

## **Manage security, users and teams Security concepts for**

### **Microsoft Dynamics CRM**

The following section contains information about users, teams, and security in Microsoft Dynamics CRM.

1. Security concepts for Microsoft Dynamics CRM
2. Invite someone to use Microsoft Dynamics CRM
3. Security roles
4. Create or edit a security role
5. Copy a security role
6. Manage users
7. Manage teams
8. Add teams or users to a field security profile
9. Synchronize user information between Microsoft Dynamics CRM and Active Directory
10. Add or remove territory members
11. Troubleshooting: User needs read-write access to the CRM organization

### **Security concepts for Microsoft Dynamics CRM**

#### **Applies To: CRM 2015 on-prem, CRM Online**

You use the security model in Microsoft Dynamics CRM to protect the data integrity and privacy in a Microsoft Dynamics CRM organization. The security model also promotes efficient data access and collaboration. The goals of the model are as follows:

1. Provide a multi-tiered licensing model for users.
2. Grant users access that allows only the levels of information required to do their jobs.
3. Categorize users and teams by security role and restrict access based on those roles.
4. Support data sharing so that users can be granted access to objects they do not own for a one-time collaborative effort.
5. Prevent access to objects a user does not own or share.

You combine business units, role-based security, record-based security, and field-based security to define the overall access to information that users have in your Microsoft Dynamics CRM organization.

#### **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**

---

You can use to group sets of privileges together into *roles* that describe the tasks that can be performed by a user or team. Microsoft Dynamics CRM includes a set of predefined security roles, each of which is a set of privileges aggregated to make security management easier. The bulk of the privileges define the ability to create, read, write, delete and share records of a specific entity type. 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.

A user that has been assigned the Vice President of Sales role can perform a wider set of tasks (and has a greater number of privileges) associated with viewing and modifying data and resources than can a user who has been assigned to the Salesperson role. A user assigned the Vice President of Sales role can, for instance, read and assign any account to anyone in the system, while a user assigned the Salesperson role cannot.

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**

---

You can use record-based security to control user and team rights to perform actions on individual records. This applies to instances of entities (records) and is provided by access rights. The owner of a record can share, or grant access to a record to another user or team. When this is done, they must choose which rights they are granting. For example, the owner of an account record can grant read access to that account information, but not grant write access.

Access rights apply only after privileges have taken effect. 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' behalf.

### **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)**

---

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.

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.

<b>Important</b>
<b>When a deployment administrator creates an organization, that administrator must give db_owner privileges for the org's databases to the other deployment administrators so that they also have full access to those organizations.</b>

Security roles

Applies To: CRM 2015 on-prem, CRM Online

To control data access, you must set up an organizational structure that both protects sensitive data and enables collaboration where appropriate. You do this by setting up business units, security roles, and field security profiles.

## Security roles

---

A security role defines how different users, such as salespeople, access different types of records. 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. Each user can have multiple security roles.



Security role privileges are cumulative: having more than one security role gives a user every privilege available in every role.

Each security role consists of record-level privileges and task-based privileges.

*Record-level privileges* define which tasks a user with access to the record can do, such as Read, Create, Delete, Write, Assign, Share, Append, and Append To. *Append* means to attach another record, such as an activity or note, to a record. *Append to* means to be attached to a record.

*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.

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. The following table lists the levels of access in Microsoft Dynamics CRM, starting with the level that gives users the most access.

	<p><b>Global.</b> 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.</p> <p>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.</p> <p>The application refers to this access level as Organization.</p>
	<p><b>Deep.</b> 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.</p> <p>Users who have Deep access automatically have Local and Basic access, also.</p> <p>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</p>

	<p>plan. This level of access is usually reserved for managers with authority over the business units.</p> <p>The application refers to this access level as <b>Parent: Child Business Units</b>.</p>
☀	<p><b>Local.</b> This access level gives a user access to records in the user's business unit.</p> <p>Users who have Local access automatically have Basic access, also.</p> <p>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.</p> <p>The application refers to this access level as <b>Business Unit</b>.</p>
🌞	<p><b>Basic.</b></p> <p>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.</p> <p>This is the typical level of access for sales and service representatives.</p> <p>The application refers to this access level as <b>User</b>.</p>
🚫	<p><b>None.</b> No access is allowed.</p>

### Important

To ensure that users can view and access all areas of the web application, such as entity forms, nav bar or command bar, all security roles in the organization must include the Read privilege on the Web Resource entity. For example, without read permissions, a user will not be able to open a form that contains a web resource and will see an error message similar to this: “Missing **prvReadWebResource** privilege

### Overriding security roles

---

The owner of a record or a person who has the Share privilege on a record can share a record with other users or teams. Sharing can add Read, Write, Delete, Append, Assign, and Share privileges for specific records.

Teams are used primarily for sharing records that team members ordinarily couldn't access. For more information, It's not possible to remove access for a particular record. Any change to a security role privilege applies to all records of that record type.