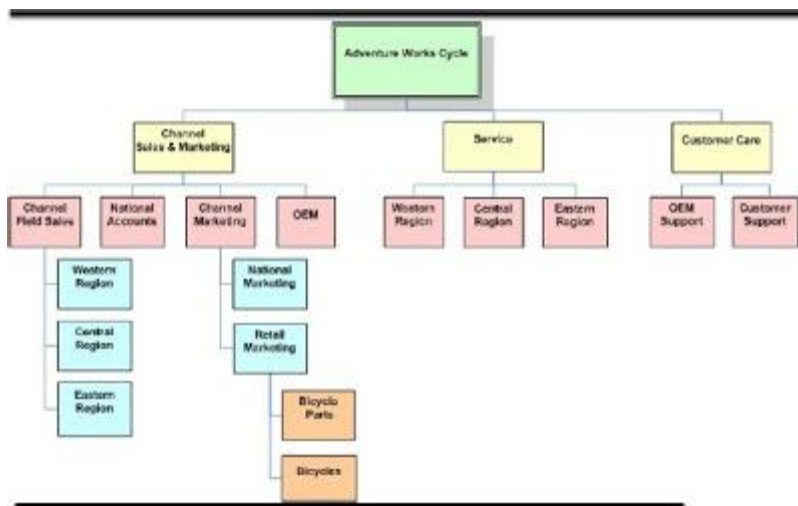


Microsoft Dynamics CRM 2011 Security Model

- Provides users with access only to the information that they require to do their jobs
- Categorizes types of users by role and restrict access based on those roles.
- Prevents users from accessing objects that they do not own or share.
- Supports data sharing by providing the ability to grant users with access to objects that they do not own to participate in a specified collaborative effort.

Create a rough model of your company's current operational structure. For each section of your organizational layout, you should identify the approximate number of users and the types of business functions those users perform. This rough organizational map to start planning how you want to set up and configure security in your Dynamics CRM deployment.



Each box in the figure represents a business unit. Each business unit can have multiple child business units. Dynamics CRM security only allows to specify one business unit per user. A single business unit for a team, each team can consist of users from one or many business units.

A rough organizational model with information about the different types of users in your system, then translate that information into Dynamics CRM security settings.

Security Model Concepts

The Microsoft Dynamics CRM security model uses two main concepts: Role-based and object-based security and Organizational structure

Organizational Structure

- **Organization (Root Business Unit)** - The organization is the top level of the Dynamics CRM business management hierarchy. Dynamics CRM automatically creates the organization based

on the name that you enter during the software installation. You cannot change or delete this information.

- **Business unit** - A logical grouping of your business operations. Each business unit can act as a parent for one or more child business units.
- **Team** - Teams are a group of users that share and collaborate on records. Team members can belong to different business units.
- **User** - Someone who typically works for the organization and has access to Dynamics CRM. Each user belongs to one (and only one) business unit, and each user is assigned one or more security roles.

Authorization is the right granted to a user (or group of users) to access the system and the data stored on it.

Role-based Security - Roles, Privileges, Access Levels

Object-based Security - Access rights, Create access, Sharing objects, Assigning objects

Role-Based Security

It is a set of access levels and privileges for each of the entities (such as Leads, Accounts, or Cases) in Dynamics CRM. Roles are associated with permissions (privileges and access levels) for the different business objects (entities). Therefore, when a user logs on to the system, Dynamics CRM looks at the user's assigned security roles and uses that information to determine what the software will allow that user to do and see throughout the system. This is known as role-based security.

Privileges define what actions a user can perform on each entity in Dynamics CRM. Privileges are pre-defined in Dynamics CRM and cannot be changed; examples of privileges include Create, Read, Write, and Delete.

