Authlogics Windows Password Policy Agent Integration Guide

With PINgrid, PINphrase & PINpass Technology

Product Version: 3.3.5816.0

Publication date: April 2019

Authlogics, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

Table of Contents

Introduction

The Authlogics Password Policy Agent is a lightweight service designed to intercept password changes made on the Windows Domain in real time, process them against a policy to see if they comply, and store them securely in the Authlogics Server Password Vault. This ensures that all new passwords comply with the latest NIST SP 800-63B guidance and it keeps the Microsoft password database and the Authlogics Server Password Vault in sync at all times regardless of which mechanism is used to change/reset an AD password.

> **Note**
> The Password Policy Agent MUST be installed on all domain controllers in the Active Directory domain.

Authlogics Authentication Server is a multi-factor authentication system which provides:

- Token and tokenless, device and device-less multi-factor authentication.
- Award-winning transaction signing/verification technology.
- Self-service password reset and unlocking.
- Web Service API and RADIUS interfaces for connectivity.
- Multiple Authentication technologies:
    - PINgrid - Pattern Based Authentication.
    - PINphrase - Random Character Authentication
    - PINpass - OATH (TOTP) Compliant Authentication

Password-less logon for Active Directory

Windows Desktop Logon Agent

The Authlogics Desktop Logon Agent allows users to logon to Windows without having to enter their Windows password. This form of password-less logon is achieved by storing the AD Password in a Server Password Vault which is retrieved and delivered to the Windows desktop on the user's behalf when logging on. Logging onto Windows in this way ensures compatibility with existing Windows applications that rely on Active Directory credentials. Password-less logon is disabled by default and can be enabled on the Authentication Server via the MMC, and on the desktops by setting the "Enable Password-less functionality to remove the Active Directory password for logon" group policy option on the Windows Desktop Logon Agent.

Considerations

Password Policies

The Authlogics Password Policy Agent complies with NIST SP 800-63B guidance, whereas the Windows Default Domain Policy does not. The Windows password policy must be modified after deploying the Authlogics Password Policy Agent to avoid conflicts.

Requirements

The Authlogics Password Policy Agent can be deployed in stand-alone mode or integrated with the Authlogics Authentication Server (version 3.1.6346.0 or higher). In order to integrate with Authlogics Authentication Server Active Directory must be used. The SQL Server directory is not supported.

Internet Access

In order for the Password Policy Agent to communicate with the Authlogics Cloud Password Breach Database and obtain licencing information, all Domain Controllers will need access to the Internet. Access can be restricted to either of the following destinations depending on the capabilities of the network firewall:

- Destination URL: https://passwordpolicyservice.authlogics.com/api/*
- Host `passwordpolicyservice.authlogics.com` on port `443`

  and

- Destination URL: https://licencing.authlogics.com/api/*
- Host `licencing.authlogics.com` on port `443`

A proxy Server can be configured using Group Policy to allow access to the Internet. Proxy authentication will automatically be performed using the Windows Machine account credentials. If the proxy does not support Windows Authentication then anonymous access must be granted to the Domain Controllers.

Licencing

In stand-alone mode, a dedicated Password Policy Agent licence is required which can be configured in the licence wizard after setup. When integrated with an Authlogics Authentication Server, a Password Policy Agent specific licence is not required as it will utilise the existing Authentication Server licence. The number of Password Policy Agent users can be increased beyond the Authentication Server licence by adding an additional Password Policy Agent licence.

When using an Authlogics Authentication Server licence, only Active Directory users which are provisioned with the Authentication Server will be protected by the Password Policy Agent.

When using a Password Policy Agent licence, all the users in the forest must be licenced for Password Policy Agent. The licence cannot be used for specific user accounts.

Language Requirements

Authlogics Password Policy Agent is only available in English. Product support and documentation is only available in English.

