How to secure your Openprovider Account ?

With the continuously increasing economic importance of domain names and our other goods, it is critical that no one but the approved entities have access to their management. This article lists Openprovider's different security layers and gives you information about how to use them.

1. Username and Password

2. User accounts

3. Password hashes

4. IP whitelisting and blacklisting

5. Two-factor authentication

Troubleshooting

1. Username and Password

The most fundamental method of user control and authentication of credentials is this. There is almost no system in the world that works without a combination of username/password and it still provides a basic level of security by choosing the right password (and password management/rotation scheme!).

If that's what you prefer, the Openprovider control panel and API are only accessible through a username/password combination. Upon account or contact creation, you set your own username and password and can change your password at any time via our control panel by editing your contact details.

2. User accounts

In each company, individuals come and go. Some way of managing users makes life easier and safer! Create every employee's personal account. If someone leaves, just delete his or her personal

account and access has been withdrawn.

Via the Openprovider Control Panel, user accounts can be created and controlled.

3. Password hashes

It's pretty safe to log in to the Openprovider control panel with your password: a protected connection and the password covered by bullets, stars or whatever other character your browser uses.

The use of the API is different: you need to state a username and password somewhere in the file, preferably in plain text. As the control panel uses the same user keys as the API, the password can be identified and signed into the control panel by those with access to the API file.

Your API secret, the so-called API hashing, should be hidden to prevent this from occurring. You use a hashed version of it to authenticate your API session, rather than your plain text password. Find this hash of passwords in your contact details (Click the "edit" button on user detail page to see the reset option).

IMPORTANT: Refer to this documentation for using password hashes in XML API requests.

If you are using REST API, you can use bearer token in your requests instead of password hash. For generating bearer tokens, use your API username and password. Refer to the documentation for example request. Please note that password hashes are not supported with REST API.

4. IP whitelisting and blacklisting

Most clients log in from only a selected series of locations to the Openprovider control panel: office, house, or from a VPN connection. API access is even much more limited: the API connection is maintained by only one server.

You may opt to restrict API or control panel access to only a couple of IP addresses with this experience. An error message may be received from those attempting to communicate from another IP address. This whitelisting can be described and handled through the contact details page.

Blacklisting is the reverse of whitelisting: allowing access from any IP address but one or a few.

Whitelisting and blacklisting are specified at the user level (a separate set of IP addresses may be allocated to each user) and the access level (API or control panel). It supports both IPv4 and IPv6, as are the IP ranges.

Getting the error "***Access Denied***" when trying to log in?
In that case you are trying to log in from a non-authorized IP address.

If you have issues logging into control panel (RCP), check out this article.

5. Two-factor authentication

IP whitelisting may not be possible if you are traveling a lot and do not have a VPN connection. In this case, by allowing two-factor authentication, you can introduce a second level of security: signing in does not only require a username and password (something you know), but also a unique code created by a personal computer (something you have).

The two-factor authentication (commonly referred to as 2FA) configuration is completed via the special settings page within a minute. Per device, two-factor authentication can be configured.

Note :

Cisco Duo Mobile does not fully support standard TOTP and causes frequent login mismatches, so please use a compliant authenticator app (e.g., Google Authenticator, Microsoft Authenticator, Authy) instead.

Time to investigate !

It's time to review your current account to appreciate the many ways in which Openprovider lets you keep your account secure. For your particular case, are the login credentials still secure enough? Review the tools listed in this article and set your account's correct security level !!!

Troubleshooting

In case you have locked yourself out of your control panel, please review this article to get access again.

Revision #2
Created 2026-08-07 14:36:52 UTC by Sarath
Updated 2026-08-07 15:51:48 UTC by Sarath