netwrix

2025

Netwrix Password Policy Enforcer v11.0

6160 Warren Parkway, Suite 100, Frisco, TX 75034 | (949) 407-5125

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of contents

Netwrix Password Policy Enforcer v11.0

Netwrix Password Policy Enforcer helps secure your network by ensuring users set strong passwords. When a user enters a password that does not comply with the password policy, Password Policy Enforcer immediately rejects the password and details why the password was rejected.

Getting Started

Review the Requirements and the Domain and Local Policies topics.

Install Products

Password Policy Enforcer (PPE Server) is installed on every domain controller to enforce the password policy for domain user accounts, or on individual servers and workstations to enforce the password policy for local user accounts. See the Install Password Policy Enforcer on a Server or Install with Group Policy Management topics for additional information.

The Configuration Console can be installed on what ever servers are convenient for you to access. It is a selectable feature in the server installation **msi** package. See the Install Password Policy Enforcer on a Server topic for additional information.

The Mailer Service is installed on a single server in each domain. See the Install Password Policy Enforcer on a Server topic for additional information.

Password Policy Enforcer client is optional, but recommended. Users receive immediate feedback when setting up their passwords. This saves your users time and frustration when picking compliant passwords. See the Install Password Policy Enforcer Client or Install with Group Policy Management topics for additional information.

Password Policy Enforcer Web is a separate product enabling users to change their Windows domain password from a web browser. See the Password Policy Enforcer Web topic for additional information.

Create the **Compromised Passwords Base** prior to enabling the Compromised Password Check. See the HIBP Updater topic for additional information.

Exclude PPE Files from AntiVirus Checks

Domain Controller

PPE.DLL if this file does not load, the password policy is not enforced.

Clients

PPEClt.dll and **APRClt.dll** if either of these files are blocked, the client does not run.

Next Steps

You can work through the Evaluate Password Policy Enforcer or open the Configuration Console.

What's New

New Netwrix Community!

All Netwrix product announcements have moved to the new Netwrix Community. See announcements for Netwrix Password Policy Enforcer in the Password Policy Enforcer area of our new community.

The following information highlights the new and enhanced features introduced in this Netwrix Password Policy Enforcer version 11.0.

Password Policy Enforcer v11.0

New: Redesigned UI

The user interface of the Management Console has been fully redesigned to reflect modern design standards and account for all the feedback our customers have given us throughout the years.

New: PowerShell cmdlets

Netwrix Password Policy Enforcer now includes a set of PowerShell cmdlets that enable administrators to easily manage policy, generate reports, and check the health of Netwrix Password Policy Enforcer from PowerShell in both interactive and automated ways.

New: Support Tools

Additional support tools have been added to allow administrators to check the health of the Netwrix Password Policy Enforcer and audit the version of each installation from one location. This allows customers to quickly identify any problems and keep their Netwrix Password Policy Enforcer installation up to date.

New: Updated Installer

The Netwrix Password Policy Enforcer QuickStart Wizard has been replaced with MSI packages for easier installation and upgrade of the client and the server.

New: Netwrix Password Policy Enforcer Web

PPE Web is now available to all licensed Password Policy Enforcer customers. PPE Web allows users to change their Windows domain passwords from a web browser and integrates with Netwrix Password Policy Enforcer to enforce customizable password policies and assist users in selecting compliant passwords.

Enhancement: Updated policy templates

The out-of-the-box policy templates have been updated to reflect recent changes in different compliance standards. Old templates will still be available, and customers' current policies will not be changed as part of this update.

Enhancement: Compatibility

- Deprecation of 32-bit server installations – The product now only supports 64-bit server installations.
- Currently supported Password Policy Server platforms – 64-bit Windows 10, 11 and Windows Server 2016, 2019, and 2022.

- Currently supported Password Policy Client platforms – 32-bit Windows 10 and 64-bit Windows 10, 11, and Windows Server 2016, 2019, and 2022.

Requirements

Netwrix Password Policy Enforcer 11 can be installed 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 Password Policy Enforcer password policies for both account types. If your users normally logon with a domain account, then you will most likely only use Password Policy Enforcer to enforce password policies for the domain accounts.

Password Policy/Web is installed on a Windows server and accessed via user browsers.

Password Policy Enforcer Server

Here are the requirements for both the full and evaluation Password Policy Enforcer installations.

- Windows Server Versions (64 bit):
  - 2016
  - 2019
  - 2022
- Windows Workstation Versions (64 bit only)
  - 10
  - 11

Password Policy Enforcer Client

Here are the requirements for both the full and evaluation Password Policy Enforcer installations.

- Windows Server Versions (64 bit):
  - 2016
  - 2019
  - 2022
- Windows Workstation Versions (64 and 32 bit)
  - 10
  - 11

Password Policy Enforcer Configuration Console

Here are the requirements for both the full and evaluation Password Policy Enforcer installations.

- Windows Server Versions (64 bit):
  - 2016
  - 2019
  - 2022
- Windows Workstation Versions (64 and 32 bit)
  - 10
  - 11
- .net framework 4.7.2 or higher

Password Policy Enforcer Web

Here are the requirements for the Password Policy Enforcer Web. Password Policy Enforcer Web can share server resources with other applications. It can be installed on an existing, well secured web server.

- Windows Server Versions:
  - 2016
  - 2019
  - 2022
  - Microsoft IIS

Domain and Local Policies

Netwrix Password Policy Enforcer enforces 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 Password Policy Enforcer password policies for both account types. If your users normally logon with a domain account, then you will most likely only use Password Policy Enforcer to enforce password policies for the domain accounts.

Installation Differences

To enforce password policies for domain user accounts, you should install Password Policy Enforcer onto all the domain controllers in the domain. If you have read-only domain controllers and aren't using the Rules, Password Policy Client, or other software (such as Netwrix Password Reset) that uses the Password Policy Enforcer Client protocol, then you do not need to install Password Policy Enforcer on the read-only domain controllers.

To enforce password policies for local user accounts, you should install Password Policy Enforcer 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 Password Policy Enforcer 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 Password Policy Enforcer on the domain controllers.

Operational Differences

Most of Password Policy Enforcer'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, Password Policy Enforcer 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 version of these rules with Password Policy Enforcer). See the Rules topic for additional information.
- Policy assignments by groups and containers. See the Assign Policies to Users & Groups topic for additional information.

Password Policy Enforcer'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 Password Policy Enforcer management console allows you to choose a configuration source. See the Connected To topic for additional information. Changes you make to Password Policy Enforcer'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 10.0\ registry key from the configured computer, and import it into the other computers.

You can also use Group Policy to distribute Password Policy Enforcer'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.

Follow the steps below to distribute Password Policy Enforcer's local configuration with Group Policy.

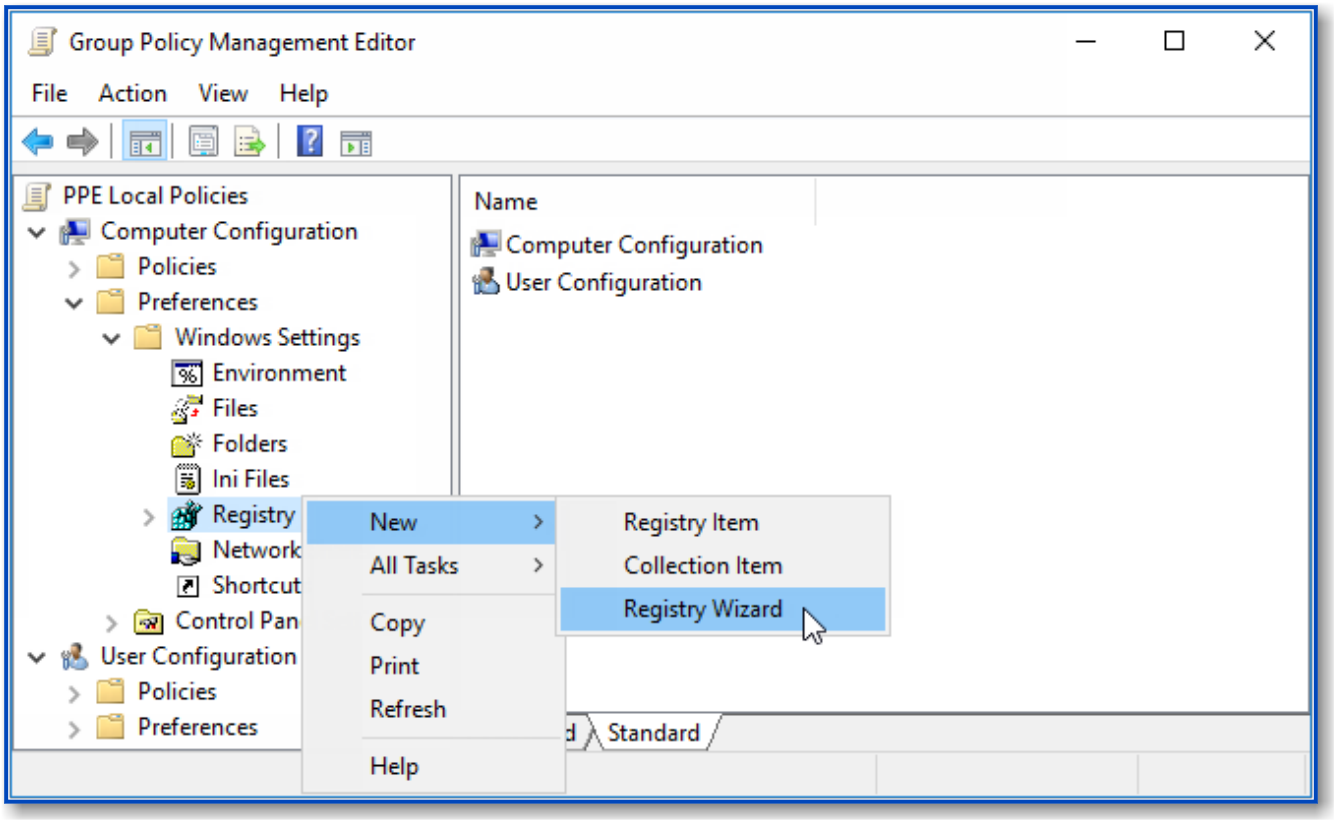
Step 1 – Start the Group Policy Management Console (gpmc.msc).

Step 2 – Expand the forest and domain items in the left pane.

Step 3 – Right-click the **Group Policy** object that you would like to use to distribute the configuration, and then click the **Edit...** button.

Step 4 – Expand the Computer Configuration, Preferences, and Windows Settings items in the left pane.

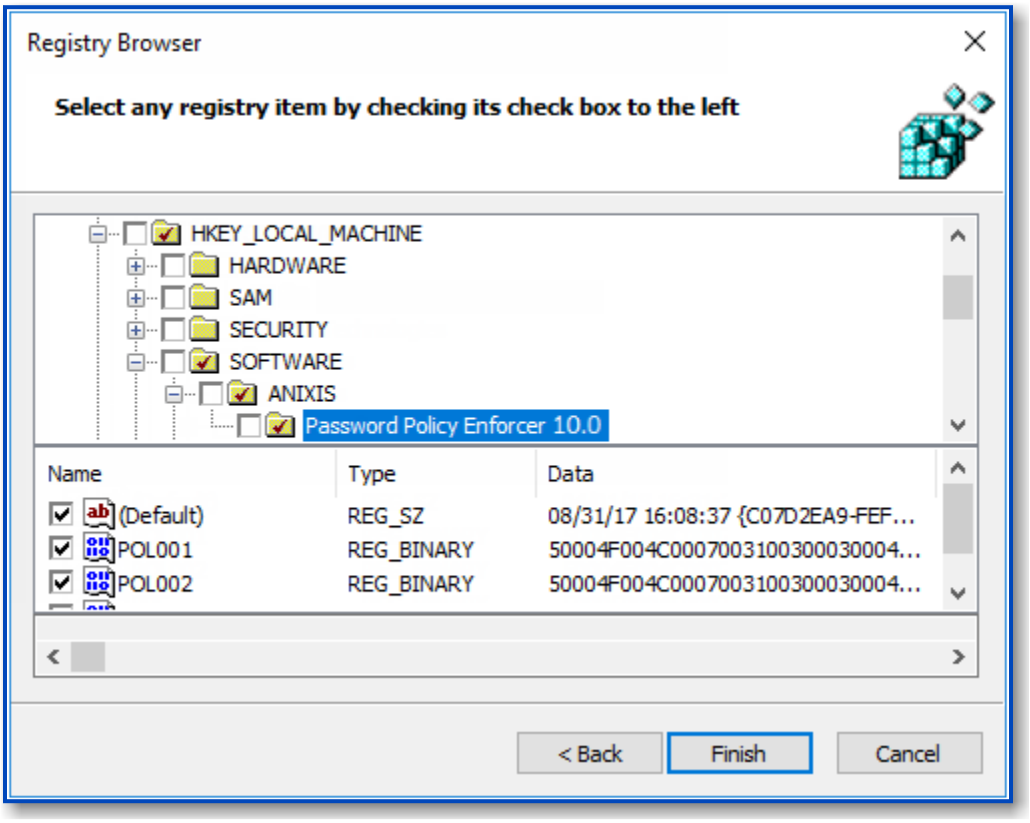
Step 5 – Right-click the **Registry** item, and then select **New** > **Registry Wizard**.



Step 6 – Select the computer that contains the Password Policy Enforcer local configuration that you want to distribute, and then click **Next**.

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

Step 8 – Click the **Password Policy Enforcer *version*** item, and then select the check boxes beside each item in the bottom pane of the window.



Step 9 – Click **Finish**.

Step 10 – Close the Group Policy Management Editor.

Password Policy Enforcer'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`

Install Password Policy Enforcer on a Server

Password Policy Enforcer server should be installed on every domain controller to enforce the password policy for domain user accounts, or on 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 Password Policy Enforcer on these servers is only necessary if you are using the following features:

- Rules
- Password Policy Client

- Netwrix Password Reset
- Password Policy Enforcer Web

The Server installation package includes multiple features selected during installation:

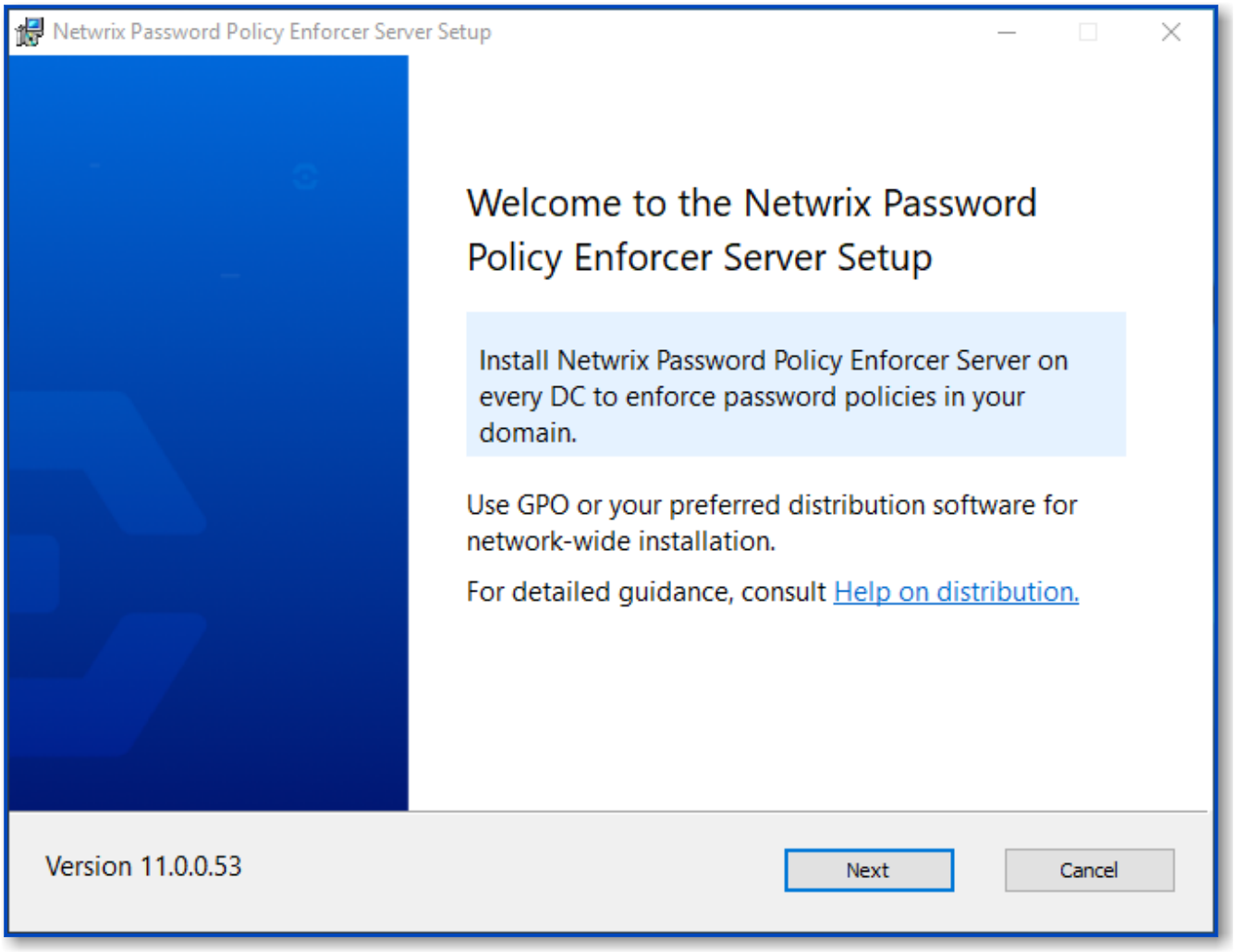
- PPE Server – enforces password policies. It can be installed on Domain Controllers for domain password policy, or on servers and workstations for local account password policy.
- Configuration Console – manages policy configuration. Install where ever needed.
- Mailer Service – sends email reminders. Install on any server.

Step 1 – Download the installation package from Netwrix.

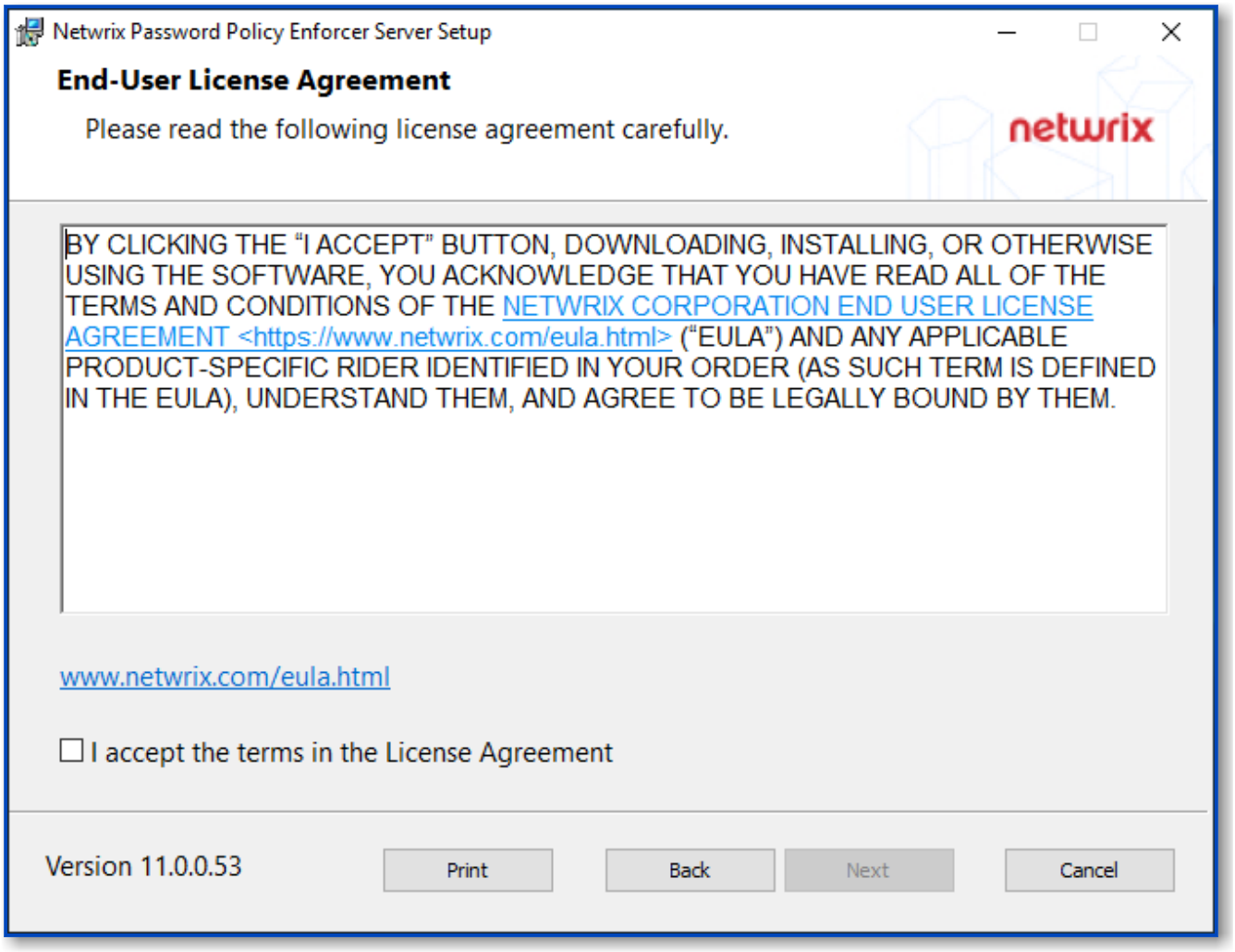
Step 2 – Extract the installers from the compressed file. If you are going to use Group Policy Manager to install Netwrix Password Policy Enforcer, copy the **msi** files to a distribution folder. See the Install with Group Policy Management topic for additional details. You can also install/uninstall the products using command line Silent Installation.

NOTE: Continue with these steps to install one or more features on your current server or domain controller. You must repeat these steps for each server where the features are installed.

Step 3 – Click on the **Netwrix_PPE_Server_*version*_x64.msi** installation package. The installer is launched.

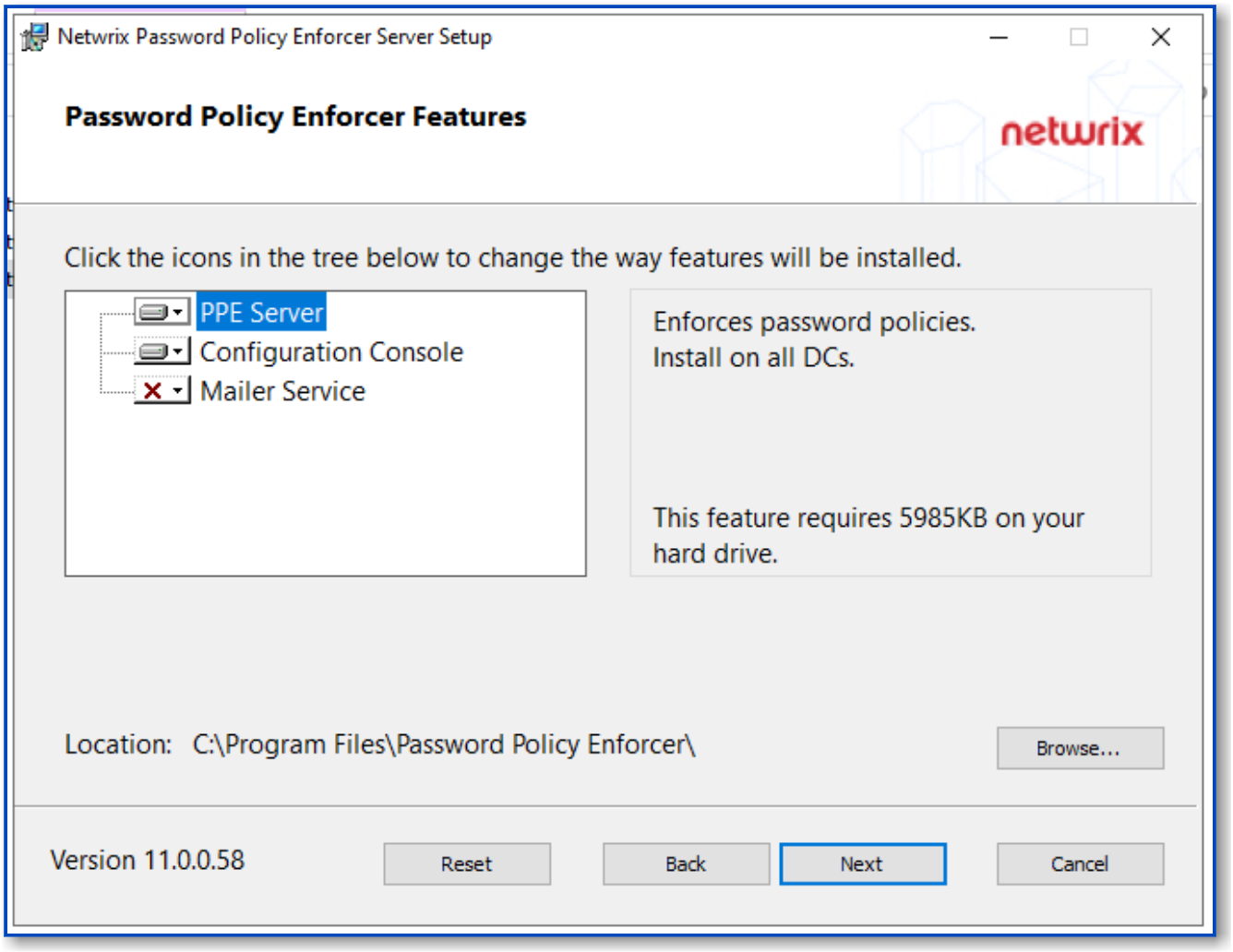


Step 4 – Click **Next**.



Step 5 – Review the End-User License Agreement. Click **I accept the terms in the License Agreement**.

Step 6 – Click **Next**.

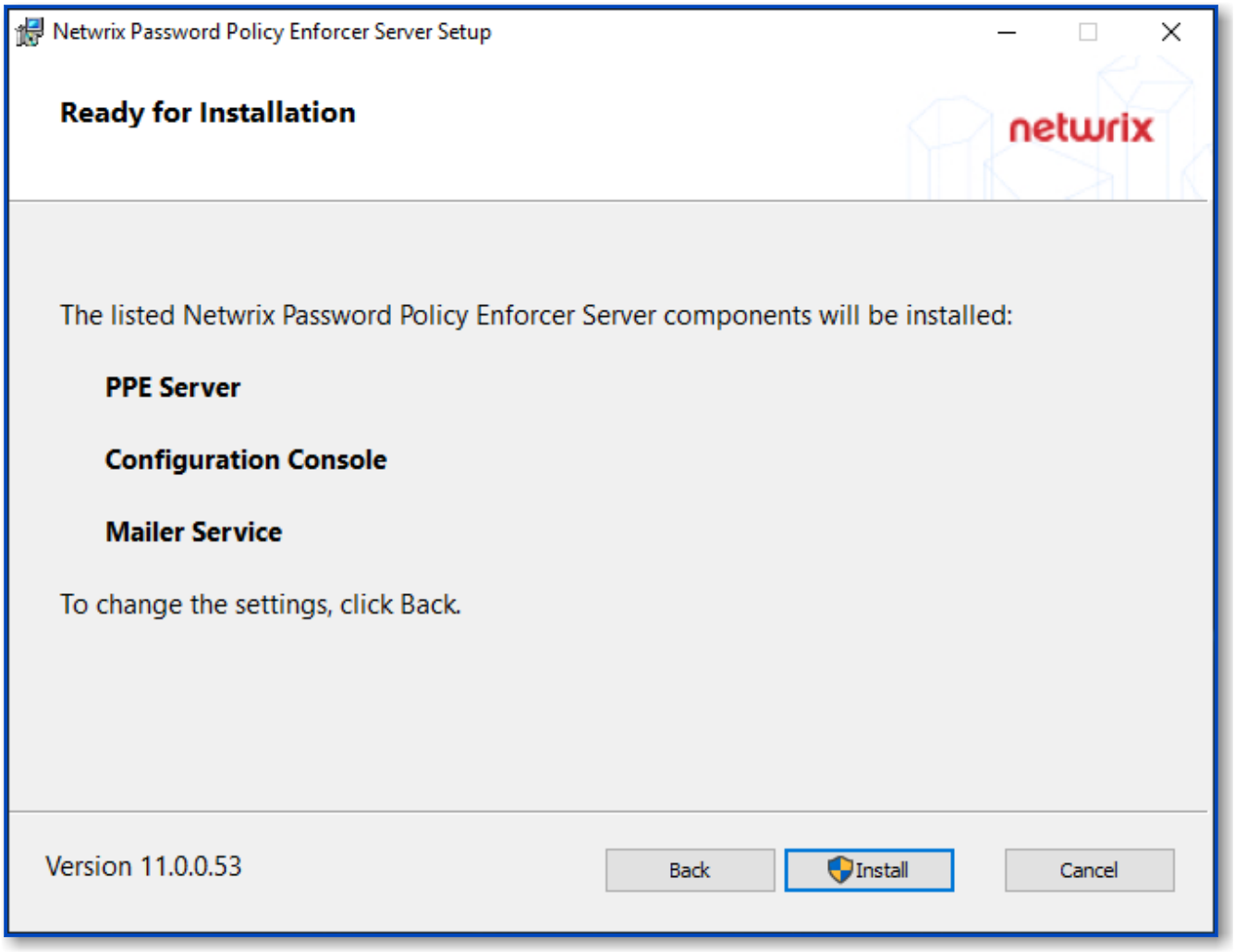


Step 7 – Select the features to install. The required storage is shown for each selection.

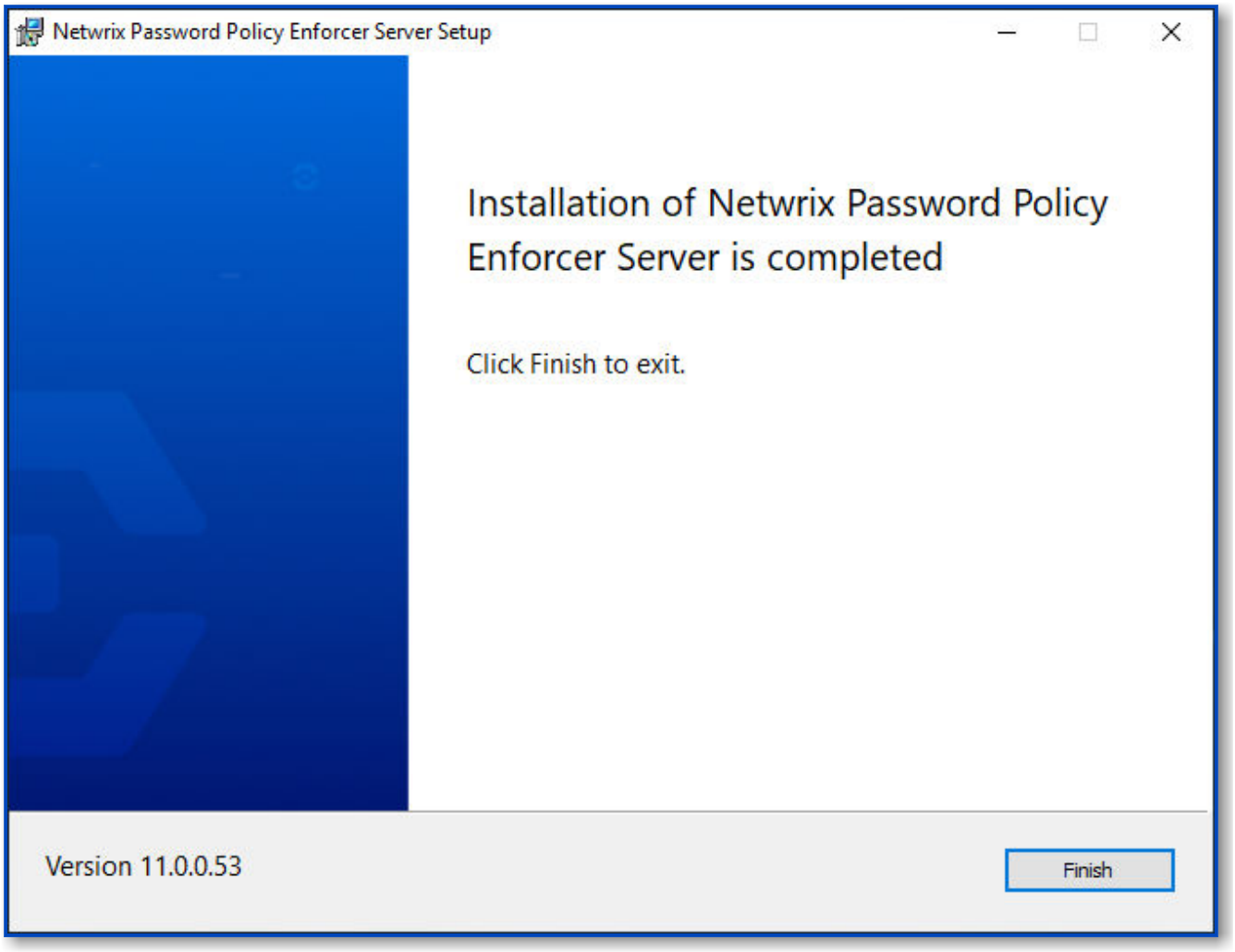
- PPE Server – enforces password policies. It can be installed on Domain Controllers for domain password policy, or on servers and workstations for local account password policy. It is not selected by default.
- Configuration Console – manages policy configuration. Install where ever needed. Selected by default.
- Mailer Service – sends email reminders. Should be installed on a Domain Controller. It is not selected by default.

Step 8 – The default location is shown. Click **Browse** and select a new location if needed.

Step 9 – Click **Next**.



Step 10 – Review your selections. Click **Back** to make any changes. When ready, click **Install**.



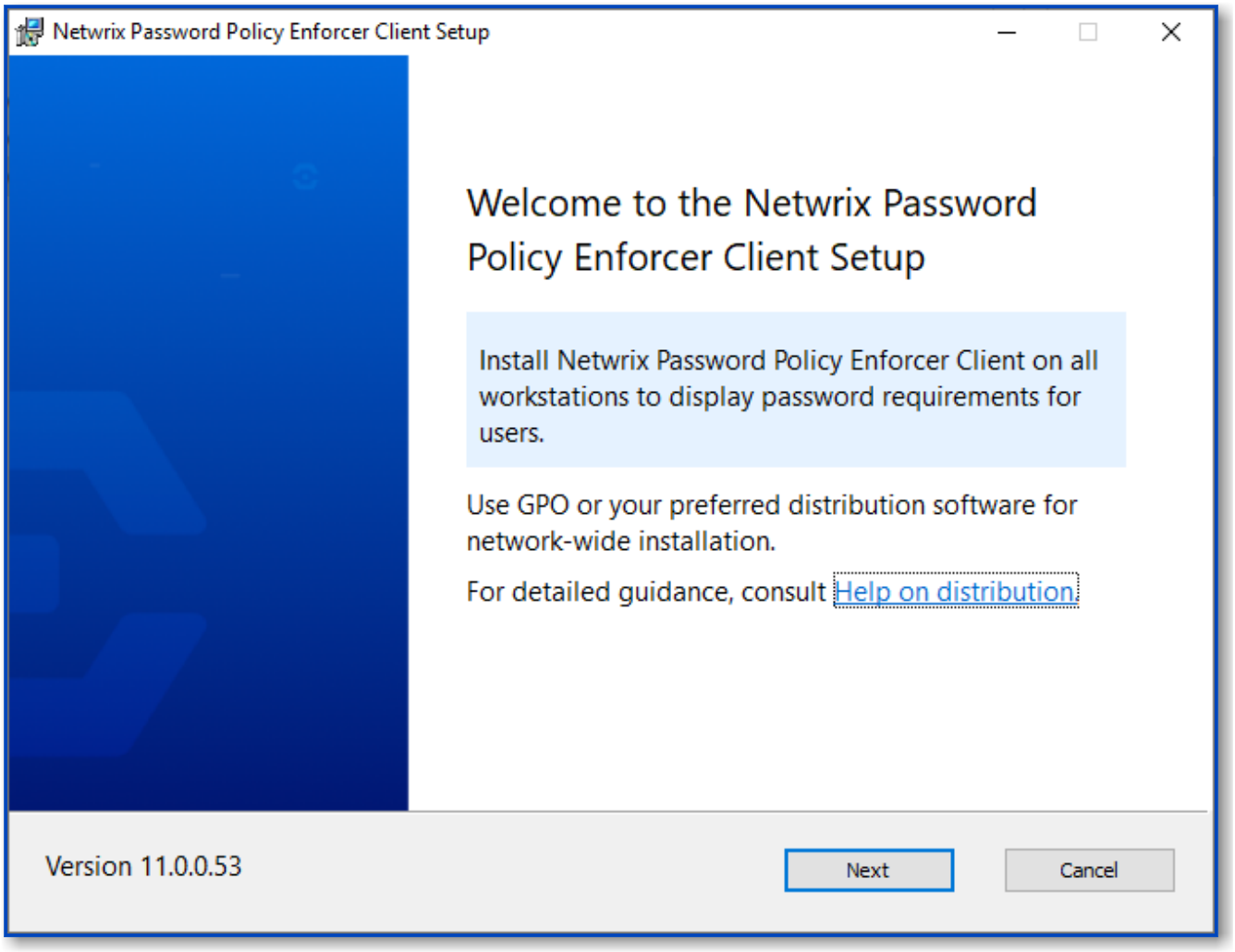
Step 11 – Click **Finish** when installation is complete. You are prompted to restart your system for the changes to take effect.

Install Password Policy Enforcer Client

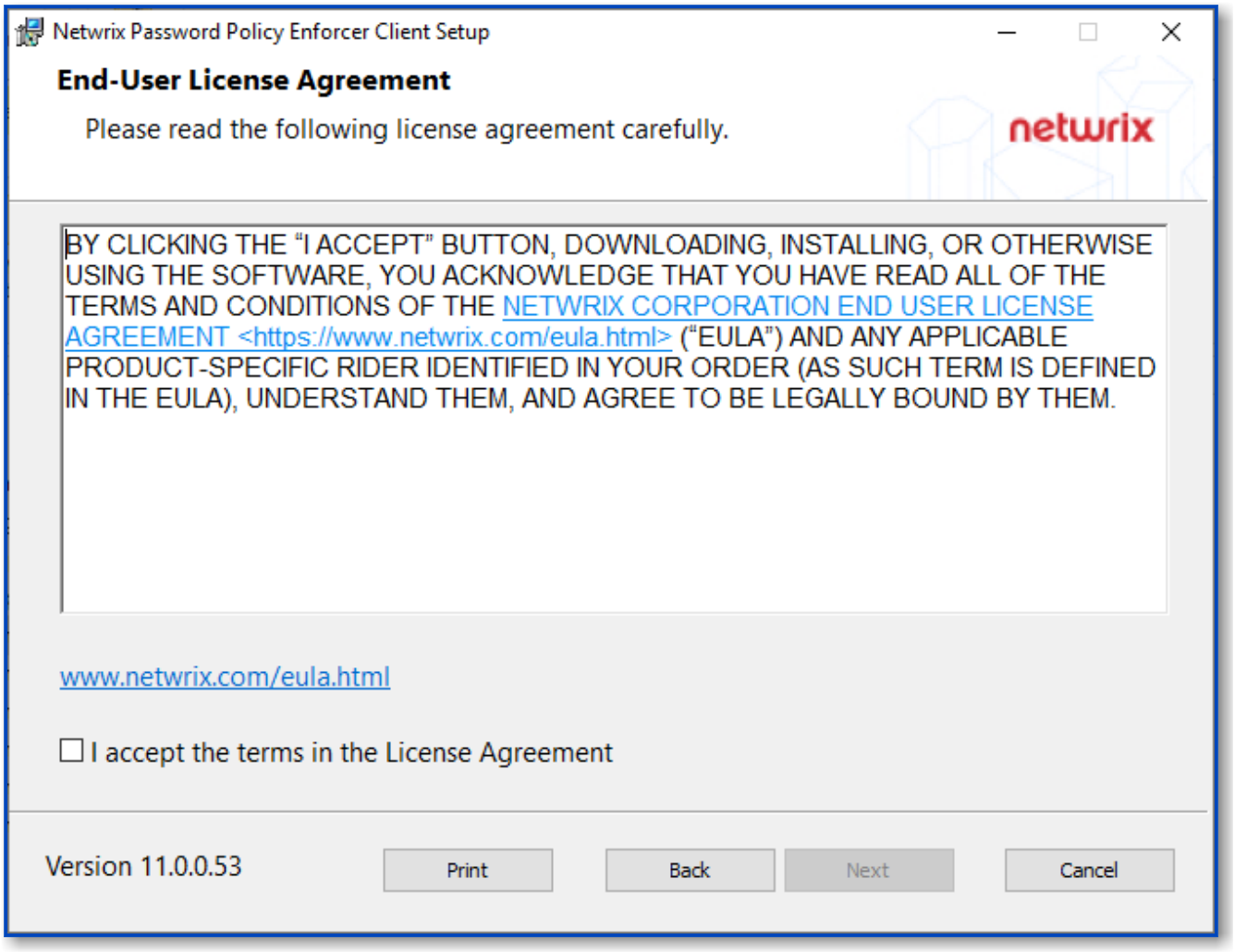
This procedure is used to install the client on your current workstation. See the Install with Group Policy Management top for details on installing the client across your network. You can also install/uninstall the products using command line Silent Installation.

Step 1 – Navigate to the folder where you extracted the installers downloaded from Netwrix.

Step 2 – Click on the **Netwrix_PPE_Client_*version*_x64.msi** (64 bit OS) or **Netwrix_PPE_Client_*version*_x86.msi** (32 bit OS) installation package. The installer is launched.

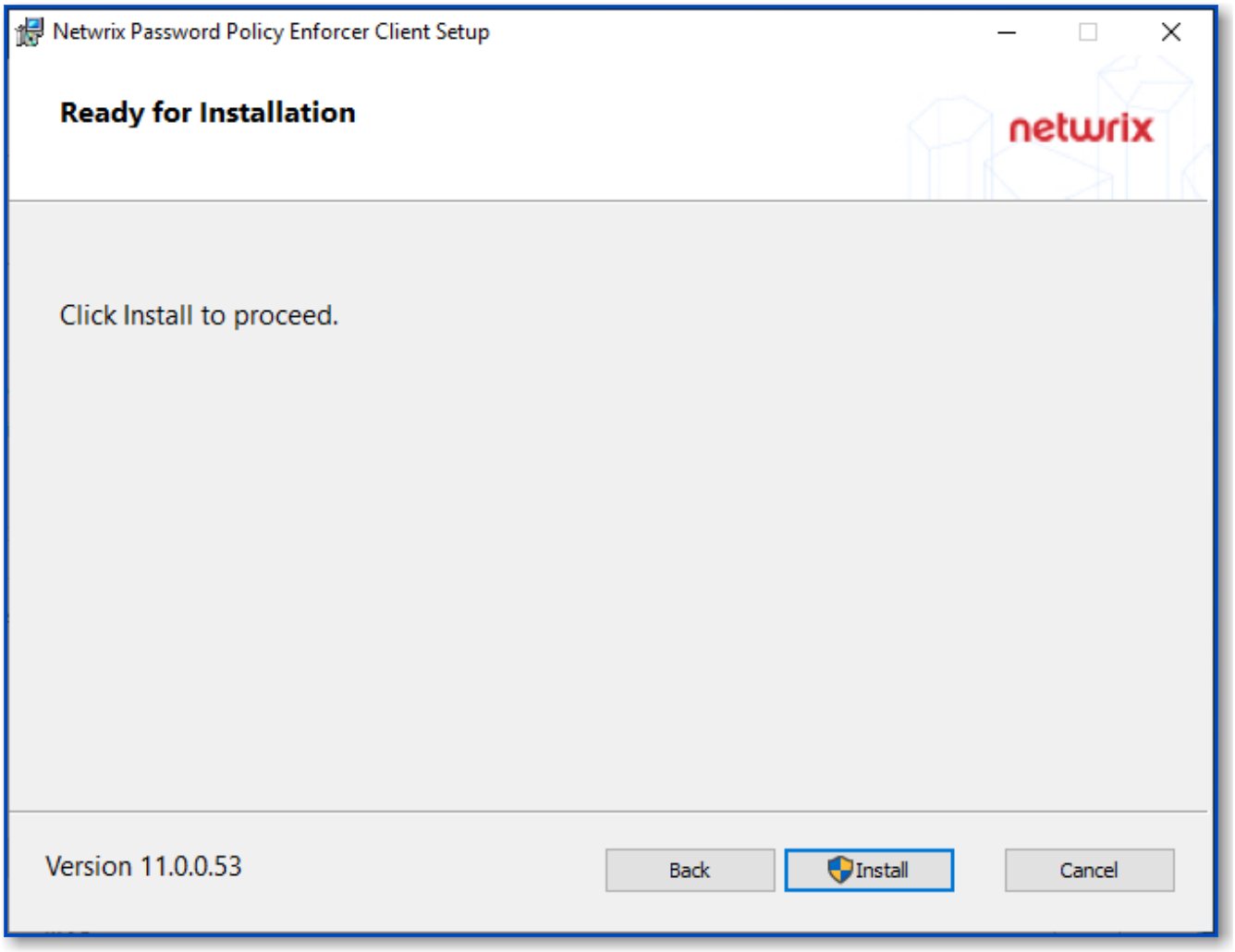


Step 3 – Click **Next**.

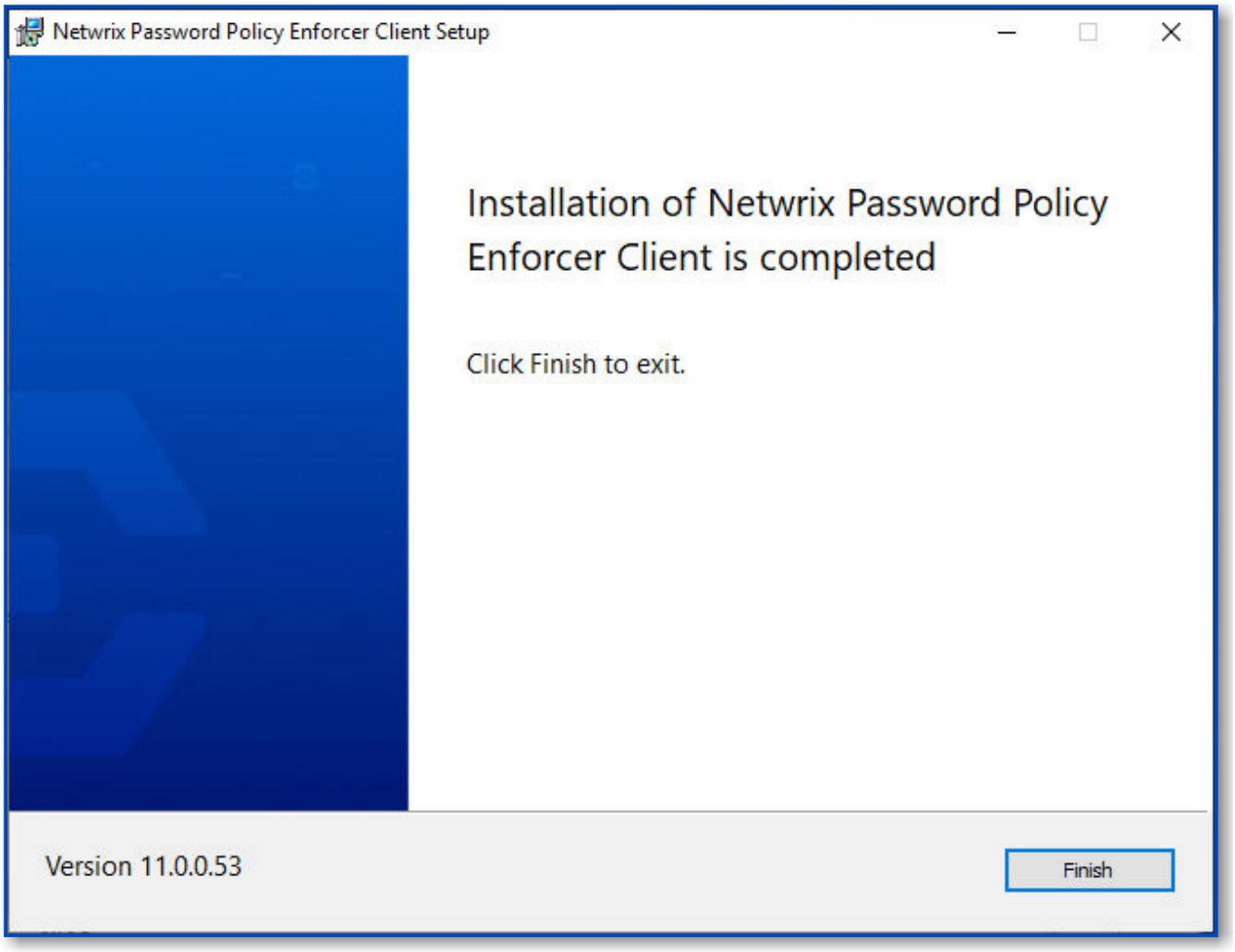


Step 4 – Review the End-User License Agreement. Click **I accept the terms in the License Agreement**.

Step 5 – Click **Next**.



Step 6 – Click **Install**.



Step 7 – Click **Finish** when installation is complete.

The client is installed. There is no associated desktop icon or menu item.

Restart each computer to complete the installation. Windows installs the Password Policy Client during startup.

Testing the Password Policy Client

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 Password Policy Enforcer policy has not been assigned to you, or because the firewall rules have not been created.

NOTE: 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 Password Policy Client

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 Password Policy Client and Password Policy Server communicate through a firewall. Firewall rules are not necessary for local policies because the Password Policy Client and Password Policy Server 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.

Follow the steps below to create the port exception on all domain controllers.

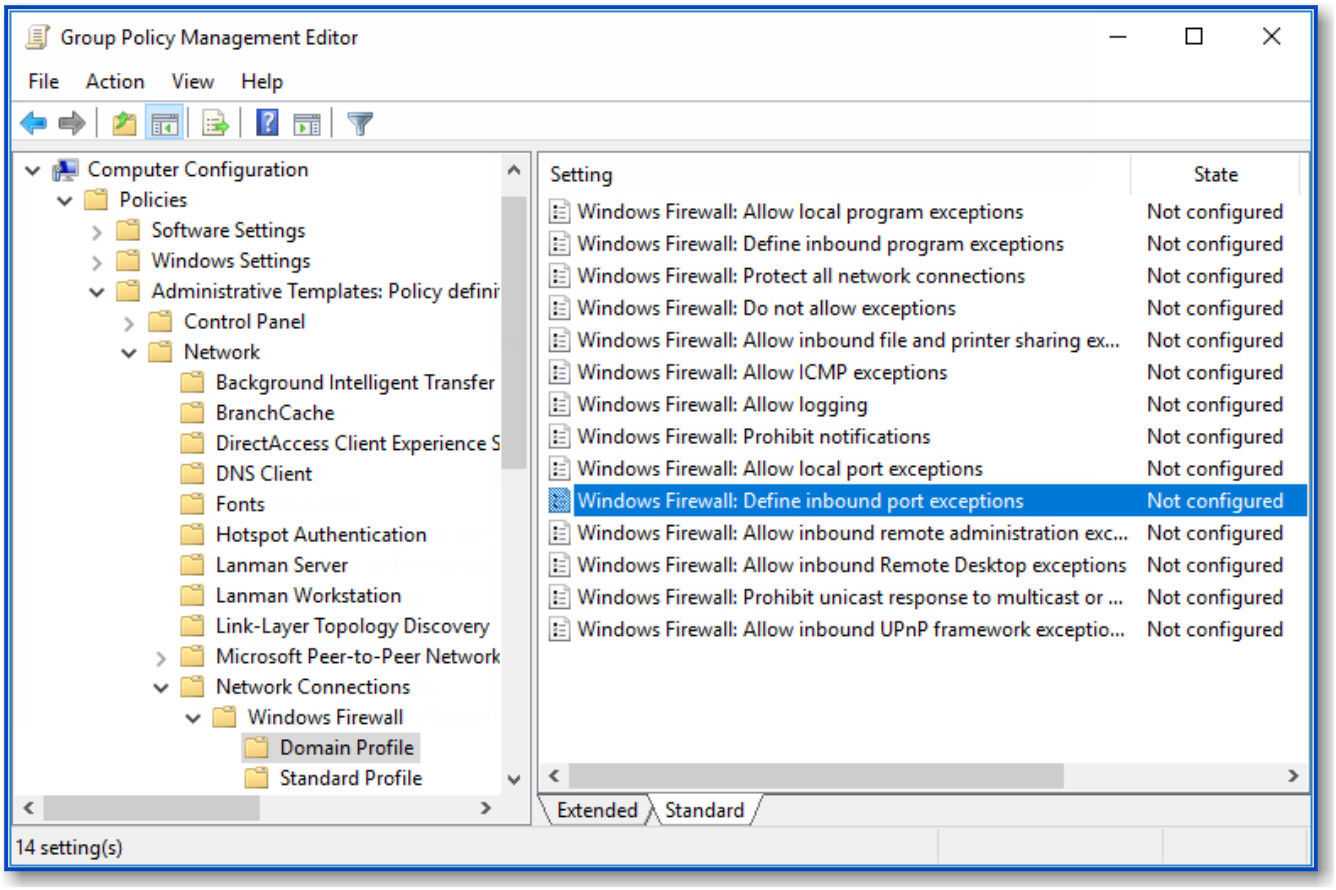
Step 1 – Use the **Group Policy Management Console** (gpmc.msc) to display the GPOs linked to the Domain Controllers OU.

Step 2 – Right-click the **Password Policy Enforcer GPO**, and then click **Edit...**.

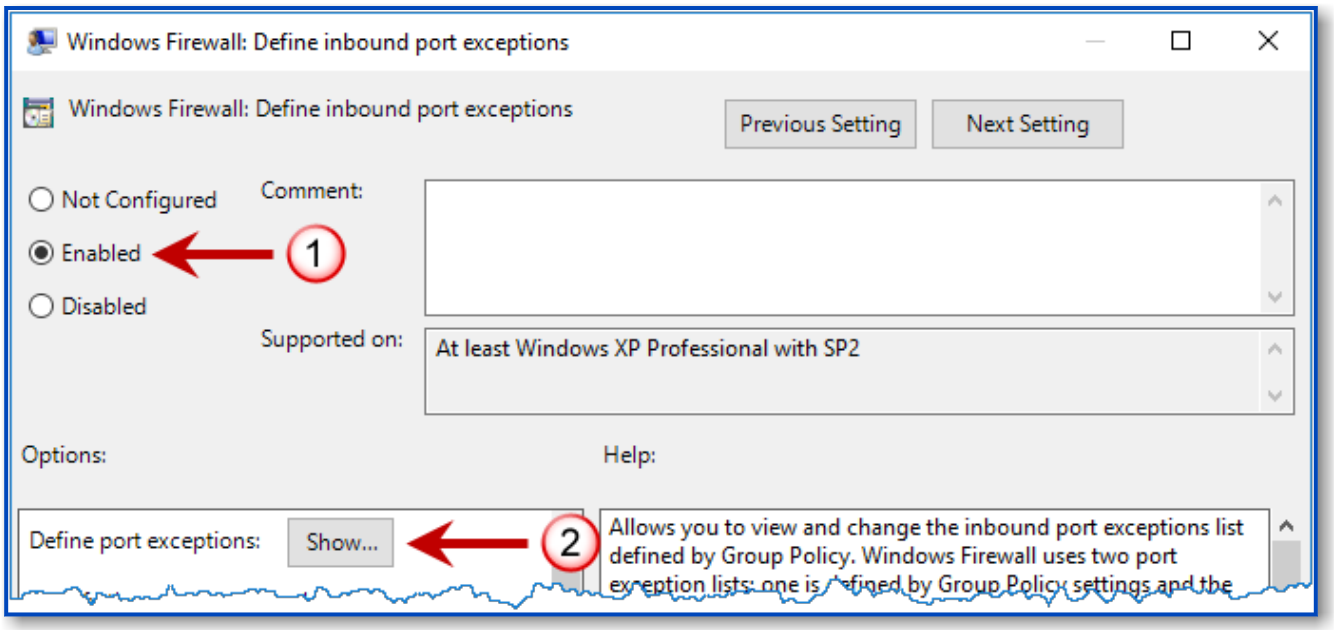
NOTE: You need to create the GPO if you chose the Express Setup option.

Step 3 – Expand the **Computer Configuration**, **Policies**, **Administrative Templates**, **Network**, **Network Connections**, and **Windows Firewall** items.

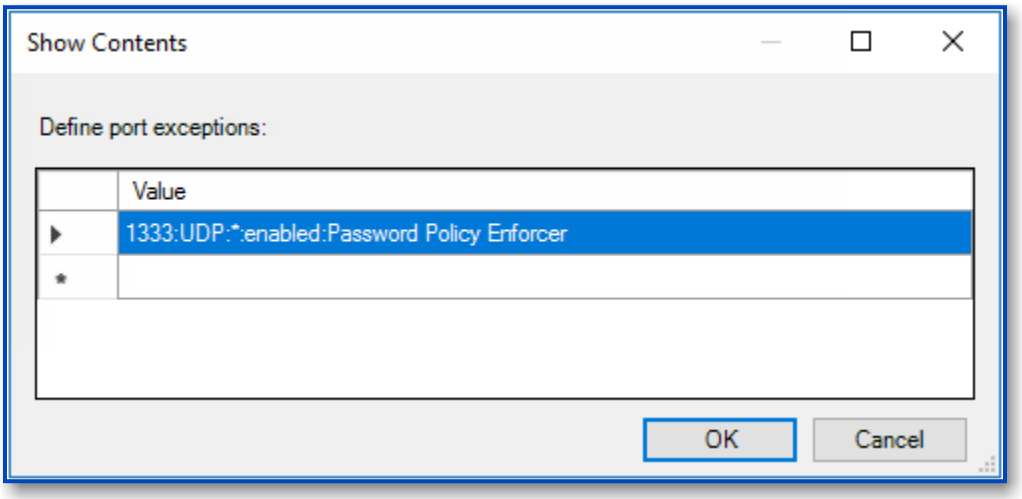
Step 4 – Click **Domain Profile** in the left pane then double-click **Windows Firewall: Define inbound port exceptions** in the right pane.



Step 5 – Select the **Enabled** option, and then click **Show...**.



Step 6 – Select the **Enabled** option, and then click **Show...**.



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

Step 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:

Attribute	Result
Protocol	UDP
Source Address	Client Computer IP address
Source Port	Any
Destination address	Domain controller IP address

Attribute	Result
Destination port	1333

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

Attribute	Result
Protocol	UDP
Source Address	Domain controller IP address
Source Port	Any
Destination address	Client Computer IP address
Destination port	Any

NOTE: If your firewall performs Stateful Packet Inspection, then only create a rule for the request datagram as the firewall automatically recognizes and allows the response datagram.

Install with Group Policy Management

An automated installation uses Group Policy to distribute Password Policy Enforcer. This type of installation is recommended when you need to install Password Policy Enforcer on many computers. This section shows you how to install Password Policy Enforcer 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. See the Domain and Local Policies topic for additional information.

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 Password Policy Enforcer distribution point:

Step 1 – Log on to a server as an administrator.

Step 2 – Create a shared network folder to distribute the files from.

Step 3 – Give the **Domain Controllers** security group read access to the share, and limit write access to authorized personnel only.

Step 4 – Download the Netwrix Password Policy Enforcer installation package from Netwrix.

Step 5 – Extract the installers from the compressed file.

