PASSWORD COMPLEXITY MANAGER

ADMINISTRATOR'S GUIDE

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION

DISCLAIMER - Tools4ever will not be held responsible for the outcome or consequences resulting from your actions or usage of the informational material contained in this user guide. Responsibility for the use of any and all information contained in this user guide is strictly and solely the responsibility of that of the user.

www.tools4ever.com

Contents

1. Introduction

Welcome to Password Complexity Manager (from here on the abbreviation 'PCM' will be used). PCM is an solution which allows you to manage the complexity of the Active Directory passwords.
Windows only supports default password complexity rules which can be turned on or off for the entire domain. PCM allows you to configure the password complexity rules and tailor them to your specific needs, and allows you to configure password complexity rules for specific organizational units.

PCM offers:

- Optimal security

By extending the standard Windows Active Directory password complexity rules, administrators can implement a more complete password policy. It is possible to configure multiple security levels for different types of end users, based on their function and role within the organization. It is also possible to flexibly configure the complexity requirements of the passwords. All this significantly improves the security of the network.

- User friendly interface

End users will be visually informed whether or not their password satisfies the password complexity rules. While typing their new password, they will be shown which rules are satisfied in the form of a checklist. End users will immediately see which rules are not yet satisfied, unlike the long error message Windows normally shows.

- Compliancy

The standard available complexity rules with a windows domain are often too limited to satisfy demands made by other applications, such as HIPA or SOX. With PCM you can configure all possible requirements.

- Simple installation

PCM is a standard product and can be easily installed and configured by a system administrator with an hour.

2. How does PCM work?

2.1. Concept

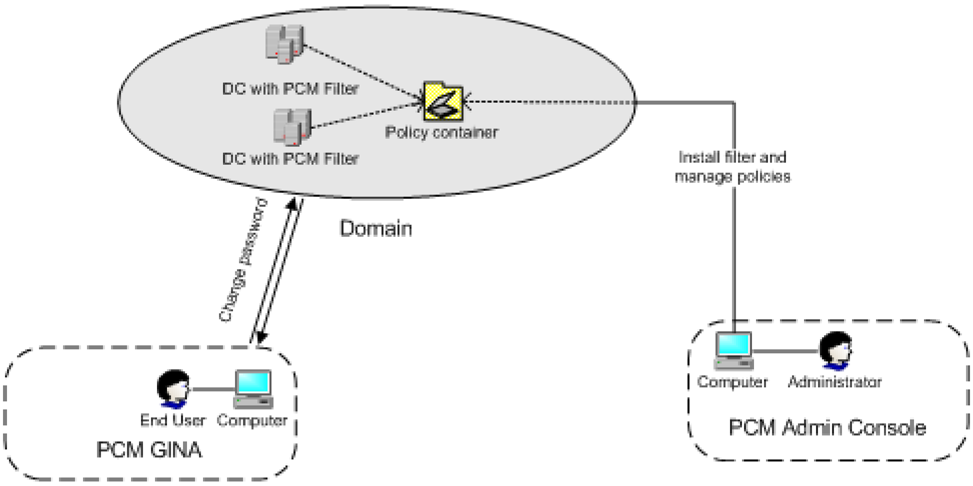
The default security policy options and the granularity in Windows are rather limited, the purpose of PCM is to offer more options and better granularity.

Compared to the default complexity rules of a windows domain, PCM offers three additional features.

- PCM allows you to configure the password complexity per OU in the domain. This allows you to distinguish between different end users and the degree of password complexity that you require of them.
- PCM offers all possible combinations of requirements. Such as providing a list of words that are not allowed in passwords or to demand a password matches a regular expression.
- PCM provides the end user with information about their password requirements during the password reset. This makes sure that end user instantly knows whether or not the password satisfies the complexity requirements.
- PCM seamlessly integrates with the domain controllers of the network and adheres to Microsoft's strict requirements for domain controller integration. The basic operation of the Microsoft password management remains unchanged and PCM in no way reduces the security levels of the Microsoft password management.

2.2. Architecture

The main architecture of PCM is shown in the figure below:



PCM consist of three main components, knowingly:

- The PCM Admin console
- The PCM Policy container
- The PCM GINA
- The PCM Filter

2.2.1. The PCM Admin Console

The PCM Admin Console is used by Administrators to install and manage the PCM Filter on Domain Controllers (this will be explained within the chapter: How to install PCM).
When PCM is installed completely, the PCM Admin Console can be used to configure the password complexity policies.
Configuring password complexity policies entails activating and configuring the password requirements and specifying to which users, organizational unit or domain the policy applies.

2.2.2. The PCM Policy container

Although not an actual software component, the policy container is an important object. It is an object in the Active directory which is created when you install PCM on a domain (see chapter: How to install PCM).
The object is named 'T4ePasswordPolicy' and is used to store the policies. The PCM Policy container isstored in the AD with the following path: "Program Data\Tools4ever\Password Complexity Manager". The other components will access the policy container to load the policies, but only the Admin console is able to save the policies.

2.2.3. The PCM Filter

The PCM Filter is a DLL file, that is installed on the domain controllers that have to apply the password complexities policies. Before a password change request is processed by the domain controller, the password will be validated by the Password Complexity Filter.

The filter loads the policies from the policy container in the Active Directory and refreshes the policy list every 5 minutes.

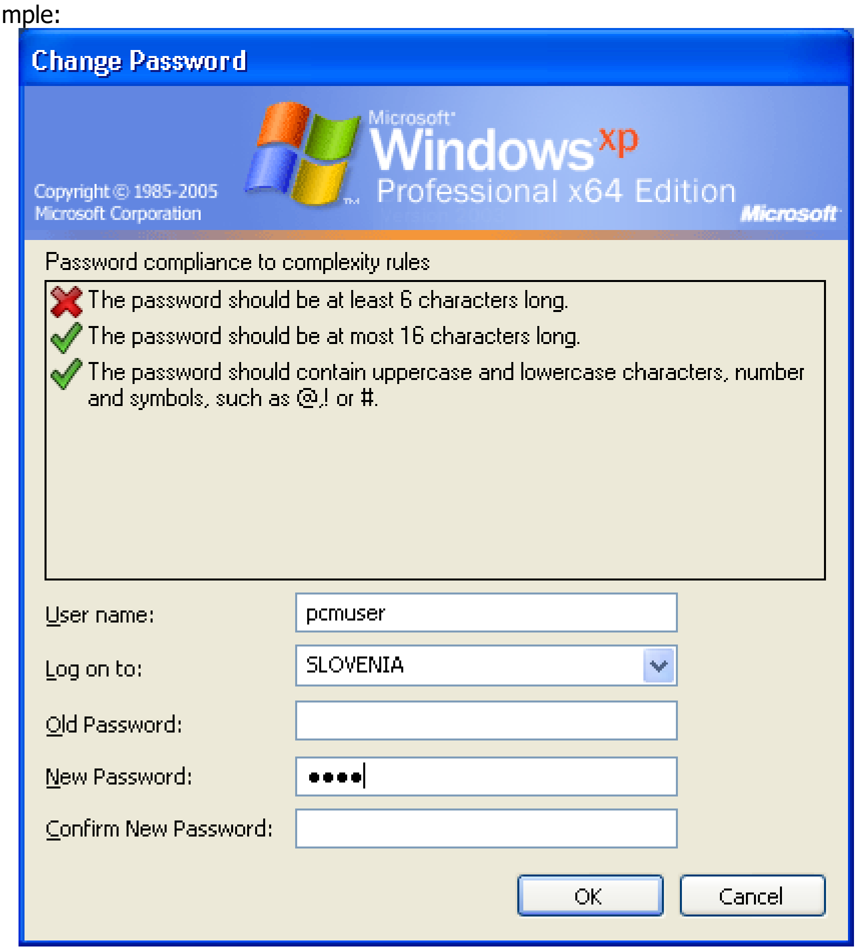
Should the filter be unable to match the user name to a policy, it will use the configured Default Behaviour setting to determine the course of action.

2.2.4. The PCM GINA

The PCM GINA is a visual aid for end users using machines running Windows XP and lower. It shows the complexity rules for the new password and to which of the rules it already satisfies. The PCM GINA is an extension on the functionality of the normal Windows logon software (GINA architecture). The PCM GINA only affects the change password dialog. The implementation is based on the concept 'GINA Chaining', which means that it is compatible with other GINA extensions, such as the SSRPM GINA.

