nFront PASSWORD FILTER DEPLOYMENT GUIDE

nFront Password Filter Overview

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

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.

Compatibility and System Requirements

The nFront Password Filter and nFront Password Filter Client are compatible with both 32-bit

and 64-bit versions. The software is supported on all server platforms from Windows 2003 through Server 2016 as well as all desktop platforms from Windows XP through Windows 10.

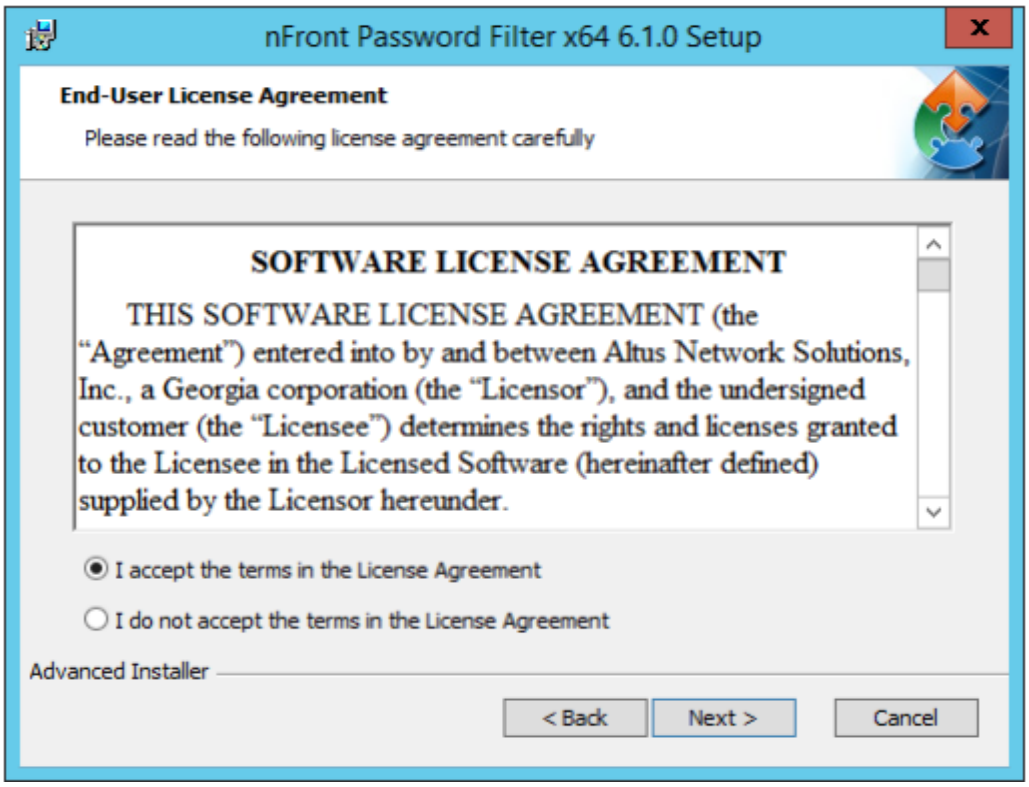
The nFront Password Expiration Service should be run on a Windows Server that is a member of

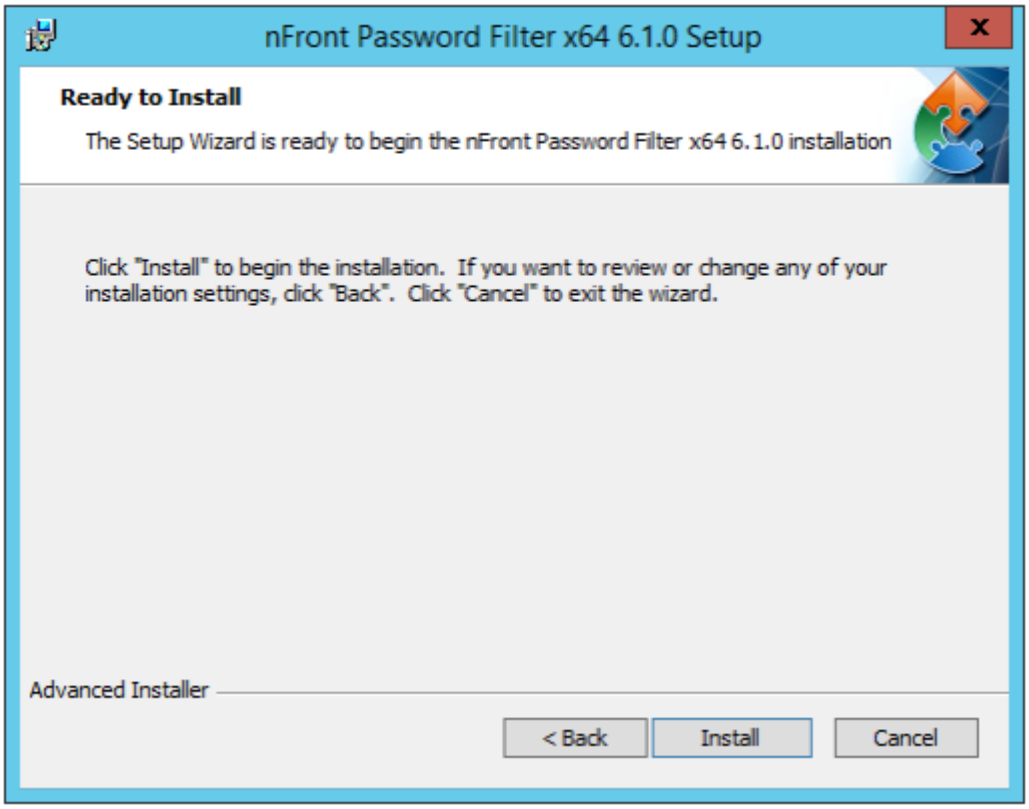
the domain or a domain controller. It is best to run it on a domain controller.

