



User Manual for USB Pratirodh Single PC Version for Windows

Centre for Development of Advanced Computing, Hyderabad



Contents

| | | |
|-------|--|----|
| 1 | What is USB Pratirodh Single PC Version? | 3 |
| 1.1 | The USB Pratirodh Console | 3 |
| 1.2 | Initial Configuration Steps:..... | 3 |
| 1.3 | The Log-In Page:..... | 5 |
| 1.4 | The Account Options Page:..... | 7 |
| 1.4.1 | Change Password:..... | 8 |
| 1.4.2 | Password Recovery:..... | 11 |
| 1.5 | The User Manager Page:..... | 14 |
| 1.6 | The Device Manager Page: | 20 |
| 1.7 | The Logs Page:..... | 22 |
| 2 | Using an already registered USB storage device | 23 |
| 2.1 | Using an unregistered USB storage device | 27 |
| 2.2 | Encryption:..... | 27 |
| 2.3 | Decryption:..... | 29 |



1 What is USB Pratirodh Single PC Version?

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 drives, Mobile phones, card readers, external hard disks etc. Only authenticated users can access the removable storage media. The latest version of USB Pratirodh is 3.4 as of 13-08-2024.

1.1 *The USB Pratirodh Console*

The USB Pratirodh Console is provided to administrate the solution properly. The Administrator can log in to this console and perform various tasks like adding/deleting users, changing the passwords and Registering /Unregistering devices for different users.

A normal user can log in through the console but only the option page will be accessible to the user to change the password.

A detailed description of each such functionality is given in the later part of the document. Please refer to the [Contents](#).

1.2 *Initial Configuration Steps:*

After the successful installation of the solution:

1. The administrator should log in 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 pop up if the administrator is logged in.



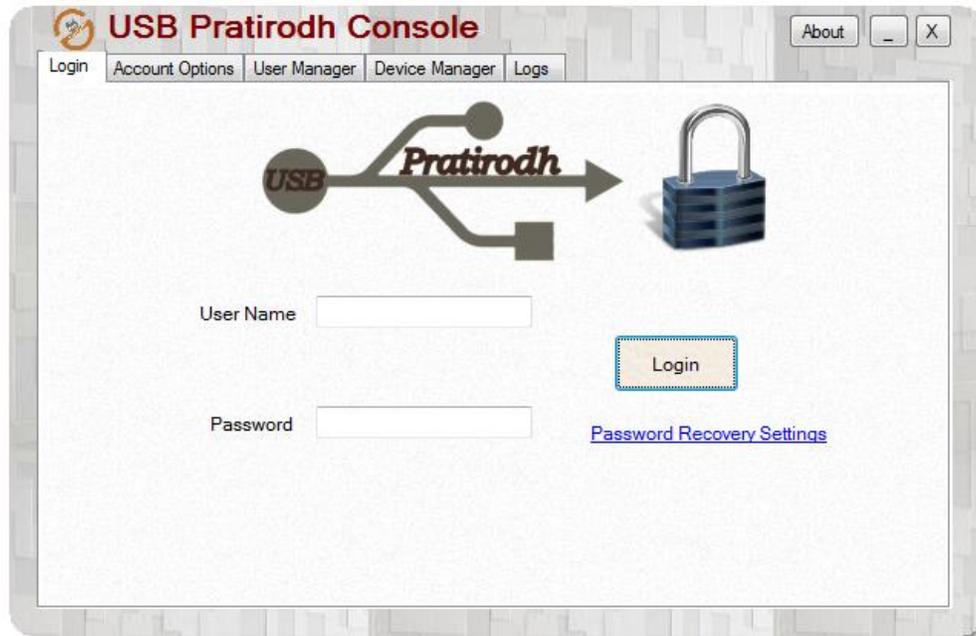
To register the device with the present users the **Yes** button should be pressed otherwise the **No** button should be pressed.

If the Yes button is pressed then the [Device Manager](#) page will come where the device can be registered to the present users.

If the No button is pressed then that device can't be registered to any of the users. But as the administrator is logged in the device will be allowed to be accessed by the administrator.

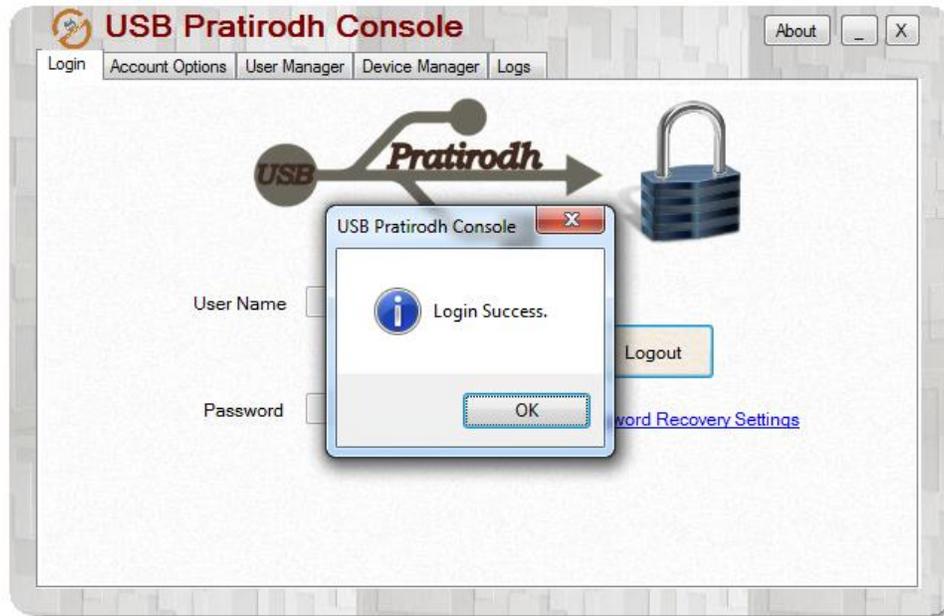


1.3 The Log-In Page:



This page has the “User Name” and “Password” fields and a “Login” button. The Administrator or a normal user can log in to the solution using the right credentials. After the successful login only, a user can perform other tasks.

After successful login, the button’s label will change to “Logout” from “Login”.



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



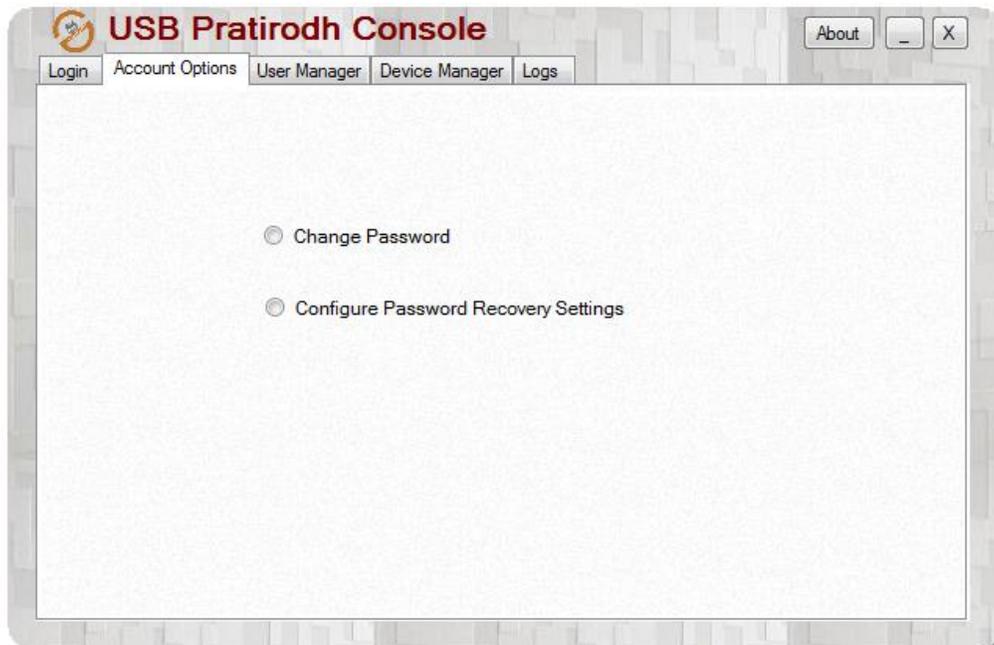
* The Uninstallation password is the same as the Administrator password.



