PASSWORD RBL

PASSWORD FIREWALL

FOR WINDOWS

ADMIN GUIDE

VERSION 6.10

Table of Contents

Introduction

Thank you for your interest in Password Firewall for Windows. Password Firewall works in tandem with Password RBL's Real-time password blacklisting service to prevent the use of bad passwords in Active Directory that often lead to unauthorized access of company resources by hackers.

What is Password Firewall?

Password Firewall is an implementation of Password RBL's password blacklisting service for Microsoft's Active Directory. This allows organizations to quickly and easily enforce the use of strong passwords that are not on Password RBL's growing blacklist of passwords used by hackers to gain unauthorized access to network accounts. Password Firewall provides significantly increased password security to the masses of Windows-based networks in a secure, easy and affordable manner.

Why use Password Firewall?

Reports of network breaches are increasing in frequency, but one aspect remains constant; weak password security is among the most common tactics used to gain unauthorized access to interior business networks as well as proprietary and customer identity data. A common method to combat these attacks is to enforce a password policy, but the built-in password policy functionality in Windows Server does not include a blacklist feature. This is where Password Firewall fits in. Password Firewall, backed with an active subscription to the Password RBL real-time blacklist database of bad passwords, is an extremely easy and cost effective way to prevent the usage of poor passwords that are likely to be exploited by hackers. This is but one of the many reasons to add Password Firewall to your network security framework. Other reasons include:

Recommended Approach – Password Blacklisting is recommended by National Institute of Standards and Technology (NIST) in the United States and the National Cyber Security Centre in the United Kingdom.

Flexible Subscription – Using Password Firewall is not a license to use one application, but rather a monthly subscription to Password RBL, which allows organizations to run Password Firewall to protect their Active Directory, but also use our API to protect various other systems, such as internal Intranet sites, public-facing websites, custom mobile apps, etc., all for one low monthly fee.

Custom Blacklisted Passwords – Customers have the option to create their own blacklisted password permutations that only affect their subscription. This feature can be used to block passwords that are known to be compromised or passwords based on public company information that would be easily guessed.

Focus on Security – All aspects of the Password RBL service were designed with Security as a priority, not as an afterthought.

Lightweight – Password Firewall for Windows is completely transparent to end-users and only requires a small installation on Active Directory Domain Controllers. There is nothing new for admins to learn and end-users don't need to do anything different when changing passwords.

Source Available – All code provided by Password RBL, including the code used by Password Firewall for Windows, is either provided in a readable language or the source code is available for download and analysis by your company's security team.

High Quality Data – Password RBL builds its password database with discovered password lists, analyzes hacker tools and uses honeypot servers to capture passwords actively being used by hackers. And all these passwords sources are reviewed by a real human before incorporating into the Password RBL database.

What's New in this Version

This version of Password Firewall implements general performance improvements upon the previous version. The functionality remains the same. Version 6.00 changed the API query method to use the Prefix-Query API call. Using this method provides additional assurances to subscribers since it only sends the first 5 characters of the computed password hash to the API. The API responds with all blacklist hashes that also begin with the same prefix. Then the complete password hash is searched for existence in the API-returned values. You can read more about this method in the Password RBL API Guide.

IMPORTANT: Upgrading to this version will require a Domain Controller reboot.

System Requirements

Password Firewall was designed to use built-in Windows APIs and function calls and therefore and has minimal overall requirements. Password Firewall requires 64-bit versions of Windows Server and is designed to be installed on Active Directory Domain Controllers. The components that make up Password Firewall are supported on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. The processing and memory requirements of Password Firewall are negligible since there is no "always on" service running. Instead, the Password Firewall code is called on demand by Windows when a password change event occurs. Additionally, all logging is performed via standard Windows Event Log entries, so disk utilization is barely noticeable.

Requirements Summary

- Operating System: Windows Server 2008 R2, 2012, 2012 R2, 2016
- Processor: Any x64 processor supported by Microsoft Windows Server
- Memory: Negligible
- Disk: 5 MB
- Network: HTTPS connectivity to Password RBL API using the standard TCP/443 port.

Components

The Password Firewall product is composed of three major components, 1) a DLL [passwdhk.dll] that "hooks" into the built-in Password Filter API of Microsoft Windows, 2) a PowerShell script [passwdfw.ps1] that provides most functionality as well as connectivity to the Password RBL API, and 3) an INI file [passwdfw.ini] where configuration options are stored.

The passwdhk.dll extends the built-in support of Microsoft Windows to call a custom Password Filter. The provided passwdhk.dll is registered with the Local Security Authority (LSA) in Windows. When a password change event occurs, Windows calls the registered passwdhk.dll, which accepts the username and password from the Windows Password Filter handoff and passes this information to the Password Firewall PowerShell script.

The second component of Password Firewall is a Windows PowerShell script [passwdfw.ps1] compatible with built-in Windows PowerShell v2 scripting. The script provides most of the Password Firewall functionality. It accepts the username and password captured by Windows (and provided to passwdhk.dll). It performs some local password policy checks and then salts and iteratively hashes the provided password with the industry standard PBKDF2 algorithm 30,000 times before forming and sending the query to the Password RBL API. (The Password Firewall script only uses the username to verify the username and password do not match and for local event logging purposes. The username is never sent to the Password RBL API.) The API response is relayed back to Windows (via passwdhk.dll). If the chosen password is listed in the Password RBL database, then Windows blocks the password change and notifies the end-user that the chosen password does not meet the organization's password policy requirements.

Deployment Considerations

This Admin Guide contains all the technical information about Password Firewall that is needed to deploy and maintain the product. But, in order to have a smooth deployment, it is important to consider some things that are not necessarily technical in nature.

- Notification: Password Firewall extends the built-in password policy in Active Directory. This policy can be configured however you need it to be, but it can affect every user in the organization. It is wise to notify the organization of any change to the password policy, including the addition of password blacklisting.
- Helpdesk Load: Even with good "marketing" of the change in password policy, there are still likely to be an increase in calls to your organization's helpdesk. If you do not have prior metrics to know how many calls to expect, it may be wise to deploy Password Firewall across the organization in phases rather than all at once. You can accomplish this in a couple ways – by deploying Password Firewall only to domain controllers in a single AD site at a time or by utilizing the GroupFilter feature.
- Domain Controller Load: The requirements of Password Firewall are minimal and the typical processing of Password Firewall only requires a few seconds per password change event. If you have a large Active Directory, and will be deploying Password Firewall across the organization on the same day, we recommend you first run some password change tests in your environment to be sure your existing Domain Controllers can handle the load. Contact support if you need guidance on performing these types of tests.

