



User Manual for USB Pratirodh Single PC Version 3.0 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:.....	4
1.3	The Log-In Page:.....	5
1.4	The Account Options Page:.....	9
1.4.1	Change Password:	10
1.4.2	Password Recovery:	13
1.5	The User Manager Page:.....	17
1.6	The Device Manager Page:	25
1.7	The Logs Page:.....	28
2	Using already registered USB storage device	29
2.1	Using unregistered USB storage device	32
2.2	Encryption:.....	33
2.3	Decryption:.....	35



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 drive, Mobile phones, card readers, external hard disk etc. Only authenticated users can access the removable storage media.

1.1 The USB Pratirodh Console

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.

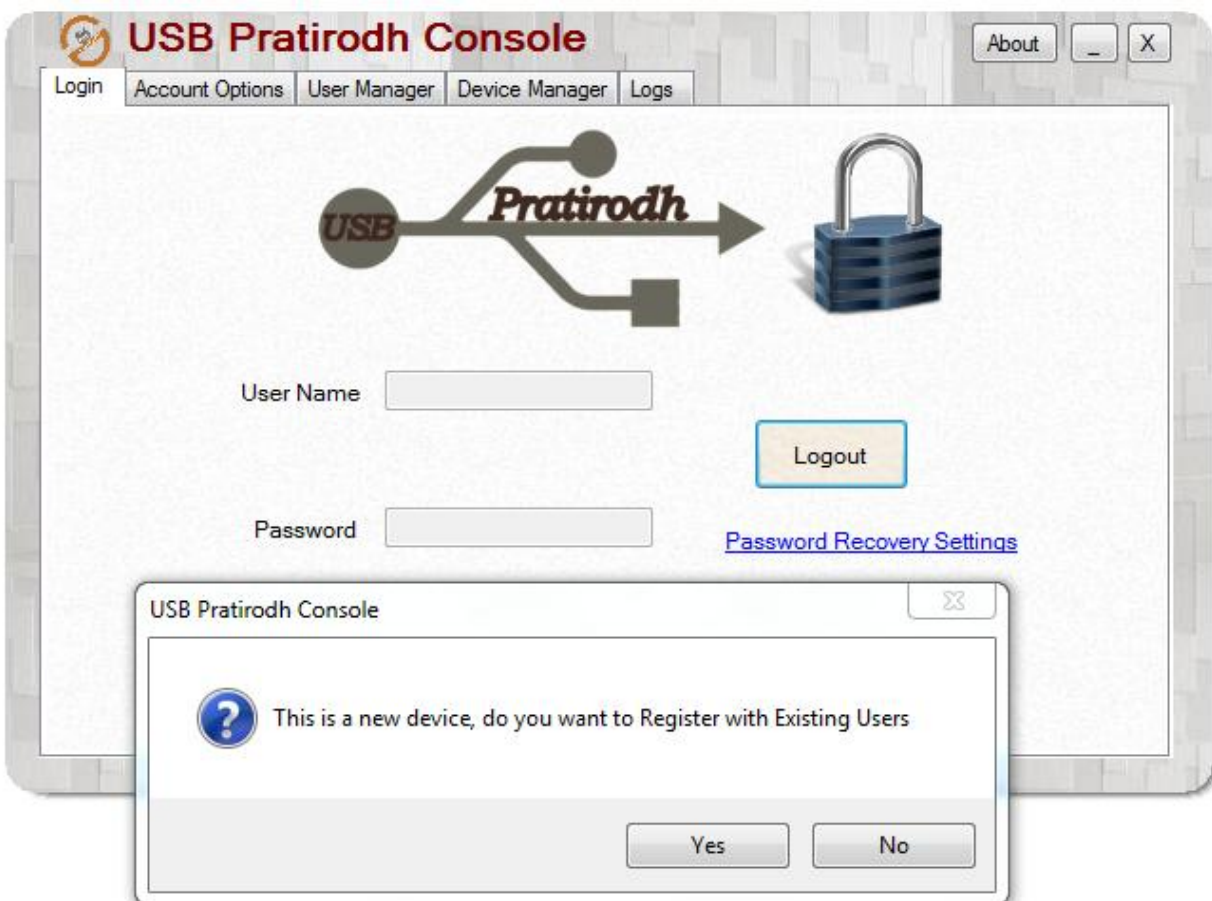
A detailed description of each such functionality is given in the later part of the document. Please refer the [Contents](#).



1.2 Initial Configuration Steps:

After the successful installation of the solution:

1. Administrator should 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.



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 user. But as the administrator is logged in so the device will be allowed to be accessed to the administrator.

1.3 The Log-In Page:

USB Pratirodh Console

Login Account Options User Manager Device Manager Logs

USB Pratirodh

User Name

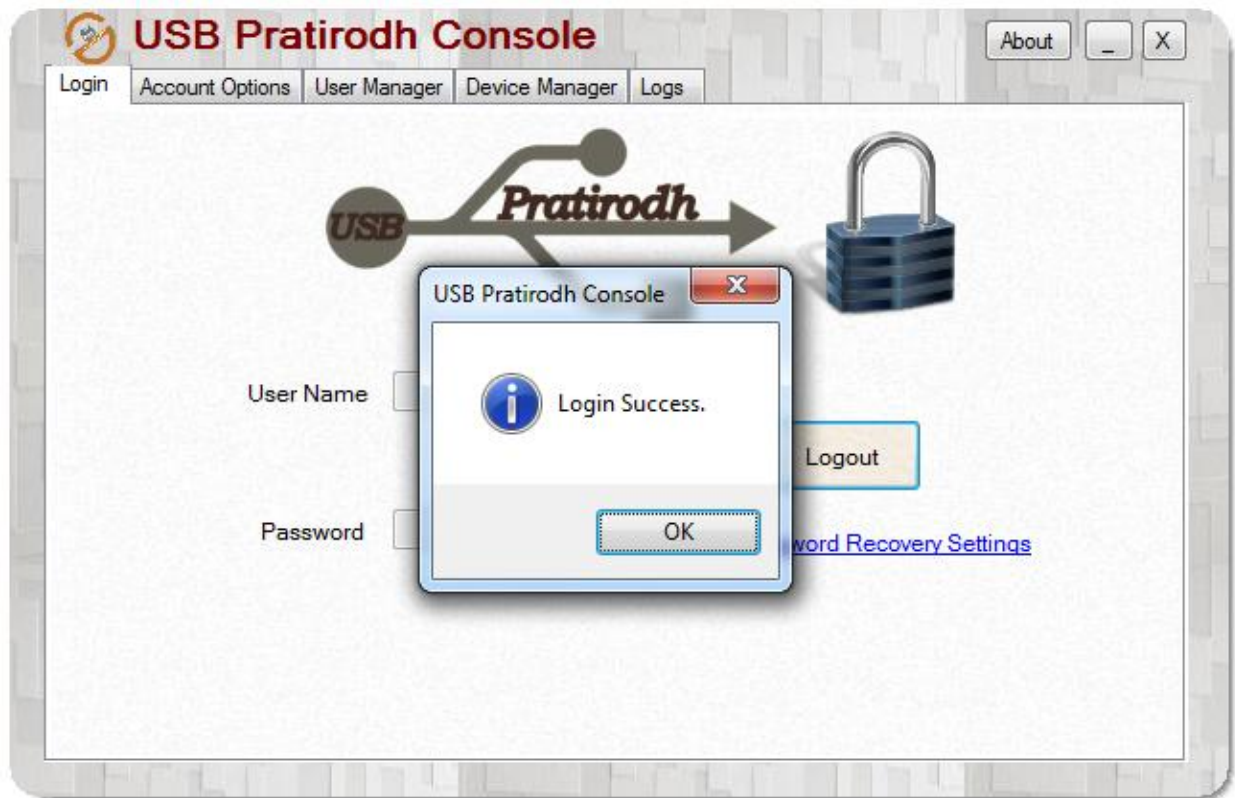
Password

Login

[Password Recovery Settings](#)

This page has the “User Name” and “Password” field and a “Login” button. The Administrator or a normal user can login to the solution using the right credential. 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.



