nFront Password Filter

Multi-policy Edition
Single Policy Edition for Domain Controllers
Single Policy Edition for Member Servers
Desktop Edition

with Client Support

Version 4.12.0

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 is essentially a plug-in for the Windows operating system that gives you the ability to define and enforce one or more very granular password policies. The policy settings go beyond those provided with the standard operating system release and therefore allow you to increase your network security.

Prior to August 2007 nFront Password Filter was sold as Passfilt Pro. Passfilt Pro was initially released in June 2003.

1.1 Versions

- ***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.

- ***nFront Password Filter Single Policy Edition for Member Servers.*** SPE for Member Servers allows you to filter the passwords of local accounts on member servers. 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 member server or via a local GPO.

- ***nFront Password Filter Desktop Edition.*** This version filters the passwords of local accounts on Windows 2000 and Windows XP 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.

- ***Client Support.*** You can optionally deploy a nFront Password Filter Client to your Windows 2000 Pro and Windows XP 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.

1.2 What's New

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.

1.3 Notes to Evaluators

- You need a Windows 2000 or Windows 2003 domain controller to test nFront Password Filter MPE. A member server or workstation will only allow you to test the Default Password Filter Configuration (i.e. a single policy with no exclusions).
- 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 1-800-676-1513 or 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 10,000 user accounts:

```
For /L %i IN (1,1,10000) DO net user test%1 valid_password /add
```

Command line syntax to change a password:

```
net user test1 abc
```

You may wish to create a batch file and desktop shortcut to it for updating the group policies in Windows 2000. Simply put the secedit syntax into a .bat or .cmd file.

```
secedit /refreshpolicy machine_policy
```

- 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 9.0.

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.
- 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 12 or less specific special characters
- Reject passwords containing vowels (a,e,i,o,u and y in upper or lower case)
- Reject passwords with consecutive identical characters (e.g. aa, bb, etc.)
- Reject passwords with 3 consecutive identical characters (e.g. aaa, bbb, etc.)
- 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 any portion of the user's full name.
- Reject passwords that contain the username within any portion of the password.
- Check the user's proposed new password against a customizable dictionary.
- Search the dictionary looking for a case-insensitive exact match or a case-insensitive substring match (i.e. dictionary word is found anywhere within the password).
- **Apply the policy to multiple global groups.
- **Exclude multiple global groups from the policy.

** Only applies to MPE version.

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 most unrestrictive policy that will apply to all Domain Users. Certain global groups can be excluded from the policy (like groups for service accounts). Use Policy 1, Policy 2, etc. 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 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 all Windows 2000 and Windows XP 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 X.XX.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 Client X.XX.msi	Optional package for domain workstations.
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 Filter Documentation.pdf	This document.

2.0 Installing nFront Password Filter

IMPORTANT NOTE: If you are testing nFront Password Filter MPE you must load it on a domain controller. The group filtering will not work if the software is installed on a workstation or member server.

2.1 Deployment Recipe

For installations where nFront Password Filter will filter passwords of domain users in the AD, here are the basic deployment steps you will follow to get nFront Password Filter into production.

1. Install nFront Password Filter on each domain controller. Reboot each DC during next scheduled downtime window.
2. (OPTIONAL) If you plan to use the MPE version and want to set different password aging intervals for different groups you must install the nFront Password Filter Password Expiration Service on one or more domain controllers. It is only needed on 1 domain controller but can be loaded on additional domain controllers for fault tolerance. The installation does not require a reboot.
3. Load and configure nFront Password Filter GPO template but do not enter registration code.
4. Make sure all domain controllers have been rebooted and are running nFront Password Filter. You can check this with winmsd.exe + Software Configuration + Loaded Modules and make sure ppro.dll is loaded.
5. On “go live” date, enter the registration code into the nFront Password Filter GPO. Within 5 to 15 minutes the setting will replicate to all DCs and nFront Password Filter will start filtering password changes based on your policy settings.

2.2 Make sure you disable Windows password complexity if enabled

If you nFront Password Filter settings will be less restrictive than the Microsoft complexity rules, you should disable Microsoft’s password filter if you have enabled it. Generally, the Microsoft password complexity is enabled by default on Windows Server 2003 but not on Windows 2000.

1. Start + Programs + Administrative Tools + Domain Security Policy + Security Settings + Account Policies + Password Policy
2. Disable policy for “Passwords must meet complexity requirements” (Figure 2.1.1).

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. You will see the screens displayed in figures 2.3.1 through 2.3.6.

Figure 2.3.1: Installshield Wizard screen 1.

Figure 2.3.2: Installshield Wizard screen 2.

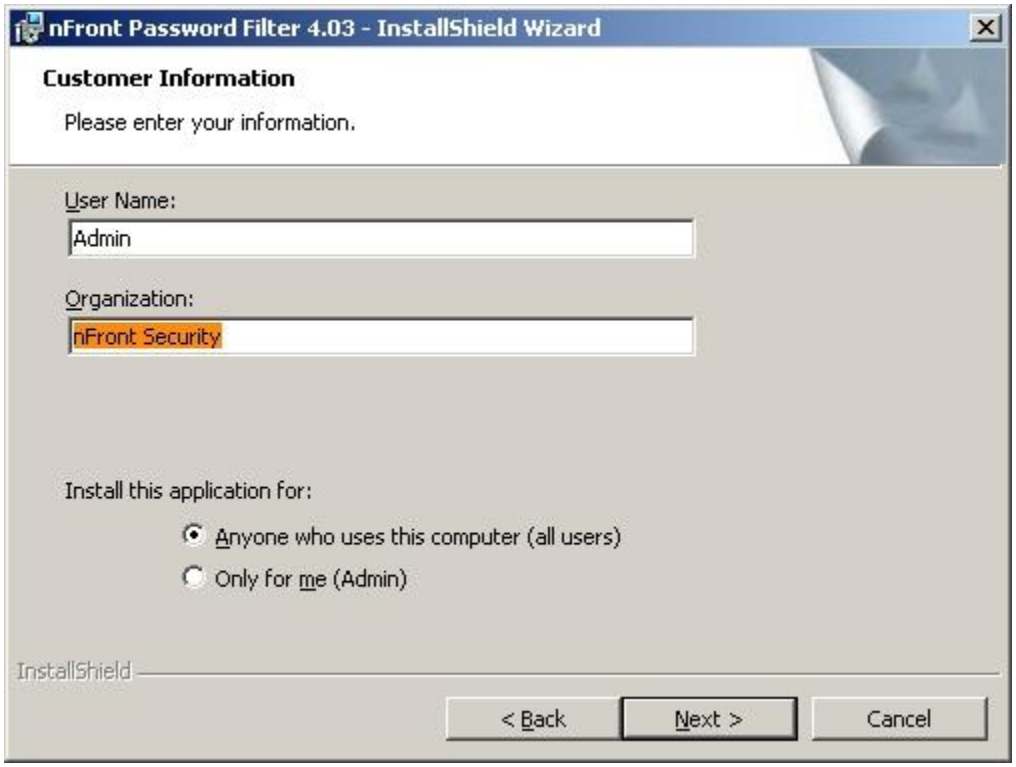

Figure 2.3.3: Installshield Wizard screen 3.

Figure 2.3.4: Installshield Wizard screen 4.

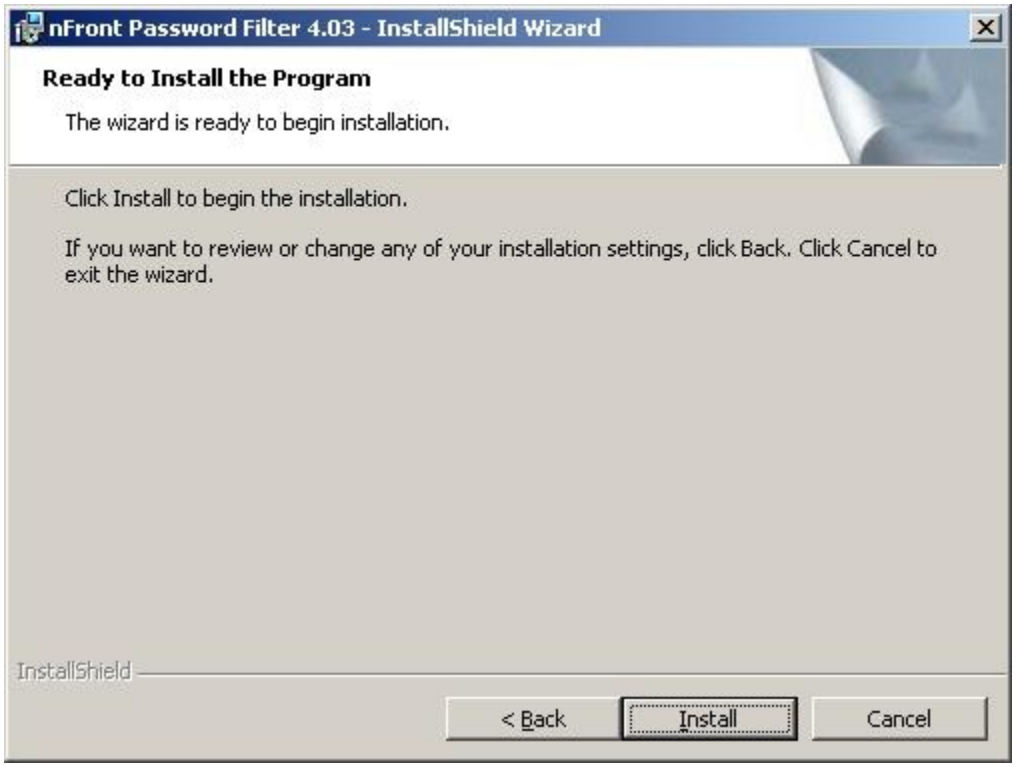

Figure 2.3.5: Installshield Wizard screen 5.

Figure 2.3.6: Installshield Wizard screen 6.

You must restart for the operating system to load the password filter DLLs on boot.

2.4 Load the group policy template

The ADM template provides group policy settings to configure and register nFront Password Filter. **Choose the correct ADM template for the version you wish to test or deploy.** On domain controllers you will load nFront-Password-Filter-MPE or nFront-Password-Filter-SPE. On member servers you will load nFront-Password- Filter-SPE-MS. On Windows 2000 Professional or Windows XP you will load nFront-Password- Filter-DE.adm

The ADM template adds a registry key (HKLM\Software\Policies\Altus\PassfiltProXXX where XXX is the version) on all domain controllers and/or member servers and workstations.

Template	Purpose
nFront-Password-Filter-MPE.adm	Settings for nFront Password Filter Multiple Policy Edition
nFront-Password- Filter-SPE.adm	Settings for nFront Password Filter SPE for Domain Controllers
nFront-Password- Filter-SPE-MS.adm	Settings for nFront Password Filter SPE for Member Servers
nFront-Password- Filter-DE.adm	Settings for nFront Password Filter Desktop Edition

IMPORTANT NOTE: On domain controllers the nFront Password Filter GPO should be created via ADUC in the Domain Controllers container. To distribute nFront Password Filter settings to member servers and workstations, the member server and workstation template may be loaded into a GPO that is deployed against the OU containing the member servers or workstations.

IMPORTANT NOTE: If you wish to test nFront Password Filter and load the ADM file directly without any AD GPO interaction, you can use Start + Run and gpedit.msc + load the ADM template under Computer Configuration + Administrative Templates.

Launch Active Directory Users and Computers (dsa.msc) for your Windows 2000 / 2003 domain. Highlight the **Domain Controllers container** for your domain, right-click and choose Properties. Select the Group Policy tab and click New. Give the new policy a name you will recognize like “nFront Password Filter 3.5.0” (Figure 2.4.1). Edit the policy you just created. This launches the Group Policy Editor. In the Group Policy Editor, drill down to Computer Configuration + Administrative Templates. Right-click Administrative Templates and choose Add/Remove Templates (Figure 2.4.2). The Add/Remove Templates dialog box will appear (Figure 2.4.3).

