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:

1. 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.
5. 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.

FIGURE 11.1
The ADSI Edit snap-in Connection Settings window.

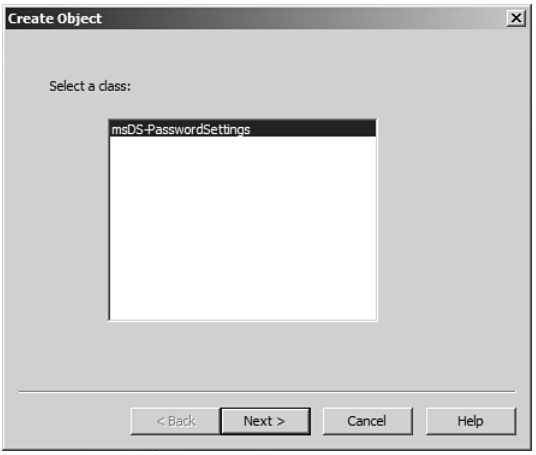

FIGURE 11.2
The Create Object window.

9. 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.

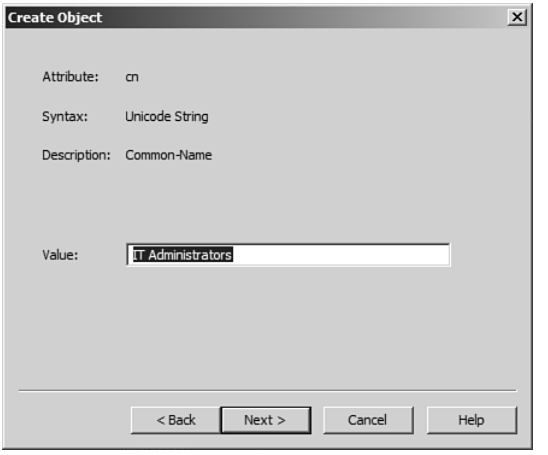

FIGURE 11.3
Creating the PSO's Common-Name.

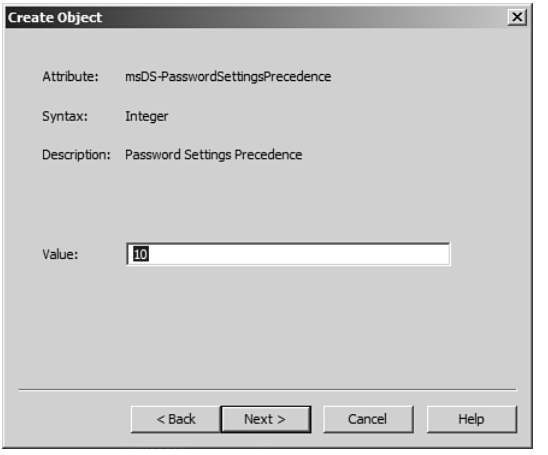

FIGURE 11.4
Creating the PSO's password settings precedence.

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.

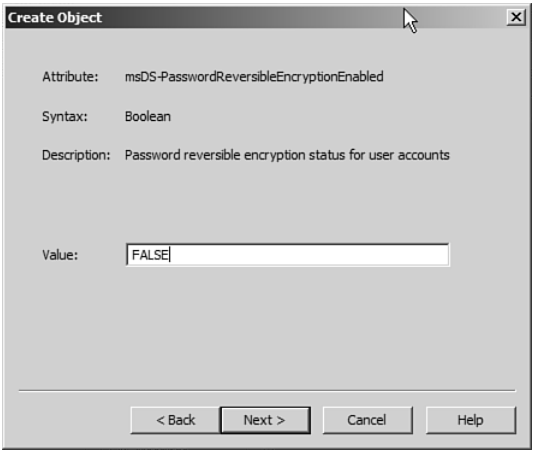

FIGURE 11.5
Creating the PSO's password reversible encryption status for user accounts.

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.

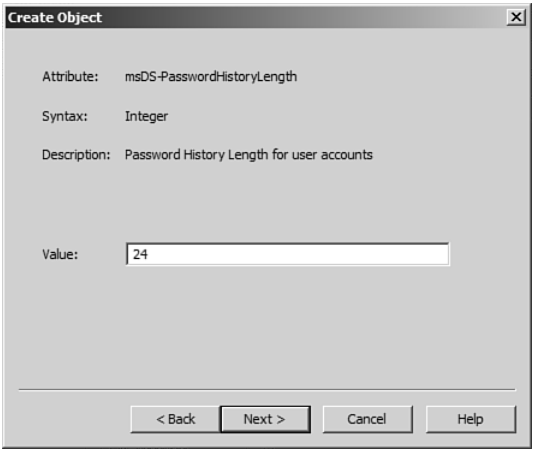

FIGURE 11.6
Creating the PSO's password history length for user accounts.

