

Salesforce Sharing and Security Cheat Sheet

Sudipta Deb Thursday, January 03, 2019



"Sharing is Caring", right?? That's the attitude I like most about Salesforce Ohana. As I am preparing myself for Sharing and Visibility Designer Architect certification, I thought of sharing some of my study notes regarding Salesforce Sharing and Security.

Security is the main pillar of Salesforce eco system and it is complex. It will give you fine-grained control over data access. So it requires a very good understanding of the concepts to implement in correctly.

I will suggest everyone to go through these below articles to understand it clearly.

[A Guide to Sharing Architecture](#)

[An Overview of Force.com Security](#)

[Record-Level Access: Under the Hood](#)

I am not going to write everything what is written in these documents, rather I would like to provide a concise, sharp cheat sheet which you can refer anytime. So let's start -

Sharing Metadata Objects/Records:

For standard object -> "Object[Share]"

For custom object -> "Object__[Share]"

Contains three types of sharing -> **managed sharing**, **User managed sharing** and **Apex managed sharing**

Fields present in the share object - **access level, record ID, user** or **group ID**

Share records are not created for OWDs, role hierarchies, or the "View All"/"Modify All"/"View All Data"/"Modify All Data" permissions.

If the owner of the record changes, sharing record with reason "Manual" will also be deleted.

Implicit Sharing:

This is applicable only for Accounts, Contacts, Cases and Opportunities.

Access to parent record - If you have access to one of the child record, you will have **Read Only** access to the parent record.

Access to child record - If you have access to parent record, you will have access to all child records(Contacts, Cases and Opportunities).

Organization Wide Defaults (OWD):

Grant access using hierarchies is enabled by default for standard objects (You cannot disable the same). For custom objects, you can enable/disable this property.

Can't be changed for contacts if person accounts are enabled.

Master Detail:

Access is controlled by parent record.

Child record will not have any share record of their own.

It is not possible to write sharing rule for child object.

Only parents in the M:D relationship will have the owner.

If the detail object is having more than one master record, then first M:D created will become the **primary relationship**.

Lookup:

Child object can have their own sharing access level and ownership.

Manual Sharing:

Removed when owner changes.

Removed when OWD becomes at least as permissive as share.

Private contacts (without Accounts) cannot be manually shared.

Apex Managed Sharing:

Using Apex code to share the record.

Requires "Modify All" permission.

Ownership-based Sharing Rules:

When you want to share records owned by user, group, queue or role with another user, group, queue or role (including portal users with role).

Criteria-based Sharing Rules:

When you want to share records based on values of a specific field or fields with another user, group, queue or role (including portal users with role).

Manual Sharing Rules:

When the record owner or someone with "Modify All" permission wants to share individual record with another user, group, queue or role (including portal users with role).

Share Group:

You want to share records owned by HVP users with internal users, groups or roles (includes portals users with roles)

Sharing Sets:

You want to share records with HVP users. Records should fulfill the below criteria:

Object's OWD is different than Public Read/Write.

Object is available for Customer Portal.

Custom object is having a lookup field to account or contact.

Portal - High Volume Portals (Service Cloud Portals):

Include High Volume Customer Portal and Authenticated Website profiles.

They have no roles and can't participate in "regular" sharing rules.

You can share their data with internal users through Share Groups.

You can share object records where the object is a child record of the HVP user's contact or account. This is done with Sharing Sets.

They can also access records that are:

Available for portals

Public R/W OWD or

Private OWD and They own the record.

They can access a record if they have access to that record's parent and the OWD is set to "Controlled by parent".

Cases cannot be transferred from non-HVP to HVP users

Large Data Volumes:

Defer sharing settings (enabled by logging a case) and group calculation on large data loads and modifications.

If there is anything you think I should put in this list, please mention the same in comment. I will be more than happy to put the same here.