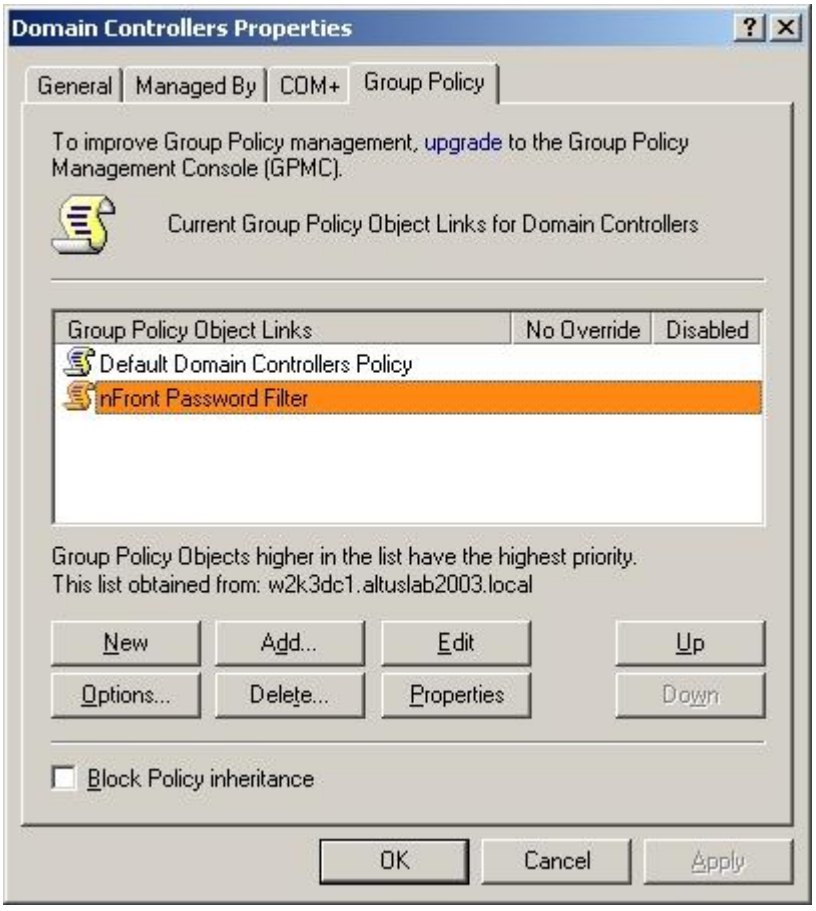

Figure 2.4.1: Creating a new policy for nFront Password Filter.

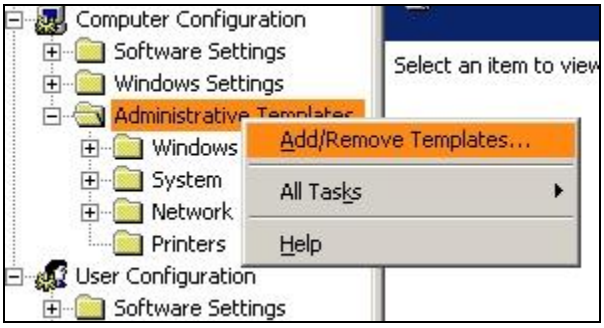

Figure 2.4.2: Add ADM template to nFront Password Filter policy

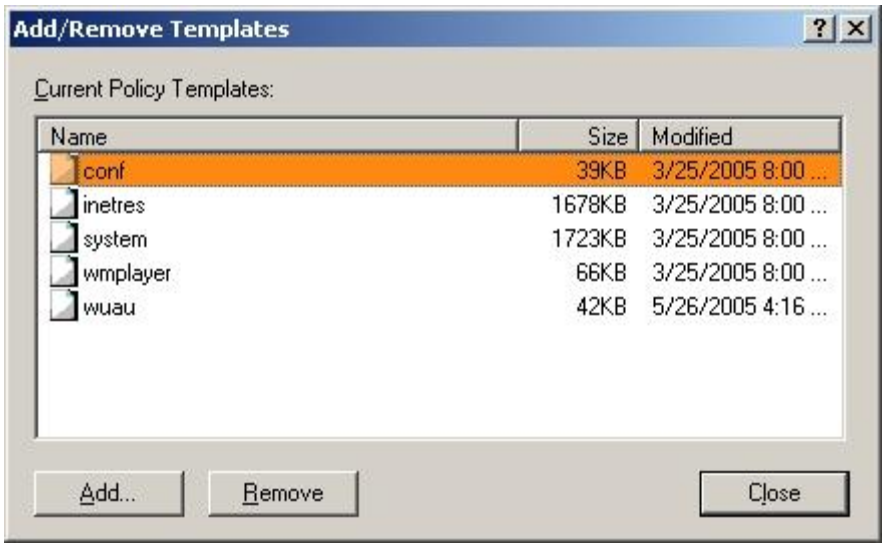

Figure 2.4.3: Add/Remove Templates dialog box

Click on **Add…** to add the nFront-Password-Filter-mpe.adm template. You should see all nFront Password Filter templates in the default c:\windows\inf search folder. However, the templates are also located in the installation directory (default installation directory is C:\Program Files\nFront Password Filter). This example shows the selection of nFront-Password-Filter-mpe.adm (Figure 2.4.4).

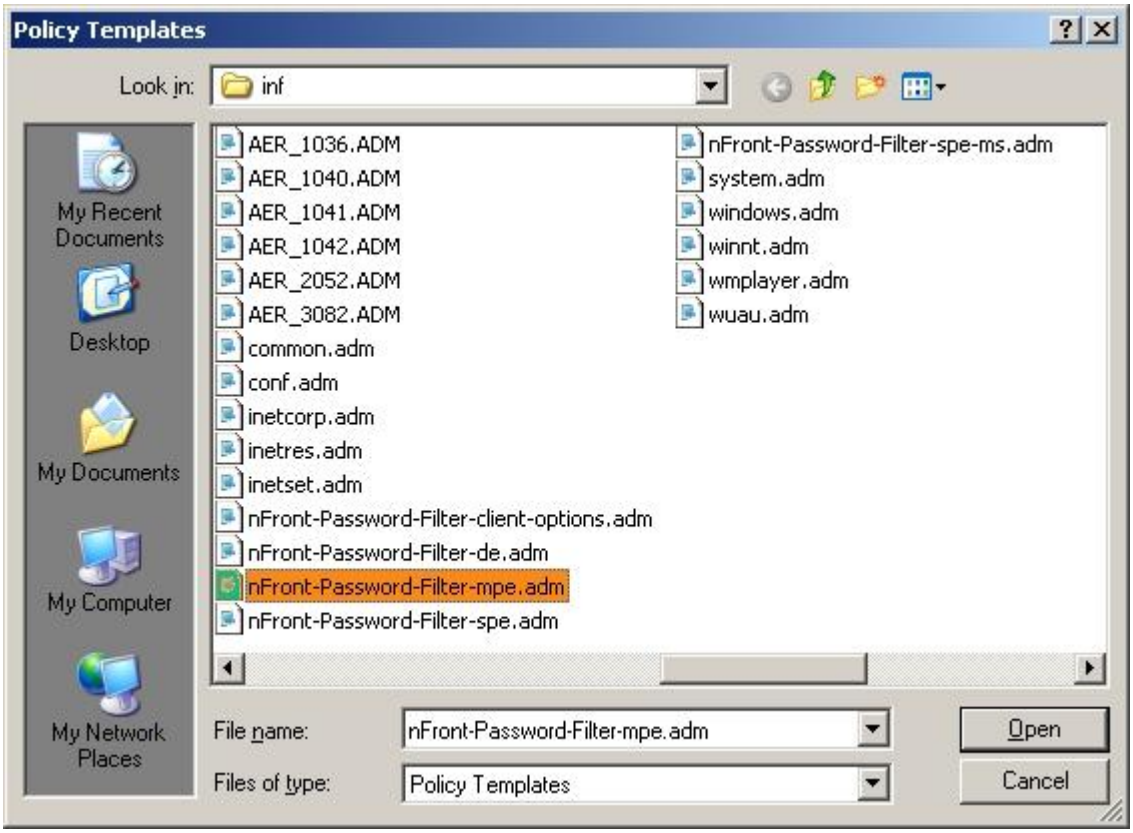

Figure 2.4.4: Add nFront-Password-Filter-mpe.adm template

Click on **Close** to complete the addition of the nFront-Password-Filter-mpe.adm template. You should now see a “nFront Password Filter – Multipolicy Edition” folder under Administrative Templates (Figure 2.4.6). Please note the policy will appear under Classic Administrative Templates in the GPMC Editor in Windows 2008 (Figure 2.4.6b). You can now proceed to the next section to configure nFront Password Filter settings.

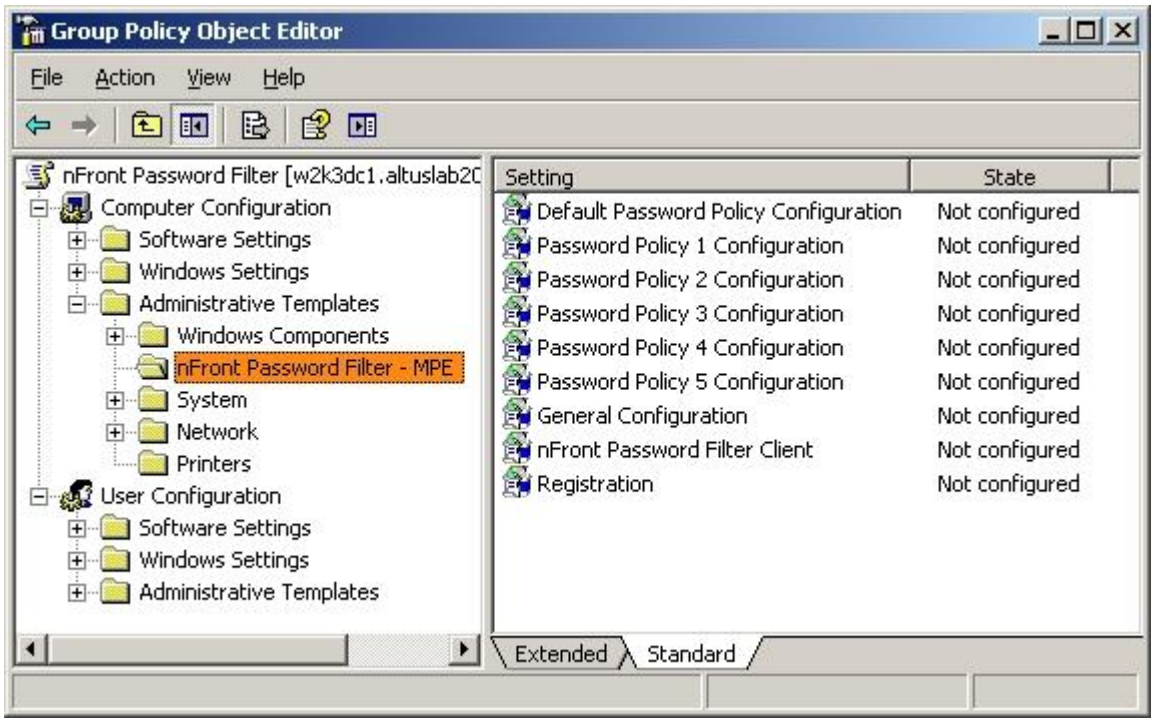

Figure 2.4.6: nFront Password Filter MPE Settings on Windows 2003.

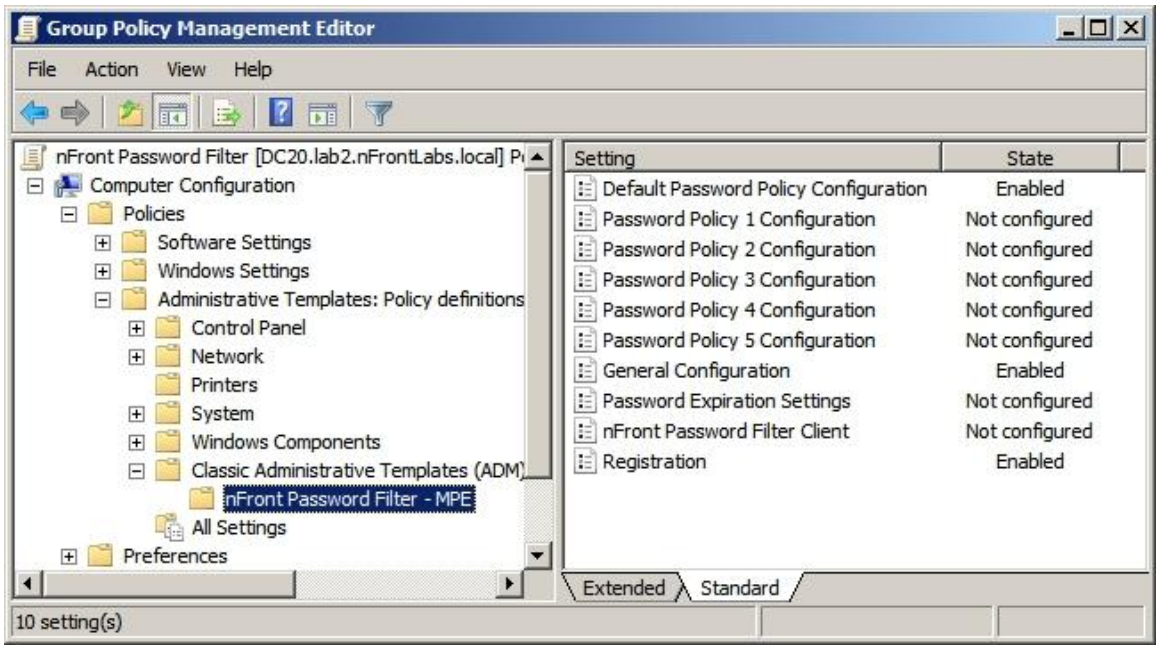

Figure 2.4.6b: nFront Password Filter MPE Settings on Windows 2008

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

2.5 Configure nFront Password Filter settings

See section 3.0 of this document.

2.6 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. However, you can modify nFront Password Filter to read the dictionary from the Netlogon share. If you modify the dictionary in the %systemroot%\sytem32 directory, please copy the modified file to the system32 directory on all domain controllers. 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.

