# Table of Contents

## Introduction
- Introduction .................................................................................................................................................. 4
- What's New .................................................................................................................................................... 5
- Domain and Local Policies .......................................................................................................................... 10
  - Installation Differences............................................................................................................................... 10
  - Operational Differences............................................................................................................................. 11
- Installing PPE ............................................................................................................................................. 13
  - Installation Types ....................................................................................................................................... 13
    - Manual Installation (Express Setup) ........................................................................................................ 14
    - Automated Installation (Advanced Setup) ............................................................................................... 15
  - Disable the Windows Password Policy Rules ........................................................................................ 18
  - Upgrading from PPE V9.x ......................................................................................................................... 19
  - Upgrading from PPE V8.x ......................................................................................................................... 20
  - Upgrading from PPE V7.x ......................................................................................................................... 22
  - Upgrading from PPE V6.x ......................................................................................................................... 25
  - Upgrading from PPE V5.x ......................................................................................................................... 28
  - Upgrading from PPE V4.x ......................................................................................................................... 31
- Configuring PPE ......................................................................................................................................... 34
  - The PPE Management Console ................................................................................................................ 34
  - Management Console Views .................................................................................................................... 35
  - Connecting to a Configuration .................................................................................................................. 37
  - Support Tools .......................................................................................................................................... 38
  - Disabling and Enabling PPE ...................................................................................................................... 39
  - PPS Properties ......................................................................................................................................... 40
- Managing Policies ................................................................................................................................. 43
  - Creating a Policy ....................................................................................................................................... 43
  - Deleting a Policy ....................................................................................................................................... 43
  - Policy Properties ....................................................................................................................................... 44
  - Assigning Policies to Users ....................................................................................................................... 46
    - Policy Assignment Conflicts .................................................................................................................. 48
    - Policy Priorities ....................................................................................................................................... 49
    - Policy Selection Flowchart .................................................................................................................... 50
  - Passphrases ............................................................................................................................................. 51
  - Testing Policies ........................................................................................................................................ 52
- PPE Rules .................................................................................................................................................. 54
  - Maximum Age Rule ................................................................................................................................. 56
  - Minimum Age Rule ................................................................................................................................. 58
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length Rule</td>
<td>59</td>
</tr>
<tr>
<td>Complexity Rule</td>
<td>60</td>
</tr>
<tr>
<td>Dictionary Rule</td>
<td>61</td>
</tr>
<tr>
<td>Compromised Rule</td>
<td>64</td>
</tr>
<tr>
<td>History Rule</td>
<td>66</td>
</tr>
<tr>
<td>Similarity Rule</td>
<td>70</td>
</tr>
<tr>
<td>User Logon Name Rule</td>
<td>71</td>
</tr>
<tr>
<td>User Display Name Rule</td>
<td>72</td>
</tr>
<tr>
<td>Character Rules</td>
<td>73</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>76</td>
</tr>
<tr>
<td>Keyboard Pattern Rule</td>
<td>77</td>
</tr>
<tr>
<td>Character Pattern Rule</td>
<td>79</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>80</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>81</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>82</td>
</tr>
<tr>
<td>Character Rules</td>
<td>76</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>83</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>77</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>78</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>79</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>80</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>81</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>82</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>83</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>85</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>85</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>86</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>87</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>88</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>89</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>90</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>91</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>92</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>93</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>94</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>95</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>96</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>97</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>98</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>99</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Character Rules</td>
<td>100</td>
</tr>
<tr>
<td>First and Last Character Rules</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Pattern Rule</td>
<td>84</td>
</tr>
<tr>
<td>Repeating Characters Rule</td>
<td>84</td>
</tr>
<tr>
<td>Unique Characters Rule</td>
<td>84</td>
</tr>
</tbody>
</table>
Introduction

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 tells them 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 Evaluator’s Guide contains step-by-step instructions to help you quickly install, configure, and evaluate PPE. Read the Evaluator’s Guide if you are using PPE for the first time.
What's New

Password Policy Server
- Accepts encrypted client requests from PPE V9.x clients. Responses to encrypted requests are also encrypted.
- A new **Compromised rule** to reject passwords from prior security breaches.
- The **History rule** can use a more secure hash function called Argon2.
- Can **log an event** when passwords are rejected.
- Can be configured to **only accept encrypted client requests**. Enabled by default for new configurations, but not when upgrading from an older version.
- Can enforce domain password policies on pure IPv6 networks.
- No longer backwards compatible with PPE V3.x clients.

Password Policy Client
- Sends encrypted client requests.
- Improved handling of responses from servers with multiple IP addresses.
- Works over Microsoft DirectAccess connections.
- Can query domain controllers on pure IPv6 networks.
- Added parameters to the Client API for **Compromised rule** client hash files.

Management Console
- **Imports PPE V8.x configuration settings.**
- Increased **maximum age** to five years.
- Improved file selection dialog default folder behavior and allow selection of read-only files.
- Depreciated the **exactly 7 or 14 characters** **Length rule** option. This option is hidden unless it is currently selected.
New in PPE V8.x (Previous Version)

Password Policy Server

- Works with additional LSA protection on Windows 2012 R2 and later.
- Uses a new communications library with better performance and more options.
- Can be configured to ignore client queries by setting the port number to zero.
- Added a configuration value to control the maximum transmit time for the Password Policy Server.
- Modified the default rule inserts to fit the space available on Windows 10.

Password Policy Client

- Hides non-essential user interface elements on the Windows 10 Change Password screen to increase the space available for the Password Policy message.
- Displays the Password Policy message in a message box on Windows 10 computers with small screens. The Password Policy message box can also be shown on larger screens by changing the default display settings.
- Replaces the leading minus sign in the Password Policy and Rejection Reason messages with a bullet character on Windows Vista and later.
- Uses a new communications library with better performance and more options.
- Improved compatibility with third-party credential providers.
- Added a parameter to the Client API to differentiate between password changes and password resets.

Management Console

- Improved warning messages relating to the enforcement of the default policy when there are no other policy assignments.
New in PPE V7.x (Older Version)

Password Policy Rules
- The **Maximum Age rule** can delay the expiry of passwords that exceed a certain length to encourage the use of longer passwords.
- A new **Character Pattern rule** detects patterns like abcde and 12345.
- A new **Repeating Pattern rule** detects passwords like Passw0rdPassw0rd and P@ssw0rdPassword. This stops users from using repetition to increase the length of a short password.
- A second **Dictionary rule** has been added to allow for more flexible detection of dictionary words. The second rule can be used with different settings, and it can remain enabled if the first Dictionary rule is disabled for passphrases. This can be used to relax requirements for passphrases without totally disabling dictionary checking.
- A new **Custom Character rule** without a predefined character set allows custom character sets to be used without overwriting one of the default character sets.

Password Policy Server
- Added support for local password policies.
- The dictionary file and password synchronization script paths can now contain environment variables.

Password Policy Client
- Improved compatibility with third-party credential providers.
- Displays a diagnostic message if the Password Policy Server does not respond to a request. This is likely to happen if a domain controller is not running PPE, or if a firewall is blocking access to the PPS port.

Management Console
- Imports PPE V6.x configuration settings.
- Option to mask passwords when testing policies.
- Improved dictionary file sorting performance by up to 400%.
- Improved performance when opening the Policy Properties page for policies where all assignments are by container.
Mailer Service

- A /test parameter has been added to test the PPE Mailer's delivery options. It sends a test e-mail to the mail server or pickup folder.
- The e-mail body filename can now contain environment variables.

Installer & QuickStart Wizard

- The PPE Client installer now attempts to complete the installation without restarting Windows on Windows Vista and later.
- The QuickStart Wizard Express Setup option now allows you to choose which component(s) to install.
- The QuickStart Wizard now displays a warning message if run on an unsupported Windows version.
New in PPE V6.x (Older Version)

Password Policy Rules
- A new History rule similar to the Windows History rule. PPE’s History rule can enforce different history requirements for each PPE policy. This rule can stop password reuse for a specified number of days, or a specified number of password changes.
- The Maximum Age rule has been redesigned to reduce the likelihood of a user being allowed to logon on the day their password expires, and then being denied access to some network resources some time after logon.

Password Policy Server
- Now compatible with Windows Server 2008 R2.
- PPE can disable some rules when a user enters a passphrase (long password). This allows you to enforce a complex password policy while still encouraging users to use passphrases.

Password Policy Client
- Now compatible with Windows 7 (x86 and x64 editions) as well as Windows Server 2008 R2.
- The PPE Client API is now included with the Password Policy Client. Send an e-mail to support@anixis.com if you would like to enforce PPE’s password policies from your own applications.

Management Console
- Imports PPE V5.x configuration settings.

Mailer Service
- The PPE Mailer reminds users to change their password by sending them e-mail reminders before their password’s expiry date.
Domain and Local Policies

Password Policy Enforcer V7.5 and later can enforce password policies for both domain and local user accounts.

Domain user accounts exist in Active Directory. Information about these accounts is kept on the domain controllers, and changes to the accounts are replicated amongst the domain controllers.

Local user accounts exist in the SAM database of workstations and servers. The workstations and servers may be standalone, or domain members. Information about these accounts is only kept on the host computer, and does not replicate to any other computers.

A typical Windows network has both domain and local user accounts, but you may not want to enforce PPE password policies for both account types. If your users normally logon with a domain account, then you will most likely only use PPE to enforce password policies for the domain accounts.

Installation Differences

To enforce password policies for domain user accounts, you should install PPE onto all the domain controllers in the domain. If you have read-only domain controllers and aren't using the Maximum Age rule, PPE Client or other software that uses the PPE Client protocol, then you do not need to install PPE on the read-only domain controllers.

To enforce password policies for local user accounts, you should install PPE onto the computers containing the user accounts you wish to enforce password policies for. These computers may be workstations or servers, and they may be standalone or domain members. It is normally not necessary to install PPE onto all the workstations and servers in a domain because most users in a domain logon with a domain account. If this is the case, then you will most likely only need to install PPE on the domain controllers.
Operational Differences

Most of PPE's rules and features can be used with both domain and local policies, but there are some differences. When enforcing the password policy for domain accounts, PPE queries Active Directory to get information about the accounts. While it is theoretically possible to get most of this information from the SAM database for local accounts, there is a technical limitation which stops password filters from querying the SAM. There is also some information, such as the user's OU, which does not exist in the SAM. Because of these limitations, the following rules and features cannot be used with local password policies:

- The Minimum Age and Maximum Age rules (you can use the Windows versions of these rules with PPE).
- Policy assignments by groups and containers.

PPE's configuration is stored in Active Directory for domain password policies, and in the Windows registry for local password policies. The Connect To page in the PPE management console allows you to choose a configuration source. Changes you make to PPE's domain configuration are replicated to all domain controllers in the domain. Changes to a local configuration are applied only to the local computer. If you want to use the same local configuration for many computers, export the HKLM\SOFTWARE\ANIXIS\Password Policy Enforcer 9.0\ registry key from the configured computer, and import it into the other computers.

You can also use Group Policy to distribute PPE's local configuration to many computers in a domain. This is only necessary for local password policies. Domain password policies automatically replicate to the domain controllers because they are stored in Active Directory.

To distribute PPE's local configuration with Group Policy:

1. Start the Group Policy Management Console (gpmc.msc).
2. Expand the forest and domain items in the left pane.
3. Right-click the Group Policy object that you would like to use to distribute the configuration, and then click Edit...
4. Expand the Computer Configuration, Preferences, and Windows Settings items in the left pane.
5. Right-click the **Registry** item, and then select **New > Registry Wizard**.

![Registry Wizard screenshot]

6. Select the computer that contains the PPE local configuration that you want to distribute, and then click **Next**.

7. Expand the **HKEY_LOCAL_MACHINE**, **SOFTWARE**, and **ANIXIS** items.

8. Click the **Password Policy Enforcer 9.0** item, and then select the checkboxes beside each item in the bottom pane of the window.

![Registry Browser screenshot]

9. Click **Finish**.
10. Close the Group Policy Management Editor.

PPE's local configuration is applied to the target computers in the domain. This does not happen immediately, as Windows takes some time to apply the changes to Group Policy. You can force an immediate refresh of Group Policy on the local computer with this command: `gpupdate /target:computer`
Installing PPE

Password Policy Enforcer V9.1 is compatible with Windows 2008, 2012, and 2016 servers. It can also be installed on Windows Vista, 7, 8, and 10 workstations to enforce local policies. If you need to install PPE on Windows 2003 domain controllers, then install V8.03 instead of V9.1. PPE V8.03 is available from the ANIXIS web site.

System Requirements

- Fifteen megabytes free disk space.
- Eight megabytes free RAM (72 megabytes if using Argon2 hashes).

Users do not have to change their password immediately after PPE is installed. They can continue using their current password until it expires, even if their current password does not comply with the password policy.

Installing PPE does not extend the Active Directory schema.

Installation Types

Password Policy Enforcer should be installed onto every domain controller to enforce the password policy for domain user accounts, or onto individual servers and workstations to enforce the password policy for local user accounts. If your domain contains some read-only domain controllers, then installation of PPE on these servers is only necessary if you are using the Maximum Age rule, Password Policy Client, ANIXIS Password Reset, or PPE/Web.

You can install PPE manually if you only need to install it on a few computers, but it is easier to perform an automated installation with Group Policy if you need to install it on many computers in a domain.
Manual Installation (Express Setup)

Manual installation is recommended for small to medium networks. You need to repeat the installation procedure below on every computer that should enforce the password policy. To install PPE onto a computer:

1. Start the PPE installer (PPE910.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 using PPE to enforce a password policy for domain user accounts, then you must repeat this procedure on the other domain controllers in the domain.

PPE has its own password rules, so you may want to disable the Windows password policy rules before configuring PPE.
Automated Installation (Advanced Setup)

An automated installation uses Group Policy to distribute PPE. This type of installation is recommended when you need to install PPE on many computers. This section shows you how to install PPE on domain controllers to enforce domain policies, but you can also use Group Policy to target member servers and workstations if you need to enforce local policies.

Create a Distribution Point

A distribution point can either be a UNC path to a server share, or a DFS (Distributed File System) path. To create a PPE distribution point:

1. Log on to a server as an administrator.
2. Create a shared network folder to distribute the files from.
3. Give the "Domain Controllers" security group read access to the share, and limit write access to authorized personnel only.

