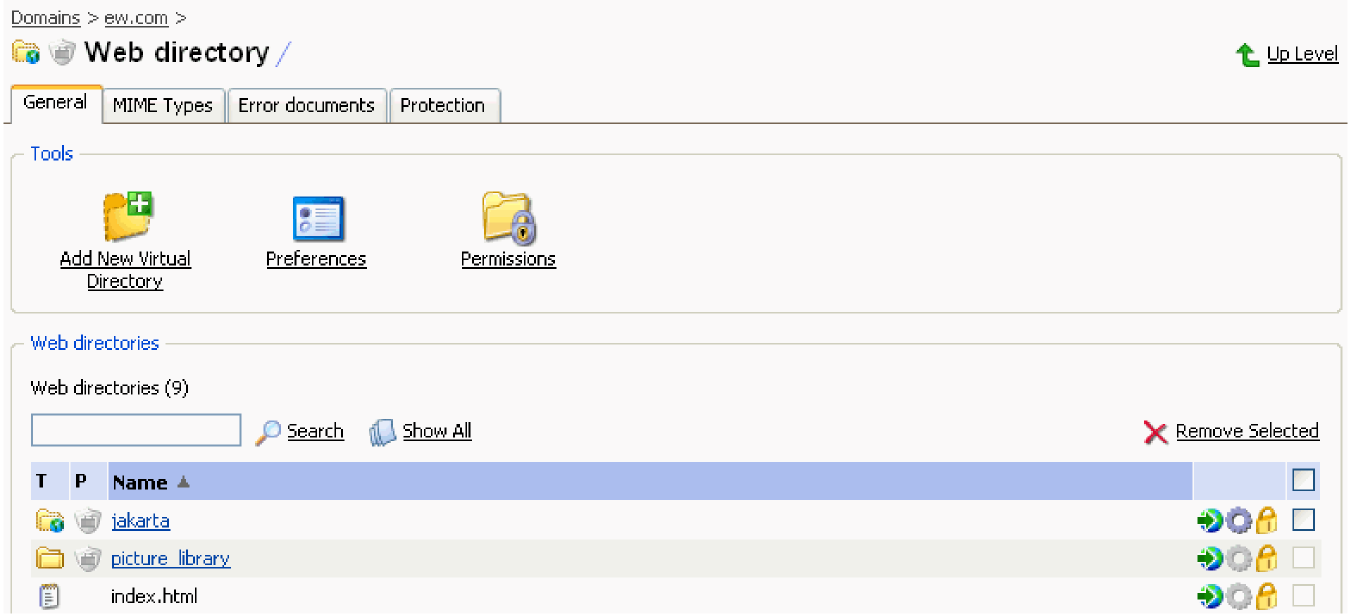
How To Manage Windows Permissions In Plesk

This article contains information about managing web directories in Plesk

Plesk allows you to see the directories of your domain the way they are seen from the web and manage their protection and settings. Generally, there are two types of directories, physical and virtual ones. Physical directories are the actual directories present on the server's hard drive while virtual ones are only abstraction, a kind of links to the existing physical directories. Therefore, virtual directories are not visible in regular file manager but you can see and manage them on the Web Directories screen at the Domain Administration page.



