ARBELA

Best Practices for Security Roles & Field Security Profile

Security Roles

What is Role-Based Security?

Role-based security is that a role contains privileges that define a set of actions that can be performed within the organization

How role-based security can be used to control access

- You can use role-based security to group sets of privileges together into roles that describe the tasks that can be performed by a user or team.
- Microsoft Dynamics 365 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.

What is a Privilege?

A privilege authorizes the user to perform a specific action on a specific entity type.

The following table lists the types of privileges that are referred to from the following entity/privilege reference:

Privilege	Description
Create	Required to make a new record. The records that can be created depends on the access level of the permission defined in your security role.
Read	Required to open a record to view the contents. The records that can be read depends on the access level of the permission defined in your security role.
Write	Required to make changes to a record. The records that can be changed depends on the access level of the permission defined in your security role.
Delete	Required to permanently remove a record. The records that can be deleted depends on the access level of the permission defined in your security role.
Append	Required to associate a record with the current record. For example, if a user has Append rights on an opportunity, the user can add a note to an opportunity. The records that can be appended depends on the access level of the permission defined in your security role.
Append To	Required to associate the current record with another record. For example, a note can be attached to an opportunity if the user has Append To rights on the note. The records that can be appended to depends on the access level of the permission defined in your security role.
Assign	Required to give ownership of a record to another user. The records that can be assigned depends on the access level of the permission defined in your security role.
Share	Required to give access to a record to another user while keeping your own access. The records that can be shared depends on the access level of the permission defined in your security role.

Access Levels

The access level or privilege depth for a privilege determines, for a given entity type, at which levels within the organization hierarchy a user can act on that type of entity.

The following table lists the levels of access in Microsoft Dynamics 365, starting with the most access. The icon is shown in the security role editor in the Web application.

Icon	Level	Description
	Global	This access level gives a user access to all records in 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. 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. 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. 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 that the user 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.

Dependencies

Sometimes, security dependencies exist because it is necessary to have more than one access right to perform a given action.

Action	Access Rights Required
To **Create** a record	CREATE READ
To **Share** a record	SHARE READ
To **Assign** a record	ASSIGN WRITE READ
To **Append To** a record	WRITE READ APPEND TO
To **Append** a record	WRITE READ APPEND

Field Level Security

What is Field Level Security?

Field Level Security is used 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.

Field Level Security is managed by the Security Profiles

Which Fields can be Secured?

Every field in the system contains a setting for whether field security is allowed

Security Profiles

A security profile determines the following:

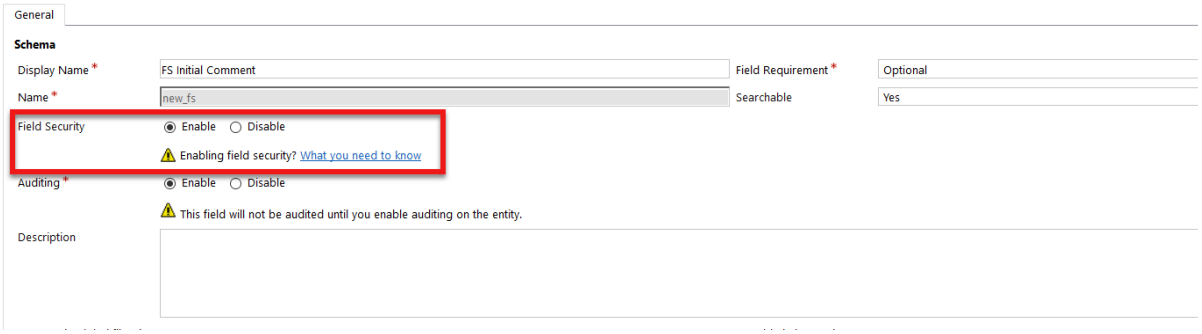
- Permissions to the secure fields
- Users and Teams
    - A security profile can be configured to grant user or team members the following permissions at the field level:
- Read. Read-only access to the field's data.
- Create. Users or teams in this profile can add data to this field when creating a 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.