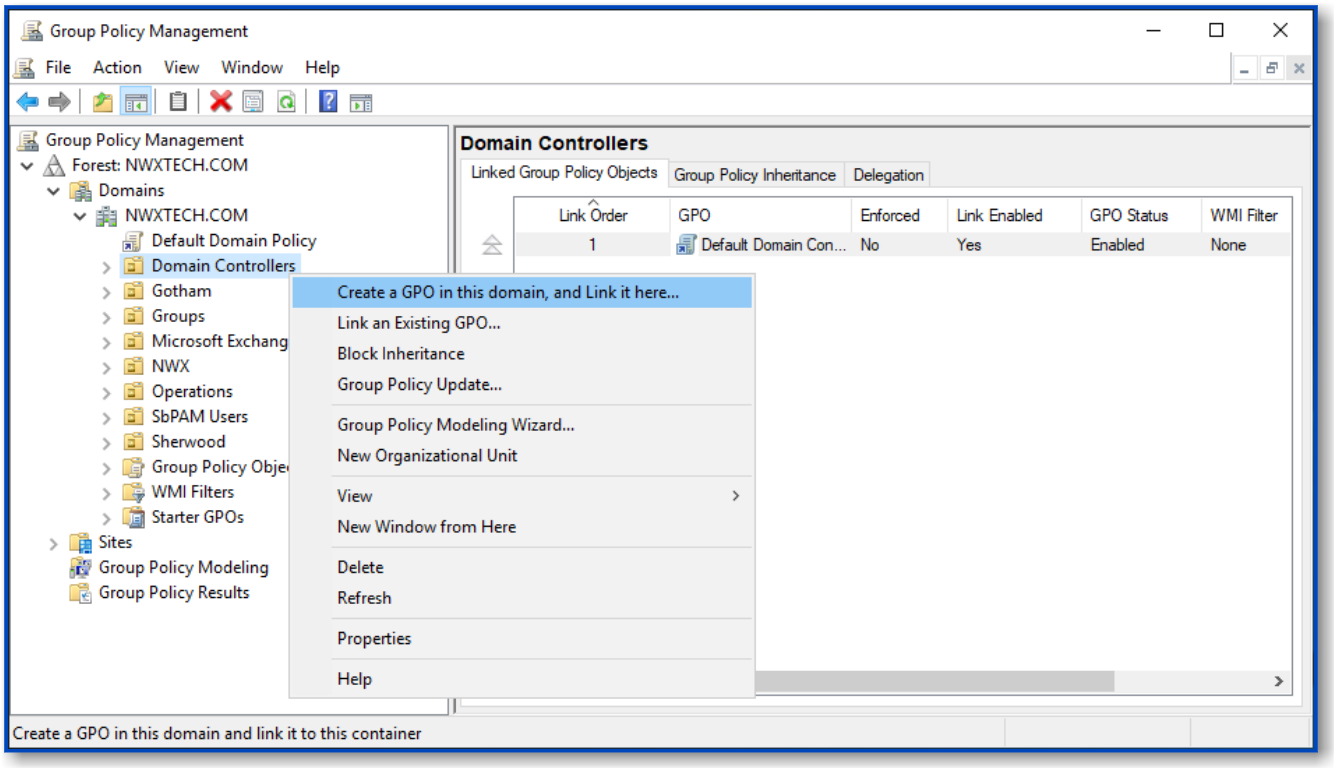
Step 6 – Copy the **.msi** files to the distribution folder.

Create a Group Policy Object

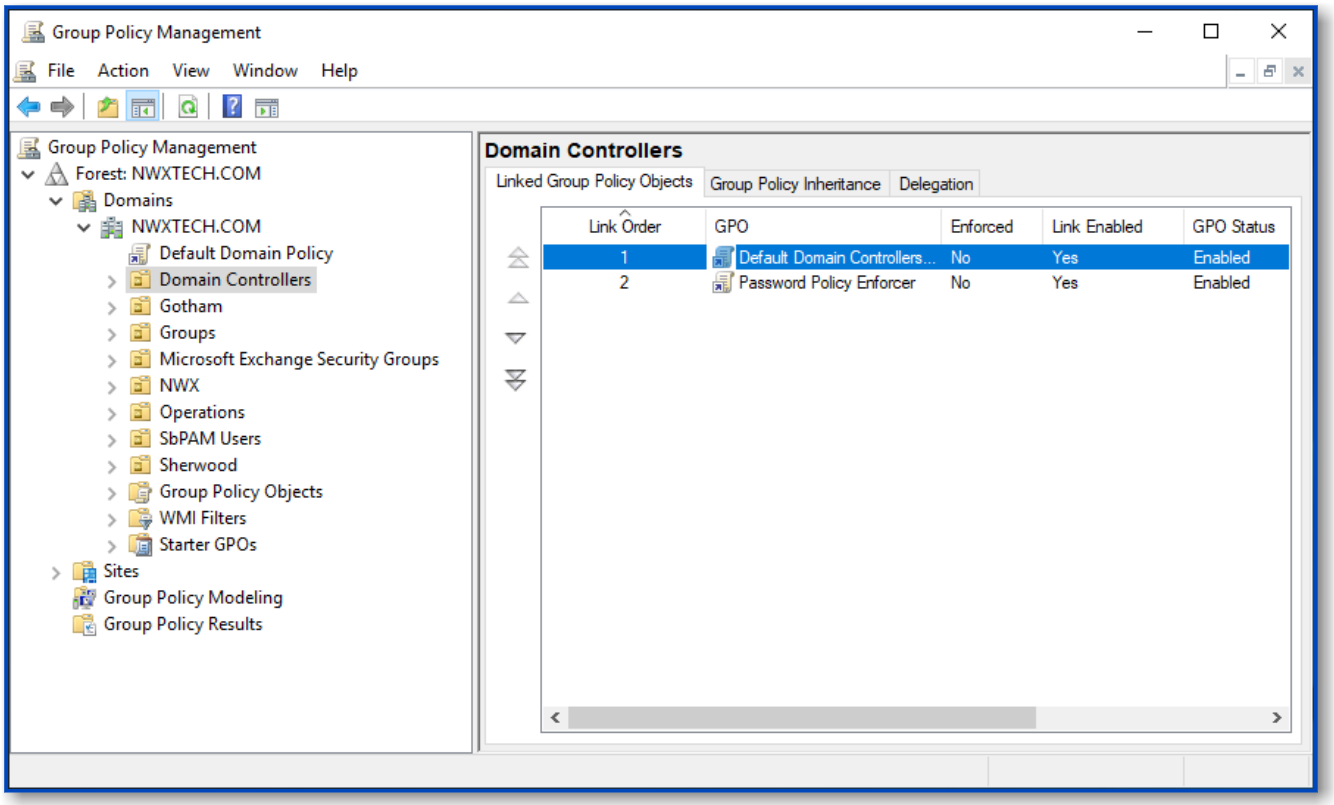
Step 1 – Start the Group Policy Management Console (**gpmc.msc**).

Step 2 – Expand the forest and domain items in the left pane.

Step 3 – Right-click the **Domain Controllers OU** in the left pane, and then click **Create a GPO in this domain, and Link it here...**



Step 4 – Enter **Password Policy Enforcer** in the provided field, and then press **Enter**.



Edit the Group Policy Object

Step 1 – Right-click the **Password Policy Enforcer GPO**, and then click the **Edit…** button.

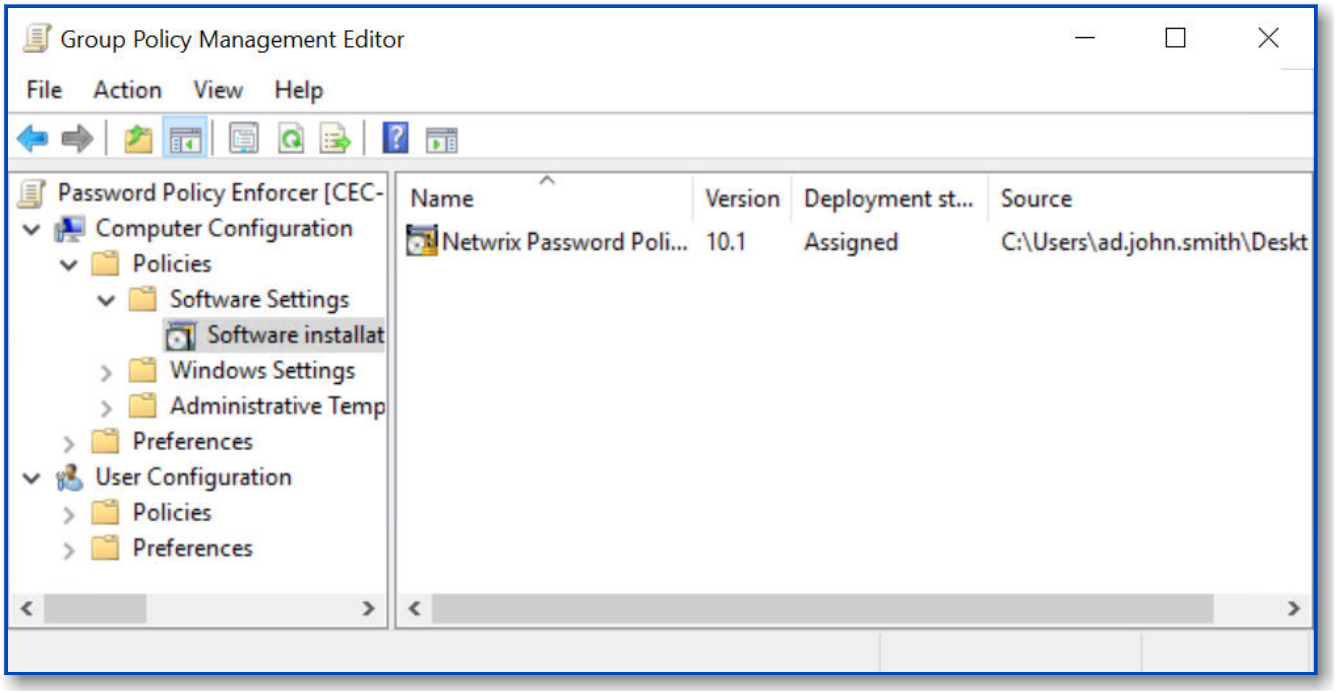
Step 2 – Expand the **Computer Configuration**, **Policies**, and **Software Settings** items.

Step 3 – Right-click the **Software installation** item, and then select **New** > **Package…**

Step 4 – Enter the full **UNC path** to your **msi** files.

NOTE: You must enter a UNC path so that other computers can access this file over the network. For example: \\file server\distribution point share\Netwrix_PPE_*version*.msi

Step 5 – Click **Open**.



Step 6 – Select **Assigned** as the deployment method.

Step 7 – Click **OK**.

Step 8 – Close the Group Policy Management Editor.

Complete the Installation

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

Password Policy Enforcer does not enforce a password policy until the policies are defined. Users can still change their password, and will only need to comply with the Windows password policy rules (if enabled).

Install the Configuration Console

The Configuration Console is used to configure and manage Netwrix Password Policy Enforcer on your domain.

The Password Policy Enforcer Configuration Console can be installed on any servers or workstations where it is convenient for you to use.

The Configuration Console is a feature package included in the server installation **.msi** file:

- PPE Server – enforces password policies. It can be installed on Domain Controllers for domain password policy, or on servers and workstations for local account password policy.
- Configuration Console – manages policy configuration. Install where ever needed.
- Mailer Service – sends email reminders. Install on any server.

Follow the procedure in Install Password Policy Enforcer on a Server, selecting the **Configuration Console** feature. You can select the other features if appropriate for the server.

You can also install/uninstall the products using command line Silent Installation.

Install Mailer Service

Netwrix Password Policy Enforcer sends email 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 Password Policy Enforcer Mailer and configure the email delivery and email message options to send email reminders to users. See the Notifications topic for additional information.

Add your email address to a service account, and the Password Policy Enforcer Mailer reminds you to change the service account password before it expires.

The Password Policy Enforcer Mailer is not installed by default. Only install it on one server in each domain. The Password Policy Enforcer Mailer can be installed on any server.

The mailer is a feature package included in the server installation **.msi** file:

- PPE Server – enforces password policies. It can be installed on Domain Controllers for domain password policy, or on servers and workstations for local account password policy.
- Configuration Console – manages policy configuration. Install where ever needed.
- Mailer Service – sends email reminders. Install on any server.

Follow the procedure in Install Password Policy Enforcer on a Server, selecting the **Mailer Service** feature. You can select the other features if appropriate for the server.

You can also install/uninstall the products using command line Silent Installation.

Install Password Policy Enforcer Web

Password Policy Enforcer Web V7.11 is a web server enabling users to change their Windows domain password from a web browser. Review the Requirements prior to running the installation.

Click the following link to download Password Policy Enforcer Web:

Password_Policy_Enforcer_WEB_7.11.zip

The PPE Web Setup Wizard

The Setup Wizard copies the required files onto the server and configures IIS to run the Password Policy Enforcer Web application.

Follow the steps below to install PPE Web.

Step 1 – Start the Password Policy Enforcer Web Setup Wizard (PPEWeb711.exe).

Step 2 – If another version of Password Policy Enforcer Web is detected, the Setup Wizard may required older files to be backed up. Back up these files if the original files have been modified. Click **Next**.

Step 3 – Click **Next**.

Step 4 – Read the License Agreement. Click **I accept the terms of the license agreement**, then click **Next** if you accept all the terms.

Step 5 – Click **Browse...** if you want to choose a different folder for the Password Policy Enforcer Web documentation and tools, then click **Next**.

Step 6 – Select an **IIS Web Site** from the dropdown. Change the default Virtual Directory, if needed.

NOTE: Password Policy Enforcer Web should be installed in its own virtual directory.

Step 7 – Click **Next** twice.

Step 8 – Wait for Password Policy Enforcer Web to install, then click **Finish**.

Upgrading from PPE Web V7.x

Some planning is needed to ensure a smooth upgrade from PPE Web V7.x. A trial run on a lab network is recommended.

Before You Begin

The HTML templates and associated images are overwritten during an upgrade. You must back up and customized HTML templates and images before upgrading. The HTML templates and images are installed in the `\Inetpub\wwwroot\ppeweb\` folder by default.

NOTE: A full backup of the PPE Web server is recommended. This allows you to roll back to the previous version if the upgrade cannot be completed. You may need to restart Windows after upgrading.

CAUTION: PPE Web V7.11 is only compatible with Password Policy Enforcer V7.0 and later. Upgrade PASSWORD POLICY ENFORCER to a compatible version if you have enabled Password Policy Enforcer integration.

Upgrading to V7.11

Step 1 – Start the PPE Web Setup Wizard and follow the prompts. The Setup Wizard uninstalls the previous version. There is no need to manually uninstall previous versions.

Step 2 – Restore any customized HTML templates and images after upgrading. Do not restore PPEWeb.dll from the backup as it belongs to the previous version.

Disable Windows Rules

The Windows password policy rules can place restrictions on password history, age, length, and complexity. If you enable the Password Policy Enforcer rules and the Windows rules, then users must comply with both sets of rules.

Password Policy Enforcer has its own history, minimum and maximum age, length, and complexity rules. See the Rules topic for additional information. You can use the Password Policy Enforcer and Windows rules together. A password is only accepted if it complies with the Windows and Password Policy Enforcer password policies.

These steps disable the Windows password policy rules:

Step 1 – Start the Group Policy Management Console **(gpmc.msc**).

Step 2 – Expand the forest and domain items in the left pane.

Step 3 – Right-click the **Default Domain Policy GPO** (or whichever GPO you use to set your domain password policy), then click **Edit...**

Step 4 – Expand the **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Account Policies**, and **Password Policy** items.

Step 5 – Double-click **Enforce password history** in the right pane of the GPO Editor.

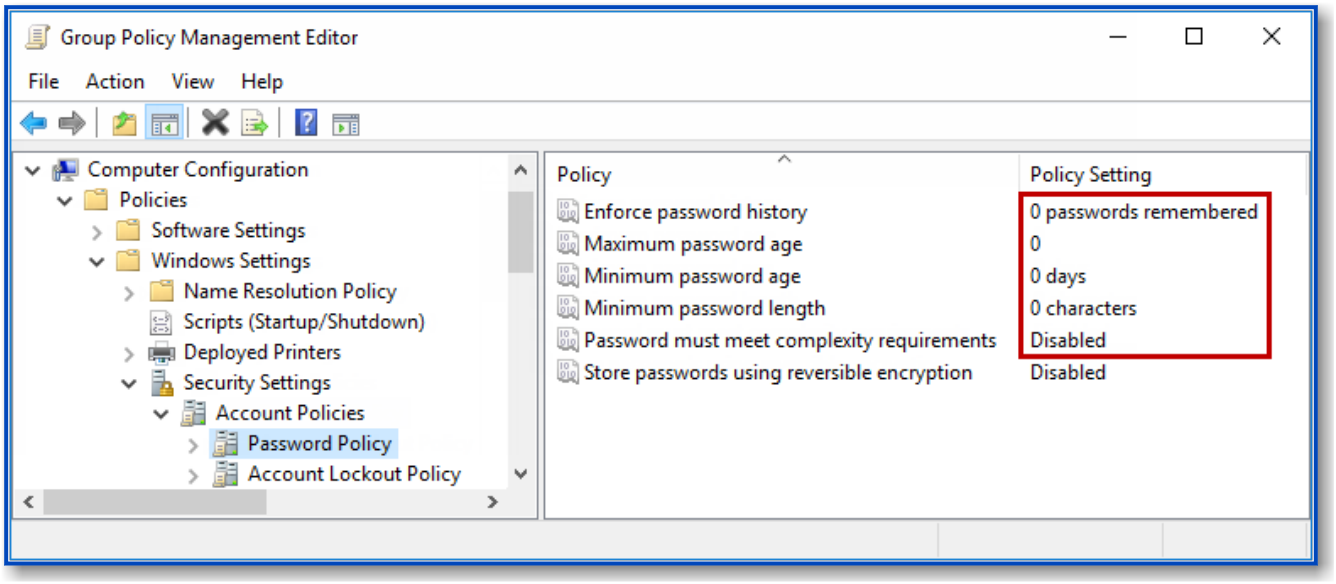
Step 6 – Enter **0** in the text box, then click **OK**.

Step 7 – Repeat the step above for the **Maximum password age**, **Minimum password age**, and **Minimum password length** policies.

Step 8 – Double-click **Password must meet complexity requirements** in the right pane.

Step 9 – Select the **Disabled** option, and then click **OK**.

Step 10 – Close the Group Policy Management Editor.



NOTE: You do not have to disable all the Windows password policy rules to use Password Policy Enforcer. You can use a combination of Password Policy Enforcer 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 Password Policy Enforcer.

HIBP Updater

Password Policy Enforcer can be configured to use the Have I Been Pwnd (HIBP) database. A copy of this database is hosted on the Netwrix website. The HIBP database contains a list of the hashes of known compromised passwords. During password change operations, the application can be configured to reject passwords with a hash that matches a hash in the HIBP database. See the Password Policy Enforcer Compromised Password Check topic for HIBP database information and configuration options.

The HIBP database must be initially deployed to a server or workstation with an internet connection that can retrieve and format the file. Once the database is formatted, you can distribute the HIBP database to your domain controllers so the Password Policy Enforcer server can check passwords against the HIBP database.

Considerations When Deploying the HIBP Database

Prior to deploying the HIBP database, consider the pros and cons when choosing its deployment location.

- The HIBP database takes up additional space on the machine where it is copied (approximately 13 GB, but subject to change)
- A network connection to the application server is not required to check passwords against the HIBP database

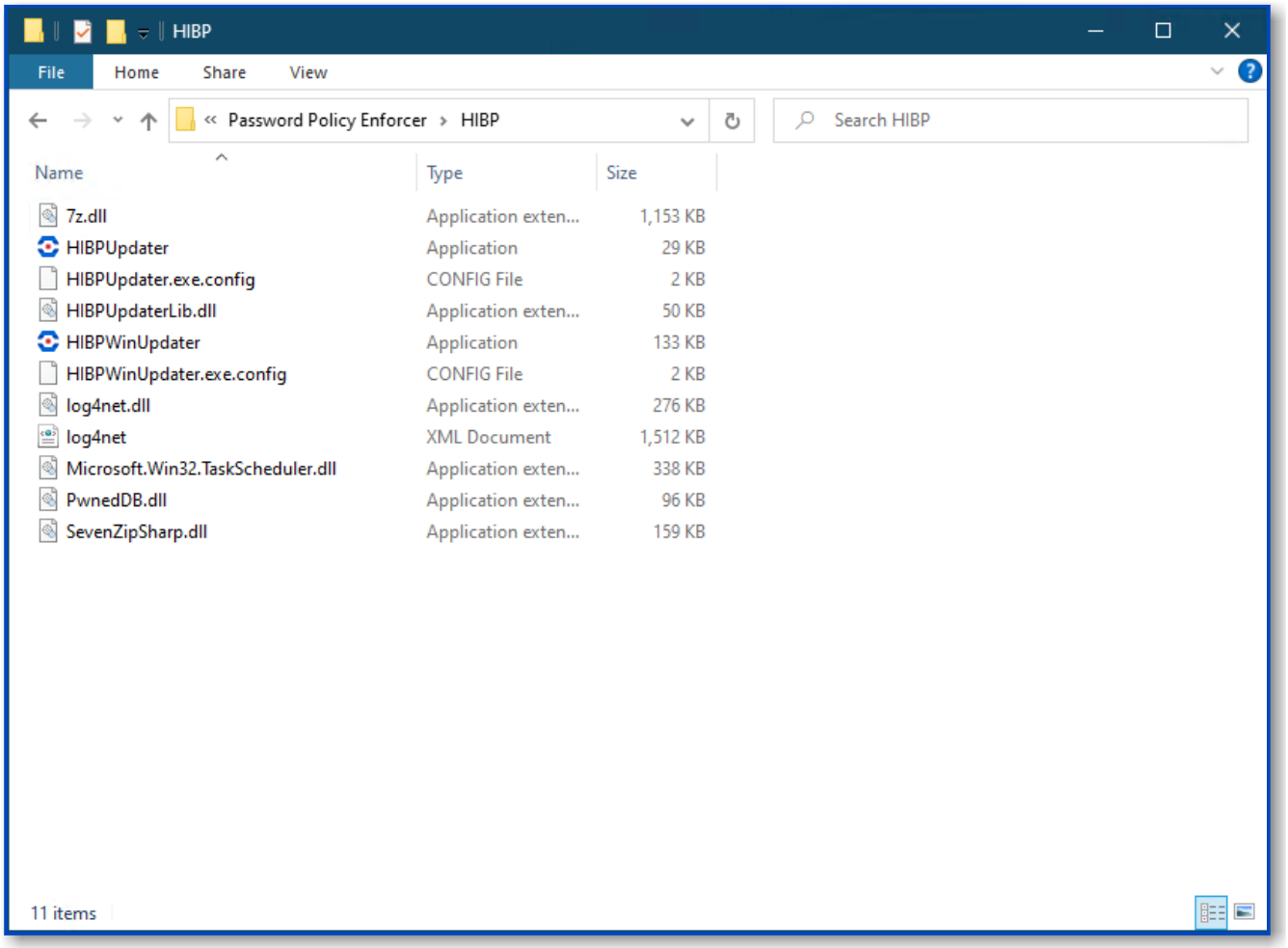
Installation and Configuration

The HIBP Updater is installed when you install the Password Policy Enforcer Configuration Console.

RECOMMENDED: Only run this from one server.

Step 1 – To access the HIBP Updater, navigate to the installation location:

```
...\Program Files\Password Policy Enforcer\HIBP\
```

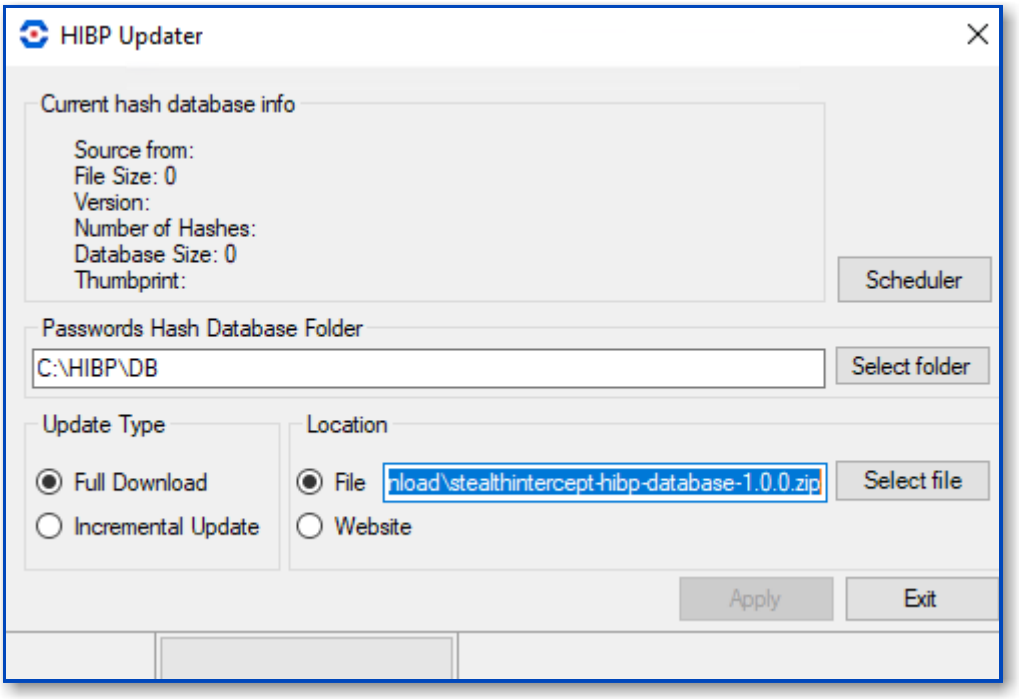


Step 2 – Click HIBPWINUpdater.

Passwords Hash Database

Password Policy Enforcer utilizes the Passwords Hash database to check if users' new and pending password (i.e. during a password reset) matches the hash of a compromised password from a data breach.

NOTE: First-time configuration of this window requires downloading the HIBP database from the Netwrix website.



CAUTION: Ensure the initial update of the database occurs during non-office hours. Due to the size of the hash file, this download takes up a significant amount of CPU and download time.

- Passwords Hash Database Folder – Central location of the Pwned database on the application server. The default path is:

  `…\HIBP\DB`

- Update Type:
  - Full Download – Download all data from the HIBP database hosted on the Netwrix website

- Incremental Update – Download updates from the HIBP database hosted on the Netwrix website instead of downloading the full HIBP database. This option is enabled after a full download of the HIBP database has completed.

  NOTE: Only the full HIBP database file obtained from the Netwrix website has version information. That full HIBP database file can be obtained using the Website option. Alternately, the HIBP database can be obtained outside of the application by downloading it directly from the Netwrix website using an FTP connection:

  - https://releases.netwrix.com/resources/stealthintercept/stealthintercept-hibp-database-1.0.0.zip
  - https://releases.netwrix.com/resources/stealthintercept/stealthintercept-hibp-database-1.0.0.zip.sha256.txt

  Then, the File option can be used and incremental updates will be enabled.

- Location:
  - File – If the application server does not have internet access, you can manually download the HIBP database and select the **File** radio button to browse to your local copy of the database
  - Web Site – This option points to the Netwrix website that hosts a copy of the latest HIBP database. This is the default option and the preferred method if the application server has internet access.
- Apply:
  - If Website is selected, then clicking **Apply** downloads the HIBP database from the Netwrix website and then processes the database for use by the application
  - If File is selected, then clicking **Apply** will process the local copy of the (manually obtained) database for use by the application

