Prevent Weak Passwords

nFront Security
Where Security & Solutions Intersect™

nFront Password Filter™
Multiple Policy Edition

"Password123" is not an option

The nFront Password Filter is designed to seamlessly protect your network by enabling the implementation of strong password policies to all end user accounts. This software also includes a flexible configuration to enforce almost any password criteria possible using a solution that is integrated at the Windows operating system level.

An optional and **fully customizable dictionary blacklist** used by nFront Password Filter is a plain text file that you can easily edit. Now you can stay one step of hackers (or auditors) and load the dictionary files used by common password cracking programs. The days of periodically running password crackers and scanning for poorly chosen passwords are over when you implement nFront Password Filter.

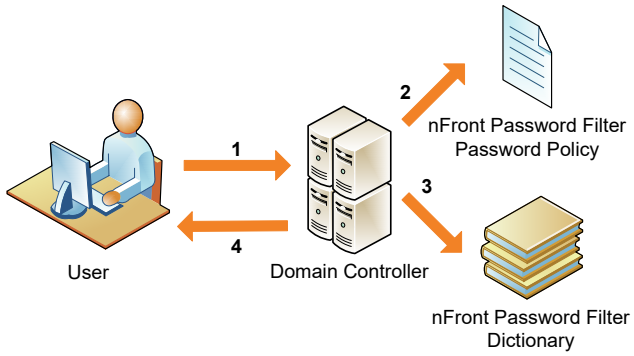
Check each user's password change against 847 million **breached passwords** in less than 60 milliseconds.

Multiple Policies to Protect High Risk Accounts

Has an external auditor ever cracked the password to an administrator's account? How about someone in the Finance department or one of the Executives? nFront Password Filter MPE gives you the flexibility to establish multiple password policies with different restrictions for different global and universal security groups. Now you can make sure wireless users, administrators and executives use sensible passwords that cannot be cracked by many of the common dictionary password crackers.

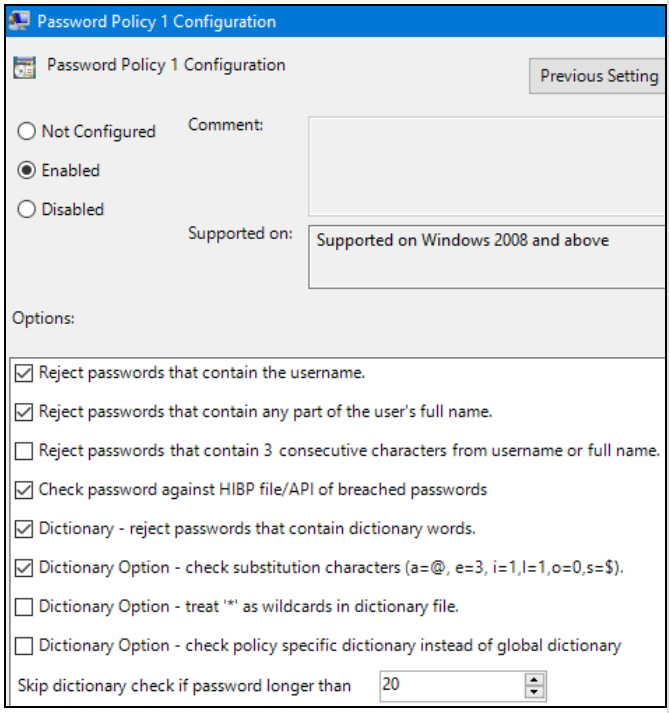
How It Works

nFront Password Filter is a package that you load on all of your domain controllers. All password changes for domain user accounts must go through the password filter DLL. Once loaded, there is no way around the DLL.

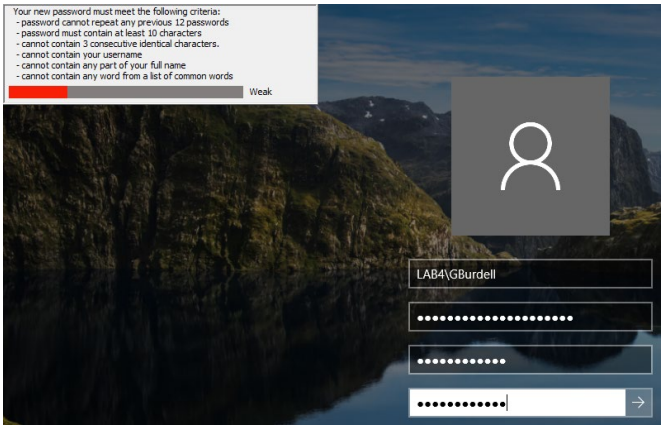


1. User submits password change.
2. LSA calls nFront Password Filter. nFront Password Filter consults password policy.
3. nFront Password Filter may check dictionary.
4. nFront Password Filter tells LSA if password is acceptable. User's password change is accepted or rejected.

www.nFrontSecurity.com
Who's enforcing your password policy? ™
US and Canada ph: 800-676-1513 International: 404-348-4678 email: sales@nFrontSecurity.com



nFront Password Filter Policy Settings



Optional client displays rules and optional strength meter

Advantages

- Easy to deploy and configure.
- Controlled by a Group Policies.
- Multiple Policies improving upon Windows AD weak policy options
- No SPOF [Single Point of Failure]. No network API calls leave the local DC ensuring that you never skip password filtering due to an unavailable password policy server.
- Optional dictionary scanning can scan over 1 million common passwords in less than 10 milliseconds.
- Check against 847 million breached passwords in less than 60 milliseconds.

Features

- Flexible configuration.
- Fast filtering engine.
- Rules to ensure password compatibility with UNIX and AS/400.
- Works with 64-bit versions of 2008, 2012, Server 2012R2, Server 2016, Server 2019, and Server 2022.
- Fully customizable dictionary supporting multiple languages.
- Optional multilanguage client which can inform users of password policy rules and provide exact reasons why a password change was rejected.
- Client works with Windows 7, Windows 10 and Windows 11.
- Separate web application available for an improved password change experience.

Learn More

Visit http://www.nFrontSecurity.com to learn more about nFront Password Filter and password hacking.

5 minute demo / evaluation

View the 5 minute demo online. In 5 minutes see the installation and configuration of 2 password policies.

Try It

You can download a 100% operational evaluation copy at www.nFrontSecurity.com.

www.nFrontSecurity.com
Who's enforcing your password policy? ™
US and Canada ph: 800-676-1513 International: 404-348-4678 email: sales@nFrontSecurity.com