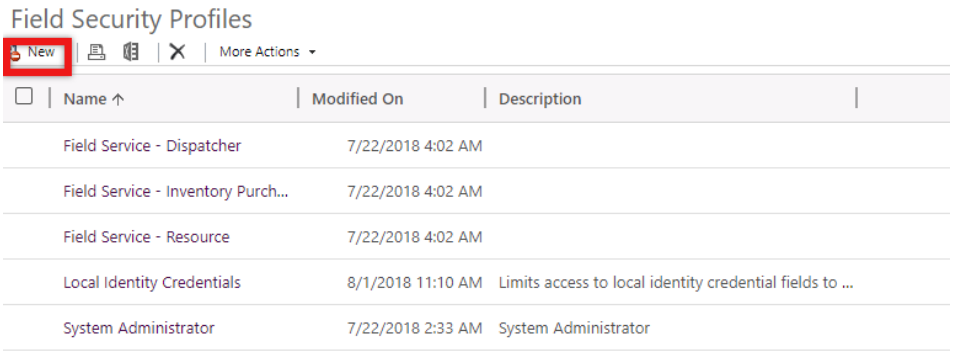
How to Restrict Access to a Field?

The following steps describe how to restrict access to a field:

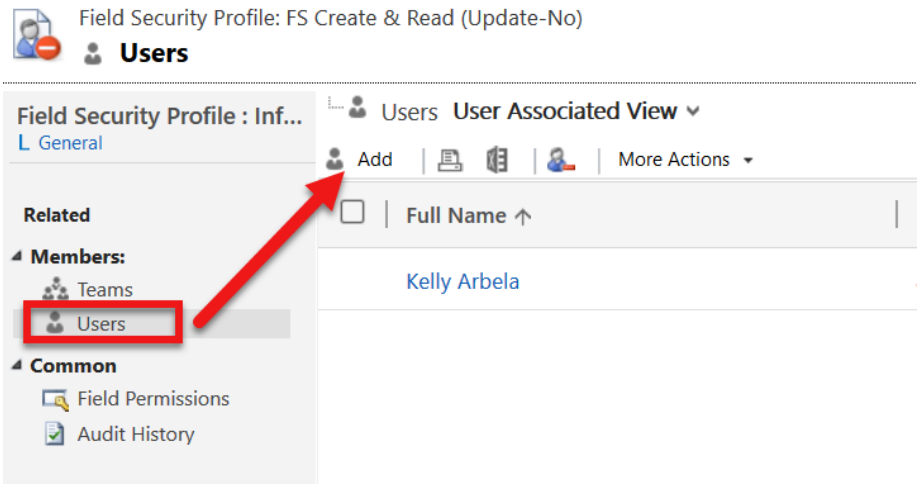
1) Enable field-level security for an attribute



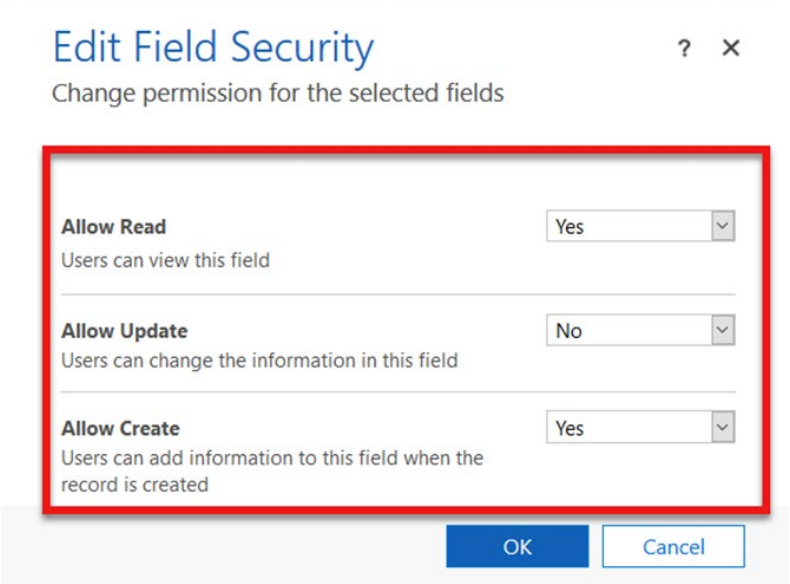
2) Create a field-level security profile



