nFront Password Filter

Multiple Policy Edition for Domain Controllers
Single Policy Edition for Domain Controllers
Single Policy Edition for Member Servers
Multiple Policy Edition for Member Servers
Desktop Edition

Version 6.2.0

Documentation

Contents

NOTE: Please report any problems with this document to feedback@nFrontSecurity.com. Your feedback is important and we sincerely appreciate your help.

1.0 nFront Password Filter Overview

nFront Password Filter provides a robust granular password policy system for Windows Active Directory, member servers and workstations. You may use it to enforce one or more very granular password policies. The comprehensive policy settings allow you to increase network security by preventing the use of weak and easily hacked passwords. Policies can target users that are organized into groups or OUs.

1.1 Versions

nFront Password Filter can be installed on domain controllers to filter passwords for Active Directory users. It may be installed on Windows servers (both member servers and standalone servers) or desktops (Windows XP – Windows 10) to filter password changes for locally defined users. In all cases 32 and 64 bit machines are supported.

The same nFront Password Filter MSI package may be used on domain controllers, member servers or desktops. The GPO template determines how the software performs (i.e. filters AD user passwords or passwords of local users on member servers or desktops).

There are 2 versions for Windows Active Directory users. Each version runs on domain controllers and filters password changes for users in the Active Directory:

- ***nFront Password Filter MPE (Multi-Policy Edition*).** The MPE version allows you to have up to 6 different password policies in a single domain. Each policy can apply to one or more global or universal security groups. This is an ideal choice for those who want to promote strong passwords but do not feel they can enforce very restrictive policies across all user accounts. nFront Password Filter MPE can be used to apply reasonable policies to most end-users and very restrictive policies against those higher privileged accounts with access to more secure information.

- ***nFront Password Filter SPE (Single Policy Edition).*** The SPE version contains a single granular password policy that will be applied to all domain users.

Client Support. You can optionally deploy nFront Password Filter Client to domain workstations. The client will provide password policy rules and more detailed reasons for password change failure if the user attempts a non-compliant password. The client also has the option of dynamically gauging the strength of the user's new password.

If you do not wish to deploy client software you may wish to consider our add-on product nFront Web Password Change. It is a web application that provides password policy rules and detailed failure messages to the end-user.

There are 2 versions for Member Servers. Each runs on a Member Server and filters password changes for users defined in the local SAM database:

- ***nFront Password Filter Single Policy Edition for Member Servers.*** SPE for Member Servers allows you to filter the passwords of local accounts on Windows servers. It may

be used on servers that are joined to a domain or servers that are a part of a workgroup. This may be a good solution on servers like database servers or extranet servers where you have many local accounts instead of the standard Administrator and guest account. This version can be controlled via a GPO which is pushed to the server or via a local GPO.

- ***nFront Password Filter Multiple Policy Edition for Member Servers.*** MPE for Member Servers allows you to filter the passwords of local accounts on Windows servers. It may be used on servers that are joined to a domain or servers that are a part of a workgroup. The MPE version supports up to 3 different password policies. The policies can target one or more local groups. This version can be controlled via a GPO which is pushed to the member server or via a local GPO.

There is 1 version for Desktop machines. It runs on a desktop (Windows XP, Windows Vista, Windows 7, Windows 8 or Windows 8.1) and filters password changes for users defined in the local SAM database:

- ***nFront Password Filter Desktop Edition.*** This version filters the passwords of local accounts on Windows desktops. While it is rare to have more than the standard built-in accounts on desktops, this version will ensure any local account is compliant with a granular password policy. This version can be controlled via a GPO which is pushed to the workstation or via a local GPO.

1.2 Compatibility and System Requirements

The nFront Password Filter and nFront Password Filter Client are compatible with both 32-bit and 64-bit versions of the following operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows 2008 R2
- Windows 2008
- Windows 2003 R2
- Windows 2003
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows XP

The software is supported on all server platforms from Windows 2003 through Server 2012 R2 as well as all desktop platforms from Windows XP through Windows 10.

The nFront Password Expiration Service should be run on a Windows Server that is a member of the domain or a domain controller. It is best to run it on a domain controller.

1.3 What's New

What is new in Version 6.2.x?

- Expiration Service was updated to support customization via plain text or html files instead of copying a new email body into the GPO textbox.
- ADMX templates are included.
- Client was modified to better support the release of Windows 10
- Modifications for better performance and logging were added.
- Code modified to log administrative resets even if configured to bypass the filter for admin resets.
- Additional improvement to Windows 10 client.
- Dictionary file modified to default to Unicode instead of ANSI.
- Settings added to provide test email and configure nFront Password Expiration service to send a test email.
- Setting added to force the check of the dictionary even if other rules are not satisfied.
- Setting added to force checking of the entire dictionary even if a match is found.

What is new in Version 6.1.x?

- Support for SAP rules in each policy was added. SAP rules are as follows:
    - Do not allow passwords that start with exclamation or questions mark
    - Do not allow 3 of the same character at the beginning of password
    - Do not allow spaces in first 3 characters
    - First 3 characters of password cannot appear in the username in the same order
- Length-based password aging is now possible. You can configure the settings to allow longer passwords to have a longer maximum password age and shorter passwords to expire more frequently.
- The password expiration email notification service was updated to allow sending of warnings at 3 specific intervals instead of daily.
- Rackspace compatibility rule added - No more than 2 consecutive characters from full name, username or display name.
- A feature to look for an exact dictionary match was added
- The custom message used for email to the end users was modified to remove the "message from your IT Administrator" phrase
- bugfix – client was modified to better support the release of Windows 10.
- bugfix - client was updated to avoid a problem when a password expires and the workstation is locked.
- bugfix - client was rejecting passwords even though the filter was configured to skip passwords longer than a specified length. This is now corrected.

For a more detailed version history see the Appendix for Detailed Version History.

1.3 Notes to Evaluators

- You need a domain controller to test nFront Password Filter MPE. You can test nFront Password Filter SPE or MPE for Member Servers on a standalone server or a member server that is part of a domain.
- What do you wish to achieve with this software? Define you test scenarios and expected output before you get started.

- Do you have a formal written password policy? If so, scan the group policy settings. If you need assistance configuring the policies to enforce your written policy give us a call at 404-348-4678.
- Start simple and then progress until you have all of your policies defined. Once you have a successful Default Policy, move to Policy 1, etc.
- You can use the command line and batch files to expedite your testing

Command line syntax to create 1,000 user accounts:

```
For /L %i IN (1,1,1000) DO net user test%1 valid_password
/add
```

Command line syntax to change a password:

```
net user test1 abc
```

Use Appendix A and B to help you with your policy design and to document the policies as you test them. Also, make use of the troubleshooting guide in Section 8.0.

1.4 Overview of Features

nFront Password Filter includes the following policy settings. nFront Password Filter MPE has a default policy and up to five additional policies. nFront Password Filter MPE policies can be applied or excluded based on membership in global groups.

nFront Password Filter allows you to control the following for each policy:

- Minimum number of characters in password.
- Maximum number of characters in password.
- **Maximum password age
- **Email users password expiration warnings.
- ***Reject a new password that matches the old password by more than X characters
- ***Reject a new password that does not differ from an old password by X characters
- Ensure passwords contain characters from a minimum number of the following four categories: (1) numeric characters (2) upper case characters (3) lower case characters (4) non-alphanumeric characters.
- Minimum and maximum number of numeric characters (0-9)
- Minimum and maximum number of upper case characters (A-Z)
- Minimum and maximum number of lower case characters (a-z)
- Minimum and maximum number of alpha characters (a-z or A-Z)
- Minimum and maximum number of non-alpha characters
- Minimum and maximum number of special (i.e. non-alphanumeric) characters
- Minimum and maximum number of spaces.
- Restrict Special character set to 32 or less specific special characters
- Enforce SAP password rules
    - Cannot start with an exclamation or question mark.
    - First three characters cannot all be the same.
    - Cannot contain a space in the first 3 characters

    - First 3 characters of password cannot appear in the same order in the username
- Reject passwords containing vowels (a,e,i,o,u and y in upper or lower case)
- Reject passwords with 2 consecutive identical characters (e.g. aa, bb, etc.)
- Reject passwords with 3 consecutive identical characters (e.g. aaa, bbb, etc.)
- Reject passwords with 3 consecutive identical characters from the same character set.
- Reject non-ASCII characters (i.e. foreign language characters)
- Reject passwords that begin with a number.
- Reject passwords that end with a number.
- Reject passwords that being with a special character.
- Reject passwords that end with a special character.
- Force passwords to contain a number in a specific position.
- Force passwords to contain a special character in a specific position.
- Reject passwords that do not contain a special character with the first X characters.
- Reject passwords that contain the username.
- Reject passwords that contain any part of the user's full name.
- Reject passwords that contain 3 consecutive characters from the username or user's full name.
- Reject passwords that contain words from a customizable dictionary.
- Reject passwords that contain words from a customizable dictionary and use character substitution (example: p@$$w0rd)
- ** Apply the policy to multiple security groups or OUs. Nested groups are supported.
- ** Exclude multiple security groups or OUs from the policy. Nested groups are supported.
- ** Apply or exclude policy from users with non-expiring passwords.

** Only applies to MPE version.
*** Only works if the password change is made via the nFront Password Filter client or nFront Web Password Change.

1.4.1 The logic behind multiple policies (MPE version only)

nFront Password Filter MPE provides a default policy and 5 others. You should use the default policy to implement the least restrictive policy that will apply to all Domain Users. Certain security groups and/or OUs can be excluded from the policy (like groups for service accounts). Use policies 1-5 to implement more restrictive policies for IT staff, executives, financial staff, etc. People with access to sensitive data and resources should have stronger passwords. Also, if you are using a RADIUS server or Cisco LEAP authentication server, your wireless user's passwords are vulnerable to a dictionary or brute force attack. A dictionary check for those users would be ideal.

The application of password filtering policies works just like permissions within the file system. You first decide who gets the policy. Then you decided if any users who will get the policy should be excluded. Remember this: "The only time you need to exclude a group is when members of that group are already included."

If a user is a member of three groups and each has a different policy applied, the user must select a password that complies with all three policies. You must take this into account with your policy design.

1.4.2 The Message Box for Rejected Passwords

If a user's password is rejected by nFront Password Filter, the user will get the generic Windows message box stating:

"Your password must be at least X characters long and cannot repeat any of your previous X passwords. Please type a different password. Type a password that meets these requirements in both text boxes."

This message is generated by the msgina.dll or credential provider on each local client.

To present the user with a list of password policy rules and a better failure message, consider deploying the optional nFront Password Filter Client to some or all client workstations. Please reference Section 9 for more information.

1.5 Information about your Evaluation Copy.

The evaluation code is listed in the email you received after downloading the software.

The evaluation code unlocks the software until the expiration date. If you have not purchased and registered your copy of nFront Password Filter, you should be aware of the following:

- AFTER THE EXPIRATION DATE ALL PASSWORD CHANGES WILL NOT BE FILTERED.
- YOU CAN PURCHASE THE PRODUCT AND ENTER THE REGISTRATION INFORMATION WITHOUT REBOOTING OR RE-LOADING THE DLL.

THE EVALUATION VERSION IS FULL FEATURED AND 100% OPERATIONAL UNTIL THE EXPIRATION DATE.

1.6 List of files included with nFront Password Filter

Filename	Purpose
nFront Password Filter.msi	Installation file. Contains ppro.dll, ppro-eng.dll, ADM templates, dictionary file, group filter service file, password policy service file and documentation.
nFront Password Filter x64.msi	x64 version of filter.
nFront Password Filter Client.msi	Optional package for domain workstations.
nFront Password Filter Client x64.msi	x64 version of client.
nFront Password Expiration Service.msi	Service to handle different password aging policies. To be installed on a single DC and only applies if using nFront Password Filter MPE.
nFront Password Expiration Service – x64.msi	x64 version of password expiration service.
nFront Password Filter Documentation.pdf	This document.
adm-templates.zip	The ADM templates will be installed to the windows\inf folder when you install the nFront Password Filter package. However, they are provided separately in case you wish to setup the GPO before deploying the MSI package.
admx-templates.zip	These are provided for customers who wish to use ADMX templates instead of ADM templates.

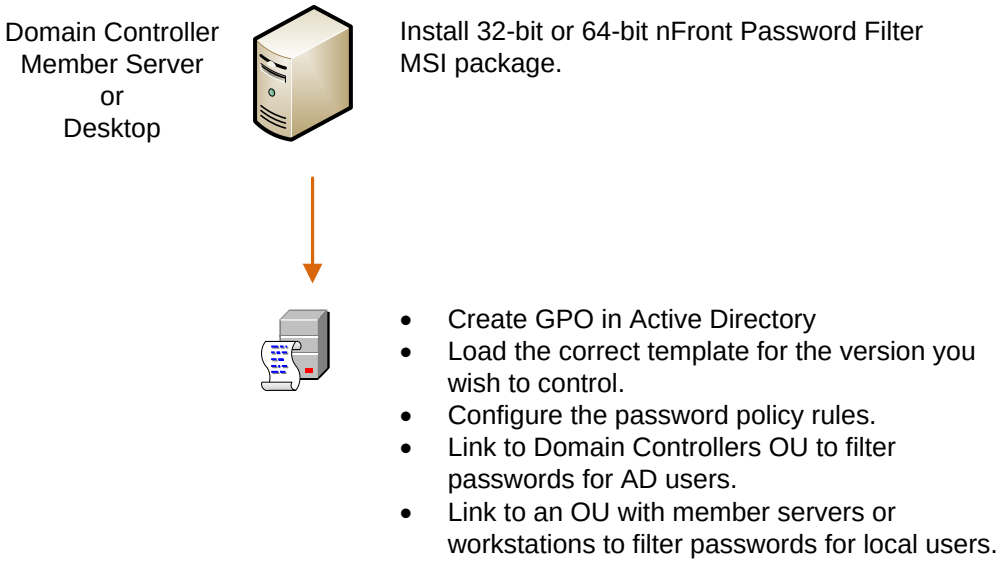
2.0 Installing nFront Password Filter

Please note there are not different MSI packages for domain controllers, member servers and desktops. You will install the 32-bit or 64-bit MSI package on the target domain controllers, member servers or workstations. Then you will load the correct GPO for the version you wish to control. It is the GPO template that determines how the filter engine behaves and the type of operating system on which it will run.

The instructions in this document will focus on installing nFront Password Filter MPE for domain controllers. Where appropriate, instructions are given for other versions and operating systems.

2.1 Deployment Overview

Below is a graphic overview of the deployment process. The remaining portion of this section will give detail of the installation and section 3 will cover the configuration options.



2.2 Optionally disable Windows password complexity

You do not have to disable the Windows password complexity requirement. However, if your nFront Password Filter settings will be less restrictive than the Microsoft complexity rules, you should disable the Windows password complexity rule.

1. Start + Programs + Administrative Tools + Domain Security Policy + Security Settings + Account Policies + Password Policy
2. Disable policy for “Passwords must meet complexity requirements” (Figure 2.2.1).

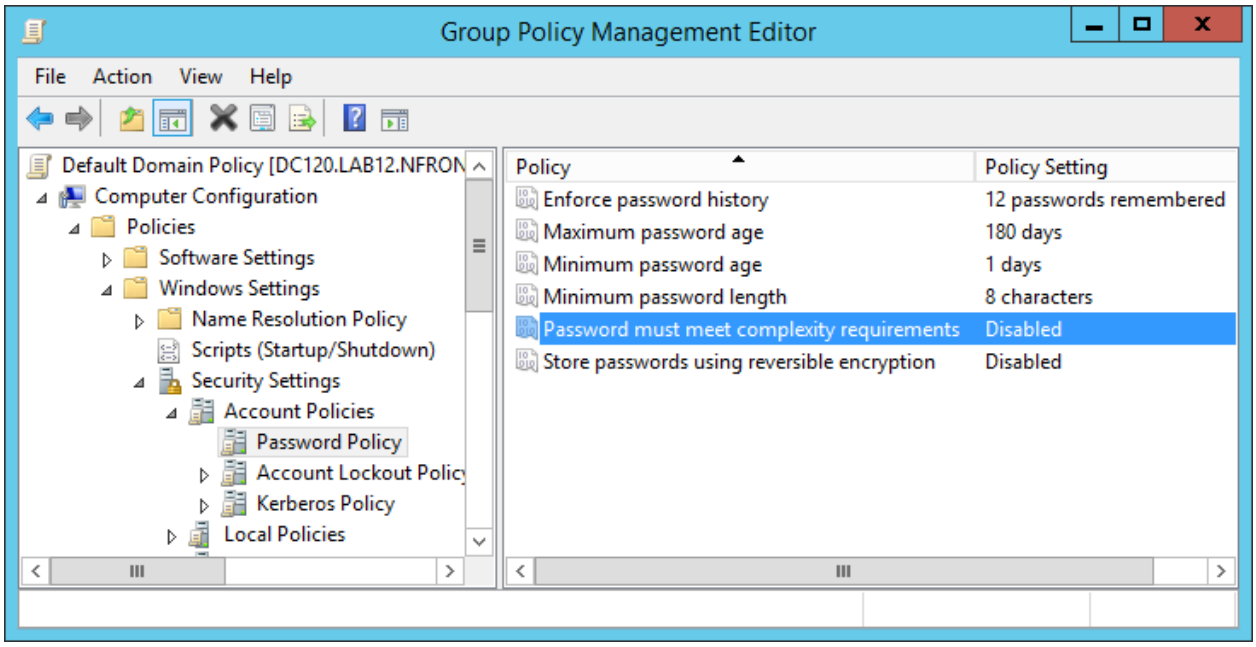


Figure 2.2.1: Disabling Microsoft password complexity check

2.3 Run nFront Password Filter Installer

Double-click the nFront Password Filter.MSI file to run the installation wizard. Be sure to run the x64 version if you are installing on an x64 server. You will see the screens displayed in figures 2.3.1 through 2.3.6.

Figure 2.3.1: Installation screen 1.

Figure 2.3.2: Installation screen 2.

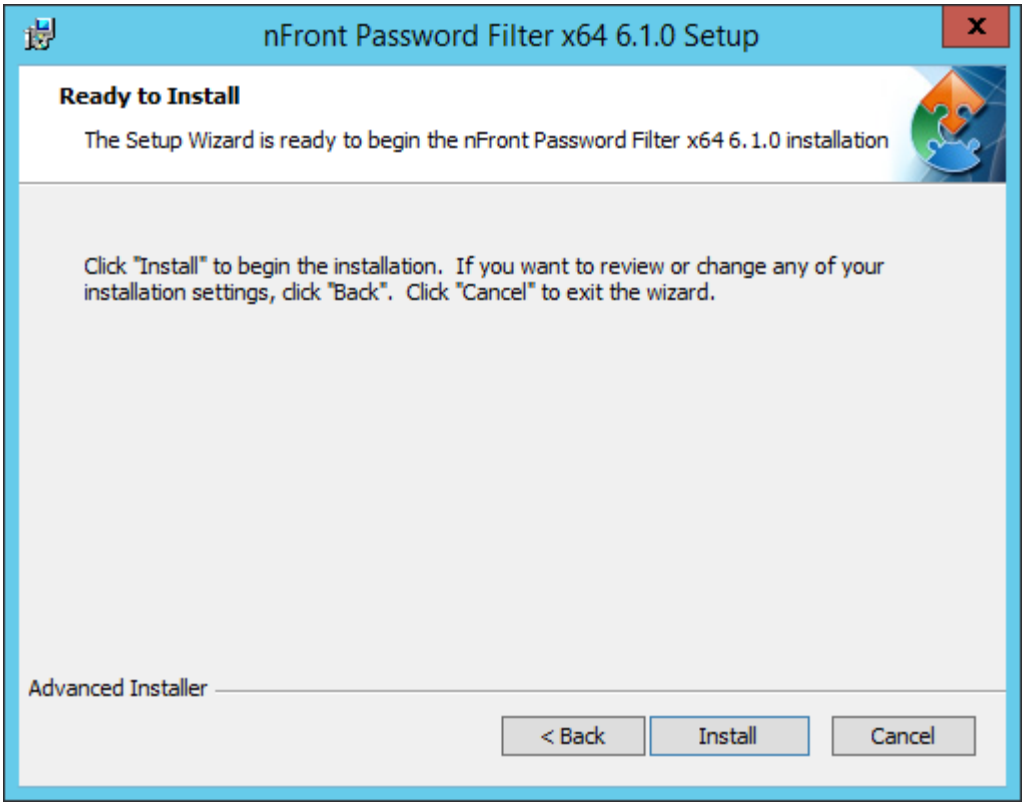


Figure 2.3.3: Installation screen 3.

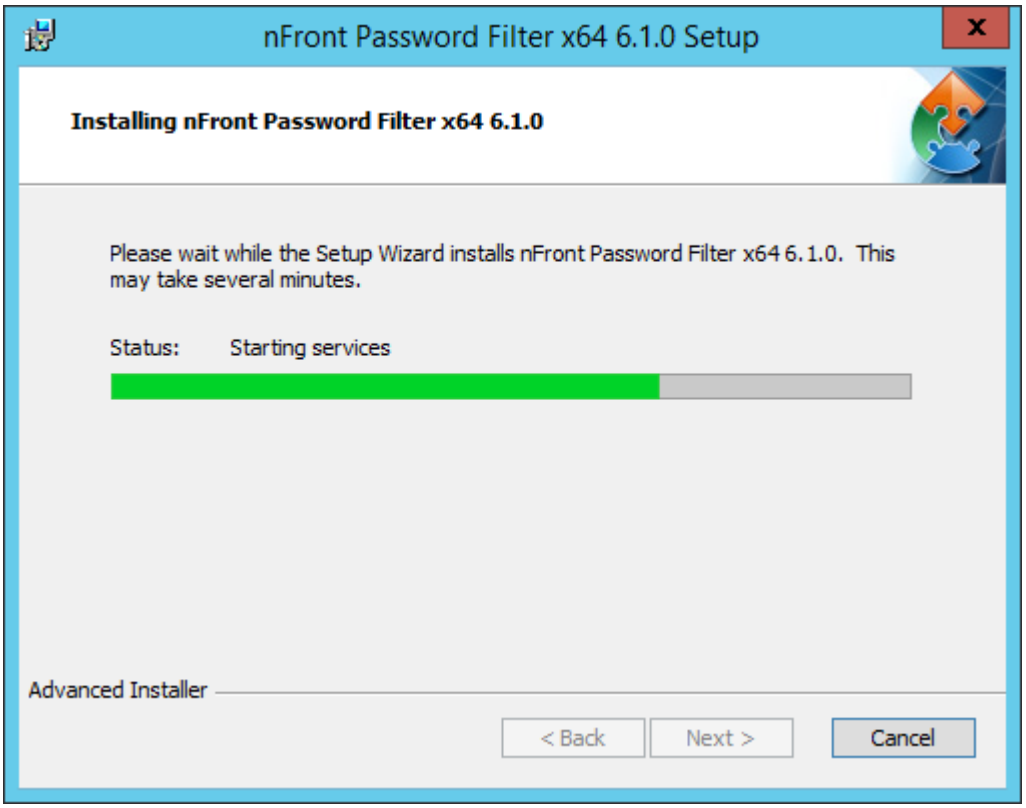


Figure 2.3.4: Installation screen 4.

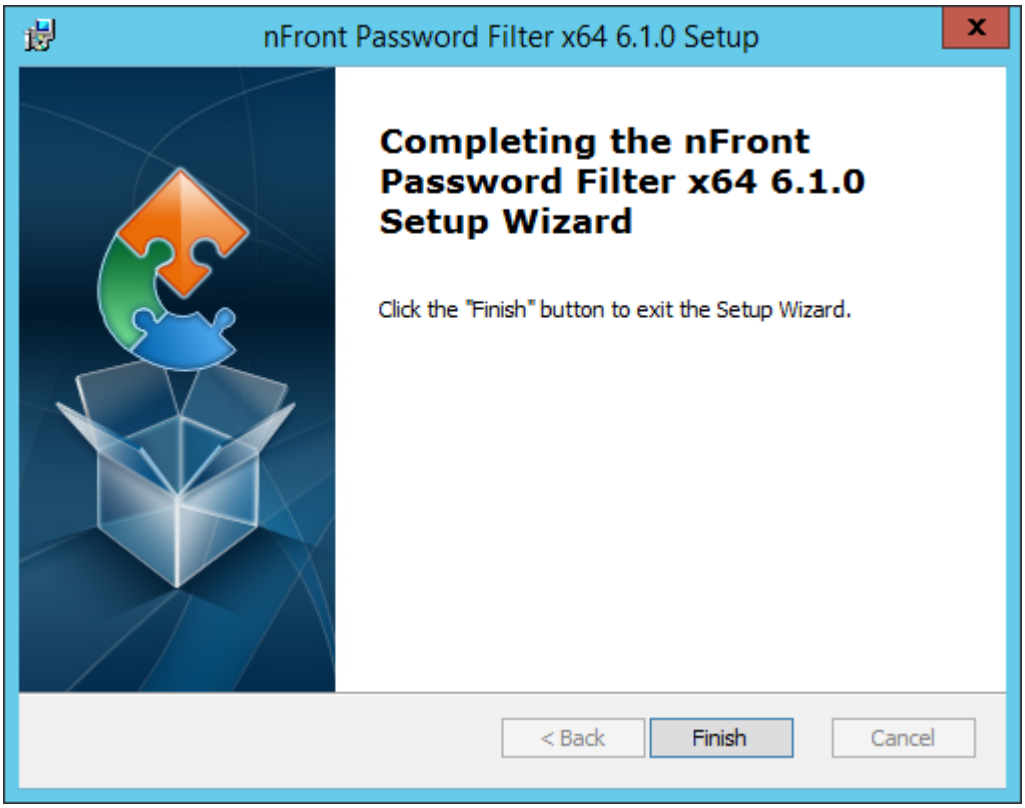


Figure 2.3.5: Installation screen 5.

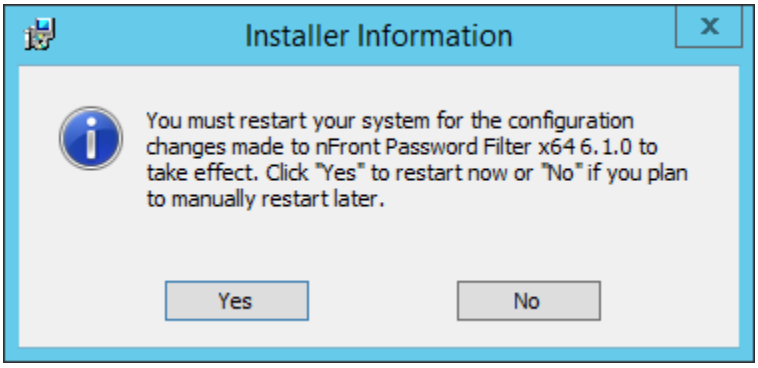


Figure 2.3.6: Installation screen 6.

You must restart for the operating system to load the password filter DLLs on boot. You can say No to the optional restart and reboot at a later time.

2.4 Decide to use ADM or ADMX templates

With release version 6.2.0 we have included ADMX templates along with ADM templates. You will find both in the downloaded zip file that contains the MSI packages. So you now have 2 options for loading templates:

1. You can copy the correct ADMX template to the Central Store so it is available for any GPO created.

2. You can load the ADM template after you create the GPO to configure the nFront software.

2.5 Load the correct ADMX template

IMPORTANT NOTE: If you plan to use the ADM templates please skip to section 2.6.

In the nfront-password-filter.zip download package you will find a zipped collection of the ADMX templates in a file called admx-templates.zip. The zip file will extract to the following template structure.

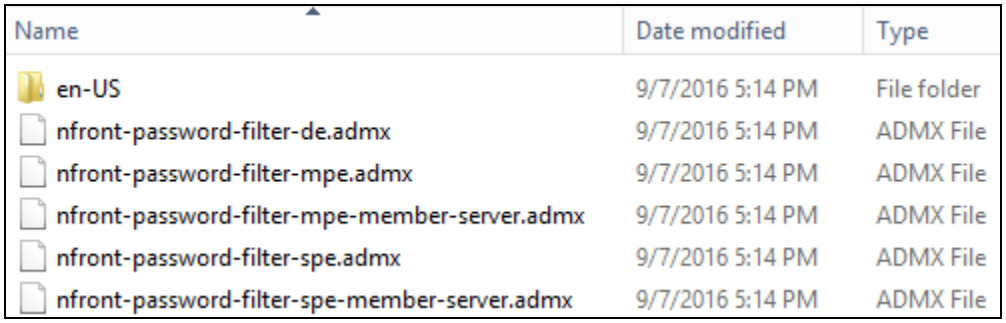


Figure 2.5.1 : List of ADMX templates

We include templates for all editions of our software but likely you only need one of the templates. The table below shows each template file and its corresponding edition. Most likely you are looking for the single or multiple policy edition for domain controllers to filter passwords for Active Directory user accounts. If you will also run the product on member servers or desktops you will need a template for the member servers and one for the desktops.

