# Password Checker Installation and usage

## Overview

The passwordchecker Active Directory plugin ensures that users do not set their password to a very common password, such as “Password123!” or “L0veYou!” This is needed because attackers guess these passwords.

This plugin checks against the top 1 million most common passwords, along with a custom list of passwords that are not allowed at our organization such as “COmpanyName!”, because that’s too obvious. If a user attempts to set a password such as “Passw0rd”, they will get an error message saying that password does not meet the required standard; the same message they would get if they tried to use a 1-character password. It is an updated version of the open source project OpenPasswordFilter.

## Installation

To install the password checker on a domain controller, simply run the setup file.

The installer will create a Windows service that does the actual checking. This is so that the password checking can run separately from the windows password change process itself, providing isolation for fault-tolerance. Once the installer is run, the password filtering will go into effect after the DC is rebooted.

After reboot, the service is in place and nothing more needs to be done for installation.

Adding New Disallowed Passwords

There are two ways to add new disallowed passwords.

### Generic common passwords

For generic common passwords, simply add them to this file:

C:\Program Files\Wherever\PasswordChecker\data\opfmatch.txt

Note this process leaves the disallowed passwords readable in plain text, so it should only be used for generic passwords like “Password123!”

### Company-specific passwords that may be in use on the network

Passwords that may actually be in use on the network, such as default passwords that many people know, need to be handled differently. To disallow future re-use of a password that may currently be in use, a hash of the password needs to be added to a different file.

To add custom disallowed passwords that may currently be in use, they can be added to the following file:

C:\Program Files\...\PasswordChecker\custom\_sha256.txt

Each line in the file should the SHA-256 of the lowercased version of the password, which can be obtained with the following Powershell:

$clearString = "**BadPassword!**" # Replace **BadPassword!**With the password you want to disallow

$hasher = [System.Security.Cryptography.HashAlgorithm]::Create('sha256')

$hash = $hasher.ComputeHash( [System.Text.Encoding]::UTF8.GetBytes( $ClearString.ToLower() ) )

[System.BitConverter]::ToString($hash).Replace('-', '').toLower()

This is the appropriate way to company-specific disallowed passwords like “C0mpany2021!”

The SHA256 hash is used in case you want to ban further use a password that is already used in the company. This will prevent the banned password from being used on new accounts, or having the password of an existing account changed to the banned password. Using the hash avoids making the actual password available to anyone who might read the file.

## Technical Details for Developers and Troubleshooting

This software works by adding an entry to the following registry key, which Windows uses to locate password filters:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages

This causes Windows to load c:\windows\system32\OpenPasswordFilter.dll on reboot.

When someone tries to change a password, the dll is called to check whether the password is acceptable. To find out, the dll calls a Windows service that is installed as part of this package. This service is named Passwordchecker. The service is an application custom-built at for this project. It uses the index files in the application data\ folder to very quickly check whether the requested password is allowed.

Any questions on this software can be sent to deepmagicbeginshere@gmail.com

It can be found on GitHub as https://github.com/sensei-hacker/OpenPasswordFilter/