

Manage Sub-Admins

A Sub-Admin is a special Admin account. You can restrict the permissions on different levels (view, edit, delete permissions, or no access) for different sections of the Admin Panel (Users, Domains, Logs, etc.). Furthermore, you can restrict login access to only specific known IPs.

Some examples for using sub-admins are the following:

- API integration - you shouldn't use your main Admin account to authenticate with the API.
- WHMCS plugin - use a Sub-Admin to authenticate your WHMCS plugin
- dividing the work and responsibilities within a team - each team member can have a Sub-Admin

Best Practices

API Integration

For API authentication, you must use an Admin username and password. This is the setup we recommend:

- secure your main Admin account by activating Two-factor authentication. You can continue to use these credentials for Admin Panel direct login and perform actions via the web interface of the Admin Panel.
- create a Sub-Admin for API access only. You can enable only the permissions you integrate with the API or allow unrestricted access.
- secure your API Sub-Admin by restricting login access to specific IPs - these should be the IPs of your servers that connect through the API.
- optional: create other Sub-Admin for your team members that will use the web interface.

WHMCS Plugin

To connect your WHMCS using our plugin, you must authenticate using an Admin username and password. This is the setup we recommend:

- secure your main Admin account by activating Two-factor authentication. You can continue to use these credentials for Admin Panel direct login and perform actions via the web interface of the Admin Panel.
- create a Sub-Admin for WHMCS access only. You can allow unrestricted permissions.
- secure your WHMCS Sub-Admin by restricting login access to specific IPs - the IP of your WHMCS server.
- optional: create other Sub-Admin for your team members that will use the web interface.

Team members

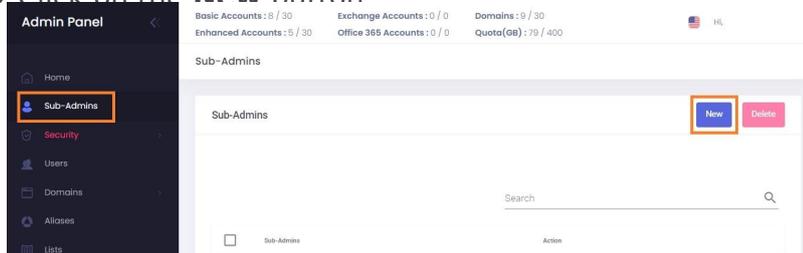
We don't recommend you share the same Admin account with other people, but instead, create a Sub-Admin for each member. This way, you can enable two-factor authentication for each and adequately secure your account.

Furthermore, you can set specific levels of access for each of the Sub-Admin and restrict the responsibilities of each member of your team.

Manage Sub-Admins

Add a Sub-Admin

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.
- Click on **Sub-Admins** in the menu.
- Click on the **New** button



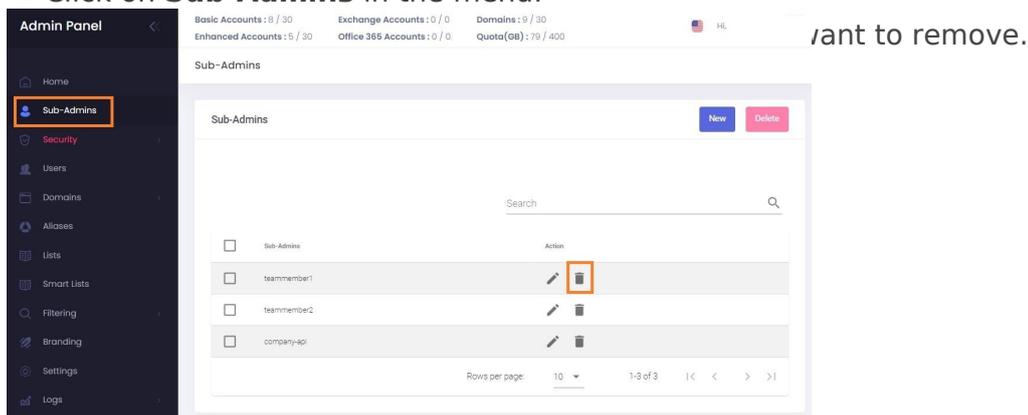
- Fill in the details of your new Sub-Admin:
 - Sub-Admin **username**
 - Sub-Admin **password**
 - Sub-Admin **e-mail address** - will be used for password recovery
 - Sub-Admin **full name**
- Select the **permissions** for each section. Each level of permission is numbered; the higher levels include the ones below it (level 2 includes level 1, level 3 includes level 1 and 2, etc.):
 - Account History: see the actions performed by Admin and Sub-Admins on the Home page
 - Users: view/manage/remove/impersonate Users (mailboxes). The highest level is **5 - Impersonate** and allows you to "sign in as" the User into Webmail and User Panel.
 - Domains: view/manage/remove Domains.
 - Aliases: view/manage/remove Aliases.
 - Lists: view/manage/remove distribution Lists.
 - Smart Lists: view/manage/remove Smart Lists.
 - Branding: view/update branding settings for the main Admin account.
 - Filtering: view/modify/remove whitelist and blacklist entries for Spam Filtering.
 - Logs: view Incoming and Outgoing Logs, Last logins.
- Click on the **Add Subadmin** button to save.