Template	Edition
nfront-password-filter-mpe.admx	nFront Password Filter Multiple Policy Edition for Domain Controllers
nfront-password-filter-spe.admx	nFront Password Filter Single Policy Edition for Domain Controllers
nfront-password-filter-spe-member-server.admx	nFront Password Filter Single Policy Edition for Member Servers
nfront-password-filter-mpe-member-server.admx	nFront Password Filter Multiple Policy Edition for Member Servers
nfront-password-filter-de.adm	nFront Password Filter Desktop Edition

If you have not setup a central store you can do so easily by simply copying the C:\Windows\PolicyDefinitions folder to C:\Windows\Sysvol\Sysvol\<domain name>\Policies on a DC.

If you have the central store setup, copy and paste the correct ADMX template file into the PolicyDefinitions folder in the central store. Also copy the corresponding ADML file from the en-US folder to the PolicyDefinitions\en-US folder in the central store.

If you have GPMC open you will need to close it and open it again for it to refresh and pull definitions from the central store.

2.6 Create a GPO via GPMC

You will use a single GPO to control the nFront software. If you are filtering passwords for Active Directory users the GPO will be linked to the Domain Controllers container. If you are using nFront to filter passwords on member servers or workstations you will link the GPO to the OU or OUs containing the target member servers or workstations.

If you are running Windows 2003 you may have to load GPMC separately. It is included with Windows 2008 and later. Click Start + Run + GPMC.MSC + expand the domain until you see the **Domain Controllers container** + right-click + select "Create a GPO in this domain, and Link it here…".

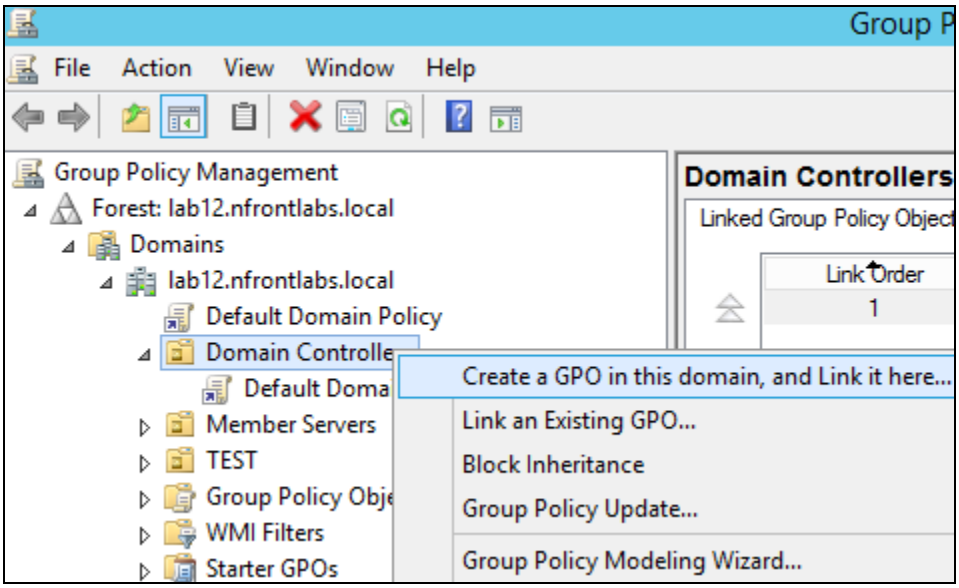


Figure 2.6.1: Creating a new GPO for nFront Password Filter.

Give the GPO a clever name.

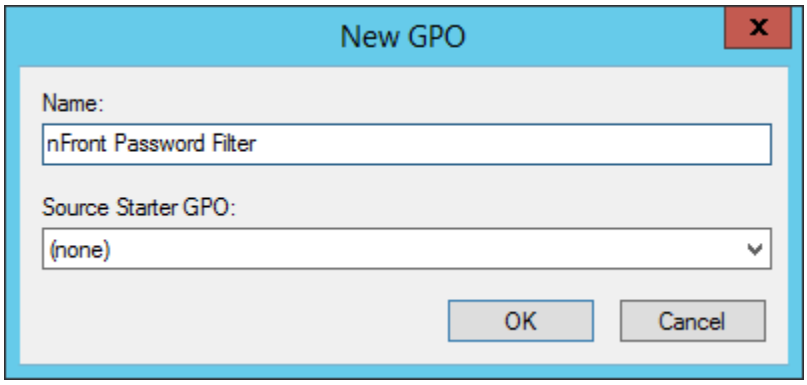


Figure 2.6.2: Naming the new GPO

The new GPO will appear on the right pane. Right-click and select Edit.

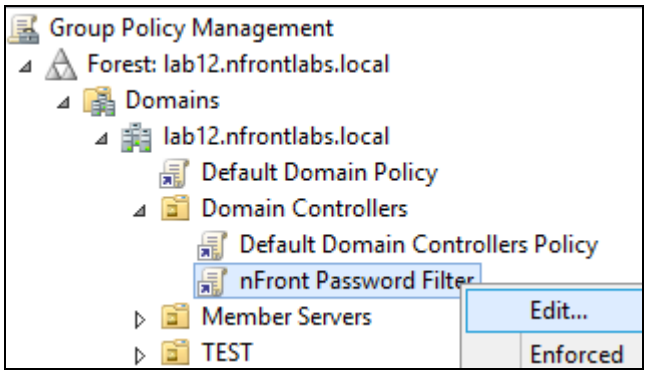


Figure 2.6.3: Edit the new GPO

IMPORTANT NOTE: The GPO should always be linked to the Domain Controllers OU (unless you are filtering local passwords on member servers or desktops) and you should never edit the permissions on the GPO. To target specific groups or OUs you will specify the group name and/or OU path at the bottom of each policy. Each DC must have permissions to read the GPO to add the configuration data to the local registry.

If you have loaded the ADMX template it will appear automatically in the new GPO. If you plan to use ADM templates please skip ahead to 2.6.1. In the new GPO, you will navigate to Computer Configuration + Policies + Administrative Templates + nFront Password Filter <edition> to configure the settings. Below is a screen clipping showing the nFront Password Filter MPE settings that appear.

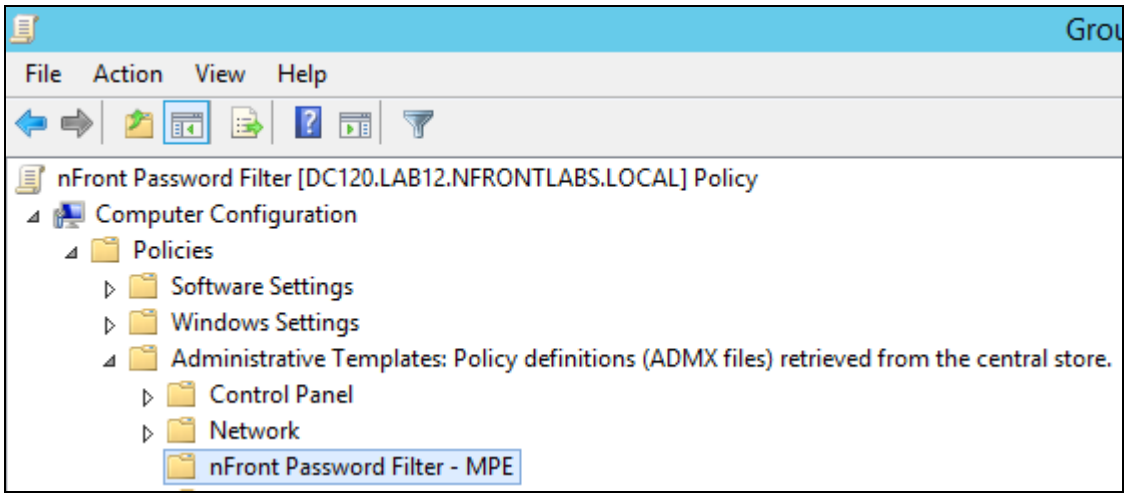


Figure 2.6.4: Edit the new GPO

Skip ahead to section 2.7 to optionally customize the dictionary file and continue with the configuration.

2.6.1 Load the correct ADM template

In the Group Policy Management Editor, drill down to Computer Configuration + Policies + Administrative Templates. Right-click Administrative Templates and choose Add/Remove Templates. The Add/Remove Templates dialog box will appear.

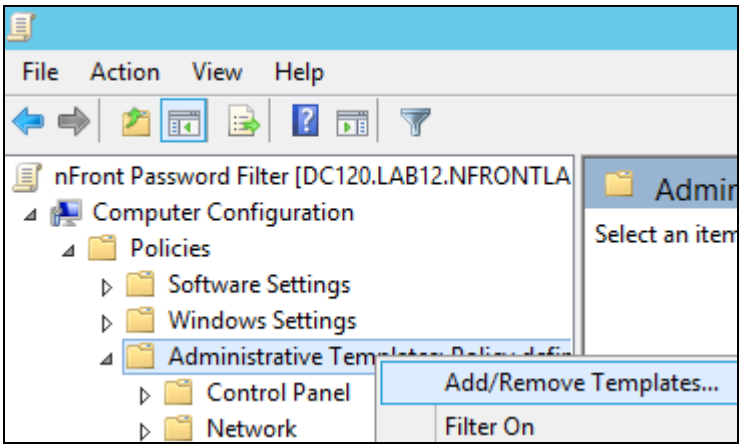


Figure 2.6.1.A: Add ADM template to nFront Password Filter policy

Click the **Add** button.

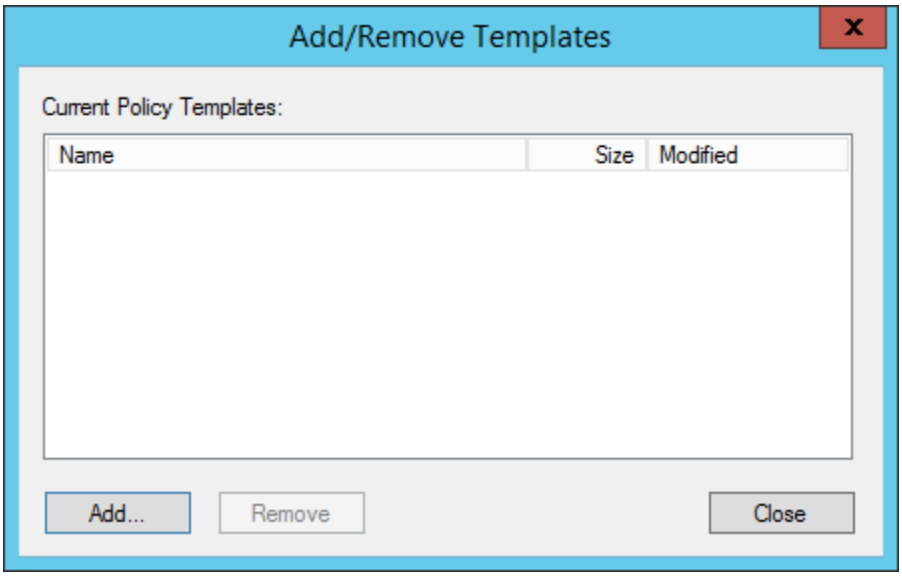


Figure 2.6.1.B: Add/Remove Templates dialog box

When you installed the nFront Password Filter.MSI package the installed copied templates for all editions of the software to the windows\inf folder. It is important you select the correct template for the edition you wish to configure. On domain controllers you will load nFront-Password-Filter-mpe.adm or nFront-Password-Filter-spe.adm depending on whether you want multiple policies or a single policy.

Here is a listing of each template the corresponding edition. Each templates uses a different registry target location.

Template	Edition
nFront-Password-Filter-mpe.adm	nFront Password Filter Multiple Policy Edition for Domain Controllers
nFront-Password-Filter-spe.adm	nFront Password Filter Single Policy Edition for Domain Controllers
nFront-Password-Filter-spe-member-server.adm	nFront Password Filter Single Policy Edition for Member Servers
nFront-Password-Filter-mpe-member-server.adm	nFront Password Filter Multiple Policy Edition for Member Servers
nFront-Password-Filter-de.adm	nFront Password Filter Desktop Edition

Select the correct template for the version you wish to install and click the **Open** button.

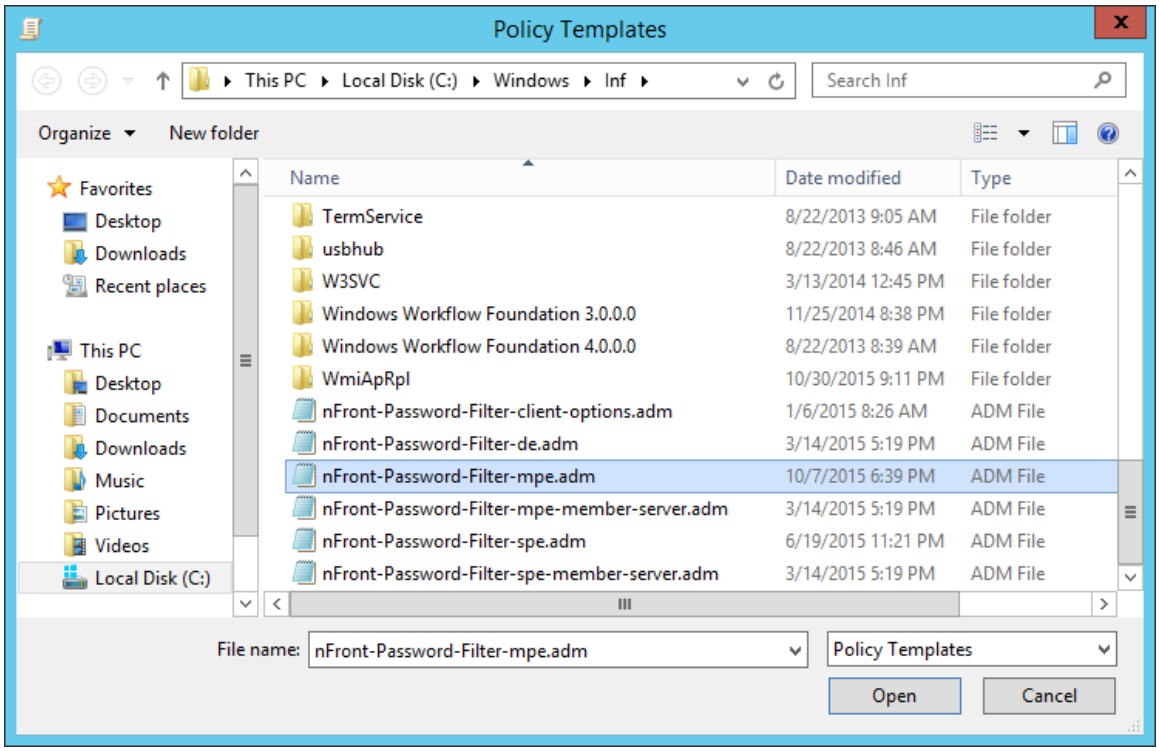


Figure 2.6.1.C: Select the correct template

Click on **Close** to complete the addition of the template. You should now see a "nFront Password Filter – MPE" folder under Classic Administrative Templates (ADM).

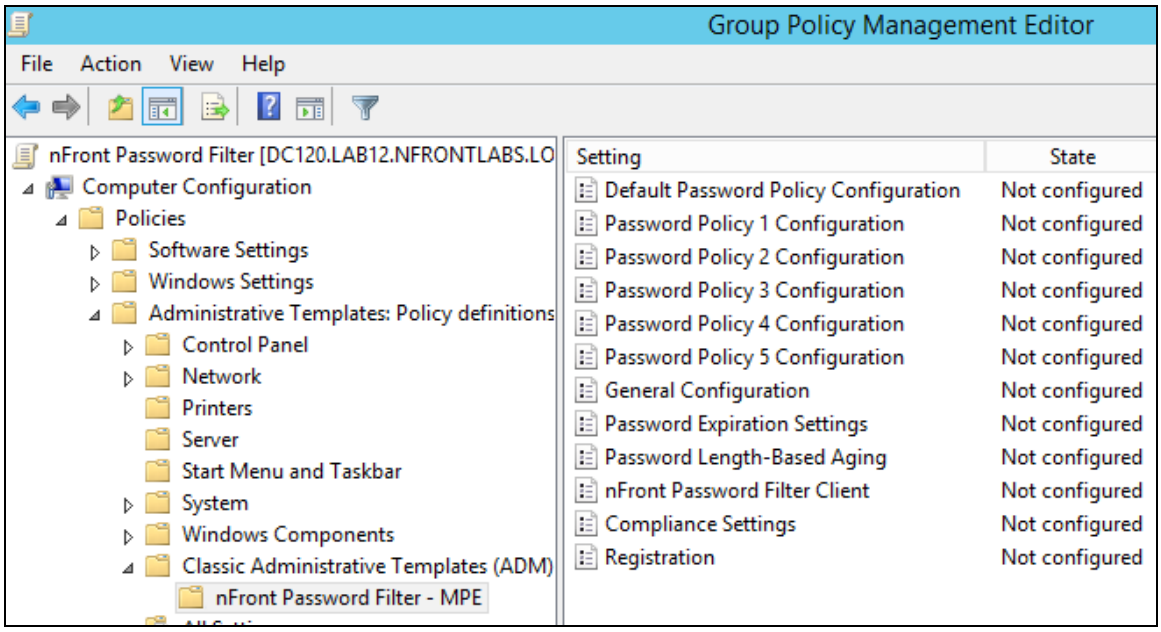


Figure 2.6.1.D: Add/Remove Templates dialog box

NOTE: BECAUSE OF REPLICATION, YOU ONLY NEED TO LOAD THE ADM TEMPLATE ON ONE DOMAIN CONTROLLER

2.7 Customize the dictionary.txt file (optional)

Perform this step only if you plan to use the dictionary checking feature and need to customize the dictionary.txt file.

The installer copies the supplied dictionary.txt file to the %systemroot%\system32 directory on each domain controller. nFront Password Filter uses this directory as the default location.

You can edit the file using Notepad or any text editor. The provide dictionary.txt file is in a Unicode format. However, we support ANSI, UTF-8 and Unicode formats. Most dictionary files found on the internet will be Unicode. Once you customize the dictionary file you will need to copy it to c:\windows\system32 on all other domain controllers. You may find it helpful to write a simple xcopy batch file to do this.

You can configure the General Configuration setting the GPO to have nFront Password Filter read the GPO from the netlogon share. This will allow you to edit the file on any DC and not worry with synchronizing the changes among DCs.

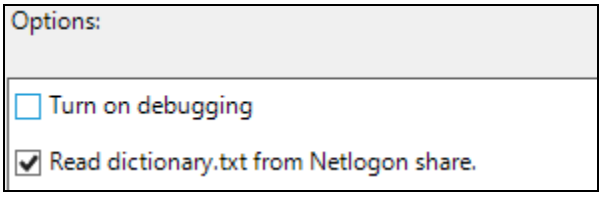


Figure 2.7.1: General Configuration settings

If using the dictionary.txt from the Netlogon share, you simply modify the file directly from the Netlogon share. Once saved, the file will be replicated among all domain controllers.

2.8 Optionally force immediate update of the group policy

Group policies update every 90 minutes plus or minus a 30 minute random offset for clients. The Domain Controller policies replicate every 5 to 15 minutes. If you cannot wait five minutes or you are testing in a lab environment and need immediate replication, open a command window and type:

gpupdate /force

This will have the effect of immediately propagating our new policy settings throughout the domain.

2.9 Optionally deploy the nFront Password Filter Password Expiration Service (MPE Only)

The nFront Password Filter MPE GPO exposes settings related to password expiration and enforcing differing maximum password ages. Each policy can have a maximum password age and you can optionally email users a warning of the upcoming expiration (Figure 2.8.1). However, you must install the nFront Password Filter Service to enforce the settings.

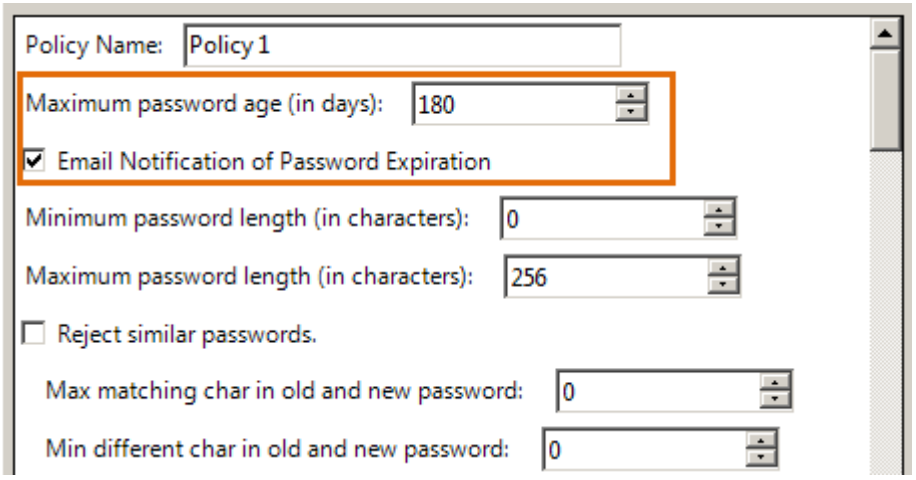


Figure 2.8.1: nFront Password Filter – Max password age settings

The nFront Password Expiration Service can only be used when you deploy the MPE version of the nFront Password Filter on domain controllers. The service can:

- Enforce different maximum password age settings for each password policy. If your password is beyond the maximum password age you are required to change your password at next logon.
- Email users with upcoming password expirations (i.e. within the warning interval)
- Notify users with upcoming password expirations at logon (only if you run our client software on the client workstation)

- Email administrators a report of upcoming password expirations.

IMPORTANT NOTE: Any age set via nFront Password Filter will be ignored if the age is greater than that of your Domain Security Policy (i.e. Password Policy settings in Default Domain Policy GPO). So if your domain policy expires passwords every 60 days, any nFront Password Filter policy with aging set to more than 60 days will be ignored.

2.9.1 Installation of nFront Password Expiration Service

Install the 32-bit or 64-bit version of the "nFront Password Filter Password Expiration Service.MSI" on a single domain controller. A reboot is not required. The service will not start upon installation and the startup mode will be set to Manual. You can optionally install the service on additional domain controllers for fault tolerance.

See section 3.6 for information on configuring the service. On the "go live" date start the service and change the startup mode to Automatic. As soon as the service starts it will read through the nFront Password Filter policies and "expire" passwords for any accounts whose password age is over the limit set in nFront Password Filter. Even for large networks the service typically completes the tasks in one or two seconds.

3.0 Configuring nFront Password Filter

nFront Password Filter MPE is used as an example in this section. nFront Password Filter SPE is configured in the same way but only has one password policy for all domain users. nFront Password Filter MPE for Member Servers offers the same settings except it only has 3 password policies and the policies target local groups (instead of domain groups and OUs). nFront Password Filter SPE for Member Servers and nFront Password Filter Desktop Edition offer a single password policy.

IMPORTANT NOTE: You should reference Appendices A and B for help with designing your password policy.

IMPORTANT NOTE: The desktop and member server products can be configured via the local Group Policy Editor (Start + Run + gpedit.msc) or via a GPO in the AD.

Pre-Configuration Considerations

- Do you have a formal written password policy that has been distributed to end-users?
- What are your overall goals with password filtering?
- What is your current written password policy?

3.1 Navigate to nFront Password Filter settings (via local or AD GPO)

Use GPMC (Windows 2008, Server 2012) or ADUC (Windows 2003) or the local GPO editor (gpmc.msc) to open the GPO with the nFront settings.

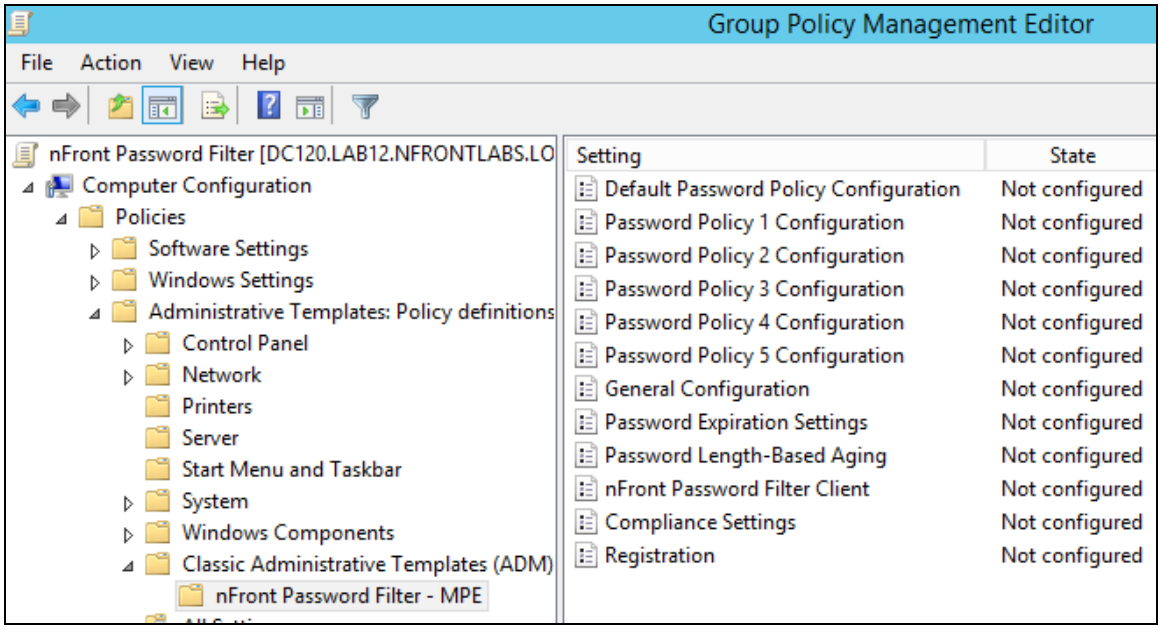


Figure 3.1.1: nFront Password Filter – Multi-Policy Edition Settings.

3.2 Configure Registration Settings

Double-click the Registration policy. Enable the policy and enter your registration code (if you purchase the product) or the evaluation registration code (received via email after download). If you have purchased the product you also must enter an annual maintenance code.

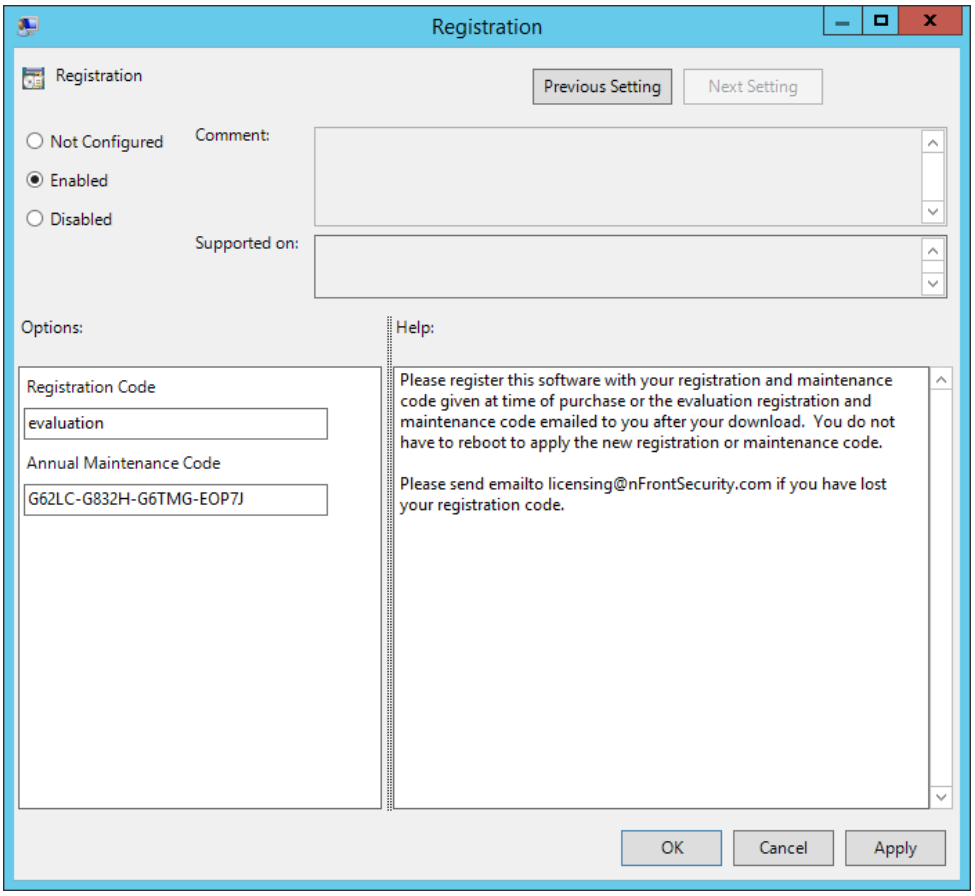


Figure 3.2.1: nFront Password Filter MPE Registration Policy.

