## CHAPTER 11

## Manage Fine-Grained Password and Account Lockout Policies

### **IN THIS CHAPTER**

- Create Password Settings Objects
- Delete Password Settings Objects
- View Settings Defined in Password Settings Objects
- Modify Settings Defined in Password Settings Objects
- Apply a Password Settings Object to Users and Security Groups
- Modify the Precedence for Password Settings Objects
- View the Resultant Password Settings Objects for a User or Group
- Create Shadow Groups

Fine-grained password and account lockout policies are a new feature in Windows Server 2008. Fine-grained password policies allow you to define multiple password policies to different sets of users in a domain. Fine-grained account lockout policies allow you to define multiple account lockout policies to different sets of users in a domain.

This chapter describes the steps required to manage fine-grained password and account lockout policies.

**NOTE** Fine-grained password and account lockout policies require a domain functional level of Windows Server 2008.

### **Create Password Settings Objects**

**Scenario/Problem:** Your company wants to enforce a stronger password policy for all IT administrators. This policy can apply only to IT administrators.

Solution: Create a password settings object (PSO).

To create a PSO, perform the following steps:

- Log on to a domain controller (DC) or a member computer that has Windows Server 2008 Remote Server Administration Tools (RSAT) installed.
- 2. Click Start, click Run, type adsiedit.msc, and then click OK.
- 3. In the ADSI Edit snap-in, right-click ADSI Edit and then click Connect to.
- 4. On the Connection Settings window, shown in Figure 11.1, in the Name field type the fully qualified domain name (FQDN) of the domain in which you want to create the password settings object (PSO), ensure Default naming context is selected in the Select a well known Naming Context field, and then click OK.
- In the console tree, expand the domain node; then expand DC=domainname, where domainname is the name of your domain.
- 6. Expand CN=System.
- 7. In the console tree, right-click the CN=Password Settings Container node, select New, and then click Object.
- 8. On the Create Object window, shown in Figure 11.2, click Next.

Connection Settings	×
Name: WS08DOMAIN01.LOCAL	
Path: LDAP://WS08DC01.WS08DOMAIN01.LOCAL/Default naming co	ont
Connection Point	
Default naming context	
Computer C Select or type a domain or server: (Server   Domain [:port]) C Default (Domain or server that you logged in to) Use SSL-based Encryption	FIGURE 11.1
Ad <u>v</u> anced OK Cancel	The ADSI Edit snap-in Connection Settings window.
Create Object Select a class: msDS-PasswordSettings	X
<back next=""> Cancel</back>	Help FIGURE 11.2

- For the cn attribute, shown in Figure 11.3, type a name for the PSO in the Value field to set a Common-Name for the PSO; click Next.
- 10. For the msDS-PasswordSettingsPrecedence attribute, shown in Figure 11.4, type a value for the precedence in the Value field to set a password settings precedence for the PSO. Then click Next.

	ate Object		x
	Attribute:	cn	
	Syntax:	Unicode String	
	Description:	Common-Name	
	Value:	IT Administrators	
		< Back Next > Cancel Help	1
			-
Cre	ate Object		×
			_
	Attribute:	msDS-PasswordSettingsPrecedence	
	Attribute: Syntax:	msDS-PasswordSettingsPrecedence Integer	
	Attribute: Syntax: Description:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description: Value:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description: Value:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description: Value:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
	Attribute: Syntax: Description: Value:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	
_	Attribute: Syntax: Description: Value:	msDS-PasswordSettingsPrecedence Integer Password Settings Precedence	_

11. For the msDS-PasswordReversibleEncryptionEnabled attribute, shown in Figure 11.5, type **TRUE** in the Value field to enable store password using reversible encryption or type **FALSE** in the Value field to disable store password using reversible encryption. Then click Next.

Create Object	ķ	×
Attribute:	msDS-PasswordReversibleEncryptionEnabled	
Syntax:	Boolean	
Description:	Password reversible encryption status for user accounts	
Value:	FALSE	
	< Back Next > Cancel	Help

- FIGURE 11.5 Creating the PSO's password reversible encryption status for user accounts.
- **12**. For the msDS-PasswordHistoryLength attribute, shown in Figure 11.6, type a value for the password history length in the Value field and click Next.

