

AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide

<http://technet.microsoft.com/en-us/library/cc770842%28v=ws.10%29.aspx>

Updated: August 20, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2

This step-by-step guide provides instructions for configuring and applying fine-grained password and account lockout policies for different sets of users in Windows Server® 2008 domains.

In Microsoft® Windows® 2000 and Windows Server 2003 Active Directory domains, you could apply only one password and account lockout policy, which is specified in the domain's **Default Domain Policy**, to all users in the domain. As a result, if you wanted different password and account lockout settings for different sets of users, you had to either create a password filter or deploy multiple domains. Both options were costly for different reasons.

In Windows Server 2008, you can use fine-grained password policies to specify multiple password policies and apply different password restrictions and account lockout policies to different sets of users within a single domain. For example, to increase the security of privileged accounts, you can apply stricter settings to the privileged accounts and then apply less strict settings to the accounts of other users. Or in some cases, you may want to apply a special password policy for accounts whose passwords are synchronized with other data sources.

To store fine-grained password policies, Windows Server 2008 includes two new object classes in the Active Directory Domain Services (AD DS) schema:

- **Password Settings Container**
- **Password Settings**

The **Password Settings Container** (PSC) object class is created by default under the System container in the domain. It stores the Password Settings objects (PSOs) for that domain. You cannot rename, move, or delete this container.

For more information, see [Appendix A: Fine-Grained Password and Account Lockout Policy Review](#).

[Who should use this guide?](#)

This guide is intended for the following audiences:

- Information technology (IT) planners and analysts who are evaluating the product from a technical perspective
- Enterprise IT planners and designers for organizations
- Administrator or managers who are responsible for IT security

[Scenario overview](#)

[Define your organizational structure](#)

Before you configure fine-grained password and account lockout policies, define your organizational structure by creating necessary groups and adding or moving users to or between the groups. It is important to consider the unique nature of your organization when you plan for the most efficient use of the fine-grained password and account lockout policies feature. How many different password policies do you need? A typical scenario might include 3 to 10 PSOs and the following password policies:

- An Administrator password policy with a strict setting (passwords expire, for example, every 14 days)
- An average user password policy with a setting that is not strict (passwords expire, for example, every 90 days)
- A service account password policy targeted at service accounts (minimum password length, for example, 32 characters)

Taking advantage of your existing group structure is equally important. What are its characteristics? Do you have existing Administrators or Users groups? The goal is to shape your group structure so that it maps directly to the desired application of the newly defined fine-grained password and account lockout policies.

PSOs cannot be applied to organizational units (OUs) directly. If your users are organized into OUs, consider creating global security groups that contain the users from these OUs and then applying the newly defined fine-grained password and account lockout policies to them. If you move a user from one OU to another, you must update user memberships in the corresponding global security groups.

Applying PSOs directly to global security groups, as opposed to directly to OUs, provides the following benefits:

- Groups offer better flexibility for managing various sets of users than OUs.
- Most Active Directory deployments use a systematic group structure to organize their users. Also, by default AD DS in Windows Server 2008 creates various groups for administrative accounts: Domain Admins, Enterprise Admins, Schema Admins, Server Operators, Backup Operators, and others.
- Group structure offers easier deployment of fine-grained password policies, and you do not have to restructure your organizations' directories by creating OUs. Modifying an OU hierarchy requires detailed planning, and it increases the risk of introducing unforced errors because it has a significant effect on Group Policy application and access control list (ACL) inheritance.

[Requirements and special considerations for fine-grained password and account lockout policies](#)

- **Domain functional level:** The domain functional level must be set to Windows Server 2008 or higher.
- **Permissions:** By default, only members of the Domain Admins group can create PSOs. Only members of this group have the Create Child and Delete Child permissions on the Password Settings Container object. In addition, only members of the Domain Admins group have Write Property permissions on the PSO by default. Therefore, only members of the Domain Admins group can apply a PSO to a group or user. You do not have to have permissions on the user object or group object to

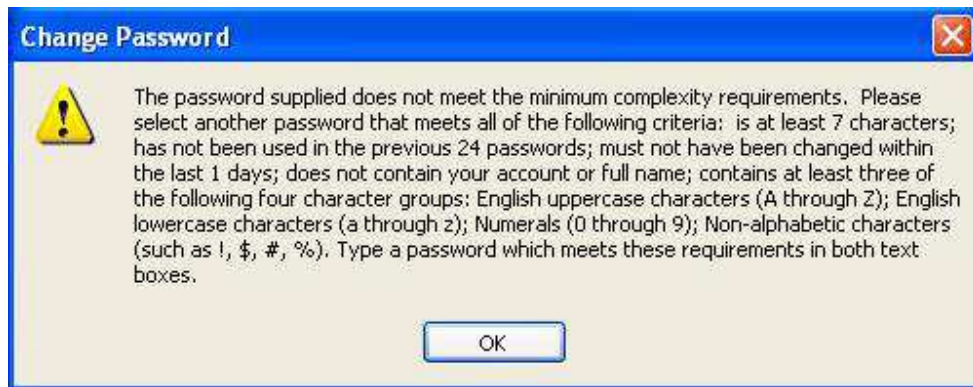
be able to apply a PSO to it. To apply a PSO to the user object or group object, you must have Write permissions on the PSO object.

- **Permissions delegation:** You can delegate Read Property permissions on the default security descriptor of the PSO object in the schema to any other group (such as Help desk personnel or a management application) in the domain or forest. This can also prevent a user from seeing his or her password settings in the directory. The user can read the **msDS-ResultantPSO** or the **msDS-PSOApplied** attributes, but these attributes display only the distinguished name of the PSO that applies to the user. The user cannot see the settings within that PSO. For more information, see [Appendix C: Group-Based Management of Fine-Grained Password and Account Lockout Policies](#).
- **Applying fine-grained password policies:** Fine-grained password policies apply only to user objects (or inetOrgPerson objects if they are used instead of user objects) and global security groups. They cannot be applied to Computer objects.