3.3 Configure General Configuration Settings

When you are testing nFront Password Filter MPE we suggest you "Turn on Debugging" to verify your configuration, see why certain passwords fail, etc. When debugging is turned on, nFront Password Filter will generate a file called nfront-password-filter-debug.txt in the %systemroot%\system32\logfiles directory. This file is overwritten with each password change so it does not keep a running history. The file contains information on your nFront Password Filter settings, the proposed password and why that password failed. This debug file can also be used to verify that you have properly registered the product with the correct registration code.

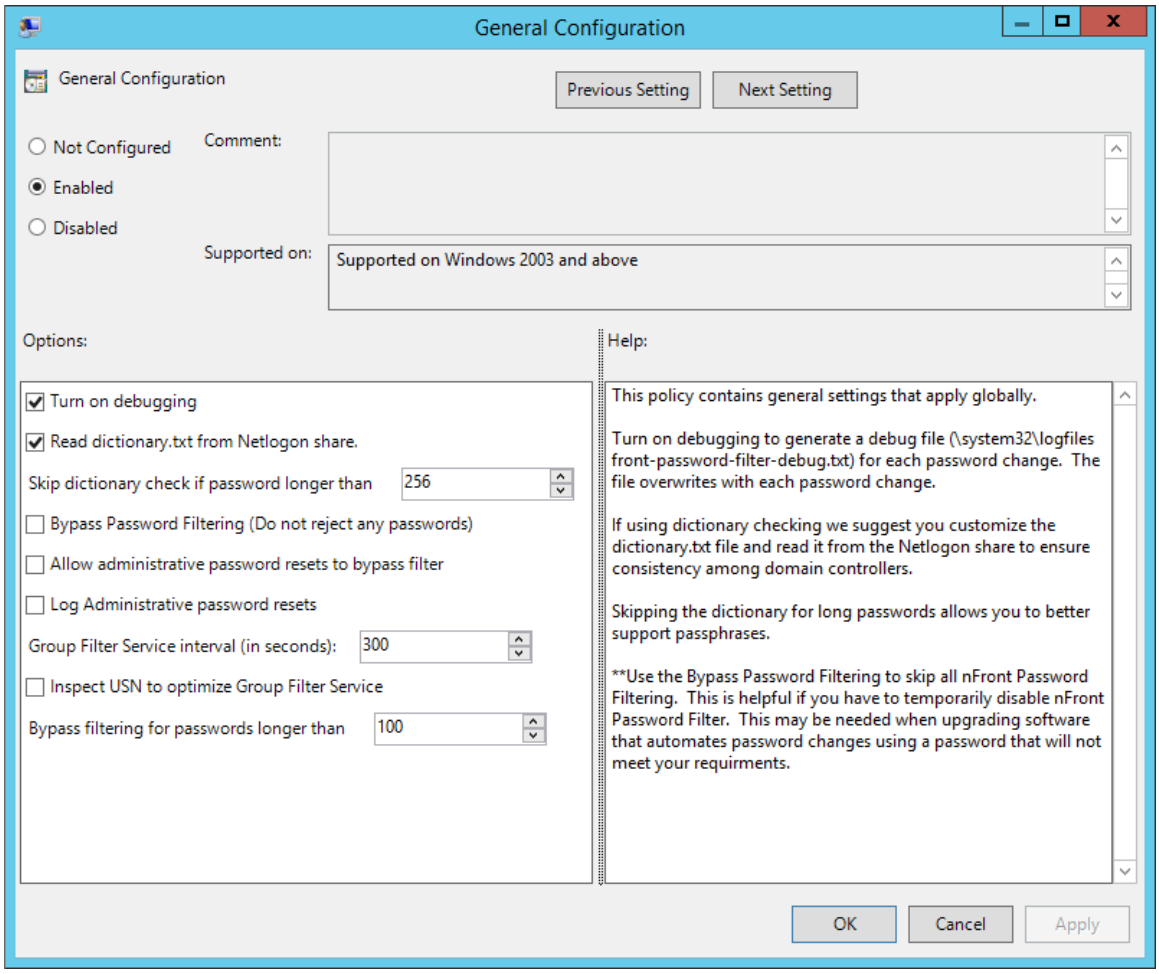


Figure 3.3.1: nFront Password Filter MPE General Configuration Policy.

Policy	Description
Turn on Debugging	Generates a file called nfront-password-filter-debug.txt in the %systemroot%\system32\logfiles directory. The file is overwritten with each password change. The file contains information on your group policy settings as well as the proposed password change, username, full name, registration information, etc.
Read dictionary.txt from Netlogon share.	Default Value: 0 This setting affects the dictionary checking which must be enabled via one of the Password Policy Configurations. By default, nFront Password Filter MPE looks for a file called dictionary.txt in the %systemroot%\system32\logfiles directory on each local domain controller. Some customers find the manually copying of the dictionary file to

	each DC to be too cumbersome. Thus, you can check this box to have nFront Password Filter MPE look for dictionary.txt in the local Netlogon share.
Skip dictionary check if password longer than XX characters	Default Value: 256 nFront Password Filter will skip any dictionary checking and / or substring dictionary checking for passwords greater than the length specified here.
Bypass password filtering (do not reject any passwords)	This setting can be used to temporarily bypass filtering. This may be needed to bypass filtering for such tasks as upgrading from Exchange 2000 to Exchange 2003 on a network with a maximum character limit of 8 characters. The Exchange System account tries to change to a 256 character password and halts during the upgrade unless you bypass the password filter.
Allow password resets to bypass the filter	This allows administrative staff to assign weaker passwords when resetting an end-user's password.
Log Administrative password resets.	Logs date/time and userid to %systemroot%\system32\logfiles\nfront-password-resets.txt file.
Inspect USN to optimize Group Filter Service	This feature only works on policies that target groups and will not work if OU paths are targeted by the policy. If checked this option will force the inspection of the USN (update sequence number) for the group object and if the number has not changed the nFront Group Filter service will not retrieve a new list of all group members. If the group is modified in any way the service will retrieve a new list of members.
Bypass filtering for passwords longer than XX characters	Default Value: 100 This feature is primarily for Exchange 2013. Exchange 2013 automatically changes passwords on system health mailboxes and sets a 128 character password. On some networks this causes a problem based on the policies implemented. You can add any value smaller than 128 here to skip password filtering for the Exchange password changes.

3.4 Compliance Settings

In release 5.4.0 a Compliance Settings section was added to the group policy settings. You can enable this policy and check any of the compliance settings to implement the compliance requirement. These settings apply to all users on the network and are the equivalent of enabling the Default Password Policy Configuration and applying the individual requirements within that policy.

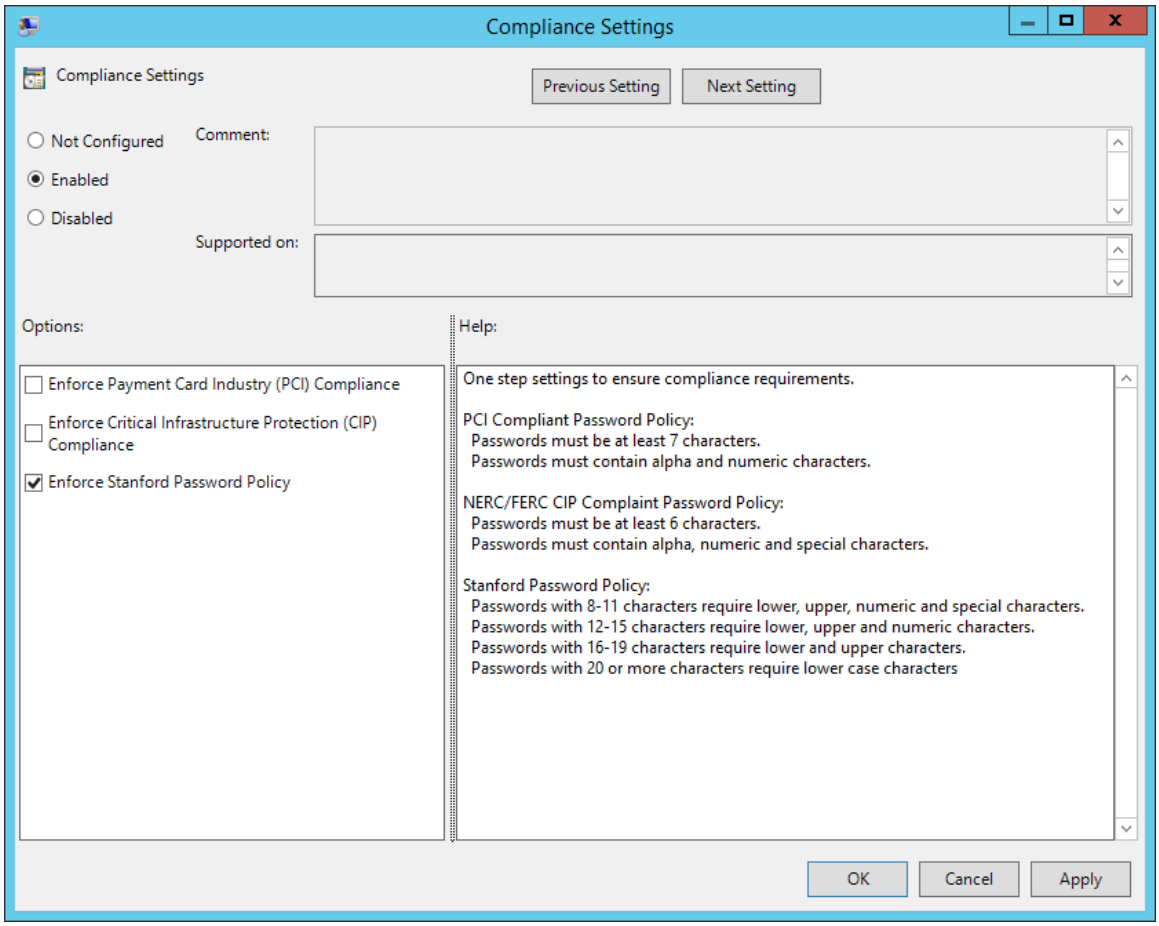


Figure 3.4.1: nFront Password Filter Compliance Settings Policy.

Policy	Description
Enforce Payment Card Industry (PCI) Compliance * This setting only present in MPE	Default Value: 0 Check this box to enforce the following settings for all users (except any you may have excluded on the default policy). • Passwords must contain at least 7 characters. • Password must contain at least 1 alpha character. • Password must contain at least 1 numeric character.

version.	
Enforce Critical Infrastructure Protection (CIP) compliance. * This setting only present in MPE version	Default Value: 0 Check this box to enforce the following settings for all users (except any you may have excluded on the default policy). • Passwords must contain at least 6 characters. • Password must contain at least 1 alpha character. • Password must contain at least 1 numeric character. • Password must contain at least 1 special character.
Enforce Stanford Password Policy * This setting only present in MPE version	The password policy adopted by Stanford is a length based password policy. The longer the password the fewer the character types required. • Passwords with 8-11 characters require lower, upper, numeric and special characters. • Passwords with 12-15 characters require lower, upper and numeric characters. • Passwords with 16-19 characters require lower and upper characters. • Passwords with 20 or more characters require lower case characters

3.5 Configure Password Policy Settings

Important Notes:

- The Default Password Policy Configuration applies to everyone except the “Excluded Groups or OUs” (at bottom of scrolling list of policy settings).
- Other polices allow you to choose groups or OUs to which the policy applies and the groups or OUs which are excluded from the policy. You must apply the policy to at least one group or OU if you configure the policy.
- The Default Password Policy Configuration is used for all new account creation.
- Policies are cumulative just like NTFS permissions. If a user is affected by 2 polices the user’s password must meet the requirements of both policies and if the same settings differs between the policies, the most restrictive setting applies.

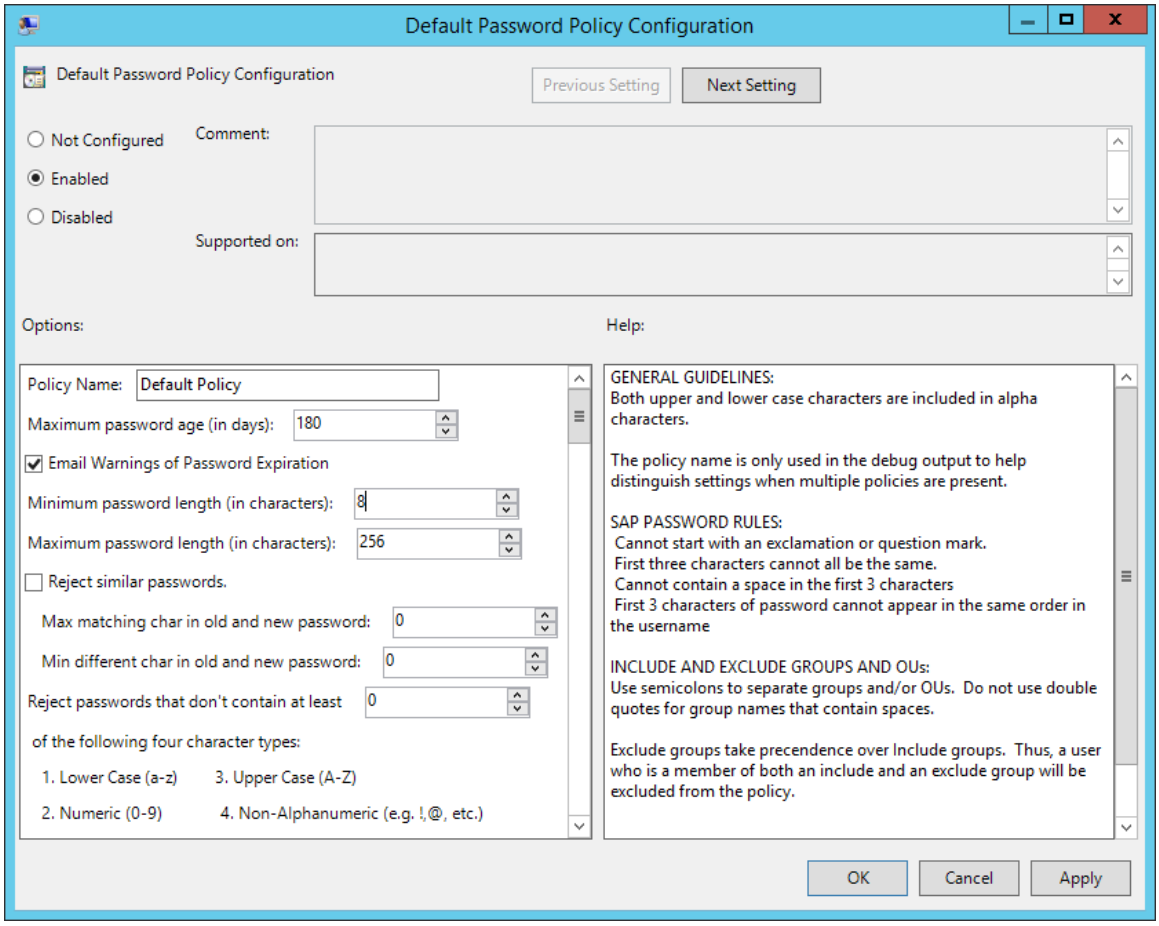


Figure 3.5.1: nFront Password Filter MPE Default Password Configuration Policy.

Policy	Description
Policy Name	Default Value: Default Policy This is the policy name that is reported in the debug output. This setting is arbitrary and

* This setting only present in MPE version.	optional. If you wish to rename the policy names that appear in the group policy editor you must edit the supplied Group Policy Template (nfront-Password-Filter-mpe.adm).
Maximum password age (in days): * This setting only present in MPE version	Valid Values: 0-365 Default Value: 0 (turned off) NOTE: The value set here cannot be greater than the overall maximum password age for the domain. This parameter is read by the nFront Password Filter Password Expiration Service which will force users to "Change Password at next logon" if their password is older than the value set. A setting of 0 means no aging is applied. IMPORTANT NOTE: The age must be less than or equal to the maximum password age set for the entire domain. You can verify the domain maximum password age via the command line ("net accounts"). IMPORTANT NOTE: For this setting to be effective you must install the separate nFront Password Expiration Service on a domain controller.
Email Notification of Password Expiration * This setting only present in MPE version	Default Value: 0 Check this box to email warnings to end users about upcoming password expirations. IMPORTANT NOTE: For this setting to be effective you must install the separate nFront Password Expiration Service on a domain controller.
Minimum password length (in characters):	Valid Values: 0-256 Default Value: 0 Controls minimum number of overall characters in password. Since you can have multiple policies you may wish to have a different minimum character limit

	for different groups. Ideally passwords should all be at least 8 characters or more. Also, passwords of more than 14 characters are not accepted by Windows Terminal Services. NOTE: This setting may conflict with the minimum password length you have established in the Default Domain Policy.
Maximum password length (in characters):	Valid Values: 0-256 Default Value: 256 Controls maximum number of overall characters in password. Useful in environments with UNIX systems or mainframes where passwords of more than 8 characters are truncated or rejected. If you use Microsoft Services for UNIX or BMC's password synchronization software you may wish to impose your maximum limits here.
Reject similar passwords.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy is used with the next 2 settings to ensure the old and new password are not "too similar" or to ensure they are different. *This feature only works for password changes made via the nFront Password Filter client or via the nFront Web Password Change portal.
Max matching char in old and new password	Valid Values: 0-256 Default Value: 0 This policy is used to select the maximum length of a character string that can be found in both the old and new password. For example, if the old password is dogcat123 and the new password is tigerdog456 the new password will be rejected if the max matching characters is 3 or less because the phrase "dog" is used in both passwords.
Min different char in old and new password	Valid Values: 0-256 Default Value: 0

	This policy is used to ensure the old and new passwords are different by XX characters. Each character in the new password is compared to every character in the old password. The new password must contain XX characters that were not used in the old password.
Reject passwords that don't contain at least <value> of the following 4 character types: 1) Lower Case (a-z) 2) Numeric (0-9) 3) Upper Case (A-Z) 4) Special (e.g.!,@,etc.)	Valid Values: 0-4 Default Value: 0 nFront Password Filter categorizes each character in the new password into one of the following four categories: 1. numeric character 2. upper case character 3. lower case character 4. non-alphanumeric character A 1 tells nFront Password Filter to make sure the new password contains characters from at least 1 category. A 2 forces the new password to contain characters from at least 2 categories. This setting is provided for customers who want a variation in the password complexity feature provided by Microsoft.
Check for lower case characters in password.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for lower case characters within the new password and make sure the number of lower case characters fits within the range specified.
Minimum Lower Case Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of lower case characters that must be present in the password.
Maximum Lower Case Characters Required:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of lower case characters that must be present in the password.
Check for upper case characters in password.	Valid Values: 0 or 1 Default Value: 0 (not checked)

	This policy tells nFront Password Filter to check for upper case characters within the new password and make sure the number of upper case characters fits within the range specified.
Minimum Upper Case Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of upper case characters that must be present in the password.
Maximum Upper Case Characters Required:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of upper case characters that must be present in the password.
Check for numeric characters in password.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for numeric characters within the new password and make sure the number of numeric characters fits within the range specified.
Minimum Numeric Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of numeric characters that must be present in the password.
Maximum Numeric Characters Allowed:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of numeric characters that must be present in the password.
Check for Special characters in password.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for non-alphanumeric characters within the new password and make sure the number of non-alphanumeric case characters fits within the range specified.
Minimum Special Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of non-alphanumeric characters that must be present in the password.
Maximum Special Characters Required:	Valid Values: 0-256 Default Value: 256

	Defines the maximum number of non-alphanumeric characters that must be present in the password.
Check for spaces in password.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for space characters within the new password and make sure the number of space case characters fits within the range specified. ** great setting for encouraging the use of passphrases
Minimum Spaces Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of space characters that must be present in the password.
Maximum Spaces Required:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of space characters that must be present in the password.
Check for alpha characters in password.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for alpha characters (upper or lower case) within the new password and make sure the number of alpha characters fits within range specified. NOTE: Alpha does NOT distinguish between upper and lower case characters.
Minimum alpha Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of alpha characters (i.e. upper or lower case) that must be present in the password.
Maximum alpha Characters Required:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of alpha characters (i.e. upper or lower case) that must be present in the password.
Check for non-alpha characters in	Valid Values: 0 or 1

password.	Default Value: 0 (not checked) This policy tells nFront Password Filter to check for non-alpha characters (numeric or special) within the new password and make sure the number of non-alpha characters fits within range specified.
Minimum non-alpha Characters Required:	Valid Values: 0-256 Default Value: 0 Defines the minimum number of non-alpha characters (i.e. numeric or special) that must be present in the password.
Maximum non-alpha Characters Required:	Valid Values: 0-256 Default Value: 256 Defines the maximum number of alpha characters (i.e. numeric or special) that must be present in the password.
Restrict special character set	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to only allow specific special characters listed in the textbox below. Note that a space is a special character.
Allowed special characters (up to 32)	List allowed special characters here. No need for quotes or commas. Just type the characters into the box. If you wish to include a space it would be a good idea to include it between other allowed special characters so it is obvious to the viewer.
Enforce SAP Password Rules	Valid Values: 0 or 1 Default Value: 0 (not checked) SAP PASSWORD RULES: • Cannot start with an exclamation or question mark. • First three characters cannot all be the same. • Cannot contain a space in the first 3 characters • First 3 characters of password cannot appear in the same order in the username
Reject passwords that contain vowels	Valid Values: 0 or 1 Default Value: 0 (not checked)

	This policy tells nFront Password Filter to check for vowels (a,e,i,o,u,y). If any vowels are found the password is rejected. This may be used to eliminate dictionary words. A dictionary containing common sequences is still recommended.
Reject passwords that contain 2 consecutive identical characters.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for 2 consecutive identical characters within the new password. For example any password containing “aa” would fail regardless of where “aa” falls within the password.
Reject passwords that contain 3 consecutive identical characters.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for 3 consecutive identical characters within the new password. For example any password containing “aaa” would fail regardless of where “aaa” falls within the password.
No more than 3 consecutive characters from same char set	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for 3 consecutive identical characters from the same character set within the new password. The character sets are upper, lower, numeric and special (i.e. non-alphanumeric). For example, any password containing “frog” would fail. It is also a great rule to prevent users from including 4-digit years in their password.
Reject non-ASCII characters (i.e. foreign language characters).	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for characters outside of the ASCII range of 32-126. This setting is typically used to disallow foreign characters for many European customers. Password like freibier4ü would be disallowed when this setting is turned on.
Reject passwords without a character between alpha characters.	Valid Values: 0 or 1 Default Value: 0 (not checked)

	This policy tells nFront Password Filter to check for a numeric character between 2 alpha characters. The numeric character is not required to have an alpha character immediately before or after it. An alpha character anywhere before and anywhere after the numeric character meets the requirement.
Reject passwords that begin with a number	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for a numeric character at the beginning of the password.
Reject passwords that end with a number	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for a numeric character at the end of the password.
Reject passwords that begin with a special character	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for a special character at the beginning of the password.
Reject passwords that end with a special character	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check for a special character at the end of the password.
Passwords must contain a numeric character in position <value>	Valid Values: 0-256 Use this setting to require a numeric character in a specific position within the password. A 0 configures nFront Password Filter not to enforce this policy.
Passwords must contain a special character in position <value>	Valid Values: 0-256 Use this setting to require a non-alphanumeric character in a specific position within the password. A 0 configures nFront Password Filter not to enforce this policy.
Passwords must contain special character before character number <value>	Valid Values; 0-256 Default: 0 Use this setting to require a non-alphanumeric

	character within a specified number of characters at the beginning of the password.
Reject passwords that contain the username.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check to see if the new password contains the username anywhere within it.
Reject passwords that contain any part of the user's full name.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check to see if the new password contains any part of the user's fullname (listed as Display Name in Windows 2000/2003). The full name of the user is parsed and broken into sections based on spaces in the full name field. Thus, the full name "George P Burdell" would be checked for "George" and "P" and "Burdell" within the new password. The check is case-insensitve, so passwords like "george123" and "GEORge123" would both be rejected. NOTE: To avoid problems with the middle initial, nFront Password Filter does not compare any portions of the "full name" that are less than 3 characters.
Reject passwords that contain 3 consecutive characters from the username or user's full name.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to parse the username and user's full name components to ensure that no sequence of 3 consecutive characters from any component is included in the password. This was a policy requirement with a large domain hosting provider.
Dictionary - reject passwords that contain dictionary words	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to scan the password for any occurrence of the dictionary line entry within the password (as opposed to looking for an exact case-insensitive match). example dictionary.txt

	january february march example passwords: JANUARY1 123january JaNuArYpW January JANuary With the substring search enabled, all 5 of the above passwords would be rejected. With the standard dictionary check, only the last two would be rejected.
Dictionary Option - check substitution characters (a=@, e=3, i=1,l=1,o=0,s=$)	Valid Values: 0 or 1 Default Value: 0 (not checked) When checked the filter will check the password for all combinations of each dictionary word that contains the substitution characters. For example, if the word in the dictionary is “password” the following words will be checked: password p@ssword pa$$word passw0rd p@$$word pa$$w0rd p@SSw0rd
Dictionary Option - treat '*' as wildcards in dictionary file	Valid Values: 0 or 1 Default Value: 0 (not checked) This option gives you the ability to use a ‘*’ in dictionary words as a wildcard where any number of characters could be used in place of the wildcard. For example if the dictionary contains the word “let*in” the following passwords would be rejected: letmein letusin lethimin letmechecktoseeificangetin

	…
Groups/OUs to which this policy applies:	Valid Values: group names or OU paths separated with semicolons (max text length is 1024 characters) Default Value: none List global groups here that should receive this policy. IMPORTANT NOTE: The setting is not present in the Default Password Policy. The Default Password Policy applies to all users and you can only add exclusions. ADVICE: Use the Default Password Policy for all Domain Users. Generally it will be your most unrestricted policy. Other policies will generally provide more restrictive filtering to protect groups that have access to sensitive network resources. Always decide first which groups should receive the policy. Then ask if there are any users in those groups who should not receive the policy. If such users exist, you need to create a global group for them and exclude that global group from this policy. Group nesting is supported so if you have many groups nested into 1 group you only need to list the 1 group. OU paths are supported. Please list the OU path in the form of "OU=NY,OU=NA". In this case NA is an OU branching from the domain and NY is an OU under NA. This is like an X.500 distinguished name without the CN or DC components. When an OU path is targeted all users in that OU and any OUs under that OU are affected.
Apply this policy to users with non-expiring passwords.	Valid Values: 0 or 1 Default Value: 0 (not checked) If checked the policy will apply to all accounts with the "Password Never Expires" flag set.

Groups/OUs EXCLUDED from this policy:	Valid Values: global group names separated with semicolons (max text length is 1024 characters) Default Value: none List global groups here that should be excluded from this policy. Many administrators find it helpful to exclude certain service accounts that may automatically change their passwords (e.g. SMS service accounts, Exchange 2003 service accounts).
Exclude this policy from users with non-expiring passwords.	Valid Values: 0 or 1 Default Value: 0 (not checked) If checked the policy will be skipped for all accounts with the "Password Never Expires" flag set.

3.5.1 Notes on the dictionary checking features

The dictionary check feature uses a plain-text file named dictionary.txt located in the %SYSTEMROOT%\System32 directory. This file contains over 27,000 entries. You can edit the file directly in any editor like Notepad (or any other text editor) to add or remove entries. The file is in an ANSI format but you can save it in ANSI or Unicode. If you edit the dictionary file, you must manually copy it to the %systemroot%\system32 directory on each domain controller.

In the General Configuration policy, you can turn on the option to "Read dictionary.txt from Netlogon share." We suggest placing the dictionary file in the netlogon share to ensure consistency among domain controllers. In such case, nFront Password Filter MPE will read the dictionary.txt file from the local Netlogon share. Administrators can edit the dictionary.txt file on any domain controller and the modified file will replicate to all other domain controllers automatically. The negative to this approach is Netlogon is readable by all end-users and they can see the dictionary file you are using. However, you can modify permissions on the file to disallow user access. The nFront product runs as a thread under the LSA process and under the security context of SYSTEM. So you need only be sure that SYSTEM has read access to the file. Likely you also want to include Administrators with Modify permission.

When dictionary password checking is enabled, the dictionary.txt file is scanned line by line and compared with the new password proposed by the user. The nFront software will look for the dictionary word anywhere within the password regardless of case.

In less than 180 milliseconds, nFront Password Filter MPE ensures that the user's proposed password does not match any of the 27,000 entries!

3.5.2 Notes on the dictionary character substitution feature

Turning on the character substitution feature can increase dictionary processing time depending on the length and contents of the dictionary file. Each time the dictionary check routine encounters a word with one or more substitution characters it must calculate all possible

combinations of the characters. Using our default dictionary of 27,000 words the nFront system can process it in 31 milliseconds without character substitution and in 152 milliseconds with character substitution.

