Password Policy

How Ultra.cc Stores Passwords

Ultra.cc uses trusted software platforms, allowing you to have the best possible experience. Here, we describe the platforms used to power our services and how each platform manages the passwords stored. Please note that most of the passwords stored on our servers are encrypted and hashed using various secure algorithms.

myUltra (WHMCS)

Ultra.cc uses WHMCS for managing sales, provisioning of slots, email dissemination, service announcements, and payment. It uses industry-leading security standards to encrypt and secure your information stored on our servers. The password stored on our servers is hashed using Bcrypt.

Ultra.cc Control Panel (Django)

Ultra.cc uses Django to power the Ultra.cc Control Panel. It provides a one-stop panel to manage your Ultra.cc slot by managing your applications and passwords. It also gives the user a quick overview of your slot.

UCP Login Password

Your login password, used to access your UCP profile, is hashed using the PBKDF2 algorithm with a SHA256 hash.

UCP App Passwords

Your app passwords, which are the password used to login to your installed applications, are stored in plain text and are only available to the user and the Ultra.cc support team; this is for the Ultra.cc support team to access your installed applications whenever you ask for support. Ultra.cc support staff would not access said installed applications unless the user sends a support ticket, or asks a staff member for it on the community Discord server via Discord Tickets. In such cases, we would encourage you to set a temporary password prior.

Third-Party App Passwords

Certain applications (for instance, Deluge or SickChill) are known to store authentication details and sensitive information in plaintext, including passwords and API keys. This behavior is beyond the control of Ultra.cc, and it is at the user’s sole discretion to decide to trust these applications with this data. If you wish to see the application’s behavior in question change, please report this issue to the project maintainers directly. That said, Ultra.cc slots are locked down so that only you can access your data on your slot and not anyone else’s.

How can you help

You can help us to make Ultra.cc more secure by choosing unique and strong passwords for your accounts. Below are some tips on how to choose a strong password:

- Make your password unique.
    - Make sure that you do not use the same password on different sites.
    - Using the same password on different accounts is risky. If someone gets your password for one account, they could access your email, address, and even your financial information.
- Make your passwords longer and easy to remember by you.
    - The longer your password, the stronger it will be. Make sure your password is at least 12 characters long.
    - Here are some tips that you can use to create long and memorable passwords:
        - A quote from a movie or film
        - A passage from a book
        - Catchphrases
    - Avoid passwords that could be easily guessed by people who know you or anything from your easily accessible personal information pages, such as your social media profiles.
    - Also, avoid passwords that use your personal information such as your nickname, initials, important dates, and others.
    - Do not use common words, keyboard patterns, and phrases such as `password`, `1234`, `abcd`, and `qwerty`.
    - Do not use a word backward such as “321drowssap,” because reversing a word doesn’t improve your password’s security in the slightest.
- Use a password manager.
- If you have difficulty managing or remembering your passwords, consider using a trusted password manager. Below are our recommendations:
    - https://bitwarden.com/
    - https://www.lastpass.com/
    - https://lesspass.com/
    - https://keepass.info/

Weak Password Policy

Ultra.cc is actively encouraging users to use strong passwords for their accounts. **Ultra.cc does not hold any responsibility if the user account gets compromised due to weak passwords or using the same password at multiple websites.** It is common for attackers to use brute force or dictionary attacks to compromise your accounts. That’s why we highly recommend using a decent length of passwords with decent complexity. Please use the strong passwords tips we have suggested in the upper paragraph.

Revision #7
Created 13 November 2020 21:20:14
Updated 11 October 2023 12:53:09 by varg