# Troubleshoot WSC Problems


- WSC UI style malformed
- Error 403 when saving the credentials form
- Correct visitor IP when using CloudFlare
- WSC Protect - Edit the Pin Check page style and text

# WSC UI style malformed

> We make no guarantees for the information on this page. You use any commands at your own risk. Please consult a Linux server administrator if in doubt and always take a backup or snapshot before making any changes.

Sometimes when uploading WSC the correct permissions might not be set. When visiting the Addon Modules > WSC the page may be missing its style sheet. This is an indicator that the permissions on the /modules/addons/tickets_credentials folder are incorrect. You can confirm this is the case by pressing CNTRL + SHIF + J to open the console in your browser. If the permissions are wrong you will see 404 or 403 errors in the console.

## WSC File & Folder Permissions

Generally speaking, there are two permissions WSC should use. That is 0644 for files and 755 for folders. This is true for cPanel, DirectAdmin and Plesk. The ownership of the folders should usually also be the account user. If you are using a barebones server with no control panel the same permissions apply but the user of those files should usually be www:data. We have provided a table below of known folder permissions. Correct the permissions on the files and folders to resolve any stylesheet errors.

| | Apache | LiteSpeed | NGINX | CloudLinux |
|---|---|---|---|---|
| cPanel | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account |
| Plesk | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account |
| DirectAdmin | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account | Files: 0644 Folder: 0755<br>Owner: User_account |
| BareBones | Files: 0644 Folder: 0755<br>Owner: www:data | Files: 0644 Folder: 0755<br>Owner: www:data | Files: 0644 Folder: 0755<br>Owner: www:data | Files: 0644 Folder: 0755<br>Owner: www:data |

If using a control panel you can usually change permissions using the in-built file manager. For barebones servers, you would use the CHMOD and CHOWN commands or the find command. Examples are below.

```
# To change all the directories to 0755 (drwxr-xr-x):

find /modules/addons/tickets_credentials -type d -exec chmod 755 {} \;

# To change all the files to 0644 (-rw-r--r--):

find /modules/addons/tickets_credentials -type f -exec chmod 644 {} \;

# Change ownership of the WSC files and folders to www-data:www-data

chown -R www-data:www-data /modules/addons/tickets_credentials
```

# Error 403 when saving the credentials form

This usually happens when your environment is running Mod_Security. Older rule sets trigger a false positive when WSC tries to save the initial tables to the database. To confirm this is the case you can visit the credentials form and you won't see any fields that can be filled out by end users. There are a couple of options to resolve this.

## Disable Mod_Security (Temporarily)

In cPanel you can disable Mod_Security on a per-domain basis. Navigate to the cPanel UI and search Mod_Security. Slide the slider to off and then try to attempt to save the credentials form again. This time if the form saves and you can see the WSC form fields when visiting the credentials form you know Mod_Security was the issue.

## Disable Mod_Security Rule

If you have cPanel and access to WHM you can navigate to the Mod_Security section to see which rule is being triggered. This rule can then be whitelisted and ModSec enabled again.

## Update RuleSet

The latest ruleset can be installed which should resolve this issue. The latest ruleset may not be shipped with control panels like cPanel and updating ModSec rules is beyond the scope of our support. cPanel, Plesk and DirectAdmin provide support for features contained in their respective control panels.

# Correct visitor IP when using CloudFlare

Cloudflare proxies traffic to your origin server. For this reason in your logs and when WSC Protect records IP information in the WSC Protect log, it will record Cloudflare's IP and not the real visitors' IP. To correct this you can use Mod Remote_IP to correct the information we receive from Cloudflare. As this is not a problem with WSC we are unable to assist you with installing Mod Remote_IP but we are providing instructions below. If you use a control panel like cPanel your host or control panel provider should help you install Remote_IP if you are not sure.

## cPanel

cPanel has provided detailed instructions on how to enable Mod Remote_IP. See the post located on the cPanel website. Unfortunately, this does require some technical knowledge. Make sure you can complete this or you could end up with a broken server, If in doubt, ask cPanel for assistance.

## LiteSpeed

If you use LiteSpeed you can log in to the LiteSpeed administration area. Navigate to Server > General > General Settings and tick the “Use Client IP in Header” option. Remember to restart the web server for the new settings to take effect.

| General Settings | | Edit |
|---|---|---|
| MIME Settings | | $SERVER_ROOT/conf/mime.properties |
| Disable Initial Log Rotation | | Yes |
| Server Signature | | Hide Version |
| Hide Error Page Signature | | Not Set |
| Enable GeoLocation Lookup | | Not Set |
| Use Client IP in Header | | Yes |
| External Application Abort | | Not Set |
| Check For Update | | Daily |
| Download Updates | | Yes |
| Administrator Email | | root@localhost |

## Other Systems

Cloudflare provides a range of instructions for other systems. These guides can be found here.

# WSC Protect - Edit the Pin Check page style and text

When 2FA is enabled, WSC will record the user's IP addresses. These are stored in a log that can be seen on the "WSC Protect" tab located on WHMCS client's profiles. It's possible to change the look of the page end users see to enter the PIN code they receive via email. Some people like to change the colour of this page to match their website. Others may need to tweak the page so text is visible correctly. Open up the below file on your desktop or in a file manager. If you are editing the file in your file manager, make a copy first.

```
/modules/addons/tickets_credentials/templates/pinchecker.tpl
```

As of V2.1.1 you also edit this page to change the text that is displayed to end users. We will add language strings in a future version. The default code of the file displays as;

```
div class="row">
   <div class="col-md-12">
      <div class="card panel panel-default card-default">
         <div class="card-body panel-body">
            <form method="POST" action="" role="form">
               <input type="hidden" name="checkpin" value="1">
               <div class="smsmanagerarea" style="background-color: #fff">
                  {if $alert}
                     <div class="alert alert-danger">Invalid PIN, please try to put right PIN to continue
login!</div>
                  {/if}
                  <center><b>It looks like you are logging in to your Dev GB account from an IP address we have
not seen before. We have blocked this login to protect your account. You should have received a random login
code to your registered email address. Please enter the code below to whitelist this new IP and access your
account.</b></center>
                  <br><br>
                  <div>
                     <div class="form-group row">
                        <label for="inputExistingPassword" class="col-xl-4 col-form-label" style="text-align:
right">PIN</label>
                        <div class="col-xl-5">
```

```
                        <input type="password" class="form-control" name="pin" id="inputExistingPassword"
autocomplete="off">
                      </div>
                    </div>
                  </div>
                  <div class="form-group text-center">
                    <input class="btn btn-primary" type="submit" name="save" value="Validate PIN Now">
                    <a class="btn btn-danger" href="logout.php">Logout</a>
                  </div>
              </form>
            </div>
          </div>
        </div>
      </div>
```

- At line 7 you can change the background of the Pin Checker form. Its default is #fff for a white background.
- At line 9 you can change the text of the warning that is displayed when an incorrect pin is entered.
- At line 11 you can change the text displayed explaining 2FA authentication is required.
- At line 22 you can change the text of the buttons on the page.