Installation Guide

Table of Contents

License and Terms

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

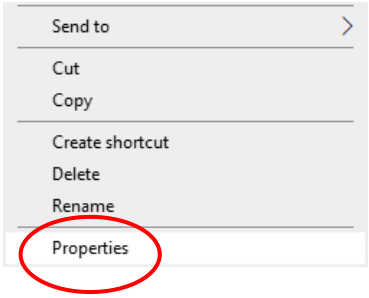
You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

For more details visit https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

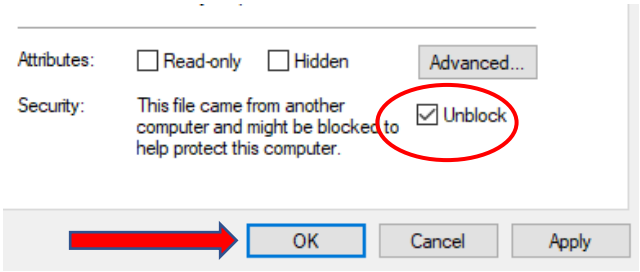
Installation

Remove Windows Security block if present for the passwdhk application file

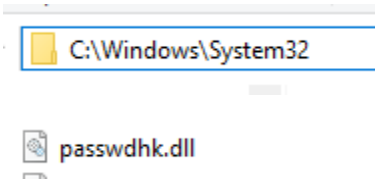
Right-click the passwdhk.dll file and choose properties



Check the box 'Unblock' and press 'Ok'. If the file properties does not contain the security block, just press 'Ok' to close the dialog.

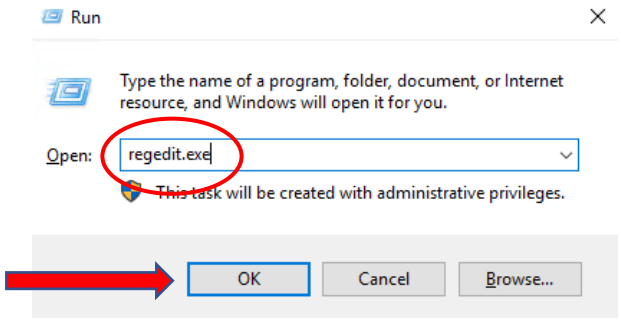


Copy the passwdhk.dll file to C:\Windows\System32



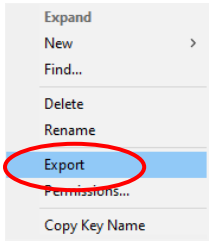
Open the registry editor

- Pressing and holding the Windows Key then pressing 'R' then typing 'regedit.exe' and clicking 'Ok' or pressing enter
- Right-clicking the Windows start menu icon and choosing 'Run'



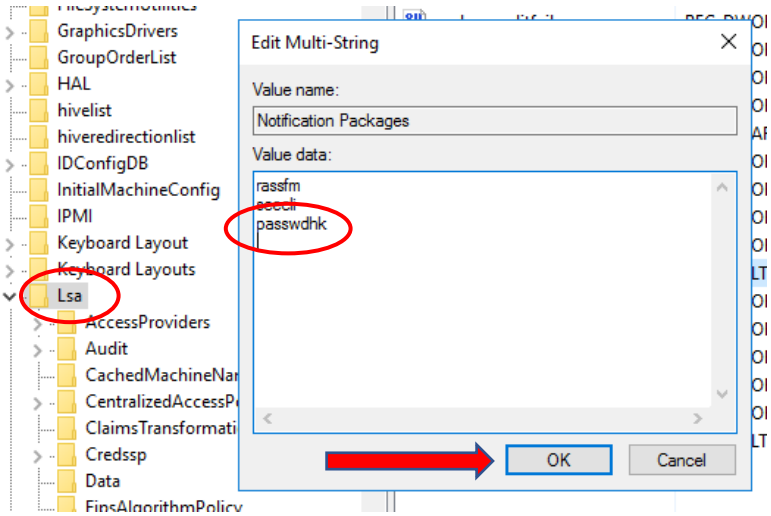
Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Right-click the 'Lsa' key and choose 'Export'



Save the export file to a safe place, i.e network share and/or external drive, NOT stored on the server itself

Right-click the 'Notification Packages' entry and on a new line type in 'passwdhk' exactly, lowercase, without the quotes. Press 'Ok'



Now would be a good time to double-check your entry, open up the 'Notification Packages' entry again and make sure it looks like the screenshot, you might now have other entries such as 'rassfm' but your entry for 'passwdhk' should look exactly the same.

Close the registry editor, DLL installation complete

Open the 'passwdhk.reg' file in your favorite text editor such as Notepad++.