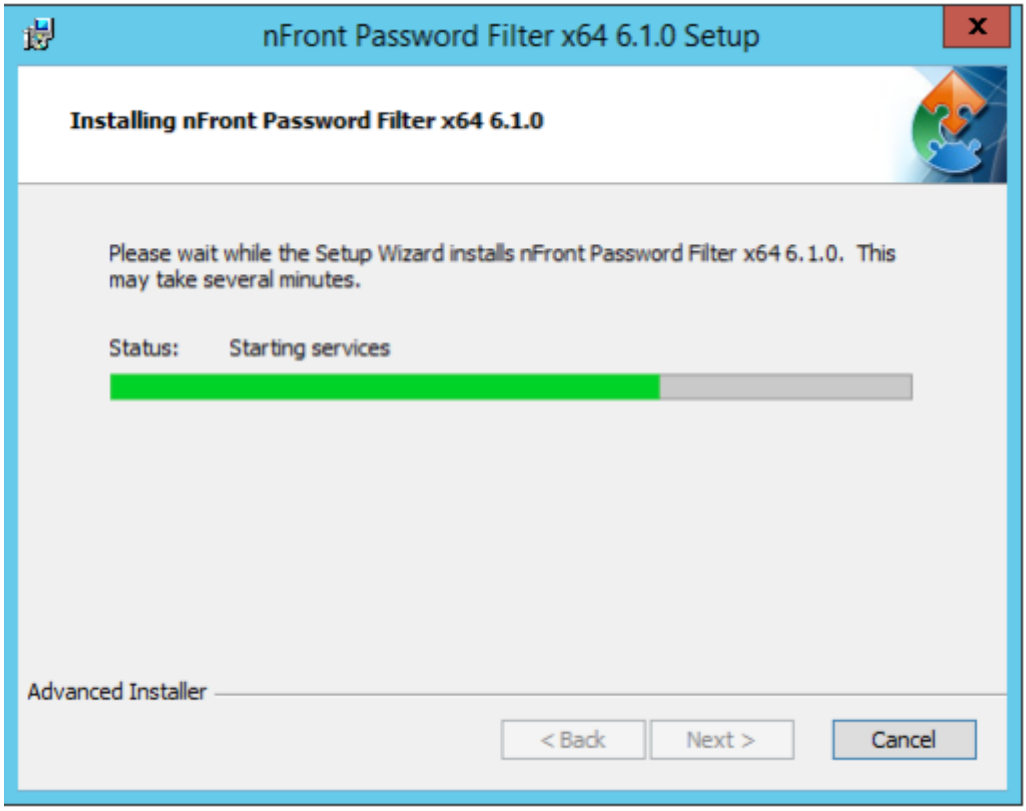
nFront PASSWORD FILTER DEPLOYMENT GUIDE

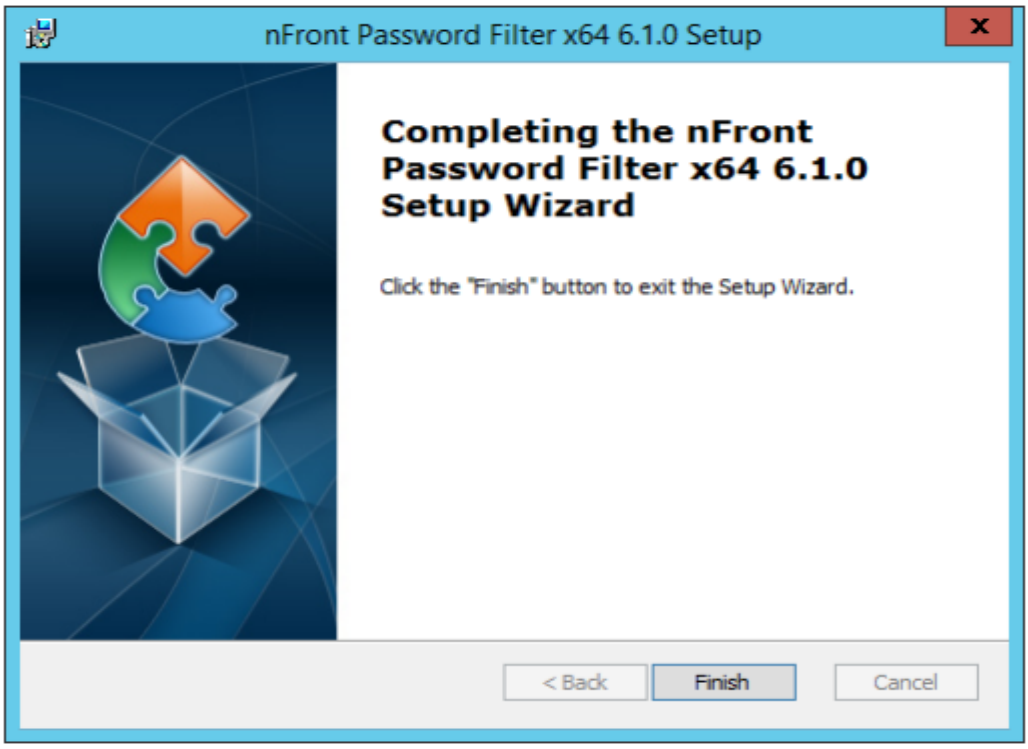
RUN nfront PASSWORD FILTER INSTALLER

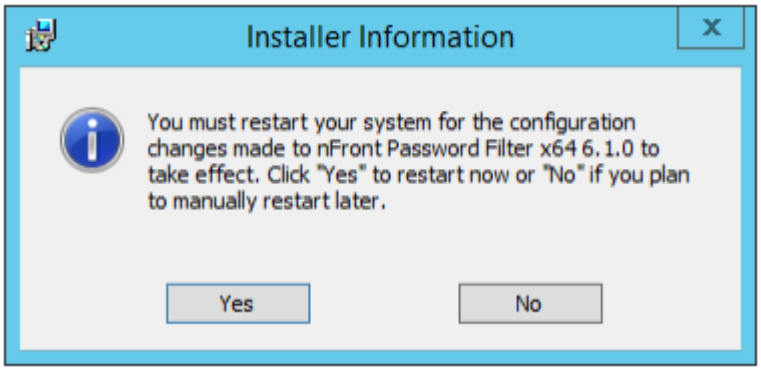
Double-click the nFront Password Filter.MSI file to run the installation wizard. Be sure to run the x64 version if you are installing on an x64 server




nFront Password Filter x64 6.1.0 Setup
Ready to Install
The Setup Wizard is ready to begin the nFront Password Filter x64 6.1.0 installation
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced Installer
< Back
Install
Cancel


nFront Password Filter x64 6.1.0 Setup
Installing nFront Password Filter x64 6.1.0
Please wait while the Setup Wizard installs nFront Password Filter x64 6.1.0. This may take several minutes.
Status: Starting services
Advanced Installer
< Back
Next >
Cancel



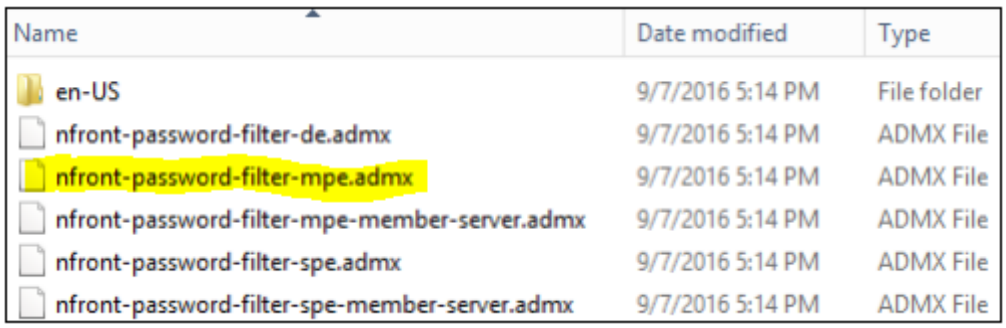


You must restart for the operating system to load the password filter DLLs on boot. You can say No to the optional restart and reboot at a later time.

NOTE: THE ABOVE INSTALL PROCESS NEEDS TO BE DONE ON EACH DOMAIN CONTROLLER.

LOADING ADMX TEMPLATES

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



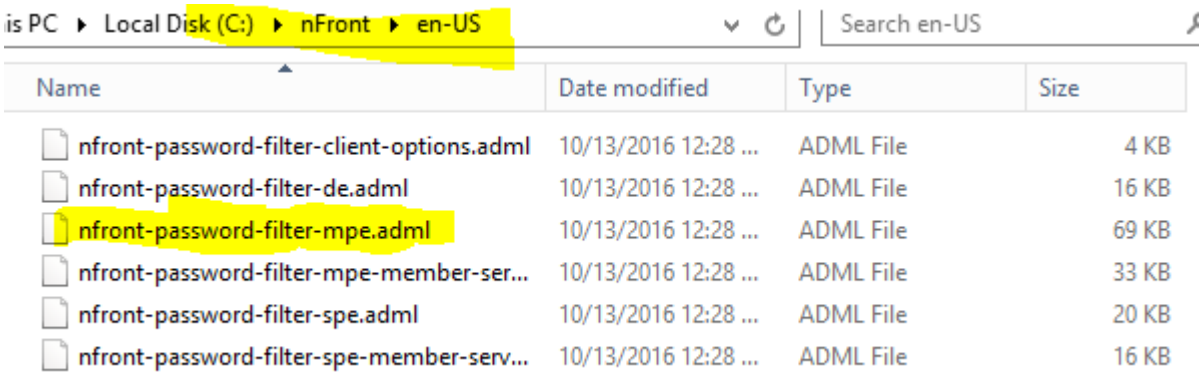
Name	Date modified	Type
en-US	9/7/2016 5:14 PM	File folder
nfront-password-filter-de.admx	9/7/2016 5:14 PM	ADMX File
nfront-password-filter-mpe.admx	9/7/2016 5:14 PM	ADMX File
nfront-password-filter-mpe-member-server.admx	9/7/2016 5:14 PM	ADMX File
nfront-password-filter-spe.admx	9/7/2016 5:14 PM	ADMX File
nfront-password-filter-spe-member-server.admx	9/7/2016 5:14 PM	ADMX File

Copy the above highlighted admx template into your central store if you do not have one follow the suggestion below

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

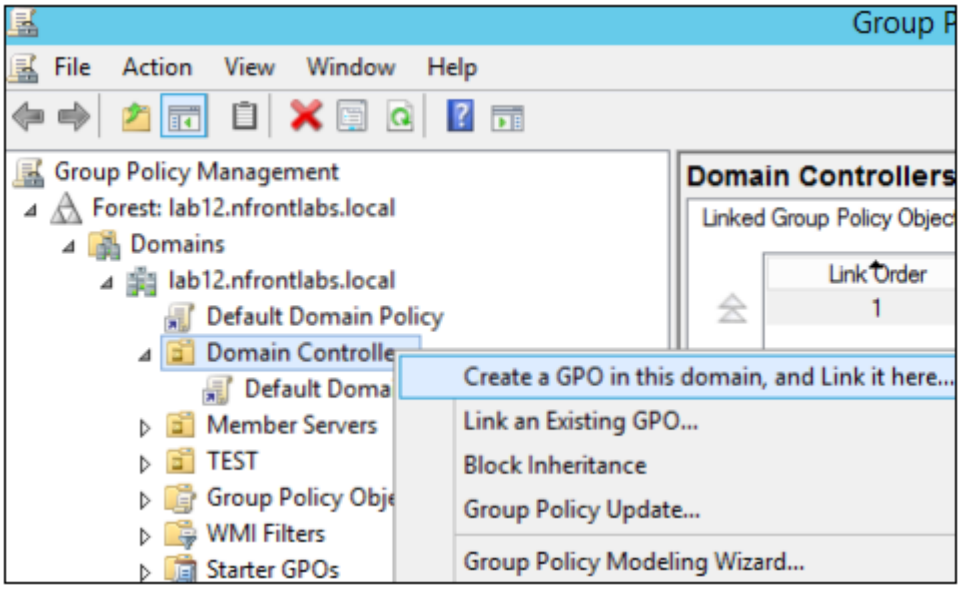
Also copy the corresponding ADML file from the enUS folder to the PolicyDefinitions\en-US folder in the central store.