Note

Because fine-grained password policies apply only to user objects, they do not affect password reset intervals for managed service accounts. For more information about managed service accounts, see Service Accounts Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkID=134695>).

- **Password filters :** Fine-grained password policies do not interfere with custom password filters that you might use in the same domain. Organizations that have deployed custom password filters to domain controllers running Windows 2000 or Windows Server 2003 can continue to use those password filters to enforce additional restrictions for passwords.
- **Custom PSCs:** In addition to the default PSC, administrators can create their own custom PSCs under the System container. However, this action is not recommended because the PSOs that are held in these custom PSCs are not taken into consideration by the Resultant Set of Policy logic.
- **Exceptional PSOs:** If you want a certain group member to conform to a policy that is different from the policy that is assigned to the entire group, you can assign the exceptional PSO directly to that particular user. If you apply a PSO directly to the user, it takes precedence over all implicit PSOs that might be linked to it when **msDS-ResultantPSO** for that user is being determined. Although not recommended as a practice, if two or more exceptional PSOs are applied directly to the user object, the resultant exceptional PSO is determined in the same manner as any PSO:
 - The PSO with the lowest priority takes precedence
 - If two PSOs have the same priority, the PSO with the smallest globally unique identifier (GUID) takes precedence. For more information about how the GUIDs are compared, see [Appendix A: Fine-Grained Password and Account Lockout Policy Review](#).
- **Password complexity errors on Windows XP® client computers:** When a user to whom an FGPP applies attempts to change his or her password on a client computer that is running the Windows XP operating system, an error message appears, informing the user that the new password does not conform to the settings that are defined in the domain policy, instead of informing the user that the new password does not conform to the settings that are defined in the FGPP. The following illustration describes this error message:



The recommended approach is to ignore this error message and to make sure that the new password matches the minimum password length, password complexity, and password history requirements that are defined in the FGPP.

[Steps to configure fine-grained password and account lockout policies](#)

When the group structure of your organization is defined and implemented, you can configure and apply fine-grained password and account lockout policies to users and global security groups. Configuring fine-grained password and account lockout policies involves the following steps:

- [Step 1: Create a PSO](#)
- [Step 2: Apply PSOs to Users and Global Security Groups](#)
- [Step 3: Manage a PSO](#)
- [Step 4: View a Resultant PSO for a User or a Global Security Group](#)

Important

You can also manage fine-grained password and account lockout policies by creating corresponding global security groups for all existing PSOs and by assigning (delegating) appropriate permissions on these global security group objects to the selected users or groups from your organization, for example, support personnel. For more information, see [Appendix C: Group-Based Management of Fine-Grained Password and Account Lockout Policies](#)

For more information, see

- [Appendix A: Fine-Grained Password and Account Lockout Policy Review](#)
- [Appendix B: PSO Attribute Constraints](#)
- [Appendix C: Group-Based Management of Fine-Grained Password and Account Lockout Policies](#)

Step 1: Create a PSO

35 out of 43 rated this helpful - [Rate this topic](#)

Updated: July 14, 2010

Applies To: Windows Server 2008, Windows Server 2008 R2

[Creating a PSO](#)

You can create Password Settings objects (PSOs):

- [Creating a PSO using the Active Directory module for Windows PowerShell](#)
- [Creating a PSO using ADSI Edit](#)
- [Creating a PSO using Ldifde](#)

[Creating a PSO using the Active Directory module for Windows PowerShell](#)

To create a PSO (fine-grained password policy) using the Active Directory module for Windows PowerShell see, [Create a New Fine-Grained Password Policy](#).

[Creating a PSO using ADSI Edit](#)

Active Directory Service Interfaces Editor (ADSI Edit) provides a view of every object and attribute in an Active Directory Domain Services (AD DS) forest. You can use ADSI Edit to query, view, and edit AD DS objects and attributes.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](#) (<http://go.microsoft.com/fwlink/?LinkId=83477>).

[To create a PSO using ADSI Edit](#)

1. Click **Start**, click **Run**, type **adsiedit.msc**, and then click **OK**.

Note

If you are running ADSI Edit for the first time on a domain controller, proceed to step 2. Otherwise, proceed to step 4.

2. In the ADSI Edit snap-in, right-click **ADSI Edit**, and then click **Connect to**.
3. In **Name**, type the fully qualified domain name (FQDN) of the domain in which you want to create the PSO, and then click **OK**.
4. Double-click the domain.
5. Double-click **DC=<domain_name>**.
6. Double-click **CN=System**.
7. Click **CN=Password Settings Container**.

All the PSO objects that have been created in the selected domain appear.

8. Right-click **CN=Password Settings Container**, click **New**, and then click **Object**.
9. In the **Create Object** dialog box, under **Select a class**, click **msDS-PasswordSettings**, and then click **Next**.
10. In **Value**, type the name of the new PSO, and then click **Next**.
11. Continue with the wizard, and enter appropriate values for all **mustHave** attributes.

Important

To disable account lockout policies, assign the **msDS-LockoutThreshold** attribute the value of 0.

Note

To avoid ADSI Edit errors, values for the four time-related PSO attributes (**msDS-MaximumPasswordAge**, **msDS-MinimumPasswordAge**, **msDS-LockoutObservationWindow**, and **msDS-LockoutDuration**) must be entered in the d:hh:mm:ss format (recommended) or the I8 format. Note that the d:hh:mm:ss format is only available in the Windows Server 2008 version of ADSI Edit. For more information about how to convert time unit values into I8 values, see "Negative PSO Attribute Values" in [Appendix B: PSO Attribute Constraints](#).