> Note: The password requirement that checks the similarity between a new password and the old password is only possible if the GINA is installed

For example:



Change Password

Password compliance to complexity rules

☒ The password should be at least 6 characters long.

✓ The password should be at most 16 characters long.

✓ The password should contain uppercase and lowercase characters, number and symbols, such as @,! or #.

User name: pcmuser

Log on to: SLOVENIA

Old Password:

New Password: ●●●●

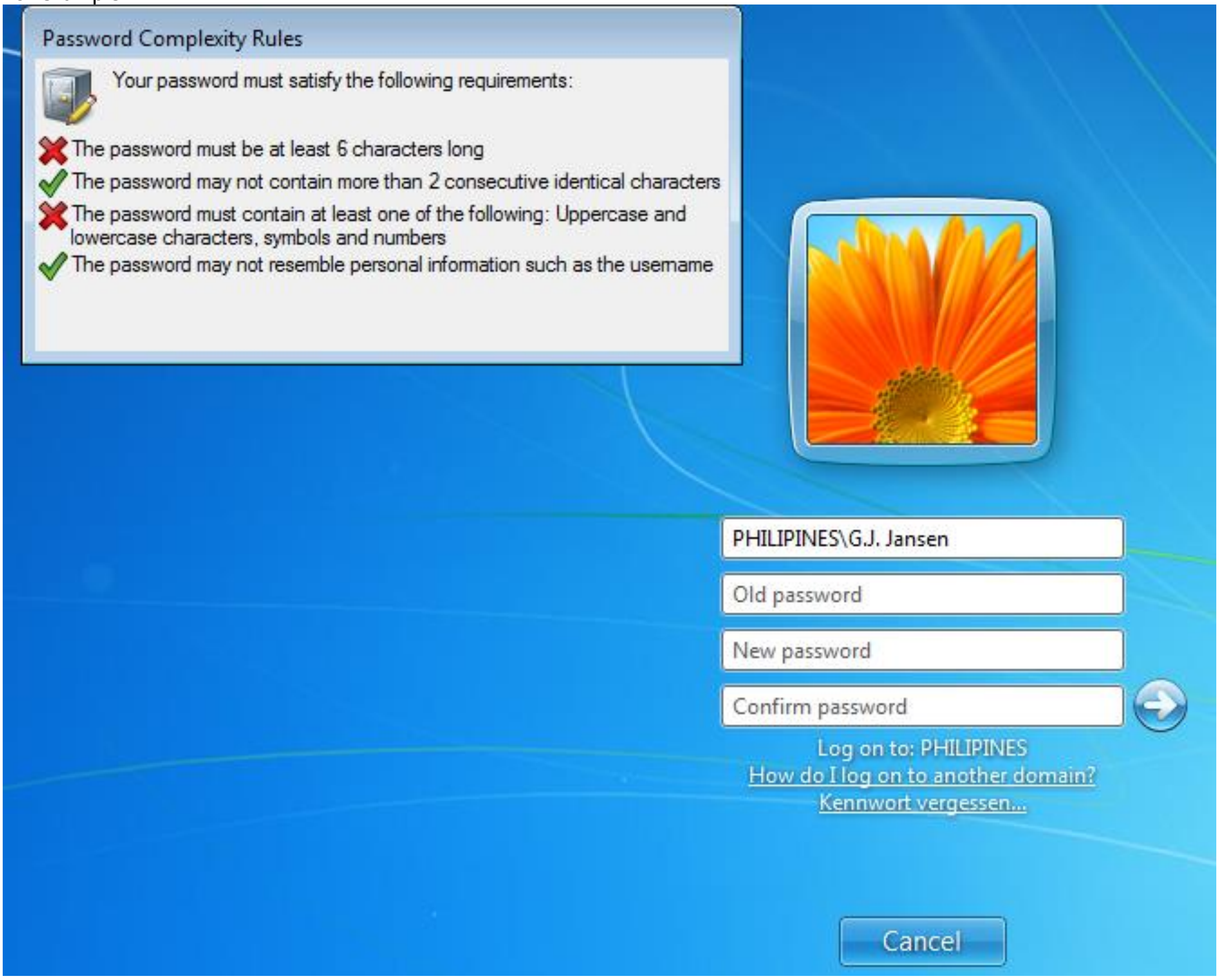
Confirm New Password:

2.2.5. The PCM Credential Provider

The PCM Credential Provider is a visual aid for end users using machines running on Windows Vista and higher. It shows the complexity rules for the new password and to which of the rules it already satisfies. The PCM Credential Provider is an extension on the functionality of the normal Windows logon software . The PCM Credential Provider only affects the change password dialog.

Note: The password requirement that checks the similarity between a new password and the old password is only possible if the Credential provider is installed

For example:



Password Complexity Rules

Your password must satisfy the following requirements:

- ✗ The password must be at least 6 characters long
- ✓ The password may not contain more than 2 consecutive identical characters
- ✗ The password must contain at least one of the following: Uppercase and lowercase characters, symbols and numbers
- ✓ The password may not resemble personal information such as the username

PHILIPINES\G.J. Jansen

Old password

New password

Confirm password

Log on to: PHILIPINES

How do I log on to another domain?

Kennwort vergessen...

Figure: The PCM Credential Provider DLL

2.2.6. The PCM COM Object

The PCM COM Object can used to get the descriptions of the password complexity rules for a specific user.
It is mainly used by Self Service Reset Password Management (SSRPM), to display password complexity rules in its web interface.

The COM object files can be found in the PCM subdirectory: 'COM' which is located within your installation directory (this is by default: 'C:\Program Files\Tools4ever\Password Complexity Manager).

By default the COM objects are registered automatically on the same machine where the PCM Admin console is installed. If you need to register the COM object on another machine, you can use the batch files 'Register.bat' or 'Registerx64.bat', depending on whether you require the 32-bit or the 64-bit COM object. You can also use the command: "regsvr32 FILENAME".

3. How to install PCM

3.1. Software requirements

Operating Systems of the PCM Admin Console:

- Windows XP (all 32-bit and x64 versions)
- Windows 2003 (all 32-bit and x64 versions)
- Windows Vista (all 32-bit and x64 versions)
- Windows 7 (all 32-bit and x64 versions)
- Windows 2008 (all 32-bit and x64 versions)
- Windows 2012 (all 32-bit and x64 versions)

Operating Systems of the PCM Filter:

- Windows 2003 (all 32-bit and x64 versions)
- Windows 2008 (all 32-bit and x64 versions)
- Windows 2012 (all 32-bit and x64 versions)
-

Operating Systems of the PCM GINA:

- Windows XP (all 32-bit and x64 versions)
- Windows 2003 (all 32-bit and x64 versions)

Operating Systems of the PCM Credential Provider:

- Windows Vista (all 32-bit and x64 versions)
- Windows 7 (all 32-bit and x64 versions)
- Windows 2008 (all 32-bit and x64 versions)
- Windows 8 (all 32-bit and x64 versions)
- Windows 10 (all 32-bit and x64 versions)

3.2. General installation

To install PCM, run the PCM setup executable, 'PasswordComplexityManager.exe', which is available for download from the Tools4ever website http://www.tools4ever.com. This executable contains all the needed PCM Software Components: the PCM Admin Console, the PCM Filter and the PCM GINA. When the download is finished you can run 'PasswordComplexityManager.exe', which will start the PCM Setup Wizard. The wizard will guide you through the installation process of PCM, which only installs the PCM Admin Console.

