**Field Security Profiles:**

**Introduction to field level security**

**Field level security is a security feature available in Microsoft Dynamics CRM 2013 using which administrators can configure individual fields in Dynamics CRM web application so that user will have restricted access to those fields.**

**In Microsoft Dynamics CRM 2013 and Online you can use field level security to configure security roles that control user and team access rights to specific fields and entities.**

**One important point to remember when enabling field security is that it can be implemented only for custom fields, and not for system fields.**

**Benefits of field security in Dynamics CRM 2013**

**Using field security users can be given Create, Read, Update to individual fields in Dynamics Web forms based on the security profiles.**

**A Security profile determines the following:**

**•Permissions to the secure fields**

**•Users and Teams**

**A Security Profile can be configured to grant the following permissions at the field level to the added users or teams:**

**•Read (read-only access to the field’s data)**

**•Create (users or teams in this profile can add data to this field when creating a record)**

**•Update (users or teams in this profile can update the field’s data after it has been created)**

**A combination of these three permissions can be configured to determine the user privileges for a specific data field.**

Which security roles allow you to see secured fields?

The System Administrator field security profile gives full access to all secured fields in Microsoft Dynamics CRM. By default, all users who have the System Administrator security role have this profile. This profile is system managed and can’t be updated or deleted.

How do secured fields behave for Retrieve and Retrieve Multiple?

Microsoft Dynamics CRM evaluates if the caller and the impersonated user have access to each retrieved record (this is the regular security process) and each secured field. The call does not throw an exception if the criteria contain secured fields for which the caller does not have access. Instead, null values are returned for secured fields if they are part of the output column set.

If the caller (or impersonated user) does not have read access to the secured fields that are included in a column set, the value returns as **null**.

When a secured attribute is in the filter condition:

If the caller (or impersonated user) does not have access to the secured fields that are included in the filter criteria, the field value is substituted with **null** during the evaluation of the filter.

When Aggregating:

Secured values are substituted with a null value,

When Grouping:

If the caller (or impersonated user) does not have access to the attribute used for grouping, the value is treated as **null** and the results are grouped together with all **null** values.

When Ordering:

If the caller (or impersonated user) does not have access to secured fields that are included in an order by condition, the values will be treated as if they are **null**.

How do secured fields behave for create or update?

**A programmer may build a client that uses Create and Update methods that interact with secured fields. When you call the Create or Update method, passing data for secured fields and the caller does not have sufficient permissions, an exception is thrown.**

How do secured fields behave when records are shared?

**A user with access to a secured field in a record can choose to share it with another user or team. The user can only give the access that they have on the record. For example, to share the record and grant Update privileges, the user must have update privileges.**

**You can share a secured field on a particular record with Read and/or Update with a security principal (user or team).  The user or team members with whom the record was shared now have that type of secured field access only on the shared secured fields on only that particular record, even if the user or team member to whom it was shared does not have a field security profile that gives them access**

How do secured fields behave for filtered views?

**An administrator secures a number of fields for access in the application and wants the fields not to be available in reports. This allows for maintaining the same set of reports for all users. Filtered views will not return data for the secured fields if the calling user does not have authorization for the fields. When no field security is applied for any of the view’s attributes, the filtered views return complete data.**

How do secured fields behave for offline synchronization?

**If you are using Microsoft Dynamics CRM for Microsoft Office Outlook with Offline Access, only the secured field values that you have access to replicate into the offline database. If you don’t have access to the data, it is not saved offline.**

**You cannot delete the System Administrator field level security profile**