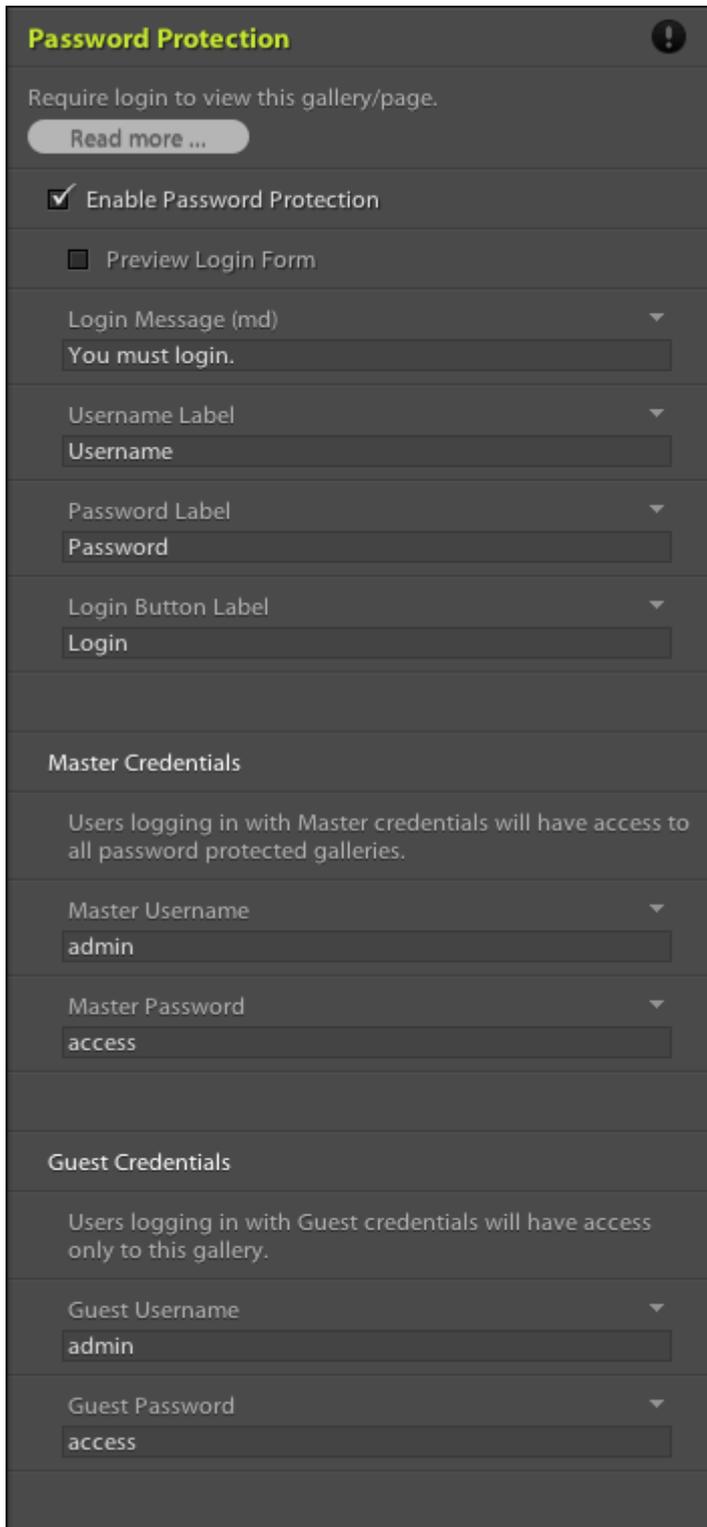


Password Protection

Some CE4 plugins include password protection features. These plugins are:

- CE4 Auto Index
- CE4 Gallery
- CE4 Stage

In these plugins, password protection is enabled using options in the **Output Settings** control pane, pictured below.



To enable password protect in an index or gallery, or in an index or gallery template for CE4 Publisher, you must tick the **Enable Password Protection** checkbox.

To preview the login screen in Lightroom's Web preview, tick the **Preview Login Form** checkbox and refresh the preview. Disable the **Preview Login Form** checkbox to return to the normal gallery view and resume setup.

Enabling password protection will cause galleries to export as PHP documents. PHP documents must be run in a web server environment and cannot be viewed from the desktop, or using Lightroom's "Preview in Browser" feature.

Master Credentials

Users logged in as **Master** will have access to all protected galleries on your website.

Master credentials are intended for use by the site administrator (that's you), so that the website may be browsed freely without the need to memorize numerous, individual client logins for gallery access.

Master credentials should not be shared with clients.

Guest Credentials

Users logged in as **Guest** will only have access to specific galleries or gallery indexes into which they have logged in directly.

Guest credentials are intended for use by clients.

Setting Passwords in TTG CE3 Publisher

See CE4 Publisher documentation ...

Logging Out

There are two ways to terminate a login:

- Upon quitting the web-browser, login credentials will be lost. The next time the browser is launched and protected galleries are accessed, the user will be prompted for login.
- A gallery may be logged out of by appending `?logout` to the end of the gallery URL, i.e.
`http://yourdomain.com/image-gallery/?logout`,
`http://yourdomain.com/image-gallery/index.php?logout`, etc.

You may create a logout hyperlink in your gallery navigation or in “the block” content, targeting the the page using relative URL.

Hyperlink target for a link in site navigation:

```
./?logout
```

Markdown syntax for block copy:

```
(Logout) [./?logout]
```

HTML syntax for block copy:

```
<a href=" ./?logout">Logout</a>
```

Security Through Obscurity

CE4 plugins use low-security, script-based password protection. *Script-based* means that protection is run *on the page*, and therefore can only protect what is *on the page*. Protection does not extend to your gallery's `/photos/`, `/thumbnails/` or `/resources/` folders, the contents of which can still be accessed directly by URL.

Because these assets can only be accessed by direct URL, however, an infiltrator would need first to know of the assets' existence, and then would also need to know both the name and location of specific assets. This is known as "security through obscurity".

If you wish to implement stricter security measures, then you will need to implement security at a server level. Such is beyond the scope of CE4 plugins. Contact your host or reference your host's knowledge base on how to do that. We recommend against using server-side password protection for galleries, however, as blocked access to your image galleries will also prevent the auto index from accessing thumbnail images for gallery index pages.

Security through obscurity can be aided by using `.htaccess` directives to block access to directories on your server containing images. For example, visitors targeting your `/photos/` folder would see a "Forbidden" error, rather than the server listing folder contents for download. The directive is:

```
<IfModule mod_autoindex.c>  
  Options -Indexes  
</IfModule>
```

For more information on using `.htaccess` directives, see our [.htaccess reference](#).

From:

<http://ce4.theturninggate.net/docs/> - **CE4 Documentation**

Permanent link:

http://ce4.theturninggate.net/docs/doku.php?id=ce4_password_protection

Last update: **2014/07/03 06:24**

