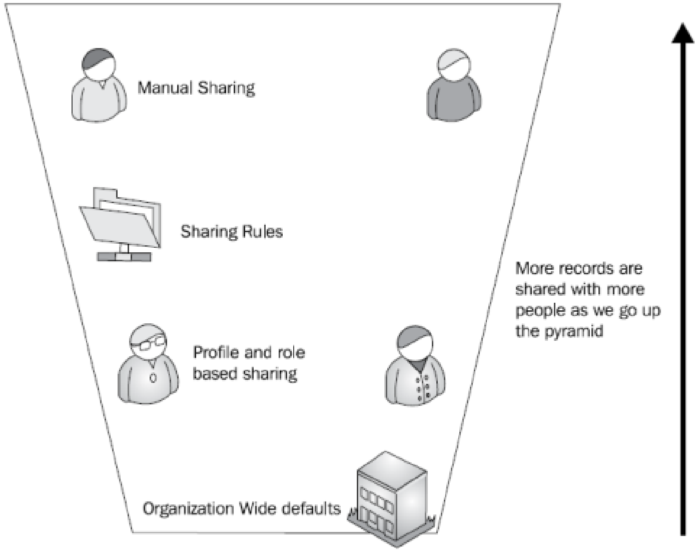
Introduction to Salesforce Security Pyramid

SOUVIK ♦ SEPTEMBER 21, 2013 ♦ 1 COMMENT

Let us introduce Salesforce Security features in a small way. Security features ensures us to understand what users **CANNOT** see in an application, instead of what users can see.

The heart of the security features comes within the security pyramid which includes Organisation Wide Default, Profiles, Roles and Sharing. We will discuss it one by one.

Let us first see the pyramid below:-


Manual Sharing
Sharing Rules
Profile and role based sharing
Organization Wide defaults
More records are shared with more people as we go up the pyramid

OWD

As we can see in this pyramid, as it goes up number of users getting access increases. This shows that Organisation Wide Default which is at the bottom of the pyramid is most restrictive and restriction decreases as we move up. Let us discuss them in detail.

Organisation Wide Default(OWD) :-

The organization wide default determines the distribution of data with the user. We use the defaults in the object to determine which people across the role hierarchy can access which objects.

Most restrictive record access is defined using a organization-wide default. If an object is accessible in OWD, it can not be restricted using roles,sharing or manual sharing, but if an object is restricted in OWD it can be extended to access by roles,sharing and manual sharing.

We can give three types of access in OWD:

1) Private – The role hierarchy is observed and people cannot view their peer records(same level or upper level heirarchy).
2) Public Read Only – Everyone in the organisation can view each others data irrespective of role hierarchy.
3) Public Read/ Write – Everyone in the organisation can view/edit each others data irrespective of role hierarchy.

Important points to be noted about OWD:-

1) We have to first find out the user with the most restrictive access for a particular object, then that access of the user will be set as default in the Organization Wide Default for that object.
2) Changing organization-wide default settings can delete manual sharing if that sharing is no longer needed.
3) Through OWD we can get the most restrictive data access.

#**Note**: When an user profile doesn't have the visible permission for a particular object then that user doesn't have the permission to view that object records even if it can be accessible through OWD. Similarly even if OWD has read/write permission and profile has read only permission then that object records will be read only for the user.

Profiles :
When we create an user, we can assign a profile to him. There are two types of profiles.

a) **Standard Profiles** – There are some standard profiles by default. They are very little customizable.
b) **Custom Profiles** – We can create custom profiles by cloning a stamdard profile or an existing custom profile.

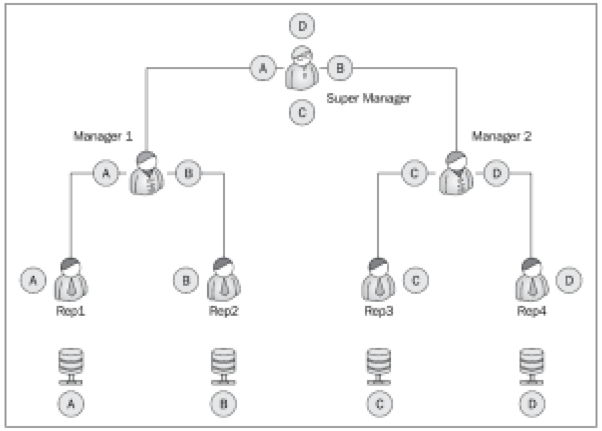
#**Note:** We can create custom profiles only in **Developer,Unlimited and Enterprise** account.

A profile contains information on what the user should see and the things he can do with the data. Let us first see what are the things that are possible through profiles.

1) Mention the applications the user can see
2) Mention the tabs the user can see
3) What are the Default Page Layouts and Default Record Types available for the user. We can enable Record Types through profiles but can't modify it.
4) Mention the objects that the user can access and the different access permissions on the object i.e Create,Read,Update,Delete also called CRUD Permissions.
5) Fields can be enabled or restricted for the profile
6) Mention the Apex Controllers and Visualforce Pages that the user can access
7) The profile also determines the hours in which the user logs in as well as the IP restriction.

Role Hierarchy :-

While profiles determine what objects can be seen by which users, roles determine which records from the object can be seen by the user.



Role Hierarchy

As shown in the above screenshot A, B, C, and D are records of the same objects owned by Rep1, Rep2, Rep3, and Rep4 respectively. Rep1 cannot see Rep2,Rep3 and Rep4 owned records and same for others. However Manager1 can see data of Rep1 and Rep2 as they are below him in the role hierarchy. Super Manager is at the top of the hierarchy and he can see all data.

So it concludes from role hierarchy that we can not see peers data and data of users above in the hierarchy. Whereas managers can access data of the users those are below them in the role hierarchy.

Sharing Rules :-

Sharing rules and settings extend the data access to users in public groups. It actually extends the access which is restricted through OWD,profiles and roles. There is a limit of 100 owner-based sharing rules.

#Note: If the object is not visible to the user profile, the records cannot be made visible by sharing rules.

We can mention the following things while creating a sharing rule:
1) Rule Type :-
a) Based On Record Owner – It describes the sharing rule on the basis of the record owner.
b) Based On Criteria – We can give criteria while setting the sharing rule i.e when field "X" equals to 'Approved' and so on.
2) Select the users to share the records – We can select the users through public groups, roles, roles and subordinates to share the records.
3) Access Level – We can set the access level(Read-Only or Read/Write) for the sharing.

Manual Sharing :-

Manual Sharing is used if the organization wide defaults access for the object is set to Private or Public read only. This is generally done by a record owner, for a single record, however Users with the Modify All object-level permission for the given object or the Modify All Data permission can also manually share a record.
Manual sharing can be removed becuase of the following reasons:
a) Changing organization-wide default settings can remove manual sharing
b) When the record owner changes, manual sharing can be removed
c) When the access granted in the sharing does not grant additional access beyond the object's organization-wide sharing default access level, then also manual sharing is deleted.