Copy PPE910.msi into the Distribution Point

1. Start the PPE installer (PPE910.exe).
2. Read the license agreement, and then click Yes if you accept all the license terms and conditions.
3. Select the Advanced option, and then click Next.
4. Right-click the PPE910.msi icon, click Copy, and then paste the file into the distribution point.
5. Give the "Domain Controllers" security group read access to the PPE910.msi file in the distribution point.
6. Click Finish.
Create a Group Policy Object
1. Start the Group Policy Management Console (gpmc.msc).
2. Expand the forest and domain items in the left pane.
3. Right-click the Domain Controllers OU in the left pane, and then click Create a GPO in this domain, and Link it here...
4. Type "Password Policy Enforcer", and then press ENTER.

Edit the Group Policy Object
1. Right-click the Password Policy Enforcer GPO, and then click Edit...
2. Expand the Computer Configuration, Policies, and Software Settings items.
3. Right-click the Software installation item, and then select New > Package...
4. Type the full UNC path to PPE910.msi in the Open dialog box. You must enter a UNC path so that other computers can access this file over the network. For example, \file server\distribution point share\PPE910.msi
5. Click Open.
6. Select the Assigned deployment method, and then click OK.
7. Close the Group Policy Management Editor.
Complete the Installation

Restart each domain controller to complete the installation. Windows installs PPE during startup, and then immediately restarts the computer a second time to complete the installation.

PPE will not enforce a password policy at this time because no policies are defined. Users can still change their password, and will only need to comply with the Windows password policy rules (if enabled).
Disable the Windows Password Policy Rules

The Windows password policy rules can place restrictions on password history, age, length, and complexity. If you enable the PPE rules and the Windows rules, then users will have to comply with both sets of rules.

PPE has its own History, Minimum Age, Maximum Age, Length, and Complexity rules. You can use the PPE and Windows rules together. A password is only accepted if it complies with the Windows and PPE password policies. If you want to disable the Windows password policy rules:

1. Start the Group Policy Management Console (gpmc.msc).
2. Expand the forest and domain items in the left pane.
3. Right-click the Default Domain Policy GPO (or whichever GPO you use to set your domain password policy), and then click Edit...
5. Double-click Enforce password history in the right pane of the GPO Editor. Type 0 in the text box, and then click OK.
6. Repeat the step above for the Maximum password age, Minimum password age, and Minimum password length policies.
7. Double-click Password must meet complexity requirements in the right pane. Select the Disabled option, and then click OK.
8. Close the Group Policy Management Editor.

You do not have to disable all the Windows password policy rules to use PPE. You can use a combination of PPE and Windows rules together if you like. Just remember that a password is only accepted if it complies with the rules enforced by both Windows and PPE.
Upgrading from PPE V9.x

The PPE V9.1 Password Policy Server is backwards compatible with the V9.x Password Policy Client. You do not have to upgrade existing V9.x Password Policy Clients to use the V9.1 Password Policy Server.

Upgrading the Password Policy Server
The PPE installer detects existing V9.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Upgrading the Password Policy Client
The Password Policy Client installer detects existing V9.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.

Upgrading the PPE Mailer
The PPE installer detects existing V9.x installations of the PPE Mailer and upgrades them to V9.1. Refer to the Installing the PPE Mailer section for complete installation instructions.
Upgrading from PPE V8.x

The PPE V9.1 Password Policy Server is backwards compatible with the V8.x Password Policy Client. You can benefit from most of the new features by upgrading the Password Policy Server on the domain controllers. Do this before deploying the V9.1 Password Policy Client.

Upgrading the Password Policy Server

The PPE installer detects existing V8.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Open the PPE V9.1 management console immediately after upgrading to automatically import the V8.x configuration settings into the new version.

The management console imports valid subscription license keys, but it will not import V8.x perpetual license keys as they cannot be used with PPE V9.1. PPE will revert to a 30-day evaluation license if it cannot import the license key. Open the PPS Properties page after an upgrade to check your license details.

You can run a combination of V8.x and V9.x Password Policy Servers, but extended use of both versions is not recommended as it adds administrative overhead. Maintain both versions only for a short time while you roll out PPE V9.x.

Any configuration changes made from the V9.1 management console will only affect V9.x domain controllers. Likewise, any changes made from the V8.x management console will only affect V8.x domain controllers. You must make configuration changes in both management consoles until all domain controllers are upgraded to V9.x. Failure to do so may lead to inconsistent enforcement of the password policy.
Older versions of the PPE Client (prior to V6.0) cannot detect passphrases. Users must comply with the policy's compliance level when these older clients are installed.

PPE V9.x accepts passphrases that comply with all enabled rules, irrespective of the compliance level. PPE V6.x did not do this, so it was possible to configure PPE in a way that would reject all passphrases because they could not meet the compliance level after some rules were disabled. PPE V6.x clients will continue to use the old compliance level calculation until they are upgraded to V9.x. Take this into consideration when setting the compliance level while PPE V6.x clients are still in use. This includes ANIXIS Password Reset V2.x, and PPE/Web V6.x.

PPE V9.x allows the use of longer rule inserts in PPC messages. Older versions of the PPE Client (prior to V7.0), including PPE/Web V6.x and ANIXIS Password Reset V2.x may truncate messages with long inserts.

PPE/Web V3.x and ANIXIS Password Reset V1.x use the PPE V3.x communication protocol. These clients are not compatible with the V9.x server.

---

Do not use the automatic tolerance option with PPE V4.x clients. These clients will enforce an extremely restrictive password policy if this option is enabled. They will reject any password that contains a character found in the comparison parameter.

---

**Upgrading the Password Policy Client**

The Password Policy Client installer detects existing V8.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.

**Upgrading the PPE Mailer**

The PPE installer detects existing V8.x installations of the PPE Mailer and upgrades them to V9.1. Refer to the Installing the PPE Mailer section for complete installation instructions.
Upgrading from PPE V7.x

The PPE V9.1 Password Policy Server is backwards compatible with the V7.x Password Policy Client. You can benefit from most of the new features by upgrading the Password Policy Server on the domain controllers. Do this before deploying the V9.1 Password Policy Client.

Upgrading the Password Policy Server

The PPE installer detects existing V7.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Open the PPE V9.1 management console immediately after upgrading to automatically import the V7.x configuration settings into the new version.

The management console imports valid subscription license keys, but it will not import V7.x perpetual license keys as they cannot be used with PPE V9.1. PPE will revert to a 30-day evaluation license if it cannot import the license key. Open the PPS Properties page after an upgrade to check your license details.

You can run a combination of V7.x and V9.x Password Policy Servers, but extended use of both versions is not recommended as it adds administrative overhead. Maintain both versions only for a short time while you roll out PPE V9.x.

Any configuration changes made from the V9.1 management console will only affect V9.x domain controllers. Likewise, any changes made from the V7.x management console will only affect V7.x domain controllers. You must make configuration changes in both management consoles until all domain controllers are upgraded to V9.x. Failure to do so may lead to inconsistent enforcement of the password policy.
Older versions of the PPE Client (prior to V6.0) cannot detect passphrases. Users must comply with the policy’s compliance level when these older clients are installed.

PPE V9.x accepts passphrases that comply with all enabled rules, irrespective of the compliance level. PPE V6.x did not do this, so it was possible to configure PPE in a way that would reject all passphrases because they could not meet the compliance level after some rules were disabled. PPE V6.x clients will continue to use the old compliance level calculation until they are upgraded to V9.x. Take this into consideration when setting the compliance level while PPE V6.x clients are still in use. This includes ANIXIS Password Reset V2.x, and PPE/Web V6.x.

PPE V9.x allows the use of longer rule inserts in PPC messages. Older versions of the PPE Client (prior to V7.0), including PPE/Web V6.x and ANIXIS Password Reset V2.x may truncate messages with long inserts.

PPE/Web V3.x and ANIXIS Password Reset V1.x use the PPE V3.x communication protocol. These clients are not compatible with the V9.x server.

⚠️ Do not use the automatic tolerance option with PPE V4.x clients. These clients will enforce an extremely restrictive password policy if this option is enabled. They will reject any password that contains a character found in the comparison parameter.

The PPE Client for Windows 8, 10, Server 2012, and Server 2016 displays messages in a smaller area than previous versions of Windows. Some of the default message components were shortened to fit the available space. Your existing templates and macros will not change, but some of the default inserts may be different to the ones your users are familiar with. Any new policies you create after upgrading to PPE V9.x will use the new templates and macros.

If you would like to use the new templates and macros for your existing policies, create a new policy and copy the templates from the new policy to your existing policies. Templates are in the Messages tab of the Policy Properties page.
Upgrading the Password Policy Client

The Password Policy Client installer detects existing V7.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.

Upgrading the PPE Mailer

The PPE installer detects existing V7.x installations of the PPE Mailer and upgrades them to V9.1. Refer to the Installing the PPE Mailer section for complete installation instructions.
Upgrading from PPE V6.x

The PPE V9.1 Password Policy Server is backwards compatible with the V6.x Password Policy Client. You can benefit from most of the new features by upgrading the Password Policy Server on the domain controllers. Do this before deploying the V9.1 Password Policy Client.

Upgrading the Password Policy Server

The PPE installer detects existing V6.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Open the PPE V9.1 management console immediately after upgrading to automatically import the V6.x configuration settings into the new version.

The management console imports valid subscription license keys, but it will not import V6.x perpetual license keys as they cannot be used with PPE V9.1. PPE will revert to a 30-day evaluation license if it cannot import the license key. Open the PPS Properties page after an upgrade to check your license details.

You can run a combination of V6.x and V9.x Password Policy Servers, but extended use of both versions is not recommended as it adds administrative overhead. Maintain both versions only for a short time while you roll out PPE V9.x. If you are using PPE's Maximum Age rule and would like to enable the new extended maximum age feature for long passwords, then you must first upgrade the domain controller holding the PDC emulator operations master role to PPE V9.x.
Any configuration changes made from the V9.1 management console will only affect V9.x domain controllers. Likewise, any changes made from the V6.x management console will only affect V6.x domain controllers. You must make configuration changes in both management consoles until all domain controllers are upgraded to V9.x. Failure to do so may lead to inconsistent enforcement of the password policy.

The **Do not check admin/helpdesk password resets** property in the **PPS Properties** page was renamed to **Enforce policy when password is reset**. The check box value changes after upgrading, but PPE enforces the same policy.

PPE V6.x included two dictionary files. DICT.TXT, and an optimized version called DICT_O.TXT. The two files had identical coverage when the tolerance was set below five, but DICT_O.TXT offered better performance due to its smaller file size. The performance difference is insignificant on modern servers, so PPE V9.x includes only DICT.TXT. If you are using DICT_O.TXT with the **Dictionary rule**, then you should reconfigure it to use DICT.TXT after upgrading.

Older versions of the PPE Client (prior to V6.0) cannot detect **passphrases**. Users must comply with the policy’s **compliance level** when these older clients are installed.

PPE V9.x accepts **passphrases** that comply with all enabled rules, irrespective of the **compliance level**. PPE V6.x did not do this, so it was possible to configure PPE in a way that would reject all passphrases because they could not meet the compliance level after some rules were disabled. PPE V6.x clients will continue to use the old compliance level calculation until they are upgraded to V9.x. Take this into consideration when setting the compliance level while PPE V6.x clients are still in use. This includes **ANIXIS Password Reset V2.x**, and **PPE/Web V6.x**.

PPE V9.x allows the use of longer **rule inserts** in PPC messages. Older versions of the PPE Client (prior to V7.0), including PPE/Web V6.x and ANIXIS Password Reset V2.x may truncate messages with long inserts.

PPE/Web V3.x and ANIXIS Password Reset V1.x use the PPE V3.x communication protocol. These clients are not compatible with the V9.x server.

---

Do not use the **automatic tolerance** option with PPE V4.x clients. These clients will enforce an extremely restrictive password policy if this option is enabled. They will reject any password that contains a character found in the comparison parameter.
The PPE Client for Windows 8, 10, Server 2012, and Server 2016 displays messages in a smaller area than previous versions of Windows. Some of the default message components were shortened to fit the available space. Your existing templates and macros will not change, but some of the default inserts may be different to the ones your users are familiar with. Any new policies you create after upgrading to PPE V9.x will use the new templates and macros.

If you would like to use the new templates and macros for your existing policies, create a new policy and copy the templates from the new policy to your existing policies. Templates are in the Messages tab of the Policy Properties page.

Upgrading the Password Policy Client
The Password Policy Client installer detects existing V6.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.

Upgrading the PPE Mailer
The PPE installer detects existing V6.x installations of the PPE Mailer and upgrades them to V9.1. Refer to the Installing the PPE Mailer section for complete installation instructions.
Upgrading from PPE V5.x

The PPE V9.1 Password Policy Server is backwards compatible with the V5.x Password Policy Client. You can benefit from most of the new features by upgrading the Password Policy Server on the domain controllers. Do this before deploying the V9.1 Password Policy Client.

Upgrading the Password Policy Server

The PPE installer detects existing V5.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Open the PPE V9.1 management console immediately after upgrading to automatically import the V5.x configuration settings into the new version.

The management console imports valid subscription license keys, but it will not import V5.x perpetual license keys as they cannot be used with PPE V9.1. PPE will revert to a 30-day evaluation license if it cannot import the license key. Open the PPS Properties page after an upgrade to check your license details.

You can run a combination of V5.x and V9.x Password Policy Servers, but extended use of both versions is not recommended as it adds administrative overhead. Maintain both versions only for a short time while you roll out PPE V9.x. If you are using PPE’s Maximum Age rule and would like to enable the new extended maximum age feature for long passwords, then you must first upgrade the domain controller holding the PDC emulator operations master role to PPE V9.x.

The Maximum Age rule in PPE V5.x granted users one grace logon after their password expired. PPE V9.x does not allow grace logons, but some grace logons may occur until all domain controllers are upgraded.
If you have deployed the Password Policy Client and will be using the passphrase feature, then update your existing Password Policy message templates to let users know that they may not have to comply with all the rules. You can use the new [PASSPHRASE_NOTICE] macro instead of hard-coding the message text into the template. PPE replaces the macro with this text "You may not have to comply with all these rules if your password contains [n] or more characters."