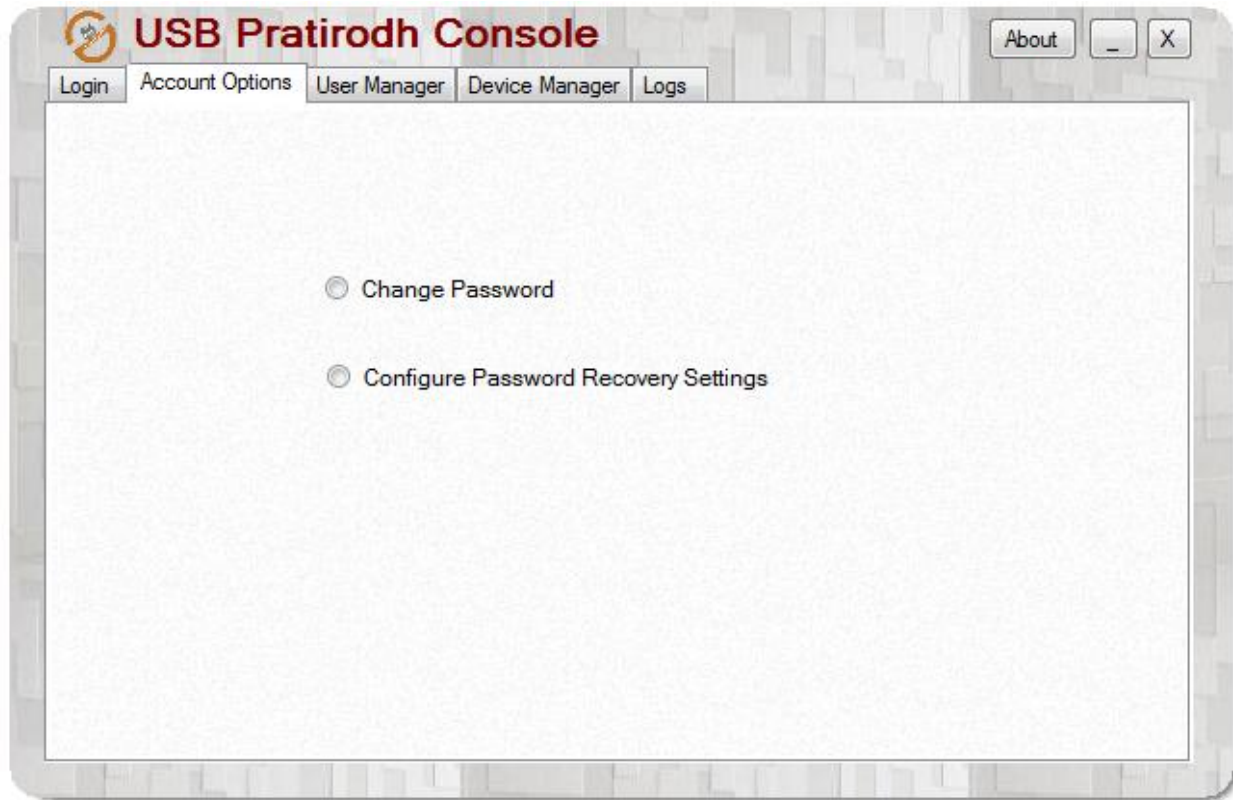
* The Un-installation password is same as the Administrator password.

* After five Wrong attempts of login, USB Pratirodh Console will be blocked. Try again later.





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 labeled “Change Password” and “Configure Password Recovery Settings” .If the Change Password radio button is clicked then new page is opened.



1.4.1 Change Password:

USB Pratirodh Console

Login Account Options User Manager Device Manager Logs

Change Password

Current Password

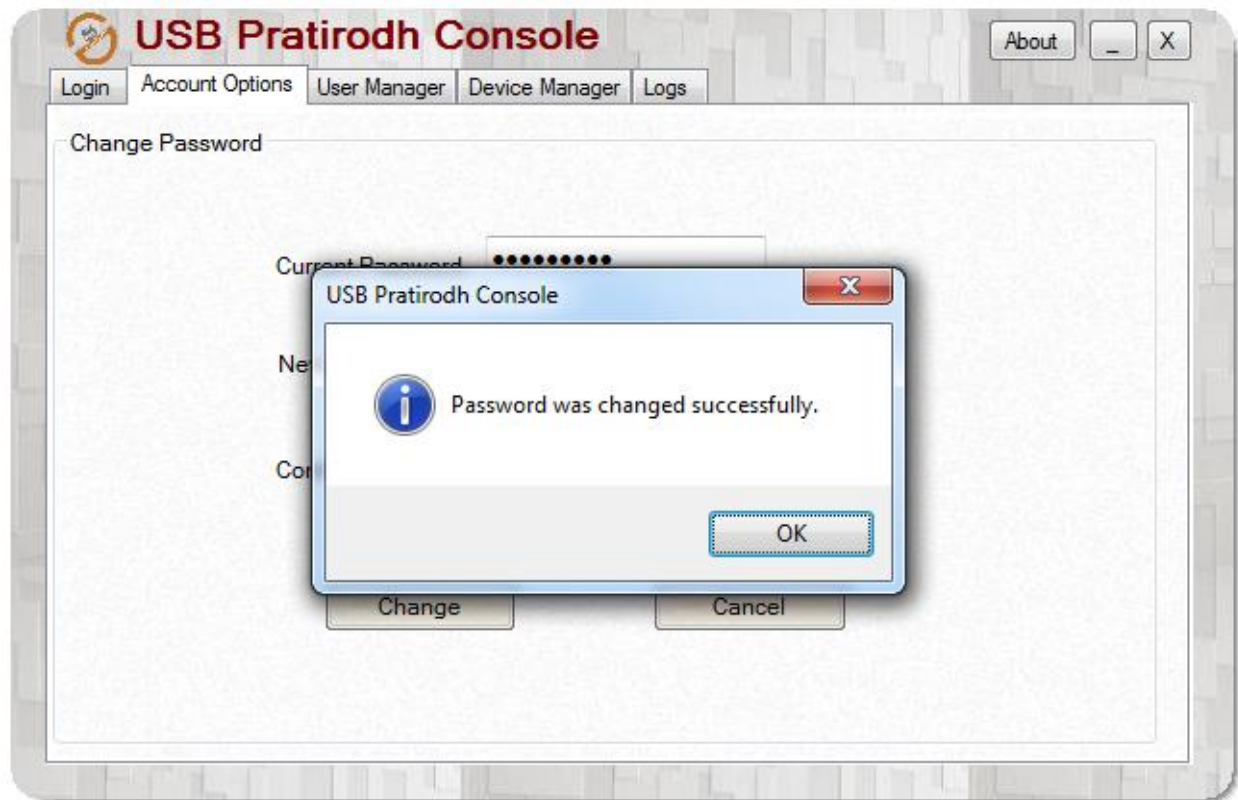
New Password

Confirm Password

Change Cancel

The above page contains three text fields labeled “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 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 given credentials are correct then “Password was changed successfully” pop up will come.



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

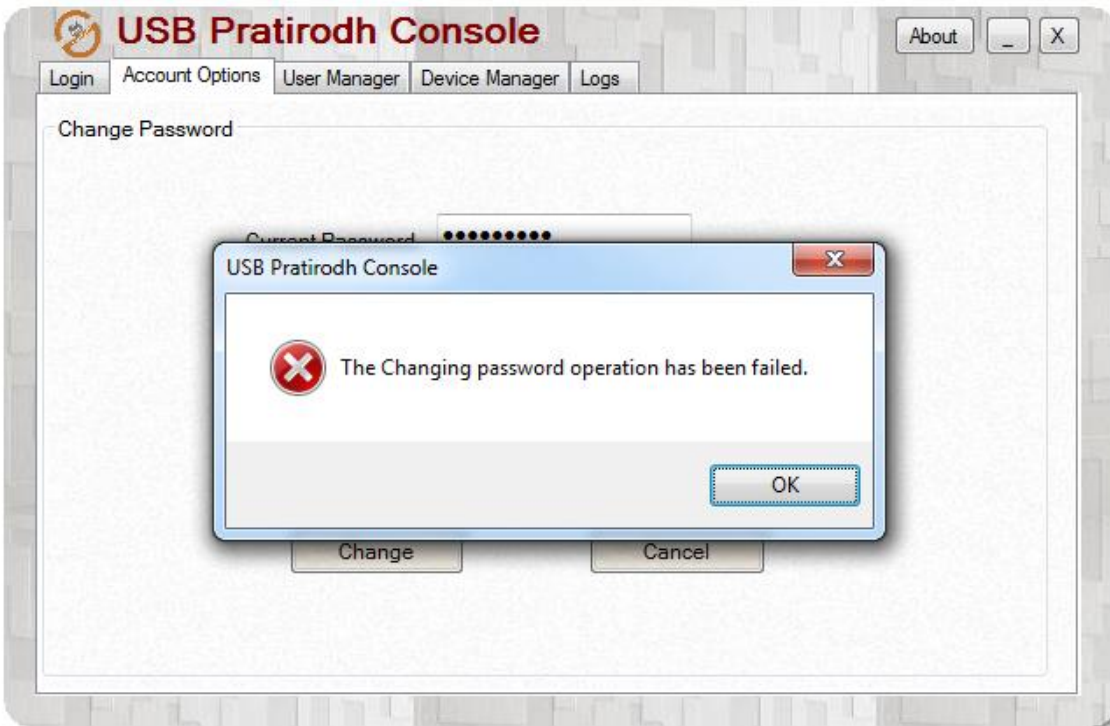
If you give password which has length less than 8 characters also “error provider” symbol will come beside text boxes. If we place cursor over that symbol “Minimum password length required is 8” message will appear.