Upgrade Information

Read the applicable section based on the existing installed version.

IMPORTANT: This version includes performance improvements in the DLL processing. Upgrading from any prior version will require a reboot. If a silent/scripted, over-install upgrade is run, the target system(s) will automatically reboot at the end of the upgrade process.

Upgrading from version 3.x or later

Performing an upgrade of an existing Password Firewall version 3.x is fast and easy; you have two options. The recommended method is to download the latest version and perform an "over install" using our wizard-based Easy Install method. This will upgrade the software to the latest version while maintaining settings such as TrackingID, BlacklistID, GroupFilter, etc.

Alternatively, if you prefer the manual installation method, replace the passwdfw.ps1 file in the standard installation folder (typically, C:\Program Files\PasswordRBL) with the new version, replace the passwdhk.dll file in the Windows System32 folder (typically, C:\Windows\System32) with the new version, and apply the latest registry changes (using the provided reg file in the full download package). See the installation section of this document for detailed manual instructions.

The upgrade must be performed on all domain controllers where Password Firewall is installed. This upgrade includes a new version of passwdhk.dll, and thus a reboot is required when

performing the upgrade. It is recommended that the reboot occur as soon as possible after the upgrade process is complete.

Upgrading from version 1.x or version 2.x

In order to upgrade Password Firewall from version 1.x or 2.x, you have two options. The recommended method is to download the latest version and perform an "over install" using our wizard-based Easy Install method. This will upgrade the software to the newer version, but you need to read the special note below in order to maintain your existing settings (TrackingID, BlacklistID, etc.).

Alternatively, if you prefer the manual installation method, replace the passwdfw.ps1 file in the standard installation folder (typically, C:\Program Files\PasswordRBL) with the new version, replace the passwdhk.dll file in the Windows System32 folder (typically, C:\Windows\System32) with the new version, and also apply the latest registry changes (using the provided reg file in the full download package). See the installation section of this document for detailed manual instructions.

IMPORTANT: When performing either upgrade method, the passwdfw.ps1 file is replaced/overwritten. If you have added a Tracking ID, Blacklist ID, GroupFilter or otherwise customized this file, it will be lost as part of the upgrade. Be sure to annotate which IDs and settings you were using for each system you upgrade so you can re-add them after the upgrade is complete. As of version 3.0, all settings are in stored in an external INI file which makes future upgrades easier and more streamlined.

The upgrade must be performed on all domain controllers where Password Firewall is installed. This upgrade includes a new version of passwdhk.dll, and thus a reboot is required when performing the upgrade. It is recommended that the reboot occur as soon as possible after the upgrade process is complete. See the following section for detailed installation instructions.

Configuration Options

Password Firewall has a modest number of configuration options available, but it will function without any additional configuration as long as you have an active subscription and have provided your source IP address(es) to Password RBL.

The below configuration options are all defined inside the passwdfw.ini file which you will find inside the PasswordRBL folder in the standard Program Files folder. For most installations of Windows this path will be:

C:\Program Files\PasswordRBL

NOTE: As of version 3.0, there is no reason to change the provided PS1 file. All of the configuration options are located in the INI file.

AllowOnError

Format: AllowOnError = [True | False]

This option allows you to choose what happens if an error occurs during the processing of a password change event. When set to True (the default), Password Firewall will allow the password change to occur even if an error occurs or it cannot connect to the Password RBL API to determine if the password choice is listed the database of bad passwords.

If this option is set to False, then Password Firewall will prevent the password change. Changing this option to False will lead to a more secure network since passwords will always have to be checked against the Password RBL API, but it is important to note that this would result in all password changes being denied until the error condition is cleared.

BlacklistID

Format: TrackingID = [32 hex characters]

Password Firewall is able to use the Custom Blacklists feature of the Password RBL API. This feature allows requests sent to the Password RBL to be searched against a custom password blacklist. This option is null (blank) by default and optional. When left null, passwords submitted to the API are only checked against the curated Password RBL database of blacklisted passwords. When set to a valid Blacklist ID, the submissions to the API are searched in the custom blacklist as well as the curated Password RBL password blacklist.

Note: Password RBL provides a separate PowerShell utility to manage the entries in your custom blacklist. Simply browse to Downloads section of the Password RBL website to download this tool (`prbl-cblmanagement.ps1`) and documentation that covers this topic.

CustomBlacklistOnly

Format: CustomBlacklistOnly = [True | False]

When using a Custom Blacklist, Password Firewall's default behavior is to query both blacklists (the curated Password RBL blacklist and your custom blacklist) simultaneously. This option allows you to control that behavior so Password Firewall only queries your custom blacklist. If you wish to only query the curated Password RBL blacklist, then do not specify a BlacklistID in the INI configuration.

Note: Even in the default setting (False), the two blacklists are queried with a single connection to the Password RBL API, so this setting does not have an impact on your Password RBL query quota.

DoubleCheck

Format: DoubleCheck = [True | False]

Password Firewall can optionally truncate chosen passwords and "double check" the resulting shorter password against blacklists. This feature combats a common practice of adding a character at the end of a chosen password to make it different than the previous password. The most common character is a number. If the initial blacklist query returns that the chosen password is not blacklisted, then the DoubleCheck feature will truncate any digits at the end of the chosen password and re-query the blacklist.

The default value for this feature is disabled so Password Firewall maintains the same function as previous versions of the software.

Note: Enabling this feature will require twice as many API queries as prior versions of Password Firewall. Password RBL has increased query quotas for existing customers upon release of this feature in Password Firewall v5.0.

GroupFilter

Format: GroupFilter = [sAMAccountName of AD group]

This optional feature limits the scope of password filtering based upon membership in the specified Active Directory group. When left blank (the default) Password Firewall scrutinizes password changes for all users regardless of group membership. The membership search is recursive, so users of nested groups will be considered members of the provided filter group. This feature is helpful when performing a phased rollout of Password Firewall across an organization or when you do not wish to subject all users to Password Firewall filtering. When entering the group name, enter the `sAMAccountName` of the group.