Any configuration changes made from the V9.1 management console will only affect V9.x domain controllers. Likewise, any changes made from the V5.x management console will only affect V5.x domain controllers. You must make configuration changes in both management consoles until all domain controllers are upgraded to V9.x. Failure to do so may lead to inconsistent enforcement of the password policy.

The Do not check admin/helpdesk password resets property in the PPS Properties page was renamed to Enforce policy when password is reset. The check box value changes after upgrading, but PPE enforces the same policy.

PPE V5.x included two dictionary files. DICT.TXT, and an optimized version called DICT_0.TXT. The two files had identical coverage when the tolerance was set below five, but DICT_0.TXT offered better performance due to its smaller file size. The performance difference is insignificant on modern servers, so PPE V9.x includes only DICT.TXT. If you are using DICT_0.TXT with the Dictionary rule, then you should reconfigure it to use DICT.TXT after upgrading.

Older versions of the PPE Client (prior to V6.0) cannot detect passphrases. Users must comply with the policy’s compliance level when these older clients are installed.

PPE V9.x allows the use of longer rule inserts in PPC messages. Older versions of the PPE Client (prior to V7.0), including PPE/Web V6.x and ANIXIS Password Reset V2.x may truncate messages with long inserts.

PPE/Web V3.x and ANIXIS Password Reset V1.x use the PPE V3.x communication protocol. These clients are not compatible with the V9.x server.

Do not use the automatic tolerance option with PPE V4.x clients. These clients will enforce an extremely restrictive password policy if this option is enabled. They will reject any password that contains a character found in the comparison parameter.
The PPE Client for Windows 8, 10, Server 2012, and Server 2016 displays messages in a smaller area than previous versions of Windows. Some of the default message components were shortened to fit the available space. Your existing templates and macros will not change, but some of the default inserts may be different to the ones your users are familiar with. Any new policies you create after upgrading to PPE V9.x will use the new templates and macros.

If you would like to use the new templates and macros for your existing policies, create a new policy and copy the templates from the new policy to your existing policies. Templates are in the Messages tab of the Policy Properties page.

Upgrading the Password Policy Client
The Password Policy Client installer detects existing V5.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.
Upgrading from PPE V4.x

The PPE V9.1 Password Policy Server is backwards compatible with the V4.x Password Policy Client. You can benefit from most of the new features by upgrading the Password Policy Server on the domain controllers. Do this before deploying the V9.1 Password Policy Client.

Upgrading the Password Policy Server

The PPE installer detects existing V4.x installations and upgrades them to V9.1. Refer to the Installing PPE section for complete installation instructions. If you are performing an Automated Installation with Group Policy, then add PPE910.msi to the same Group Policy Object used to install the older version.

Open the PPE V9.1 management console immediately after upgrading to automatically import the V4.x configuration settings into the new version.

The management console imports valid subscription license keys, but it will not import V4.x perpetual license keys as they cannot be used with PPE V9.1. PPE will revert to a 30-day evaluation license if it cannot import the license key. Open the PPS Properties page after an upgrade to check your license details.

You can run a combination of V4.x and V9.x Password Policy Servers, but extended use of both versions is not recommended as it adds administrative overhead. Maintain both versions only for a short time while you roll out PPE V9.x.

If you have deployed the Password Policy Client and will be using the passphrase feature, then update your existing Password Policy message templates to let users know that they may not have to comply with all the rules. You can use the new [PASSPHRASE_NOTICE] macro instead of hard-coding the message text into the template. PPE replaces the macro with this text "You may not have to comply with all these rules if your password contains [n] or more characters."
Any configuration changes made from the V9.1 management console will only affect V9.x domain controllers. Likewise, any changes made from the V4.x management console will only affect V4.x domain controllers. You must make configuration changes in both management consoles until all domain controllers are upgraded to V9.x. Failure to do so may lead to inconsistent enforcement of the password policy.

The **Do not check admin/helpdesk password resets** property in the PPS **Properties** page was renamed to **Enforce policy when password is reset**. The check box value changes after upgrading, but PPE enforces the same policy.

PPE V4.x included two dictionary files, DICT.TXT, and an optimized version called DICT_O.TXT. The two files had identical coverage when the tolerance was set below five, but DICT_O.TXT offered better performance due to its smaller file size. The performance difference is insignificant on modern servers, so PPE V9.x includes only DICT.TXT. If you are using DICT_O.TXT with the **Dictionary rule**, then you should reconfigure it to use DICT.TXT after upgrading.

Older V4.x clients will work with the new server, but you should upgrade to the V9.x client as it has many improvements.

Older versions of the PPE Client (prior to V6.0) cannot detect **passphrases**. Users must comply with the policy’s **compliance level** when these older clients are installed.

PPE V9.x allows the use of longer **rule inserts** in PPC messages. Older versions of the PPE Client (prior to V7.0), including PPE/Web V6.x and ANIXIS Password Reset V2.x may truncate messages with long inserts.

PPE/Web V3.x and ANIXIS Password Reset V1.x use the PPE V3.x communication protocol. These clients are not compatible with the V9.x server.

Do not use the **automatic tolerance** option with PPE V4.x clients. These clients will enforce an extremely restrictive password policy if this option is enabled. They will reject any password that contains a character found in the comparison parameter.

The PPE Client for Windows 8, 10, Server 2012, and Server 2016 displays messages in a smaller area than previous versions of Windows. Some of the default **message components** were shortened to fit the available space. Your existing templates and macros will not change, but some of the default inserts
may be different to the ones your users are familiar with. Any new policies you create after upgrading to PPE V9.x will use the new templates and macros.

If you would like to use the new templates and macros for your existing policies, create a new policy and copy the templates from the new policy to your existing policies. Templates are in the Messages tab of the Policy Properties page.

**Upgrading the Password Policy Client**
The Password Policy Client installer detects existing V4.x installations and upgrades them to V9.1. Refer to the Installing the PPC section for complete installation instructions. If you are distributing the PPC with Group Policy, then add PPEClt910.msi to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.
Configuring PPE

This section introduces you to the PPE management console, and explains how to configure PPE's global properties. You will also learn how to disable and enable PPE without uninstalling it.

The PPE Management Console

The PPE management console is a Microsoft Management Console snap-in that is used to edit PPE's configuration. The management console is installed by default when PPE is installed, but you can also install it on your computer if you want to remotely configure PPE.

Installing the Management Console

To install the PPE management console onto your computer so that you can remotely configure PPE:

1. Start the PPE installer (PPE910.exe).
2. Read the license agreement, and then click Yes if you accept all the license terms and conditions.
3. Select the Advanced option, and then click Next.
5. Click Next when the PPE Installation Wizard opens.
6. Select I accept the license agreement, and then click Next.
7. Select the Custom option, and then click Next.
8. Click the icon beside the Password Policy Server feature, and then click Entire feature will be unavailable.
9. Click Next twice.
10. Wait for the management console to install, and then click Finish.
Opening the Management Console

Click **Start > Password Policy Enforcer 9 > PPE Configuration** to open the PPE management console. If you are opening the management console for the first time, then click **Yes** when asked if you would like to create a new PPE configuration.

The management console images in this document are taken from a computer running Windows Server 2016. Other Windows versions may display the management console slightly differently, however the management console is used identically on all Windows versions.

Press F1 while using the management console to display help information for the current window.

Management Console Views

The PPE management console has four views. Click an item in the left pane of the management console to select a view.

PPE View

Click **Password Policy Enforcer** in the left pane to display this view. Use this view to:

- Read the PPE documentation.
- **Connect to** a configuration.
PPS View

Click PPS in the left pane to display this view. Use this view to:

- Edit PPS properties.
- Connect to a configuration.
- Display the Support Tools page.

Policies View

Click Policies in the left pane to display this view. Use this view to:

- Edit policy properties.
- Test policies.
- Create and delete policies.
- Set policy priorities.

Rules View

Click a policy name in the left pane to display this view. Use this view to configure the rules for a policy.
Connecting to a Configuration

PPE's configuration settings are stored in Active Directory or the registry. An Active Directory configuration is called a domain configuration, and it defines the password policies for domain user accounts. A registry configuration is called a local configuration, and it defines the password policies for local user accounts.

Connecting to a Domain Configuration

A domain configuration exists on every domain controller. Changes to the configuration replicate to all the domain controllers in the domain, so you only need to configure one domain controller in each domain. If you are using PPE in more than one domain, then you will need to configure each domain separately. To connect to a domain configuration:

1. Click the **Password Policy Enforcer** item to display the PPE view.
2. Click **Connect To** in the right pane of the management console.
3. Select the **Domain** option.
4. Type the name or IP address of a domain controller, and then click **OK**.

---

You cannot make changes to the PPE configuration while the management console is connected to a read-only domain controller.

Connecting to a Local Configuration

A local configuration is used by only one computer, so it does not replicate to any other computers. You can copy a local configuration to another computer by exporting the configuration from the registry, and then importing it into the registry of the other computer. You can also use Group Policy to **distribute** a local configuration to many computers. To connect to a computer's local configuration:

1. Click the **Password Policy Enforcer** item to display the PPE view.
2. Click **Connect To** in the right pane of the management console.
3. Select the **Local** option, and then click **OK**.

---

Domain configurations are stored in the
CN=Password Policy Enforcer 9.0,CN=System object.

Local configurations are stored in the
HKLM\SOFTWARE\ANIXIS\Password Policy Enforcer 9.0\ registry key.

Users with write permission to these objects can configure PPE.
Support Tools

Use the Support Tools page to create a Configuration Report that you can send to ANIXIS Support, or to directly edit PPE's configuration settings.

Configuration Report
Create a Configuration Report and e-mail it to ANIXIS Support if PPE is not working as expected. The Configuration Report will help us to diagnose the problem. To create a Configuration Report:

1. Click the PPS item to display the PPS view.
2. Click Support Tools in the right pane of the management console.
3. Click Save Configuration Report...
4. Type a file name, and then click Save.

Property Editor
The Property Editor allows you to directly edit the PPE configuration. You should only use the Property Editor if instructed to by ANIXIS Support. To open the property editor:

1. Click the PPS item to display the PPS view.
2. Click Support Tools in the right pane of the management console.
3. Click the Property Editor tab.
Disabling and Enabling PPE

You can disable PPE to stop checking new passwords for compliance with the password policy. To disable PPE:

1. Click the PPS item to display the PPS view.
2. Click PPS Properties in the right pane of the management console.
3. Click Disable PPE.
4. Click Yes to confirm, and then click OK.
5. Click OK to close the PPS Properties page.

The PPS icon in the left pane of the management console changes to ⬇ when PPE is not checking passwords. To re-enable PPE:

1. Click the PPS item to display the PPS view.
2. Click PPS Properties in the right pane of the management console.
3. Click Enable PPE, and then click OK.
4. Click OK to close the PPS Properties page.

PPE is disabled or enabled immediately, but if the management console is connected to a domain configuration, there will be some delay while Active Directory propagates the change to the other domain controllers.

A user's password history may be updated even when PPE is disabled. See the History rule for more information.
PPS Properties

The PPS (Password Policy Server) is the PPE component that checks passwords and responds to queries from the Password Policy Client. PPS properties are global settings that apply to all PPE policies. To open the PPS Properties page:

1. Click the PPS item to display the PPS view.
2. Click PPS Properties in the right pane of the management console.

Click the Disable/Enable PPE button to disable or enable PPE.

Select the Enforce policy when password is reset check box if PPE should enforce the password policy when a password is reset. If this option is not selected, administrators and helpdesk operators will not have to comply with the password policy when resetting a user's password, or creating a new user account. This option does not change the behavior of the Minimum Age rule, as this rule is never enforced during a reset. The History rule is only enforced during a reset if this check box is selected, and the Enforce this rule when a password is reset check box is selected in the History Rule Properties page.

Select the Log event when password not checked by PPE check box if PPE should add an entry to the Windows Application Event Log whenever it accepts a password without checking it. This may occur if:

- PPE is disabled.
- The policy assigned to a user is disabled.
- No policy is assigned to a user or an error occurs when determining the assigned policy, and a Default Policy is not specified.
- A password is reset, and the Enforce policy when password is reset check box is not selected.
Select the **Log event when password rejected by PPE** check box if PPE should add an entry to the Windows Application Event Log whenever it rejects a password. The logged event includes the username, source (client or server), and the rules the password did not comply with. Most PPE rules are enforced by both the Password Policy Client and Password Policy Server. If the PPE Client is installed, then it will often reject a non-compliant password before Windows sends it to the domain controller. The following limitations apply when a password is rejected by the Password Policy Client:

- An event is only logged if the PPE Client version is 9.0 or later. If a password is rejected by an earlier client version, then no event is logged. If a password is rejected by the Password Policy Server, then an event is logged irrespective of the client version.

- The logged event may not show all the rules the password did not comply with because some rules are only enforced by the Password Policy Server. For example, a password that does not comply with the **Length**, **Complexity**, and **Compromised** rules would only show the Length and Complexity rules in the event when rejected by the PPE Client because the Compromised rule is only enforced by the server. If the PPE Client is not installed, then the server will log the event with all three rules because the server enforces all these rules.

- Client rejections may not be logged, or they may be logged more than once if the Password Policy Client and Password Policy Server cannot communicate reliably.

---

**PPE does not send passwords or password hashes over the network, even when logging rejections by the Password Policy Client.**

---

Select the **Only accept encrypted client requests** check box if PPE should only accept encrypted requests from the Password Policy Client, ANIXIS Password Reset, and PPE/Web. Client requests do not contain passwords or password hashes, and they were not encrypted prior to PPE V9.0. Select this option if you are not using the PPE V8.x Password Policy Client, ANIXIS Password Reset V3.x, or PPE/Web V7.x (or earlier). PPE accepts both encrypted and unencrypted requests if this option is not selected.
Choose a password policy from the **Default Policy** drop-down list. Users must comply with the default policy if no other policy is assigned to them. Using PPE without a default policy is not recommended, as it may leave some passwords unchecked. To exempt some users from having to comply with the password policy when a default policy is specified:

1. Create a new policy for these users.
2. Leave all the rules disabled for this policy.
3. Assign this policy to the users who do not have to comply with any PPE rules.

This allows you to exclude some users from the password policy, while still ensuring that all other users comply with a policy.