Hash File Replication

Password Policy Enforcer 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.db
```

See the Compromised Rule topic for additional information.

The path above only works if the computer has a Sysvol share. This will not be the case if you are using a workstation for policy testing, or if you are using Password Policy Enforcer to enforce local policies. If you are using Password Policy Enforcer 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.

CAUTION: %SystemRoot%. hash files should only be read from a local disk. Using shared hash files degrades performance, and could jeopardize security.

Scheduler

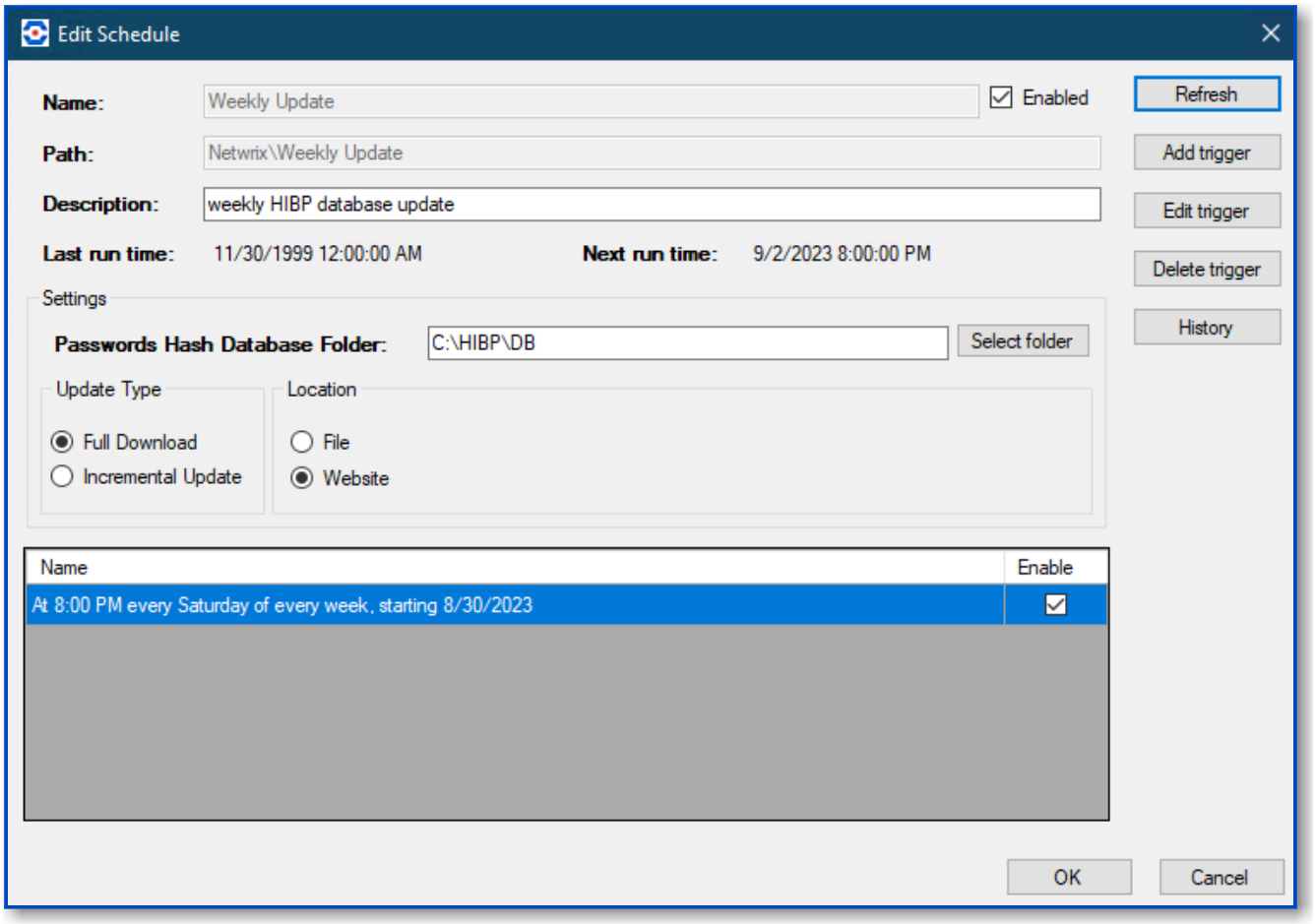
Password Policy Enforcer administrators can use the Scheduler portion of the HIBP Updater to automate the tool to retrieve and/or prepare the HIBP dataset. The Scheduler utilizes Microsoft Task Scheduler technology to execute the process.

How to Schedule a Task

Follow the steps to schedule a task.

Step 1 – Click **Scheduler** in the HIBP Updater.

Step 2 – Click **Add Schedule**. An Edit Schedule window appears that looks similar to the HIBP Updater window.



Step 3 – Enter the Name and Description of the schedule.

Step 4 – Select **Add Trigger** to add the interval that you wish to have the schedule run.

- You can add as many triggers as you want to a schedule.

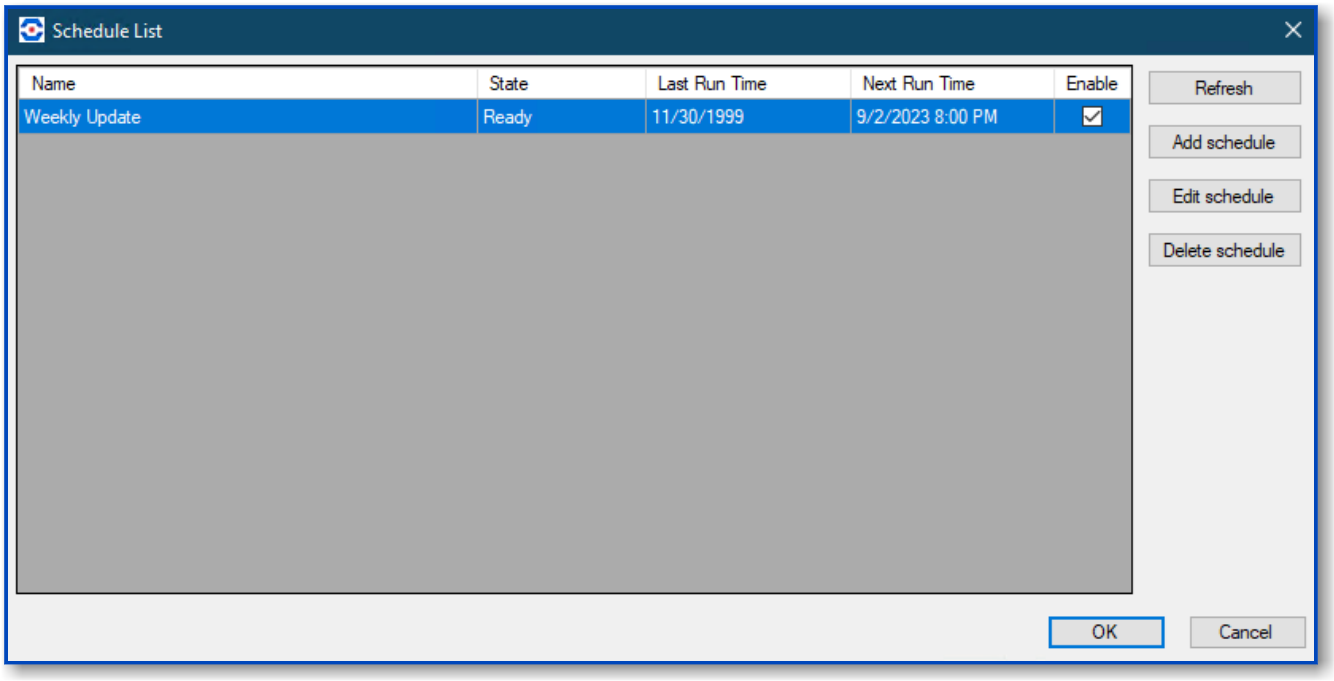
Step 5 – Select the Update Type and Location to get the update.

Step 6 – Once you have setup your schedule, click **OK** to save the schedule.

The HIBP database will be updated according to the configurations.

Schedule List

The Schedule List window shows the names, run times, next run times, and whether the schedule is enabled or not.



Use this window to Add, Edit, or Delete schedules for the HIBP Updater.

Enforce Password Reset with Azure Password Writeback

You can use Password Policy Enforcer to enforce password policies for passwords reset from Microsoft Entra ID and O365 by enabling password writeback in Microsoft Entra ID. See the How does self-service password reset writeback work in Microsoft Entra ID? Microsoft knowledge base article for additional information on password writeback in Microsoft Entra ID. Password writeback sends all new passwords from Microsoft Entra ID to an available, on-premises domain controller to check with Password Policy Enforcer. This happens while the user is resetting their password. See the Tutorial: Enable Microsoft Entra self-service password reset writeback to an on-premises environment and How it works: Microsoft Entra self-service password reset Microsoft knowledge base articles for additional information on password writeback for Microsoft Entra ID.

Upgrading Password Policy Enforcer

Upgrades are supported for versions 9.0 and above. Contact Customer Support at https://www.netwrix.com/support.html if you need assistance upgrading older versions

You can also install/uninstall the products using command line Silent Installation.

Upgrading the Password Policy Server

The Password Policy Enforcer installer detects existing installations and upgrades them to 11. See the Install Password Policy Enforcer on a Server topic for additional information. If you are performing an automated installation with Group Policy, then add the new **.msi** installer files to the same Group Policy Object used to install the older version. See the Install with Group Policy Management topic for additional information.

NOTE: Upgrade all your servers and domain controllers. Configuration changes performed with the new version do not affect servers running an older version. If you have multiple versions, you must make configuration changes in both configuration consoles until all domain controllers are upgraded to 11. Failure to do so may lead to inconsistent enforcement of the password policy.

Open the License settings on the Configuration Console after an upgrade to check your license details. Password Policy Enforcer reverts to a 30-day evaluation license if it cannot import the license key.

Upgrading the Password Policy Client

The Password Policy Client installer detects existing installations and upgrades them to 11. See the Install Password Policy Enforcer ClientInstall Password Policy Enforcer Client topic for additional information. If you are distributing the Password Policy Client with Group Policy, then add the new client **.msi** file to the same Group Policy Object used to install the older version. Upgrade and reboot the Password Policy Servers before upgrading the clients.

The Password Policy Enforcer 11 Password Policy Server is backwards compatible with the V10.x and V9.x Password Policy Client. You are not required to update the Password Policy Clients, but it is recommended.

Upgrading the Mailer

The Password Policy Enforcer installer detects existing installations of the Password Policy Enforcer Mailer and upgrades them to 11. See the Install Mailer Service topic for additional information.

Upgrade Notes

- Versions 9.x and above do not support perpetual license keys.

Uninstall Netwrix Password Policy Enforcer

Follow the steps to uninstall Password Policy Enforcer.

You can uninstall Password Policy Enforcer on every domain server and computer, or use Group Policy Management to remove the PPE Server and PPE Client on all machines.

You can also install/uninstall the products using command line Silent Installation.

Step 1 – Open **Start** > **Control Panel** > **Programs and Features** on each system where a PPE component is installed.

Step 2 – Click **Uninstall a program**.

Step 3 – Select Netwrix Password Policy Enforcer to uninstall the PPE Server, PPE Configuration Console and Mailer.

Step 4 – Click **Uninstall**.

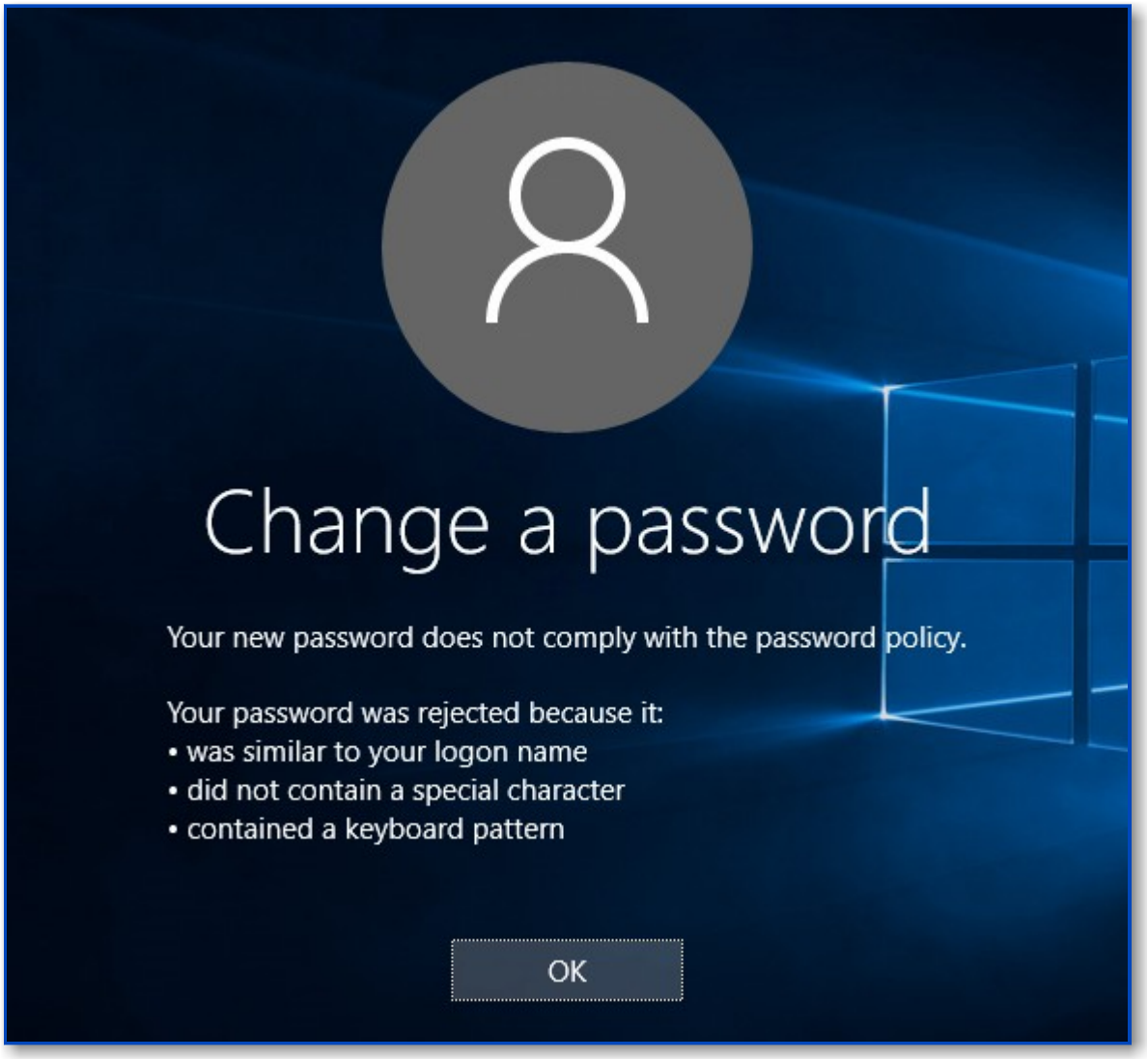
Step 5 – Select Netwrix Password Policy Client to uninstall the client.

Step 6 – Click **Uninstall**.

Step 7 – Reboot the Domain Controller.

Administration

Netwrix Password Policy Enforcer helps secure your network by ensuring users set strong passwords. When a user enters a password that does not comply with the password policy, Password Policy Enforcer immediately rejects the password and details why the password was rejected.



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

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

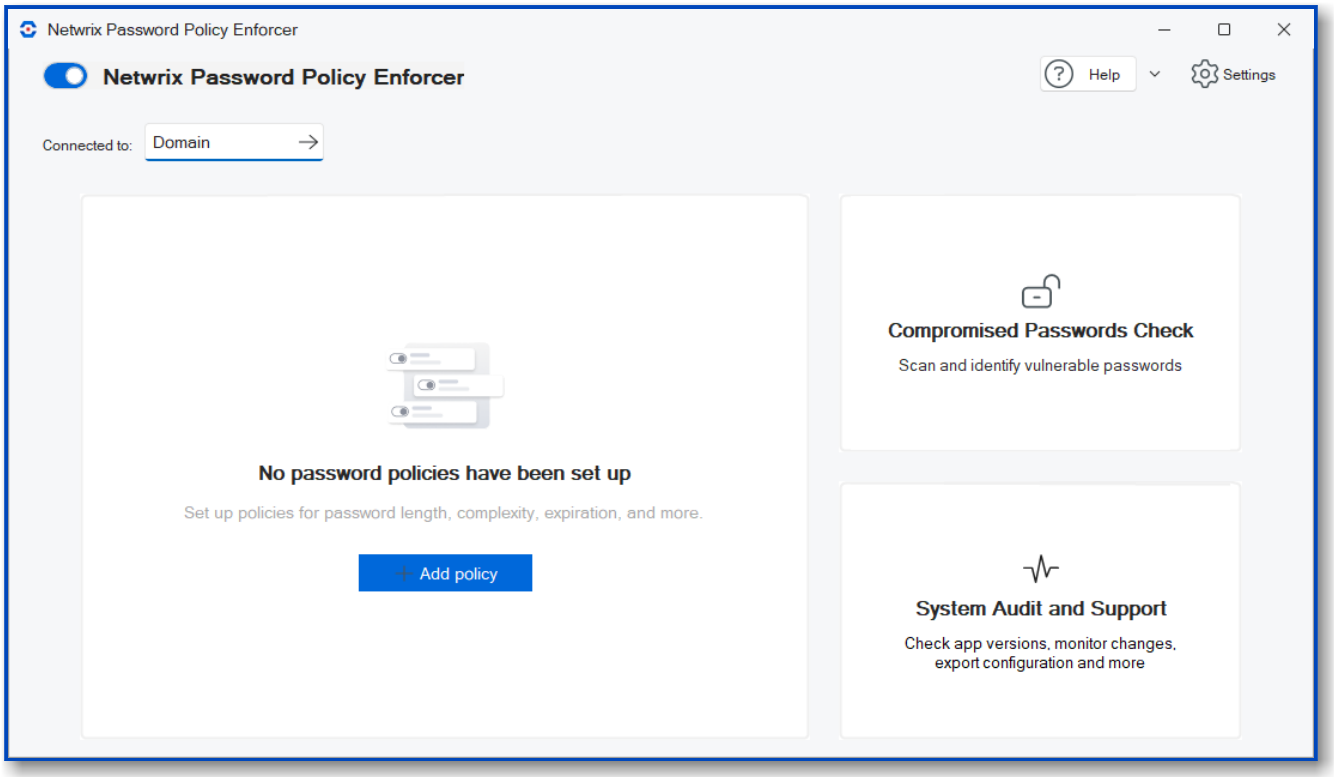
NOTE: The Evaluate Password Policy Enforcer contains step-by-step instructions to help you quickly install, configure, and evaluate Password Policy Enforcer. Consider using the Evaluation Guide if you are using Password Policy Enforcer for the first time, prior to installing and deploying on your domains.

Configuration Console

The PPE Configuration Console manages Password Policy Enforcer across your domain. It can be installed on multiple servers/workstations as convenient.

Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.



Dashboard Controls

The Configuration Console dashboard has all the tools you need to set up and manage Password Policy Enforcer.

- Enable/Disable Password Policy Enforcer

- Connected To
- Help
- Settings - General, Notifications, License

In addition, there are tiles to access Password Policy Enforcer major features:

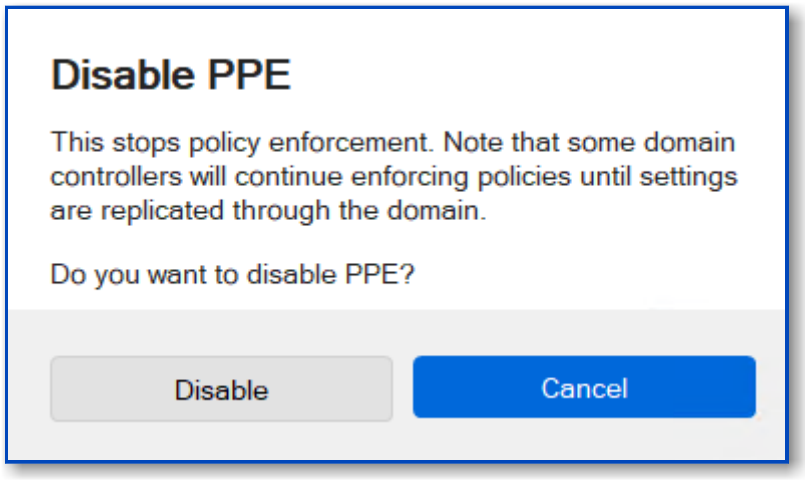
- Manage Policies
- Compromised Password Check
- System Audit and Support - Version Tracker, Support Tools, Property Editor

See the specific topics for details.

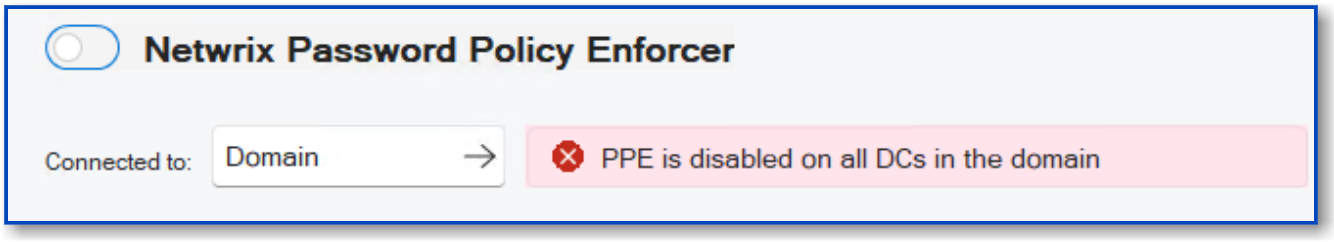
Enable/Disable Password Policy Enforcer

The toggle enables/disables Password Policy Enforcer on all domain controllers. It is enabled by default.

Click the toggle to disable PPE:



If PPE is disabled, click the toggle to enable:



Connected To

Sets the configuration for **Domain** (default) or **Local**. Password Policy Enforcer'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.

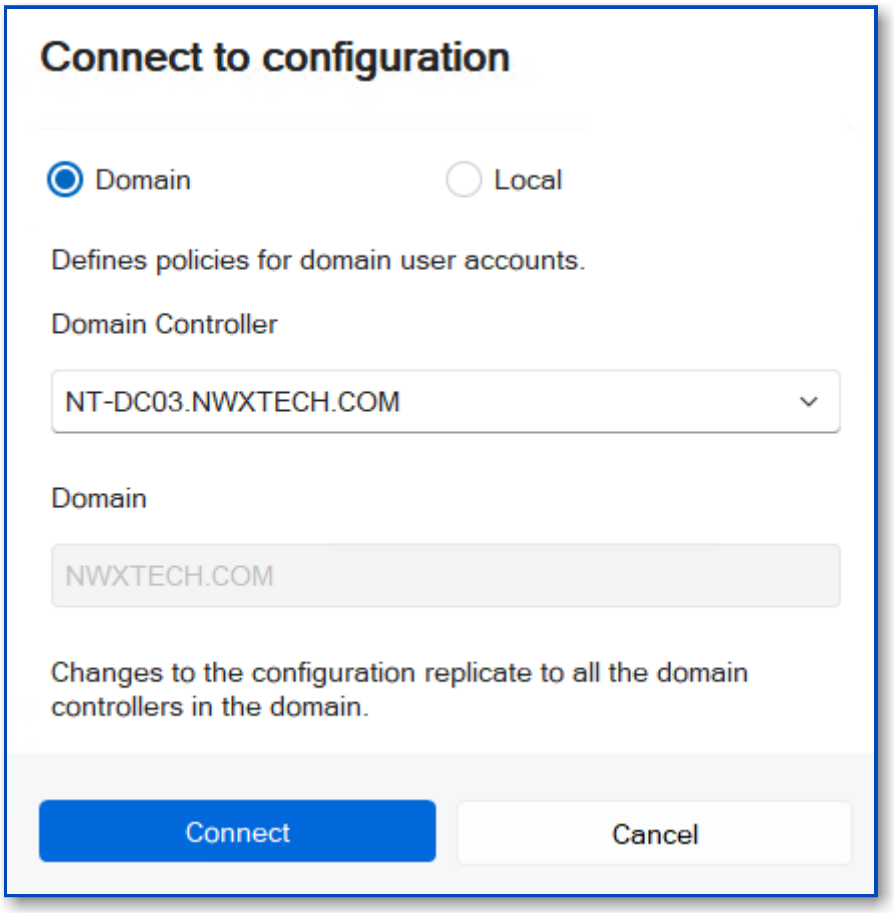
Domain configurations are stored in the **CN=Password Policy Enforcer** *version***,CN=System object**.

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

NOTE: Users with write permission to these objects can configure Password Policy Enforcer.

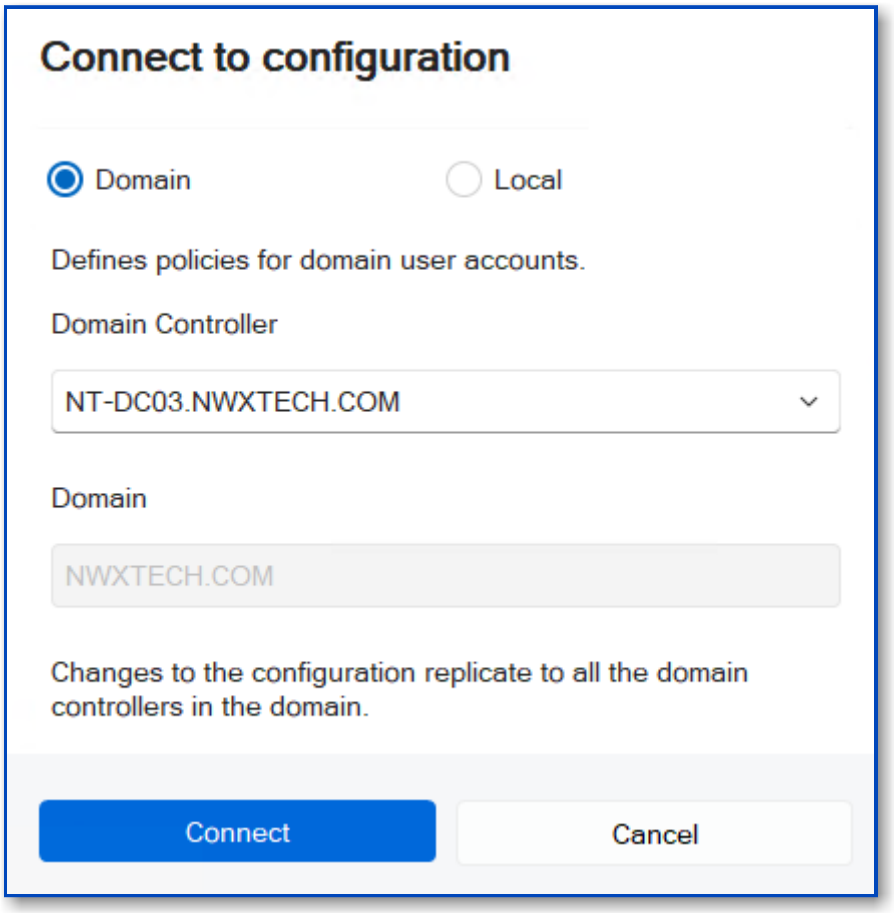
Domain

- Defines policies for domain user accounts.
- Select a Domain Controller from the list of domain controllers where PPE is installed.
- Configuration is replicated to all the domain controllers in the domain.



Local

- Defines policies for local user accounts.
- Only affects the computer where it is set.
- 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. See the Domain and Local Policies topic for additional information.



Help

Links to documentation and support tools.

- **Netwrix Help Center** launches the Password Policy Enforcer help.
- **About** displays the Configuration Console version.
- **Export Configuration Report** opens an export dialog. You can export the configuration as an html or txt file. Browse to the folder where you want the report.
- **Open Property Editor** launches the Property Editor.

  NOTE: Properties should only be changed when advised by Netwrix Support.

Settings

There are three tabs:

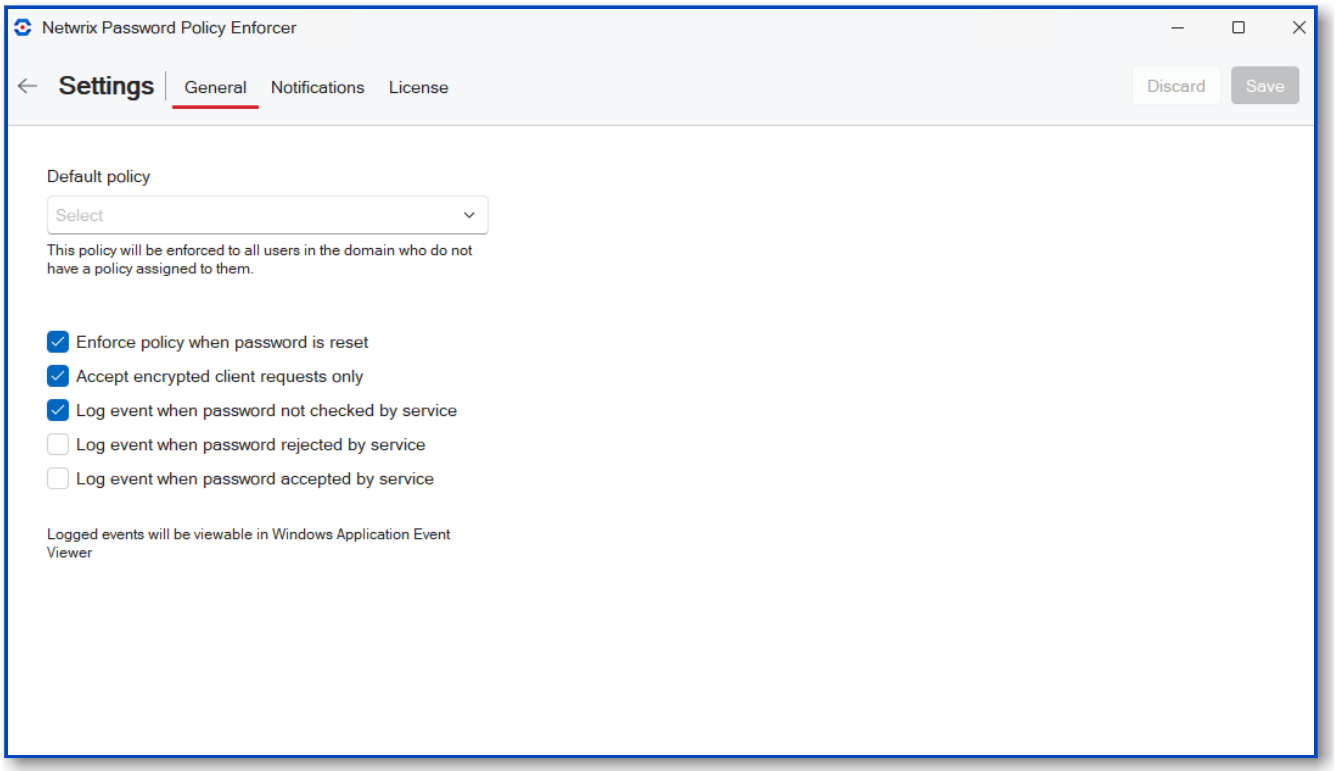
- General
- Notifications
- License

General

Open the **Settings** > **General** tab to set up policy and log settings. The general settings apply to either the domain or to a local computer, depending on your Connected To configuration setting.

If you make changes, click **Save** to keep your changes or **Discard** to cancel.

Here are the default settings.



- **Default policy** sets the policy to be enforced on the domain or local computer unless users have a different policy assigned to them.

- **Enforce policy when password is reset** requires users, administrators and helpdesk operators to comply with the password policy when resetting a password or creating a new user account. Default is checked.
    - Minimum Age rule is never enforced during a reset.
    - History rule is enforced if this option is selected and the **Enforce this rule when a password is reset** option is selected on the History Rule Properties.
- **Accept encrypted client request only** specifies requests from Password Policy Client, Netwrix Password Reset and Password Policy/Web must be encrypted. Client requests do not contain passwords or password hashes. See the Password Policy Client topic for additional information. Default is checked.
- **Log event when password not checked by service** adds an entry to the Windows Application Event Log whenever it accepts a password without checking it. Default is checked. This can occur if:
    - Password Policy Enforcer 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** is not selected.
- **Log event when password rejected by service** adds an entry to the Windows Application Event Log whenever a password is rejected. Default is not checked. The logged event includes:
    - Username
    - Source (client or server)
    - Rules the password does not meet.

      NOTE: Passwords or password hashes are not sent over the network.

  Most rules are enforced by both the Password Policy Client and Password Policy Server. If the Password Policy Enforcer Client is installed, a non-compliant password can be rejected 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 Password Policy Enforcer Client version is 9.0 or later. If a password is rejected by the Password Policy Server, then the event is logged.

- Client logged events only show the local rules the password violated. For example, the Compromised rule is only enforced by the Password Policy Server. See the Rules topic for additional information.
- Client rejections can be lost or duplicated if there are communication issues between the Password Policy Client and Password Policy Server.

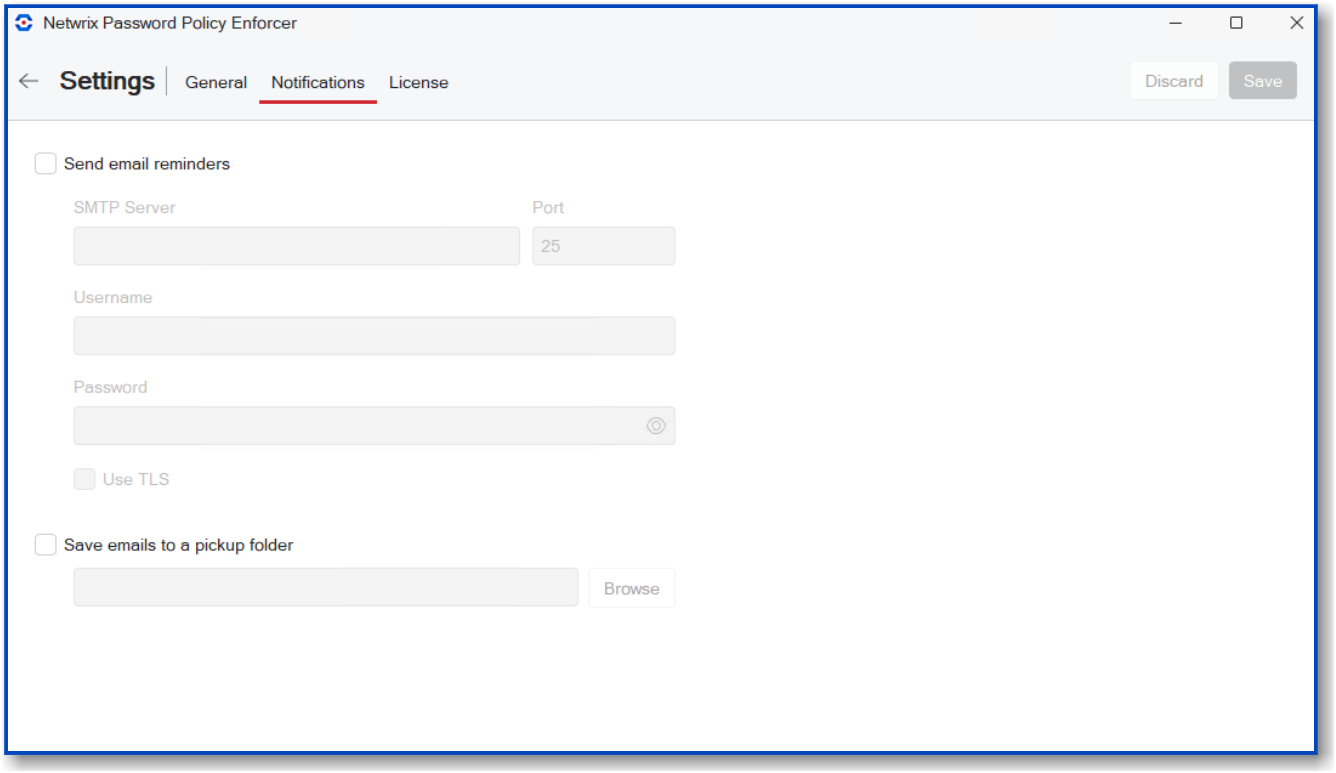
- **Log event when password accepted by service** adds an entry to the Windows Application Event Log whenever a password is accepted. The logged event includes the username. Default is not checked.

Notifications

Open the **Settings** > **Notifications** tab to set up notifications. Notifications are only available when **domain** is selected with the Connected To configuration setting.

If you make changes, click **Save** to keep your changes or **Discard** to cancel.

Here are the default settings.



- **Send email reminders**: check this option to send reminders. Default is not checked.
  - **SMTP Server**: enter IP address.

    - **Port**: enter port number.
    - **Username**: enter your username.
    - **Password**: enter your password.
    - **Use TLS**: check this option to enable TLS email encryption.
- **Save email to a pickup folder**: check this option to have the Mailer save emails to a folder for later delivery by a mail server. The mail server must monitor this folder for new email.
    - **Path**: Click **Browse** and select the path to the pickup folder.

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

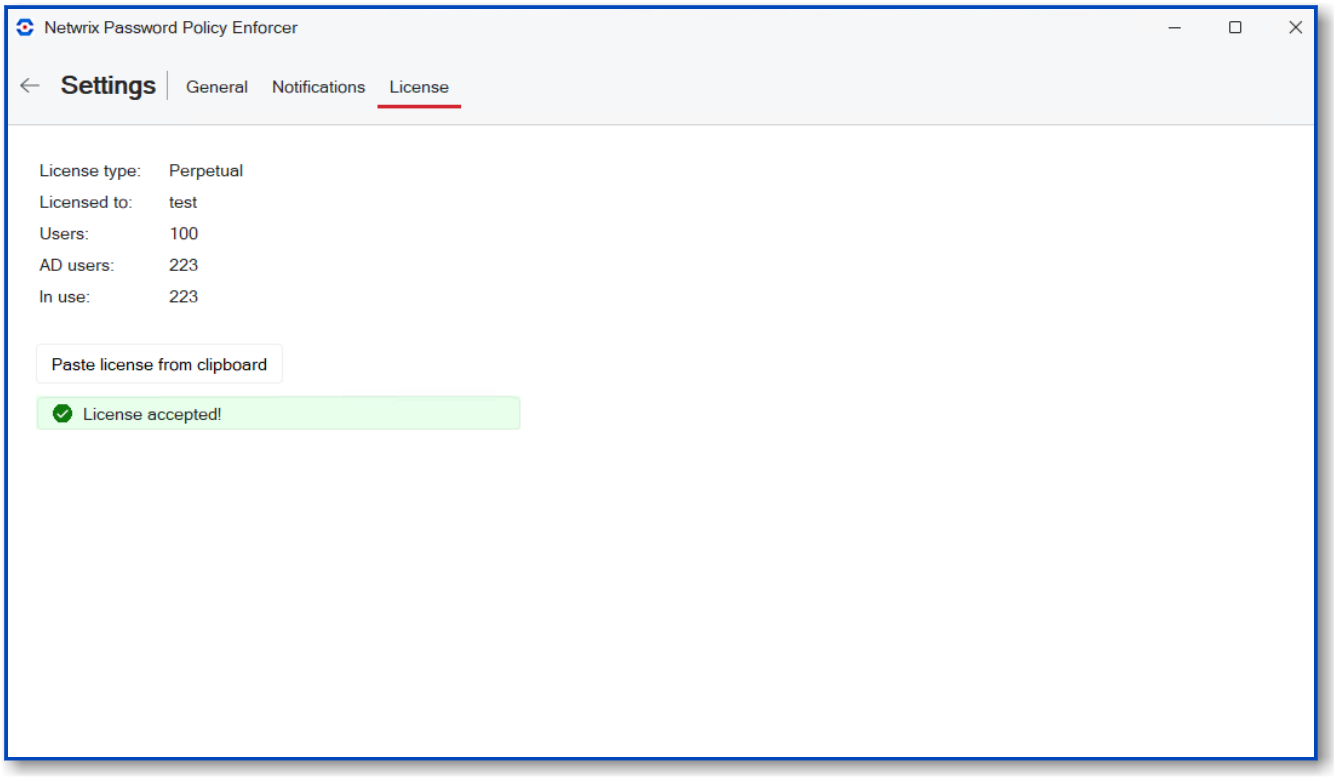
The Password Policy Enforcer Mailer sends emails at 2:00 AM every day (local time on your server). Check the Windows Application Event Log to monitor its progress. You can also run the Password Policy Enforcer Mailer from the command line to send email immediately, or to troubleshoot problems.

NOTE: You can change the time the mailer runs. Set the **PPE Mailer** service startup to **Disabled** or **Manual**, then stop the service. Create a task to run "**PPEMail /send**" at the desired time.

License

Open the **Settings** > **License** tab to view your current license. The license settings apply to either the domain or to a local computer, depending on your Connected To configuration setting.

To add or update your license, copy it from the email or file, then click **Paste license from clipboard**.



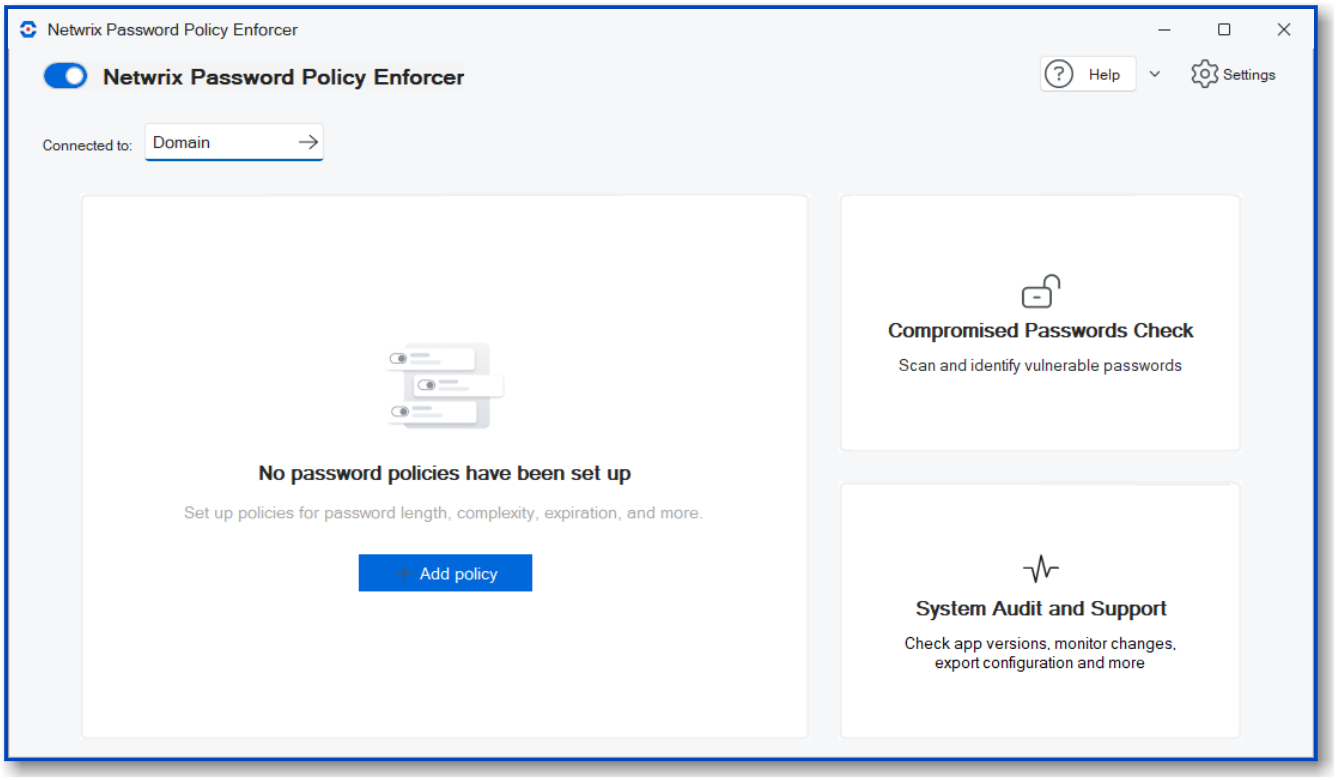
- **License type** and **Licensed to** are set based on your sales agreement.
- **Users** is the total number of available licenses.
- **AD Users** is the total number of Active Directory user accounts.
- **In use pertains** to active AD user accounts, disregarding disabled accounts.

Manage Policies

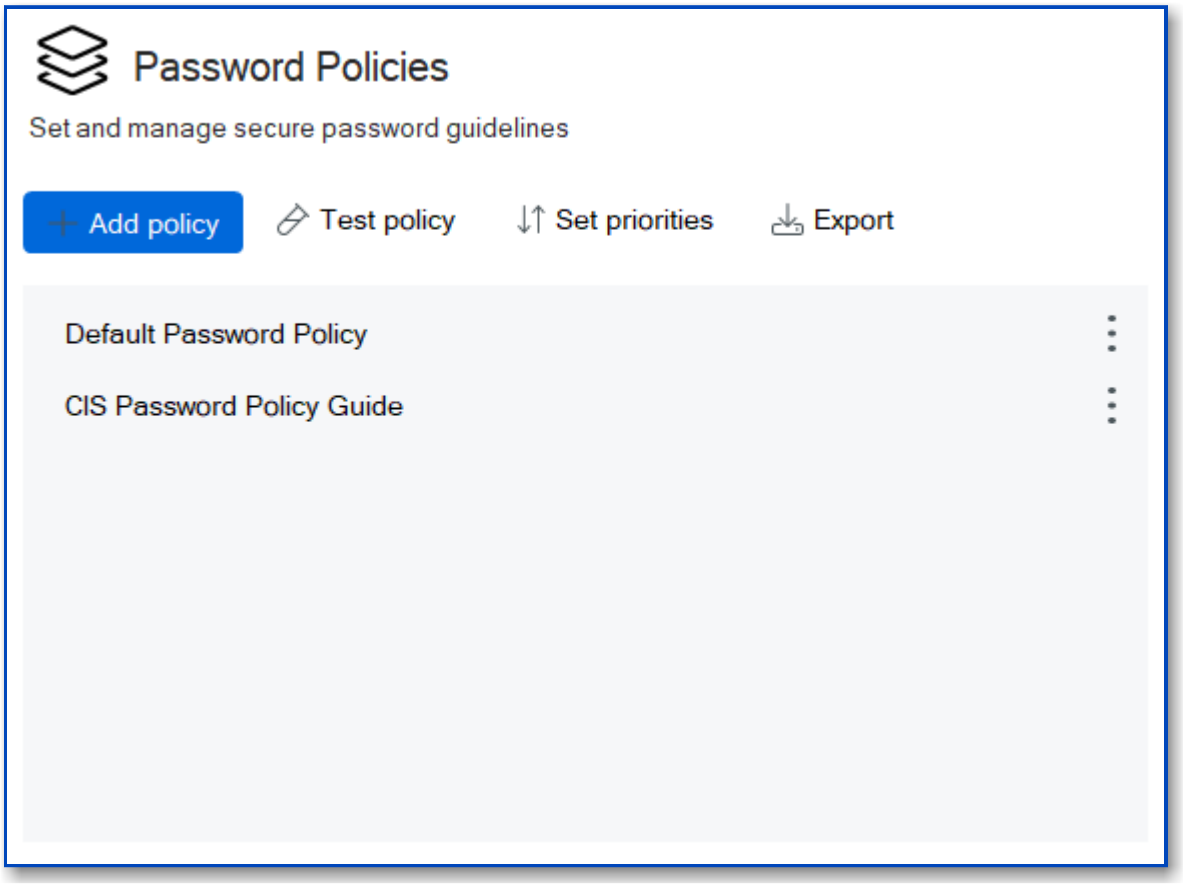
Netwrix Password Policy Enforcer can enforce up to 256 different password policies. You can assign policies to users directly, or indirectly through Active Directory security groups and containers (Organizational Units). See the Assign Policies to Users & Groups topic for additional information.

Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.



The Configuration Console dashboard shows **No password policies have been set up** when you are getting started with Password Policy Enforcer. Once you **Add a policy**, the dashboard shows the defined policies and tool links. In this example, the Default Password Policy and CIS Password Policy Guide have been added.



The policy management links are all on the Password Policies tile:

- Add a Policy.
- Set Up a Policy (click on existing policy name).
- Test Policy.
- Set Priorities.
- Export.
- Context menu (3 stacked dots) beside each defined policy Make Copy, Make Default/ Remove Default, Rename and Delete .

Add a Policy

Step 1 – Click **Add policy** from the Configuration Console.

Step 2 – Enter a unique policy name. Maximum is 32 characters.

Step 3 – Select a Policy template or **None** if you are creating your own.

Step 4 – Click **Create policy**.

Alternatively, you can select an existing policy and use the Context menu Make Copy option to start with the selected policy.

Policy Templates

Password Policy Enforcer contains Out-of-the-box Policy Templates based on the requirements of the most popular regulatory frameworks.

- Center for Internet Security (CIS) Password Policy Guide – See the CIS Password Policy Guide article for additional information.
- Center for Internet Security (CIS) Password Policy Guide MFA – See the CIS Password Policy Guide article for additional information.
- Cybersecurity Information Sharing Act (CISA)
- Criminal Justice Information Services (CJIS) Security Policy
- Cybersecurity Maturity Model Certification (CMMC)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Gramm-Leach-Bliley Act (FedRAMP)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPPA) – HIPAA Security Rule requires that organizations must implement procedures for creating, changing, and safeguarding passwords.
    - It also recommends training the workforce on ways to safeguard password information and establish guidelines to create and change passwords in a periodic cycle.
    - HIPAA doesn't offer any specific password complexity guidelines. To comply with HIPAA, organizations are better off following NIST password guidelines.
    - Most of healthcare institutions use the NIST framework.

- International Organization for Standardization (ISO/IEC) 27002 – See the NIST Special Publication 800-63B article for additional information.
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) – See the CIP-007-6 — Cyber Security – Systems Security Management article for additional information.
- National Institute of Standards and Technology (NIST) Special Publication 800-171
- National Institute of Standards and Technology (NIST) Special Publication 800-53
- National Institute of Standards and Technology (NIST) Special Publication 800-63b – See the NIST Special Publication 800-63B article for additional information.
- Payment Card Industry Data Security Standard (PCI DSS) – See the PCI Document Library web site for additional information.
- Payment Card Industry Data Security Standard (PCI DSS) (version 4)

Set Up a Policy

Once you add a policy, it needs to be set up or reviewed if you used a template. Click on the policy name to edit the policy. For each policy:

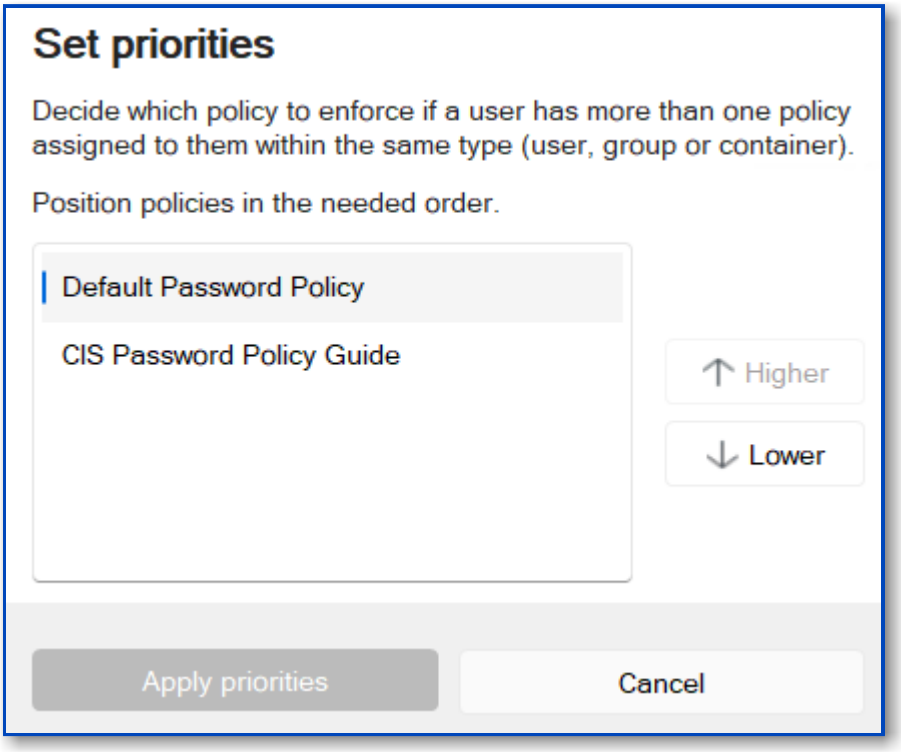
- Set up Rules.
- Assign Policies to Users & Groups.
- Enable the use of an optional Passphrase.
- Set up Policy Properties.
- Set up Messages for your users.

Test Policy

Launches the Test policy tool in a separate window. You can test **By user** and by **Password bulk test**. See the Test Policy topic for additional information.

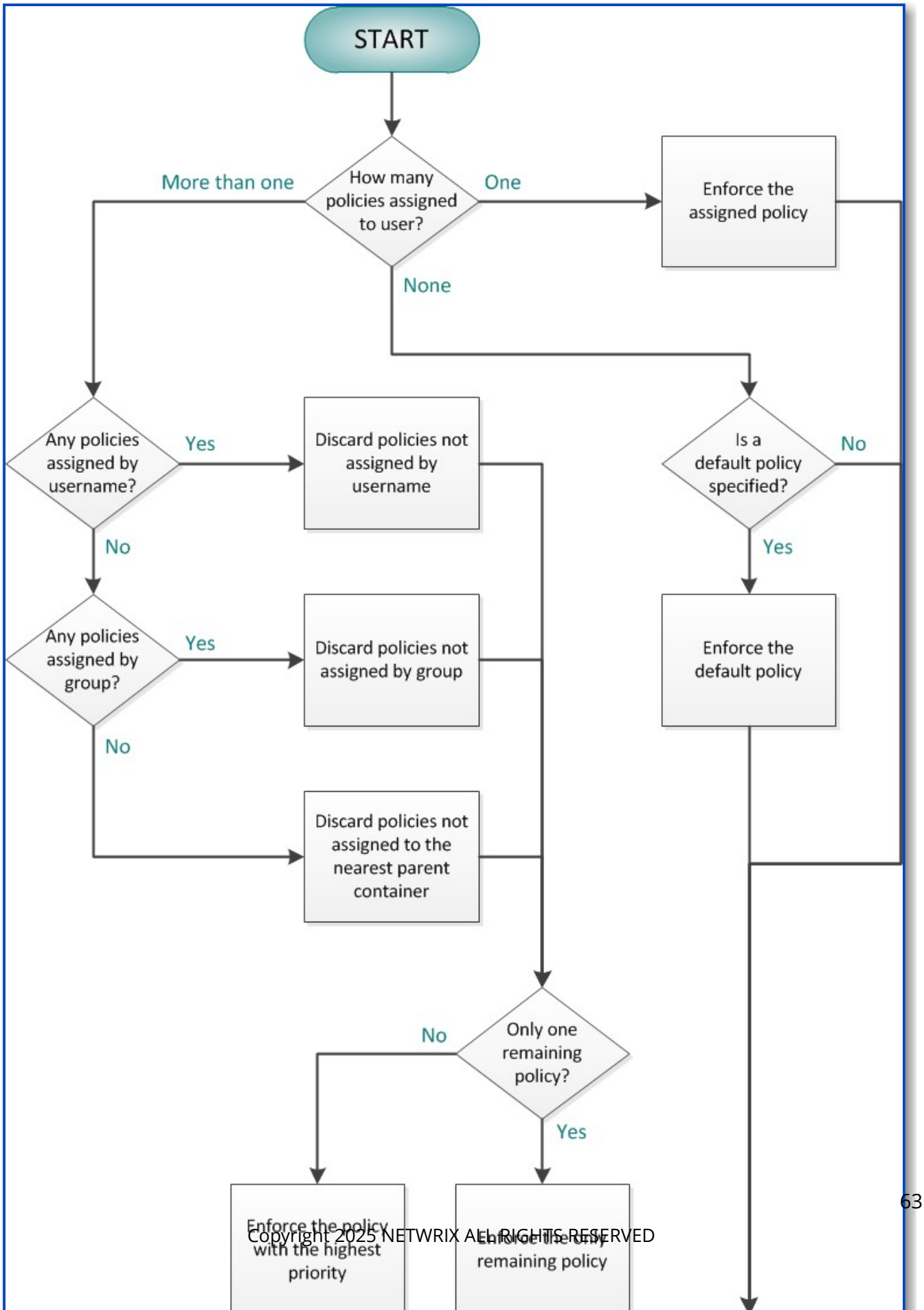
Set Priorities

Set priorities determines which policy to enforce if users have more than one policy. Click **Apply priorities** to save the new order.



Policy Selection Flowchart

This flowchart shows how Password Policy Enforcer determines a policy for each user. Use the Test Policy tool to quickly determine which policy Password Policy Enforcer is enforced for a particular user.



Export

Exports your policy configuration to **C:\Program Files\Password Policy Enforcer\Report\report.html**

Make Copy

Duplicates a policy. This context menu item is also available when you are editing a policy.

Step 1 – Click the context menu next to the policy to copy.

Step 2 – Select **Make copy** from the context menu.

Step 3 – Enter a unique name for the policy.

Step 4 – Click **Make copy**.

Make Default/Remove Default

Assigns the selected policy as the default, or removes the selected policy as the default. These context menu items are also available when you are editing a policy.

Step 1 – Click the context menu next to the policy to set as the default.

Step 2 – Select **Make default** from the context menu. The policy is assigned to all domain users who do not have a specific policy assigned. **Default** is indicated in the policy list. The context menu changes to **Remove Default**.

NOTE: If you assign a different policy as the default you are prompted that an existing default is set.

Rename

Renames a policy.

Step 1 – Click the context menu next to the policy to rename.

Step 2 – Select **Rename** from the context menu.

Step 3 – Enter a unique name for the policy.

Step 4 – Click **Rename**.

Delete

Deletes a policy. This context menu item is also available when you are editing a policy.

Step 1 – Click the context menu next to the policy to delete.

Step 2 – Select **Delete** from the context menu.

Step 3 – Click **Delete**. A warning confirmation is displayed if you delete the default policy.

Exempt Users from a Password Policy

You can exempt users from having to comply with the password policy when a default policy is specified.

Step 1 – Create a new policy for these users.

Step 2 – Leave all the rules disabled for this policy.

Step 3 – Assign this policy to the users who do not have to comply with any Password Policy Enforcer rules.

CAUTION: If PASSWORD POLICY ENFORCER has only one policy and that policy is also the default policy, then PASSWORD POLICY ENFORCER 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 Password Policy Enforcer 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.

Rules

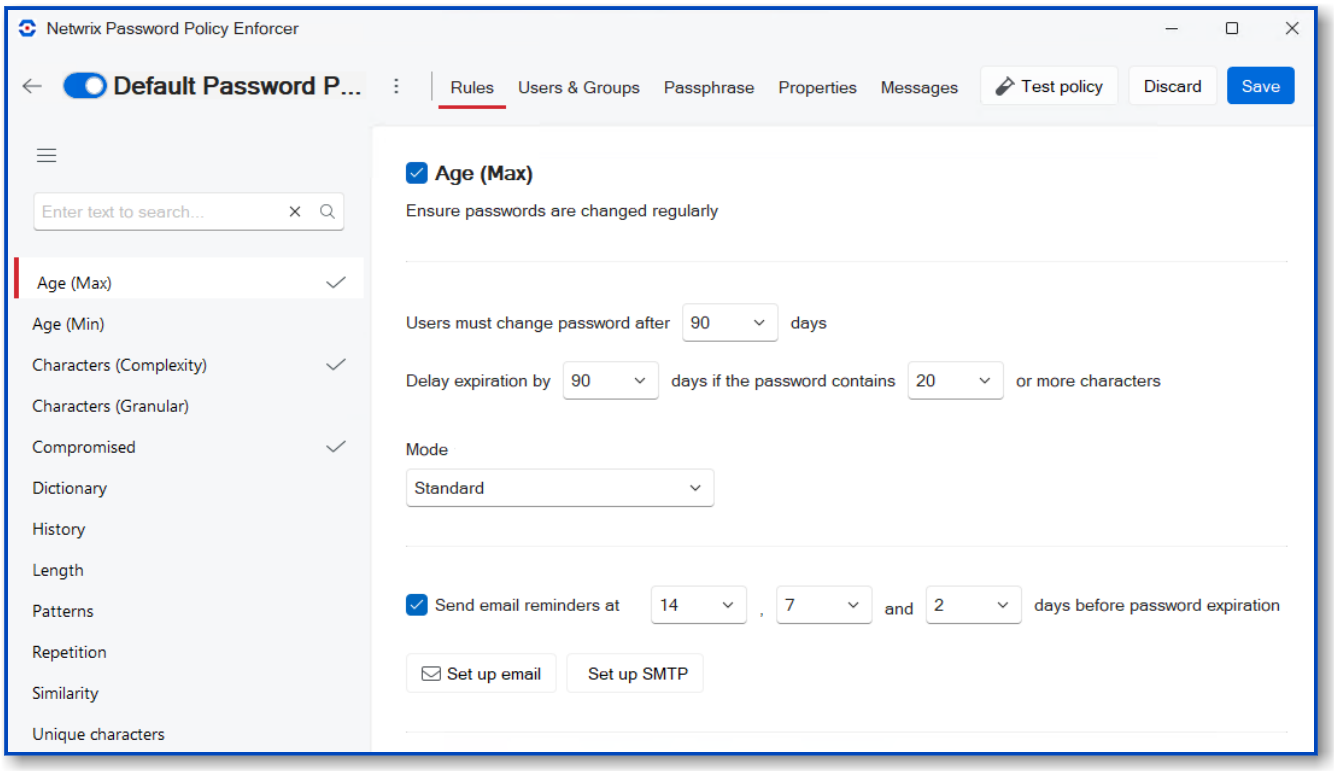
Netwrix Password Policy Enforcer uses rules to decide if it should accept or reject a password. Each policy has rules that are configured independently of the rules in other policies. To display the rules for a policy:

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

Step 2 – Click on a policy name to open the policy configuration page.

The **Rules** tab opens by default. A check mark beside a rule indicates that the rule is enabled (being enforced). Click a rule to set the rule's properties.



Review the sections on **Detecting Character Substitution** and **Tolerance** prior to setting up the rules for your policy.

You can **Save** each rule and use **Test Policy** as you are setting your rules. Turn on **Verbose logging** on the **Test Policy** window to see which rules you have tested.

Rules:

- Age (Max) Rule

- Age (Min) Rule
- Characters (Complexity) Rule
- Character (Granular) Rules
- Compromised Rule
- Dictionary Rule
- History Rule
- Length Rule
- Patterns Rule
- Repetition Rule
- Similarity Rule
- Unique Characters Rule

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

Original		Substituted
A	a	^ @
B	b	8

Original		Substituted		
C	c	**(or {**	<	[
D	d	**) or }**	>	]
E	e	3		
G	g	6 or 9		
I	i	**! or |**	1	
O	o	0 or (zero)		
S	s	$ or 5		
T	t	+ or 7		
Z	z	2		

Tolerance

Some Password Policy Enforcer 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. Password Policy Enforcer rejects a password if the specified tolerance is exceeded. For example, the logon name "mary**jones**", and the password "**Jones**town" contain five consecutive matching characters (shown in bold type). Password Policy Enforcer 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 Patter rules have an Auto tolerance option. Setting the tolerance to Auto instructs Password Policy Enforcer 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 Password Policy Enforcer 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 Password Policy Enforcer to calculate an appropriate tolerance during every password change.

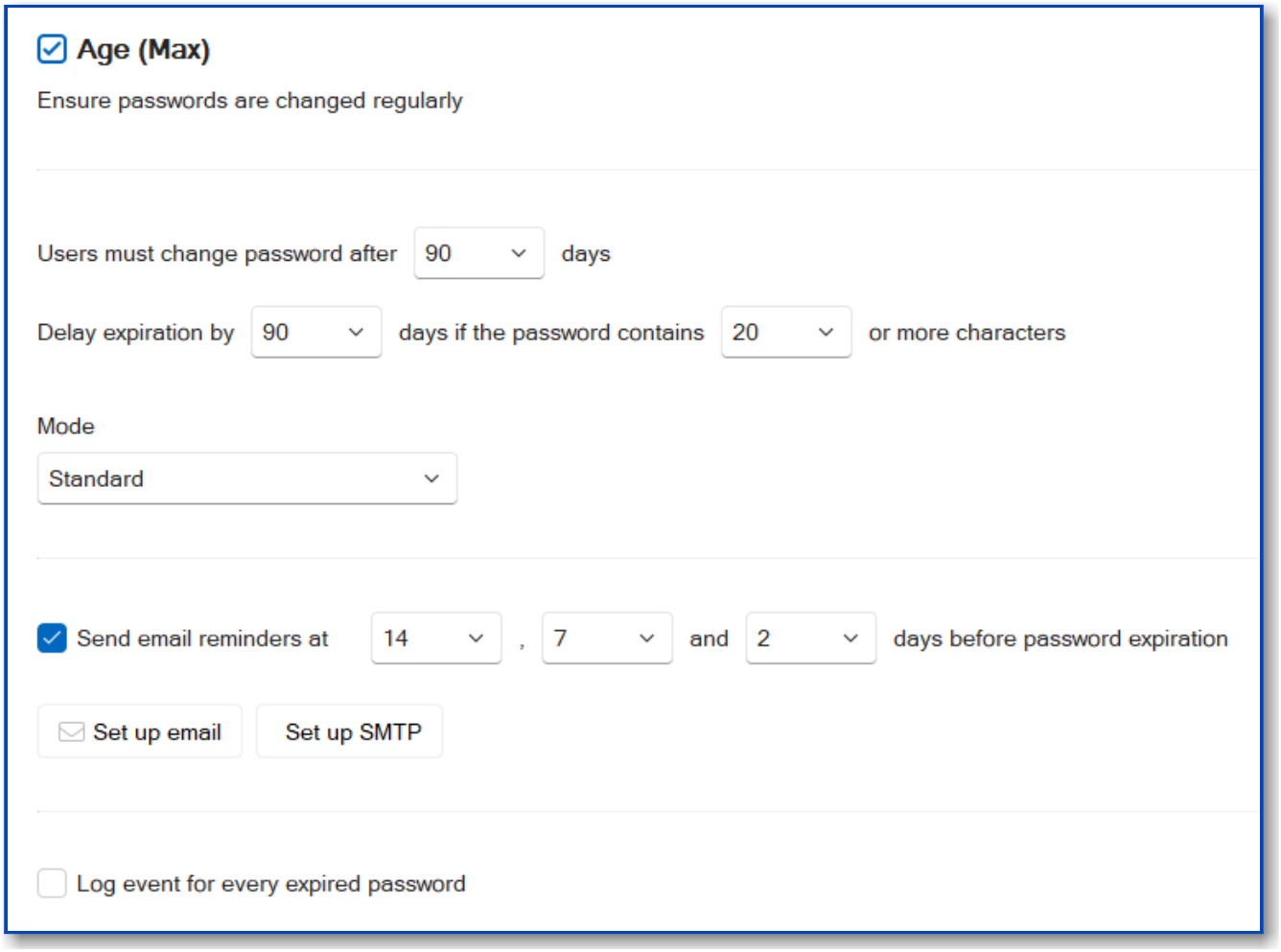
Password Policy Enforcer sets the tolerance to the length of the comparison parameter minus one. The table below shows some parameter values and the calculated tolerance. Password Policy Enforcer rejects a password if it contains all the text in the Value column (or a derivative of it if character substitution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

Rule	Parameter	Value	Tolerance
User Logon Name	Logon name	maryjones	8
User Display Name	Display name	Mary Jones	9
Similarity	Current password	oldpass	6
Character Pattern	Character pattern	abcdefgh	7

Password Policy Enforcer'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 Password Policy Enforcer accepts passwords that contain the parameter value if the comparison parameter only contains one or two characters. Contact Netwrix support if you need to change the minimum limit.

Age (Max) 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 **Age (Max)** checkbox 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 do 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 length.

NOTE: 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". Password Policy Enforcer 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. Contact Netwrix support if you must change the pre-Windows 2000 name. Change a Password Policy Enforcer configuration setting (any setting) after moving or renaming the group to trigger a cache update in Password Policy Enforcer. Password Policy Enforcer recreates this group if you delete it. To stop creating a group, make the two days values equal in all policies.

Choose a value from the Mode drop-down list to specify how Password Policy Enforcer 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.

Use the Warning and Transitional modes to gradually introduce a new password policy. These modes reduce the number of forced password changes, allowing the help desk 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.

NOTE: 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. You can alter this behavior in the Windows Group Policy security settings. See the Interactive logon: Prompt user to change password before expiration Microsoft article for additional information.

Password Policy Enforcer 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. Password Policy Enforcer 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.

Set up Email

Click the **Set up email** to configure the e-mail message options.

Type the name and email address you wish to appear in the email's From field in the **From** text box. The correct format is "Display Name" <mailbox@domain.com>

Type the text for the email's Subject field in the **Subject** text box.

Type the body of the email in the large text box. The email is sent as plain text unless the body includes the <html> tag. If sending email 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 Password Policy Enforcer Mailer will read the email body from the specified file.

The email's subject and body can contain various macros. Use these macros to personalize the email.

Macro	Replaced with
[LOGON_NAME]	User's logon name
[FIRST_NAME]	User's first name
[LAST_NAME]	User's last name
[DAYS_TO_EXPIRY]	Days until password expires

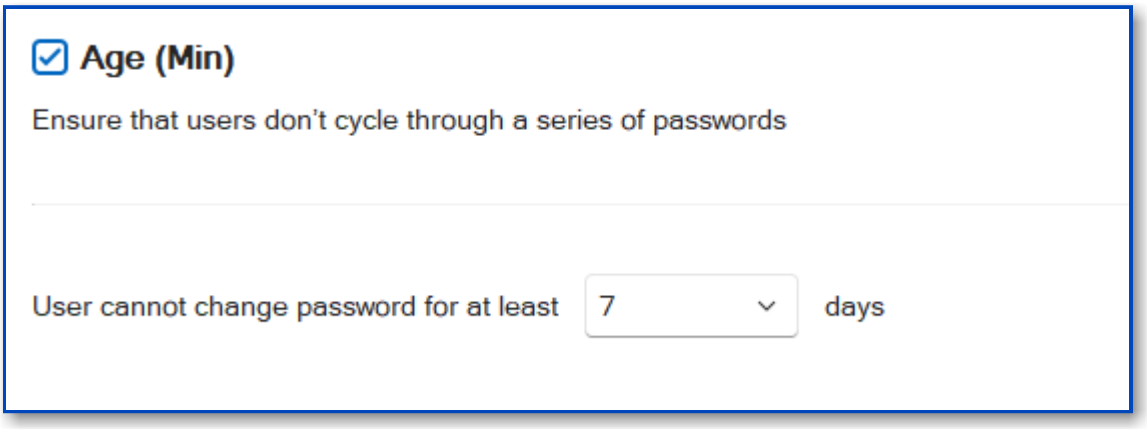
Macro	Replaced with
[EXPIRY_DATE]	Expiry date in short format
[EXPIRY_DATE_LONG]	Expiry date in long format
[EXPIRY_DAY]	Expiry day (1 to 31)
[EXPIRY_DAY_NAME]	Expiry day (Monday, Tuesday, ...)
[EXPIRY_MONTH]	Expiry month (1 to 12)
[EXPIRY_MONTH_NAME]	Expiry month (January, February, ...)
[EXPIRY_YEAR]	Expiry year (2021, 2022, ...)

Set up SMTP

Opens the Notification settings. See the Configuration Console topic for additional details.

Age (Min) 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 **Age (Min)** check box to enable the Minimum Age rule.

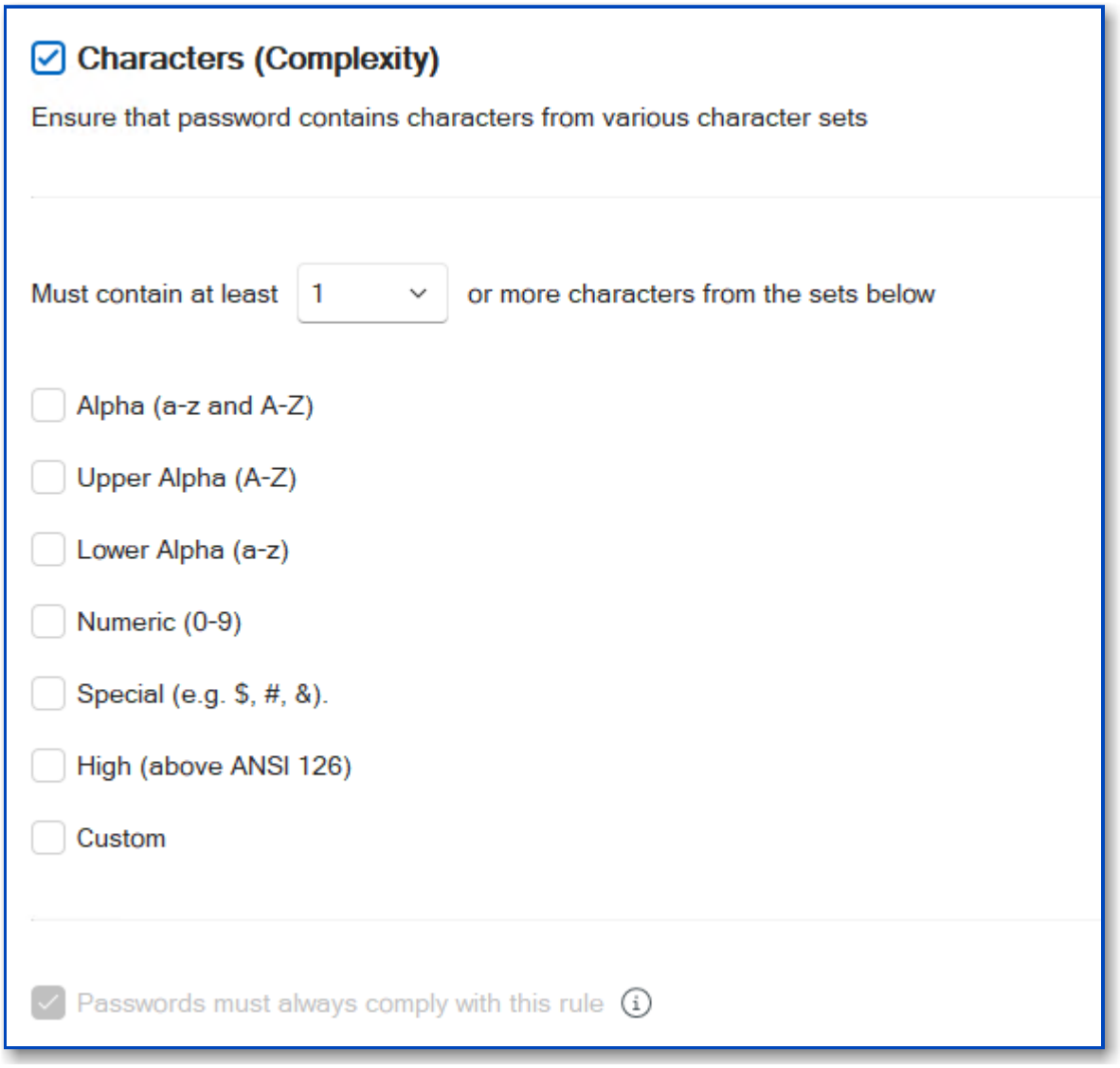
Select the number of days before a user can change their password.

NOTE: 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 Password Policy Client only displays the Minimum Age rule's Reason insert. See Password Policy Client topic for additional information. 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.

Characters (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 **Characters (Complexity)** checkbox to enable the Character Complexity rule.

Select the number of required character sets. Passwords are rejected if they do not contain characters from at least the specified number of character sets.

Select the available character sets. 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. Password Policy Enforcer 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. See the Passphrase topic for additional information.

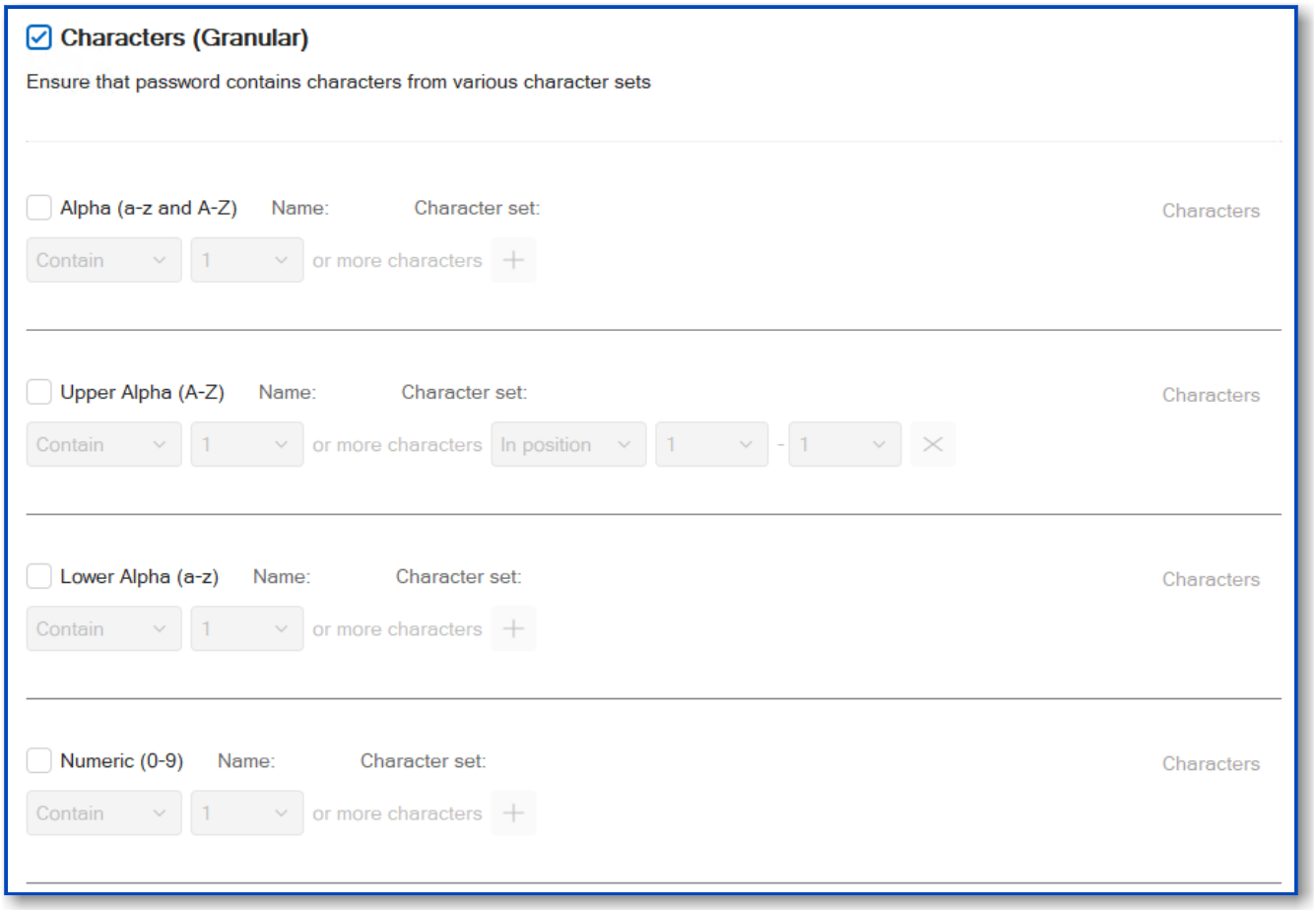
NOTE: The Complexity rule uses custom character set definitions from the Character rules, even if the Character rules are disabled.

This default character set contains the following:

Rule	Default character set
Alpha Lower	Lowercase alphabetic (a - z)
Alpha Upper	Uppercase alphabetic (A - Z)
Alpha	Uppercase and lowercase alphabetic (a - z & A - Z)
Numeric	Numerals (0 - 9)
Special	All characters not included above
High	All characters above ANSI 126
Custom	No default characters

Character (Granular) Rules

Password Policy Enforcer 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. By default, the Password Policy Enforcer selects the Password Policy Enforcer character on the Set Priorities page.

NOTE: Only Password Policy Enforcer 11 and higher will contain the Windows character set. Password Policy Enforcer 9, Netwrix Password Reset3 and Password Policy Enforcer Web 7 (and older for all products) use the Password Policy Enforcer character set.

Select the **Characters (Granular)** check box to enable the Characters rule.

For each selected character set, select whether they **Contain** or **Not contain** the specified number of characters.

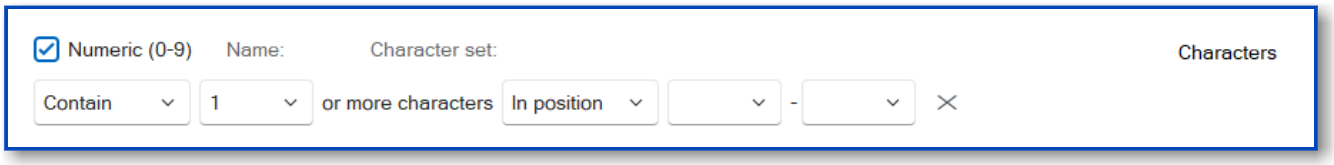
Select the **contain** option if this rule should ensure that new passwords contain certain characters. Only one character is required by default, but you can specify a different value by choosing the required number of characters from the drop-down list beside the **contain** option.

Select the **not contain any...** option if this rule should ensure that new passwords do not contain certain characters.

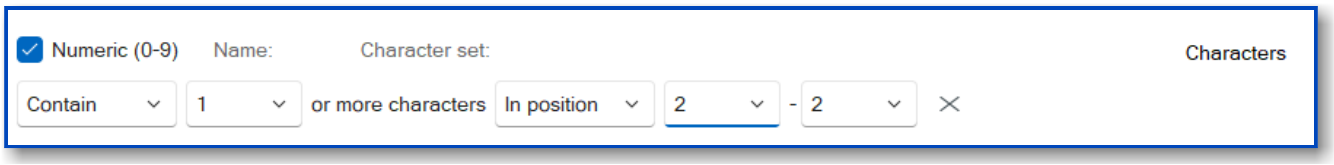
You can further restrict the rule by defining positions or embedding characters.

Click the + sign by the character set.

Select **In position**.



If you want to restrict this rule to certain character positions, choose the starting position from the first entry box and the ending position from the second entry box. 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.



Click the + sign by the character set.

Select **Embedded**.

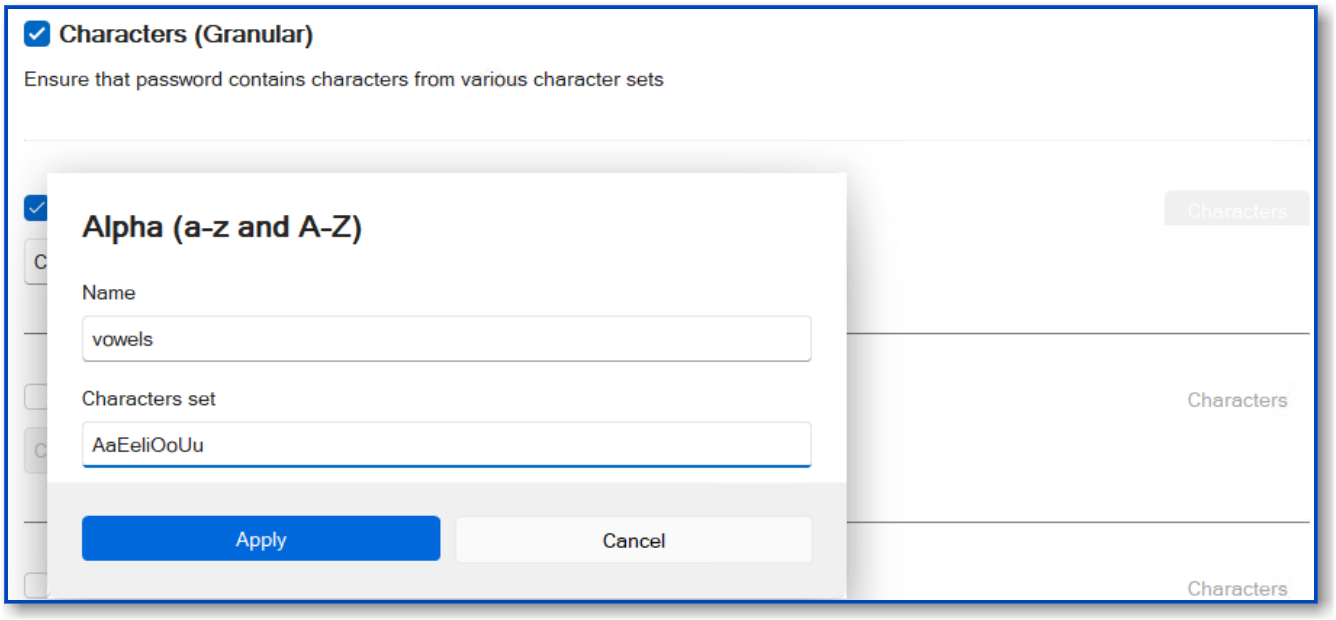
Select the **Embedded** check box if users are required to embed these characters within their passwords. For example, the passwords "12hello", "1hello", and "hello$987" do not contain any embedded numeric characters, but these passwords do contain embedded numeric characters (shown in bold type): "he**7**llo", "4he**3**llo", "23hello**7**$45". Embedded numeric and special characters can help to protect passwords from cracking attacks.

NOTE: 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.

You can customize character sets with the Characters option for a selected set.

Step 1 – Click **Characters** beside a selected Character set.

Step 2 – Enter a **Name**. This example uses **vowels**.



Step 3 – Enter the **Characters**. This example uses **AaEeIiOoUu**.

Step 4 – Click **Apply**.

If you save and test the policy, you see **vowels** is listed as a requirement.

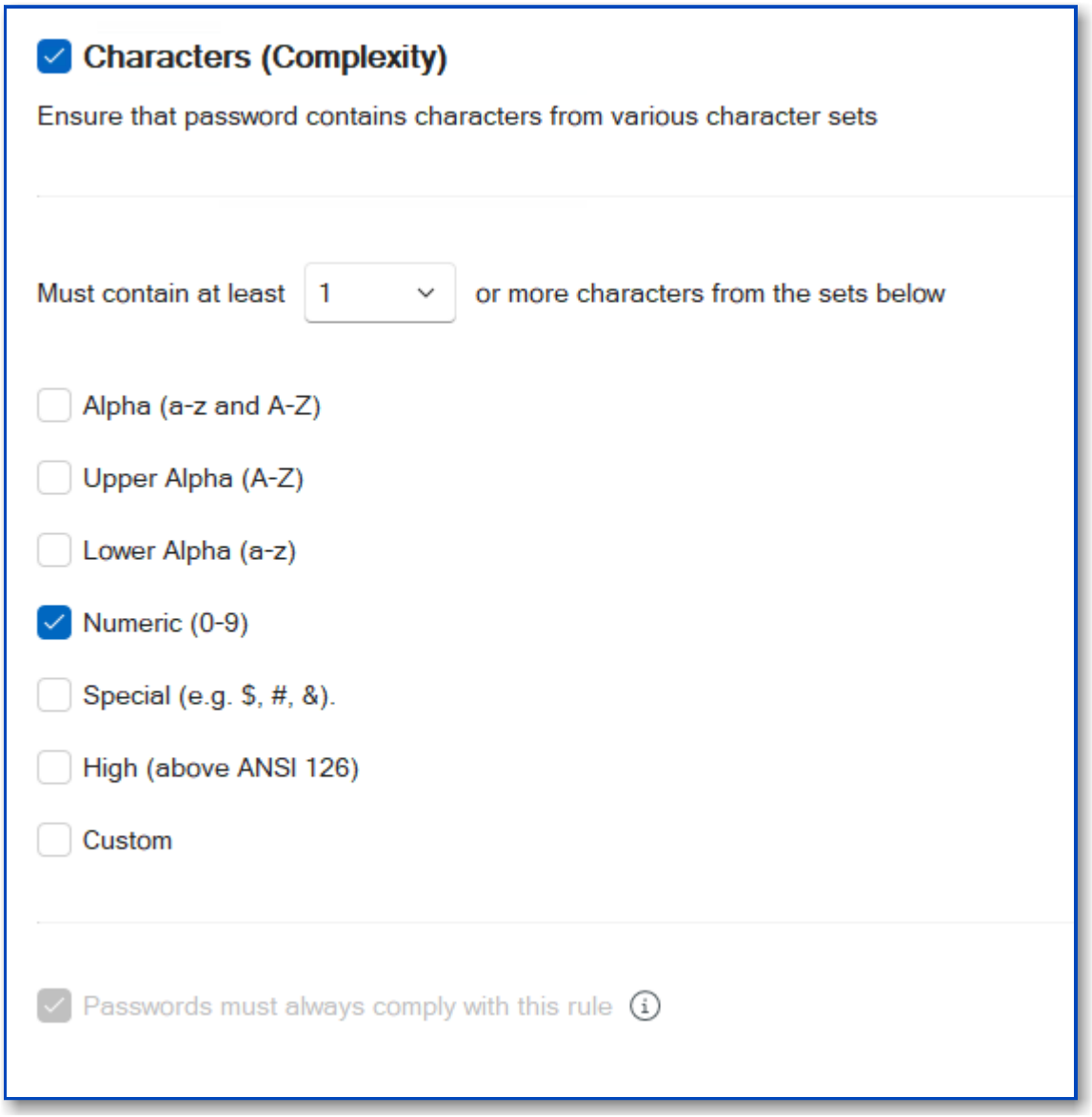
To remove a custom set, click **Characters** and delete the information. Click **Apply**.

Enforcing Complex Character Requirements

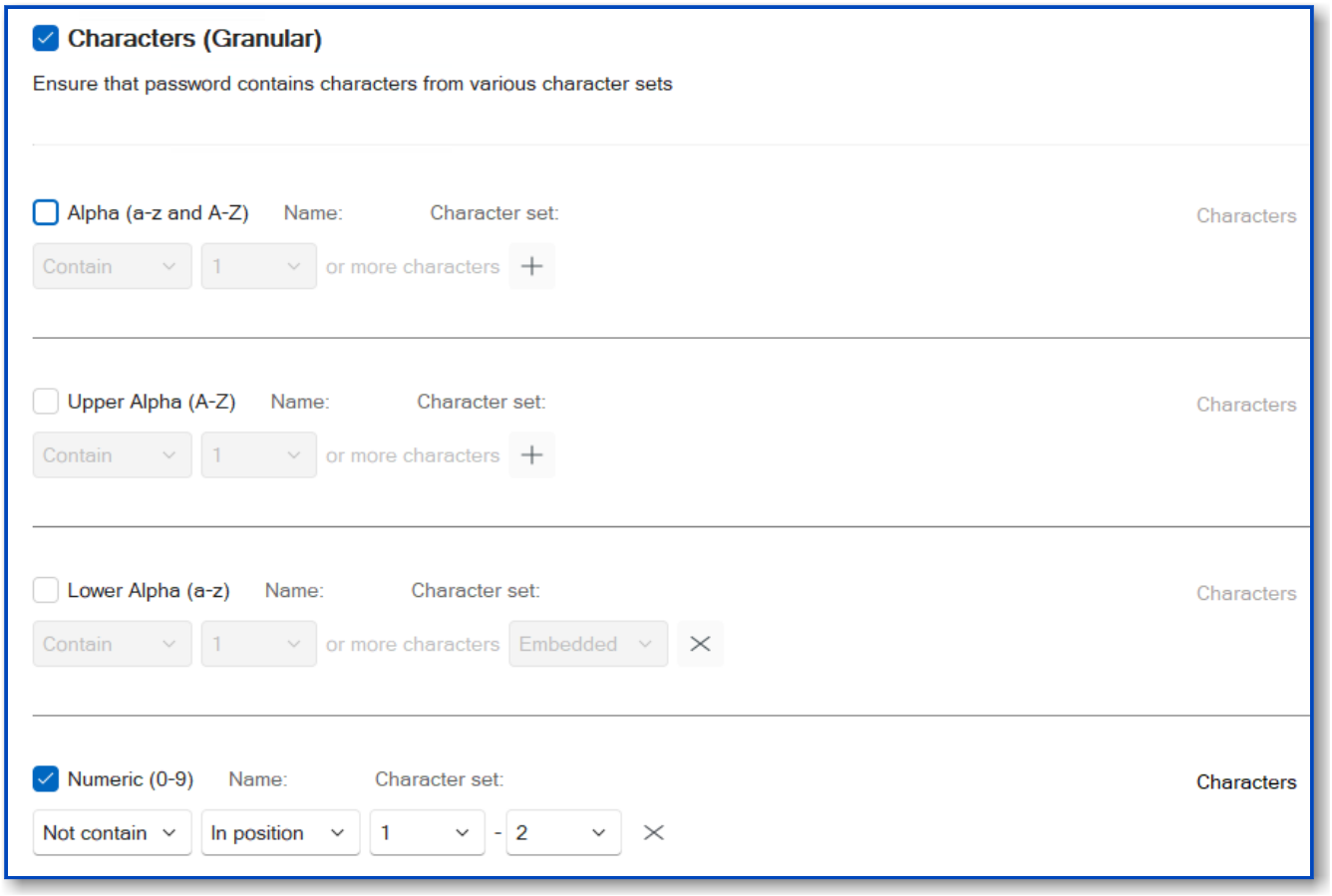
Character rules can be combined to enforce complex password requirements. For example, you may need to enforce a policy such as "passwords must contain a numeric character, but not in the first two positions" to ensure compatibility with some other system.

This is done by using two of the Character rules:

Set **Characters (Complexity)** to require 1 Numeric character.

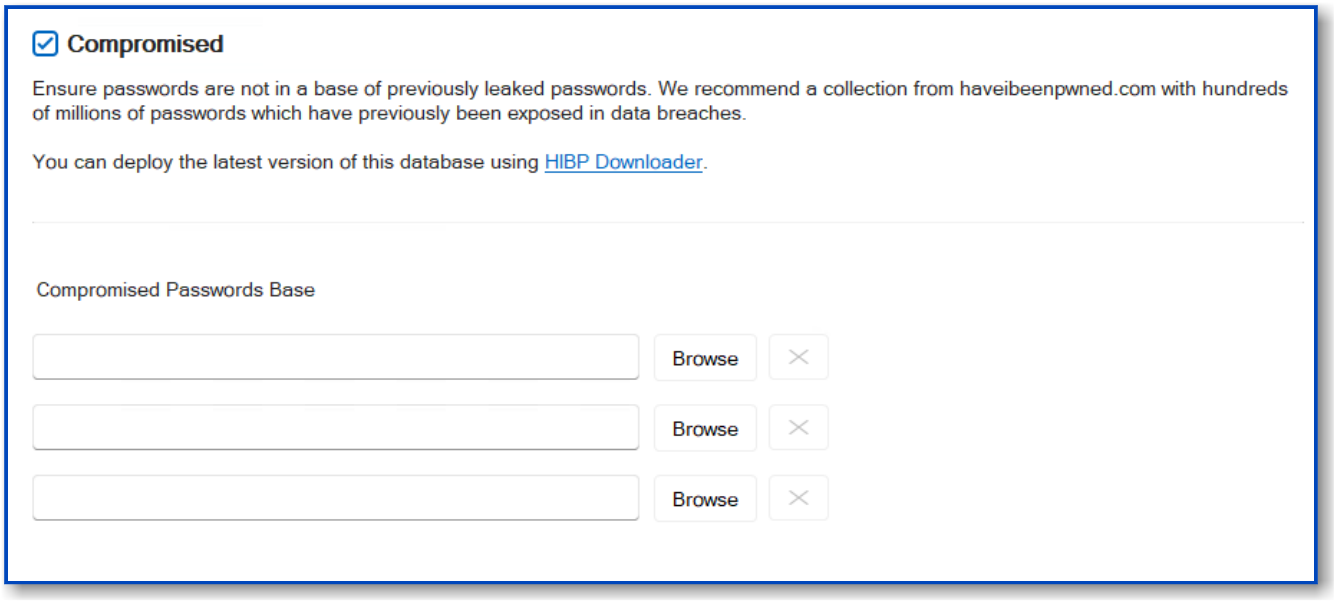


Set **Characters (Granular)** to not contain numeric values in the first two positions.



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

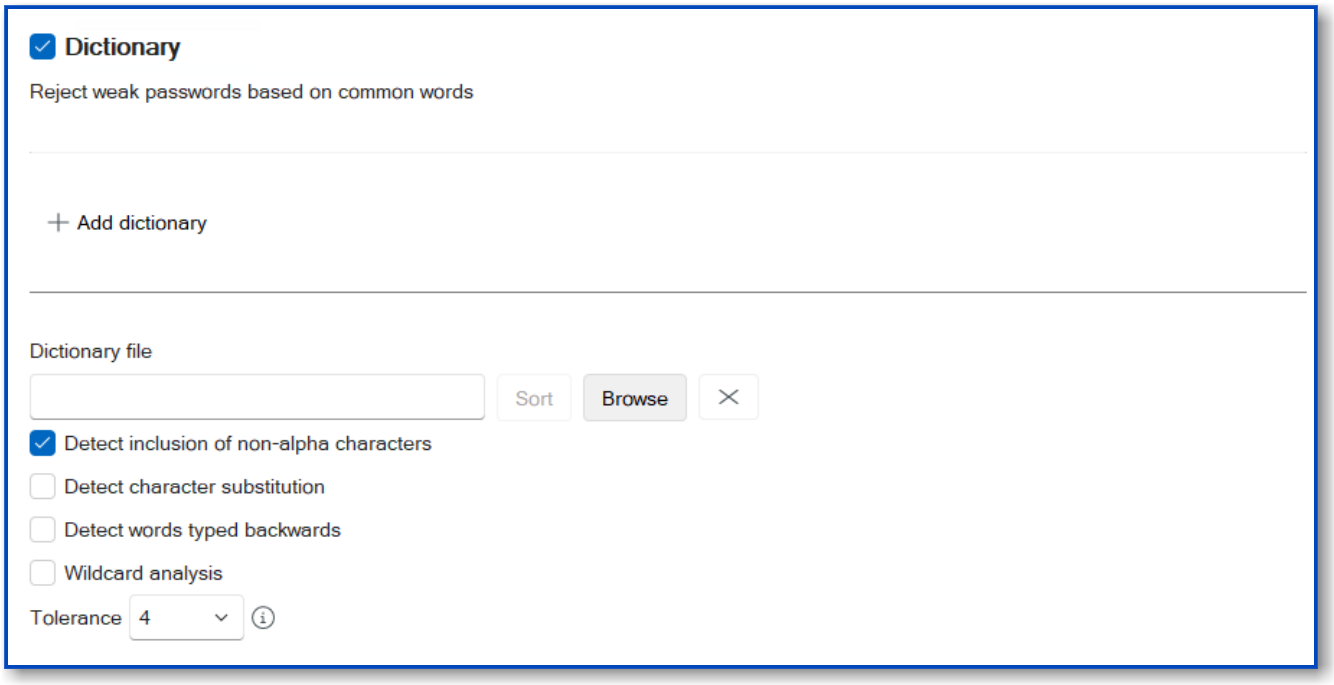
You can browse to your compromised passwords base files or type a path into the text box. The path can contain environment variables like

CAUTION: %SystemRoot%. hash files should only be read from a local disk. Using shared hash files degrades performance, and could jeopardize security.

See the HIBP Updater topic for the information about the Have I Been Pwnd (HIBP) database usage.

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

Browse to a dictionary file. A sample file **Dict.txt** is installed in the **\Program Files\Password Policy Enforcer** folder. This file is sorted and ready to use. It contains approximately 257,000 words, names, and acronyms.

Select the **Detect inclusion of non-alpha characters** check box if Password Policy Enforcer should remove all non-alphabetic characters during analysis. This allows Password Policy Enforcer to reject passwords such as "myp8asswor8d."

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

Select the **Detect words typed backwards** check box if Password Policy Enforcer 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 Password Policy Enforcer should search for wildcard templates in the dictionary file. Wildcard templates are specially formatted dictionary words that Password Policy Enforcer uses to reject a range of passwords. The Dictionary rule supports two wildcard template formats:

Format	Example	Description
Prefix	**!!BAN*!!**	**Rejects passwords that start with BAN.** **For example: band, banish, ban, bank, etc.**
	!!2*!!	**Rejects passwords that start with the numeric character 2.** **For example: 2ABC, 2123, etc.**
Suffix	!!*ING!!	Rejects passwords that end with ING. For example: pushing, howling, trying, etc.

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 Password Policy Enforcer 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 Password Policy Enforcer will tolerate before rejecting a password. For example, the dictionary word "**sword**", and the password "4my**sword**%" contain five consecutive matching characters (shown in bold type). Password Policy Enforcer 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.

NOTE: 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 Password Policy Enforcer configuration.

Click the **Sort** button if the dictionary file is being used with Password Policy Enforcer for the first time, or if words have been added to the file since it was last sorted. The Password Policy Enforcer management console will sort and reformat the file so that Password Policy Enforcer 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 Password Policy Client message if the password is rejected by both rules.

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 Password Policy Enforcer, and make sure that all computers have a local copy of the updated and sorted file.

The custom dictionary should meet the following requirements:

1. The dictionary should begin and end with a blank line.
2. All words are capitalized.
3. The sort button is pressed after pointing to a file in the dictionary rule.

NOTE: If you are using a custom dictionary, please provide a different filename. The default dictionary file (dict.txt) may be replaced during an upgrade.

Dictionary File Replication

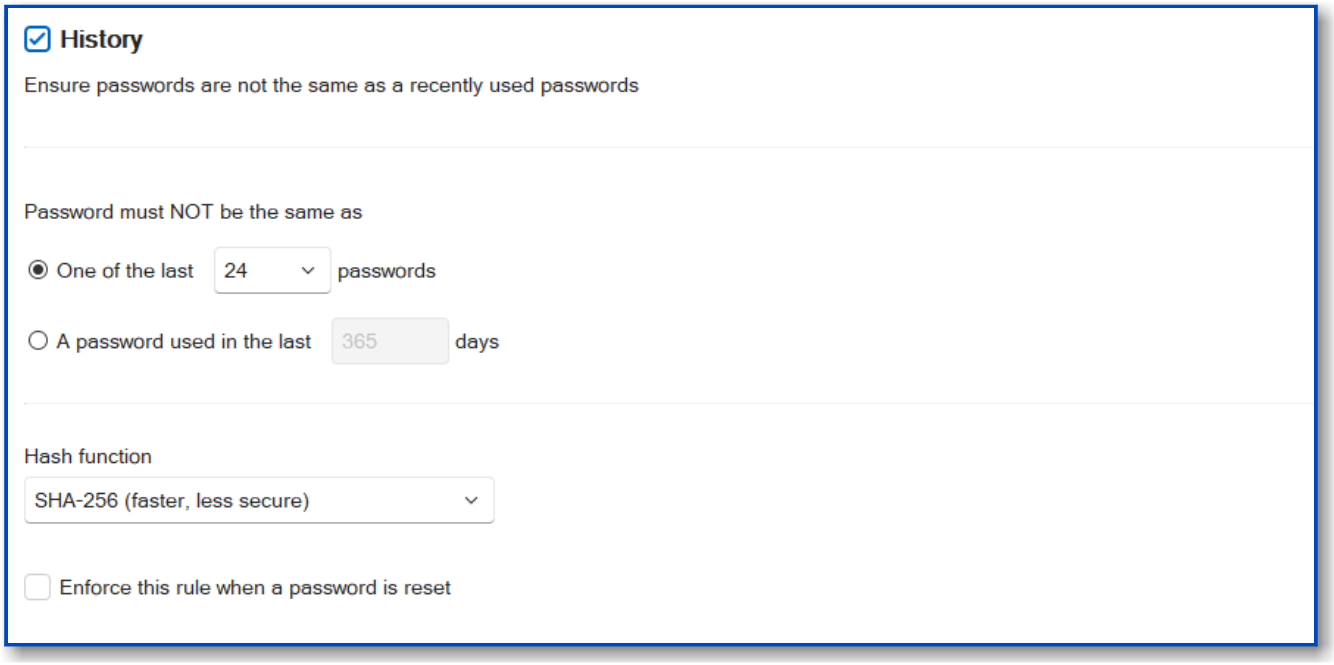
Password Policy Enforcer does not distribute dictionary file updates to other computers, but you can use the Windows Distributed File System to ensure that all domain controllers have the latest dictionary file. Copy the dictionary file into the Sysvol share on one domain controller, and the Distributed 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 Password Policy Enforcer to enforce

local polices. If you are using Password Policy Enforcer 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.

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. Password Policy Enforcer can stop users from reusing passwords for a specified number of password changes or a number of days.



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

Select one of the options:

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.

A 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.

NOTE: 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 Password Policy Enforcer 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.

NOTE: The History rule is not enforced when testing passwords from the Test Policies page.

Password Policy Enforcer updates a user's password history whenever their password changes. The password history is updated even if Password Policy Enforcer 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.

Password Policy Enforcer'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 Password Policy Enforcer to use an existing attribute.

Disable Password Policy Enforcer's History rule if you do not want Password Policy Enforcer to store the password history.

NOTE: Password Policy Enforcer 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 Password Policy Enforcer to store a password history, then leave the History rule disabled. You can use the Windows History rule together with Password Policy Enforcer's other rules to enforce your password policy.

Password Policy Enforcer 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 Password Policy Enforcer is configured to reject the last 24 passwords, then only the last 24 password hashes are stored. Reconfiguring Password Policy Enforcer 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 Password Policy Enforcer will then have 30 stored password hashes for each user.

Leave both the Windows and Password Policy Enforcer 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 Password Policy Enforcer 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. Password Policy Enforcer 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.

CAUTION: PASSWORD POLICY ENFORCER 's password history attribute is confidential to stop authenticated users from accessing the password history of other users. See the Microsoft Article Mark an attribute as confidential in Windows Server 2003 Service Pack 1 Microsoft article for additional information. 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.

Follow the steps below to create a new Active Directory attribute for the password history.

Step 1 – Log on to the server holding the Schema Operations Master role with an account that is a member of the Schema Admins group.

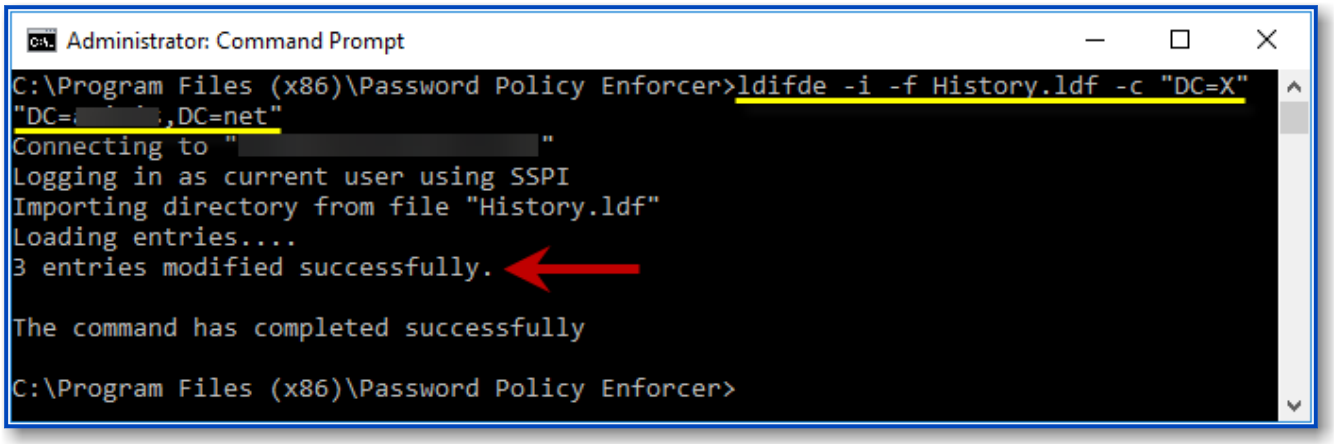
Step 2 – Open a Command Prompt window to the Password Policy Enforcer installation folder.