Privileges by Entity






Privilege	Description
Create	Create an entity.
Read	View entities.
Write	Make changes to entities for users.
Delete	Remove entities for users.
Append	Permits the user to attach another entity to, or associate another entity with, a parent record. Associate a selected entity to another entity.
Append To	Permits the user to attach other entities to, or associate other entities with, the record. To associate an entity to this entity.
Assign	Give access to entities to another user.
Share	Give access to entities to another user while keeping your own access.
Reparent	Assign a different parent to an entity.
Enable/Disable	Give or take away privileges.

Miscellaneous Privileges

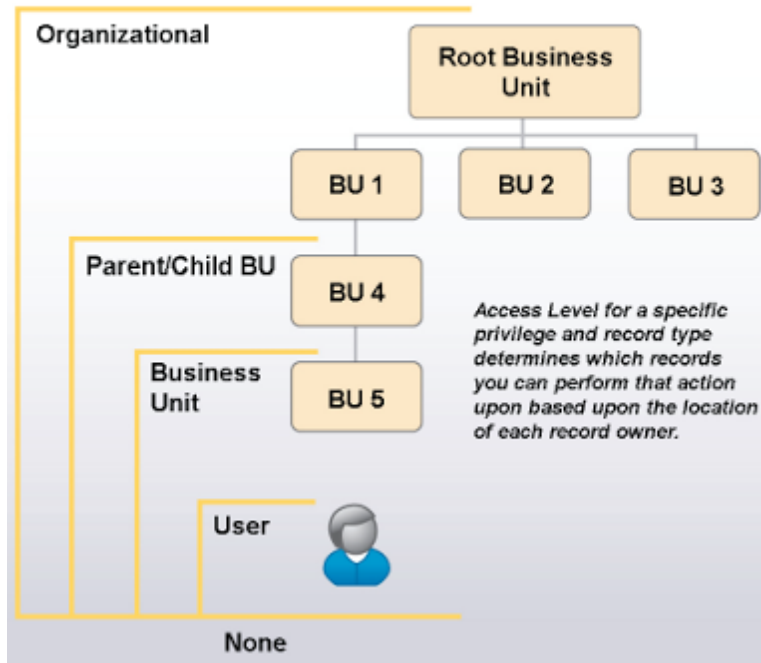
Add Reporting Services Reports (upload RDL), Delete Audit Partitions (audit partitions for each three-month period), Publish Duplicate Detection Rules, Publish Mail Merge Templates to Organization, View Audit History, View Audit Summary, Bulk Delete,...

Access levels

Access levels indicate which records associated with each entity the user can perform actions upon. Although default access levels are assigned to each privilege, the access level can be changed. For example, if a role allows the user to delete accounts, the access level associated with the account delete privilege indicates the specific accounts that the user can delete.

SDK Name	Access Level	Description
 Global	Organization	This global access level lets the user work with all record types within the entire organization, regardless of the business unit hierarchical level to which the entity or user belongs. Users who have Organization access automatically have Parent: Child Business Units, Business Unit, and User access as well.
 Deep	Parent: Child Business Units	This deep access level lets the user work with record types in the user's business unit, and all business units subordinate to the user's business unit. Users with Parent: Child Business Units access automatically have Business Unit and User access as well. For example, if a user has Parent: Child Business Units Read Account privileges, the user can read all accounts in his or her business unit, as well as all accounts in any child business unit of that business unit.
 Local	Business Unit	This middle access level lets the user work with record types in the user's business unit. Users who have Business Unit access automatically have User access as well. For example, if a user has Business Unit Read Account privileges, the user can read all accounts in the local business unit.
 Basic	User	This entry access level lets the user work with record types they own, record types that are shared with the user, and record types that are shared with the team of which the user is a member. For example, if a user is assigned the User Read Account privilege, the only accounts that can be read are those that are owned by or shared to the user.
 None	None Selected	This access level denies the user privileges at any level. A privilege is not added to the security role.

Security: Access Levels



Object-Based Security

Object-based security in Dynamics CRM focuses on how users gain access to individual instances of business objects (entities) and is provided by using access rights. Define different security parameters for the various records (such as Lead, Account, Contact, ...) because each record has an owner.

