LAB Manual

PART A

(PART A: TO BE REFFERED BY STUDENTS)

**Experiment No: 8**

**A.1 Aim:**

To control the usage of removable storage media

**A.2 Prerequisite:**

Fundamentals of USB usage, malware and scan operations.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. USB device control with password protection

2. Data Encryption on USB devices

3. Auto run protection and Malware Detection

4. Configurable read/write privilege protection

**A.4 Theory:**

Software provided controls unauthorized usage of removable storage media. This solution blocks and controls the usage of removable storage media like pen drive, Mobile phones, card readers, external hard disk etc. Only authenticated users can access the removable storage media.

Follow the installation steps as per the pdf file

The USB Console is provided to administrate the solution properly. The Administrator can login to this console and perform various tasks like adding/deleting users, changing the passwords and Registering /Un-Registering devices for different users. A normal user can login through the console but only the option page will be accessible to the user for the purpose of changing the password.

**Task: (refer user manual)**

1. Administrator login to the solution using the Login Page.

2. Add the required users to the database in the User Manager Page.

3. Insert a USB device. Whenever a new USB mass storage device is inserted in the USB port, the following message will popup if the administrator is logged in.

4. If the credentials provided are not correct then a login failed message will popup.

5. As administrator create/delete users.

6. Add/remove devices

7. Use of Device Manager Page

8. Check logs about the operations which are performed on enabled USB Mass storage device and Authentication responses

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)***

|  |  |
| --- | --- |
| Roll. No.: N049 | Name: Tarun Tanmay |
| Class: MBATech CE | Batch: B3 |
| Date of Experiment: 3/9/20 | Date of Submission: |
| Grade: | |

**B.1 Theory written by student:**

USB Pratirodh is a software solution which controls unauthorized usage of removable storage media.

This solution blocks and controls the usage of removable storage media like pen drive, Mobile phones, card readers, external hard disk etc.

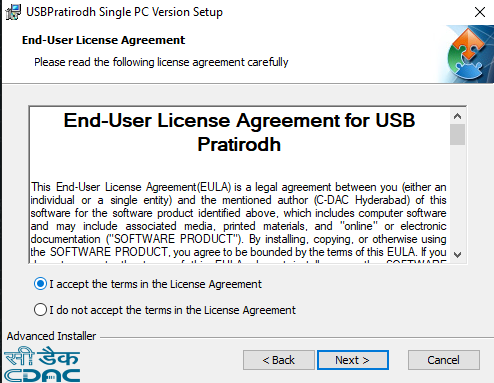
Only authenticated users can access the removable storage media.

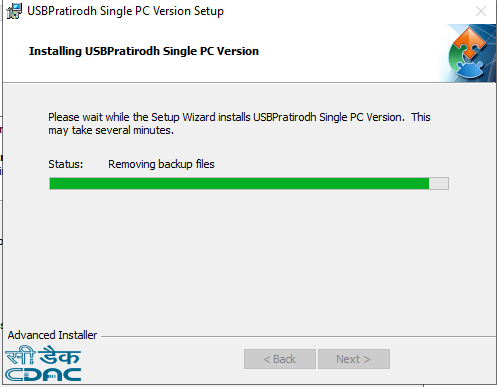
The USB Pratirodh Console is provided to administrate the solution properly.

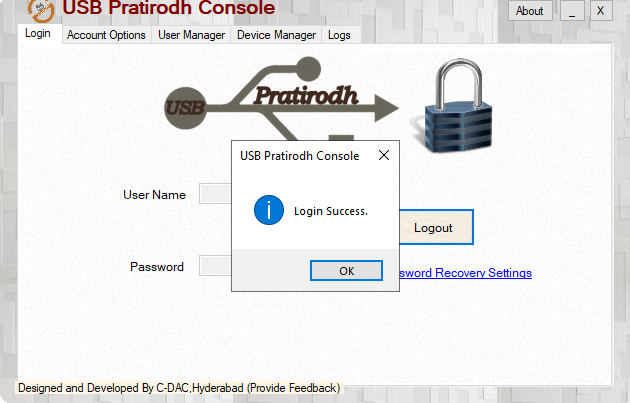
The Administrator can login to this console and perform various tasks like adding/deleting users, changing the passwords and Registering/Un-Registering devices for different users.

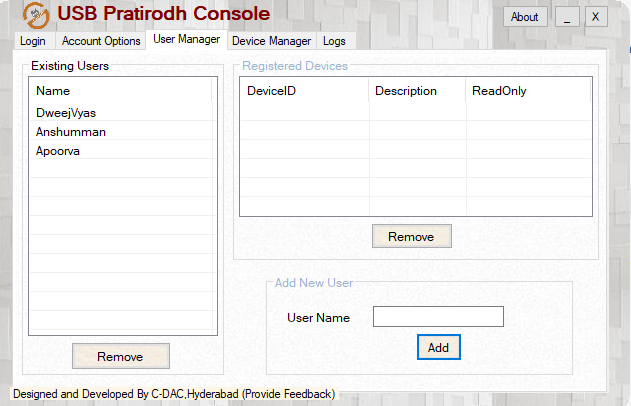
A normal user can login through the console but only the option page will be accessible to the user for the purpose of changing the password.

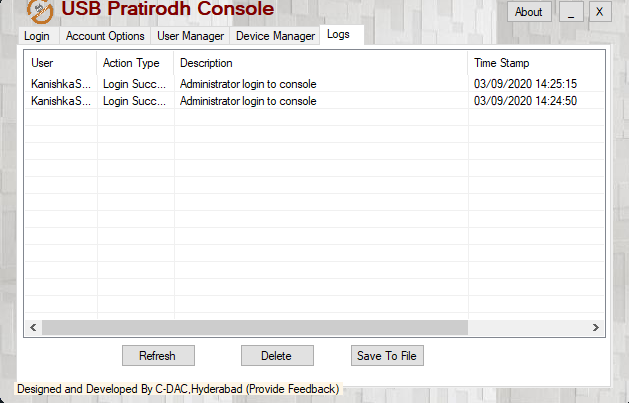
**B.2 Input and Output:**

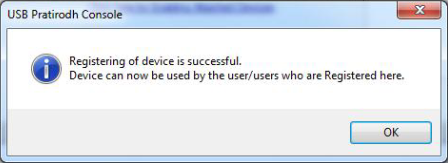
****

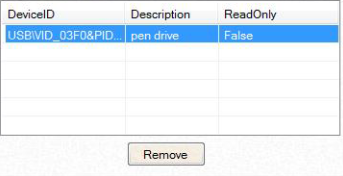
****

****

****

****

****

****

**B.3 Observations and learning:**

Leant about USB Pratirodh Console and how to use it.

**B.4 Conclusion:**

Understood use case of USB Pratirodh, add users, add devices or remove it.