Note

For more information about time-related PSO attributes, see "PSO Attributes Referential Integrity" in [Appendix B: PSO Attribute Constraints](#).

13.

Attribute name	Description	Acceptable value range	Example value
msDS-PasswordSettingsPrecedence	Password Settings Precedence	Greater than 0	10
msDS-PasswordReversibleEncryptionEnabled	Password reversible encryption status for user accounts	FALSE / TRUE (Recommended: FALSE)	FALSE
msDS-PasswordHistoryLength	Password History Length for user accounts	0 through 1024	24
msDS-PasswordComplexityEnabled	Password complexity status for user accounts	FALSE / TRUE (Recommended: TRUE)	TRUE
msDS-MinimumPasswordLength	Minimum Password Length for user accounts	0 through 255	8

MinimumPasswordLength	m Password Length for user accounts		
msDS- MinimumPasswordAge	Minimum Password Age for user accounts	<ul style="list-style-type: none"> ○ (None) ○ 00:00:00 through 1:00:00:00 (1 day) ○ (Never) 	msDS- MaximumPassw ordAge value
msDS- MaximumPasswordAge	Maximum Password Age for user accounts	<ul style="list-style-type: none"> ○ To set the time to (never), set the value to -9223372036854775808. ○ 42:00:00:00 (42 days) ○ msDS- MinimumPassw ordAge value through (Never) ○ msDS- MaximumPassw ordAge cannot be set to zero 	msDS- MinimumPassw ordAge value
msDS-LockoutThreshold	Lockout threshold for lockout of user accounts	0 through 65535	10
msDS- LockoutObservationWindow	Observation Window for lockout of user accounts	<ul style="list-style-type: none"> ○ (None) ○ 00:00:00 through 0:00:30:00 (30 minutes) 	msDS- LockoutDuratio n value
msDS-LockoutDuration	Lockout duration for locked out user accounts	<ul style="list-style-type: none"> ○ (None) ○ (Never) ○ 0:00:30:00 (30 minutes) 	msDS- LockoutObserv ationWindow value through

(Never)

msDS-PSOAppliesTo	Links to objects that this password settings object applies to (forward link)	0 or more DNs of users or global security groups	"CN=u1,CN=Users,DC=DC1,DC=contoso,DC=com"
--------------------------	---	--	---

Note

To create a PSO without applying it to any users or global security groups, proceed to step 17. Otherwise, proceed to step 12.

15. On the last screen of the wizard, click **More Attributes**.
16. On the **Select which property to view** menu, click **Optional** or **Both**.
17. In the **Select a property to view** drop-down list, select **msDS-PSOAppliesTo**.
18. In **Edit Attribute**, add the distinguished names of users or global security groups that the PSO is to be applied to, and then click **Add**.
19. Repeat step 15 to apply the PSO to more users or global security groups.
20. Click **Finish**.

Note

If you receive this error:

Operation failed. Error code: 0x57

The parameter is incorrect.

Check the syntax of the distinguished name of the account. The following characters in the distinguished name need to be escaped with a backslash:

, \ # + < > ; " =

For example, cn=Smith\, John,ou=West,dc=contoso,dc=com

[Creating a PSO using Ldifde](#)

You can use the **Ldifde** command as a scriptable alternative for creating PSOs.

LDAP Data Interchange Format (LDIF) is an Internet standard for a file format that you can use to perform batch operations against directories that conform to Lightweight Directory Access Protocol (LDAP) standards. You can use LDIF to export and import data. LDIF performs batch operations such as add, create, and modify against AD DS. When you install the AD DS role, a utility program called LDIFDE is included to support batch operations that are based on the LDIF file standard. For more information, see Using LDIFDE to import and export directory objects to Active Directory (<http://go.microsoft.com/fwlink/?LinkId=87487>).

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (<http://go.microsoft.com/fwlink/?LinkId=83477>).

[To create a PSO using Ldifde](#)

1. Define the settings of a new PSO by saving the following sample code as a file, for example, pso.ldf:
2. dn: CN=PSO1, CN=Password Settings Container,CN=System,DC=dc1,DC=contoso,DC=com
3. changetype: add
4. objectClass: msDS-PasswordSettings
5. msDS-MaximumPasswordAge:-1728000000000
6. msDS-MinimumPasswordAge:-864000000000
7. msDS-MinimumPasswordLength:8
8. msDS-PasswordHistoryLength:24
9. msDS-PasswordComplexityEnabled:TRUE
10. msDS-PasswordReversibleEncryptionEnabled:FALSE
11. msDS-LockoutObservationWindow:-18000000000
12. msDS-LockoutDuration:-18000000000
13. msDS-LockoutThreshold:0
14. msDS-PasswordSettingsPrecedence:20
15. msDS-PSOAppliesTo:CN=user1,CN=Users,DC=dc1,DC=contoso,DC=com

Note

When you use **ldifde** to create PSOs, values for the four time-related PSO attributes (**msDS-MaximumPasswordAge**, **msDS-MinimumPasswordAge**, **msDS-LockoutObservationWindow**, and **msDS-LockoutDuration**) must be entered in the I8 format. For more information about how to convert time unit values into I8 values, see "Negative PSO Attribute Values" in [Appendix B: PSO Attribute Constraints](#).

Note

For more information about time-related PSO attributes, see "PSO Attributes Referential Integrity" in [Appendix B: PSO Attribute Constraints](#).

16. Open a command prompt. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
17. Type the following command, and then press ENTER:
18. `ldifde -i -f pso.ldf`

Parameter	Description
ldifde	Specifies a utility program that supports batch operations that are based on the LDIF file standard.
-i	Specifies that Import Mode is turned on.
-f pso.ldf	Specifies the name of the input file that you created.