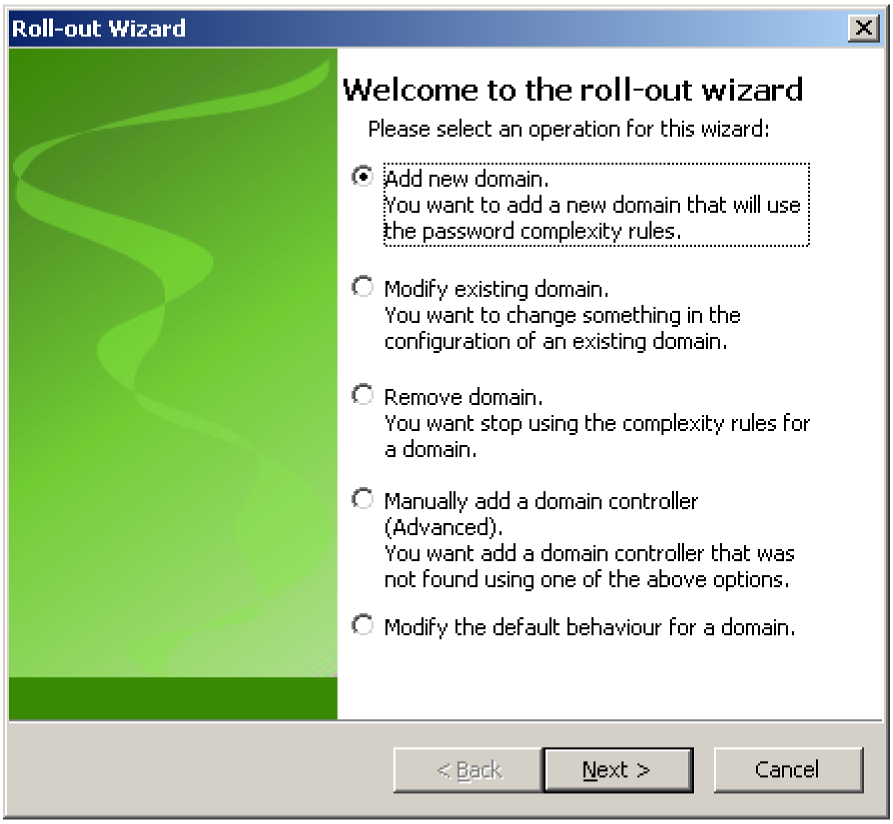
> Note: The user account which you'll use to install PCM must have administrative privileges on the target computer on which you want to install PCM.

Once you've finished the installation of PCM you can start the PCM Admin Console to continue with the installation and configuration of PCM. When you've started the PCM Admin Console for the first time, the Roll-out Wizard will be shown, which guides you through the installation of the PCM Filter.

3.3. The PCM Filter

You can install the filter on the domain controllers using the PCM Roll-out Wizard.

> Note: After the installation of the filter the domain controllers must be rebooted. It is also recommended to reboot a domain controller after uninstalling the filter.



Roll-out Wizard

Welcome to the roll-out wizard

Please select an operation for this wizard:

● Add new domain.
You want to add a new domain that will use the password complexity rules.

○ Modify existing domain.
You want to change something in the configuration of an existing domain.

○ Remove domain.
You want stop using the complexity rules for a domain.

○ Manually add a domain controller (Advanced).
You want add a domain controller that was not found using one of the above options.

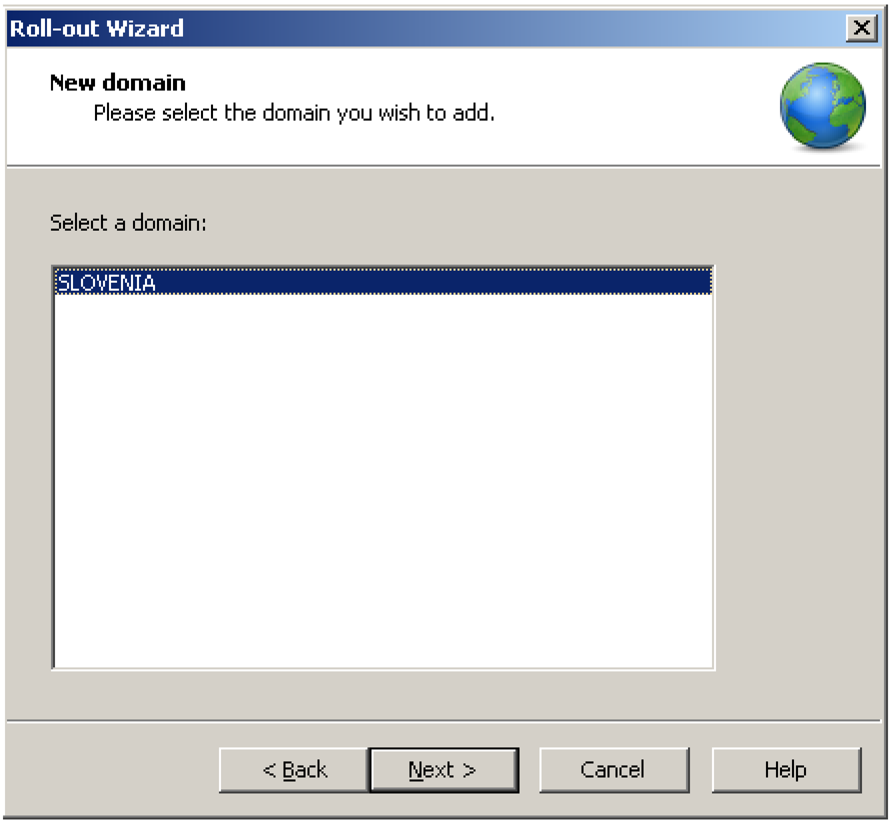
○ Modify the default behaviour for a domain.

Installation process options :

- Add new domain: This will create the policy container in the Active Directory and install the filter on the specified domain controllers.
- Modify existing domain: Add/Remove the filter to/from specified domain controllers.
- Remove domain: Remove the policy container from the Active Directory and uninstalls the filter from the domain controllers.
- Manually add a domain controller: If for some reason a domain controller does not show up in the Add New Domain wizard or the modify wizard, you can add the domain controller manually here.
- Modify default behaviour: Change the default behaviour of the domain, meaning how a domain should handle password change requests for users that do not match to any policy. You can specify whether passwords change requests should be denied or accepted in that case.

If you are installing PCM for the first time you should select "Add new domain" and click next.

First you should select on which domain you want to install PCM.



Roll-out Wizard

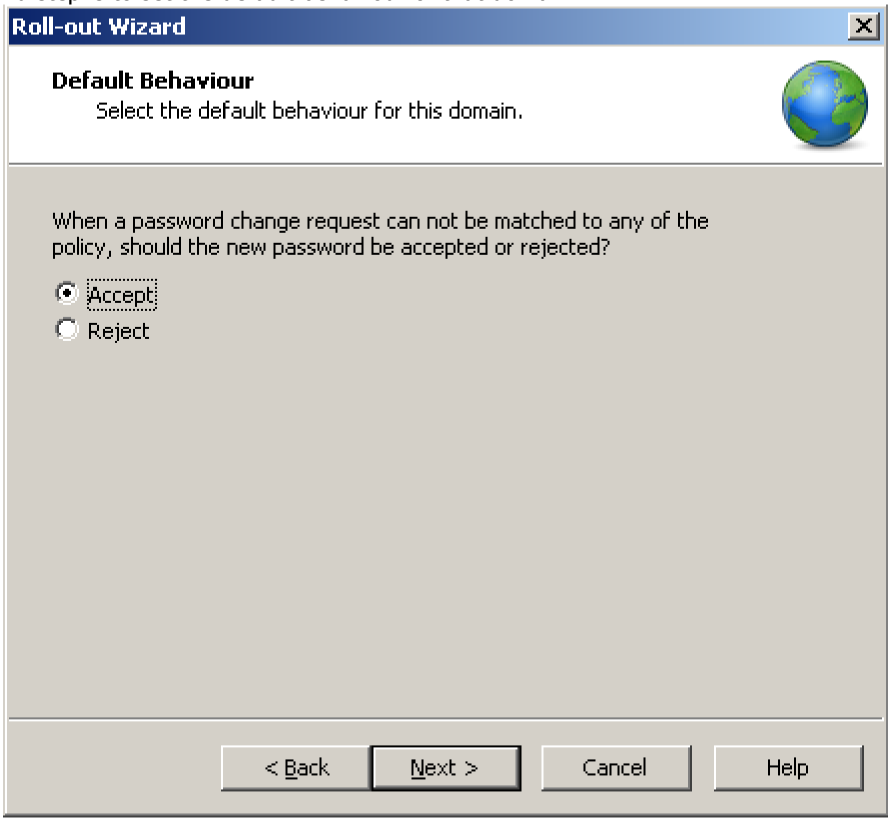
New domain

Please select the domain you wish to add.