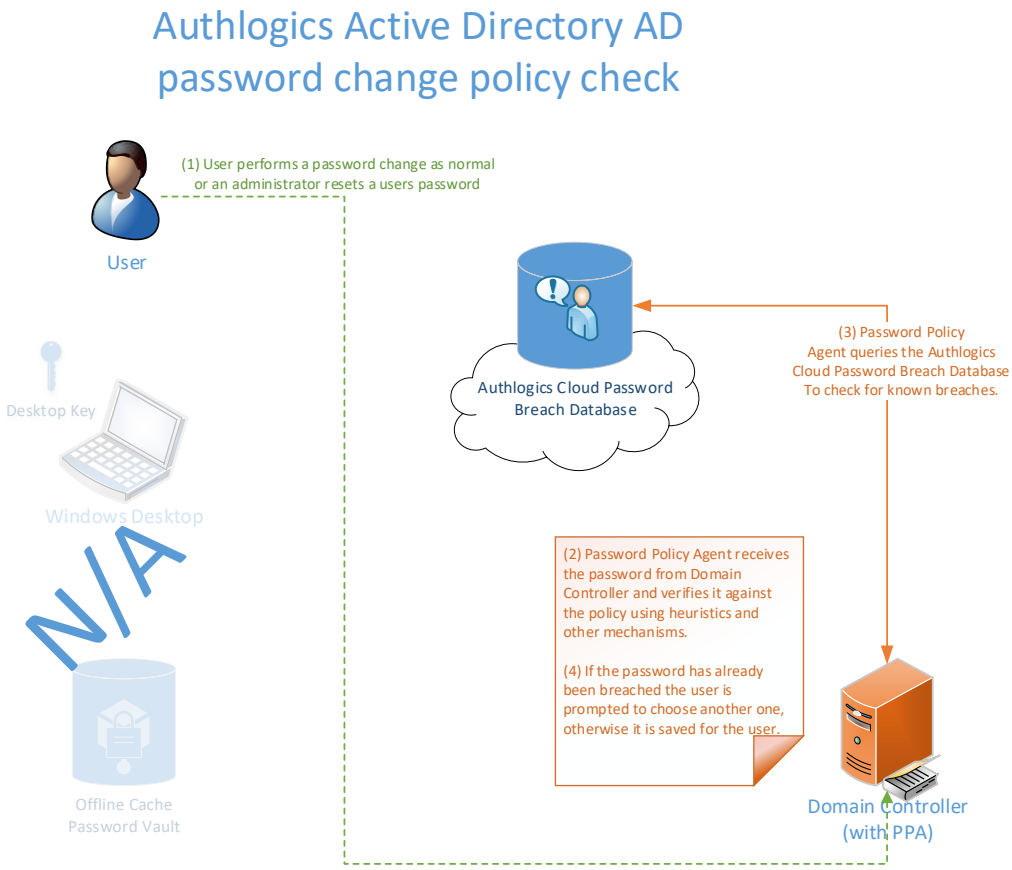
Design and Deployment Scenarios

The Authlogics Password Policy Agent has been designed to work seamlessly in a Windows and Active Directory environment.

The Password policy is controlled via Active Directory Group Policy for flexible, centralised management.

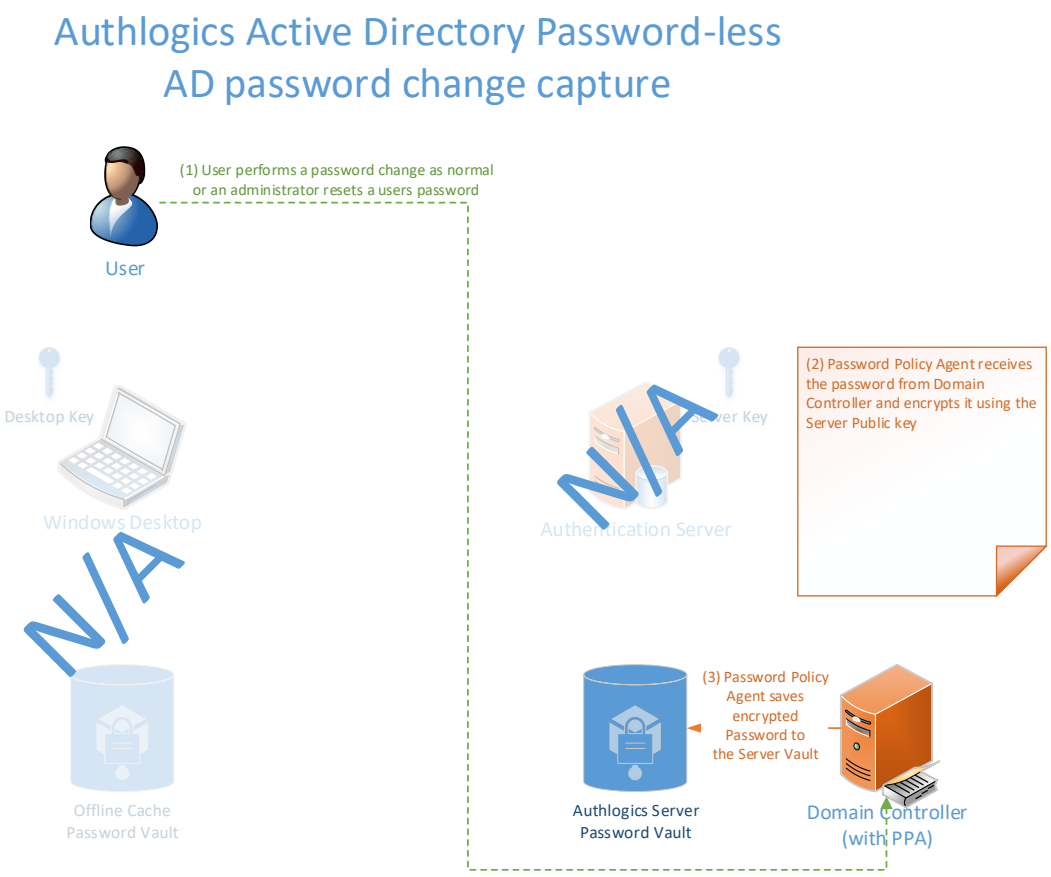
Active Directory password change workflow – Policy Check