The relationship between an access right and a privilege is that access rights apply only after privileges have taken effect. For example, if users do not have the privilege to read accounts, they will be unable to read any account, regardless of the access rights another user might grant them to a specific account through sharing.

Access Rights

Right	Enumeration Name	Description
Read	ReadAccess	View an entity instance.
Write	WriteAccess	Make changes to entities for users.
Delete	DeleteAccess	Remove entities for users.
Append	AppendAccess	Associate a selected entity to another entity.
Append To	AppendToAccess	To associate an entity to this entity.
Assign	AssignAccess	Give access to entities to another user.
Share	ShareAccess	Give access to entities to another user while keeping your own access.

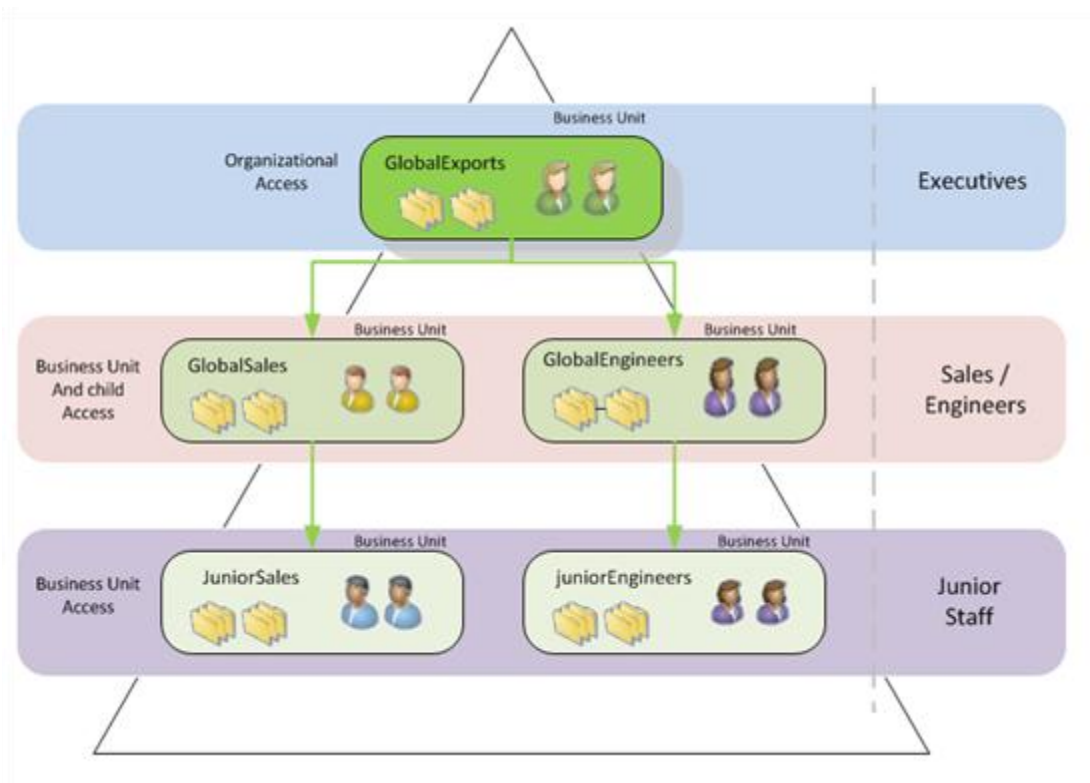
Business Unit Data isolation

I would like to think data isolation as company departments, which work on different floors and have different network drives accessed strictly by that department AD accounts. Business units are great to isolate data, however this approach can be very complex if your company spans multiple countries or multiple offices. The below example, the company Global Exports has 3 levels of security.

On the below diagram the concept is simple; We have 1 Parent business unit GlobalExports and 2 Child business units GlobalSales and GlobalEngineers and each also have a child business unit GlobalSales - > JuniorSales and GlobalEngineers->JuniorEngineers

1. Executives have full access to all data. Executives are placed on the top Business Unit GlobalExports
2. Sales representative are placed on the GlobalSales Business Unit. Only Executives can access sales data, also junior sales staff cannot access GlobalSales representatives data.
3. The same applies to the engineers business unit.