Refer to the **Policy Selection Flowchart** for a diagrammatic representation of PPE’s policy selection algorithm, or use the **Test Policies** page to quickly determine which policy PPE will enforce for a particular user.

---

If PPE has only one policy and that policy is also the default policy, then PPE enforces the policy for all users.

---

The **Password Policy Client** and Password Policy Server communicate over UDP port 1333 by default. If you need to change the default port, then type the new port number in the **Password Policy Server Port** text box. Setting the port number to zero stops PPE from accepting client requests. If you change the port number, then you must also:

- Restart all the Password Policy Server computers.
- Configure the Password Policy Client to use the new port.

Click the **E-mail** tab to configure the e-mail delivery options. Click the **License** tab to display your PPE license details. To install a new license, copy the license to the clipboard, and then click **Get license from clipboard**.
Managing Policies

PPE can enforce up to 256 different password policies. You can assign policies to users directly, or indirectly through Active Directory security groups and containers (Organizational Units). This section explains how to create and configure PPE password policies.

Creating a Policy

There are no password policies defined when PPE is first installed. PPE accepts all passwords in this state, so users only need to comply with the Windows password policy rules (if enabled). To create a new password policy:

1. Click the Policies item to display the Policies view.
2. Click New Policy in the right pane of the management console.
3. Type a unique policy name in the New policy name text box.
4. If the new policy should inherit its default configuration from an existing policy, then choose a policy from the Copy settings from drop-down list.
5. Click OK.
6. Modify the default policy properties as needed.
7. Click OK to close the Policy Properties page, and then configure the rules for this policy.

Deleting a Policy

To delete a policy that is no longer required:

1. Click the Policies item to display the Policies view.
2. Click Delete Policy in the right pane of the management console.
3. Select a policy to delete, and then click OK.
Policy Properties

To open the Policy Properties page:

1. Click the Policies item to display the Policies view.
2. Click the desired policy in the right pane of the management console.
3. Click Properties in the right pane of the management console.

Each PPE policy must have a unique name. To change the name of a policy, type the new name in the text box beside the policy icon.

PPE only enforces enabled policies. Select the Enabled check box if PPE should enforce this policy, or deselect it to disable the policy. The policy’s icon in the left pane of the management console changes to ☑️ when a policy is disabled.

A user’s password history may be updated even when the policy assigned to the user is disabled. See the History rule for more information.

The Reject passwords that do not comply with drop-down list specifies the required compliance level for this policy. The default value (all the rules) requires users to comply with all enabled rules. Choose an alternative option if PPE should enforce a more lenient password policy. The Minimum Age and Maximum Age rules are excluded from compliance level calculations.

When setting the compliance level, consider that some rules may be disabled when a user enters a passphrase. PPE accepts passphrases that comply with all enabled rules, irrespective of the compliance level. This ensures that passphrases can be used, even if they do not meet the compliance level when PPE is configured to disable one or more rules for passphrases.
PPE can start a password synchronization application or script whenever a user successfully changes their password. Enter the full path to the executable in the **Execute this program when a password is changed** text box. The path can contain environment variables like %SystemRoot%. Every computer running PPE should have a local copy of the program, and only authorized users should have access to it, or any of its components.

The user logon name and new password are sent to the program as command-line parameters. For example, if you add the commands below to a batch file, PPE will record each user's logon name and new password in a text file called `passwords.txt`:

```
echo Username: %1 >> c:\passwords.txt
echo Password: %2 >> c:\passwords.txt
```

This script is shown as an example only. You should not store user passwords.

Record any configuration notes about this policy in the **Notes** text box.

Click the **Assigned To** tab to **assign** this policy to users, groups, or containers.

Click the **Passphrases** tab to specify which rules should be disabled when a user enters a passphrase.

Click the **Messages** tab to customize the Password Policy Client **message templates** for this policy.
Assigning Policies to Users

PPE uses policy assignments to decide which policy to enforce for each user. Domain policies can be assigned to users, groups, and containers (Organizational Units). Local policies can only be assigned to users.

When a policy is assigned to a group, PPE enforces the policy for all members of the group as well as any nested groups. For example, if the Helpdesk group is a member of the Info Tech group, then any policy assigned to the Info Tech group also applies to the members of the Helpdesk group. If this behavior is not desired, then you can assign a different policy to the Helpdesk group.

When a policy is assigned to a container, PPE enforces the policy for all users in the container as well as any child containers. For example, if the Helpdesk and Managers OUs are children of the Info Tech OU, then any policy assigned to the Info Tech OU also applies to the two child OUs. If this behavior is not desired, then you can assign a different policy to a child OU.

When a domain policy is assigned to a user or group, PPE stores the user or group SID in the configuration. The assignment remains valid even if the user or group is renamed. When a local policy is assigned to a user, PPE stores the username in the configuration. The assignment is invalidated if the user is renamed.
To assign a password policy:

1. Click the **Policies** item to display the **Policies view**.
2. Click the desired policy in the right pane of the management console.
3. Click **Properties** in the right pane of the management console.
4. Click the **Assigned To** tab.
5. Click the appropriate **Add...** button.
6. Select the desired user, group, or container, and then click **OK**.
7. Click **OK** to close the Policy Properties page.

To remove a policy assignment:

1. Click the **Policies** item to display the **Policies view**.
2. Click the desired policy in the right pane of the management console.
3. Click **Properties** in the right pane of the management console.
4. Click the **Assigned To** tab.
5. Select the policy assignment that you wish to remove.
6. Click the appropriate **Remove** button.
7. Click **OK** to close the Policy Properties page.

---

Different assignment types can be used for a single policy. For example, you may assign users to a policy by both OU and group at the same time.
Policy Assignment Conflicts

A policy assignment conflict occurs when more than one policy is assigned to a user. PPE can resolve these conflicts and choose one policy for each user.

PPE first tries to resolve a policy assignment conflict by examining the assignment type. Assignments by user take precedence over assignments by group, which in turn take precedence over assignments by container. For example, if Policy A is assigned to a user by group, and Policy B is assigned to the same user by container, then PPE will enforce Policy A because assignments by group take precedence over assignments by container.

If all the policies are assigned to the user by container, then PPE enforces the policy that is assigned to the nearest parent container. For example, if Policy A is assigned to the Users OU, and Policy B is assigned to the Users\Students OU, then PPE will enforce Policy B for all users in the Users\Students and Users \Students\Science OUs because it is the policy assigned to the nearest parent container.

If a policy assignment conflict still exists, then PPE checks the priority of each remaining policy, and enforces the policy with the highest priority. Refer to the Policy Selection Flowchart for a diagrammatic representation of this algorithm.

Use the Log tab in the Test Policies page to quickly determine which policy PPE will enforce for a particular user.
Policy Priorities

Policy priorities help PPE to resolve policy assignment conflicts. If more than one policy is assigned to a user, and PPE cannot decide which policy to enforce using the other conflict resolution rules, then PPE always enforces the policy with the highest priority. To set a policy’s priority:

1. Click the Policies item to display the Policies view.
2. Click Set Priorities in the right pane of the management console. This option is only visible when there is more than one password policy.
3. Select the desired policy.
4. Click the arrow buttons to increase or decrease the priority of the policy.
5. Click OK to close the Policy Priorities page.

Refer to the Policy Selection Flowchart for a diagrammatic representation of PPE’s policy selection algorithm, or use the Test Policies page to quickly determine which policy PPE will enforce for a particular user.
Policy Selection Flowchart

This flowchart shows how PPE chooses a policy for each user. Use the Test Policies page to quickly determine which policy PPE will enforce for a particular user.
Passphrases

Passphrases have gained popularity in recent years as they can be more difficult to crack and easier to remember than passwords. The difference between passwords and passphrases is their length. Passwords are rarely longer than 15 characters, but passphrases commonly contain 20 or more characters.

Complexity and dictionary rules are less important for passphrases as passphrases rely primarily on length for security. You may therefore want to relax some password policy requirements for passphrases. To configure a password policy with fewer requirements for passphrases:

1. Click the Policies item to display the Policies view.
2. Click the desired policy in the right pane of the management console.
3. Click Properties in the right pane of the management console.
4. Click the Passphrases tab.
5. Choose the minimum number of characters a password must contain before some rules are disabled from the drop-down list.
6. Select the rules that will be disabled.
7. Click OK to close the Policy Properties page.

Disabled rules are not counted when calculating the compliance level, but PPE will accept passphrases that comply with all enabled rules, irrespective of the compliance level. This ensures that passphrases can be used, even if they do not meet the compliance level when PPE is configured to disable one or more rules for passphrases.

Oppinions differ on how long a passphrase needs to be. Even a 30 character passphrase can be weaker than a well-chosen password. Do not disable too many rules under the assumption that length alone will make up for the reduced complexity as this is not always true.
Testing Policies

You can quickly test your PPE configuration by simulating a password change from the PPE management console. To test your PPE configuration:

1. Click the **Policies** item to display the Policies view.
2. Click **Test Policies** in the right pane of the management console.

3. Type a user name in the **User name** text box, and a password in the **Old Password** and **New Password** text boxes.
4. Click **Test**, or wait a few seconds if **Test passwords as I type** is selected.

   Policy testing simulates a password change, but it does not change the password. As it is only a simulation, you do not have to enter the correct password in the **Old Password** text box.

   The PPE management console 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.

   Click the **Results** tab to view 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 event log can help you to understand why PPE accepted or rejected a password. For example, you can use the event log to see which:

- Computer the configuration was read from.
- Policy was **assigned** to the user, and **why**.
- **Dictionary** word or **keyboard pattern** matched with the password.
- Errors or warnings occurred during testing.

### Policy Testing vs. Password Changes

Policy testing simulates a password change, but it may not always reflect what happens when a user changes their password. A password change may yield different results to a policy test because:

- Policy testing does not simulate the Windows password policy rules. If the Windows password rules are enabled, then Windows may reject a password even though it complies with all the PPE rules.
- Policy testing does not enforce the **Minimum Age** rule.
- Policy testing does not enforce the **History** rule.
- Policy testing enforces the password policy even if PPE or the **assigned policy** is disabled. This allows you to test your configuration before enabling PPE, or a new password policy.
- Policy testing occurs on the computer that the management console is running on. If the management console is **connected to** a remote domain configuration, then it may not find the **dictionary** file on the local computer, or the local dictionary file may be different to the one on the domain controller. Copy the dictionary file onto the local computer (in the same path) to avoid this problem.
- If the management console is **connected to** a domain configuration and the PPE configuration was modified recently, then Active Directory may still be propagating the new configuration to the other domain controllers.
PPE Rules

PPE uses rules to decide if it should accept or reject a password. Each policy has rules that are configured independently of the rules in other policies. To display the rules for a policy:

1. Click the Policies item to display the Policies view.
2. Double-click the desired policy in the right pane of the management console.

Rules are shown in the right pane of the management console. A check mark beside a rule indicates that the rule is enabled (being enforced). Double-click a rule to show the rule's properties.

Detecting Character Substitution

Character substitution is a technique used by some users to improve password quality. They replace some alphabetic characters with non-alphabetic characters that have a similar appearance. For example, "sold" becomes "$old". Many of these substitutions are well known, and do little to improve password strength.

Some PPE rules have a Detect Character Substitution check box. When this check box is selected, PPE tests passwords with, and without character substitution. This stops users from circumventing the rule by substituting some characters. PPE detects these common character substitutions:

<table>
<thead>
<tr>
<th>Original</th>
<th>Substituted</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>^</td>
</tr>
<tr>
<td>B</td>
<td>8</td>
</tr>
<tr>
<td>C</td>
<td>( { &lt; [</td>
</tr>
<tr>
<td>D</td>
<td>) } &gt; ]</td>
</tr>
<tr>
<td>E</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>6 9</td>
</tr>
<tr>
<td>I</td>
<td>!</td>
</tr>
<tr>
<td>O</td>
<td>0 (zero)</td>
</tr>
<tr>
<td>S</td>
<td>$ 5</td>
</tr>
<tr>
<td>T</td>
<td>+ 7</td>
</tr>
<tr>
<td>Z</td>
<td>2</td>
</tr>
</tbody>
</table>
**Tolerance**

Some PPE rules have a **Tolerance** drop-down list that allows you to control how strictly the rule is enforced. Tolerance is normally expressed as the maximum allowable number of consecutive matching characters in the password and some other parameter. PPE rejects a password if the specified tolerance is exceeded. For example, the logon name "mary\textit{jones}" and the password "\textit{Jones}town" contain five consecutive matching characters (shown in bold type). PPE will reject this password if the tolerance for the **User Logon Name rule** is four (or lower), and accept it if the tolerance is five (or higher).

The **User Logon Name**, **User Display Name**, **Similarity**, and **Character Pattern** rules have an Auto tolerance option. Setting the tolerance to Auto instructs PPE to only reject passwords that contain the entire parameter being compared. This is very useful when the length of the comparison parameter is unknown. For example, if you want PPE to reject passwords that contain the user's entire logon name, then you cannot specify a fixed tolerance unless all logon names have the same length. Setting the tolerance to Auto allows PPE to calculate an appropriate tolerance during every password change.

PPE sets the tolerance to the length of the comparison parameter minus one. The table below shows some parameter values and the calculated tolerance. PPE rejects a password if it contains all the text in the Value column (or a derivative of it if **character substitution** detection or bi-directional analysis is enabled).

<table>
<thead>
<tr>
<th>Rule</th>
<th>Parameter</th>
<th>Value</th>
<th>Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Logon Name</td>
<td>Logon name</td>
<td>maryjones</td>
<td>8</td>
</tr>
<tr>
<td>User Display Name</td>
<td>Display name</td>
<td>Mary Jones</td>
<td>9</td>
</tr>
<tr>
<td>Similarity</td>
<td>Current password</td>
<td>oldpass</td>
<td>6</td>
</tr>
<tr>
<td>Character Pattern</td>
<td>Character pattern</td>
<td>abcdefgh</td>
<td>7</td>
</tr>
</tbody>
</table>

PPE's Auto tolerance calculation has a minimum limit to stop passwords from being rejected when the comparison parameter is very short. The limit is set to two characters by default, so PPE will accept passwords that contain the parameter value if the comparison parameter only contains one or two characters. Send an e-mail to **support@anixis.com** if you need to change the minimum limit.