Step 2: Apply PSOs to Users and Global Security Groups

2 out of 2 rated this helpful - [Rate this topic](#)

Updated: August 24, 2007

Applies To: Windows Server 2008, Windows Server 2008 R2

[Applying PSOs](#)

You can apply Password Settings objects (PSOs) to users or global security groups:

- [Applying a PSO using the Active Directory module for Windows PowerShell](#)
- [Applying PSOs to users or global security groups using the Windows interface](#)
- [Applying PSOs to users or global security groups using Ldifde](#)

[Applying a PSO using the Active Directory module for Windows PowerShell](#)

To apply a PSO (fine-grained password policy) using the Active Directory module for Windows PowerShell see, [Apply a Fine-Grained Password Policy](#).

[Applying PSOs to users or global security groups using the Windows interface](#)

To apply a PSO to the user object or group object, you must have Write permissions on the PSO object.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](#) (<http://go.microsoft.com/fwlink/?LinkId=83477>).

[To apply PSOs to users or global security groups using the Windows interface](#)

1. Open Active Directory Users and Computers. To open Active Directory Users and Computers, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. On the **View** menu, ensure that **Advanced Features** is checked.
3. In the console tree, click **Password Settings Container**.

Where?

- Active Directory Users and Computers*domain node*\System>Password Settings Container.
4. In the details pane, right-click the PSO, and then click **Properties**.
 5. Click the **Attribute Editor** tab.
 6. Select the **msDS-PsoAppliesTo** attribute, and then click **Edit**.

Note

If you do not see **msDS-PsoAppliesTo** attribute in the **Attributes** list, click **Filter**, and then click **Show**

attributes/Optional. Also, clear the **Show only attributes that have values** check box.

7. In the **Multi-valued String Editor** dialog box, enter the Distinguished Name (also known as DN) of the user or the global security group that you want to apply this PSO to, click **Add**, and then click **OK**.

Note

To obtain the full distinguished name of a user or a global security group, in the details pane, right-click the user or the global security group, and then click **Properties**. On the **Attribute Editor** tab, view the value of the **Distinguished Name** attribute in the **Attributes** list.

[Applying PSOs to users or global security groups using Ldifde](#)

You can use the **Ldifde** command to apply a PSO to multiple users or global security groups quickly.

LDAP Data Interchange Format (LDIF) is an Internet standard for a file format that you can use to perform batch operations against directories that conform to the Lightweight Directory Access Protocol (LDAP) standards. You can use LDIF to export and import data. LDIF performs batch operations such as add, create, and modify against AD DS. When you install the AD DS role, a utility program called LDIFDE is included to support batch operations that are based on the LDIF file format standard. For more information, see [Using LDIFDE to import and export directory objects to Active Directory \(http://go.microsoft.com/fwlink/?LinkId=87487\)](#).

To apply a PSO to the user object or group object, you must have Write permissions on the PSO object.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups \(http://go.microsoft.com/fwlink/?LinkId=83477\)](#).

[To apply PSOs to users or global security groups using Ldifde](#)

1. Specify what PSO you want to apply to which users or global security groups by copying the following sample code into a file, for example, apply-a-psy.ldf:
 2. dn: CN=Demo Policy,CN=Password Settings Container,CN=System,DC=dc1,DC=contoso,DC=com
 3. changetype: modify
 4. add: msDS-PSOAppliesTo
 5. msDS-PSOAppliesTo: CN=user1,CN=Users,DC=dc1,DC=contoso,DC=com
 6. msDS-PSOAppliesTo: CN=user5,CN=Users,DC=dc1,DC=contoso,DC=com
 7. -

Note

The hyphen in the last line of the code in the file is required.

8. Open a command prompt. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
9. Type the following command, and then press **ENTER**:
10. `Ldifde -i -f apply-a-psy.ldf`

Parameter	Description
ldifde	Specifies a utility program that supports batch operations that are based on the LDIF file standard.
-i	Specifies that Import Mode is turned on.

-f apply-a-
pso.ldf

Specifies the name of the input file that you created.

Step 3: Manage a PSO

2 out of 3 rated this helpful - [Rate this topic](#)

Updated: August 24, 2007

Applies To: Windows Server 2008, Windows Server 2008 R2

Managing Password Settings objects (PSOs) includes the following tasks:

- [Deleting a PSO](#)
- [Viewing and modifying PSO settings](#)
- [Modifying PSO precedence](#)

You must have Write permissions on the PSO object to perform any of the tasks above.

[Deleting a PSO](#)

You can delete a PSO:

- [Delete a PSO using the Active Directory module for Windows PowerShell](#)
- [Deleting a PSO using ADSI Edit](#)
- [Deleting a PSO using Idifde](#)

[Delete a PSO using the Active Directory module for Windows PowerShell](#)

To delete a PSO (fine-grained password policy) using the Active Directory module for Windows PowerShell see, [Delete a Fine-Grained Password Policy](#).

[Deleting a PSO using ADSI Edit](#)

Active Directory Service Interfaces Editor (ADSI Edit) provides a view of every object and attribute in an Active Directory Domain Services (AD DS) forest. You can use ADSI Edit to query, view, and edit AD DS objects and attributes.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (<http://go.microsoft.com/fwlink/?LinkId=83477>).

[To delete a PSO using ADSI Edit](#)

1. Click **Start**, click **Run**, type **adsiedit.msc**, and then click **OK**.
2. Double-click the domain that contains the PSO that you want to delete.
3. Double-click **DC=<domain_name>**.
4. Double-click **CN=System**.
5. Double-click **CN=Password Settings**.