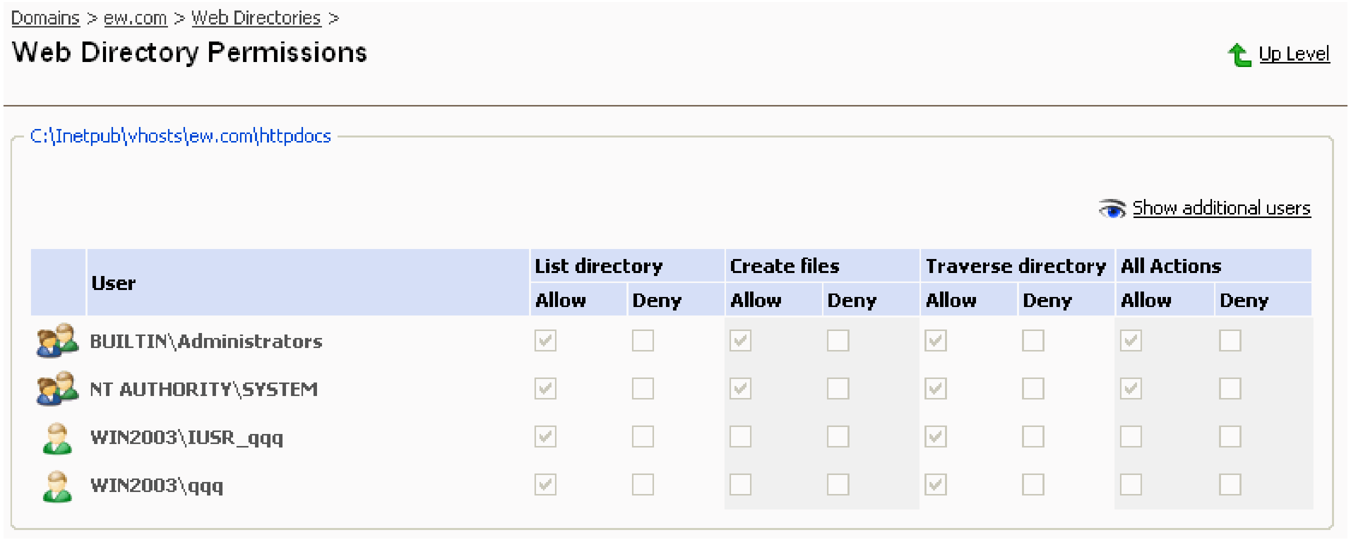
Web directories (9)

T	P	Name ▲		□
		jakarta		□
		picture_library		□
		index.html		□

Further, URLs for directories may be protected and unprotected. Everybody can access unprotected URLs, while only privileged users can access URLs with protection.

Managing Web Directory Permissions

Plesk allows setting up permissions for a web directory; this way you control what types of actions different uses can perform with the directory. To manage permissions of the current web directory, click the Permissions button on the General tab. The following page will open:



Domains > ew.com > Web Directories >

Web Directory Permissions

C:\Inetpub\vhosts\ew.com\httpdocs

User	List directory		Create files		Traverse directory		All Actions	
	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny
BUILTIN\Administrators	☑	□	☑	□	☑	□	☑	□
NT AUTHORITY\SYSTEM	☑	□	☑	□	☑	□	☑	□
WIN2003\IUSR_qqq	☑	□	□	□	☑	□	□	□
WIN2003\qqq	☑	□	□	□	☑	□	□	□

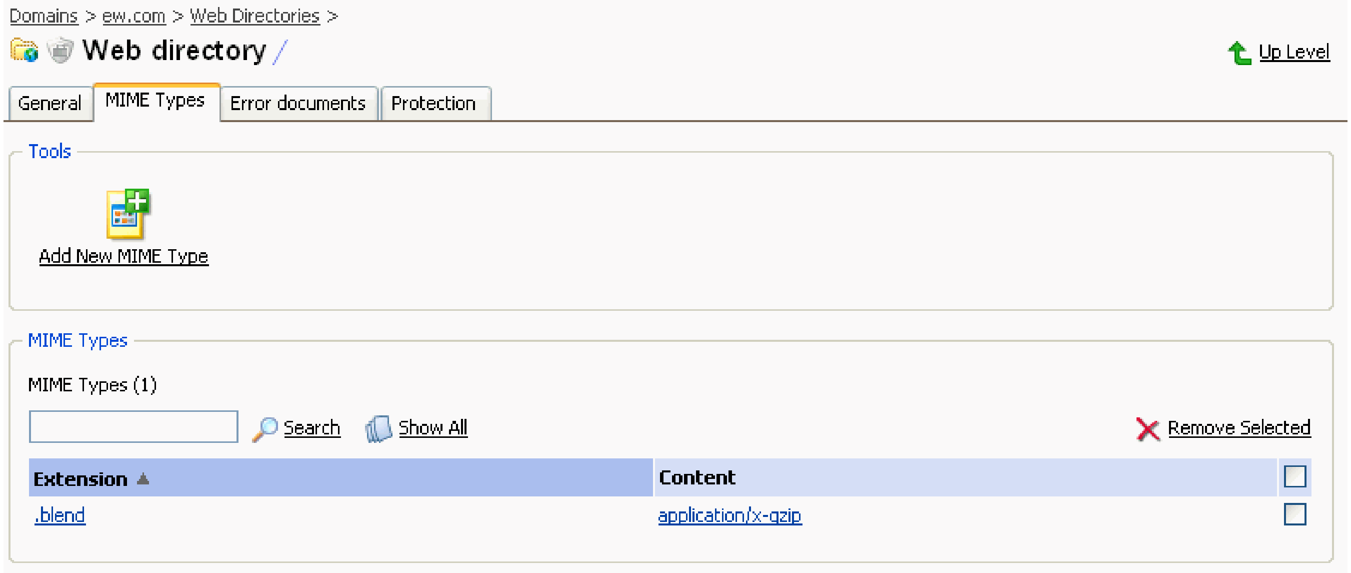
- When setting permissions for folders: using the appropriate checkboxes, allow or disallow users to view the folder and its contents, to create files within the directory, and to traverse the directory. You can also select appropriate checkboxes in All Actions column if you want to allow or deny all operations for the given user/user group.
- When setting permissions for files: using the checkboxes, allow or disallow users to read and write to the file, and define permissions for file execution. You can also select appropriate checkboxes in All Actions column if you want to allow or deny all operations for the given user/user group.

