Planning Security

Microsoft Dynamics CRM can be configured to meet the organization's security requirements. It provides a framework to reflect the security profile of the company. Planning and architecting a security design is essential to accomplish the following:

- Protect information from being mis-handled by users who lack understanding
- Protect private knowledge from getting into the wrong hands
- Ensure that users have the power to take actions commensurate with their profile

The first step in architecting Microsoft Dynamics CRM security is creating a map of the organization structure. This structure can be helpful in the creation of business units and in assessing the level of authority that should be assigned to an individual or team. However, it has to be noted that the construction of the business unit's structure does not necessarily have to follow the organizational hierarchy.

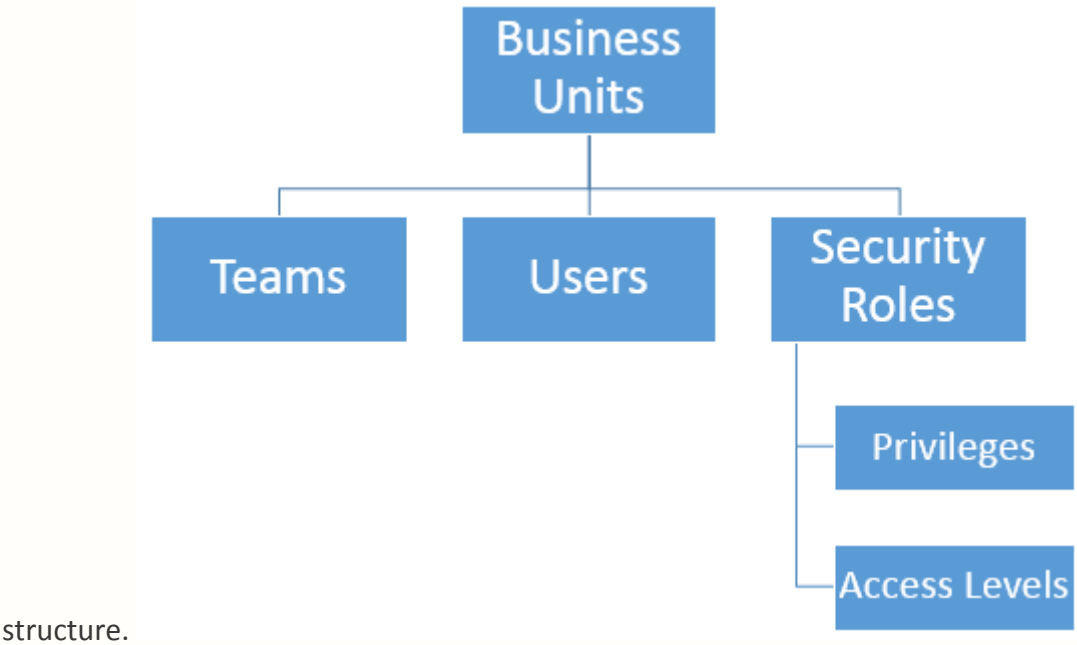
To learn more, explore the following:

- Business units
- Security roles
- Users
- Teams
- Field security profiles

Business Units

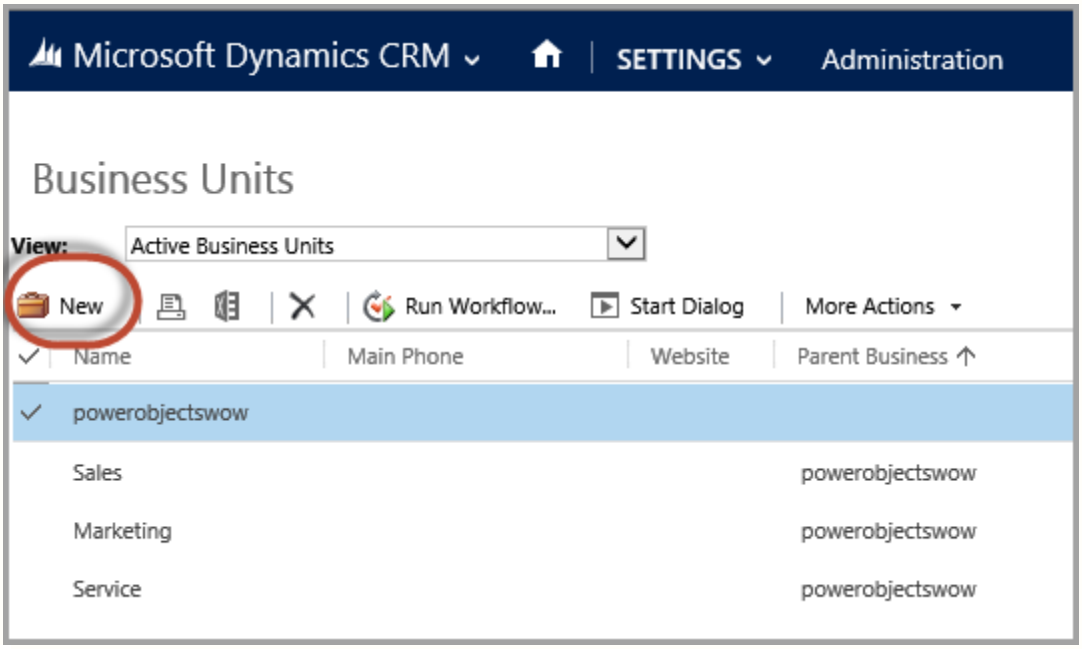
Business units are the foundation of the security structure in Microsoft Dynamics CRM. Each user in the CRM has to be part of a business unit. There is a default business unit that is created when CRM is installed. This is called the root business unit, and it cannot be deleted or disabled–only renamed. More business units can be created if different levels of access to information is required for different groups within the organization. **Root business unit**: There must be at least one business unit in CRM and only one root business unit. The root business unit is the top most point of the CRM organizational hierarchy and all other business units are its children. The root business unit is usually the corporation or the holding company and the child units are subsidiaries, divisions or departments of the business. This is the only unit that

cannot be deleted or disabled as it forms the root of the



structure.

How to Create a Microsoft Dynamics CRM Business Unit



1. On the **Navigation Bar**, select **Microsoft Dynamics CRM**, then select **Settings**, then**Administration**, then **Business Units**.
2. On the list toolbar, click **New**.
3. This will open the business unit form. Enter the information for the new business unit to be created ensuring the required fields are filled in. Save.
4. Click the record types under **Organization** to see a list of related records. The teams list will show a default team.

5. Save and close.

Dynamics CRM business units can also be reorganized, disabled and deleted. While deleting a business unit, any child Business Units, Users or Teams must be removed either by deleting or reassigning them. It is better to disable a business unit rather than delete it because once deleted it cannot be undone.

Security Roles

Security roles in Microsoft Dynamics CRM are a matrix of privileges and access levels for the various entities. They are grouped under different tabs based on their functionality. These groups include: Core Records, Marketing, Sales, Service, Business Management, Service Management, Customization and Custom Entities.

Privileges

Privileges are the basic security units that delineate what action a user can perform on the CRM system. These cannot be added or deleted but only modified. The common privileges in Microsoft Dynamics CRM for each entity are as follows:

- Create — Allows the user to add a new record
- Read — Allows the user to view a record
- Write — Allows the user to edit a record
- Delete — Allows the user to delete a record