* After five Wrong attempts of login, the USB Pratirodh Console will be blocked. Users can try after 5 minutes only.



1.4 The Account Options Page:





The Account Options page is used to change the password and for password recovery. This page contains two radio buttons labelled “Change Password” and “Configure Password Recovery Settings”. If the Change Password radio button is clicked then a new page is opened.

1.4.1 Change Password:

The screenshot shows a window titled "USB Pratirodh Console" with a menu bar containing "Login", "Account Options", "User Manager", "Device Manager", and "Logs". The "Account Options" tab is active, and the "Change Password" section is displayed. It features three text input fields labeled "Current Password", "New Password", and "Confirm Password". At the bottom of the dialog, there are two buttons: "Change" and "Cancel".

The above page contains three text fields labelled “Current Password”, “New Password” and “Confirm Password” and two buttons “Change” & “Cancel”. After successful login, the only page that a normal user can access is the Account options page where the user can change the password. The Administrator also can use this page to change only his password apart from access to the other pages of the GUI.

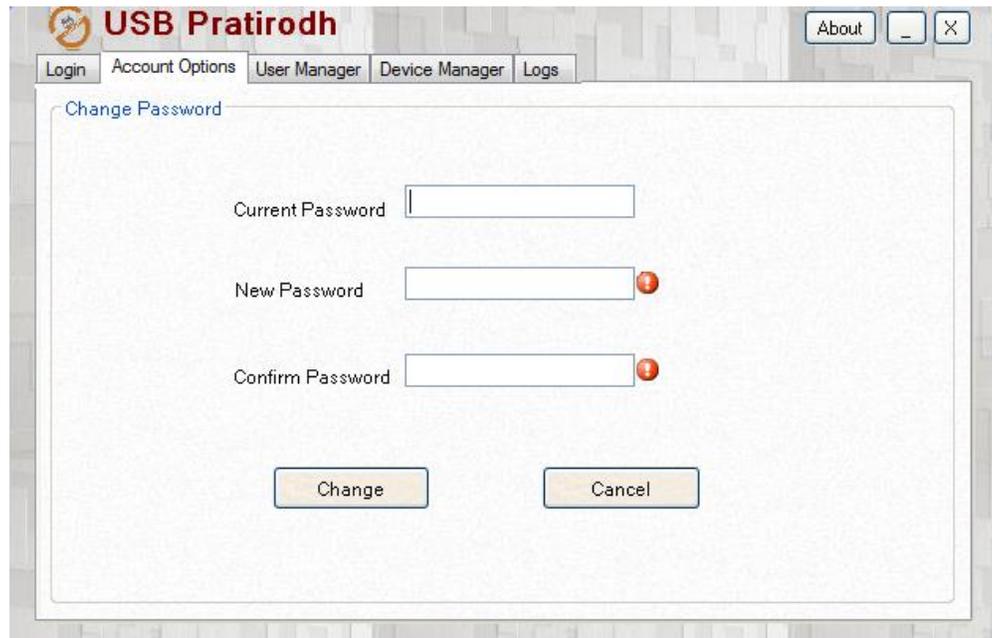
If the given credentials are correct then the “Password was changed successfully” pop-up will come.



If you give different passwords in a new password and confirm the password then the “error provider” symbol will come beside the text boxes. If we place a cursor over that symbol “Passwords entered are not matching” message will appear.

If you give a password which has a length of less than 8 characters also “error provider” symbol will come beside the text boxes. If we place a cursor over that symbol “Minimum password length required is 8” message will appear.

If you give a password which is not a combination of lowercase, uppercase letters, digits and special characters “error provider” symbol will come beside text boxes. If we place a cursor over that symbol “Password must contain lowercase letters, uppercase letters, digits and special characters” message will appear.



If you give the current password wrong then the following message box will be displayed.





1.4.2 Password Recovery:

The screenshot shows the 'USB Pratirodh Console' application window. The title bar includes 'About', a minimize button, and a close button. The menu bar contains 'Login', 'Account Options', 'User Manager', 'Device Manager', and 'Logs'. The main content area is titled 'Password Recovery Settings' and contains three sets of security questions, each with a corresponding text input field:

- Question : What is your maternal grandmother's maiden name?
Answer :
- Question : In which city does your nearest sibling live?
Answer :
- Question : What school did you attend for sixth grade?
Answer :

At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

If the administrator forgets the password, by using these security questions the password will be recovered.

This screenshot shows the same 'USB Pratirodh Console' window as above, but with an error dialog box overlaid. The dialog box has a red 'X' icon and the text: 'Not a valid answer: Please consider the following'. It lists two requirements:

- 1) Answer should start with alphabets and optionally mix with numbers
- 2) Answer should not contain special characters other than _ and .

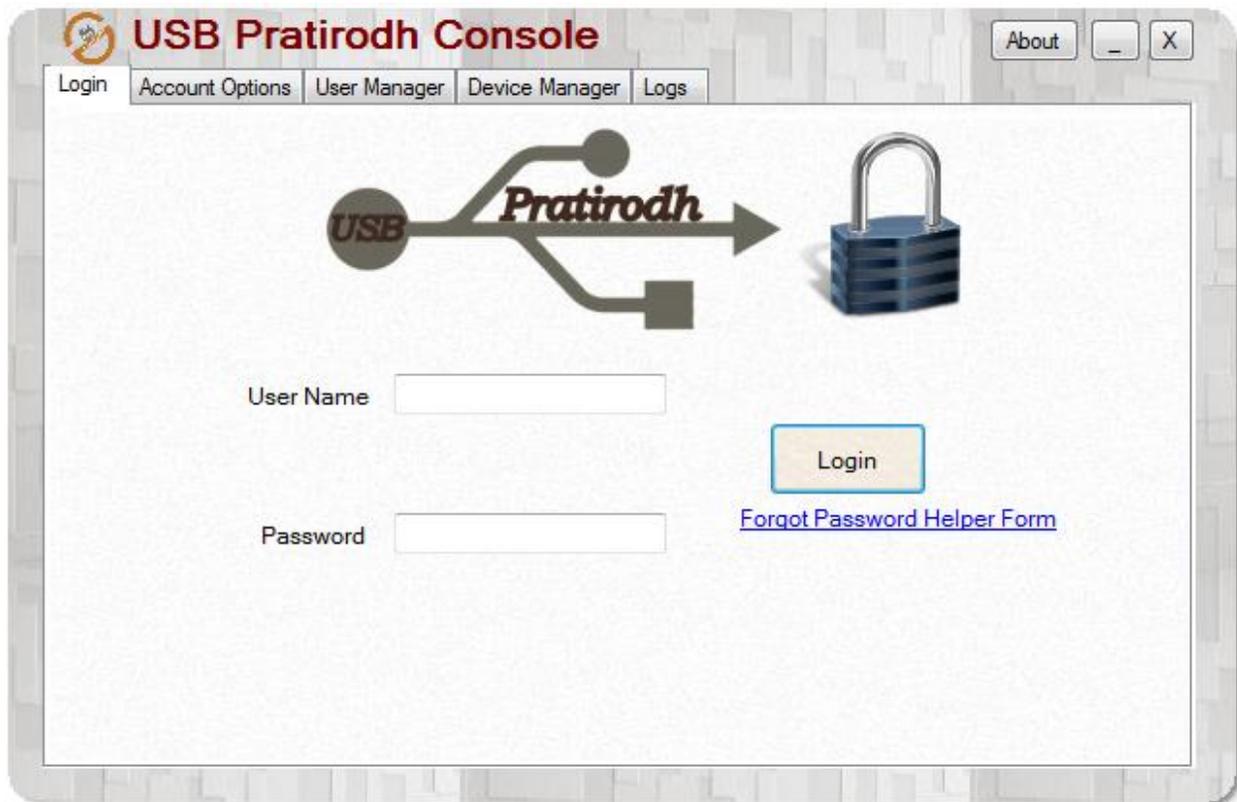
An 'OK' button is located at the bottom right of the dialog box.



