



Password Policy Enforcer

Evaluator's Guide

V6.1



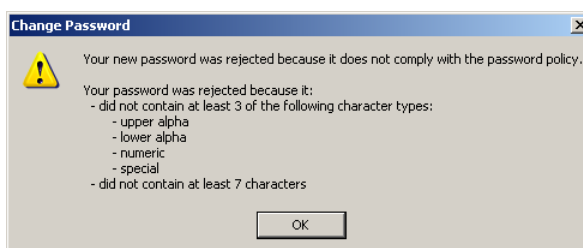
© Copyright 1998 - 2011 ANIXIS. All rights reserved.

ANIXIS, Password Policy Enforcer, Password Policy Server, Password Policy Client, Password Policy Protocol, ANIXIS Password Reset and PPE/Web are trademarks of ANIXIS. Microsoft, Microsoft Management Console, Windows Installer, Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 are either registered trademarks or trademarks of Microsoft Corporation. Other product and company names may be the trademarks of their respective owners.

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. You should read this guide if you are evaluating PPE, or if you are using PPE for the first time.

Password Policy Enforcer helps you to secure your network by ensuring that users choose strong passwords. When a user chooses a password that does not comply with the password policy, PPE immediately rejects the password and explains to 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 network security.

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

The [PPE Administrator's Guide](#) contains additional installation and configuration information.

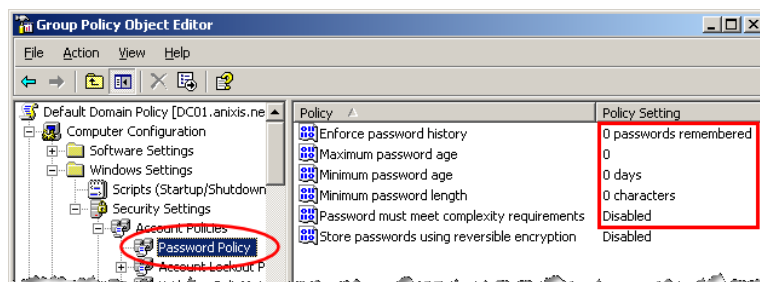
Preparing a Computer for the Evaluation

You only need one computer for the evaluation, a Windows 2000, 2003, or 2008 domain controller. Prepare your test computer by installing Windows on it, and promoting it to a domain controller.

Disable the Windows Password Policy Rules

If you enable both the PPE and Windows password policy rules at the same time, then users will have to comply with both sets of rules. There is no technical problem with doing this, but it is not recommended during the evaluation because you will change your password many times. If the Windows password policy rules are enabled during your evaluation, they may stop you from using the same password more than once, or from changing your password more than once a day. To disable the Windows password policy rules:

1. Use the Group Policy Management Console, or Active Directory Users and Computers Console to display the GPOs linked at the domain level.
2. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
3. Expand the **Computer Configuration, Policies** (Server 2008 only), **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 previous step 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 Object Editor.



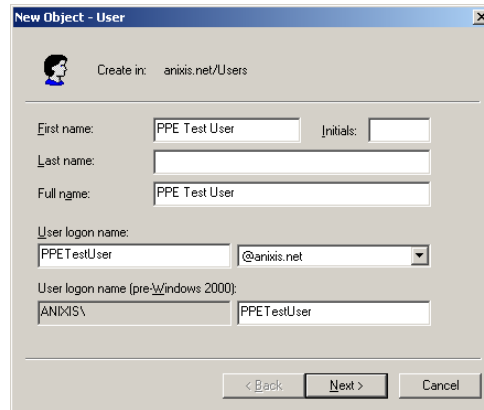
Execute the following command to force an immediate refresh of Group Policy on the domain controller:

Windows 2000: `secdit /refreshpolicy machine_policy`

Windows 2003 and 2008: `gpupdate /target:computer`

Create Test Accounts

Create two domain user accounts for the evaluation, PPETestUser and PPETestAdmin. Make PPETestUser a member of the Domain Users group, and PPETestAdmin a member of the Domain Admins group.



The screenshot shows the 'New Object - User' dialog box in Active Directory. The 'Create in' field is set to 'anixis.net/Users'. The 'First name' field contains 'PPE Test User', and the 'Full name' field also contains 'PPE Test User'. The 'User logon name' field contains 'PPETestUser', and the domain dropdown is set to '@anixis.net'. The 'User logon name (pre-Windows 2000)' field contains 'AND\S\PPETestUser'. The dialog has '< Back', 'Next >', and 'Cancel' buttons at the bottom.