```
(\Program Files (x86)\Password Policy Enforcer\)
```

Step 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.
```

Step 4 – Press **ENTER** and check the output for errors.



Using an Existing Attribute for the Password History

Password Policy Enforcer 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. Contact Netwrix Support if you would like to use an existing attribute for the password history.

Password Histories for Local User Accounts

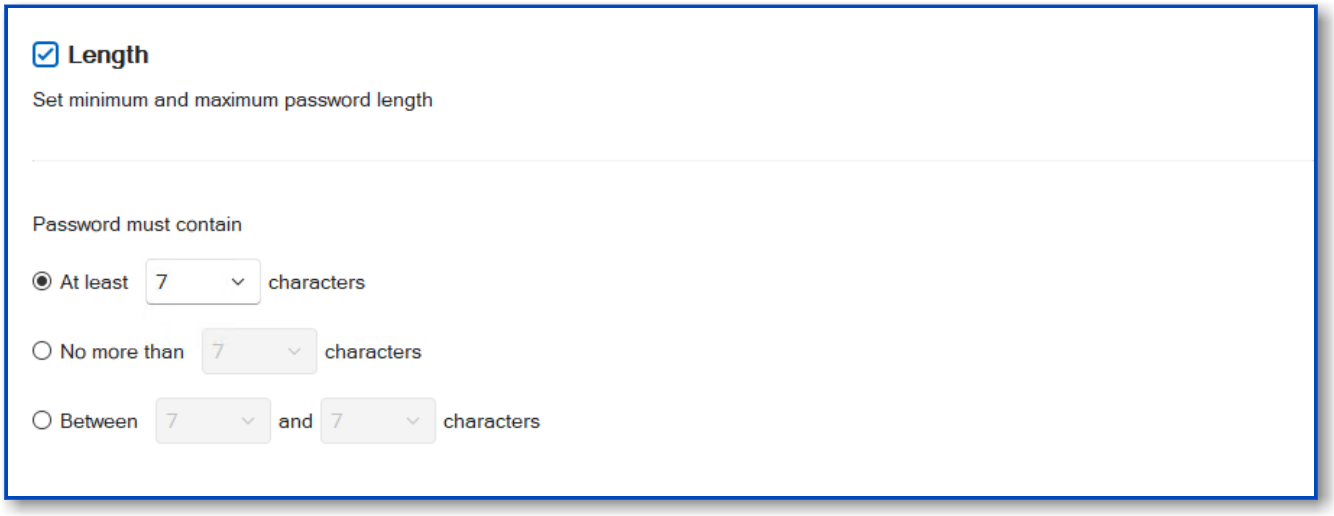
The password histories of local user accounts are stored in the HKLM\SECURITY\PPE Password History\ registry key. Users are not granted access the HKLM\SECURITY\ registry key by default, so a user cannot read the password history of any user (including themselves). This is also true for members of the 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.

CAUTION: 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.

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

Select one of the options:

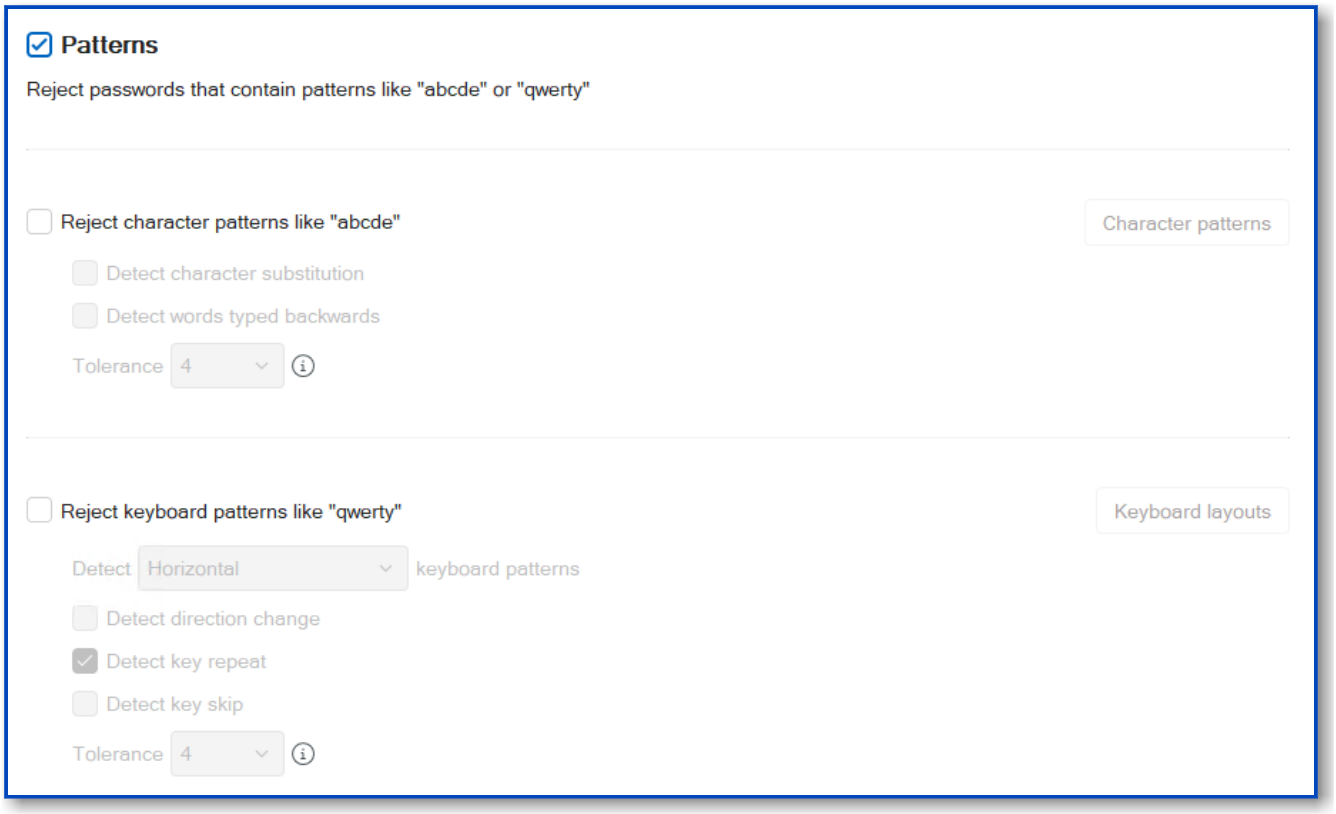
At least specifies the minimum number of characters that passwords must contain. Choose the minimum number of characters from the drop-down list.

No more than specifies the maximum number of characters that passwords can contain. Choose the maximum number of characters from the drop-down list.

Between specifies 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.

Patterns Rule

The Patterns rule rejects passwords that contain character patterns such as "abcde". Character patterns weaken the password.



Select the **Patterns** check box to enable the Patterns rule.

Select **Reject character patterns like "abcde"** to check for character patterns.

Select **Character patterns** to set the patterns to apply. Default is both **English alphabet (a-z)** and **Numbers (0-9)**.

Select **Detect character substitution** if Password Policy Enforcer should reject passwords that rely on character substitution to comply with this rule.

Select **Detect words typed backwards** if Password Policy Enforcer should additionally test passwords with their characters reversed. Enabling this 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 Password Policy Enforcer allows before rejecting a password. For example, the password "password**wxyz**" contains a four-character pattern (shown in bold type). Password Policy Enforcer rejects 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.

Select **Reject keyboard patterns like "qwerty"** to check for keyboard patterns.

Select **Keyboard layouts** to set the keyboard type. Default is **United States**.

Select the type of keyboard pattern: **Horizontal**, **Vertical** or **Horizontal and Vertical**.

Select **Detect direction change** for entries that change direction. For example, **qweewq**.

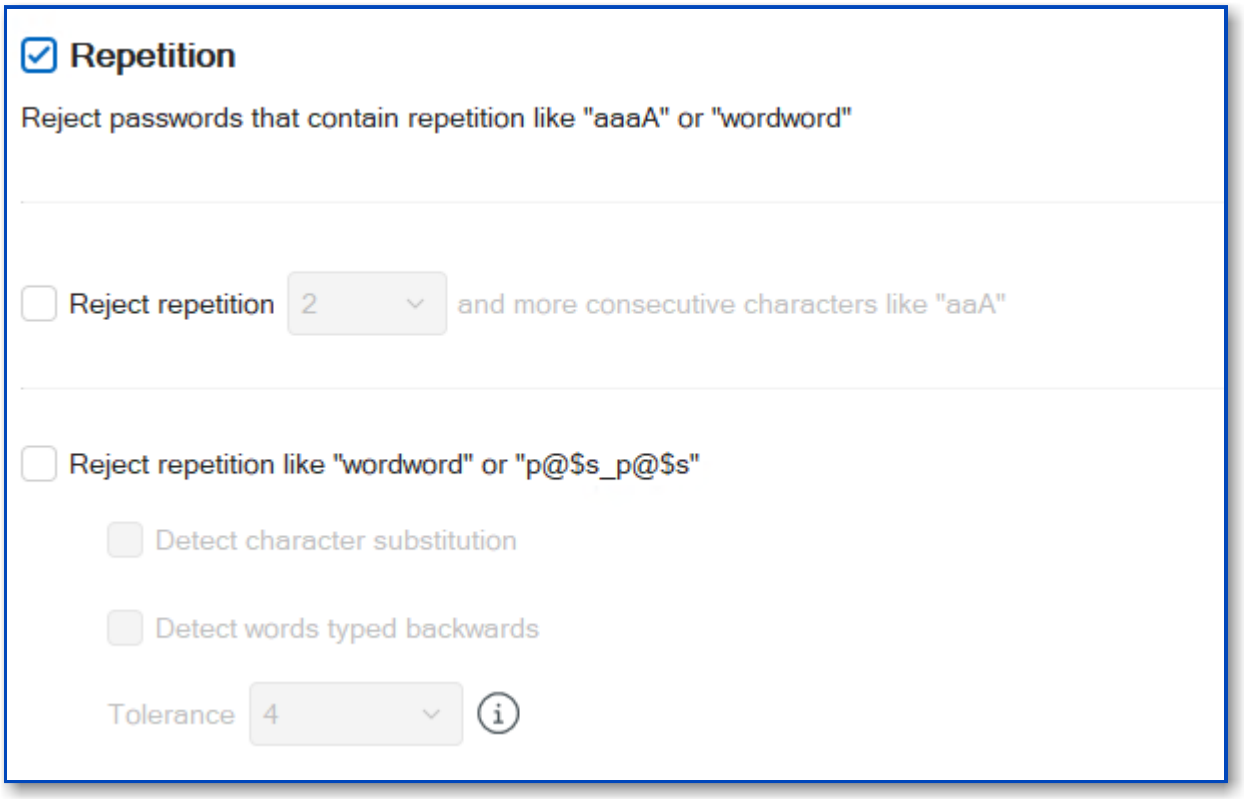
Select **Detect key repeat** for repeated keys, based on the **Tolerance** value. If Tolerance is 4, **aaaa** is accepted and **aaaaa** is rejected.

Select **Detect key skip** for skipped keys, such as **qetuo**.

Set **Tolerance** for the number of characters in a keyboard pattern is allowed before the password is rejected.

Repetition Rule

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



Select the **Repetition** check box to enable the repetition rule.

Select the **Reject repetition** option and set the maximum number of consecutive repeating characters that passwords can contain.

Select the **Reject repetition like "wordword" or "p@$s_p@$s"** option to enable pattern repetition.

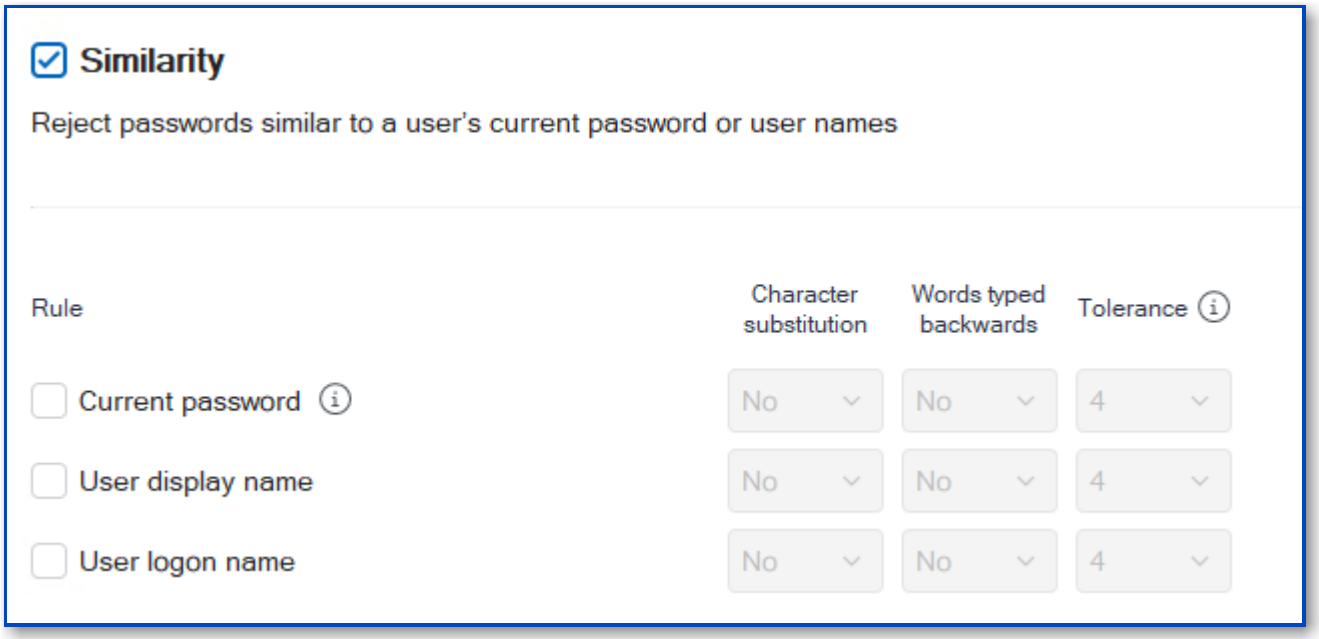
Select **Detect character substitution** if Password Policy Enforcer should reject passwords that rely on character substitution to comply with this rule.

Select **Detect words typed backwards** if Password Policy Enforcer should additionally test passwords with their characters reversed. Enabling this 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 Password Policy Enforcer allows before rejecting a password. For example, the password "password**wxyz**" contains a four-character pattern (shown in bold type). Password Policy Enforcer rejects 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.

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". Password serialization allows an attacker to guess the new password.



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

Select **Current password** to apply the similarity rules the user's existing password. The Password Policy Enforcer client must be installed on the user's machine to enforce this rule.

Select **User display name** to reject passwords that are similar to a user's Active Directory display name (full name for local accounts).

Select **User logon name** to reject passwords that are similar to a user's logon name (user name).

For each option enabled, set the rules:

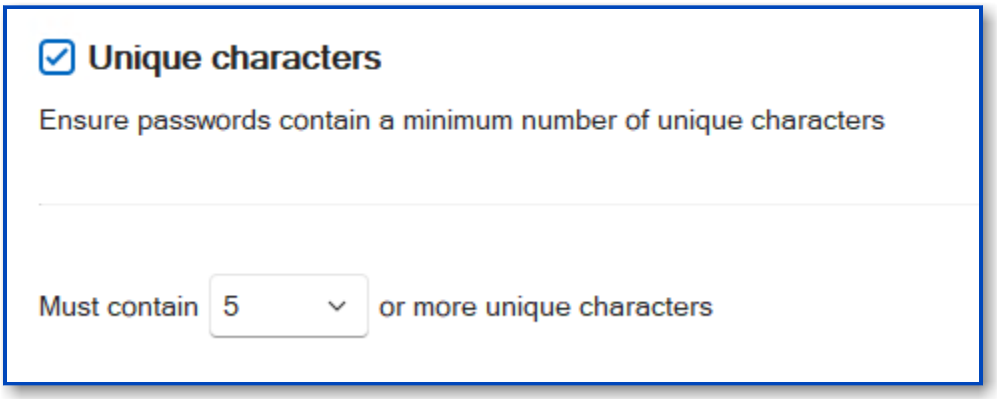
Set **Character substitution** to **Yes** to reject passwords that rely on character substitution to comply with this rule.

Set **Words typed backward** to **Yes** to 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".

Set a **Tolerance** value to specify the maximum number of matching characters that Password Policy Enforcer allows before rejecting a password. For example, the two passwords "old**passwd**" and "new**passwd**" contain six consecutive matching characters (shown in bold type). Password Policy Enforcer rejects the new password if the tolerance is five (or lower), and accepts it if the tolerance is six (or higher).

Unique Characters Rule

The Unique Characters rule rejects passwords that do not contain a minimum number of unique characters. For example, the password "aaaaaaaa" only contains one unique character (a), whereas "mypassword" contains nine unique characters (mypasword). Increasing the number of unique characters in a password increases 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 **Unique characters** check box to enable the Unique Characters rule.

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

Assign Policies to Users & Groups

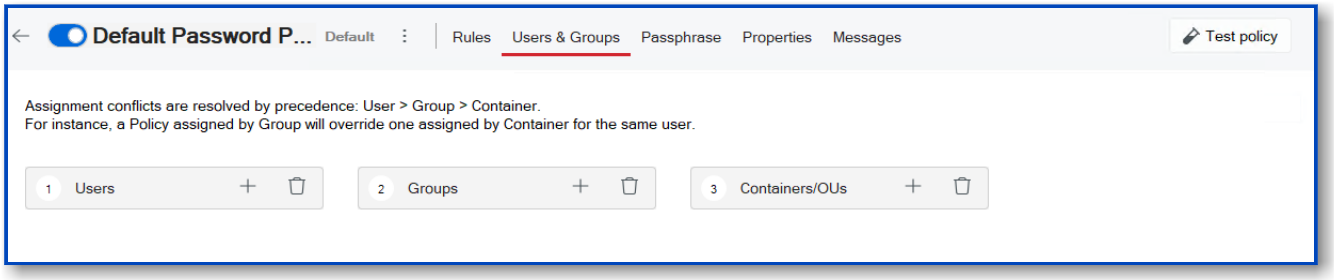
Password Policy Enforcer uses policy assignments to decide which policy to enforce for each user. Domain policies can be assigned to users, groups, and containers (Organizational Units). Local policies can only be assigned to users. See the Domain and Local Policies topic for additional information.

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

Step 2 – Click on a policy name to open the policy configuration page.

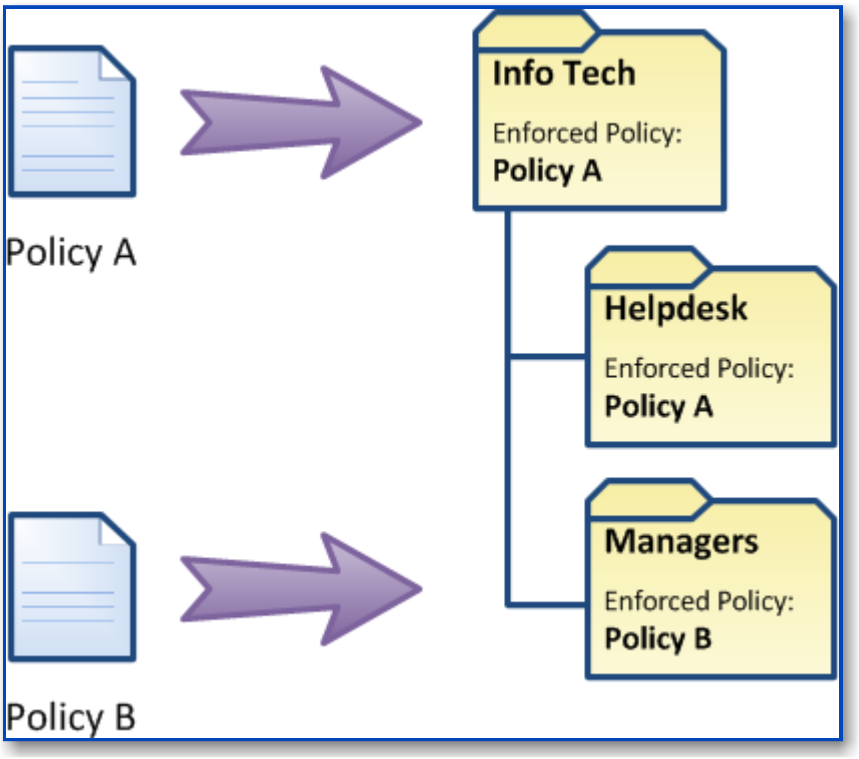
Step 3 – Open the **Users & Groups** tab.



When a domain policy is assigned to a user or group, Password Policy Enforcer 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, Password Policy Enforcer stores the username in the configuration. The assignment is invalidated if the user is renamed.

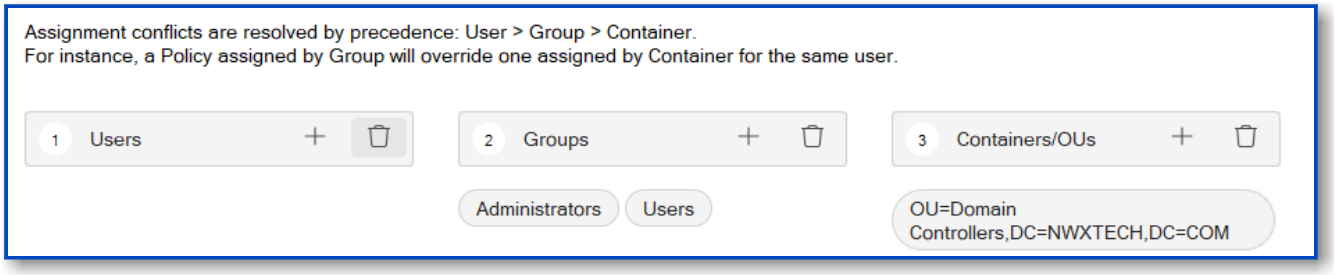
When a policy is assigned to a group, Password Policy Enforcer enforces the policy for all members of the group as well as any nested groups. For example, if the Helpdesk group is a member of the Info Tech group, then any policy assigned to the Info Tech group also applies to the members of the Helpdesk 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, Password Policy Enforcer 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.



NOTE: 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.

As you assign users and groups to the policy, they are displayed on the page.



To remove a policy assignment:

Step 1 – Select the user, group or container. For example, **Administrators** under **Groups**.

Step 2 – Click the trash can icon in the appropriate header. For example, **Groups**.

Policy Assignment Conflicts

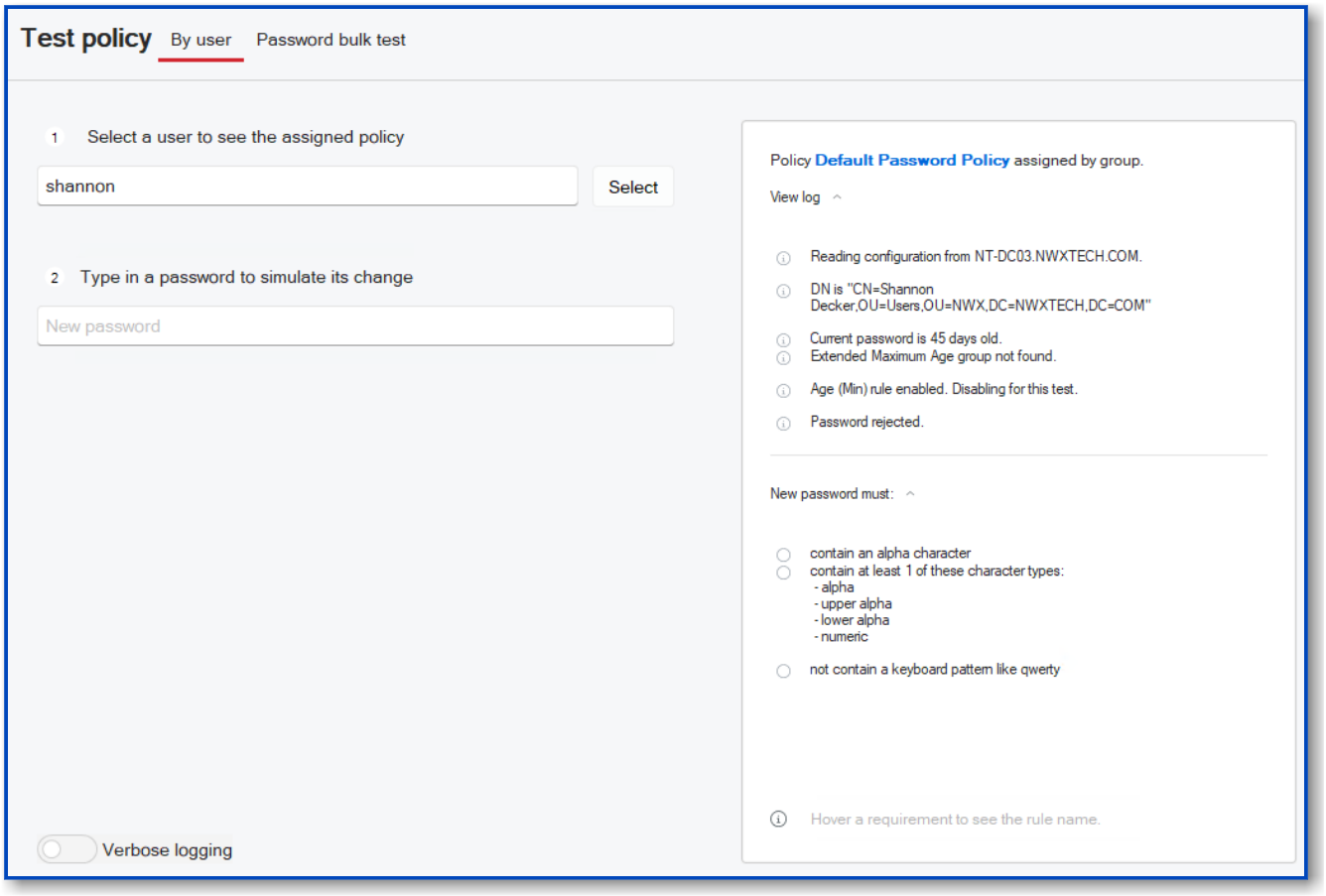
A policy assignment conflict occurs when more than one policy is assigned to a user. Password Policy Enforcer can resolve these conflicts and choose one policy for each user.

Password Policy Enforcer 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 Password Policy Enforcer enforces Policy A because assignments by group take precedence over assignments by container.

If all the policies are assigned to the user by container, then Password Policy Enforcer 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 Password Policy Enforcer enforces 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 Password Policy Enforcer checks the priority of each remaining policy, and enforces the policy with the highest priority. See the Policy Selection Flowchart topic for a diagrammatic representation of this algorithm.

Click **Test Policy** and expand the **View log** to see which policy Password Policy Enforcer enforces for a particular user.



Passphrase

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.

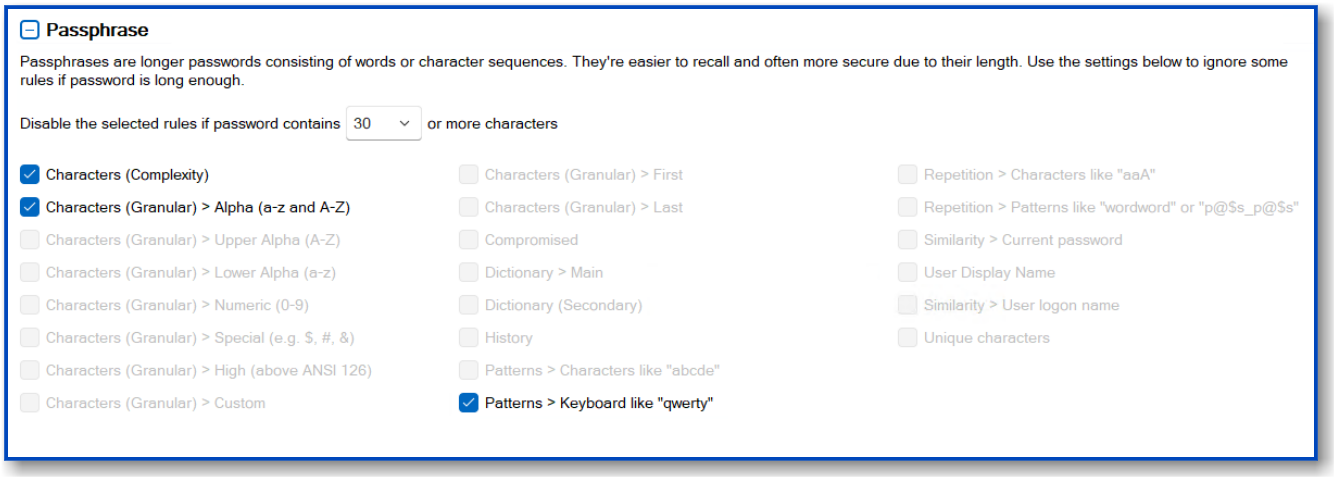
Complexity and dictionary rules are less important for passphrases as passphrases rely primarily on length for security. You may want to relax some password policy requirements for passphrases.

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

Step 2 – Click on a policy name to open the policy configuration page.

Step 3 – Open the **Passphrase** tab.



Step 4 – Select the number of characters the password must contain before the selected rules are disabled.

Step 5 – Select the rules to be disabled.

Disabled rules are not counted when calculating the compliance level, but Password Policy Enforcer 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 Password Policy Enforcer is configured to disable one or more rules for passphrases.

NOTE: Opinions 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 makes up for the reduced complexity.

Policy Properties

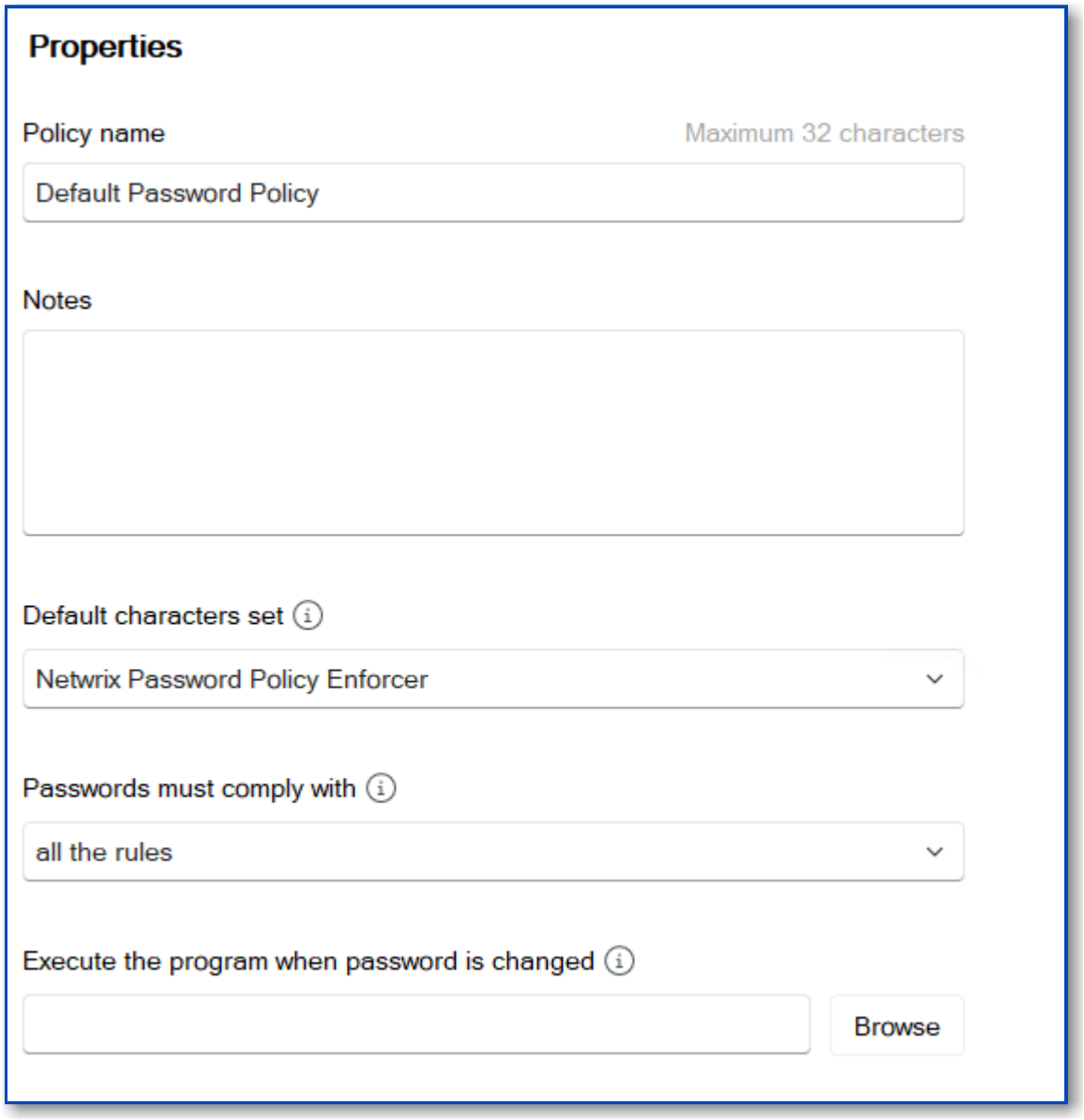
Sets the properties for the selected policy.

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

Step 2 – Click on a policy name to open the policy configuration page.

Step 3 – Open the **Properties** tab.



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

Enter any **Notes** about the policy

Select the **Default characters set**. The default value (Netwrix Password Policy Enforcer) requires users to comply with rules that use the Password Policy Enforcer character set. Choose the alternate option (Windows) to have users comply with rules that use the Windows character set.

NOTE: Only Password Policy Enforcer 10.0 and higher contain the Windows character set. Password Policy Enforcer 9, Netwrix Password Reset and Password Policy Enforcer/Web 7 (and older for all products) always use the Password Policy Enforcer character set.

- Some languages such as Japanese do not distinguish between uppercase and lowercase. These characters are in the Windows Alpha set, but not in the Upper or Lower sets.
- Characters classified as a space, punctuation, control or blank by Windows are included in the Special character set. If these characters are also included in some other set by Windows (for example, a superscript one is both a decimal digit and punctuation), then Password Policy Enforcer only includes them in the Special character set when the Windows character set is selected.
- When using the Password Policy Enforcer character set, all characters above ANSI 126 are included in the High set. When using the Windows character set, a character is only included in the High set if it is above ANSI 126 and not included in any other set by Windows.

Select the number of rules for **Passwords must comply with** from the drop-down list to specifiy 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 Password Policy Enforcer should enforce a more lenient password policy. The Minimum Age and Maximum Age rules are excluded from compliance level calculations. See the Rules topic for additional information.

When setting the compliance level, consider that some rules may be disabled when a user enters a passphrase. See the Passphrase topic for additional information. Password Policy Enforcer 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 Password Policy Enforcer is configured to disable one or more rules for passphrases.

Password Policy Enforcer 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 the program when password is changed** text box. The path can contain environment variables like `%SystemRoot%`. Every computer running Password Policy Enforcer 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, Password Policy Enforcer records each user's logon name and new password in a text file named **passwords.txt**:

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

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

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

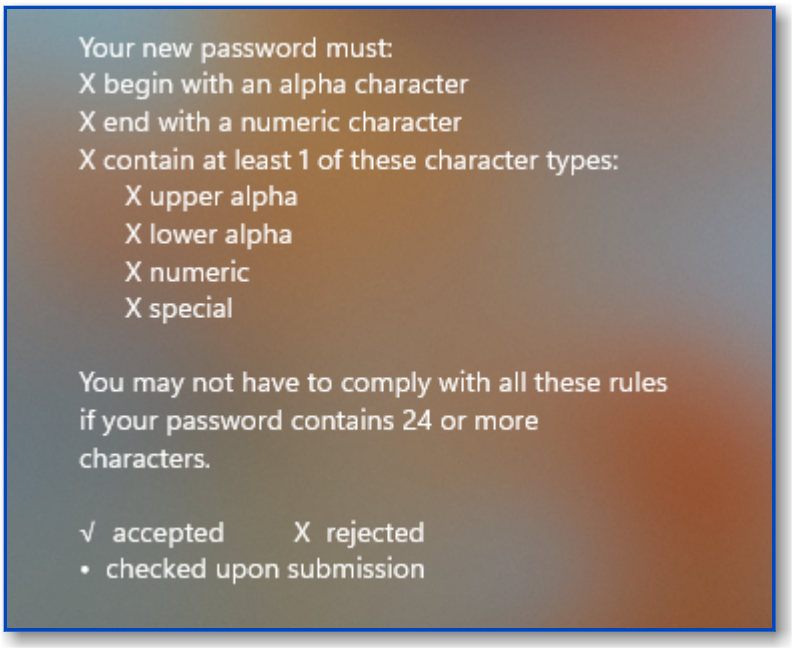
The command can now include the [USERNAME] and [PASSWORD] macros. If neither is specified, then the command is executed with both parameters to maintain compatibility with existing programs/scripts.

RECOMMENDED: Use the [USERNAME] parameter if the password is not needed by the program/script so that the password is not unnecessarily sent to the change notification command/script.

Messages

Each Password Policy Enforcer password policy has multiple message templates, one for each of the Password Policy Client messages.

- Password Policy – Displays the password policy guidelines on clients that have the Netwrix Password Policy Enforcer Client installed.
- [POLICY] – Customize the text for the active rules.
- [LIVE_POLICY] – Password Policy Client (10.2 and above) messages can be configured to display live feedback for the active rules to users as they enter their passwords. This feature enables users to see if their passwords meet the requirements of the policy set by the organization. Here is an example of a live policy message.



NOTE: Start each custom message with two spaces, a hypen, and a space before your message so the X and checks can appear for the rule. For example: " **- Include an upper case alpha character.**" The quotes are only there to illustrate the message.

- Rejection Reason – Displays why an intended password was rejected on clients that have the Netwrix Password Policy Enforcer Client installed

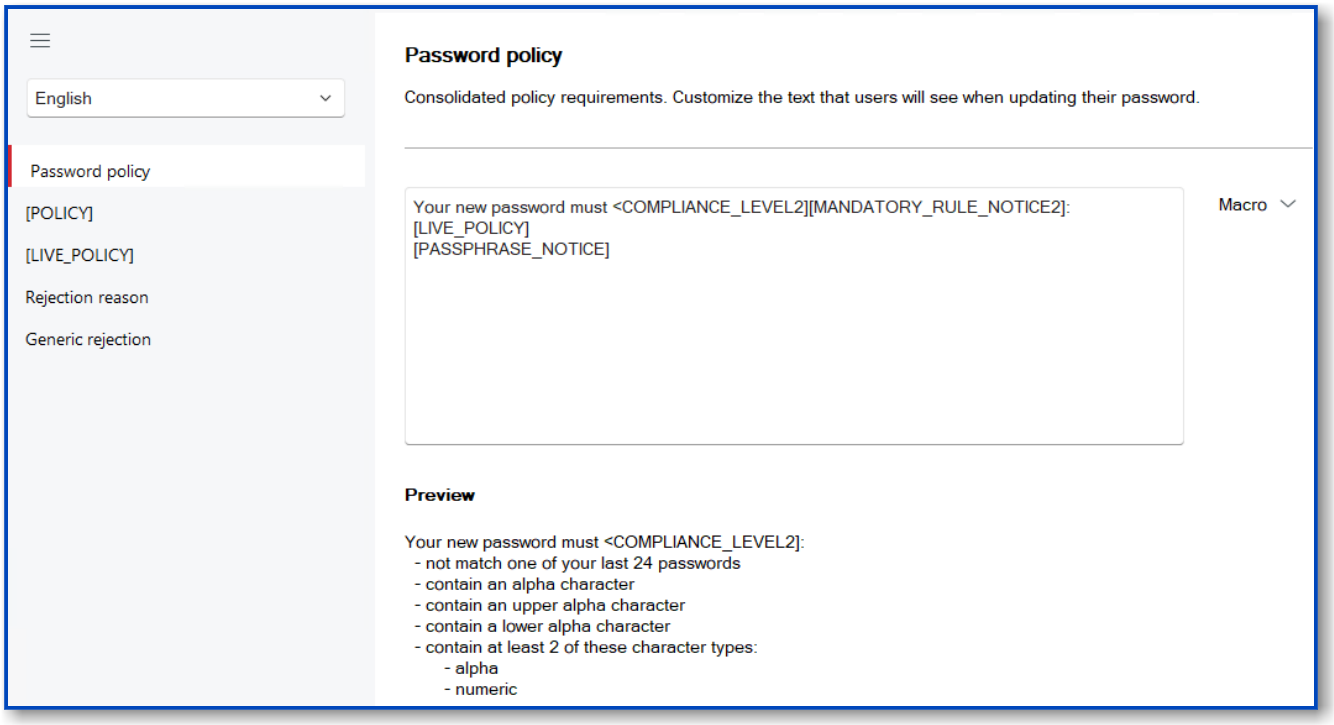
- Generic Rejection – Displays if Password Policy Enforcer does not have a specific reason for the rejection, generally because the password does not comply with the Windows password policy

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

Step 2 – Click on a policy name to open the policy configuration page.

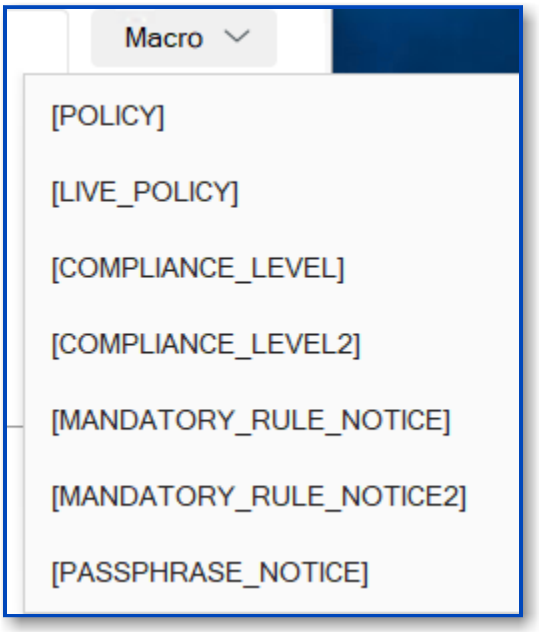
Step 3 – Open the **Messages** tab.



Step 4 – Select the message language from the drop-down list. You can set messages for multiple languages. You do not have to create a Password Policy Enforcer policy for each language. To set multiple languages, pick one, edit the message templates. Select another language, and edit the message templates. Repeat for each language you want to implement. The correct message is displayed to users based on their selected language.

Step 5 – Edit the message templates in the Password policy, [POLICY], [LIVE_POLICY], Rejection Reason, and Generic rejection messages for any of the components you want to use.

Step 6 – Insert the macros into your message. Click **Macro** and pick one to insert it.