The following workflows depict the steps performed during an AD password reset/change to check the password against the defined policy:



Active Directory password change workflow – Vault Update

The following workflows depict the steps performed during an AD password reset/change to update the Authlogics Server Password Vault:



Deployment

The following deployment overview walks through the installation process for deploying the Authlogics Password Policy Agent.

Overview

The Password Policy Agent can be deployed as a stand-alone product or in conjunction with the Authlogics Authentication Server.

This deployment section assumes that at least one Authlogics Authentication Server has already been installed and is functional. See the Authlogics Authentication Server Installation and Configuration Guide for further information on setting up the Authlogics Authentication Server.

Stand-alone deployment

A stand-alone deployment is suited to scenarios where only password policy checking is required, i.e. there is no requirement for Multi-Factor Authentication or Active Directory Password-less logons.

Authlogics Authentication Server deployment

If Multi-Factor Authentication or Active Directory Password-less logons is required then the Authlogics Authentication Server must be deployed.

Pre-requisites

The installer will check for pre-requisites and install them automatically where possible. The required pre-requisites are:

- Microsoft Visual C++ 2010 SP1 Runtime Libraries
- Microsoft .NET Framework 4.6.2

Note

The Visual C++ 2010 Runtime and .NET Framework 4.6.2 Libraries for 64bit systems are included in the agent installation package.

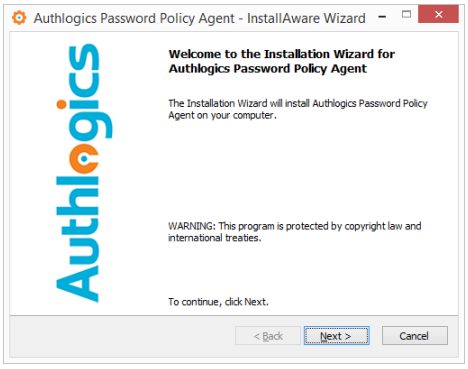
If the installation of a pre-requisite fails then the installation will also fail.

Installing/Removing the Authlogics Password Policy Agent

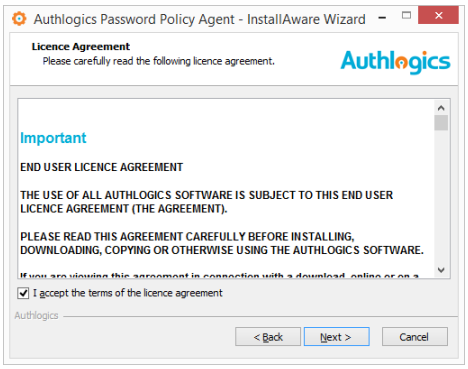
> **Note**
> The Authlogics Password Policy Agent is contained within a dedicated installer separate to the Authentication Server installation.