---

**Warning:** Do not use the automatic tolerance option with PPE V4.x or V3.x clients, including PPE/Web V3.x and ANIXIS Password Reset V1.x.
Maximum Age Rule

The Maximum Age rule forces users to change their passwords regularly. This decreases the likelihood of an attacker discovering a password before it changes. This rule can only be enforced by domain policies.

Select the **Enabled** check box to enable the Maximum Age rule.

Choose a value from the first **days** drop-down list to specify how many days must elapse before passwords expire.

You can encourage users to choose longer passwords by extending the lifetime of their password if it exceeds a certain length. To enable this feature, choose a higher value from the second **days** drop-down list and a minimum length from the **contains** drop-down list. Passwords that contain the required number of characters will not expire until the second (higher) **days** value. If both **days** values are identical, then passwords will expire after the specified number of days, irrespective of their length.

When the Maximum Age rule is configured to delay the expiry of longer passwords, it creates an Active Directory security group called "PPE Extended Maximum Age Users". PPE uses this group to identify which users are eligible for a delayed password expiry. Users are added and removed from the group automatically. You can move and rename this group, but do not change the pre-Windows 2000 name. Send an email to support@anixis.com if you must change the pre-Windows 2000 name.

PPE recreates this group if you delete it. To stop PPE from creating the group, make the two **days** values equal in all policies.
Choose a value from the **Mode** drop-down list to specify how PPE handles expired passwords. The Standard mode forces all users with expired passwords to change their password during logon. The Transitional modes force a percentage of users with expired passwords to change their password during logon. The Warning mode warns users that their password has expired without forcing them to change it.

Click the **E-mail** tab to configure the e-mail message options.

Use the Warning and Transitional modes to gradually introduce a new password policy. These modes reduce the number of forced password changes, allowing the helpdesk to deal with any extra calls relating to the new policy. Switch to the Standard mode after most users have had a chance to change their password.

It takes approximately 50 days for all users with expired passwords to be forced to change them in the 2% Transitional mode (2% every day). The 5% Transitional mode reduces this to 20 days, and the 10% Transitional mode further reduces it to 10 days. The selection algorithm is randomized, so these are estimates only. You must switch to the Standard mode to ensure that all old passwords will expire.

Users with expired passwords are always prompted to change their password, even in the Transitional and Warning modes. Users can ignore the prompt to change their password unless they are being forced to change it.

The password expiry prompt is a Windows client feature, and is displayed even if the **Password Policy Client** is not installed. Windows clients display the prompt 5 days before passwords expire by default (14 days prior to Windows 7 and 2008 R2). You can alter this behavior with the **Interactive logon: Prompt user to change password before expiration** security setting in Group Policy.

PPE expires passwords at 1:00 AM every day on the domain controller holding the PDC emulator operations master role. It sets "User must change password at next logon" for users whose password has expired, or is due to expire on that day. PPE does not expire passwords if the Maximum Age rule is in Warning mode, or for users with "Password never expires" set in Active Directory. Some passwords will not expire immediately when the Maximum Age rule is in a Transitional mode.
Minimum Age Rule

The Minimum Age rule stops users from quickly cycling through a series of passwords in order to evade the History and Similarity rules. This rule can only be enforced by domain policies.

Select the Enabled check box to enable the Minimum Age rule.

Choose a value from the days drop-down list to specify how many days users must wait before changing their password.

Click the Messages tab to customize the Password Policy Client rule inserts. Only the Reason insert is shown because minimum age requirements are not included in the Password Policy message.

The Minimum Age rule is unique because users cannot comply with it by choosing a different password; they must wait until the required number of days has elapsed. The Password Policy Client consequently handles rejections by this rule differently to other rules. Rather than displaying the usual message components, the PPC only displays the Minimum Age rule's Reason insert. The Rejection Reason template, macros, and inserts from other rules are not displayed when a password change is denied by the Minimum Age rule.

The Minimum Age rule is not enforced during policy testing, but the test log does show the user's password age. A log entry is also added if the Minimum Age rule would have rejected the password change.
Length Rule

The Length rule rejects passwords that contain too few or too many characters. Longer passwords are generally stronger, so only specify a maximum password length if password compatibility must be maintained with a system that cannot accept long passwords.

Select the **Enabled** check box to enable the Length rule.

Select the **at least** option to specify the minimum number of characters that passwords must contain. Choose the minimum number of characters from the drop-down list.

Select the **no more than** option to specify the maximum number of characters that passwords can contain. Choose the maximum number of characters from the drop-down list.

Select the **between** option to specify the minimum and maximum number of characters that passwords can contain. Choose the minimum number of characters from the first drop-down list, and the maximum from the second drop-down list.

Click the **Messages** tab to customize the Password Policy Client rule inserts.
Complexity Rule

The Complexity rule rejects passwords that do not contain characters from a variety of character sets. Using several character types can make passwords more difficult to crack.

Select the **Enabled** check box to enable the Complexity rule.

Choose the number of required character sets from the drop-down list. Passwords will be rejected if they do not contain characters from at least the specified number of character sets.

Choose the available character sets by selecting the check boxes beside the character set names. The number of available character sets must be equal to or greater than the number of required character sets.

Select the **Passwords must always comply with this rule** check box to make the Complexity rule mandatory. PPE rules are mandatory by default, but can be made optional by changing the **Reject passwords that do not comply with** value in the **Policy Properties** page. A mandatory rule can still be disabled when a passphrase is used.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

The Complexity rule uses custom character set definitions from the **Character rules**, even if the Character rules are disabled.
Dictionary Rule

The Dictionary rule rejects passwords that are vulnerable to guessing, hybrid, and precomputed attacks. These attacks can crack weak passwords in seconds, and they can be very effective if passwords are based on common words.

There are two Dictionary rules in each password policy. You can use the second rule with a different dictionary file, or to enforce a more tolerant policy for passphrases by disabling the primary rule for long passwords.

Select the **Enabled** check box to enable the Dictionary rule.

Select the **Detect inclusion of non-alpha characters** check box if PPE should remove all non-alphabetic characters during analysis. This allows PPE to reject passwords such as "myp8ass8wor8d".

Select the **Detect character substitution** check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the **Bi-directional analysis** check box if PPE should additionally test passwords with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in their password. For example, a user may enter "drowssapym" instead of "mypassword".
Select the **Wildcard analysis** check box if PPE should search for wildcard templates in the dictionary file. Wildcard templates are specially formatted dictionary words that PPE uses to reject a range of passwords. The Dictionary rule supports two wildcard template formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>!!BAN*!!</td>
<td>Rejects passwords that start with BAN. For example: band, banish, ban, bank etc.</td>
</tr>
<tr>
<td></td>
<td>!!2*!!</td>
<td>Rejects passwords that start with the numeric character 2. For example: 2ABC, 2123 etc.</td>
</tr>
<tr>
<td>Suffix</td>
<td>!!*ING!!</td>
<td>Rejects passwords that end with ING. For example: pushing, howling, trying etc.</td>
</tr>
</tbody>
</table>

Partial matching is performed even if Wildcard analysis is disabled. For example, the dictionary word "**password**" will reject the passwords "My**Password**$$", "**Password**100", and "12**password**34" even if Wildcard analysis is disabled. Wildcard analysis should only be used to limit matching to the characters at the start or end of a password.

Enabling Wildcard analysis slightly increases search times, so only enable this option if the dictionary file contains wildcard templates. The sample dictionary file included with PPE does not contain any wildcard templates.

Choose a value from the **Tolerance** drop-down list to specify the maximum number of consecutive matching characters that PPE will tolerate before rejecting a password. For example, the dictionary word "**sword**", and the password "4**mysword**%" contain five consecutive matching characters (shown in bold type). PPE will reject this password if the tolerance is four (or lower), and accept it if the tolerance is five (or higher).

Click the **Browse** button to select a dictionary file, or type a path into the text box. The path can contain environment variables like %SystemRoot%. A sample dictionary is installed in the `\Program Files (x86)\Password Policy Enforcer\` folder. The dictionary file should be read from a local disk. Using a shared dictionary degrades performance, and could jeopardize security.

---

The `\Program Files (x86)` folder does not exist on 32-bit Windows, so move the dictionary into the `\Program Files\Password Policy Enforcer\` folder if you have 32-bit and 64-bit computers sharing a common PPE configuration.
Click the Sort button if the dictionary file is being used with PPE for the first time, or if words have been added to the file since it was last sorted. The PPE management console will sort and reformat the file so that PPE can use it. Sorting also removes duplicate words, so the sorted file may be smaller than the original.

Click the Messages tab to customize the Password Policy Client rule inserts. If both Dictionary rules have identical inserts, then only one of the inserts is shown in the corresponding PPC message if the password is rejected by both rules.

Sample Dictionary File
A sample dictionary file called DICT.TXT is installed in the \Program Files (x86) \Password Policy Enforcer\ folder. This file is sorted and ready to use. It contains approximately 257,000 words, names, and acronyms.

Creating a Custom Dictionary
You can add words to the sample dictionary file, or download larger dictionary files from the Internet. Always sort a dictionary file before using it with PPE, and make sure that all computers have a local copy of the updated and sorted file.

Dictionary File Replication
PPE does not distribute dictionary file updates to other computers, but you can use the Windows Distributed File System to ensure that all domain controllers have the latest dictionary file. Copy the dictionary file into the Sysvol share on one domain controller, and the Distributed File System will copy the file into the Sysvol share of all other domain controllers. Configure the Dictionary rule to read the file from \127.0.0.1\sysvol\your.domain\filename.txt

The path above only works if the computer has a Sysvol share. This won't be the case if you are using a workstation for policy testing, or if you are using PPE to enforce local policies. If you are using PPE for local policies and want all computers to receive dictionary file updates, then use the Sysvol share for file replication and a script or scheduled task to copy the file to a local folder.
Compromised Rule

The Compromised rule rejects passwords from prior breaches. These passwords should not be used as they are vulnerable to credential stuffing attacks.

Select the **Enabled** check box to enable the Compromised rule.

Click the ... (ellipsis) button beside each text box to select a hash file. You can also type a path into the text box. The path can contain environment variables like %SystemRoot%. Hash files should be read from a local disk. Using shared hash files degrades performance, and could jeopardize security.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

**Downloading and Preparing a Hash File**

The Compromised rule can use the data from [haveibeenpwned.com](https://haveibeenpwned.com). You can download the current data file from [https://haveibeenpwned.com/Passwords](https://haveibeenpwned.com/Passwords). Download the file sorted by prevalence.

Use the HIBPPrep utility to prepare the file for use with PPE. HIBPPrep copies the hashes to a new file without the prevalence information. The resulting file is about 30% smaller than the original. HIBPPrep can also create a smaller file with fewer hashes to enforce a less restrictive policy. Do not limit the file size due to performance concerns as the Compromised rule typically searches the whole file in under a millisecond and only uses a few kilobytes of memory.

You can download HIBPPrep from [https://www.anixis.com/ftp/ppe/HIBPPrep100.zip](https://www.anixis.com/ftp/ppe/HIBPPrep100.zip)

Further instructions are in the Readme.txt file inside the zip file.
Creating a Custom Hash File
You can create your own hash file for the Compromised rule. Each line should contain one SHA-1 hash in hexadecimal format (40 characters). Use uppercase hexadecimal characters, and save the file in the DOS/Windows format with a CR and LF character at the end of each line. Sort the hashes in ascending order. The file should not contain blank lines, but one blank line at the end is acceptable. Use the Test Policies page to ensure the file works correctly.

Hash File Replication
PPE does not distribute hash file updates to other computers, but you can use the Windows Distributed File System to ensure that all domain controllers have the latest hash files. Copy the hash files into the Sysvol share on one domain controller, and the Distributed File System will copy the files into the Sysvol share of all other domain controllers. Configure the Compromised rule to read the files from \127.0.0.1\sysvol\your.domain\filename.txt

The path above only works if the computer has a Sysvol share. This won’t be the case if you are using a workstation for policy testing, or if you are using PPE to enforce local policies. If you are using PPE for local policies and want all computers to receive hash file updates, then use the Sysvol share for file replication and a script or scheduled task to copy the file to a local folder.
History Rule

The History rule rejects passwords that are identical to recently used passwords. Password reuse should be avoided because it defeats the purpose of regular password changes. PPE can stop users from reusing passwords for a specified number of password changes or a number of days.

Select the **Enabled** check box to enable the History rule.

Select the **one of the last** option to stop passwords from being reused for a specified number of password changes. Choose the number of password changes from the drop-down list.

Select the **password used in the last** option to stop passwords from being reused for a specified number of days. Type the number of days in the text box.

Choose an item from the **Hash function** drop-down list. Argon2 is recommended for best security. The Argon2 option uses 100,000 times more computing power to create a hash, so an attacker needs 100,000 more computing power to crack Argon2 hashes. Argon2 increases password change times by 400%, so a domain controller that can handle 1,000 password changes a minute with SHA-256 can be expected to handle 250 password changes a minute with Argon2. All numbers are approximate. Use Argon2 if your domain controllers can handle the load.

---

**Changing the Hash function** does not modify existing history records. It sets the function to be used for new password history records. If a user has Argon2 and SHA-256 hashes in their password history, then PPE calculates both the Argon2 and SHA-256 hashes during a password change to ensure the new password is not in the password history.
The History rule is normally not enforced when a password is reset. Select the **Enforce this rule when a password is reset** check box to override the default behavior. You must also select the **Enforce policy when password is reset** option in the [PPS Properties](#) page to enforce this rule when a password is reset.

Click the **Messages** tab to customize the Password Policy Client [rule inserts](#).

---

The History rule is not enforced when testing passwords from the [Test Policies](#) page.

PPE updates a user’s password history whenever their password changes. The password history is updated even if PPE or the **assigned policy** is disabled. A user’s password history is deleted if the user does not have an assigned policy, or if the History rule is disabled at the time of the password change.

PPE’s password history is stored in Active Directory for domain user accounts, and in the registry for local user accounts. You can create a new Active Directory attribute for the password history, or configure PPE to use an existing attribute. Disable PPE’s History rule if you do not want PPE to store the password history.