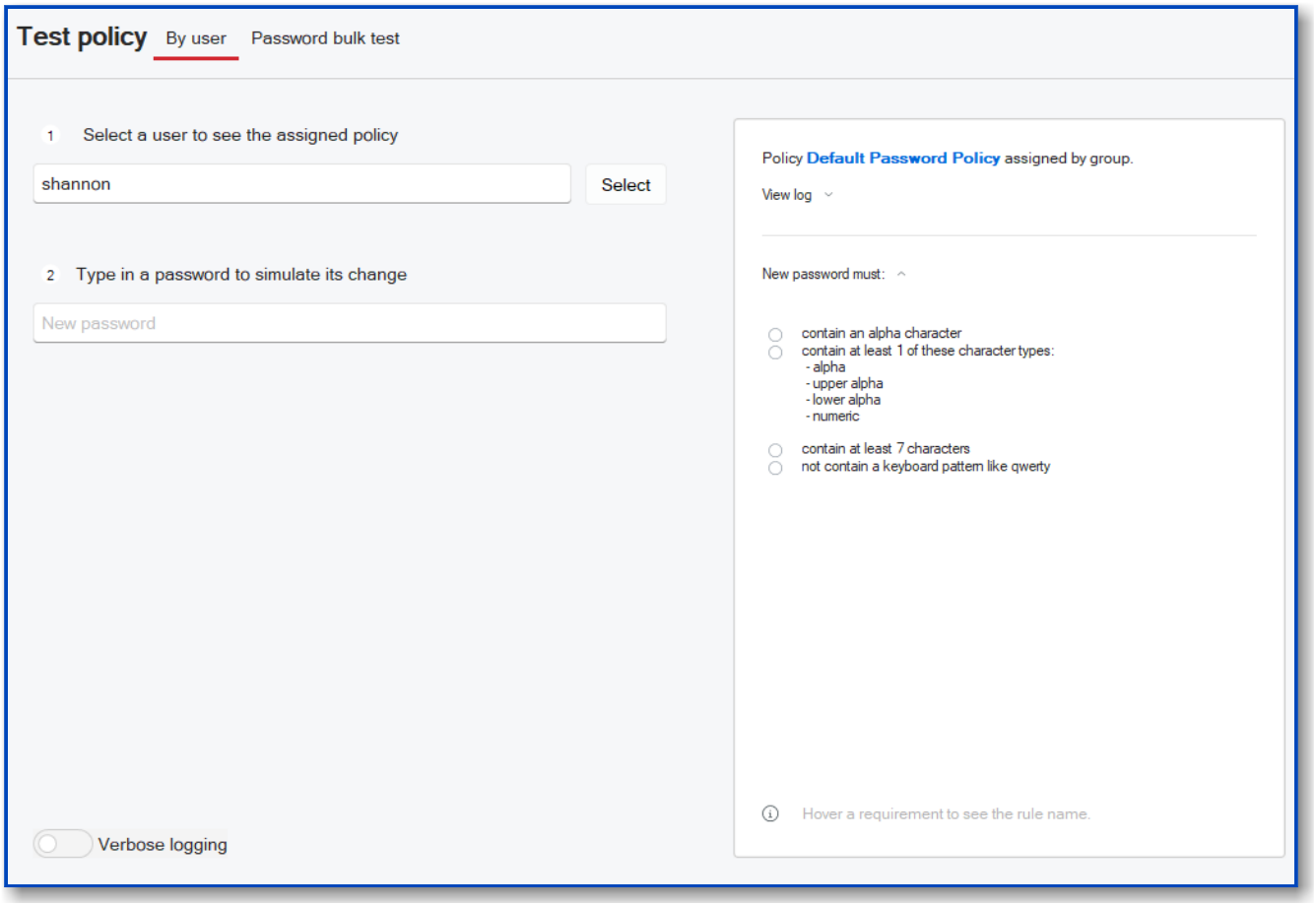
Step 7 – Click **Save** and review your changes in the Preview area. Click **Save** f you edit the message.

NOTE: If you do not see the **Preview**, contact your network administrator to set up the firewall to allow Password Policy Enforcer to communicate.

Test Policy

You can quickly test your Password Policy Enforcer configuration by simulating a password change. Click **Test Policy** from the Configuration Console dashboard or when you are setting up a policy. Test policy opens in a separate window. Remember to **Save** your rules and changes prior to testing.

Test policy opens on the **By user** tab.



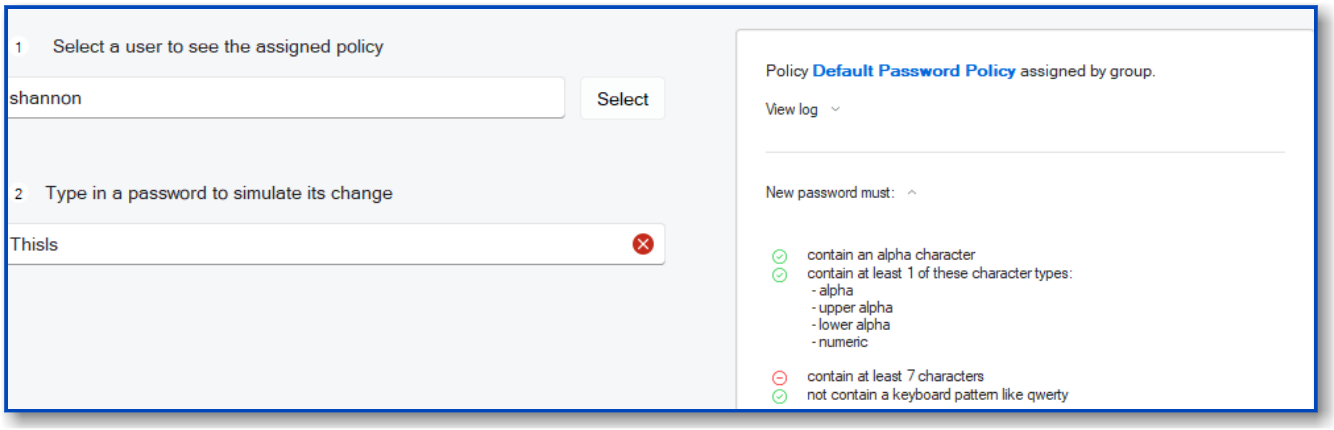
By User

Policy testing simulates a password change, but it does not change the password.

Step 1 – Click **Test policy** from the Configuration Console dashboard or when you are setting up a policy.

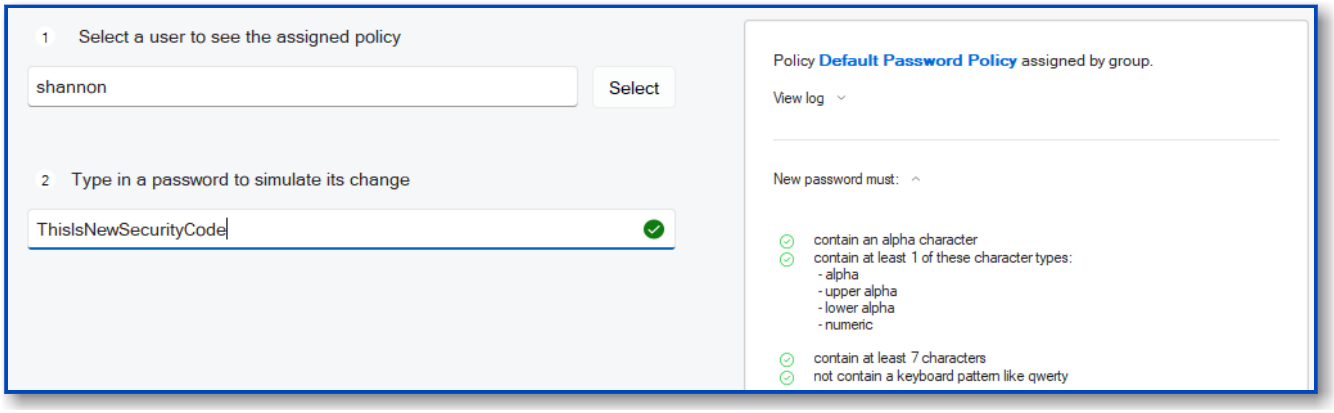
Step 2 – Select a **user**.

Step 3 – Type in a password to simulate its change. As you type, the new password is evaluated and the results are displayed.



The entered password is failing in this example, due to not meeting the length requirement. There is a red x indicating the failure. You can hover over the requirements to see the rule name.

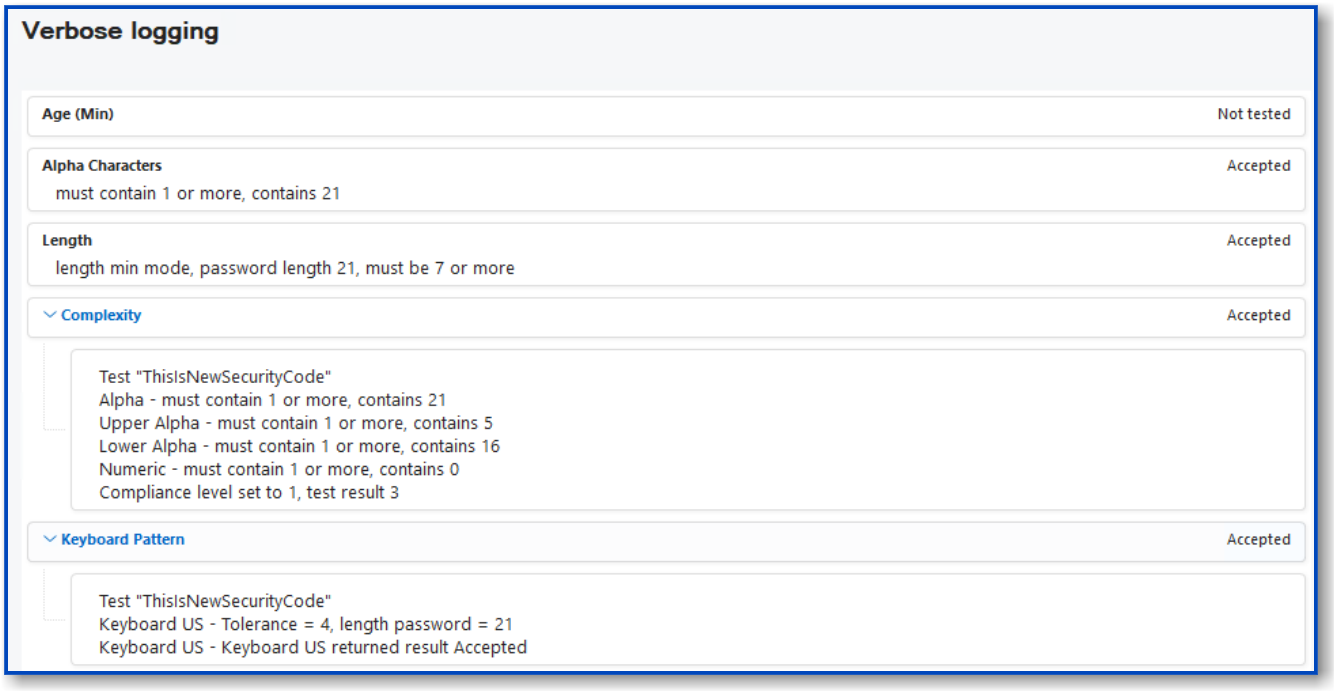
In this example, the password passes. Notice the green check beside the entered password.



Expand the **View log** for details:

- 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.

Turn on **Verbose Logging** to view the performed tests and results.

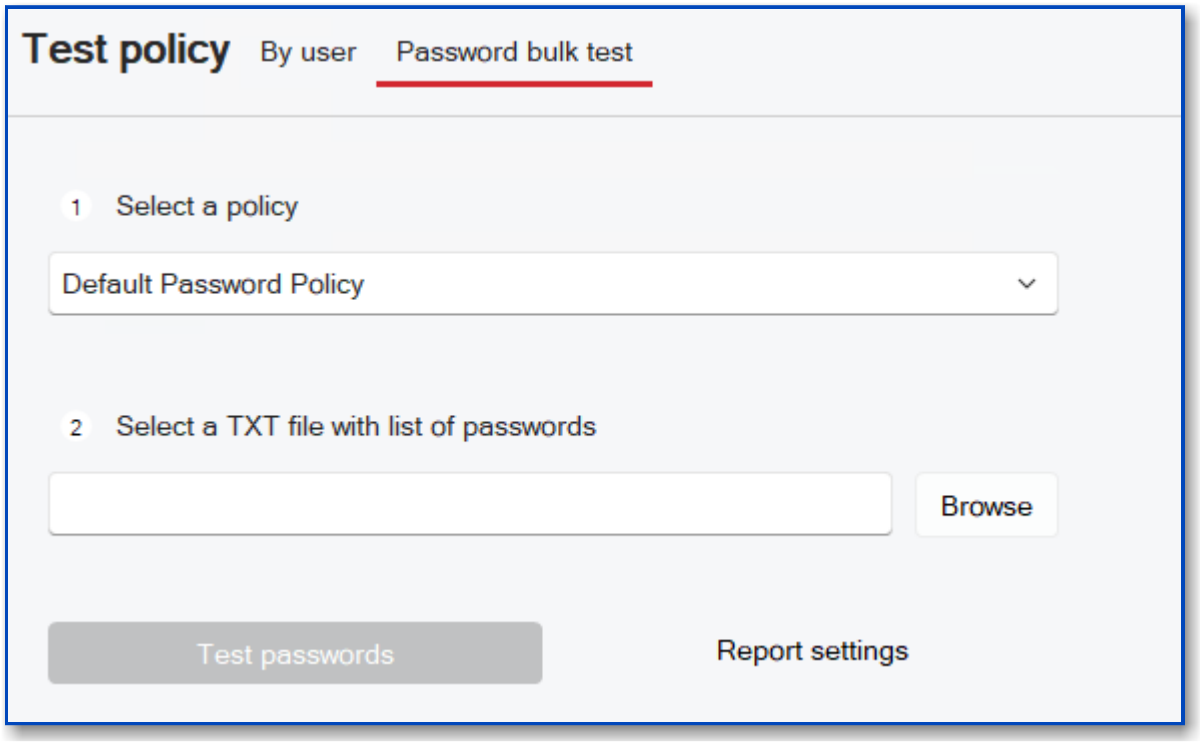


Bulk Password Test

Bulk Password Test feature allows to check a large number of passwords against a selected policy and a get a report of the accepted and rejected passwords.

Step 1 – Click **Test policy** from the Configuration Console dashboard or when you are setting up a policy.

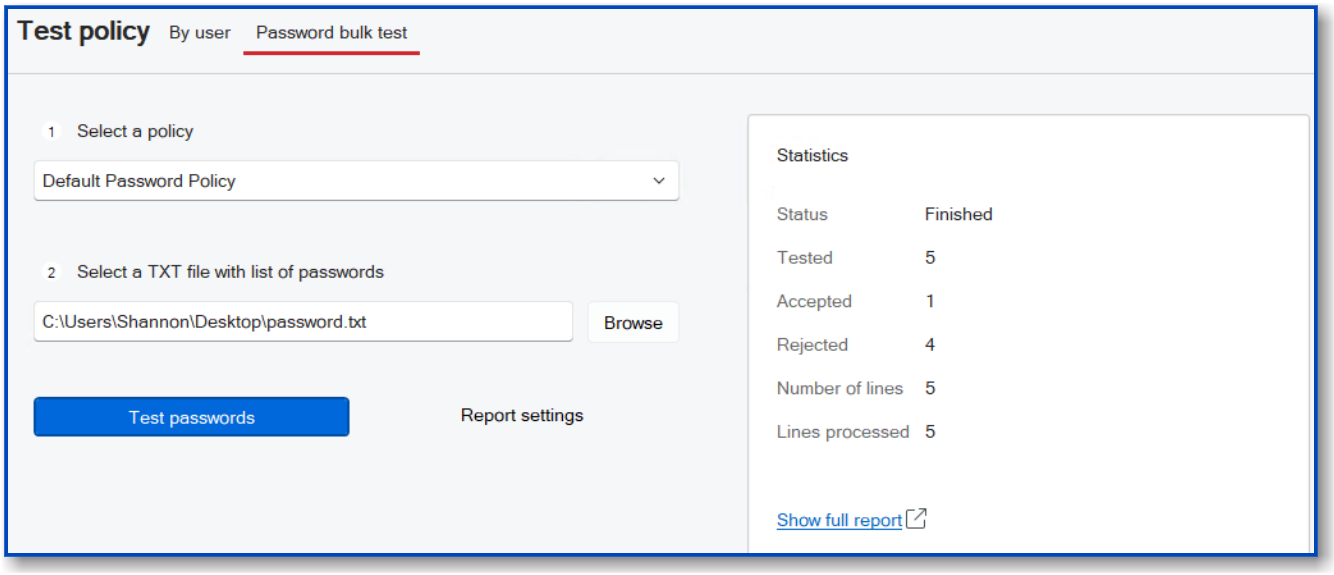
Step 2 – Open the **Password bulk test** tab.



Step 3 – Select a policy for the test.

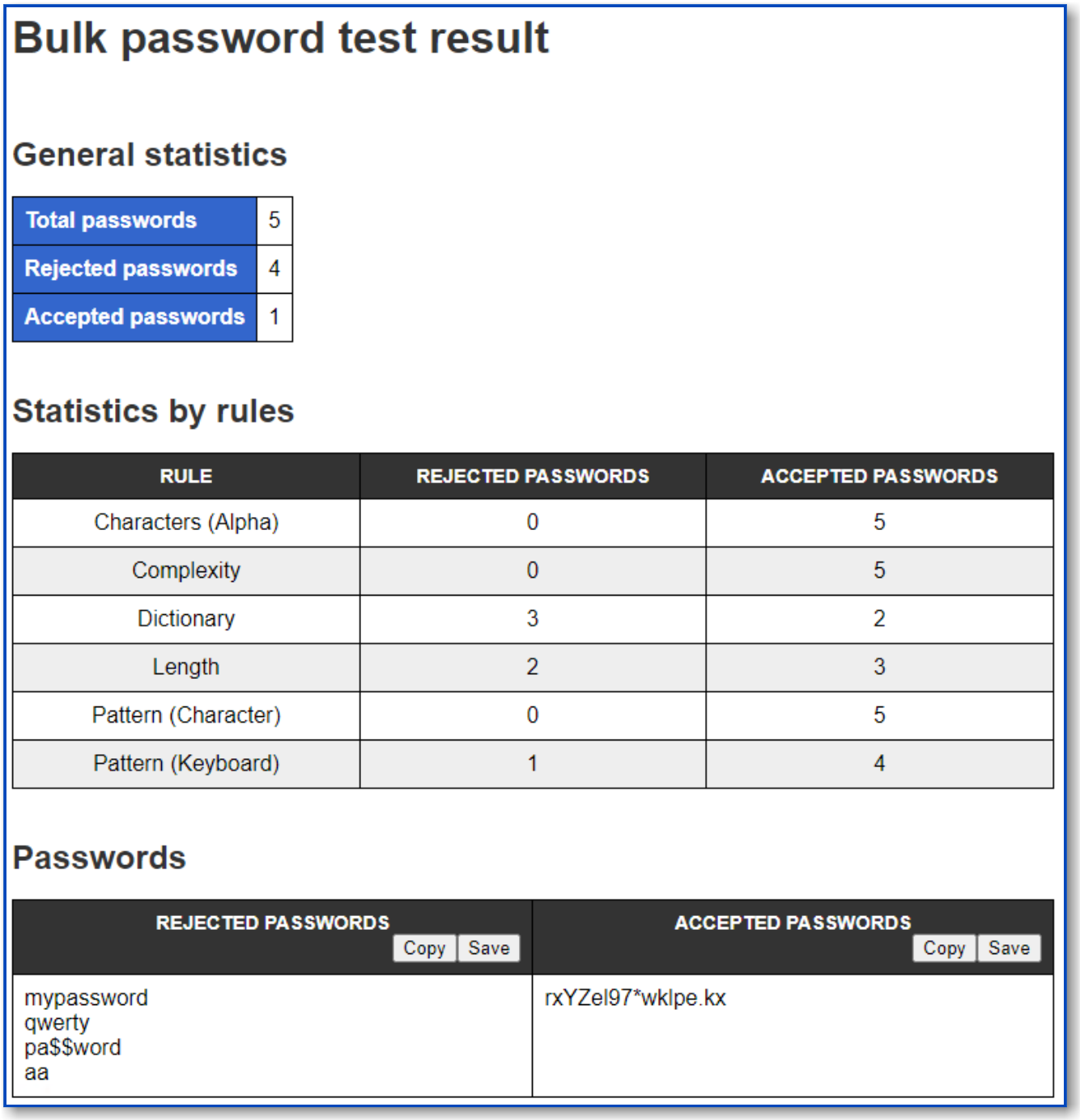
Step 4 – Browse to the text file containing the passwords to test. Processing is faster if the file is not on a shared drive.

Step 5 – Click **Test passwords**. The **Statistics** are displayed.



Statistics of the Bulk Password Testing	
Status	Shows whether the operation is ready for scanning, processing, terminated, or finished.
Tested	Number of tested passwords.
Accepted	Number of accepted passwords.
Rejected	Number of rejected passwords.
Number of lines	Number of lines within the file.
Lines processed	Shows the number of the processed lines.

Click **Show full report** to view the test details.



Bulk password test result

General statistics

Total passwords	5
Rejected passwords	4
Accepted passwords	1

Statistics by rules

RULE	REJECTED PASSWORDS	ACCEPTED PASSWORDS
Characters (Alpha)	0	5
Complexity	0	5
Dictionary	3	2
Length	2	3
Pattern (Character)	0	5
Pattern (Keyboard)	1	4

Passwords

REJECTED PASSWORDS Copy Save	ACCEPTED PASSWORDS Copy Save
mypassword qwerty pa$$word aa	rxYZel97*wklpe.kx

You can use the **Report settings** to customize the report:

- Result report folder. Processing is faster if this is not a shared drive.
- Show accepted passwords
- Show rejected passwords

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 Password Policy Enforcer 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 Password Policy Enforcer or the assigned policy is disabled. This allows you to test your configuration before enabling Password Policy Enforcer, 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 Password Policy Enforcer configuration was modified recently, then Active Directory may still be propagating the new configuration to the other domain controllers.

Compromised Password Check

The Compromised Password Checker finds compromised passwords. Users can be notified via email and advised or forced to change their password. The check can be scheduled to check existing passwords against a compromised hash list at any time.

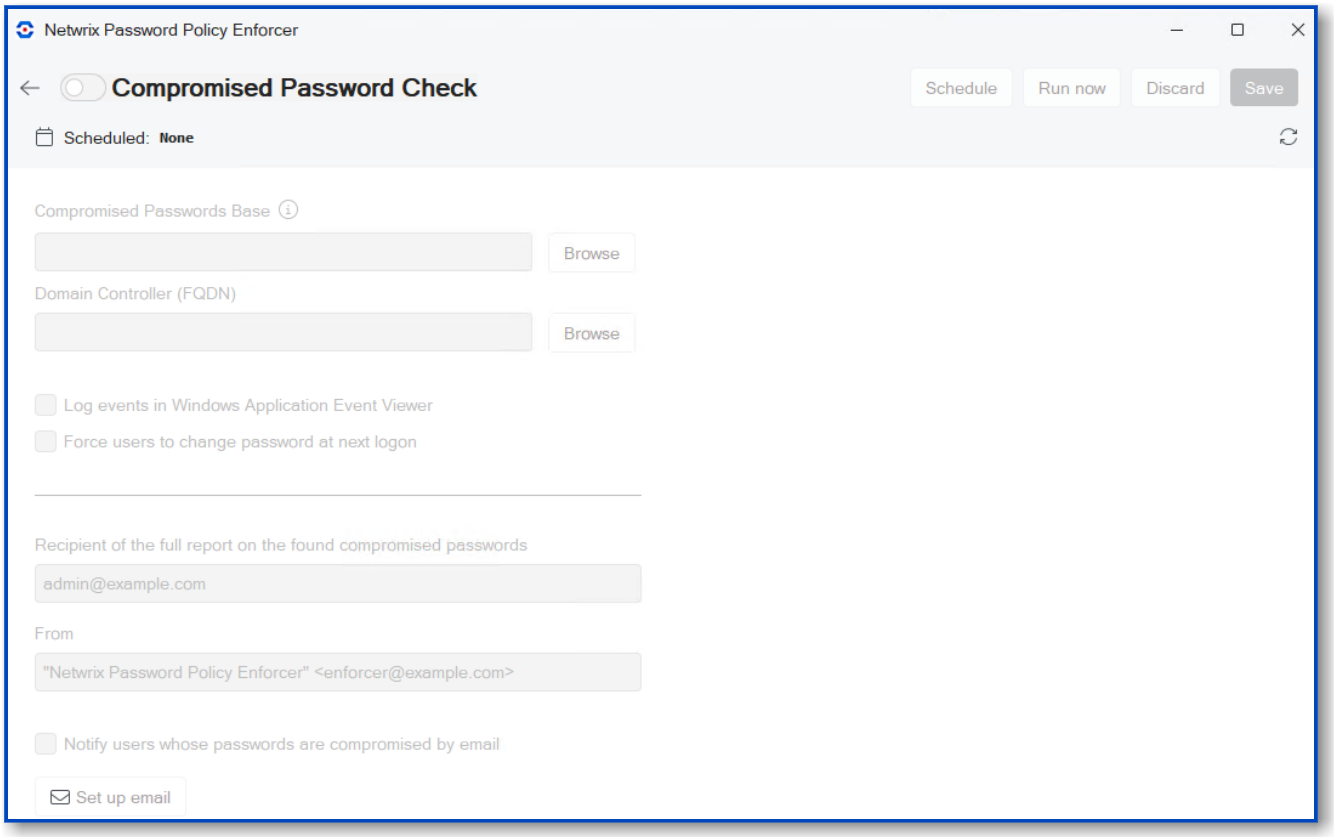
NOTE: Create the **Compromised Passwords Base** file prior to enabling the Compromised Password Check. See the HIBP Updater topic for instructions.

The Compromised Password Checker is launched from the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

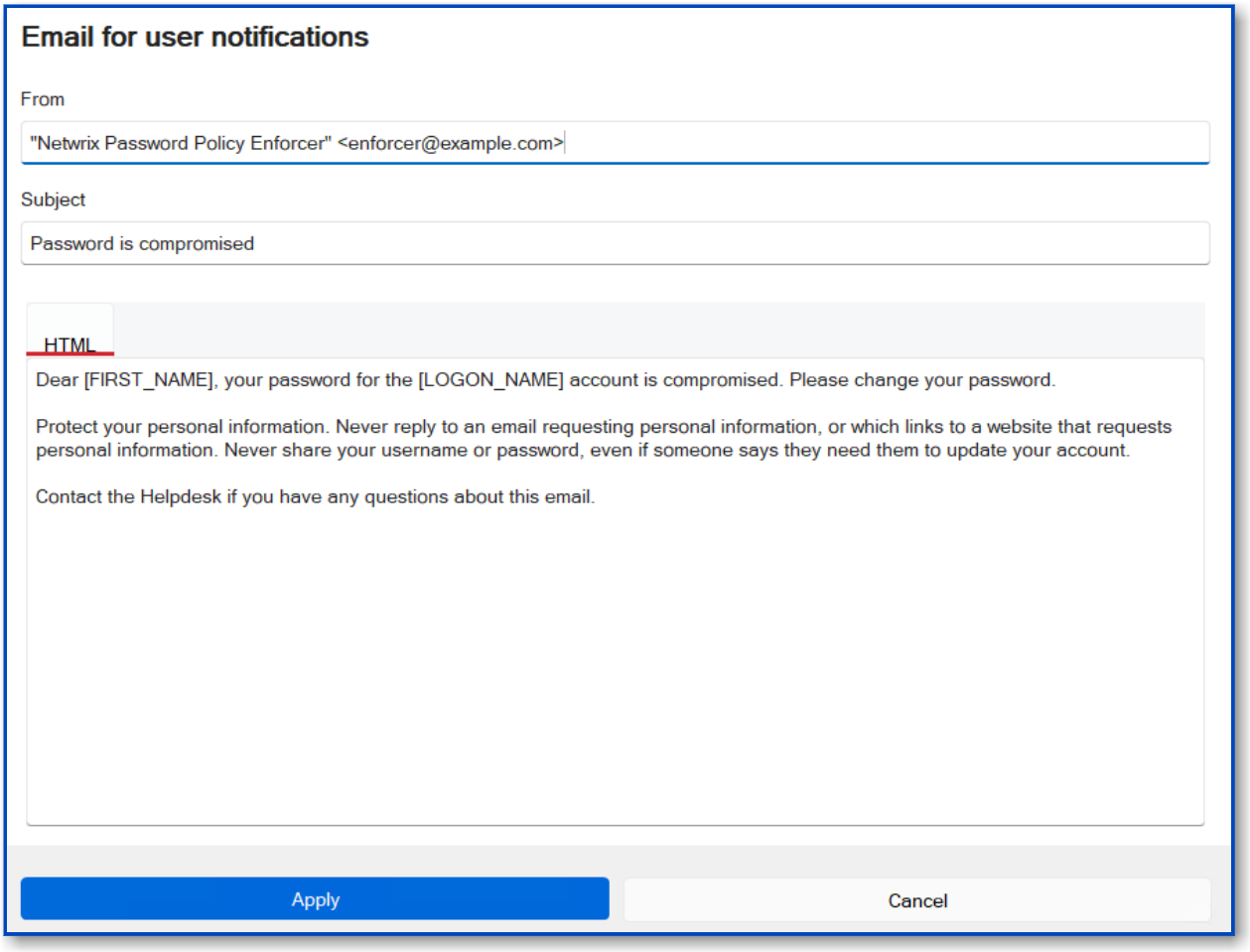
Click the **Compromised Passwords** tile on the Configuration Console dashboard. This feature is only available when **domain** is selected with the Connected To configuration setting. The Compromised Password Check is disabled by default, and the schedule is set to **None**.

Click the **Compromised Password Check** toggle to enable/disable the feature.



- **Compromised Passwords Base** specify the database to use when checking for compromised passwords. Netwrix recommends using the HIBP Updater to create this database. Click **Browse** to navigate to the folder. Default is **C:\HIBP\DB**
- **Domain Controller (FQDN)** specify the fully qualified domain controller name where you want to run the password check. Click **Browse** and select from the list.
- **Log events in Windows Application Event Viewer** select this option if you want to log events.
- **Force users to change password** select this option to force users to change compromised passwords.
- **Recipient of the full report on the found compromised passwords** specify the email address of the administrator who should receive the full report.
- **From** specify the email sender.
- **Notify users whose passwords are compromised by email** select this option to send email notification to users their password appears in the compromised list.

- **Set up email** click to set up the email message for users. Enter the **From** address and edit the subject and body template as needed. Click **Apply** to save changes.



Click **Save** to save your settings before running the check or setting up a schedule.

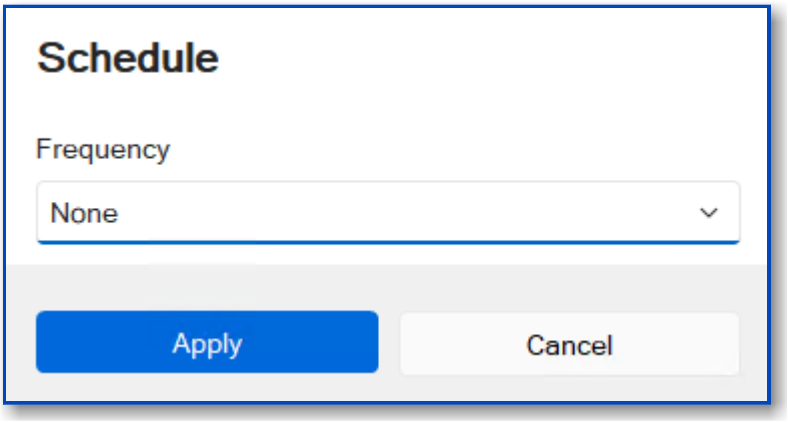
Click **Run now** to run the check. Depending on your network, the check can take quite a while to complete. You can schedule it for off hours instead of running it now.

Here is an example of the compromised passwords list:

List of compromised passwords				
User	Account	Sid	Email	Description
admin	Administrator	S-1-5-21-1006207104-1546379664-2458629591-500		Sending emails is not possible due to the lack of an email address in the account.
user2	user2	S-1-5-21-1006207104-1546379664-2458629591-1118	user2@company.com	Email has been sent

Schedule the Compromised Password Check

Click **Schedule** to set up a schedule to run the Compromised Password Check.



Select the **Frequency**:

- None: no scheduled runs.
- Run now: run the check now. No scheduled runs.
- Once: set the **Start date** and **Start time** to run the check a single time.
- Daily: set the **Start date** and **Start time** to run the check daily.
- Weekly: set the **Start date**, **Start time** and select the day of the week to run the check weekly.
- Monthly: set the **Start date**, **Start time** and select the day of the month to run the check monthly.

Click **Apply**.

System Audit and Support

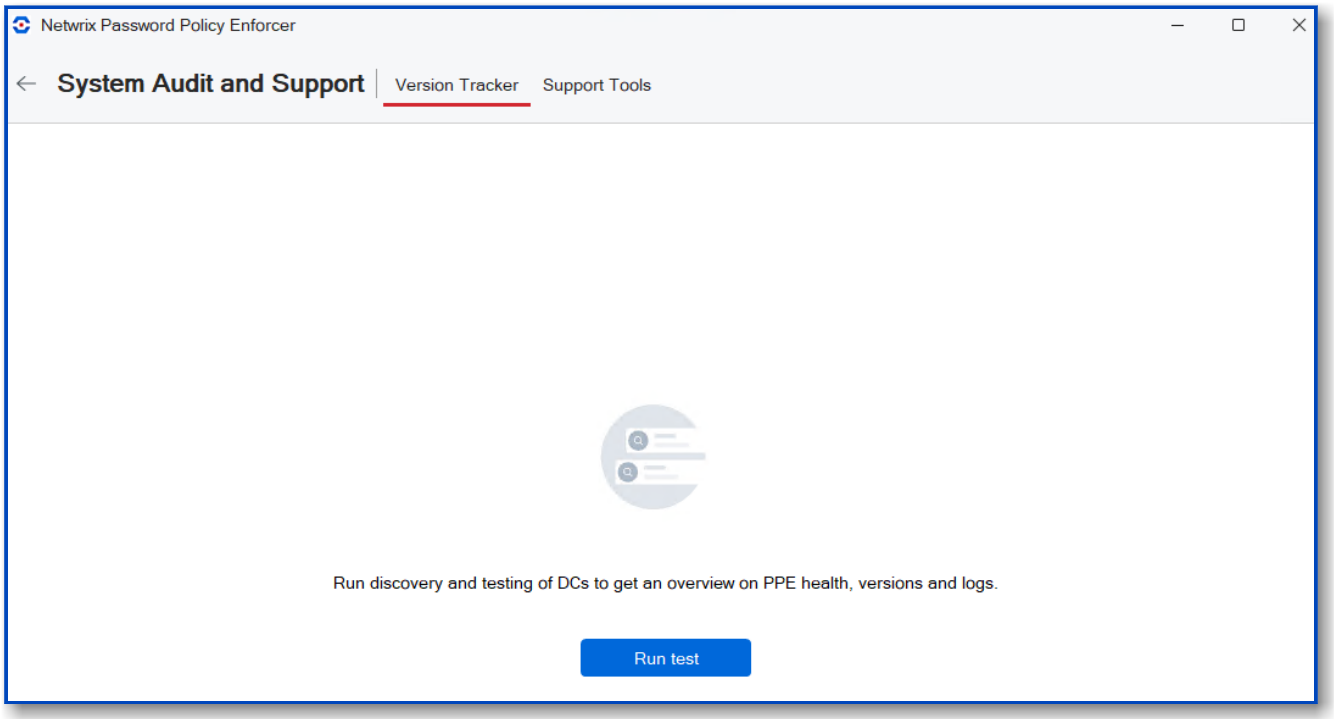
Password Policy Enforcer can run a discovery and testing of your domain controllers for an overview on PPE health, versions and logs.

Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.

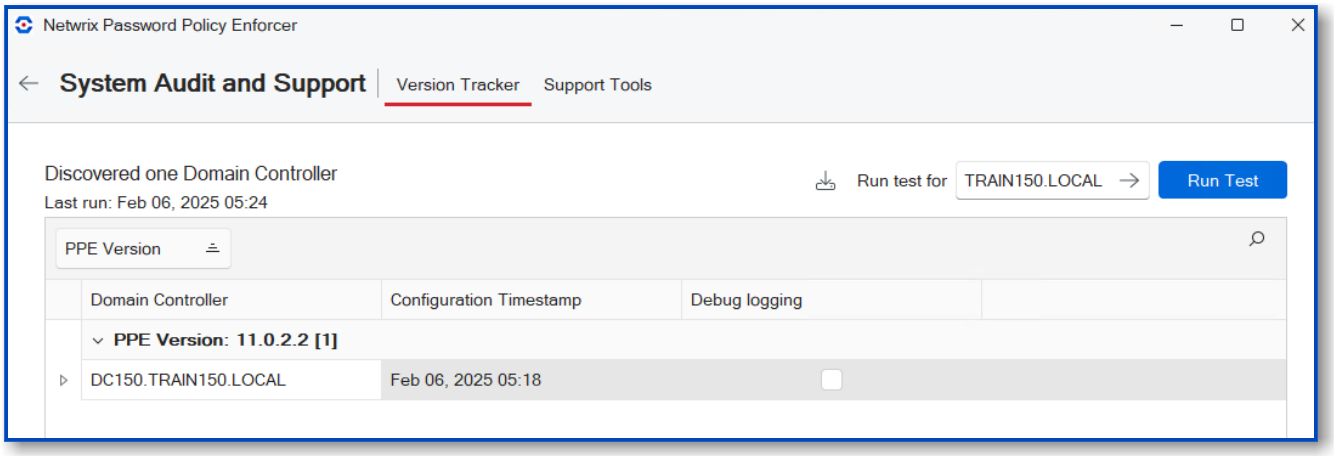
Click the **System Audit and Support** tile on the Configuration Console dashboard. This feature is only available when **domain** is selected with the Connected To configuration setting. System Audit and Support opens on the **Version Tracker** tab.

Version Tracker



Click **Run test**. The audit reports the discovered domain controllers and versions.

NOTE: If you do not see the **Configuration Timestamp**, contact your network administrator to set up the firewall to allow Password Policy Enforcer to communicate.

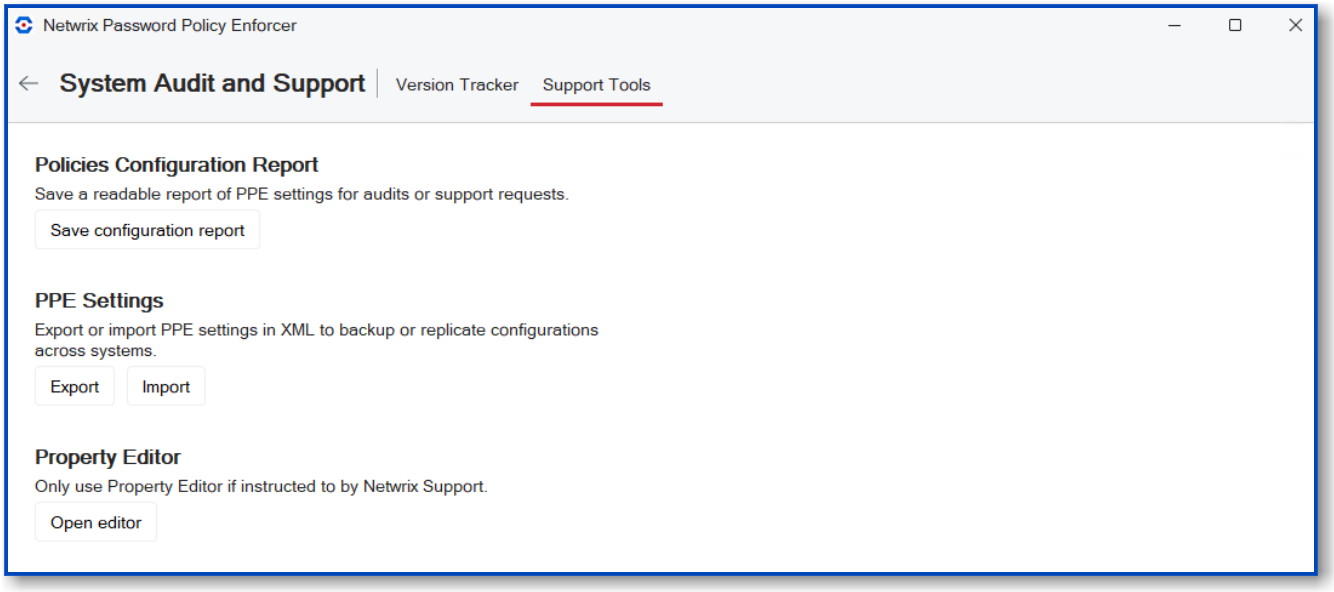


You can click the export icon to download your results. The file name is **Audit**_*timestamp*.**xlxs**, it is downloaded into the default **Downloads** folder. For large domains, you can apply filters or use the Search feature to make it easier to navigate your list.

NOTE: **Debug logging** should only be enabled when you are actively debugging your system. Leaving it enabled impacts Password Policy Enforcer performance and uses free disk space to create the logs.

Support Tools

The **Support Tools** tab enables you to save a configuration report, export/import PPE settings, and open the property editor.



- **Policies Configuration Report** saves the configuration as a text file. Browse to the folder where you want the report. The default filename is **PPEConfig.txt**.
- **PPE Settings** export your PPE settings for a backup. You can import the settings to replicate configurations across systems.
  - **Export** exports the PPE settings to an xml file. Browse to the folder where you want the file. The default filename is **PPEExport.xml**.
  - Import imports the settings from an exported xml PPE Settings file. Browse to the location of the **PPEExport.xml** file. Click **Open**. A status message is displayed when complete.

- **Open Property Editor** launches the Property Editor.

  NOTE: Properties should only be changed when advised by Netwrix Support.

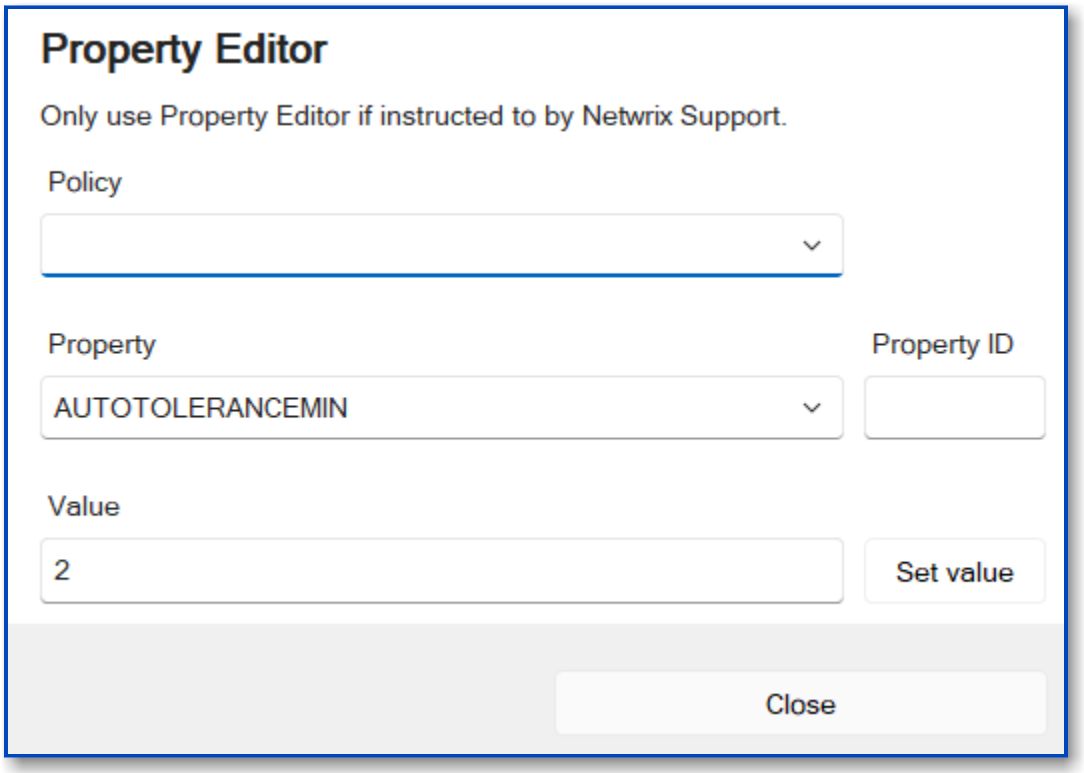
Property Editor

The Property Editor enables you to edit the Password Policy Enforcer configuration. It should only be used instructed by Netwrix Support. It is accessed from the Configuration Console:

Help > **Open Property Editor**

or

System Audit and Support > **Support Tools** > **Open editor**

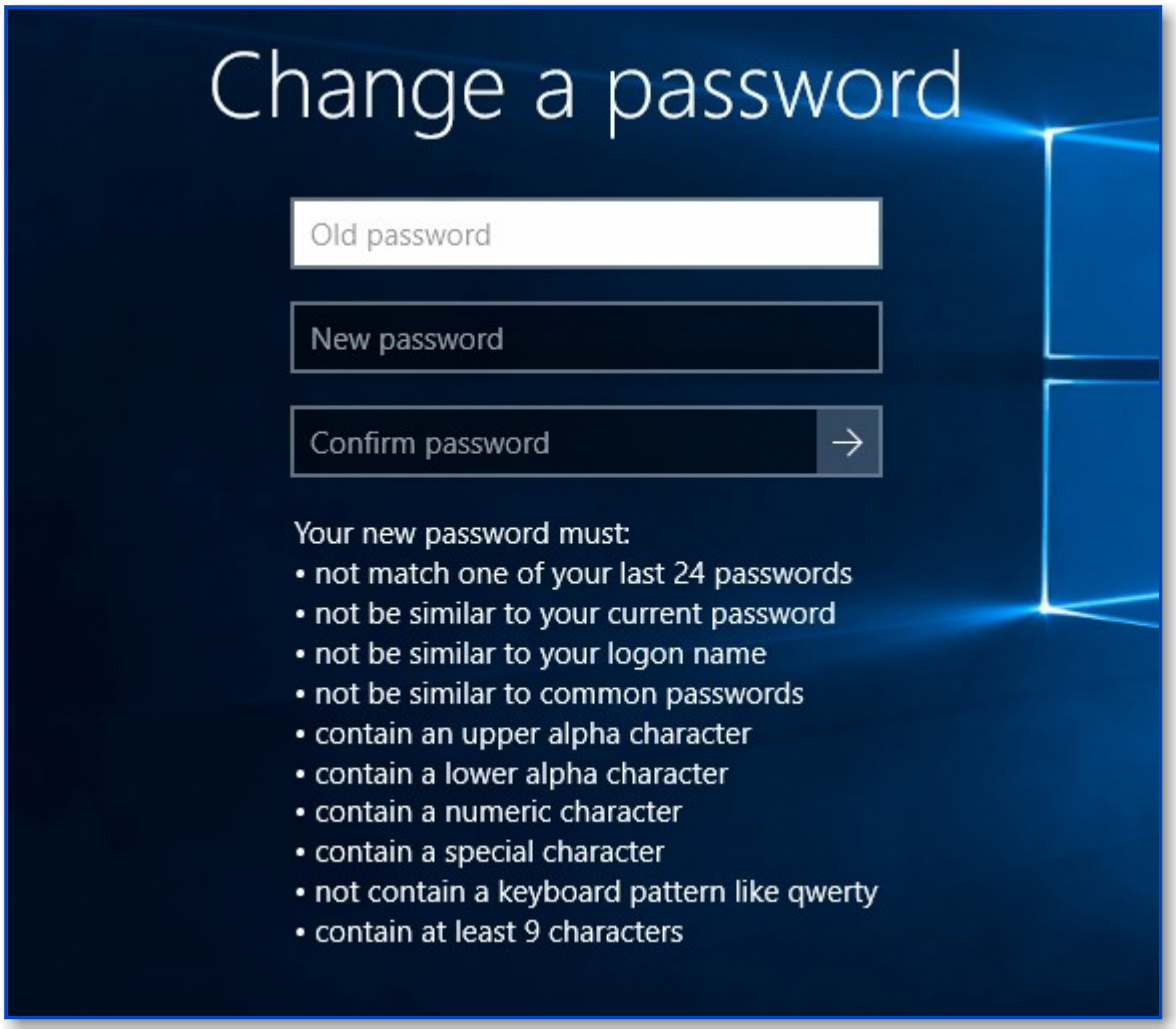


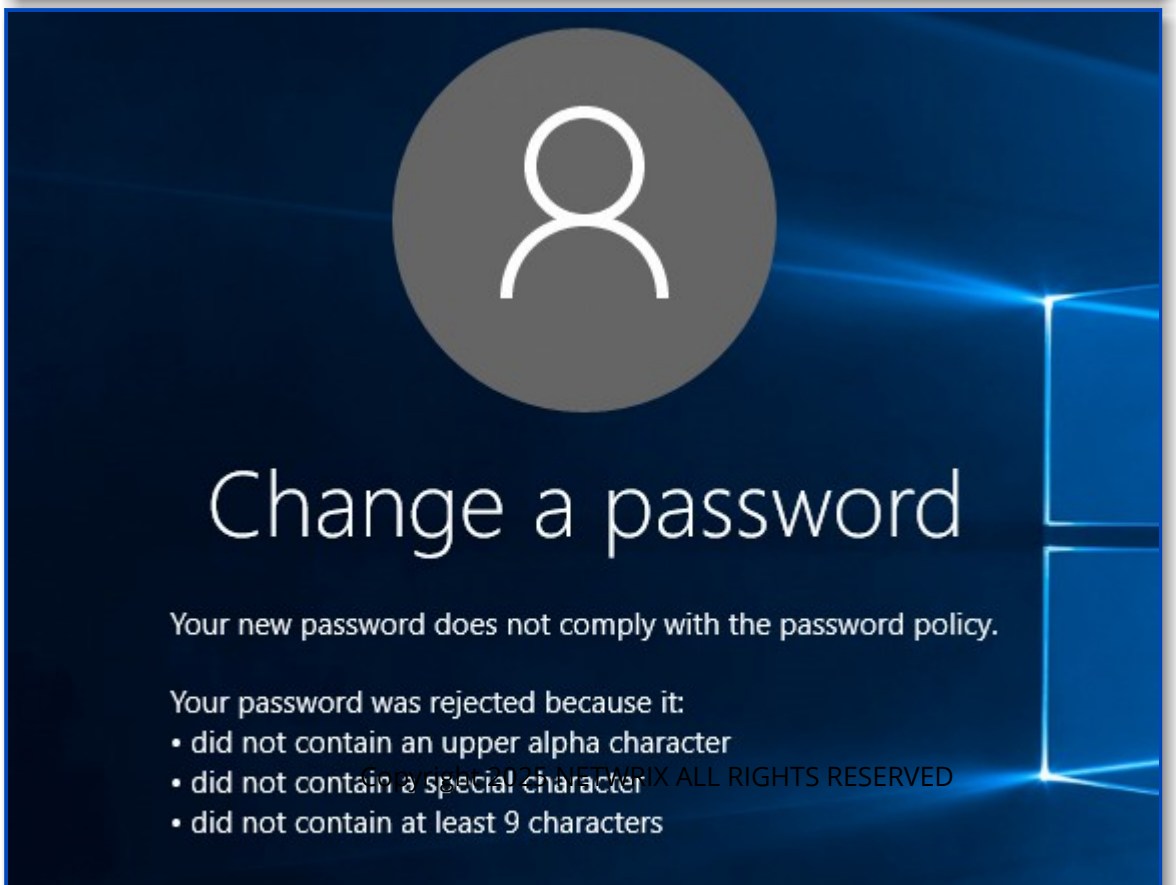
- **Policy**: select the policy to edit.
- **Property**: select the property to change.
- **Property ID**: enter the ID supplied by Netwrix Support.
- **Value**: enter the new value supplied by Netwrix Support. Click **Set value**.

Password Policy Client

The Password Policy Client helps users to choose a compliant password. Detailed information is provided if their new password is rejected.

The Password Policy Client is optional. If it is not installed, the Similarity Rule can not be enforced. Users only see the default Windows error message if their password is rejected, not the detailed help they receive from the Password Policy Client.





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

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

Configuring the Password Policy Client

The Password Policy Client is self-configuring and does not require manual configuration in most cases. See the Install Password Policy Enforcer Client topic for additional details. You may need to manually configure the Password Policy Client if:

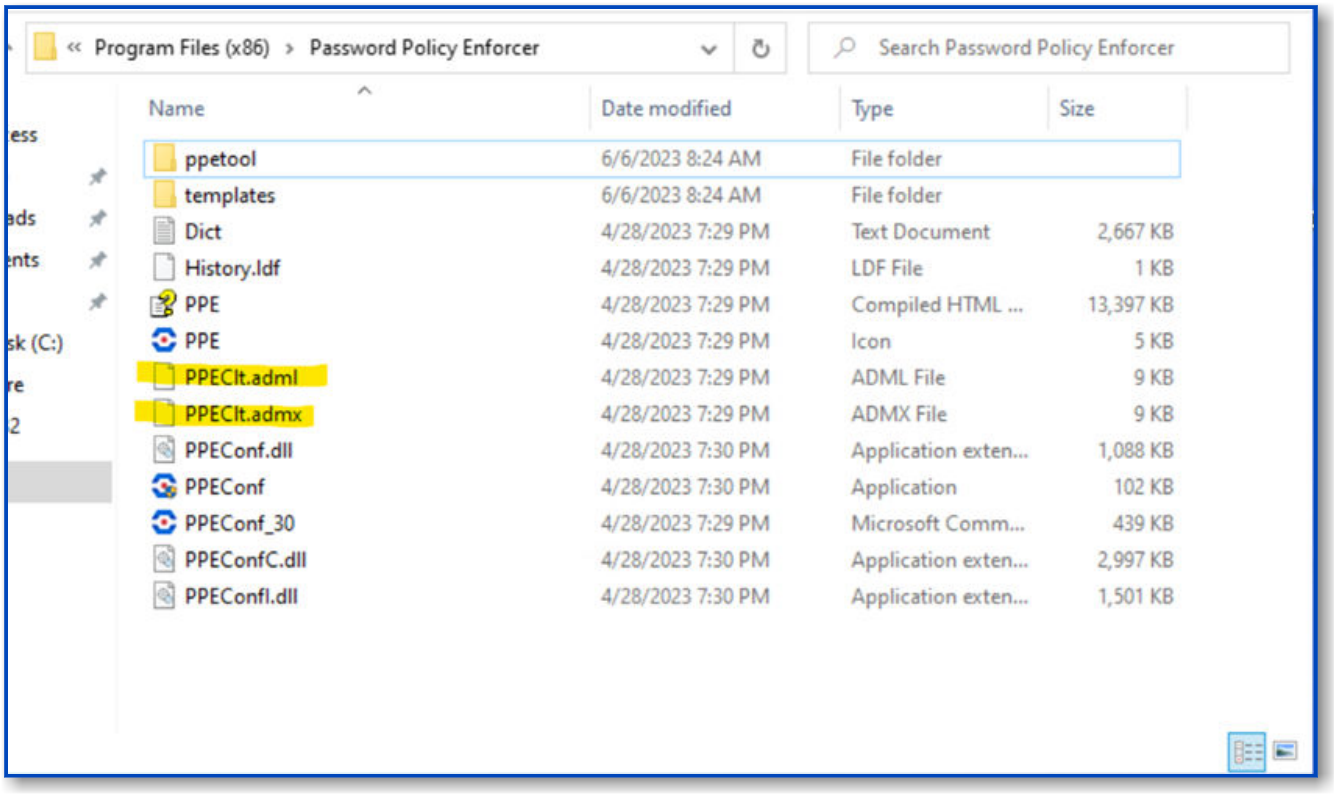
- You want to install it in a disabled state to be enabled later.
- You want to change the display settings for small screens.
- Password Policy Client displays policy messages in the wrong language.
- Default communication settings are not suitable (for example, if you change the default Password Policy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

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

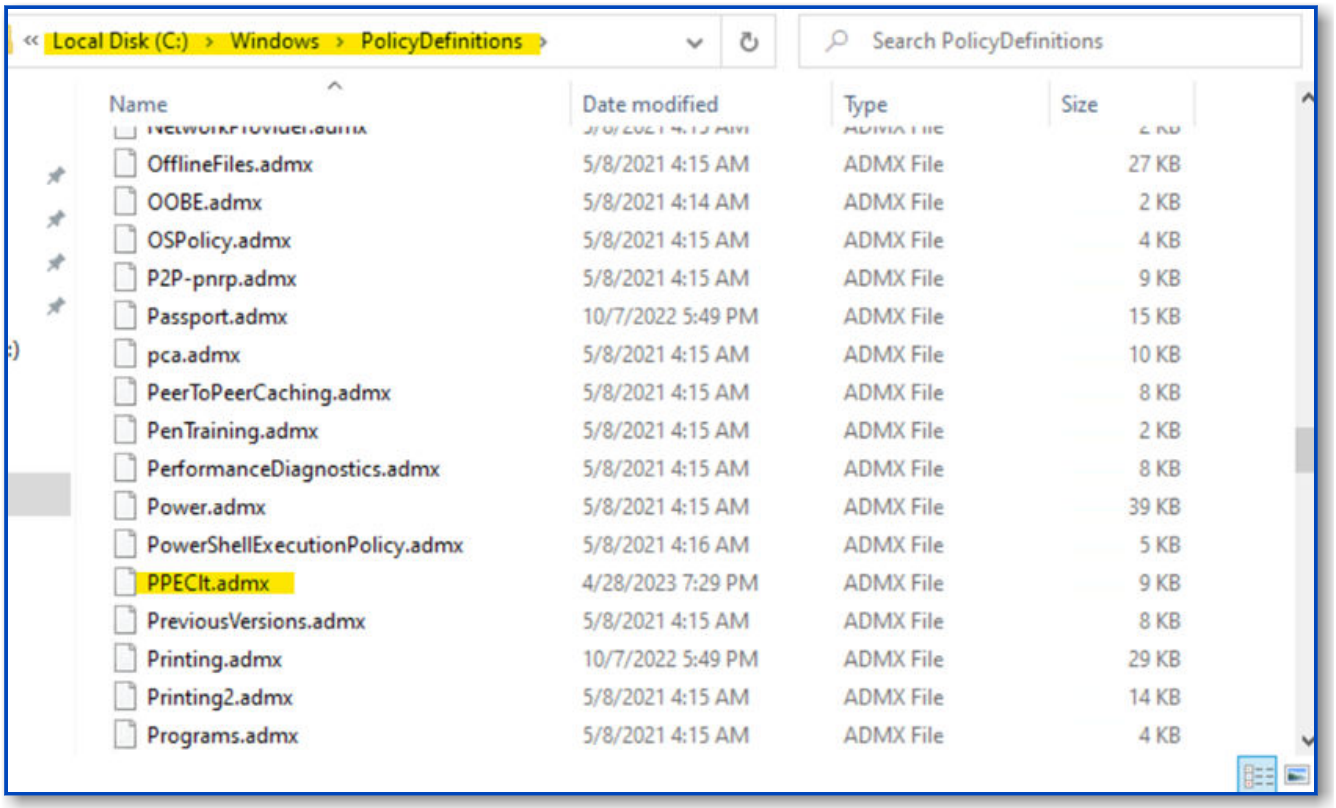
Install the Password Policy Client Administrative Template

Step 1 – Connect to any Domain Controller where you have Password Policy Enforcer installed and have the group policy management console available.

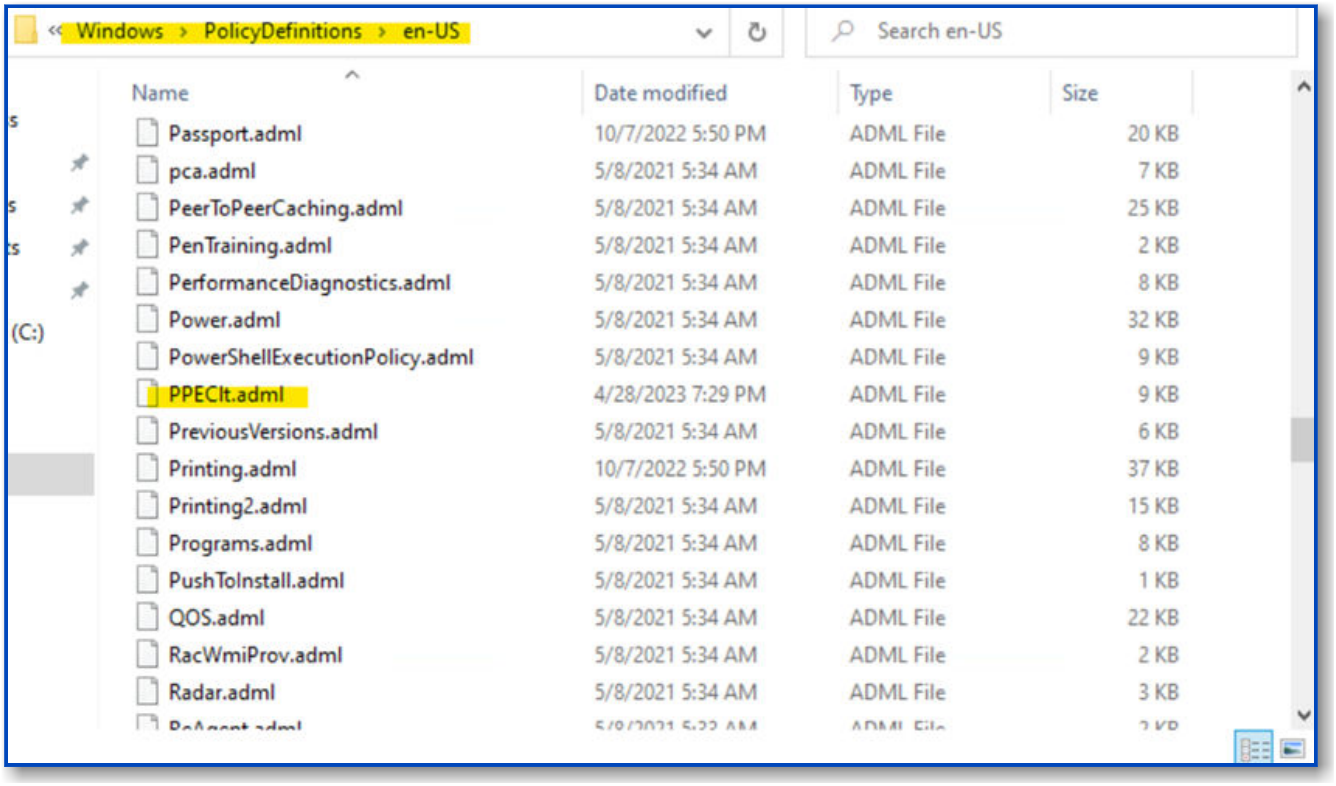
Step 2 – Go to Password Policy Enforcer install directory (C:\Program Files or C:\Program Files (x86)\Password Policy Enforcer) and copy the **PPEClt.adml** and **PPEClt.admx** files (highlighted in yellow):



Step 3 – Go to C:\Windows\Policy Definitions and paste the .admx file in the root of this folder.