3) Associate users or teams with the profile

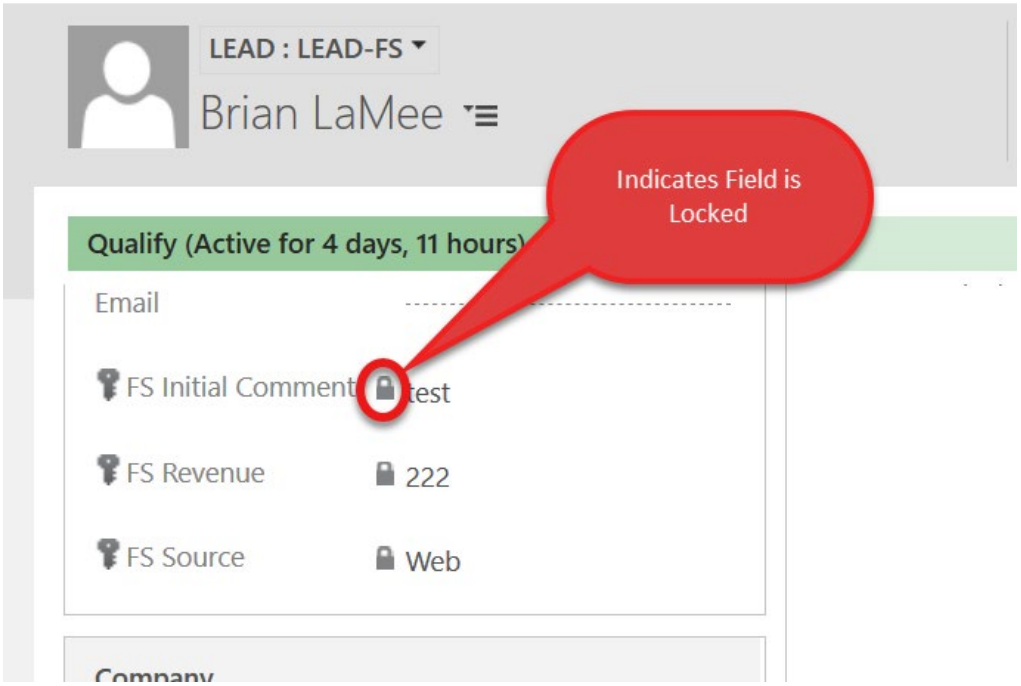


4) Add specific field permissions, such as Create, Update or Read for a specific attribute

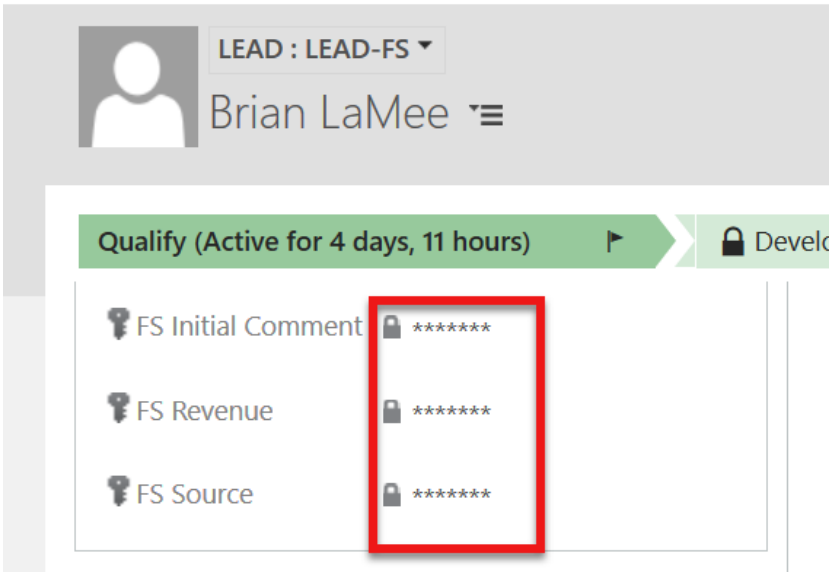


How do I know if a Field is Secure?

How does it look when User has Read-Only permission?



How does it look if a User does not have permissions?



Best Practice for Field Security

- When you use calculated fields that include a field that is secured, data may be displayed in the calculated field to users that don't have permission to the secured field. In this situation, both the original field and the calculated field should be secured.
  - Some data, such as addresses, are actually made up of multiple fields. Therefore, to completely secure data that includes multiple fields, such as addresses, you must secure and configure the appropriate field security profiles on multiple fields for the entity. For example, to completely secure addresses for an entity, secure all relevant address fields,

such as address_line1, address_line2, address_line3, address1_city, address1_composite, and so on.

Best Practices for Modifying Roles

- Do **NOT** Modify Out of the box Security Roles
    - Copy the role then modify
    - This will avoid potential issues with future upgrades as well as a point of reference

Security Design Tips

- Always have your security model in mind
- Plan for the future
- Keep it simple
- Don’t ignore protentional security issues
- Understand & Clarify