Running an installation

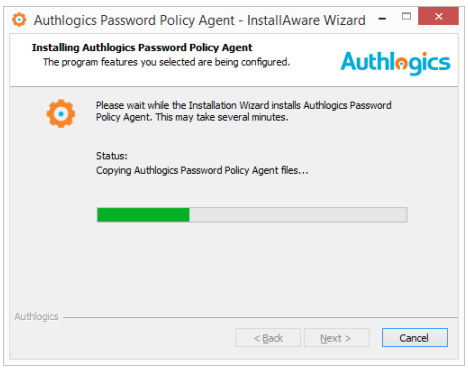
(1) To start the Authlogics Password Policy Agent installation, run the *Authlogics Password Policy Agent xxxxx.exe* installer with **elevated privileges**.



(2) Click *Next* to continue.



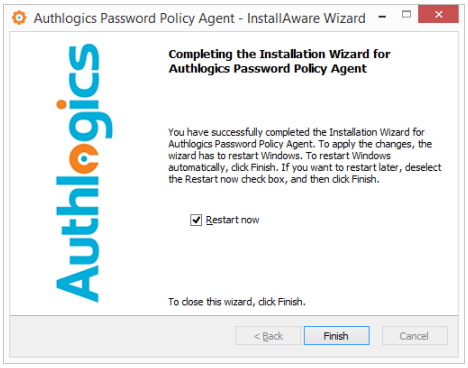
(3) After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



The installation is being performed.

Note

The Domain Controller MUST be restarted for changes to take effect.



(4) If you plan to reboot later untick the *Restart now* box.
Click *Finish* to complete the installation process.

(5) After the reboot, the Password Policy Agent Configuration will start automatically.

Running a removal

Uninstalling the Authlogics Password Policy Agent does NOT remove the password data from the Authlogics Server Password Vault.

If you want to disable the Password Policy Agent functionality this can be done via Group Policy. This avoids the need to uninstall which requires a reboot of the Domain Controller.

If you no longer require Authlogics Password Policy Agent you can remove it by performing an uninstall as follows:

To start the Authlogics Windows Password Policy Agent un-installation, execute the *Authlogics Password Policy Agent xxxxx.exe* installer or use the *Uninstall or change a program* option in Control Panel and click *Remove*.

Password Policy Agent Configuration

The Authlogics Password Policy Agent Configuration will start automatically once you log in after the setup reboot. It can be run again at any time from the start menu or desktop shortcut.

The Configuration utility performs the following tasks:

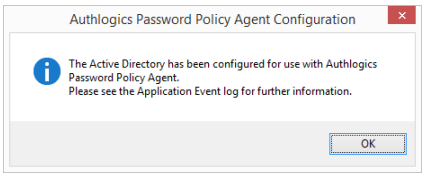
(1) Configures the Active Directory for use with Password Policy Agent.
   a. This may have already been done if the Authlogics Authentication Server is already installed.

(2) Import a licence for Password Policy Agent.
   a. This is not performed if Authlogics Authentication Server is already installed and licenced.

(3) Start the Password Policy Agent Windows Service.
   a. This is only performed if the service is currently not running.

(1) Start the Authlogics Password Policy Agent Configuration buy rebooting after setup, or afterwards from a shortcut.

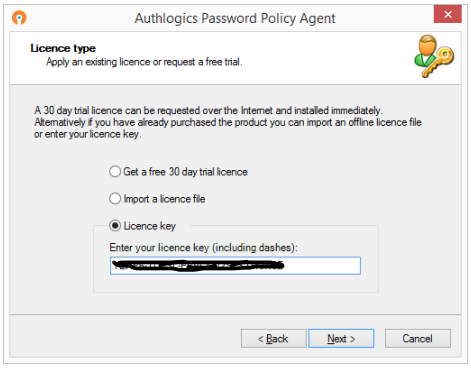
(2) If the directory was configured a notice will be displayed.



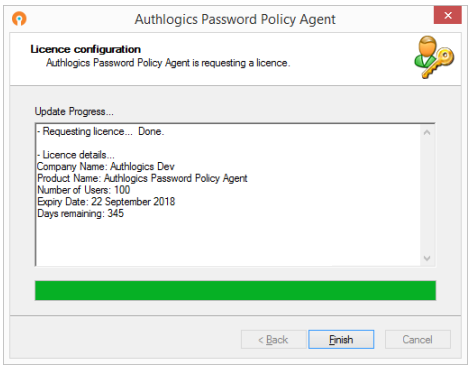
(3) Click *OK* to continue.

(4) If a licence is required then the Licence Configuration Wizard will start.

(5) Click *Next* to continue.

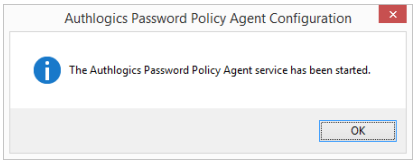


(6) Select a licence option and Click *Next* to continue.



