IP banning prevents users with specified IP addresses from using your website. Kentico provides several levels of IP address banning:

- **Access to the website** - users with the specified IP address cannot access the site at all.
- **Login** - users cannot log in to the site.
- **Registration** - users cannot register on the site.
- **All user actions** - users can enter the site, but they are not allowed to register or log in, and they are not allowed to add any content to the site (e.g., blog comments, board messages, etc.).

How IP banning works

In the **Banned IPs** application, you can specify, which addressed will be banned. When typing an IP address, you can use the asterisk (*) wildcard character to cover a range of IP addresses (for example, 192.168.0.*).

If a user has the **Access to the website** ban type, then the user gets redirected when trying to access your website. Other IP ban types are handled by individual parts of the system. The user gets usually informed about not being able to complete the given action (log in or register).

The IP address is provided by the HTTPHelper.UserHostAddress property, which is a value either set in the system, or obtained from the .NET (HttpContext.Current.Request.UserHostAddress).

When you ban an IP address globally, you have an option to **Allow sites to overwrite the ban**. This way, the site administrators can cancel the global ban (using the **Allow IP address for this site if the IP address is banned globally** option) on their sites.

Banned IPs integration

If you want to integrate the IP banning into your own code or modules, use the *BannedIPInfoProvider.IsAllowed* method:

```
using CMS.Protection;
using CMS.SiteProvider;

...

// Checks if the client IP address (from HttpContext) is completely banned for the
current site
if (!BannedIPInfoProvider.IsAllowed(SiteContext.CurrentSiteName, BanControlEnum.
Complete))
{
        ...
}
```