As shown below, the word “password” results in 7 different words to check:

password
p@ssword
pa$$word
passw0rd
p@$$word
pa$$w0rd
p@SSw0rd

If you wish to optimize dictionary checking and check for substitution characters it would be best to pre-process your dictionary file and generate the substitutions you prefer to check. Suppose you want to use the following words but only check for i=”!” and a=”@” (instead of our standard substitution characters):

password
company
internet

You could generate the substitutions for each word and just use our standard dictionary checking option (without the substitution option turned on):

password
p@ssword
company
comp@ny
internet
!nternet

Such customization allows you to directly select which characters you wish to substitution and it makes the dictionary checking routine faster since you have pre-populated the dictionary with the exact words you wish to check.

3.5.2 Notes on the dictionary wildcard feature

The wildcard feature (Dictionary Option - treat '*' as wildcards in dictionary file) is a different approach to dictionary process. In any word containing a ‘*’ character the character will be treated as a wildcard. Suppose the dictionary contains one word:

p*word

The following passwords would be rejected:

password
passssword
poorlychosenword

This feature would allow you to eliminate many variations not otherwise possible with standard dictionary checking or character substitution. However, you must be careful because it could eliminate words or phrases you have not intended.

3.6 Configure Password Expiration Settings (MPE Only)

The Password Expiration Settings Policy (Figure 3.6.1) can be used to control the Password Expiration Service.

The nFront Password Expiration Service includes the ability to email end users about upcoming password expirations. The software uses the user's email address that is specified on their AD user account. The software will not only email end user's about their upcoming password expirations but can also email a report to the administrator which lists the configuration settings, has a table of user's with upcoming password expirations and has a table of users whose passwords have been expired during this run of the service.

Features:

- You can set a warning threshold such that users are notified XX days before the password expiration. The warning threshold applies to all policies.
- You can control the timing of the service. We suggest running the process every 24 hours.
- You can customize the message to the end user (perhaps giving remote users an intranet location to be used for password changes). You can customize the "from" email address, the subject and the body of the message.
- Emails to the end users can be sent in plain text or HTML. The default is HTML.
- You can customize the body of the email message to the end user. The following variables may be used within the body of the message. When the email is sent the correct information will be substituted based on the user account.

  <%username%>
  <%firstName%>
  <%lastName%>
  <%daysUntilExpiration%>

- Emails to the administrator are sent using HTML for a better formatted report.
- You can run the system in a report only mode. In report only mode an administrative report is emailed. However, end users do not have their passwords expired and no email goes to the end user. You receive a complete report of those with upcoming expirations and a list of users whose passwords would be expired by the system.
- You do not have to create a MAPI profile. You simply specify an SMTP server name or IP address and some parameters regarding the messaging.
- You can choose to email only certain groups of users because the choice to email warnings is set on a per policy basis. So those on Password Policy 1 may receive warnings and those on Password Policy 2 may not.

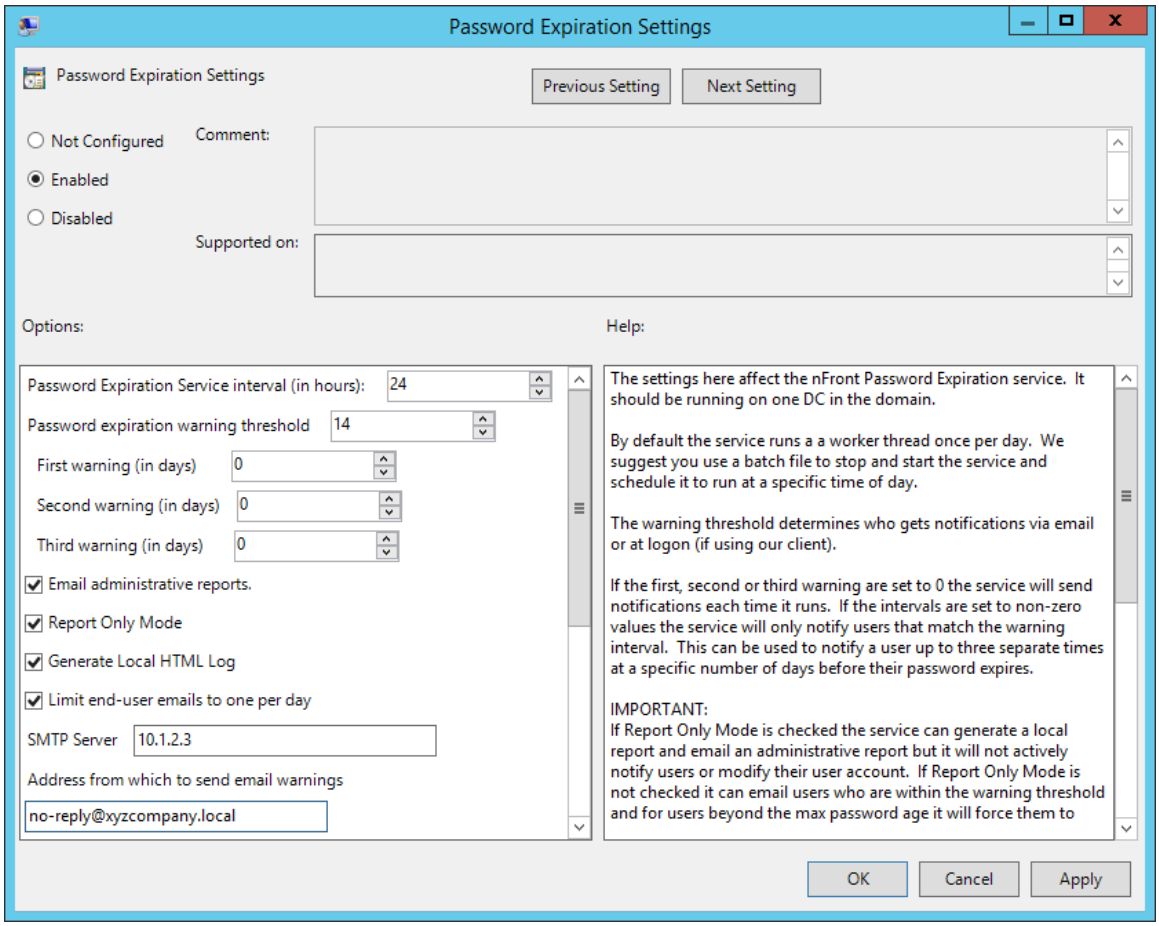


Figure 3.6.1: nFront Password Expiration Settings

The table below shows a list of configuration settings related to the Password Expiration Settings section.

Policy	Description
Password Expiration Service interval (in hours)	Default Value: 24 Min: 1 Max: 120 This controls how often end-user emails and administrative reports are generated.
Password expiration warning threshold	Default Value: 14 This parameter corresponds to the number of days in advance to warn the user of an upcoming password change. **If you use the first, second, or third warning you must be sure this setting is set to the longest of the warnings.

First Warning (in days)	Default Value: 0 Min: 1 Max: 365 If set to a non-zero value this will cause the expiration service to only send emails on the warning interval specified. The value specified is the number of days before password expiration. You can specify up to three different warning days.
Second Warning (in days)	Default Value: 0 Min: 1 Max: 365 If set to a non-zero value this will cause the expiration service to only send emails on the warning interval specified. The value specified is the number of days before password expiration. You can specify up to three different warning days.
Third Warning (in days)	Default Value: 0 Min: 1 Max: 365 If set to a non-zero value this will cause the expiration service to only send emails on the warning interval specified. The value specified is the number of days before password expiration. You can specify up to three different warning days.
Report Only Mode	Default Value: checked Uncheck this box to send emails to end users about password expirations and expired passwords on those accounts overdue for a password change.
Generate Local HTML Log	Default Value: not checked This will generate a file named “nfront-expiration-report.html” in the c:\windows\system32\logfiles directory. The file contains the body of the message that is sent in the administrative email report.
Limit end-user emails to one per day	Default Value: not checked This will prevent multiple password expiration warning emails to an end user in the event of a server or service restart.
SMTP Server	Default Value: “”

	Specify the name or IP address of the SMTP server you wish to use. This is required for any email notifications to users or administrators.
SMTP Username	Default Value: “” Can be used to specify credentials to authenticate to an SMTP server for email.
SMTP Password	Default Value: “” Can be used to specify credentials to authenticate to an SMTP server for email.
Email administrative reports	Default Value: 0 You can choose to skip the email of administrative reports.
To: email address for email reports	Default Value: “” This parameter is required if you wish to have the administrative reports emailed to an individual or department email address. After each run of service, you will receive an email with a summary of users with upcoming password expirations and a list of passwords that have been expired during this run.
From: email address for email warnings	Default Value: “” This is the email address from which the warnings are sent. It can be a real or fake address depending on if you wish to allow and accept user replies to the email. This parameter is required if you wish to email users or administrators.
Subject of password expiration warning message	Default Value: “” This parameter is optional. If left blank the user receives an email stating “YOUR WINDOWS PASSWORD WILL EXPIRE SOON.” You can change the text to any 128-character string you would like.
Password Expiration Email Body Customization	IMPORTANT NOTE: This setting was removed in release 6.2.0. You can now edit the plain text or html file in the local system32 directory. The filenames are nFrontEmailExpiration.txt and nFrontEmailExpiration.html. The system will send the html version if it is present. If you prefer plain text rename the html version and the plain text file will be used. You can customize both versions just by editing the file.

Only send a test email	Default Value: 0 If you set this to a 1 and provide a test email address the service will send the test email on startup. This can be used to test customizations to the email subject or body without affecting production users. Since no test username is provided it will use a username of GBurdell with a full name of George Burdell. It also assumes the password expires in 10 days. If you have used variables in your email template customization they should reflect this test username, first name, etc.
Email address for test email	Default Value: “” This is the email to which the test message will be sent. The test message will appear as it would for an end-user on the network whose password expires in 10 days.

3.6.1 Working with the nFront Password Expiration Service

When the service installs the service is not started and it defaults to a Manual Startup mode. When you start the service it accomplishes its work in less than one or two seconds. By default, the configuration defaults to Report Only mode and we suggest you keep the setting checked until you are ready to go live and actively email users. In the Report Only mode the service will run all of its calculations and build a local logfile and / or email you the administrative report. You can then review the results and see what would have happened if it were not in Report Only mode.

To test the expiration settings, you simply restart the service. Be sure to run gpupdate /force after you change any GPO settings and then restart the service.

TIP: To have the service run at a specific time of day we suggest you schedule the following batch file via Task Scheduler.

```
net stop “nfront password expiration service”
net start “nfront password expiration service”
```

If you run the service via a batch file we suggest you set the Password Expiration Service Interval to a longer interval than the time between runs of the batch file. For example, if you wish to run the batch file daily then you should set the interval to 25 hours or more. That avoids a potential issue with the service thread waking up to run again at the same time the batch file is restarting the service.

3.6.2 Logging

When not in Report Only mode the service generates two comma-delimited log files. The files are located in the c:\windows\system32\logfiles directory. We suggest you copy the files to

another location and rename the extension to ".csv" such that you can easily open the files in Excel or other spreadsheet programs.

Below is information on each log file and excerpts from each:

- nFront-expired-pw.log. This file logs the accounts whose passwords have been expired due to the policies configured in nFront Password Filter. It gives us the date and time the account was expired, the account name, the age of the password (in days) at time of expiration. The last two columns a successful or failed operation and an error code if one was returned.

```
"5/15/2014 15:57:37","test750","46","successful"
"5/15/2014 15:57:37","test751","46","successful"
```

- nFront-expiring-soon.log. This file maintains an up-to-date listing of passwords that will expire in the next XX days (where XX days is the warning interval you have configured via nFront settings).

```
"Date of Run, Username, Days before expiration
"5/16/2014  9:28:55","jsmith","2"
"5/16/2014  9:28:55","test302","4"
"5/16/2014  9:28:55","test51","14"
```

3.6.3 Example Administrative Report

Subject: nFront Password Expiration Report

HTML Body:

nFront Password Expiration Report

DATE OF RUN: 1/1/2016 5:00:00

Settings:

Service Interval (in hours)	25
SMTP Server	
Warning Threshold	15
Email at specific intervals	1
Warning 1	15
Warning 2	7
Warning 3	1
Report Only	1
Email Admin Report	0
Limit Emails	0
Email length-based password aging users	0
Last Email Day	12

Users with upcoming password expirations:

Username	Email	Email Warnings	Days until Expiration	Emailed
test1	none	1	4	no
test5	none	1	15	no
fred	fred@nFrontSecurity.com	1	15	yes
bob	bob@nFrontSecurity.com	1	13	no

Users with passwords expired during this run:

Username	Email	pw Age	Max pw Age	Status
test100	john.doe@nFrontSecurity.com	90	90	PASSWORD EXPIRED
test101	jane.doe@nFrontSecurity.com	90	90	PASSWORD EXPIRED
test102	jane.smith@nFrontSecurity.com	117	90	PASSWORD EXPIRED

3.6.4 Example Email to End-User:

```
Subject: YOUR PASSWORD WILL EXPIRE SOON

Body:
Your Windows password will expire in 7 days.

You can change your password before the expiration date to avoid
additional password expiration emails. If you do not change your
password before the expiration date you will be prompted to
change your password prior to logon on the day of expiration.
```

3.6.5 Customizing the email body and using variables

In release 6.2.0 the method to customize the email body has changed. In prior releases customization was done via GPO. Now it is much easier. Also it is now possible to send HTML emails as well as plain text emails. In c:\windows\system32 are the following two files:

nFrontEmailExpiration.html
nFrontEmailExpiration.txt

You can directly edit these files and modify the messaging as needed. The expiration service will always attempt to read the HTML version. If the HTML version is not present it will use the plain text version. If you wish to use plain text we suggest you simply rename the HTML version in case you wish to use HTML in the future. You can simply add a .old extension or any other method to change the name.

You can use the following variables in your custom message:

```
<%username%>
<%firstName%>
<%lastName%>
<%daysUntilExpiration%>
```

Here is the default HTML file:

```
<html>
<body>
<p>
Your Windows password will expire in <%daysUntilExpiration%> days.
</p>
<br/>
<p>
You can change your password before the expiration date to avoid
additional password expiration emails. If you do not change your
password before the expiration date you will be prompted to change your
password prior to logon on the day of expiration.
</p>
</body>
</html>
```

Here is the default plain text file:

```
Your Windows password will expire in <%daysUntilExpiration%> days.

You can change your password before the expiration date to avoid
additional password expiration emails. If you do not change your
password before the expiration date you will be prompted to change your
password prior to logon on the day of expiration.
```

After making any modifications to the templates you will likely want to send a test email. You can easily do this by configured the GPO to "Only send a test email" and providing a test email address. These settings are at the bottom of the Password Expiration Settings policy. If you configure these parameters, the service will send a test email when started. It will put the service in ReportOnly mode even if that is not configured via GPO. This will prevent the service from sending any emails to the end users. You can experiment with modifications to the email templates and repeatedly test by restarting the service with no disruption to production users.

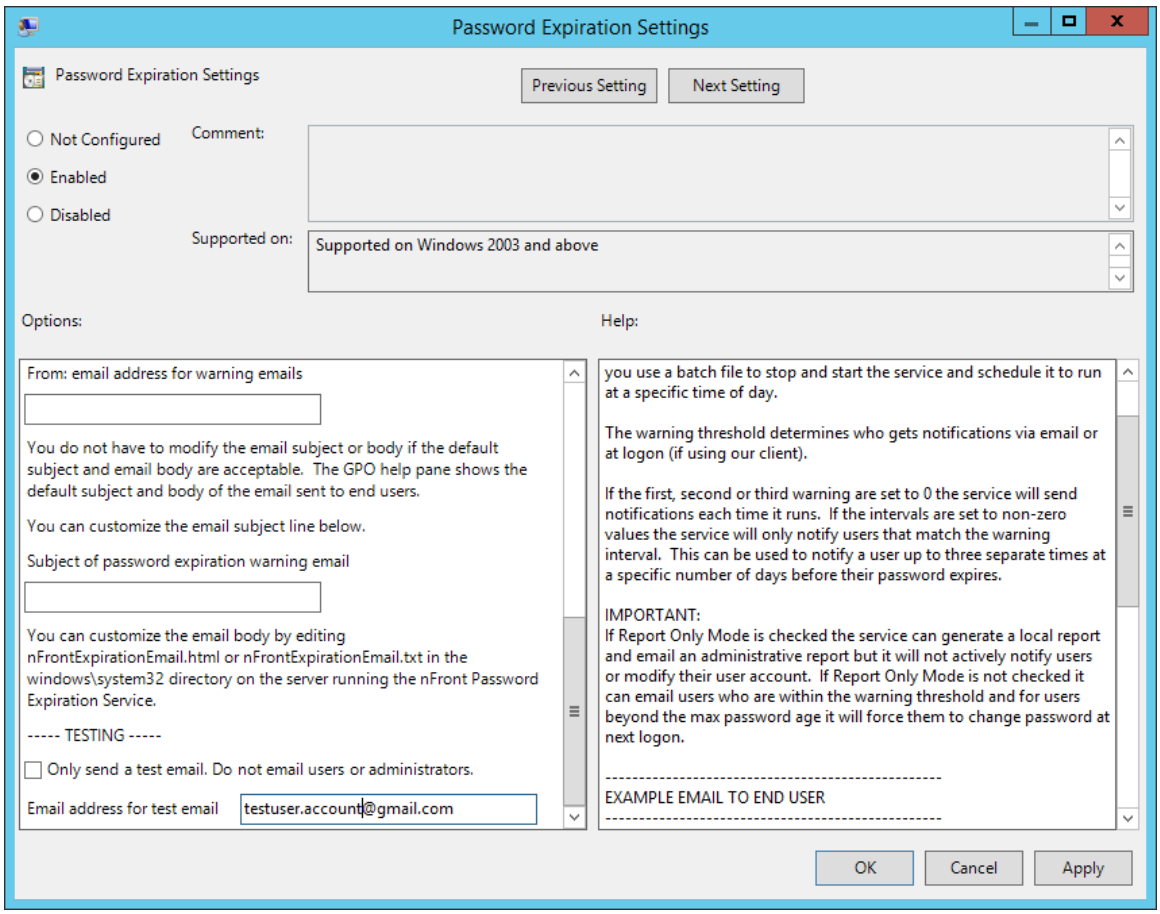


Figure 3.6.2: Password Length-Based Aging settings

3.7 Optionally configure Password Length-Based Aging Setting

Password Length-Based Aging is a feature introduced with release 6.1.0. It allows you to enforce different maximum password age settings based on the length of the password. Please note the overall windows maximum password age must be equal to or greater than the longest age set within the nFront software.

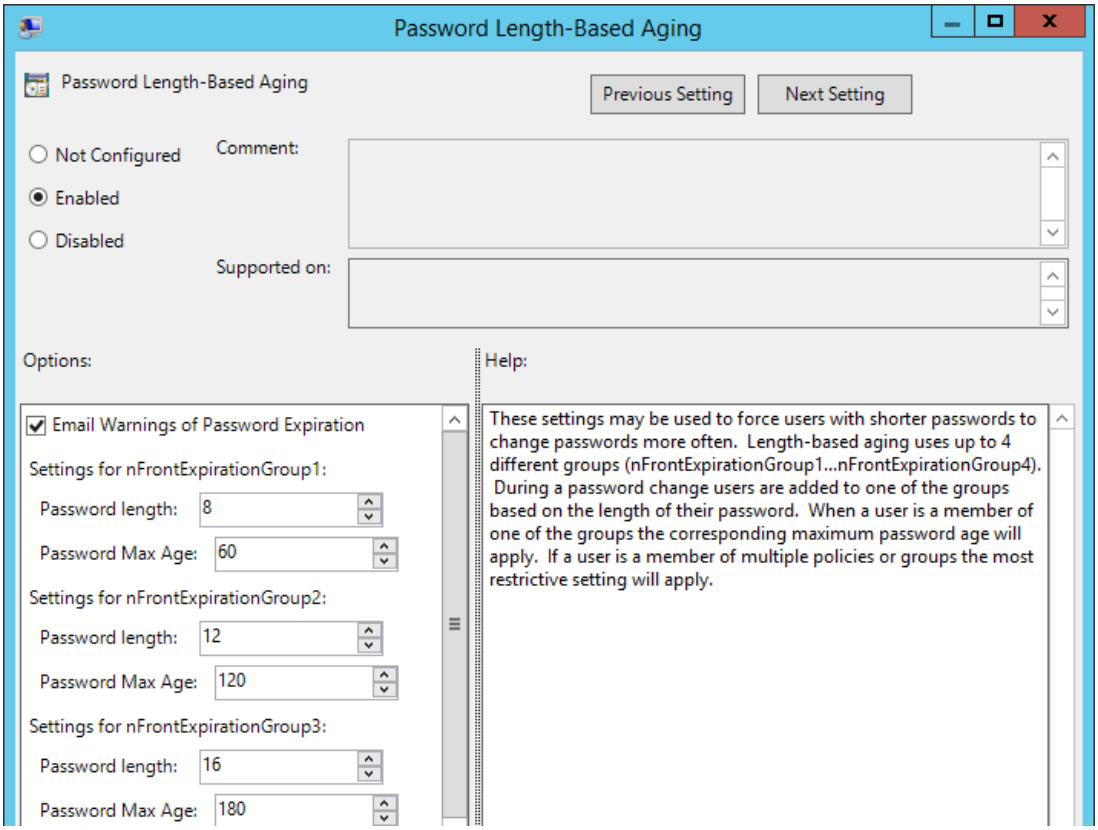


Figure 3.7.1: Password Length-Based Aging settings

To use this feature, you must create the following 4 groups.

- nFrontExpirationGroup1
- nFrontExpirationGroup2
- nFrontExpirationGroup3
- nFrontExpirationGroup4

The groups can be created anywhere in the AD. The groups are populated with usernames based on the length of password chosen by the user. The nFront Password Filter will place users into the correct group based on your settings

You must also have the nFront Password Expiration Service.MSI (or x64 version) installed on one of your domain controllers.

You can use up to 4 different password lengths. Each length has a corresponding maximum age that will be enforced for password greater or equal to that length (unless a longer length is defined with a greater maximum age).

Suppose we have the following 4 settings:

	Password Length	Password Max Age
nFrontExpirationGroup1	8	60
nFrontExpirationGroup2	12	120
nFrontExpirationGroup3	16	180
nFrontExpirationGroup4	20	365

If a user changes to a password with 8 to 11 characters their maximum password age will be 60 days. If they select a password that is 12-15 characters they can keep the password for up to 120 days. If the password is 16-19 characters, the maximum password age will be 180 days. If the password is 20 characters or more it may be kept up to 365 days.

You can enter the length and age in any order you wish. The system will automatically sort the lengths and corresponding ages and determine the ranges for a specific maximum password age.

Once this feature is activated the 4 groups above will populate with users as they change their passwords. Using the example, nFrontExpirationGroup1 will contain all users who have selected passwords that are 8 to 11 characters long and nFrontExpirationGroup4 will contain users who chose passwords of 20 characters or more.

3.8 Optionally configure nFront Password Filter Client Setting

For detailed information on the optional client see Section 9. Configuration of this policy is not necessary for the nFront Password Filter Client to work. It contains settings related to the display of a custom message to the end user.

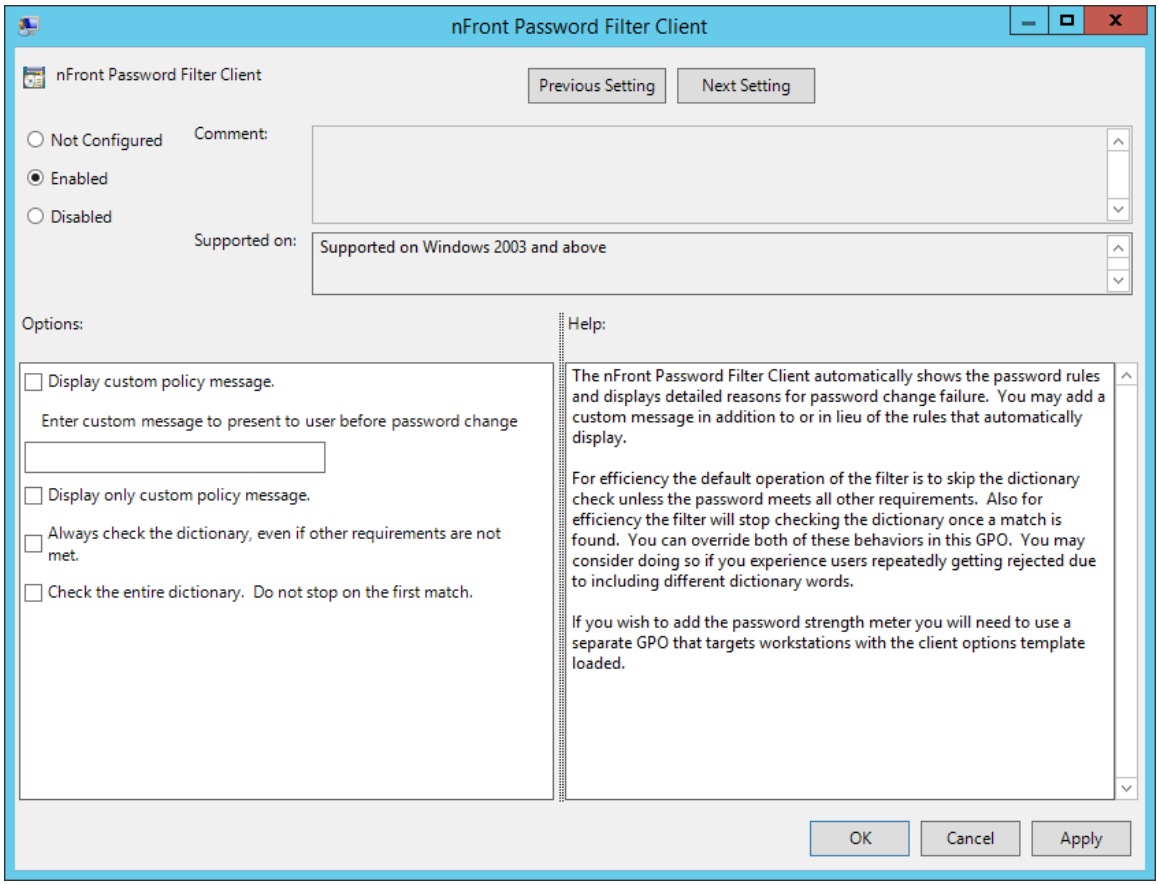


Figure 3.8.1: nFront Password Filter client settings

You can choose to:

- Display a custom message to the end-user in addition to our default message.
- Display a custom message only
- Always check the dictionary
- Check the entire dictionary

If you customize the message you will need to enter it into the GPO textbox as a single line of text. The textbox will accept up to 2048 characters. It is advised to type the message you wish to present into Notepad or your text editor of choice. To add carriage returns to the custom message use "\\" (without the double quotes) as a carriage return. If you have typed the message into Notepad you can simply replace the real carriage returns with the double backslashes and collapse all the text onto one line. Then you can easily paste the line into the GPO textbox.

The custom message would also display in the **nFront Web Password Change** product. The example below shows the phrase "Please choose your password wisely" added to the rules displayed. To learn more about **nFront Web Password Change** visit our company website.

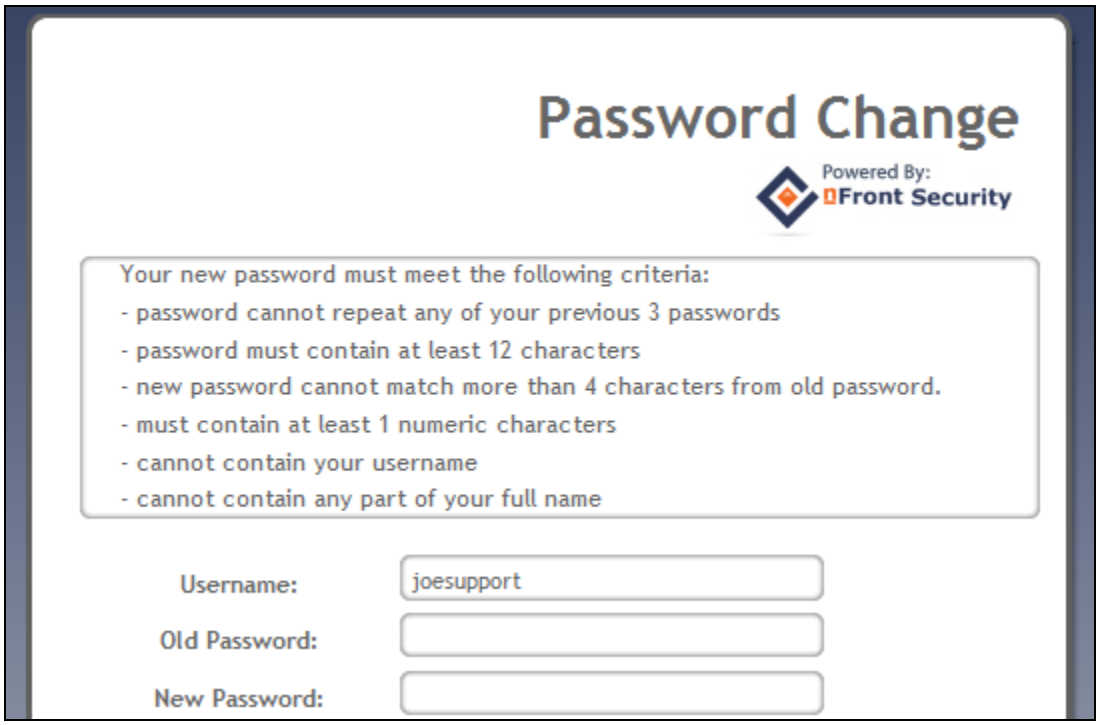


Figure 3.8.2: nFront Web Password Change displaying requirements

The settings to “always check the dictionary” and “check the entire dictionary” were added to bypass some efficiencies in the dictionary checking routine. By default, the filter does not check the dictionary unless all other requirements are met. Also, it will not check the entire dictionary if a match is found. The client will display multiple reasons for failure. However, if the password contains a dictionary word and does not meet other rules the client will display the rules which are not met but will not indicate the password contains a dictionary word. If you configure the system to “always check the dictionary” it will always check the dictionary and provide a more complete error message in cases where the password contains and dictionary word and violates other rules.

