

Password Security Management

Quick Start Guide

Product Version: 4.2.1030.0

Call us on: +44 1344 568 900 (UK/EMEA) +1 408 706 2866 (US)

Email us: sales@authlogics.com



Authlogics, 329, Doncastle Road, Bracknell, Berkshire, RG12 8PE, UK www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866



Introduction

This guide provides an overview of the steps required to setup Authlogics Password Security Management in a new environment. For detailed information about a specific feature or deployment scenario please see the *Authlogics Authentication Server Installation and Configuration Guide*.

Considerations

- (1) Authlogics Password Security Management requires a Windows Server and an Active Directory domain to be available before installation.
- (2) A Domain Administrator / Enterprise Administrator account is required to perform the installation.
- (3) After the installation, the server will require a reboot.
- (4) Internet access to <u>https://*.authlogics.com</u> is required.

Required information

- (1) AD administrator credentials.
- (2) SMTP Server details: name, port, authentication requirements.
- (3) The DNS name for the server.
- (4) Understanding of which password policy settings to use.

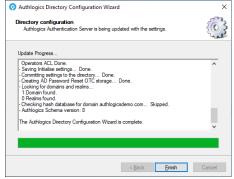


Installing the Authentication Server

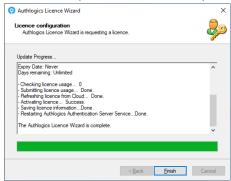
- (1) Download the Authentication Server installer from <u>https://authlogics.com/downloads/</u> and extract the ZIP.
- (2) Run the setup file in the Install folder.
- (3) Follow the Installation Wizard instructions to install the product binaries.

O Authlogics	Authentication Server - InstallAware Wizard	-		\times
	Authlogics Authentication Server am features you selected are being configured.	Aut	hløg	ics
Ø	Please wait while the Installation Wizard installs Authle Authentication Server. This may take several minutes.			
	Status: Configuring Windows Server Roles			
Authlogics ——	< Back	ext >	Can	:el

(4) Follow the Directory Configuration Wizard to setup the AD for use with Authlogics.



(5) Follow the Licence Wizard to configure a licence for Authlogics PSM. If you do not have a licence key the wizard can request a 30 day evaluation licence for you.



(6) **Reboot the Server** after the Authlogics Management Console loads to complete the initial setup.



Configuring the Authentication Server

- (1) Launch the Authlogics Management Console, right click "Authlogics PSM" and select properties.
- (2) Configure the SMTP Server settings to be able to deliver alerts and new user emails.

Running the PSM Wizard

- (1) Right click "Authlogics PSM" and select "Password Security Management Wizard".
- (2) Tick the domains in the forest to protect with PSM.

Password	Security Management Wizard	×
	and Shared Password Protected Domains Domains for use with Password Security Management.	3
Directory Br	ecuity Management provides real-time and retrospective protection of Act eached and Shared Password per Domain. Selected domains will be confi Breached and Shared Password protection and unselected domains will n Enabled on Domains	gured
	< Back Next >	Cancel

(3) Choose a schedule when PSM should look for new breached and shared passwords, as well as send alerts.

Password Security Management Wizard	×
Remediation and Alerting Processing Schedule Configure when scheduled Remediation and Alert sending should run.	3
Scheduled user account scans for breached and shared passwords are important maintaining the security of passwords as they could become compromised after the been changed.	
Remediation and Alerting Schedule Schedule start: 15 June 2021 C2:00:00 Pepeet cycle: Daily Recur every: 1 day	
< <u>B</u> ack <u>N</u> ext >	Cancel

(4) Choose the action to take when breached and shared passwords are found.