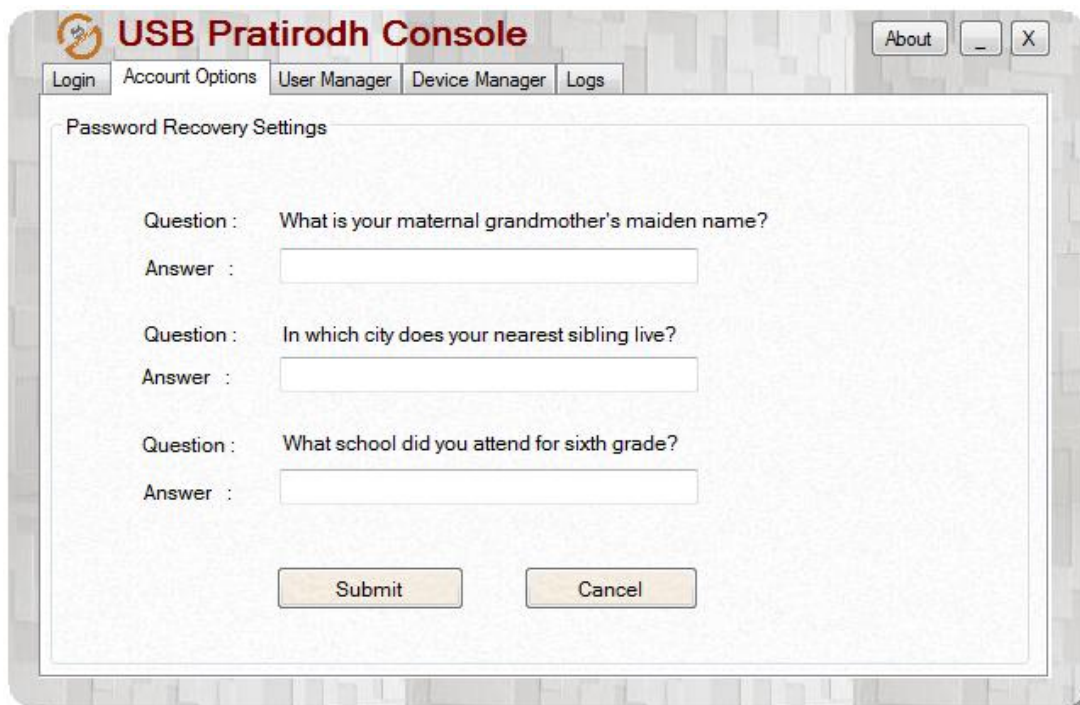
If you give password which is not the combination of lowercase, uppercase letters, digits and special characters “error provider” symbol will come beside text boxes. If we place cursor over that symbol “Password must contain lowercase letters, uppercase letters, digits and special characters” message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

The screenshot shows the 'USB Pratirodh' application window. It has a menu bar with 'Login', 'Account Options', 'User Manager', 'Device Manager', and 'Logs'. The 'Change Password' dialog box is open, containing three text input fields: 'Current Password', 'New Password', and 'Confirm Password'. The 'New Password' and 'Confirm Password' fields have a red circular error icon to their right. At the bottom of the dialog are 'Change' and 'Cancel' buttons. The 'Change' button is highlighted in yellow.

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

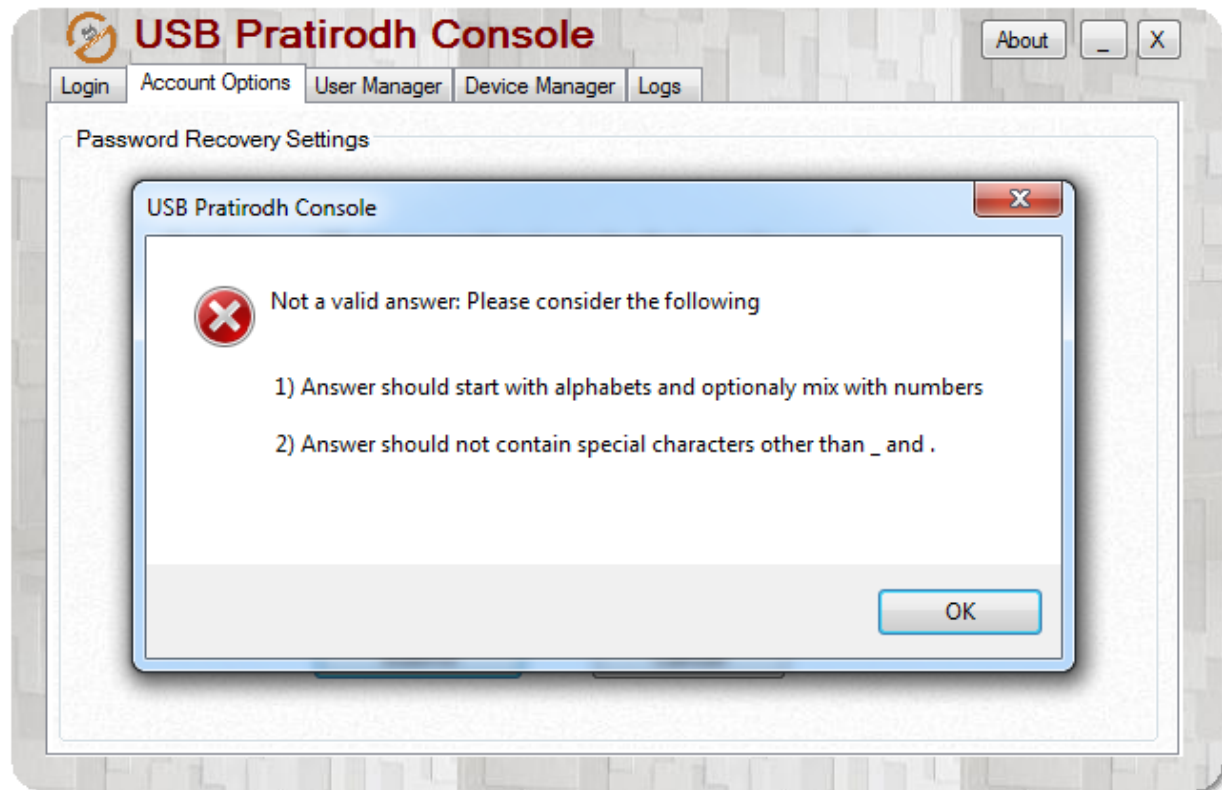


1.4.2 Password Recovery:





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



Administrator needs to follow above mentioned rules. Otherwise above error message will be popped up.



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

USB Pratirodh Console

Login Account Options User Manager Device Manager Logs

USB *Pratirodh*

User Name

Password

Login

[Forgot Password Helper Form](#)



After clicking “Forgot Password helper form” link, then “Password Recovery Settings” page will be displayed. It contains the security questions which have filled previously. After filling the answers, by clicking “Retrieve” button, it will check if 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 "Account Options" menu is selected, showing a sub-menu with "Password Recovery Settings". The "Password Recovery Settings" window contains three security questions, each with a corresponding answer field. The questions are: "What is your maternal grandmother's maiden name?", "In which city does your nearest sibling live?", and "What school did you attend for sixth grade?". At the bottom of the window are two buttons: "Retrieve" and "Cancel".

Question	Answer
What is your maternal grandmother's maiden name?	<input type="text"/>
In which city does your nearest sibling live?	<input type="text"/>
What school did you attend for sixth grade?	<input type="text"/>

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



USB Pratirodh Console

Login Account Options User Manager Device Manager Logs

About _ X

Change Password

New Password

Confirm Password

Change Cancel

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

Note: Normal user is also able to log-in to the USB Pratirodh Console by using his/her credentials.

He/She can only access the “Change Password” feature which is present in 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:

In order to register any device a user name is required. So by using following page administrator is able to create/delete users.