Create Object	×
Attribute: msDS-PasswordHistoryLength	
Syntax: Integer	
Description: Password History Length for user accounts	
Value: 24	
	_ FIGURE 11.6
< Back Next > Cancel Help	Creating the PSO's password

13. For the msDS-PasswordComplexityEnabled attribute, shown in Figure 11.7, type TRUE in the Value field to enable password complexity or type FALSE in the Value field to disable password complexity; then click Next.

Crea	ate Object		×	
	Attribute:	msDS-PasswordComplexityEnabled		
	Syntax:	Boolean		
	Description:	Password complexity status for user accounts		
	Value:	TRUE		
				FIGURE 11.7
_		< Back Next > Cancel Help		Creating the PSO's password complexity status for user accounts.

14. For the msDS-MinimumPasswordLength attribute, shown in Figure 11.8, type a value for the minimum password length in the Value field and click Next.

Cre	ate Obiect		X
	Attribute:	msDS-MinimumPasswordLength	
	Syntax:	Integer	
	Description:	Minimum Password Length for user accounts	
	Value:	12	
-		c Pade Novt > Cancol	Holp
		< back ivext > Cancel	неір

**15.** For the msDS-MinimumPasswordAge attribute, shown in Figure 11.9, type a value for the minimum password age in the Value field. Then click Next.

Create Object	_	x
Attribute:	msDS-MinimumPasswordAge	
Syntax:	Duration	
Description:	Minimum Password Age for user accounts	
Value:	1:00:00:00	
	< Back Next > Cancel Help	_

- FIGURE 11.9 Creating the PSO's minimum password age for user accounts.
- **16.** For the msDS-MaximumPasswordAge attribute, shown in Figure 11.10, type a value for the maximum password age in the Value field and click Next.

Create Obj	ect	_	×	
Attribu	ite: msDS-MaximumPasswordAg	ge		
Syntax	c: Duration			
Descrip	otion: Maximum Password Age for	r user accounts		
Value:	30:00:00			
	< Back Next >	Cancel	Help	FIGURE 11.1 Creating the word age for

- FIGURE 11.10 Creating the PSO's maximum password age for user accounts.
- **17**. For the msDS-LockoutThreshold attribute, shown in Figure 11.11, type a value for the lockout threshold in the Value field; then click Next.

Create Object		×
Attribute:	msDS-LockoutThreshold	
Syntax:	Integer	
Description:	Lockout threshold for lockout of user accounts	
<u>V</u> alue:	3	
	< Back Next > Cancel Help	

FIGURE 11.11
Creating the PSO's lockout thresh-
old for lockout of user accounts.

**18.** For the msDS-LockoutObservationWindow attribute, shown in Figure 11.12, type a value for the observation window for lockout of user accounts in the Value field and click Next.

Create Object		x	
Attribute:	msDS-LockoutObservationWindow		
Syntax:	Duration		
Description:	Observation Window for lockout of user accounts		
Values	0.00.20.00	_	
<u>v</u> alue:	10:00:30:00		
			FIGURE 11.12
			Creating the PSO's observation
	< <u>B</u> ack <u>N</u> ext > Cancel	Help	window for lockout of user
			accounts.

**19.** For the msDS-LockoutDuration attribute, shown in Figure 11.13, type a value for the duration of the lockout of user accounts in the Value field; then click Next.

Create Object	<u> </u>	×
Attribute:	msDS-LockoutDuration	
Syntax:	Duration	
Description:	Lockout duration for locked out user accounts	
<u>V</u> alue:	(never)	
	< <u>B</u> ack <u>N</u> ext > Cancel Help	1

FIGURE 11.13 Creating the PSO's lockout duration for lockout of user accounts.

20. On the Create Object window, shown in Figure 11.14, click Finish to create the PSO.

Create Object	X
To set more attributes, click More Attributes. More Att	ributes
c Back Einich Concol	FIGURE 11.14
	Completing the Create PSO Wizard.

**NOTE** The time-related PSO attributes (msDS-MaximumPasswordAge, msDS-MinimumPasswordAge, msDS-LockoutObservationWindow, and msDS-LockoutDuration) must be entered in the d:hh:mm:ss format or the I8 format. The d:hh:mm:ss format is only available in the Windows Server 2008 version of ADSI Edit.

#### **Delete Password Settings Objects**

**Scenario/Problem:** You previously created a PSO in your domain. The PSO is no longer required and you want to prevent it from being used in the future.

#### Solution: Delete the PSO.

To delete a PSO, perform the following steps:

- **1**. Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected.
- 4. In the console tree, expand the System node and then select the Password Settings Container node.
- 5. In the details pane, right-click the PSO you want to delete; then click Delete.
- 6. Select Yes on the confirmation screen to delete the PSO.