O Password Security Management Wizard	×
PSM Remediation and Alert Actions Choose the action to take when a specific p	password issue is found.
When a password scan finds a breached or sh automatically updated to reduce its risk. Alerts people regarding the action taken.	
Breached Password Found	Shared Password Found
Set account status to:	Set account status to:
No change 🗸 🗸	No change ~
Send alert notification email to:	Send alert notification email to:
Administrators	Administrators
Manager User	Manager
User	User
	< Back Next > Cancel
	Career Tour >



(5) Choose the action to take when dormant accounts are found

Dormant Account Remediation and Alert Actions Choose the action to take when a specific account issue is found.				
	ccount, the account status can be automatically ent via email to one or more relevant people			
Dormant AD Account Found	Dormant MFA Account Found			
Set account status to:	Set account status to:			
No change v	No change \sim			
Send alert notification email to:	Send alert notification email to:			
Administrators	Administrators			
	Manager			
Manager				
User				

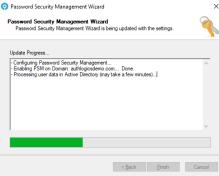
(6) PSM will protect all ENABLED user accounts in the domain. This can be limited to members of an AD group if required. This can be useful for gradual deployments of new policy settings to users, or if sufficient licences are not currently available.

. ,	0	
O Password Se	ecurity Management Wizard	×
	ecurity Management Users optional group of user accounts who will use PSM.	
is not specifie	word Security Management protection to members of d then all enabled user accounts in the AD Forest will SM user requires a PSM locnce. Password Security Management Users Enable Password Security Management User	be protected.
	< Back	Next > Cancel

(7) PSM will perform alerting and remediation on all PSM enabled user accounts. Accounts can be excluded from remediation and alerting by adding them to an AD group. This may be useful for service accounts.

Password Security Management Wizard	×
Remediation and Alerts Exclusion Select an optional group of user accounts to exclude from remediation and alerts.	3
Remediation and Alerts will not be actioned on members of the specified group, howev real-time password policy checks will still apply when a password is changed. This can useful for Service Accounts.	
Remediation and Alerts Exclusion	
Enable Remediation and Alerts Exclusion group	
Browse	
browse	
< <u>B</u> ack <u>N</u> ext >	Cancel

(8) Applying settings.



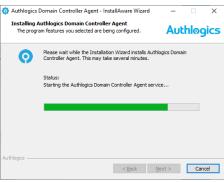
Applying the settings may take some time depending on how many users exist in the AD.



Install the Domain Controller Agent

The Domain Controller agent must be installed on ALL domain controllers in the domain to protect all password changes are protected. The domain controllers MUST be rebooted after the agent is installed. Installing the agent will have no effect on password changes until the policy is configured later on.

- (1) Download the Domain Controller Agent installer from <u>https://authlogics.com/downloads/</u> and extract the ZIP.
- (2) Start the installation by running the "Authlogics Domain Controller Agent 4.0.xxxx.x.msi" file.



Note Note

If Windows does not allow the installer to be run due to a policy, simply start an Admin Command prompt and run the MSI from the command prompt to ensure it is launched with admin rights.

(3) Restart the Domain Controller when complete.

Authlogics Domain Cor	ntroller Agent - InstallAware Wizard — 🗌 🗙
<u>S</u>	Completing the Installation Wizard for Authlogics Domain Controller Agent
<u> </u>	You have successfully completed the Installation Wizard for Authlogics Domain Controller Agent. To apply the changes, the wizard has to restort Windows. To restart Windows automatically, dick Finish. If you want to restart later, deselect the Restart now check box, and then dick Finish.
Auth	Restart now
	To close this wizard, click Finish.
	< Back Finish Cancel



Configuring the Authlogics Password Policy

The Authlogics Password Policy is configured using Active Directory group policy. The policy must be applied to the Domain Controllers as well as the Authlogics Authentication Servers.

These steps are typically done on a Domain Controller however can be done from anywhere that has the AD management tools installed.

- (1) Open the Group Policy Management Console.
- (2) Create a NEW Group Policy Object called "Authlogics Password Policy".
- (3) Edit the new policy and import the "AuthlogicsDCAgent.admx" and "AuthlogicsPasswordPolicy.admx" template files. The templates can be found inside the downloaded ZIP files GPO folder, or the "C:\Program Files\Authlogics Authentication Server\" on the Authlogics Authentication Server.
- (4) Expand the Authlogics Password Security Management policy tree and set "Enable Authlogics Password Policy" to Enabled.