2.7 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:

```
Windows 2000:
secedit /refreshpolicy machine_policy

Windows 2003:
gpupdate /force
```

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

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

This should only be done if you are using nFront Password Filter MPE and plan to set different password aging policies for different groups of users. For example, your domain-level password aging policy may have users change passwords every 90 days. If you wish for Domain Admins or other groups to change their passwords more often you can deploy this service.

We suggest install the "nFront Password Filter Password Expiration Service.MSI" on a single domain controller. The service is not CPU-intensive and by default only runs every two hours. You can control the timing via the nFront Password Filter GPO (General Settings Policy). Setting the service to run once every 24 hours would be fine.

2.8.1 Installation

Here are the steps:

1. Install "nFront Password Filter Password Expiration Service.MSI" on the domain controller. 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.

By default the service runs every two hours. The service reads the password aging parameters configured for nFront Password Filter and applies the aging policies to the user accounts targeted by each password policy. For example, if a user named Fred is part of a group to which Password Policy 1 applies.

2.8.2 Configuration

The GPO created to control nFront Password Filter MPE is also used to control the service. The only two related parameters are: (1) the timer for the service and (2) the maximum password age for each policy. Those settings go into the registry of each DC. The DC running the nFront Password Filter Password Expiration Service will read the registry settings, process password expirations and generate reports of activity. Figure 2.8.2a shows the General Settings of the nFront Password Filter GPO where you can control the interval at which the service runs. By default the service runs every two hours. If you change this parameter you must stop and restart the service to have it read the new interval. Figure 2.8.2b shows the password age

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 60 days or more will be ignored.

IMPORTANT NOTE: Users will not be notified in advance of password expiration. You can view the log files and see a list of users whose passwords will be set to expire in the next 14 days. We do plan to integrate advance notification of password expiration into our nFront Password Filter Client and also add a feature to email users regarding an upcoming password change.

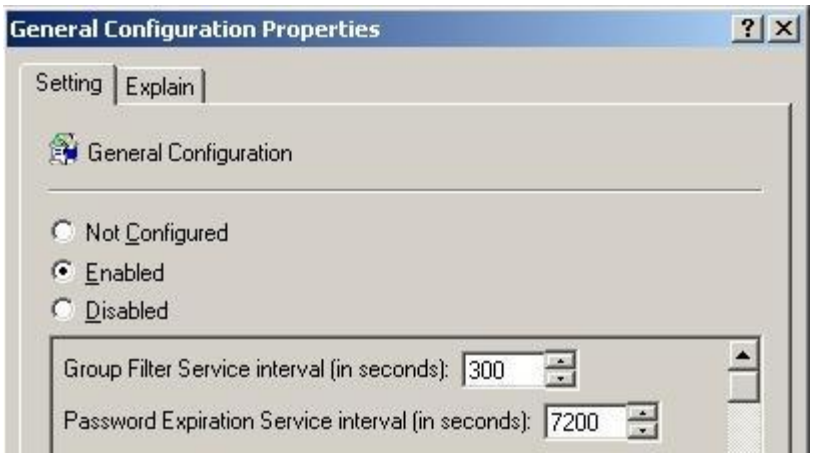

Figure 2.8.2a: Password Expiration Service runs every 2 hours by default

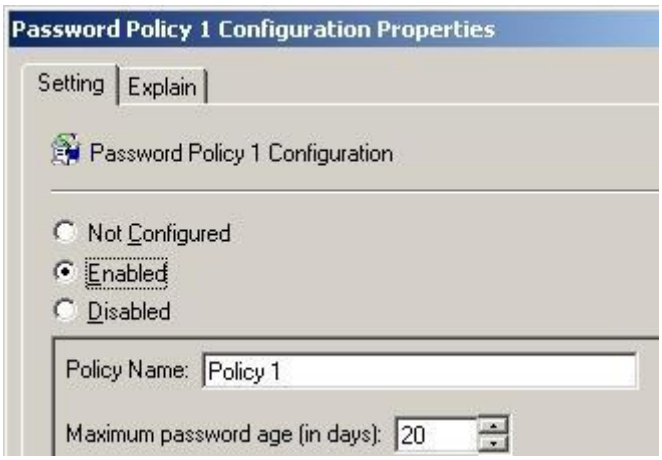

Figure 2.8.2b: Different maximum password ages can be set in Policies 1 through 5.

2.8.3 Reporting

The service generates two reports which are contains in comma-delimited 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. In the future we will provide a utility that will convert these files to HTML reports.

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.

  5/15/2007 15:57:37,test750,46,successful,
  5/15/2007 15:57:37,test751,46,successful,
  5/16/2007 0:17:37,test300,5,successful,
  5/16/2007 0:17:37,test301,5,successful,

- nFront-expiring-soon.log. This file maintains an up-to-date listing of passwords that will expire in the next 14 days.

  Date of Run, Username, Days before expiration
  5/16/2007 9:28:55,administrator,2

```
5/16/2007  9:28:55,jsmith,2
5/16/2007  9:28:55,test302,4
5/16/2007  9:28:55,test303,4
5/16/2007  9:28:55,test51,14
5/16/2007  9:28:55,test52,14
```

3.0 Configuring nFront Password Filter

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

nFront Password Filter MPE is used as an example in this section. Settings for other versions of nFront Password Filter are identical with the exception that they only allow the configuration of a single password policy.

3.1 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

1. Start + Programs + Active Directory Users and Computers
2. Right-click the Domain Controllers OU and select Properties.
3. Select the group policy object where you loaded the nFront-Password-Filter-mpe.adm and click on Edit (from step 2.3). If you only see the Default Domain Controller Policy try that one.
4. In the Group Policy Editor click on Computer Configuration + Administrative Templates + nFront Password Filter – Multipolicy Edition (Figure 3.1.1)

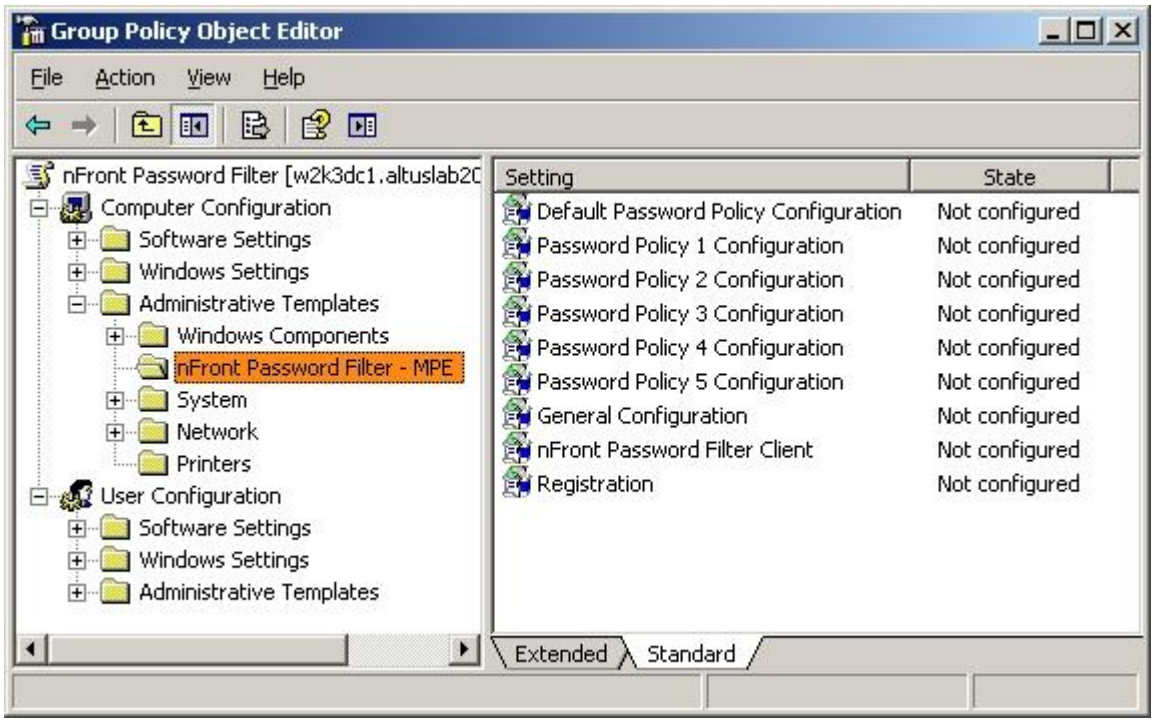

Figure 3.1.1: nFront Password Filter – Multi-Policy Edition Settings.

3.2 Configure Registration policy

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.

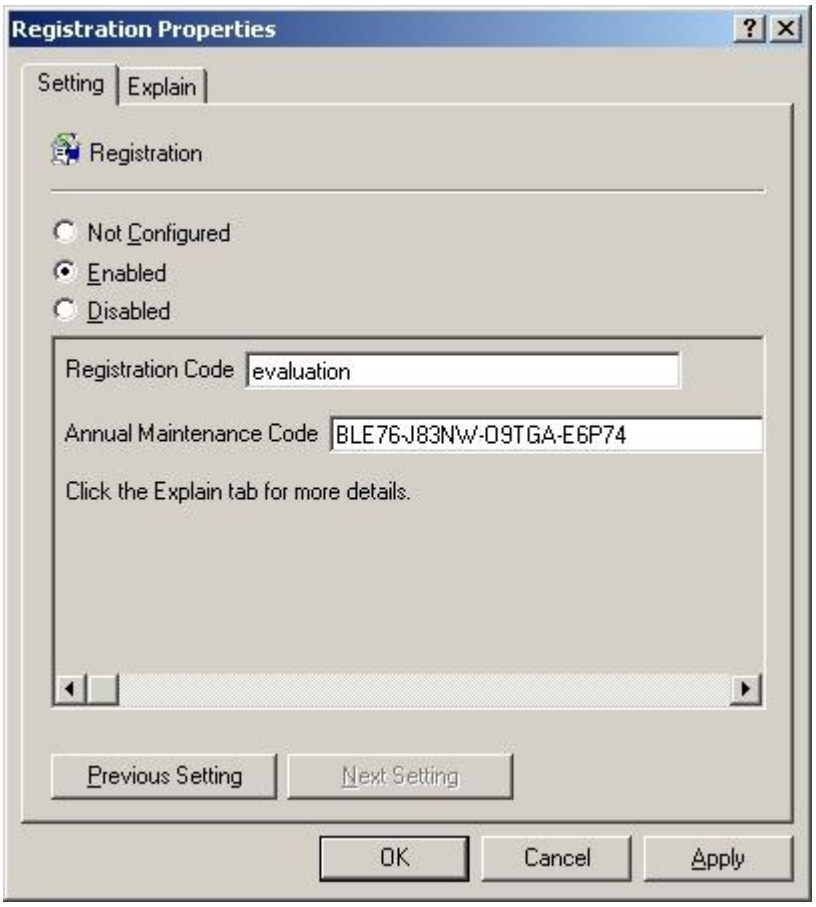

Figure 3.2.1: nFront Password Filter MPE Registration Policy.

3.3 Configure General Configuration policy

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.

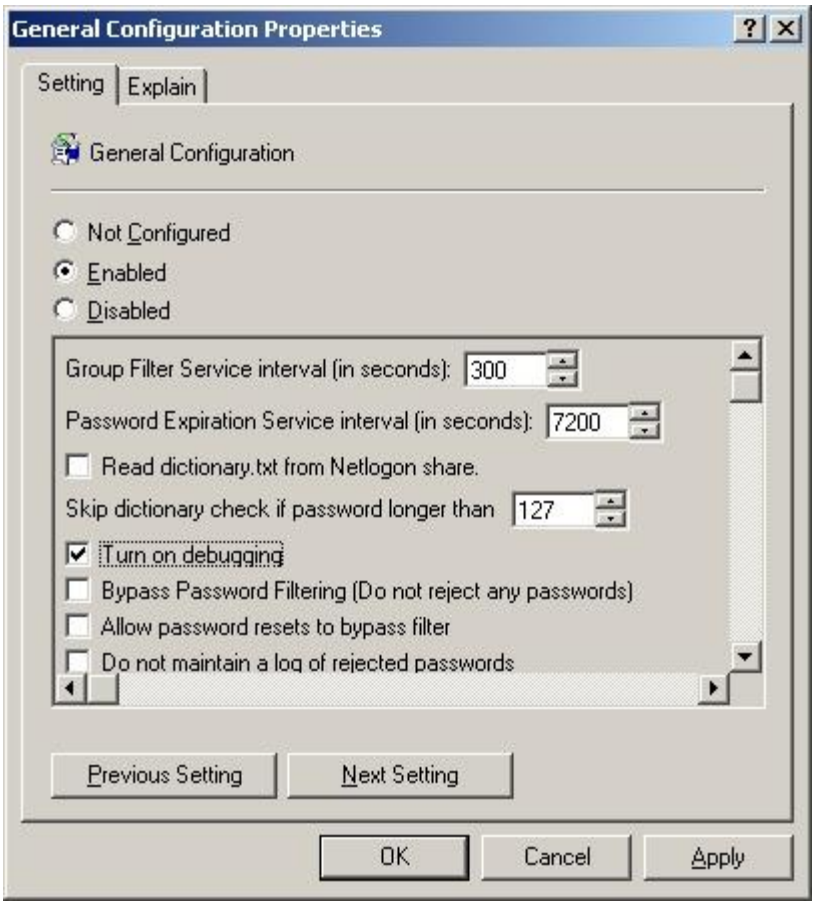

Figure 3.3.1: nFront Password Filter MPE General Configuration Policy.