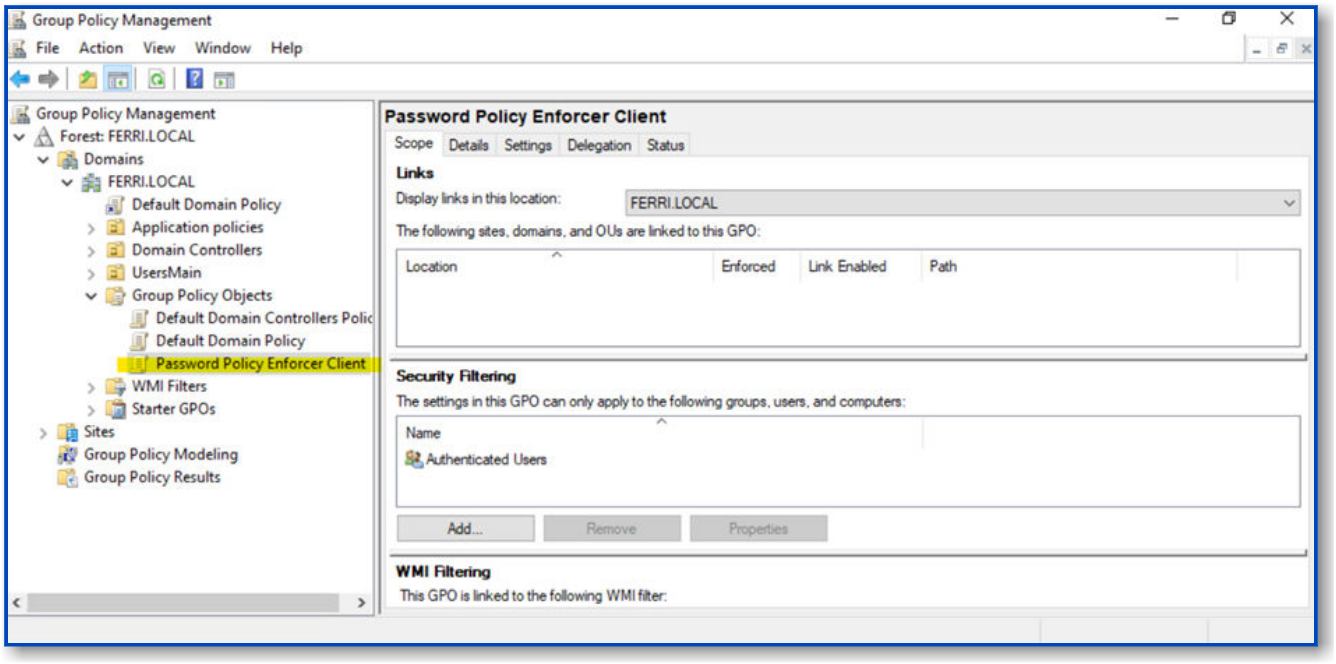
Step 4 – Go to C:\Windows\Policy Definitions\en-US and paste the .adml file in the root of this folder.



Step 5 – Open **Group Policy Management** console and check if you have a GPO created for Client. If not, see the topic's section for additional information.

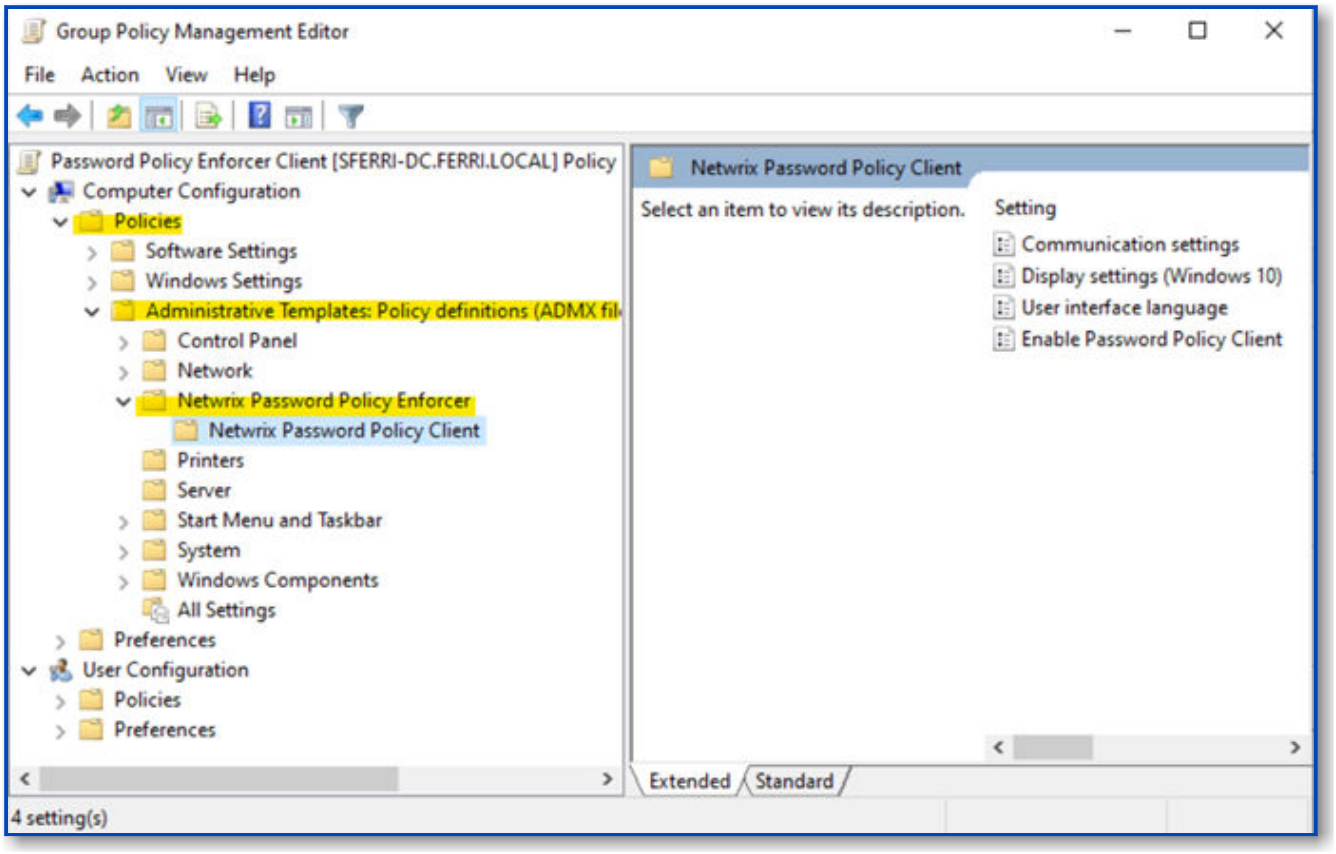
Step 6 – In the left pane, navigate to **Forest: <forest_name>** > **Domain** > **<domain_name>**, right-click **<OU_name>** and select **Create a GPO** in this domain and Link it here.

Once the GPO is configured, this view is available:

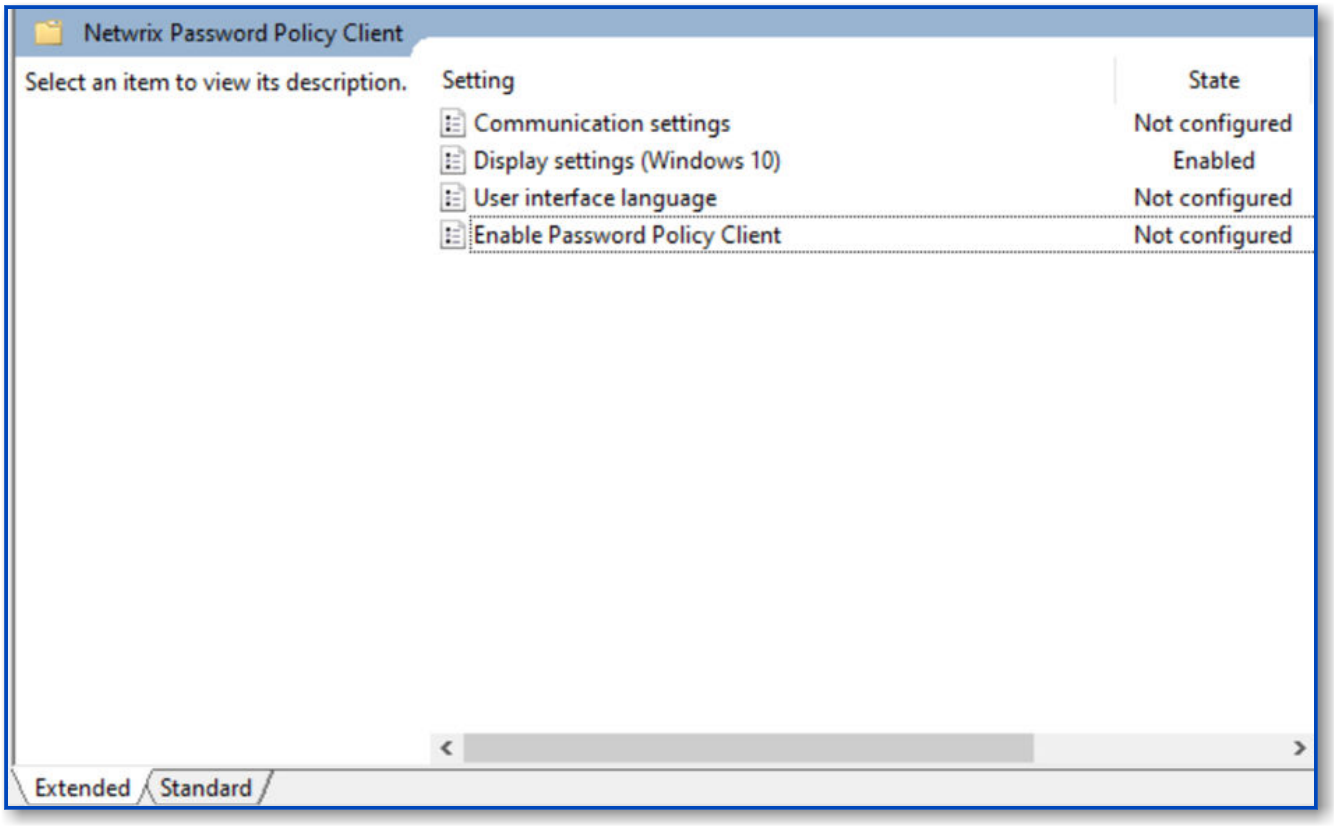


Step 7 – Right-click the newly created GPO and select **Edit** from the pop-up menu.

Step 8 – Expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Netwrix Password Policy Enforcer**



Step 9 – Click on **Netwrix Password Policy Client** to open a list of modification settings.

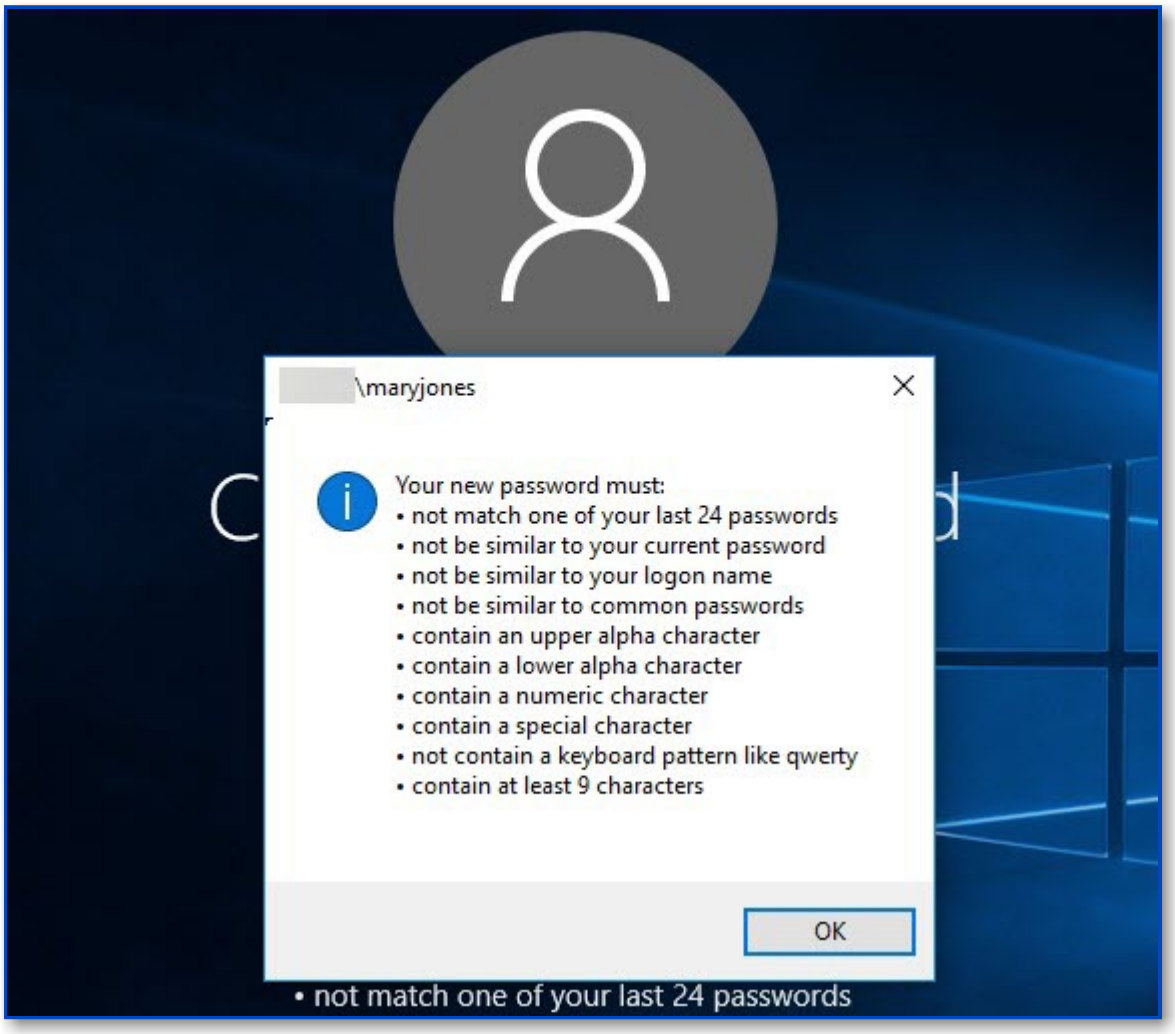


Step 10 – Select the one you need, then modify and save it.

Changing the Default Display Settings

The Windows 10 and 11 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 and 11 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.

Follow the steps below to change the default display settings for the Password Policy Client on Windows 10 and 11.

Step 1 – Use the **Group Policy Management Console** (gpmc.msc) to display the GPOs linked at the domain level.

NOTE: If you are not using Active Directory, then open the Local Group Policy Editor (**gpedit.msc**) and skip step 2.

Step 2 – Right-click the **Password Policy Client GPO**, then click the **Edit…** button.

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

Step 4 – Double-click the **Display settings (Windows 10)** setting in the right pane of the Group Policy Management Editor.

NOTE: Information about each option is shown in the Help box.

PPE cmdlets

The PPE Cmdlets are available to manage Password Policy Enforcer from a Windows PowerShell. The cmdlets are not case-sensitive.

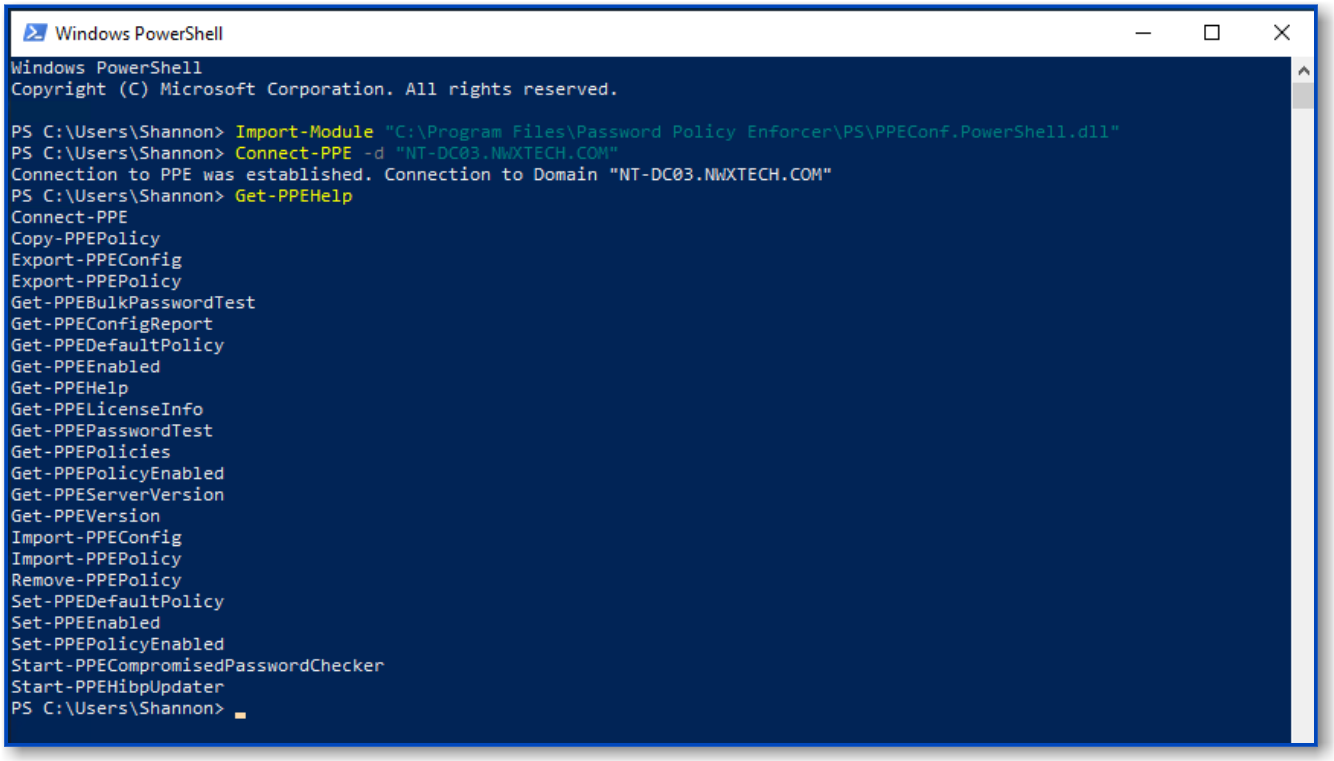
To establish the connection:

Step 1 – Open a Windows PowerShell. Some cmdlets require administrative permissions. You can use the **Run as Administrator** option.

Step 2 – Import the PPE cmdlets module:**Import-Module "C:\Program Files\Password Policy Enforcer\PS\PPEConf.PowerShell.dll"**

Step 3 – Connect to your domain:**Connect-PPE -d "*domain*"** where *domain* is the full name of your domain controller. **NT-DC03.NWXTECH.COM** in this example.

Get-PPEHelp with no parameters, displays a list of available cmdlets. Use the PowerShell **get-help** *Cmdlet* for information about the cmdlet.



Click a PPE cmdlet name for details.

- Connect-PPE
- Copy-PPEPolicy
- Export-PPEConfig
- Export-PPEPolicy
- Get-PPEBulkPasswordTest
- Get-PPEConfigReport
- Get-PPEDefaultPolicy
- Get-PPEEnabled
- Get-PPEHelp
- Get-PPELicenseInfo
- Get-PPEPasswordTest
- Get-PPEPolicies
- Get-PPEPolicyEnabled
- Get-PPEServerVersion
- Get-PPEVersion
- Import-PPEConfig
- Import-PPEPolicy
- Remove-PPEPolicy
- Set-PPEDefaultPolicy
- Set-PPEEnabled
- Set-PPEPolicyEnabled
- Start-PPECompromisedPasswordChecker
- Start-PPEHibpUpdater

Connect-PPE

The **Connect-PPE** cmdlet establishes a connection to the PPE Server.

SYNTAX

Connect-PPE [[**-Local**] <*SwitchParameter*>] [[**-Domain**] <*string*>] [<*CommonParameters*>]

PARAMETERS

-Domain <*string*>

Name of the domain controller to connect. Can also use **-D** or **-d**.

-Local <*SwitchParameter*>

Connect to PPE Server installed locally. Can also use **-L** or **-l**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Connect-PPE -d "DCNAME1.COMPANY.COM"

Connection to PPE was established. Connection to Domain
"DCNAME1.COMPANY.COM"
```

Copy-PPEPolicy

The **CopyPPEPolicy** cmdlet makes a copy of a PPE policy.

SYNTAX

Copy-PPEPolicy -DestPolicyName <*string*> **-SrcPolicyName** <*string*> [<*CommonParameters*>]

PARAMETERS

-SrcPolicyName <*string*>

Source PPE Policy Name. Can also use **-S** or **-s**.

-DestPolicyName <*string*>

Destination PPE Policy Name. Can also use **-D** or **-d**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Copy-PPEPolicy -s "Eval Policy" -d "User Policy"

The "User Policy" policy was created based on the "Eval Policy".
```

Export-PPEConfig

The **Export-PPEConfig** cmdlet exports the Password Policy Enforcer configuration to a file.

SYNTAX

Export-PPEConfig [**-File** <*string*>] [<*CommonParameters*>]

PARAMETERS

-File <*string*>

Name of the file to create.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Export-PPEConfig -file c:\ppe\ppe_config

Configuration export has been successfully completed. The file
"c:\ppe\ppe_config" has been created.
```

Export-PPEPolicy

The **Export-PPEPolicy** exports a Password Policy Enforcer policy to a file.

NOTE: This cmdlet calls the **PPE Tool**. You must be an administrator to run this cmdlet. Start PowerShell with the **Run as Administrator** option.

SYNTAX

Export-PPEPolicy -PolicyName <*string*> [**-File** <*string*>] [<*CommonParameters*>]

PARAMETERS

-PolicyName <*string*>

Name of the to export.

-File <*string*>

Name of the file to create.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Export-PPEPolicy -PolicyName "Eval Policy" -File C:\ppe\EvalPolicy

Configuration export has been successfully completed. The file
"C:\ppe\EvalPolicy" has been created.
```

Get-PPEBulkPasswordTest

The **Get-PPEBulkPasswordTest** cmdlet runs the Password Policy Enforcer bulk password test of the specified policy.

SYNTAX

Get-PPEBulkPasswordTest -PasswordFile <*string*> **-Policy** <*string*> **-ResultFolder** <*string*> [<*CommonParameters*>]

PARAMETERS

-PasswordFile <*string*>

Path and name of the text file containing the passwords to test. Passwords in your test file are 1 per line.

-Policy <*string*>

The name of the policy to enforce for the test.

-ResultFolder *<string>*

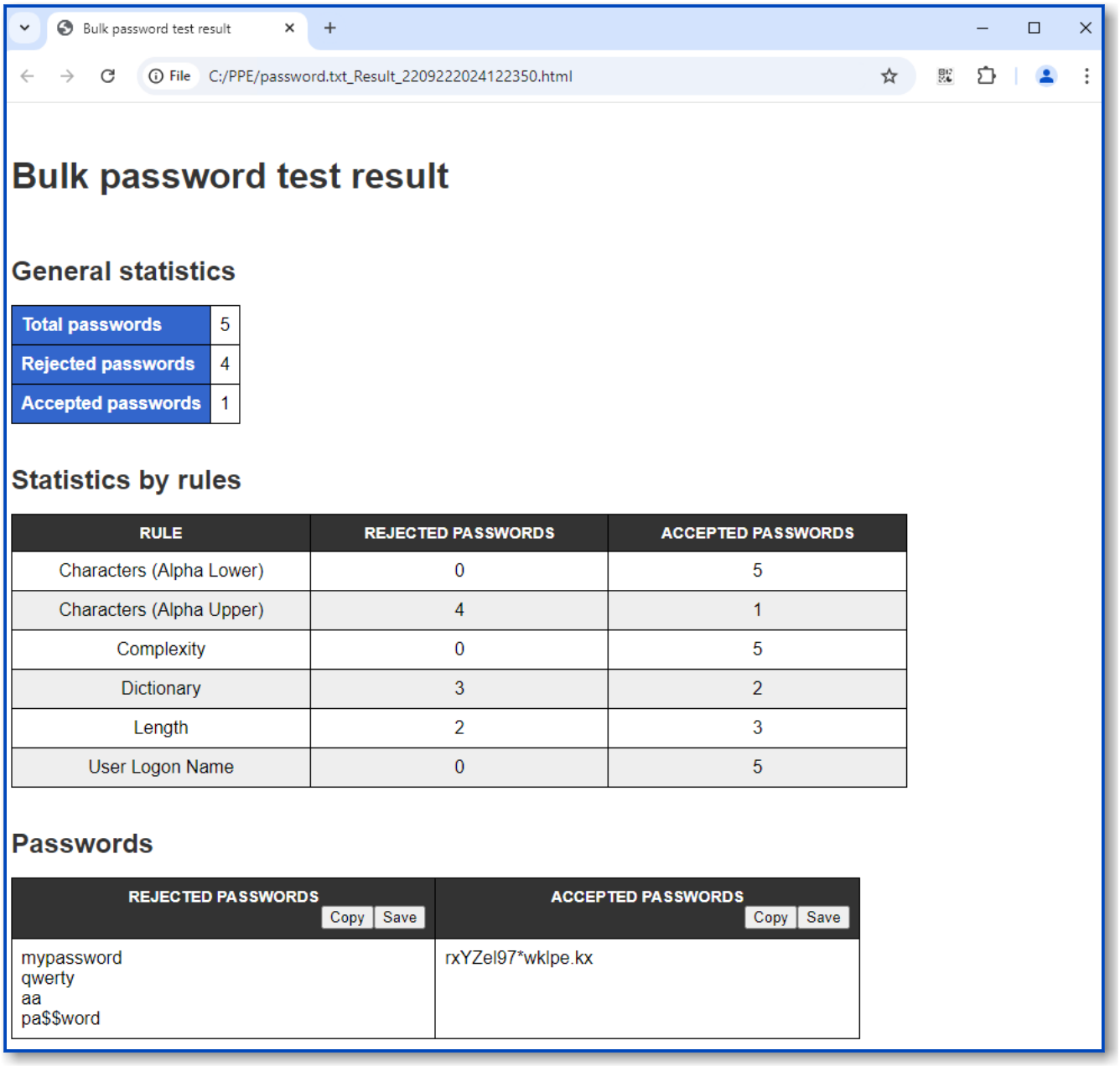
The folder for the created html report.

<CommonParameters>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEBulkPasswordTest -PasswordFile C:\PPE\password.txt -Policy
"Eval Policy" -resultFolder C:\PPE

Bulk test is running...

The report is created: "C:\PPE\password.txt_Result_2209222024122350.html".
```



Get-PPEConfigReport

The **Get-PPEConfigReport** cmdlet saves a Password Policy Enforcer configuration report.

NOTE: This cmdlet calls the PPE Tool. You must be an administrator to run this cmdlet. Start PowerShell with the **Run as Administrator** option.

SYNTAX

Get-PPEConfigReport -Folder] <*string*>

PARAMETERS

-Folder <*string*>

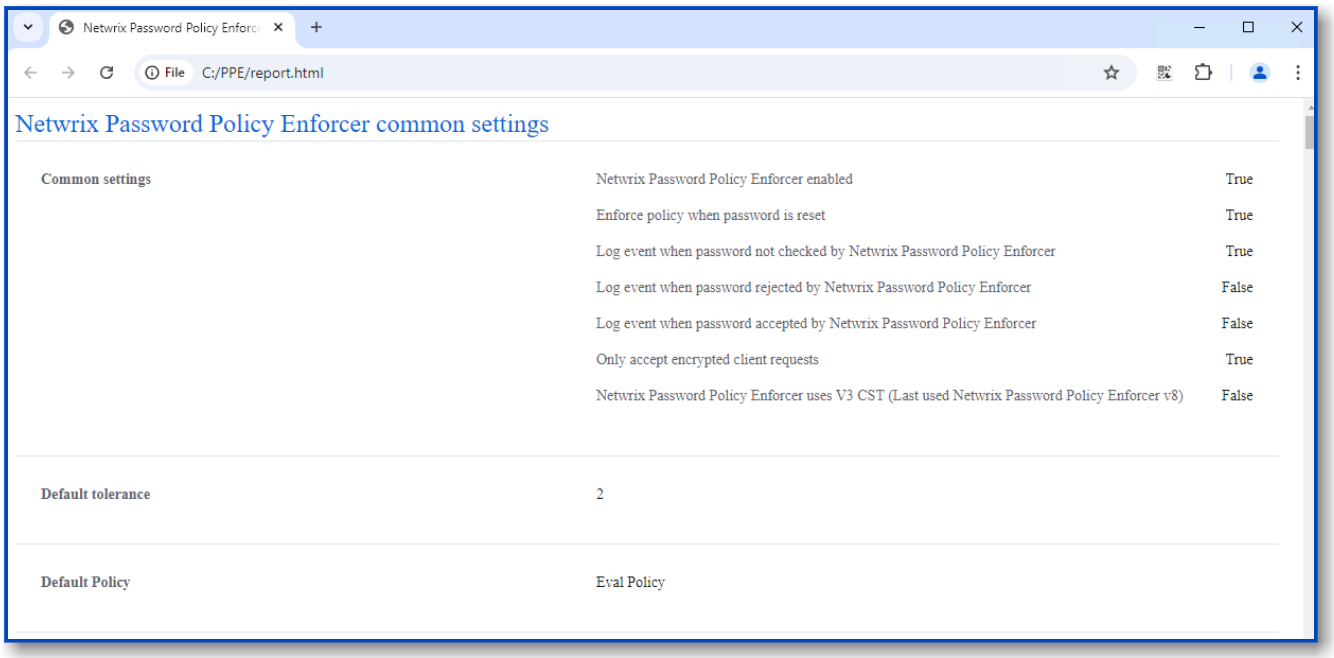
Name of the folder to save the report.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEConfigReport -Folder C:\PPE

The report is created: "C:\PPE\report.html".
```



Get-PPEDefaultPolicy

The **Get-PPEDefaultPolicy** cmdlet reports the name of the Password Policy Enforcer default Policy.

SYNTAX

Get-PPEDefaultPolicy [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEDefaultPolicy

Default policy : Eval Policy
```

Get-PPEEnabled

The **Get-PPEEnabled** cmdlet returns the enabled/disabled status of the PPE Server.

SYNTAX

Get-PPEEnabled [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEEnabled

Status PPE : Enabled
```

Get-PPEHelp

The **Get-PPEHelp** cmdlet lists the available Password Policy Enforcer cmdlets. If a cmdlet is specified, returns help for the cmdlet.

SYNTAX

Get-PPEHelp [[**-Cmdlet**] <*string*>]

PARAMETERS

-Cmdlet <*string*>

Name of the cmdlet for help. Can also use **-C** or **-c**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> get-ppehelp get-ppehelp

NAME

Get-PPEHelp

SYNOPSIS

Get a list of the PPE Cmdlet

SYNTAX

Get-PPEHelp [[-Cmdlet] <string>] [<CommonParameters>]

DESCRIPTION

Get a list of the PPE Cmdlet

RELATED LINKS

https://www.netwrix.com/password_policy_enforcer.html

REMARKS

To see the examples, type: "get-help Get-PPEHelp -examples".

For more information, type: "get-help Get-PPEHelp -detailed".

For technical information, type: "get-help Get-PPEHelp -full".

For online help, type: "get-help Get-PPEHelp -online"
```

Get-PPELicenseInfo

The **Get-PPELicenseInfo** cmdlet returns the Password Policy Enforcer license information.

SYNTAX

Get-PPELicenseInfo [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPELicenseInfo

ANIXIS Software License Certificate

Product: Password Policy Enforcer

License type: Perpetual

Licensed to: test

Version: 11

Users: 100

<ANIXIS_LICENSE>JrPQdyhsxWrLj7RsuX322Ni8vwIRr6ozC+sY3M16aJba

XuRXG6VjOjWUMT1XwqO4c3VA0eIB8+z4KyUNEzLjmSZKvtLsHb0kFYi1zRiL

6EBVflEmzxYIsCvAlsg1fNfK1JgjFefOc1gENy2CBikDTbe+HnHf3aVBq6p2

Va1eXmMXToi3NDNJCNFzQHy7ZGC5AhQ8GIjQfgK8z9s1sHzpdj2Gn+9BEyQQ

nv833QdoFhjKoAXN/xCecZclkCkP9f1GLuq4kN0Emsh5qqXl686JBJlisA3o

XWQrEQ0Me9P3TkSUpb742JCngQaGcjKHvQoufBJ+GIrcwWG2DZJ1i9xrOJMT

g8D5eFDz/OiqXuZyBHFTInbq77V59x/xtIlUffBW7sCUmY8B+ZhLR2XpLdxr

S+4E37Lhf46bScltZxfHZbDQKZuT4hdMKnnzgNHEzkMh8Q3T/40sMvQbAV4O
```

```
tDF633YsQMH3Ttbyc+vAvIvbAHJOVhBpNd9TCybfas+j6uQL5fa4qo8dFrx+

+UrPakOmSL/eDR7xB5/zmB37shDXIPfzfG/Vu7I1/EQuH01rZDyafHnzTmmm

1hCMqyi+oVzxZtN8I3sIpAH3FLu+1N37CuHJFrXD97Iu6RjKi+11nG9BmZ2Q

0SX5EYc=</ANIXIS_LICENSE>
```

Get-PPEPasswordTest

The **Get-PPEPasswordTest** cmdlet runs the Password Policy Enforcer password test for a user.

SYNTAX

Get-PPEPasswordTest -Password <*string*> **-Username** <*string*> [**-OldPassword** <*string*>] [<*CommonParameters*>]

PARAMETERS

-Password <*string*>

The password to test.

-User <*string*>

The username to test. Can also use **-U** or **-u**.

-OldPassword <*string*>

The old password to test.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEPasswordTest -Password qwerty -User PPETestUser

Assigning default policy "Eval Policy"

Log

- Info : Reading configuration from NT-DC03.nwxtech.com.

- Info : DN is "CN=PPE Test User,CN=Users,DC=NWXTECH,DC=COM"
```

```
- Info : Current password is 5 days old.

- Info : Extended Maximum Age group not found.

- Info : Dictionary rule found "QWERTY".

- Info : Password rejected.

Password must:

- Accepted : contain a lower alpha character

- Rejected : contain an upper alpha character

- Accepted : contain at least 1 of these character types:

- upper alpha

- lower alpha

- Rejected : not be similar to a common password

- Rejected : contain at least 7 characters

- Accepted : not be similar to your logon name
```

Get-PPEPolicies

The **Get-PPEPolicies** cmdlet returns the Password Policy Enforcer policies.

SYNTAX

Get-PPEPolicies [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEPolicies

Admins Policy
```

```
Eval Policy

Test

User Policy
```

Get-PPEPolicyEnabled

The **Get-PPEPolicyEnabled** cmdlet returns the enabled/disabled status of a Password Policy Enforcer policy.

SYNTAX

Get-PPEPolicyEnabled -PolicyName <*string*> [<*CommonParameters*>]

PARAMETERS

-PolicyName <*string*>

Name of the policy. Can also use **-P** or **-p**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEPolicyEnabled -PolicyName "Eval Policy"

Policy "Eval Policy" is Enabled
```

Get-PPEServerVersion

The **Get-PPEServerVersion** cmdlet returns the Password Policy Enforcer server version.

SYNTAX

Get-PPEServerVersion [**-DC**] <*string*>] [<*CommonParameters*>]

PARAMETERS

-DC <*string*>

Name of the domain controller running the PPE Server. If not specified, the current domain controller is used.

-Local <*SwitchParameter*>

Connect to PPE Server installed locally. Can also use **-L** or **-l**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEServerVersion -DC NT-DC03.NWXTECH.COM

Version: 11.0.0.74
```

Get-PPEVersion

The **Get-PPEVersion** cmdlet returns the version of the Password Policy Enforcer PowerShell module.

SYNTAX

Get-PPEVersion [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Get-PPEVersion

Version: 11.0.0.74
```

Import-PPEConfig

The **Import-PPEConfig** cmdlet imports a Password Policy Enforcer configuration file.

NOTE: This cmdlet calls the **PPE Tool**. You must be an administrator to run this cmdlet. Start PowerShell with the **Run as Administrator** option.

SYNTAX

Import-PPEConfig -File] <*string*> <*CommonParameters*>]

PARAMETERS

-File <*string*>

Name of the configuration file. Can also use **-F** or **-f**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Import-PPEConfig -File C:\PPE\ppe_config

Config import successful.
```

Import-PPEPolicy

The **Import-PPEPolicy** cmdlet imports a Password Policy Enforcer policy from a file.

NOTE: This cmdlet calls the **PPE Tool**. You must be an administrator to run this cmdlet. Start PowerShell with the **Run as Administrator** option.

SYNTAX

Import-PPEPolicy -File] <*string*> [<*CommonParameters*>]

PARAMETERS

-File <*string*>

Name of the policy file. Can also use **-F** or **-f**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Import-PPEPolicy -File "C:\PPE\EvalPolicy"

Config import successful.
```

Remove-PPEPolicy

The **Remove-PPEPolicy** cmdlet removes a Password Policy Enforcer policy.

SYNTAX

Remove-PPEPolicy -PolicyName] <*string*> [<*CommonParameters*>]

PARAMETERS

-PolicyName <*string*>

Name of the policy. Can also use **-P** or **-p**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Remove-PPEPolicy -PolicyName Test

PS C:\>
```

Set-PPEDefaultPolicy

The **Set-PPEDefaultPolicy** cmdlet sets the Password Policy Enforcer policy as the default.

SYNTAX

Set-PPEDefaultPolicy -PolicyName] <*string*> [<*CommonParameters*>]

PARAMETERS

-PolicyName <*string*>

Name of the policy. Can also use **-P** or **-p**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Set-PPEDefaultPolicy -PolicyName "Eval Policy"

Default policy : Eval Policy
```

Set-PPEEnabled

The **Set-PPEEnabled** cmdlet sets the enabled/disabled status for the PPE Server.

SYNTAX

Set-PPEEnabled -Enable] <*int*> [<*CommonParameters*>]

PARAMETERS

-Enable <*int*>

Specify **1** to enable the PPE Server, specify **0** to disable the PPE Server. Can also use **-E** or **-e**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLES

```
PS C:\> Set-PPEEnabled -Enable 0

Status PPE : Disabled

PS C:\> Set-PPEEnabled -Enable 1

Status PPE : Enabled
```

Set-PPEPolicyEnabled

The **Set-PPEPolicyEnabled** cmdlet sets the enabled/disabled status for a Password Policy Enforcer policy.

SYNTAX

Set-PPEPolicyEnabled -PolicyName <*string*> **-Enable**] <*int*> [<*CommonParameters*>]

PARAMETERS

-PolicyName <*string*>

The policy name.

-Enable <*int*>

Specify **1** to enable the policy, specify **0** to dis -Poliable the policy. Can also use **-E** or **-e**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLES

```
PS C:\> Set-PPEPolicyEnabled -PolicyName "Eval Policy" -Enable 0

Policy "Eval Policy" is Disabled

PS C:\> Set-PPEPolicyEnabled -PolicyName "Eval Policy" -Enable 1

Policy "Eval Policy" is Enabled
```

Start-PPECompromisedPasswordChecker

The **Start-PPECompromisedPasswordChecker** cmdlet runs the Password Policy Enforcer Compromised Password Checker.

SYNTAX

Start-PPECompromisedPasswordChecker [<*CommonParameters*>]

PARAMETERS

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Start-PPECompromisedPasswordChecker

PS C:\>
```

Start-PPEHibpUpdater

The **Start-PPEHibpUpdater** cmdlet starts an update of the Hibp database.

SYNTAX

Start-PPEHibpUpdater [[**-Web**] <*SwitchParameter*>] **-Folder** <*string*> [**-File** <*string*>] **[-Inc** <*SwitchParameter*>]

[<*CommonParameters*>]

PARAMETERS

-Web <*SwitchParameter*>

Specify the update uses the NTLM Hashes file from the netwrix website.

-Folder <*string*>

Folder with the HIBP database. Can also use **-D** or **-d**.

-Inc <*SwitchParameter*>

Type of update. Specify **full** to update the entire database or **incremental**to add new entries to the existing database. Can also use **-I** or **-i**.

-File <*string*>

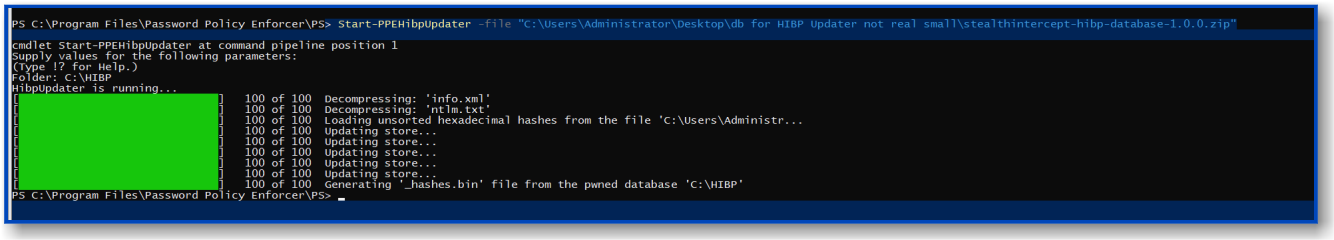
File with list of NTLM hashes. Can also use **-S** or **-s**.

<*CommonParameters*>

This cmdlet supports the common parameters: **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer**, **PipelineVariable**, and **OutVariable**. For more information, see about_CommonParameters https:/go.microsoft.com/fwlink/?LinkID=113216.

EXAMPLE

```
PS C:\> Start-PPEHibpUpdater -Folder "C:\HIBP\DB" -File
"C:\Users\Administrator\Desktop\db for HIBP Updater not real
small\stealthintercept-hibp-database-1.0.0.zip
```



Command Line Interface

Silent Installation

Replace *version* with the complete version and build number of the **msi** file. For example, 11.0.0.74.

Install only PPE Server: msiexec /i Netwrix_PPE_Server_*version*_x64.msi ADDLOCAL=FeatureServerPPE /q

Install only Console: msiexec /i Netwrix_PPE_Server_*version*_x64.msi ADDLOCAL=FeatureConsole /q

Install only Mailer Server: msiexec /i Netwrix_PPE_Server_*version*_x64.msi ADDLOCAL=FeaturePPEMailerServer /q

Install all 3 components:

msiexec /i Netwrix_PPE_Server_*version*_x64.msi ADDLOCAL=FeaturePPEMailerServer,FeatureConsole,FeatureServerPPE /q

By default Console only installed: msiexec /i Netwrix_PPE_Server_*version*_x64.msi /q

Uninstall all: msiexec /uninstall Netwrix_PPE_Server_*version*_x64.msi /q

Uninstall only particular feature: msiexec /i *path_to_your_msi_file.msi* REMOVE=*FeatureName* /qn

If a reboot was not done, add **/forcerestart** at the end

Mailer

You can run the Password Policy Enforcer Mailer from the command line to deliver email immediately, or to troubleshoot problems. PPEMail.exe is copied into the \Program Files (x86)

\Password Policy Enforcer\ folder when the Password Policy Enforcer Mailer is installed.

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

Running PPEMail.exe with the /send parameter disables simulation mode. Any emails 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 emails to users.

To test email delivery options without sending any emails to users, run PPEMail.exe with the /test parameter followed by your email address. For example, PPEMail.exe /test johnsmith@netwrix.com. This will send one test email to your mail server or pickup folder.

PPE Tool

The PPE Tool is designed to configure local and domain instances of Password Policy Enforcer and produce reports pertaining to the configuration of Password Policy Enforcer. The PPE Tool is designed to perform the following functions:

- Export the configuration from the existing instance of Password Policy Enforcer, regardless if the server is local or domain.
- Import existing PPE configurations on another PPE server instance.
- Generate user-friendly reports that contain configuration values and descriptions.
- Create HTML reports with configuration values and descriptions of the PPE server instance.

This topic will cover how to install the PPE Tool, customize and run reports, and configuration options in the PPE Tool.

Using the PPE Tool

The PPE Tool installs with the default installation of Password Policy Enforcer under the `C:\Program Files (x86)\Password Policy Enforcer\ppetool` folder. Once installed, the PPE Tool allows users to perform a number of operations related to Password Policy Enforcer functionality which are described in the table below.

NOTE: All PPE Tool operations can be executed from the Command Prompt, if run with administrator rights.

PPE Tool Operations

RECOMMENDED: PPE Tool operations should only be executed one at a time. For example, you should not execute the /e (Export) and /i (Import) operations simultaneously; you should not run /e (Export) and /r (Report) operations simultaneously.

Common PPE Tool Operations

Operation	Operation Name	Operation Description
`/?`	help	• Displays Help and exits the application. All other options are ignored.
`/m`	minimal	• Configures the PPE Tool to operate in Minimal mode. • This operation strips away all extraneous information (e.g., policy messages, license information, etc.) while importing or exporting to the PPE Tool. • By default, the PPE Tool imports and exports all information available (e.g., policy messages, license information, etc.).

Operation	Operation Name	Operation Description
/d	domain [in controller]	• Configures the PPE Tool to operate in Domain mode. • The default controller is localhost. • This operation will make PPE Tool work with the LDAP Password Policy Enforcer instance. PPE Tool imports or exports configurations from the local registry. • To use this operation , you must run PPE Tool as a domain administrator user. However, this operation can be used on both the domain controller and on any member. If an invalid domain controller is provided as an argument, then the PPE Tool will fail at the import / export stage. • This operation is ignored when used to create reports from the file source (present with the /c (Config [in file name]) option). When the PPE Tool starts in a domain environment without the /d (Domain [in controller]) operation, a warning message will appear. However, this will not prevent the PPE Tool from operating on a local environment.
/c	config [in file name]	• Uses a config file instead of Password Policy Enforcer export when exporting

Operation	Operation Name	Operation Description
		reports (in the case of /i (Import), /h (Human [out file name]), and /r (Report [out file name]). • The default file is `config.xml`. • This operation defines the input file for the i/ (Import) operation, and thus is necessary for importing files to the PPE Tool. An error message will appear if the /c (Config [in file name]) option is omitted. • By default, the /h (Human [out file name]) and /r (Report [out file name]) operations use the Password Policy Enforcer instance as the reporting source. The /c (Config [in file name]) operation should provide the source configuration file as an argument to create reports. If an invalid file name is provided as an argument in this operation, the PPE Tool will display the appropriate error message and will fail.

Operations PPE Tool options are as follows:

Task	Task Name	Task Description
/e	export [out file name]	• Exports config data (default) from the Password Policy Enforcer instance to the file.

Task	Task Name	Task Description
		• This operations is enabled by default. • This operation can not be used with /c (Config [in file name]) or i/ (Import) operations, but can be combined with /h (Human [out file name]).
/i	import	• Imports the config file. • Imports existing configuration using the input configuration file defined by the /d (Domain [in controller]) . If the /c (Config [in file name]) operation is omitted, the PPE Tool will display an error message and exit the application. • When i/ (Import) is used with the /h (Human [out file name]) or /r (Report [out file name]) operations, the latter will be ignored. • /d (Domain [in controller]) and /m (Minimal) operations my affect the result of the import.
/h	human [out file name]	• Converts the config file to a human-readable format and produces a human-readable report based on the current Password Policy Enforcer instance configuration or the configuration provided by

Task	Task Name	Task Description
		the /d (Domain [in controller]). • If no custom file name is provided, the default file name will be `config_human_readable.xml`.
/r	report [out file name]	• Converts the config file to HTML and produces an HTML report file based on the current Password Policy Enforcer instance configuration or the configuration provided by the /d (Domain [in controller]). • Generates the HTML report into `C:\Program Files (x86)\Password Policy Enforcer\Report` alongside the .css file. • The default files name is `report.html`.

PPE Usage Samples

This section covers some sample operations usable in either the PPE Tool or in the Command console (with administrator rights). Each operation can be executed after the following commands have been executed:

```
C:\Windows/system32>cd..
```

C:\[location of PPE Tool]>[operation]

Once this location has been accessed in the Command console, enter one of the following commands in the [operation] variable above to execute a PPE Tool operation in the Command console.

Action	Operation	Message
Simple Config export operation	• `ppetool`	Warning: PPETool started in domain environment without /d option. Using local source. Hope you know what are you doing. Config successfully exported.
Simple Config export in domain environment with DC %Full computer name of Domain Controller%	• `ppetool /d localhost` • `ppetool /d %Full computer name of Domain Controller%`	Config successfully exported.
Export local config into local.xml and create it from the HR.xml and report.html reports	• `ppetool /e local.xml /h HR.xml /r Report.html`	Warning: PPETool started in domain environment without /d option. Using local source. Hope you know what are you doing. Config successfully exported. Human readable config representation successfully exported. HTML config representation exported successfully.
Import Config from config.xml	• `ppetool /c config.xml /i`	Warning: PPETool started in domain environment without /d option. Using local source. Hope you know what are you doing. Config import successful.

Generating Reports with Custom Descriptions

The PPE Tool generates user-friendly reports by processing configuration tags (i.e., <PPE>). For example, the PPE Tool will search for the file tagname.xml (or, ppe.xml in this case). This file has root elements which name match each file name. Each root tag contains child tags (e.g., <tag>). Each tag has the following attributes:

- name — Contains the original tag name from the input configuration file. If this attribute is missed, then the original tag and its value will be absent in the human-readable report.
- DisplayName — Contains the user-friendly description for the original tag. If this attribute is missed, then the original tag and its value will be presented in the report without a description.

The <tag> tag can also contain the child <FLAGS> tag. This tag can have an optional attribute 'mode' and this attribute can have the following values:

- value (default) — With the default value, the report will only contain tag descriptions for the child <flag> tag. The 'value' attribute matches the child <flag> tag with the value of the original tag.
- combined — With the combined value, the report will contain the child <flag> tags which contain values that are bitwise or are the result of the original values.

Example of 'value' mode

Original configuration

```
<MAILMODE>1</MAILMODE>
```

Transform configuration

```
<tag name="MAILMODE" DisplayName="Mail delivery method">
 <FLAGS mode="value">
  <flag DisplayName="Disable e-mail reminders" value="1"/>
  <flag DisplayName="Send e-mail to SMTP server" value="2"/>
  <flag DisplayName="Save e-mail to a pickup folder" value="3"/>
 </FLAGS>
</tag>
```

Transformation result

```
<MAILMODE DisplayName="Mail delivery method">
 <options>
  <option DisplayName="Disable e-mail reminders">True</option>
  <option DisplayName="Send e-mail to SMTP server">False</option>
  <option DisplayName="Save e-mail to a pickup folder">False</option>
 </options>
</MAILMODE>
```

Example of 'combined' mode

Original configuration

```
<FLAGS>25</FLAGS>
```

Transformation configuration

```
<tag name="FLAGS" DisplayName="Common settings">
 <FLAGS mode="combined" DisplayName="Common settings">
  <flag DisplayName="Netwrix Password Policy Enforcer enabled"
  value="0x00000001"/>
  <flag DisplayName="Enforce policy when password is reset"
  value="0x00000002" inverted="true"/>
  <flag DisplayName="Log event when password not checked by Netwrix
  Password Policy Enforcer" value="0x00000008"/>
  <flag DisplayName="Log event when password rejected by Netwrix Password
  Policy Enforcer" value="0x00000020"/>
  <flag DisplayName="Log event when password accepted by Netwrix Password
  Policy Enforcer" value="0x00000040"/>
  <flag DisplayName="Only accept encrypted client requests"
  value="0x00000010"/>
```

```
  <flag DisplayName="Netwrix Password Policy Enforcer uses V3 CST (Last
  used Netwrix Password Policy Enforcer v8)" value="0x00000004"/>

 </FLAGS>

</tag>
```

Result human-readable report

```
<FLAGS DisplayName="Common settings">

 <options>

  <option DisplayName="Netwrix Password Policy Enforcer enabled">False</
  option>

  <option DisplayName="Enforce policy when password is reset">True</
  option>

  <option DisplayName="Log event when password not checked by Netwrix
  Password Policy Enforcer">True</option>

  <option DisplayName="Log event when password rejected by Netwrix
  Password Policy Enforcer">False</option>

  <option DisplayName="Log event when password accepted by Netwrix
  Password Policy Enforcer">False</option>

  <option DisplayName="Only accept encrypted client requests">True</
  option>

  <option DisplayName="Netwrix Password Policy Enforcer uses V3 CST (Last
  used Netwrix Password Policy Enforcer v8)">False</option>

 </options>

</FLAGS>
```

Customize HTML Report

The PPE Tool comes with a pre-defined template.css file in the configuration folder, found here: `C:\Program Files (x86)\Password Policy Enforcer\config`. The template.css defines the visual design (formatting, colors, fonts etc.) of HTML report. See the XSLT - Transformation article for additional information of transforming .xml to .xhtml.

Troubleshooting

This topic contains troubleshooting information for the most common support questions. Contact Netwrix support with any questions.

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 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. See the Password Policy Client topic for additional information.

If Password Policy Enforcer 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 Password Policy Enforcer since the last restart on any domain controller, then make sure that Password Policy Enforcer is installed on that domain controller and restart it. Check the Windows Application Event Log again after the restart to ensure that Password Policy Enforcer 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 Password Policy Client and Password Policy Server 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. See the Configuration Console topic for additional information.

Make sure that the Password Policy Client is enabled. See Password Policy Client topic for additional information.

Accepting passwords that do not comply with the policy

If Password Policy Enforcer 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 Password Policy Enforcer since the last restart on any domain controller, then make sure that Password Policy Enforcer is installed on that domain controller and restart it. Check the Windows Application Event Log again after the restart to ensure that Password Policy Enforcer started. For local policies, search the Application Event Log on the local computer.

Use the Test Policies page to test a password that Password Policy Enforcer is accepting. Examine the test results and event log to determine why Password Policy Enforcer accepted the password. If the Test Policies page rejects the password, you must configure the policy. See the Policy Testing vs. Password Changes topic for additional information.

If the **Enforce policy when password is reset** check box is not selected in the PPS Properties page, then Password Policy Enforcer 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.

Rejecting passwords that comply with the policy

Use the Test Policies page to test a password that Password Policy Enforcer is rejecting. Examine the test results and event log to determine why Password Policy Enforcer rejected the password. If the Test Policies page rejects the password, you must configure the policy. See the Policy Testing vs. Password Changes topic for additional information.

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 Password Policy Enforcer is configured to enforce a minimum password age. Disable the Minimum Age rule in Windows and Password Policy Enforcer 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.

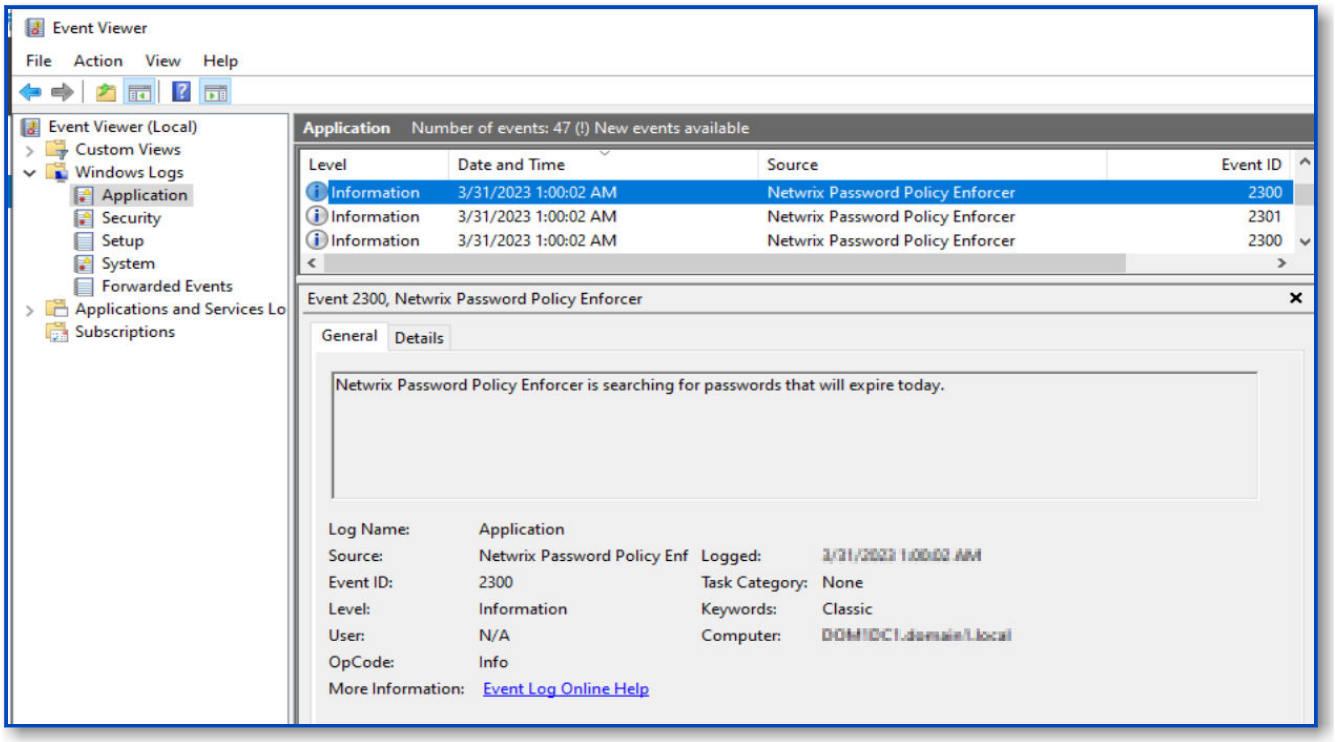
Passwords that are accepted in the Test Policies page are rejected during a password change

See the Policy Testing vs. Password Changes topic for additional information.

View Event Logs in Windows Event Viewer

Follow the steps below to view events logs in Windows Event Viewer.

Step 1 – Open **Windows Event Viewer**.



