Lesson 18: Configuring Account Polices

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

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

© 2013 John Wiley & Sons, Inc.

Working with Account Policies

Lesson 18: Configuring Account Polices

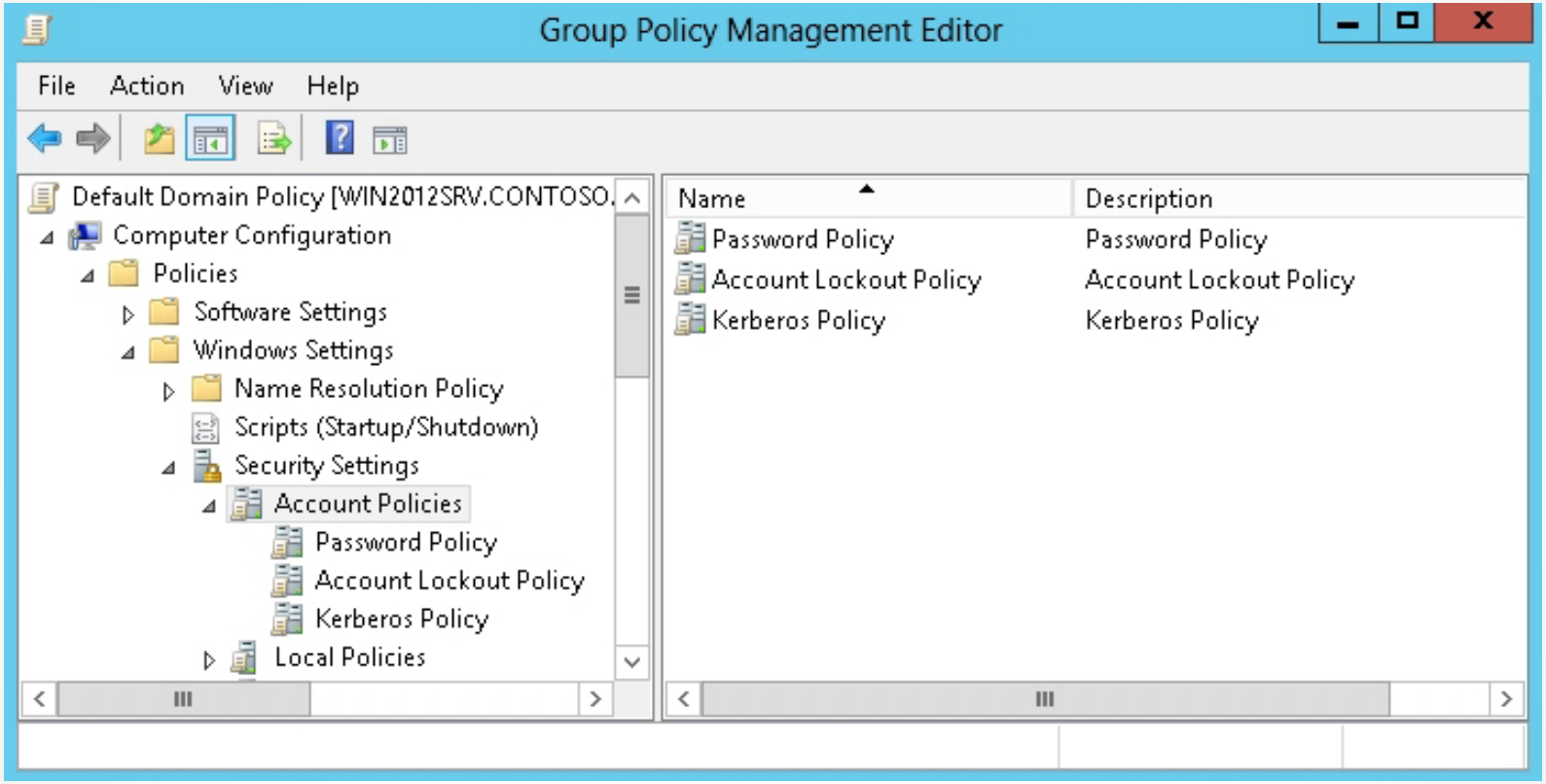
© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