When the dictionary is searched the filter will stop searching when a dictionary word is found within the password. If the password contains multiple dictionary words it can be frustrating to the user to not list all dictionary words causing the failure. We added the feature to check the entire dictionary to provide the user with a list of up to 5 dictionary words contained within the password. The feedback is limited to 5 words to avoid display issues with the client feedback.

3.9 Force immediate update of the group policy

Group policies update every 90 minutes plus or minus a 30 minute random offset for clients. The Domain Controller policies replicate every 5 minutes. If you cannot wait five minutes or you are testing in a lab environment and need immediate replication, open a command window and type:

```
gpupdate /force
```

This will have the effect of immediately propagating our new policy settings throughout the domain.

4.0 Uninstallation Instructions

4.1 Delete the nFront Password Filter GPO

Your GPO settings for nFront Password Filter should be in a dedicated GPO and not part of any other policy. In this way you can delete the GPO with the nFront Settings to remove the configuration data. You may do this using GPMC (or ADUC on Windows 2003). Below are instructions for GPMC.

Launch GPMC and navigate to Domains\<domain name>\Group Policy Objects (not the Domain Controllers container). Find the GPO for the nFront configuration and delete it. You will be prompted with a message informing you that all GPO links in this domain will be removed as well. Just answer Yes to remove the GPO and the link to the Domain Controllers container.

NOTE: BECAUSE OF REPLICATION, YOU ONLY NEED TO PERFORM THIS STEP ON ONE DOMAIN CONTROLLER

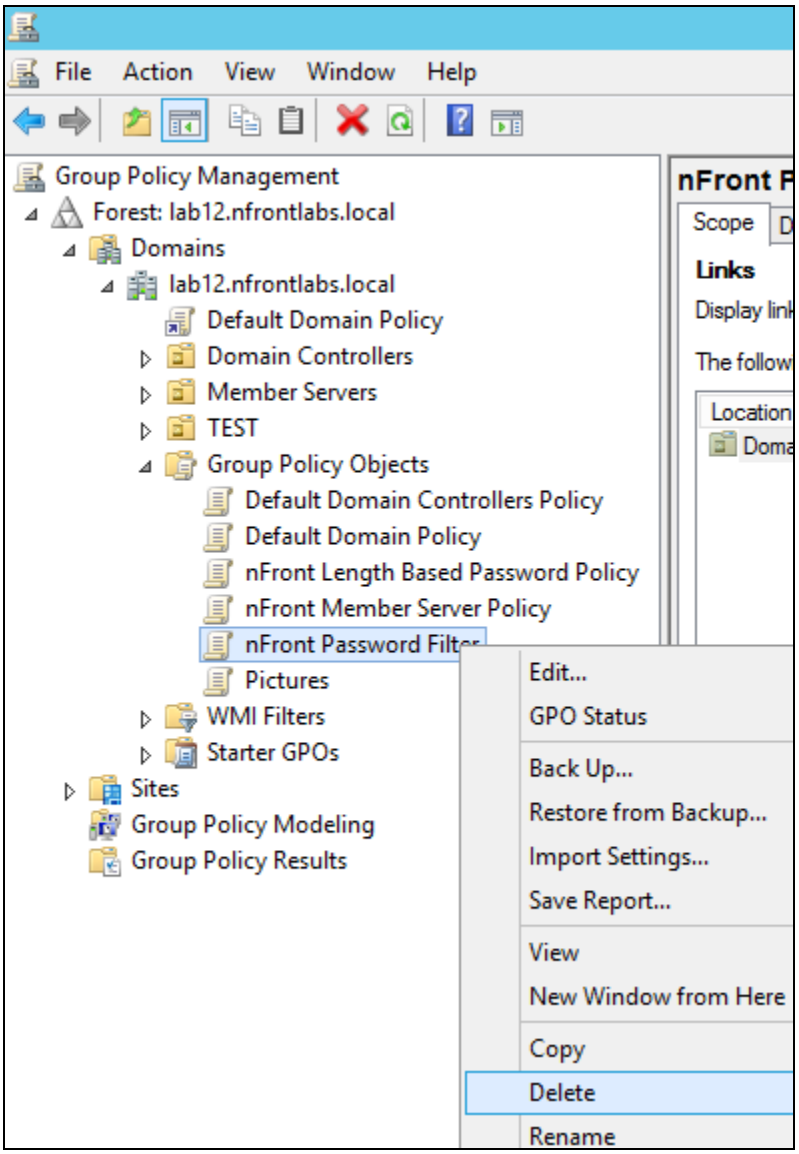


Figure 4.1.1: Deleting the nFront Password Filter policy.

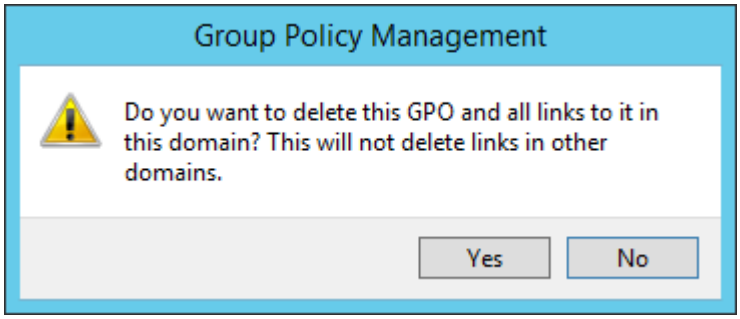


Figure 4.1.2: Deleting the nFront Password Filter policy.

IMPORTANT NOTE: If you simply need to quickly disable nFront Password Filter, you can simply turn on the setting to "bypass password filtering" in the General Configuration policy and then uninstall and reboot at your convenience.

4.2 Run Uninstallation

Go to Start + Control Panel + Programs + Uninstall a program + Uninstall nFront Password Filter. At the end of the uninstallation routine you will be prompted for an optional reboot. You do not have to reboot at that time. The uninstallation removes the filter engine and supporting services. At that point the software is not operational. A reboot is needed to remove the base DLL that is locked by the OS.

5.0 Verifying your Registration of nFront Password Filter

If you have purchased nFront Password Filter, you will receive an email with a registration code. The registration code must be entered into the nFront Password Filter group policy.

IMPORTANT: The registration code contains groups of capital letters and numbers separated by dashes. It must be entered exactly as emailed or printed on the box label (all capital letters with dashes).

1. Launch GPMC and navigate to Domains\<domain name>\Domain Controllers. Right-click the nFront Password Filter MPE policy you created and click the Edit button.
2. From the Group Policy Window select Computer Configuration + Administrative Tools + nFront Password Filter (Figure 5.0.1). Double-click General Configuration and select the checkbox to "Turn on debugging" (Figure 5.0.2). Select OK to close the General Configuration dialog box. Double-click the Registration policy. It should already be enabled. If not, please Enable the Registration policy. Enter the registration code that you were sent via email or the one that appears on the box label (Figure 5.0.3). The code must be typed using capital letters and the code must include the dashes. You must also enter the annual maintenance code that you received with the purchase. Click OK to close the Registration dialog box. **Minimize** the Group Policy editor.

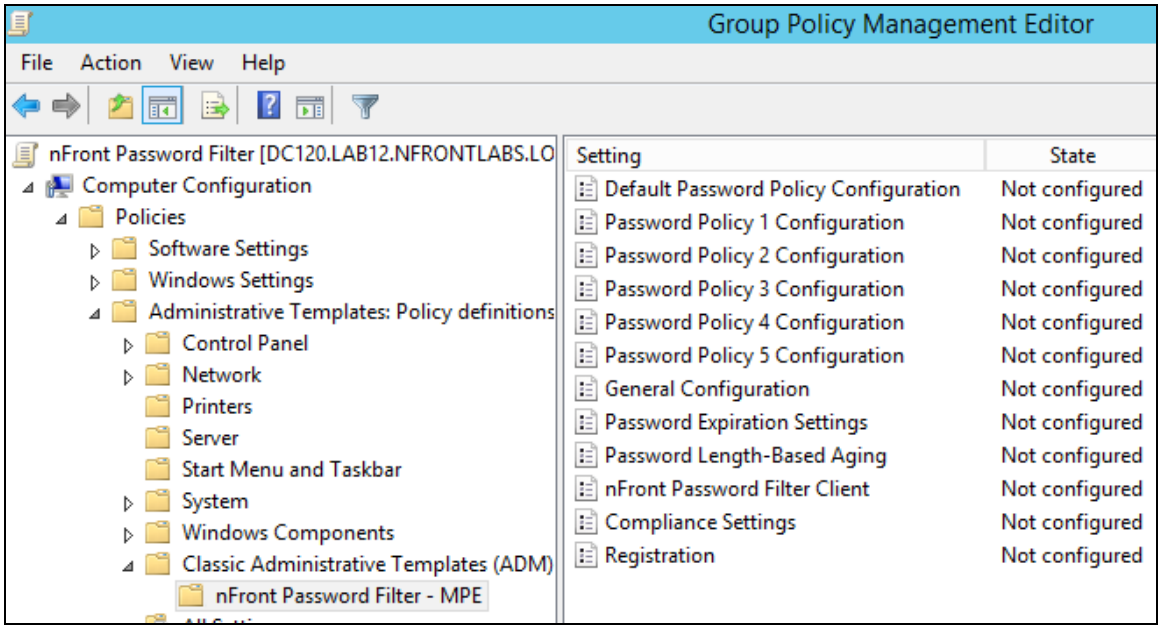


Figure 5.0.1: nFront Password Filter Group Policy

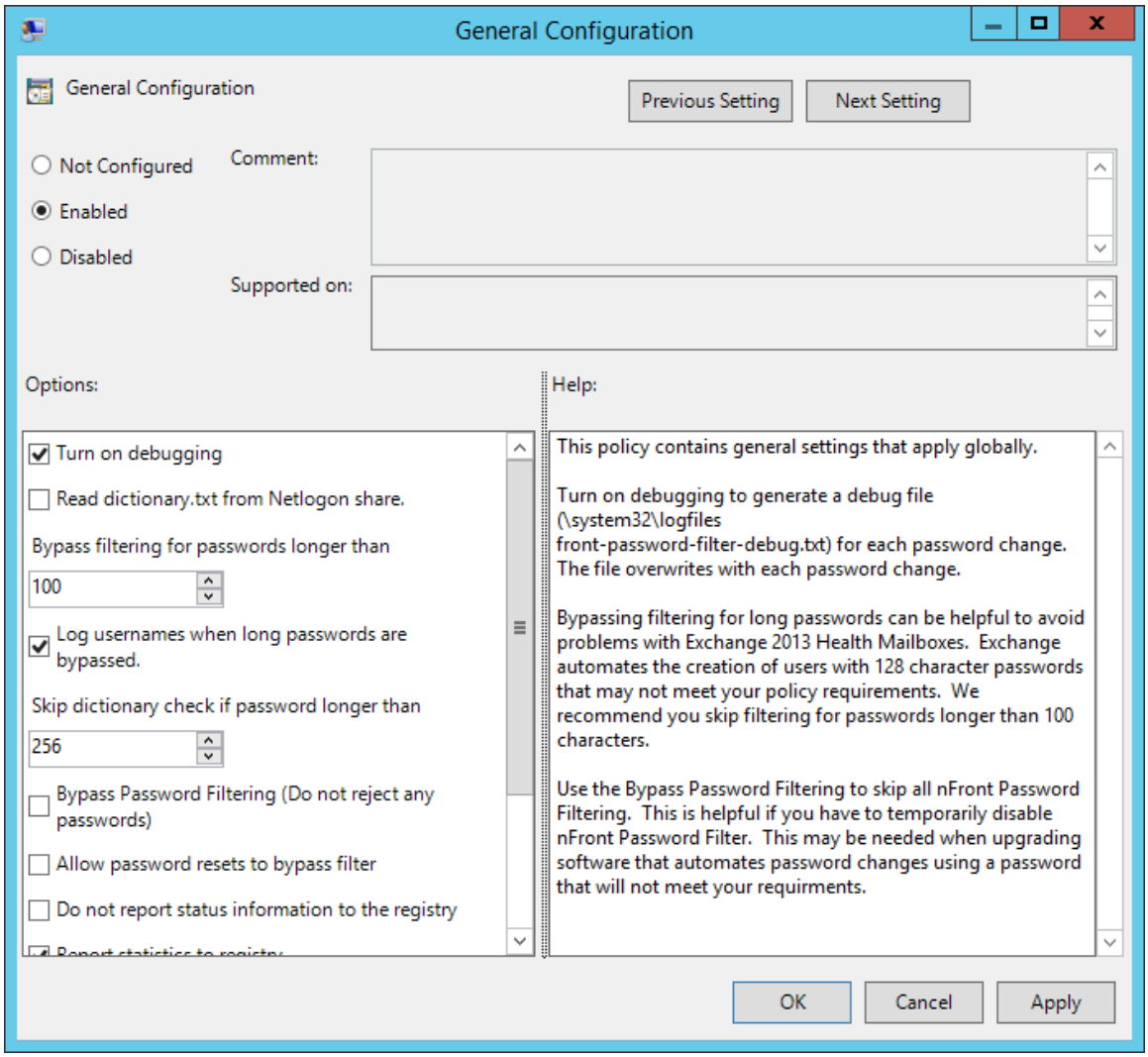


Figure 5.0.2: Turn on debugging

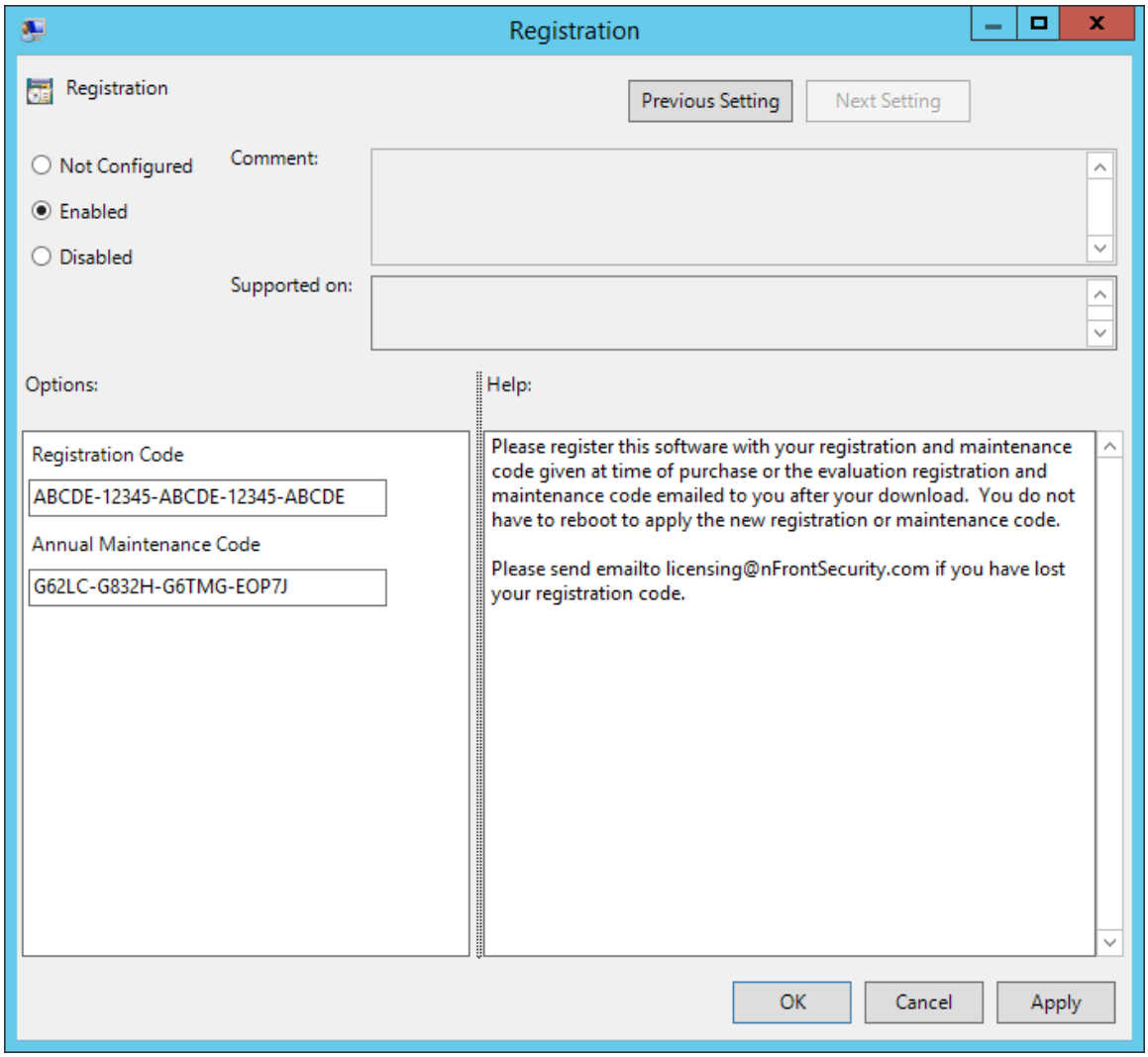


Figure 5.0.3: Enter Registration Code (all CAPS, include dashes)

3. Run `gpupdate /force` to propagate the new policy settings.

4. Change the password on a test account.

TIP: Change the password from the command line.
Example: net user <username> <password>

5. Inspect the %sytstemroot%\system32\logfiles\nfront-password-filter-debug.txt file. You should see the following lines:

registered = 1
Annual Maintenance Code = <maintenance code>
  Contract expires on <contract expiration date>

This line indicates that nFront Password Filter MPE is properly registered.

6. Maximize the Group Policy editor. Remove the debugging by double-clicking the General Configuration policy and removing the checkbox for the item labeled “Turn on debugging.” The policy will replicate in the next 5 minutes. Run gpupdate to force immediate replication.

7. Close the Group Policy editor.

6.0 Upgrade Instructions

You can confirm your current version by going to Control Panel + Add/Remove Programs and look at the properties for nFront Password Filter. If the version is not listed as part of the name you can click on the link for support information to confirm the version.

Upgrading from Passfilt Pro 5.x.x (or later) to the latest version of nFront Password Filter
You do not have to uninstall the old version. Simply run the installer for the latest version. If you watch closely you will notice it stop the current services and replace them with new ones. If you have customized the dictionary.txt file it will not be overwritten.

Upgrading from Passfilt Pro 3.5x (or later) or nFront Password Filter 4.x (or later) to the latest version of nFront Password Filter
The new version does not upgrade the ppro.dll "skeleton" file locked in memory. It does upgrade the ppro-eng.dll file and add a new service. To update to the latest version:

1. Uninstall old version. Do not reboot if prompted to do so.
2. Install new version. No reboot needed. Check to see that you now have a nFront Password Filter Password Policy service installed and running.

Since the new version will update the ADM templates in the c:\windows\inf folder you will not need to modify the GPO for nFront Password Filter. In fact, if you open the GPO you may see some new settings depending on the features added by the latest version to which you upgraded.

Upgrading from Passfilt Pro version 3.5 or earlier to the latest version of nFront Password Filter
Since the new version uses a new filter name, you can uninstall the old version and install the new version with no reboot in between.

1. Uninstall old version. Do not reboot if prompted to do so.
2. Install new version. Optionally reboot at end or at next opportunity.

Open the GPO where you have loaded the nFront Password Filter Group Policy Template. Right-click Administrative Templates and remove the old template. Then add the new template (nFront-Password-Filter-mpe.adm, nFront-Password-Filter-spe.adm, nFront-Password-Filter-spe-

ms.adm or nFront-Password-Filter-de.adm). After clicking OK the GP Editor will refresh and your old registry settings from the previous version are preserved. The new template will expose a section titled “nFront Password Filter Client.” You do not have to enable it for the client to work. You do need to deploy the nFront Password Filter Client.MSI package to any workstations on which you wish to replace the standard password change dialogs with those customized for nFront Password Filter.

7.0 Implementation Guide

Implementing and enforcing a new password policy can be a little tricky. It can impact on your users and your staff who support them. Here are some guidelines to make the transition as smooth as possible.

- **Everyone needs to know the new password policy in advance.** This will give your users time to think of passwords that conform to the new policy. We suggest sending a company-wide email informing users of the new policy and exactly when it will be put into place.
- **Force everyone to conform to the policy.** When it comes time to implement the new policy, configure all accounts to change password on next logon. In Windows 2003 and up you can select multiple accounts + Properties + Account + User must change password at next logon.
- **Thoroughly test the password policy in a test environment.** While we promise nFront Password Filter performs as advertised, we cannot promise it will "do what you mean" and not "do what you tell it." Make sure you have made the proper selections in the group policy and entered the correct information into the passfiltpro.ini file to enforce your advertised password policy.
- **Use reasonable standards for your password policy.** Keep in mind that if the password policy is very restrictive, users will be more inclined to write down their password on a post-it. If you want users to not write down passwords, try to implement a password synchronization mechanism. In many environments users feel the need to write down passwords because they must have so many, not because the passwords are complex.
- **A dictionary check may not be needed.** If your company requires multiple non-alphanumeric characters in the password, it is very unlikely such a password will be found in a dictionary. However, if you have customized your dictionary with many words containing non-alphanumeric characters such as !@#$%^ (hold SHIFT and press 123456).
- **Customize the dictionary to include terms from your industry.** The dictionary is intended to thwart common passwords. The supplied dictionary contains some common key sequences but consists mostly of true dictionary words. We suggest you open the dictionary.txt file and add common words specific to your profession or industry. Although the supplied file is in alphabetical order, it does not have to be. Thus, you could simply add your additional words to the bottom of the file. The dictionary check is case-insensitive, so there is no need to type your additional words using variation in case (i.e. uppercase, lowercase, mixed case versions, etc.). If you demand a sorted dictionary, you can always open the file in a spreadsheet program like Microsoft Excel, sort it and save it as plain text (ANSI).

8.0 Troubleshooting

8.1 Common Problems

Symptom	Proposed Troubleshooting
System is not filtering passwords.	Registration Code may be wrong / mistyped. Turn on debugging. Change the password for a test account and look at the debug file (usually c:\winnt\system32\logfiles\nfront-password-filter- debug.txt). If you are evaluating and evaluation = 0, your evaluation registration code is wrong or expired. Annual Maintenance Code may be wrong / mistyped. Turn on debugging. Change the password for a test account and look at the debug file. If the maintenance code is mistyped or expired there will be an obvious message in the debug file. Evaluation copy may have expired. Turn on debugging. Change the password for a test account and look at the debug file. If the evaluation product has expired it will be obvious in the debug file. The file will have a message in capital letters stating the product has expired. Registry configuration missing. On the domain controller experiencing the problem, run regedit and look for HKLM\Software\Policies\Altus\PassfiltPro. If the key is not present the Group Policy template is not loaded or is loaded under the wrong OU and not replicating to your domain controller. See the installation instructions and double-check to see that you have loaded the passfiltpro-mpe.adm template. nFront Password Filter may not be installed on this DC. Start + Run + winmsd. Expand Software Environment + Loaded Modules. Look for ppro.dll (or pprompe.dll or passfilt.dll). If ppro.dll is not found the DLL was not loaded by the operating system at boot. Perhaps the installation failed. Check the registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages to see if it shows an entry for PPRO (or PPROMPE or PASSFILT for older versions). If so the DLL failed to load on the last boot cycle. Verify the c:\winnt\system32 directory contains a pprompe.dll. Try rebooting the DC to see if it will load. If not, please call or email our technical support.
Everyone is getting the Default Password Configuration Policy (i.e. other policies not working and exclusions not working)	Group Filter Service files are likely missing. Open a command window and type net start You should see the “nFront Password Filter Group Filter Service” running. If not, type net start “nFront Password Filter Group Filter Service” Wait about 1 minute. Open Windows Explorer and search the Windows\System32 directory for the keyword “pass.” You should see files named: passfiltpro_policy1_include.txt
Dictionary check not working correctly.	File format may not be ANSI. If you edited the file in Notepad and saved in an ANSI format you should have not problems. However, if you used another editor or saved in a non-ANSI format you may have problems. Regardless of how you edited the file before, open it in Notepad. Perform a File + Save As operation and make sure you select the ANSI format. Recheck nFront Password Filter MPE by changing

	another password.

8.2 Sample Debug File

```
Username = test1
FullName = Joe Smith

Password change does NOT meet nFront Password Filter rules.
************************************************************
**
* nFront Password Filter Multi-Policy Edition
************************************************************
**
Version Information
-----------------------
evaluation = 1
expired = 0
evaluation expiration date: 4/30/2010
registered = 0
registrationCode = <eval code here>
Annual Maintenance Code = <maintenance code here>
   Contract expires on <maintenance code expiration date>

nFront Password Filter version 5.0.0 Build 2011020901
------------------------------------------------------------
-
Licensing Information
-----------------------
Number of Domain Controllers = 1
Number of nFront Password Filter Licenses = 15
------------------------------------------------------------
-
Dictionary Check Information
-----------------------
global dictionary check = 0
global substring check = 0
------------------------------------------------
POLICY NAME: Default Policy

maxCharacters = 256
minCharacters = 0
minCharTypes = 0
checkNumeric = 1
  minNumericChar = 2
  maxNumericChar = 256
checkUpper = 0
  minUpperChar = 0
  maxUpperChar = 256
checkLower = 0
```

```
  minLowerChar = 0
  maxLowerChar = 256
checkAlpha = 0
  minAlphaChar = 0
  maxAlphaChar = 256
checkNonAlphaNumeric = 0
  minNonAlphaNumericChar = 0
  maxNonAlphaNumericChar = 256
restrictSpecialChar = 0
  allowedSpecialChar =
checkVowels = 0
noBeginNumeric = 0
noEndNumeric = 0
numericPosition = 0
specialPosition = 0
checkConsecutive = 0
checkUsername = 0
checkFullname = 0
checkDictionary = 0
substringSearch = 0
applyGroups =
excludeGroups = Service Accounts

This policy applies to the user.
THE PASSWORD DOES NOT MEET THE POLICY REQUIREMENTS.
THE FAILURE CODE IS 8
THE PASSWORD FAILED THIS POLICY BECAUSE:
 - Password does not meet requirement for numeric
characters.
-------------------------------------------------
POLICY NAME: Policy 1

maxCharacters = 256
minCharacters = 0
minCharTypes = 0
checkNumeric = 0
  minNumericChar = 0
  maxNumericChar = 256
checkUpper = 1
  minUpperChar = 2
  maxUpperChar = 256
checkLower = 0
  minLowerChar = 0
  maxLowerChar = 256
checkAlpha = 0
  minAlphaChar = 0
  maxAlphaChar = 256
checkNonAlphaNumeric = 0
  minNonAlphaNumericChar = 0
  maxNonAlphaNumericChar = 256
checkVowels = 0
```

```
noBeginNumeric = 0
noEndNumeric = 0
numericPosition = 0
specialPosition = 0
checkConsecutive = 0
checkUsername = 0
checkFullname = 0
checkDictionary = 0
substringSearch = 0
applyGroups = Wireless Users
excludeGroups = Executives

This policy applies to the user.
THE PASSWORD DOES NOT MEET THE POLICY REQUIREMENTS.
THE FAILURE CODE IS 16
THE PASSWORD FAILED THIS POLICY BECAUSE:
 - Password does not meet requirement for upper case
characters.
-------------------------------------------------
```

9.0 The nFront Password Filter Client

The nFront Password Filter Client is an optional component that you can add to workstations to

1. Display password rules that apply to the user.
2. Display optional password strength meter.**
3. Provide a better error message for rejected password changes.
4. Display optional message box at logon warning the user of upcoming password expiration based on nFront policy settings.**

The client works on Windows XP, Windows 7, Windows 8 and Windows 8.1, and Windows 10. There are 32-bit and 64-bit versions of the client. The 32-bit version will not install on a 64-bit OS. The 64-bit client supports all OS except Windows XP.

