**Role based Security**

**Role based Security**

Users and Teams are assigned security roles in Microsoft Dynamics CRM which define their privileges and access level, or in other words it defines what user/team is authorized to perform in CRM.

Role based Security has two components

1. Privileges
2. Access Level

**Privileges**

Microsoft Dynamics CRM platform validates the user request to perform a specific operation against the privileges (defined in security role) assigned to a user and accepts/rejects based on it.

Common privileges available per entity are

* Create - Ability to create entity records.
* Read - Ability to read entity records.
* Write - Ability to modify entity records.
* Delete - Ability to delete entity records.
* Append - Ability to associate a selected entity record to another entity record.
* Append To - Ability to associate another entity record to this entity record.
* Assign - Give ownership of entity record to another user/team.
* Share - Give access to entity records to other user/team.

**Access Level**

Access Level uses the ownership of the object to determine if a user can apply privileges on a specific object.  
  
Microsoft has classified Access Levels as

* None
* User/Team
* Business Unit
* Parent: Child Business Units
* Organization

In short

* **Privileges determine "WHAT" a user can perform on an object.**
* **Access Level determines on "WHICH" object a user can perform this action.**

|  |  |
| --- | --- |
| Access level global | **Global**. This access level gives a user access to all records within the organization, regardless of the business unit hierarchical level to which the instance or the user belongs. Users who have Global access automatically have Deep, Local, and Basic access, also.  Because this access level gives access to information throughout the organization, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the organization.  The application refers to this access level as **Organization.** |
| Access level deep | **Deep**. This access level gives a user access to records in the user's business unit and all business units subordinate to the user's business unit.  Users who have Deep access automatically have Local and Basic access, also.  Because this access level gives access to information throughout the business unit and subordinate business units, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the business units.  The application refers to this access level as **Parent: Child Business Units**. |
| Access level local | **Local**. This access level gives a user access to records in the user's business unit.  Users who have Local access automatically have Basic access, also.  Because this access level gives access to information throughout the business unit, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the business unit.  The application refers to this access level as **Business Unit**. |
| Access level basic | **Basic**.  This access level gives a user access to records he or she owns, objects that are shared with the user, and objects that are shared with a team of which the user is a member.  This is the typical level of access for sales and service representatives.  The application refers to this access level as **User**. |
| Access level none | **None**. No access is allowed. |