IMPORTANT: If your Active Directory has multiple domains, you must create a specific GroupFilter Active Directory group in each domain. This is because when Password Firewall queries Active Directory for group membership, it can only find groups in the specific domain hosted by the domain controller where the password change is happening – not groups from other domains in the same forest.

Note: During the query process, a Global Catalog may be used in certain circumstances. It is typically considered a best practice for every site with Active Directory domain controllers to have at least one Global Catalog server. Speak with your Active Directory architect for additional information on your organization's Global Catalog topology configuration. As of version 5.20, an Active Directory-based search is performed to confirm the results returned from

the Global Catalog. This increases the reliability of Group Membership searches, especially when a Global Catalog server is unavailable, malfunctioning, or returns stale membership data.

GroupFilterType

Format: GroupFilterType = [Inclusion | Exclusion]

This feature was introduced in version 3.10 and determines if the group specified in the GroupFilter option is a collection of user accounts that should have their password choices scrutinized (Inclusion) or should be exempted from Password Firewall processing (Exclusion). The default is Exclusion.

Note: Prior to version 3.10, the GroupFilter feature operated only as an Inclusion group. During upgrade from version 3.00, if a GroupFilter group is specified, GroupFilterType is set to Inclusion to match the previous manner of operation.

IMPORTANT: The choice between Inclusion and Exclusion affects whether or not Password Firewall processes passwords during new account creation. When set to the default, Exclusion, Password Firewall will process passwords during new user account creation process. When set to Inclusion, passwords will not be processed for new accounts as they are created.

ProxyAddress

Format: ProxyAddress = [FQDN | IP]

If your network requires that use of an explicit proxy server in order to access the Internet, use this configuration item to enter the proxy's fully qualified DNS name or IP address. Do not specify the proxy's port here, use the ProxyPort configuration option (below) to specify the proxy's port.

ProxyPort

Format: ProxyAddress = [Number between 1 - 65535]

If you use a proxy in order to access the Internet and also specified the ProxyAddress configuration option (above), use this option to specify the port that the proxy operates on. This should be a number between 1-65535, without any delimiting characters.

ReportingOnlyMode

Format: ReportingOnlyMode = [True | False]

Reporting Only Mode is an option that still processes all password change events using the Password Firewall software but regardless the final determination, all chosen passwords are

allowed to be used. The allows IT managers to determine how often their user population is choosing passwords that are identified by Password RBL as bad passwords, while not impacting end-users' password choices. IT managers can either count the API responses (matches or misses) to get desired metrics or combine the ReportingOnlyMode with the TrackingID (below) option to have Password RBL provide reporting information.

RequiredCharSets

Format: RequiredCharSets = [0 - 5]

This option allows you to choose how many of the 5 available character sets a password must contain. The character sets are: lowercase letters, uppercase letters, numbers, ASCII special characters, and all remaining characters (includes all unicode characters). This option is set to zero by default, to disable this requirement.

Note: This option is similar to a well-known component of the built-in Windows password policy complexity requirements, which requires passwords to contain 3 of the aforementioned character sets. The Windows policy option also enforces other checks, but it is not configurable. If both policy options are used, the highest complexity setting will be required. For example, if Windows complexity requirements is enabled and RequiredCharSets is set to 4, then passwords will be required to have 4 of the 5 character sets present. Conversely, if Windows complexity is enabled but RequiredCharSets is set to 2, passwords will be required to have 3 character sets present, because that is mandatory when Windows complexity requirements is enabled.

TrackingID

Format: TrackingID = [32 hex characters]

This feature allows requests sent to the Password RBL to include a customer's assigned TrackingID for use in metrics reporting. This option is null (blank) by default and optional. When left null, queries submitted to the API are not tagged or counted. When set to a valid Tracking ID, the submissions to the API are tagged with the supplied tracking ID and customers can then use the My Metrics page on the Password RBL website to get report on how frequently password choices matched a blacklisted password.

Installation

The recommended method for installing Password Firewall is to use the wizard-based Easy Install. This method will copy the necessary files into the proper locations and create the needed registry keys. Additionally, the wizard registers the installation with Windows to make uninstallation just as easy. Alternatively, and to provide complete transparency to how the software functions, customers have the option to perform a manual installation.

IMPORTANT: For new installs, it is important to note, that no matter which method is chosen, a reboot will be required to activate the password hook DLL with the Windows Local Security Authority (LSA) subsystem. Some upgrades require reboots and some do not. See the Upgrade section for specifics.

REMEMBER: You need to install Password Firewall on every domain controller to ensure complete protection from bad passwords.

Before Installing

Before you get started installing Password Firewall, be sure the server has recent successful backups and you've subscribed to Password RBL and have provided the public IP address(es) that will be used when domain controllers connect to the Password RBL API. This is commonly the edge firewall's WAN interface IP address assigned by the Internet Service Provider (ISP). If you do not know this IP address, you can follow this short procedure to determine the correct IP address (in most circumstances).

1. Using a web browser on the domain controller(s) where Password Firewall will be installed…
2. Browse to `www.whatismypublicip.com`
3. This website will show your public IP address on the screen.
4. Provide this IP address to Password RBL when subscribing.

If you are deploying Password Firewall to a new site, then you will need to provide this new public IP address to Password RBL so it can be authorized on your account. This may require upgrading to a larger subscription package. See www.PasswordRBL.com for current subscription package information, features and costs.

Interactive Installation – Easy Install

The provided wizard-based easy install is the recommended method for deploying Password Firewall throughout your organization. This wizard automatically creates the necessary registry keys and copies the needed files to the server. To perform an easy install, simply follow the below steps.

REMEMBER: You only need to install Password Firewall on your Active Directory domain controllers – not on member servers or workstations.