The administrator needs to follow the above-mentioned rules. Otherwise, the above error message will be popped up.

Note: This feature is not available for non-administrator users. If they forget the password, then the administrator can create new users and bindings.

After filling out the form our Login page will look like the following.



After clicking the “Forgot Password helper form” link, the “Password Recovery Settings” page will be displayed. It contains the security questions which have been filled previously. After filling in the answers, clicking the “Retrieve” button will check if the entered answers are correct or not.



The screenshot shows a window titled "USB Pratirodh Console" with a menu bar containing "Login", "Account Options", "User Manager", "Device Manager", and "Logs". The main content area is titled "Password Recovery Settings" and contains three sets of questions and answers:

- Question : What is your maternal grandmother's maiden name?
Answer :
- Question : In which city does your nearest sibling live?
Answer :
- Question : What school did you attend for sixth grade?
Answer :

At the bottom of the window are two buttons: "Retrieve" and "Cancel".

If the answers are correct then you will be redirected to the “Change Password” page where you can change the password.

The screenshot shows a window titled "USB Pratirodh Console" with a menu bar containing "Login", "Account Options", "User Manager", "Device Manager", and "Logs". The main content area is titled "Change Password" and contains two input fields:

- New Password
- Confirm Password

At the bottom of the window are two buttons: "Change" and "Cancel".



The same rules which are there for “Change Password” are applicable here too.

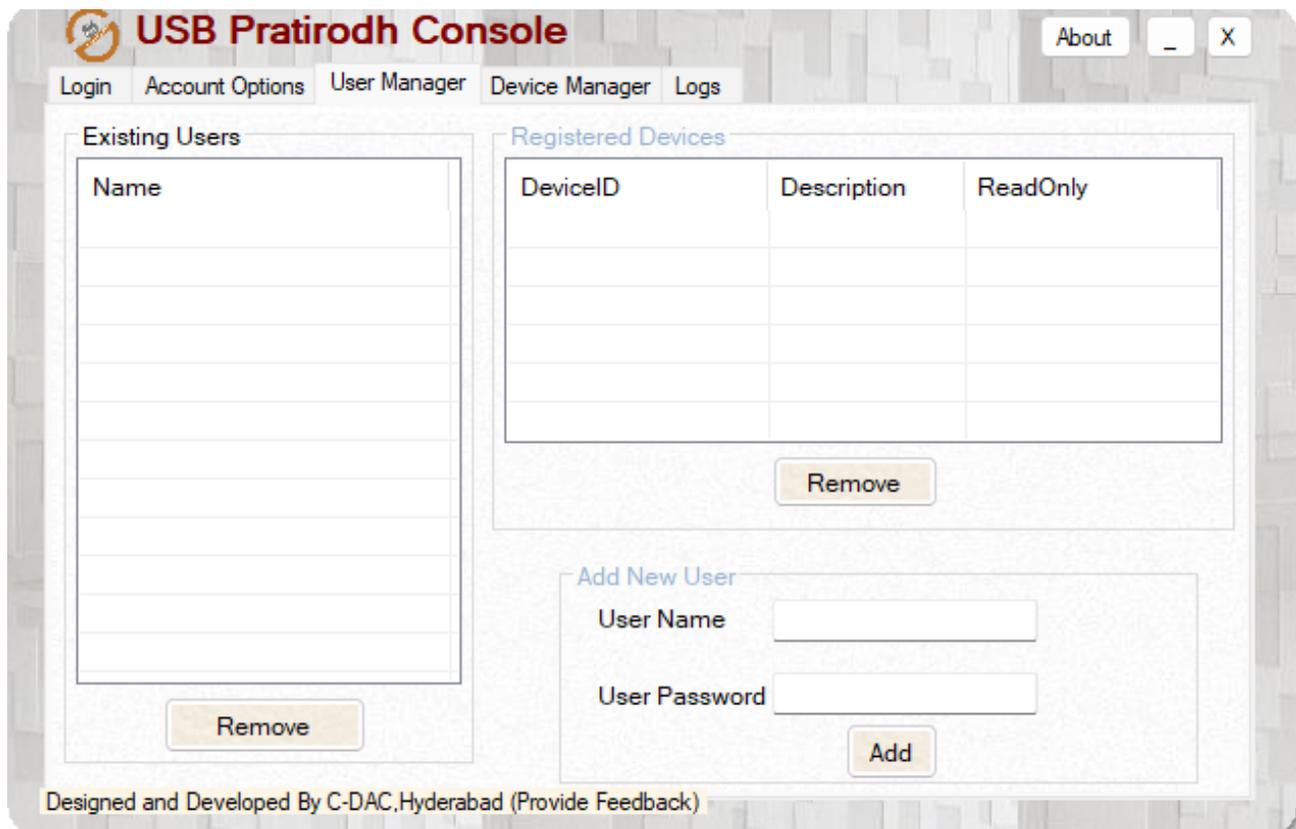
Note: Normal users are also able to log in to the USB Pratirodh Console by using his/her credentials.

One can only access the “Change Password” feature which is present on the Account Options page to change his/her password.

Rest all features and pages are not accessible by the normal user.

1.5 The User Manager Page:

To register any device a user name and password is required. So, by using the following page administrator can create/delete users.