(7) The licence is configured. Click *Next* to continue.

(8) If the Password Policy Agent Windows Service is not running it will be started and a confirmation is displayed.



(9) Click *OK* to continue.

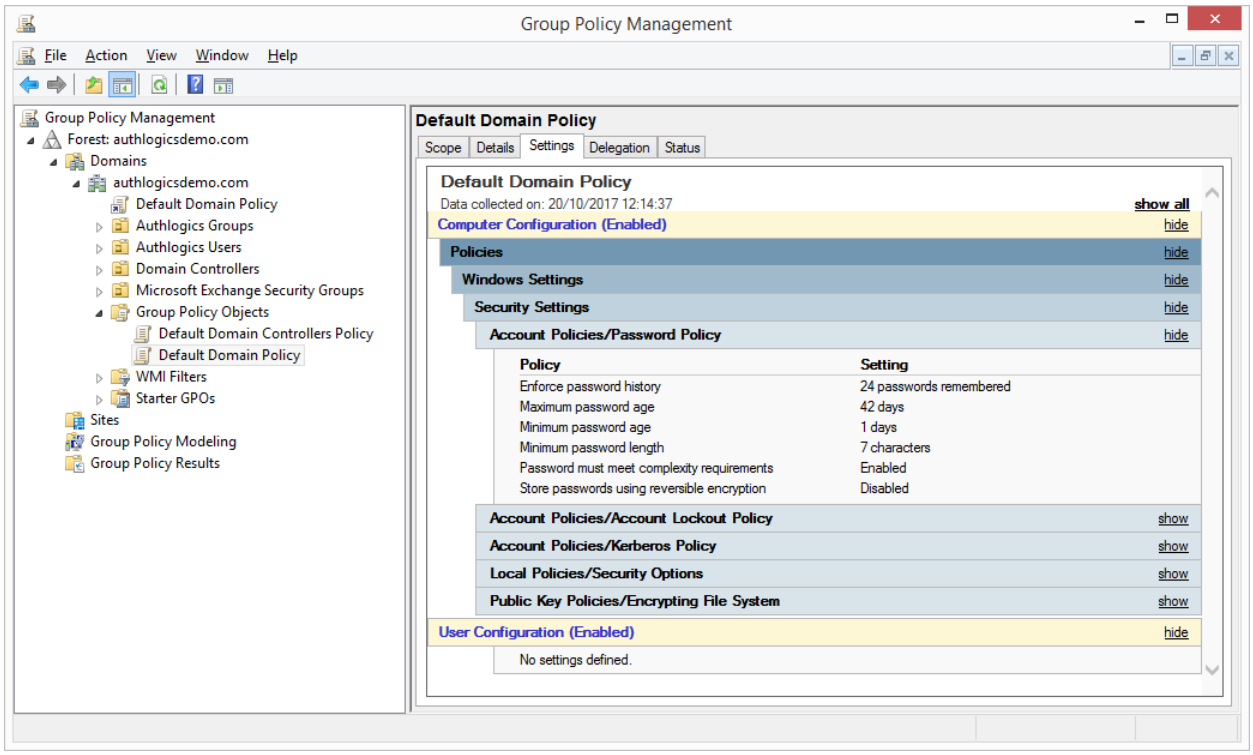
(10) The configuration is now complete. Check the Windows Application Event log for further information.

Active Directory Domain Password Policy

After installing the Authlogics Password Policy Agent on a Domain Controller it will be active immediately after the server reboot. The default Password Policy Agent policy, which is NIST SP 800-63 compliant, will conflict with the Active Directory Domain password policy. The Active Directory Domain password policy will always take precedence and my block a compliant password before allowing the Authlogics Password Policy Agent to analyse it. The Default Domain Policy password settings should be modified to avoid such conflicts.