N



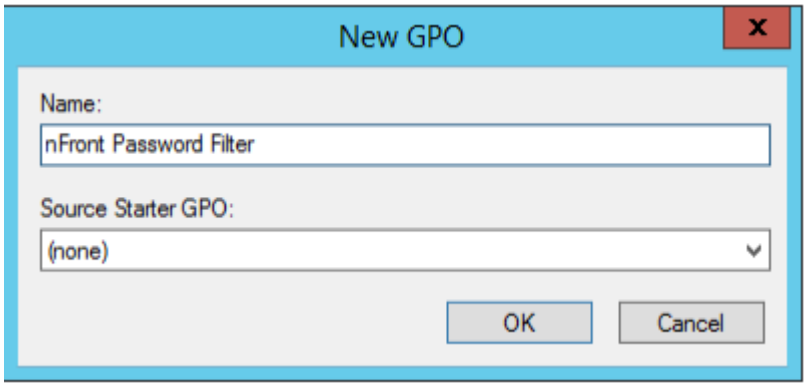
CREATE A GPO VIA GPMC

You will use a single GPO to control the nFront software. This GPO will be link to the Domain Controllers container

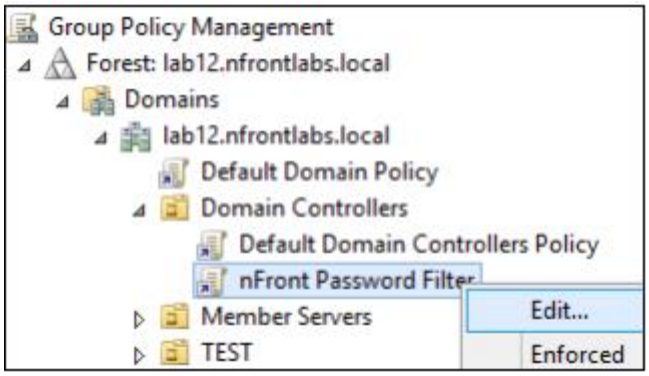


Give the GPO the following name

nfront Password Filter



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



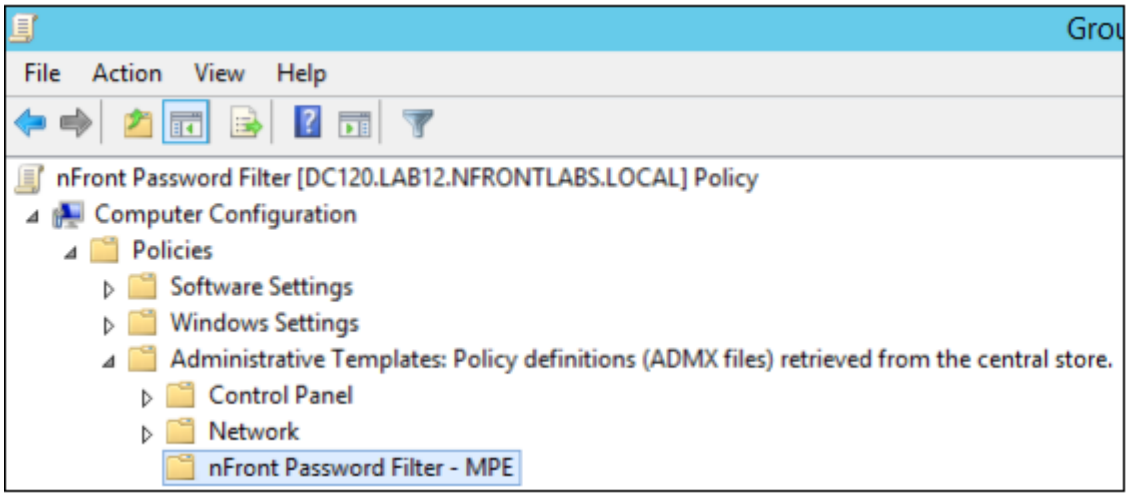
If you have loaded the ADMX template it will appear automatically in the new GPO.

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

Each DC must have permissions to read the GPO to add the configuration data to the local registry.

IMPORTANT NOTE: **nFront Password Filter Policy only needs to be created once on the primary domain controller. All other domain controllers will get the GPO via replication. All that is required is to make sure all other domain controllers have the nFront Password Filter installed.**

In the new GPO, you will navigate to Computer Configuration + Policies + Administrative Templates + nFront Password Filter to configure the settings. Below is a screen clipping showing the nFront Password Filter MPE settings that appear.



CUSTOMIZE THE DICTIONARY.TXT FILE

We will be using a dictionary file with this deployment of nFront. 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.

A dictionary file has been provided for you and you will need to overwrite the existing one with the one that has been provided by placing it in the below location on **ALL DOMAIN CONTROLLERS**

C:\windows\system32\

You can edit the file using Notepad or any text editor. **Make sure to save the dictionary in plaintext (ANSI format)**

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

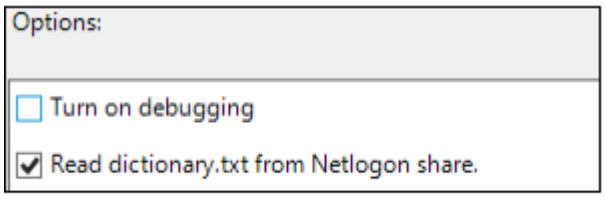
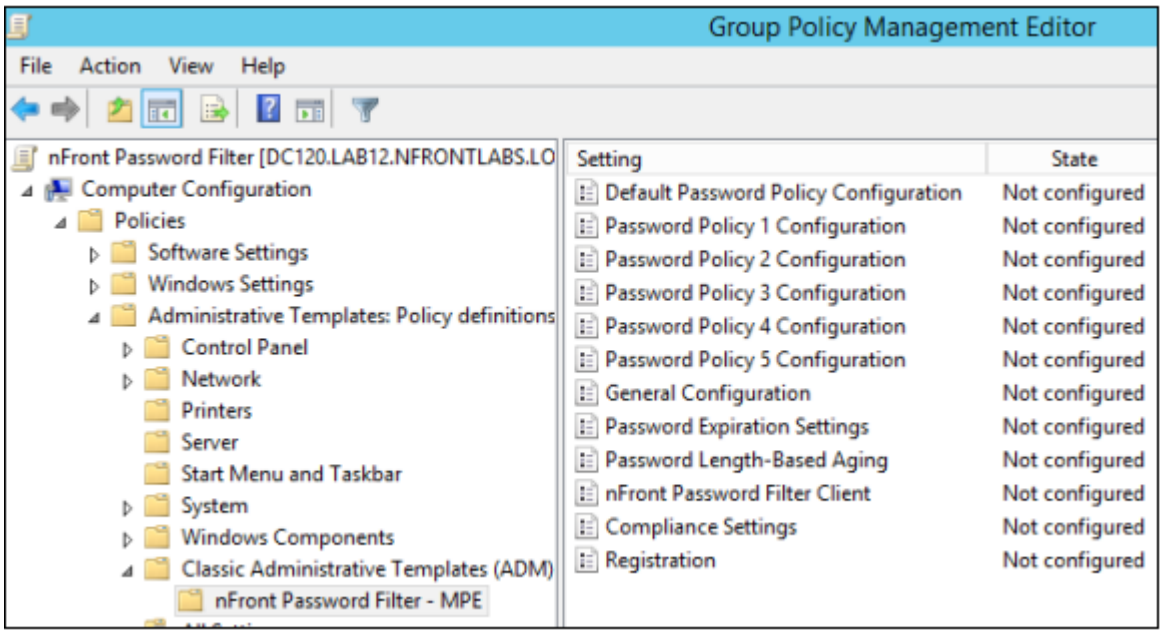