USB Pratirodh Console

Login Account Options **User Manager** Device Manager Logs

About X

Existing Users

Name

Remove

Registered Devices

DeviceID	Description	ReadOnly

Remove

Add New User

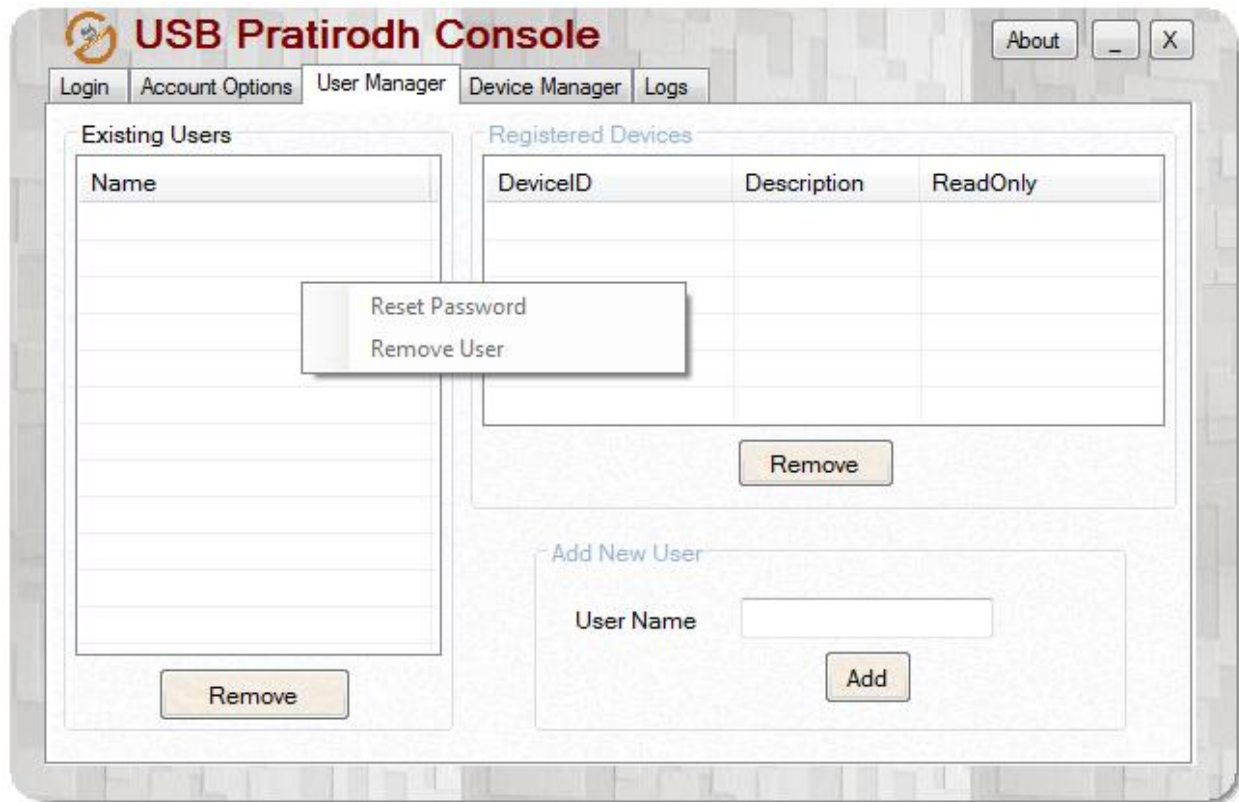
User Name

Add

This page can only be accessed by the administrator of the solution after 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 “Add New User” group box which is present at right corner of User Manager tab. If you click mouse right button on the Name list which is present in “Existing Users” list table, then below popup menu will be displayed.



It has two options.

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

Remove User: we can remove user by clicking remove user option.

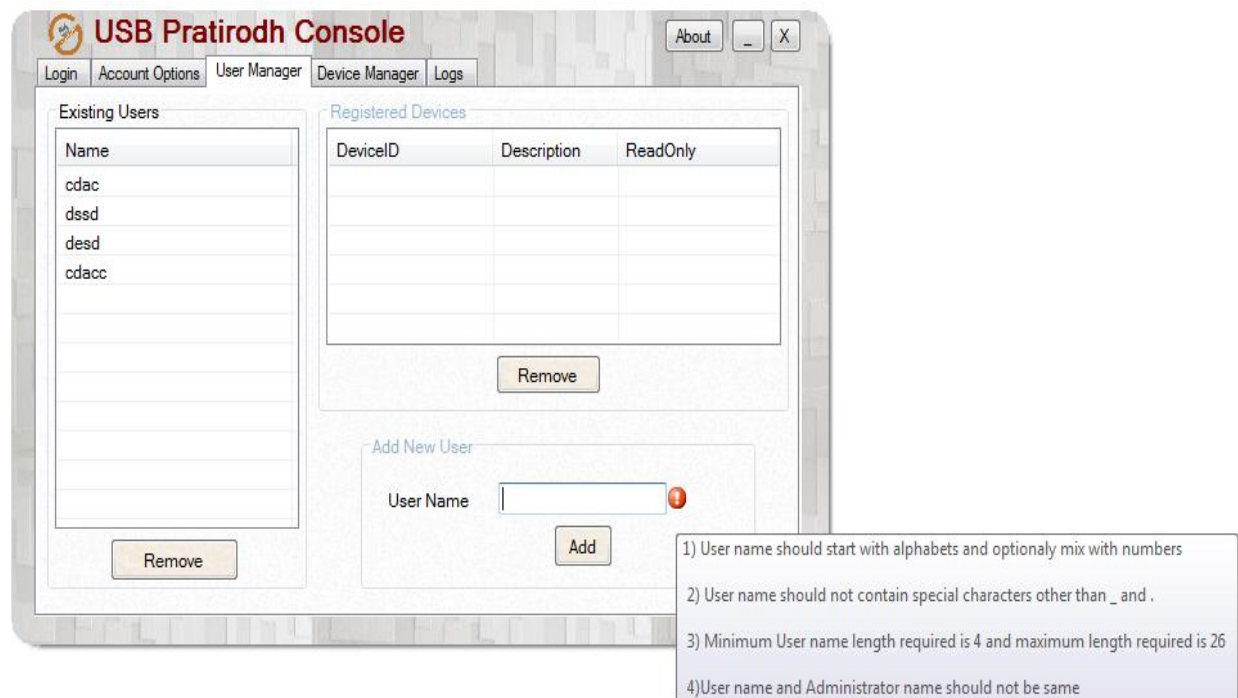
After adding user when we right click on particular user only “Reset Password” and “Remove user” options will be enabled.

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



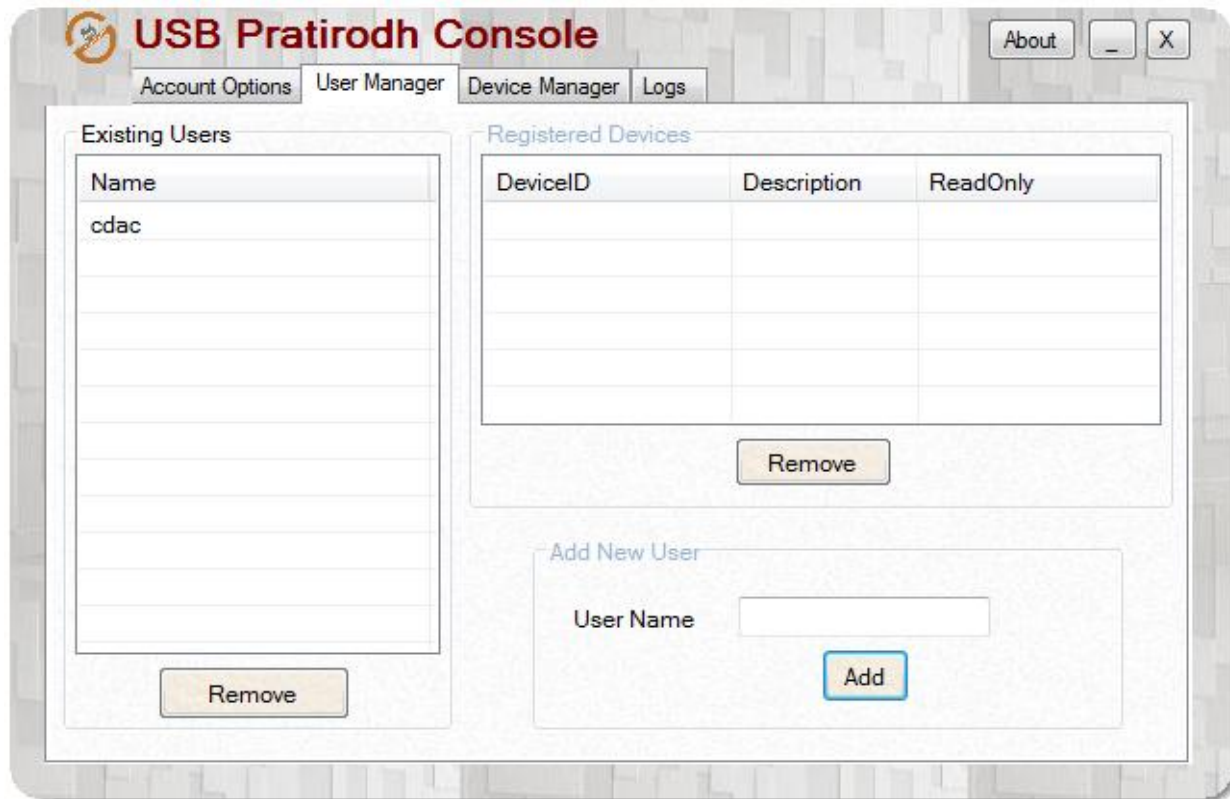
If adding user fails:

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

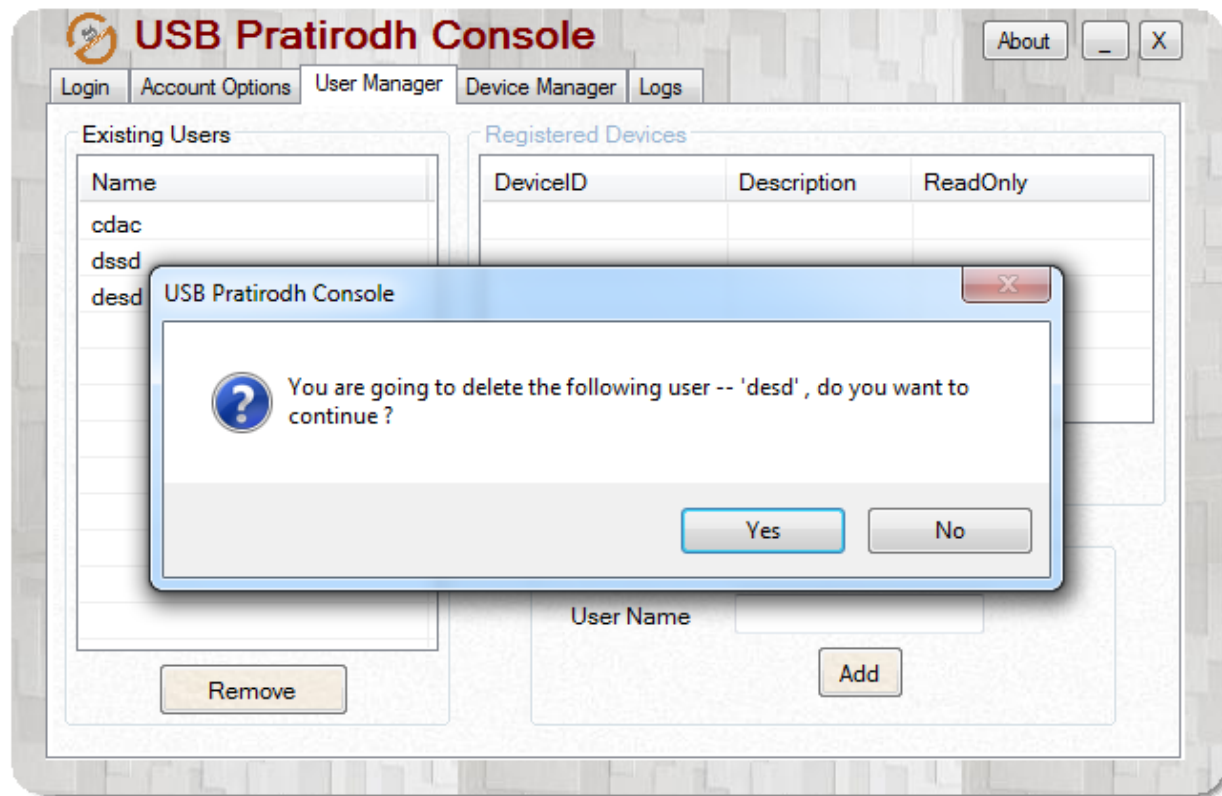




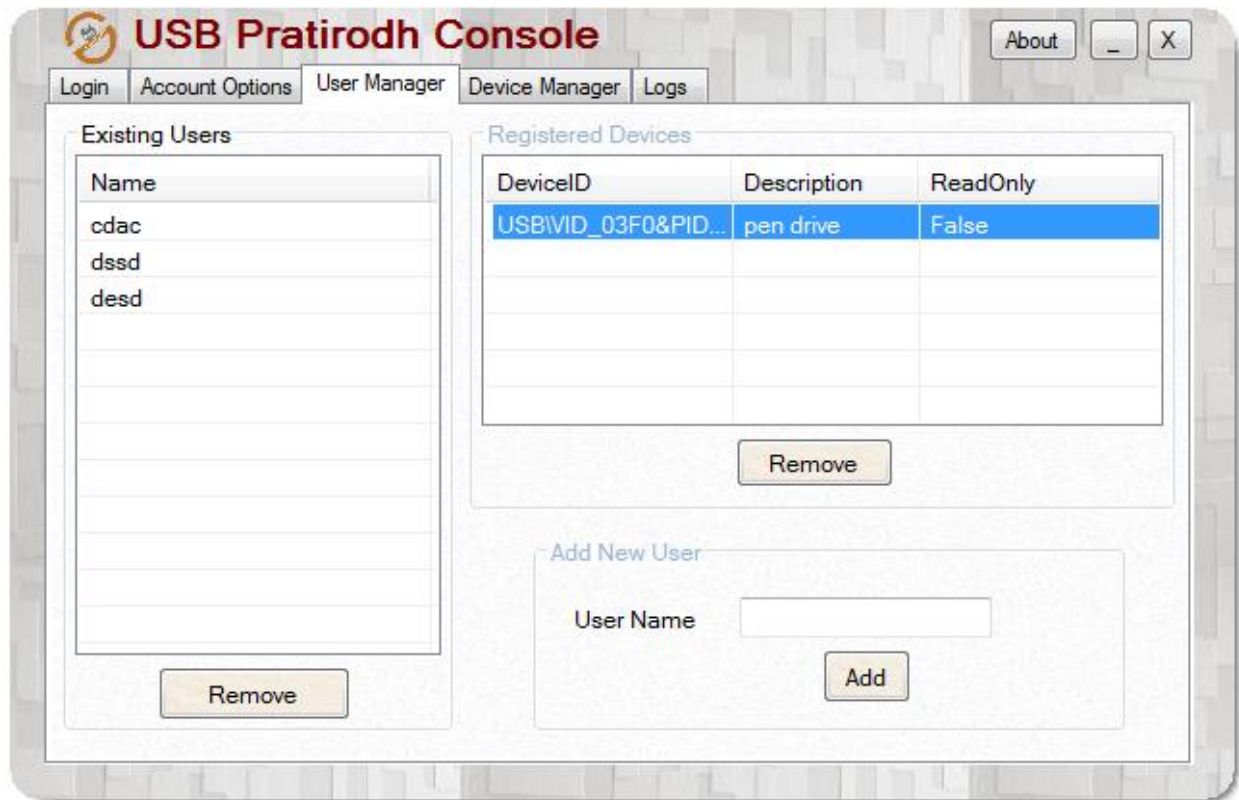
If succeeds:



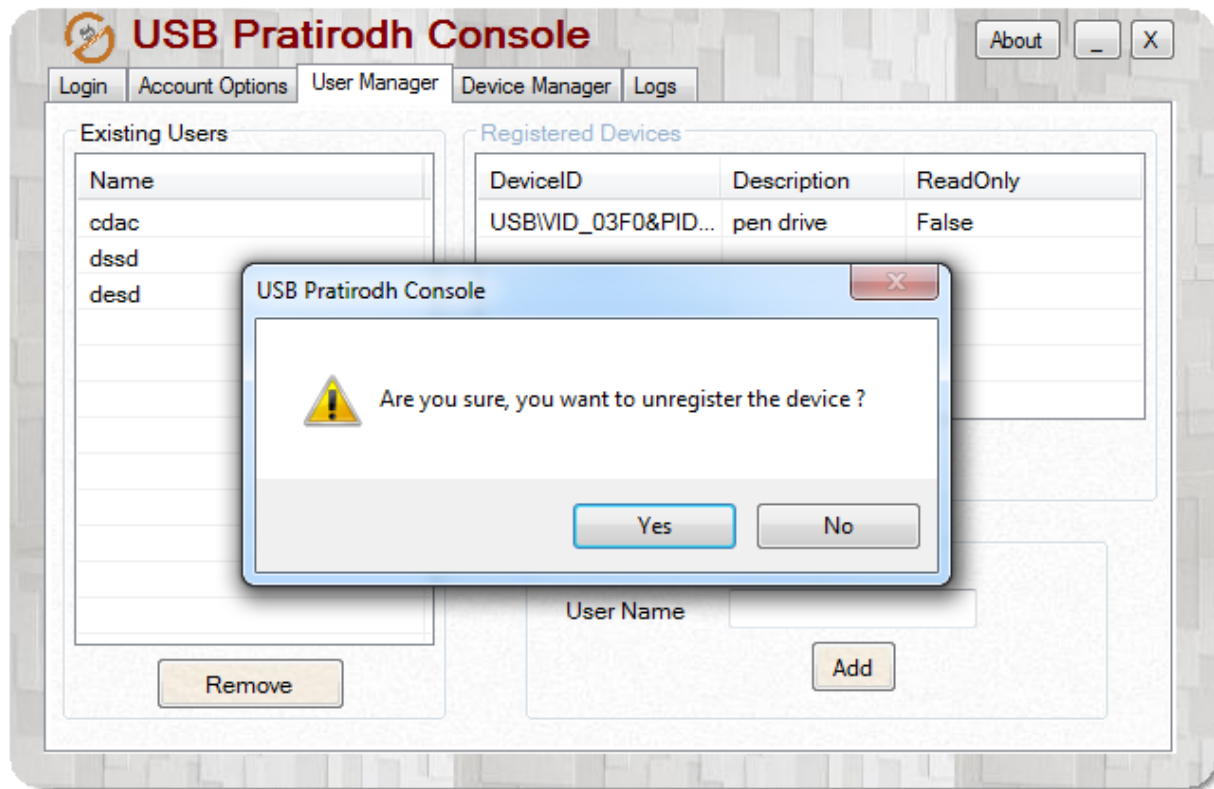
The Administrator can remove any of the existing users by selecting a user from the list and then clicking on the “Remove” button at the bottom of the list or clicking the mouse right on the user which you want to remove and select the “Remove User” option, and then clicking the “Yes” button in the popped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



