

KNOWLEDGE BASE · PUBLIC DOCUMENT

Securing your WHMCS: the admin folder, two-step login, file permissions and updates

Choosing the Right Plan

CODE

RLX-MZ-KB-2122

VERSION

v2026.10.16

COUNTRY · LANGUAGE

Mozambique · English

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

<https://www.meu.interweb.co.mz/knowledgebase/2122>



This article is for resellers who run their own WHMCS. WHMCS is another company's product: we neither sell nor resell licences, as explained in **what WHMCS is**. Menu names change from one WHMCS version to the next. **The short answer:** a WHMCS holds your customers' details, your invoices and the key that creates and deletes accounts in WHM. You protect it on five fronts: an **admin folder** with a different name, **two-factor login** for every administrator, a read-only **configuration file**, the **writable folders** moved out of the public area, and **updates** kept current, always with a backup first.

What to protect, and why

Item	The risk if left as shipped
The <code>admin</code> folder	It is the first address bots try. With the default name, anyone knows where the door is.
Administrator accounts	One stolen password opens everything: customers, invoices and the WHM key. Without a second factor there is no second barrier.
The <code>configuration.php</code> file	It holds the database password and the key that encrypts stored data. If it can be changed, an attacker can settle in.
Folders WHMCS writes to (attachments, downloads, compiled templates)	Inside the public area, a file someone uploads can be opened from a browser.
The <code>install</code> folder	Left on the server, it lets the installer run again on top of your install.
An old version	Flaws the maker fixed become public knowledge. Whoever does not update keeps them.

The steps, in this order

1

Take a backup first: files and database, kept outside the account. See **making and keeping your own backup**.

2

Delete the `install` folder if it is still there.

3

Rename the admin folder. Rename it in File Manager and tell WHMCS the new name with this line in `configuration.php` (use your own name):
`$customadminpath = 'a-name-only-you-know';` Bookmark the new address: the old one stops answering.

4

Switch on two-factor login: in **Configuration > System Settings > Two-Factor Authentication**, enable a method and make it compulsory for administrators. Each administrator finishes the setup in their own profile. Do the same on your account with us: **enabling two-factor authentication**.

5

Make `configuration.php` read only (for example 400 or 444), as WHMCS's own health screen recommends. See **file permissions explained**.

6

Move the writable folders out of the public area (attachments, downloads, compiled templates) and, if you like, the `crons` folder. The WHMCS documentation names the configuration line that points to each new place. If you move `crons`, fix the cron job path in cPanel in the same minute: **cron jobs**.

7

Open the System Health screen (in the utilities menu) and deal with whatever it flags as a warning.

8

Update when a new release comes out, after checking your licence covers it and the folder's PHP version is supported. Always update the same way: the WHMCS updater or the cPanel application installer, not both in turn.

Do not lose the second factor without a plan B. Keep the backup codes somewhere other than your phone. And do not keep retrying the password when login fails: repeated attempts can block your IP, and that is no longer WHMCS: **unblocking your IP**.

One person, one administrator. Do not share a single admin account between colleagues. With separate accounts you give each person only the permissions they need, and the activity log tells you who did what.

Think someone got into your WHMCS? Tell us the address and the time, and we will check the server logs on our side.

[Open a support ticket](#)

SEE ALSO

[Installing WHMCS on your account](#)

[The most common WHMCS problems, and what causes them](#)

[File permissions explained: what 755, 644 and 777 mean](#)

[Files that must never be public: .git folders, .env, backups and database dumps](#)

[How to enable or disable two-factor authentication \(2FA\)](#)

[Making and keeping your own backup, and testing that it works](#)



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

Interweb Mozambique

RLX Holdings, S.A. • Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 • CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed