1. Data Security
2. Control Access to Fields

Control Access to Fields

Learning Objectives

After completing this unit, you'll be able to:

- List reasons to limit access to specific fields.
- View and edit field-level security settings.

Modify Field-Level Security

Defining field-level security for sensitive fields is the second piece of the security and sharing puzzle, after controlling object-level access.

In some cases, you want users to have access to an object, but limit their access to individual fields in that object. Field-level security settings—or field permissions—control whether a user can see, edit, and delete the value for a particular field on an object. These are the settings that allow us to protect sensitive fields such as a candidate's social security number without having to hide the candidate object.

Unlike page layouts, which only control the visibility of fields on detail and edit pages, field-level security controls the visibility of fields in any part of the app, including related lists, list views, reports, and search results. In fact, to make absolutely sure that a user can't access a particular field, it's important to use the field-level security page for a given object to restrict access to the field. There are simply no other shortcuts that provide the same level of protection for a particular field.

For example, here are some field-level security settings you can set for the Recruiting app.

- Position object—hide minimum and maximum pay from standard employees and interviewers.
- Candidate object—hide social security numbers from hiring managers and interviewers.
- Job Application object—make the Position and Candidate lookup fields read-only for hiring managers.

Field settings can be applied either by modifying profiles or permission sets or from the Field Accessibility menu in Setup.

After setting field-level security for users, you can:

- Create page layouts to organize the fields on detail and edit pages.
- Verify users' access to fields by checking the field accessibility.
- Customize search layouts to set the fields that display in search results, in lookup dialog search results, and in the key lists on tab home pages.

Restrict Field Access with a Profile

You apply field settings by modifying profiles or permission sets. Let's try *restricting* a user's general access with a profile. Then we can *expand* it as needed with a permission set.

Tip

If you haven't already done it, before you start, enable the enhanced profile user interface. Type `User Management Settings` in the **Quick Find** box in Setup, then turn on **Enhanced Profile User Interface**.

1. Use the Quick Find box to find **Profiles** in Setup.
2. Select the profile you want to change. "Standard User" will do nicely.
3. Click **Object Settings** and select the object for which you want to update the field settings.
4. Click **Edit**.
5. For each field, specify the kind of access you want for users with this profile, and save your settings.

Now that you've set field-level security for sensitive data, you can create page layouts to organize the fields for users' convenience, and customize how the fields display in search results and lists. For the final piece of the puzzle, specify the individual records to which each user needs access. By combining security controls at all three levels, you can set up a highly secure data access model which is flexible enough to meet the needs of many different types of users.

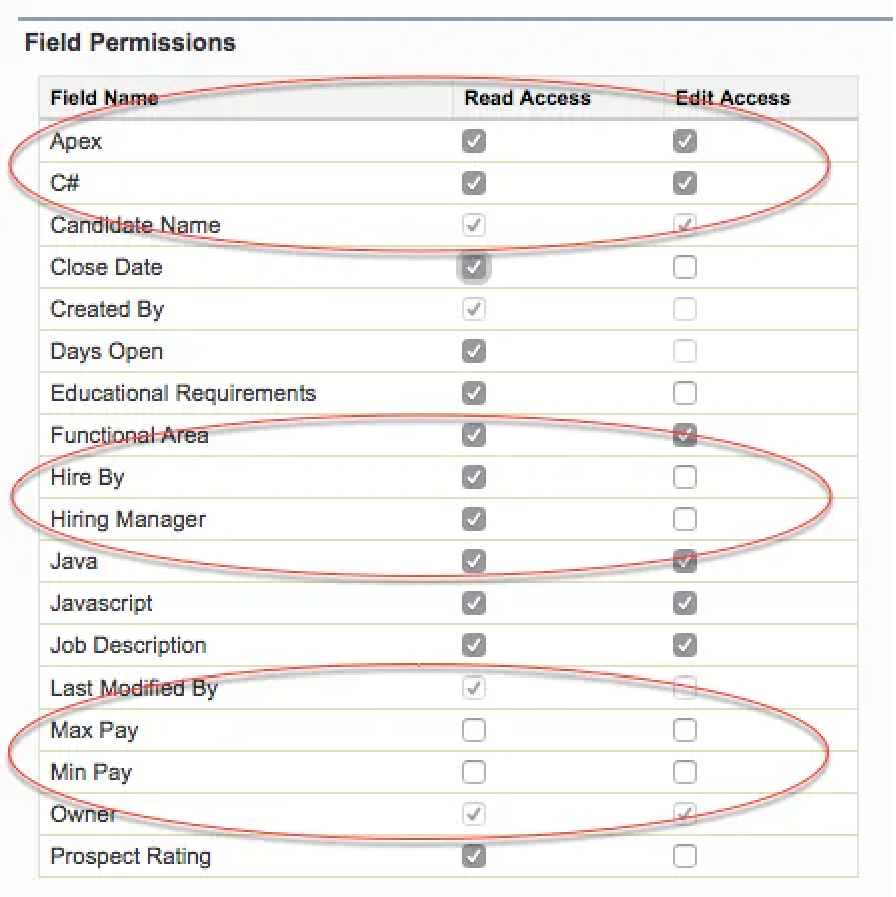
Add Field Access with a Permission Set

Let's look at how field settings can be applied by modifying permission sets. Remember, a permission set is for *expanding* a user's access to fields that are restricted in their profile.

Let's set up our interviewers to update the candidate record when they've interviewed a candidate. We'll assume our interviewers have the Standard User profile.

We worked with Permission Sets when we set up our custom objects. Now we'll go back to that Setup page to make sure the right fields in one of our objects are available to the users who need them.

1. In Setup, use the Quick Find box to find **Permission Sets**.
2. Select a permission set and click **Object Settings**.
3. Click the object you're working with, then click **Edit**.
   In this example, we're modifying the Candidate object.
4. Under **Field Permissions**, specify the kinds of access your interviewers need, then save this permission set.



Field Permissions

Field Name	Read Access	Edit Access
Apex	☑	☑
C#	☑	☑
Candidate Name	☑	☑
Close Date	☑	□
Created By	☑	□
Days Open	☑	□
Educational Requirements	☑	□
Functional Area	☑	☑
Hire By	☑	□
Hiring Manager	☑	□
Java	☑	☑
Javascript	☑	☑
Job Description	☑	☑
Last Modified By	☑	□
Max Pay	□	□
Min Pay	□	□
Owner	☑	☑
Prospect Rating	☑	□

   See how we've enabled our interviewers to both read and change the values of the Apex and C# checkboxes? Now they can check or uncheck those boxes when they've determined the candidate's command of those skills. We've prevented them from changing the Hire By date or the name of the hiring manager, but they can see that information. And they don't need to know the pay rate for the position, so we've removed both their Read and Edit access for those fields.
5. Click **Manage Assignments** and select the users who you expect to need the permissions you've just specified. Click **Add Assignments** and **Done**, and you're done!

Now you've defined field-level security for sensitive data. For the final piece of the puzzle, specify the individual records each user needs access to. By combining security controls at all three levels, you can set up a highly secure data access model that's flexible enough to meet the needs of many different types of users.

Resources

- Security Implementation Guide

Assessment Complete!

+500 points

Data Security
100%
Progress: 100%
Retake this Challenge
View more modules