Default Domain Policy

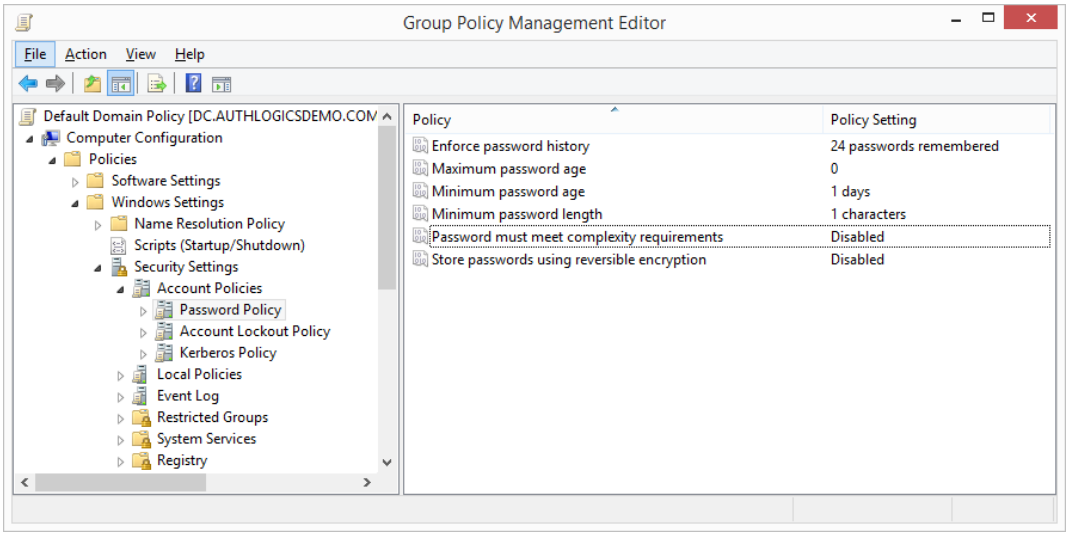
The following password settings apply to the Default Domain Policy by default:



Default Domain Policy Changes - REQUIRED

The following password settings for the Default Domain Policy must be changed so that Windows does not conflict with the Authlogics Password Policy Agent policy:

- **Maximum password age: 0**
    - This should be set to 0 to comply with NIST SP 800-63 which states that passwords should not periodically expire.
- **Minimum password length: 1**
    - This should be set to 1 so that it does not conflict with the Password Policy Agent Minimum Password Length setting.
- **Passwords must meet complexity requirements: Disabled**
    - This should be set to Disabled to comply with NIST SP 800-63B which states that passwords should not be forced to contain complexity rules.



Configuring the Authlogics Password Policy Agent Group Policy Settings

The Authlogics Password Policy Agent includes an AD Group Policy Template file `AuthlogicsPPA.adm` which is used to create policies. The *User Configuration* section of the GPO can be disabled as the settings only apply to the *Computer Configuration*.

By default, installing the Authlogics Windows Password Policy Agent does NOT disable any existing Password Policy existing on the target Domain Controller.

The following Active Directory Group Policy settings are available for configuring the agent:

Setting	Disable Password Policy Agent
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the Authlogics Password Policy Agent functionality without needing to uninstalling the product, which would require a reboot of the Domain Controllers. If you enable this policy no complexity and validity checks will be performed on the passwords thus deeming all received passwords as acceptable. If you disable or do not configure this policy then the agent will function as per the configured policy.	

Setting	Disable Fail-Safe
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting controls the behaviour of the agent in the case of a catastrophic failure. E.g. The agent is unable to connect to the Cloud Password Blacklist on the Internet, or the licence becomes invalid. Fail-safe relates to the security of the AD passwords, not the ability to change AD passwords, this is to ensure passwords are kept secure. If you enable this policy then any agent failure will result in password changes being ALLOWED. If you disable or do not configure this policy then any agent failure will result in password changes being DENIED.	

Setting	Disable Cloud Password Blacklist lookups
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents the agent from querying the Authlogics Cloud Password Blacklist database consisting of hundreds of millions of known previously hacked passwords. If you enable this policy then no checks against the Authlogics Cloud Password Blacklist database will be performed. If you disable or do not configure this policy a SHA-1 HASH of the password will be sent over SSL to the Cloud for analysis. The password will be rejected if it is a known/previously breached password found on the blacklist or a dictionary word. to comply with NIST SP 800-63B.	

Setting	Disable Local Password Blacklist lookups
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting allows the agent to query a local Password Blacklist database consisting of passwords entered by an administrator. If you enable this policy then no checks against the local Blacklist database will be performed. If you disable or do not configure this policy then entered passwords will be compared with the contents of the local database and is also be available for use by the heuristics engine. The password will be rejected if it is found on the custom blacklist to comply with NIST SP 800-63B. Refer to ***Configuring the Local Password Blacklist Lookups*** for information on how to define the Local Password Blacklist.	

