User Manual: Password Management Program

Welcome to the Password Management Program user manual! This guide will walk you through using the program to securely manage your passwords.

Table of Contents

1. Installation

Before you can use the Password Management Program, you need to ensure that Node.js and MongoDB are installed on your system. Follow these steps to get started:

1. Install Node.js: Visit Node.js website and follow the instructions for your operating system.
2. Install MongoDB: Visit MongoDB website and follow the instructions for your operating system.

Once Node.js and MongoDB are installed, you can proceed with setting up the Password Management Program:

3. Download the program files from GitHub repository.
4. Extract the downloaded files to a folder on your computer.

2. Usage

Now that you have installed the program, follow these steps to use it:

1. Open a terminal or command prompt on your computer.
2. Navigate to the folder where you extracted the program files.
3. Run the following command to install dependencies:

```
npm install
```

4. Create a `.env` file in the root directory of the program and add the following line:

```
URI=<your_MongoDB_connection_string>
```

Replace `<your_MongoDB_connection_string>` with your MongoDB connection string.
5. To encrypt passwords and upload them to the database, run the following command:

```
node index.js password.enc.txt
```

Replace `password.enc.txt` with the desired name of the encrypted password file.

6. Follow the prompts to provide the necessary information.
7. To check credentials, run the following command:

```
node index.js <email> <password>
```

Replace `<email>` with your email address and `<password>` with your password.

3. Troubleshooting

If you encounter any issues while using the program, try the following troubleshooting steps:

- Ensure Node.js and MongoDB are properly installed and running on your system.
- Check that you have provided the correct MongoDB connection string in the `.env` file.
- Verify that the input file (`password.txt`) exists and contains valid email addresses and passwords.
- Make sure you have provided both email and password when checking credentials.

If the issue persists, feel free to reach out to our support team for assistance.

4. Frequently Asked Questions (FAQs)

Q: Can I use this program without installing MongoDB? A: No, MongoDB is required for storing and retrieving encrypted passwords.

Q: How secure is my data in MongoDB? A: MongoDB stores data securely using encryption and access control mechanisms.

Q: Can I change my MongoDB connection string after installation? A: Yes, you can update the `.env` file with the new connection string.

Q: Is it safe to store passwords in plaintext? A: No, it is not safe. This program encrypts passwords before storing them in the database to ensure security.

That's it! You are now ready to securely manage your passwords using the Password Management Program. If you have any further questions or need assistance, don't hesitate to contact us.