How can I set up agent permissions, permission groups and department access?

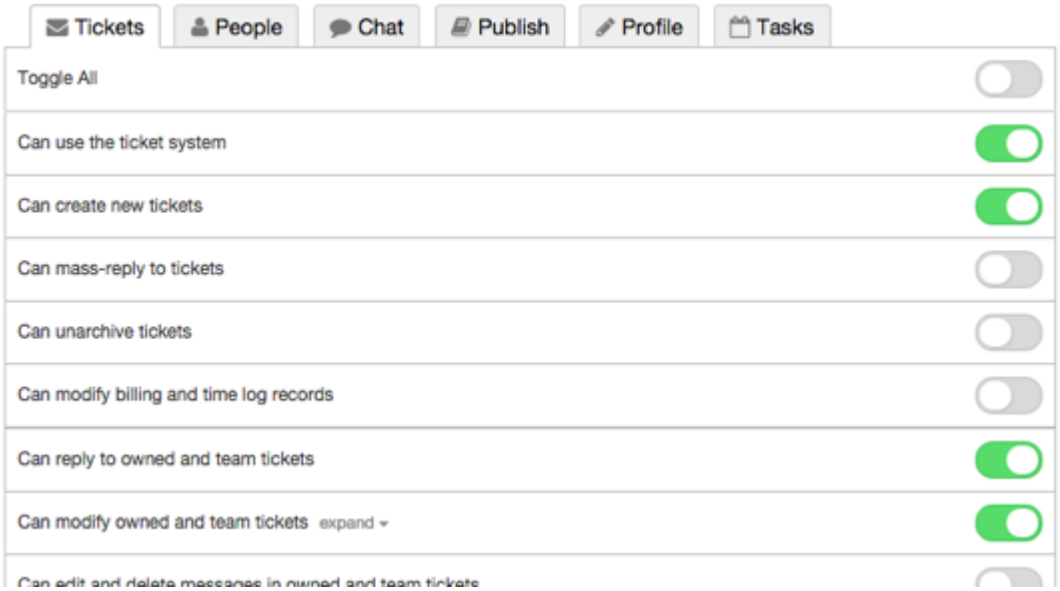
Ben Henley - 2024-02-07 - Sylwadau (0) - Deskpro Legacy

The Deskpro agent permissions system is designed to give admins fine control over what agents can see and do on the helpdesk. In this article, we'll explain how to quickly set up the permissions you need for various different situations.

Basic concepts

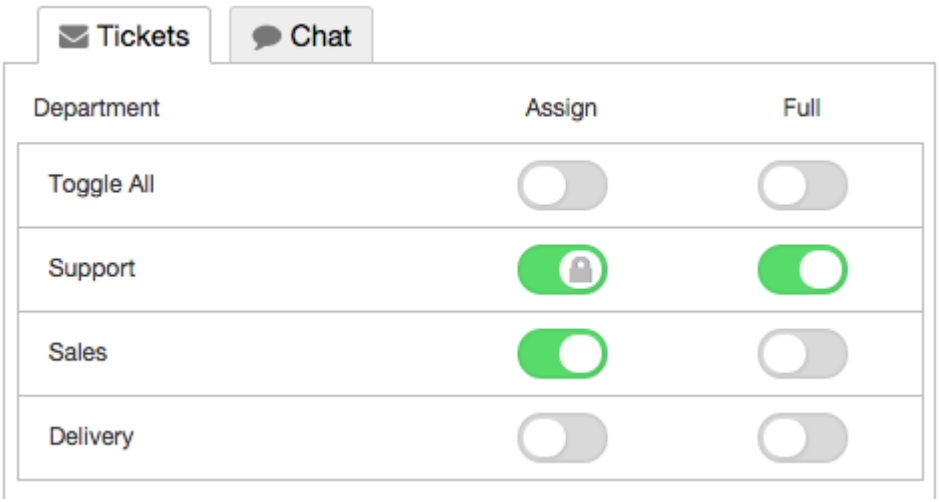
Each agent account has a set of permissions which grant access to different functions.

In the **Agents** section you can grant permissions to each agent individually:



Agents also have department permissions. There are two levels of department permission:

- **full** permission means that you can see tickets in a department
- **assign** permission means that you can assign tickets to the department, but not see them afterwards



Because this agent has full permission for the Support department, you can't disable the assign permission, so it is locked.

To save time, you can use **permission groups** to grant permissions to multiple agents at once. A permission group stores a set of permissions, and when you add an agent to the group, the agent is granted all those permissions. You can add an agent to more than permission group.