Group Policy Management Editor					-	×
Eile Action View Help						
I DLA [SUB-DC.SPAWN.AUTHLOGICSDEMO.COM] Policy	Password Security Management					
V 🛃 Computer Configuration	Enable Authlogics Password Policy	Setting	State	Comment		
V 🦀 Policies	Enable Authority assword Folicy	Exception Password Policy	State	connent		
> in Software Settings	Edit policy setting	Primary Password Policy				
> iii Windows Settings		Brinary Password Policy	Not configured	No		
 Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer. Authlogics 	Requirements: Authlogics Password Security	Enable Authogics Password Policy	Not configured	NO	4	
→ Authlogics	Management 4.0					
Password Security Management						
Exception Password Policy	Description: This policy setting enables the					
> in Primary Password Policy	Authlogics Password Policy					
> 🧮 Control Panel	functionality on all Agents and					
> 🔛 Network	Servers where this Group Policy is					
Printers 1	applied.					
Server Server	If you enable this policy complexity					
> 🧾 Start Menu and Taskbar	and validity checks will be performed					
> 🧮 System	on the passwords.					
 Windows Components Classic Administrative Templates (ADM) 	If you disable or do not configure this					
 Classic Administrative Templates (ADM) All Settings 	policy then no password processing					
> Preferences	will function as per the configured policy thus deeming all passwords as					
Visit User Configuration	acceptable.					
> Policies						
> Preferences						
	Extended Standard					
1 setting(s)						

- (5) Review the rest of the password policy options and set them accordingly. In most cases, the default complexity rules should suffice.
- (6) We recommend enabling the following features:
 - a. Enable Passphrases = Enabled
 - b. Password Expiry Default Zone
 - c. Password Never Expires Zone





(7) Link the new "Authlogics Password Policy" to the Domain. Configure the security filtering to "Domain Controllers" and "Authlogics Servers" groups only.

📓 Group Policy Management					-		×
<u>File Action View Window H</u> elp						-	Б×
Group Policy Wanagement Group Policy Group	Authlogics Password Polic Score [Details Setting: Delegation: Display links in this (ocation: The following stee, domains, and OL Location authlogicsdemo.com	authiogicademo.com authiogicademo.com Brance Inked to this GPO: Erforced No	Link Enabled Yes	Path authlogicsdemo.com			~
Results	Name Reg. Authorized to Control up op Authorized to Control up Authorized to Control up Add Bem WHI Filtering This GPO is linked to the following b (conce)	CSDEMO\Authlogics Serven) CSDEMO\Domain Controllers) ove Propetties					



Disabling the Windows Password Policy

The Windows password policy must be disabled so that it does not conflict with the Authlogics password policy.

- (1) Open the Group Policy Management Console.
- (2) Edit the "Default Domain Policy".
- (3) Change the following settings. The settings must be set to the specified values, DO NOT set them to "Not Defined":
 - a. Maximum password age: 0
 - b. Minimum password length: 1
 - c. Passwords must meet complexity requirements: Disabled

Group Policy Management Editor		- 🗆 X
Eile Action View Help		
🗢 🔿 🔁 📆 🗙 🔒 🛛 🖬		
▼ ● Computer Configuration ↑ Policies > > ● Policies > > ● Name Resolution Policy > > ● Software Settings > > ● Name Resolution Policy > > ● Dipoled Printers > > ● Account Policies > ● Account Policies > ● Exercity Settings > > ● Account Policies > ● Exercited Groups > > ● Software Settinges > > ● Exercited Groups > > ● Software Network (IEEE 802.3) Policie > ■ Wired Network (IEEE 802.3) Policie > ■ Wired Network (IEEE 802.3) Policie > ■ Public Key Policies > ■ Public Key Policies > ■ Public Key Policies	Policy Enforce password history Maimum password age Minimum password length Minimum password length Minimum password length audit Password nut: meet complexity requirements Store passwords using reversible encryption	Policy Setting 24 passwords remembered 0 1 days 1 characters Not Defined Disabled Disabled
< >>	٢	>



Testing password changes and schedules

Group Policy changes can take up to 15 minutes to apply to a server and up to a further 15 mins to take effect within Windows. To avoid waiting this can be sped up by running "GPUPDATE /FORCE" from an admin command prompt and rebooting the server.