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.

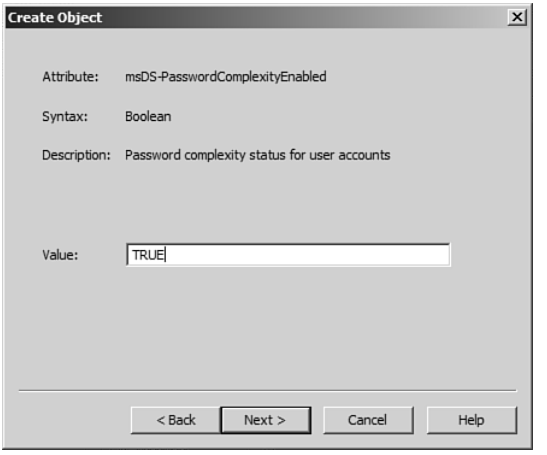

FIGURE 11.7
Creating the PSO's password complexity status for user accounts.

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.

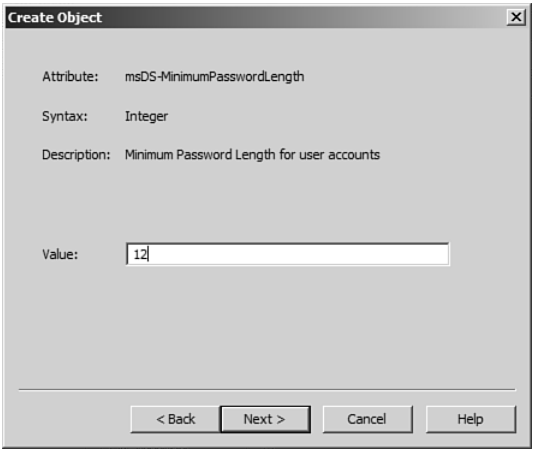

FIGURE 11.8
Creating the PSO's minimum password length for user accounts.

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.

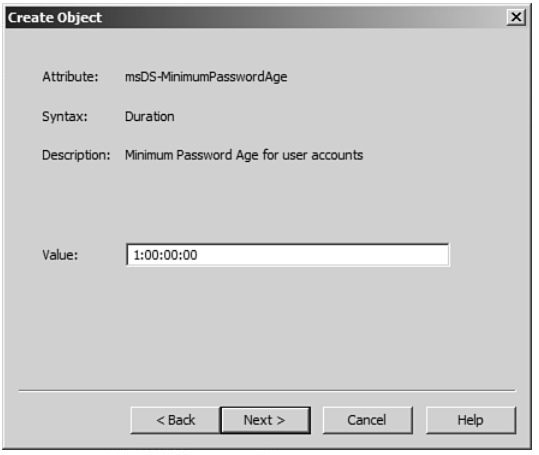

FIGURE 11.9
Creating the PSO's minimum password age for user accounts.

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.

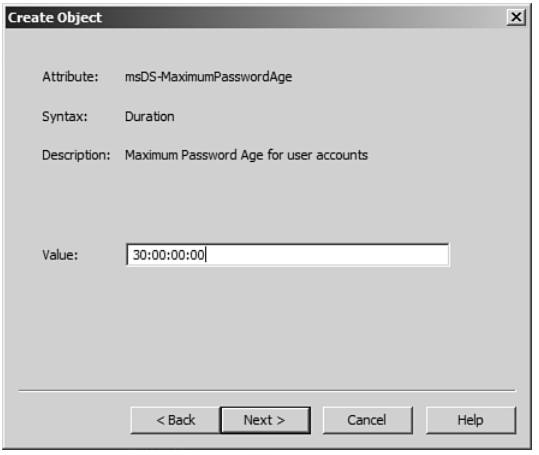

FIGURE 11.10
Creating the PSO's maximum password age for user accounts.

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.