Figure 2.7.1: General Configuration settings

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

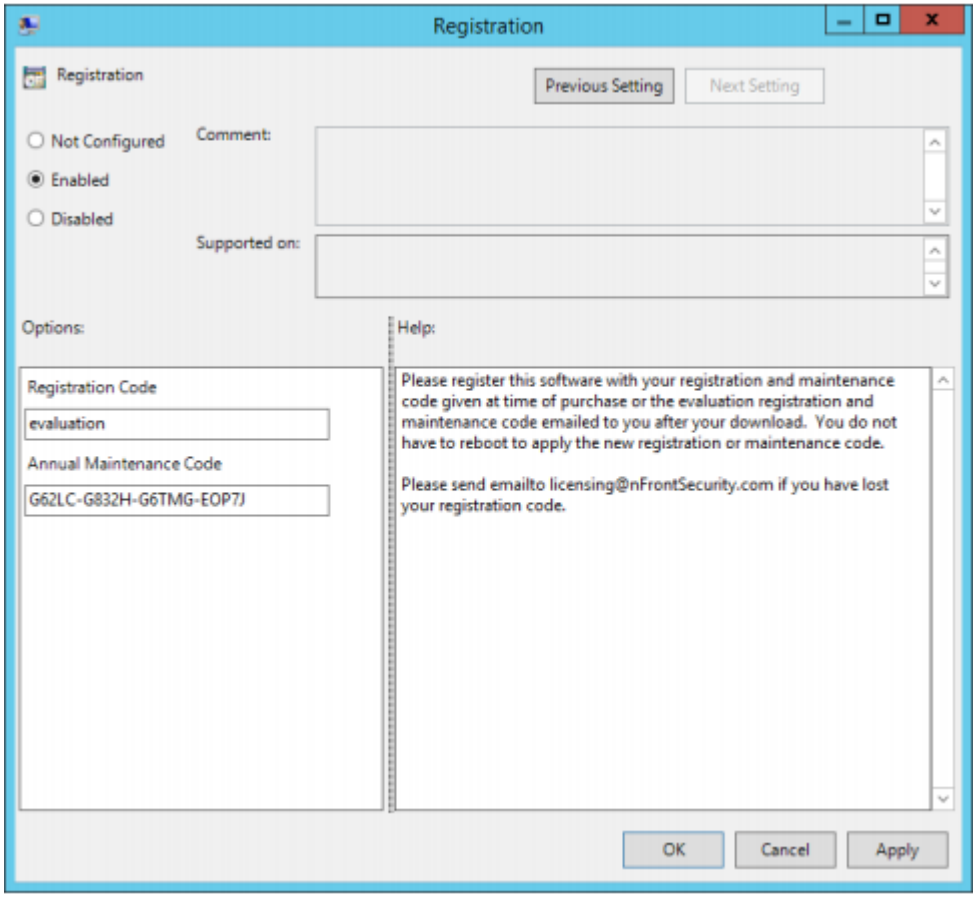
CONFIGURING NFRONT PASSWORD FILTER

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



CONFIGURE REGISTRATION SETTINGS

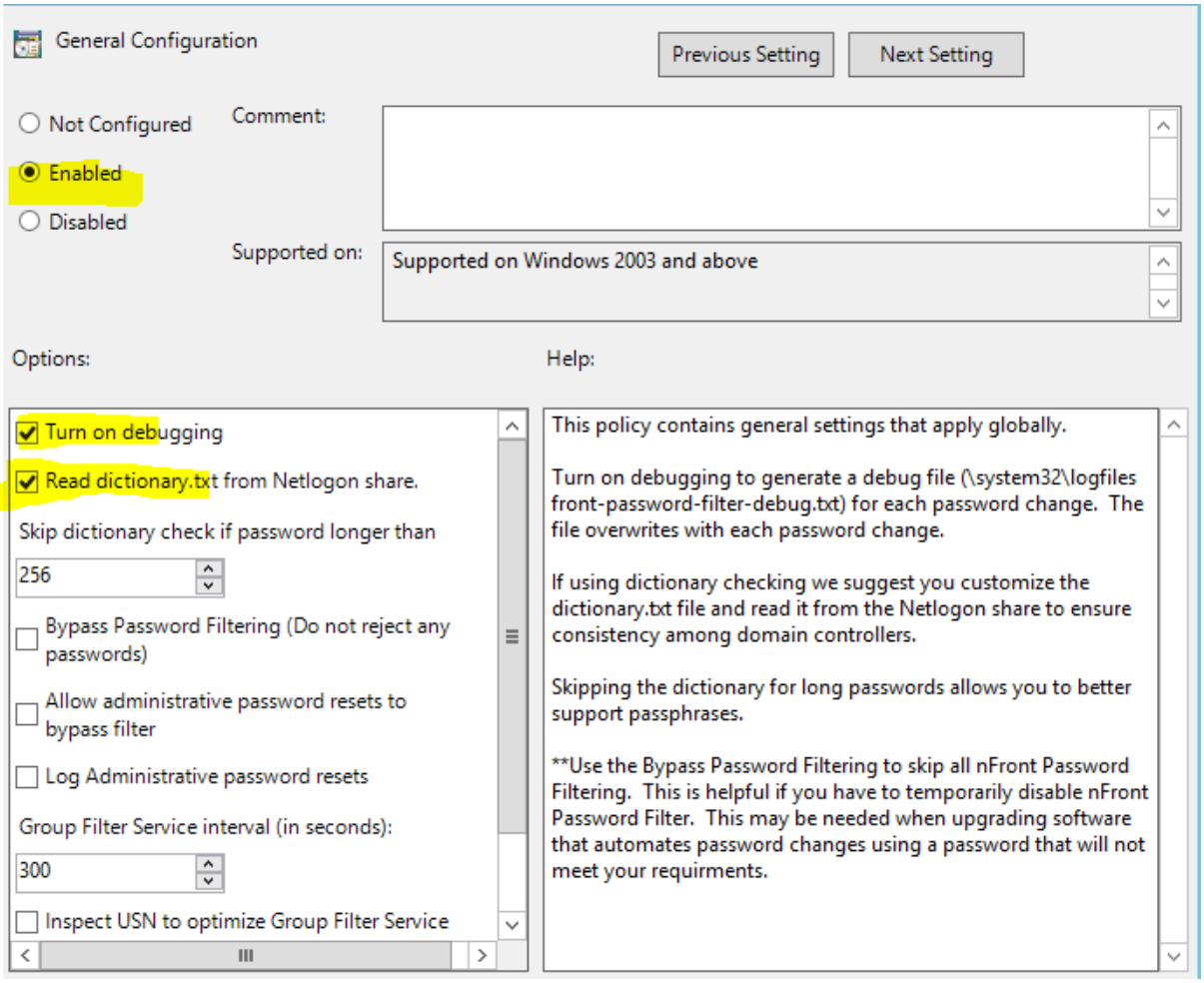
Double-click the Registration policy. Enable the policy and enter the registration code provided.



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.

CONFIGURE GENERAL CONFIGURATION SETTINGS

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



CONFIGURE PASSWORD POLICY SETTINGS

Important Notes:

♣ The Default Password Policy Configuration applies to everyone except the "Excluded Groups or OUs" (at bottom of scrolling list of policy settings).

♣ Other polices allow you to choose groups or OUs to which the policy applies and the groups or OUs which are excluded from the policy. You must apply the policy to at least one group or OU if you configure the policy.

♣ The Default Password Policy Configuration is used for all new account creation.

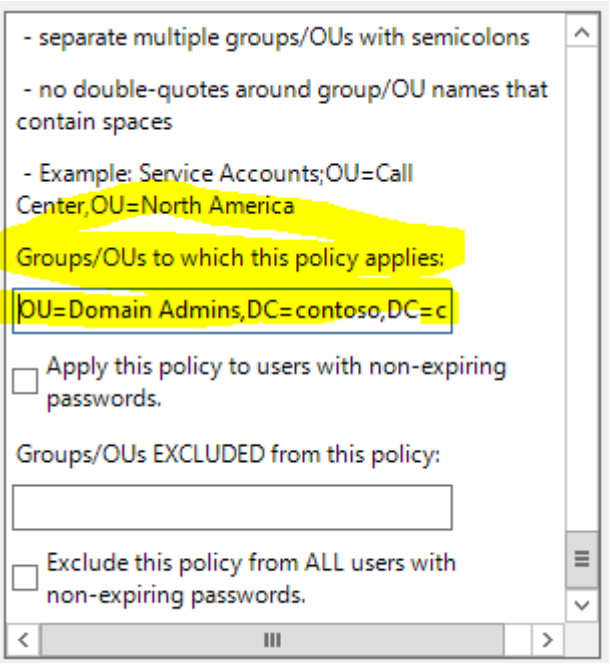
♣ Policies are cumulative just like NTFS permissions. If a user is affected by 2 polices the user's password must meet the requirements of both policies and if the same settings differs between the policies, the most restrictive setting applies.

