#### Lesson 18: Configuring Account Polices

MOAC 70-411: Administering Windows Server 2012



WILEY

#### Overview

- Exam Objective 5.4: Configure Account Policies
- Working with Account Policies

#### Working with Account Policies

Lesson 18: Configuring Account Polices

© 2013 John Wiley & Sons, Inc.

# **Group** Policies

- Group Policies provide centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.
- Use Group Policy to specify how often a user has to change his or her password, background images on users' computers, or whether spell check is required before sending e-mail.

#### **Group Policy Management Editor**



#### Accessing the account policies

### Group Policy Objects (GPOs)

Group Policy Objects (GPOs) are collections of user and computer settings including:

- **System settings**: Application settings, desktop appearance, and behavior of system services.
- Security settings: Local computer, domain, and network security settings.

# Group Policy Objects (GPOs)

Group Policy Objects (GPOs) are collections of user and computer settings including (continued):

- Software installation settings: Management of software installation, updates, and removal.
- Scripts settings: Scripts for when a computer starts or shuts down and for when a user logs on and off.
- Folder redirection settings: Storage for users' folders on the network.

### **Account Policies**

Account policies (Computer Configuration\Windows Settings\Security Settings\Account Policies) are domain level policies that define the security-related attributes assigned to user objects.

Account policies contain three subsets:

- Password Policy: Settings for passwords, such as enforcement and lifetimes.
- Account Lockout Policy: The circumstances and length of time that an account is locked out of the system.
- **Kerberos Policy**: Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos Policy settings do not exist in local computer policies.

### Configuring Domain User Password Policy

- A password policy defines the password parameters that a user uses.
- The strength of a password is determined by the password's length, complexity, and randomness.

### Configuring Password Policy Settings

Password Policy settings include:

- **Enforce password history**: The number of unique, new passwords that must be associated with a user account before an old password can be reused. The default setting is 24 previous passwords.
- Maximum password age: The number of days that a password can be used before the user must change it. The default setting is 42 days.
- **Minimum password age**: The number of days that a password must be used before the user can change it. The default value is one day, which is appropriate if you also enforce password history.

### Configuring Password Policy Settings

Password Policy settings include (continued):

- **Minimum password length**: The minimum number of characters that a user's password must contain. The default value is seven.
- **Complexity requirements**: A default password filter that is enabled by default. A complex password:
  - Does not contain your name or your username.
  - Contains at least six characters.
  - Contains characters from three of the following four groups: uppercase letters [A...Z], lowercase letters [a...z], numerals [0...9], and special, nonalphanumeric characters (such as !@#)(\*&^%).

#### **Password Policy Settings**

<u>I</u>	Group Policy Management Editor	
File     Action     View     Help       Image: Computer Configuration     Image: Computer Configuration     Image: Computer Configuration       Image: Computer Configuration     Image: Computer Configuration     Image: Computer Configuration	Policy	Policy Setting
<ul> <li>▷ Software Settings</li> <li>■ Windows Settings</li> <li>▷ Name Resolution Policy</li> <li>⊗ Scripts (Startup/Shutdown)</li> <li>△ Security Settings</li> <li>△ Account Policies</li> <li>Password Policy</li> <li>▷ Account Lockout P</li> <li>▷ Kerberos Policy</li> <li>∨</li> </ul>	Maximum password age Minimum password age Minimum password length Password must meet complexity requirements Store passwords using reversible encryption	42 days 1 days 7 characters Enabled Disabled

Viewing the Password Policy settings

#### **Password Policy Settings**

Enforce password history Properties	?	x
Security Policy Setting Explain		
Enforce password history		
Define this policy setting		
Keep password history for:		
24 passwords remembered		
OK Cancel	Ap	ply

Viewing the Enforce password history

#### **Password Policy Settings**

Password must meet complexity requirements Pro ? ×
Security Policy Setting Explain
Password must meet complexity requirements
Define this policy setting:
Enabled
⊖ Disabled
OK Cancel Apply

Viewing the Complexity requirements

### Configuring Account Lockout Settings

To help prevent hacking, Windows uses account lockout settings that specify when an account is locked when there are too many incorrect logon attempts.