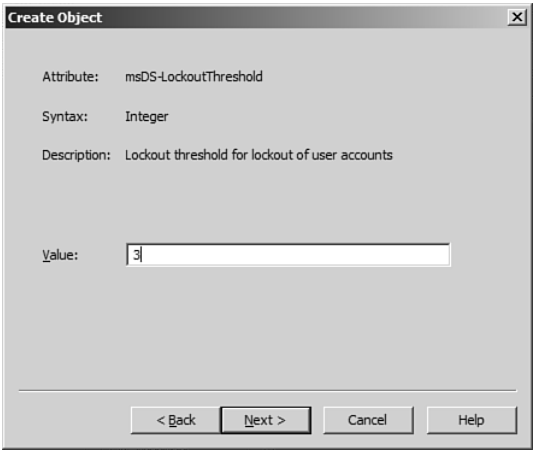

FIGURE 11.11
Creating the PSO's lockout threshold for lockout of user accounts.

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.

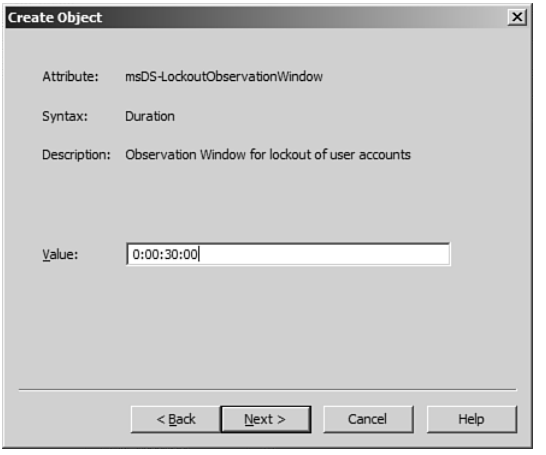

FIGURE 11.12
Creating the PSO's observation window for lockout of user accounts.

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.

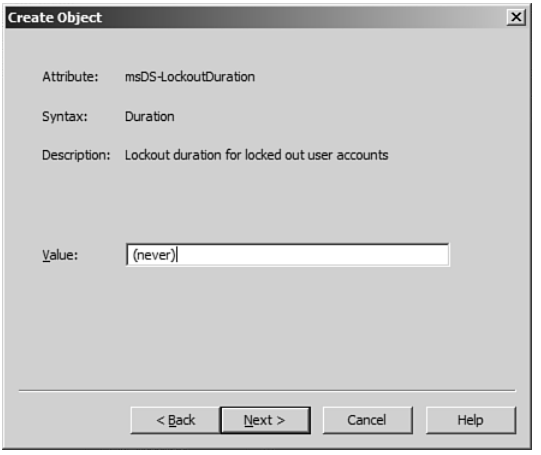

FIGURE 11.13
Creating the PSO's lockout duration for lockout of user accounts.

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

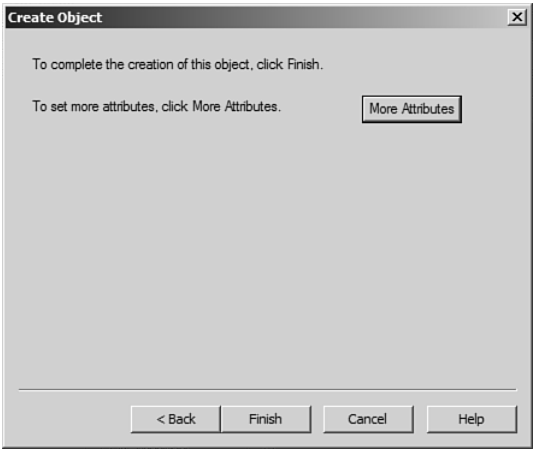

FIGURE 11.14
Completing the Create PSO Wizard.

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.
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 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:

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 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.

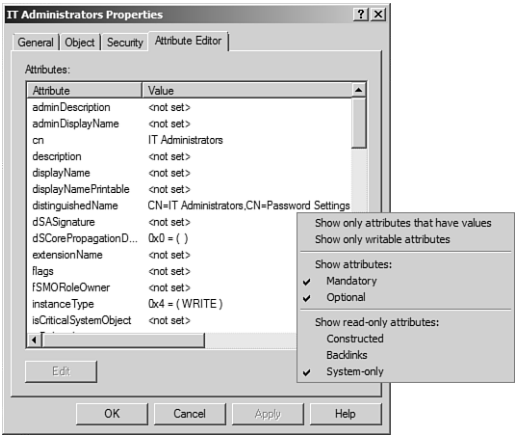

FIGURE 11.15
Customizing the list of attributes shown on the Attribute Editor tab.

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.

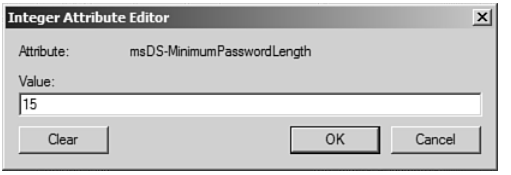

FIGURE 11.16
Modifying the settings defined in a PSO.

