Password Policy Enforcer

Evaluator’s Guide

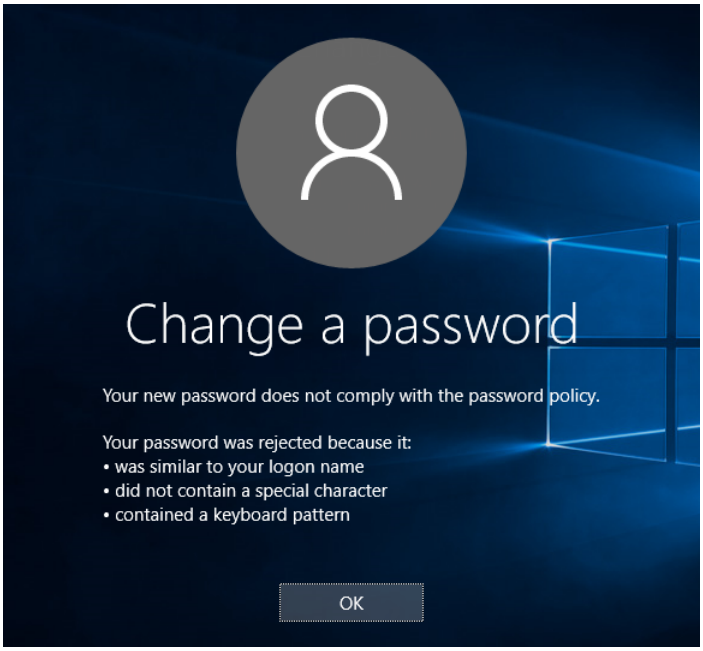
V9.0

Table of Contents

Introduction

Password Policy Enforcer is an advanced password filter for Windows. This Evaluator's Guide shows you how to quickly install, configure, and test PPE.

Password Policy Enforcer helps you to secure your network by ensuring that users choose strong passwords. If a user chooses a password that does not comply with the password policy, PPE immediately rejects the password and tells the user why their password was rejected.



Unlike password cracking products that check passwords after they are accepted by the operating system, PPE checks new passwords immediately to ensure that weak passwords do not jeopardize system security.

You can also use PPE to ensure that passwords are compatible with other systems, and to synchronize passwords with other systems and applications.

The PPE Administrator's Guide contains additional installation and configuration information. Refer to the Administrator's Guide for more detailed coverage of the topics in this document.

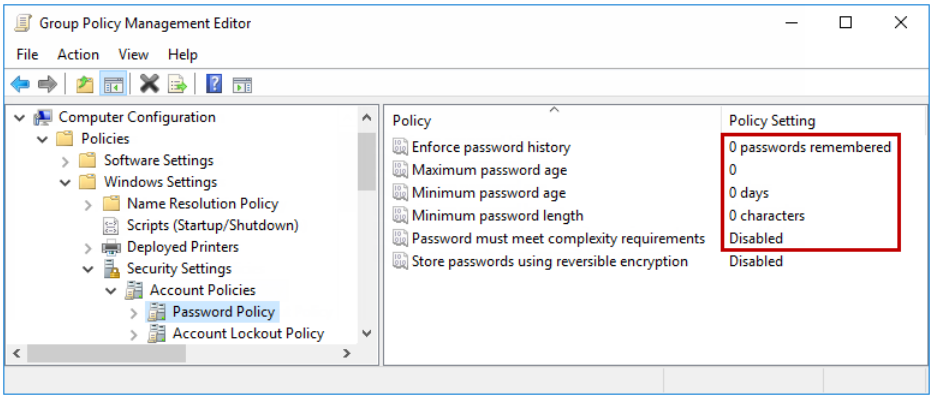
Preparing the Computer

You only need one computer for the evaluation. A Windows 2008, 2012, or 2016 domain controller in its own domain is recommended. You can also use Windows Vista, 7, 8, or 10 if you only need to enforce policies for local accounts.