### Configuring Account Lockout Settings

Group policies include the following account lockout settings:

 Account lockout duration: The length of time a lockout will remain in place before another logon attempt can be made. This can be set from 0 to 99,999 minutes. If set to 0, an administrator will need to manually unlock the account.

### Configuring Account Lockout Settings

Group policies include the following account lockout settings (continued):

- Account lockout threshold: The number of failed logons permitted before account lockout occurs. This can be set from 0 (no account lockouts) to 999 attempts before lockout.
- **Reset account lockout counter after**: The period of time, in minutes, that must elapse before the account lockout counter is reset to 0 bad logon attempts.

#### **Account Lockout Policies**

Account lockout duration Properties 2	Account lockout threshold Properties 2
Security Policy Setting Explain	Security Policy Setting Explain
Account lockout duration	Account lockout threshold
☑ Define this policy setting	Define this policy setting
Account is locked out for: 30 minutes	Account will not lock out.

Viewing account lockout policies

## Configuring/Applying Password Settings Objects

- **Fine-grained password policies** allow you to specify multiple password policies within a single domain.
- To enable fine-grained password policies:
  - 1. Create a **Password Settings Object (PSO)**.
  - 2. Configure the same settings that you configure for the password and account lockout policies.

#### Create and Configure Password Settings Container

8	Active	e Directory Administrative Co	enter	_ <b>D</b> X
Syste	em • Password Set	tings Container		🔹 🗭   Manage Help
🔺 Active Directory 🔇	Password Settings Contain	er (0)		Tasks
	Filter	► (1) ► (1)	$\odot$	Password Settings Container
<ul> <li>Contoso (local)</li> <li>\Password Settings Contai System</li> <li>Deleted Objects</li> <li>Dynamic Access Control</li> <li>Resource Property Lists</li> <li>Claim Types</li> <li>Global Search</li> </ul>	Name	Precedence Type	Description	New Delete Search under this node Properties
WINDOWS POWERSHELL HIS	TORY			$\odot$

#### Opening the Password Settings Container

#### Create and Configure Password Settings Container

Create Passw	vord Settings:	TASKS ▼ SECTIONS ▼
<ul> <li>Password Settings Directly Applies To</li> <li>Name: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Precedence: Preceden</li></ul>	Password Settings          Name:       *         Precedence:       *         Image: I	Password age options:  Password age options:  Password age User cannot change the password within ( * 1  Pathore maximum password age User must change the password after (day * 42  Enforce account lockout policy:
	Password must meet complexity requirements  Store password using reversible encryption  Protect from accidental deletion  Description:  Directly Applies To	Reset failed logon attempts autowed: Reset failed logon attempts count after (mins): Account will be locked out
	Name Mail	Add Remove
More Information		OK

#### Creating a New Password Settings Container

Create/Configure Password Settings with Windows PowerShell To create and manage PSOs in your domain using Windows PowerShell, use the following

command:

New-ADFineGrainedPasswordPolicy

To modify an existing PSO, use the following command:

Set-ADFineGrainedPasswordPolicySubject

### Determining the Resultant PSO

- 1. If a single PSO is linked directly to a user object, the resultant PSO is the single PSO.
- 2. If multiple PSOs are linked directly to the user object, the PSO with the lowest msDS-PasswordSettingsPrecedence value is the resultant PSO. If two PSOs have the same precedence, the PSO with the mathematically smallest objectGUID is the resultant PSO.
- 3. If no PSOs are assigned to the user object, and if a single PSO is assigned to a group the user is a member of, the assigned PSOs is applied.

### Determining the Resultant PSO

- 4. If multiple PSOs are linked to a group that the user is a member of, the PSO with the lowest msDS-PasswordSettingsPrecedence value is the resultant PSO. If two PSOs have the same precedence, the PSO with the mathematically smallest objectGUID is the resultant PSO.
- If you do not link any PSOs to the user object, either directly or through group membership, the policy defined in the Default Domain Policy is applied.