Policy	Description
nFront Password Filter Group Filter Service update interval	Default Value: 300 seconds This setting controls how often the nFront Password Filter Group Filter Service enumerates the users who are members of global groups that are included or excluded from the policies. There should be no need to adjust this timer on most production networks. In testing it is handy to lower the timer to 30 seconds. TIP: If you modify the timer settings you must stop and restart the nFront Password Filter Group Filter Service on each DC since the service reads this configuration parameter only at startup.
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: 127 nFront Password Filter will skip any dictionary checking and / or substring dictionary checking for passwords greater than the length specified here.
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.
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 127 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.
Do not maintain a log of rejected passwords	Disables running log of failed password changes. The log file is %systemroot%\system32\logfiles nfront-password-filter -password-failures.txt
Do not report status information to the registry	Disables reporting of very basic status information to local registry.
Report statistics to registry	If enabled this setting allows nFront Password Filter to keep a running log of the number of

	passwords changed or filtered.

3.4 Configure Default Password Policy Configuration

Important Notes:

- The Default Password Policy Configuration applies to everyone except the “Excluded Groups”
- Other polices allow you to choose global groups to which the policy applies and global groups which are excluded from the policy.
- The Default Password Policy Configuration is used for all new account creation (since new accounts initially have no group information available for filtering).

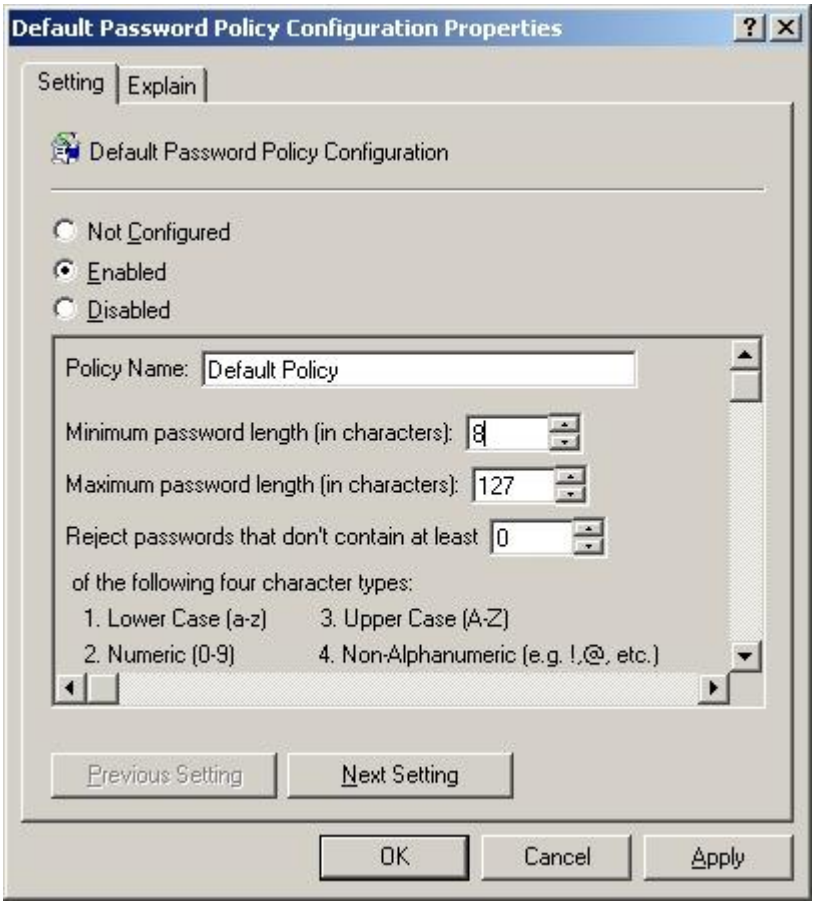

Figure 3.4.1: nFront Password Filter MPE Default Password Configuration Policy.

Policy	Description
Policy Name * This setting only present in MPE version.	Default Value: Default Policy This is the policy name that is reported in the debug output. This setting is arbitrary and 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 and only in policies other than the Default Password Policy.	Valid Values: 0-365 Default Value: 0 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 old than the value set. A setting of 0 means no aging is applied. IMPORTANT NOTE: For this setting to be effective you must install the separate nFront Password Filter Password Expiration Service on at least one domain controller.
Minimum password length (in characters):	Valid Values: 0-127 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: 0-127 Default Value: 127 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 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) Non-Alphanumeric (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 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: 0-127 Default Value: 0 Defines the minimum number of numeric characters that must be present in the password.
Maximum Numeric Characters Allowed:	Valid Values: 0-127 Default Value: 127 Defines the maximum number of numeric 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: 0-127 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: 0-127 Default Value: 127 Defines the maximum number of upper case characters that must be present in the password.
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: 0-127 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: 0-127 Default Value: 127 Defines the maximum number of lower case 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: 0-127 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	Valid Values: 0-127

Required:	Default Value: 127 Defines the maximum number of alpha characters (i.e. upper or lower case) that must be present in the password.
Check for non-alphanumeric 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 Non-Alphanumeric Characters Required:	Valid Values: 0-127 Default Value: 0 Defines the minimum number of non-alphanumeric characters that must be present in the password.
Maximum Non-Alphanumeric Characters Required:	Valid Values: 0-127 Default Value: 127 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: 0-127 Default Value: 0 Defines the minimum number of space characters that must be present in the password.
Maximum Spaces Required:	Valid Values: 0-127 Default Value: 127 Defines the maximum number of space characters that must be present in the password.
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.
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: 0-127 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: 0-127 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; 0-127 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.
Enable dictionary password checking.	Valid Values: 0 or 1 Default Value: 0 (not checked) This policy tells nFront Password Filter to check the password against a "dictionary.txt" file. A 27,000 word dictionary.txt file is copied to the %systemroot%\system32 directory during installation. By default nFront Password Filter looks in the system32 working directory. However, it can be configured (under Global Configuration) to look for the dictionary.txt file in the local Netlogon share. If it finds a case-insensitive exact match to any entries contained in "dictionary.txt" the proposed password change is rejected. TIP: Most customers find the substring search to be the best because it looks for the dictionary word anywhere within the password.
Enable dictionary substring search	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.
Global Groups EXCLUDED from this	Valid Values: global group names

policy:	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). NOTE: The Default Password Filter Configuration Policy only contains the exclusion capability. Other policies allow you to apply the policy to global groups and exclude the policy from others. IMPORTANT NOTE: The idea is to use the Default Password Filter Configuration 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.
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 any account with the "Password Never Expires" flag set.

3.5 Configure Other Policies as needed

All other policies (Figure 3.5.1) have the same exact settings as the Default Password Filter Configuration policy. However, other policies include three additional settings:

1. Maximum Password Age
2. Email Notification of Password Expiration
3. Global Groups to which this policy applies.

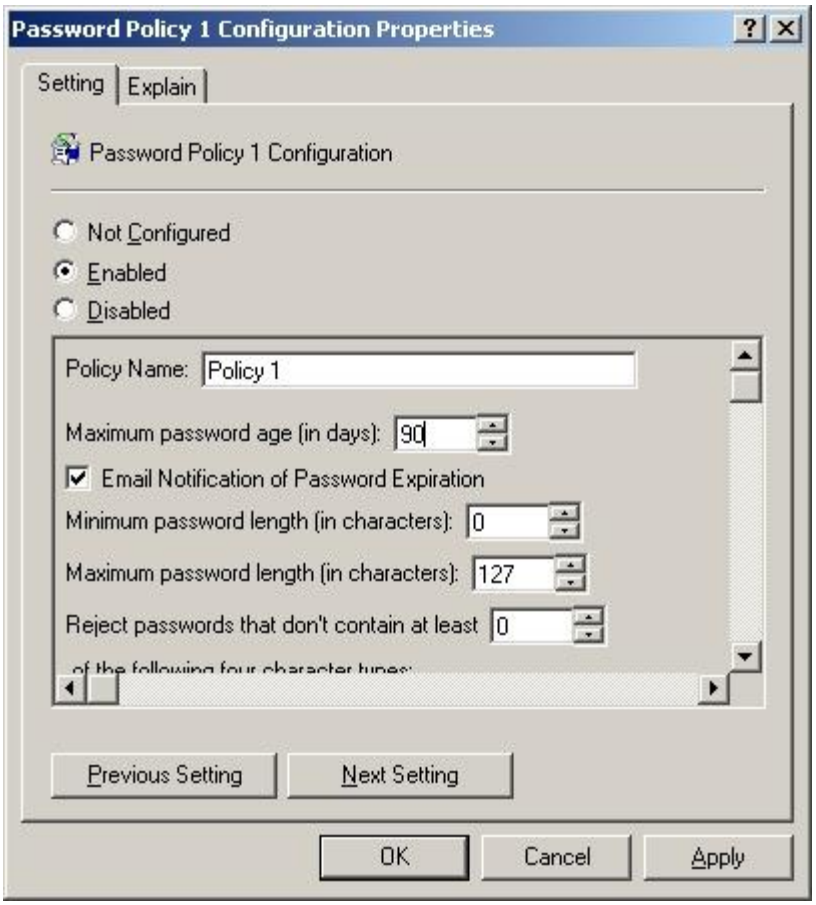

Figure 3.5.1: nFront Password Filter MPE Policy 1.

Policy	Description
Maximum Password Age (in days)	Valid Values: 0-365 Default Value: 0 (turned off) Configure a value from 1 to 365 to set the maximum password age for the groups to which this policy applies. For example, you can set this to a max of 30 days and apply it to Domain Admins. In such case the nFront Password Expiration Service (installed on only 1 DC in the domain) will read the settings and expire the passwords based on the timing here. NOTE: The value set here must be less than the overall maximum password age set via the Windows Password Policy.
Email Notification of Password Expiration	Default Value: 0

	Check this box to email warnings to end users about upcoming password expirations.
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 any account with the "Password Never Expires" flag set.
Global Groups 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: 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.

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. A new feature added in nFront Password Filter 4.5 is the ability for the service to email the end user and to generate administrative emails.

The updated version of 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.
- 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 are sent in plain text. 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.

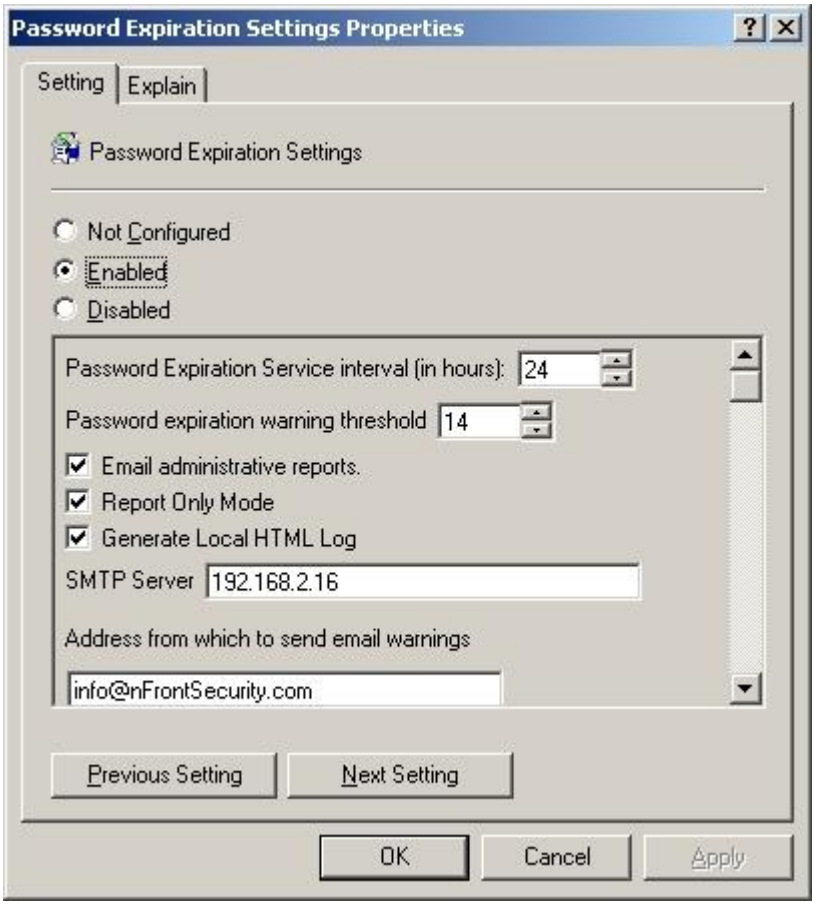

Figure 3.6.1: nFront Password Expiration Settings

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.
Email administrative reports	Default Value: 0 You can choose to skip the email of administrative reports.
Report Only Mode	Default Value: checked Uncheck this box to send emails to end users about password expirations and to 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.
Address from which to send 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.
Email address for administrative 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.
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	Default Value: “” The email to the end user will always contain a default body and can contain an optional custom message. If you fill in the optional custom message it will appear just below a header that reads: ---------- Message from your IT Administrator: ---------- The GPO textbox does not properly handle carriage returns. To include a carriage return in your message use two backslashes. Example: Please visit the following website:\\ to change your password\\ http://intranet/changepw
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.