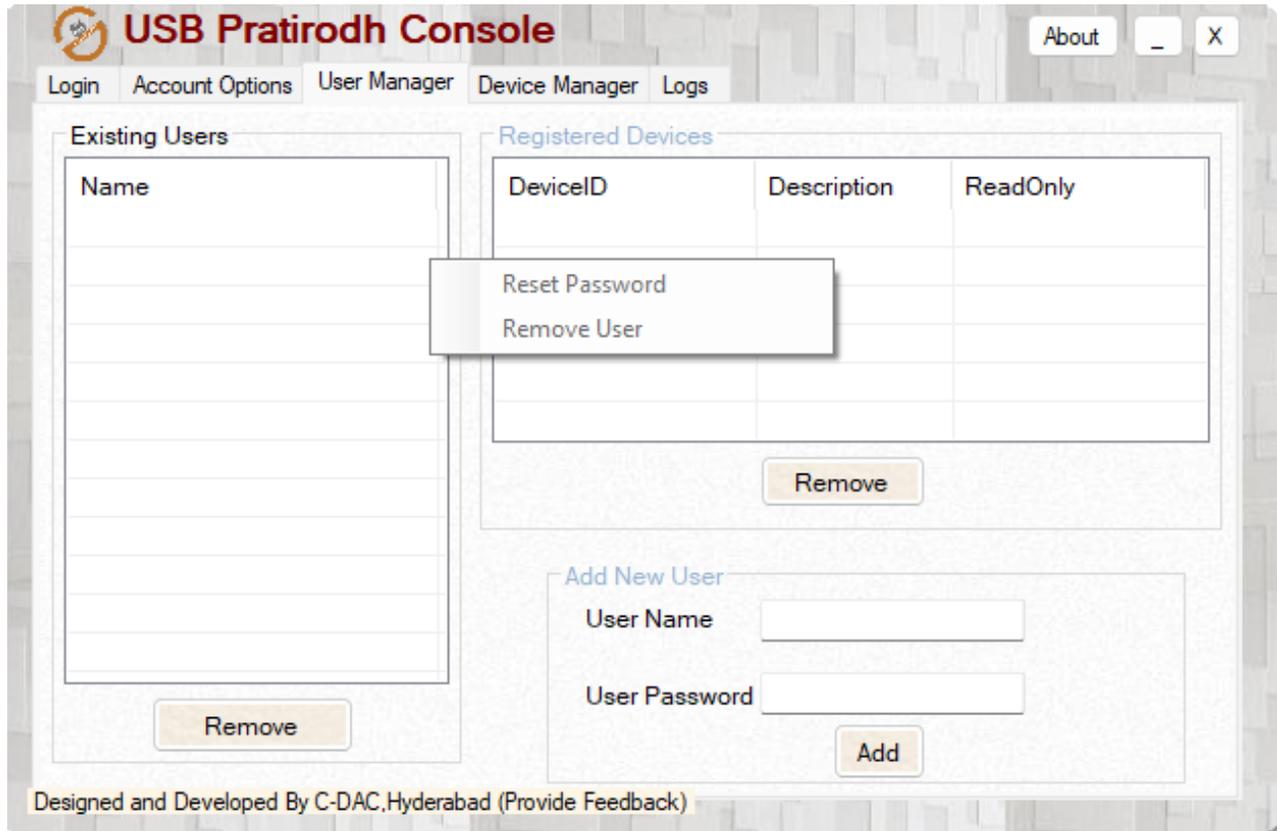


This page can only be accessed by the administrator of the solution after a successful login.

This page contains the “Existing Users” list table and the “Registered Devices” list table.



For adding devices, we have to add users by using the “Add New User” group box which is present at the right corner of the User Manager tab. If you click the mouse right button on the Name list which is present in the “Existing Users” list table, then the below popup menu will be displayed.



It has two options.

Reset Password: If any user changes his password by clicking on the reset password option that password will be reset.

Remove User: we can remove the user by clicking the “remove user” option.

After adding a user when we right-click on a particular user only the “Reset Password” and “Remove user” options will be enabled.

If adding a user is successful then it will be displayed in the Existing Users list.



If adding a user fails:

If Add User fails then the error provider will come showing the reasons for failure. Please see the below screenshot for details.

The screenshot shows the 'USB Pratirodh Console' interface. The 'Add New User' section has a red error icon next to the 'User Name' field. A tooltip with the following error messages is displayed:

- 1) User name should start with alphabets and optionally mix with numbers
- 2) User name should not contain special characters other than _ and .
- 3) Minimum User name length required is 4 and maximum length required is 26
- 4) User name and Administrator name should not be same

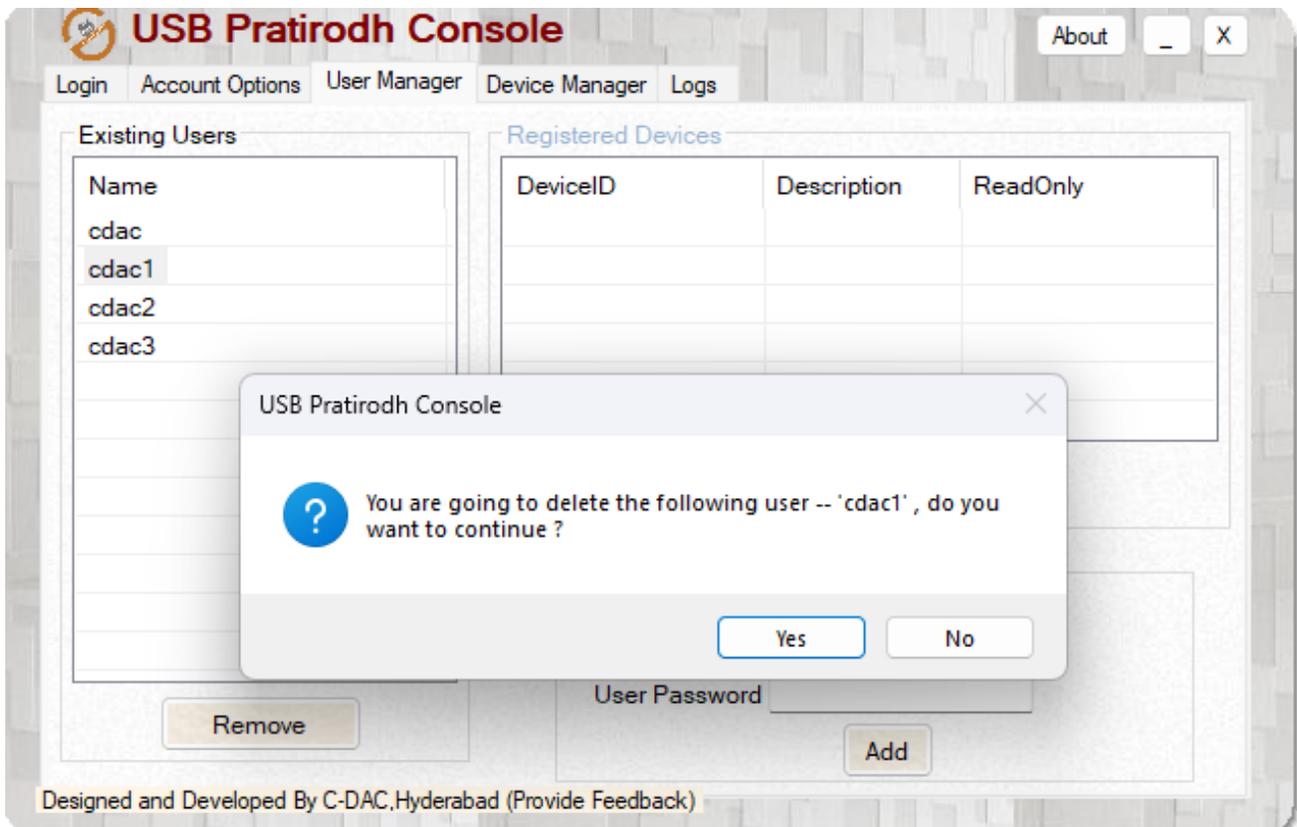
The interface also shows 'Existing Users' (cdac, cdac1, cdac2) and 'Registered Devices' (empty table).