Edit the value entries for your environment, you must escape all special chars \\, each defined below:

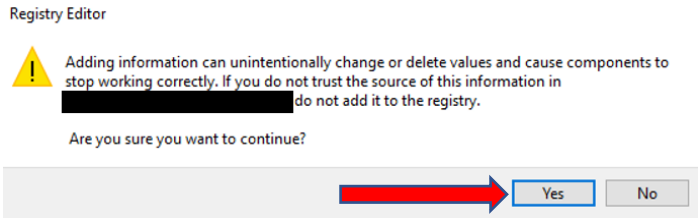
- preChangeProg: Full path to pre-change program exe, such as C:\\Windows\\System32\\cmd.exe
- preChangeProgArgs: Arguments to pass to program
- preChangeProgSkipComp: Skip computer accounts
- preChangeProgWait: Max execution to wait for response in milliseconds
- postChangeProg: Full path to post-change program exe, such as C:\\Windows\\System32\\cmd.exe
- postChangeProgArgs: Arguments to pass to program
- postChangeProgSkipComp: Skip computer accounts
- postChangeProgWait: Max execution to wait for response in milliseconds
- loglevel: Logging level, 0 = OFF, 1 = Error, 2 = Debug, 3 = All
- logfile: Full path to log file such as C:\\WINDOWS\\System32\\LogFiles\\passwdhk.log
- maxlogsize: Maximum log size in bytes
- output2log: Should log be used
- workingdir: Full path to current working directory
- priority: CPU priority, 0 = Normal
- urlencode: toggles URL encoding of password. Must be "true" or "false"
- doublequote: toggles encapsulation of password with double-quotes ("). Must be "true" or "false"

Below settings require the use of Powershell and the postChangeFilter.ps1 script

- emailEnabled: enable email notifications
- emailAlert: alert email address
- emailNotification: notification email address
- beenPwnedEmail: use 'haveibeenpwned' to check if password has been pwned
- beenPwnedPassword: use 'haveibeenpwned' to check if user email/account has been pwned
- wordlistUseWildcard: use wildcard match in banned wordlist
- wordlistUseWordlist: use the banned wordlist feature
- syncGSuite: custom, use GSuite sync,
- syncOpenDJ: custom, use OpenDJ sync

Once you have made your changes, import the registry script by right-clicking the file and selecting 'Merge'

Select 'Yes' to Merge then Press 'Ok' to close the dialog.



Installation is complete, Restart your server so the PasswdHk Filter becomes active.

Making Changes

If you need to adjust any settings for PasswdHk, just edit the registry file and re-import/merge which will override any of the values.

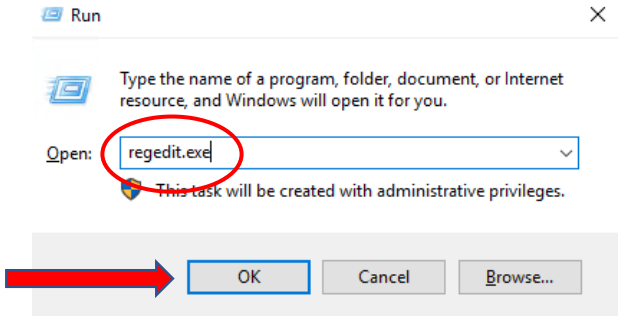
See Page 5 for a settings overview.

Uninstallation

Uninstalling PassWdHk is pretty simple process. We will just reverse the steps in Page 4

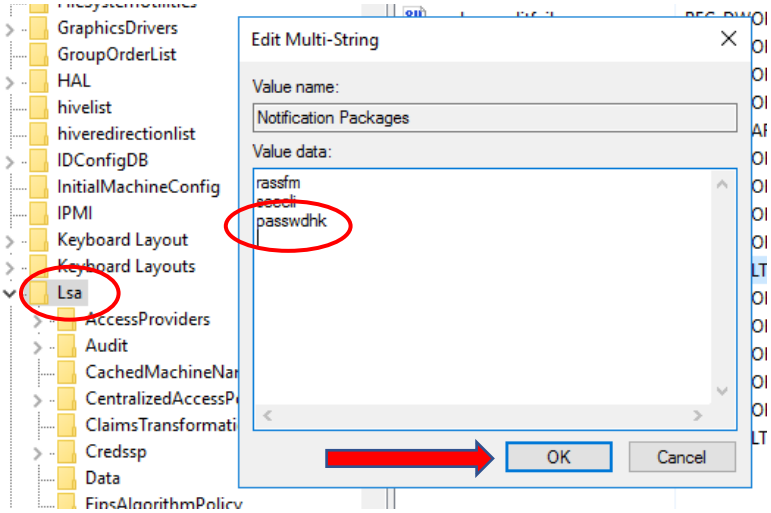
Open the registry editor

- Pressing and holding the Windows Key then pressing 'R' then typing 'regedit.exe' and clicking 'Ok' or pressing enter
- Right-clicking the Windows start menu icon and choosing 'Run'



Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Right-click the 'Notification Packages' entry and REMOVE the 'passwdhk' entry



Again, double-check your entry, open the 'Notification Packages' entry again and make sure it contains the system default value(s). You can open the backup file of the registry you created during install and check the value(s). You could 'Merge' the backup registry but it also contains many other keys and settings and so it is simpler to just edit the 'Notification Packages' entry.

Close the registry editor. DLL installation complete