Disable the Windows Password Policy Rules

If the PPE and Windows password policies are both enabled, then users will have to comply with both policies. This is not recommended for the evaluation because the Windows policy may stop users from reusing recent passwords, or from changing their password more than once a day. These restrictions can make it difficult to evaluate PPE. To disable the Windows password policy:

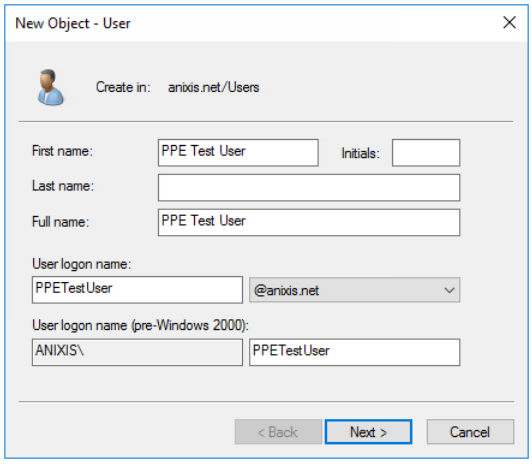
1. If you are evaluating PPE on a domain, use the Group Policy Management Console (gpmc.msc) to display the GPOs linked at the domain level. Right-click the **Default Domain Policy** GPO (or whichever GPO you use to set the password policy), and then click **Edit...**
2. If you are evaluating PPE on a standalone server or workstation, open the Local Group Policy Editor (gpedit.msc).
3. Expand the **Computer Configuration**, **Policies** (if it exists), **Windows Settings**, **Security Settings**, **Account Policies**, and **Password Policy** items.
4. Double-click **Enforce password history** in the right pane of the GPO Editor. Type 0 in the text box, and then click **OK**.
5. Repeat the step above for the **Maximum password age**, **Minimum password age**, and **Minimum password length** policies.
6. Double-click **Password must meet complexity requirements** in the right pane. Select the **Disabled** option, and then click **OK**.
7. Close the Group Policy Management Editor.



8. Execute this command to refresh Group Policy: gpupdate /target:computer

Create Test Accounts

Create two user accounts for the evaluation, PPETestUser and PPETestAdmin. Make PPETestAdmin a member of the Domain Admins group if you are evaluating PPE on a domain controller.



Installing PPE

You can install PPE manually, or you can automate the installation with a software distribution tool. The instructions below show you how to install PPE manually as this is the fastest option for an evaluation.

Refer to the PPE Administrator's Guide to learn how to install PPE with Group Policy. You can also use other software distribution tools like Microsoft's System Center Configuration Manager to install PPE.

Installing PPE does not extend the Active Directory schema.

---

1. Start the PPE installer (PPE900.exe).
2. Read the license agreement, and then click **Yes** if you accept all the license terms and conditions.
3. Select the **Express** option, and then click **Next**.
4. Select the **Password Policy Server** check box if it is not selected.
5. Click **Next** to install PPE.
6. Click **Yes** when asked to restart the computer.

If you are evaluating PPE on a domain with more than one domain controller, then repeat the steps above on every domain controller in the domain.

The Password Policy Client is an optional PPE component that helps users to choose a compliant password. You do not have to install the Password Policy Client to enforce a PPE password policy, but installing the PPC will make it easier for users to choose a password. If you are testing PPE on a domain that contains client computers, then repeat the steps above on any Windows client computers if you would like to evaluate the Password Policy Client. You do not need to select the **Password Policy Server** check box to install the PPC on a client computer.

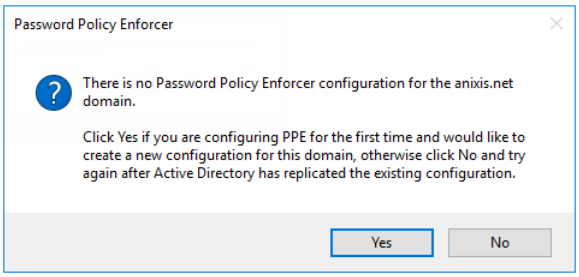
You may need to create a firewall port exception on the domain controllers if you are evaluating the Password Policy Client on a domain with client computers. See the "Creating Firewall Rules for the PPC" section in the PPE Administrator's Guide for more information.