---

PPE does not store passwords in the password history, it only stores the Argon2 or SHA-256 hashes. A salt protects the hashes from precomputed attacks, including rainbow tables. If you do not want PPE to store a password history, then leave the History rule disabled. You can use the Windows History rule together with PPE’s other rules to enforce your password policy.

PPE can store up to 100 password hashes for each user, but it only stores the minimum needed to enforce the current password policy. For example, if PPE is configured to reject the last 24 passwords, then only the last 24 password hashes are stored. Reconfiguring PPE to reject the last 30 passwords will not have an immediate effect as only 24 password hashes are currently stored. The full effect of the new configuration will be realized after users change their passwords six more times as PPE will then have 30 stored password hashes for each user.

Leave both the Windows and PPE History rules enabled when transitioning from one to the other. This allows the old rule to enforce the policy until the new rule has built up its password history. The old rule can be disabled after users have completed the required number of password changes to enforce the new rule.
As PPE is limited to storing the last 100 password hashes, it is possible for the History rule to run out of storage space before the specified number of days. Use the **Minimum Age rule** to avoid this problem. For example, if the History rule is configured to not allow password reuse for 365 days, then set the minimum password age to four or more days. Even if a user changes their password every four days, they can only perform 91 password changes in 365 days.

**Creating a new attribute for the password history**

Windows stores a domain user's password history in two Active Directory attributes, but these attributes cannot be used by other applications. PPE can store the password history in a new or existing attribute. A new attribute is recommended, but you can use an existing attribute if you do not want to extend the AD schema. An AD attribute is only needed for domain user accounts because the password history for local user accounts is stored in the registry.

---

**PPE’s password history attribute is confidential to stop authenticated users from accessing the password history of other users.**

Microsoft Article [922836](https://support.microsoft.com/en-us/help/922836/understand-confidential-attributes-in-active-directory) has more information about confidential attributes.

Confidential attributes have additional protection in Active Directory, but they are not as well protected as the Windows password history attributes. There is a higher risk of unauthorized access to the password history if it is stored outside the Windows password history attributes.

---

To create a new Active Directory attribute for the password history:

1. Log on to the server holding the Schema Operations Master role with an account that is a member of the Schema Admins group.
2. Open a Command Prompt window to the PPE installation folder. (`C:\Program Files (x86)\Password Policy Enforcer\`)
3. Type the following command:

   ```
   ldifde -i -f History.ldf -c "DC=X" "DC=yourdomain,DC=yourdomain"
   ```

   Replacing the last parameter with your domain’s DN.
4. Press ENTER and check the output for errors.
Using an existing attribute for the password history
PPE can store the password history in an existing attribute. The desktopProfile attribute is well suited because it is not used by Windows. Other attributes are also suitable if they are not being used. Send a e-mail to support@anixis.com if you would like to use an existing attribute for the password history.

Password histories for local user accounts
The password histories of local user accounts are stored in the HKLM\SECURITY\PPE Password History\ registry key. Users are not granted access the HKLM\SECURITY\ registry key by default, so a user cannot read the password history of any user (including themselves). This is also true for members of the Administrators group, but administrators can change the default permissions. If an administrator accesses the password history they might be able to extract the hashes for cracking, but they cannot extract the passwords directly because the password history does not contain any passwords.

⚠️ The password history of a local user account is not automatically deleted when the user account is deleted. If a local user account is deleted, then another local user account is created on the same computer with the same username, the new user will inherit the deleted user’s password history. The default registry permissions stop users from accessing their own password history, so it is difficult for the new user to use this information. They could try to guess the deleted user’s password during a password change to see if it is rejected by the History rule, but they would only have a few attempts to guess correctly before the old hashes are overwritten with new hashes. The user’s current password is validated, and the Windows Minimum Age rule is enforced before the password history is checked, so every compliant and incorrect password guessed will overwrite one hash in the password history.

This information applies only to local user accounts. The password history for domain user accounts is deleted when users are deleted.
Similarity Rule

The Similarity rule rejects passwords that are similar to a user's current password. Password similarity may indicate that a user is serializing their passwords. For example, "password1", "password2", "password3", etc. Password serialization should be avoided because it may allow an attacker to guess the new password.

Select the **Enabled** check box to enable the Similarity rule.

Select the **Detect character substitution** check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the **Bi-directional analysis** check box if PPE should additionally test passwords with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in their password. For example, a user may enter "drowssapdloym" instead of "myoldpassword".

Choose a value from the **Tolerance** drop-down list to specify the maximum number of consecutive matching characters that PPE will tolerate before rejecting a password. For example, the two passwords "oldpasswd" and "newpasswd" contain six consecutive matching characters (shown in bold type). PPE will reject the new password if the tolerance is five (or lower), and accept it if the tolerance is six (or higher). Choose the **Auto** value to reject passwords that contain the user's entire current password.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

---

This rule is only enforced if the **Password Policy Client** is installed. It does not store or transmit passwords or password hashes.
User Logon Name Rule

The User Logon Name rule rejects passwords that are similar to a user’s logon name (user name). Passwords that are similar to a user’s logon name are not desirable because they are easily guessed.

Select the Enabled check box to enable the User Logon Name rule.

Select the Detect character substitution check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the Bi-directional analysis check box if PPE should additionally test passwords with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in their password. For example, a user may enter "emannogolym" instead of "mylogonname".

Choose a value from the Tolerance drop-down list to specify the maximum number of consecutive matching characters that PPE will tolerate before rejecting a password. For example, the logon name "maryjones", and the password "Jones town" contain five consecutive matching characters (shown in bold type). PPE will reject this password if the tolerance is four (or lower), and accept it if the tolerance is five (or higher). Choose the Auto value to reject passwords that contain the user’s entire logon name.

Click the Messages tab to customize the Password Policy Client rule inserts.
User Display Name Rule

The User Display Name rule rejects passwords that are similar to a user's Active Directory display name (full name for local accounts). Passwords that are similar to a user's display name are not desirable because they are easily guessed.

Select the **Enabled** check box to enable the User Display Name rule.

Select the **Detect character substitution** check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the **Bi-directional analysis** check box if PPE should additionally test passwords with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in their password. For example, a user may enter "emanyalpsidym" instead of "mydisplayname".

Choose a value from the **Tolerance** drop-down list to specify the maximum number of consecutive matching characters that PPE will tolerate before rejecting a password. For example, the display name "John Smithers", and the password "12smithtown" contain five consecutive matching characters (shown in bold type). PPE will reject this password if the tolerance is four (or lower), and accept it if the tolerance is five (or higher). Choose the **Auto** value to reject passwords that contain the user's entire display name.

Click the **Messages** tab to customize the Password Policy Client rule inserts.
Character Rules

PPE has seven Character rules that reject passwords if they contain, or do not contain certain characters. These rules can increase password strength or ensure password compatibility with other systems.

All the Character rules work identically, but each has their own default character set. A character set is the collection of characters that each rule searches for when checking a password. You can use the Character rules with their default character sets, or define your own. The default character sets are:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Default character set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha Lower</td>
<td>Lowercase alphabetic (a - z)</td>
</tr>
<tr>
<td>Alpha Upper</td>
<td>Uppercase alphabetic (A - Z)</td>
</tr>
<tr>
<td>Alpha</td>
<td>Uppercase and lowercase alphabetic (a - z &amp; A - Z)</td>
</tr>
<tr>
<td>Numeric</td>
<td>Numerals (0 - 9)</td>
</tr>
<tr>
<td>Special</td>
<td>All characters not included above</td>
</tr>
<tr>
<td>High</td>
<td>All characters above ANSI 126</td>
</tr>
<tr>
<td>Custom</td>
<td>No default characters</td>
</tr>
</tbody>
</table>

Select the **Enabled** check box to enable the Character rule.

Select the **contain** option if this rule should ensure that new passwords contain certain characters. Only one character is required by default, but you can specify a different value by choosing the required number of characters from the drop-down list beside the **contain** option.
Select the **not contain any**... option if this rule should ensure that new passwords do not contain certain characters.

If you want to restrict this rule to certain character positions, then choose the starting position from the **in position** drop-down list, and the ending position from the **to** drop-down list. For example, you may want to enforce a rule that requires a numeric character in the second character position to maintain compatibility with some other system.

Select the **Embedded** check box if users are required to embed these characters within their passwords. For example, the passwords "12hello", "1hello", and "hello$987" do not contain any embedded numeric characters, but these passwords do contain embedded numeric characters (shown in bold type): "he7llo", "4he3llo", "23hello7$45". Embedded numeric and special characters can help to protect passwords from cracking attacks.

Type a character set name in the **Name** text box. The Password Policy Client displays the new name, but the PPE management console continues to display the original character set name.

Type some characters in the **Characters** text box if you would like to define a custom character set to replace the default. For example, enter "AaEeliOoUu" to create a vowel character set.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

---

The **First Character**, **Last Character**, and **Complexity** rules are easier to configure, and easier for users to understand. Use these rules instead of the Character rules if they can enforce your desired policy.
Enforcing complex character requirements

Character rules can be combined to enforce complex password requirements. For example, you may need to enforce a policy such as "passwords must contain a numeric character, but not in the first two positions" to ensure compatibility with some other system. This is done by using two of the Character rules. The first rule (shown on the left below) ensures that passwords contain at least one numeric character. The second rule ensures that passwords do not contain any numeric characters in the first two positions.

PPE has only one Numeric rule, so the second requirement must be enforced by one of the other rules. Any unused Character rule can be used for this purpose by changing its name and default character set. In this example, the Custom rule was chosen as it was not being used. The character set name was changed to "numeric", and the character set was defined as "1234567890".
First and Last Character Rules

The First and Last Character rules reject passwords that do not begin or end with an appropriate character. These rules are typically used to ensure password compatibility with other systems.

Select the **Enabled** check box to enable the First or Last Character rule.

Select the **begin** (First Character rule) or **end** (Last Character rule) option if you want to specify the **acceptable** character sets.

Select the **not begin** (First Character rule) or **not end** (Last Character rule) option if you want to specify the **unacceptable** character sets.

Choose one or more character sets by selecting the check boxes beside the character set names.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

The First and Last Character rules use custom character set definitions from the [Character rules](#), even if the Character rules are disabled.
Keyboard Pattern Rule

The Keyboard Pattern rule rejects passwords that contain keyboard patterns such as "qwerty". Passwords should not contain keyboard patterns because they are vulnerable to cracking attacks and shoulder surfing (observing users as they enter their password).

The examples for this rule are taken from a US keyboard layout. These patterns may not exist on other keyboard layouts.

Select the **Enabled** check box to enable the Keyboard Pattern rule.

Choose the pattern detection mode from the **keyboard patterns** drop-down list. The Horizontal mode only detects horizontal patterns such as "qwerty" and "zxcvbn". The Vertical mode only detects vertical patterns such as "4esz" and "4rfc". The "Horizontal or vertical" mode detects patterns in both axes.

Select the **Detect direction change** check box if PPE should detect keyboard patterns that contain direction changes. For example, "qwewq" and "4rfr4" are both recognized as five-character keyboard patterns if direction change detection is enabled.

PPE detects direction changes in both axes if the pattern detection mode is set to "Horizontal or vertical". For example, "qaweds", "qwedsa", "qwedcy", and "qwsazx" are all recognized as six-character keyboard patterns if direction change detection is enabled and the pattern detection mode is set to "Horizontal or vertical".
Select the **Detect key repeat** check box if PPE should detect keyboard patterns that contain repeated keystrokes. For example, "qwwert" and "qwwwer" are both recognized as six-character keyboard patterns if key repeat detection is enabled.

Select the **Detect key skip** check box if PPE should detect keyboard patterns that contain a horizontally skipped key. For example, "qwryui" is recognized as a six-character keyboard pattern if key skip detection is enabled.

Choose a value from the **Tolerance** drop-down list to specify the longest keyboard pattern that PPE will tolerate before rejecting a password. For example, the password "myqwerpw" contains a four-character keyboard pattern (shown in bold type). PPE will reject this password if the tolerance is set to three (or lower), and accept it if the tolerance is set to four (or higher).

Click the **Keyboard Layouts** button to select which keyboard layouts PPE uses for pattern detection. You must select at least one layout.

Click the **Messages** tab to customize the Password Policy Client rule inserts.

Modifier keys such as Shift and AltGr will not evade pattern detection.

Key positions can differ, even in keyboards with matching layouts. The Keyboard Pattern rule may not detect some patterns because of these differences. Please report any missed patterns to support@anixis.com.
Character Pattern Rule

The Character Pattern rule rejects passwords that contain character patterns such as "abcde". Passwords should not contain character patterns because they can weaken the password.

Select the **Enabled** check box to enable the Character Pattern rule.

Select the **Detect character substitution** check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the **Bi-directional analysis** check box if PPE should additionally test passwords with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in their password. For example, a user may enter "edcba" instead of "abcde".

Choose a value from the **Tolerance** drop-down list to specify the longest pattern that PPE will tolerate before rejecting a password. For example, the password "passwordwxyz" contains a four-character pattern (shown in bold type). PPE will reject this password if the tolerance is set to three (or lower), and accept it if the tolerance is set to four (or higher). Choose the **Auto** value if passwords should be rejected if they only contain a single, continuous, character pattern. For example, "abcde" would be rejected, but "abcdz" and "abc123" would not.

Click the **Character Patterns** button to select which character patterns PPE will detect. You must select at least one pattern.

Click the **Messages** tab to customize the Password Policy Client rule inserts.
Repeating Pattern Rule

The Repeating Pattern rule rejects passwords that contain repeating character sequences. Users may use repetition to artificially increase the length of a short password. This should be avoided as it can weaken the password.

Select the **Enabled** check box to enable the Repeating Pattern rule.

Select the **Detect character substitution** check box if PPE should reject passwords that rely on character substitution to comply with this rule.

Select the **Bi-directional analysis** check box if PPE should search for patterns with their characters reversed. Enabling bi-directional analysis stops users from circumventing this rule by reversing the order of characters in the repeated pattern. For example, a user may enter "password@drowssap" instead of "password@password".

Choose a value from the **Tolerance** drop-down list to specify the maximum number of consecutive matching characters that PPE will tolerate before rejecting a password. For example, the password "**mypwd4mypwd5**" contains a five-character repeating pattern (shown in bold type). PPE will reject this password if the tolerance is four (or lower), and accept it if the tolerance is five (or higher).

