# visibility controls

This document discusses how Issuetrak can control access to issues based on a combination of user permissions and membership in the entities: Organizations, Departments, or Projects.

A user's access to an issue is controlled through:

- **Administrator rights**: All administrators are able to view all issues.
- **A role on the issue:** Are they assigned to the issue, did they submit the issue, or are they a member of the issue through an email distribution list? With a **direct role** in the issue, a user can always view the issue.
- **User permission:** Without a role on the issue, a user needs the permission, "Can view issues submitted by others" to view any additional issues. With this permission, they can view all issues in the site unless bound by entity membership.
- **Entity Membership:** Being associated to an entity can limit access to issues. If an entity is restricted to an internal view, then users can only view issues that belong to that entity.
- **Project Membership:** If a project is marked as exclusive, only administrators and users that are members of that project can view any issues associated to that project.

When put together, these options control any individual user's access to view issues as well as user lists in Issuetrak. This allows you to control whether a user sees all issues within the site or is locked down to only a specific subset of issues.

## *administrator rights*

Users designated as administrators within Issuetrak are not impacted by visibility controls and see all the issues and user lists within the site. They cannot be limited. A user is considered an administrator when they have any one of the following:

- Agents with the "Sys Admin" parameter
- Agents with the "Can access and maintain Administration functions" permission
- End Users or Agents with the "Allowed Read Only access to Administration information" permission

## *issue roles*

The following roles always grant access to an issue. A user cannot be restricted from seeing an issue they play a role on.

- Enterer: Person logging the issue
- Submitter: Person with the problem that the issue is for
- Assignee: Owner of the issue
- Task Assignee: Owner of part of the issue process/workflow

Email distribution lists can also grant access to view an issue. Distribution lists can be set up by Priority, Issue Type, Subtype, or Project, as well as the entities of Organization, Department, and Location.

## *internal versus external entities*

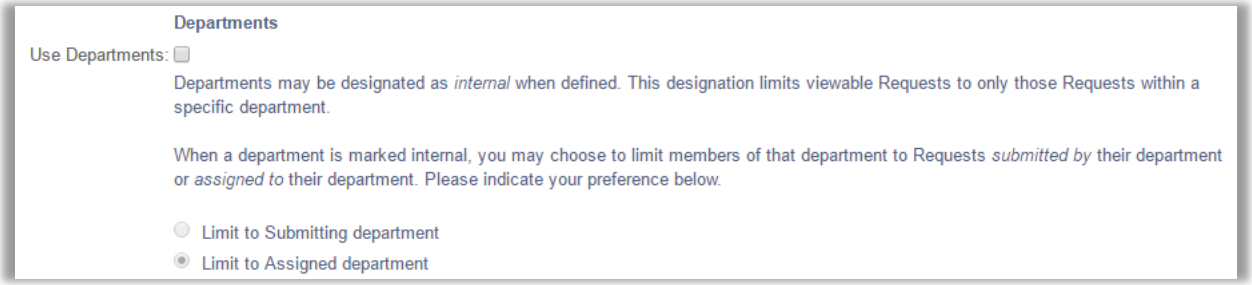
Organizations and Departments each have an optional value of "internal" that can be set. When the entity is marked as "Internal", then members of that entity are restricted. Regardless of these settings, a user must have the permission to see other's issues in order to see anything beyond what they play a role in.

### organizations

For Organizations, that means members with the permission to see other's issues can only view *issues submitted by other users of that organization*. If the organization is not marked as internal, it is considered "external," meaning that members can see all the issues and all the users from their own, as well as all other organizations. When organizations are created, they are marked as internal by default. That option can be unchecked when creating or editing the organization information.

### departments

When the optional Department entity is enabled, you have a choice how internal views affect your users. The option "Limit to Submitting department" looks at the submitting user's department, and if a user belongs to that department, then that issue can be seen. The option "Limit to Assigned department" looks at the department of the assigned agent or group, and if a user belongs to that department, then they can see that issue. When departments are created, they are external by default, but this can be changed when creating or editing the department information.



## *user visibility*

The ability to see users in a dropdown list or search is controlled by the same visibility controls. Administrators see all users and can't be restricted. The rest of the users would only see other users if they have the permission to see others' issues or the ability to assign issues or tasks to others. When they have one of those permissions, if they're in an internal organization or department, they only see the users within that entity.

## *exclusive projects*

A Project can be used as an additional visibility control for issues. Every project has the option to be marked as "Exclusive." Any issues associated to an exclusive project are hidden from everyone except administrators and users designated as members of that project.

## *the end result*

There are multiple ways to control the visibility of issues within Issuetrak, and not all of them may be needed in your site. The best results come from using a combination to create a layered structure that meets your company goals. If you have any questions on which options will work best for you, please contact your sales engineer or sales@issuetrak.com.