The administrator can Un-Register any of the listed devices from the list by selecting it and 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 user 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

The Description text field, Here the administrator will describe the device with in 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.

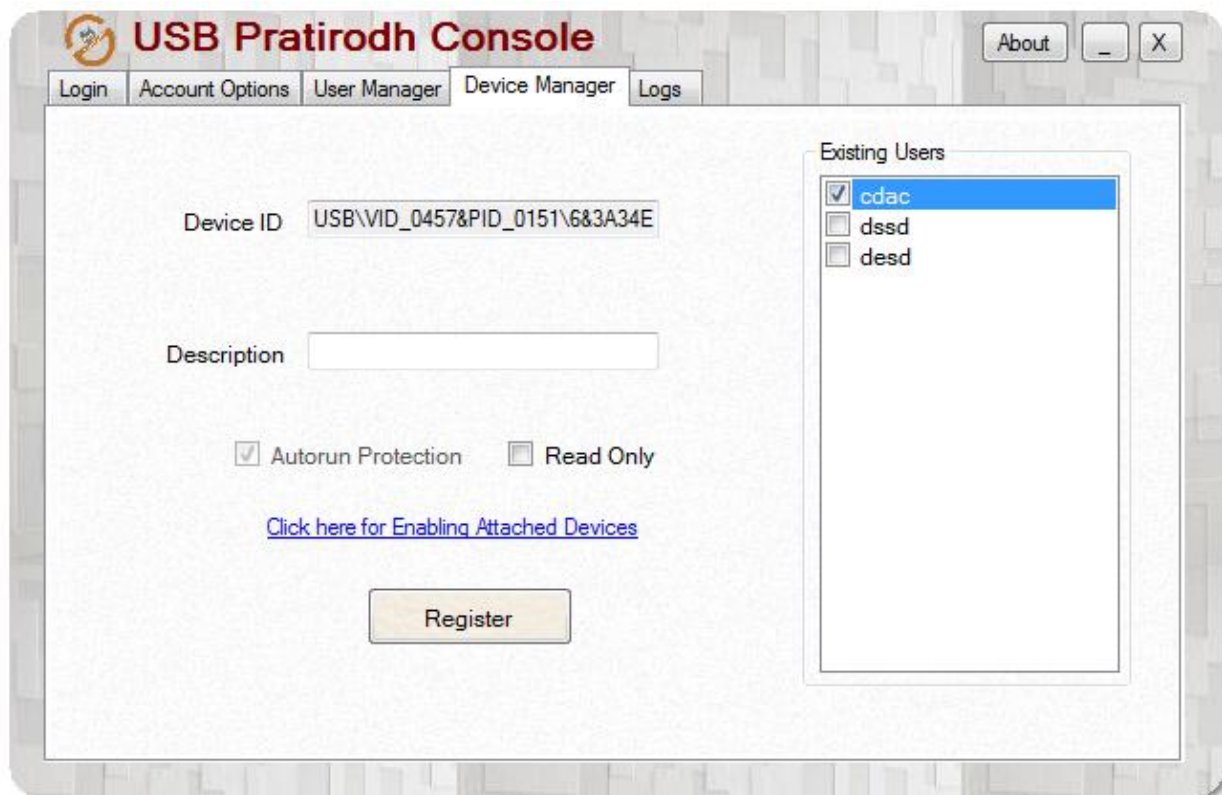
Autorun Protection Check Box, This will allow adding autorun.inf protection for the USB Mass Storage device

Read Only Check Box, Using this functionality an USB Mass Storage device can be registered as read only. If the device is registered as read only, 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 corresponding device's device id will be filled in Device ID text box for registering with user.

The following figure illustrates the scenario that whether the particular device is registered to particular user or not. If device is registered with particular user then that user's check box will be checked and deactivated. If it is not registered yet then particular user's checkbox will not be checked and 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 need to select the user to which the new device is to be registered/ bound and also the administrator need to provide some description of the device for better identification and then clicking the Register button will do the job.

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

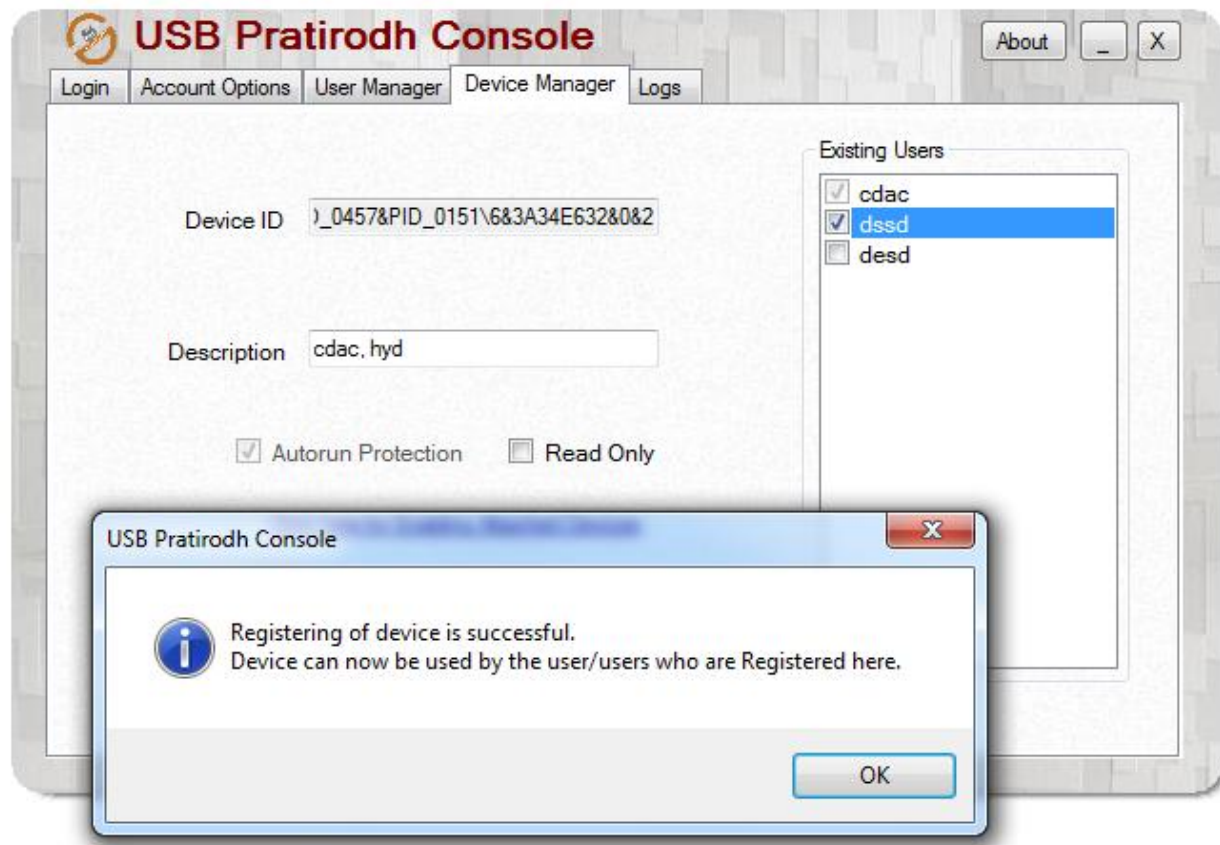


If a device is removed from the list of a user then the device must be registered to that user again to gain access.

* 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 administrator is logged in.