#### View the msDS-ResultantPSO Attribute

Т	est Use	r Prope	rties		?	x
Published Certificates     Me       Security     Enviro       General     Address     A       Remote Desktop Service	ember Of nment Account es Profile	Passwor Sess Profile C	d Replica ions Telepł OM+	ntion D Ren nones Attr	ial-in note cor Organi ibute Ec	Object Itrol zation litor
Attributes: Attribute accountExpires accountNameHistory aCSPolicyName adminCount adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescription adminDescriptio	Value (never) <not set=""> <not set=""> <not set=""> shadowFl msTSSec ms-net-iee <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not></not></not>	ag; shado condaryDe ee-80211-1 ee-80211-1	wExpire; sktops; rr āroupPol āroupPol	shadowli 1sTSPrim icy; nTFF icy; nTFF	nactive aryDes 3SSubs 3SSubs Filter	×
ОК	C	ancel	Ap	ply	Н	elp

Viewing user attributes

### Configuring Local User Password Policy

- Execute secpol.msc from a command prompt to open the Local Security Policy console.
- Local Security Policy console

   Security Settings
  - Account Policies
    - password-policy and account-policy settings

#### Local Security Policy Console

<b>a</b>	Local Security Policy	
File Action View Help		
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Application Control Policies</li> <li>IP Security Policies on Local Computer</li> <li>Advanced Audit Policy Configuration</li> </ul>	Name Account Policies Local Policies Windows Firewall with Advanced Security Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies IP Security Policies on Local Computer Advanced Audit Policy Configuration	Description         Password and account lockout policies         Auditing, user rights and security options policies         Windows Firewall with Advanced Security         Network name, icon and location group policies.         Application Control Policies         Internet Protocol Security (IPsec) Administration. Manage         Advanced Audit Policy Configuration
	< 111	>

Opening the Local Security Policy

## Delegating Password Settings Management

- By default, only members of the Domain Admins group can set fine-grained password policies.
- You can also delegate the ability to set these policies to other users.
- The Domain Admins group has Read and Write capabilities to the Default Domain Policy.
- To give access to others to manage the Default Domain Policy, add the user to the access list and assign permissions.

#### Manage GPO Permissions

<u></u>	Group Policy Management	_ <b>D</b> X
🔜 File Action View Window Help		_ <b>-</b> ×
Group Policy Management Group Policy Management Group Policy Management Group Domains Group Policy Objects Group Policy Objects Group Policy Objects Group Policy Objects Group Policy Object Group Policy Object Group Policy Object Group Policy Object Group Policy Object Group Policy Object Group Policy MindowsUpdates Sites Group Policy Modeling Group Policy Results	Default Domain Policy         Scope       Details       Settings       Delegation         These groups and users have the specified permission for this GPO       Groups and users:         Name       Allowed Permissions         Authenticated Users       Read (from Security Filtering)         Domain Admins (CONTOSO\Domain Ad       Custom         Enterprise Admins (CONTOSO\Enterpris       Custom         ENTERPRISE DOMAIN CONTROLLERS       Read         SYSTEM       Edit settings, delete, modify security	Inherited No No No No No
< III >	Add Remove Properties	Advanced

Displaying the Delegation tab

#### Manage GPO Permissions

Add Group or User	X
Group or user name:	
Netmon Users	Browse
Read V	
OK	Cancel

Assigning permissions to a GPO

#### Manage Password Settings Object Permissions

est Passwor	JSettingsContainer TASKS	▼ SECTIONS ▼
assword Settings Directly Applies To xtensions	Protect from accidental deletion     Or a duration of (mins):     Until an administrator manually     Description:	* 30 unlocks the account
	Directly Applies To	۲
	Name Mail	
	Domain Users	Add
	Security Attribute Editor Group or user names: Reveryone	
	Permissions for Everyone Allow Deny	
	Full control	

Viewing the users and groups that have access to the PSO

# Lesson Summary

- Group Policies provide centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.
- Group Policy Objects (GPOs) are collections of user and computer settings.
- Account policies are domain level policies that define the security-related attributes assigned to user objects.
- There is only one account policy per domain, which is usually defined in the Default Domain Policy.

# Lesson Summary

- As the name indicates, a password policy defines the password parameters that a user uses.
- To help prevent hacking, Windows uses account lockout settings that specify when an account is locked when there are too many incorrect logon attempts.
- If you need to use different password policies for different sets of users, you can use fine-grained password policies, which are applied to user objects or global security groups.
- If you have a standalone computer that is not part of a domain, you can still configure password policies and/or account lockout policies using the local policies.

#### Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