Testing password changes via the Self Service Portal

- (1) On the Authlogics Authentication Server log in to the Self Service Portal.
- (2) Enter some test passwords to see which pass/fail the current policy.

Authlogics Self Service Portal × +				-	×
← → C ▲ Not secure https://localhost:1-	4443	ŵ	£^≡	Ē	
Authlogics	authlogics self service portal Account	(adm	inistrato	or) 🤱	
Account MORE View User Guide	Enter the number used to deliver text / SMS messages to your phone. Use international dialing code format, e.g. *+44 700 123 4567*.				
Logout	Mobile / Cellular Number Number Save ✓ At least 8 characters long ✓ No more than 9 of the same character				
	✓ No more than 4 of the same character in a row (e.g. aaaa) often. ✓ Not used by another user × Not previously breached s password in each box below. A longer password can be password	be chang	jed less		
	Confirm password				
	Your new password will expire on 16 August.				
	42 days never				
	Change				
	To unlock your Windows account, click the Unlock button.				

- (3) The following "test" passwords are designed to pass most password complexity checked but are contained within our ONLINE breach database and thus should fail.
 - Authl0g1c\$Test!
 - IL0v3Coff33!
 - Н@рруD@у5
 - Sh@nk5t3r5!



$ \rightarrow$ C \land Not secure $ $ https:/	localhost:14443	íô	£≦	æ	9
Authlogics	AUTHLOGICS SELF SERVICE PORTAL ACCOUNT	(adn	ninistrato	or) 1 1	
Account MORE	Your Password was updated successfully.				
View User Guide Logout	Enter the number used to deliver text / SMS messages to your phone. Use international dialing code format, e.g. *+44 700 123 4567*.				
	Mobile / Cellular Number Number Save To change your Windows password, enter your new Windows password in each box below. A longer your Number of the same of the sa	ger password can be chan	ged less		
	often. Password Confirm				
	Your new password will never expire . 42 days	never			
	Change	never			
	To unlock your Windows account, click the Unlock button.				

(4) When a valid password is entered, click "Change" to save it.

- (5) Look for Event ID 1425 on the domain controller Application Event Log showing the successful change.
- (6) Look for Event ID 1400 on the Authlogics Authentication Server Application Event Log showing the successful change.

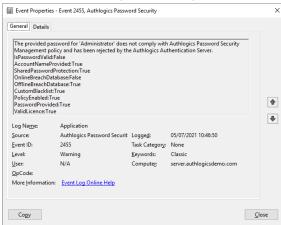
Testing password changes via Active Directory

- (1) On the Domain Controller open Active Directory Users and Computers.
- (2) Locate a test user account, right click and select "Reset Password..."
- (3) Enter a known non-complaint password, e.g:
 - Authl0g1c\$Test!
 - ILOv3Coff33!
 - H@ppyD@y5
 - Sh@nk5t3r5!
- (4) Ensure the password is not accepted.





(4) Look for Event ID 2455 on the domain controller Application Event Log showing the unsuccessful change, including the results of the checks that were performed.

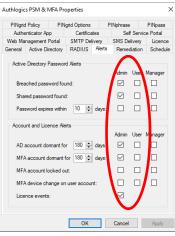


Note Note

Event ID 2455 will appear twice when resets are performed via Active Directory Users and Computers due to a known issue with the Active Directory Users and Computers tool. This does not happen during normal user password changes.

Testing Alerting and Remediation

(1) Ensure alerts are enabled for the administrators and users.





(2) Ensure remediation is configured.