1. Download the latest version of the Easy Install from the Downloads section of the Password RBL website.
    a. We recommend you compare the file hash to verify you have the correct file.
2. Run the setup executable file
3. Click Next to begin the setup
4. Setup prompts you to provide configuration options, such as Tracking ID, Custom Blacklist ID, and GroupFilter settings. Follow the prompts to make your choices. If you do not wish to use a specific feature, then simply leave them blank and click Next.
5. Setup then installs the program files and creates the necessary registry keys
6. Click the Finish button to complete the setup.
7. If this is a new installation (or an upgrade that requires a reboot), you will be prompted to restart the server in order to activate the software.

Automated Installation

The provided wizard-based Easy Install can be used in an automated fashion by running the installation in “silent” mode and providing all desired settings as command-line parameters. This method works especially well with Group Policy based deployments of Password Firewall across an entire organization’s Domain Controllers.

When automating the installation, you must provide two command-line arguments in order to put the installer in “silent” mode. You can then provide any of the below mentioned optional arguments. If you do not specify the required “silent” parameters, then installation runs in interactive mode, requiring clicks to advance the installation.

IMPORTANT: When you run a new installation of Password Firewall in “silent” mode, the installer will trigger an immediate reboot of the domain controller. Some upgrades may also trigger an immediate reboot if it is required. See the upgrade section for specific details.

Basic Syntax:

```
setup-passwordfirewall.exe [ Required Parameters ] [ Optional Parameters ]
```

Parameter Listing

Below is a listing of all available command line options.

IMPORTANT: During automated installation, there is no verification of the values supplied to each parameter. As long as the syntax is correct, the installation will be successful. Verification

of configuration values will occur when Password Firewall is called as part of a password change event. Check the Event Log for errors.

Parameter	Required	Description and Format
/VERYSILENT	Yes	Instructs setup to run in silent/automated mode. The VERYSILENT parameter automates installation without any display. Format: /VERYSILENT
/SUPPRESSMSGBOXES	Yes	Suppresses and auto-answers any message box prompts during setup. Required when VERYSILENT has been used. Format: /SUPPRESSMSGBOXES
/LOG	No	Use this option to specify a logging location for the installation process. Use quotes if the file path contains spaces. The specified path must be complete, beginning with a drive letter, and every specified folder in the path must already exist. The file will be created if it doesn't already exist. **IMPORTANT**: Installation will fail if a folder cannot be found or the log file cannot be created. Format: /LOG=<Full Path to log file>
/TrackingID	No	Use to specify the Tracking ID to be used for this installation. Format: /TrackingID=<32 hex characters>
/BlacklistID	No	Use to specify the custom Blacklist ID to be used for this installation. Format: /BlacklistID=<32 hex characters>
/CustomBlacklistOnly	No	Use this option to control which blacklists are queried. This option only has an effect if a BlacklistID is specified in the INI file. Format: /CustomBlacklistOnly=<True or False>

/GroupFilter	No	Use to specify the Active Directory group that defines which accounts are subjected to Password Firewall scrutiny. Use quotes if the group name contains spaces. Format: /GroupFilter=<sAMAccountName>
/GroupFilterType	No	Use to control if the group specified in the GroupFilter option is an inclusionary or exclusionary group. Format: /GroupFilterType=<Inclusion | Exclusion>
/DoubleCheck	No	Use to enable or disable the password DoubleCheck feature. Format: /DoubleCheck=<True or False>
/RequiredCharSets	No	Use to enforce a minimum character set complexity of chosen passwords. Format: /RequiredCharSets=< 0 – 5 >
/VerboseLogging	No	Use to enable additional logging information when Password Firewall runs. Format: /VerboseLogging=<True or False>
/AllowOnError	No	Use to control whether or not Password Firewall allows password changes when an error occurs. Format: /AllowOnError=<True or False>
/ReportingOnlyMode	No	Use to put Password Firewall in Reporting Only Mode so that password changes are allowed even if the password exists in the blacklist. Format: /ReportingOnlyMode=<True or False>
/ProxyAddress	No	Use to specify the FQDN or IP Address of an explicit proxy that provides access to the Internet for domain controllers. Format: /ProxyAddress=<FQDN or IP>
/ProxyPort	No	Use to specify the port used by the explicit proxy specified in the ProxyAddress parameter Format: /ProxyPort=<Number between 1-65535>
/HashType	No	Use to control which cryptographic hashing algorithm is used with Password RBL. /Format: /HashType=<PBKDF2 or SHA256>

Examples

The following command runs setup in silent mode and enables verbose logging.

```
Setup-passwordfirewall.exe /VERYSILENT /SUPPRESSMSGBOXES /VerboseLogging=True
```

This command runs setup without any display and enables VerboseLogging and sets a specific TrackingID to be used

```
Setup-passwordfirewall.exe /VERYSILENT /SUPPRESSMSGBOXES /VerboseLogging=True
/TrackingID="1234567890abcdef1234567890abcdef"
```

This example runs setup without any display, enables the installation log file and limits password scrutiny only to users in the specified group.

```
Setup-passwordfirewall.exe /VERYSILENT /SUPPRESSMSGBOXES
/Log="C:\pfinstall.log" /GroupFilter="Password Firewall Group"
```

This example runs setup without any display, enables the installation log file and limits password scrutiny to all users except those in the specified group.