The PPC does not replace or modify any Windows system files. You can install it with Group Policy, or some other software distribution tool in your production network.

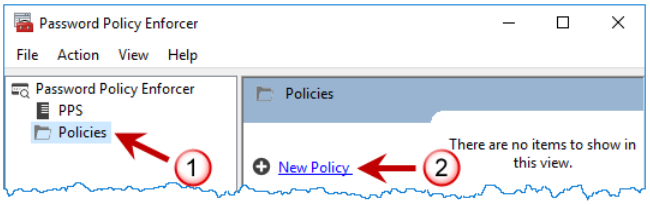
Creating a Password Policy

You can now create your first PPE password policy. To create a password policy with the PPE management console:

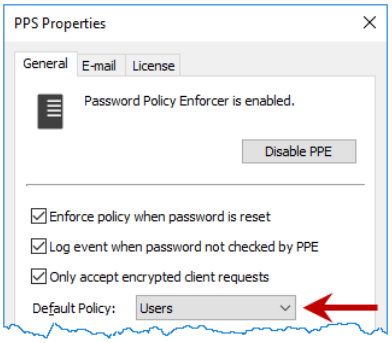
1. Click **Start > Password Policy Enforcer 9 > PPE Configuration** to open the PPE management console. Click **Yes** when asked if you would like to create a new PPE configuration.



2. Click the **Policies** item in the left pane of the management console, and then click **New Policy** in the right pane.



3. Type "Users" in the **New policy name** text box, and then click **OK**.
4. The Policy Properties page opens. Click **OK**, and then click **No** when asked if you would like to assign users to the policy.
5. Click the **PPS** item in the left pane of the management console, and then click **PPS Properties** in the right pane.



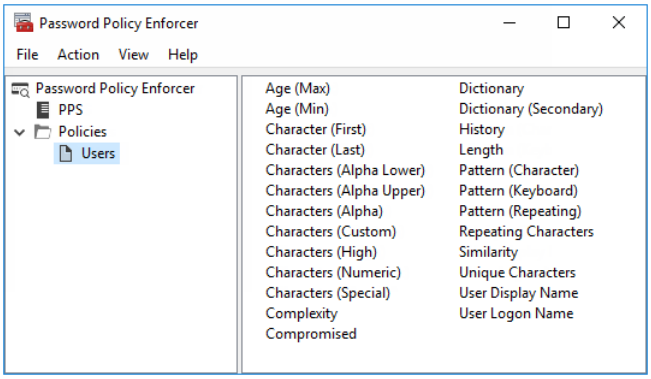
6. Choose the "Users" policy from the **Default Policy** drop-down, then click **OK**.
7. Click **Yes** when asked to confirm the choice of Default Policy.

Configuring Policy Rules

The policy you just created does not enforce any password requirements yet. You can now configure the policy to enforce these rules:

- Password must contain at least seven characters.
- Password must contain at least one lowercase alpha character.
- Password must contain at least one uppercase alpha character.
- Password must not be similar to the user's logon name.
- Password must not exist in a dictionary of common passwords.

1. Click the **Users** policy in the left pane of the management console to display the policy's rules. Rules are displayed in the right pane.



2. Double-click the **Length** rule.
3. Select the **Enabled** check box, and then click **OK**.
4. Double-click the **Characters (Alpha Lower)** rule.
5. Select the **Enabled** check box, and then click **OK**.
6. Double-click the **Characters (Alpha Upper)** rule.
7. Select the **Enabled** check box, and then click **OK**.
8. Double-click the **User Logon Name** rule.
9. Select the **Enabled** check box, and then click **OK**.
10. Double-click the **Dictionary** rule.
11. Select the **Enabled** check box.
12. Click **Browse**, select Dict.txt from the \Program Files (x86)\Password Policy Enforcer\ folder, click **Open**, and then click **OK**.