PINgrid Policy	PIN	grid Options	F	PINphrase	PINpass	
Authenticator App		Certificates		Self Service Portal		
Web Management Portal		SMTP Delivery		SMS Delivery	Licence	
General Active Dir	ectory	RADIUS	Alerts	Remediation	Schedule	
PSM Remediation	Action					
Domant AD Ac	count	No chang	e			
	1					
	1	if account	not use	d within 180	- days	
Breached Password:		No change 🗸 🗸				
Shared Passwo		Marchan				
Shared Passwol	ra:	No chang	e		/	
Enable PSN	I Reme	diation and A	lerts Exc	clusion group		
				Brow	rse	
MFA Remediation	Action					
Dormant MFA A	ccount:	No chang	e		~	
		if account	not use	d within 180	🗘 days	
		= uccount	1101 000		e days	

(3) On the schedule tab, click "Run Now" and click "Yes".



- (4) To avoid waiting up to 15 mins for the schedule to run simply restart the "Authlogics Authentication Server" Windows service.
- (5) Look for Event IDs 1966 and 1962 on the Authlogics Authentication Server Application Event Log to show when the tasks have completed. Also look for Event ID 1953 to see when the schedule will next run.
- (6) Check the user and administrator mailbox for alters:

🔲 🔯 Mail – Administrator@au	thlogis x + X
\leftarrow \rightarrow C \blacktriangle Not s	ecure https://localhost/owa/#path=/mail
iii Mail	🔺 🌣 ? 💽
Search Mail and People 👂	⊕ New ×
Favourites Administrator	Inbox Filter Authlogics Shared Password Security Administrator Summary administrator@authlogicsdemo
Inbox Drafts	Authiogics Breached Password Security I, Adminit 0958 Breached Password Security for authiogicsdemo.com To
Sent Items Deleted Items Junk Email Notes	administrator@authlogicsdemo Authlogics Shared Password Security for authlogicidemo.com To: A Shared Password Security for authlogicidemo.com To: A
	To: Authiogics Administrators Email: Administrator@authiogicsdemo.com A scan of the Active Directory database of the domain authiogicsdemo.com has found that the foliowing user accounts are currently using a shared / non-unique password in the domain, which does not comply with the password policy:



🔲 📴 Mail – Administrator@au	uthlogic x +	-	o ×
\leftarrow \rightarrow C \blacktriangle Not s	secure https://localhost/owa/#path=/mail	<u>ن</u>	g
🗰 Mail		\$?	
Search Mail and People	⊕ New ♥	5	2 Undo
Favourites	Inbox Filter - Authlogics Breached Password Security Administrator Summary		ĺ
Administrator Inbox Drafts	■ administrator@authlogicsdemo ■	Reply a	II ¥
Sent Items Deleted Items Junk Email Notes	administrator@authlogicsdemo Authlogics Shared Password Security Administr. 02:58 Shared Password Security for authlogicsdemo.com To: A Breached Password Security for authlogicsdemo.com		
	To: Authlogics Administrators Email: Administrator@authlogicsdemo.com A scan of the Active Directory database of the domain authlogicsdemo com has four that the following user accounts are currently using a known breached password , which does not comply with the password policy: • Administrator [Never Expires] Access the Authlogics Password Security Portal for details on public password brea affecting your company. Password Security Portal		
	Powered by Authlogics		

(7) Verify the remediation action was performed on the reported accounts:

Addie Hintz Properties					×
Member Of Pa	ssword Re	plication	Dial-in	Envir	onment
Sessions Remote of	ons Remote control Rem			Profile	COM+
General Address	Account	Profile	Telephone	s Org	anization
User logon name: State minz User logon name (pre-1 AUTHLOGICSDEMOV Logon Hours Unjock account Account antices:		000): addie.h	ogicsdemo.co		~
User must chang	e passwor	d at next logo			^
Password never Store password u		sible encryptic	on		~
Account expires Never End of:	4 August	2021]-
ОК		Cancel	Apply		Help





Monitoring PSM Usage

Authlogics Server includes a Dashboard to graphically display the state of your PSM deployment.

Launch the Authlogics Admin portal via https://localhost:14443/admin.

Select System - Dashboards - Password Security.

The dashboard reflects MFA actions for:

- External Breaches
- Total Accounts at Risk
- Failed Password Changes
- Accounts at Risk