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.
7. Click Filter, ensure the Show only attributes that have values option is not checked, as shown in Figure 11.18.

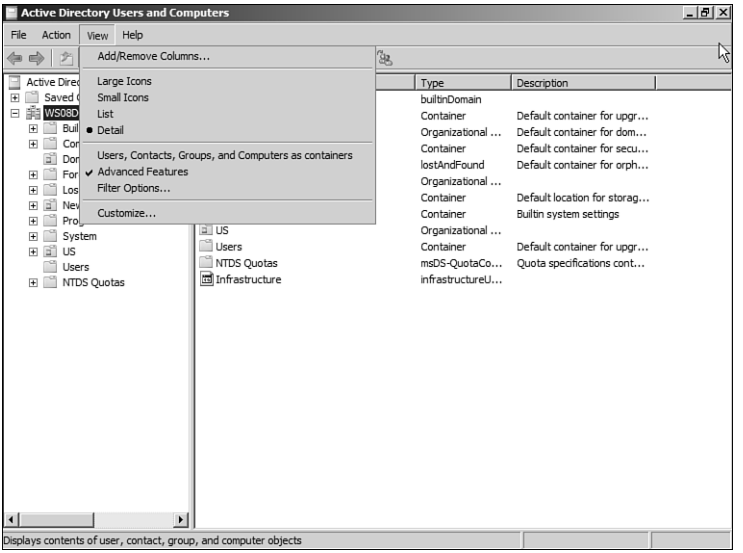

FIGURE 11.17
Advanced features in the Active Directory Users and Computers console.

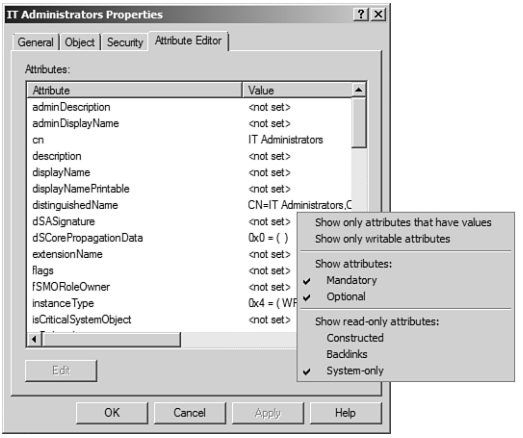

FIGURE 11.18
Filtering attributes in the Attribute Editor.

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.

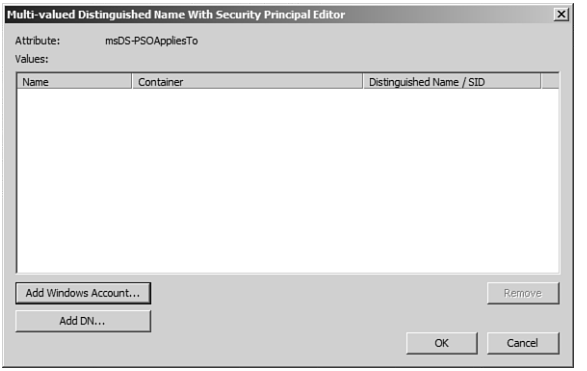

FIGURE 11.19
The Multi-valued Distinguished Name with Security Principal Editor window.

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.

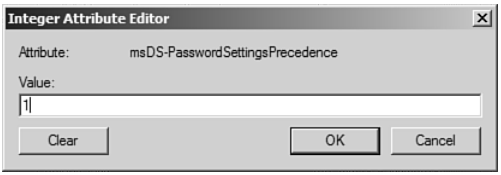

FIGURE 11.20
The Integer Attribute Editor window.

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.

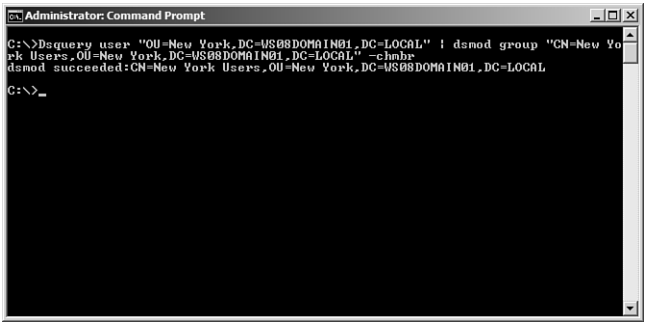

FIGURE 11.21
Creating shadow groups.