Select a domain:

SLOVENIA

The second step is to set the default behaviour of that domain.



Roll-out Wizard

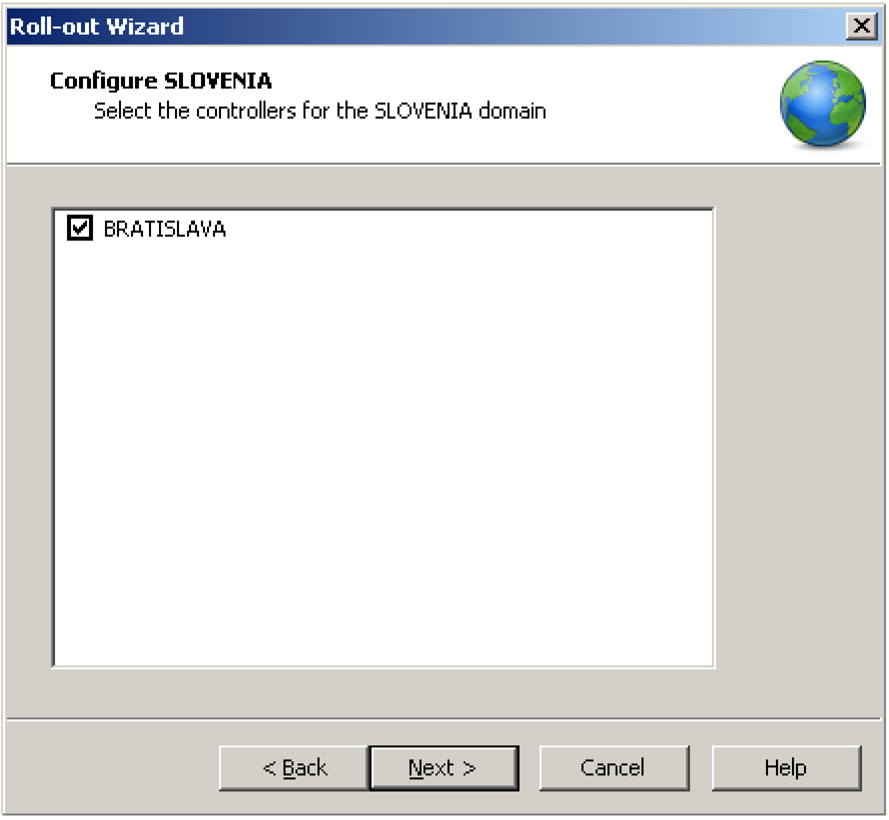
Default Behaviour

Select the default behaviour for this domain.

When a password change request can not be matched to any of the policy, should the new password be accepted or rejected?

● Accept
○ Reject

The third step is to select on which domain controllers the filter should be installed.



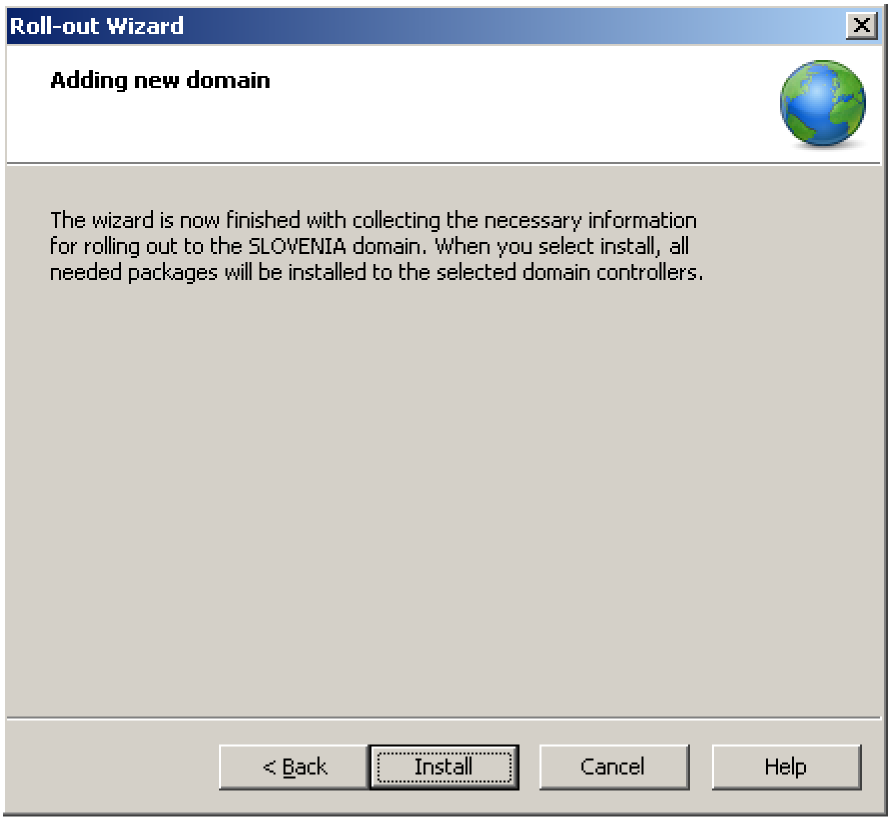
Roll-out Wizard

Configure SLOVENIA

Select the controllers for the SLOVENIA domain

☑ BRATISLAVA

After this the roll-out wizard is ready to install the policy container, set the default behaviour and install the filter. If you are sure everything is correct, click the install button. If not, you can go back and change the settings or cancel the installation.

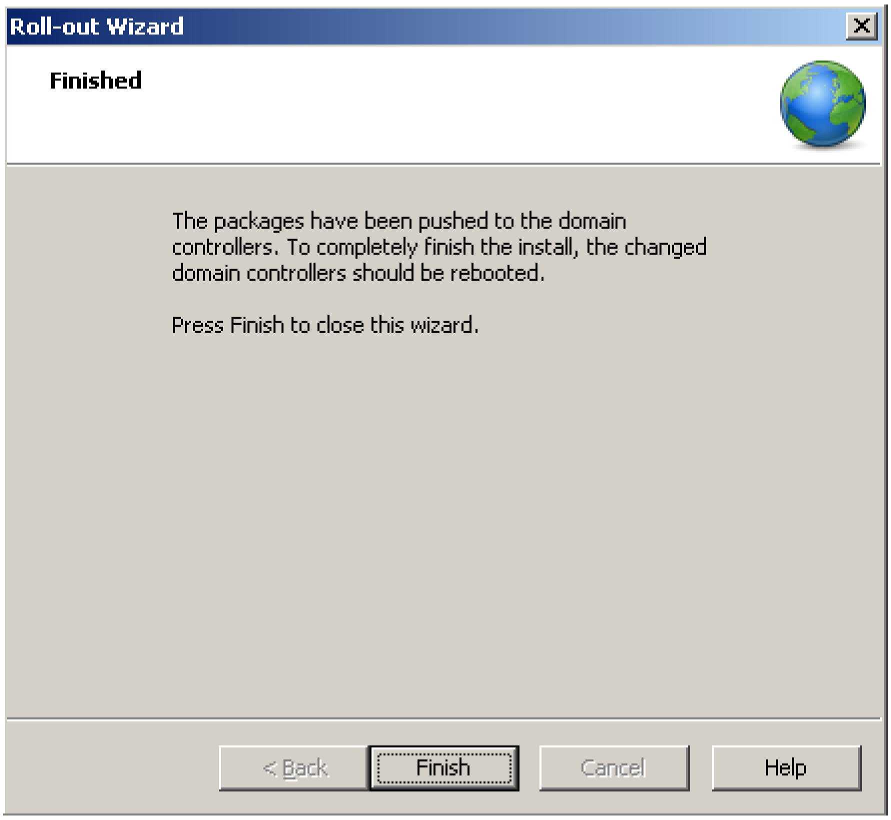


Roll-out Wizard

Adding new domain

The wizard is now finished with collecting the necessary information for rolling out to the SLOVENIA domain. When you select install, all needed packages will be installed to the selected domain controllers.

During the installation the rollout wizard willl display a status bar, followed by the Finished dialog.
If errors occurred during install it will be displayed here, you can check the log window for more specific information about the errors. But if all went well it will look like this.