To read the diagram, the green arrows indicate how data-read flows (downwards), you see that no user can go back up and read their parent data.



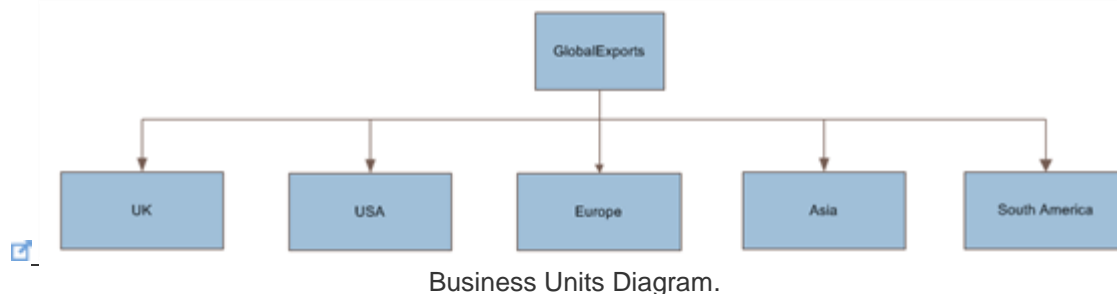
Advantages:

- Junior staff can only access data in their own business unit, they cannot go back and read data on the GlobalSales or GlobalEngineers Business data.
- GlobalSales and GlobalEngineers are separate departments and do not access either data.
- Executives can access all company data, and no child business units can access GlobalExports Business Unit.

Disadvantages:

- If the Executives would like to share data with sales representatives on the GlobalSales Business Unit, the only available process will be Sharing Records with individual users or creating teams and sharing the records with teams, increasing management time and complexity.
- The same applies to sales representatives or engineers wanting to share data with their junior staff, can only share records with individual users or teams.
- Assigning records to users in different business units can move all child records which hold a parental relationship, adding more extra management complexity with entity relationships. e.g. sales representative assigns a record to a junior staff, the record and all child activities (phone calls, emails, tasks) will be also moved and ownership taken by the new owner.

To understand better why sharing records with individual users or teams is a disadvantage and how increases management complexity, the below diagram illustrates the company GlobalExports with a CRM design based on Regions:



From the above diagram we can ask ourselves a few questions:

1. How users would share data between themselves?
2. After sharing records during 1 year what is the sense of levels of access?
3. If you created different Security roles for different users in order for them to be able to read across regions, how many security roles or how many users would be associated with these security roles and how would they be managed?

