Manage teams Dynamics CRM 2015

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

You can use two types of teams:

- 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.
- 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.

---

1. Owner team or access team?
2. About owner teams
3. About access teams and team templates
4. Maximum settings for system-managed access teams

Owner team or access team?

Choosing the type of the team may depend on the goals, nature of the project, and even the size of your organization. There are a few guidelines that you can use when choosing the team type.

When to use owner teams

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

When to use access teams

- 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.
- The number of teams is not known at the design time of your Microsoft Dynamics CRM system.
- 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.
- A unique set of users requires access to a single record without having an ownership of the record.

About owner teams

An owner team can own one or more records. To make a team an owner of the record, you must assign a record to the team.

If an owner team doesn't own records and doesn't have security roles assigned to the team, it can be converted to an access team. It is a one-way conversion. You can't convert the access team back to the owner team. During conversion, all queues and mailboxes associated with the team are deleted. When you create a team in the Web application, you have to choose the team type **Owner**.

About access teams and team templates

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.

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.

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.

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.

Note

A user must have sufficient privileges to join an access team. For example, if the access team has the Delete access right on an account, the user must have the Delete privilege on the Account entity to join the team. If you're trying to add a user with insufficient privileges, you'll see this error message: "You can't add the user to the access team because the user doesn't have sufficient privileges on the entity."

Maximum settings for system-managed access teams

The maximum number of team templates that you can create for an entity is specified in the **MaxAutoCreatedAccessTeamsPerEntity** deployment setting. The default value is 2. The maximum number of entities that you can enable for auto-created access teams is specified in the **MaxEntitiesEnabledForAutoCreatedAccessTeams** deployment setting. The default value is 5.