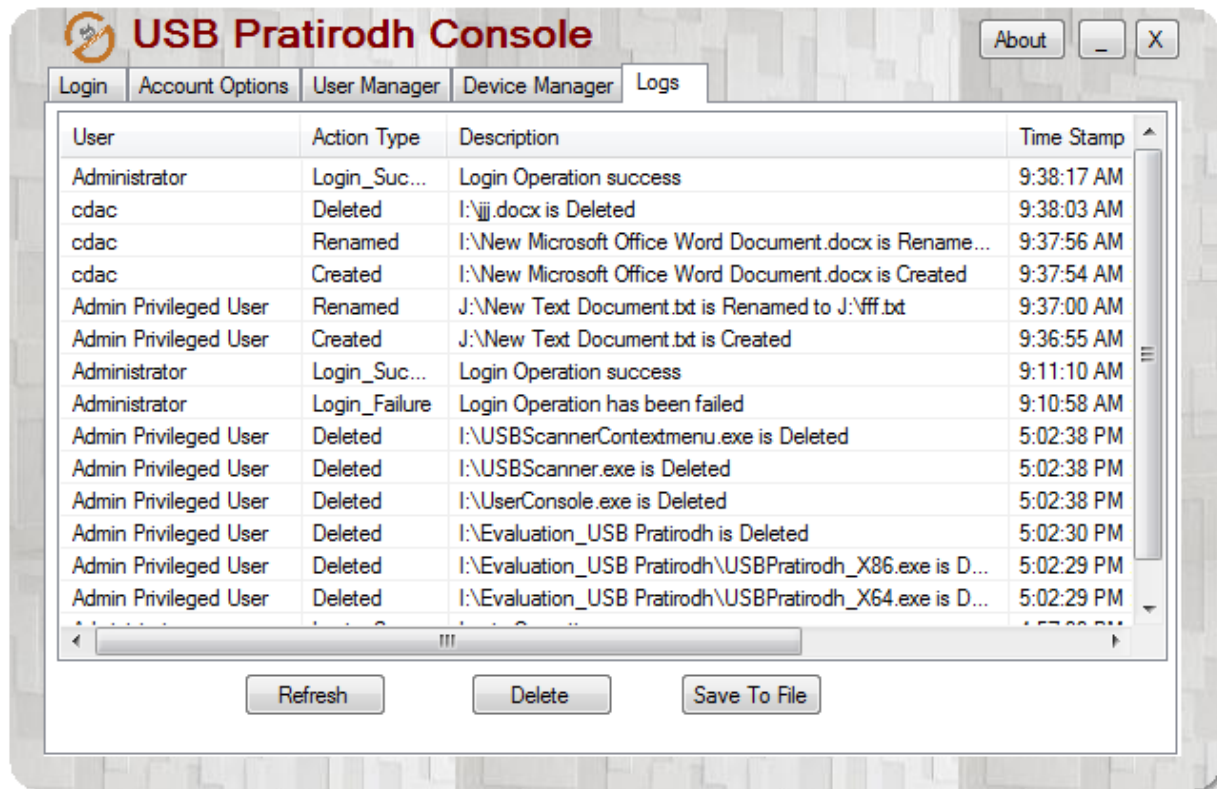
After registering the device with particular user and if you want to register the device with another user then also user needs to insert the device, then one message will popped up saying “This device is already Registered, do you want to Register with some other users”. If user wants then he can proceed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

- If file has been created in USB device then “xxx file is created” log will come.
- If file has been renamed in USB device then “xxx file is renamed to yyy” log will come.
- If file has been deleted in USB device then “xxx file is deleted” log will come.
- If Login Operation success/fail then “Login operation success/failure” log will come.



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



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

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

2 Using already registered USB storage device

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

USB Pratirodh User Login

User Name

Password

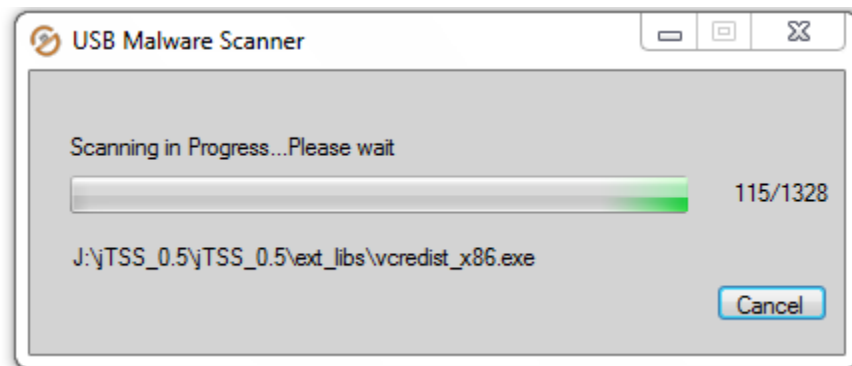
Login Cancel

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

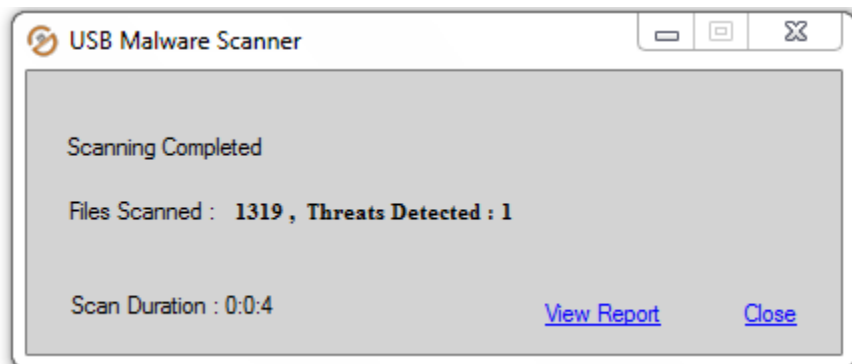




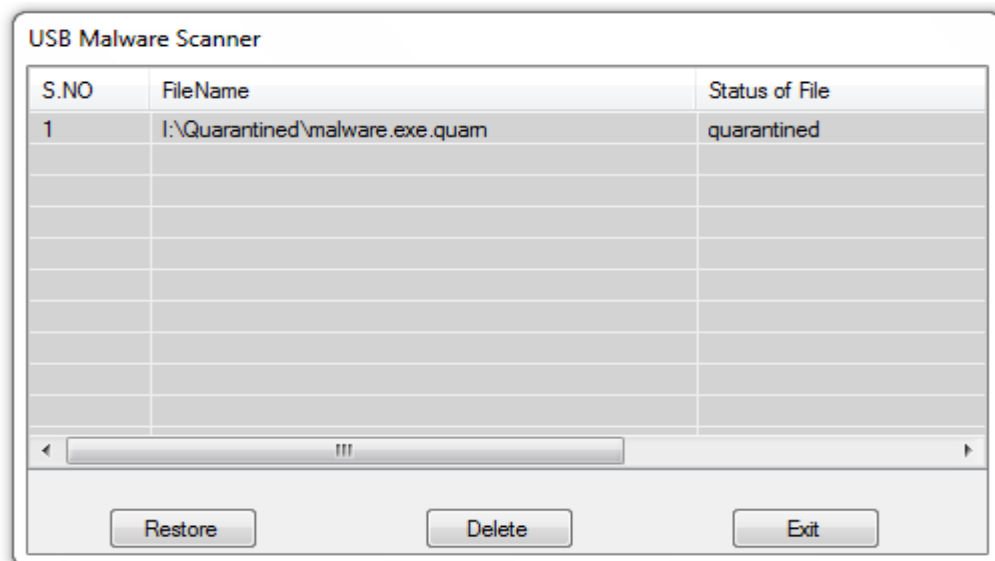
After enabling the device, Scanner named “USB Malware Scanner” starts automatically for scanning your USB Mass Storage device for malware. Wait for sometime till scanning is completed.