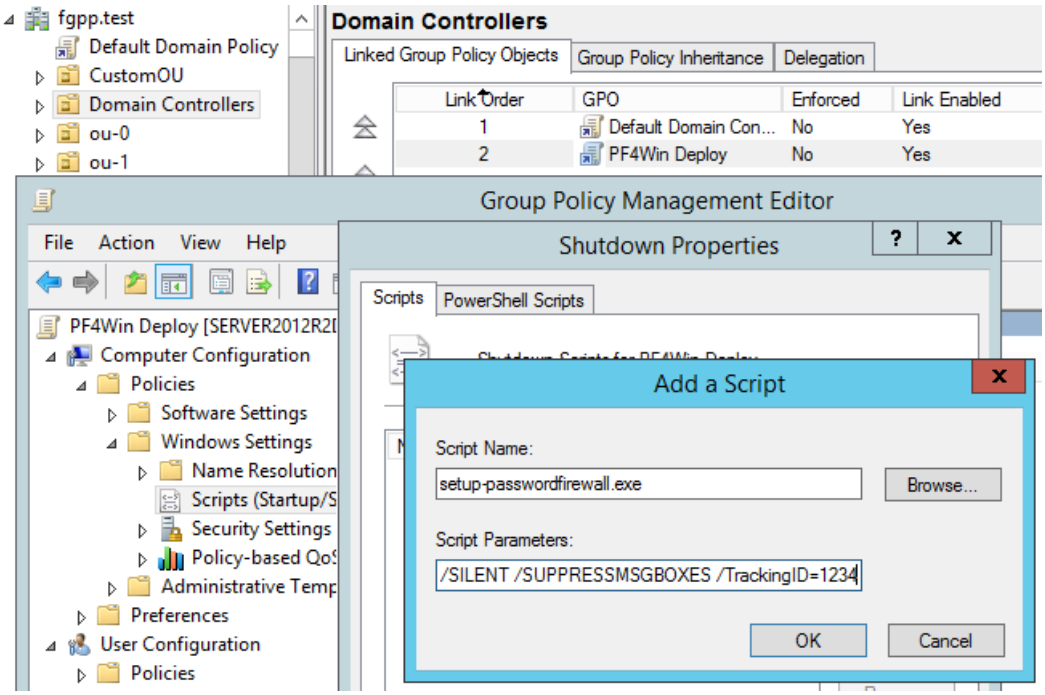
```
Setup-passwordfirewall.exe /VERYSILENT /SUPPRESSMSGBOXES
/Log="C:\pfinstall.log" /GroupFilter="PF Group" /GroupFilterType=Exclusion
```

Using Group Policy

The automated installation method is compatible with Microsoft's Group Policy. Using Group Policy is a great way to deploy and configure Password Firewall throughout your organization with minimal effort. Use the below procedure as a guide when deploying with Group Policy.

1. Edit the Default Domain Controllers Group Policy Object (GPO) or create a new GPO and link it to the Organizational Unit that contains your Domain Controllers
2. Expand the Group Policy navigational tree through the following path:
    a. Computer Configuration > Policies > Windows Settings > Scripts
3. Double-click on Startup or Shutdown depending on your desired installation time.
    a. Password RBL recommends scheduling the installation of Password Firewall at computer shutdown since new installations will trigger an immediate restart of the domain controller to activate the software with Windows.

4. Click the Show Files button at the bottom of the window.
5. Drag the “setup-passwordfirewall.exe” Easy Install package into the shown folder.
6. Close the Explorer window
7. Click the Add button
    a. Click browse to open the GPO’s folder. Choose the “setup-passwordfirewall.exe” file that you placed in this location in the previous step
    b. Type in the required parameters and any optional parameters to the installation program following the Parameter Listing above.
    c. Your display should resemble the picture below:



8. Click OK until you are back to the Group Policy Object editor window.
9. Exit the Group Policy Editor which will save your changes.

NOTE: When a new server is promoted to domain controller, it commonly takes an extra reboot (after the reboot that is part of the promotion) because the new Group Policy hasn’t yet applied to this server so quickly after it has been promoted.

Manual Installation

The recommended installation method is to use the Easy Install (see above) in either interactive or automated mode, but customers can instead follow the below steps to perform a completely manual installation of Password Firewall.

IMPORTANT: If a manual installation is performed, then in order to uninstall Password Firewall, the manual uninstallation method must be used as there will be no uninstallation program created during the manual installation procedure.

1. Download the latest version of the installation files from the Downloads section of the Password RBL website.
2. Copy Files
   - Copy the `passwdhk.dll` file to the System32 folder of your Windows directory.
     - Example: `C:\Windows\System32`
   - Create a folder named “PasswordRBL” in the 64-bit Program Files folder
     - Example: `C:\Program Files\PasswordRBL`
     - Notice there is no space in PasswordRBL
   - Copy the `passwdfw.ps1` file to the PasswordRBL folder that was just created.
   - Also copy the `passwdfw.ini` file to this same folder
3. Make Registry Changes
   - Run regedit.exe
     - Note: this must be the 64-bit version of regedit.exe from the System32 folder. Do not run the 32-bit version (from the SysWOW64 folder).
   - Register Password Hook DLL with LSA
     - Browse to the following registry key and **append** the value “passwdhk” being careful not to remove any existing values in this key
     - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
     - **Note**: There is no “.dll” on this value!
     - This change will not be activated until the server is rebooted.
   - Register the Password Firewall Event Log Source
     - Create the following key & value, creating any folders in the process
     - HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application\Password Firewall
     - Type: REG_EXPAND_SZ
     - Name: EventMessageFile
     - Value: <Depends on Windows Version>
       - 2008 R2 - .NET version 2 {win}\Microsoft.NET\Framework64\v2.0.50727\EventLogMessages.dll
       - 2012 and later - .NET version 4 {win}\Microsoft.NET\Framework64\v4.0.30319\EventLogMessages.dll
       - where {win} is the path to the Windows folder on this system
   - Register the Password Hook DLL settings
     - Merge the provided “.reg” file to automatically create the necessary values for the DLL. These settings have a very specific format. If you’d like to review the exact changes that will be made, simply open this file using MS Notepad or any other basic text editor program.
4. Update PowerShell Script Execution Policy

- Open an Administrative 64-bit PowerShell Window (right-click and choose Run as Administrator)
- Check existing Execution Policy by running the cmdlet “Get-ExecutionPolicy”
- If the above command returns “Restricted” or “AllSigned” then run this command
  - Set-ExecutionPolicy RemoteSigned

5. Restart the server

Reconfiguration

Password Firewall’s behavior is controlled by the options specified in the INI file. You can either edit this file using a basic text editor, such as Notepad, or re-run the installer (in silent or interactive mode) to reconfigure Password Firewall after it has been installed. Changes to the INI file will take effect during the very next run of Password Firewall. There is no need to reboot the server if you are not changing versions. Some upgrades may require a reboot. See the upgrade section for specific upgrade paths and requirements.

If you are using Group Policy to deploy and configure Password Firewall, you can edit your group policy settings to apply new configuration settings to the INI file using the command-line parameters. Those changes will be applied when Group Policy applies. See the Group Policy section for general details and your Active Directory administrator for Group Policy configuration as it pertains to your organization.

Un-installation

Below are the steps required for un-installation. If you utilized the Easy Install method for installation then wizard-based uninstallation is available. However, if you originally performed a manual installation then you must use the manual uninstallation method below.