If succeeds:

The screenshot shows the 'USB Pratirodh Console' interface after a successful user addition. The 'Existing Users' list now includes 'cdac', 'cdac1', 'cdac2', and 'cdac3'. The 'Add New User' section is empty, and the 'Registered Devices' table remains empty.



The Administrator can remove any of the existing users by selecting a user from the list and then clicking on the “Remove” button at the bottom of the list or clicking the mouse right on the user which you want to remove and selecting the “Remove User” option, and then click the “Yes” button in the popped-up confirmation message.



The “Registered Devices” table will display “all the devices and the respective description of the device” for a particular user. I.e. if a user is clicked in the Existing Users list, then the Registered Devices table will display all the devices and their description related/ mapped/registered to that particular user.



USB Pratirodh Console

About _ X

Login Account Options User Manager Device Manager Logs

Existing Users

| Name |
|-------|
| cdac |
| cdac1 |
| cdac2 |
| cdac3 |
| |
| |
| |
| |
| |
| |
| |

Remove

Registered Devices

| DeviceID | Description | ReadOnly |
|---------------------|-------------|----------|
| USB\VID_03F0&PID... | cdac | False |
| | | |
| | | |
| | | |
| | | |

Remove

Add New User

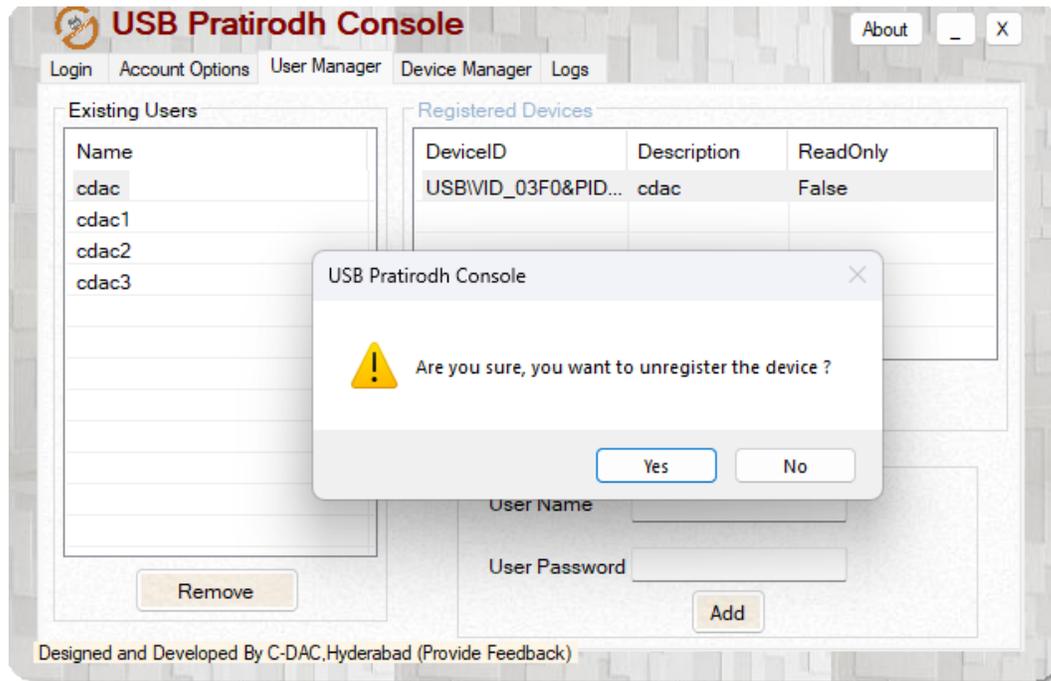
User Name

User Password

Add

Designed and Developed By C-DAC,Hyderabad (Provide Feedback)

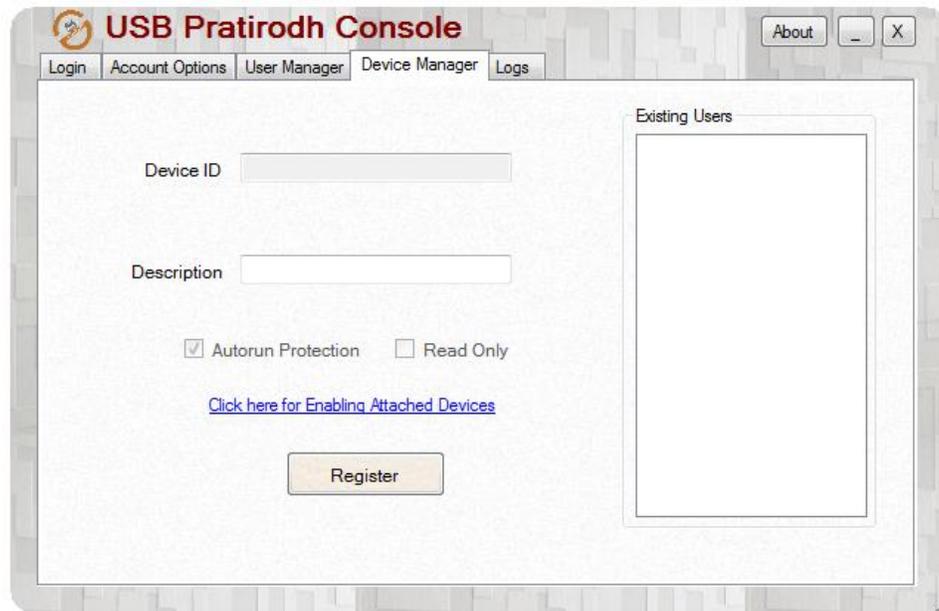
The administrator can Un-Register any of the listed devices from the list by selecting it then clicking the Remove button and then clicking “Yes” in the confirmation message that is popped up.



Doing this will remove the device from the list of a particular user and that user can't access the removed device any more. But if the same device is present in the list of other users, they will remain intact and the other users can access that device.



1.6 The Device Manager Page:



The Device Manager page is used to register the device to the users. This page contains

The Device ID text field, this field is not editable. Whenever a device is plugged in, the ID of the device will be displayed here

In the Description text field, Here the administrator will describe the device within 50 characters.

The Existing Users list box, if any user is present in the database, then the list of the users will be displayed here in the list box.

Autorun Protection Check Box, this will allow adding autorun.inf protection for the USB Mass Storage device