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

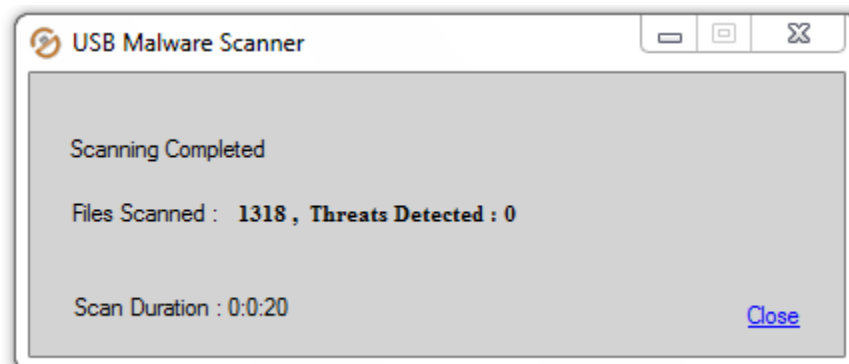


If user wants to see the report he needs to click “View Report” link. If any malware has been detected, then below window will appear. If any malware is detected then it is automatically quarantined and saved in the folder named “Quarantined” which is created automatically in the USB device. If you want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



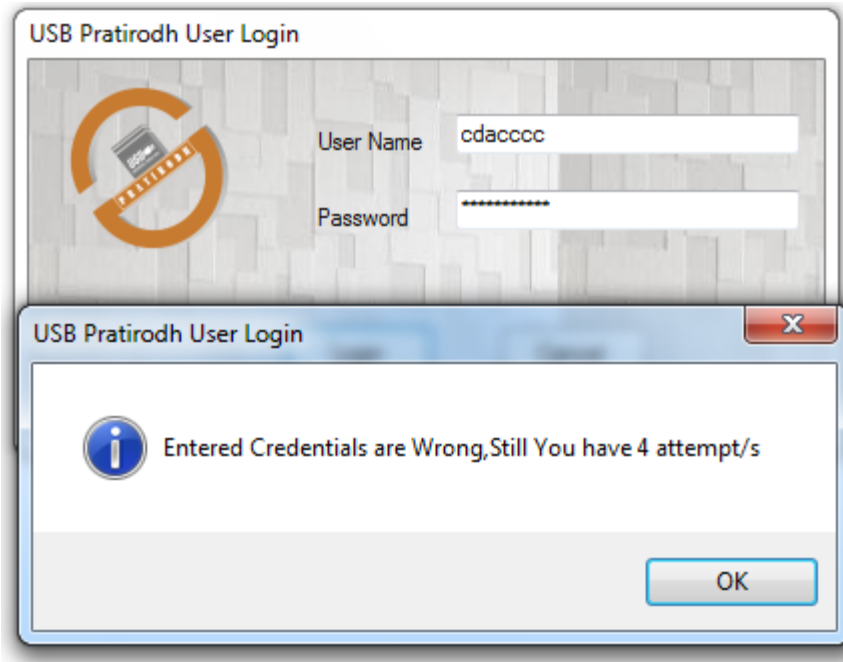
If user clicks “Restore” button then malware will be restored in the USB device’s “Restore” named folder. This folder is created automatically when we click on Restore button.

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



Note: It is recommended that 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 wrong credentials then appropriate message will be appeared.

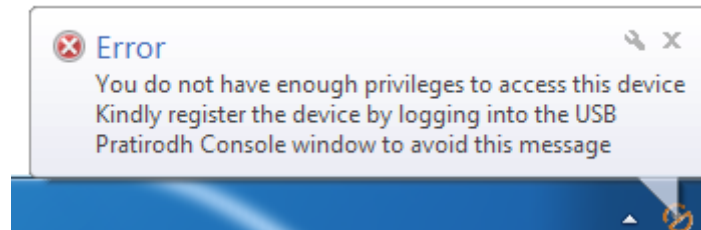


(Note: - The user should provide the details within 60 seconds from the pop up of the login screen. After 60 seconds the above screen will disappear and a message box will appear with the message “Session has been expired, please reinsert the device and try again.” and the device will be blocked. If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

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

2.1 Using unregistered USB storage device

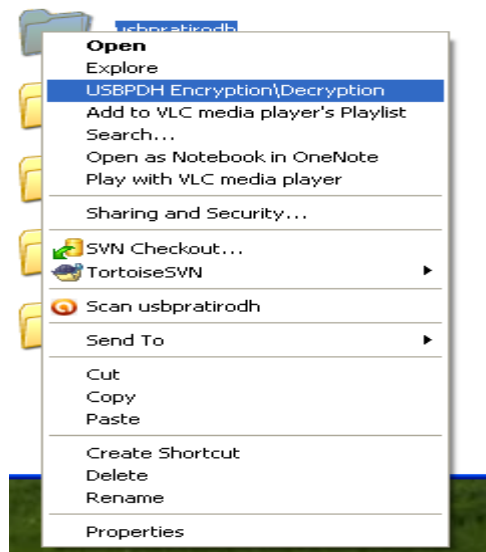
If the administrator is not logged in and a new device is plugged in (which is not registered with any user) then the following balloon tip will appear.



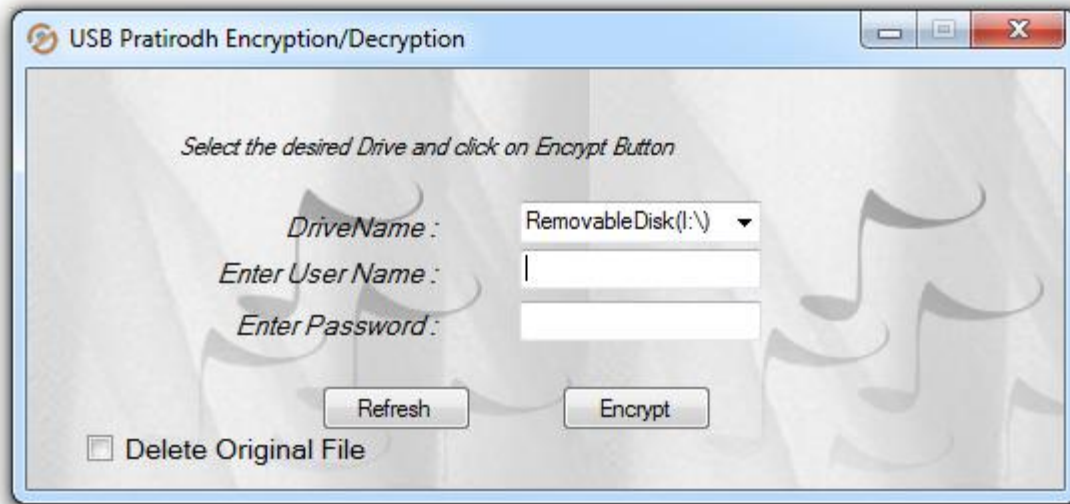
2.2 Encryption:

This feature is to provide security to your sensitive data. If you want to keep any confidential information into any USB Mass storage device you can save the data in encrypted format, it 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 context menu i.e “USBPDH Encryption\Decryption”.



Click on “USBPDH Encryption/Decryption” menu. Then following GUI will be appeared.

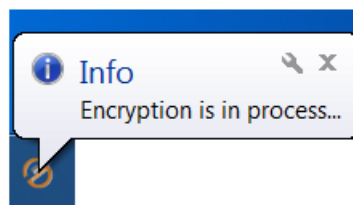


Press refresh button, it displays all attached devices those are authenticated in dropdown box, select any one of them, give the user name and password and press encrypt button, encrypted file or folder will be stored in the selected device.

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

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

While encryption balloon tip displays the status of encryption.





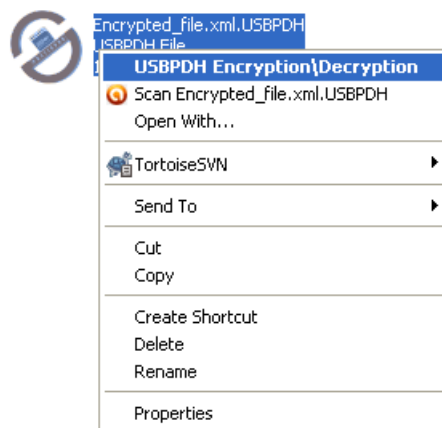
Select the check box of “Delete Original File”, then original file will be deleted from the system. Only encrypted will be present in the device.

Whenever the encryption process completes following message box will appear.



2.3 Decryption:

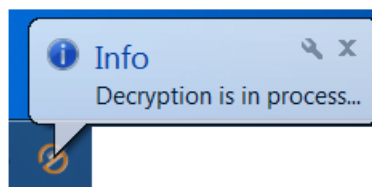
To decrypt any folder or file which is in encrypted format(Which file/folder contains the extension .USBPDH, then user needs to understand that, the file/folder encrypted by using USBPratirodh software), then right click on folder/file then in the shell extension , find the “USBPDH Encryption/Decryption”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



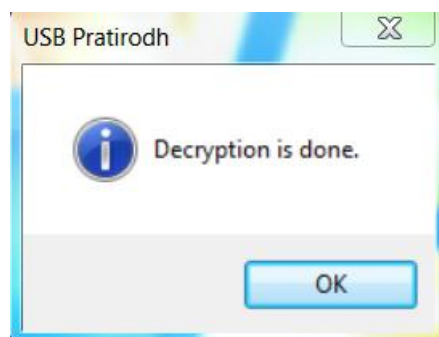
Click on “USBPDH Encryption/Decryption” menu. Then GUI will be appeared.



Give the destination path, user name, Password which user has given while encryption and click on “Decrypt” button, then file or folder will be decrypted and saved in the selected path. While 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 same.

3. Read Only and Encryption feature is not provided to the Mobile Phones.