PASSWORD REQUIREMENTS FOR EACH USER GROUP

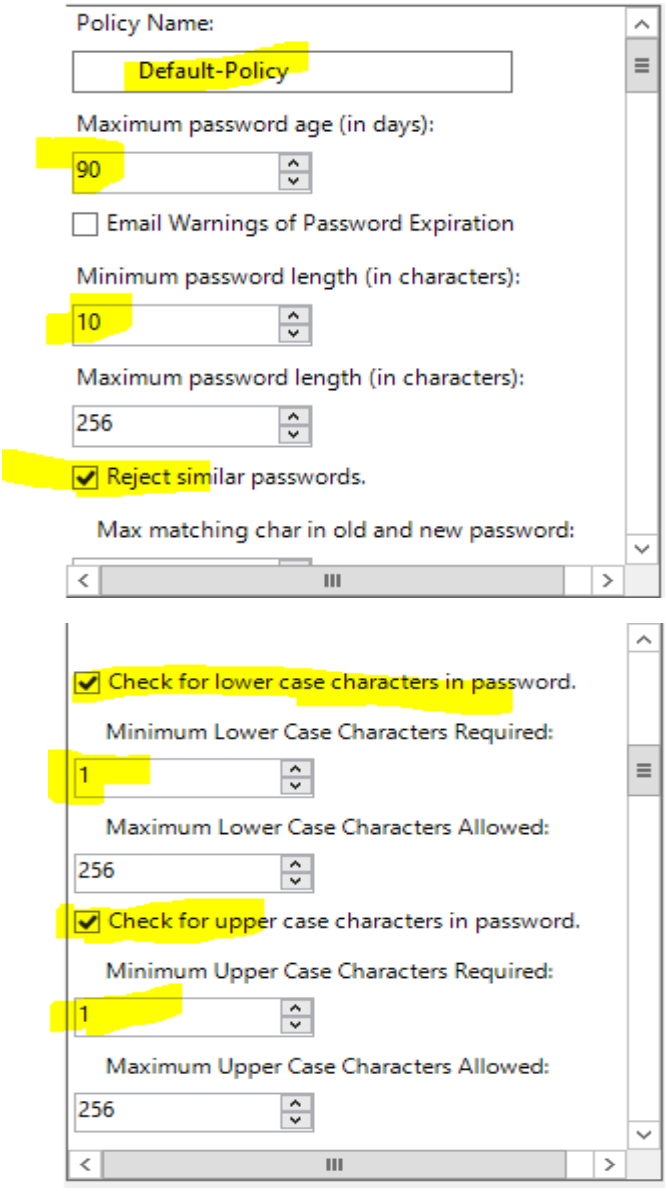
DOMAIN USERS	DOMAIN ADMINS	SERVICE ACCOUNTS
10 Characters	16 Characters	24 Characters
1 Special Character	1 Special Character	1 Special Character
1 number	1 number	1 number
1 lower case letter	1 lower case letter	1 lower case letter
1 upper case letter	1 upper case letter	1 upper case letter

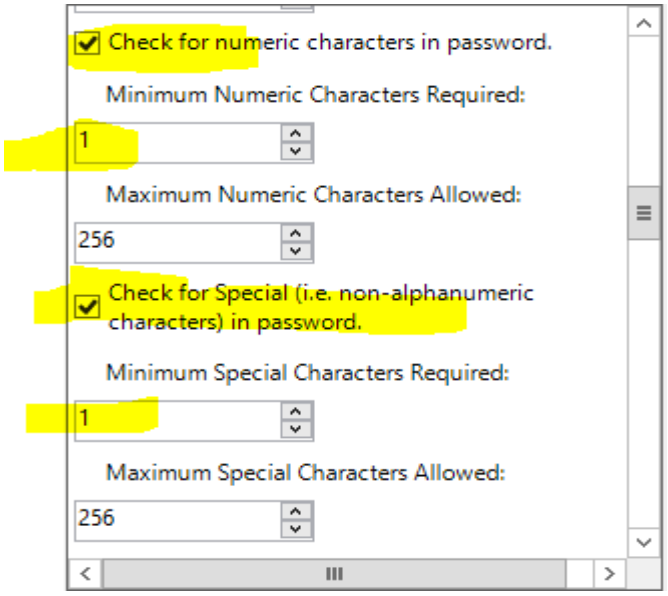
BELOW ARE THE SETTINGS TO BE FOLLOWED FOR EACH USER POLICY

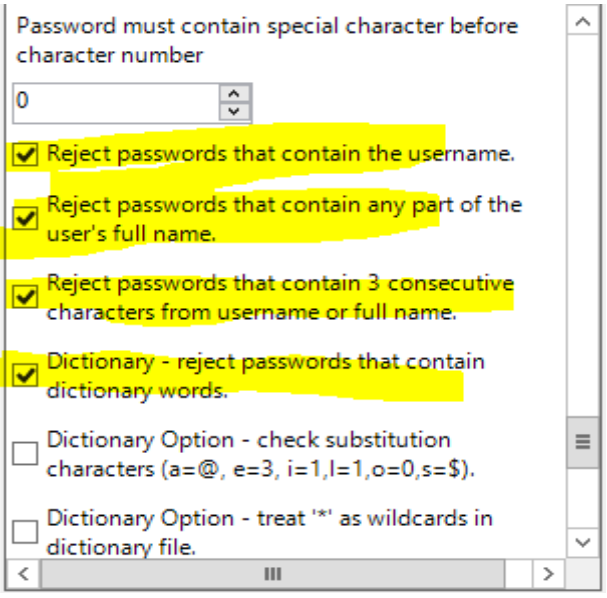
NOTE: EACH POLICY WILL NEED TO BE APPLIED TO THE CORRESPONDING USER OU OR GROUP AS BELOW. YOU ALSO HAVE THE ABILITY TO EXCLUDE CERTAIN GROUPS OR OUS FROM A SPECIFIC POLICY.



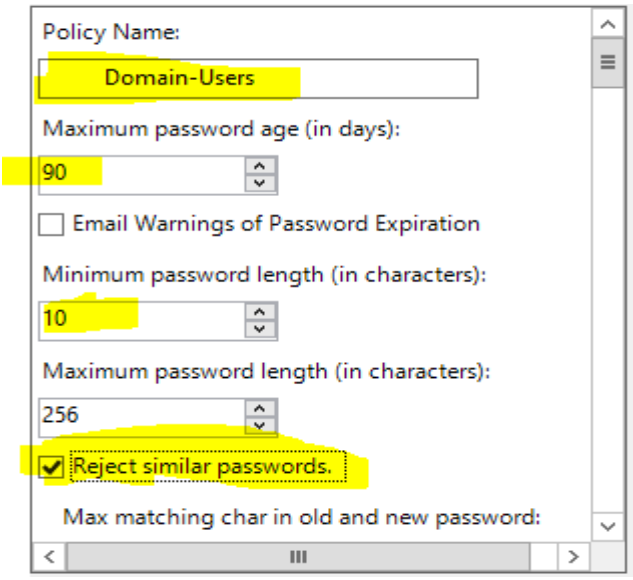
DEFAULT POLICY

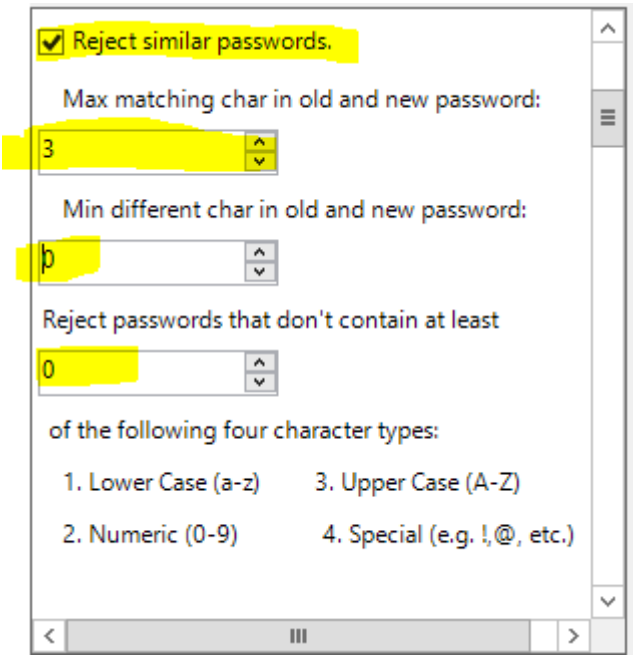


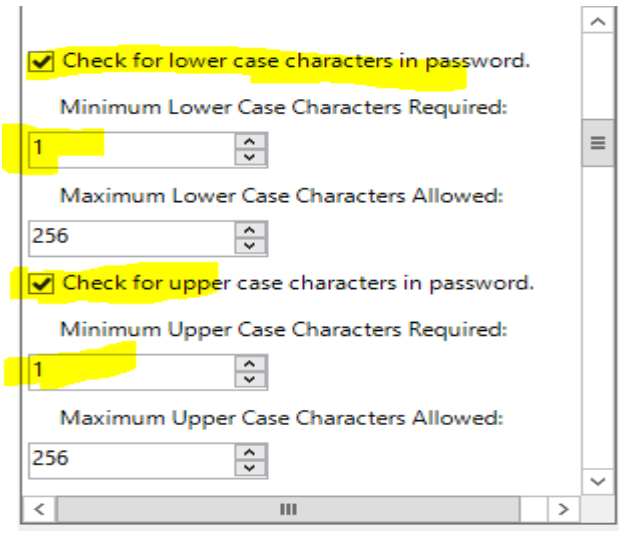

Check for numeric characters in password.
Minimum Numeric Characters Required:
1
Maximum Numeric Characters Allowed:
256
Check for Special (i.e. non-alphanumeric characters) in password.
Minimum Special Characters Required:
1
Maximum Special Characters Allowed:
256