IMPORTANT: No matter which uninstallation method is used, a reboot will be required to deactivate the password hook DLL from the Windows Local Security Authority (LSA) subsystem. This reboot should happen as soon as possible after the software is uninstalled because all password changes will be blocked by Windows until the reboot occurs.

Before Uninstalling

Before you uninstall Password Firewall, it is recommended that your server has had recent successful backups. This is especially true if you are performing a manual uninstallation since direct manipulation of the registry is required.

Easy Uninstall

If you originally performed an installation using the Easy Install Wizard, then uninstallation is just as easy. You can either perform an interactive uninstall or perform an automated uninstallation using the provided Windows Batch script.

Interactive Uninstall

You will find a link to run the uninstallation wizard in the Program folder of the Start Menu/Screen as well as in the Programs and Features applet in Control Panel.

1. Use either option to launch the uninstall wizard.
2. Click Next to begin the uninstallation process
3. The uninstaller will remove the PowerShell script from the program folder. Additionally, it will unregister the password hook DLL from the LSA and mark the DLL file for deletion upon next reboot.
4. Click the Finish button to complete the wizard.
5. Restart the server to complete the removal of the software

Automated Uninstallation

The complete download package of Password Firewall contains a Windows Batch script that can be used to uninstall Password Firewall in an automated manner. Password RBL provides the below instructions for deploying this script in a Group Policy object. Password RBL recommends using the Computer Configuration Shutdown Script functionality of the Group Policy Object since the uninstall process will immediately reboot the domain controller to complete the uninstallation process

IMPORTANT: The automated uninstallation will immediately reboot the server upon completion.

Using Group Policy

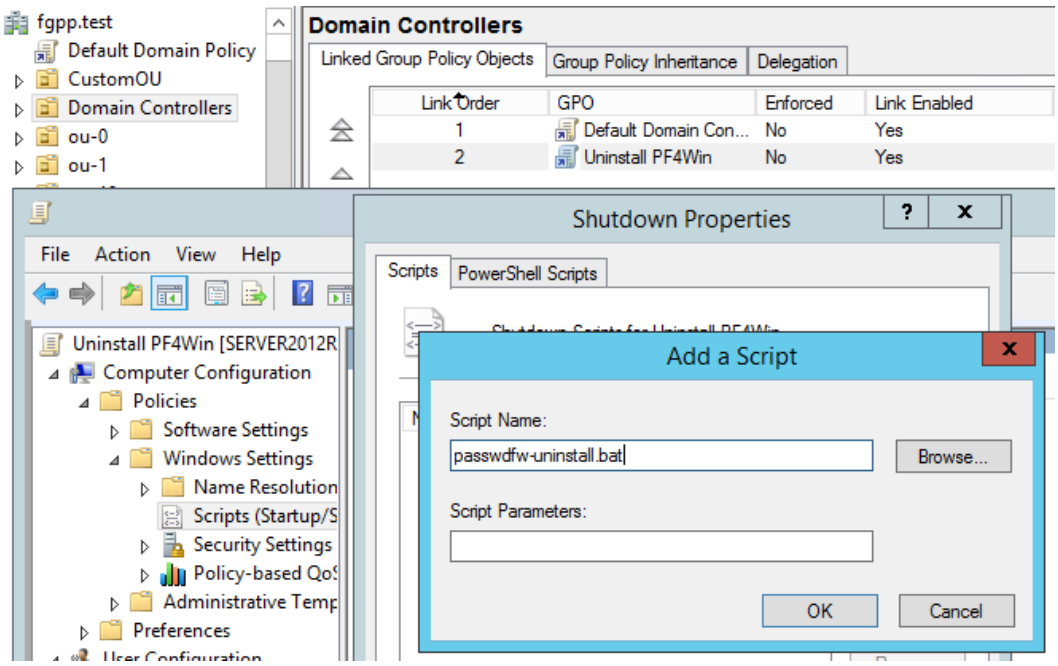
The automated uninstall method is compatible with Microsoft's Group Policy. Using Group Policy is a great way to remove Password Firewall from all domain controllers in your organization with minimal effort. Use the below procedure as a guide when performing an automated uninstall using Group Policy.

IMPORTANT: Be sure you've removed or disabled any GPOs that run an automated installation of Password Firewall before you schedule an automated uninstallation.

1. Edit the Default Domain Controllers Group Policy Object (GPO) or create a new GPO and link it to the Organizational Unit that contains your Domain Controllers
2. Expand the Group Policy navigational tree through the following path:

a. Computer Configuration > Policies > Windows Settings > Scripts

3. Double-click on Startup or Shutdown** depending on your desired uninstallation time.
   a. Password RBL recommends scheduling the uninstall of Password Firewall at computer shutdown since the uninstaller will trigger an immediate restart of the domain controller in order to deactivate the software with Windows.
4. Click the Show Files button at the bottom of the window.
5. Drag the “passwdfw-uninstall.bat” uninstaller script into the shown folder.
6. Close the Explorer window.
7. Click the Add button
   a. Click browse to open the GPO’s folder. Choose the “passwdfw-uninstall.bat” file that you placed in this location in the previous step
   b. Your display should resemble the following picture:



8. Click OK until you are back at the GPO Editor window.
9. Exit the Group Policy Editor which will save your changes.

Manual Uninstallation

The manual uninstallation process requires manipulating the registry, which, if not done properly, could lead to significant system problems. Therefore it is always recommended to verify that you have good backups of your server(s) before following the below procedure.

1. [Required] Deactivate the Password Hook DLL
   - Run regedit.exe

- Note: this must be the 64-bit version of regedit.exe from the System32 folder. Do not run the 32-bit version (from the SysWOW64 folder).

➢ Browse to the following registry key and remove ONLY this value: `passwdhk`
➢ Leave any other values that are present in this key.
➢ HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
➢ This change will not be activated until the server is rebooted.

