Field Security

Field Security controls access to specific fields. Most fields[1] in your database can have…

- **Full Access** – is the default permission for all fields for all users and allows a user to view, add, edit, or remove information in that field without restriction.
- **Read-Only Access** – restricts specific users and/or teams from editing or deleting a field while allowing them to view the contents. The field contains a grey background for Read-Only Access. This permission allows you to restrict editing access to those who are responsible for updating the data.
- **No Access** – restricts which users can even see specific fields. Fields defined as No Access appear empty with a grey background. It is only available in the Premium version.

Premium

Procedure: ***To add Field Security***

1. **Tools Define Fields...**.

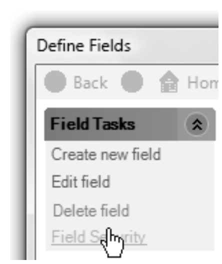
   Only users with Administrator or Manager roles can assign Field Security.

2. Select the table that contains the fields for Field Security by changing the "View fields for:" to Contacts, Companies, Groups, or Opportunities.

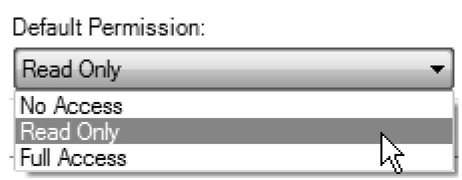
   Security is set on a field-by-field basis.

   ☞ *Neither Groups "Group Name" nor Companies "Company Name" can be set to anything but Full Access.*

3. Select the field you want to restrict access to and click **Field Security** in the "Field Tasks" area at the upper left.

4. Assign the "Default Permission:" for the field. Select from **Full Access**, **Read Only**, or **No Access** if you are a Premium user.

   Default permission is applied to all users. Then you can assign user or team permission to override the default.

---

[1] Fields in the Contacts, Groups, or Companies tables which are restricted and cannot have security applied: Company, Contact, City, State, ZIP Code, Phone, E-mail, ID/Status, Salutation, Groups Name or Company Name. Opportunity fields will support the "Read Only" access level, but not the "No Access" level.

5. Click **Yes** to assign the default permission for all users.

6. Select the **Users** or **Teams** tab.

   Teams can be a much more efficient way of assigning field-level access. As your company changes, simply add, replace, or delete users assigned to a team and permissions are updated for all fields immediately.

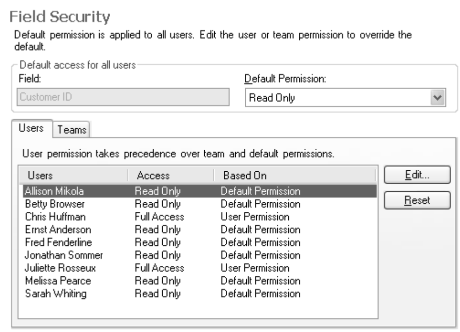
   Premium

7. Click **Edit…**.

   A complete list of users (or teams) displays.

8. Select each user (or team) and define their Access Level: from the drop-down. When finished, click **OK**.

9. To change a user's access back to the Default Permission, select the user and click **Reset**.



10. Click **Finish**.

    Fields that have Field Security permissions assigned display a Private icon to the left of their name.

☞ *If a user does not have permission to view the contents of a field (No Access), then the field name will not be available for queries, importing or exporting, or for displaying in any list view. Company Fields and Contact fields (even though linked) do not share access levels and therefore may not be updated if user doesn't have full access.*

Mini-Exercise: Changing Field Security

Step	What to do	How to do it/Comments
1.	Enter 50,000 into User 3 field on a record (or two).	
2.	Now, let's rename "User 3" field to "Credit Rating" and then assign Field Security of Read-Only by default. Exit Define Fields and view the Credit Rating. Can you change it?	**Tools, Define Fields**. Double-click User 3 field and rename it to "Credit Rating." Click **Finish**. While the field is still selected, click **Field Security**. Change from Full Access to Read Only and click Yes to verify the changes. Click **Finish**. No you can't change or enter new values.