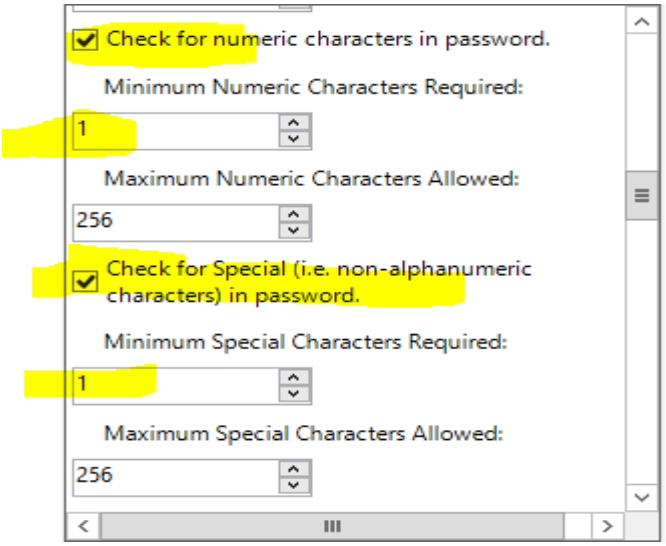

Password must contain special character before character number
0
Reject passwords that contain the username.
Reject passwords that contain any part of the user's full name.
Reject passwords that contain 3 consecutive characters from username or full name.
Dictionary - reject passwords that contain dictionary words.
Dictionary Option - check substitution characters (a=@, e=3, i=1,l=1,o=0,s=$).
Dictionary Option - treat '*' as wildcards in dictionary file.

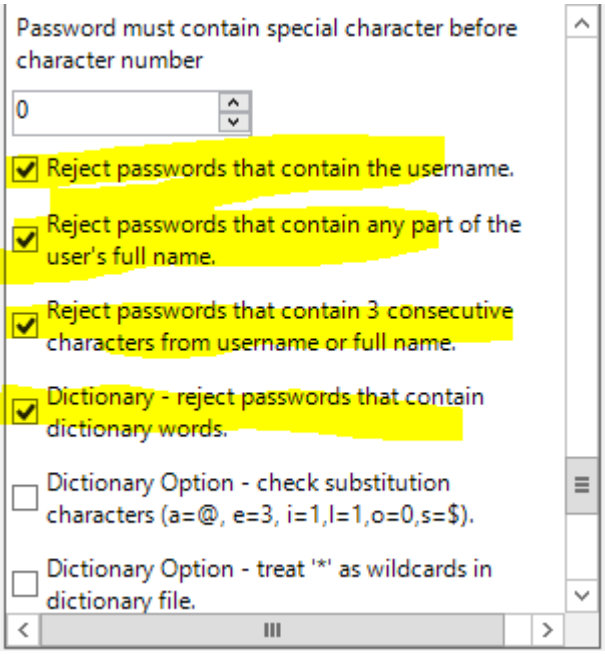
DOMAIN USERS POLICY

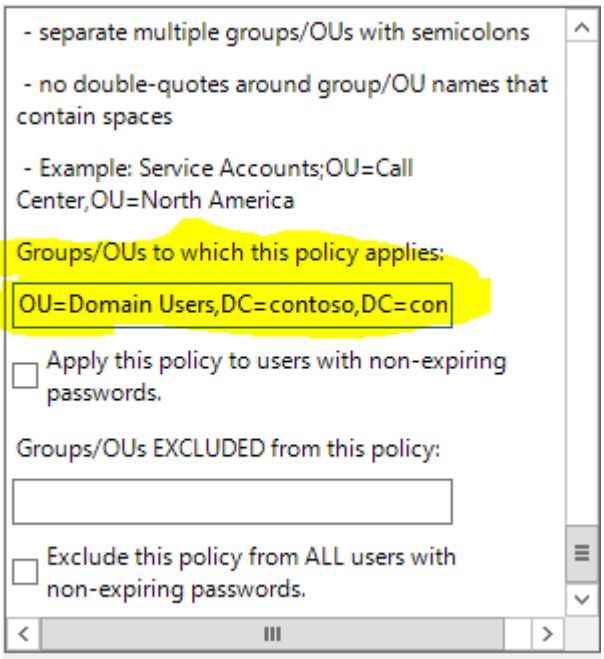




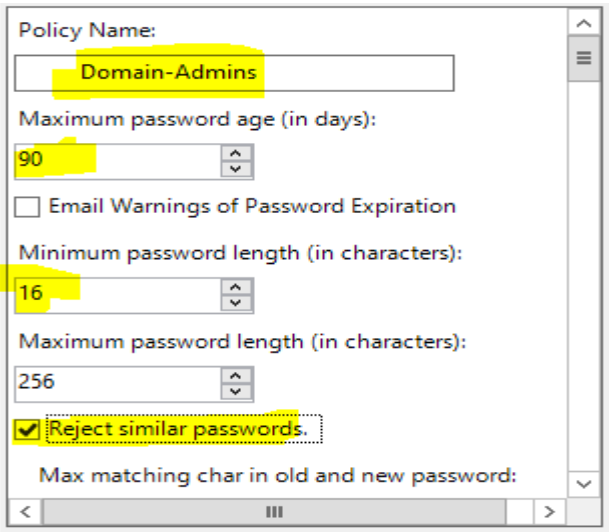


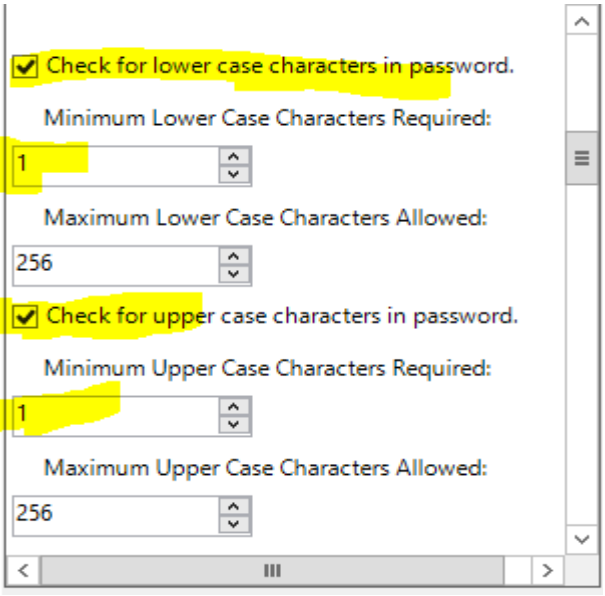

Check for numeric characters in password.
Minimum Numeric Characters Required:
1
Maximum Numeric Characters Allowed:
256
Check for Special (i.e. non-alphanumeric characters) in password.
Minimum Special Characters Required:
1
Maximum Special Characters Allowed:
256

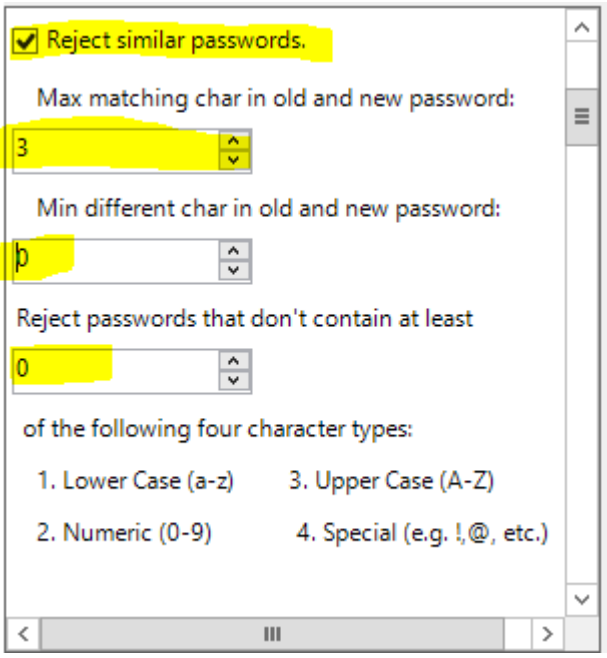

Password must contain special character before character number
0
Reject passwords that contain the username.
Reject passwords that contain any part of the user's full name.
Reject passwords that contain 3 consecutive characters from username or full name.
Dictionary - reject passwords that contain dictionary words.
Dictionary Option - check substitution characters (a=@, e=3, i=1,l=1,o=0,s=$).
Dictionary Option - treat '*' as wildcards in dictionary file.