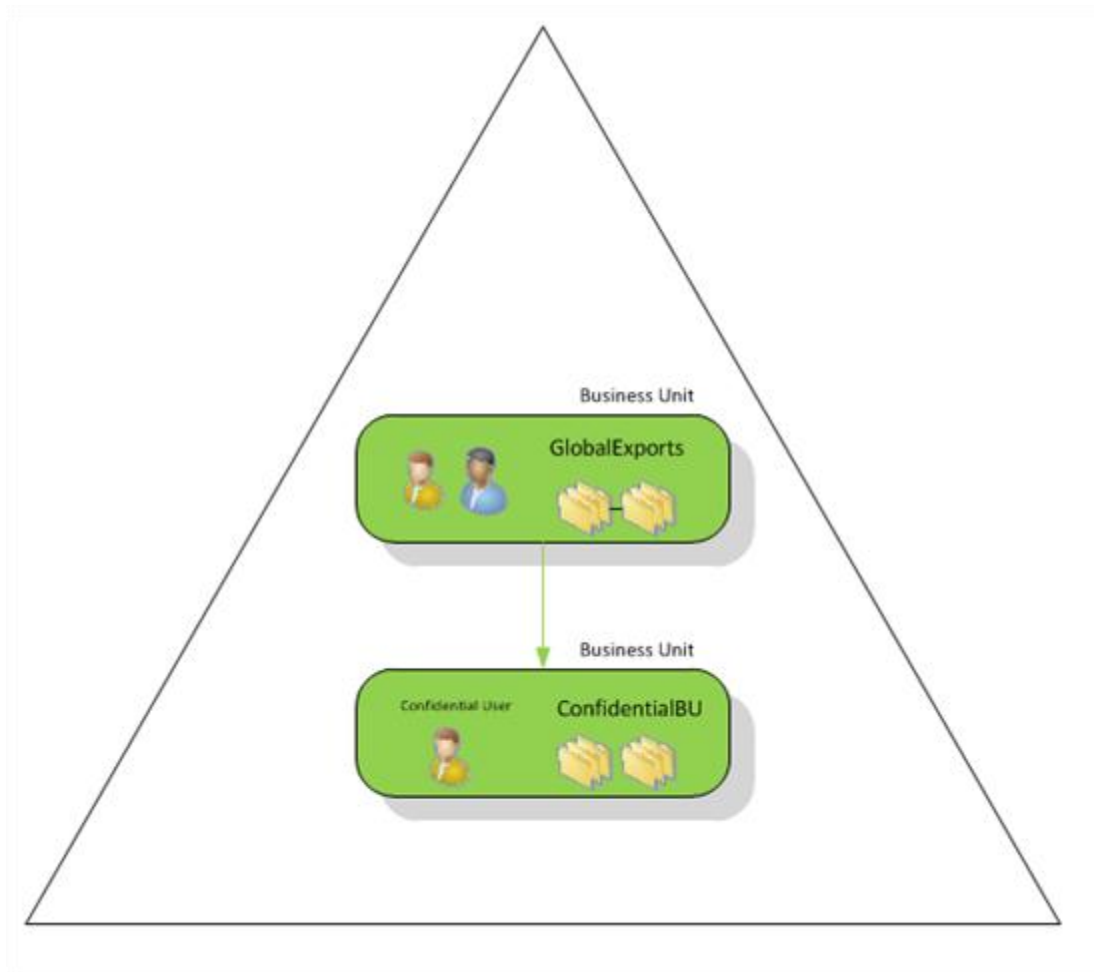
Business Units for data isolation is something that needs carefully planning. Hopefully the above example gives you a good picture of the complexity. However our first example with Junior sales and Junior Engineers are the perfect example how and why we would use Business Units for data isolation.

Confidential records

Business Units are great to isolate data and differentiate departments and keep data secure. A good example about isolating data with Business Units is the implementation of confidential records. Below is a brief description on the design concept:

1. A confidential Business Unit is created under the Parent Business Unit GlobalExports.
2. A user account is created and assigned to that Business unit. (crm.confidential)
3. All users within GlobalExports BU have Business Unit access level.
4. When users would like to make an opportunity confidential they assign the record to the confidential user moving the records automatically to the confidential Business unit, all child records with parental relationships will also move.
5. Because GlobalExports BU users permissions is based on Business Unit access level, no records can be read from the confidential business unit.

6. The way to access data on the confidential Business unit is to share the records between users or teams. This can be accomplished automatically with the CRM free plugin that auto-share records via workflows, so you could tick a box on the form and save, and this would trigger the confidential workflow which would assign the record and auto-share with user triggering the action. <http://crm2011sharestep.codeplex.com/>