Note

All the PSO objects that have been created in the selected domain appear.

6. Right-click the PSO that you want to delete, and then click **Delete**.

Note

When the PSO is deleted, the password policy it represented will no longer be in effect for the members of the global security group that it was applied to.

[Deleting a PSO using ldifde](#)

You can use **ldifde** as a scriptable alternative for deleting PSOs.

LDAP Data Interchange Format (LDIF) is a proposed Internet standard for a file format that you can use for performing batch operations against directories that conform to Lightweight Directory Access Protocol (LDAP) standards. You can use LDIF to export and import data. LDIF performs batch operations such as add, create, and modify against AD DS. When you install the AD DS role, a utility program called LDIFDE is included to support batch operations that are based on the LDIF file format standard. For more information, see [Using LDIFDE to import and export directory objects to Active Directory](#) (<http://go.microsoft.com/fwlink/?LinkId=87487>).

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](#) (<http://go.microsoft.com/fwlink/?LinkId=83477>).

[To delete a PSO using ldifde](#)

1. Specify which PSO you want to delete by saving the following sample code in a file, for example, delete-a-psy.ldf:
 2. dn: CN=PSO1, CN>Password Settings Container, CN=System, DC=dc1, DC=contoso, DC=com
 3. changetype: delete
4. Open a command prompt. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
5. Type the following command, and then press ENTER:
 6. ldifde -i -f delete-a-psy.ldf

Parameter	Description
ldifde	Specifies a utility program that supports batch operations that are based on the LDIF file standard.
-i	Specifies that Import Mode is turned on.
-f delete-a-psy.ldf	Specifies the name of the input file that you created.

[Viewing and modifying PSO settings](#)

To view the details of a PSO (fine-grained password policy) using the Active Directory module for Windows PowerShell see, [Retrieve Details of a Fine-Grained Password Policy](#).

To modify a PSO (fine-grained password policy) using the Active Directory module for Windows PowerShell see, [Modify a Fine-Grained Password Policy](#).

[To view or modify PSO settings using the Windows interface](#)

1. Open Active Directory Users and Computers. To open Active Directory Users and Computers, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. On the **View** menu, ensure that **Advanced Features** is checked.
3. In the console tree, click **Password Settings Container**.

Where?

- Active Directory Users and Computers*domain node*\System>Password Settings Container.
4. In the details pane, right-click the PSO, and then click **Properties**.
 5. Click the **Attribute Editor** tab.
 6. Select the attribute whose setting you want to view or edit, and then click **View** (for editable values) or **Edit** (for read-only values).

Note

If you do not see attributes whose settings you want to view or edit, click **Filter** to customize the list of attributes that is shown on the **Attribute Editor** tab.

Note

To view or edit the **msDS-PSOAppliesTo** attribute, click **Filter**, and then click **Show attributes/Optional**. Clear the **Show only attributes that have values** check box.

[Modifying PSO precedence](#)

[To modify PSO precedence using the Windows interface](#)

1. Open Active Directory Users and Computers. To open Active Directory Users and Computers, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. On the **View** menu, ensure that **Advanced Features** is checked.
3. In the console tree, click **Password Settings Container**.

Where?

- Active Directory Users and Computers*domain node*\System>Password Settings Container
4. In the details pane, right-click the PSO, and then click **Properties**.
 5. Click the **Attribute Editor** tab.
 6. Select the **msDS-PasswordSettingsPrecedence** attribute, and then click **Edit**.
 7. In the **IntegerAttribute Editor** dialog box, enter the new value for the **PSO Precedence**, and then click **OK**.

Step 4: View a Resultant PSO for a User or a Global Security Group

1 out of 3 rated this helpful - [Rate this topic](#)

Updated: August 24, 2007

Applies To: Windows Server 2008, Windows Server 2008 R2

You can view the resultant Password Settings object (PSO) for a user object:

- [Viewing the resultant PSO for users using the Active Directory module for Windows PowerShell](#)
- [Viewing the resultant PSO for users using the Windows interface](#)
- [Viewing the resultant PSO for users from the command line using dsget](#)

[Viewing the resultant PSO for users using the Active Directory module for Windows PowerShell](#)

To view the resultant PSO (fine-grained password policy) for users using the Active Directory module for Windows PowerShell see, [Get Resultant Password Policy of a User](#).

[Viewing the resultant PSO for users using the Windows interface](#)

[To view the resultant PSO for a user using Windows interface](#)

1. Open Active Directory Users and Computers. To open Active Directory Users and Computers, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. On the **View** menu, ensure that **Advanced Features** is checked.
3. In the console tree, click **Users**.

Where?

- Active Directory Users and Computers*domain node*\Users
4. In the details pane, right-click the user account for which you want to view the resultant PSO, and then click **Properties**.
 5. Click the **Attribute Editor** tab, and then click **Filter**.
 6. Ensure that the **Show attributes/Optional** check box is selected.
 7. Ensure that the **Show read-only attributes/Constructed** check box is selected.
 8. Locate the value of the **msDS-ResultantPSO** attribute in the **Attributes** list.

Note

If the value of the **msDS-ResultantPSO** attribute is Null, the **Default Domain Policy** is applied to the selected user account.

[Viewing the resultant PSO for users from the command line using dsget](#)

[To view the resultant PSO for a user from the command line using dsget](#)

1. Open a command prompt. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type the following command, and then press ENTER:

3. dsget user <User-DN> -effectivepso

Example: **dsget user "CN=u1,CN=Users,DC=corp,DC=contoso,DC=com" -effectivepso**

Note

If the PSO name is not returned by the **dsget** command, the **Default Domain Policy** is applied to the specified user account.