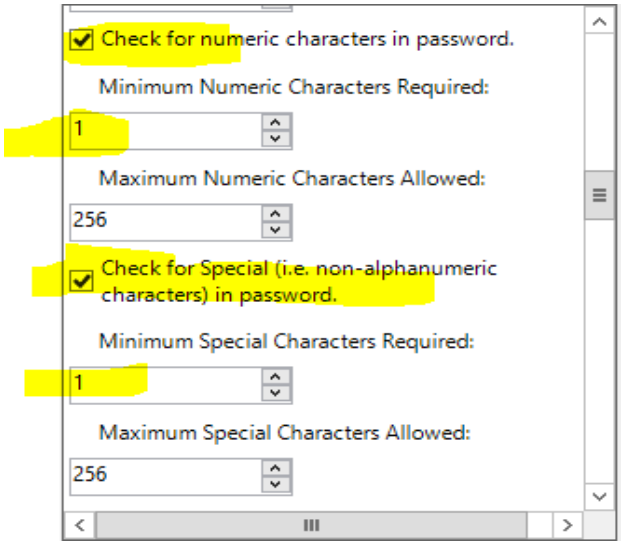


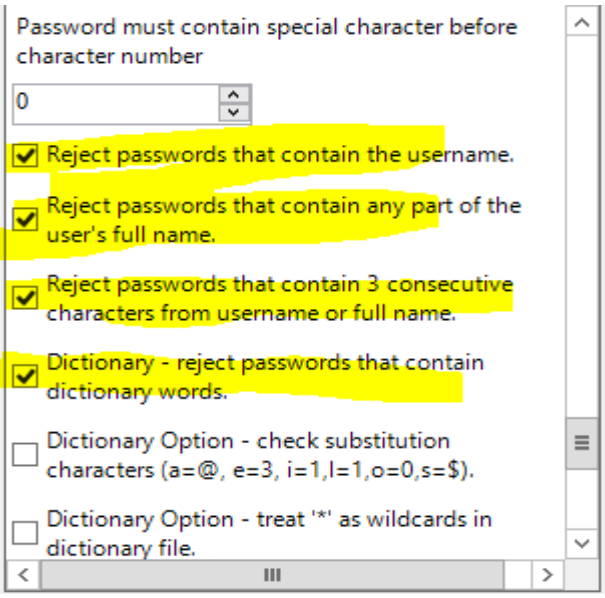
DOMAIN ADMINS POLICY

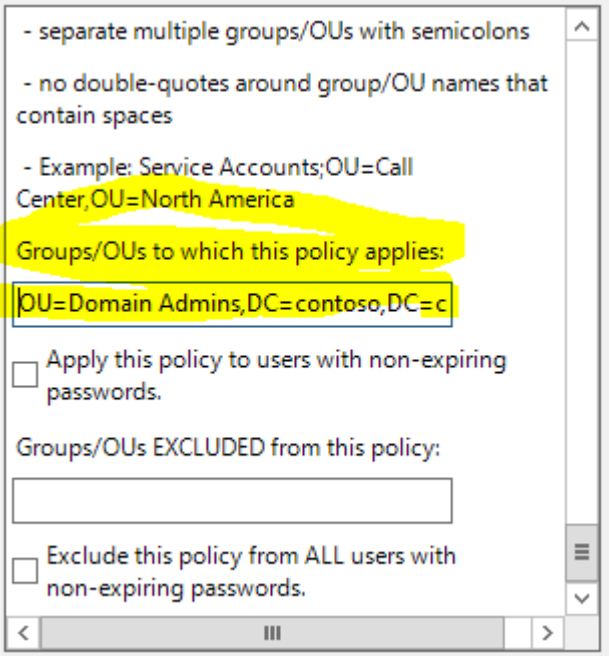



Check for lower case characters in password.
Minimum Lower Case Characters Required:
1
Maximum Lower Case Characters Allowed:
256
Check for upper case characters in password.
Minimum Upper Case Characters Required:
1
Maximum Upper Case Characters Allowed:
256

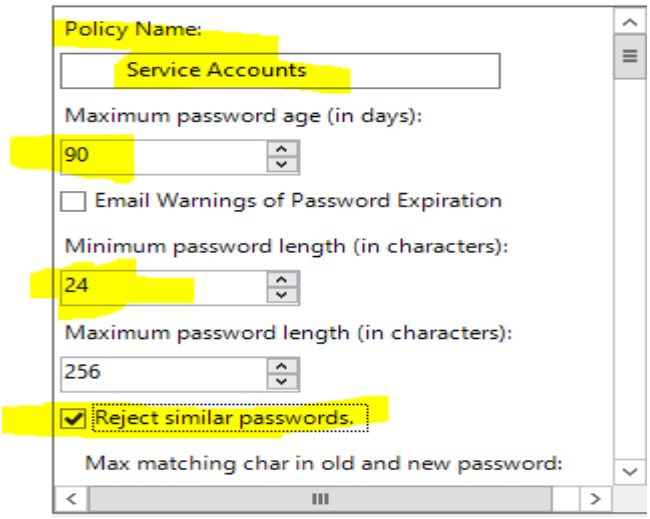

Reject similar passwords.
Max matching char in old and new password:
3
Min different char in old and new password:
0
Reject passwords that don't contain at least
0
of the following four character types:
1. Lower Case (a-z)
3. Upper Case (A-Z)
2. Numeric (0-9)
4. Special (e.g. !,@, etc.)

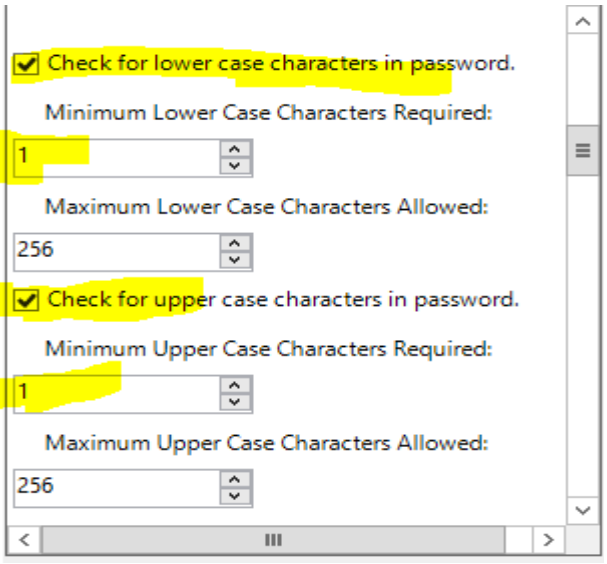

Check for numeric characters in password.
Minimum Numeric Characters Required:
1
Maximum Numeric Characters Allowed:
256
Check for Special (i.e. non-alphanumeric characters) in password.
Minimum Special Characters Required:
1
Maximum Special Characters Allowed:
256

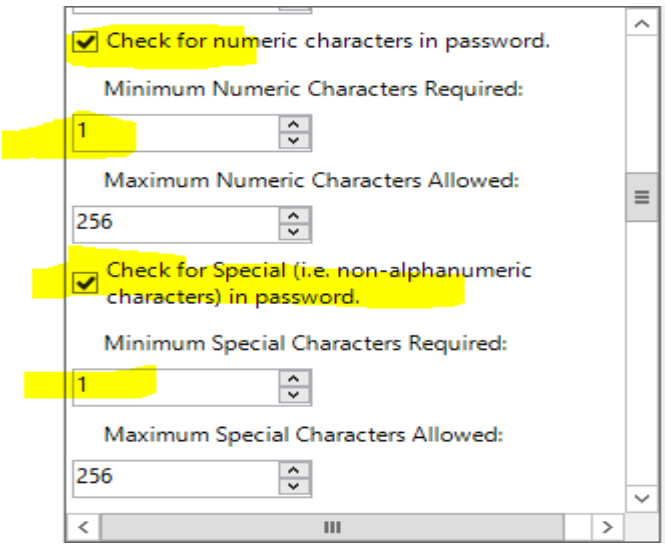

Password must contain special character before character number
0
Reject passwords that contain the username.
Reject passwords that contain any part of the user's full name.
Reject passwords that contain 3 consecutive characters from username or full name.
Dictionary - reject passwords that contain dictionary words.
Dictionary Option - check substitution characters (a=@, e=3, i=1,l=1,o=0,s=$).
Dictionary Option - treat '*' as wildcards in dictionary file.