**IMPORTANT NOTE: If you wish to display the password strength meter or display the password expiration warning message box at logon you must create a separate GPO to target the workstations with registry settings from our client options GPO template.

IMPORTANT NOTE: If you are running Windows 2008 or Server 2012 domain controllers with the local firewall enabled you will need to edit the firewall settings to allow inbound port 1333 to support the nFront Password Filter client. This port is used by the client to send encrypted RPC communication with the nFront Password Policy service to retrieve the rules and the correct failure message. For more information, see our online knowledge base.

Windows provides the following failure message for rejected passwords.

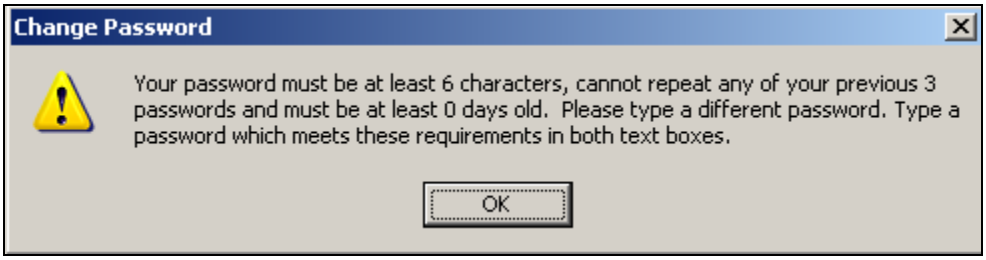


Figure 9.0.1A: Windows XP default message for failed passwords.

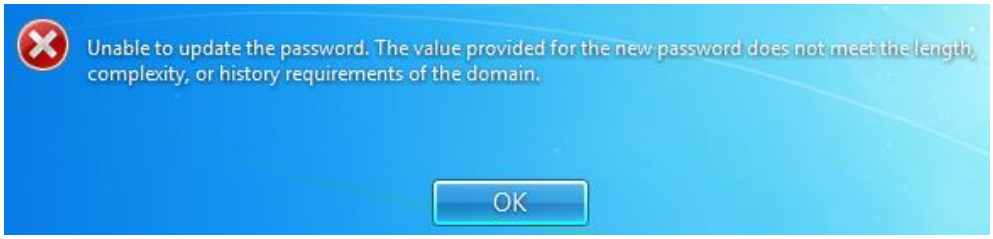


Figure 9.0.1B: Windows 7 default message for failed passwords.

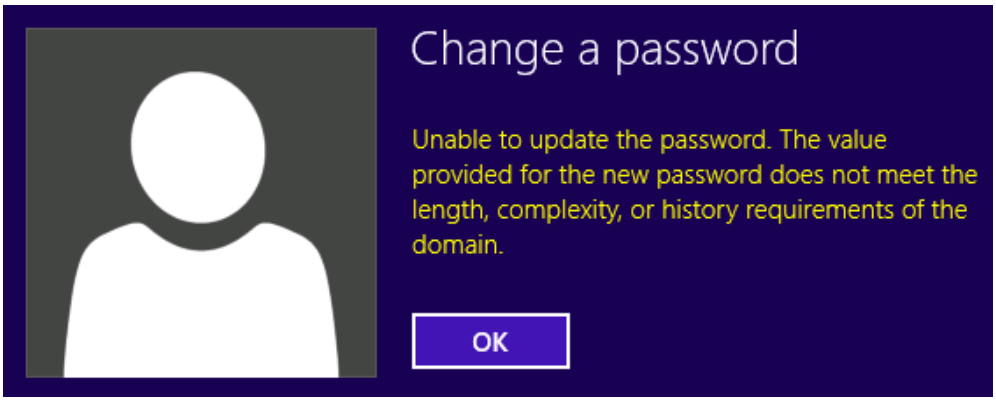


Figure 9.0.1C: Windows 8.1 default message for failed passwords.

The nFront Password Filter Client modifies the Password Change dialog box and displays password rules for the specific user. The dialog below shows the optional password strength meter which dynamically gauges the password strength. As the user types a new password, it can calculate the mathematically "crackability" of a password and gauge the password's strength based on thresholds set via a group policy.

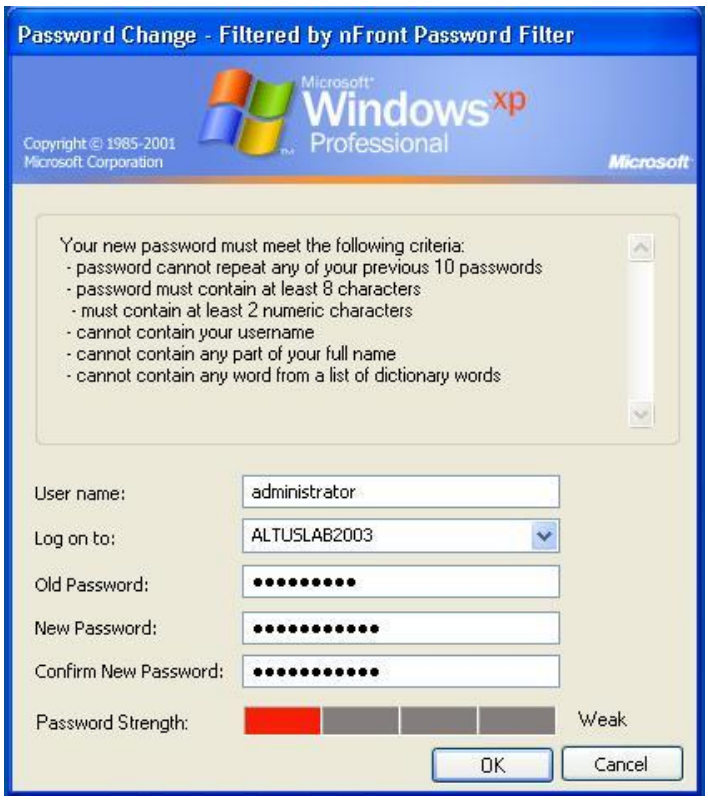


Figure 9.0.2A: Password Change dialog with nFront Password Filter Client installed (shown with optional password strength meter enabled)

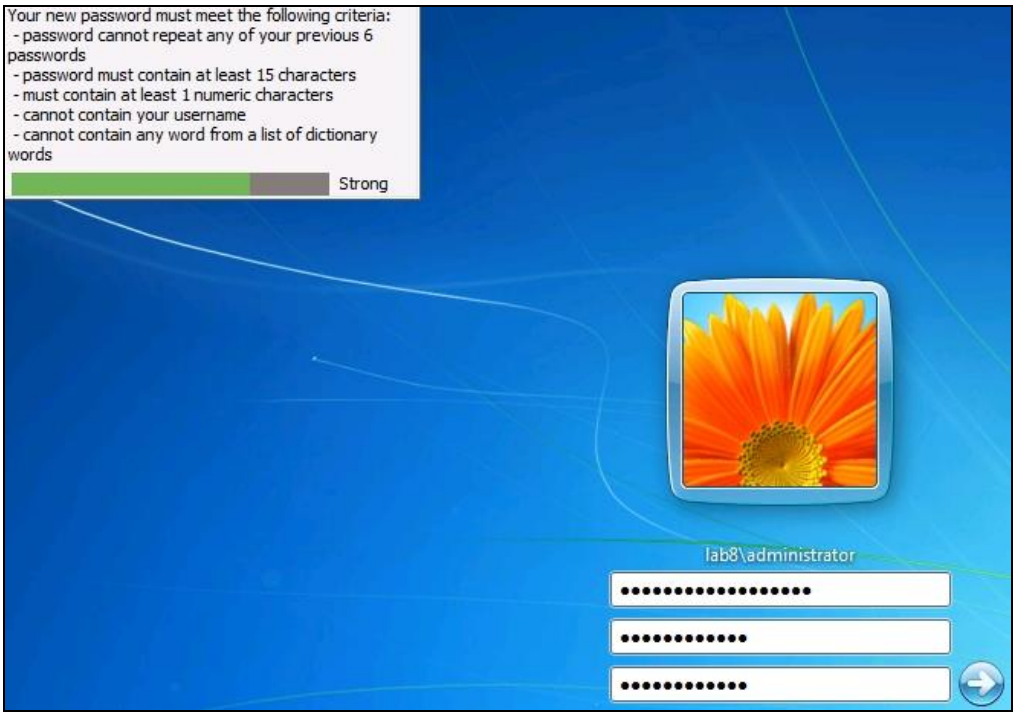


Figure 9.0.2B: nFront Password Filter Client on Windows 7 (shown with optional password strength meter enabled)

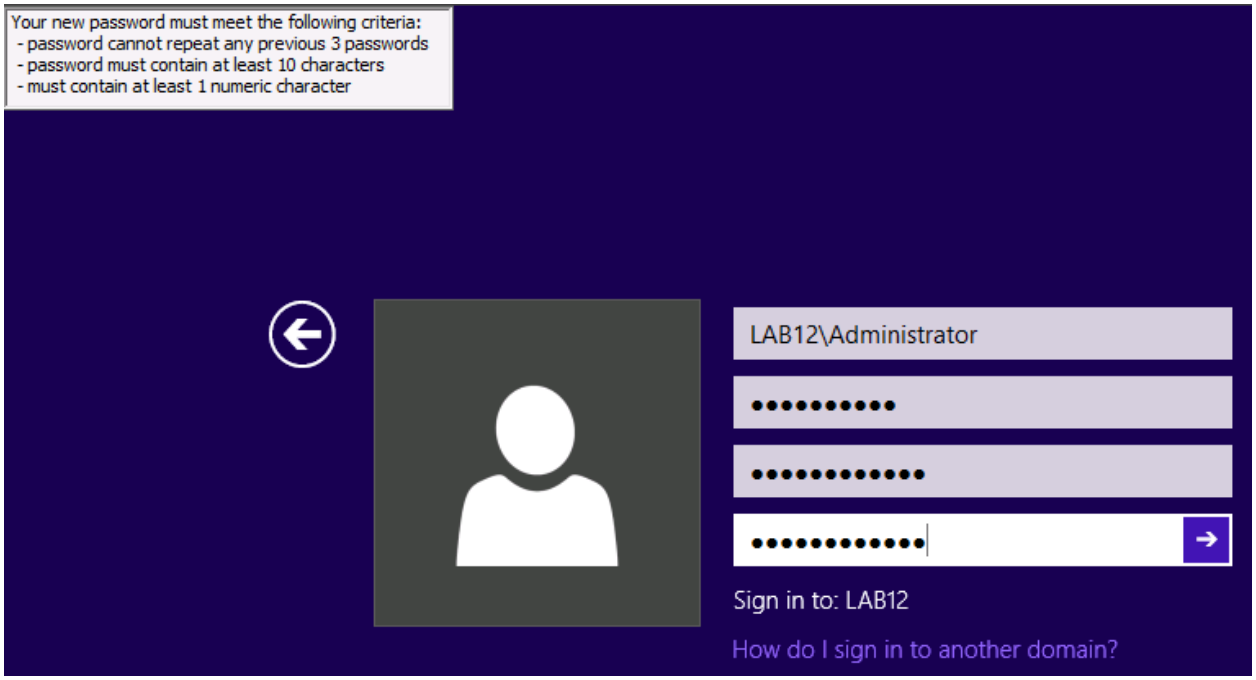


Figure 9.0.2C: nFront Password Filter Client on Windows 8.1 (without password strength meter)

If the user attempts a password change that does not comply with the rules, he or she will be given detailed reasons for the password change failure. If the password fails because it contained a dictionary word the actual dictionary word that caused the failure will be displayed.

Figure 9.0.3A: Password change failure message on Windows XP

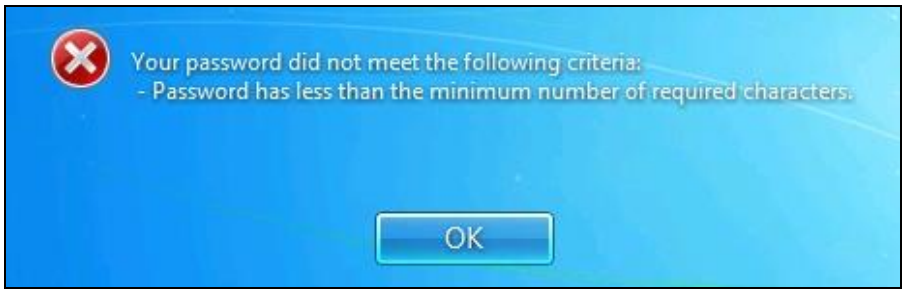


Figure 9.0.3B: Password change failure message on Windows 7

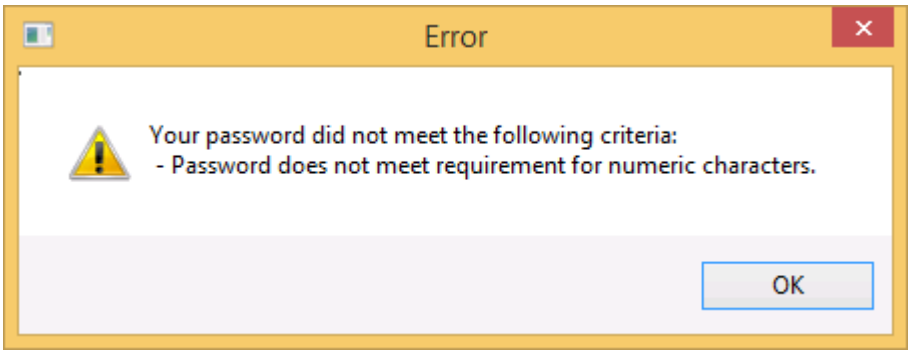


Figure 9.0.3C: Password change failure message on Windows 8.1

9.1 Technical Overview

On Windows XP the password change dialog box and failure message are generated by a DLL called MSGINA.DLL. We do not replace the MSGINA.DLL. Instead our software works as a "gina stub dll" and this is on the only Microsoft approved method for modifying the password change screen. There is an alternative method that can be used (called winlogon hooking) but the method is discouraged by Microsoft and not supported.

On Windows 7, 8, 8.1 and Windows 10 the password change screen is controlled by a logon credential provider. On those systems our software works as a credential provider.

9.1.1 Components

The nFront Password Filter client is packaged in an MSI format so it can be automatically distributed to 2 or 2000 workstations via a software deployment GPO. There are 2 MSI packages, one for 32-bit operating systems and one for x64 operating systems. The client can target Windows XP, Windows 7, Windows 8, Windows 8.1 or Windows 10. The client has been

tested with x64 versions of Windows 7, Windows 8 and Windows 8.1. During install the client detects the OS and installs the "gina stub" on Windows XP or the credential provider on Windows 7, Windows 8, Windows 8.1 or Windows 10.

The client components communicate via encrypted RPC to an RPC service running on each domain controller. The RPC service is labeled "nFront Password Filter Password Policy Service." All text displayed by the client is supplied by the service. This will make future upgrades much easier. The service file can be replaced without a reboot. Future modifications will include support for multiple languages.

9.1.2 Rules displayed by nFront Password Filter Client

The listing of rules presented to the client may contain any of the following. You also have the option of displaying your custom message only.

Password Policy Information:
<optional custom message here – controlled via GPO>

Your new password must meet the following criteria:

- password cannot repeat any of your previous XX passwords
- password must contain at least XX characters
- password cannot contain more than XX characters
- must contain characters from at least XX of the following character types
  upper-case characters lower-case characters
  numeric characters non-alphanumeric characters
- must contain at least XX and no more than XX numeric characters
- must contain at least XX and no more than XX upper case characters
- must contain at least XX and no more than XX lower case characters
- must contain at least XX and no more than XX upper or lower case characters
- must contain at least XX and no more than XX non-alphanumeric characters
- can only contain these special characters: <list of special char>
- cannot contain vowels (a,e,i,o,u, or y)
- cannot contain consecutive identical characters
- cannot begin with a number
- cannot end with a number
- must contain a number in position X
- must contain a special character in position X
- cannot contain your username
- cannot contain any part of your full name
- cannot contain any word from a list of common words

We combine the Microsoft Password Policy settings with nFront Password Filter rules to determine the overall requirements. The nFront Password Filter Client determines the password history (i.e. "previous XX passwords") based on your Windows Password Policy settings. It also queries the domain password policy for the minimum length. If your Windows Password Policy is set to a minimum of 10 characters and nFront Password Filter is set to a

minimum of 8, the Windows policy is more restrictive and the rules displayed with will show a minimum length of 10 characters.

9.1.3 Multiple Domain Support

The nFront Password Filter Client is designed to work with multiple domains. So if a user's account is defined in xyz.com and the user logs onto a workstation in sales.xyz.com, the nFront Password Filter Client will query an xyz.com domain controller to get the password rules and to perform the password change operation.

9.1.4 Multiple Language Support

The nFront Password Filter Client lists rules in English, German, Italian, French and Spanish. If you would like the rules in another language, please email us at support@nFrontSecurity.com with a language request. The client already reports the user's interface language to the server component.

9.1.5 GINA chaining (Windows XP Only)

Microsoft allows only one Gina stub DLL on a client workstation. The GINA hook is described by a registry key:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL, REG_SZ, <DLL Name>

Vendors such as RSA and others have designed what they refer to as gina chaining. Upon install they inspect this registry key. If they discover another GinaDLL, they make a note of it in the registry configuration for their GinaDLL and replace the current GinaDLL key with their DLL. Their DLL code is then designed to call the "next gina" in the chain instead of simply calling the real MSGINA.DLL. This design makes some assumptions that could be dangerous. It assumes that the MSGINA.DLL is eventually called. It assumes the GINA dll chain is not broken. It assumes there is no overlap in product functionality.

Other gina based systems can chain to our DLL. We will support our DLL chaining to another vendor's DLL but you must contact us to get details on how to implement that process.

9.2 Steps to install the client via Software Installation GPO

We like this approach because it automatically installs the client on any new workstation that you may have overlooked (if the new workstation is part of the OU where the software install GPO is deployed).

If you have not done so already, create a new shared folder on a server to store the MSI package for deployment. Make sure the permissions are set such that Authenticated Users have READ access. We suggest a hidden share like:

\\server.xyz.com\deploy$

Copy the MSI package to the shared directory.

Now create and configure the software deployment GPO. In the following example, we use the GPMC SP1 add-on for Windows 2003 to create the policy linked to the ALTUS OU.

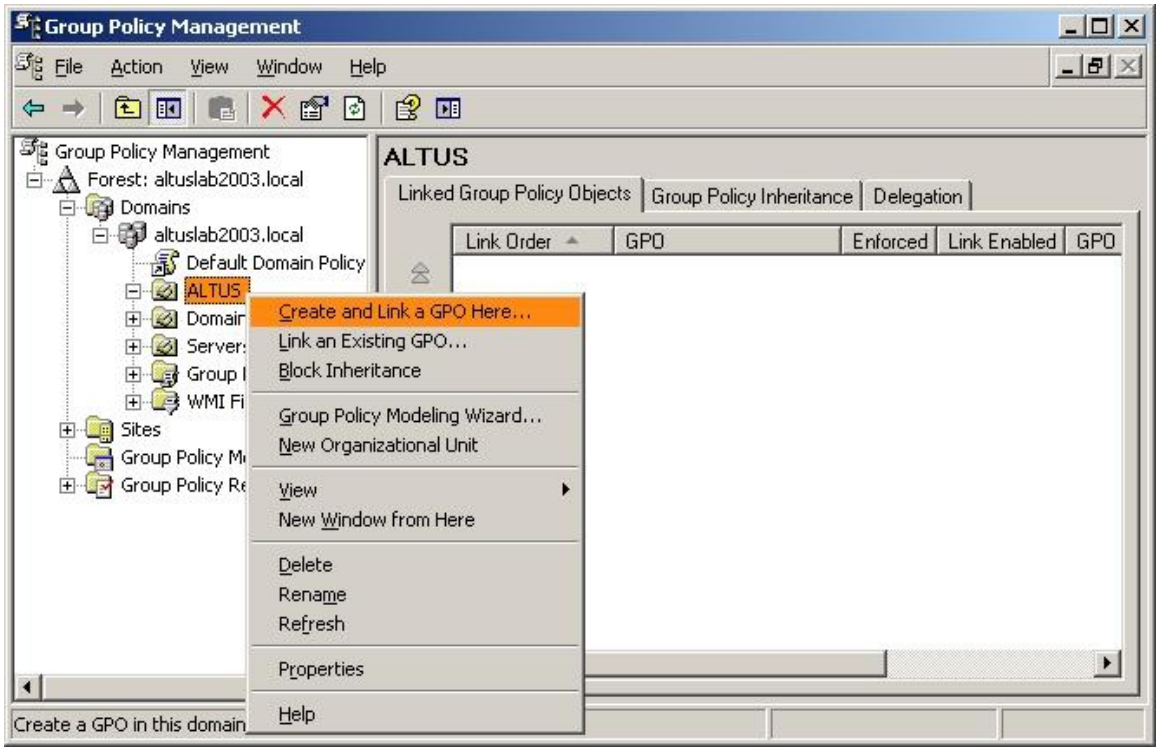


Figure 9.2.1: Creating a new software deployment GPO via GPMC

The newly created GPO will appear in the right-pane. Right-click and select Edit to edit the GPO. This will launch the Group Policy Object Editor. Go to Computer Configuration + Software Settings + Software Installation + right-click + New + Package

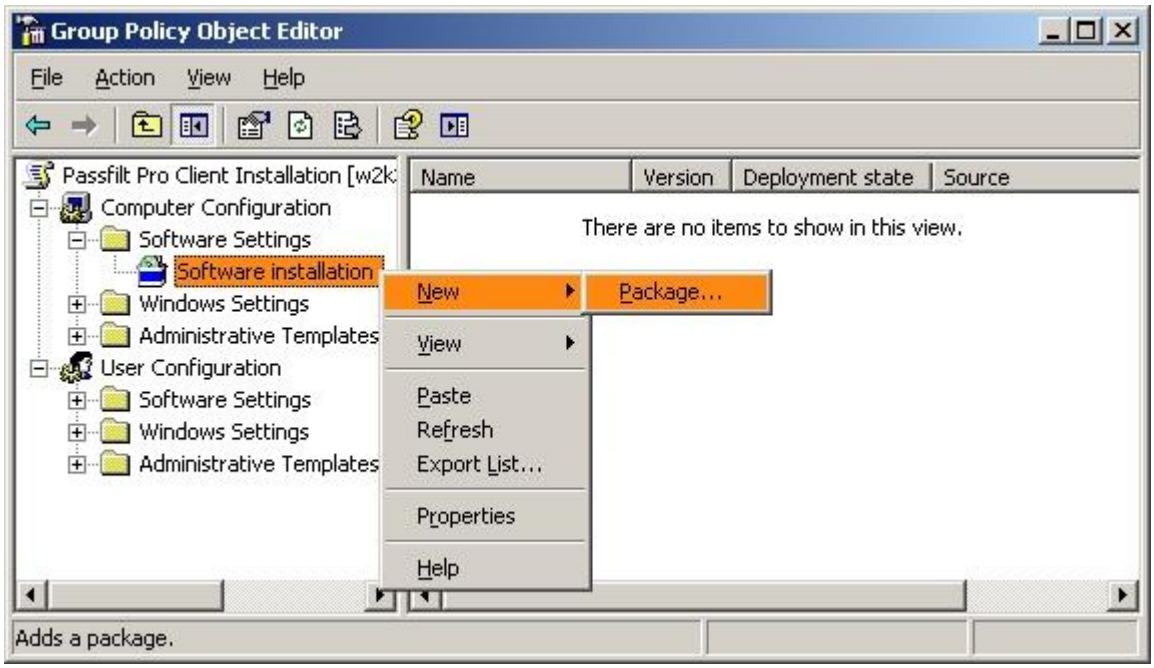


Figure 9.2.2: Adding a new package to the software deployment GPO

Note the package location in Figure 9.2.3. You should always use \\server.domain.local\share instead of \\server\share. The path provided must be one accessible to all clients will receive the GPO. Thus, this should always be a path to a shared directory.

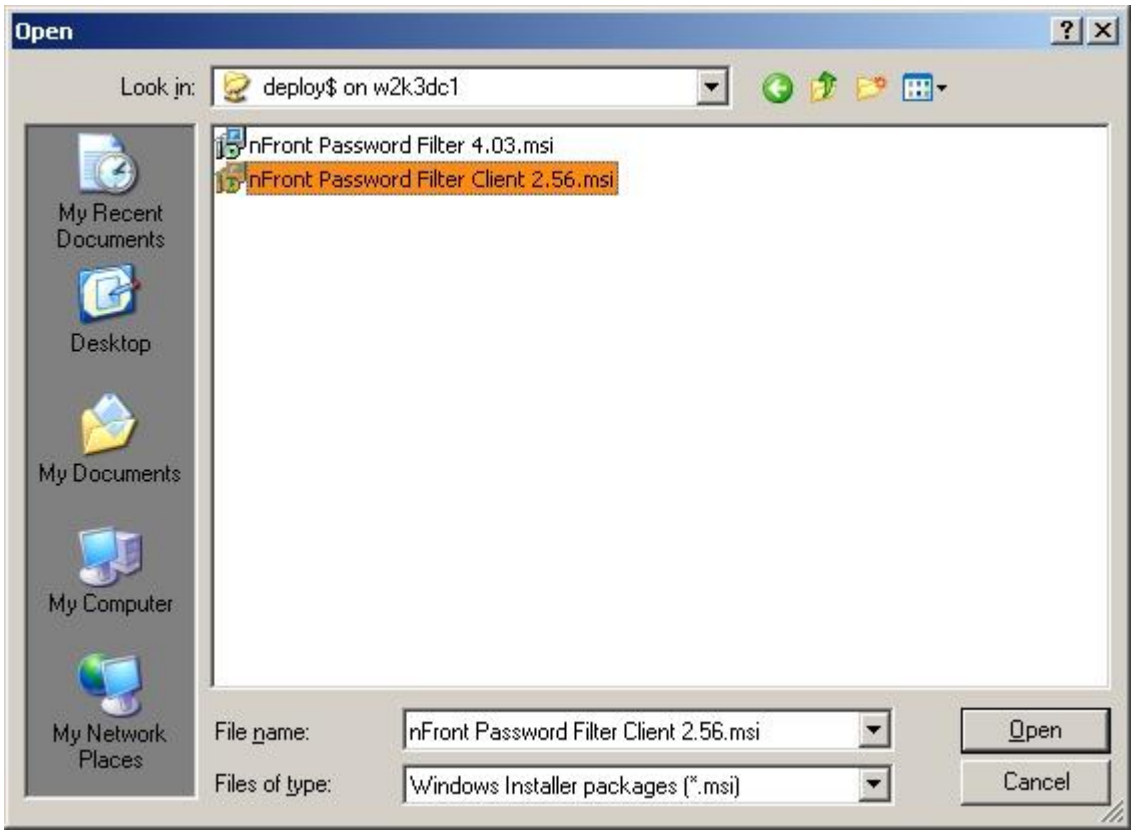


Figure 9.2.3: Providing the package location

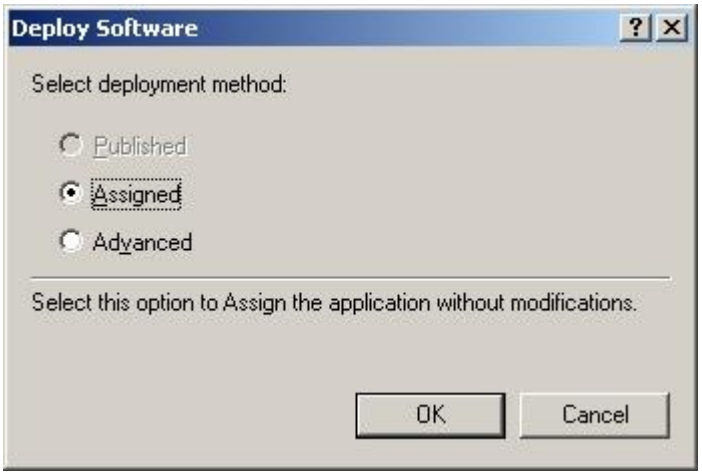


Figure 9.2.4: Always assign the application

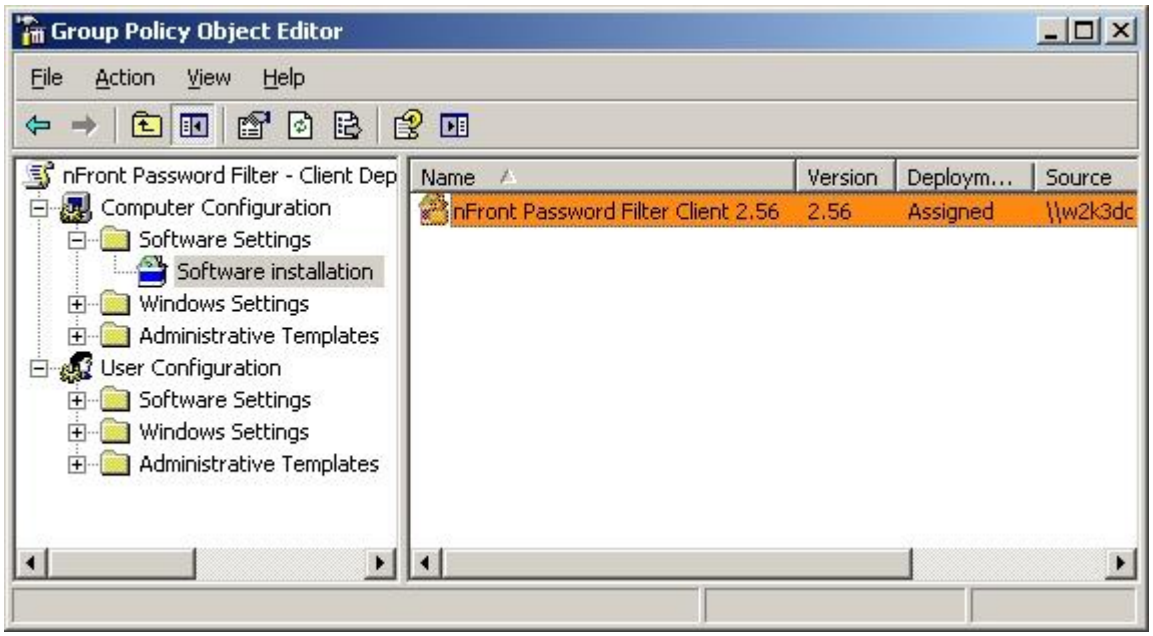


Figure 9.2.5: The package now appears in the right pane

There is one final and important step. You would prefer to uninstall the application if the computer is removed from the targeted OU / Domain. Right-click and edit the Properties of the nFront Password Filter Client package. Go to the Deployment tab and check the box for "Uninstall this application when it falls out of the scope of management."

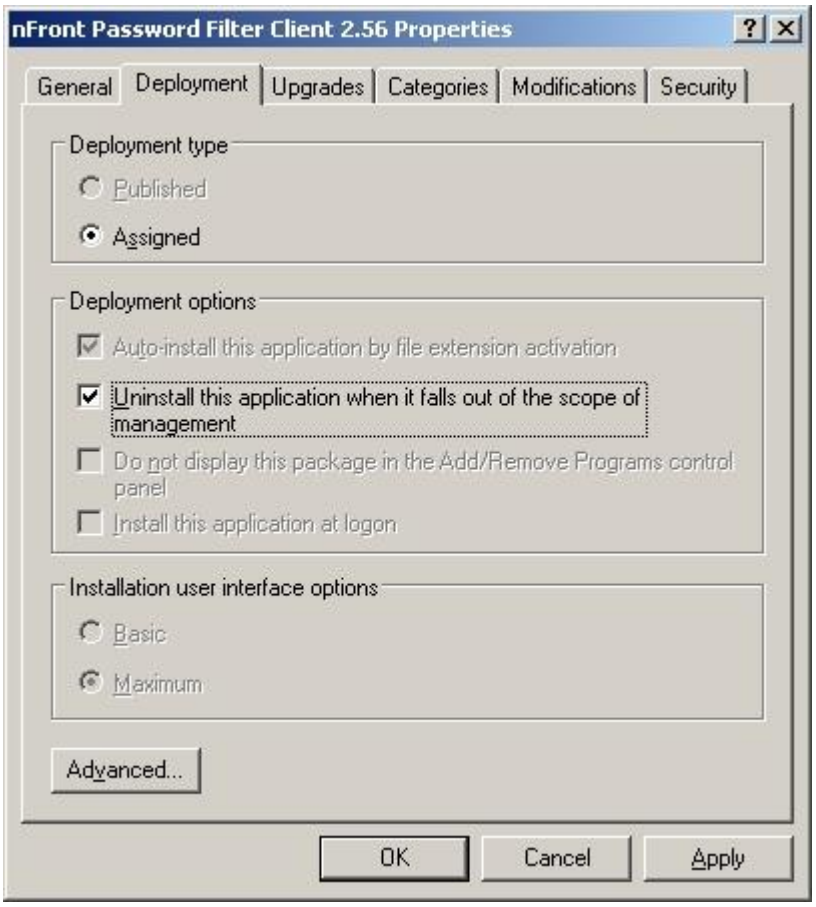


Figure 9.2.6: Changing the deployment options

Now, any computer that is a part of the ALTUS OU will receive the GPO on next boot. The software will be installed during boot and you will see a screen like the one in Figure 9.2.7.

Figure 9.2.7: Pre-logon screen showing automated software installation

Another reboot will be needed to complete the install on Windows XP (not on Windows Vista or Windows 7). The user is not prompted and the reboot is not forced. For Windows XP, the pre-logon software installation assigns the GinaDLL registry key and tells the operating system to

load the altusgina.dll on next boot. After the second reboot the nFront Password Filter Client will be functional.

9.3 Configuration

There are 2 GPO's that can be used to control the client behavior. The GPO deployed against the Domain Controllers OU controls the text delivered to the client from the RPC server on each domain controller. You can deploy another optional GPO to add the password strength meter or to globally disable all nFront Password Filter clients.

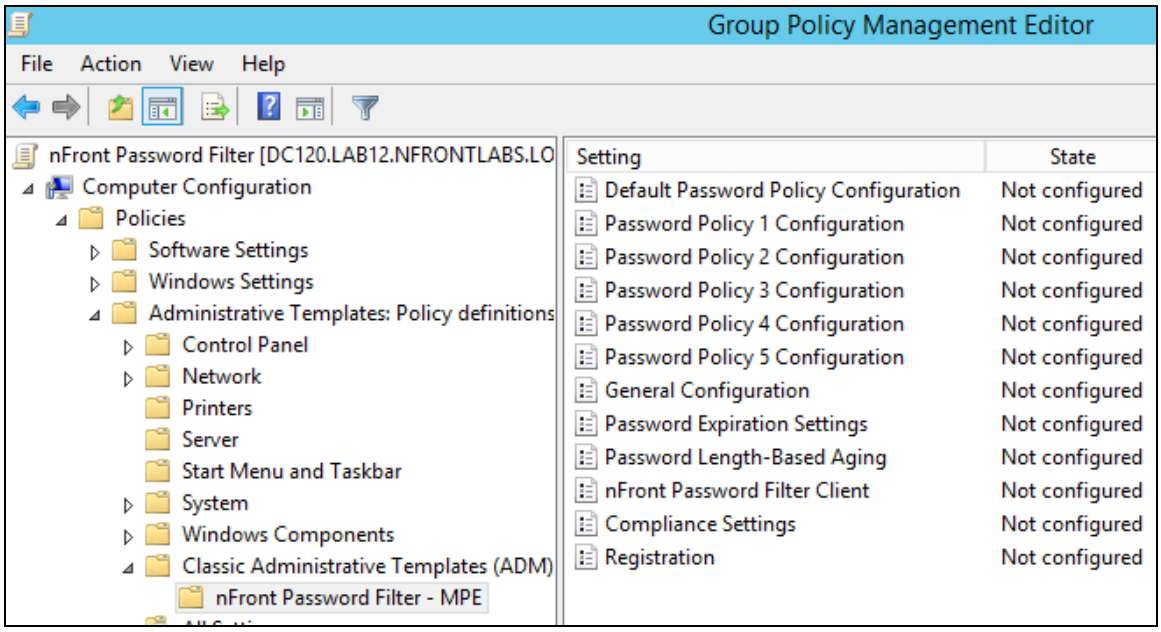


Figure 9.3.1: nFront Password Filter GPO for domain controllers OU

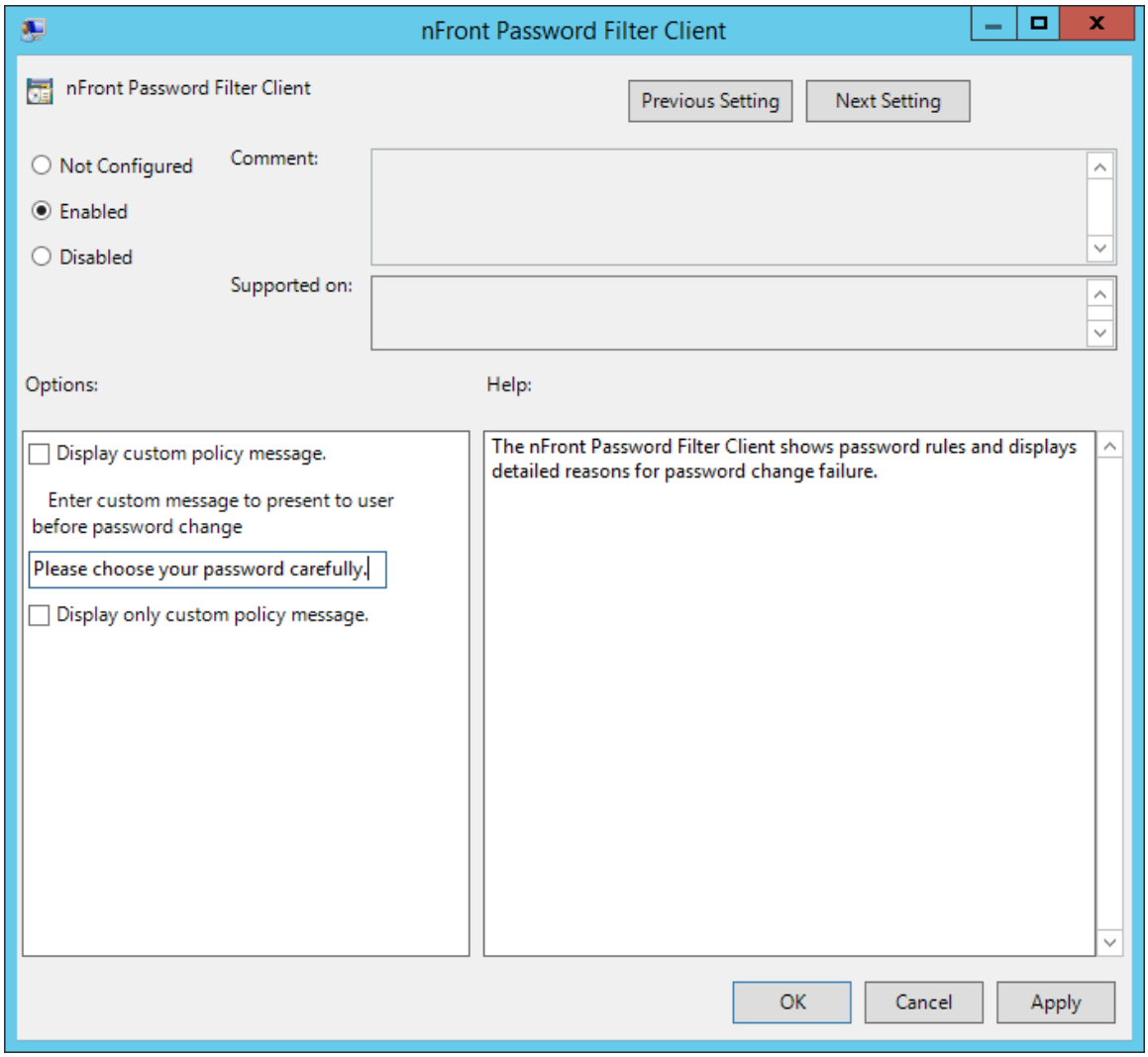


Figure 9.3.2: nFront Password Filter Client settings applied to the domain controller

Policy	Description
Display custom policy message	Displays custom message typed in text box. The message is limited to 1024 characters.
Display only custom policy message	Eliminates the standard display of nFront Password Filter policy requirements and displays only the custom message.

9.4 Configuring the Client Options GPO

The installation of the nFront Password Filter.MSI on each domain controller adds a nFront-Password-Filter-client-options.adm file to the c:\windows\inf directory on the domain controller. This template is needed to enable the password strength meter, to display the

password expiration warning message box at logon or to globally disable the nFront Password Filter client.

The client options GPO can be linked to any OU. If you wish to target all computers in the domain, it is fine to link it to the root of the domain. The configuration results in the distribution of about 8 registry entries on each workstation.

Figures 9.4.1 and 9.4.2 show a GPO linked to the root of the domain and the loading of the nFront-Password-Filter-client-options.adm template.

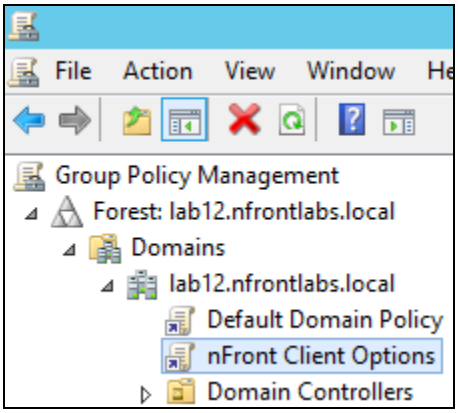


Figure 9.4.1: nFront Client Options GPO created and linked to root of domain

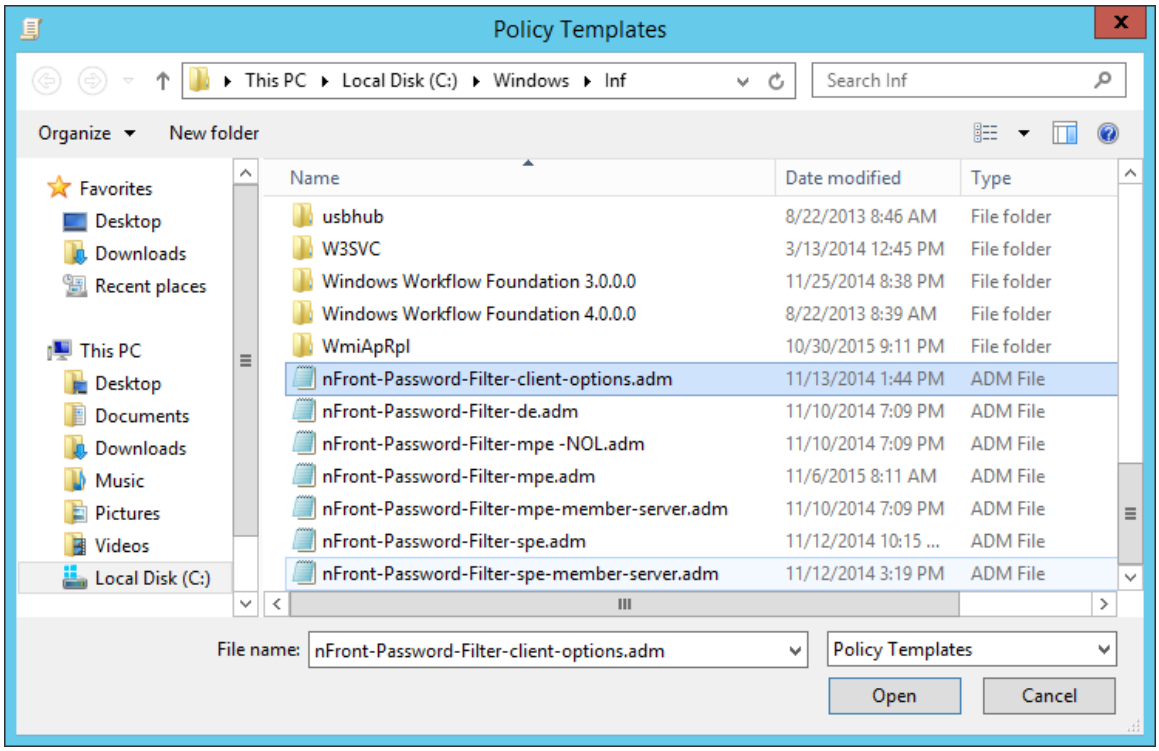


Figure 9.4.2: Loading the client options GPO ADM template

9.4.1 Configuring the optional Password Strength Meter

Suppose you want to display the password strength meter on all computers in the Accounting OU. You would create a new GPO at the Accounting OU level. In the new GPO, load the nFront-Password-Filter-client-options.adm template under Computer Configuration + Administrative Templates. Then configure the options as seen in figure 9.3.3. Clients refresh their policies every 90 minutes plus or minus a 30 minute random offset, so your changes will take place in 60 to 120 minutes. If you want to see the immediate effect, you can logon to the client, open a command window and type “gpupdate” or try “gpupdate /force.”

Figure 9.4.3 shows the optional settings and figure 9.4.4 shows the nFront Password Filter Client with the strength meter enabled.

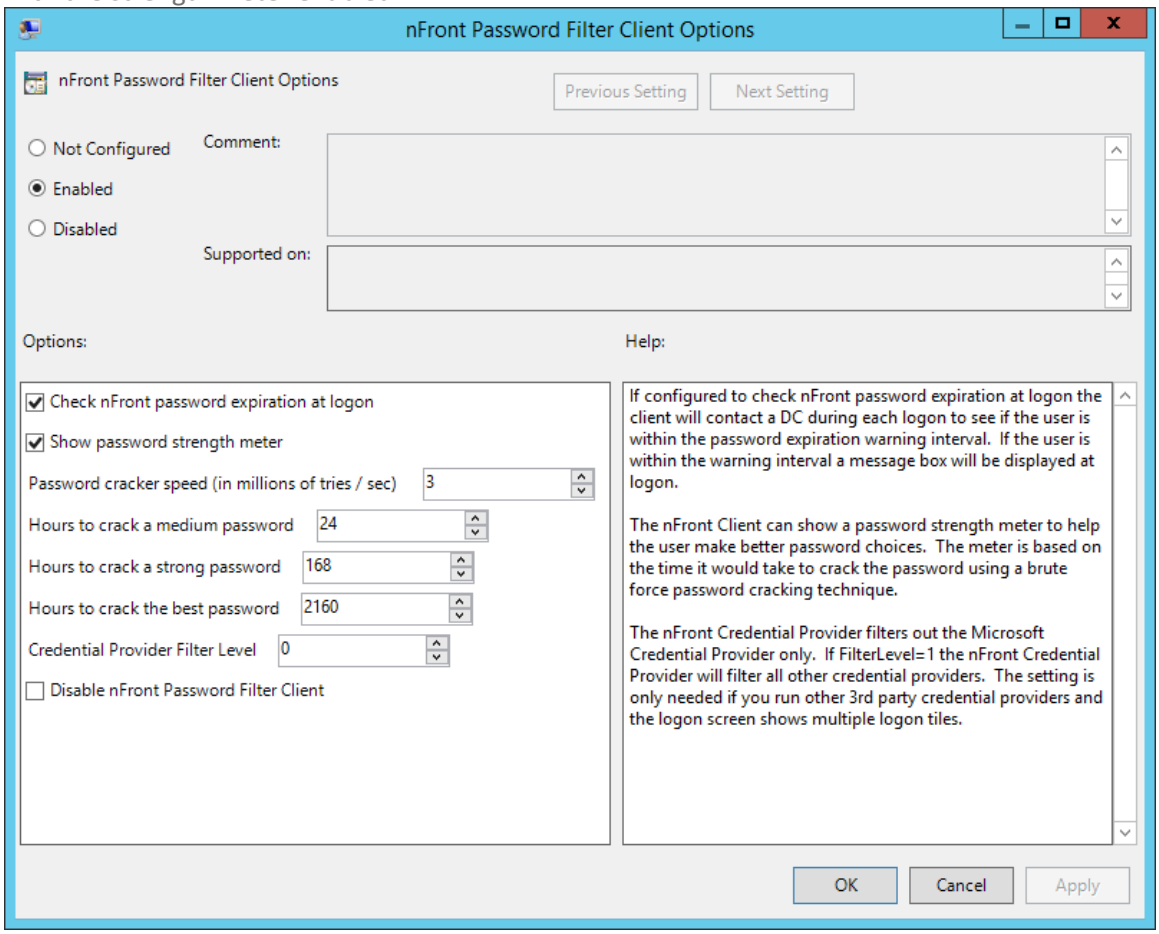


Figure 9.4.3: nFront Password Filter Client Options deployed at domain or OU level.

Policy	Description
Check nFront password expiration at	The client will contact any DC to get the

logon	password expiration time and it will notify the user via a message box at logon if the user's password expiration time is within the warning interval set in the nFront configuration(the GPO linked to the Domain Controllers container).
Show password strength meter	Displays password strength meter at bottom of password change dialog.
Password cracker speed (in millions of tries / sec)	Enter the average speed of current password crackers when performing a brute force attack.
Hours to crack a medium password Hours to crack a strong password etc.	Define the thresholds of time needed to crack a specific level password. In the example above the password will be rated medium only if it can be cracked in 6 to 24 hours. Please note that regardless of the setting for the Best threshold the password must be at least 15 characters to be considered a Best level.
Credential Provider Filter Level	Default: 0 Valid Values: 0 or 1 Only set to a 1 if you notice additional logon "tiles" on the logon screen. This indicates there is another 3rd party credential provider on the system. Setting the value to a 1 has our credential provider "filter" the other provider. This may result in partial or full loss of functionality implemented by the other provider. It would be a good idea to contact us and the other manufacturer if you notice multiple logon tiles.
Disable nFront Password Filter Client	Provides a way to globally disable all nFront Password Filter Clients affected by this GPO. If disabled the client remains loaded in memory, however, it passes all password change procedures directly to the MSGINA.DLL.

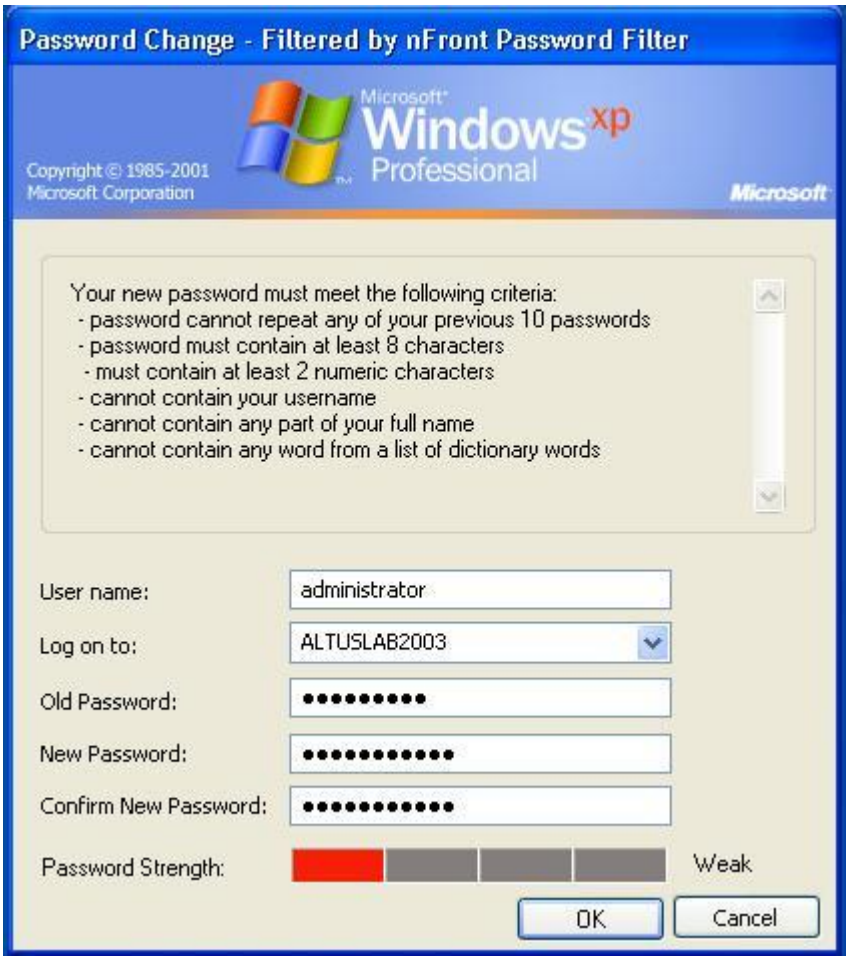


Figure 9.4.4: Client on Windows XP with password strength meter enabled

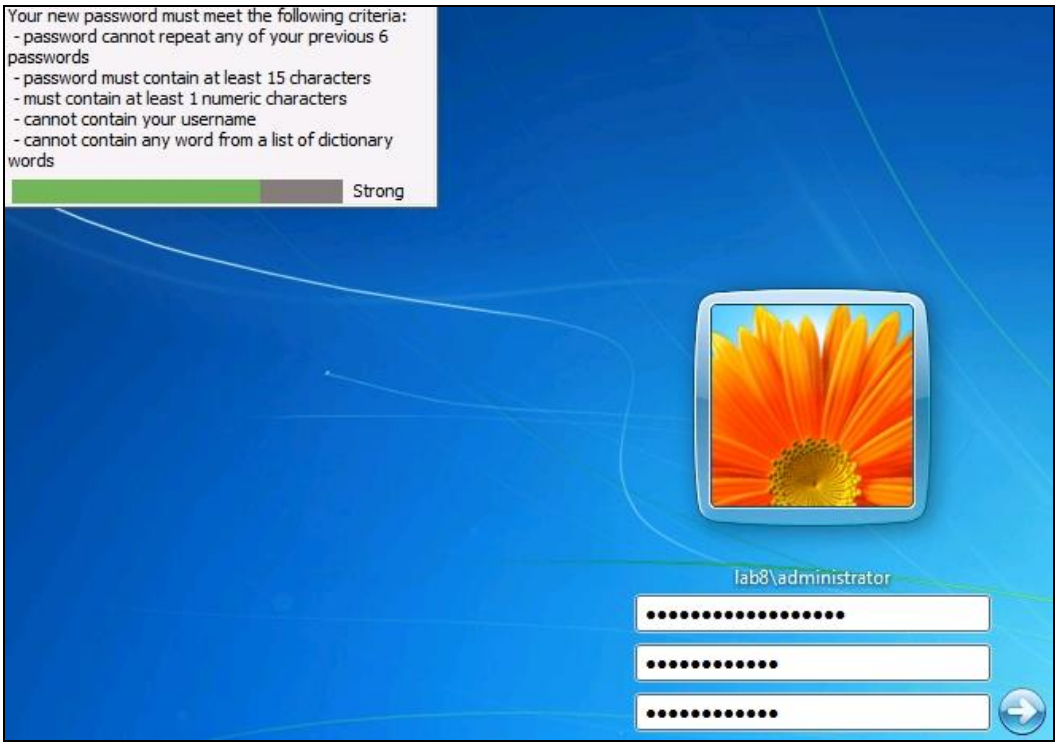


Figure 9.4.5: Client on Windows 7 with password strength meter enabled

The password strength is based on the mathematical "crackability" of the password. If the user has a 6 character password that is all lowercase, there are 6 positions with 26 possible letters used for each of the positions. The number of combinations would be 26^6. If a cracker can try at 3 million tries per second, the password can be cracked in about 102 seconds.

If the registry turns on the strength meter but is missing values for the thresholds, the default thresholds are assigned. A password cracker is assumed to try 2 million times per second. The thresholds are 168 hours (7 days) for medium, 2160 hours (90 days) for strong and 8760 hours (365 days) for best strength.

With version 6.0 the meter was modified to always rate passwords "weak" if they contain certain common words like "password" and if they contain consecutive repeating characters.

9.4 Troubleshooting

Windows XP
If the altusgina.dll file is deleted or if it is corrupted, the Windows XP operating system will display the message in figure 9.4.6 on boot. The solution is to reboot and press F8 during boot. Boot into Safe Mode and edit the registry.