The packages have been pushed to the domain controllers. To completely finish the install, the changed domain controllers should be rebooted.

Press Finish to close this wizard.

3.3.1. Technical Details

The filter installation procedure is as follows:
1. Create a policy container object in the Active Directory. The object is named “T4ePasswordPolicy” and is stored in the following OU: “Program Data\Tools4ever\Password Complexity Manager”.
2. Copy the filter DLL file to the specified domain controllers. The file will be placed in the system32 folder.
3. Register the DLL as a notification package. This mean adding the file name (without the extension) to the registry key: “HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages”
4. Set registry values to configure the filter. For this we use the registry key: “HKLM\Software\Tools4ever\Password Complexity Manager\PCM Filter”
5. Create a license container object in the Active Directory. The object is named “T4ePcmLicenses” and is stored in the following OU: “Program Data\Tools4ever\Password Complexity Manager”.

3.4. The PCM GINA

The GINA can be installed manually or through distributed installation.

Manual

To perform a manual installation, you must run the PCM GINA Installer (on each workstation on which you want to use the PCM GINA) yourself. This installer is shipped with PCM as an MSI-package (called: 'Gina.msi') and can be found in the PCM subdirectory: 'Gina' which is located within your installation directory (this is by default: 'C:\Program Files\Tools4ever\Password Complexity Manager).

To install the PCM GINA manually, perform the following actions when you've located the MSI-package:

1. Copy the installer to the target computer (if the target computer is not the same computer on which you're running the PCM Admin Console)
2. Install the PCM GINA on target computer by running the MSI-package.

3. Reboot the remote machine
4. Check to the GINA by logging on and going to the change password dialog.

Distributed installation

Instead of installing the PCM GINA manually on each workstation, it is possible to distribute the PCM GINA automatically to each of these workstations. This can be done by using Group Policy Objects .The GPO distribution guide explains how to install the PCM Gina using GPO's.

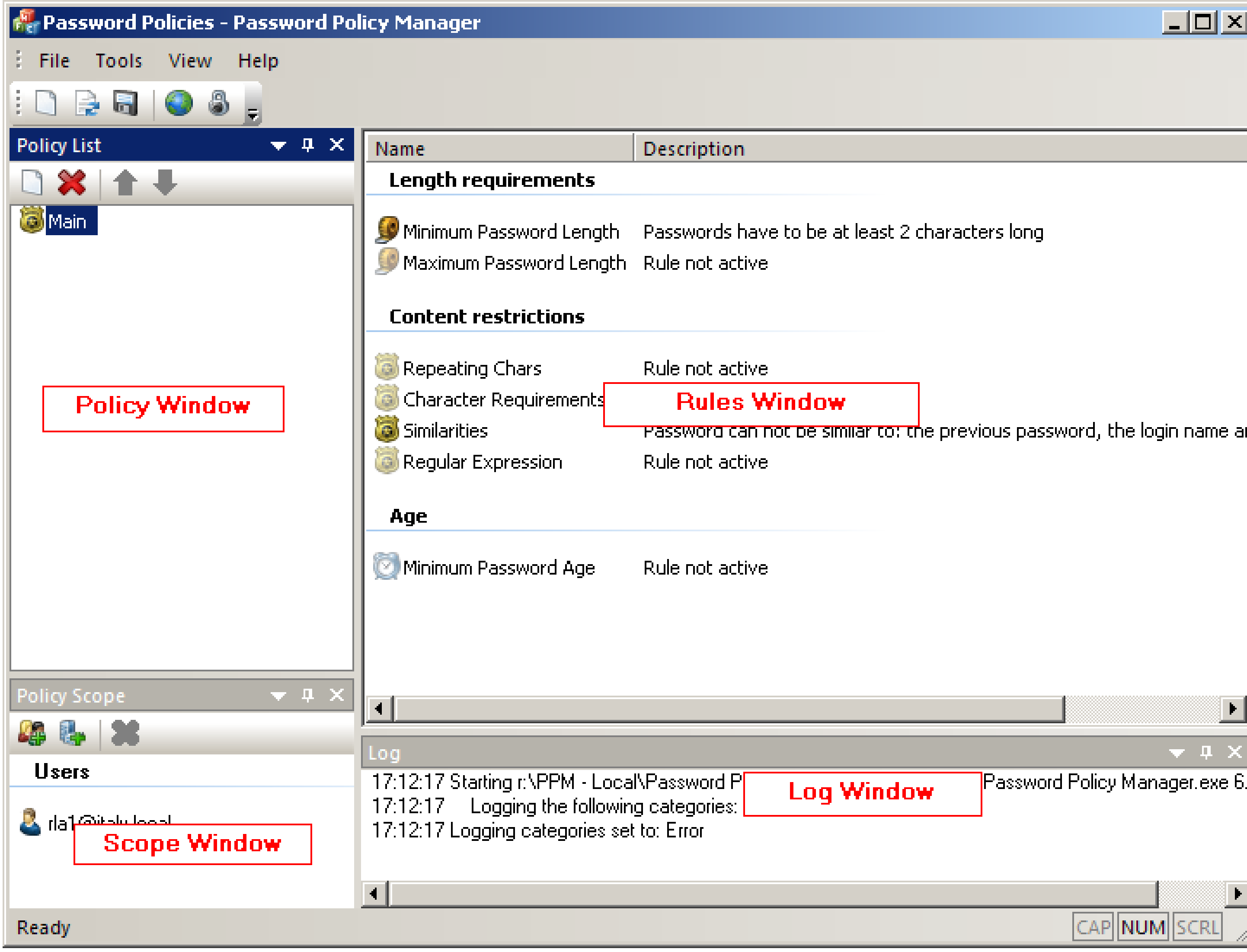
4. Using PCM

4.1. Admin Console

When you've successfully installed the Admin console and the filter, PCM is ready for use.

The Admin console consists of several windows:

- The policy window, which contains a list of the configured password policies.
- The scope window, which shows the scope of the currently selected policy.
- The rules window, this window shows all the available rules. By double clicking on the individual rules opens the associated rule configuration dialog.
- The log window, here you can find feedback from the actions which were performed.



Name	Description
Length requirements	
Minimum Password Length	Passwords have to be at least 2 characters long
Maximum Password Length	Rule not active
Content restrictions	
Repeating Chars	Rule not active
Character Requirements	
Similarities	Password can not be similar to: the previous password, the login name ar
Regular Expression	Rule not active
Age	
Minimum Password Age	Rule not active

Users

rla1@italy.local

```
17:12:17 Starting r:\PPM - Local\Password P                    Password Policy Manager.exe 6.
17:12:17     Logging the following categories:
17:12:17 Logging categories set to: Error
```

4.2. Policies

You can create one or more policies. The policies will be checked in the same order as which they are shown in the scope window. Should the scopes of one or more policies overlap, the policy with the highest ranking in the policy list takes precedence. Therefore it is considered a best practice to order the policies based on their importance.

A policy consists of password complexity rules and one or more scopes.

> Note: The windows domain password policy remains active. To avoid conflicts between the default windows domain password policy and the PCM policies, it is advisable to make sure that the PCM policies are never less strict than the windows domain password policy. This ensures that passwords approved by the PCM Filter will also be accepted by the Windows password manager.