Select the Show additional users checkbox for users with non-defined access rights to be shown in the list, so that you could grant them appropriate rights.

Click OK to submit your changes or click Cancel to discard all changes and return to the previous page.

Managing MIME Types

To set up MIME types for the current web directory, go to the MIME Types tab. The following screen will appear:



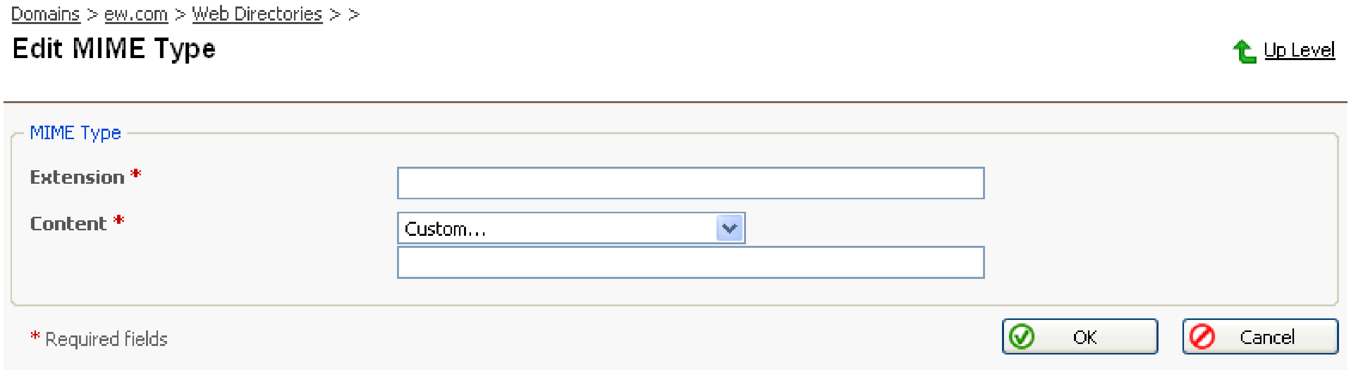
Extension ▲	Content	□
.blend	application/x-gzip	□

Multipurpose Internet Mail Exchange (MIME) types instruct a Web browser or mail application how to handle files received from a server. For example, when a Web browser requests an item on a server, it also requests the MIME type of the object. Some MIME types, like graphics, can be displayed inside the browser. Others, such as word processing documents, require an external helper application to be displayed.

When a web server delivers a Web page to a client Web browser, it also sends the MIME type of the data it is sending. If there is an attached or embedded file in a specific format, IIS also tells the client application the MIME type of the embedded or attached file. The client application then knows how to process or display the data being received from IIS.

IIS can only operate files of registered MIME types. These types could be defined both on the global IIS level and on the domain or virtual directory level. Note that globally defined MIME types are inherited by all the domains and virtual directories while ones defined on the domain or virtual directory level are used only for the area where they are defined. Otherwise, if the web server receives request for a file with unregistered MIME type, it returns the 404.3 (Not Found) error.

To add a new MIME type, click on the corresponding icon. To edit an existing type, click on its name in the list at the bottom of page. The following screen will appear:



Extension *

Content * Custom...

* Required fields

In the Extension box, type the file name extension beginning with a dot (.), or use a wildcard (*) to serve all files regardless of file name extension.

