best practices

issuetrak

user permissions

Permissions control what users can do or access within Issuetrak. With over 50 permissions available, it can be challenging to understand what the separate permissions do and how to best manage them. These guidelines are meant to assist you in managing the permissions for your user accounts.

Your purchased pricing model determines what type of users are available. For the purpose of this document, we will speak to the Support model.

user type

Every user must be designated as either an Agent or an End User. This determines what permissions your users have access to. Certain permissions always require a user to be an agent, while others can be granted to either agents or end users. In the Team pricing model, all users are agents, and there is no end user designation.

permissions, parameters and access rules

Other than Permissions, two other options may control visibility in Issuetrak: parameters and access rules.

- Permissions – Control what each user can do within Issuetrak
- Parameters – Determine whether the user is active, can log into the site and whether the user is a System Administrator (Sys Admin)
- Access Rules – Establish which issues and users can be seen in the site. Access rules are not discussed in this document

user permissions

User permissions break down into three main areas.

- **Agent permissions** – These are always restricted to agents.
    - Can Assign Issues
    - Can Be Assigned Issues
    - Can Assign Next Action
    - Can Be Assigned Next Action
    - Can submit Issues on behalf of other users
    - Can access and maintain Administration functions
    - Sys Admin parameter

  The number of agents allowed is determined by the number of agent licenses purchased. These permissions fall under the “Agent Permissions” section of the permissions list.

- **Services Based** – Control which features (services) can be accessed within the Issuetrak site. This includes access to the Knowledge Base, ability to create Reports, view the Calendar or use the Dashboard
- **Data Access Based** – Control which fields are visible on the issue, which ones may be edited or which private fields can be seen. Included in this would be the permission "Can view issues submitted by other users", which allows access to issues the user did not submit or enter.

For a complete list of the permissions and what they do in the site, please consult the Administration Guide included with your installation or in Knowledge Base article 62 on the Support site.

granting permissions

Users do not need permissions to exist in the Issuetrak database. Some users are not allowed to log in, so no permissions are needed, but their profile by default must at least include the menu option "My Issues".

These are the methods to create a user:

- Manually add under Administration > Users > Add
- Clone an existing user under Administration > Users > Clone
- Add as a "New Caller" from the Submit screen by a user with "Can Submit on Behalf of Others" permission
- Use the "Register Now" link when Self Registration is enabled
- Create automatically by Incoming Email when emailing in an issue
- Log into the site to synchronize against or be included with a scheduled import from Active Directory using the Active Directory Module.

Users added manually have permissions set by the Administrator when creating the user. Cloned users inherit all the permissions from the original account being cloned. All other users receive their permissions by using pre-created templates. Templates normally have "end user" as the user type, then permissions granting only the most basic rights, such as the ability to submit an issue, and access to the Knowledge Base. The templates are created and controlled by the Administrator of the site.

With most users only having the most basic set of permissions, additional permissions are granted to users using groups. Groups allow you to grant permissions and the agent designation to multiple users at the same time. A group has the same permission options as a user. When a user belongs to a group, they inherit all the permissions from the group. If the group has the agent designation, all users in that group are counted as agents. If a user belongs to more than one group, the user inherits all the permissions from all groups. Cloning a user also clones group memberships.

special accounts

- **System Administrators** – a designated agent user with the parameter “Sys Admin” is granted almost all permissions by default. However, to assign issues or tasks to this user, you will need to grant them the specific permissions to be assigned issues or tasks. A System Administrator has unlimited access to every area of the site and can change system-wide settings. No restrictions set within the site apply to the System Administrator.

- **Admin/Administrator users** – a designated agent user with the permission “Can Access and maintain Administration Functions”. These users have the same default permissions as System Administrators except they are not allowed access to the “System Settings” portion of the Administration menu. This prevents them from making changes that enable or disable features and functionality within the site. As with System Administrators, no restrictions set within the site apply to Administrators.

best practices

Define your groups to match the roles your users will have in your site. Customer, End User, Technician, Customer Service Rep, Administrator, Managers, Supervisors, Help Desk, and Service Desk are common examples.

Grant as few permissions as possible to the individual user account. It’s recommended to grant only “My Issues” to the individual user and let the groups control all other permissions.

If you are manually creating new users, it helps to clone existing users. By cloning an account, the permissions and group memberships are brought over to the new account. This allows users with similar functions have the correct permissions with little overhead.

Use a good naming convention for templates. It’s suggested to give a template the last name “Template”. This allows for easier searching and identification.

Active Directory set ups need to only use one template for all users. Additional permissions should be granted through Issuetrak groups.

There are two permissions that reference read only access: “Allow Read Only access to Administration information” and “Allow Read Only access to Asset Management information”. These permissions allow users to view the specified areas, but not to add, edit or delete values. However, if mixed with “Can access and maintain Administration functions” or “Can access and maintain Asset Management Module functions”, then the ability to change any information is overridden. These are the only cases where permissions contradict one another. Conflicting permissions cannot be set on the individual user account, but could be inherited by membership in two separate groups.

This is only meant to be a general guideline about managing user permissions within Issuetrak. Please contact us at proservices@issuetrak.com if you have any questions.