Example:

Username	<input type="text" value="Username"/>	company-api	✓
Password	<input type="password" value="Password"/>	luh\$bg/3--	✓
Email Address	<input type="text" value="Email Address"/>	api@company.com	✓
Full Name	<input type="text" value="Full Name"/>	API	✓
Account History	0 - No access	0 - No access	⌵
Users	0 - No access	5 - Impersonate	⌵
Domains	0 - No access	3 - Remove	⌵
Aliases	0 - No access	3 - Remove	⌵
Lists	0 - No access	3 - Remove	⌵
Smart Lists	0 - No access	3 - Remove	⌵
Branding	0 - No access	0 - No access	⌵
Filtering	0 - No access	0 - No access	⌵
Logs	0 - No access	0 - No access	⌵

Remove a Sub-Admin

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.
- Click on **Sub-Admins** in the menu.

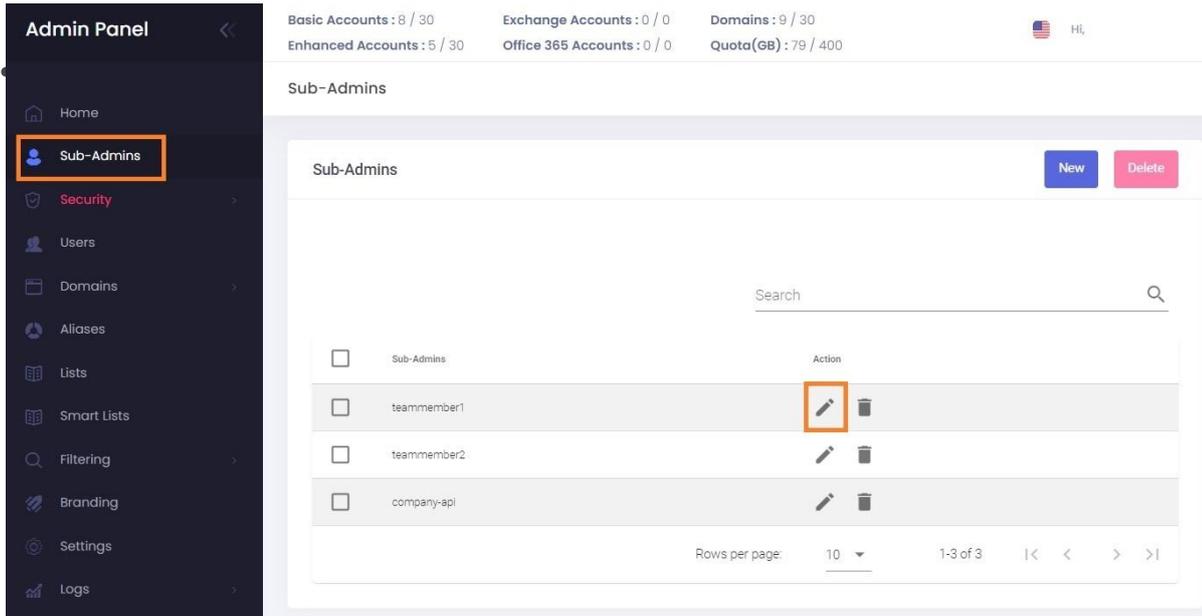


Update a Sub-Admin

You can update all the details and permissions of a Sub-Admin.

- Go to the [Admin Panel](#).
- Log in using your **main Admin username** and password.

- Click on **Sub-Admins** in the menu.
- Click on the **Edit (pencil)** button next to the Sub-Admin you want to update.
- Update the details. Leave the Password field blank if you want to update permissions but



Update teammember2

Higher level permissions include the ones before them

Username	teammember2
Password	Password
Email Address	
Full Name	teammember2
Account History	0 - No access
Users	5 - Impersonate
Domains	3 - Remove
Aliases	0 - No access
Lists	0 - No access
Smart Lists	0 - No access
Branding	0 - No access
Filtering	0 - No access
Logs	0 - No access

Cancel Update

Restrict Sub-Admin login access

Log in as the Sub-Admin and [follow the instructions for restricting login access.](#)

Two-factor authentication for Sub-admins

Log in as the Sub-Admin and [follow the instructions for enabling two-factor authentication.](#) Please note you cannot enable two-factor authentication for a Sub-Admin that you use for API or WHMCS

authentication - use restricted login access instead.

Revision #5

Created 24 August 2024 04:54:19 by Support

Updated 3 June 2025 21:57:22 by Support