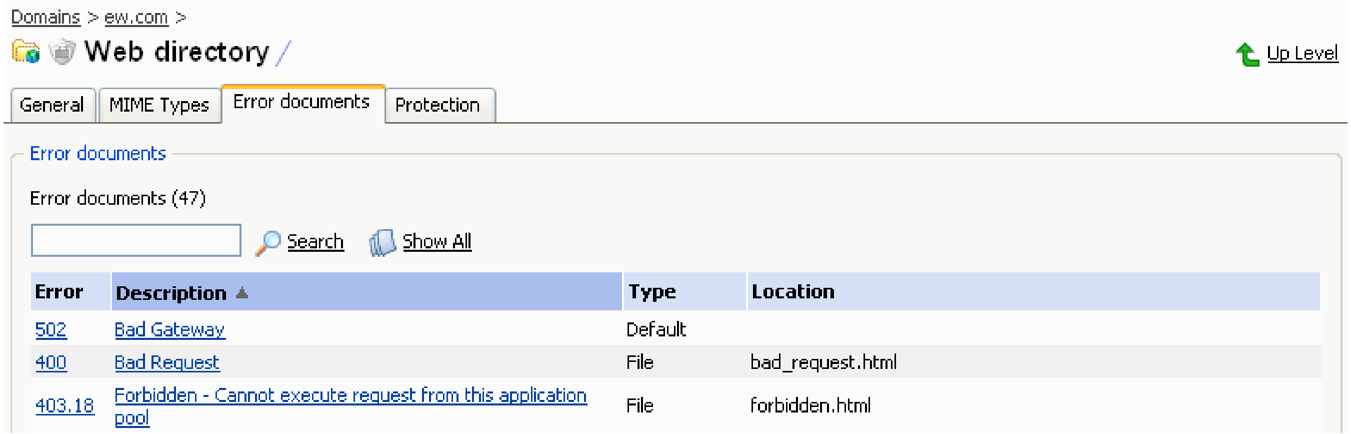
Specify the file content type in the Content box. You can either select the appropriate value from the list or define a new content type. To do this, select Custom... and enter the content type in the input box provided.

Click OK to submit your choice.

Managing Custom Error Documents

Plesk allows managing error documents sent to clients in cases of web server errors. The error codes are standardized in the HTTP protocol. For each error type you can either leave the default error document or replace it with the custom one.

To set up custom error documents, go to the Error Docs tab. The following screen appears:

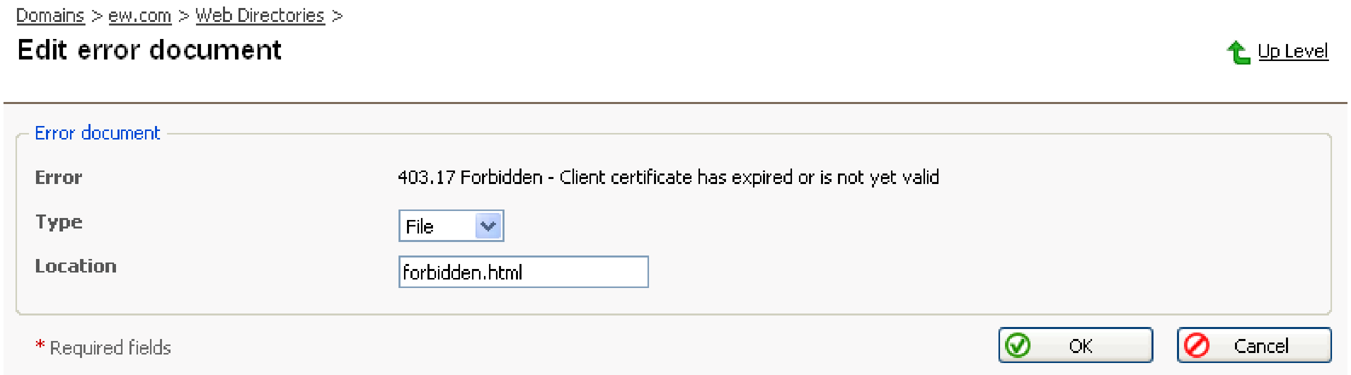


Error documents (47)

Error	Description ▲	Type	Location
502	Bad Gateway	Default	
400	Bad Request	File	bad_request.html
403.18	Forbidden - Cannot execute request from this application pool	File	forbidden.html

The changes made on this screen affect only the current directory and all of its subdirectories.