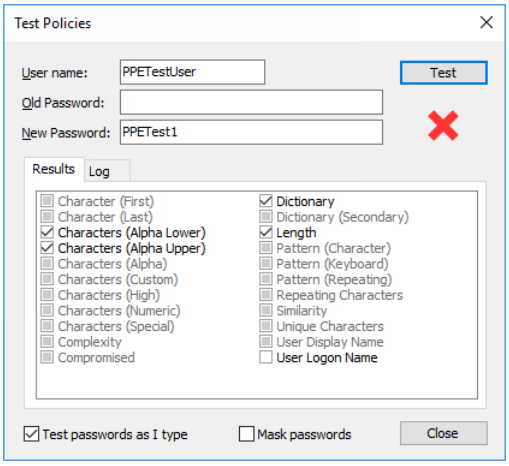
Testing the Password Policy

The Users policy is now being enforced for all users. You can test the policy from the PPE management console, the Windows Change Password screen, or the Active Directory Users and Computers / Local Users and Groups consoles.

PPE Management Console

This is often the best way to test password policies because it shows you the most information. To test password policies from the PPE management console:

1. Click the **Policies** item in the left pane of the management console, and then click **Test Policies** in the right pane.



2. Type a user name in the **User name** text box, and a password in the **Old Password** and **New Password** text boxes.

The PPE management console tests the password by simulating a password change, but it does not change the user's password. It displays a green check mark below the **Test** button if the new password complies with the PPE password policy, or a red cross if it does not comply. Detailed test results appear in the results panel below the **New Password** text box.

The **Results** tab shows the test results for each rule. The check boxes show which rules the new password complied with.

☐ Dictionary	Rule disabled, or not tested.
☑ Dictionary	Rule enabled, password complies with rule.
☐ Dictionary	Rule enabled, password does not comply with rule.

Click the **Log** tab to view PPE's internal event log. The information in the event log can help you to understand why PPE accepted or rejected a password.

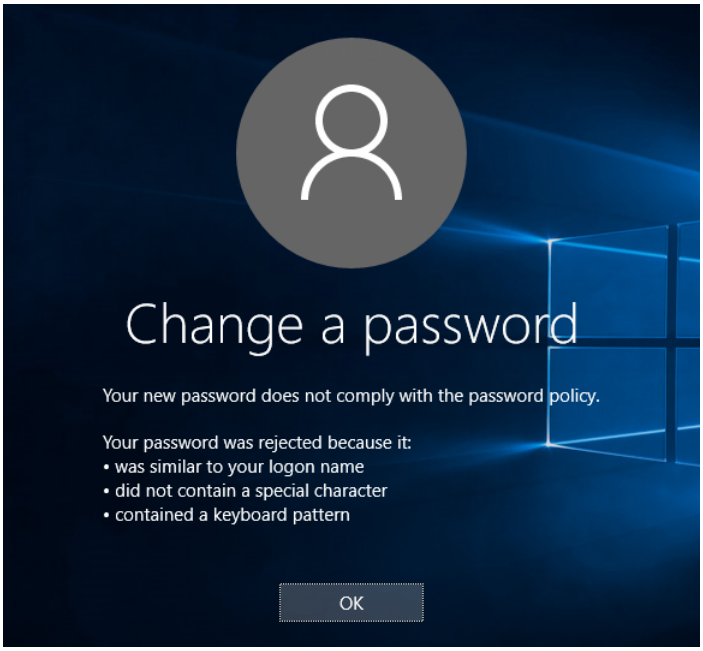
Policy testing simulates a password change, but it may not always reflect what happens when a user changes their password. The "Policy Testing vs. Password Changes" section of the PPE Administrator's Guide explains why.