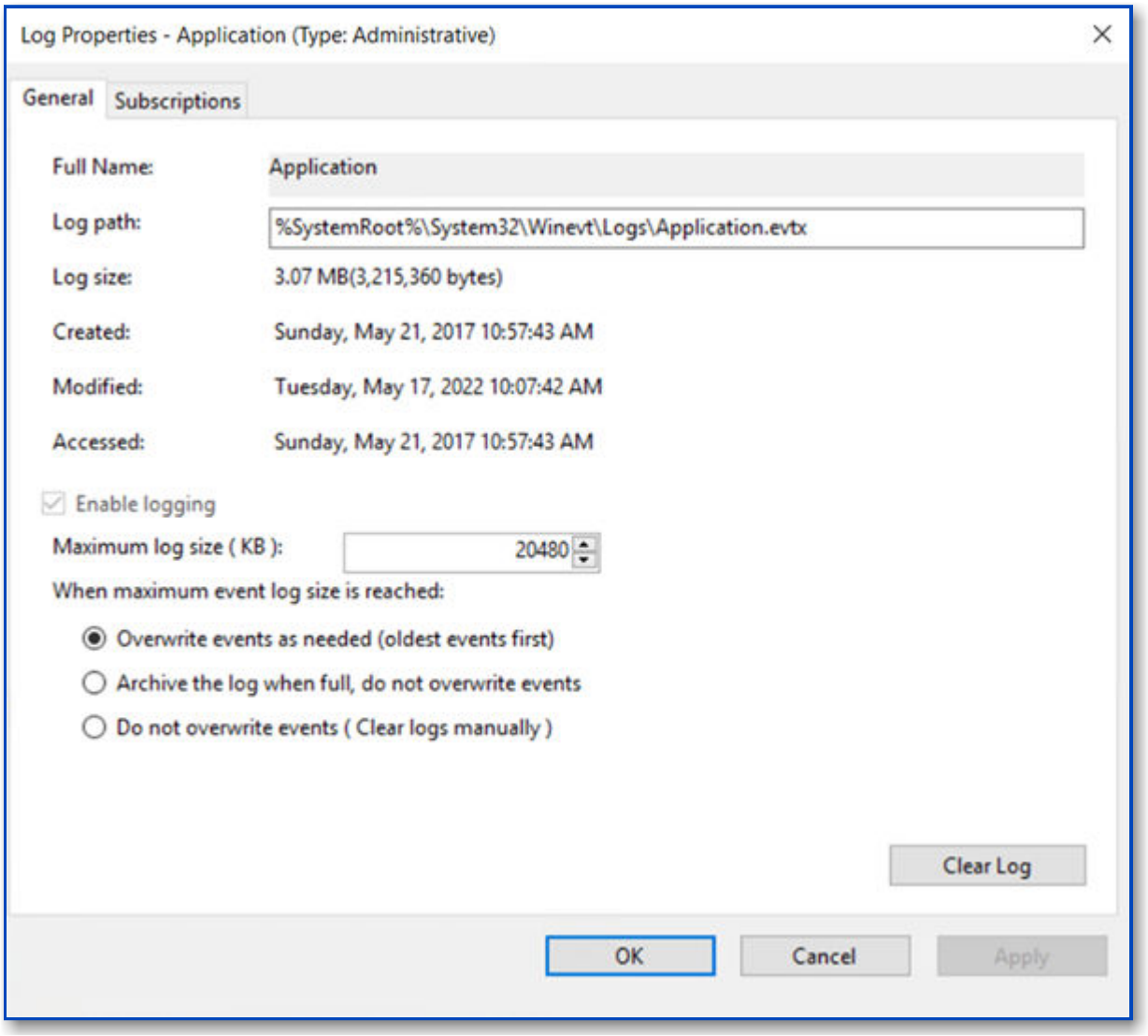
Step 2 – Navigate to **Windows Logs** > **Application**.

Step 3 – In the Application list, select a Netwrix Password Policy Enforcer event under the Source column.

The General tab shows details for the selected event. The Details tab shows...

View Log Properties

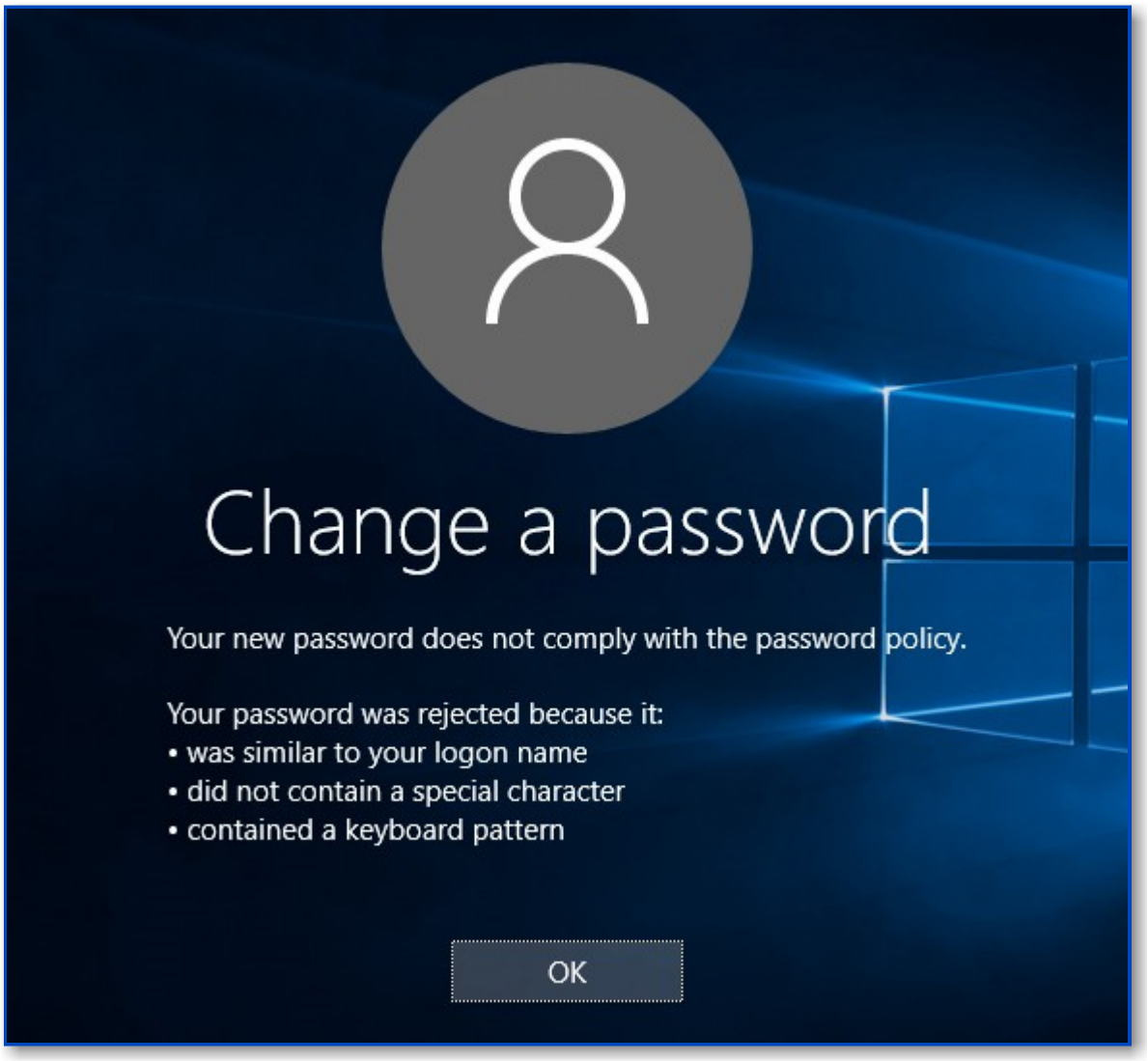
To view Log Properties, navigate to the Actions menu and select **Properties**.



The Log Properties window displays. Settings for this log can be configured from this window.

Evaluate Password Policy Enforcer

Netwrix Password Policy Enforcer is an advanced password filter for Windows. Use this guide to quickly install, configure, and test an evaluation version of Password Policy Enforcer. Netwrix Password Policy Enforcer helps secure your network by ensuring users set strong passwords. When a user enters a password that does not comply with the password policy, Password Policy Enforcer immediately rejects the password and details why the password was rejected.



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

NOTE: You can also use Password Policy Enforcer to ensure that passwords are compatible with other systems, and to synchronize passwords with other systems and applications.

Prepare the Computer

You only need one computer for the evaluation. A Windows Server 2016, 2019, or 2022 domain controller in its own domain is recommended. You can also use Windows 10 or 11 if you only need to enforce policies for local accounts.

Disable the Windows Password Policy Rules

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

This procedure disables the Windows password policy:

Step 1 – Open the appropriate policy management tool:

- If you are evaluating Password Policy Enforcer on a domain, use the Group Policy Management Console (**gmpc.msc**) to display the GPOs linked at the domain level. Right-click the **Default Domain Policy GPO** (or whichever GPO you use to set the password policy), then click the **Edit...** button.
- If you are evaluating Password Policy Enforcer on a standalone server or workstation, open the **Local Group Policy Editor** (**gpedit.msc**).

Step 2 – Expand the following items:

- Computer Configuration
- Policies (if it exists)
- Windows Settings
- Security Settings
- Account Policies
- Password Policy

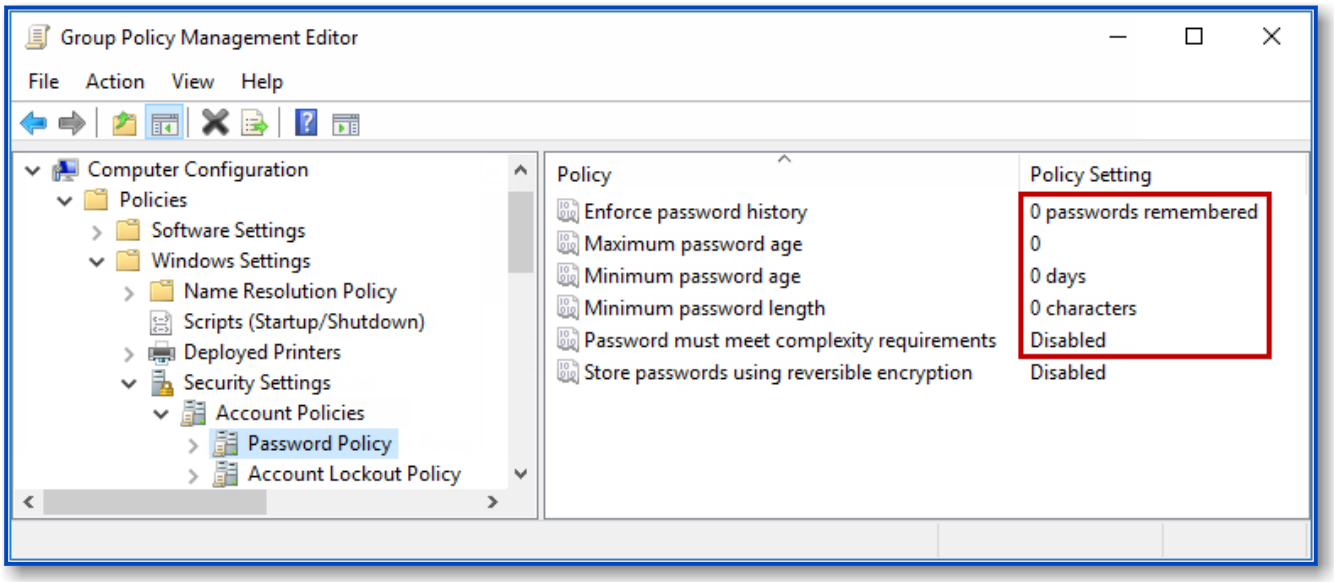
Step 3 – Double-click **Enforce password history** in the right pane of the GPO Editor.

Step 4 – Enter **0** in the text box, then click **OK**.

Step 5 – Repeat the step above for the Maximum Password Age and Minimum Password Length policies.

Step 6 – Double-click the **Group Policy Management Editor**.

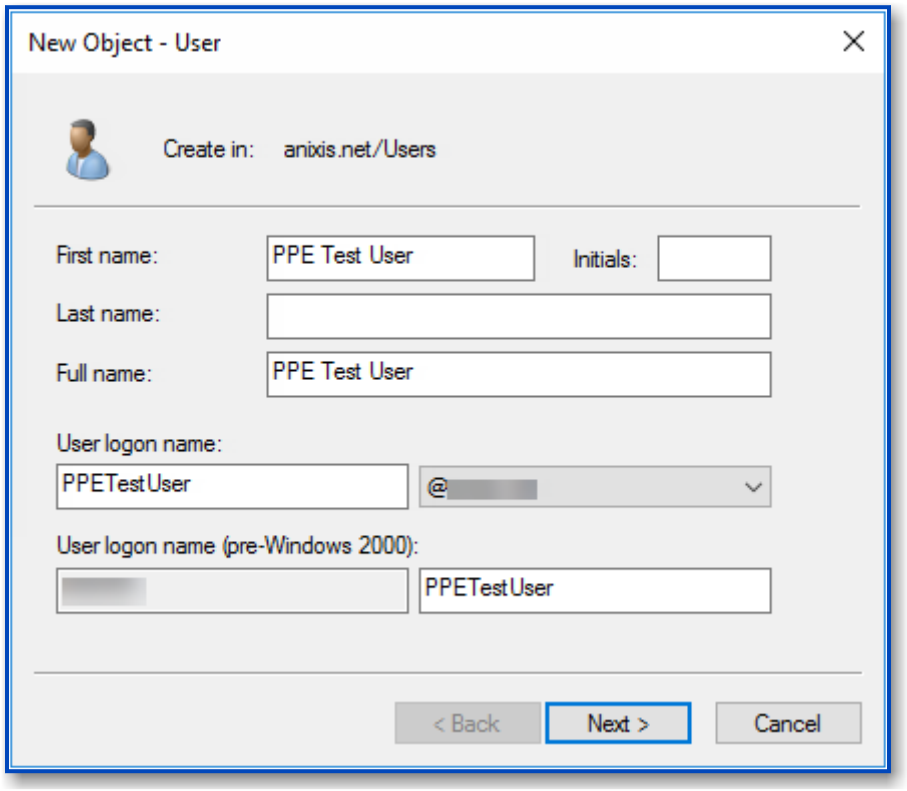
Step 7 – Close the **Group Policy Management Editor**.



Step 8 – Execute the `gpupdate/target:computer` command to refresh the Group Policy.

Create Test Accounts

Create two user accounts for the evaluation, **PPETestUser** and **PPETestAdmin**.



Make **PPETestAdmin** a member of the Domain Admins group if you are evaluating Password Policy Enforcer on a domain controller.

Install Password Policy Enforcer for Evaluation

The evaluation installation uses the standard installation packages:

- Server Installation: install on each server and domain controller in the domain you are evaluating. You can install manually using the procedure in Install Password Policy Enforcer on a Server or automatically with Install with Group Policy Management procedure. Installing Password Policy Enforcer does not extend the Active Directory schema. Be sure and install the **Configuration Console** feature on at least one server.

- Client Installation: install on each workstation you are evaluating. The Password Policy Client is an optional Password Policy Enforcer component to help users choose compliant passwords. Follow the Install Password Policy Enforcer Client procedure, or Install with Group Policy Management.

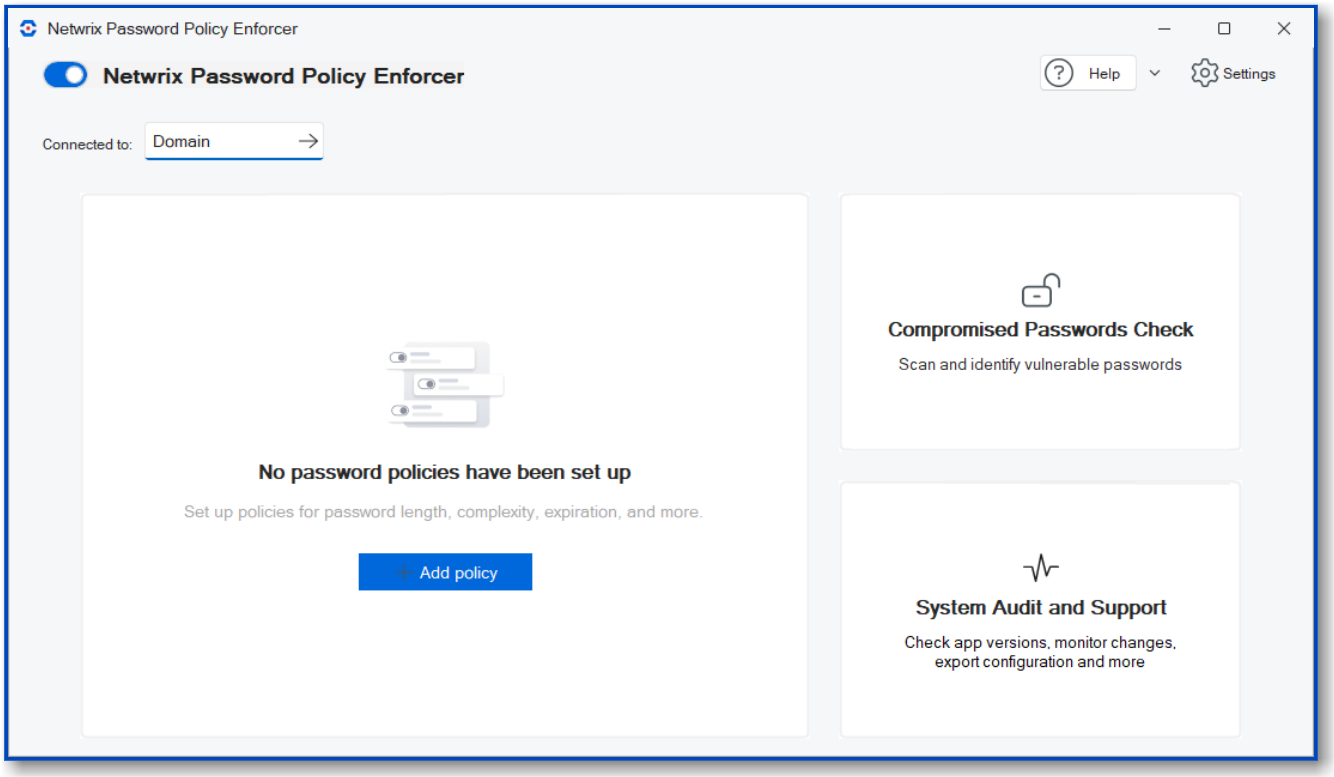
You may need to create a firewall port exception on the domain controllers if you are evaluating the Password Policy Client on a domain with client computers. See the Password Policy Client topic for additional information.

Create a Password Policy

There are no password policies defined when Password Policy Enforcer is first installed. You can now create your first Password Policy Enforcer password policy. Password Policy Enforcer accepts all passwords in this state, so users only need to comply with the Windows password policy rules (if enabled).

Step 1 – Open the Configuration Console:

Click **Start** > **Netwrix Password Policy Enforcer** > **PPE Configuration**or Double click the **PPE Configuration** desktop shortcut.



The Configuration Console dashboard shows **No password policies have been set up** when you are getting started with Password Policy Enforcer.

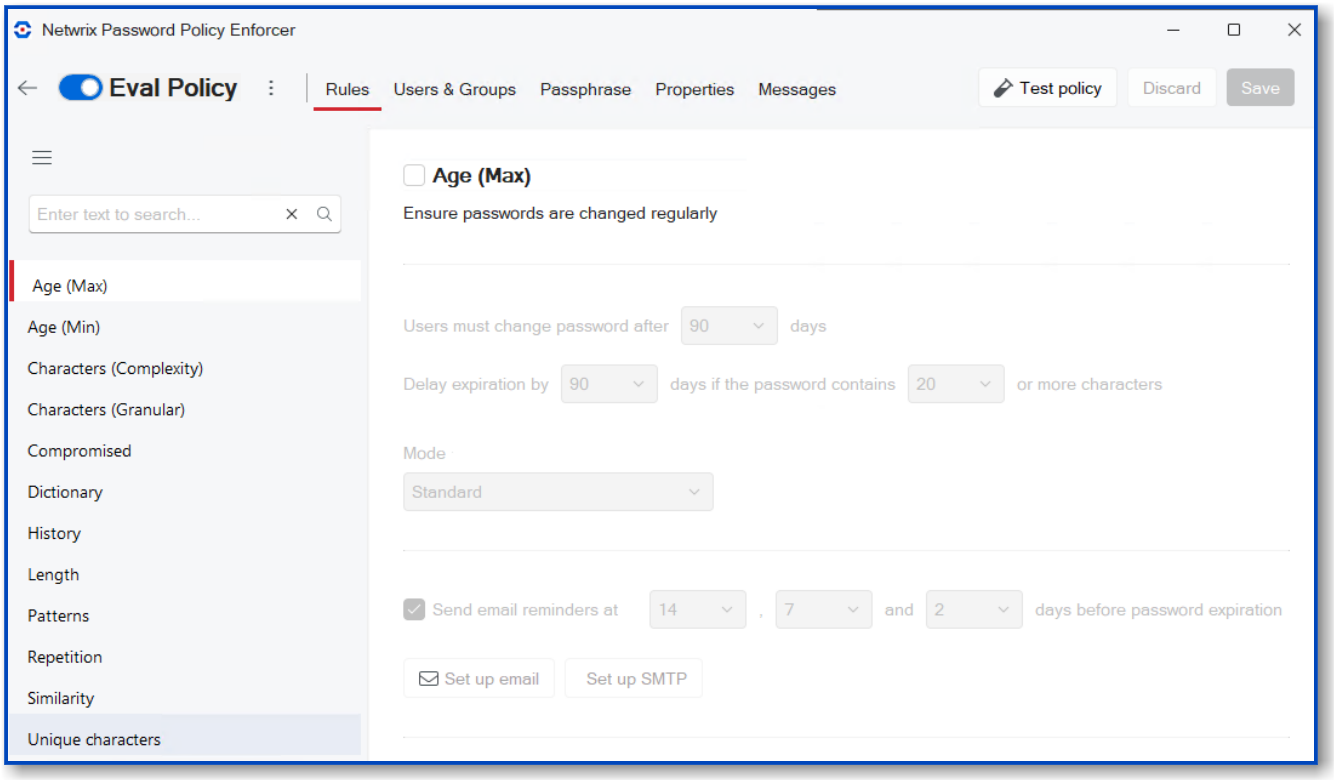
Step 2 – Click **Add policy**.

Step 3 – Enter a unique policy name. Maximum is 32 characters. **Eval Policy** is used for this example.

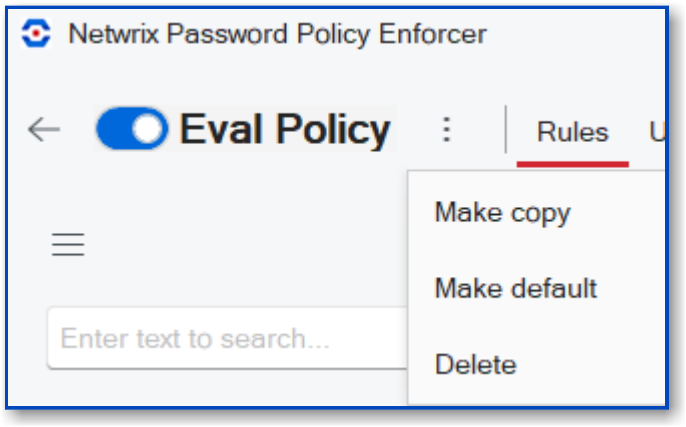
Step 4 – Select a Policy template or **None** if you are creating your own. For a list of policies see Policy Templates .

Step 5 – Click **Create policy**.

Your policy is created. The policy settings are opened, showing the first item on the **Rules** tab.



Step 6 – Click the context menu (beside the policy name and select **Make default**.



Policy Templates

Password Policy Enforcer contains Out-of-the-box Policy Templates based on the requirements of the most popular regulatory frameworks.

- Center for Internet Security (CIS) Password Policy Guide – See the CIS Password Policy Guide article for additional information.

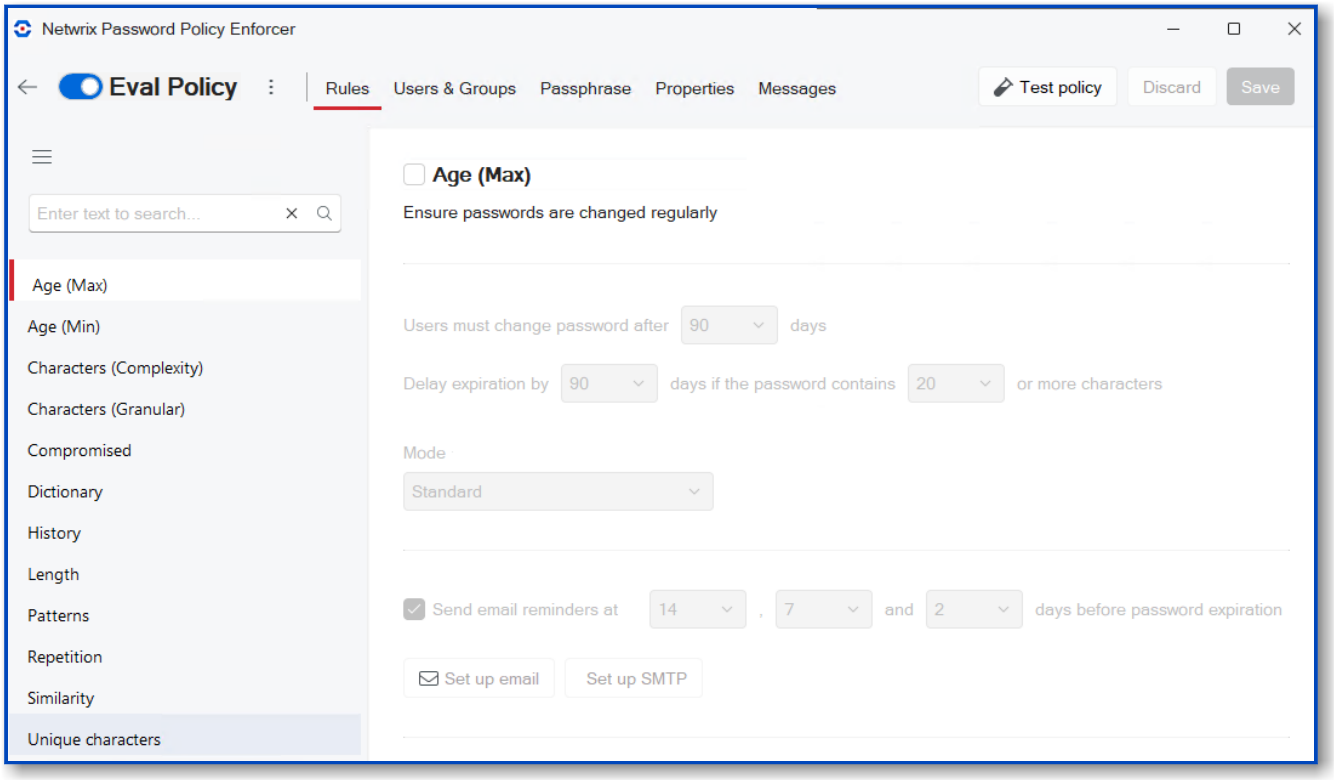
- Center for Internet Security (CIS) Password Policy Guide MFA – See the CIS Password Policy Guide article for additional information.
- Cybersecurity Information Sharing Act (CISA)
- Criminal Justice Information Services (CJIS) Security Policy
- Cybersecurity Maturity Model Certification (CMMC)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Gramm-Leach-Bliley Act (FedRAMP)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPPA) – HIPAA Security Rule requires that organizations must implement procedures for creating, changing, and safeguarding passwords.
    - It also recommends training the workforce on ways to safeguard password information and establish guidelines to create and change passwords in a periodic cycle.
    - HIPAA doesn't offer any specific password complexity guidelines. To comply with HIPAA, organizations are better off following NIST password guidelines.
    - Most of healthcare institutions use the NIST framework.
- International Organization for Standardization (ISO/IEC) 27002 – See the NIST Special Publication 800-63B article for additional information.
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) – See the CIP-007-6 — Cyber Security – Systems Security Management article for additional information.
- National Institute of Standards and Technology (NIST) Special Publication 800-171
- National Institute of Standards and Technology (NIST) Special Publication 800-53
- National Institute of Standards and Technology (NIST) Special Publication 800-63b – See the NIST Special Publication 800-63B article for additional information.
- Payment Card Industry Data Security Standard (PCI DSS) – See the PCI Document Library web site for additional information.
- Payment Card Industry Data Security Standard (PCI DSS) (version 4)

Configure Policy Rules

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

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

When you create a policy, the policy settings are opened. You can open the settings for a policy at any time by clicking the policy name on the Configuration Console dashboard.



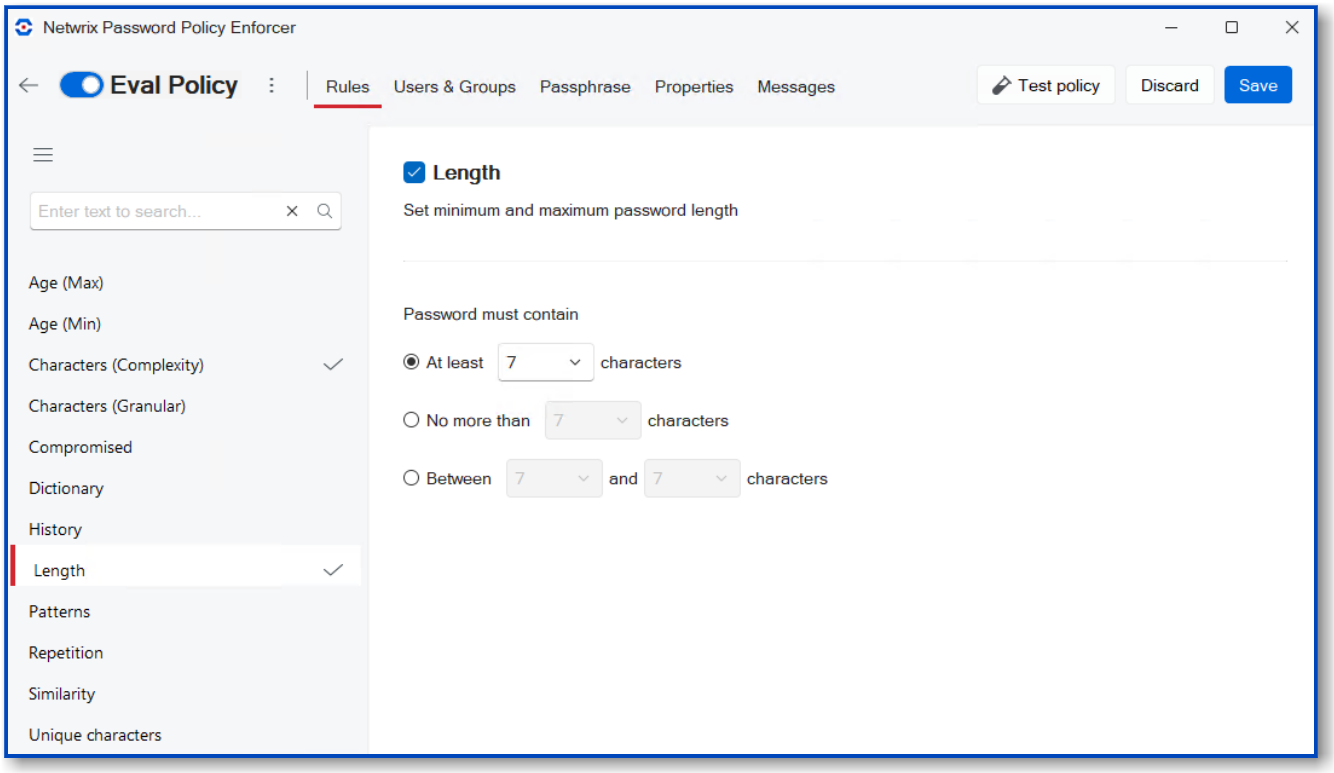
Requirement: Password must contain at least seven characters.

This condition is set with the **Length** rule.

Step 1 – Select **Length**.

Step 2 – Click the **Length** checkbox to enable the rule.

Step 3 – Select **7** for the **At least…** value. Depending on the template, this might be the default.



Requirement: Password must contain at least one lowercase alpha character.

This condition is set with the **Characters (Complexity)** rule.

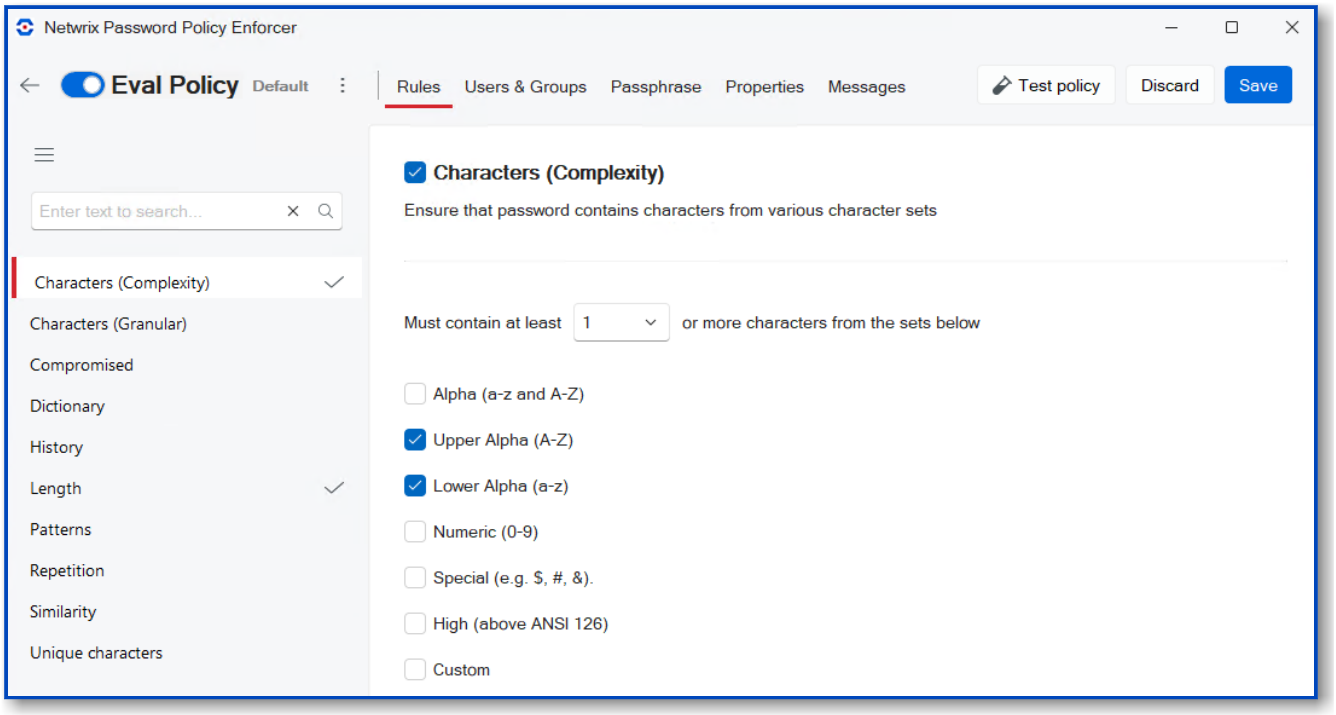
Step 1 – Select **Characters (Complexity)**.

Step 2 – Click the **Characters (Complexity)** checkbox to enable the rule.

Step 3 – Select **1** as the **Must contain at least…** value.

Step 4 – Select **Lower Alpha (a-z)**.

Step 5 – Select **Upper Alpha (A-Z)** for the next requirement while you are here.



Password must contain at least one uppercase character.

This condition is set with the **Characters (Granular)** rule.

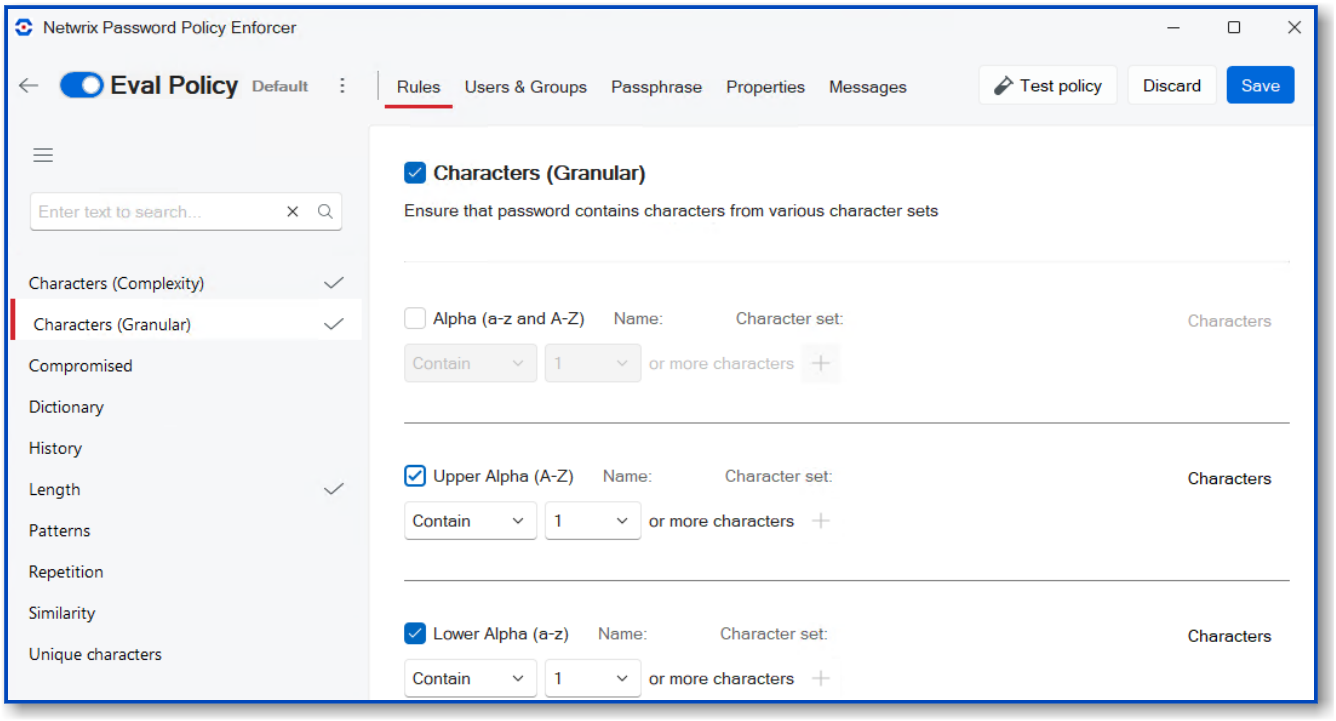
Step 1 – Select **Characters (Granular)**.

Step 2 – Click the **Characters (Granular)** checkbox to enable the rule.

Step 3 – Select **1** as the **Must contain at least...** value.

Step 4 – Select **Upper Alpha (A-Z) Contain 1** or more characters.

Step 5 – Select **Lower Alpha (a-z) Contain 1** or more characters.



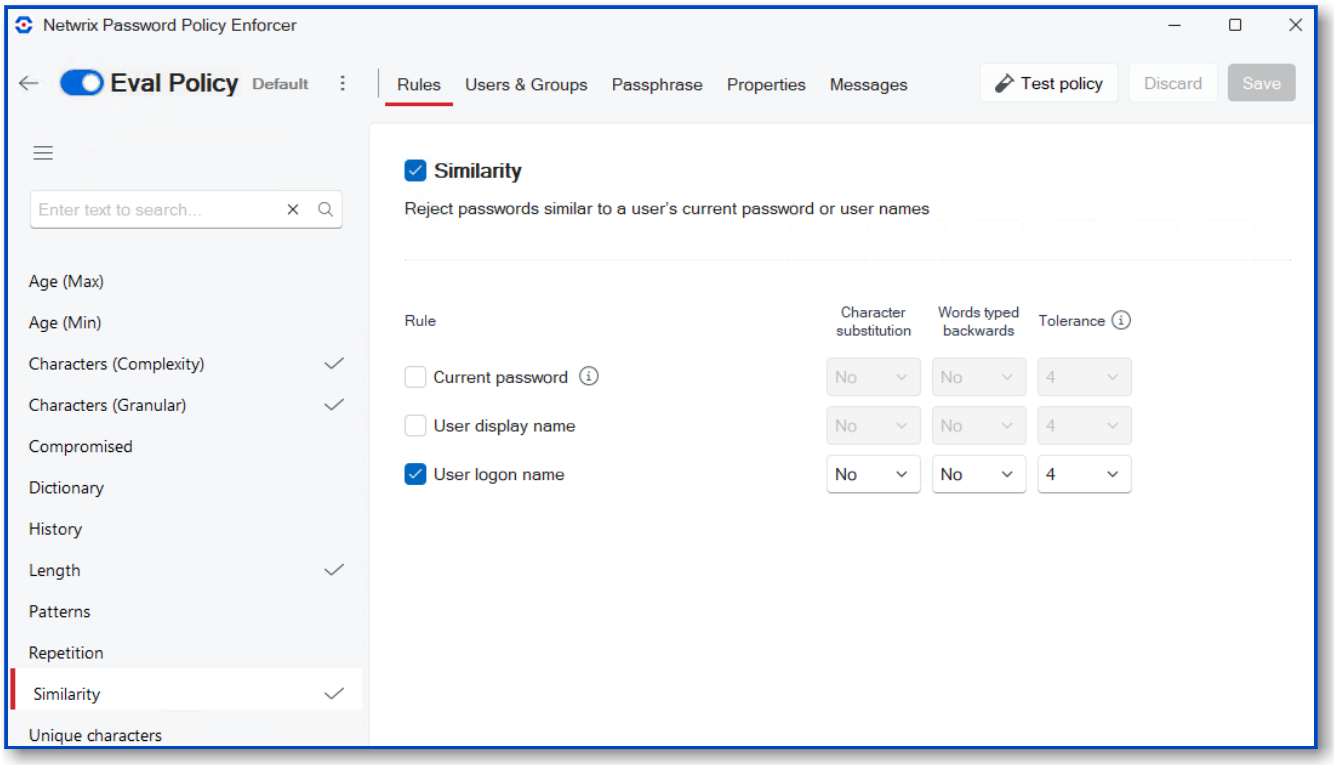
Requirement: Password must not be similar to the user's logon name.

This condition is set with the **Similarity** rule.

Step 1 – Select **Similarity**.

Step 2 – Click the **Similarity** checkbox to enable the rule.

Step 3 – Select **User logon name**.



Requirement: Password must not exist in a dictionary of common passwords.

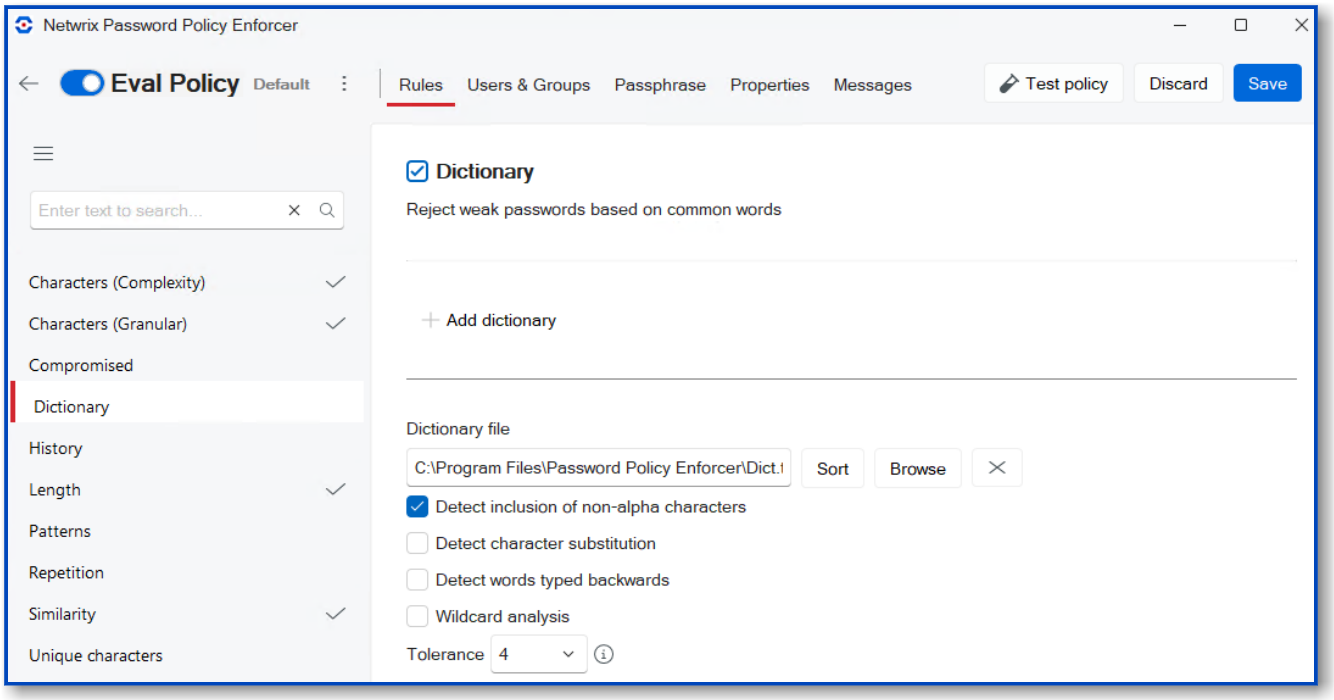
This condition is set with the **Dictionary** rule.

Step 1 – Select **Dictionary**.

Step 2 – Click the **Dictionary** checkbox to enable the rule.

Step 3 – Click **Browse**.

Step 4 – Navigate to **\Program Files\Password Policy Enforcer** folder and select**Dict.txt**.



When you have added all the rules, click **Save** to save your new policy.

Test the Password Policy

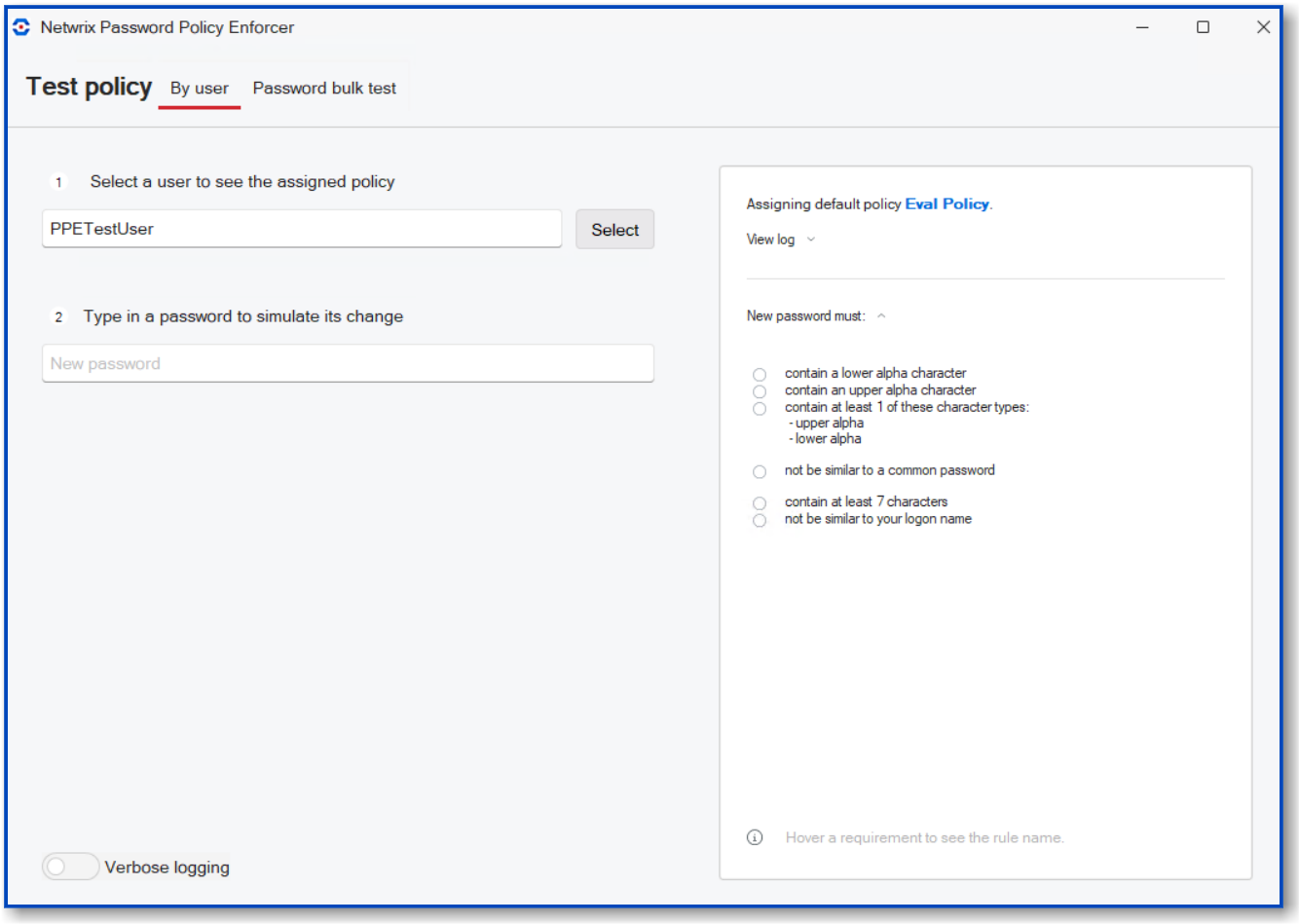
You can test the policy from the policy settings right where you are in the policy settings. You can also test it from the Password Policy Enforcer configuration console dashboard, the Windows Change Password screen, or the Active Directory Users and Computers / Local Users and Groups consoles.

Configuration Console

Test policy is available in the policy settings and on the configuration console dashboard. This option shows you the most information about the policy.

Step 1 – Click **Test policy**.

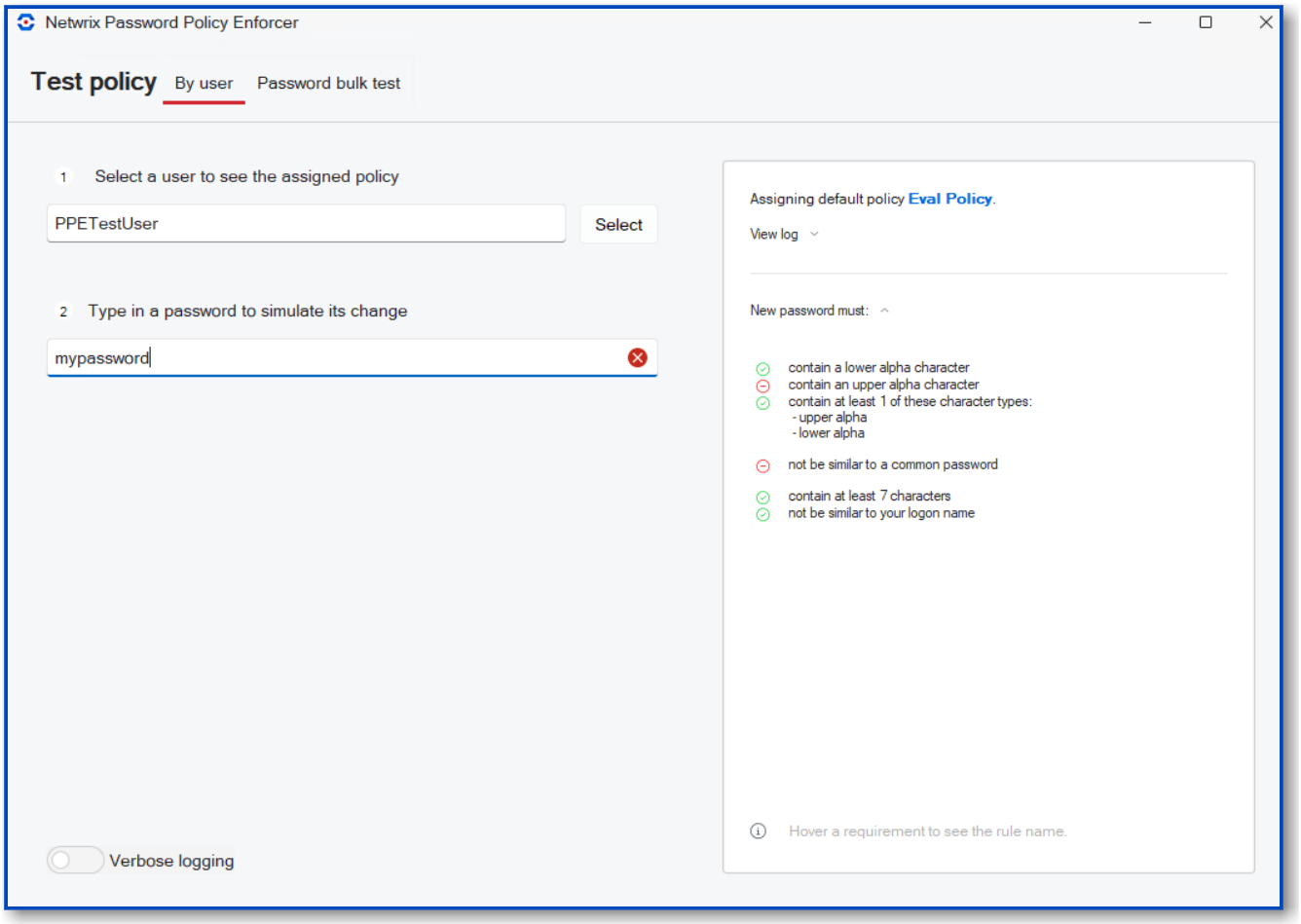
Step 2 – Select the **PPETestUser** you created. The details pane displays the policy applied to the selected user.



Step 3 – Enter a password to test.

The Password Policy Enforcer configuration console tests the password by simulating a password change, but it does not change the user's password. A green check mark indicates the password complies, a red and white x indicates the password fails. Detailed test results appear in the results pane.

mypassword fails two requirements. You can hover over the requirements to view the associated rule.



Click **View log** to expand Password Policy Enforcer's internal event log. The information in the event log can help you to understand why Password Policy Enforcer accepted or rejected a password.

NOTE: Policy testing simulates a password change, but it may not always reflect what happens when a user changes their password. See the Policy Testing vs. Password Changes topic for additional information.

Windows Change Password Screen

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

From the Windows Change Password screen:

Step 1 – Press **CTRL + ALT + DEL**.

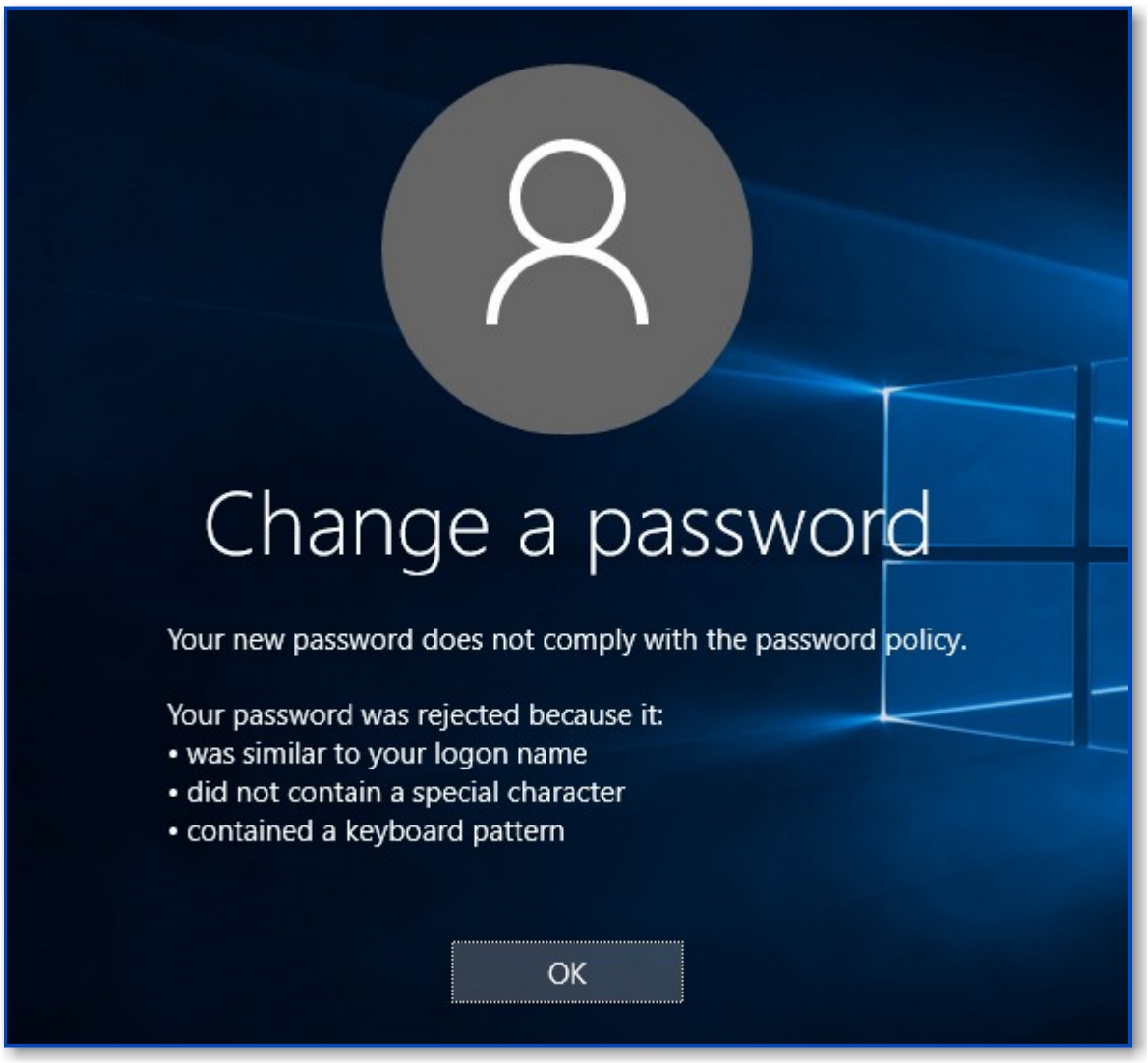
Step 2 – Click the **Change a password** option.

Step 3 – Enter a user name in the User name text box.

Step 4 – Enter passwords in the Old Password, New Password, and Confirm Password text boxes.

Step 5 – Click the **submit arrow**.

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



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

Active Directory Users / Computers Console and local Users and Groups Console

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

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

Password Policy Enforcer can enforce the password policy for both password changes and password resets. It does this by default, but you can configure it to only enforce the password policy for password changes. The Minimum Age rule is never enforced when a password is reset.

Follow the steps below to test password policies from these consoles.

Step 1 – Open the appropriate console:

- If Password Policy Enforcer is enforcing a domain policy, open the Active Directory Users and Computers console
- If Password Policy Enforcer is enforcing a local policy, open the Local Users and Groups console

Step 2 – Right-click a user, then click **Reset Password**.

Step 3 – Enter a password in the **New password** and **Confirm password** text boxes.

Step 4 – Click **OK**.

NOTE: These consoles do not explain why a password was rejected. Use the Password Policy Enforcer configuration console, or the Change Password screen with the Password Policy Enforcer Client installed to see this information.

Here are some sample passwords and expected test results when the Users policy is enforced. Try to change the password for the PPETestUser account to confirm that Password Policy Enforcer is enforcing the password policy correctly.

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

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

- tseTEPP is part of the user logon name with the characters reversed

- kravdraA is Aardvark with the characters reversed
- Aardv@rk is Aardvark with an @ substituting an "a."

These three passwords are only marginally stronger than the rejected passwords. The next section shows you how to improve the password policy so Password Policy Enforcer rejects these passwords.

NOTE: Contact Netwrix support if Password Policy Enforcer is not working as expected. We can help you resolve the problem.