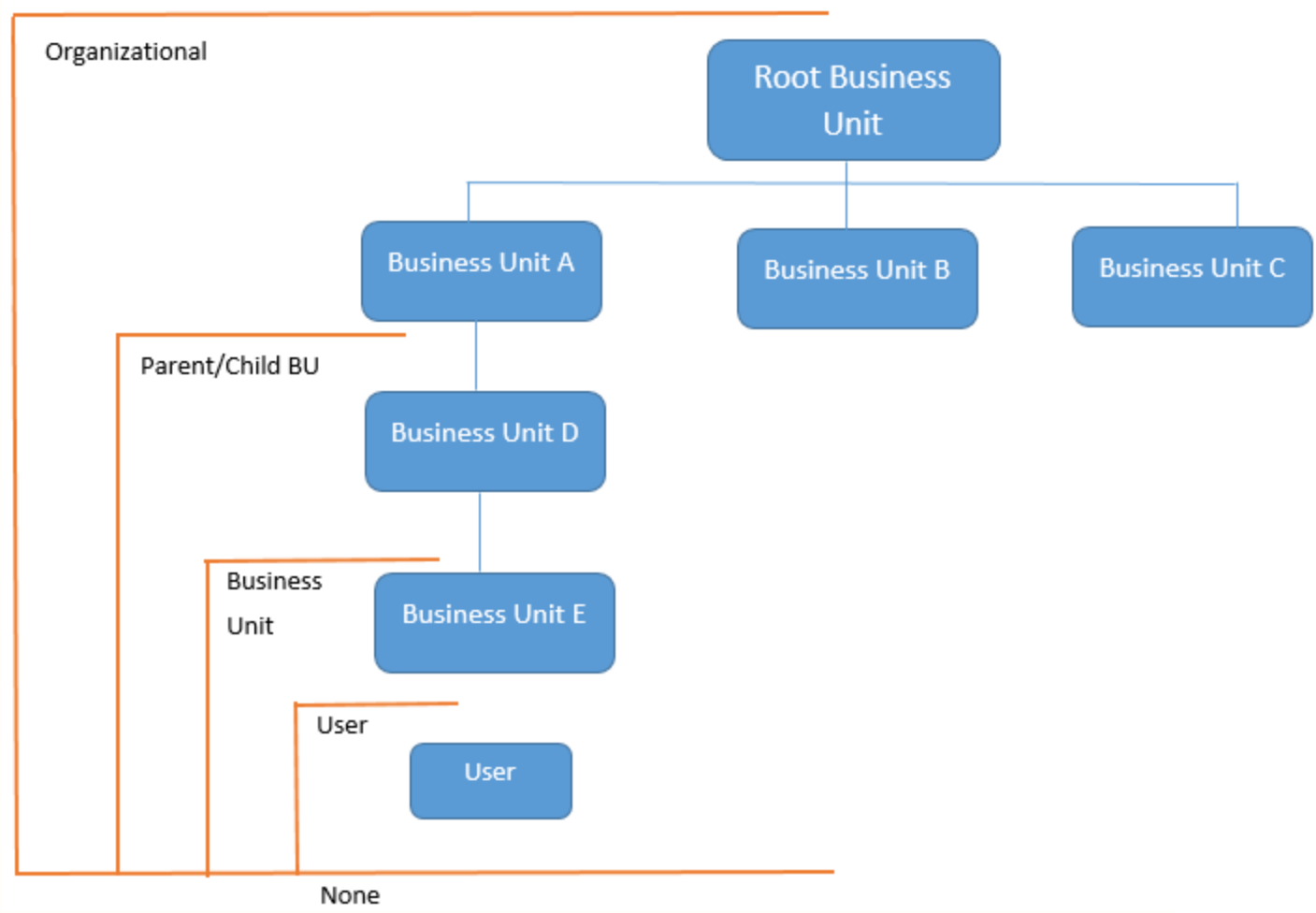
- Append — Allows the user to attach other entities to, or associate other entities with a parent record
- Append to — Allows the user to attach other entities to, or associate other entities with the record

The bottom level lists miscellaneous privileges such as viewing audit history/summary, bulk delete, publish e-mail templates/reports/articles and so on.

Levels of Access

This is indicated by the degree of fill and color of the little circles against each entity for each privilege. These levels determine the records of an entity upon which the user can perform a given privilege. The 5 levels of access are as follows:

- None — No privileges given
- User — Privileges to the records owned by the user or shared with the user. Also includes the privileges owned by the team to which the user belongs.
- Business Unit — Privileges for all records owned in the business unit to which the user belongs
- Parent: Child Business Unit — Privileges for all records owned in the business unit to which the user belongs and to all the child business units subordinate to that business unit
- Organization — Privileges for all records in the organization regardless of who owns it



A security role has a set of privileges and access levels associated with it. There are some pre-defined security roles that can be used.

System Administrator

System Administrator is the highest level role which encompasses all the privileges and has over-riding rights. The System Administrator has the authority to allow and remove access of other users and define the extent of their rights. For example, the System Administrator and the System Customizer are given access to custom entities by default while all other users need to be given access. This is the only role that cannot be edited.

System Customizer

The System Customizer role is similar to the System Administrator role which enables non-system administrators to customize Microsoft Dynamics CRM. A Customizer is a user who customizes entities, attributes and relationships.