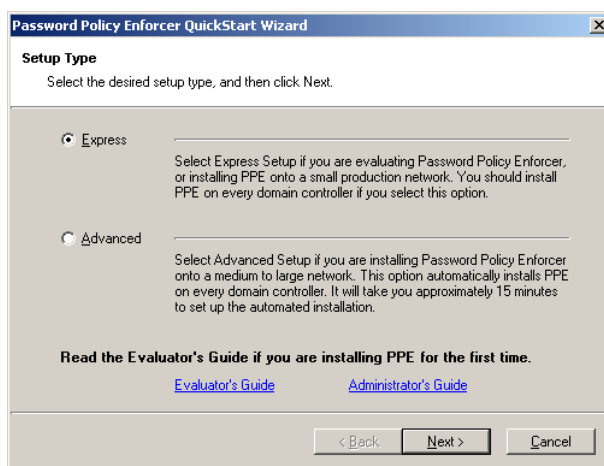
Installing PPE

You can install PPE manually, or you can automate the installation with Group Policy. The instructions below show you how to install PPE manually, as this is the fastest option for a small network.

Refer to the [PPE Administrator's Guide](#) if you would like to learn how to install PPE with Group Policy.

Installing PPE does not extend the Active Directory schema.

1. Start the PPE installer (PPE61.exe) on the domain controller.
2. Read the license agreement carefully, and then click **Yes** if you accept all the license terms and conditions.
3. Select the **Express** option, and then click **Next**.



4. Click **Next** to install PPE.
5. Click **Yes** when asked to restart the computer.

Install PPE on every domain controller in your test network.

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.

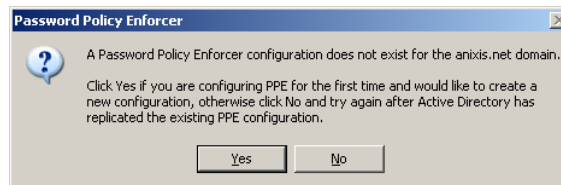
Repeat the installation steps above on any Windows clients or workstations in your test network if you would like to evaluate the Password Policy Client.

The PPC does not replace or modify any Windows system files, and you can install it with Group Policy on your production network.

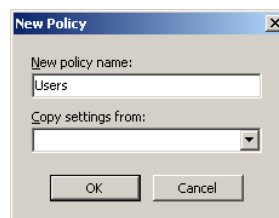
Creating a Password Policy

You are ready to create your first PPE password policy. To create a password policy with the PPE management console:

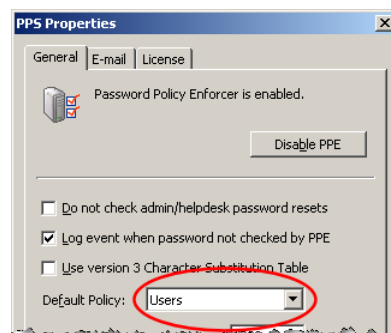
1. Click **Start > [All] Programs > Password Policy Enforcer 6 > PPE Configuration** to open the PPE management console. Click **Yes** when asked if you would like to create a new PPE configuration.



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 appears. 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.



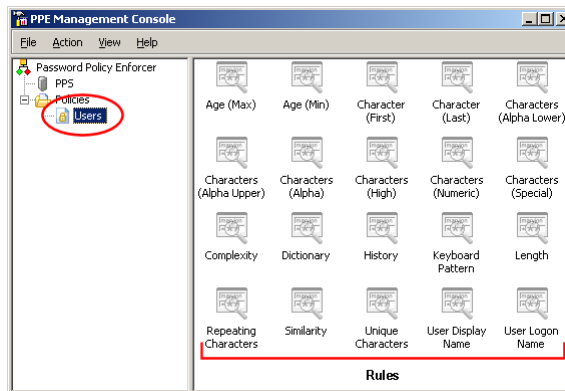
6. Choose the “Users” policy from the **Default Policy** drop-down list, and then click **OK**.

Configuring Policy Rules

You will now configure the Users policy to enforce the following 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** icon.
3. Select the **Enabled** check box, and then click **OK**.
4. Double-click the **Characters (Alpha Lower)** icon.
5. Select the **Enabled** check box, and then click **OK**.
6. Double-click the **Characters (Alpha Upper)** icon.
7. Select the **Enabled** check box, and then click **OK**.
8. Double-click the **User Logon Name** icon.
9. Select the **Enabled** check box, and then click **OK**.
10. Double-click the **Dictionary** icon.
11. Select the **Enabled** check box.
12. Click **Browse**, select Dict.txt from the \Program Files\Password Policy Enforcer\ folder (\Program Files (x86)\Password Policy Enforcer\ on Windows x64), and then click **Open**.
13. Click **OK**.