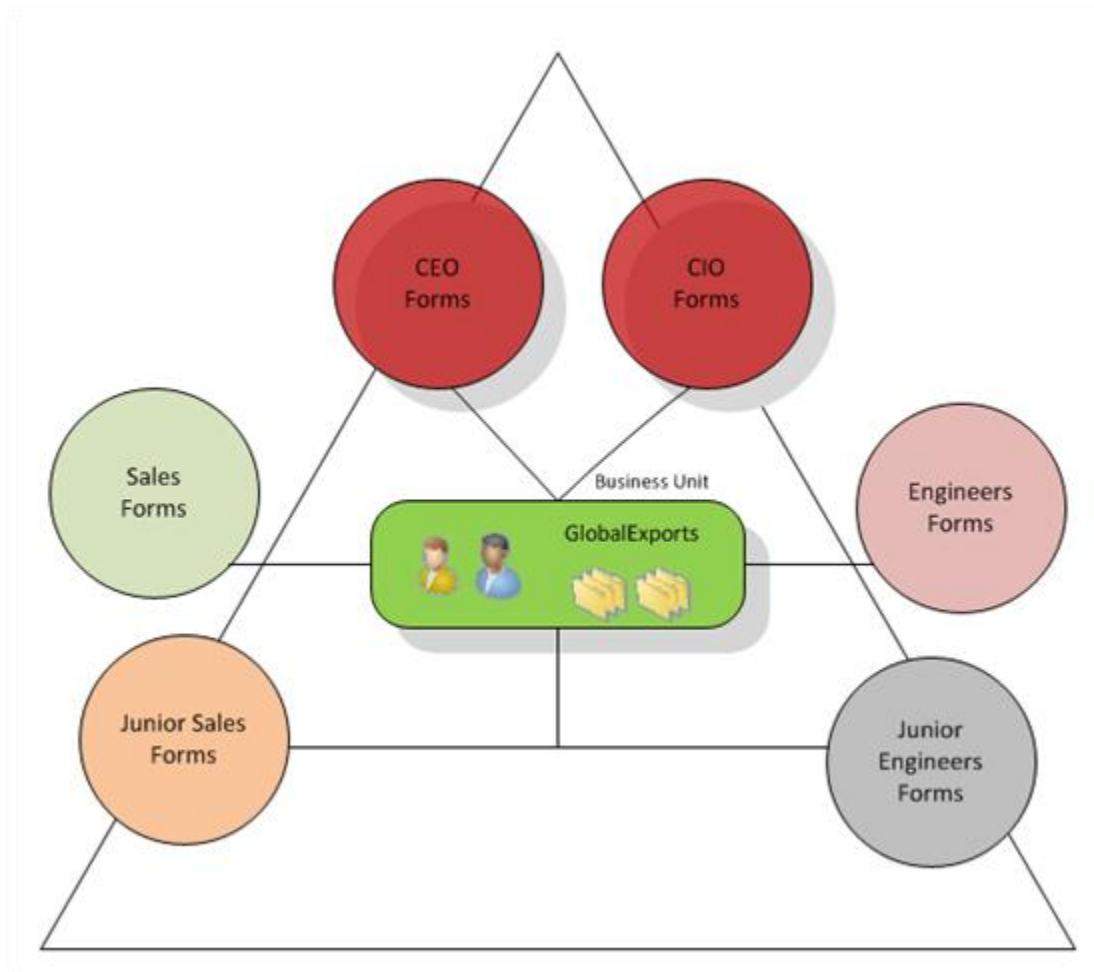


Security Roles Data visibility

Again to help connecting data visibility with real world scenarios I would like to think data visibility as employee job title, employees that work on the same department but that do not necessarily access the same level of information, e.g. Sales representative and a junior sales representative, or a support engineer and a project manager. Assigning forms to different security roles is a new feature in CRM 2011. It provides a more robust way to expose different sets of data to users with different interests. E.g. Engineers and Sales want to get more information about company XYZ however both users are looking at different levels of information, so why provide the same form when we can give them just what they looking for?

At the same time, there is no department boundaries, all data lives in the same Business Unit and can be found by everyone. No need for sharing records.

The below diagram illustrates the company Global Exports CRM design but based on Security Roles data visibility:



Advantages:

- Keep the design simple with one Business Unit (or two if confidential records are required)
- No need to share record
- Ability to mix security roles and provide multiple forms.

Disadvantages:

- No data isolation
- Extra administration maintaining multiple security roles.