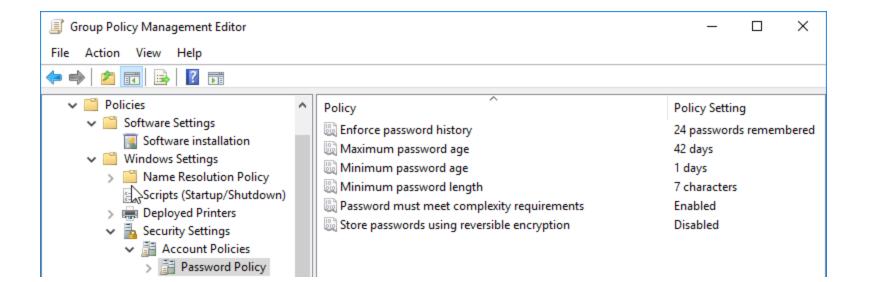
Securing Passwords with GPO Password Policies



Microsoft Password Complexity Requirements

In Windows 10 and Active Directory, we can enable Microsoft's **Password must meet complexity requirements** policy, which ensures user passwords are complex. This is enabled by default in the Default Domain Policy in AD.

Group Policy Management Editor			_		×	
File Action View Help						
🗢 🏟 🚈 📰 📴 🖥 🖬						
 Policies Software Settings Software installation Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings 	*	Policy © Enforce password history © Maximum password age © Minimum password age © Minimum password length © Password must meet complexity requirements © Store passwords using reversible encryption	Policy Setting 24 passwords remembe 42 days 1 days 7 characters Enabled Disabled		mbered	
 Security Settings Account Policies Password Policy 						

vord must meet o		
	complexity requirements Properties	?
urity Policy Setting	Explain	
anty rolicy Setting		
-		
Password must n	neet complexity requirements	^
This security sett complexity requir	ting determines whether passwords must meet ements.	
If this policy is en minimum requiren	nabled, passwords must meet the following ments:	
name that excee Be at least six ch	user's account name or parts of the user's full sd two consecutive characters naracters in length ars from three of the following four categories:	
English uppercas	se characters (Athrough Z) e characters (a through z)	
Complexity requir	characters (for example, !, \$, #, %) rements are enforced when passwords are ted.	
changed or creat		
		÷
Changed of crea		ľ

Cance

Password Complexity Requirement Details

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
 - Complexity requirements are enforced when passwords are changed or created.

Microsoft Minimum Password Length

We can also enable Microsoft's **Minimum password length** policy to further make a password more secure, which ensures user passwords are complex. This value is set to 7 by default for the Default Domain Policy in AD.

Group Policy Management Editor			– 🗆 X			
File Action View Help						
 Policies Software Settings Software installation Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings 	^	Policy Enforce password history Maximum password age Minimum password age Minimum password length Password must meet complexity requirements Store passwords using reversible encryption	Policy Setting 24 passwords remembered 42 days 1 days 7 characters Enabled Disabled			
✓ J Account Policies						

Password Polic

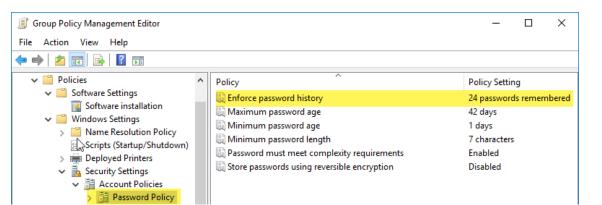
Minimum pa	ssword le	ngth Pro	perties	?		×
Security Polic	y Setting	Explain				
This se that a value o no pas Defaul 7 on d 0 on st Note: 1	password f of between sword is re t: omain cont and-alone	ing determ for a user a 1 and 20 equired by trollers. servers. member of	nines the least number of cha account may contain. You ca characters, or you can estal setting the number of charac computers follow the configur	an set a blish that cters to 0.	<	
	e informati s, <u>see the</u>		security policy and related W website	indows		