Click the **Messages** tab to customize the Password Policy Client rule inserts.
Repeating Characters Rule

The Repeating Characters rule rejects passwords that contain excessive character repetition. Reducing character repetition can increase resistance to both brute-force and dictionary cracking algorithms. The Repeating Characters rule is not case sensitive, so "mypaSssSword" contains four consecutive repeating characters (SssS).

Select the Enabled check box to enable the Repeating Characters rule.

Choose the maximum number of consecutive repeating characters that passwords can contain from the **consecutive repeating characters** drop-down list.

Click the Messages tab to customize the Password Policy Client rule inserts.
Unique Characters Rule

The Unique Characters rule rejects passwords that do not contain a minimum number of unique characters. For example, the password "aaaaaaa" only contains one unique character (a), whereas "mypassword" contains nine unique characters (mypassword). Increasing the number of unique characters in a password can increase password strength by avoiding repetitive sequences that are easily guessed. The Unique Characters rule is case sensitive, so "LoOpHole" contains seven unique characters (LoOpHle).

Select the Enabled check box to enable the Unique Characters rule.

Choose the minimum number of unique characters that passwords must contain from the unique characters drop-down list.

Click the Messages tab to customize the Password Policy Client rule inserts.
The Password Policy Client

The Password Policy Client reduces user frustration and password related helpdesk calls by helping users to choose a compliant password. You do not have to install the Password Policy Client to use PPE, but the Similarity rule is only enforced if the PPC is installed.

The PPC helps users to choose a compliant password by explaining the password policy to them, and by telling them why their password was rejected. If the PPC is not installed, then users will see the default Windows error message when their password is rejected.

The PPC displays the password policy during a password change so that users can see the policy while they choose their password. The PPC also displays a detailed rejection message to explain why a password was rejected. Both these messages are customizable.

The Password Policy Client does not modify any Windows system files. It also does not send passwords or password hashes over the network.
Installing the PPC

The Password Policy Client is compatible with Windows XP, Vista, 7, 8, and 10. It is also compatible with Windows Server 2003, 2008, 2012, and 2016. The PPC can be used with Remote Desktop Services on these operating systems.

System Requirements

- Windows XP, Vista, 7, 8, 8.1, or 10.
- One Megabyte free disk space.
- 256 Kilobytes free RAM (per session if using Remote Desktop Services).

You can install the PPC manually by running the PPE installer (PPE910.exe) and choosing the Express Setup option if you only need to install it on a few computers. If you have many computers, then follow the instructions below to perform an automated installation with Group Policy, or use your regular software distribution tool to do the same.

Create a Distribution Point

A distribution point can either be a UNC path to a server share, or a DFS (Distributed File System) path. You can use the distribution point you created earlier for PPE to distribute the PPC. If you did not create a distribution point for PPE, then create one now. To create a PPC distribution point:

1. Log on to a server as an administrator.
2. Create a shared network folder to distribute the files from.
3. Give the "Domain Computers" security group read access to the share, and limit write access to authorized personnel only.
Copy PPECIt910.msi into the Distribution Point

1. Start the PPE installer (PPE910.exe).
2. Read the license agreement, and then click Yes if you accept all the license terms and conditions.
3. Select the Advanced option, and then click Next.
4. Right-click the PPECIt910.msi icon, click Copy, and then paste the file into the distribution point.
5. Give the "Domain Computers" security group read access to the PPECIt910.msi file in the distribution point.
6. Click Finish.
Create a Group Policy Object
1. Start the Group Policy Management Console (gpmc.msc).
2. Expand the forest and domain items in the left pane.
3. Right-click the domain root node in the left pane, and then click Create a GPO in this domain, and Link it here...
4. Type “Password Policy Client”, and then press ENTER.

Edit the Group Policy Object
1. Right-click the Password Policy Client GPO, and then click Edit...
2. Expand the Computer Configuration, Policies, and Software Settings items in the left pane.
3. Right-click the Software installation item, and then select New > Package...
4. Type the full UNC path to PPEClt910.msi in the Open dialog box. You must enter a UNC path so that other computers can access this file over the network. For example, \file server\distribution point share\PPEClt910.msi
5. Click Open.
6. Select the Assigned deployment method, and then click OK.

7. Close the Group Policy Management Editor.
Complete the Installation
Restart each computer to complete the installation. Windows installs the Password Policy Client during startup.

Testing the PPC
Test the Password Policy Client by logging on to a computer and pressing the CTRL + ALT + DEL keys and clicking the **Change a password** item. If you do not see the password policy, it could be because a PPE policy has not been **assigned** to you, or because the **firewall rules** have not been created.

---

The Password Policy Client does not store or send passwords or password hashes over the network. An attacker cannot determine user passwords by sniffing the communication protocol. The protocol is also encrypted by default for additional protection.
Creating Firewall Rules for the PPC

You may need to create firewall rules for the Password Policy Client if your domain controllers are running a software (host) firewall, or if the PPC and PPS communicate through a firewall. Firewall rules are not necessary for local policies because the PPC and PPS are on the same computer.

Windows Firewall

If Windows Firewall is enabled on your domain controllers, then you must create a port exception to allow connections to the Password Policy Server. Windows Firewall is enabled by default on Windows Server 2008 and later. To create the port exception on all domain controllers:

1. Use the Group Policy Management Console (gpmc.msc) to display the GPOs linked to the Domain Controllers OU.
2. Right-click the Password Policy Enforcer GPO, and then click Edit... You need to create the GPO if you chose the Express Setup option.
4. Click Domain Profile in the left pane, and then double-click Windows Firewall: Define inbound port exceptions in the right pane.
5. Select the **Enabled** option, and then click **Show...**

6. Type "1333:UDP:*:enabled:Password Policy Enforcer" (without quotes) in the port exceptions list.

7. Click **OK** until you return to the Group Policy Management Editor.

8. Close the Group Policy Management Editor.
Other Firewalls

Use the information on this page to create appropriate rules for your firewall that allow the Password Policy Client and Password Policy Server to communicate through the firewall.

The Password Policy Client initiates a request by sending a datagram with the following attributes to the Password Policy Server:

- **Protocol**: UDP
- **Source address**: Client computer IP address
- **Source port**: Any
- **Destination address**: Domain controller IP address
- **Destination port**: 1333

The Password Policy Server responds by sending a datagram with the following attributes back to the Password Policy Client:

- **Protocol**: UDP
- **Source address**: Domain controller IP address
- **Source port**: 1333
- **Destination address**: Client computer IP address
- **Destination port**: Any

If your firewall performs Stateful Packet Inspection, then only create a rule for the request datagram as the firewall will automatically recognize and allow the response datagram.
Customizing PPC Messages

The Password Policy Client displays three messages to help users choose a password:

- The Password Policy message is shown as the user changes their password. This message explains the password policy to the user.
- The Rejection Reason message is shown if a password does not comply with the PPE password policy. This message tells the user why their password was rejected.
- The Generic Rejection message is shown if PPE does have a specific reason for the rejection, generally because the password does not comply with the Windows password policy.

PPC Message Components

PPC messages are built using templates, macros, and inserts. The image below shows a sample policy message with the template in blue, a macro in green, and policy inserts in white.

```
Your new password must:
- not match one of your last 24 passwords
- not be similar to your current password
- not be similar to your logon name
- not be similar to your name
- contain a numeric character
- contain a special character
- not contain a keyboard pattern like qwerty
- contain at least 9 characters

You may not have to comply with all these rules if your password contains 30 or more characters.

Call the help desk on 555-555-5555 if you have difficulty choosing a password.
```
Customizing Message Templates

Each PPE password policy has three message templates, one for each of the PPC messages. To edit a policy's message templates:

1. Click the **Policies** item to display the [Policies view](#).
2. Click the desired policy in the right pane of the management console.
3. Click **Properties** in the right pane of the management console.
4. Click the **Messages** tab.
5. Choose a language from the **Language** drop-down list.

The default **Password Policy** and **Rejection Reason** templates contain macros. PPE replaces macros with password policy information. The most important macros are [POLICY] and [REASON]. PPE replaces them with [rule inserts](#).

Customizing Rule Inserts

Rule inserts allow the Password Policy and Rejection Reason messages to display the most appropriate information for each user. Most PPE rules have a Policy and Reason insert. The Policy insert is used by the [POLICY] macro, and the Reason insert is used by the [REASON] macro. To edit a rule's inserts:

1. Click the **Policies** item to display the [Policies view](#).
2. Double-click the desired policy in the right pane of the management console.
3. Double-click the desired rule to display the Rule Properties page.
4. Click the **Messages** tab.
5. Choose a language from the **Language** list.
6. Edit the rule inserts in the **Policy** and **Reason** text boxes.

The **Policy** and **Reason** text boxes are blank by default because PPE automatically generates rule inserts from the rule's properties. If you do not want PPE to automatically generate the rule inserts, then enter the desired text in the **Policy** and **Reason** text boxes.

---

*Use the \n escape sequence to start a new line in a message template or rule insert (PPC V5.1 and later).*

*Inserts and lines starting with two or more spaces, a minus, and a space are shown with a bullet to the left (PPC V8.0 and later).*
Multilingual Messages

The Password Policy Client initially displays all messages in English, but you can configure it to display messages in 30 other languages. To configure PPC for another language:

1. Configure message templates for the new language (see Customizing Message Templates).
2. Configure rule inserts for each enabled rule (see Customizing Rule Inserts).

Include the [POLICY] and [REASON] macros in the non-English message templates, but do not include any other macros. The images below show Japanese message templates, and a sample rule insert.

The Password Policy Client uses the Windows client language settings to determine which language to display.

You do not have to create a PPE policy for each language. Each policy can have messages defined in multiple languages.
Configuring the PPC

The Password Policy Client is self-configuring and does not require manual configuration in most cases. You may need to manually configure the PPC if:

- You want to install it in a disabled state to be enabled later.
- You want to change the display settings for small screens.
- The PPC displays policy messages in the wrong language.
- The default communication settings are not suitable (for example, if you change the default PPS Port).

PPE includes an administrative template to help configure the PPC. You can use Active Directory GPOs to configure many computers, or the Local Group Policy Editor to configure one computer. The PPC configuration is stored in the HKLM \SOFTWARE\Policies\ANIXIS\Password Policy Client\ registry key. To install the PPC administrative template:

1. Use the Group Policy Management Console (gpmc.msc) to display the GPOs linked at the domain level. If you are not using Active Directory, then open the Local Group Policy Editor (gpedit.msc) and skip the next step.
2. Right-click the Password Policy Client GPO, and then click Edit... You need to create the GPO if you installed the PPC manually.
3. Expand the Computer Configuration item.
4. Expand the Policies item if it is visible.
5. Right-click the Administrative Templates item, and then click Add/Remove Templates...
6. Click Add... and then browse to the PPE installation folder (\Program Files (x86)\Password Policy Enforcer)\)
7. Select PPEClt.adm, and then click Open.
8. Click Close.
To configure the Password Policy Client:

1. Use the Group Policy Management Console (gpmc.msc) to display the GPOs linked at the domain level. If you are not using Active Directory, then open the Local Group Policy Editor (gpedit.msc) and skip the next step.

2. Right-click the **Password Policy Client** GPO, and then click **Edit**.

3. Expand the **Computer Configuration, Policies** (if it exists), **Administrative Templates, Classic Administrative Templates (ADM)**, **Password Policy Enforcer**, and **Password Policy Client** items.

4. Double-click one of the settings in the right pane, and then configure the available options. Information about each option is shown in the Help box.

5. Click **OK**.

6. Close the Group Policy Management Editor.

If you are using an Active Directory GPO to configure the PPC, then the configuration is applied to all computers in the domain. This does not happen immediately. You can force an immediate refresh of Group Policy on the local computer with this command: `gpupdate /target:computer`
Changing the Default Display Settings

The Windows 10 Change Password screen has less space for the Password Policy message than earlier Windows versions. Users may need to scroll to see the message if their screen is small, or if their computer is set to use large fonts.

The Password Policy Client for Windows 10 maximizes the available screen space by hiding non-essential user interface elements on small screens. It can also display the Password Policy message in a message box to draw attention to the password policy.

You can change the default display settings to control which user interface elements are hidden, and the point at which they are hidden. The display of the Password Policy message box is also configurable. To change the default display settings for the Password Policy Client on Windows 10:

1. Use the Group Policy Management Console (gpmc.msc) to display the GPOs linked at the domain level. If you are not using Active Directory, then open the Local Group Policy Editor (gpedit.msc) and skip the next step.
2. Right-click the Password Policy Client GPO, and then click Edit...
3. Expand the Computer Configuration, Policies (if it exists), Administrative Templates, Classic Administrative Templates (ADM), Password Policy Enforcer, and Password Policy Client items.
4. Double-click the Display settings (Windows 10) setting in the right pane of the Group Policy Management Editor. Information about each option is shown in the Help box.
The PPE Mailer

PPE can send e-mail reminders to domain users before their passwords expire. This is especially useful for users who logon infrequently, and for remote users who access the network without logging on to the domain. You must install the PPE Mailer and configure the e-mail delivery and e-mail message options to send e-mail reminders to users.

Add your e-mail address to a service account, and the PPE Mailer will remind you to change the service account password before it expires.

Installing the PPE Mailer

The PPE Mailer is not installed by default. Only install it on one server in each domain. The PPE Mailer can be installed on any server, including a domain controller. To install the PPE Mailer:

1. Start the PPE installer (PPE910.exe).
2. Read the license agreement, and then click Yes if you accept all the license terms and conditions.
3. Select the Advanced option, and then click Next.
5. If you are prompted to Modify, Repair, or Remove the installation, then select Modify and then click Next. Skip to step 11. Do not disable the other features as described below.
6. Click Next when the PPE Installation Wizard opens.
7. Select I accept the license agreement, and then click Next.
8. Select the Custom option, and then click Next.
9. Click the icon beside the Password Policy Server feature, and then click Entire feature will be unavailable.
10. Repeat the previous step for the Management Console, Documentation, and Dictionaries features unless you also want to configure PPE from this server.
11. Click the icon beside the PPE Mailer Service feature, and then click Will be installed on local hard drive.
12. Click Next twice.
13. Wait for the PPE Mailer to install, and then click Finish twice.
E-mail Delivery Options

You must configure the e-mail delivery options in the PPS Properties page before the PPE Mailer will send e-mail to users. To configure the e-mail delivery options:

1. Click the PPS item to display the PPS view.
2. Click PPS Properties in the right pane of the management console.
3. Click the e-mail tab.