3.6.1 Example Administrative Report

Subject: nFront Password Expiration Report

HTML Body:

nFront Password Expiration Report

DATE OF RUN: 3/08/2008 17:12:06

Settings:

Service Interval (in hrs)	24
SMTP Server	192.168.2.16
Warning Threshhold	30
Report Only	0
Email Admin Report	1

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	no
bob	bob@nFrontSecurity.com	1	15	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

3.6.2 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.

-----------------------------------
Message from your IT Administrator:
-----------------------------------
Please visit the following website to
change your password:
http://intranet.local/changepw
```

3.7 Optionally configure nFront Password Filter Client Policy

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.

You can choose to:

- Display a custom message to the end-user in addition to our default message.
- Display a custom message only

To add carriage returns to the custom message use "\\" (without the double quotes) as a carriage return.

3.8 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 Wordpad to add or remove entries. You must save the file in an ANSI format. As long as you can save the file in an ANSI format you can include characters from your native language (é, ü, etc.). If you edit the dictionary file, you must manually copy it to the %systemroot%\system32 directory on each domain controller. Or you can turn on the General Configuration option to "Read dictionary.txt from Netlogon share." 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.

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 comparison routine in nFront Password Filter looks for a case-insensitive match between the proposed new password and each line-entry in the dictionary.txt file. In less than 200 milliseconds, nFront Password Filter MPE ensures that the user's proposed password does not match any of the 27,000 entries!

You can configure nFront Password Filter to look for the dictionary word anywhere within the password (instead of looking for an exact match). The comparison is case-insensitive. This is the most helpful dictionary search and will prevent users from using common people names, months, days of the week, etc. within their passwords. You must be careful when enabling the substring search. If you are not careful in the construction of your dictionary file, you may be blocking an unusually high number of passwords. For example, if you were to include line entries with all of the characters of the alphabet all passwords with any alpha characters would be rejected. Since 'a' is found as a line entry in the dictionary, any password containing the letter 'a' is rejected.

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:

```
Windows 2000:
secedit /refreshpolicy machine_policy

Windows 2003:
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

Launch Active Directory Users and Computers (dsa.msc) for your Windows 2000 / 2003 domain. Highlight the **Domain Controllers container** for your domain, right-click and choose Properties. Select the Group Policy tab. Highlight the policy you created for nFront Password Filter (Figure 4.1.1). Click the Delete button. You will be prompted to remove the link or remove the link and delete the GPO (Figure 4.1.2). It is safe to delete the entire GPO as long as you have not configured any settings other than nFront Password Filter MPE settings in this GPO.

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

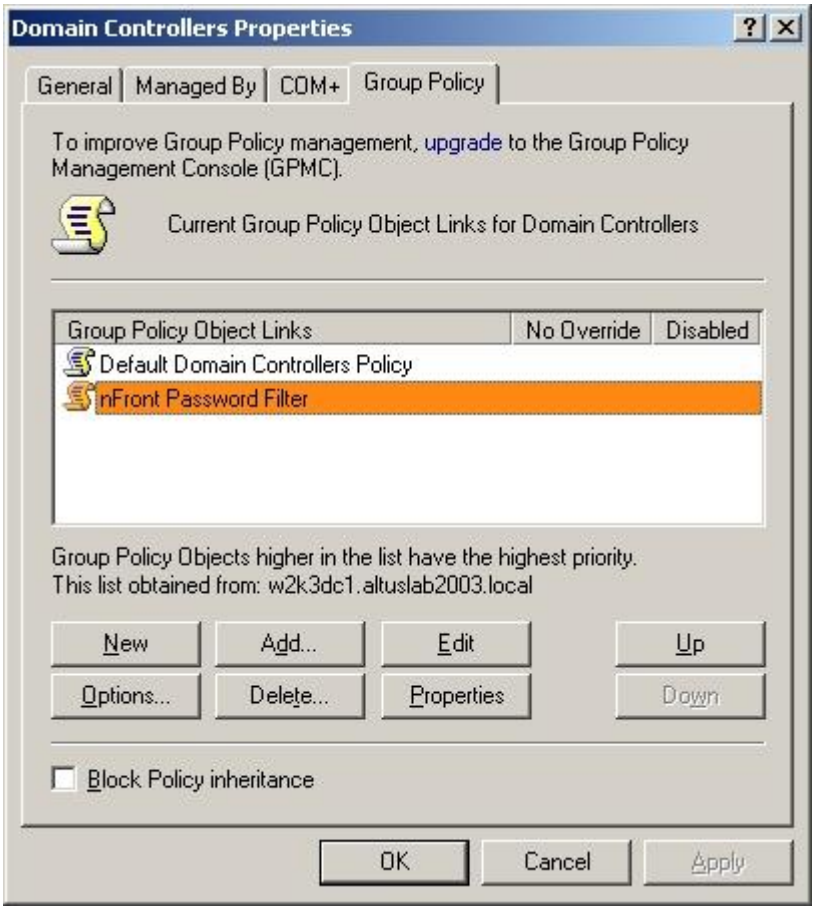

Figure 4.1.1: Deleting the nFront Password Filter policy.

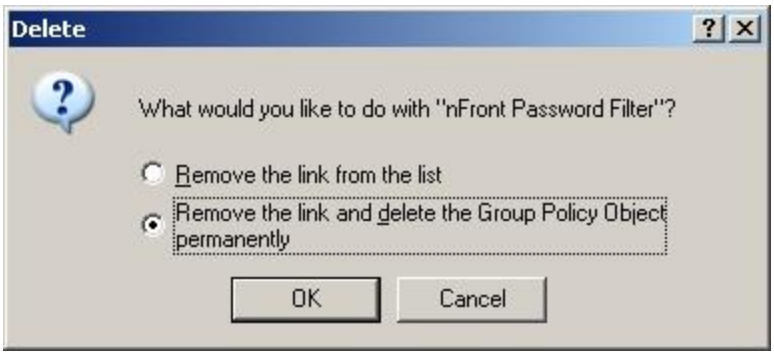

Figure 4.1.2: Deleting the nFront Password Filter policy.

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 + Programs + nFront Password Filter + Uninstall nFront Password Filter Edition. Once the uninstallation is complete you will need to reboot to unload the filtering DLLs from memory. You can always postpone the reboot as long as you have deleted the GPO or configured it to bypass filtering.

Alternatively, you can go to Start + Control Panel + Add/Remove Programs to remove the software.

4.3 Reboot

If you removed the registry settings as suggested in step 4.1 you are not forced to reboot immediately. Of course the DLL will remain loaded. However, it will not filter any passwords since it has no configuration data in the registry.

4.4 Delete unused files

Once you reboot, you can delete the following files to completely remove nFront Password Filter:

- C:\WINNT\SYSTEM32\PPRO.DLL

NOTE: DO NOT TRY TO REMOVE THE ABOVE FILE BEFORE REBOOTING IN STEP 4.3.

5.0 Verifying your Registration of nFront Password Filter

If you have purchased nFront Password Filter, you will receive an email or boxed copy 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 Active Directory Users and Computers (dsa.msc) for your Windows 2000 / 2003 domain. Highlight the **Domain Controllers container** for your domain, right-click and choose Properties. Select the Group Policy tab, highlight 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.

