Configuring permissions securely

Permissions allow you to **control access** to the particular sections of the Kentico administration interface by users. To learn how the whole system wor

- User types
- Impersonation
- Permissions and UI elements
- Roles
- Memberships
- Access control lists
- Special permissions - the special permissions include Edit ASCX code, Edit SQL code and Edit SQL queries.

The rule of thumb here is to **assign the least privileges possible**. You should only grant permissions to users who really need to perform the particula

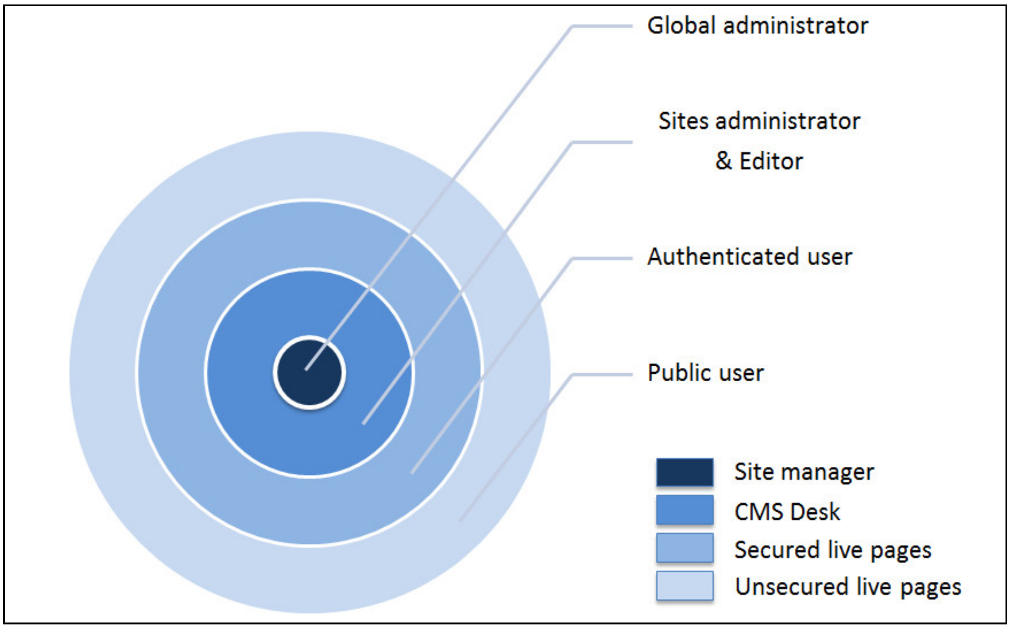
User types

Kentico CMS has three different user interfaces:

- **Live site** - front end for site visitors.
- **CMS Desk** - administration of one certain site. The place where content is edited.
- **Site manager** - administration of the whole CMS platform. The place where sites are managed.

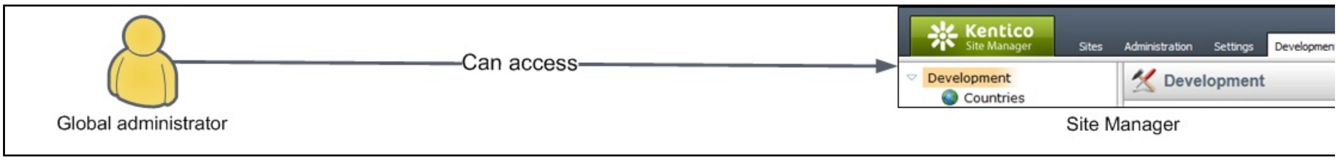
Kentico CMS divides users on the following levels:

- **Public user** - has permissions to see live unsecured resources (pages, documents, images …) on the live site, represents a site visitor who h
- **Authenticated user** - a logged in site visitor, can see some secured resources on the live site (depending on assigned roles).
- **Editor** - has access to CMS Desk on the assigned sites.
- **Sites administrator** - has access to CMS Desk on all sites within the system. The site administrators can manage all objects of all sites but d
- **Global administrator** - has access to Site manager. User with all permissions.