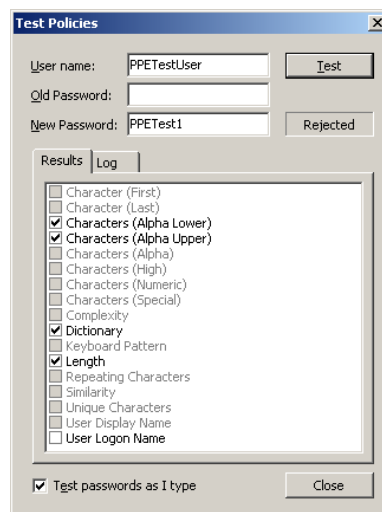
Testing the Password Policy

PPE is now enforcing the Users policy for all domain accounts. You can test policies from the PPE management console, the Windows Change Password dialog, or the Active Directory Users and Computers Console.

PPE Management Console

This is often the best way to test password policies because it allows you to see how PPE analyzes passwords. 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.
3. The PPE management console tests the password by simulating a password change, but it does not change the user's password.

The PPE management console displays “Accepted” beside the **New Password** text box if the new password complies with the PPE password policy, or “Rejected” if it does not comply. Detailed test results appear in the results panel below the **New Password** text box.

Click the **Results** tab to view the test results for each rule. The check boxes show which rules the new password complied with, and which rules it did not comply with.

- | | |
|--|---|
| <input type="checkbox"/> Dictionary | Rule disabled, or not tested. |
| <input checked="" type="checkbox"/> Dictionary | Rule enabled, password complies with rule. |
| <input type="checkbox"/> Dictionary | Rule enabled, password does not comply with rule. |

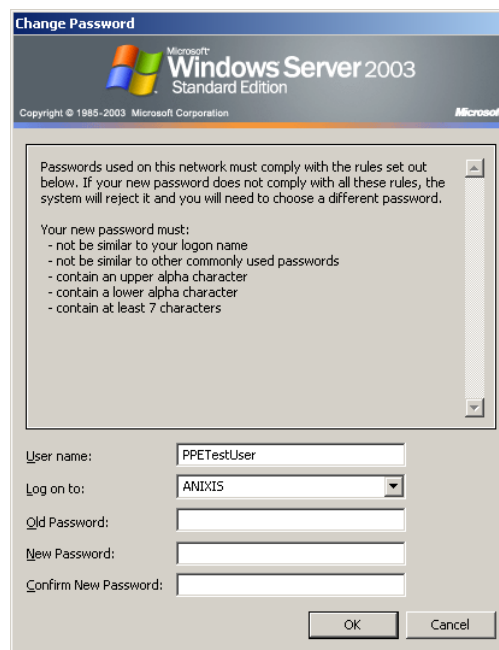
Click the **Log** tab to view PPE's internal event log. The event log contains valuable troubleshooting information that helps you to understand why PPE accepted or rejected a password.

Policy testing simulates a password change, but it may not always reflect what happens when a user changes their password. The [PPE Administrator's Guide](#) explains why.

Windows Change Password Dialog

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

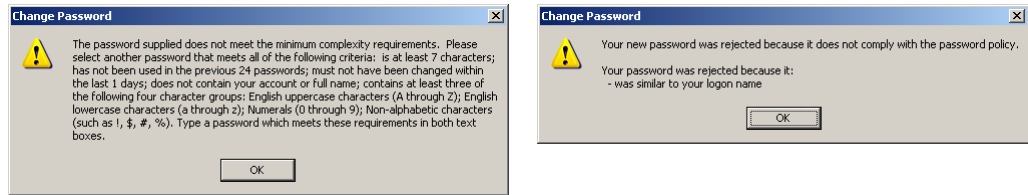
1. Press the CTRL + ALT + DEL keys.
2. Click **Change Password...**



3. Type a user name in the **User name** text box, and passwords in the **Old Password**, **New Password**, and **Confirm New Password** text boxes.
4. Click **OK**.

You probably noticed that the Change Password dialog looks different after installing PPE. The Password Policy Client displays the password policy in a panel above the **User name** text box. This allows users to see the policy as they choose their password.

The Password Policy Client also changes the message that users see when their password is rejected. The Windows Password Rejected message (left) is very complex, and does not tell users which rules they failed to comply with. The PPC message tells users exactly which rules they did not comply with.