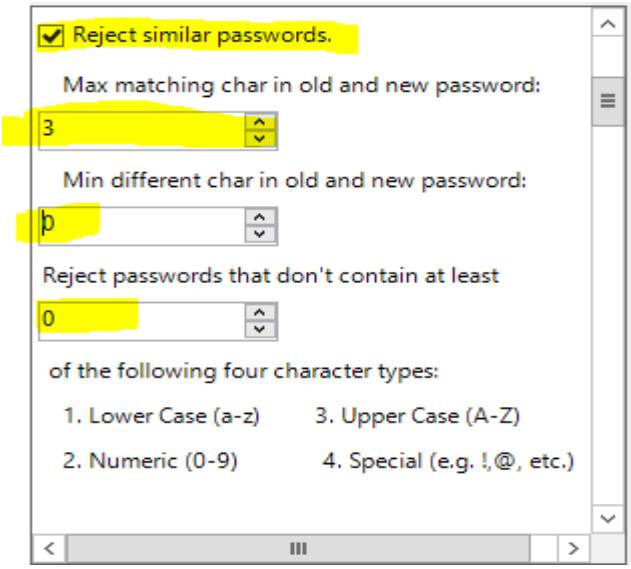

- separate multiple groups/OUs with semicolons
- no double-quotes around group/OU names that contain spaces
- Example: Service Accounts;OU=Call Center,OU=North America
Groups/OUs to which this policy applies:
OU=Domain Admins,DC=contoso,DC=c
Apply this policy to users with non-expiring passwords.
Groups/OUs EXCLUDED from this policy:
Exclude this policy from ALL users with non-expiring passwords.

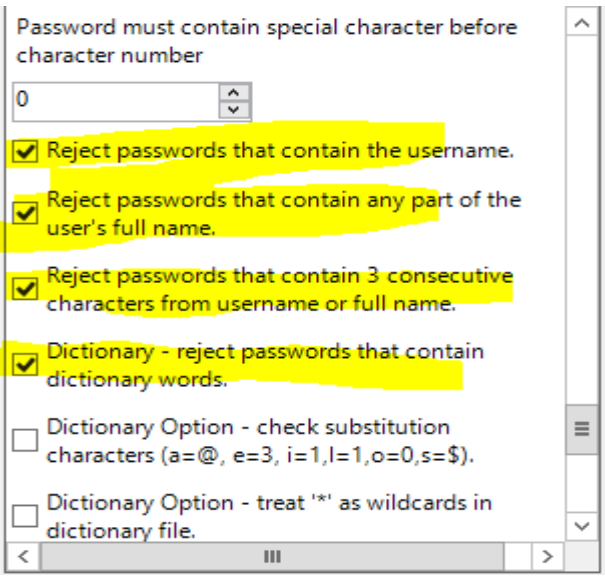
SERVICE ACCOUNT POLICY

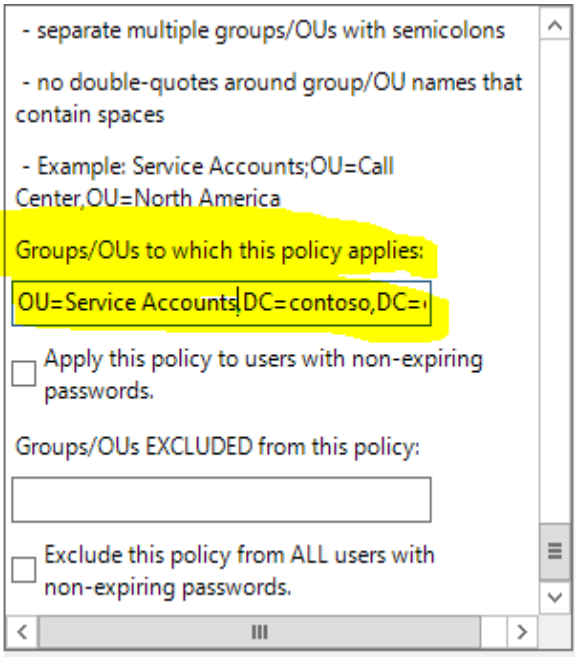







Reject similar passwords.
Max matching char in old and new password:
3
Min different char in old and new password:
0
Reject passwords that don't contain at least
0
of the following four character types:
1. Lower Case (a-z)
3. Upper Case (A-Z)
2. Numeric (0-9)
4. Special (e.g. !,@, etc.)


Password must contain special character before character number
0
Reject passwords that contain the username.
Reject passwords that contain any part of the user's full name.
Reject passwords that contain 3 consecutive characters from username or full name.
Dictionary - reject passwords that contain dictionary words.
Dictionary Option - check substitution characters (a=@, e=3, i=1,l=1,o=0,s=$).
Dictionary Option - treat '*' as wildcards in dictionary file.


- separate multiple groups/OUs with semicolons
- no double-quotes around group/OU names that contain spaces
- Example: Service Accounts;OU=Call Center,OU=North America
Groups/OUs to which this policy applies:
OU=Service Accounts,DC=contoso,DC=
Apply this policy to users with non-expiring passwords.
Groups/OUs EXCLUDED from this policy:
Exclude this policy from ALL users with non-expiring passwords.

TROUBLESHOOTING

IFIFFF

8.1 Common Problems

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

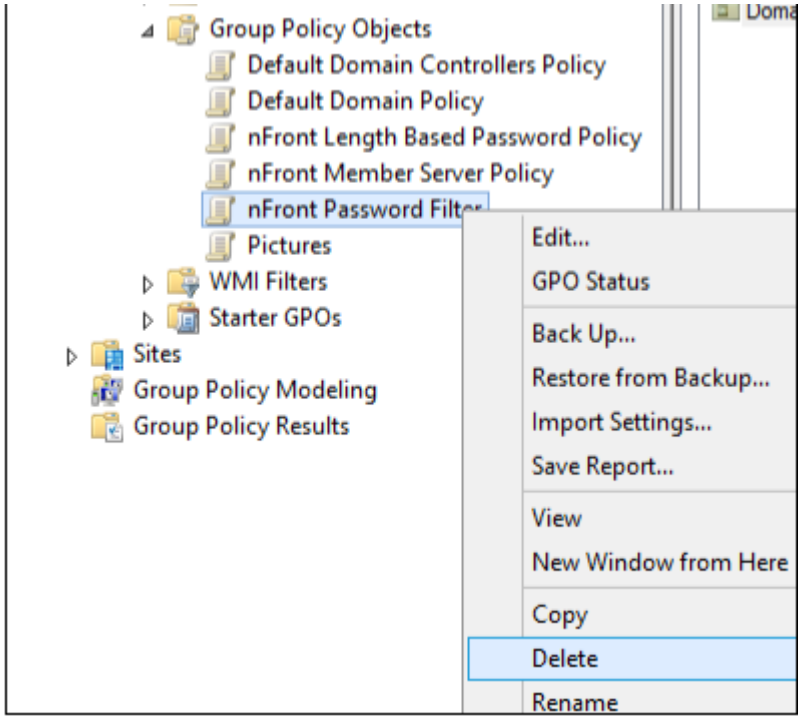
NOTE: IF DEBUG FILE IS MISSING, ATTEMPT A PASSWORD CHANGE WITH ANY DOMAIN USER ACCOUNT AND THIS WILL GENERATE THE DEBUG LOG FILE

UNINSTALLATION INSTRUCTIONS

If you would like to delete the GPO with the nFront Settings

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

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



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.

After nFront GPO has been deleted, navigate to Start + Control Panel + Programs + Uninstall a program + Uninstall nFront Password Filter.

BEST PRACTICES AND RECOMMENDATIONS:

- After installation has been successful, create a test user group or ou and test the different policies with several accounts to make sure
  - nFront GPO replication is working between all Domain Controllers
  - Policies are being applied correctly
  - Policy exclusions, if any, are working
  - Test password changes for each test case and validate that all password requirements are being met. Refer to nFront error log for any issues related to testing
  - Test dictionary file and always refer to nFront error log for issues related to testing

- Validate that all users and accounts are in correct OU/Groups before enterprise wide deployment.

- Send out nfront user communication email alerting all users of new policy updates and new password requirements. Recommended advisement time frame is at least 1 week before deployment.

- Periodically review dictionary file and update accordingly with passwords that do not meet recommended password criteria.