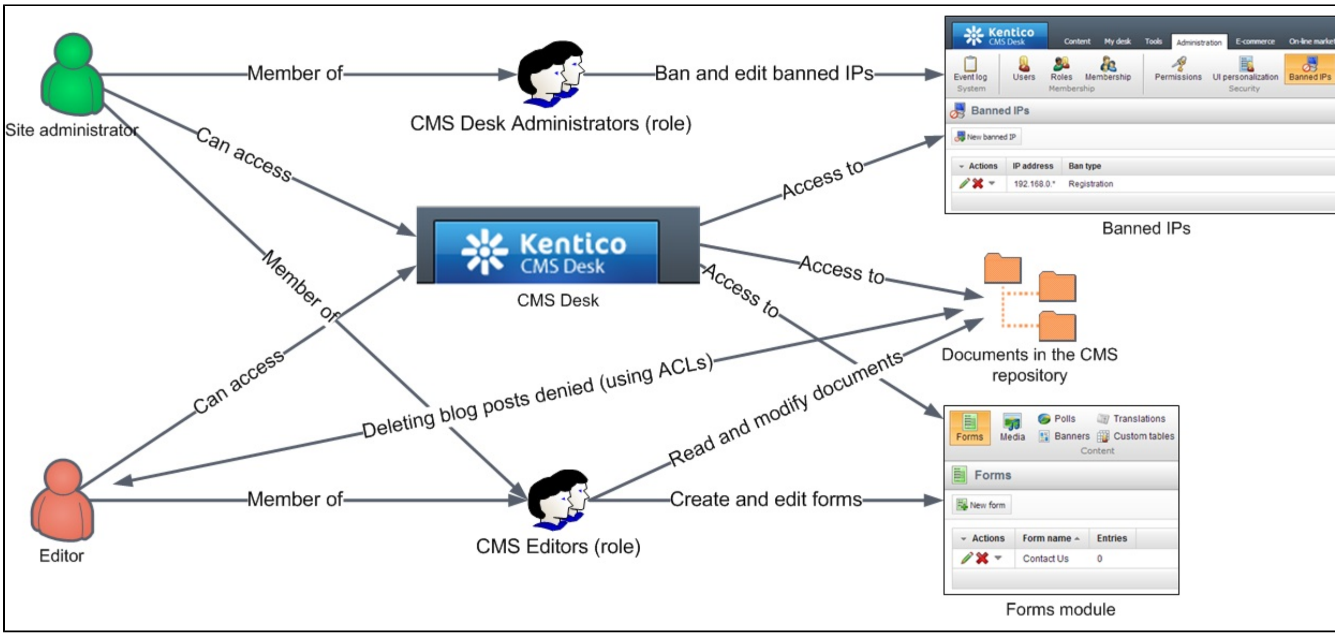


The Public user, Sites administrator and Global administrator user types have permissions determined by their user level. The other two types, Authent

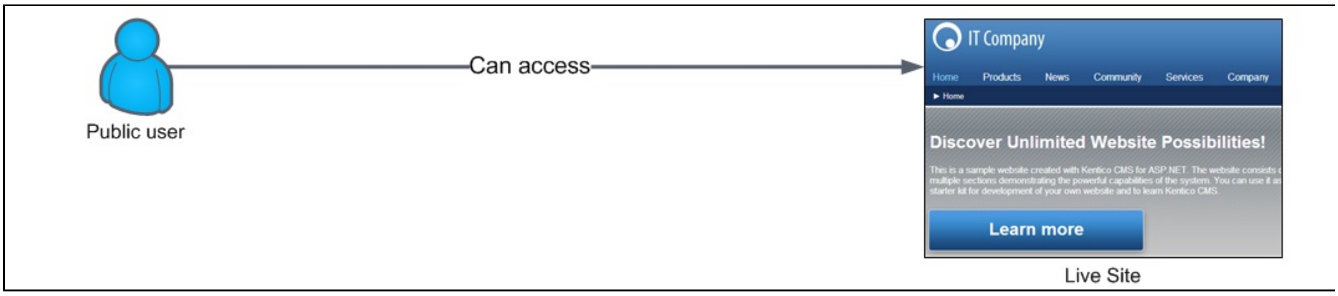
Global administrator is the only one who can access Site Manager.



Users who want to access CMS Desk (and see the content) must have the **Is editor** option checked in **Site Manager -> Administration -> Users -> e** users' needs.



Public users (users who are not global administrators nor editors) can access only the Live site.



Impersonation

Global administrators can sign in to the system as other users. This allows them to view the user interface from the users' perspective.

Due to the security reasons, only the global administrators can impersonate other users. Additionally, it is not possible to impersonate other global adm

On this page

In this section

Related pages

- User management
- Role management
- Managing memberships
- Permissions overview
- UI Personalization

Permissions and UI elements

Permissions for the whole system can be managed in one place in the **Administration** interface. They are role based – you cannot assign specific peri
There are two types of permissions:

- **Functional (permissions)** - permission check is done after the user performs an action. If the action is not permitted, an error message is sho
- **Visual (UI elements)** - permission check is done during the page rendering. If a certain action is not available, the corresponding action buttoi

There are two standard permissions – read and modify (manage). Also, many modules have their own specific set of permissions for better granularity
roles" which allows a given role to add or remove a user from/to a role.

> To allow roles to modify documents and other parts of the system, you need to assign them both the **read** and **manage** permissions.
>
> If you assign only the **manage** permission to a role, then this role will not be allowed to view the specified pages.

There are also modules, for example the Forum module, where you can specify a special set of permissions directly in the module's configuration and e
have access to the Administration interface (CMS Desk).

> ⚠ Be careful when assigning permissions, as some permissions can have other security implications. For example, you should assign the **Manag**

Roles

Each user can belong to any number of roles, their relationship is N:M. The roles are related N:1 to sites, every role belongs to a certain site.

You can learn how to manage roles in the Role management topic.

Memberships

Memberships group existing roles together, forming another security layer. Memberships are intended to be used mainly in the E-commerce module.

You can learn how to manage memberships in the Managing memberships topic.

Access control lists (ACL)

Every document (page) created in Kentico CMS has its own access control list (ACL). In this list you can specify which roles are permitted to read, moc

You can learn how to work with ACLs in the Document-level permissions topic.

Special permissions

The special permissions include Edit ASCX code, Edit SQL code and Edit SQL queries and their settings can influence the possibility of privilege eleva