Windows Change Password Screen

This is how most users change their password. Testing password policies from the Windows Change Password screen is useful because it allows you to see what your users see. To test password policies from the Windows Change Password screen:

1. Press the CTRL + ALT + DEL keys.
2. Click **Change a password.**
3. Type a user name in the **User name** text box, and passwords in the **Old password**, **New password**, and **Confirm password** text boxes.
4. Click →

You may have noticed that the Change Password screen looks different after installing PPE. The PPE password policy is shown during password changes if the Password Policy Client is installed. This helps users to choose a compliant password. The Password Policy Client also changes the message that users see when their password is rejected. Both these messages are customizable.



The Password Policy Client does not modify any Windows system files, and you do not have to install it to enforce a PPE password policy. Web browser based versions of the PPE client are also available. See the ANIXIS Password Reset and PPE/Web pages for more information. ANIXIS Password Reset and PPE/Web are licensed separately.

Active Directory Users and Computers / Local Users and Groups Consoles

Administrators often change domain passwords from the Active Directory Users and Computers console, and local passwords from the Local Users and Groups console. In fact, these consoles do not change passwords; they reset them. This is an important distinction because a password reset is:

- Restricted to privileged users.
- Performed without knowing the current password.

PPE can enforce the password policy for both password changes and password resets. It does this by default, but you can also configure it to only enforce the password policy for password changes. The Minimum Age rule is never enforced when a password reset. To test password policies from these consoles:

1. Start the Active Directory Users and Computers console if PPE is enforcing a domain policy, or the Local Users and Groups console if PPE is enforcing a local policy.
2. Right-click a user, and then click **Reset Password...**
3. Type a password in the **New password** and **Confirm password** text boxes.
4. Click **OK**.

These consoles do not explain why a password was rejected. Use the PPE management console, or the Change Password screen with the PPE client installed to see this information.

The table below contains some sample passwords and expected test results when the Users policy is enforced. Try to change the password for the PPETestUser account to confirm that PPE is enforcing the password policy correctly.

Password	Result	Reason
AbdF6	Rejected	Does not contain at least 7 characters
abd65fgo	Rejected	Does not contain an upper alpha character
ABD65FGO	Rejected	Does not contain a lower alpha character
PPETest1	Rejected	Similar to user logon name
Aardvark	Rejected	Similar to common password (dictionary file)
tseTEPP	Accepted	
kravdraA	Accepted	
Aardv@rk	Accepted	

PPE accepts the last three passwords in the table because they comply with the password policy, but this highlights some weaknesses in this policy:

- tseTEPP is part of the user logon name with the characters reversed.
- kravdraA is Aardvark with the characters reversed.
- Aardv@rk is Aardvark with an @ substituting an a.

These three passwords are only marginally stronger than the rejected passwords. The next section shows you how to improve the password policy so PPE will reject these passwords.

Send an e-mail to support@anixis.com if PPE is not working as expected, and we will help you to resolve the problem.

Improving the Password Policy

PPE rules have properties that control how rules are enforced. You can improve the effectiveness of the Users policy by enabling "character substitution detection" and "bi-directional analysis" for the User Logon Name and Dictionary rules.

When character substitution detection is enabled, PPE searches passwords for common character substitutions. For example, an S replaced with a $. If a password only complies with the policy because of the substitution (i.e. the substitution is needed to make the password compliant), then PPE rejects the password.

Bi-directional analysis tests passwords with their characters reversed to stop users from circumventing a rule by entering a non-compliant password backwards. For example, "drowssapym" instead of "mypassword".

To enable the character substitution detection and bi-directional analysis properties for the User Logon Name and Dictionary rules:

1. Click the **Users** policy in the left pane of the management console.
2. Double-click the **User Logon Name** rule.
3. Select the **Detect character substitution** and **Bi-directional analysis** check boxes, and then click **OK**.
4. Double-click the **Dictionary** rule.
5. Select the **Detect character substitution** and **Bi-directional analysis** check boxes, and then click **OK**.