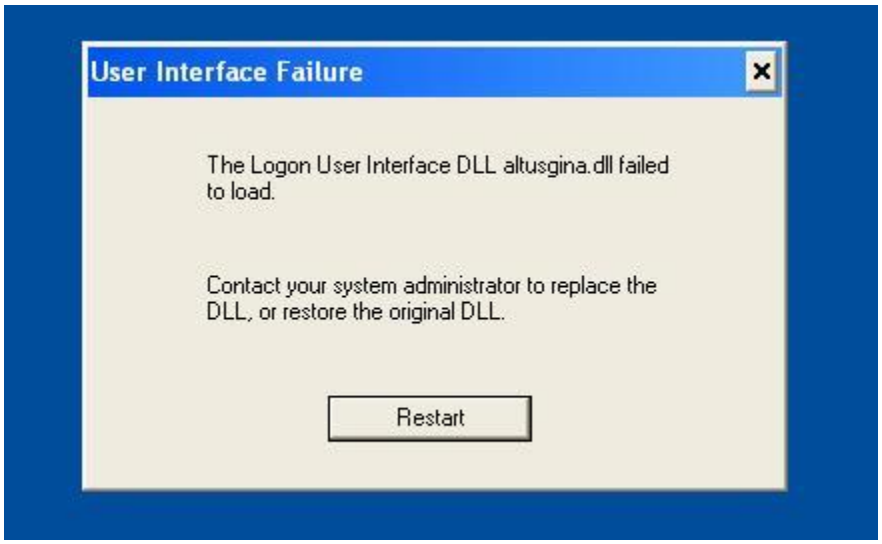


Figure 9.4.6: Missing or invalid GINA results in this message on boot

To temporarily disable the nFront Password Filter Client you can add the following registry value:
HKLM\Software\Policies\Altus\PassfiltProClient\Disable,REG_DWORD,1

To bypass loading the nFront Password Filter Client on boot, delete the following registry value:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL

Windows Boot problems (XP only)

If you experience a problem a blank logon screen (no prompt for userid or password) on boot, you will need to remove the nFront Password Filter client (i.e. the logon credential provider). To do this, reboot and press F8 to go into safe mode. Then use a System Restore Point to reverse the system back to the state prior to client installation.

Windows 7, 8, 8.1, 10 – multiple "tiles" at logon

If you see multiple tiles on the logon screen it is likely you have another non-Microsoft credential provider loaded. By default the nFront client only filters out the Microsoft credential provider during a password change. To ensure the nFront client is the only credential provider referenced you can add the following registry value:

HKLM\Software\Policies\Altus\PassfiltProClient\filterLevel, REG_DWORD, value=1

Or you can use the client options ADM template to make a GPO

RPC Errors

You may encounter the dialog in figure 9.4.7 if the communication with the domain controller fails. This could be a network problem, a domain controller that is unavailable or an error / failure in the nFront Password Filter Password Policy Service on the domain controller. You

should check the DC availability first and then check the service on the DC. If everything looks OK, try stopping and restarting the nFront Password Filter Password Policy service on the domain controller. There is a dependency on the Microsoft RPC service so you may want to check the status of that service and restart it as well.

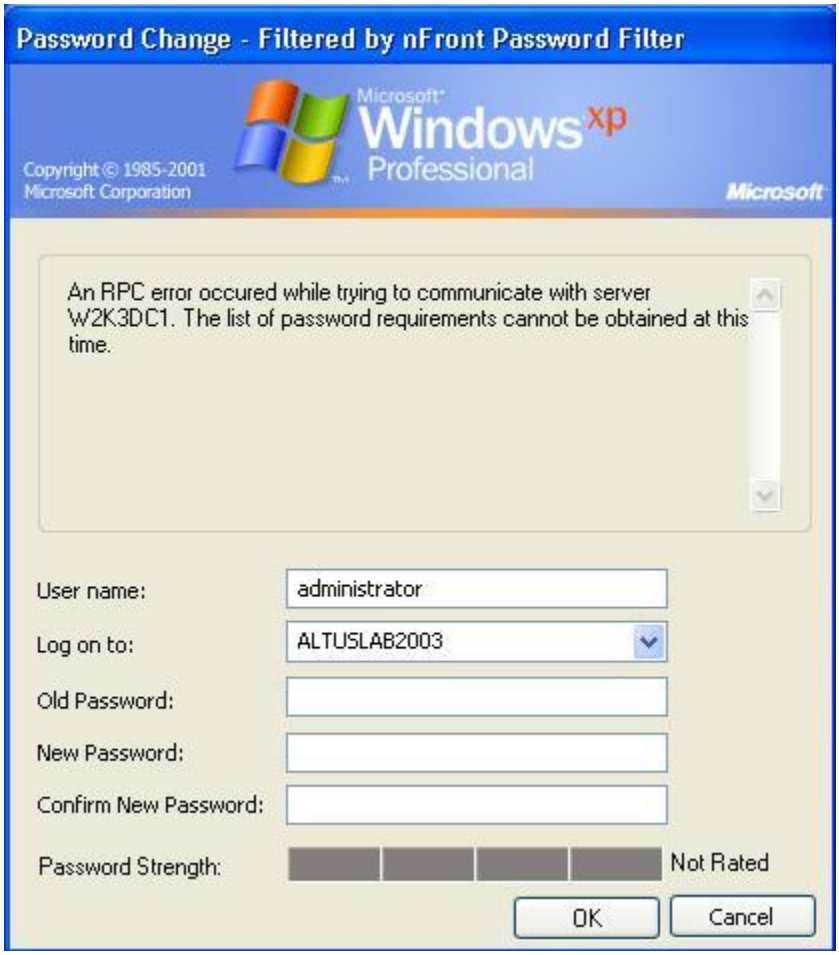


Figure 9.4.7: DC Unavailable or nFront Password Filter Password Policy Service not running

If the end-user receives the message in Figure 9.4.7 and continues to change his or her password, he or she may receive the error message in 9.4.8 (if the RPC server is still unavailable). After clicking OK, the password change is sent to the standard OS password change process and the end-user will get the standard Windows Password Change error message (Figure 9.4.8) if the password was rejected. These errors do not mean that nFront Password Filter is not working. They only mean that the client cannot communicate with the nFront Password Filter Password Policy Service and thus cannot verify password rules or compliance.

Figure 9.4.8: DC Password Change message if the client cannot communicate with the nFront Password Filter Password Policy Service on the DC.

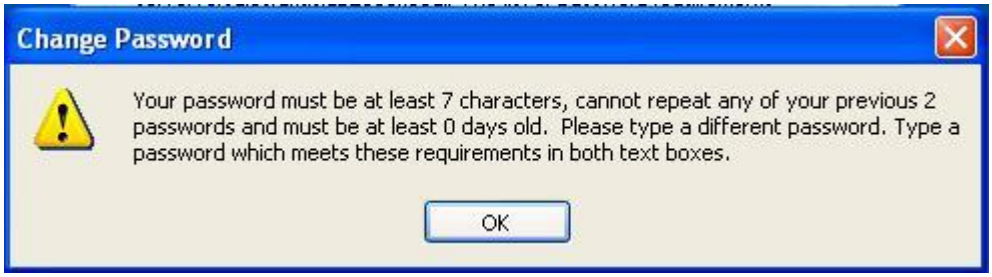


Figure 9.4.9: Standard Windows XP password change error message.

Symptom	Proposed Troubleshooting
The nFront Password Filter Client displays the correct rules but allows non-compliant passwords	The RPC service on the server does not check nFront Password Filter to ensure it is properly registered or licensed. Most likely there is an error in the registration code, an expired evaluation version, or a licensing issue where the number of DCs exceeds the registered qty. Registration Code may be wrong / mistyped. Turn on debugging. Change the password for a test account and look at the debug file (usually c:\winnt\system32\nfront-password-filter-debug.txt). If you are evaluating and evaluation = 0, your evaluation registration code is wrong or expired. Annual Maintenance Code may be wrong / mistyped. Turn on debugging. Change the password for a test account and look at the debug file. If the maintenance code is mistyped or expired there will be an obvious message in the debug file. Evaluation copy may have expired. Turn on debugging. Change the password for a test account and look at the debug file. If the evaluation product has expired it will be obvious in the debug file. The file will have a message in capital letters stating the product has expired.
nFront Password Filter Client displays an empty set of rules	**There is most likely a GPO replication issue with the nFront Password Filter GPO linked to the Domain Controllers OU.** Check the registry for any nFront Password Filter configuration parameters. Look in HKLM\Software\Policies\Altus for any PassfiltPro keys. If none are found you have a GPO replication issue. See Microsoft's support site for help troubleshooting GPO replication

	problems.
The nFront Password Filter Client is installed but I get the standard Password Change Dialog.	**The system32\pproclient.dll file is missing or the disable registry key is set to 1.** Check for the pproclient.dll file. Check HKLM\Software\Policies\Altus\PassfiltProClient\disable and set equal to zero. **The GinaDLL registry key may have been deleted manually or by malware.** Check HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL, REG_SZ, altusgina.dll. If they value is not present the altusgina.dll file will not be loaded. Check Control Panel + Add / Remove programs to see if the nFront Password Filter Client has been installed. Check %systemroot%\system32 for altusgina.dll. If the file is missing, the nFront Password Filter Client should be uninstalled and reinstalled.

9.5 Uninstalling

Control Panel + Add / Remove Programs + nFront Password Filter Client + Remove. A reboot will be needed to completely remove the software. Otherwise, the operating system maintains an exclusive lock on altusgina.dll and will continue to use the altusgina.dll until the next boot.

If you deployed via a software GPO the software should uninstall if you move the computer to a different OU or if you delete the GPO.

10.0 Purchase Information

Please visit http://www.nFrontSecurity.com for purchasing information.

11.0 Support / Contact Information

Please visit http://www. nFrontSecurity.com for the latest support and contact information or send email to support@nFrontSecurity.com.

Appendix A - nFront Password Filter Settings Matrix

Policy Name:	On / Off	Value
Minimum Password Length (in characters):		
Maximum Password Length (in characters):		
Reject passwords that don't contain at least <value> of the following character types:		
Check for numeric characters in password.		
Minimum Numeric Characters Required:		
Maximum Numeric Characters Allowed:		
Check for upper case characters in password.		
Minimum Upper Case Characters Required:		
Maximum Upper Case Characters Allowed:		
Check for lower case characters in password.		
Minimum Lower Case Characters Required:		
Maximum Lower Case Characters Allowed:		
Check for alpha characters in password.		
Minimum Alpha Characters Required		
Maximum Alpha Characters Allowed:		
Check for non-alphanumeric characters in password		
Minimum Non-Alphanumeric Characters Required		
Maximum Non-Alphanumeric Characters Allowed:		
Restrict special character set		
Allowed special characters		
Reject passwords that contain vowels (a,e,i,o,u,y)		
Reject passwords that contain 2 consecutive identical characters		
Reject passwords that begin with a number.		
Reject passwords that end with a number.		
Reject passwords that begin with a special character.		
Reject passwords that end with a special character.		
Passwords must contain a numeric character in position <value>.		
Passwords must contain a special character in position <value>.		
Password must contain special character before character number <value>.		
Reject passwords that contain the username.		
Reject passwords that contain any part of the user's full name.		
Enable dictionary substring search		
Include Groups		
Exclude Groups		

NOTES:

Appendix B - nFront Password Filter MPE Policy Design Worksheet

Purpose:

- To visually check if there are any group / OU conflicts with policy application

Important Notes:

- Unless you add excluded global groups the Default Policy applies to everyone.
- You should always think first of "to which groups should I apply this policy?" Then, you must think "are there any users who are a member of those groups who should not get this policy?" If the answer to the later question is none you do not need to exclude any groups. If the answer is "there are 5 people who are managers who should not get the policy," then create a group for those 5 people and exclude that group from the policy.
- If you only want to apply password filtering to a few small groups enable the Default Policy and Policy 1. Leave the default configuration for the Default Policy (only rejects passwords over 256 characters) and define more restrictive settings for Policy 1. Tie Policy 1 to the appropriate groups for which you wish to filter passwords.

Instructions:

Fill in the table below with your groups in the leftmost column. Then check the policies that apply or are excluded. From there consider the user membership in the groups. Are there any users

Step 1: Fill in the Chart Below

	Policies						
	Default Policy	Policy 1		Policy 2		Policy 3	
Groups / OUs	Excluded	Apply	Exclude	Apply	Exclude	Apply	Exclude
Example Group1	Yes						
Example Group2		Yes					
Example Group3			Yes				
Example Group4				Yes	Yes		
Example Group5						Yes	

* You should not have any groups that look like Example Group 4. If you apply the policy and exclude the policy

** If a user is a member of Example Group 5 and Example Group 2, they will have to select a password that complies with Policy 3, Policy 1 and the Default Policy.

Step 2: Consider User Membership in the above groups

- Are there any users who are a member of more than one group listed above?
- Will they be affected by more than one policy?
- Do the policies make it impossible for that user to choose a reasonable password?

Appendix C - nFront Password Filter Failure Codes

Failure Code	Failure Reason
1	- Password has less than the minimum number of required characters.
2	- Password exceeded maximum number of characters.
4	- Password has less than the minimum number of required character types.
8	- Password does not meet requirement for numeric characters.
16	- Password does not meet requirement for upper case characters.
32	- Password does not meet requirement for lower case characters.
64	- Password does not meet requirement for alpha characters.
1048576	- Password does not meet requirement for non-alpha characters.
128	- Password does not meet requirement for non-alphanumeric characters.
262144	- Password contains special characters that are not allowed.
131072	- Password contains one or more vowels.
524288	- Password does not meet requirement for space characters.
256	- Password contains 2 or more consecutive identical characters.
2097152	- Password contains 3 or more consecutive identical characters.
33554432	- Password contains non-ascii characters with code outside of 33 through 126.
512	- Password begins with a number.
1024	- Password ends with a number.
4194304	- Password begins with a special character.
8388608	- Password ends with a special character.
2048	- Password does not contain a number in the correct position.
4096	- Password does not contain a special character in the correct position.
8192	- Password contains the username.
16384	- Password contains a part of the user's full name.
65536	- Password contains the following common word:
16777216	- Password does not contain a special character within the first X characters specified by your administrator.

The failure codes are processed based binary bits. To decode a failure code of 10 you would need to find the largest number in the table above which you can subtract from 10 without yielding a negative result. With a failure code of 10, you can subtract 8 leaving a result of 2. You go through the process again using the result of 2. A failure code of 10 is really 8 plus 2 so the reasons for failure correspond to those for 8 and 2. Here is the example in a different way:

```
10
-8      - Password does not meet requirement for numeric characters.
-2      - Password exceeded maximum number of characters.
--
0
```

Appendix D – Detailed Version History

What is new in Version 6.0.x?

- Support for Stanford password policy via filter and client messaging. In April 2014 Stanford University adopted a length-based password policy and many companies have opted for the same policy. The policy varies the character type requirements based on the length of the password. You can find more information here - https://itservices.stanford.edu/service/accounts/passwords/quickguide.
- Adds support for Unicode dictionary. Also continues to read ANSI encoded dictionary files.
- Adds ability to log administrative password resets.
- ADM now has maximum character limit set to 256 instead of 256. The GUI supports a max of 256 characters but some systems that do automated password changes like Exchange 2013 change to a 128 character password.
- Option to skip password filtering for passwords longer than XX characters and option to log the users who are skipped. This is needed in some cases with Exchange 2013 which automates password changes using a 128 character password change that may fail depending on the policy settings.
- ADM templates now have a maximum password warning interval of 999 days (instead of 60 days). This makes it easier to test in a lab environment.
- ADM template set to max service interval of 168 hours (7 days) instead of 120 hours.
- Dictionary supports character substitution. All combinations of the following character substitutions are checked: `a=@, s=$, e=3, i=1, l=1, o=0.`
- Support for interpreting the '*' character in the dictionary as a wildcard.
- Bugfixes related to the client on Windows 8 and 8.1 were fixed.
- Client is updated to support notification of password expiration at logon for Windows 7, Windows 8 and Windows 8.1.
- Client improved to pre-check password during the password change instead of submitting the change and trapping any subsequent error.
- Logging files for failures, password resets and skipped users configured to use double quotes and comma separator for easy import into Excel or other CSV parsing programs.
- We removed the rule to look for passwords that exactly match a dictionary word.
- Password strength meter has been modified to do additional checks and display "weak" for passwords that contain a few common password sequences (e.g. "password", "letmein", "qwerty", etc.) and passwords that contain consecutive repeating characters.
- Default logging of rejected passwords was removed. (v.6.0.2).
- Defaults to skip all password changes that are 100 characters or more to avoid issue with automated password changes by Microsoft Exchange and other applications. (v.6.0.2)
- Bugfix for German language phrases (v.6.0.2)
- Bugfix for "reportOnly" mode with nFront Password Expiration service. (v.6.0.3). The prior version remained in report only mode when flag was cleared.
- Feature added to turn debugging file into a continuous log by setting HKLM\Software\Policies\Altus\PassfiltProMPE\runningLogs, REG_DWORD (32-bit), value=1. (v.6.0.3).

- Support for SAP password requirements added. Passwords cannot start with an exclamation or a question mark. Passwords cannot start with the same 3 consecutive characters.

What is new in Version 5.6.x?

- Added support to extend the assignment of maintenance codes.
- A bugfix was implemented to fix an issue with slow password changes on Windows 2012 servers.

What is new in Version 5.4.x?

- A Compliance section was added to the policy settings to allow one checkbox implementation of NERC CIP password compliance and PCI password compliance.
- A bugfix was implemented related to the "allowed special characters" settings. Prior versions incremented the failure code for each disallowed character which resulted in an incorrect failure message. The filter correctly filtered the password each time but the failure message was incorrect.
- The custom email message now supports variables that allow you to substitute in the username, first name, last name, and include the days until the password expires.

What is new in Version 5.3.x?

- The Windows 7 client has been modified to support the presentation of policy requirements for local logon when the NPF-DE or NPF-SPEMS or NPF-MPEMS version is installed locally. If there is no local installation of NPF the client will disable itself if the logon is local. It will continue to work fine for domain logons.
- Windows 2008 R2 now works correctly with Windows 7 (x86 and x64) clients and the option to allow administrative resets to bypass the nFront requirements. If a password change is sourced from Windows 7 the Windows 2008 R2 system uses a very large number for the Boolean value for SetOperation. The value should be a 1 for administrative resets and a 0 otherwise. We have contacted Microsoft regarding this issue. However, our programming modification now correctly handles the cases.
- The limit of allowed special characters specified was increased from 12 to 32.
- Additional debugging options were added for the nFront Password Expiration Service.
- Windows 7 client and nFront Password Policy service modified to handle Canadian French correctly.
- Issue with check for 3 consecutive characters at beginning of password resolved.
- Issue with password change at logon when RPC server unavailable solved.

What is new in Version 5.2.x?

- The Windows 7 client has been modified to include an option to filter other credential providers. This eliminates multiple tiles at logon and unlock which sometimes appear if you run other credential providers.
- The feature to check for 2 or more and 3 or more consecutive identical characters was modified to treat upper and lowercase characters as identical. In other words 'a' and 'A' are treated as identical and a password of 'Aardvark' would be considered to have 2 or more consecutive identical characters.

What is new in Version 5.1.x?

- The filter has been modified to ignore the krbtgt account (See Microsoft KB article 2549833).
- nFront Password Filter client was modified to correct an issue with Citrix VDA interoperability. Citrix logs the user in using a UPN and the UPN was not correctly handled by the nFront Client. This issue only affected Windows XP workstations with Citrix VDA.
- Some component debug settings and logfiles were modified to better assist with troubleshooting client interaction.
- Multiple language support was added for the Password Strength Meter. It now displays in English, German, French, Italian and Spanish. A client side language DLL was added and future languages may be added by simply deploying a new language DLL.

The Windows 7 client was modified to allow filtering of all other credential providers (instead of filtering only the Microsoft credential provider). This may be needed if you run other credential providers that present the user with multiple "tiles" on the logon interface. It is only an issue if you run additional credential providers.

What is new in Version 5.0.x?

- Version 5.0 introduces multiple policy support for member servers.
- The license check thread was modified to reduce performance impact on Windows 2008 servers.
- nFront Password Filter can now block the usage of "similar" passwords. Passwords that match more than XX characters of a prior password can be rejected. Passwords that do not contain a minimum number of different characters may also be rejected.
- nFront Password Filter can reject passwords with more than 3 characters from the same character set.
- The nFront Group Filter service was modified to exclude computer accounts when targeting an OU. This had no effect on the operation of nFront Password Filter but resulted in extraneous items on the report generated by the nFront Password Expiration Service.
- The nFront Password Filter and nFront Password Expiration service are packaged with a new installer. The result is a better installation system that makes upgrades easier. It also blocks the installation of the 32-bit version on x64 servers.

What is new in Version 4.16.x

- A timer used to start the nFront Group Filter Server was modified
- Uninstall of client was corrected to remove only the GinaDLL value under the winlogon key.
- Version 4.15.2 introduced a bug that resulted in processing of the Default Policy on systems where the Default Policy was not enabled in the GPO. This has been corrected such that only policies enabled in the GPO are processed.
- System now correctly filters passwords when configured to read dictionary from netlogon share. Version 4.15.1 introduced a bug that resulted in bypassing the filter when configured to use the dictionary file from the netlogon share.

What is new in Version 4.15.x

- A timer used to start the nFront Password Expiration Service was modified. The old timer had a 32-bit resolution and would cycle through zero every 49 days and could result in a missed run of the services.
- The client setup program has been modified to detect the installation of other Gina based systems on Windows XP clients, Citrix servers, etc. In release 4.14 the client did not correctly handle the presence of another Gina and it resulted in the overwrite of the GinaDLL value.

What is new in Version 4.14.x

- Greatly enhanced performance of the nFront Group Filter service on large networks.
- New rule to reject a new password that matches an old password by more than X characters. This feature only works if the password change is made using the nFront Password Filter Client or nFront Web Password Change.
- A fix was implemented to correct the use of the “Domain Users” group. Prior versions incorrectly identified any group with “domain users” in the name as the actual Domain Users group and applied policies to all domain users instead of the group with the phrase in the name.
- A fix was implemented to correctly support the rule for specific special characters that are allowed. Prior versions exhibited intermittent failures in policy processing when the rule was applied.
- Support for Windows 7 / Vista client (32-bit and 64-bit).

What is new in Version 4.13.x

- Client can now notify users at logon if their password will expire in XX days based on the maximum password age within nFront policies.
- Client now supports Spanish.
- Client has been improved to accommodate gina chaining to other GINA DLLs on Windows XP. Fault tolerance has been built in to avoid problems with other GINA DLL files.
- Client can be pointed to a specific DC for password expiration warnings, password rules and password failure messages.
- You can now set a maximum password age on the Default Password Policy and notify users via email.
- nFront Password Expiration Service has been fixed to work correctly on Windows 2008 R2.
- nFront Password Expiration Service has been optimized to process policies with lower max password age first and to notify users only once if they appear on multiple policies. The most restrictive max password age applies.
- All service files have been modified to allow for command-line install and uninstall.
- More features were added to support a forthcoming monitoring utility.

What is new in Version 4.12

- Some RPC functions added in the 4.11 password policy service and client had to be removed for backwards compatibility with older client releases.

What is new in Version 4.11

- This version corrects an issue with version 4.10 with regard to the use of Domain Users. There was a problem properly handling exclusions when Domain Users were applied to a policy.
- Some features were added to support a forthcoming monitoring utility.
- The new version features an x64 password expiration service.
- The password expiration service was modified such that you can now use email features even if your policy age settings match your domain password expiration settings.
- The group filtering service has been modified to more efficiently handle large groups.

What is new in Version 4.10

- This version corrects an issue with version 4.9 and Windows 2003. On reboot of 2003 the group filter service in 4.9 would be stopped by the OS and log an error. The service now works fine on the reboot of all versions of Windows.
- The client has been simplified into one DLL instead of two.
- The filtering engine has been modified to more efficiently handle the inclusion and exclusion of “Domain Users” on large networks (with over 20,000 user accounts).
- The group filtering service has been modified to more efficiently handle large groups.

What is new in Version 4.9

- Policy engine updated to create system32\Logfiles directory on machines without the directory. In prior versions this caused an error if debugging was turned on and the LogFiles directory was not present.
- x64 nFront Password Policy service has been corrected to send the correct rules and failure message to a client.
- Group Filter service corrected. Group Filter in version 4.8 did group enumeration based on “cn” and not “samAccountName” so it worked only if the user has no full name defined.

What is new in Version 4.8

- Policies can now be applied or excluded to nested groups. Consider a group called NorthAmericaHR and that contains a NYHR and LAHR group. If you apply an nFront Password Filter policy to NorthAmericaHR it will apply to members of all groups.
- Policies now support Domain Local Groups (Global and Universal groups have always been supported)
- Policies can now be linked to OU paths. Simply specify “OU=NY,OU=NA” in the policy and all users who are a member of the NY OU will have the policy applied.

What is new in Version 4.7

- Policies can now be applied or excluded from users with non-expiring passwords.
- Password Expiration Service was improved to handle a custom message of up to 1024 characters.
- Debug file no longer contains clear text password.
- ADM template corrected to fix GUI issue.

What is new in Version 4.6

- Enhanced email reporting for user with password expired or upcoming expirations. Report now shows the current password age, the maximum password age, etc.

- Password Expiration service skips accounts that are disabled.
- Password Expiration service has option to limit email warnings to end-user to once per day.
- Password Filter settings now allow more control of the use of space characters in password. The new settings can help encourage the use of passphrases.

What is new in Version 4.5

- nFront Password Expiration supports emails to end users and administrative reporting via email.

What is new in Version 4.4

- Client modified to correct button alignment problems with Windows XP Classic interface
- nFront Password Policy service modified to allow processing of carriage returns when using a custom message to the nFront Password Filter client.
- nFront Password Expiration Service was correct to properly handle maximum password age settings beyond 150 days.

What is new in Version 4.3

- Product name changed to nFront Password Filter.

What is new in Version 4.2

- Added support for different dialects of German and Italian.
- Bugfix for client. Any non-US English system was defaulting to displaying rules in Italian. The fix only requires the replacement of the server files on the domain controller. So an uninstall and re-install of the package for the domain controller with correct the problem if you downloaded 4.1. The new version should have PProPolicySvc.exe version 3.54 installed.

What is new in Version 4.1

- Added display of client password rules in German and Italian.

What is new in Version 3.56

- Added ability to set different password aging policies for different groups of users.

What is new in Version 3.55

- Bugfix related to SQL 2005 and the NetValidatePasswordPolicy() API call. Bugfix applies to nFront Password Filter member server version.

What is new in Version 3.54

- Filtering engine updated with new feature to ensure a numeric character between alpha characters.
- Client updated to fix issue with inconsistent failure message. Previous clients responded differently depending on whether a user pressed Enter or clicked the OK button.
- Debug file for filtering engine updated. Previous debug files may have printed information in addition to the user's full name.

What is new in Version 3.53

- nFront Password Filter filtering engine was modified to better support the nFront Password Filter client.
- nFront Password Filter client was improved. The client now passes control to the MSGINA for handling the actual password change. Previously the password change was handled by the client and the real MSGINA could not corrected keep track of state information. This led to problems when changing a password at first logon and could lead to potential problems updating network providers on the client. The new nFront Password Filter client now takes the least invasive approach while still informing the end-user of password rules and failure to comply with nFront Password Filter policies.

What is new in Version 3.52

- nFront Password Filter by default maintains a running text file which records all rejected passwords. This feature can be turned off but must be explicitly turned off via the nFront Password Filter group policy settings. Logging rejected passwords is a requirement of Sarbanes Oxley and was specifically intended to support customers who must maintain SOX compliance.
- nFront Password Filter now includes an optional client. The client can retrieve password policy rules from any DC. If the user attempts a password change that does not comply with the rules the client will provide detailed reasons for failure, include the dictionary word contained within the password if you performing dictionary checking.

What is new in Version 3.5

- nFront Password Filter now has an architecture which will allow upgrades, cross-grades and bug-fixes without the need to reboot. This is all due to a new dynamic password filtering engine which is dynamically replaceable.
- All versions now share the exact same code base. In previous releases there have been slight differences among the versions due to features added to one version and not the other. Now, all versions use the exact same source code, even the 64-bit versions.
- nFront Password Filter MPE now supports 5 policies in addition to the default policy. Previous versions only supported 3 additional policies.
- Improved architecture of dictionary placed in netlogon share.
- Administrators can now configure nFront Password Filter to bypass password filtering on administrative resets. Thus, administrators can reset passwords to ones which may not meet your password policy. This is helpful to companies that have password reset conventions which do not comply with the new password policy. As long as users are forced to change their password at first logon the security risk exposure should be minimal. Users will, of course, have to select a password that complies with the new policy upon the forced password reset at logon.
- The debug file now has a timestamp and displays the dictionary word found if the password failed due to a dictionary check.
- A great option for passphrase support. Dictionary checking can be skipped if password is longer than a specific number of characters. Suppose you configure nFront Password Filter to skip dictionary checking for passwords greater than 15 characters. In such case a password like “Egg1976” would get rejected due to the word “egg” in the dictionary. However, the passphrase “I like POACHED eggs” would not be checked against the dictionary and would be acceptable assuming it meets your other password requirements.

- Dictionary checking has been optimized to check the dictionary only once (even if multiple password policies with dictionary checking apply to the end-user) and only if all other password criteria are met. In other words, nFront Password Filter does not waste time checking the dictionary if the end-user has not met all other policy requirements.
- nFront Password Filter can check for special characters within the first X characters of a password.
- nFront Password Filter now reports some basic status information back to the local registry. This can be disabled via the GPO for more efficient password filtering. We will be introducing a tool to offer reporting on the software installation, versioning, etc.
- nFront Password Filter can maintain statistics on the number of passwords changed or filtered on each DC. Again, a reporting tool will be released to query this information across multiple DCs.