#### **View Settings Defined in Password Settings Objects**

**Scenario/Problem:** You need to determine the settings that are applied in a PSO.

Solution: View settings defined in the the PSO.

To view the settings defined in a PSO, perform the following steps:

- Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected.
- 4. In the console tree, expand the System node and then select the Password Settings Container node.
- 5. In the details pane, right-click the PSO you want to view; then click Properties.

6. If you do not see attributes whose settings you want to view, click Filter to customize the list of attributes shown on the Attribute Editor tab. The filter dialog box is shown in Figure 11.15.

IT Administrators Propertie	15	? ×	
General Object Security	Attribute Editor	1	
Attroutes: Attroutes: Attroutes: adminDesplayName or or or description or description or displayName Printable or displayName Printable or displayName Printable or displayName CI disASignature or dSCorePropagationD be edemsionName or ISMORoleOwner or instanceType bb isOrticaSystemObject or Edit	alue           not set>           not set>           Administrators           not set>           not set>      not set>           not s	srd Settings Show only attributes that have values Show only witable attributes Show attributes: Show attributes: Optional Show read-only attributes: Constructed Badoinks System-only Help	FIGURE 11.15 Customizing the list of attributes shown on the Attribute Editor tab.

7. Scroll the list of attributes to view the settings defined.

### Modify Settings Defined in Password Settings Objects

**Scenario/Problem:** You previously created a PSO. You need to change the minimum password length in this PSO.

Solution: Modify settings defined in a PSO.

To modify the settings defined in a PSO, perform the following steps:

- 1. Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- 2. Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected.
- 4. In the console tree, expand the System node; then select the Password Settings Container node.
- 5. In the details pane, right-click the PSO you want to modify and click Properties.

- 6. If you do not see attributes whose settings you want to view, click Filter to customize the list of attributes shown on the Attribute Editor tab.
- 7. Select the attribute you want to modify, and click Edit.
- 8. Modify the value for the attribute, as shown in Figure 11.16, click OK, and then click OK to close the Attribute Editor.

Integer Attrib	ute Editor 🔀
Attribute:	msDS-MinimumPasswordLength
Value:	
15	
Clear	OK Cancel

FIGURE 11.16 Modifying the settings defined in a PSO.

# Apply a Password Settings Object to Users and Security Groups

**Scenario/Problem:** You created a new PSO in your domain. You want to ensure the PSO is applied to all IT administrators.

**Solution:** Apply the PSO to an Active Directory Domain Services (AD DS) group to which all IT administrators belong.

To apply a PSO to a user or group, perform the following steps:

- 1. Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- 2. Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected as shown in Figure 11.17.
- 4. In the console tree, expand the System node and then select the Password Settings Container node.
- 5. In the details pane, right-click the PSO you want to configure and select Properties.
- 6. On the PSO properties page, click the Attribute Editor tab.
- Click Filter, ensure the Show only attributes that have values option is not checked, as shown in Figure 11.18.

Active Directory Users and Complete Active Directory Users Active Directory Users and Complete Active Directory Users and Complete Active Directory Users Active D	uters				_ 8 ×
File Action View Help					
( Add/Remove Columns.		(38)			R
Actve Drec Large Ions  Actve Drec Large Ions  Saved Small Ions List  D of Users, Contacts, Group  F or V Advanced Features  Nev Customize  System  Us	se, and Computers as containers US USers 에 NTDS Quotas 에 Infrastructure		Type builtinDomain Container Organizational Container IostAndround Organizational Container Container Organizational Container msDS-QuotaCo infrastructureU	Description   Default container for upgr Default container for sec Default container for sec Default container for orph Default location for storag Builtin system settings Default container for upgr Quota specifications cont	
Displays contents of user, contact, group,	and computer objects				

#### FIGURE 11.17

Advanced features in the Active Directory Users and Computers console.