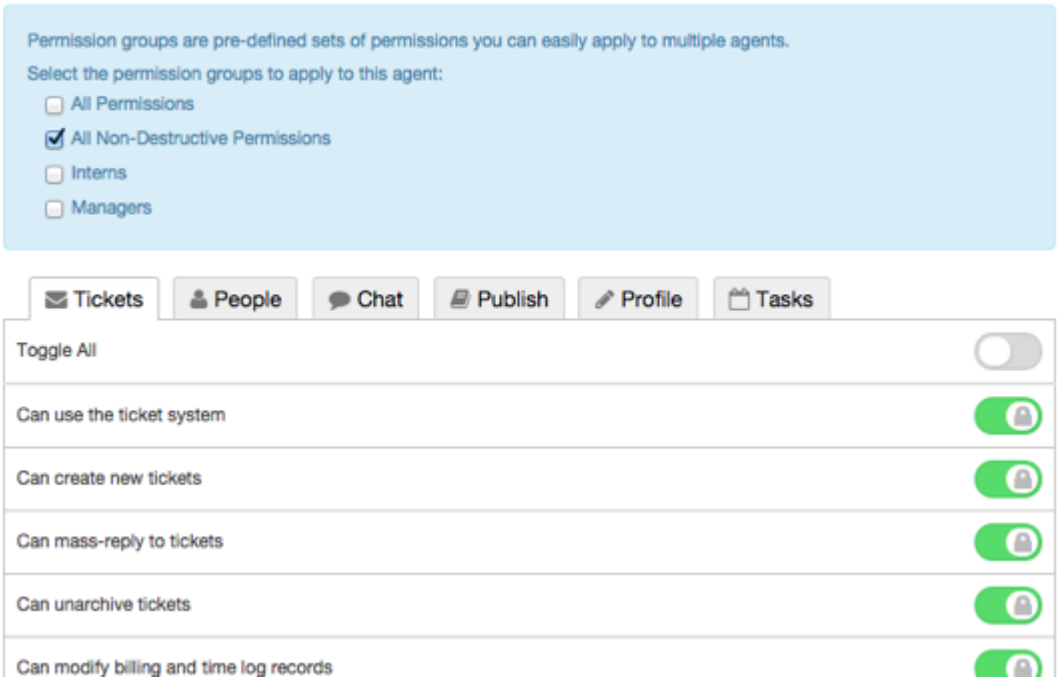
There are built-in groups for All Permissions and All Non-Destructive Permissions, and you can also create your own permission groups from **Agents > Permission Groups**.

Permissions are additive

The key concept to remember is that **permissions are always additive**, whether you grant them through the agent's individual account or by adding the agent to a permission group.

If you add an agent to 3 different permission groups, they will have *every* permission that is granted by *any* one of their groups.

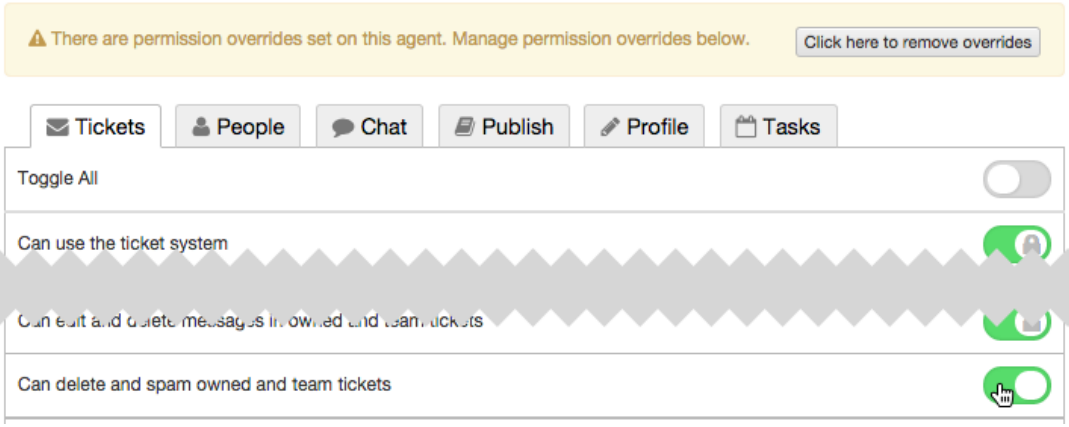
You can't take away a permission on an agent's individual account that's been granted from a permission group. For example, here's the profile of an agent who's a member of the **All Non-Destructive Permissions** group.