OK

Cance

Microsoft Enforce Password History

We can also enable Microsoft's **Enforce Password History** policy to further make a password more secure, which ensures user's don't reset their password to previously used passwords. This value is set to 24 by default for the Default Domain Policy in AD.



force password hist	ory Prope	erties	?	×
ecurity Policy Setting	Explain			
F -(
Enforce passwor				
passwords that h	ave to be ssword ca	nines the number of unique new associated with a user account n be reused. <mark>The value must be rds.</mark>		
		strators to enhance security by Is are not reused continually.		
Default:				
24 on domain co 0 on stand-alone				
their domain con To maintain the allow passwords changed by also policy setting. Fo	trollers. effectivene to be cha enabling t r informatio	computers follow the configuration o ess of the password history, do not nged immediately after they were ju the Minimum password age security on about the minimum password age.	st	
			\vee	
For more informat features, see the		security policy and related Windows website	3	

OK



Cancel Ap

Microsoft Maximum Password Age

We can also enable Microsoft's **Maximum Password Age** policy to further make a password more secure, which ensures are changed after a certain amount of time. This value is set to 42 by default for the Default Domain Policy in AD.

🗐 Group Policy Management Editor	– 🗆 ×					
File Action View Help						
🗢 🌩 🚈 📰 🛃 👔 📷						
 Policies Software Settings Software installation Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Maccount Policies Ressword Policy 						

Maximum password age Properties	?	
Security Policy Setting Explain		
Maximum password age This security setting determines the period of time (in days) th password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days. Note: It is a security best practice to have passwords expire every 30 to 90 days, depending on your environment. This w an attacker has a limited amount of time in which to crack a user's password and have access to your network resources Default: 42.	um . If d	< >
For more information about security policy and related Window features, see the Microsoft website.	vs	
	_	

Microsoft Minimum Password Age

We can also enable Microsoft's **Minimum Password Age** policy to further make a password more secure, which ensures users must wait a certain amount of time before they can change a password. This value is set to 2 by default for the Default Domain Policy in AD.

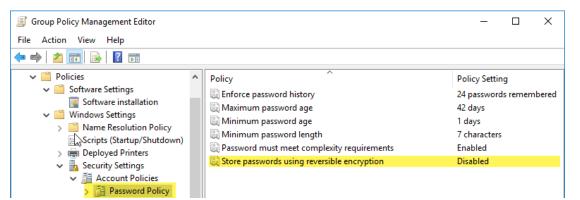
Group Policy Management Editor		– 🗆 X
File Action View Help		
🔶 🖄 📰 🗟 🖬		
 Policies Software Settings Software installation Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Password Policy 	Policy Characteristic password history Characteristic password age Characteristic password age Characteristic password age Characteristic password length Characteristic password must meet complexity requirement Characteristic passwords using reversible encryption Characteristic passwords using re	Policy Setting 24 passwords remembered 42 days 1 days 7 characters ts Enabled Disabled

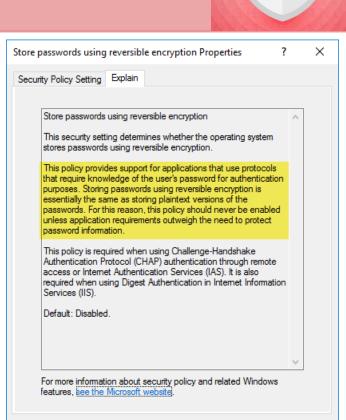
inimum password age Properties ?		×
ecurity Policy Setting Explain		
Minimum password age	^	
This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0.		
The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.		
Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator		
can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.		
	×	
For more information about security policy and related Windows features, see the Microsoft website.		

Cancel

Microsoft Reversible Encryption

We can also enable Microsoft's **Store Passwords using Reversible Encryption** policy if we want to be able to decrypt passwords and view them in plain text. This is not recommended and is disabled in the Default Domain Policy in AD. When disabled, passwords are stored as a hash that cannot be decrypted.





OK

Cancel