Select the Disable e-mail reminders option to disable e-mail delivery.

Select the Send e-mail to an SMTP server option to have the PPE Mailer send e-mails directly to an SMTP server. Type the name or IP address of an SMTP server in the Server text box, and the SMTP port number in the Port text box.

Select the Save e-mail to a pickup folder option to have the PPE Mailer save e-mails to a folder for later delivery by a mail server. Click the Browse button to select a folder. The mail server must monitor this folder for new e-mail.

Saving e-mail to a pickup folder is the fastest and most reliable delivery method. Use this option if your mail server supports pickup folders.

The PPE Mailer sends e-mails at 2:00 AM every day. Check the Windows Application Event Log to monitor its progress. You can also run the PPE Mailer from the command line to send e-mail immediately, or to troubleshoot problems.
E-mail Message Options

E-mail message options are set for each password policy from the Maximum Age rule properties page. To configure the e-mail message options for a policy:

1. Click the Policies item to display the Policies view.
2. Double-click the desired policy in the right pane of the management console.
3. Double-click the Age (Max) rule.
4. Select the Enabled check box to enable the Maximum Age rule.
5. Choose a value from the Days and Mode drop-down lists.
6. Click the E-mail tab.

Choose values from the days drop-down lists to specify when e-mails will be sent. By default, e-mails are sent 14, 7, and 2 days before a user’s password expires. Choose the first item in a list (blank) to send fewer than three e-mails.

Type the name and e-mail address you wish to appear in the e-mail’s From field in the From text box. The correct format is “Display Name” <mailbox@domain.com>

Type the text for the e-mail’s Subject field in the Subject text box.

Type the body of the e-mail in the large text box. The e-mail is sent as plain text unless the body includes the <html> tag. If sending e-mail as HTML, you must include the complete HTML document starting with <html> and ending with </html>. If the body is too long to fit in the text box, type a path to a file like this: file:C:\path\filename.ext

The path can contain environment variables like %SystemRoot%. Do not use quotes for long filenames and do not include any other text. The PPE Mailer will read the e-mail body from the specified file.
The e-mail's subject and body can contain various macros. Use these macros to personalize the e-mail.

<table>
<thead>
<tr>
<th>Macro</th>
<th>Replaced with</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LOGON_NAME]</td>
<td>User's logon name</td>
</tr>
<tr>
<td>[FIRST_NAME]</td>
<td>User's first name</td>
</tr>
<tr>
<td>[LAST_NAME]</td>
<td>User's last name</td>
</tr>
<tr>
<td>[DAYS_TO_EXPIRY]</td>
<td>Days until password expires</td>
</tr>
<tr>
<td>[EXPIRY_DATE]</td>
<td>Expiry date in short format</td>
</tr>
<tr>
<td>[EXPIRY_DATE_LONG]</td>
<td>Expiry date in long format</td>
</tr>
<tr>
<td>[EXPIRY_DAY]</td>
<td>Expiry day (1 to 31)</td>
</tr>
<tr>
<td>[EXPIRY_DAY_NAME]</td>
<td>Expiry day (Monday, Tuesday, ...)</td>
</tr>
<tr>
<td>[EXPIRY_MONTH]</td>
<td>Expiry month (1 to 12)</td>
</tr>
<tr>
<td>[EXPIRY_MONTH_NAME]</td>
<td>Expiry month (January, February, ...)</td>
</tr>
</tbody>
</table>

**Command Line Interface**

You can run the PPE Mailer from the command line to deliver e-mail immediately, or to troubleshoot problems. PPEMail.exe is copied into the \Program Files (x86) \Password Policy Enforcer\ folder when the PPE Mailer is installed.

PPEMail.exe starts a simulation when run without any parameters. It finds users whose password will expire soon, but no e-mail is sent or saved to the pickup folder. Use the simulation mode to find common configuration errors that may stop the PPE Mailer from delivering e-mail.

Running PPEMail.exe with the /send parameter disables simulation mode. Any e-mails that are due to be sent today are sent immediately. PPEMail.exe can identify a wider range of configuration errors when run in this mode. Use the /send parameter judiciously to avoid sending duplicate e-mails to users.

To test e-mail delivery options without sending any e-mails to users, run PPEMail.exe with the /test parameter followed by your e-mail address. For example, PPEMail.exe /test maryjones@anixis.net. This will send one test e-mail to your mail server or pickup folder.
Troubleshooting

This section contains troubleshooting information for the most common support questions. You can also e-mail questions to support@anixis.com.

**Password policy assigned to some users is being enforced for all users.**
Check the **Default Policy** in the **PPS Properties** page. Users must comply with the default policy if no other policy is assigned to them. Select the first (blank) item in the drop-down list if you do not want a default policy.

**Password policy not displayed during a password change.**
Open the **Programs and Features** list in Control Panel on the computer you are changing the password from, and check if the **Password Policy Client** is in the list of installed programs. If it is not, then **install the Password Policy Client**.

If PPE is enforcing a **domain policy**, then search the Windows Application Event Log on every domain controller for events from Password Policy Enforcer. If there are no events from PPE since the last restart on any domain controller, then make sure that PPE is installed on that domain controller and restart it. Check the Windows Application Event Log again after the restart to ensure that PPE started. For **local policies**, search the Application Event Log on the local computer.

If there is a firewall between the client computer and the domain controllers (including Windows Firewall), then you must **create firewall rules** to allow the PPC and PPS to communicate. Windows firewall is enabled by default on Windows Server 2008 and later.

Use the **Test Policies** page to test a password for the user. Click the **Log** tab to see if a password policy is assigned to the user.

Make sure that the Password Policy Server is **enabled**.

Make sure that the Password Policy Client is **enabled**.

**PPE accepts passwords that do not comply with the policy.**
If PPE is enforcing a **domain policy**, then search the Windows Application Event Log on every domain controller for events from Password Policy Enforcer. If there are no events from PPE since the last restart on any domain controller, then make sure that PPE is installed on that domain controller and restart it. Check the Windows Application Event Log again after the restart to ensure that PPE started. For **local policies**, search the Application Event Log on the local computer.
Use the **Test Policies** page to test a password that PPE is accepting. Examine the test results and event log to determine why PPE accepted the password. See Policy Testing vs. Password Changes if the Test Policies page rejects the password.

If the **Enforce policy when password is reset** check box is not selected in the **PPS Properties** page, then PPE will not enforce the password policy for passwords that are reset from the Active Directory Users and Computers console, or the Local Users and Groups console. You should select this option during testing, or test password changes from the Windows Change Password screen.

PPE rejects passwords that comply with the policy.
Use the **Test Policies** page to test a password that PPE is rejecting. Examine the test results and event log to determine why PPE rejected the password. See Policy Testing vs. Password Changes if the Test Policies page accepts the password.

Set **User must change password at next logon** for the user and repeat the password change test. If the password is accepted, then either Windows or PPE is configured to enforce a minimum password age. Disable the Minimum Age rule in **Windows** and **PPE** to facilitate testing. If you cannot disable the Minimum Age rule, then set **User must change password at next logon** before every password change test to bypass the rule.

**Passwords that are accepted in the Test Policies page are rejected during a password change.**
See Policy Testing vs. Password Changes.
ANIXIS Password Reset and PPE/Web

ANIXIS Password Reset and PPE/Web 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.

Go to www.anixis.com for more information, or to download an evaluation copy.
License Agreement

ANIXIS PTY LTD (“ANIXIS”) IS WILLING TO LICENSE THIS SOFTWARE ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS SOFTWARE LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY. IF YOU DO NOT AGREE WITH THESE TERMS, THEN ANIXIS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU.

ANIXIS SOFTWARE LICENSE AGREEMENT AND WARRANTY STATEMENT

(End-User Trial Use License With Option For Extended Use/Redistribution Prohibited)

1. The Software.
The Software licensed under this Agreement consists of computer programs, data compilation(s), and documentation referred to as Password Policy Enforcer V9.x (the “Software”).

2. Trial Use.
You are authorized to use the Software for evaluation purposes during a trial use term of thirty (30) days, unless prior to the expiration of the trial use term this license is terminated by You for convenience or terminated by either party for material breach. You have the option to register for full use of the Software at any time by paying the required license fee. Registration will authorize You to use an unlocking key which will convert the Software to full use, subject to the terms and conditions of this agreement. Your use of the Software under this trial use license for any purpose after the expiration of the initial trial use term is not authorized without the prior written consent of ANIXIS. Upon expiration of the limited trial use term, the Software may automatically disable itself. Immediately upon expiration of the limited trial use term, You shall either register for full use of the Software, or destroy all copies of the Software and documentation.

3. Perpetual Term.
If You purchase a perpetual license, then the term of the license granted herein shall be perpetual unless terminated by You for convenience or terminated by either party for material breach. Immediately upon termination of this license for any reason, You shall destroy all copies of the Software and documentation.

4. Subscription Term(s).
If You purchase a subscription license, then the term of this license is on a subscription basis with an initial term of one (1) year, and optional renewal terms of one (1) year each, unless prior to renewal this license is terminated by You for convenience or terminated by either party for material breach. Renewal procedures are available from ANIXIS, and unless such procedures are strictly satisfied, including the payment of any required license fee, Your use of the Software for any purpose after the expiration of the subscription term is not authorized. Upon expiration of the subscription term, the Software may automatically disable itself. Immediately upon expiration or termination of this license for any reason, You shall destroy all copies of the Software and documentation.
5. **License Grant.**
You are granted non-exclusive rights to install and use the Software on any computer and/or transmit the Software over a computer network, provided that You acquire and dedicate a licensed copy of the Software for each user who may access the Software. A license for the Software may not be shared or used concurrently by different users. You may purchase additional licenses for the Software from time to time. This Agreement shall take precedence over any purchase order, and any conflicting, inconsistent, or additional terms in such purchase orders shall be null and void. You may copy the Software for archival purposes, provided that all copies must contain the original Software's proprietary notices in unaltered form.

6. **Restrictions.**
You may not: (i) permit others to use the Software, except as expressly provided above for authorized network use; (ii) modify or translate the Software; (iii) reverse engineer, decompile, or disassemble the Software, except to the extent this restriction is expressly prohibited by applicable law; (iv) create derivative works based on the Software; (v) merge the Software with another product; (vi) copy the Software, except as expressly provided above; or (vii) modify, remove or obscure any copyright, trademark or other proprietary rights notices or labels on the Software.

7. **Transfers.**
You may not transfer the Software or any rights under this Agreement without the prior written consent of ANIXIS, which consent shall not be unreasonably withheld. A condition to any transfer or assignment shall be that the recipient agrees to the terms of this Agreement. Any attempted transfer or assignment in violation of this provision shall be null and void.

8. **Ownership.**
ANIXIS and its suppliers own the Software and all intellectual property rights embodied therein, including copyrights and valuable trade secrets embodied in the Software's design and coding methodology. The Software is protected by Australian copyright laws and international treaty provisions. This Agreement provides You only a limited use license, and no ownership of any intellectual property.

**LIMITED WARRANTY STATEMENT; LIMITATION OF LIABILITY.** ANIXIS warrants only to You that the Software shall, in unmodified form, perform substantially in accordance with accompanying documentation under normal use for a period of thirty (30) days from the purchase date. The entire and exclusive liability and remedy for breach of this Limited Warranty shall be, at ANIXIS' option, either (i) return of the amount received by ANIXIS for the Software, or (ii) replacement of defective Software and/or documentation. ANIXIS AND ITS SUPPLIERS AND RESELLERS SPECIFICALLY DISCLAIM THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SYSTEM INTEGRATION, AND DATA ACCURACY. THERE IS NO WARRANTY OR GUARANTEE THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT THE SOFTWARE WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE, QUALITY, ACCURACY, PURPOSE, OR NEED, EXCEPT AS EXPRESSLY PROVIDED IN THE LIMITED WARRANTY. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT. NO USE OF THE SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER. No action for the above Limited Warranty may be commenced after one (1) year following the expiration date of the warranty. To the extent that this Warranty Statement is inconsistent with the jurisdiction where You use the Software, the Warranty Statement shall be deemed to be modified consistent with such local law. Under such local law, certain limitations may not apply, and You may have additional rights which vary from jurisdiction
to jurisdiction. For example, some states in the United States and some jurisdictions outside the United States may: (i) preclude the disclaimers and limitations of this Warranty Statement from limiting the rights of a consumer; (ii) otherwise restrict the ability of a manufacturer to make such disclaimers or to impose such limitations; or (iii) grant the consumer additional legal rights, specify the duration of implied warranties which the manufacturer cannot disclaim, or prohibit limitations on how long an implied warranty lasts.

INDEPENDENT OF THE FORGOING PROVISIONS, IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING WITHOUT LIMITATION, TORT, CONTRACT, OR STRICT PRODUCTS LIABILITY, SHALL ANIXIS OR ANY OF ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER MALFUNCTION, OR ANY OTHER KIND OF COMMERCIAL DAMAGE, EVEN IF ANIXIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

IN NO EVENT SHALL ANIXIS’ LIABILITY FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF ACTION, EXCEED THE AMOUNT OF THE PURCHASE PRICE PAID, IF ANY, FOR THE SOFTWARE LICENSE.

EXPORT CONTROLS. You agree to comply with all local laws in Your jurisdiction which might impact Your right to import, export or use the Software, and You represent that You have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

MISCELLANEOUS. This Agreement constitutes the entire understanding of the parties with respect to the subject matter of this Agreement and merges all prior communications, representations, and agreements. This Agreement may be modified only by a written agreement signed by the parties. If any provision of this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be construed under the laws of the State of New South Wales, Australia, excluding rules regarding conflicts of law. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The parties have requested that this Agreement and all documents contemplated hereby be drawn up in English.

U.S. GOVERNMENT END USERS: If the Software and documentation is acquired by or for the United States Government then it is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19 or clause 18-52.227-86(d) of the NASA supplement to the FAR, as applicable. Manufacturer is ANIXIS PTY LTD, 9 Monteray Terrace, Glenmore Park, NSW 2745 Australia.