

Permissions allow you to **control access** to the particular sections of the Kentico administration interface by users. To learn how the whole system works, continue through the following sections:

- [User types](#)
- [Impersonation](#)
- [Permissions and UI elements](#)
- [Roles](#)
- [Memberships](#)
- [Access control lists](#)
- [Special security 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 particular actions.

User types

Kentico has two basic user interfaces:

- **Live site** – front end for site visitors.
- **Administration** – interface for managing the system and editing content, separated into applications.

Kentico divides users on the following levels:

- **Public user** – can see live unsecured resources (pages, images ...) on the live site. Represents a site visitor who has not signed in. Has [privilege level](#) None.
- **Authenticated user** – a signed in user. May see secured resources on the live site (depending on assigned roles). Has privilege level None.
- **Editor** – has access to the administration interface for assigned sites. Permissions are determined by assigned roles.
- **Administrator** – has access to the administration interface for all sites within the system. Administrators can manage all objects of all sites, but cannot use applications that are restricted to global administrators (typically those that affect the entire system, for example *Sites*) or perform certain restricted actions.
- **Global administrator** – has unrestricted access to all functionality in the system.

Public users, Administrators and Global administrators have permissions determined by their [privilege level](#). The other two types, authenticated users and Editors, are more flexible and their permissions are determined by their roles.

Users who want to access the administration interface must have at least the **Editor** privilege level. Moreover, they need to have assigned roles with permissions configured according to these users' needs.

Public users (users with the **None** privilege level) can access only the Live site.

Impersonation

Administrators can sign in to the system as other users. This allows them to view the user interface from the given user's perspective. To impersonate other users, edit a user in the **Users** application and click **Log in as this user**.


Due to security reasons, only users with the *Administrators* or *Global administrator* privilege level can use impersonation. Additionally, it is not possible to impersonate other administrators.

Permissions and UI elements

Permissions for the whole system can be managed in one place in the administration interface in the **Permission** application. They are role based – you cannot assign specific permissions to users directly, you always need to **assign the user to a role** and then give the role certain permission(s). 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 shown in the interface.
- **Visual (UI elements)** - permission check is done during the page rendering. If a certain action is not available, the corresponding action button/link is not rendered and the user doesn't see it in the interface.

There are two standard permissions – read and modify (manage). Also, many modules have their own specific set of permissions for better granularity or for better handling of special scenarios. For example, the Users module has the special permission “Manage user roles” which allows a given role to add or remove a user from/to a role.

 To allow roles to modify pages 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 even from the live site. It is assumed that these modules will be managed directly by Authenticated users who don’t have access to the administration interface.

 Be careful when assigning permissions, as some permissions can have other security implications. For example, you should assign the **Manage user roles** permission (from the Users module) only to a role with properly instructed users.

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 solution.

You can learn how to manage memberships in the [Membership management](#) topic.

Access control lists (ACL)

Every page created in Kentico has its own access control list (ACL). In this list you can specify which roles or users are permitted to read, modify, create, delete or destroy (delete permanently) the current page or its child pages.

You can learn how to work with ACLs in the [Page-level permissions \(ACLs\)](#) 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 elevation attack. Find more information in the [Special security permissions](#) topic.