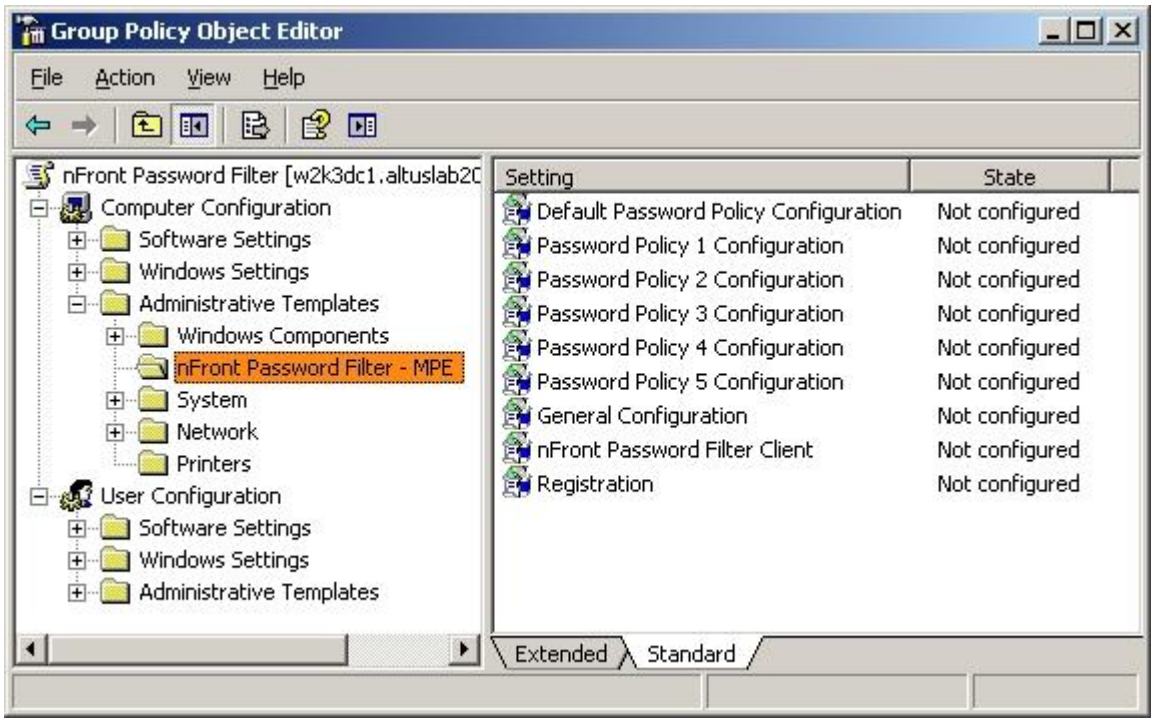

Figure 5.0.1: nFront Password Filter Group Policy

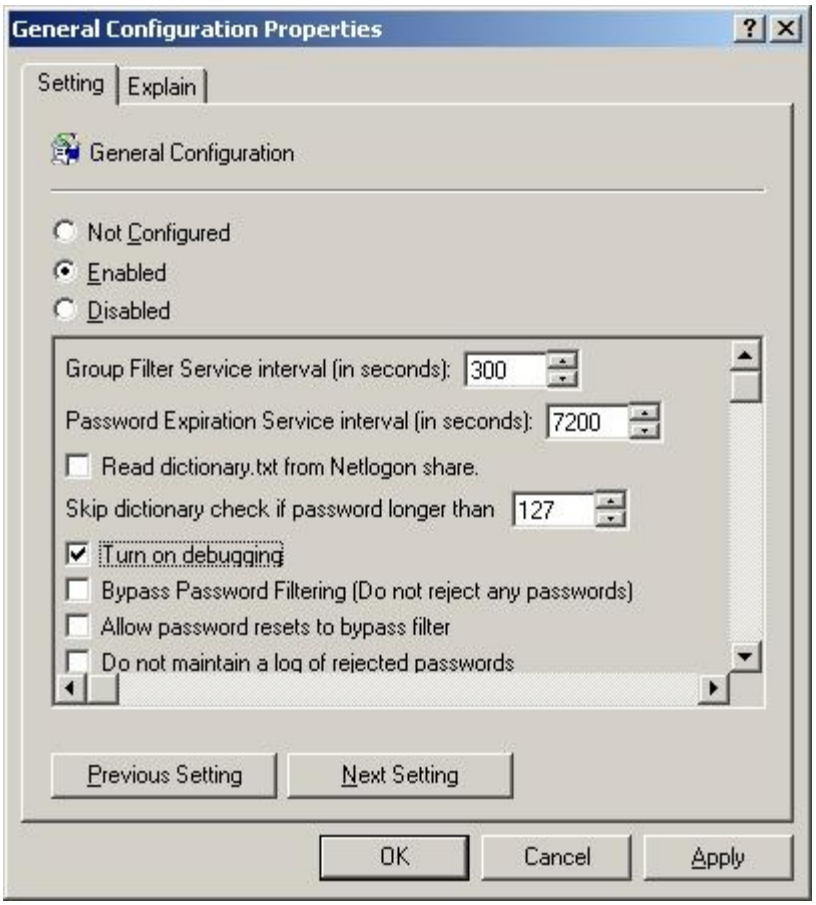

Figure 5.0.2: Turn on debugging

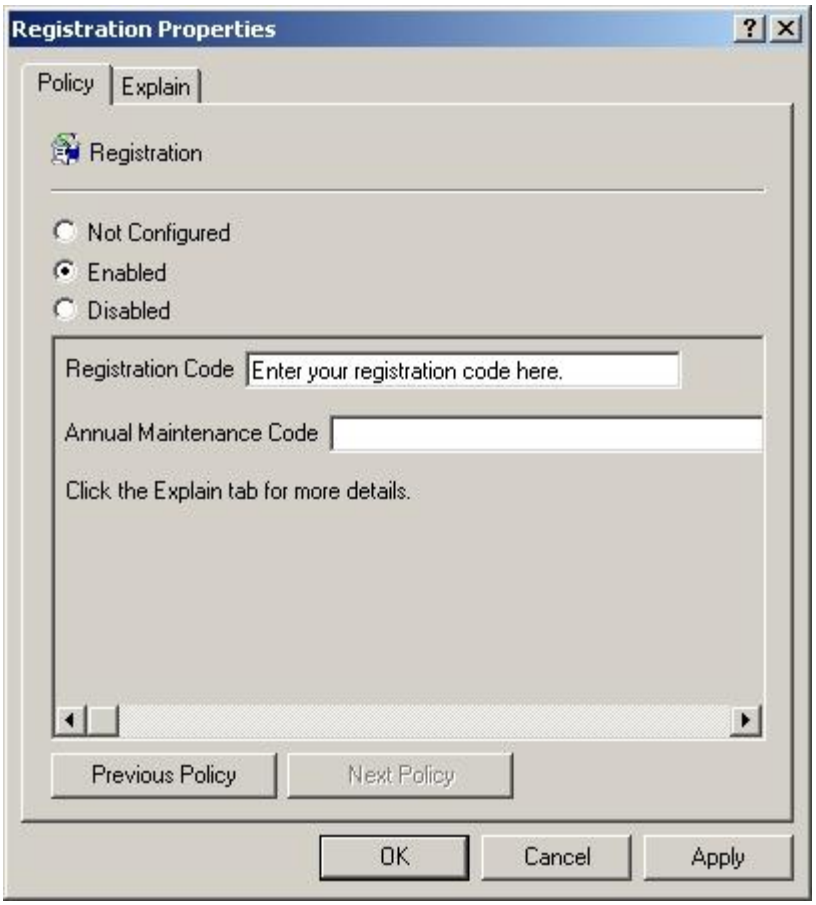

Figure 5.0.3: Enter Registration Code (all CAPS, include dashes)

3. Run `secedit /refreshpolicy machine_policy` or `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 test1 testpassword

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 secedit or gpupdate to force immediate replication.

7. Close the Group Policy editor and ADUC.

6.0 Upgrade Instructions

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.

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.

7.0 Implementation Guide

Implementing and enforcing a new password policy can be a little tricky. It will likely have a big 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 you can select multiple accounts + Properties + Account + User must change password at next logon. Windows 2000 has a problem with the Object Picker. Thus, you cannot select multiple user accounts and view or change properties. See the ADSI script in next section to assist you with Windows 2000 environments.

- **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).

7.1 Windows 2000 ADSI Script to force users to change passwords

As you have likely noticed, Windows 2000 does not allow you to highlight all user objects and modify their properties collectively. In other words, if you want to set each account to "User must change password at next logon", you will have to modify the properties of each account individually. To prevent repetitive motion injury while operating the mouse, you can use the script below. Simply modify the LDAP path at the top to indicate the container and domain where your user accounts are located. Do not forget this modifies ALL user accounts in the container, so if you have service or template accounts, you will have to remove the setting for those accounts.

chgpw.vbs

```
adpath = "LDAP://cn=users,dc=xyz,dc=com"
set oContainer = getobject(adpath)
oContainer.filter = array("user")

For each oUser in oContainer
   WScript.echo "Setting ""User must change password on next logon"" for " & oUser.name
   oUser.pwdLastSet = 0
   oUser.setinfo
Next
```

To use the script above, type in the text (or cut and paste this text) into a text editor such as Notepad. Modify the first line to point to your domain and the container(s) where you have created user accounts. Save the file with a .vbs extension. Open a command window and navigate to the directory where you saved the file. Then run the script using cscript.

```
c:\temp\cscript chgpw.vbs
```

NOTE: You will still need to manually select each account you did not want modified (like service accounts) and deselect the checkbox for "User must change password on next logon."

8.0 Troubleshooting

8.1 Common Problems

Symptom	Proposed Troubleshooting
System is not filtering any 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.
Installation or upgrade to Exchange 2003 is failing	**Exchange cannot set a system account password that meets your password policies.** Temporarily disable nFront Password Filter by editing the group policy. Go to the General Configuration policy and check the box to "Bypass Password Filtering." This will go into effect within the standard 5 to 15 minute DC group policy replication interval. Expedite the propagation of the policy with a secedit or gpudpate command. After the policy change, complete the installation of Exchange and then change the policy back to its original state to re-apply filtering.

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: 4/30/2004
registered = 0
registrationCode = <eval code here>
Annual Maintenance Code = <maintenance code here>
   Contract expires on <maintenance code expiration date>

nFront Password Filter version 4.0.0 Build 2007062503
------------------------------------------------------------
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 = 127
minCharacters = 0
minCharTypes = 0
checkNumeric = 1
  minNumericChar = 2
  maxNumericChar = 127
checkUpper = 0
  minUpperChar = 0
  maxUpperChar = 127
checkLower = 0
  minLowerChar = 0
  maxLowerChar = 127
checkAlpha = 0
  minAlphaChar = 0
  maxAlphaChar = 127
checkNonAlphaNumeric = 0
  minNonAlphaNumericChar = 0
  maxNonAlphaNumericChar = 127
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 = 127
minCharacters = 0
minCharTypes = 0
checkNumeric = 0
  minNumericChar = 0
  maxNumericChar = 127
checkUpper = 1
  minUpperChar = 2
```

```
  maxUpperChar = 127
checkLower = 0
  minLowerChar = 0
  maxLowerChar = 127
checkAlpha = 0
  minAlphaChar = 0
  maxAlphaChar = 127
checkNonAlphaNumeric = 0
  minNonAlphaNumericChar = 0
  maxNonAlphaNumericChar = 127
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 display password rules and improve the error message for rejected password changes.

Without the nFront Password Filter Client Windows XP and Windows 2000 will provide the following failure message for rejected passwords. It may be the case the end user has selected a password that meets these criteria but has failed due to nFront Password Filter password rules.

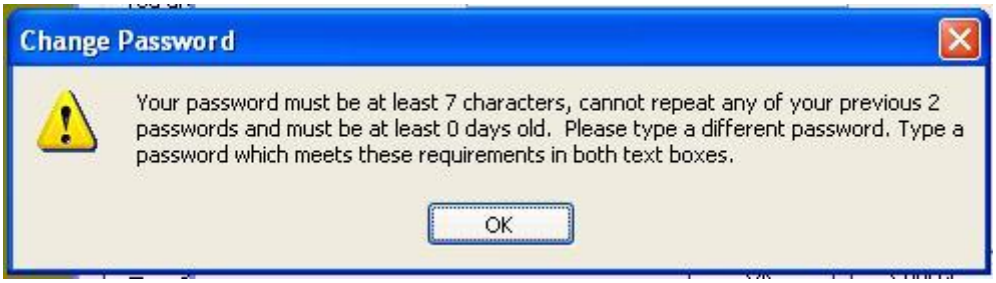

Figure 9.0.1: Windows default message for failed passwords.

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.

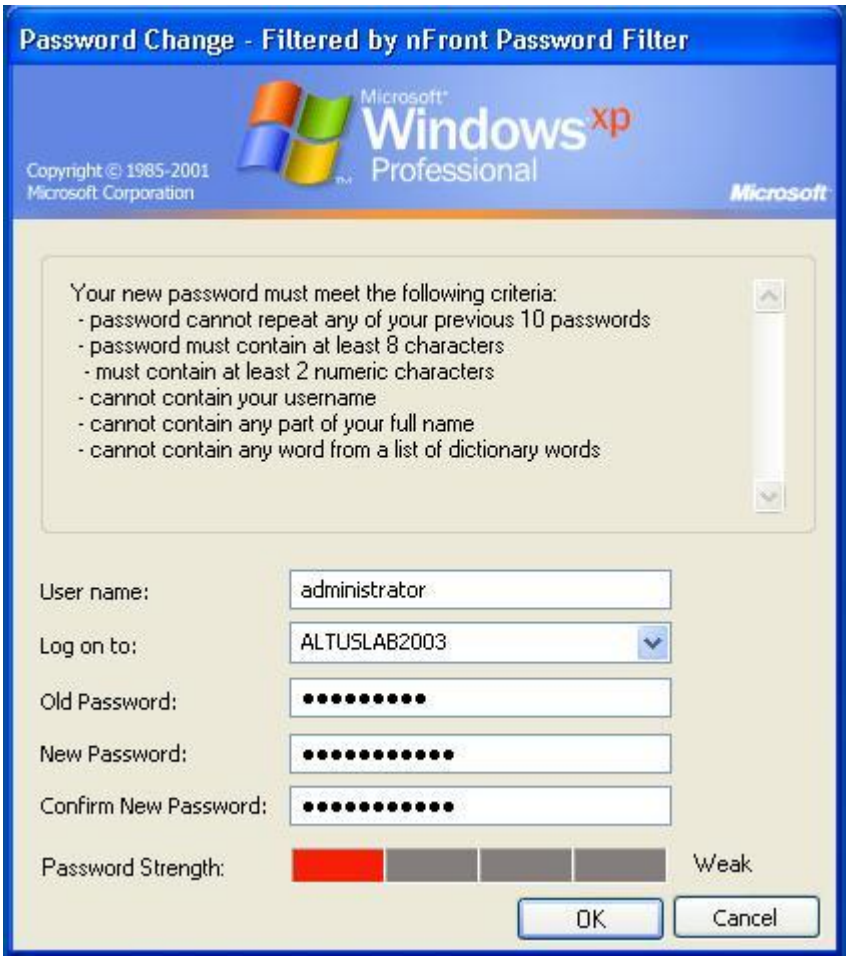

Figure 9.0.2: Password Change dialog with nFront Password Filter Client installed (shown with optional password strength meter enabled)

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 9.0.3: Password failure message generated by nFront Password Filter Client

9.1 Technical Overview

This message is generated by a DLL on each client workstation called MSGINA.DLL. The DLL is a critical component of Windows. We do not replace the MSGINA.DLL. Instead our software works as a "ginahook." A ginahook is allowed to handle certain function calls and pass others to the regular MSGINA.DLL.

Please note that this is the only architecture supported by Microsoft for the modification of the Windows Change Password dialog. Any client that uses .NET code or attempts to hook Windows dialogs via a winlogon notify package is not supported by Microsoft. To our knowledge there are 2 other companies which currently offer a client component. Both are using winlogon notify packages and 1 uses .NET technologies which are not supported by Microsoft for any kernel mode component.

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. The nFront Password Filter Client consists of two files installed the end-users workstation: altusgina.dll and pproclient.dll. We have attempted to maximize the upgradeability of the client. Consequently the pproclient.dll can be dynamically replaced at any time. However, the altusgina.dll is exclusively locked by the operating system and not as easily upgraded with a reboot. 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.

9.1.1 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 match any word from a list of dictionary words
- cannot contain any word from a list of dictionary 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 the 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 and Italian. Other languages will be added soon. If you would like the rules in another language please email us at info@altusnet.com with a language request. The client already reports the user's interface language to the server component.

9.1.5 GINA chaining

Microsoft allows only one ginahook 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.

Our initial release of the nFront Password Filter Client does not support GINA chaining. Please notify us if you are currently using a 3rd party GINA. We will be happy to work with you to see if GINA chaining can be accomplished with your existing 3rd party GINA.

9.1.6 Know Limitations

- Does not work for local password changes
- Does not list nFront Password Filter rule for "must contain numeric character in position X"
- Does not list nFront Password Filter rule for "must contain special character in position X"
- The RPC server will work on x64 domain controllers. The client components have not yet been packaged for install on x64 versions of Windows XP.

9.2 Installation

Individual and enterprise deployment

Step 1: Upgrade nFront Password Filter on Domain Controllers.
You can follow the upgrade instructions listed previously in this document. If running 3.5X or later you can simply go to Control Panel + Add Remove Programs + Remove nFront Password Filter. Ignore the prompt to reboot. Then install the new nFront Password Filter.MSI package and ignore the reboot prompt again. This will replace the ppro-eng.dll (the filtering engine) and add 1 additional service needed for client support. If running a version of nFront Password Filter prior to 3.5X you will need to uninstall the old version, reboot and install the latest version.

Step 2a: Install nFront Password Filter Client on individual workstation
Simply install the nFront Password Filter Client.MSI package and reboot when prompted. After a reboot the Change Password Dialog box should now be modified and display rules provided by a domain controller.

Step 2b: Install nFront Password Filter Client across many workstations using a software GPO
We like this approach because it automagically 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.