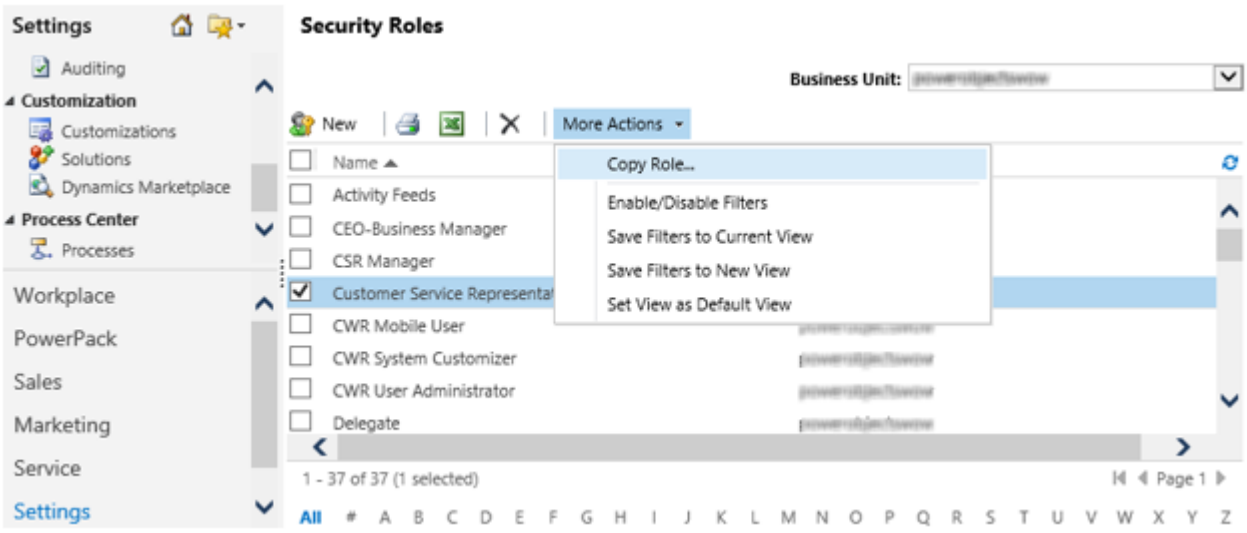
Standard Roles

There are some other built in organizational roles in CRM such as CEO, Marketing Manager, Sales Manager, Salesperson, etc., that can be assigned to a user.

How to Create a Security Role

Usually a base security role is assigned to each user. Additional privileges can be assigned by adding a role with more privileges since the higher authority prevails. If the default security roles are not meeting the organizations' security needs, new roles can be created in one of three ways-

- Modifying a default role
- Creating a new custom role from scratch
- Copying an existing role as a new role



1. On the left navigation pane, click on **Settings**. In the **System** section, click on **Administration** and then **Security Roles**.
2. The Business Unit into which you want to copy the role should be selected in the drop down list.
3. Select the Security Role that you want to copy.
4. On the Actions toolbar click on **More Actions**. In the box that opens click **Copy Role**.
5. A dialog box opens. In the **New Role Name** field type the name of the new role.
6. If you want to change the privileges for the new Security Role, choose the 'Open a new Security Role when copying is complete' check box. Click OK.

Users

Users in Microsoft Dynamics CRM are individuals who have specific logins and passwords and a set of attached privileges at various access levels. Each user can have one or more security roles but each user should belong to at least one security role to be able to access CRM. In case of conflict between two roles the least restrictive role will be upheld. Each user is part of a business unit and can be assigned to only one business unit.
Microsoft Dynamics CRM provides the following functionality for user maintenance:

- Creating Users
- Creating Teams
- Enabling and disabling Users
- Deleting Users
- Assigning Security Roles to Users
- Identifying managers for Users
- Assigning Users to Teams

Creating Users

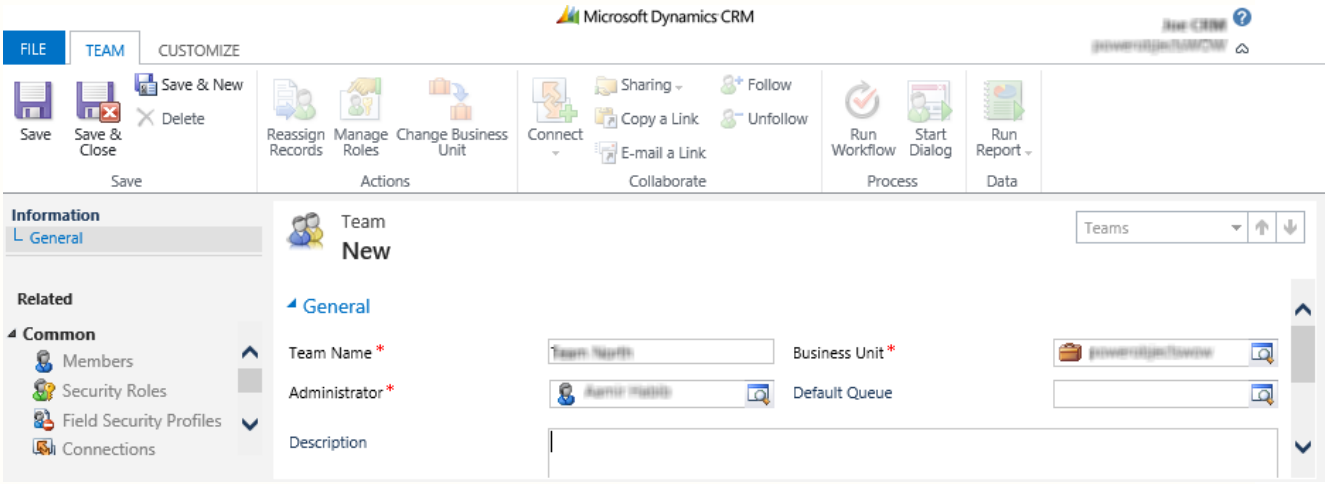
Single users or multiple users can be added. For creating a single user:

1. In the left navigation pane, click on **Settings**. In the **System** section click on **Administration** and then **Users**.
2. On the Ribbon, click **New**.
3. Enter the domain logon name.
4. Choose the relevant business unit for the user from the lookup
5. Select the **E-mail access type**
6. Select the **Access Mode**
7. Select the **License Type**

Teams

Microsoft Dynamics CRM teams are a collection of users who can belong to the same or different business units. Creation of a team facilitates easy sharing and also the ease of applying shared security roles to a group versus individuals. Standard teams are sales teams, regional

teams, etc. A user can belong to multiple teams? A user belonging to a team has all the privileges that the team is entitled to except if the user has been restricted from some of them.

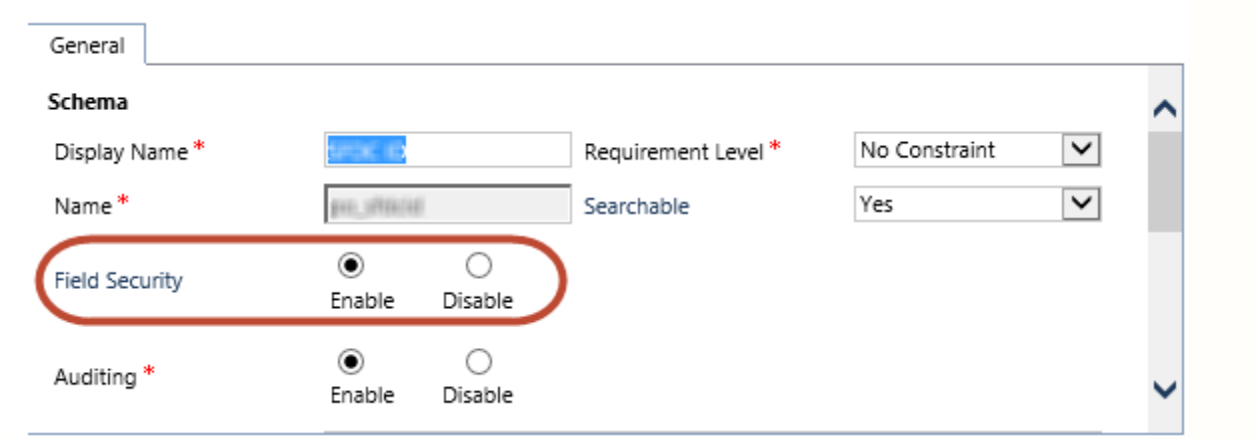


Creating Microsoft Dynamic CRM Teams

1. In the left navigation pane, click on **Settings**. In the **System** section click on **Administration** and then **Team.**
2. Click on **New** in the Ribbon.
3. Enter Team Name and Administrator – the required fields. Select the business unit from the lookup. Save.
4. To add Users to the Team, click on **Members**
   - Add Members in Ribbon
   - Add the **Users** who should belong to the team and click **OK**
5. To add Security Roles, click on **Security Roles**
   - Manage Roles
   - Select the Roles and click **OK**
6. To add Field Security Profiles, click on **Field Security Profiles**
   - Click Add
   - Select profiles and click **OK**

Field Security Profiles

In addition to defining security around users and teams, a more minute level regulation of security can be done around a field. This applies to only custom fields. Field security profile is used to give access to fields that have been enabled for field level security to users other than the default System Administrator. Read, Update and Create privileges to these fields are given. The fields enabled for field level security are seen with a small key beside the name indicating that its status is secure. This security permission can be granted to users or teams.



Creating a new field form

Field with Field Security enabled