Setting	Minimum Password Length
Values	(4 - 127)
Default	8
Description	
This policy setting sets the minimum number of characters allowed for a compliant password. Setting this value too high may make the password too difficult for users to remember the password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the length of the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 8 will be used to comply with NIST SP 800-63B.	

Setting	Maximum Password Length
Values	(4 - 127)
Default	127
Description	
This policy setting sets the maximum number of characters allowed for a compliant password. Setting this value too low may stop users from selecting passphrases which are typically more secure than passwords. The password will be rejected if the length of the password is more than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 127 will be used to comply with NIST SP 800-63B.	

Setting	Minimum Lowercase Characters
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the minimum number of allowed lowercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of lowercase letters in the password is less than the value specified. If you enable this policy then you must specify a value.	

If you disable or do not configure this policy then the check will not be performed.

Setting	Minimum Uppercase Characters
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the minimum number of allowed uppercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of uppercase letters in the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Numeric Characters
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the minimum number of allowed numeric digits a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of numeric digits in the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Special Characters
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the minimum number of allowed special characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of special characters in the password is less than the value specified. The following are recognised as special characters ! " # % & ' ( ) * , - . / : ; ? @ [\ ] _ { }' If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Unicode Characters
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the minimum number of allowed Unicode characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of Unicode characters in the password is less than the value specified. Unicode characters are non-printable characters that are not punctuation or alphanumeric characters. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Maximum Repeating Characters
Values	(0 - 126)
Default	8
Description	
This policy setting sets the maximum number of times a character can be repeated anywhere within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 8 will be used to comply with NIST SP 800-63B.	

Setting	Maximum Consecutive Repeating Characters
Values	(0 - 126)
Default	3
Description	
This policy setting sets the maximum number of times a character can be consecutively repeated within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 3 will be used to comply with NIST SP 800-63B.	

Setting	Maximum Sequential Characters
Values	(0 - 127)
Default	3
Description	
This policy setting sets the maximum number of times a sequence of characters can be used within a compliant password. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of characters in a sequence is more than the value specified. Sequential characters are both forward and backwards i.e. ABC and CBA are deemed to be sequential. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 3 will be used to comply with NIST SP 800-63B.	

Setting	Allow Username
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting allows the use of the users' username within the password. If you enable this policy a password will not be blocked if the user's username is found within the entered password. If you disable or do not configure this policy then the password may not contain the username to comply with NIST SP 800-63B.	

Setting	Maximum Allowed Characters From Username
Values	(1 - 127)
Default	Disabled
Description	
This policy setting sets the maximum number of characters from a user's username that are allowed in a password. Passwords will be rejected if the number of characters from the user's username in a password is more than this value specified. e.g. If the username is Robert and the value is 3 then passwords containing "robe", "ober" and "bert" will be rejected. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Maximum Sequential Keyboard Characters
Values	(0 - 5)
Default	Disabled
Description	
This policy setting sets the maximum sequential keyboard characters allowed within a compliant password. The password will be rejected if the number of keyboard layout characters in sequence is more than the value specified. Sequential characters are both forward and backwards i.e. "qwerty" and "ytrewq" with both be deemed to be sequential. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Disallow Month and Day names
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disallows the use of month and day names in the password. If you enable this policy a password will be rejected if a month or day name is found in an entered password. If you disable or do not configure this policy then the check will not be performed.	

Setting	Disallow spaces
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disallows the use of a space character in a password. If you enable this policy a password will be rejected if a space is found in an entered password. If you disable or do not configure this policy then the check will not be performed.	

Setting	Disable Heuristic Scanning
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting controls the heuristic scanning engine behaviour on passwords. Heuristic scanning will undergo a series of checks where known character replacements are detected and reverted to their original base value and then revalidated for compliance. For example, '@' reverts to 'a', '!' to 'i' etc. If you enable this policy the heuristic scanning engine will not be active. If you disable or do not configure this policy then heuristic scanning will be performed to comply with NIST SP 800-63B.	

Setting	Enable Cloud Heuristics Scanning
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting controls the heuristic scanning engine behaviour on passwords with the Authlogics Cloud Password Breach Database. Heuristic scanning will undergo a series of checks where known character replacements are detected and the various derivatives will the evaluated to see if they have been breached. For example, '@' reverts to 'a', '!' to 'i' etc. If you enable this policy the heuristic scanning will be used when checking the Authlogics Cloud Password Breach Database. Warning: By enabling this policy the full password hash will be sent over the Internet to Authlogics as k-Anonymity cannot be used. If you disable or do not configure this policy then heuristic scanning will not be performed with the Authlogics Cloud Password Breach Database and k-Anonymity will still be used.	

