We recommend that you only allow users to access the file system directories that they actually need. This means that you should forbid access to directories for all users that do not need them.

You can configure directory restrictions in the project's web.config file. The following example **forbids access** to the *CMSSiteUtils* directory according to the configuration of the **<authorization>** element. See the Security Authorization article for more information about the available options.

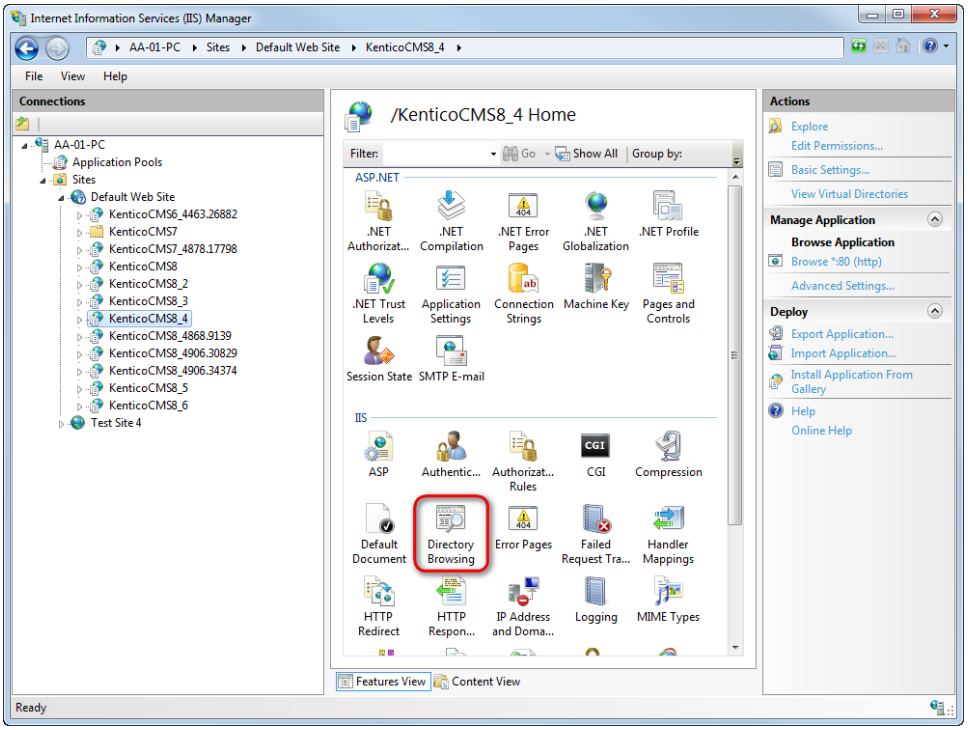
```
<location path="CMSSiteUtils">
    <system.webServer>
        <security>
            <authorization>
                <remove users="*" roles="" verbs="" />
                <add accessType="Allow" users="" roles=""/>
            </authorization>
        </security>
    </system.webServer>
</location>
```

The *CMSSiteUtils* directory contains export files and is therefore the most vulnerable and must be protected properly.

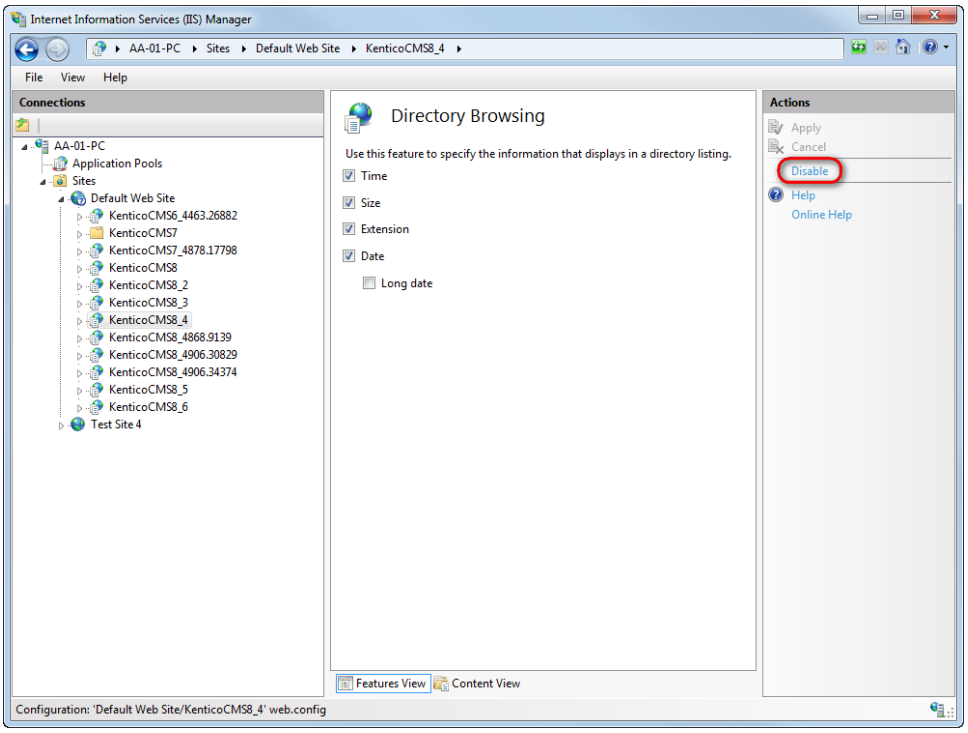
## Disabling directory browsing

Another important security precaution is to disallow listing of files in directories. This can be set in the IIS (and should be already set as default configuration). It is recommended to disable directory listing for the whole website, although you can also disable this feature only for individual directories. In such case, do not forget to disable directory browsing for the CMSSiteUtils directory.

1. Open the IIS Manager.
2. Select the project for which you want to disable the listing of files.
3. Double-click the **Directory Browsing** icon in the IIS section.



4. Click **Disable**.




Now it is not possible to list files in directories on your website.

## Disabling unnecessary execution of scripts

You should forbid the execution of scripts where it is not required. This mainly applies to directories with multimedia or directories where you allow uploading of images. This can be set in the IIS, see Edit Feature Permissions for the Handler Mappings Feature (IIS 7) for instructions.

## Keeping the web servers clean

The server where your web presentation is located should not contain any other unnecessary data. It is not wise to store any sensitive information there (e.g., database exports).

## CDN and external storage

In Kentico, it is possible to store data to Azure blob storage and Amazon S3 storage. Both can be configured to allow public access so that anyone can download files, which were stored in Kentico.

The thing is that, to enable distribution of data over CDN, you need to **enable public access** to these data. This can pose a security risk, as you do not usually want everyone to be able to download all files from these storages. Therefore, you can set only certain containers (Azure blob) and buckets (Amazon S3) to be publicly available.

You can find more information in Configuring file system providers.