4.3. Scopes

A scope is an entity to which the policy applies, this can be:

- a single Organizational Unit
- an Organizational Unit and all it's children
- a specific user
- a domain

4.4. Rules

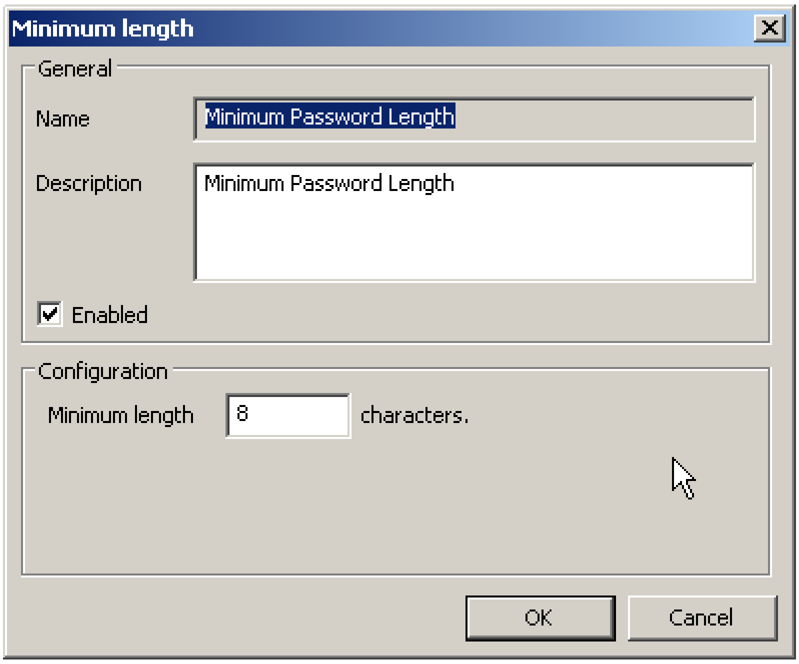
This chapter contains a description of the available password policy rules.

For each rule the following applies:

- Rules are only applied if they are enabled.
- Make sure the description is clear and easy to understand, because it will be shown to the end user by the PCM GINA. The PCM GINA shows a checklist of the rules that the user needs to adhere to, and the checklist uses the descriptions of the rules.

4.4.1. Minimum Password Length

The password must be at least the specified amount of characters long.



Name: Minimum Password Length

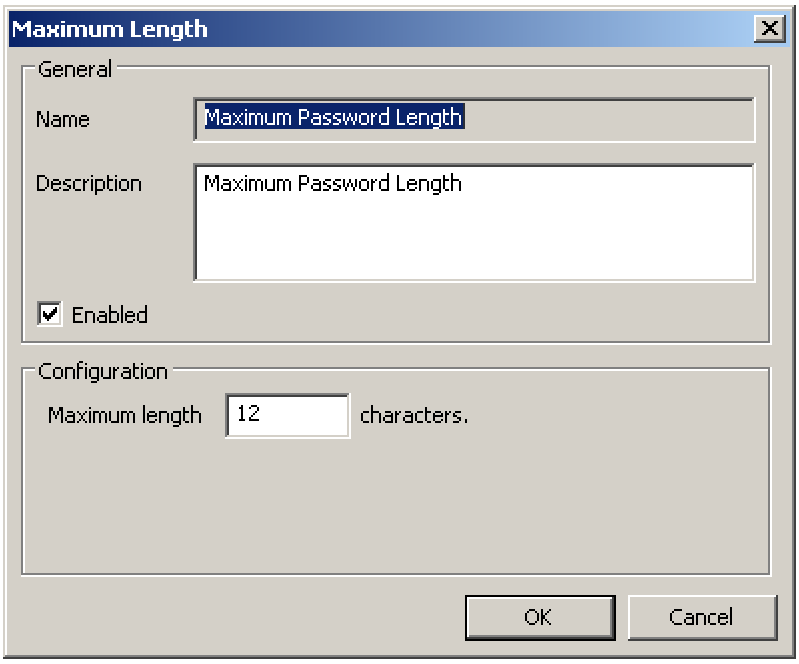
Description: Minimum Password Length

☑ Enabled

Minimum length 8 characters.

4.4.2. Maximum Password Length

The password must be shorter than the specified number of characters.



Name: Maximum Password Length

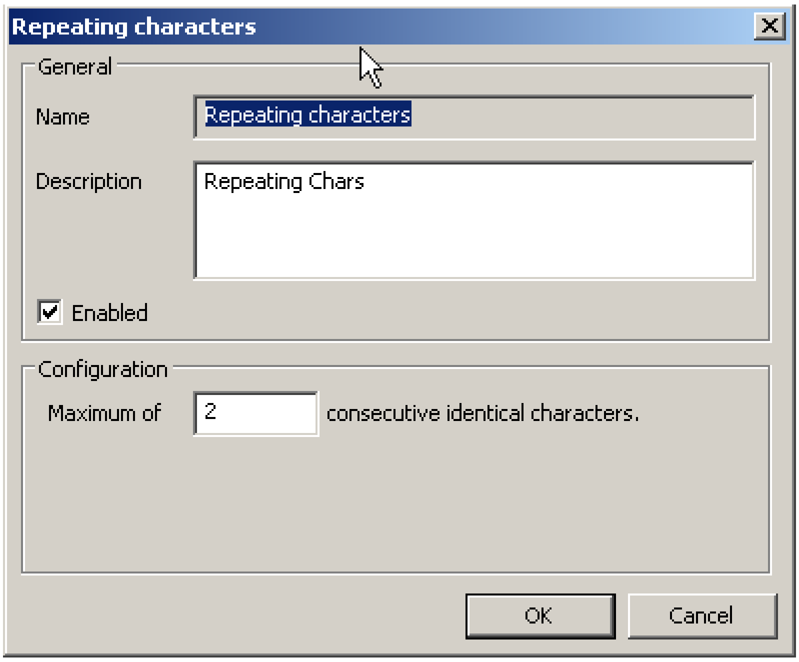
Description: Maximum Password Length

☑ Enabled

Maximum length 12 characters.

4.4.3. Repeating Chars

This rule limits the number of times a specific character can be entered in a row within a password.



Repeating characters

General

Name: Repeating characters

Description: Repeating Chars

☑ Enabled

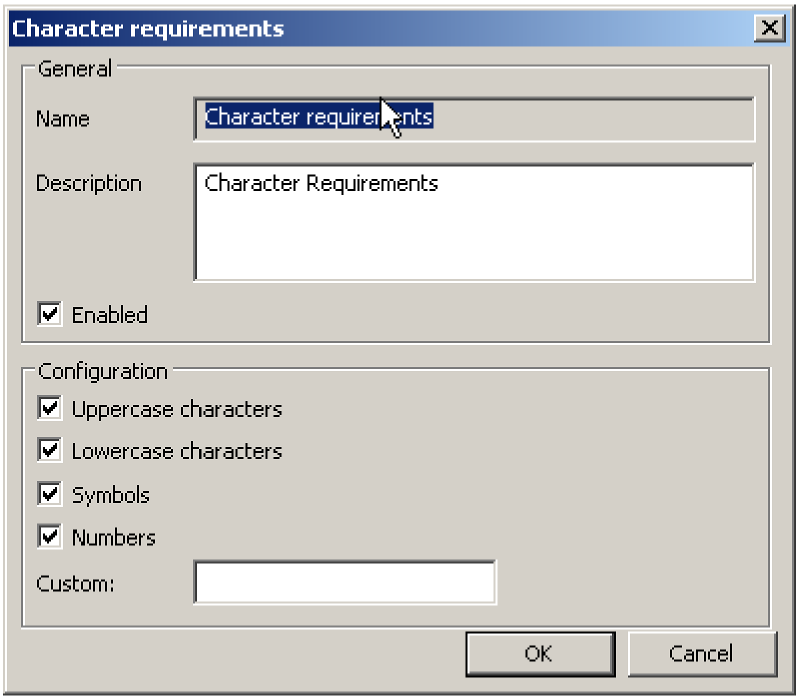
Configuration

Maximum of 2 consecutive identical characters.

Setting this to 2 means a character can not be repeated more than 2 times. This means than "babaab" would still be allowed, but "babaaab" is not allowed. As can be seen in the example, it does not limit the number of times a specific character can appear in a password.

4.4.4. Character Requirements

This rule ensures that a password contains specific groups of characters, like capitals or numbers. It is even possible to provide a list of custom symbols.