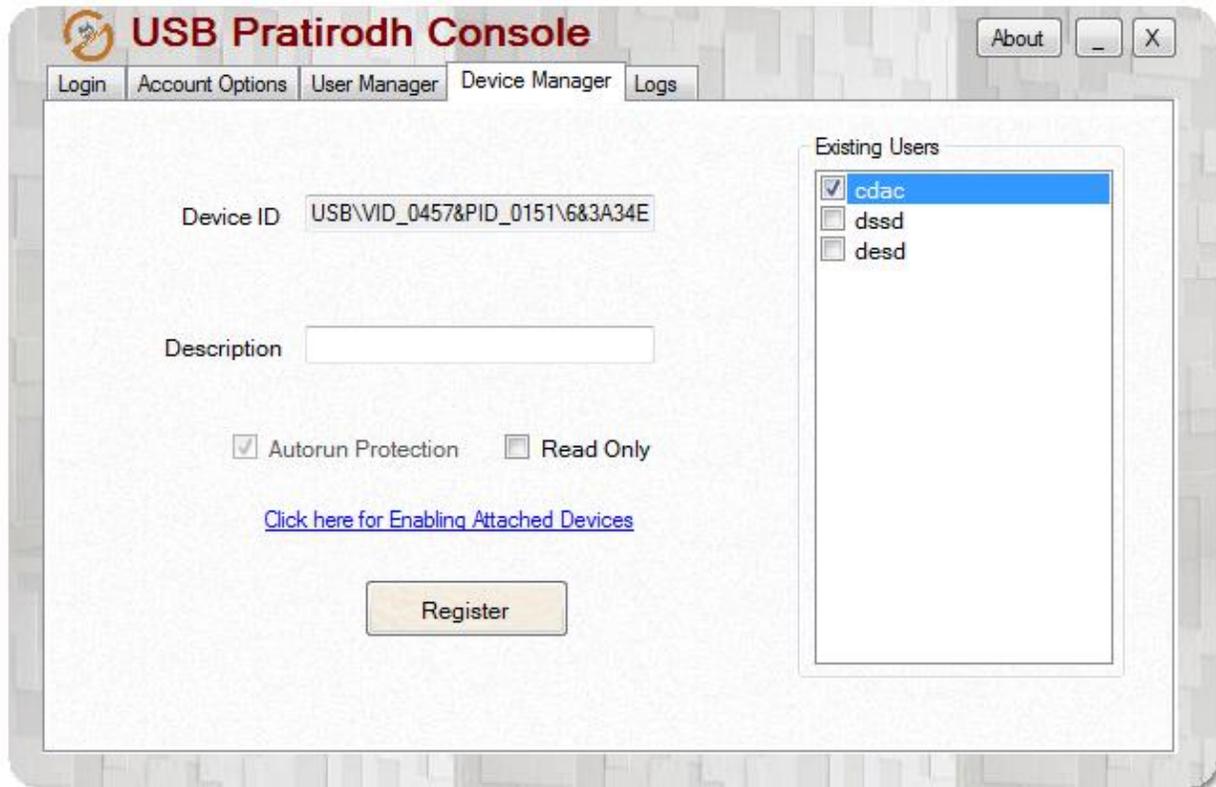
Read Only Check Box, using this functionality a USB Mass Storage device can be registered as read-only. If the device is registered as read-only, the file cannot be copied to the pen drive.

Click here for Enabling Attached Devices, by clicking this hyperlink if any USB mass storage devices are present then the corresponding device's device ID will be filled in the Device ID text box for registering with the user.

The following figure illustrates the scenario of whether the particular device is registered to a particular user or not. If the device is registered with a particular user, then that user's check box will be checked



and deactivated. If it is not registered yet then the particular user's checkbox will not be checked and the user is in enable state.



If a device is plugged in then the Device ID and the list of Existing Users are available will be displayed. The administrator needs to select the user to which the new device is to be registered/ bound and also the administrator needs to provide some description of the device for better identification and then clicking the Register button will do the job.

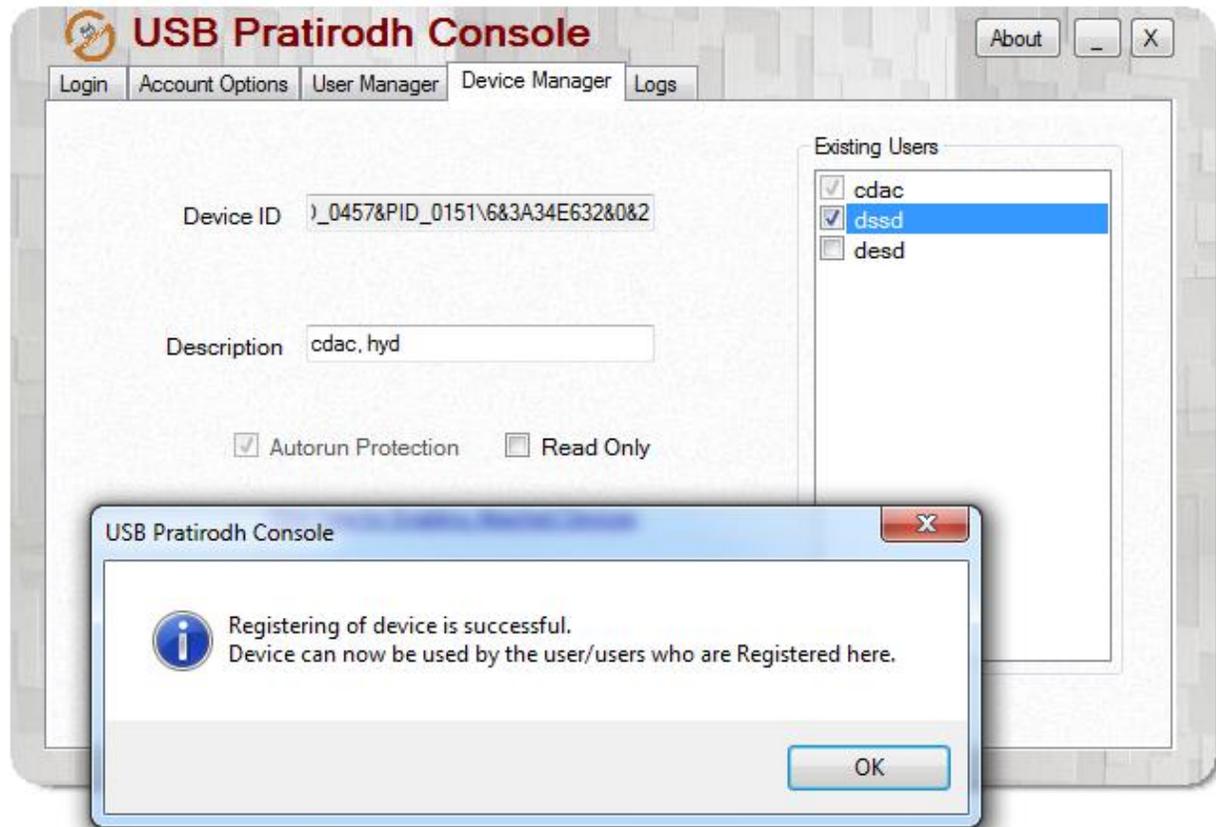
If the Registration is a success, then a success message will come otherwise a failure message will come.

If a device is removed from the list of a user, then the device must be registered to that user again to gain access.

* By default, all the devices are accessible by the administrator.

* By default, Autorun protection is enabled.

By default, Malware Scanning is performed when USB is enabled if an administrator is logged in.



After registering the device with a particular user if you want to register the device with another user then also the user needs to insert the device, then one message will pop up saying “This device is already Registered, do you want to Register with some other users”. If the user wants then he can proceed by clicking the “Yes” button in the popped-up message box.