Parameter	Description
dsget user	Displays various properties of a user in the directory.
<User-DN>	Specifies full distinguished name of the user object for which you want to view the resultant PSO.
-effectivepso	Specifies the resultant PSO.

Appendix A: Fine-Grained Password and Account Lockout Policy Review

5 out of 6 rated this helpful - [Rate this topic](#)

Updated: August 20, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2

[Storing fine-grained password policies](#)

Windows Server 2008 includes two new object classes in the Active Directory Domain Services (AD DS) schema to store fine-grained password policies:

- **Password Settings Container**
- **Password Settings**

The **Password Settings Container** (PSC) object class is created by default under the System container in the domain. It stores the Password Settings objects (PSOs) for that domain. You cannot rename, move, or delete this container.

A PSO has attributes for all the settings that can be defined in the **Default Domain Policy** (except Kerberos settings). These settings include attributes for the following password settings. Attribute names appear in parentheses.

- **Enforce password history (msDS-PasswordHistoryLength)**
- **Maximum password age (msDS-MaximumPasswordAge)**
- **Minimum password age (msDS-MinimumPasswordAge)**
- **Minimum password length (msDS-MinimumPasswordLength)**
- **Passwords must meet complexity requirements (msDS-Password-ComplexityEnabled)**
- **Store passwords using reversible encryption (msDS-PasswordReversibleEncryptionEnabled)**

These settings also include attributes for the following account lockout settings:

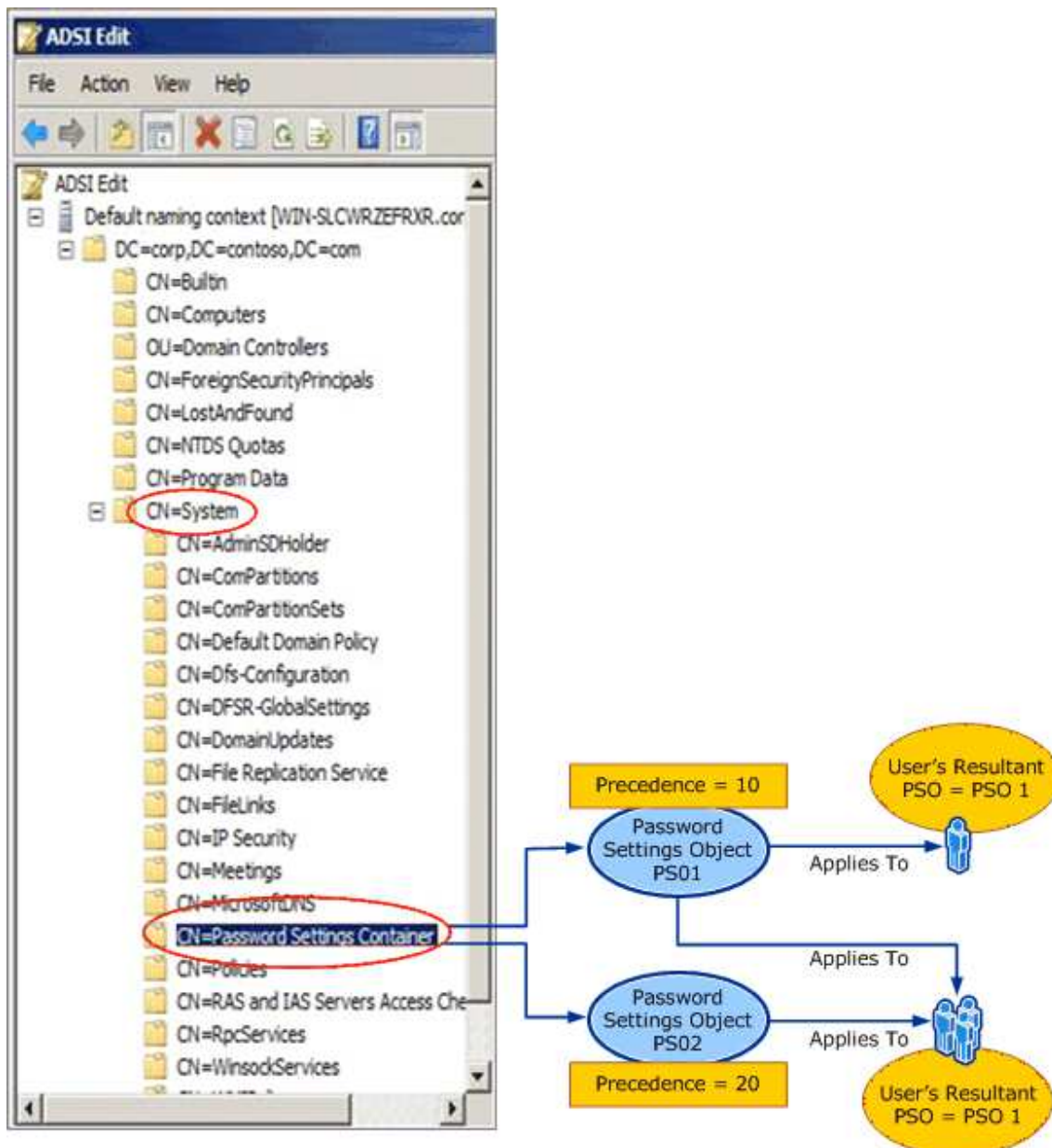
- **Account lockout duration (msDS-LockoutDuration)**
- **Account lockout threshold (msDS-LockoutThreshold)**
- **Reset account lockout counter after (msDS-LockoutObservationWindow)**

In addition, a PSO has the following two new attributes:

- **PSO link (msDS-PSOAppliesTo).** This is a multivalued attribute that is linked to users and group objects.
- **Precedence (msDS-PasswordSettingsPrecedence).** This is an integer value that is used to resolve conflicts if multiple PSOs are applied to a user or group object.