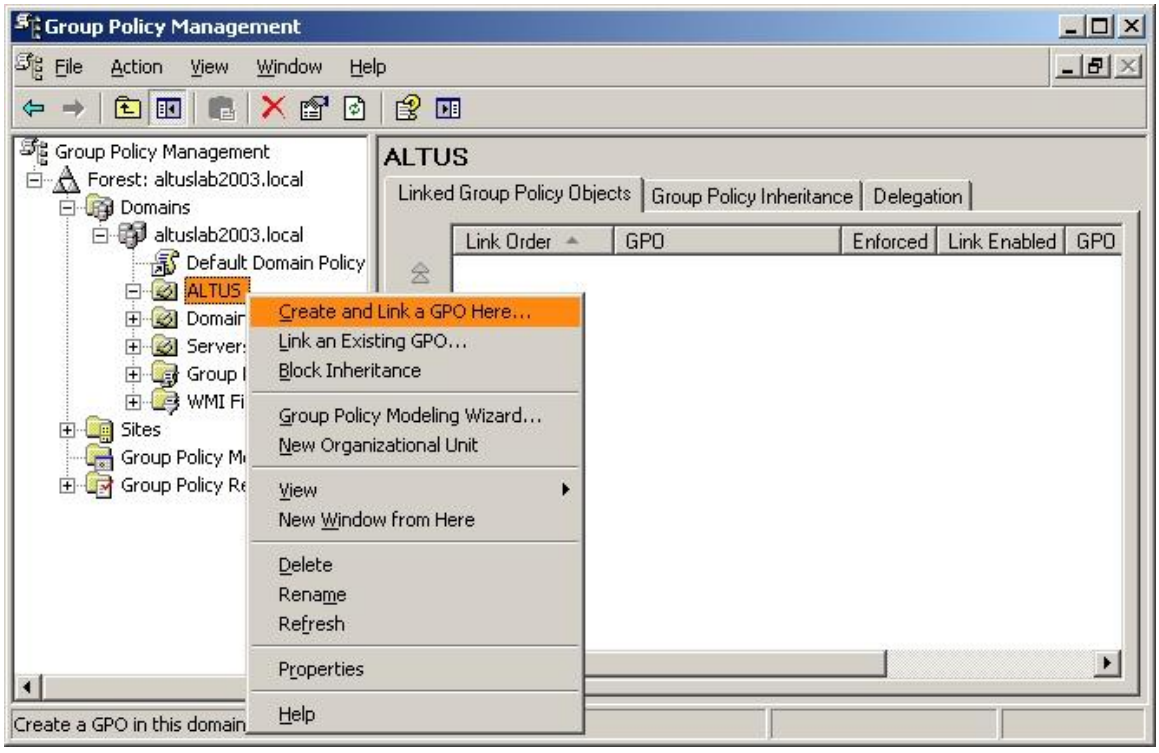

Figure 9.2.1: Creating a new software deployment GPO via GPMC

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

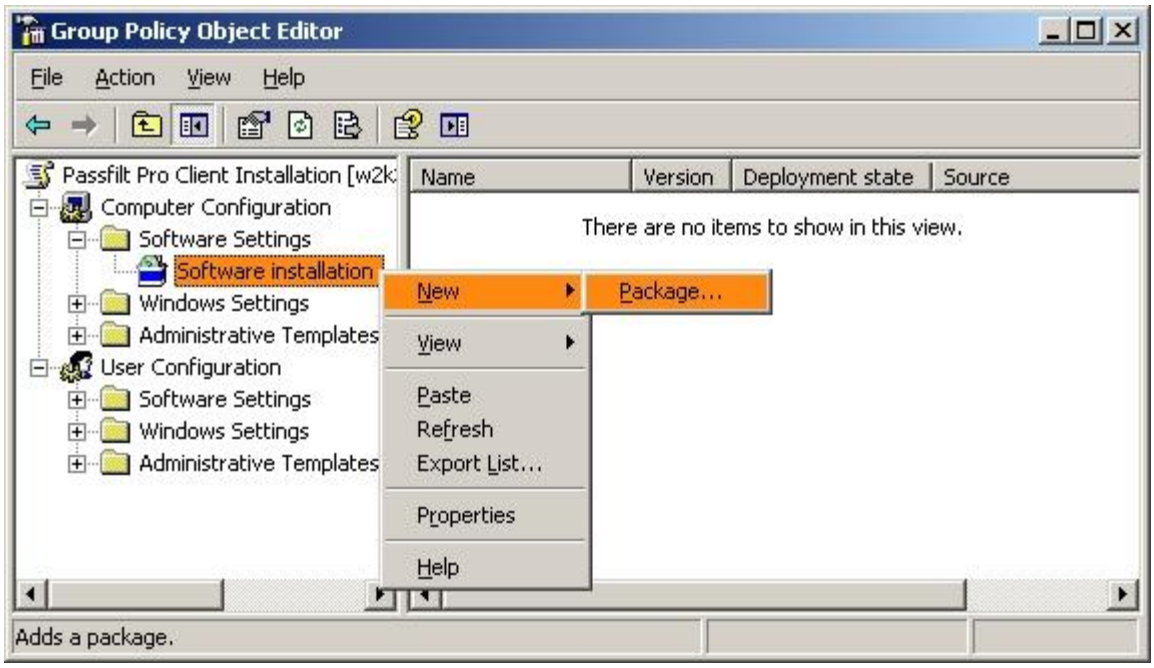

Figure 9.2.2: Adding a new package to the software deployment GPO

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.

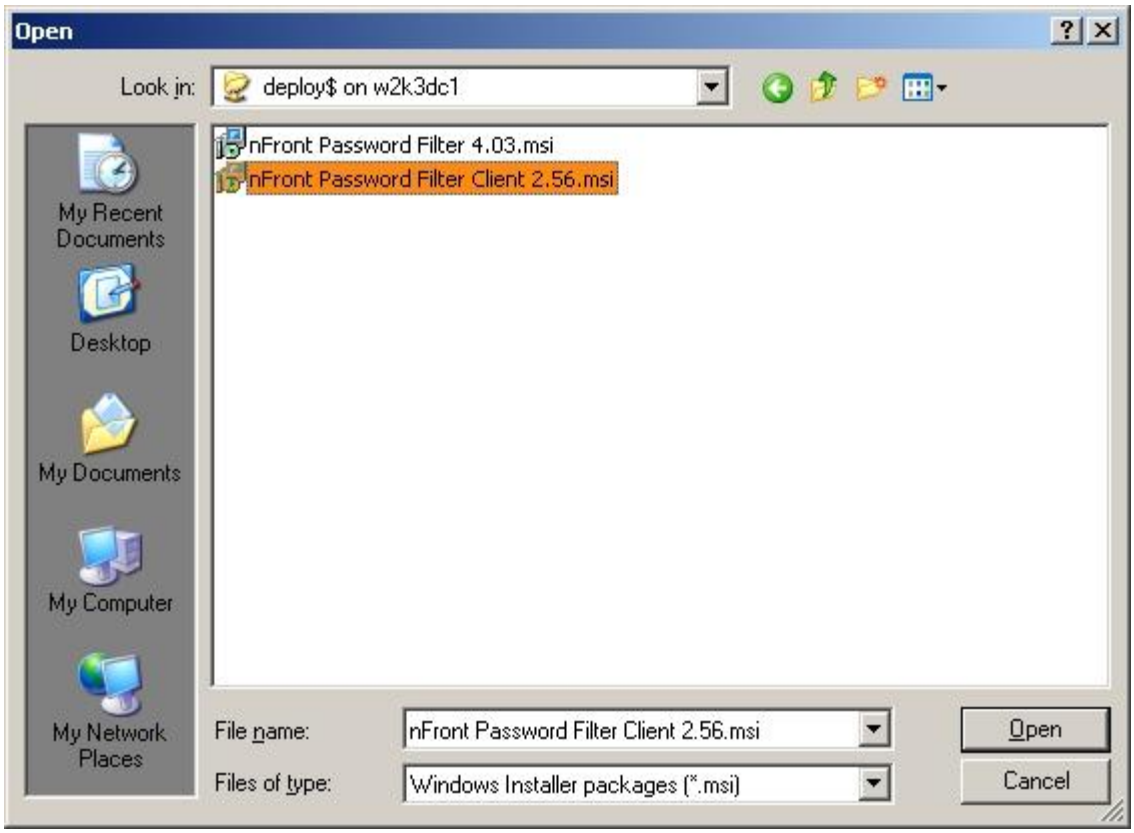

Figure 9.2.3: Providing the package location

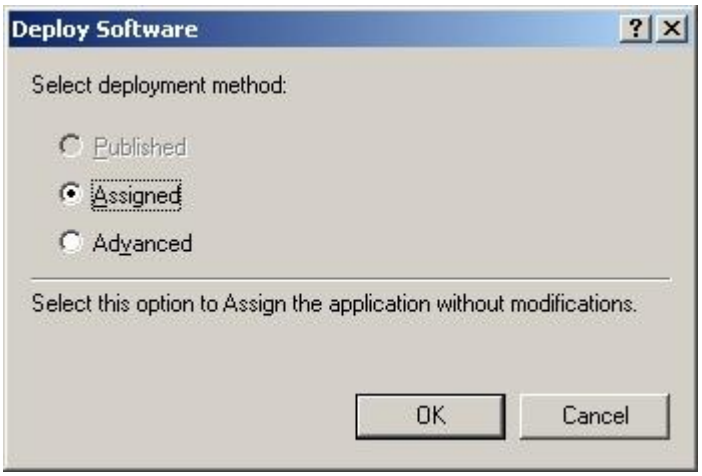

Figure 9.2.4: Always assign the application

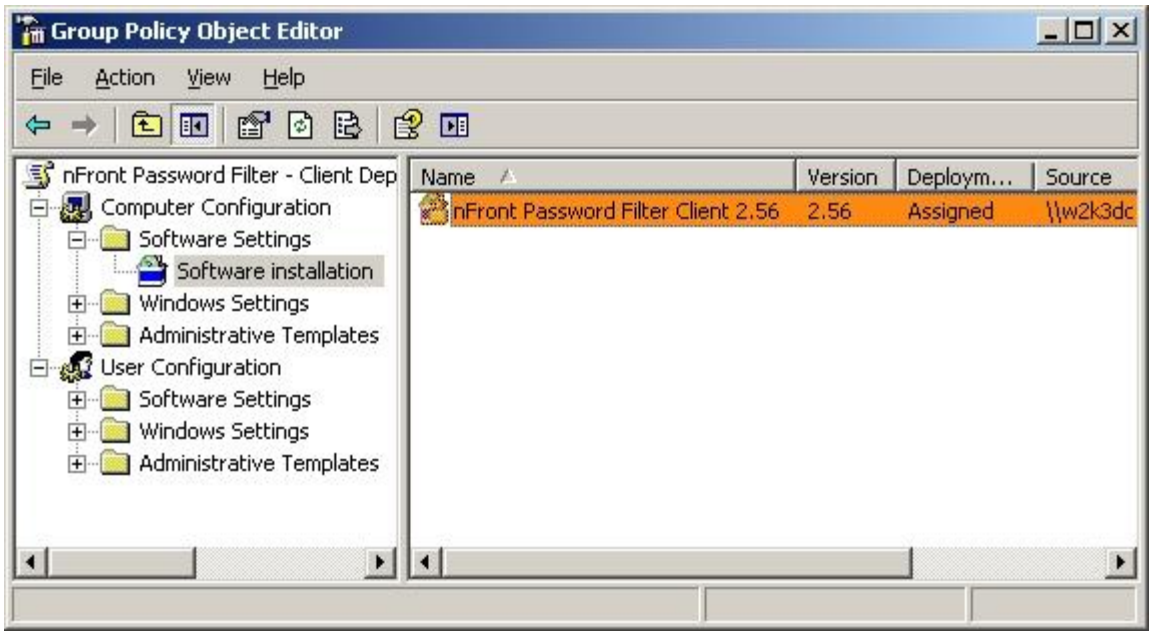

Figure 9.2.5: The package now appears in the right pane

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."

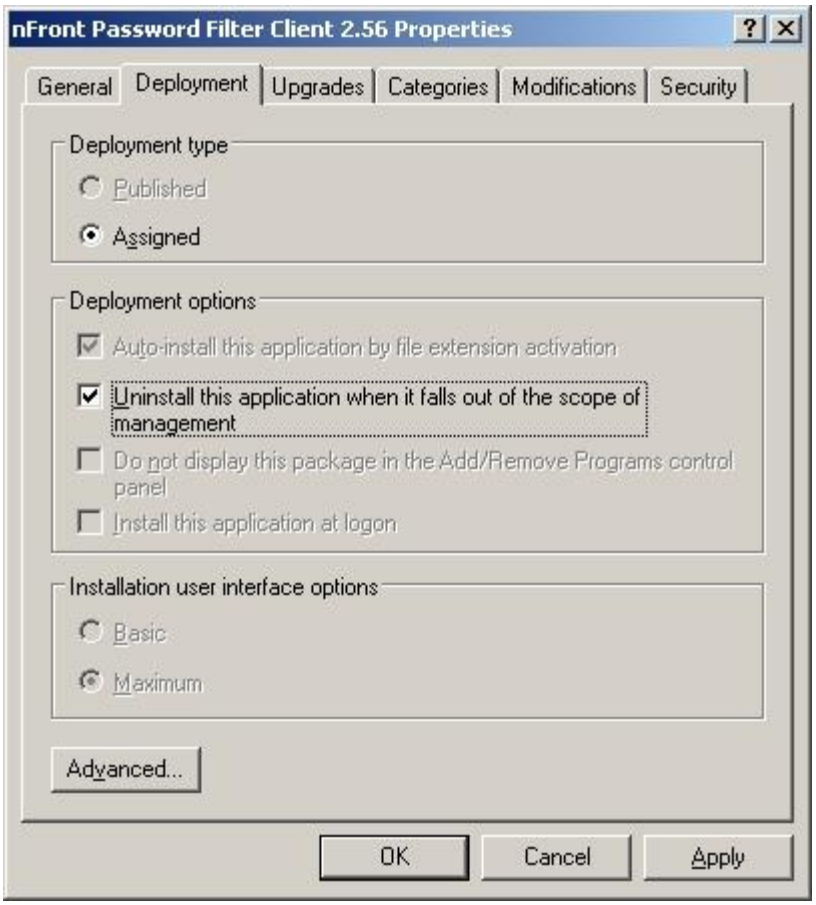

Figure 9.2.6: Changing the deployment options

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. The user is not prompted and the reboot is not forced. 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.