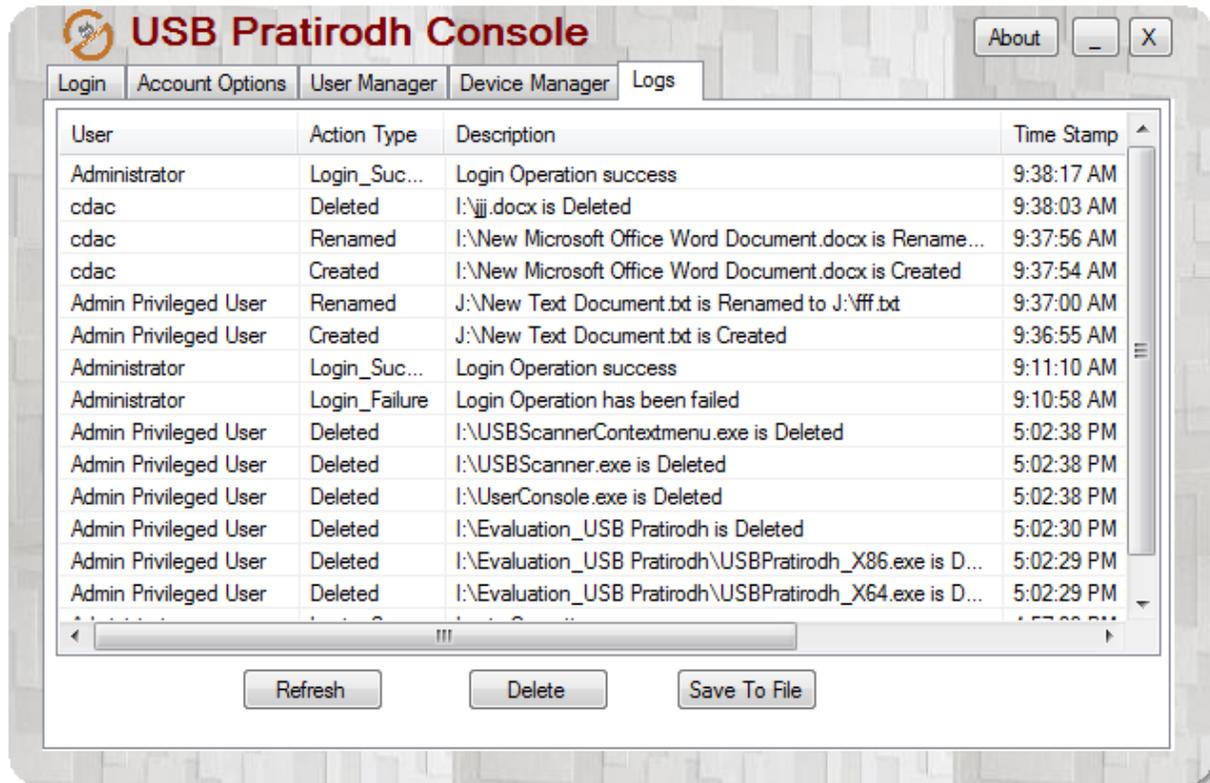
1.7 The Logs Page:

The Logs page contains all the logs about the operations which are performed on enabled USB Mass storage devices and Authentication responses.

- If the file has been created in a USB device, then the “xxx file is created” log will come.
- If the file has been renamed in a USB device, then the “xxx file is renamed to yyy” log will come.
- If the file has been deleted in a USB device, then the “xxx file is deleted” log will come.



- If the Login Operation success/fail then the “Login operation success/failure” log will come.



It has three buttons “Refresh”, “Delete” and “Save To File”. If recent logs are not present on the logs page user needs to click the “Refresh” button and if the user wants to save/backup the logs then the user needs to click “Save To File”, and then it will ask for the destination folder where the user wants to save. The backup file will be saved in text(.txt) format.

If the Administrator wants to delete the logs permanently without saving then by clicking the “Delete” button he can delete the logs permanently.

If the administrator performs any file/folder operations in the USB device, then in the user column “Admin Privileged User” will come.

2 Using an already registered USB storage device

Whenever a registered USB storage device is inserted, the following window will appear for authentication purposes.



USB Pratirodh User Login

User Name

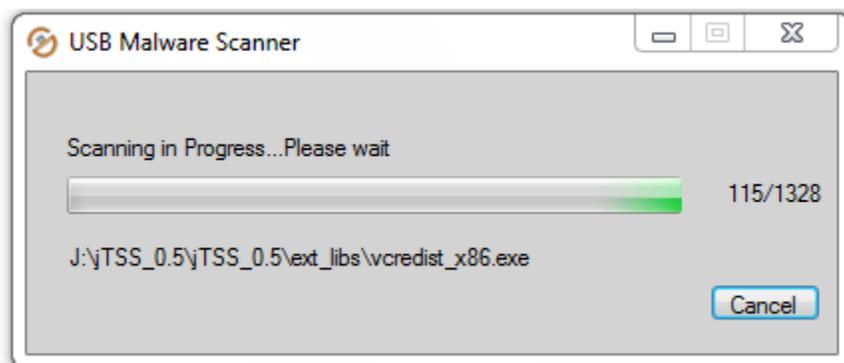
Password

Login Cancel

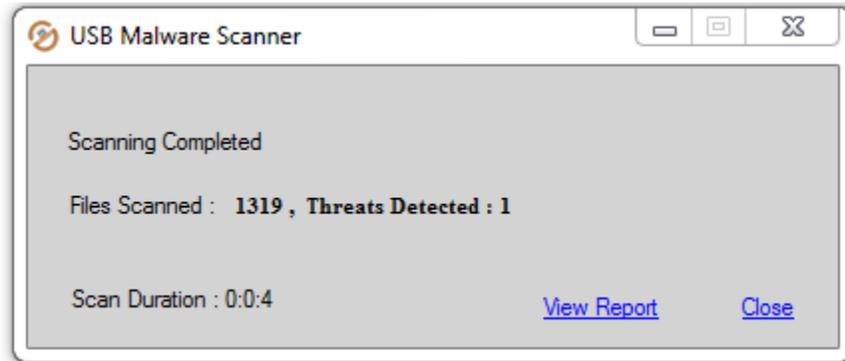
If the correct user's name and password are provided then the form will be disappeared and the device will be accessible.



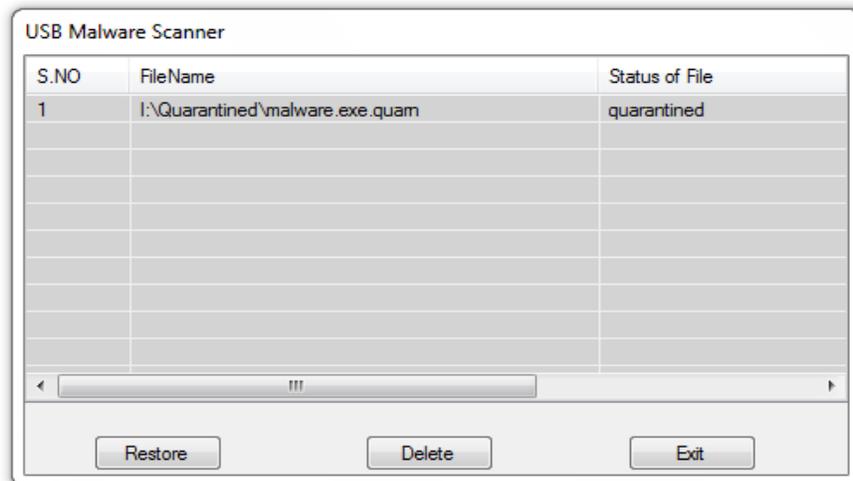
After enabling the device, the Scanner named "USB Malware Scanner" starts automatically scanning your USB Mass Storage device for malware. Wait for some time till scanning is completed.



After completion of scanning following Scanning Report window will be displayed.