All HTTP errors for which you can change the error page are listed in the Error docs list. To view the current settings for an error or change them, click on the error's name or number. The Edit Error Document page will open where you can change the default error document for the chosen type of error to your own one.



Error	403.17 Forbidden - Client certificate has expired or is not yet valid
Type	File
Location	forbidden.html

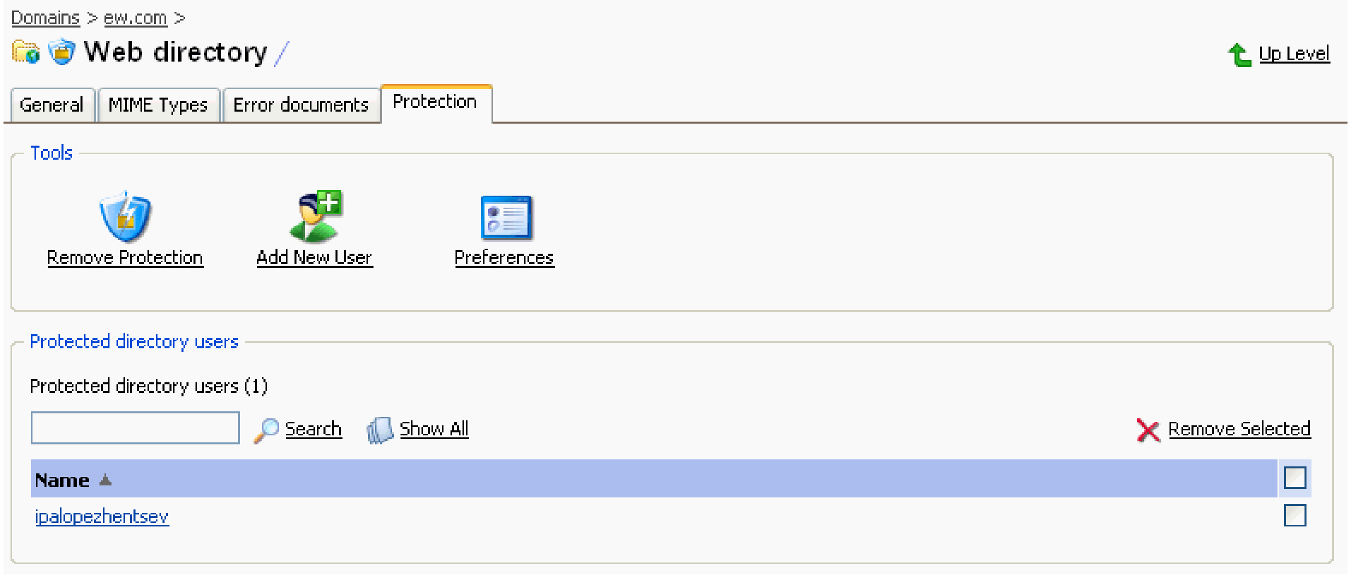
* Required fields

The Error label contains the standard error number along with its description.

The Type drop-down list contains two items: Default and File. When it is set to Default, the default IIS documents are used and the Location field below is inactive. To force server to show your page instead of the default one for the selected error type, select the File option in the Type drop-down field and type the name of the desired HTML document in the corresponding field. The error documents should lie in the errordocs directory and the Location field should only contain the name of document, e.g. 404.html.

Managing Protected URLs

Plesk allows setting protection on a URL for a web directory, which means the URL will be accessible only by users allowed to do so. You can protect both physical and virtual folders. To manage URL protection of the current directory, go to the Protection tab. The following screen will appear:



Protected directory users (1)

Name ▲	□
ipalopezhentsev	□

To protect the URL for the current directory, press the Protect button. Now you can start adding users which will have access to it. To do this, press the Add New User button. A new screen will open where you will have to specify new user's name and password. When the user tries to access the protected URL via browser, a window opens where user should enter his/her name and password.

Click the Preferences button to set up the current protected URL's settings.

The list at the bottom of page shows all users which have permission to access the URL. You can click on user's name to change its password.

If you want to disable URL protection for the current directory, press the Remove protection button.

Related articles

Content by label

There is no content with the specified labels