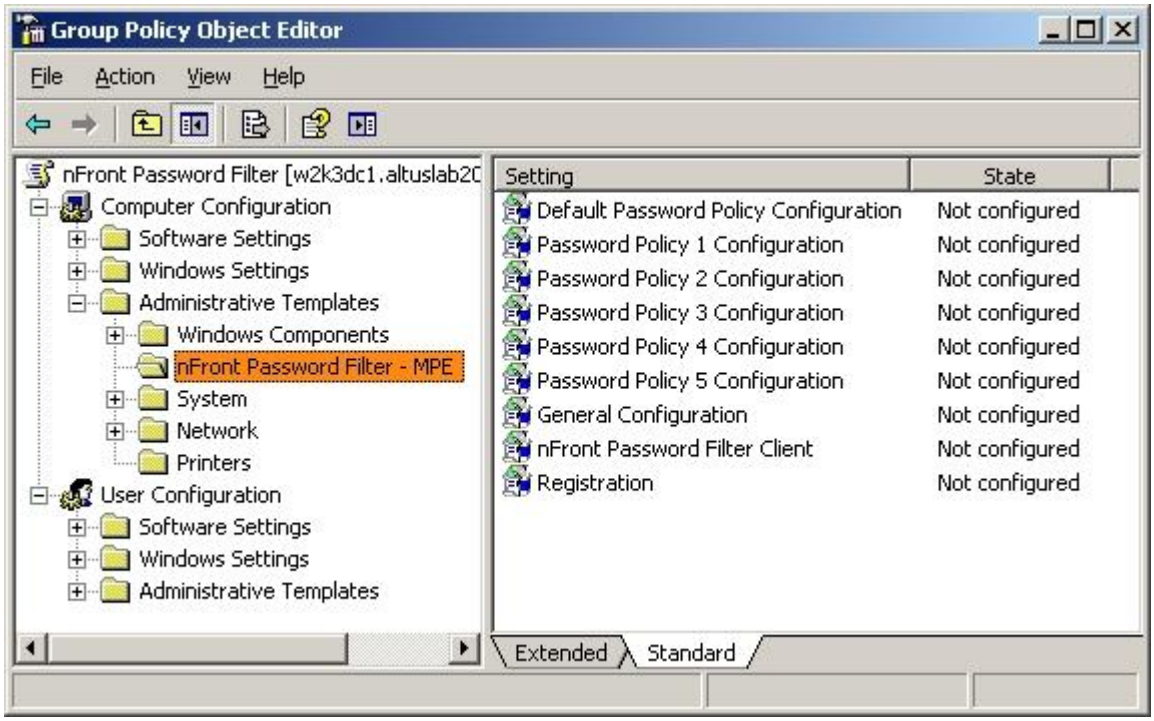

Figure 9.3.1: nFront Password Filter GPO for domain controllers OU

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.

Optional Password Strength Meter

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 or to globally disable the nFront Password Filter client.

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 9.3.3 shows the optional settings and figure 9.3.4 shows the nFront Password Filter Client with the strength meter enabled.

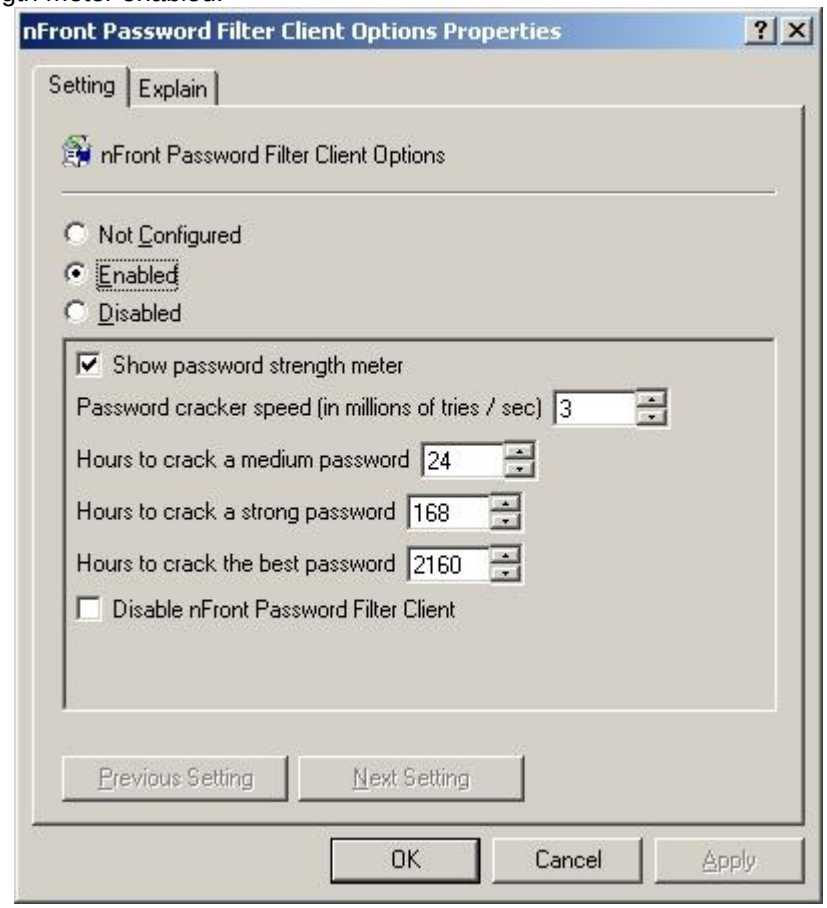

Figure 9.3.3: nFront Password Filter Client Options deployed at domain or OU level.

Policy	Description
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.
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.

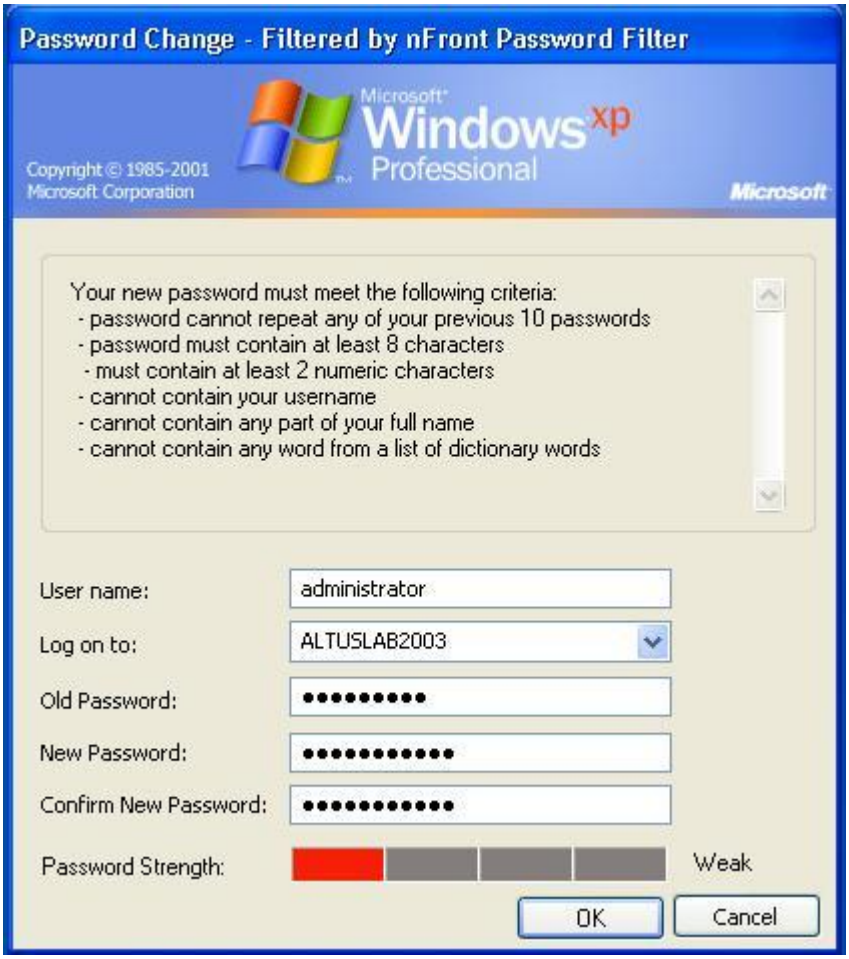

Figure 9.3.4: nFront Password Filter Client with password strength meter enabled

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.

9.4 Troubleshooting

If the altusgina.dll file is deleted or if it is corrupted, the Windows 2000 or XP operating system will display the message in figure 9.4.1 on boot. The solution is to reboot and press F8 during boot. Boot into Safe Mode and edit the registry.

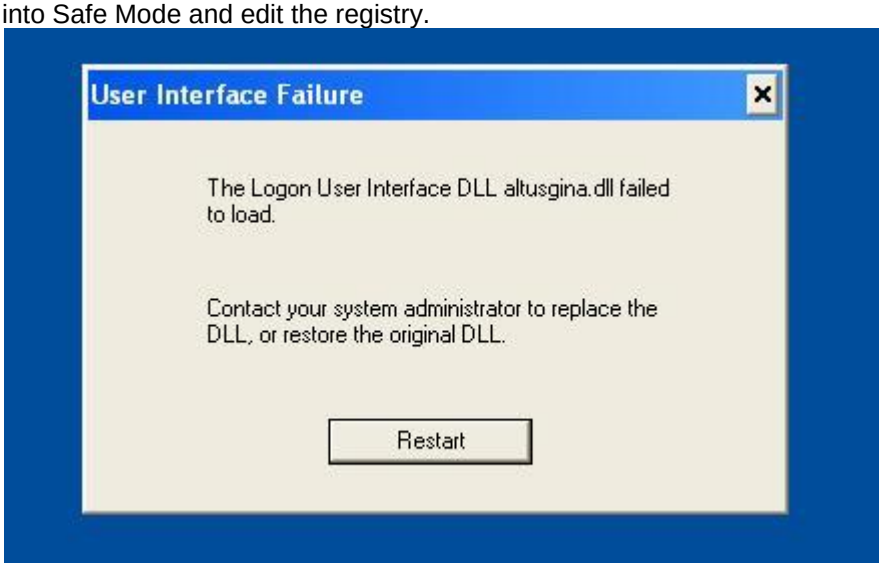

Figure 9.4.1: Missing or invalid GINA results in this message on boot

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

You may encounter the dialog in figure 9.4.2 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 9.4.2: DC Unavailable or nFront Password Filter Password Policy Service not running

If the end-user receives the message in Figure 9.4.2 and continues to change his or her password, he or she may receive the error message in 9.4.3 (if the RPC server is still unavailable). After clicking OK, the password change is sent to the starndard MSGINA.DLL and the end-user will get the standard Windows Password Change error message (Figure 9.4.4) 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 9.4.3: DC Password Change message if the client cannot communicate with the nFront Password Filter Password Policy Service on the DC.

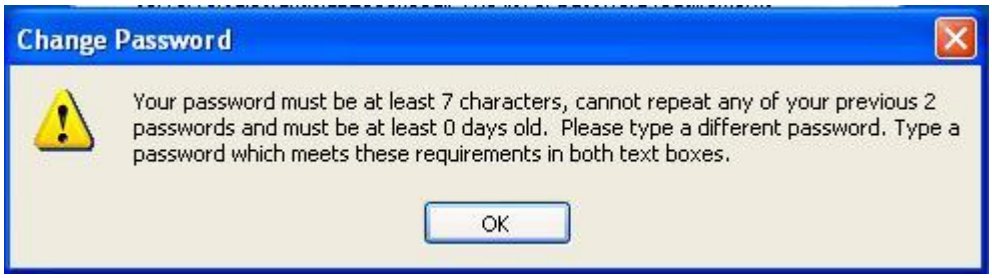

Figure 9.4.4: Standard Windows XP / 2000 password change error message.

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 password checking.		
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 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 127 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	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.
32767	- Password matches the following word from dictionary.txt:
65536	- Password contains the following word from dictionary.txt:
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
```