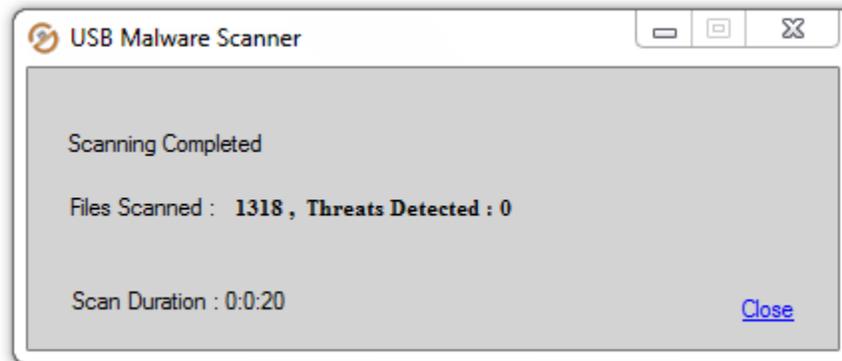


If the user wants to see the report, he needs to click the “View Report” link. If any malware has been detected, then the below window will appear. If any malware is detected then it is automatically quarantined and saved in the folder named “Quarantined” which is created automatically in the USB device. If you want to restore, you can restore by clicking on the Restore button. You can delete malware by clicking on the Delete button.



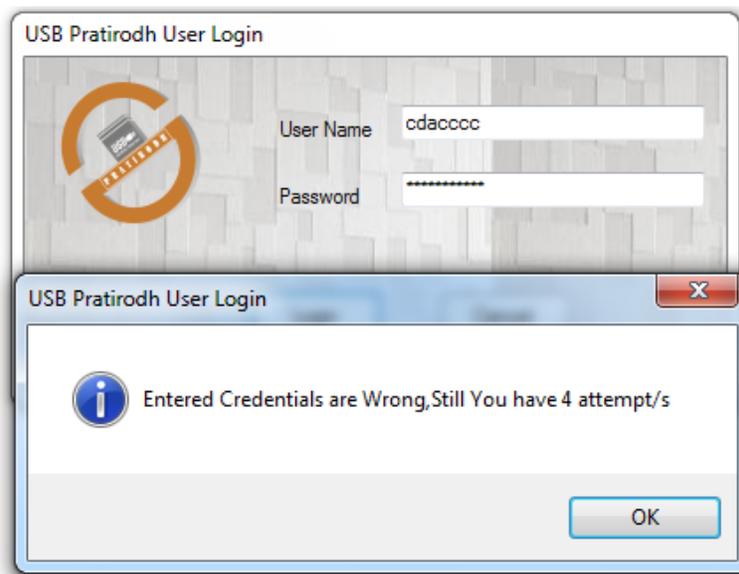
If the user clicks the “Restore” button then malware will be restored in the USB device’s “Restore” named folder. This folder is created automatically when we click on the Restore button.

If no malware is detected, then the following window will be shown.



Note: It is recommended that the user should not perform any file/folder (i.e., creating, copying, writing, renaming etc.) operations while scanning is performed, otherwise he/she may not get appropriate results.

If we provide the wrong credentials then an appropriate message will be appeared.



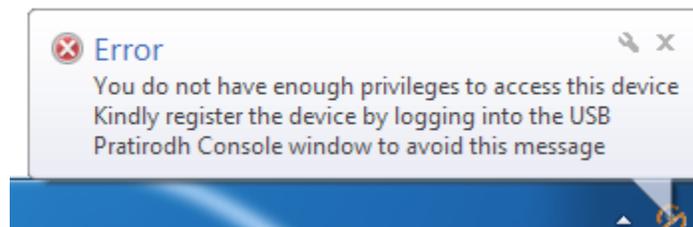
(Note: - The user should provide the details within 60 seconds from the pop-up of the login screen. After 60 seconds the above screen will disappear and a message box will appear with the message “Session has expired, please reinsert the device and try again.” and the device will be blocked. If the user wants to use the device, then it should be inserted again. *The administrator can't log in using this console.



If the user gives the five times wrong credentials, then the login operation is blocked. Please try again later.

2.1 Using an unregistered USB storage device

If the administrator is not logged in and a new device is plugged in (which is not registered with any user) then the following balloon tip will appear.



2.2 Encryption:

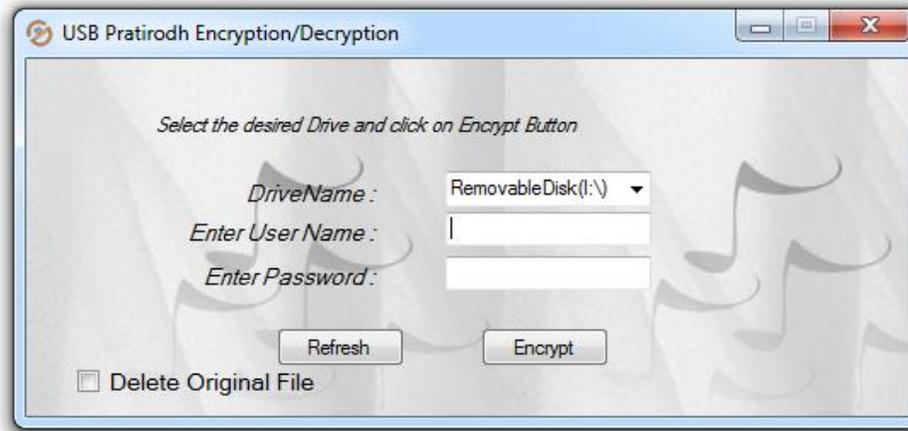
This feature is to provide security to your sensitive data. If you want to keep any confidential information in any USB Mass storage device you can save the data in encrypted format, which means Data on the USB storage devices can be encrypted.

To encrypt any folder or file, right-click on folder/file, then in the shell extension you can find the context menu i.e. “USBPDH Encryption\Decryption”.





Click on the “USBPDH Encryption/Decryption” menu. The following GUI will appear.



Press the refresh button, and it displays all attached devices that are authenticated in the dropdown box, select any one of them, give the username and password and press the encrypt button, the encrypted file or folder will be stored in the selected device.

Note: The username and password can be any of the USB Pratirodh users (Which the user has created in the user manager tab of User Console GUI).

With which USB Pratirodh user, the user has done encryption with that particular user only the user can perform decryption.

While the encryption balloon tip displays the status of encryption.



Select the check box of “Delete Original File”, and then the original file will be deleted from the system. Only encrypted will be present in the device.

Whenever the encryption process completes following message box will appear.



2.3 *Decryption:*

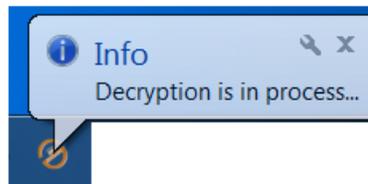
To decrypt any folder or file which is in an encrypted format (Which file/folder contains the extension USBPDH, the user needs to understand that, the file/folder is encrypted by using USB Pratirodh software), then right-click on the folder/file then in the shell extension, find the “USBPDH Encryption/Decryption” menu.



Click on the “USBPDH Encryption/Decryption” menu. Then GUI will appear.



Give the destination path, user name, and Password which the user has given while encryption and click on the “Decrypt” button, the file or folder will be decrypted and saved in the selected path. While the decryption balloon tip displays the status of decryption.



Whenever the decryption process completes following message box will appear.



Note: -1. If we encrypt any folder, we should not decrypt individual files or folders which are present in the encrypted folder.

2. While decrypting source path and destination path should not be the same.



3. Read Only and Encryption feature is not provided to the Mobile Phones.
4. The Malware Scan feature is not provided for Mobile phones.
5. Encryption Features are not provided for Mobile phones.