Object, Field and Record Access: The Three Layers Admins Confuse

All three must pass for a value to appear. Confusing them is the most common misdiagnosis.

> Short answer: Salesforce evaluates access at three independent levels, object, field and record. All three must pass for a value to appear on screen. Because a user needs all three simultaneously, an access problem is very often diagnosed at the wrong layer, which leads to a fix that does not fix anything.

What are the three layers, exactly?

Object access. Can the user create, read, edit or delete this object at all, regardless of record or field. Granted by profile, extended by permission sets and permission set groups.

Field-level security. Of the fields the user can access, which specific fields can they see or edit. A setting independent of object access entirely.

Record-level access. Of the records that exist, which specific rows can this user reach. Governed by org-wide defaults, role hierarchy, sharing rules and manual shares, none of which are visible from the profile or permission set screens.

Why must all three pass together?

The three layers combine with an AND, not an OR. A value only appears if the user has object access, field access, and record access, all three, for that specific piece of data. A failure at any one layer produces the identical symptom: the user cannot see the value. Nothing about that symptom alone tells you which layer failed.

Where does the confusion actually happen?

Assuming object access implies field access. A user with full edit access to Opportunity does not automatically see every field on it. If a commission field is hidden at the field level, that user sees the record and edits other fields, while that one field simply does not appear.

Assuming a record-level fix will resolve a field-level problem. If the actual cause is field-level security, adjusting sharing rules changes nothing, because the user could already reach the record.

Diagnosing at the layer that is easiest to check. Field-level security has a dedicated screen, Field Accessibility. Record-level access has no equivalent, and requires checking several mechanisms. Under time pressure, the easy layer gets checked first and the investigation stops there even if it is not the actual cause.

A worked example

A regional sales rep reports she cannot see the discount percentage on an Opportunity a colleague can see.

Wrong path: assume it is record-level since the reps are in different territories, spend time on role hierarchy and sharing rules, find nothing conclusive.

Correct path: confirm object-level access is equal for both, quick to check. Then check field-level security on the discount field specifically, since confidentiality-restricted fields are common. If the colleague has a permission set granting edit and the reporting rep does not, that is the entire explanation.

How does seeing all three together remove the guesswork?

Who Sees What resolves all three layers for a chosen user at once, object permissions, field-level security, and record-level reachability, each annotated with the specific rule responsible. Because all three are visible together, there is no point at which a plausible answer at the wrong layer gets mistaken for the actual cause.

Get Who Sees What free on the AppExchange →

Who Sees What is built and maintained by TwinStack Solutions, a Salesforce partner. Questions about setup: info@twinstack.net