Improve the Password Policy

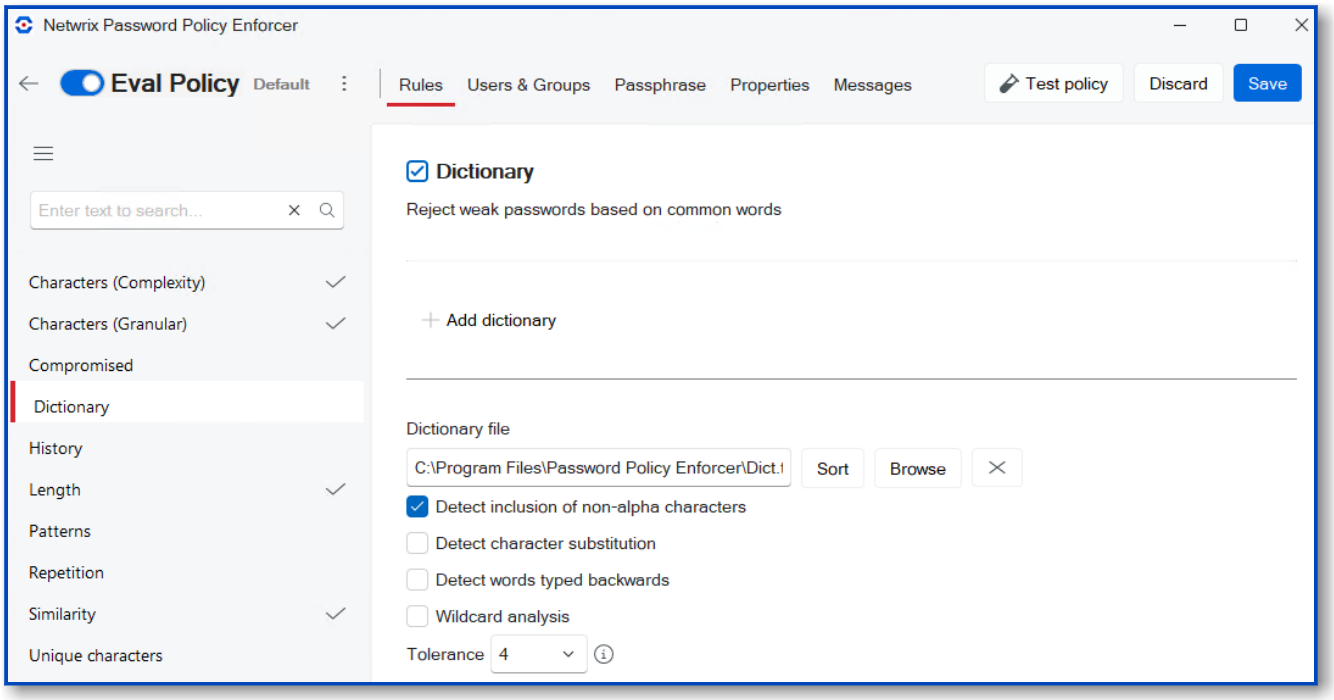
Password Policy Enforcer rules have properties that control how rules are enforced. You can improve the effectiveness of the Users policy by enabling character substitution detection and bi-directional analysis (words typed backwards) for the **Similarity** and **Dictionary** rules.

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

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

Click on your policy name on the Configuration Console dashboard if needed.

Step 1 – Open the **Dictionary** rule.



Step 2 – Select the **Detect character substitution** and **Detect words typed backwards** check boxes.

Step 3 – Open the **Similarity** rule.

Step 4 – For **User logon name** select **Yes** for **Character substitution** and **Words typed backwards**.

Step 5 – Click **Save**.

Test the improved policy with passwords that were accepted under the previous policy. Password Policy Enforcer should reject all of them.

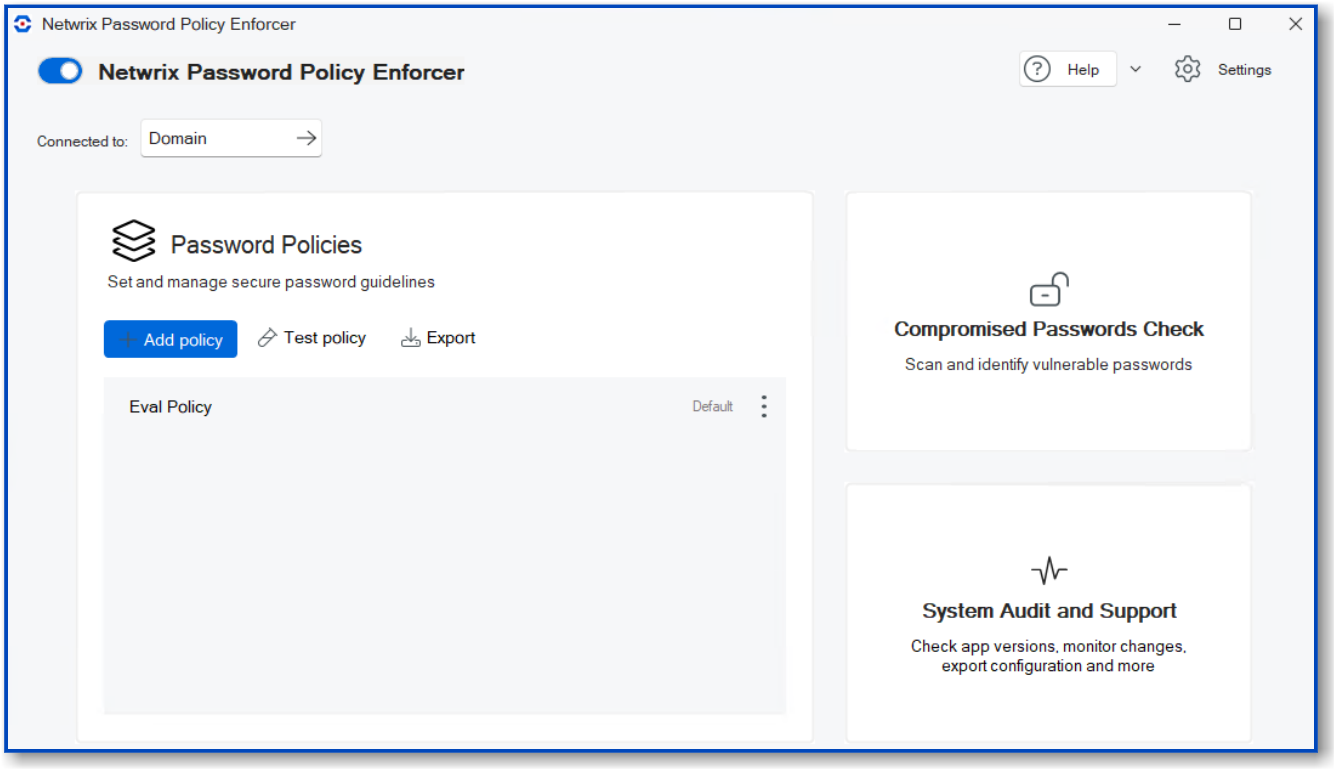
Password	Result	Reason
tseTEPP	Rejected	Similar to user logon name
kravdraA	Rejected	Similar to word in dictionary file
Aardv@rk	Rejected	Similar to word in dictionary file

Enforce Multiple Policies

Password Policy Enforcer can enforce up to 256 password policies on each domain or computer. You can assign policies to users directly, or indirectly through Active Directory security groups and containers (Organizational Units).

Create Additional Password Policy

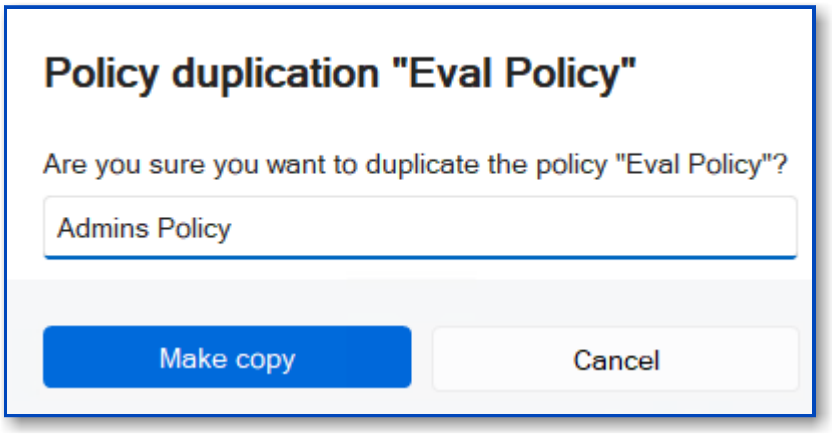
If you are in the settings for your first policy, click the left arrow beside the policy name to return to the Configuration Console dashboard.



Create an additional password policy.

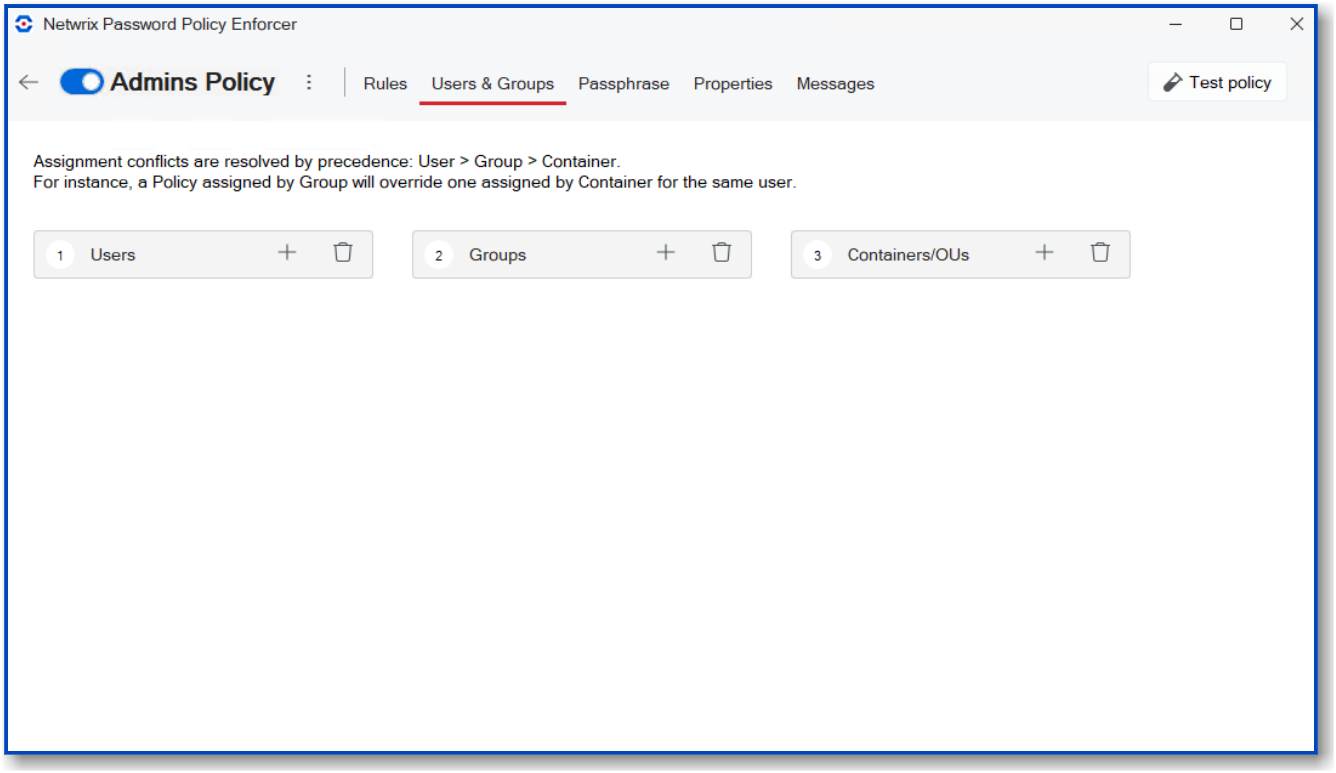
Step 1 – Click the context menu beside your first policy and select **Make copy**.

Step 2 – Enter **Admins Policy** for the Policy duplication.



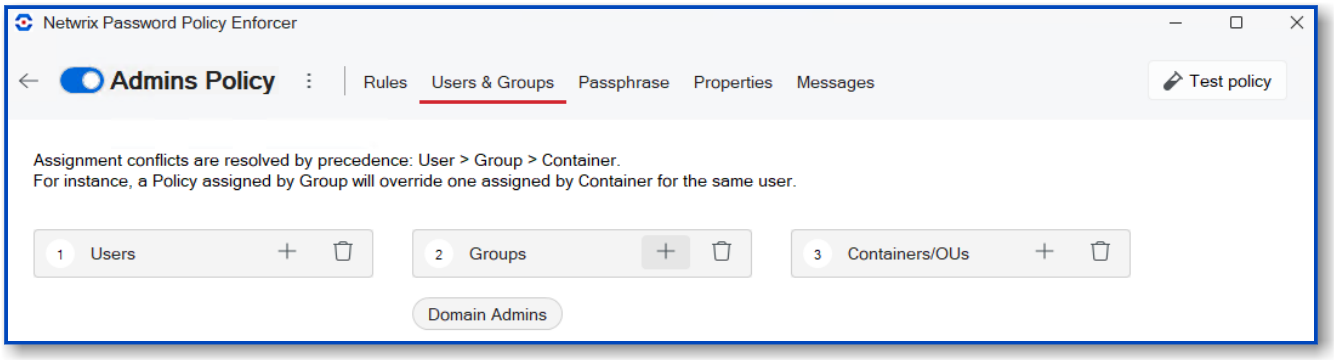
Step 3 – Click **Make copy**.

Step 4 – Open the **Users & Groups** tab.



Step 5 – Click the **+** in the **Groups** list and enter **Domain Admins**. Specify a Domain or local **Location** depending on your evaluation set up.

Step 6 – Click **OK**. Domain Admins are added to the **Groups**.



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

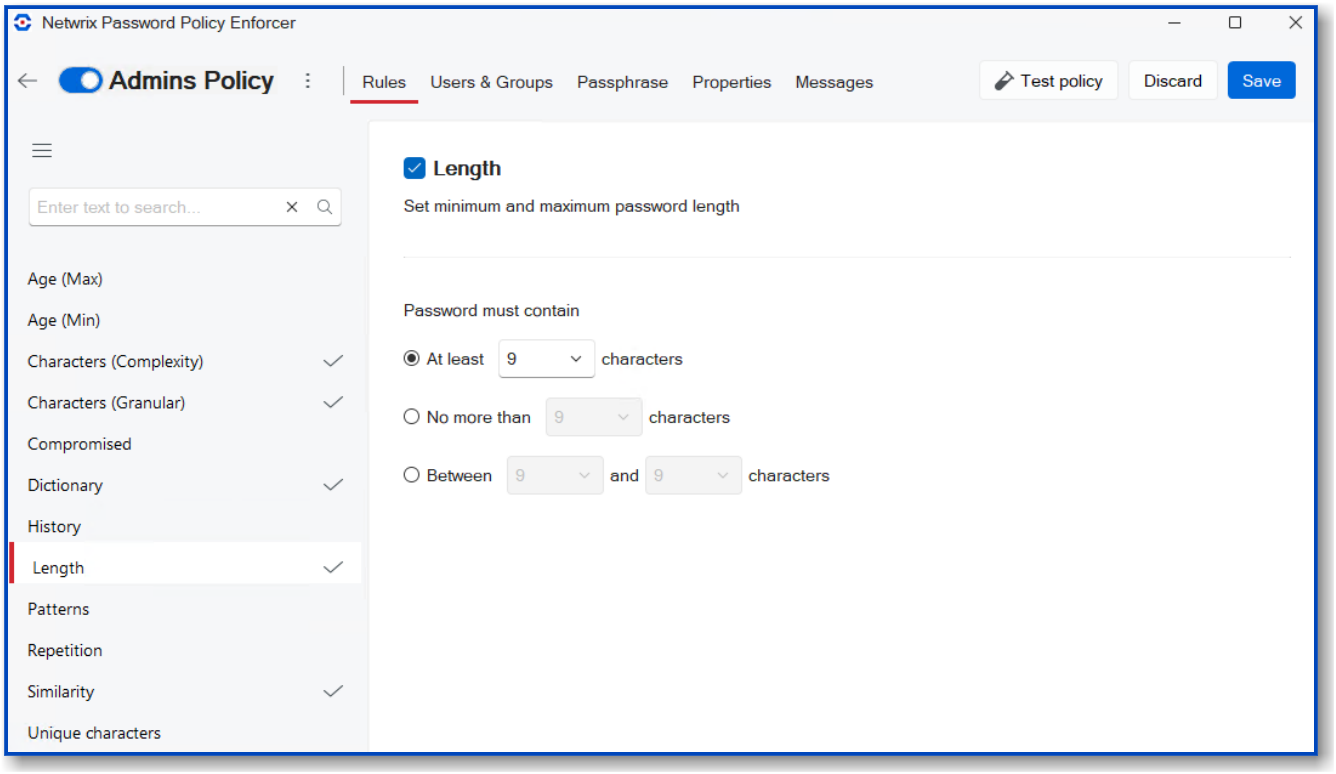
Differentiate Password Policies

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

Step 1 – Open the **Rules** tab.

Step 2 – Open the **Length** rule.

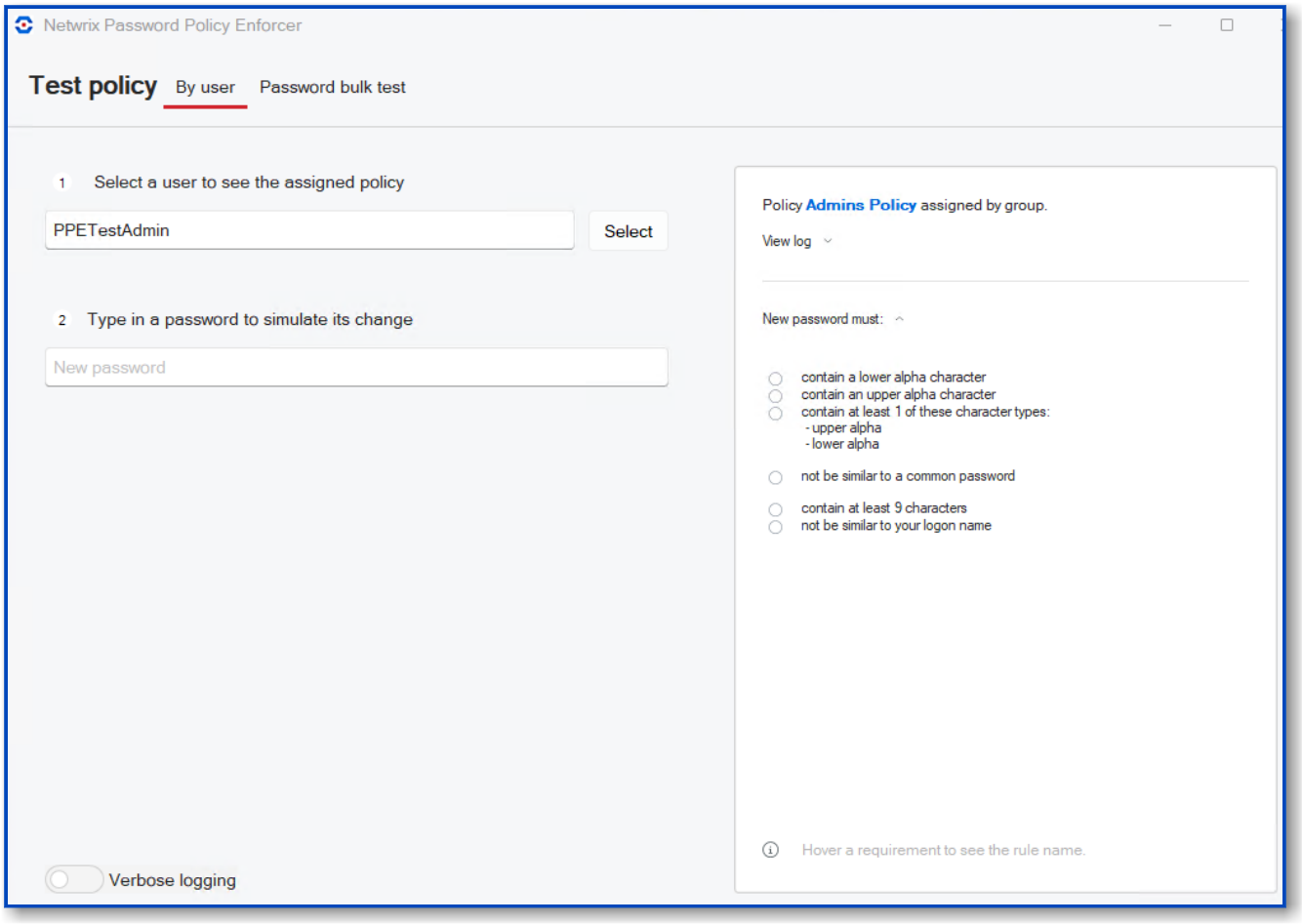
Step 3 – Select **9** from the **At Least** drop-down list.



Step 4 – Click **Save**.

Step 5 – Click **Test policy**.

Step 6 – Select the **PPETestAdmin** user. The results pane shows the **Admins Policy** is being applied, and the password must **contain at least 9 characters**.



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

NOTE: The Set Priorities topic contains more information about policy assignments, and how Password Policy Enforcer resolves policy assignment conflicts that occur when more than one policy is assigned to a user.

Conclusion

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

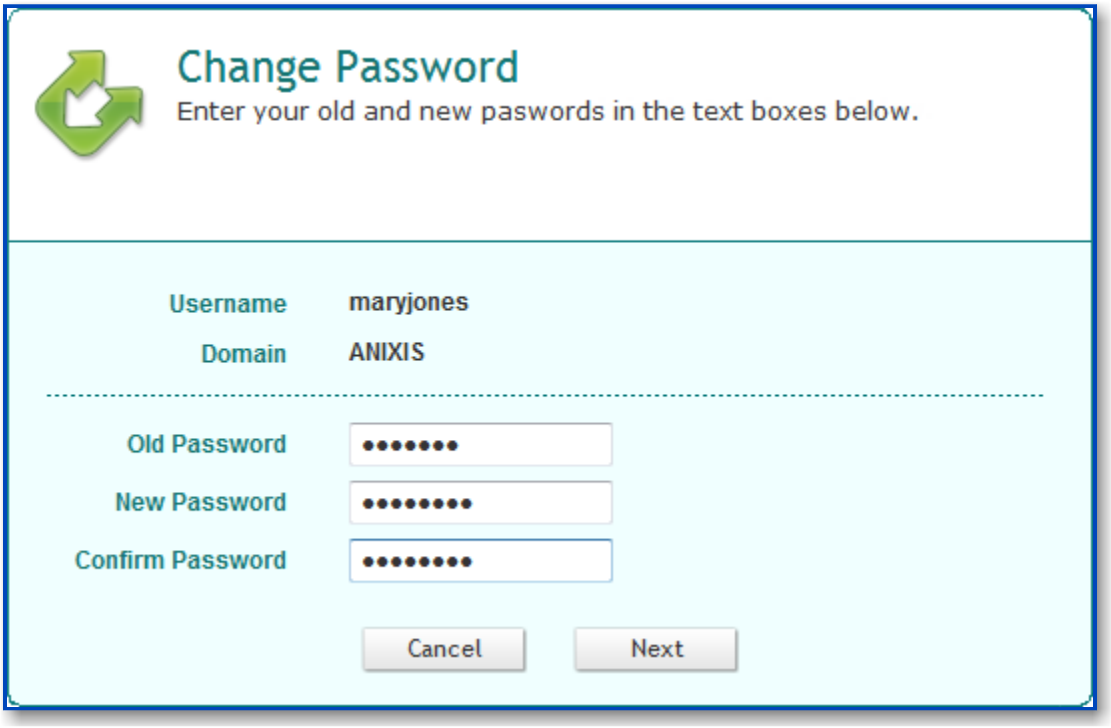
The Password Policy Enforcer Web application enables users to securely manage their passwords from a web browser, ensuring passwords comply with the password policy, and helping users choose compliant passwords.

Password Policy Enforcer Web

Password Policy Enforcer Web enables users to change their Windows domain password from a web browser. It can optionally integrate with Password Policy Enforcer to enforce customizable password policies and help users set compliant passwords.

Download Password Policy Enforcer Web:

Password_Policy_Enforcer_WEB_7.11.zip



Password Policy Enforcer Web communicates directly with the domain controllers, so it works best when both the web server and domain controllers are on the same network. If you need to put the web server in a DMZ for extra security, then consider using Netwrix Password Reset instead of Password Policy Enforcer Web.

Password Reset also allows users to change their password from a web browser, but it has many other features including the ability to work in a DMZ without any domain controllers. Use Password Reset if you need to:

- Allow users to reset a forgotten password or unlocked their account by answering questions about themselves, such as their date of birth, first pet's name, etc. Users can access APR from the web browser, or from the Windows Logon and Unlock screens if the APR Client is installed.

- Send e-mail alerts to users whenever their account is used in the password management system.
- Keep a detailed, searchable audit log of all user activity.
- Separate the web server from he internal network for extra security.

See the Netwrix Help Center page for documentation on the Password Reset product.

What's New

User Interface

- Displays a diagnostic message if the Password Policy Enforcer does not respond to a request. This is likely to happen if a domain controller is not running Password Policy Enforcer, or if a firewall is blocking access to the PPS port.

Compatibility

- Compatible with Windows Server 2012 and 2012 R2 (as well as Windows Server 2003, 2003 R2, 2008, and 2008 R2).
- Improved Setup Wizard to ensure that PPEWeb.dll is always added to the list of Web Service Extensions on Windows 2003 and 2003 R2 64-bit editions.

Other

- Uses the Password Policy Enforcer V7.x libraries for improved compatibility with new features in recent version of Password Policy Enforcer.
- The Configuration Console prompts for elevation to ensure that user has sufficient permissions to write configuration settings.
- Imports PPE Web V6.x configuration settings. See the Install Password Policy Enforcer Web topic for additional information.

NOTE: PPE Web V7.11 integrates with Password Policy Enforcer V7.0 or later. Disable Password Policy Enforcer integration in the PPE Web Configuration console if you need to use PPE Web with an older version of Password Policy Enforcer.

New in PPE Web V6.x (Previous Version)

User Interface

- Updated HTML Templates allow customization of all user interface elements including error messages.
- The Password Policy Enforcer policy message is now shown during password changes. Earlier version of PPE Web had this message hard-coded in the HTML template.
- A Configuration console to configure system setting and instal license keys.
- The Setup Wizard installs and configures PPE Web without the manual setup steps from earlier versions.

Compatibility

- Compatible with Windows Server 2008 and 2008 R2 (as well as Windows Server 2003 and 2003 R2).
- Compatible with 64-bit and 32-bit Windows editions.

Other

- Additional validation of all user input to improve security.
- Can get user and domain names from URL parameters.
- Uses the Password Policy Enforcer V6.0 libraries for improved compatibility with new features in recent versions of Password Policy Enforcer.
- Can be used without Password Policy Enforcer if Password Policy Enforcer's additional password policy controls are not needed.

NOTE: PPE Web V6.0 integrates with Password Policy Enforcer V6.0 or later.

Install Password Policy Enforcer Web

Password Policy Enforcer Web V7.11 is a web server enabling users to change their Windows domain password from a web browser. Review the Requirements prior to running the installation.

Click the following link to download Password Policy Enforcer Web:

Password_Policy_Enforcer_WEB_7.11.zip

The PPE Web Setup Wizard

The Setup Wizard copies the required files onto the server and configures IIS to run the Password Policy Enforcer Web application.

Follow the steps below to install PPE Web.

Step 1 – Start the Password Policy Enforcer Web Setup Wizard (PPEWeb711.exe).

Step 2 – If another version of Password Policy Enforcer Web is detected, the Setup Wizard may required older files to be backed up. Back up these files if the original files have been modified. Click **Next**.

Step 3 – Click **Next**.

Step 4 – Read the License Agreement. Click **I accept the terms of the license agreement**, then click **Next** if you accept all the terms.

Step 5 – Click **Browse...** if you want to choose a different folder for the Password Policy Enforcer Web documentation and tools, then click **Next**.

Step 6 – Select an **IIS Web Site** from the dropdown. Change the default Virtual Directory, if needed.

NOTE: Password Policy Enforcer Web should be installed in its own virtual directory.

Step 7 – Click **Next** twice.

Step 8 – Wait for Password Policy Enforcer Web to install, then click **Finish**.

Upgrading from PPE Web V7.x

Some planning is needed to ensure a smooth upgrade from PPE Web V7.x. A trial run on a lab network is recommended.

Before You Begin

The HTML templates and associated images are overwritten during an upgrade. You must back up and customized HTML templates and images before upgrading. The HTML templates and images are installed in the `\Inetpub\wwwroot\ppeweb\` folder by default.

NOTE: A full backup of the PPE Web server is recommended. This allows you to roll back to the previous version if the upgrade cannot be completed. You may need to restart Windows after upgrading.

CAUTION: PPE Web V7.11 is only compatible with Password Policy Enforcer V7.0 and later. Upgrade PASSWORD POLICY ENFORCER to a compatible version if you have enabled Password Policy Enforcer integration.

Upgrading to V7.11

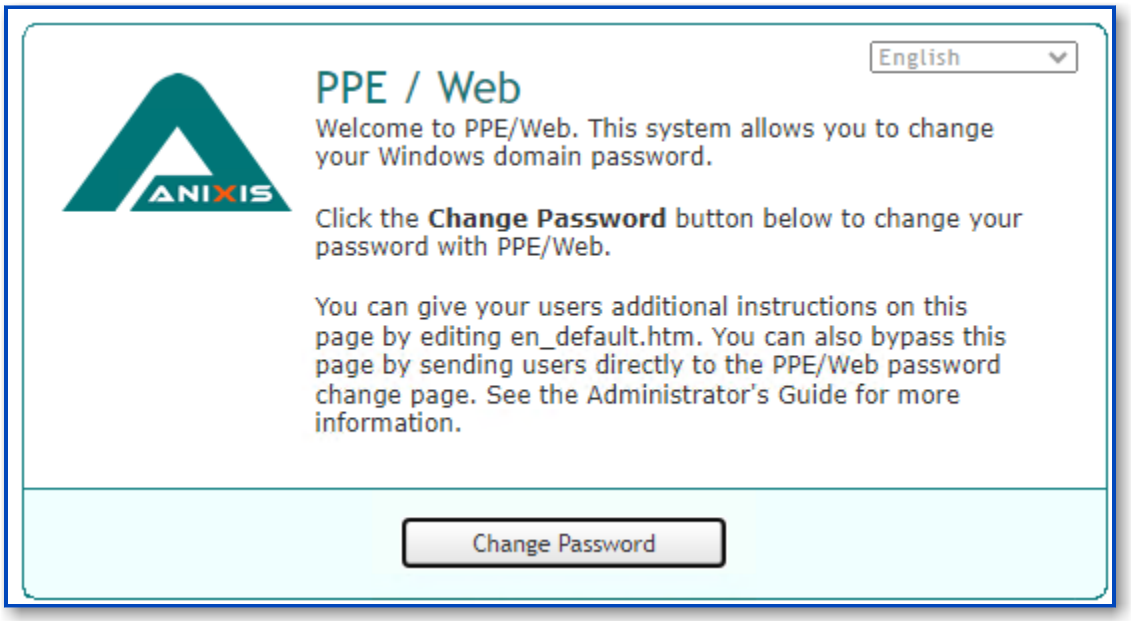
Step 1 – Start the PPE Web Setup Wizard and follow the prompts. The Setup Wizard uninstalls the previous version. There is no need to manually uninstall previous versions.

Step 2 – Restore any customized HTML templates and images after upgrading. Do not restore PPEWeb.dll from the backup as it belongs to the previous version.

Launch Password Policy Enforcer Web

The default URL for Password Policy Enforcer Web is: `http://[server]/ppeweb/`

Where [server] is the name or IP address of the server hosting Password Policy Enforcer Web.



The default page is called the Welcome page. You can customize the information on this page by editing **en_default.htm**, or you can bypass this page and send users directly to the Password Change page:

`http://[server]/ppeweb/ppeweb.dll`

You can also include the username and/or domain in the URL:

`http://[server]/ppeweb/ppeweb.dll?username=maryjones&domain=ANIXIS`

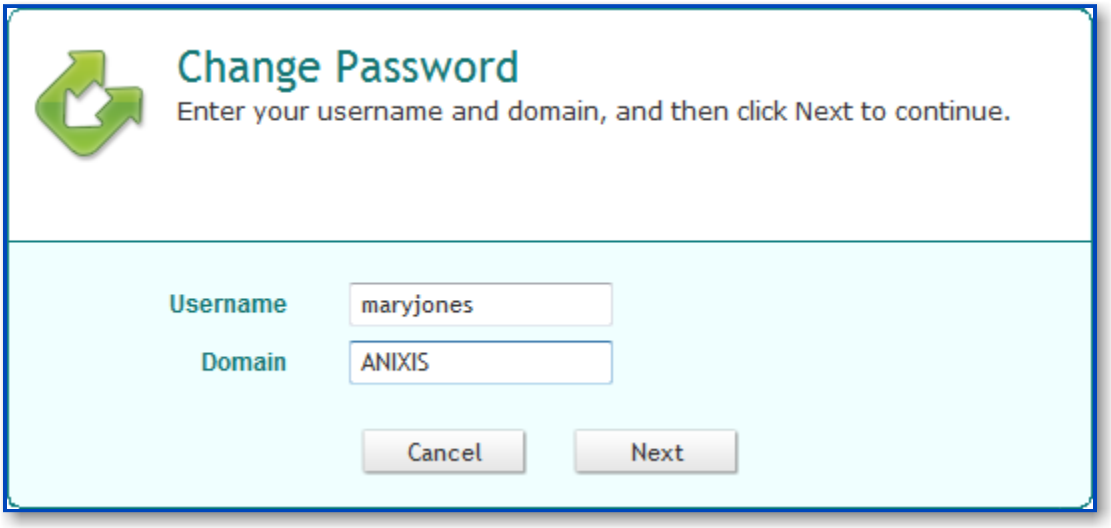
RECOMMENDED: Install the SSL Certificate the web server and use the HTTPS protocol if Password Policy Enforcer Web will be used on an unencrypted network. See the Install an SSL Certificate topic for additional information.

NOTE: A license reminder message is shown occasionally when Password Policy Enforcer Web is used without a license key. Contact Netwrix support if you would like to evaluate Password Policy Enforcer Web without the reminder message.

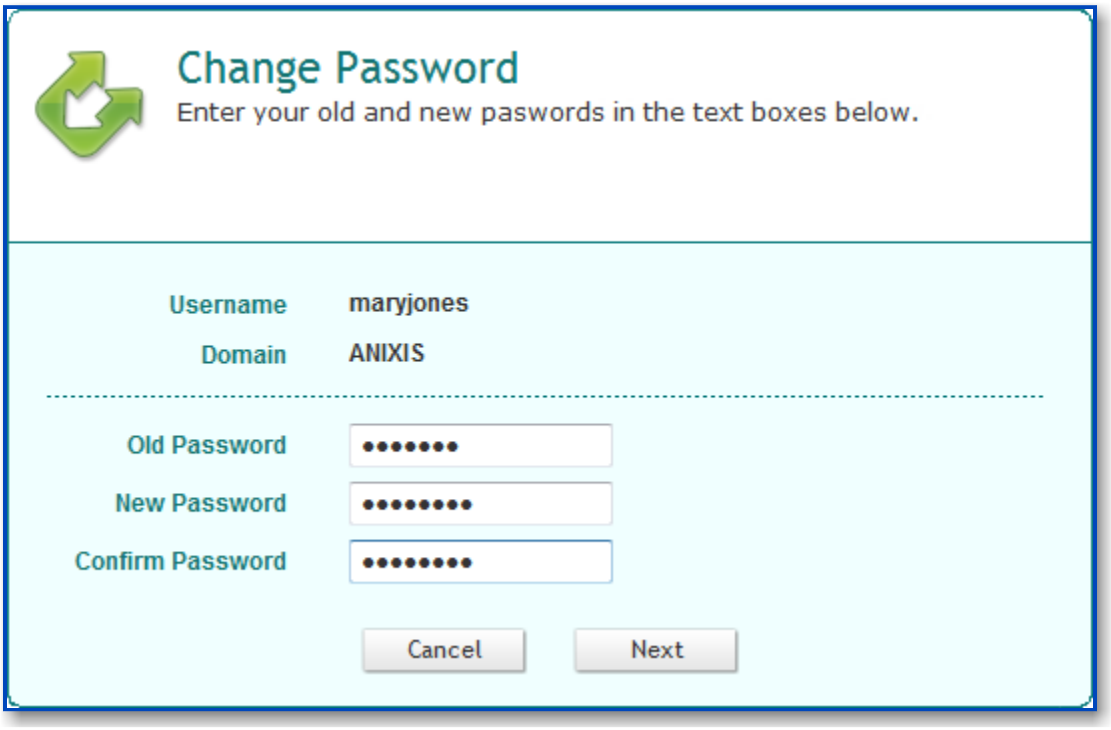
Change Password

To change a password with Password Policy Enforcer Web:

Step 1 – Click **Change Password** on the Welcome page.



Step 2 – Enter a **Username** and **Domain**, then click **Next**.

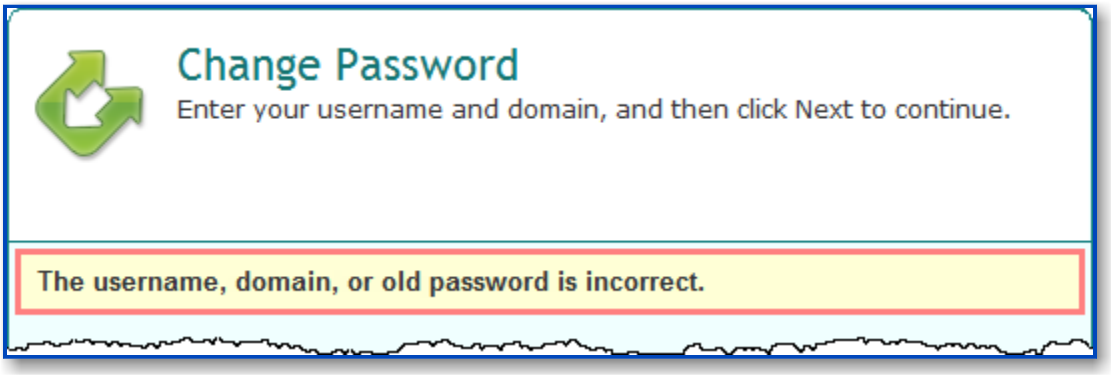


Step 3 – Enter the **Old Password**, **New Password**, and **Confirm Password**, then click **Next**.

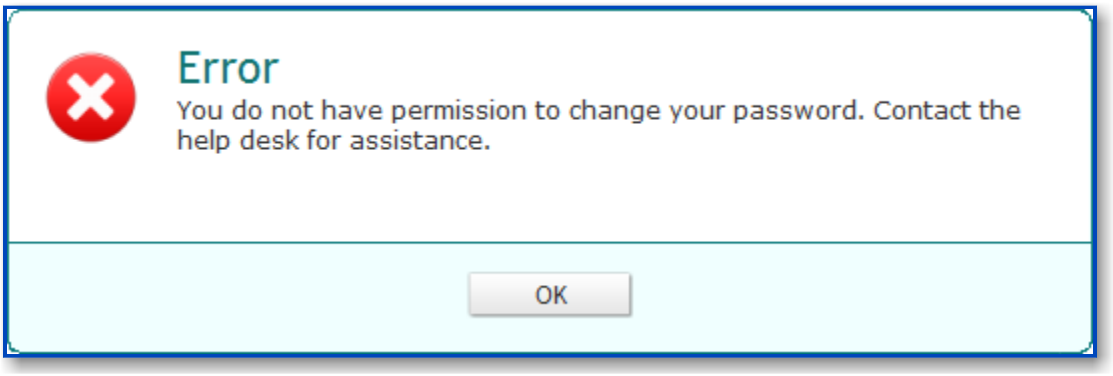
NOTE: Windows increments the bad password count in Active Directory every time a user enters their old password incorrectly. This may trigger a lockout if the Windows account lockout policy is enabled.

Error Messages

Validation errors are shown in a yellow box below the page instructions. Validation errors are normally caused by invalid user input. They can often be overcome by changing the value of one or more input fields and resubmitting the form.



Critical errors are shown on their own page. These errors are mostly a result of configuration or system errors. Users can sometimes overcome a critical error by following the instructions in the error message, but most critical errors are beyond the user's control.



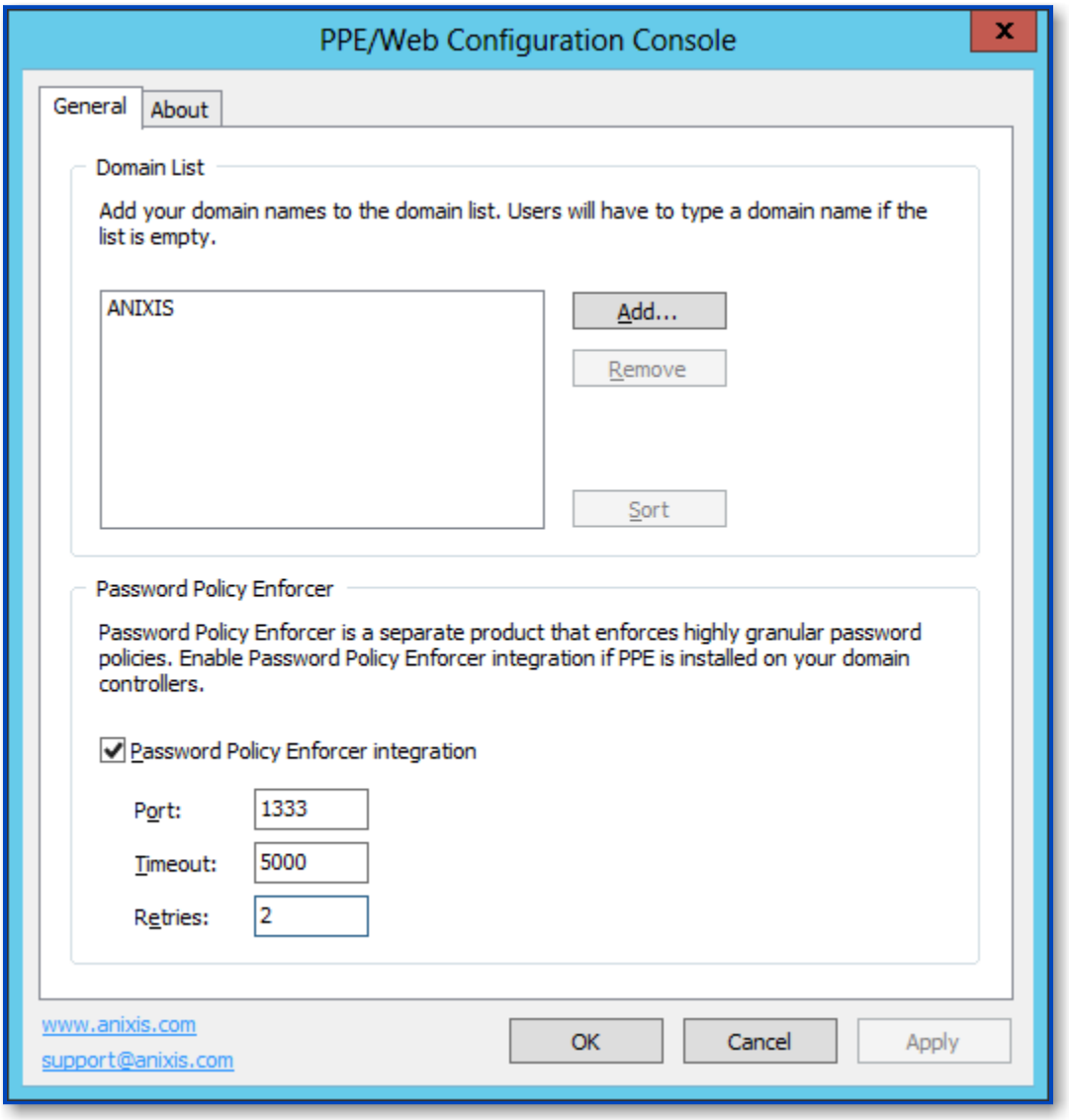
Validation and critical error messages are stored in the HTML templates. You can modify the default messages by editing the templates. See the Edit HTML Templates topic for additional information.

Configuration

Click **Start** >**[All] Programs** > **PPE Web Configuration Console** to open the Password Policy Enforcer Web Configuration Console.

General Tab

Use the General tab to maintain the list of managed domains, and to configure Password Policy Enforcer integration. See the Password Policy Enforcer topic for additional information.



Domain List

When Password Policy Enforcer Web is first installed, the Domain List is empty and users must type their domain name. You can configure Password Policy Enforcer Web to display a list of domains instead of an empty text box.

Add Domain

Follow the steps below to add a domain to the list.

Step 1 – Click the **Add...** button.

Step 2 – Enter a NetBIOS (NT Compatible) or DNS domain name.

Step 3 – Click **OK**, the click **Apply**.

NOTE: The most frequently used domain should be first in the list as it will be the default. You can rearrange the domains by dragging them to another position. You can also click **Sort** to sort them alphabetically.

Remove Domain

Follow the steps below to remove a domain from the list.

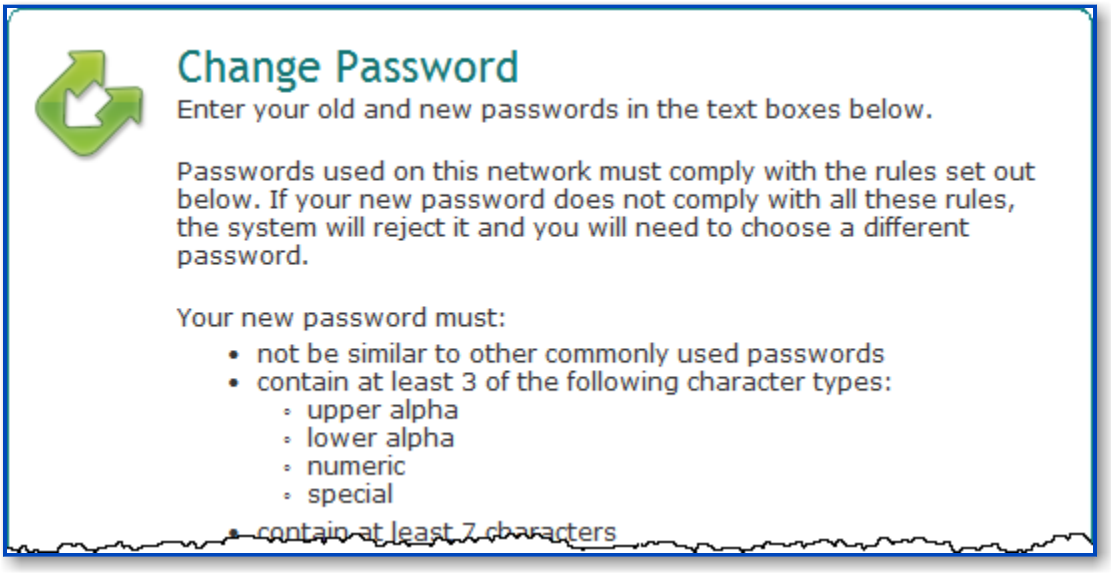
Step 1 – Select the domain name from the Domain List.

Step 2 – Click **Remove**, then click **Yes** when asked to confirm.

Step 3 – Click **Apply**.

Password Policy Enforcer

Password Policy Enforcer is a configurable password filter that enforces granular password policies with many advanced features. Password Policy Enforcer Web can integrate with Password Policy Enforcer to help users choose a compliant password.



Password Policy Enforcer Web displays the Password Policy Enforcer password policy message when a user is prompted for their new password, and the Password Policy Enforcer rejection message if the new password does not comply with the password policy. Select the **Password Policy Enforcer integration** check box if you have installed and configured Password Policy Enforcer on your domain controllers.

You can also set the Port, Timeout, and number of Retries for the Password Policy Protocol if the defaults are not suitable.

NOTE: A Password Policy Enforcer Web license does not include a Password Policy Enforcer license. Go to netwrix.com/password_policy_enforcer to learn more about Password Policy Enforcer.

About Tab

The **About** tab contains version and license key information.

To install a new license key.

Step 1 – Copy the entire license e-mail to the clipboard.

Step 2 – Click **Get license from clipboard**.

Step 3 – Click **Apply**.

Secure Password Policy Enforcer Web

Password Policy Enforcer Web is designed to operate securely, but you must ensure that the web server is also secure. Follow Microsoft's recommendations to secure the web server, and always install and use an SSL certificate if Password Policy Enforcer Web will be used on an unencrypted network.

Install an SSL Certificate

Password Policy Enforcer Web sends passwords to the domain controllers over a secure connection, but you need to set up SSL (Secure Sockets Layer) encryption for the connection between the web browser and the web server.

CAUTION: Do not use PASSWORD POLICY ENFORCER Web on a production network without SSL encryption.

You can use a self-signed certificate, but most organizations purchase certificates from a certificate authority. This is a recurring cost, and you will need to complete forms for the certificate authority to verify your identity. You can install Password Policy Enforcer Web on a server that already has an SSL certificate if you would rather not purchase another one.

The IIS documentation explains how request, install, and use SSL certificates.

See the Configure Server Certificates in IIS 7 Microsoft knowledge base article for additional information.

Ensure that users only access Password Policy Enforcer Web over an encrypted connection after the SSL certificate is installed. The URL should start with https://. Web browsers can be redirected to always use the secure URL.

Edit HTML Templates

Password Policy Enforcer Web's user interface is built with customizable templates. You can easily modify the user interface by editing the templates.

User Interface Files

Password Policy Enforcer Web installs four .htm files for every language. Each filename starts with a language code. The files for the US English language are:

Filename	Content
en_default.htm	Static HTML for the Welcome page. See the Launch Password Policy Enforcer Web topic for additional information.
en_ppeweb.htm	Template for the Password Change page. See the Change Password topic for additional information.
en_finished.htm	Template for the Finished page.

Filename	Content
en_error.htm	Template for the Password Critical Error page. See the Error Messages topic for additional information.

The other user interface files are language independent. Most of the formatting is in ppeweb.css, and some additional CSS for Internet Explorer is in ppeweb_ie.css. The image files are in the images folder. These files are installed into the `\Inetpub\wwwroot\ppeweb\` folder by default.

NOTE: Always backup the user interface files before and after editing them. Your changes may be overwritten when Password Policy Enforcer Web is upgraded, and some changes could stop Password Policy Enforcer Web from working correctly. Web browsers display pages differently, so test your changes with several versions of the most popular browsers to ensure compatibility.

The en_default.htm contains static HTML, but the other .htm files contain special comment tags that are used to prepare the pages. Some of these comments define ranges. A range looks like this:

```
<!—RANGE_NAME-→Some text or HTML<!--/RANGE_NAME-→
```

Password Policy Enforcer Web deletes ranges (and the text inside them) when they are not needed. Some ranges span only one word, while others span several lines. The other type of comment tag is called a field.

```
<!--USERNAME-->
```

Fields are replaced by some other information. For example, the field above is replaced with a username.

Resource Strings

Templates end with a resource string section.

```
<!--RESOURCE_STRINGS-→<!—

@RES_EMPTY_FIELD_USERNAME: Enter your username in the Username box.

@RES_EMPTY_FIELD_DOMAIN:    Enter your domain name in the Domain box.

--><!--/RESOURCE_STRINGS-->
```

Resource strings are mostly validation error messages, but they can contain any text Password Policy Enforcer Web may need to build the page. See the Error Messages topic for additional information. Do not modify the identifiers on the left, only edit the text on the right. Resource strings are always inside a range called RESOURCE_STRINGS. Password Policy Enforcer Web deletes this range before sending the page to the user's web browser.

CAUTION: You may rebrand the PASSWORD POLICY ENFORCER Web user interface, but it is a violation of the License Agreement to modify, remove or obscure any copyright notice. See the License Agreement topic for additional information.

Examples

This topic contains examples of common customizations. Use these examples to gain a better understanding of Password Policy Enforcer Web's templates. You don't need to be an expert in HTML to follow these examples, but a basic understanding of HTML will help. Work through them carefully, and backup files before you edit them. The examples in this section are from the US English files, but the format is the same for all languages.

Replacing the Netwrix Logo

The Netwrix logo is shown in the top left corner of the Welcome page. The logo is installed into the `\Inetpub\wwwroot\ppeweb\images\` folder by default, and it is called logo.gif. You can replace this file with one containing your organization's logo.

Your logo may appear distorted if it is not the same size as the Netwrix logo. You can fix this by opening en_default.htm in a text editor such as Notepad. Search for the line shown below, and replace the width (116) and height (69) with the dimensions of your logo in pixels.

```
<img class="logo" src="images/logo.gif" alt="ANIXIS" width="116"
height="69" ↗
```

Edit Page Instructions

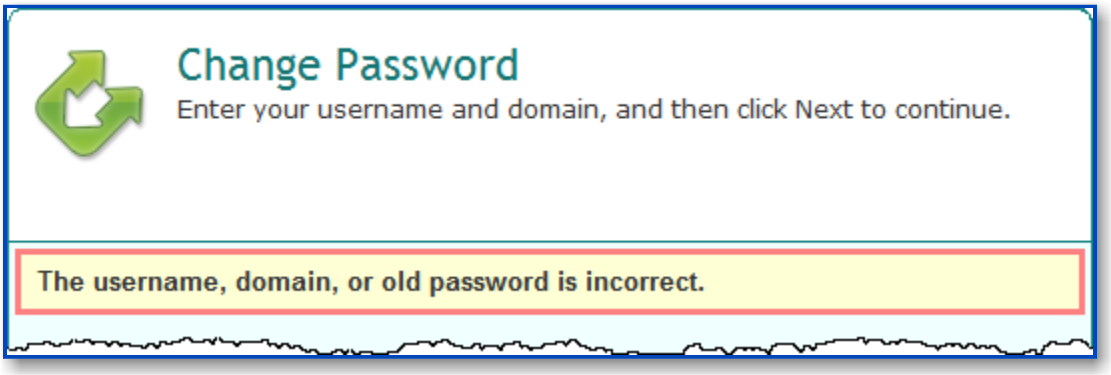
Instructions appear at the top of the Password Change page in the white section above the input fields. You can edit these instructions by opening `en_ppeweb.htm` and searching for the text you wish to modify.

Instructions are inside ranges called SECTION_A and SECTION_B. Each section contains the instructions for a page in the template. Make sure you edit the instructions in the correct section, or they may be displayed on the wrong page.

```
<!--SECTION_A-->

 <p>Enter your username and domain, and then click Next to continue…

<!--/SECTION_A-->

<!--SECTION_B-->

 <p>Enter your old and new passwords in the text boxes below.</p>

<!--/SECTION_B-->
```

Edit Validation Error Messages

Validation error messages are shown in a yellow box below the page instructions. Validation errors are normally caused by invalid user input.



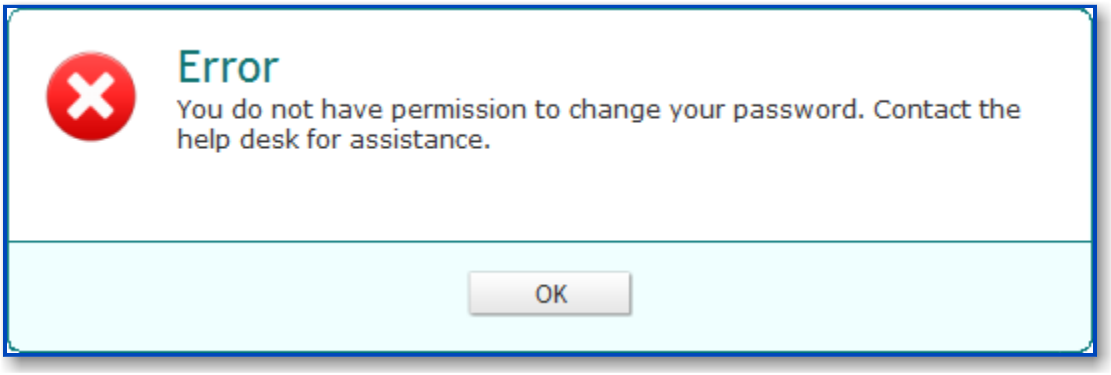
Validation error messages are defined in en_ppeweb.htm. The error messages are in the resource strings section near the end of the file. See the Resource Strings topic for additional information.

String	Error Message
@RES_EMPTY_FIELD_USERNAME	Enter your username in the Username box.
@RES_EMPTY_FIELD_DOMAIN	Enter your domain name in the Domain bo…

String	Error Message
@RES_BAD_USERNAME_OR_PASSWORD	The username, domain, or old password i…

Edit Critical Error Messages

All the critical error messages are defined in `en_error.htm`. The error messages are in the resource strings section near the end of the file. See the Resource Strings topic for additional information.



You may see placeholders like %1 and %2 in some error messages. These are replaced with more information about the error. You should keep these as they provide important information about the error, but you can delete them if you do not want them.

String	Error Message
@RES_ACCESS_DENIED	You do not have permission to change your pas…
@RES_ACCOUNT_LOCKED_OUT	Your account is currently locked out. Try aga…

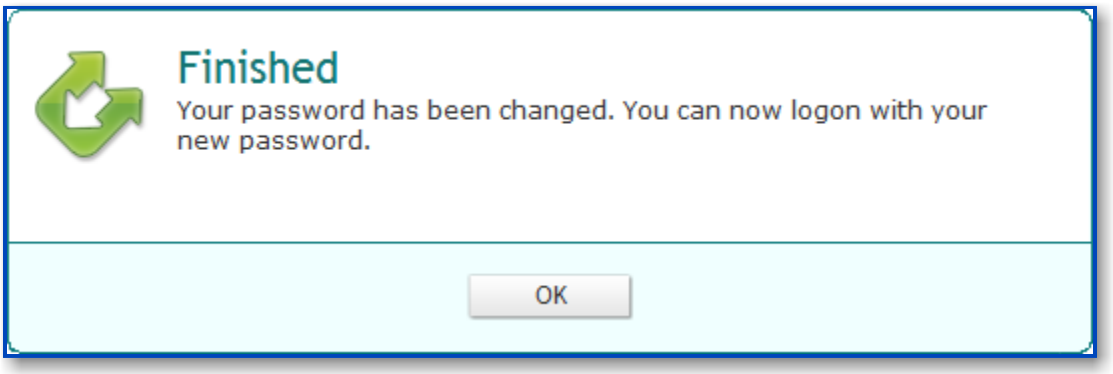
String	Error Message
@RES_LICENSE_MISSING	License reminder. Your password was not chang…

If you want to display some text for all error messages, then insert your text above or below the <p><!--ERROR-→↙p> line. For example:

```
<p><!--ERROR--></p>

<p>The help desk phone number is 555-555-5555.</p>
```

Edit Finished Message

The finished message is shown after users successfully change their password. This message is defined in en_finished.htm.




```
<h1>Finished</h1>

<p>Your password has been changed. You can now logon with your new pass…
```

Change Font Sizes and Colors

ppeweb.css contains most of the user interface formatting information. You can easily change font sizes and colors by editing this file. You can even reposition and resize items, but you will need some understanding of CSS to do this. For example, this is the CSS for the validation error box:

```
.error {
 background-color: #ffffd6;
 border: 3px solid #ff8080;
 color: #333333;
 font: bold 1.3em/1.2em Arial, sans-serif;
 margin: 3px 0 0 4px;
 padding: 6px 22px 6px 8px;
 width: 499px;
}
```

Edit these properties to change the appearance of the error box. You may need to clear your web browser's cache to see the changes.

NOTE: Web browsers display pages differently, so test your changes with several versions of the most popular browsers to ensure compatibility.

Replace URLs to the Welcome Page

Password Policy Enforcer Web shows the Welcome page when users click OK or Cancel on the Password Change, Error, and Finished pages.

To display a different page when users click OK or Cancel, search for `en_default.htm` in `en_ppeweb.htm`, `en_finished.htm`, and `en_error.htm` and replace `en_default.htm` with an alternative URL. For example:

```
https://myserver/accounts/login.htm
```