

nFront Password Filter™ Single Policy Edition for Desktops

Protecting the Integrity of Your Network

nFront Password Filter supports a single password policy that applies to all local accounts on desktops. nFront Password Filter is designed to seamlessly protect your network by forcing sensible passwords. nFront Password Filter prevents weak passwords and gives you the ability to enforce strong passwords using a solution that applies to all local accounts on desktops. The nFront Password Filter is compatible with most Desktop system versions (Windows 2000 Professional - 32 bit only, Windows XP - 32 bit, Windows Vista - 32 bit or Windows 7 - 32 or 64 bit).

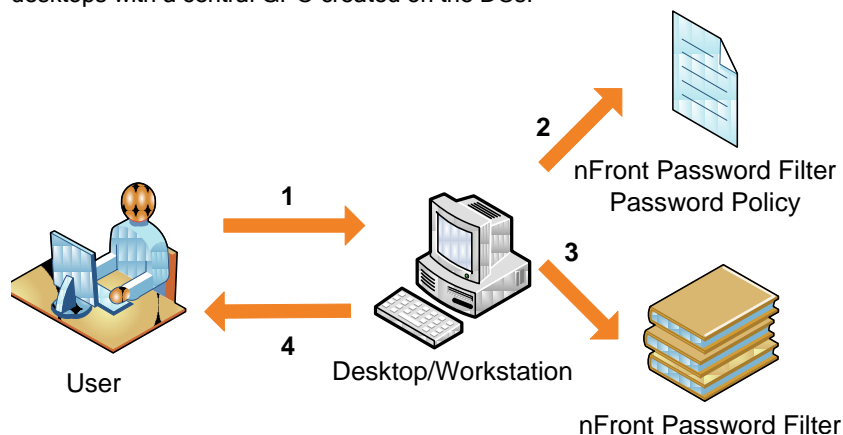
nFront Password Filter offers a very flexible configuration to enforce almost any password criteria imaginable. Furthermore, it includes a dictionary password check. The dictionary used by nFront Password Filter is a plain text file and 100% customizable. Now you can stay one step of hackers and load the dictionary files used by their password crackers. This leaves only a brute force attack and forces hackers to seek easier prey. The days of periodically running password crackers and scanning for poorly chosen passwords are over when you implement nFront Password Filter.

Stronger than Windows Built-In Complexity

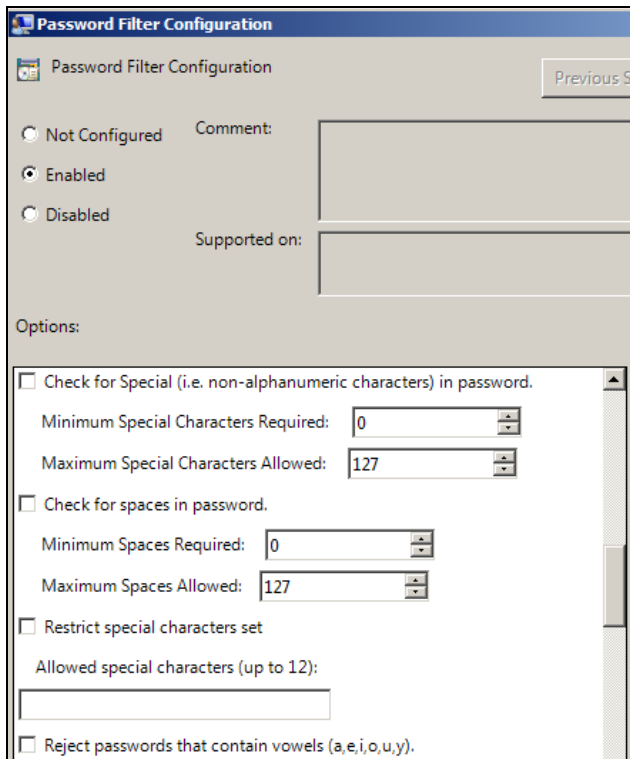
Windows built-in complexity still allows for weak passwords such as "Password1". Having a good password policy that is enforced across all users is fundamental to good security practices. You are probably already spending money on firewalls, anti-virus, encryption and data leakage products. However, if you are using the built-in Windows Password Policy you might as well burn the money you are spending for all the security software and devices. nFront Password Filter enforces the use of stronger passwords so your company does not fall victim to costly data breaches due to the use of stupid passwords.

How It Works

The GPO can be locally edited on each workstation but this would not be reasonable for a large number of clients. If the client machines are joined to the domain the settings can be pushed to the desktops with a central GPO created on the DCs.



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.



nFront Password Filter Group Policy

Advantages

- Easy to deploy and configure.
- Controlled by a Group Policies at local or domain level.
- 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!
- Performance. If dictionary scanning is used, nFront Password Filter can scan over 2.5 million common passwords in less than one second.

Features

- Very flexible configuration.
- Very fast filtering engine.
- Compatible with most Desktop Editions (Windows 2000 Professional - 32 bit only, Windows XP - 32 bit, Windows Vista - 32 bit or Windows 7 - 32 or 64 bit). * The product does not support x64 versions of Windows XP and Windows Vista.
- Fully customizable dictionary supporting multiple languages.

Learn More

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

5 minute demo

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 from www.nFrontSecurity.com.