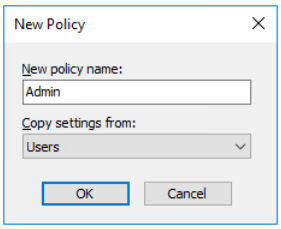
Test the improved Users policy with the passwords that were previously accepted. PPE should reject all of them.

Password	Result	Reason
tseTEPP	Rejected	Similar to user logon name
kravdraA	Rejected	Similar to word in dictionary file
Aardv@rk	Rejected	Similar to word in dictionary file

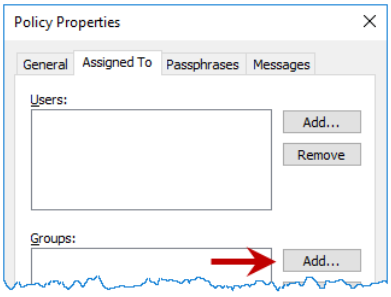
Enforcing Multiple Policies

PPE can enforce up to 256 password policies on each domain or computer. You can assign policies to users directly, or indirectly through Active Directory security groups and containers (Organizational Units). To create another password policy:

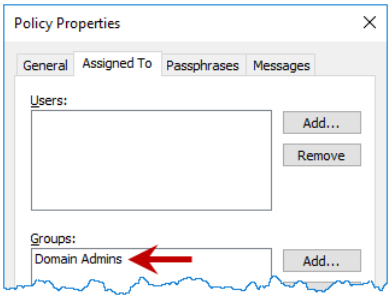
1. Click the **Policies** item in the left pane of the management console, and then click **New Policy** in the right pane.



2. Type "Admins" in the **New policy name** text box, and choose the Users policy from the **Copy settings from** drop-down list.
3. Click **OK** to create the policy, and then click the **Assigned To** tab.



4. Click the **Add...** button beside the **Groups** list, and then type "domain admins" (without quotes). If the test computer is not a domain controller, then click the **Add...** button and type "PPETestAdmin" (without quotes).
5. Click **OK**.



6. Click **OK** to close the Policy Properties page.

Members of the Domain Admins group (or the PPETestAdmin user if you are not using a domain controller) must now comply with the Admins policy. All other users must comply with the Users policy. Users will not notice any difference at this point because the two policies are enforcing identical rules.

To differentiate the policies, change the minimum password length for the Admins policy from seven to nine characters:

1. Click the **Admins** policy in the left pane of the management console.
2. Double-click the **Length** rule.
3. Choose 9 from the **at least** drop-down list, and then click **OK**.

Use the PPE management console, the Windows Change Password screen, the Active Directory Users and Computers console, or the Local Users and Groups console to test password changes and resets for the PPETestUser and PPETestAdmin accounts. PPE should enforce the Users policy for PPETestUser, and the Admins policy for PPETestAdmin.

The PPE Administrator's Guide contains more information about policy assignments, and how PPE resolves policy assignment conflicts that occur when more than one policy is assigned to a user.

Conclusion

Congratulations! You have successfully installed, configured, and tested Password Policy Enforcer. This guide is only an introduction to PPE's capabilities. You can enforce almost any password policy imaginable with PPE, customize the Password Policy Client messages, and even synchronize passwords with other networks and applications. The PPE Administrator's Guide contains more information to help you get the most out of PPE.

You may also be interested in ANIXIS Password Reset and PPE/Web. These products allow users to securely manage their passwords from a web browser. Both products integrate with Password Policy Enforcer to ensure that passwords comply with the password policy, and to help users choose compliant passwords.

ANIXIS Password Reset is a self-service password management system that allows users to change their password, reset a forgotten password, and unlock their account without calling the helpdesk. It includes the Password Reset Client, which allows users to access APR from the Windows Logon and Unlock screens.

PPE/Web allows users to change their password from a web browser.