IT Administrators Properties	<u>? x</u>	
General Object Security Attribute Editor		
Attributes:		
Attribute	Value 🔺	
adminDescription	<not set=""></not>	
adminDisplayName	<not set=""></not>	
cn	IT Administrators	
description	<not set=""></not>	
displayName	<not set=""></not>	
displayNamePrintable	<not set=""></not>	
distinguishedName	CN=IT Administrators,C	_
dSASignature	<not set=""> Show only attributes that have values</not>	
dSCorePropagationData	0x0 = ( ) Show only writable attributes	
extensionName	<not set=""></not>	-
flags	<not set=""> Mandatase</not>	
fSMORoleOwner	<not set=""></not>	
instanceType	Dx4 = (WF	-
isCriticalSystemObject	<not set=""> Show read-only attributes:</not>	
4	Constructed	
	Backlinks	
Edt	<ul> <li>System-only</li> </ul>	FIGURE 11.18
OK Cancel	Apply Help	Filtering attributes in the Attribute
		Editor.

- 8. Select the msDS-PsoAppliesTo attribute, and click Edit.
- 9. On the Multi-valued Distinguished Name with Security Principal Editor window, shown in Figure 11.19, click Add Windows Account.

Multi-valued Distinguished Name With Security Principal Editor			×
Attribute: msDS-	PSOAppliesTo		
Values:			
Name	Container	Distinguished Name / SID	
1	7		
Add Windows Account.		_	Remove
Add DN			
		ок	Cancel



- **10.** In the Select Users, Computers, or Groups window, type the name of the user or global group to which you want to apply the PSO, and click OK.
- **11**. Click OK on the Multi-valued Distinguished Name with Security Principal Editor window; then click OK to close the properties for the PSO.

#### Modify the Precedence for Password Settings Objects

**Scenario/Problem:** You have multiple PSOs in your domain that are applied to global security groups. You want to ensure that a particular PSO is always applied to members of the IT Administrators AD DS group.

**Solution:** Modify the precedence for the PSO.

To modify the precedence for PSOs, perform the following steps:

- **1.** Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- 2. Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected.
- 4. In the console tree, expand the System node and then select the Password Settings Container node.
- 5. In the details pane, right-click the PSO for which you want to modify the precedence; then select Properties.
- 6. On the PSO properties page, click the Attribute Editor tab.
- 7. Select the msDS-PasswordSettingsPrecedence attribute and click Edit.

8. In the Integer Attribute Editor window, shown in Figure 11.20, enter the new value for the PSO Precedence, and then click OK.

**TIP** When multiple PSOs are applied to users or global groups in AD DS, the PSO with the lowest precedence value wins.

Integer Attribu	ıte Editor	×
Attribute:	msDS-PasswordSettingsPrecedence	
Value:		
1		
Clear	OK Cancel	

FIGURE 11.20 The Integer Attribute Editor window.

# View the Resultant Password Settings Objects for a User or Group

**Scenario/Problem:** You have multiple PSOs defined in your domain. You need to determine the effective PSO for a user account.

Solution: View the resultant PSOs for a user.

To view the resultant PSO for a user or group, perform the following steps:

- 1. Log on to a DC or a member computer that has Windows Server 2008 RSAT installed.
- 2. Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
- 3. On the View menu, ensure Advanced Features is selected.
- 4. Locate the user account or group for which you want to view the resultant password settings objects, and click Properties.
- 5. Click the Attribute Editor tab.
- 6. Click Filter.
- 7. Ensure that the Show attributes/Optional check box is selected.
- 8. Ensure that the Show read-only attributes/Constructed check box is selected.
- 9. Select the msDS-ResultantPSO attribute and click View.
- 10. The resultant PSO is listed.

#### **Create Shadow Groups**

**Scenario/Problem:** You recently created a PSO in your domain. You need to apply the PSO to all user accounts located in an organizational unit called New York.

Solution: Create a shadow group in AD DS.

To create a shadow group, perform the following steps:

- 1. Log on to a DC.
- 2. Click Start, and click Command Prompt.
- 3. In the Command Prompt window, type the following command and press Enter:

```
Dsquery user "OU=New York,DC=WS08DOMAIN01,DC=LOCAL" ¦ dsmod group
"CN=New York Users,OU=New York,DC=WS08DOMAIN01,DC=LOCAL" -chmbr
```

Table 11.1 lists each parameter used in the previous command.

Table 11.1 Parameters to Create a Shadow Group

Parameter	Meaning
"OU=New York,DC=WS08DOMAIN01,DC=LOCAL"	The DN of the OU that contains the user accounts.
"CN=New York Users,OU=New York,DC= WS08DOMAIN01,DC=LOCAL"	The DN of the group you want to use as the shadow group.
-chmbr	Replace group membership.

4. Verify that the results of the dsmod command entered above returns dsmod succeeded, shown in Figure 11.21.



FIGURE 11.21 Creating shadow groups.