You do not have to install the Password Policy Client to enforce a PPE password policy, but installing the PPC reduces user frustration and helpdesk calls. Studies show that password problems account for a large percentage of helpdesk calls, so making it easier for users to choose a compliant password will reduce operating costs.

The V6.1 Password Policy Client does not install a GINA DLL or modify any Windows system files.

Active Directory Users and Computers

This is how administrators and helpdesk operators often change user passwords. In fact, the Active Directory Users and Computers Console does not change passwords; it resets them. This is an important distinction because a password reset is:

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

PPE's default configuration treats password resets just like password changes, but you can configure PPE so that reset passwords are not required to comply with the password policy. To test password policies from the Active Directory Users and Computers Console:

1. Start the Active Directory Users and Computers Console (dsa.msc).
2. Right-click a user object, and then click **Reset Password...**
3. Type a password in the **New Password** and **Confirm Password** text boxes.
4. Click OK.

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

The Active Directory Users and Computers Console does not tell you why a password was rejected. Use the PPE management console, or the Change Password dialog to see this information.

| 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 word in dictionary file |
| tseTEPP | Accepted | |
| kravdraA | Accepted | |
| Aardv@rk | Accepted | |

PPE accepts the last three passwords 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 will show you how to improve this password policy.

E-mail 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 PPE enforces each rule. You can improve the effectiveness of the Users policy by enabling “character substitution detection” and “bi-directional analysis”.

When character substitution detection is enabled, PPE searches new passwords for common character substitutions. For example, a user may replace an S with a \$. If a password only complies with the policy because of the substitution (i.e. the substitution was required 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 weak password backwards. For example, a user may try to use “drowssapym” instead of “mypassword”.

To enable the character substitution detection and bi-directional analysis properties for the Users policy:

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

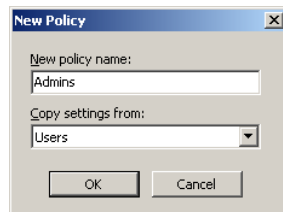
Test the improved Users policy with the weak passwords that were previously accepted. PPE should reject all of them.

| 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 |

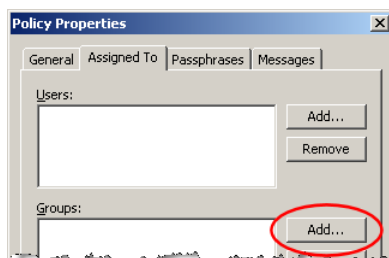
Enforcing Multiple Policies

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

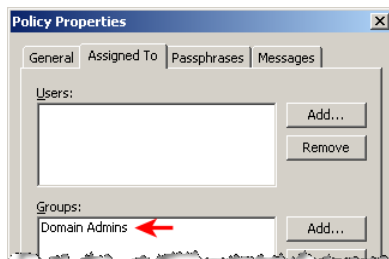
1. Click the **Policies** item in the left pane of the management console, and then click **New Policy** in the right pane.



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.
5. Type “domain admins” (without quotes), and then click **OK**.



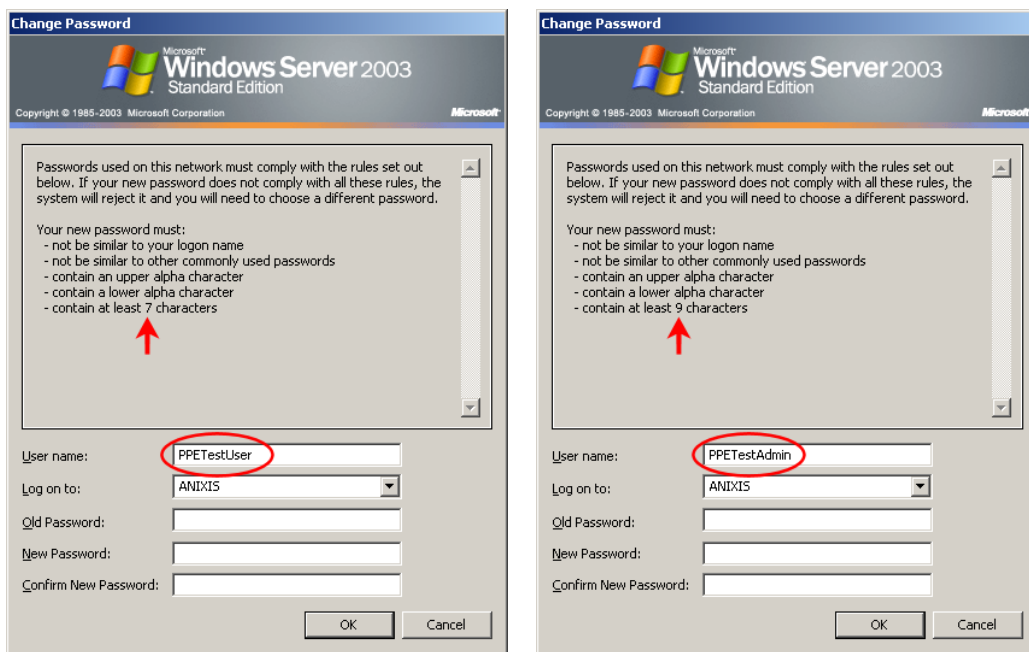
6. The Domain Admins group should appear in the **Groups** list. Click **OK** to close the Policy Properties page.