2. [Required] Restart the server to release the lock on the `passwdhk.dll` file
3. [Optional] Delete Files
   ➢ Delete the `passwdhk.dll` file from the System32 folder of your Windows directory.
      - Example: `C:\Windows\System32`
   ➢ Delete the folder named "PasswordRBL" in the 64-bit Program Files folder
      - Example: `C:\Program Files\PasswordRBL`
      - Notice there is no space in PasswordRBL
4. [Optional] Remove Registry Changes
   ➢ Run regedit.exe
      - Note: this must be the 64-bit version of regedit.exe from the System32 folder. Do not run the 32-bit version (from the SysWOW64 folder).
   ➢ Delete the Password Hook DLL registry settings
   ➢ Browse to the following registry key and delete the entire folder named "passwdhk"
      - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\passwdhk
5. [Optional] Update PowerShell Script Execution Policy
   ➢ Open an Administrative 64-bit PowerShell Window (right-click and choose Run as Administrator)
   ➢ Set the PowerShell script Execution Policy to your desired level. Note the defaults are below:
      - 2008 R2 – Restricted
      - 2012 – Restricted
      - 2012 R2 – RemoteSigned
      - 2016 - RemoteSigned
      - Example: Set-ExecutionPolicy RemoteSigned
6. Uninstall is complete, but you must reboot as soon as possible to deactivate the software with Windows.

Troubleshooting

Installation

If you are having trouble installing Password Firewall, first make sure you are installing on a supported Operating System that meets all the requirements listed earlier in this document. Most notably, Password Firewall is only supported on 64-bit versions of Windows Server and

must be installed on every domain controller in Active Directory to ensure all password changes are being processed.

If the Easy Install wizard is not functioning or gives an error before completion, please contact support or perform a manual installation using the instructions in this document.

Operation

Since Password Firewall is launched on demand when Windows processes a password change and there is no running service or process it can be difficult to determine if Password Firewall is functioning properly. The best way to determine if Password Firewall is functioning is to review log messages in the Windows Application Event Log. Password Firewall log entries will have an event source name of "Password Firewall." Each time Password Firewall runs it will generate log entries.

Tip: Enable Verbose Logging (see Configuration Options section) to increase the number of event messages logged to the Event Log. This aids in troubleshooting.

When Password Firewall is functioning properly, you should see various log entries that provide feedback on the status of Password Firewall. Below is an example of an information type entry that lists the username associated with the password change event.

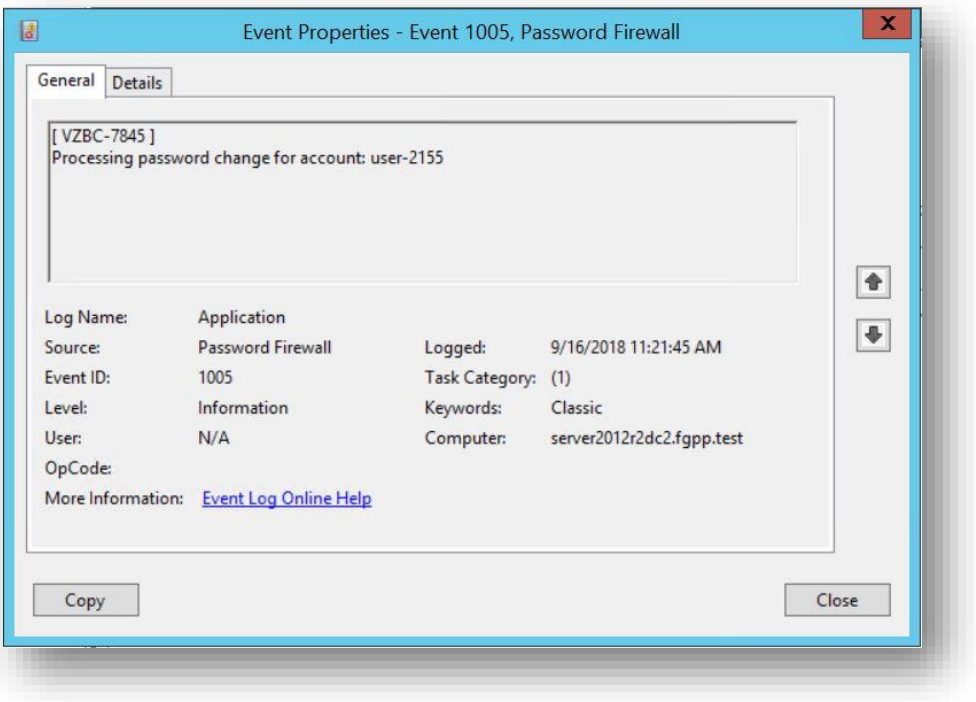


Figure 1: Example Event Log entry

Error Messages

If you are instead receiving an error, the error message will be descriptive of the problem. The most common errors are HTTP timeouts or unauthorized messages.

Timeouts are caused when the system running Password Firewall cannot connect to the Password RBL API via HTTPS. This can be due to DNS lookup errors. Make sure this system can resolve the name "api.passwordrbl.com." Timeouts may also be caused if your organization limits outbound connections from the server(s) running Password Firewall and/or performs man-in-the-middle inspection of HTTPS traffic and these proxies are preventing a connection from the Password Firewall software to the hosted API service. Resolving these issues are outside the scope of this document. Contact Password RBL support for guidance with proxy issues.

Unauthorized messages mean that Password Firewall has successfully contacted the Password RBL API but the source IP address is not an authorized IP to utilize the API. Password RBL limits connections to IPs associated with customer accounts. In this case, you need to inform Password RBL of the public/Internet IP address for this server. This is not likely the IP address assigned to the Network Interface in Windows. The IP that is needed is the IP address from the Internet Service Provider (ISP). To determine which IP address this server uses when it connects to Internet destinations, open a web browser and browse to `www.whatismypublicip.com`. Copy this IP address and paste it in the Contact Form at the Password RBL website to update your account (note: this may require upgrading your subscription depending on the number of source IPs allocated).

Slow Password Changes

If password changes are occurring, but take an extended amount of time to complete, this is typically because the domain controller's public IP has not been added to your account with Password RBL. You will see errors in the Windows Event Log reporting this is the case. Use the procedure from earlier in this document to determine the associated public IP and provide it to Password RBL using the contact form at www.PasswordRBL.com.

If the IP address has already been authorized, then slow password changes are typically due to the use of the GroupFilter feature and the queries to Active Directory are taking longer than expected. To determine if this is the case, enable Verbose Logging and review the time stamps of the log entries as Password Firewall runs.