Setting	Proxy Server Host
Values	FQDN or IP Address of the Proxy Server
Default	{blank}
Description	
This policy setting configures the Proxy Server Host name which will be used to connect to the Internet for access to the Authlogics Cloud Password Breach Database on the URL https://passwordpolicyservice.authlogics.com/api/*. If you enable this policy you must specify a FQDN or IP Address, e.g. proxy.mycompany.com If you disable or do not configure this policy a proxy server will not be used and a routable Internet connection will be required.	

Setting	Proxy Server Port
Values	(1024 – 65535)
Default	8080
Description	
This policy setting configures the Proxy Server TCP Port number which will be used to connect to the Internet. The server name will be located automatically via Active Directory lookups. This setting MUST be used in conjunction with the "Proxy Server Host" policy setting. If you enable this policy you must specify a TCP port number, e.g.8080 If you disable or do not configure this policy the default port 8080 will be used.	

Setting	Enable Debug Logging
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enabled debug logging on all servers running Password Policy Agent. This should only be enabled if requested by an Authlogics Support engineer. This setting performs the same function as manually setting the LoggingEnabled registry key to 1. If you enable this policy, debug logging will be active. If you disable or do not configure this policy then debug logging will not be active.	

Configuring the Local Password Blacklist Lookups

Authlogics Password Policy Agent provides administrators with the ability to insert their own passwords in a locally defined blacklist that will be rejected. The blacklist allows for the rejection password based on full passwords as well as those matching wildcard characters "*" and "#".

To enable the local Password Blacklist, modify the contents of the Text file "blacklist.txt" located in the Authlogics Password Policy Agent installation folder "C:\Program Files\Authlogics Password Policy Agent\". Once a blacklist file has been defined, this file will need to be copied to all the Domain Controllers where PPA has been installed.

Once modified, restart the Authlogics Password Policy Agent server service for the changes to take the effect.

> **Note**
> Checks against the local Blacklist will be performed when the policy ***Disable Local Password Blacklist lookups*** policy is **not** enabled i.e. Disabled/Not configured.

Wildcard Usage within Local Blacklist

To enforce password rejection, full words and wildcards characters "*" and "#" can be added to the local blacklist file. If a password matches what is defined in the local blacklist file, the password will be rejected. How a password is processed is dependent on the positioning of the wildcard i.e. front, middle, back.

The wildcard "*" refers to any character for any length, If a "*" is entered on its own, all passwords will be rejected.

The wildcard "#" refers to a single numeric number and translates to 9 i.e. **##** = 99. Numeric numbers within passwords will be converted to a numeric and then, if less than the restricted value, the password will be rejected.

The following table shows examples of how PPA will process the provided password based on the Blacklist entry.

Blacklist Entry	Description	Password	Result
Authlogics	Direct matches to a restricted word will be rejected	Authlogics	Rejected
		Authlogics01	Accepted
Auth*	Passwords starting with ***Auth*** will be rejected	Authlogics	Rejected
		HelloAuthlogics	Accepted
Auth	Passwords with ***Auth*** in the middle will be rejected	Authlogics01	Accepted
		heloAuth123	Rejected
***Auth**	Passwords ending with ***Auth*** will be rejected	heloAuth123	Accepted
		Authlogics	Accepted
		helloAuth	Rejected
Authlogics##	Reject any Password starting with word ***Authlogics*** ending in 2 digits	Authlogics12	Rejected
		Authlogics12	Rejected
		Authlogics112	Accepted
		Hellowworld12	Accepted
##Authlogics	Reject any Password starting with 2 digits and ending with the word ***Authlogics***	12Authlogics	Rejected
		123Authlogics	Accepted
##*	Reject any password starting with 2 digits	12Authlogics	Rejected
		Authlogics12	Accepted
		1Authlogics	Accepted
		123Authlogics	Rejected
***##**	Reject any password ending with 2 digits	12Authlogics	Accepted
		Authlogics12	Rejected
		Authlogics123	Accepted
##	Reject any password with 2 consecutive digits in the middle of the password.	12Authlogics	Accepted
		Authlogics12	Accepted
		Auth12logics	Rejected
		Authlogics123logics	Accepted