Character requirements

General

Name: Character requirements

Description: Character Requirements

☑ Enabled

Configuration

☑ Uppercase characters

☑ Lowercase characters

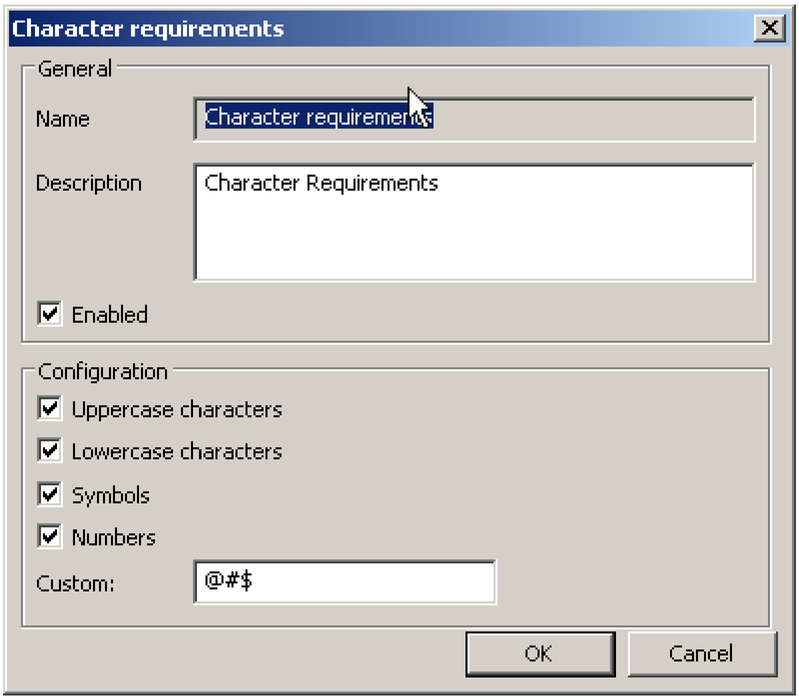
☑ Symbols

☑ Numbers

Custom:

Each group of character you enable must appear in a password. The custom box gives you the ability to enter a custom group of characters. At least one of the characters of this custom group must be in a password.

For exampl, suppose this is your configuration:



Character requirements

General

Name: Character requirements

Description: Character Requirements

☑ Enabled

Configuration

☑ Uppercase characters

☑ Lowercase characters

☑ Symbols

☑ Numbers

Custom: @#$

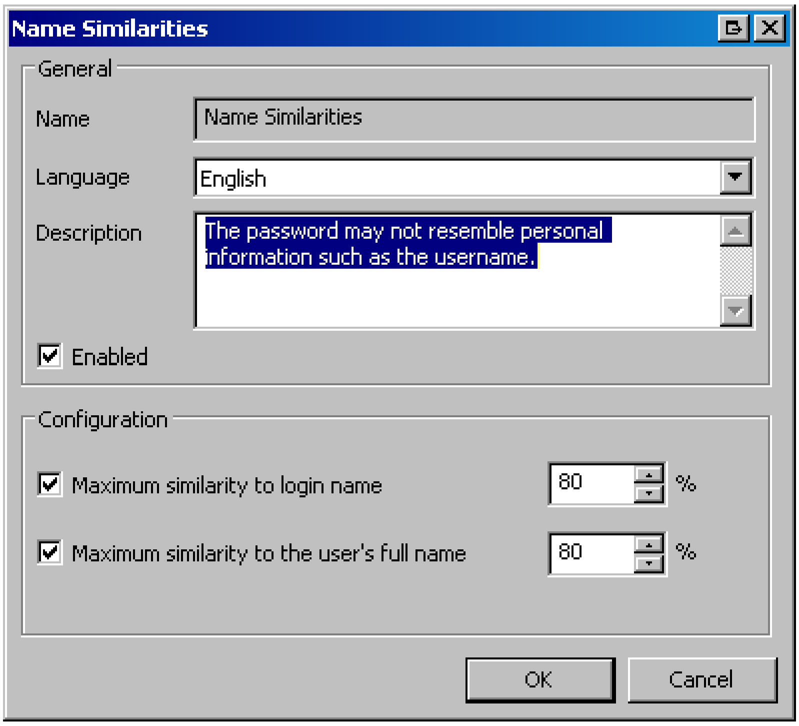
This means that the password must have:

- at least 1 uppercase character, like A, B C,...
- at least 1 lowercase character, like a, b, c,...
- at least 1 symbol, like !, @, #, $, %, ~, ...
- at least 1 number, like 0, 1, 2, ...
- at least one of these characters: @, # or $.

Based on just this rule, passwords like "Ab1!" and "AaaaB^@1" will be accepted. And passwords like "ABB1#", "abc#@" and "Aba12%" will be rejected, for missing: a lowercase character, a number, and of these characters: "@, # or $", respectively.

4.4.5. Name Similarities

This rule compares a new password to the login name and to the user's full name. Meaning it calculates the difference percentage of the 2 compared values, the resulting percentage has to be smaller than specified similarity percentage.



Name Similarities

General

Name: Name Similarities

Language: English

Description: The password may not resemble personal information such as the username.

☑ Enabled

Configuration

☑ Maximum similarity to login name 80 %

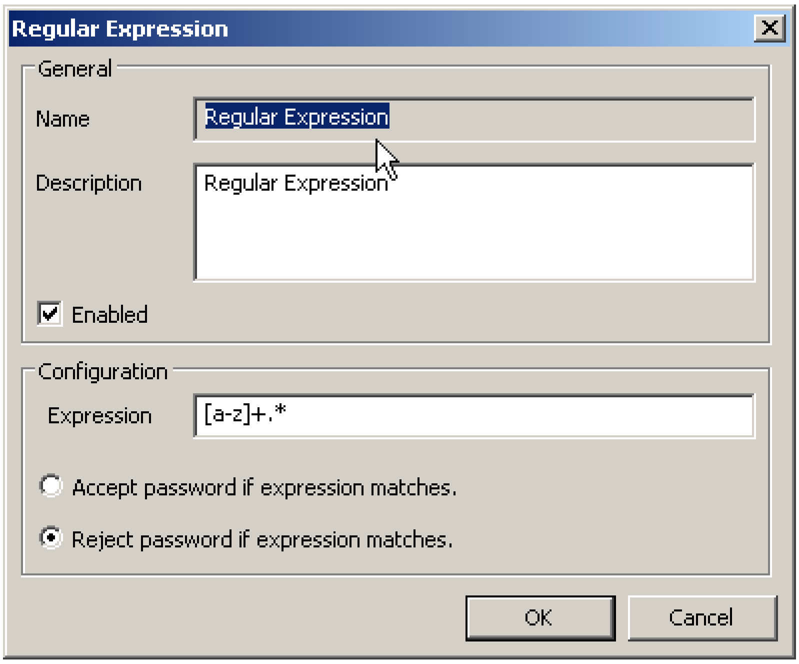
☑ Maximum similarity to the user's full name 80 %

For example: Suppose you set the maximum similarity rate with the old password at 80%. This means, that for a 10 letter password, the two passwords need to be different for at least 2 characters. Let's say the username is 'abcdefghij', the following passwords will then be rejected abcdefghij, abcdefghi, abcdefghi1, bcdefghij12. The following passwords would be approved: bcdefghij123, 123b, abcdefgh.

4.4.6. Regular Expression

The password will be matched against the specified regular expression. Regular expressions are very powerful and have a lot of applications. The password can be accepted when the match the expression or they can be rejected when they match the expression.

For example, take the configuration form the dialog with the expression: "[a-z]+.*".
This expression matches to passwords that start with at least 1 lower case character. So it matches with passwords like "aBcd" or "bAbc". However, since the rule is configured to reject passwords that match the regular expression, none of those passwords will be accepted. Only password that do not start with a lowercase character will be accepted by PCM, i.e. "123abc" or "Abc".



Name: Regular Expression

Description: Regular Expression

☑ Enabled

Expression: [a-z]+.*

○ Accept password if expression matches.

