ARCHER®
SUMMIT 2025

Rule the Archer Universe with Access Control

Tyler Hunt & Jason Ingle | September 16th 2025

BLUEPRINT FOR GRC SUCCESS

Permissions are like a tree

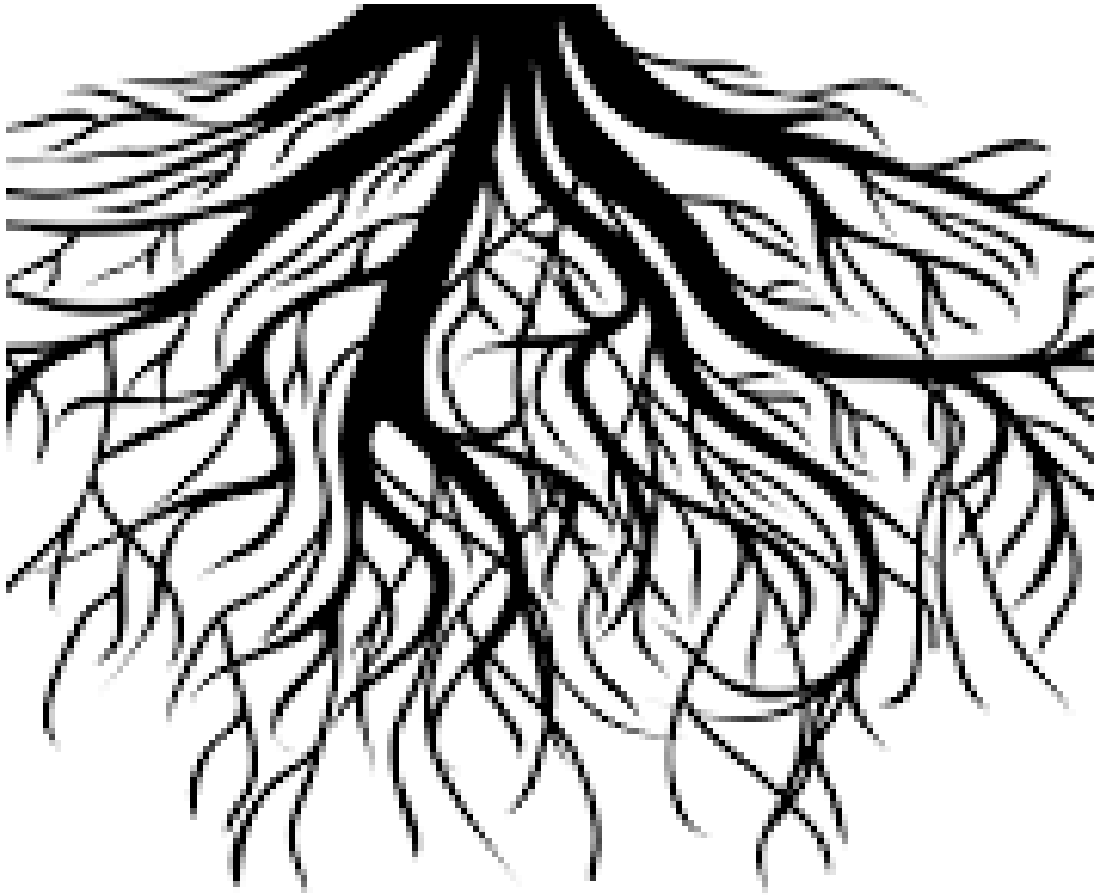
Field Permissions

Record Permissions

Roles

Authentication/Login

Authentication/Login



- The first level of access control is the login itself. The user must be authorized via a granted login/password or authenticate via SSO permissioning.
- This grants basic entry into Archer with default permissions based upon the general user role.
- USERS MUST HAVE LOGIN TO GET ROLES

Roles

- Roles are how rights are assigned
  - In admin, manage access roles
- Rights are assigned broken down by
  - Solution
  - Application/Questionnaire name
  - Page Type
    - Administrator
    - End User
  - CRUD
    - Create – create new record
    - Read – look at existing data
    - Update – edit existing data inside record
    - Delete – delete record
- The Access Control reports show Role permissions

How do users get role rights?

- Groups are assigned roles
  - Users are assigned groups, hence user gets role
  - In admin, manage groups
- Users may also be assigned roles directly
  - In admin, manage users
- USERS MUST HAVE ROLE PERMISSIONS TO GET THOSE RECORD PERMISSIONS

How do users get role rights?

- Record permissions give the user permission to that particular record at the assigned permission level ONLY IF THE ROLE PERMISSIONS ALLOW IT
- Record permissions for the user add together to get highest assigned permission set
- If the application has no record permissions fields, ROLE permissions prevail for all records

Record Permissions

- There are 3 types of record permissions
  - Manual
  - Inherited
  - Automatic
- These may be used in any combination in an application or questionnaire
- The different types add together to determine ultimate permissions

Record Permissions

- Manual record permissions allow users to populate
  - Groups
  - Users
  - Record Creator
- Group(s) or Record Creator may be set as default
- Rules can be added to allow adjustment to permission set based on field selections

Inherited Record Permissions

- Inherited record permissions pull permissions from other applications/questionnaires they are related to
  - Unrestricted – fields from all related records inherit
  - Restricted – selected fields from related records inherit
    - Must set up multiple cross-refs to same application to use this feature
    - Choose particular fields from each cross-ref
- Cannot be changed by user

Automatic Record Permissions

- Automatic record permissions create permissions based on field criteria rules
- Each rule has its own set of permissions to assign
- Permissions can change based on rule triggering
- Multiple rules may be true and, if so, permissions will add together
- Default record permissions may be assigned but are only used when no rules are true

Record Permissions? Which kind should I use?

- Manual
  - When users should assign permissions
    - Review data
    - Get notifications (based on RP)
- Inherited
  - When using the same permissions as another application's fields (based on cross-ref records)
    - Retains consistency
- Automatic
  - When field criteria defines user's permissions
    - Very flexible as it adjusts as the record changes

- USERS MUST HAVE RECORD PERMISSION TO SEE FIELDS

Record Permissions Troubleshooting Tip

- If you have a user that cannot see a record, the issue is probably record permissions
  - An easy way to troubleshoot is to create a report with the trackingid and all the record permissions fields
    - In search modify, choose “Type” from the drop-down next to the magnifying glass and type in perm in the box
      - All record permissions will display
      - Use this to determine who has access

Field Permissions

- Public
  - As long as the user has record permission, they will see this field and have assigned permission
- Private
  - Only users selected can see that field
  - Users will have assigned permission
    - Full access checked grants read and edit
      - User only gets edit if allowed in their record permissions, even though box is checked
    - Unchecked is read only
    - Cascade extends the rights to subgroups of the selected group(s)
- DDEs can also display/hide and set fields to read-only

Summary

- Permissions are hierarchical. Each permission type is required before the next.

- You must have Login to get a Role
  - You must have Role to get to application records
    - You must have Record Permissions to see any fields
      - You must have Field Permission to see each field

Lab Work

https://80076.se.archerirm.us/Default.aspx

- Earth01Admin
- Earth01User
- Archer123!