The permissions granted through the group are shown as locked; you can't remove them individually (because permissions are additive) - so if you wanted this agent not to be able to create new tickets, you'd have to remove them from the permission group altogether.

However, you can *add* extra permissions to an individual agent's account. Because it's not granted through a permission group, it's considered a **permission override**.

For example, this agent is a member of the **All Non-Destructive Permissions** group, which doesn't grant the *Can delete and spam owned and team tickets* permission. You can add that permission as an override.



Managing permissions with only a few agents

The point of permission groups is to make it quicker to edit large numbers of agents.

If you only have a few agents who need widely different permissions, there is no need to set up permission groups. It's quicker just to edit permissions on each agents' profile.

If you have a small number of agents who all need the same custom permissions, you could add them all to the same custom permission group. That way, if you decide to change your permissions policy, you can change all of them at once.

Removing a permission that's granted through a built-in group

Suppose you initially chose to give every agent **All Non-Destructive Permissions**. Later, after an unfortunate incident, you decide you don't want to allow them to make mass replies to tickets.

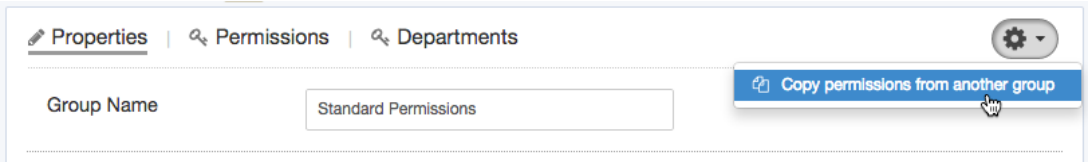
You can't simply disable the *Can mass-reply to* tickets permission in the **All Non-Destructive Permissions** group, because it's built in.

The quickest way to remove the unwanted permission is to make a clone of the **All Non-Destructive Permissions** group.

1. Go to **Agents > Permission Groups** in the admin interface.

2. Click **Add**.

3. Create a new group and use the gear control to **Copy permissions from another group** - in this case, the **All Non-Destructive Permissions**.



4. Save the new group.

5. Now remove all agents from **All Non-Destructive Permissions**, and add them to the new group.

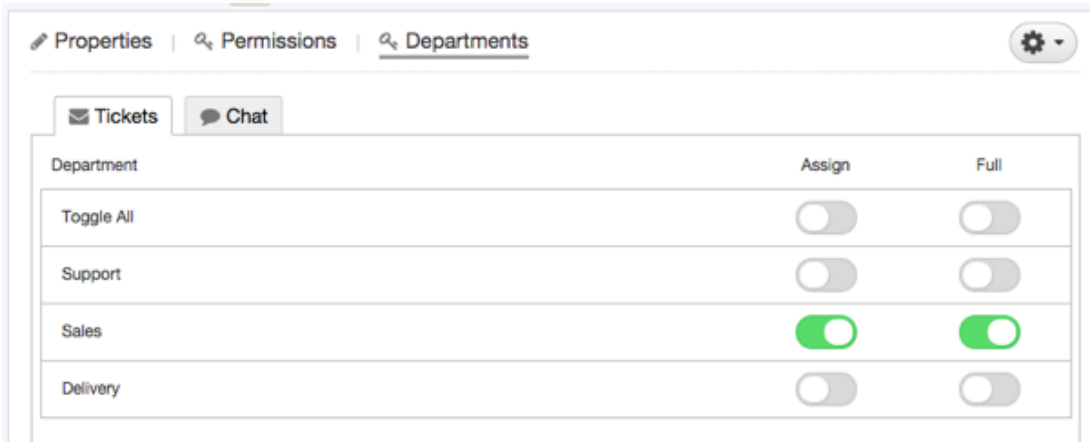
Separate permission levels and department access

Suppose your helpdesk is divided up like this:

- different agents may need access to one or more of three departments: Sales, Support and Accounts
- agents include:
    - trainees who need limited permissions
    - standard employees who need more permissions
    - managers who need all permissions.

Clearly, it's impractical to make groups for Sales Trainee, Support Trainee, Accounts Trainee, Sales & Support Trainees etc.

A better way to implement this would be to set up a "Sales Dept Access" permission group that *only* grants Sales department access, and nothing else:



then do the same for the Support and Accounts departments, etc.

Then set up a Trainee permission group, a Standard permission group and a Managers permission group.

This lets you apply permissions like this:

