Security concepts for Microsoft Dynamics CRM Dynamics CRM 2015

Microsoft Dynamics CRM offers a wide range of security modeling features, and it is important to choose the most appropriate approach to implementing a particular solution.

Each feature offers a combination of characteristics that provides a balance between granularity of access control, administrative ease, and impact on scalability.

Having an understanding of the underlying mechanisms supporting each security modeling feature can be useful when selecting the best approach to solving a particular challenge, especially when planning to develop a large volume system.

Granting access for a user to the system involves two factors:

- **Authentication**, which determines who users are and confirms that they are who they say they are
- **Authorization**, which defines whether authenticated users are entitled to access the system and what within the system they are permitted to see or do

- Authentication in Dynamics CRM is handled using platform features such as Integrated Windows Authentication or Claims Based Authentication with an identity provider such as Active Directory Federation Services. These determine the identity of the users requesting access to the system.

- After users have been identified, information recorded within the Dynamics CRM system about the users, such as their security roles and team memberships, is used to determine whether they are allowed to use the system and what they are allowed to see and do within the system, or what they are authorized to do.

Microsoft Dynamics CRM 2015 and Microsoft Dynamics CRM Online provide a security model that protects data integrity and privacy, and supports efficient data access and collaboration. The goals of the model are as follows:

1. Provide users with the access only to the appropriate levels of information that is required to do their jobs.

2. Categorize users by role and restrict access based on those roles.

3. Support data sharing so that users and teams can be granted access to records that they do not own for a specified collaborative effort.

4. Prevent a user's access to records the user does not own or share.

Role-based security in Microsoft Dynamics CRM focuses on grouping a set of privileges together that describe the responsibilities (or tasks that can be performed) for a user. Microsoft Dynamics CRM includes a set of predefined security roles. Each aggregates a set of user rights

to make user security management easier. Also, each application deployment can define its own roles to meet the needs of different users.

Record-based security in Microsoft Dynamics CRM focuses on access rights to specific records.

Field-level security in Microsoft Dynamics CRM restricts access to specific high business impact fields in an entity only to specified users or teams.

Combine role-based security, record-level security, and field-level security to define the overall security rights that users have within your custom Microsoft Dynamics CRM application.

Business units

A business unit basically is a group of users. Large organizations with multiple customer bases often use multiple business units to control data access and define security roles so that users can access records only in their own business unit.

Role-based security

1. You can use to group sets of privileges together into *roles* that describe the tasks that can be performed by a user or team.
2. Microsoft Dynamics CRM includes a set of predefined security roles, each of which is a set of privileges aggregated to make security management easier.
3. The bulk of the privileges define the ability to create, read, write, delete and share records of a specific entity type.
4. Each privilege also defines how broadly the privilege applies: at the user level, business unit level, the entire business unit hierarchy or across the entire organization.

- **For example, if you sign in as a user that is assigned the Salesperson role, you have the privileges to read, write and share accounts for the entire organization, but you can only delete account records that you own.**
- **Also, you have no privileges to perform system administration tasks such as install product updates, or to add users to the system.**

There are two roles that have very broad privileges: System Administrator and Customizer. To minimize misconfiguration, the use of these two roles should be limited to a few people in your organization responsible for administering and customizing Microsoft Dynamics CRM. Organizations can also customize existing roles and create its own roles to meet their needs.

Record-based security

1. You can use record-based security to control user and team rights to perform actions on individual records.
2. This applies to instances of entities (records) and is provided by access rights.
3. The owner of a record can share, or grant access to a record to another user or team.

4. When this is done, they must choose which rights they are granting.
5. For example, the owner of an account record can grant read access to that account information, but not grant write access.
6. Access rights apply only after privileges have taken effect.
7. For example, if a user does not have the privileges to view (read) account records, they will be unable to view any account, regardless of the access rights another user might grant them to a specific account through sharing.

Hierarchy security

You can use the hierarchy security model for accessing hierarchical data. With this additional security, you gain a more granular access to records, allowing managers to access the records of their reports for approval or do work on reports'

Field-based security

You can use field-level security to restrict access to specific high business impact fields in an entity only to specified users or teams. Like record-based security, this applies after privileges have taken affect. For example, a user may have privileges to read an account, but can be restricted from seeing specific fields in all accounts.

Deployment-wide administrative-level security (on-premises only)

1. During installation, Microsoft Dynamics CRM Server Setup creates a special deployment-wide administrator role and attaches it to the user account that is used to run Microsoft Dynamics CRM Server Setup. Deployment Administrators have complete and unrestricted access to all organizations in Deployment Manager in the Microsoft Dynamics CRM (on-premises) deployment. The Deployment Administrator role is not a security role and does not appear in the Microsoft Dynamics CRM web application as such.
2. Deployment Administrators can create new organizations or disable any existing organization in the deployment. Conversely, members of the System Administrator Role only have permissions within the organization where the user and security role are located.

Security roles

1. A security role defines how different users, such as salespeople, access different types of records.
2. To control access to data, you can modify existing security roles, create new security roles, or change which security roles are assigned to each user.
3. Each user can have multiple security roles.
4. Security role privileges are cumulative: having more than one security role gives a user every privilege available in every role.
5. Each security role consists of record-level privileges and task-based privileges.

6. ***Record-level privileges*** define which tasks a user with access to the record can do, such as
    a. Read,
    b. Create,
    c. Delete,
    d. Write,
    e. Assign,
    f. Share,
    g. Append, and Append To.
    h. *Append* means to attach another record, such as an activity or note, to a record. *Append to* means to be attached to a record.
7. ***Task-based privileges***, at the bottom of the form, give a user privileges to perform specific tasks, such as publish articles or perform a mail merge.
8. The colored circles on the security role settings page define the access level for that privilege. Access levels determine how deep or high in the organizational business unit hierarchy the user can perform the specified privilege.
9. The following table lists the levels of access in Microsoft Dynamics CRM, starting with the level that gives users the most access.

	**Global**. This access level gives a user access to all records within the organization, regardless of the business unit hierarchical level that the instance or the user belongs to. 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**.
	**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**.
	**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**.
	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 that the user is a member of. This is the typical level of access for sales and service representatives. The application refers to this access level as **User**.
	None. No access is allowed.

Manage users

CRM user record fields populated from Active Directory

1. When you create a new user or update an existing user in Microsoft Dynamics CRM 2015 (on-premises), some fields in the CRM user records, such as the name and phone number, are populated with the information obtained from Active Directory Domain Services (AD DS).
2. The synchronization between Active Directory user accounts and the CRM user records is not automatic. If you change user fields in Active Directory, the information isn't propagated to CRM until you refresh the user records in CRM.

The following table shows the fields that are populated on the CRM user form (user record) from Active Directory user account:

CRM User form	Active Directory User	Active Directory object tab
User name	User logon name	Account
First name	First name	General
Last name	Last name	General
Main Phone	Telephone number	General
Primary Email	Email	General
*Address	City	Address

*Address	State/province	Address
Home phone	Home	Telephones

The CRM Address field is comprised of the values from the City and State/province fields in Active Directory.

Manage teams

1. Using teams in Microsoft Dynamics CRM is optional.
2. However, teams provide an easy way to share business objects and let you collaborate with other people across business units.
3. While a team belongs to one business unit, it can include users from other business units.
4. You can associate a user with more than one team.

You can use two types of teams:

1. **An *owner* team** owns records and has security roles assigned to the team.
    - The team's privileges are defined by these security roles.
    - In addition to privileges provided by the team, team members have the privileges defined by their individual security roles and by the roles from other teams in which they are members.
    - A team has full access rights on the records that the team owns.
2. **An *access* team** doesn't own records and doesn't have security roles assigned to the team.
    - The team members have privileges defined by their individual security roles and by roles from the teams in which they are members.
    - The records are shared with an access team and the team is granted access rights on the records, such as Read, Write, or Append.

When to use owner teams

1. Your organization's policies require the ability for records to be owned by entities other than users, such as the team entity.
2. The number of teams is known at the design time of your Microsoft Dynamics CRM system.
3. Daily reporting on progress by owning teams is required.

When to use access teams

1. The teams are dynamically formed and dissolved. This typically happens if the clear criteria for defining the teams, such as established territory, product, or volume are not provided.

2. The number of teams is not known at the design time of your Microsoft Dynamics CRM system.

3. The team members require different access rights on the records. You can share a record with several access teams, each team providing different access rights on the record. For example, one team is granted the Read access right on the account and another team, the Read, Write, and Share access rights on the same account.

4. A unique set of users requires access to a single record without having an ownership of the record.

About access teams and team templates

1. You can create an access team manually by choosing the team type Access, or let the system create and manage an access team for you. When you create an access team, you can share multiple records with the team.
2. A **system-managed access team** is created for a specific record; other records can't be shared with this team. You have to provide a team template that the system uses to create a team. In this template, you define the entity type and the access rights on the record that are granted to the team members when the team is created.

3. A team template is displayed on all record forms for the specified entity as a list. When you add the first user to the list, the actual access team for this record is created. You can add and remove members in the team by using this list. The team template applies to the records of the specified entity type and the related entities, according to the cascading rules. To give team members different access on the record, you can provide several team templates, each template specifying different access rights. For example, you can create a team template for the Account entity with the Read access right, which allows the team members to view the specified account. For another team that requires more access to the same account, you can create a team template with Read, Write, Share and other access rights. To be added to the team, a minimum access level a user must have on the entity specified in the template is Basic (User) Read.
4. Because of the parental relationship between the team template and system-managed access teams, when you delete a template, all teams associated with the template are deleted according to the cascading rules. If you change access rights for the team

template, the changes are applied only to the new auto-created (system-managed) access teams. The existing teams are not affected.