To resolve this issue, you can stop utilizing the GroupFilter feature by removing the group name specified in the INI file. If you need to use the GroupFilter feature to limit the scope of Password Firewall, review your organization's Global Catalog topology and make sure every site with domain controllers has at least one Global Catalog server available. Contact support if this issue persists.

No Log Entries in Event Viewer

If no log entries are being generated in the Application Event Log, then either the server has not been restarted since the installation of Password Firewall or there was a problem with the installation process. If the server has already been restarted, then please contact support or verify the installation worked properly by walking through the manual installation procedure listed earlier in this document.

Frequently Asked Questions

How do I know Password RBL is not just reading all my network passwords?

Because it's not possible. Passwords submitted to the Password RBL API have already been salted and cryptographically hashed 30,000 times with the industry standard PBKDF2 algorithm. Cryptographic hash functions are one-way functions that cannot be reversed or "decrypted." Additionally, starting with Password Firewall v6.00, only a partial hash value is sent to the API. These design elements prevent Password RBL from being able to see the clear text version of the password that has been chosen. And Password Firewall is source-available, so you can open the passwdfw.ps1 script and verify it's operation for yourself.

Where do I install Password Firewall in my network?

Password Firewall needs to be installed on every Active Directory Domain Controller to ensure complete protection from bad passwords. Payment to utilize Password Firewall follows the Password RBL subscription model and is not licensed per installation so you are not necessarily paying more for additional installations. The installation is lightweight, quick and easy but does require the server(s) to be restarted, so plan accordingly.

Do I install Password Firewall on Read-Only Domain Controllers (RODCs)?

No. Read-Only Domain Controllers do not directly process password changes, so you only need to install Password Firewall on writeable Domain Controllers.

Do my end-users have to do anything different when changing their network password?

No. This is one of the greatest features of Password Firewall. End-users, Helpdesk, and Administrators use the normal built-in methods for updating Active Directory passwords. There is nothing new to learn and users/helpdesk employees don't need to do anything differently.

Why is Password Firewall programmed in PowerShell?

Some applications have pre-requisites that make installation and support more complex. PowerShell is already built-in to all Windows Servers and has all the functionality needed to support Password Firewall, so utilizing PowerShell keeps the Password Firewall client software lightweight and easy to deploy and upgrade with minimal impact to operations. Furthermore, PowerShell scripting is a humanly readable format that is easy to understand (even for non-

programmers) and any legitimate security-based software solution should be able to show its source code without impacting the security of the solution.

Can I change the passwdfw.ps1 script?

There is nothing preventing you from changing this file. If you choose to, exercise extreme caution. The passwdfw.ps1 script is executed with SYSTEM level permissions so it is very important to follow all programming best practices so you don't expose your system to any security risks. For example, it would not be wise to log any of the usernames or passwords as this would compromise the security of your network. Be aware that re-installations and upgrades using the Password Firewall Easy Installer will overwrite any changes you've made to the passwdfw.ps1 script. Additionally, Password RBL will not be able to support any of your changes.

How do I get a report of how many bad passwords are being blocked?

The easiest way to do this is to use the Tracking IDs assigned to your Password RBL account. If you add your specific Tracking ID to the passwdfw.ini file (see the Additional Configuration section) then you can utilize the My Metrics page at PasswordRBL.com to obtain a report and download lifetime statistics.

How does password firewall fit in with Windows Password Policy?

Password Firewall extends the built-in Windows password policy with password blacklisting. Password Firewall will apply in addition to whatever portions of the built-in Password Policies you have chosen to implement. For maximum security, you should enable every built-in policy and use Password Firewall to block all the passwords that are bad but are not captured by the built-in policy (i.e., Password1, Monkey123, etc.).

I have followed the instructions for automated installation with Group Policy but installation is not happening. What is wrong?

Assuming that Group Policy is functioning normally and the GPO has been configured properly, then the most common reason for a failed automated install is either neglecting to upload the setup-passwordfirewall.exe file into the GPO Computer Scripts folder or you have specified the /LOG option as part of your automated installation, but the installer cannot open this file. This is likely because an intermediary folder in the provided path does not exist.

Additional FAQs

More FAQs are available on our website: www.PasswordRBL.com

Password Firewall Version History

Version	Notable Changes
Current Version	General performance improvements. No feature changes
6.00	Move blacklist queries to new prefix-query API method call. Additional parameter checking and encoding between components. Updates and clarification to logging. Capture Display Name during password change events for better log entries. Add timing check to verify all executions are within maximum limit.
5.21	Updates and clarification to some Event Log messages
5.20	Add second group membership query to Active Directory to confirm results from Global Catalog-based query
5.10	Add RequiredCharSets feature Create new EventIDs to clarify final decision of Password Firewall processing.
5.01	Bug fix for some improper formats of Proxy Port option causes passwords to be denied without check to AllowOnError
5.00	Add password DoubleCheck feature.
4.30	Add support for explicit proxies
4.20	Simplified GroupFilter code Changed Active Directory connectivity to .NET LDAP libraries
4.10	Added CustomBlacklistOnly feature to control which blacklists are queried when using a Custom Blacklist
4.00	Bug fix that prevented password changes by end-users who had certain special characters in their username.
3.50	Performance update for queries to Active Directory when utilizing the GroupFilter option.
3.10	Added unique session ID to each log entry in Event Log Added GroupFilterType option to choose if specified group is an Inclusion or Exclusion group.
3.00	Moved custom configuration settings out of PS1 file and into dedicated INI Added automated/silent install and uninstall support Added option to provide some configuration settings during interactive install Updated basic password policy to include passwords that contain username
2.30	Added new .NET-based Active Directory query function with fallback to previous PowerShell-based method
2.20	Consolidated logging function; unique Event IDs for each log message. Added dedicated exit function; move secure erasure of variables here. Prefer .NET v4 calls for event logging to remove warnings in log messages Adjust timeout values
2.10	Added GroupFilter feature
2.00	Added compatibility with new Custom Blacklist feature
1.10	Added compatibility and changed default hashing to PBKDF2
1.03	Maintenance release; enhancements, bug fixes
1.00	Original Release