Members of the Domain Admins group must now comply with the Admins policy. All other users must comply with the Users policy.

The Users and Admins policies are currently enforcing identical rules, so change the minimum password length for the Admins policy to nine characters:

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

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



The PPC displays the correct policy for each user when the cursor leaves the **User name** text box.

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.

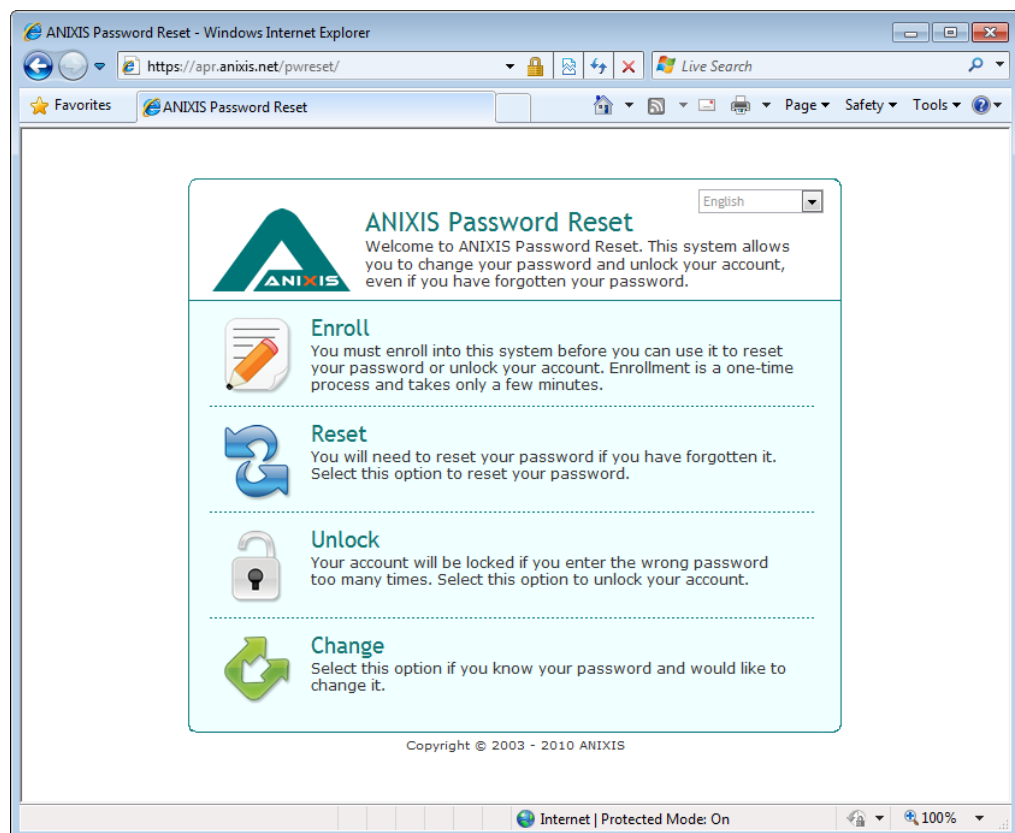
Conclusion

Congratulations! You have successfully installed, configured, and tested Password Policy Enforcer. This brief guide has introduced you to PPE, but PPE can do much more.

You can enforce almost any password policy imaginable with PPE's comprehensive rules, customize the Password Policy Client messages in 31 languages, and even synchronize passwords with other systems and applications.

PPE can integrate with ANIXIS Password Reset, a self-service password management system that allows users to change their password, reset a forgotten password, or unlock their account without calling the helpdesk.

Visit our web site www.anixis.com to learn more about PPE, PPE/Web, and ANIXIS Password Reset.



ANIXIS Password Reset main menu