All attributes except **msDS-PSOAppliesTo** are **mustHave** attributes. This means that you must define a value for each one. Settings from multiple PSOs cannot be merged.

The following illustration shows the storage location of the PSOs in a given domain and the method for calculating the resultant PSO that is eventually applied to the user accounts.



For more information about password policies and account lockout settings, see [Password Policy](#).

[Defining the scope of fine-grained password policies](#)

A PSO can be linked to a user (or inetOrgPerson) or a group object that is in the same domain as the PSO:

- A PSO has an attribute named **msDS-PSOAppliesTo** that contains a forward link to only user or group objects. The **msDS-PSOAppliesTo** attribute is multivalued, which means that you can apply a PSO to multiple users or groups. You can create one password policy and apply it to different sets of users or groups.
- A new attribute named **msDS-PSOApplied** has been added to the user and group objects in Windows Server 2008. The **msDS-PSOApplied** attribute contains a back-link to the PSO. Because the **msDS-PSOApplied** attribute has a back-link, a user or group can have multiple PSOs applied to it. In this case, the Resultant Set of Policy (RSOP), represented by the new **msDS-ResultantPSO** attribute, must be calculated for that user. For more information, see "The logic behind precedence: calculating RSOP."

You can link a PSO to other types of groups in addition to global security groups. However, when the RSOP for a user object is being determined, only those PSOs that are directly linked to the user object or to the global security groups that the user is a member of are considered. PSOs that are linked to distribution groups or other types of security groups are ignored.

[The logic behind precedence: calculating RSOP](#)

A user or group object can have multiple PSOs linked to it, either because of membership in multiple groups that each have different PSOs applied to them or because multiple PSOs are applied to the object directly. However, only one PSO can be applied as the effective password policy. Only the settings from that PSO can affect the user or group. The settings from other PSOs that are linked to the user or group cannot be merged in any way.

RSOP can be calculated only for a user object. The PSO can be applied to a user object in either of the following two ways:

- Directly: The PSO is linked to the user.
- Indirectly: The PSO is linked to groups that the user is a member of.

Each PSO has an additional attribute named **msDS-PasswordSettingsPrecedence** that assists in the calculation of RSOP. The **msDS-PasswordSettingsPrecedence** attribute has an integer value of **1** or greater. A lower value for the **msDS-PasswordSettingsPrecedence** attribute indicates that the PSO has a higher rank, or a higher priority, than other PSOs. For example, suppose that an object has two PSOs linked to it. One PSO has a **msDS-PasswordSettingsPrecedence** value of **20**, and the other PSO has a **msDS-PasswordSettingsPrecedence** value of **40**. In this case, the PSO that has the **msDS-PasswordSettingsPrecedence** value of **20** has a higher rank. Therefore, it is applied to the object.

Important

If multiple PSOs are linked to a user or group, the resultant PSO that is applied is determined as follows:

- A PSO that is linked directly to the user object is the resultant PSO. If no PSO is linked to the user object, the global security group memberships of the user—and all PSOs that are applicable to the user based on those global group memberships—are compared. The PSO with the lowest **msDS-PasswordSettingsPrecedence** value is the resultant PSO.
- If no PSO is obtained from the preceding conditions, the **Default Domain Policy** is applied.

We recommend that you assign a unique **msDS-PasswordSettingsPrecedence** value for each PSO that you create. However, you can create multiple PSOs with the same **msDS-PasswordSettingsPrecedence** value. If multiple PSOs with the same **msDS-PasswordSettingsPrecedence** value are obtained for a user from the preceding conditions, the PSO with the smallest globally unique identifier (GUID) is applied.

In order to determine the smallest GUID, the GUIDs are compared at the byte level. The right-most byte of the first portion of the GUID is compared first. For example, suppose that two PSOs with the following GUIDs have the same **msDS-PasswordSettingsPrecedence** value:

1. d1742912-87cd-4172-ac6e-ad1e94965e6b
2. 7b41e54e-a075-4a4d-869d-0b0e1433de89

Although you might think that PSO #2 will be applied since 7b comes before d1 numerically, PSO #1 will be applied because the memory comparison operation compares the right-most byte of the first portion of the GUID, and 12 is lower than 4e. To help prevent unexpected results, do not apply the same **msDS-PasswordSettingsPrecedence** value to different PSOs.

A new attribute named **msDS-ResultantPSO** has been added to the user object. An administrator can query on this attribute to retrieve the distinguished name of the PSO that is ultimately applied to that user (based on the rules listed previously). If there is no PSO object that applies to the user, either directly or by virtue of group membership, the query returns the NULL value.

The user object has three bits, which can be set in the **userAccountControl** attribute of the user object, that override the settings that are present in the resultant PSO (much as these bits override the settings in the **Default Domain Policy** in Windows 2000 and Windows Server 2003):

- **Reversible password encryption required**
- **Password not required**
- **Password does not expire**

Important

It is recommended to apply PSOs to group objects as opposed to user objects directly because of the constraint of the **msDS-PSOApplied** user or group attribute that is especially problematic when you copy a user or a group object. The constraint of the **msDS-PSOApplied** attribute is that when you copy a user or a group object, its **msDS-PSOApplied** attribute is not also copied. As stated previously, in Windows Server 2008, a user or group can have multiple PSOs applied to it since the **msDS-PSOApplied** attribute of the user and group objects has a back-link to the PSO. Consider the following scenario: an administrator copies "User1" user account (a member of "Group1" group) to create a new "User2" user account which he also wants to be a member of "Group1". "Group1" has a PSO "PSO_Group" applied to it in which **msDS-PasswordComplexityEnabled** attribute is set to FALSE. "User1" has a PSO "PSO_User" applied to it in which **msDS-PasswordComplexityEnabled** attribute is set to TRUE. Since "PSO_User" is applied directly to the user object, it has a higher rank than "PSO_Group" (applied to a group object) and is therefore the resultant PSO for "User1". When the administrator copies "User1" in order to create a new user account "User2", he wants "PSO_User" to also be applied to "User2". However, since the **msDS-PSOApplied** attribute is not copied for "User2" and yet the group membership to "Group1" is copied by default, "User2" ends up with the resultant PSO of "PSO_Group" (with the **msDS-PasswordComplexityEnabled** attribute set to FALSE) which will cause "User2" account to silently fail to comply with the required security policies.