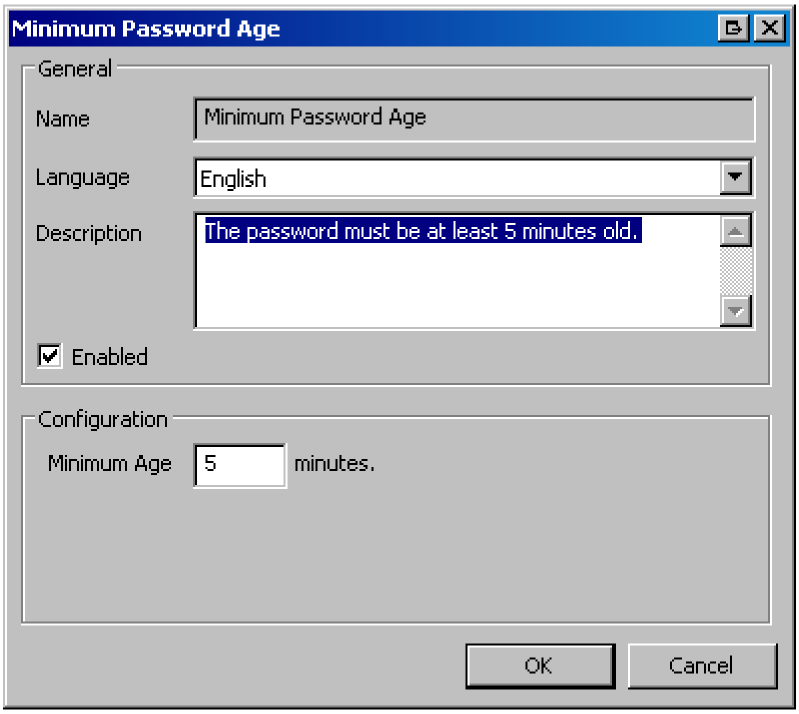
● Reject password if expression matches.

Another example:
Suppose the rule is configured to accept password that match the expression. And we use the expression "Welcome[0-9]+". With this configuration PCM only accepts passwords that start with "Wecome" followed by 1 or more digits, i.e. Welcome1, Welcom50, Welcome123, etc..

For more information about regular expression, please check the appendices of the help documentation.

4.4.7. Minimum Age

The password must be unchanged for at least the specified number of minutes, before it can be changed again.



Name: Minimum Password Age

Language: English

Description: The password must be at least 5 minutes old.

☑ Enabled

Minimum Age: 5 minutes.

PCM will reject the new password if you try to change it before the number of specified minutes have past.

4.5. The PCM Filter

Once properly installed, the filter will validate all password changes. Depending on the policies, passwords will be accepted or rejected.

Should the filter be unable to match the user name to a policy, it will use the configured Default Behaviour setting to determine the course of action.

The filter reloads the policies periodically (every 5 minutes).

4.5.1. Configuration

The PCM filter reads the configuration from the registry for every password filter.

Registry path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Tools4ever\Password Complexity Manager\PCM Filter

Default behaviour

Description:	This key is set using the PCM Admin Console. It specifies the behaviour of the PCM filter, wh
Registry value type:	REG_DWORD
Registry value name:	DefaultBehaviour
Registry value data:	0: Reject password 1: Accept password
Registry value syntax:	0 or 1

Enable log

Description: Use this key to enable or disable logging. By default the PCM filter does not log anything.

Registry value type: REG_DWORD

Registry value name: LogEnabled

Registry value data: 0: Disable logging (default)

1: Enable logging

Registry value syntax: 0 or 1

Log filename

Description: The path of the log file. If logging is enabled and this key is not set, it will use the default va permissions to create and write to the file. The simplest solution is to give everyone full cont

Registry value type: REG_SZ

Registry value name: FileLogFilename

Registry value data: The path for the log file, for example: c:\pcm_filter_log.txt

Registry value syntax: File path

Log message mask

Description: Determines the message types that will be logged. If logging is enabled and this key is not s

Implementation: This is implemented as a bitwise mask. This means that PCM will determine if a message sho returns a value bigger than 0. A bitwise AND-operation only returns a value bigger than zero

For example: The number 3 is represented in binary as 0011. If we perform a bitwise AND-o '0010'.

Because that is the only 1 that the values 3 (00**1**1) and 2 (00**1**0) have in common.

So if you set the mask to 3, this is means that only message with the type information and e

Options

NONE	= 0 (0000)
INFORMATION	= 1 (0001)
ERROR	= 2 (0010)
WARNING	= 4 (0100)
DEBUG	= 8 (1000)
ALL	= 0xffffffff (1111)

*The value between the brackets is a binary representation.

Registry value type: REG_DWORD

Registry value name: FileLogMask

Registry value data: 0 : None
1 : Information
2 : Error
4 : Warning
8 : Debug messages
ffffffff : All messages

Registry value syntax: Any

Maximum log file size

Description: The maximum size of the log file, if not specified the maximum size will be set to 5 Mb

Registry value type: REG_DWORD

Registry value name: FileLogMaxFileSize

Registry value data: A valid number

Registry value syntax: A valid number

Log Immediately

Description: This will cause the PCM filter to log the message immediately, as opposed to saving messag
the log file unreadable especially if multiple reset calls are being processed simultaneously.

Registry value type: REG_DWORD

Registry value name: FileLogImmediately

Registry value data: 0: No
1: Yes

Registry value syntax: 0 or 1

4.5.2. Known issues

Synchronization problem

As stated earlier the PCM Filter reloads the policies periodically. This can give you the impression that it is not working properly.
For example:
Suppose you just changed the policy and increased the minimum password length from 6 characters to 10 characters. To test it, you try to reset the password of a test account to 'Abc123'. And surprisingly the password is accepted, even though it was only 6 characters. This is due to the fact that the filter has not yet reloaded the policies and is still using the old policy, where the minimum length is 6 characters.

Synchronization problem with GINA

This an extension of the problem mentioned above, only now we're also taking the PCM GINA in to consideration.
Unlike the PCM Filter, the GINA loads the policies when the user opens the change password dialog.
Here a conflict can arise, since the PCM Filter might be using an "outdated" policy, but the PCM GINA is using the new policy.
The problem in that scenario is that the PCM GINA validates a password based on the new policy, but the PCM Filter validates it using the old policy.

In such a scenario the behavior is defined by the policies:

1. Both policies are identical, nothing happens
2. The new policy is stricter than the old policy. No impact, since the PCM Filter will not deny the password.

3. The old policy is stricter than the new policy. It is possible that the PCM Filter rejects the password even though the PCM GINA accepts it.
4. The new and the old policy have contrary requirements. Simply said, the PCM GINA only accepts passwords that will be denied by the PCM Filter and vice versa. In this scenario a user is unable to change his/her password.

4.6. The PCM Gina

4.6.1. Configuration

The PCM GINA reads the configuration from the registry, at start up.

Registry path: HKEY_LOCAL_MACHINE\SOFTWARE\Tools4ever\Password Complexity Manager\Password Gina

Enable log

Description: Use this key to enable or disable logging. By default the PCM filter does not log anything.

Registry value type: REG_DWORD

Registry value name: LogEnabled

Registry value data: 0: Disable logging (default)

1: Enable logging

Registry value syntax: 0 or 1

Log filename

Description: The path of the log file. If logging is enabled and this key is not set, it will use the default va

Registry value type: REG_SZ

Registry value name: FileLogFilename

Registry value data: The path for the log file, for example: c:\pcm_gina_log.txt

Registry value syntax: File path

Log message mask

Description: Determines the message types that will be logged. If logging is enabled and this key is not s

Implementation: This is implemented as a bitwise mask. This means that PCM will determine if a message sho
returns a value bigger than 0. A bitwise AND-operation only returns a value bigger than zero

For example: The number 3 is represented in binary as 0011. If we perform a bitwise AND-o
'0010'.

Because that is the only 1 that the values 3 (00**1**1) and 2 (00**1**0) have in common.

So if you set the mask to 3, this is means that only message with the type information and e

Options

NONE	= 0 (0000)
INFORMATION	= 1 (0001)
ERROR	= 2 (0010)
WARNING	= 4 (0100)
DEBUG	= 8 (1000)
ALL	= 0xffffffff (1111)

*The value between the brackets is a binary representation.

Registry value type: REG_DWORD

Registry value name: LogEnabled

Registry value data:
0 : None
1 : Information
2 : Error
4 : Warning
8 : Debug messages
ffffffff : All messages

Registry value syntax: Any

Maximum log file size

Description: The maximum size of the log file, if not specified the maximum size will be set to 5 Mb

Registry value type: REG_DWORD

Registry value name: FileLogMaxFileSize

Registry value data: A valid number

Registry value syntax: A valid number

Log Immediately

Description: This will cause the PCM filter to log the message immediately, as opposed to saving messag
the log file unreadable especially if multiple reset calls are being processed simultaneously.

Registry value type: REG_DWORD

Registry value name: FileLogImmediately

Registry value data:
0: No
1: Yes

Registry value syntax: 0 or 1

5. Index