Appendix B: PSO Attribute Constraints

2 out of 5 rated this helpful - [Rate this topic](#)

Updated: March 26, 2010

Applies To: Windows Server 2008, Windows Server 2008 R2

[Negative PSO attribute values](#)

When you use ADSI Edit to create Password Settings objects (PSOs), enter the values of the four time-related PSO attributes (**msDS-MaximumPasswordAge**, **msDS-MinimumPasswordAge**, **msDS-LockoutObservationWindow**, and **msDS-LockoutDuration**) in d:hh:mm:ss format.

When you use the **ldifde** command to create PSOs, you must enter the values of these attributes in I8 format, which stores time in the intervals of -100 nanoseconds. (Schema: attributeSyntax = 2.5.5.16 (I8).) Windows Server 2003 **Default Domain Policy** employs this exact time unit for its corresponding time-related attributes. To set these attributes to appropriate values, convert time values in minutes, hours, or days to time values in the intervals of 100 nanoseconds, and then precede the resultant values with a negative sign.

You can use the following conversion guide and multiplication factors to obtain the corresponding I8 values. To set the time to *never*, set the value to -9223372036854775808.

Time unit	Multiplication factor
<i>m</i> minutes	$-60 \cdot (10^7) = -600000000$
<i>h</i> hours	$-60 \cdot 60 \cdot (10^7) = -3600000000$
<i>d</i> days	$-24 \cdot 60 \cdot 60 \cdot (10^7) = -86400000000$

For example, if you want to set the **msDS-MaximumPasswordAge** to 10 days, multiply 10 by -86400000000 and apply the resulting I8 value to the **msDS-MaximumPasswordAge** attribute (in this example, -864000000000). If you want to set **msDS-LockoutDuration** to 30 minutes, multiply 30 by -600000000 to get the corresponding I8 value (in this example, -18000000000).

[PSO attributes referential integrity](#)

Consider the following information when you create new PSOs:

- The value of **msDS-MinimumPasswordAge** must be smaller than or equal to the value of **msDS-MaximumPasswordAge**.
- The value of **msDS-LockoutObservationWindow** cannot be larger than the value of **msDS-LockoutDuration**. The **msDS-LockoutObservationWindow** determines how long the bad password counter is active. The **msDS-LockoutDuration** determines how long an account stays locked out for when the bad password count threshold is reached. It is not possible to keep the bad password counter active longer than the time that the account is locked out.

- The value of **msDS-MaximumPasswordAge** cannot be set to zero.

Appendix C: Group-Based Management of Fine-Grained Password and Account Lockout Policies

0 out of 1 rated this helpful - [Rate this topic](#)

Updated: August 24, 2007

Applies To: Windows Server 2008, Windows Server 2008 R2

Group-based management of fine-grained password and account lockout policies involves the following steps:

- Step 1: Create all necessary Password Settings objects (PSOs). For more information, see [Step 1: Create a PSO](#).
- Step 2: For every existing PSO, create a corresponding global security group. For more information about creating groups, see [Create a new group \(http://go.microsoft.com/fwlink/?LinkId=98721\)](http://go.microsoft.com/fwlink/?LinkId=98721).
- Step 3: Apply all PSOs to their corresponding global security groups. For more information, see [Step 2: Apply PSOs to Users and Global Security Groups](#).
- Step 4: Assign appropriate permissions on your PSO-corresponding global security groups to the selected users or groups (delegated administrators) from your organization. For more information, see [Assign, change, or remove permissions on Active Directory objects or attributes \(http://go.microsoft.com/fwlink/?LinkId=98723\)](http://go.microsoft.com/fwlink/?LinkId=98723).

A group-based approach is the recommended solution for the most effective management of fine-grained password and account lockout policies because the direct management permissions over the attributes of PSOs are retained only by the members of the Domain Admins group. Members of this group can revisit and revise existing fine-grained password and account lockout policies when necessary, based on the changes in their organization.

This approach ensures fewer sporadic changes to the fine-grained password and account lockout policies because the delegated administrators—for example, technical support specialists—can manage fine-grained password and account lockout policies only by attesting that all appropriate PSOs are applied to their corresponding global security groups. In other words, delegated administrators do not have permissions over the PSO attributes. They cannot, for example, add a universal group or a domain-local group to a PSO's **msDs-PSOAppliesTo** attribute—an erroneous action that will not have any effect on the PSO. Neither can they commit the error of adding a universal group or a domain-local group to the PSO-corresponding global security groups that they have the permissions to manage because, by design, global security groups allow as members only other global security groups or users from the same domain.

The privilege of assigning exceptional PSOs that take precedence over all implicit PSOs that are applied to the group that the user is a member of is also retained only by members of the Domain Admins group. This contrasts with various exceptional PSOs being assigned to users or groups by multiple delegated administrators, which can eventually lead to a complicated and possibly convoluted PSO structure.

The risk of introducing errors in PSO precedence values (for example, more than one PSO with the same value applied to the same user object) is also significantly decreased when only members of the Domain Admins group have the permission to manage PSO attributes directly.