Group Policy Management Editor



Accessing the account policies

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

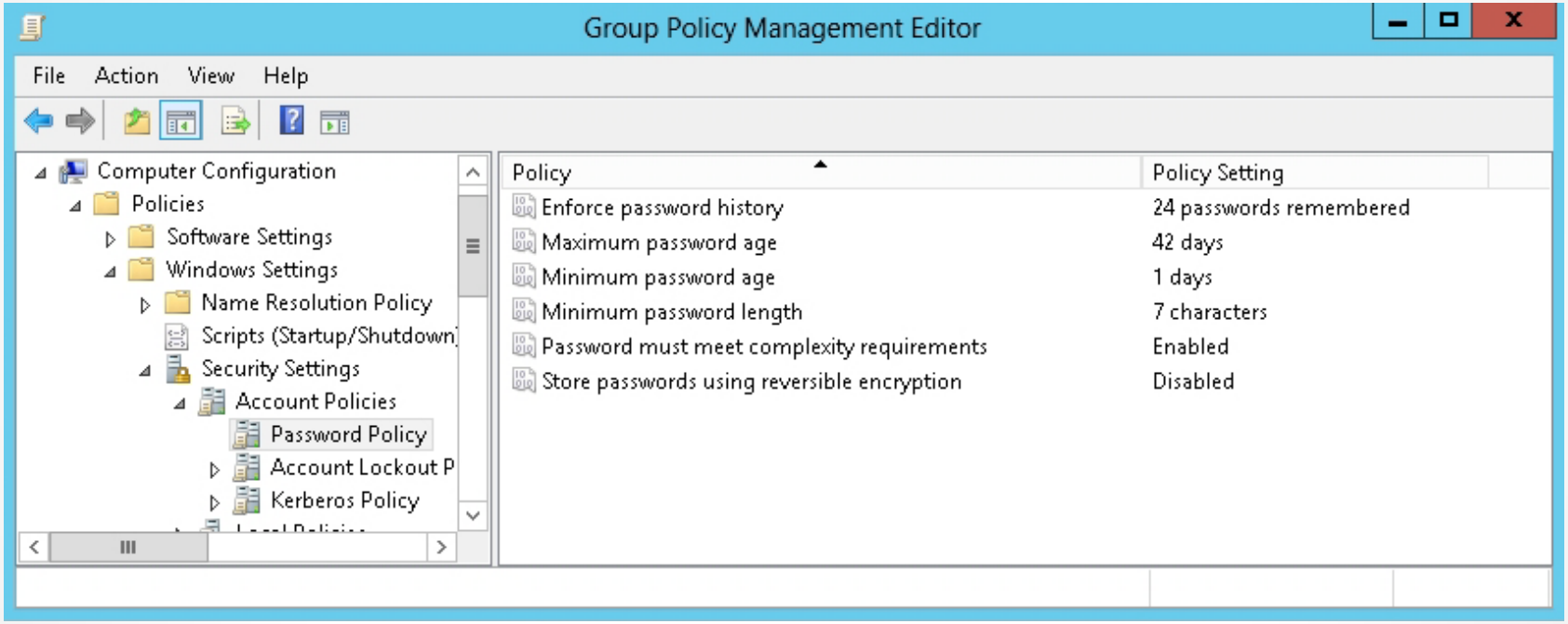
Configuring Password Policy Settings

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, non-alphanumeric characters (such as !@#)(*&^%).

© 2013 John Wiley & Sons, Inc.

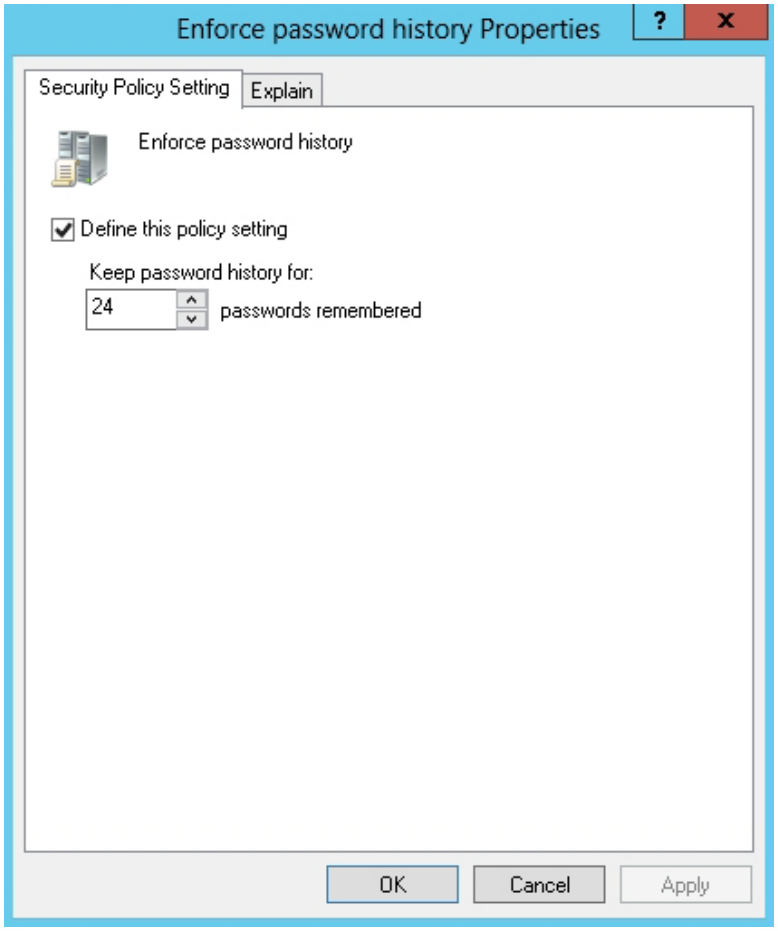
Password Policy Settings



Viewing the Password Policy settings

© 2013 John Wiley & Sons, Inc.

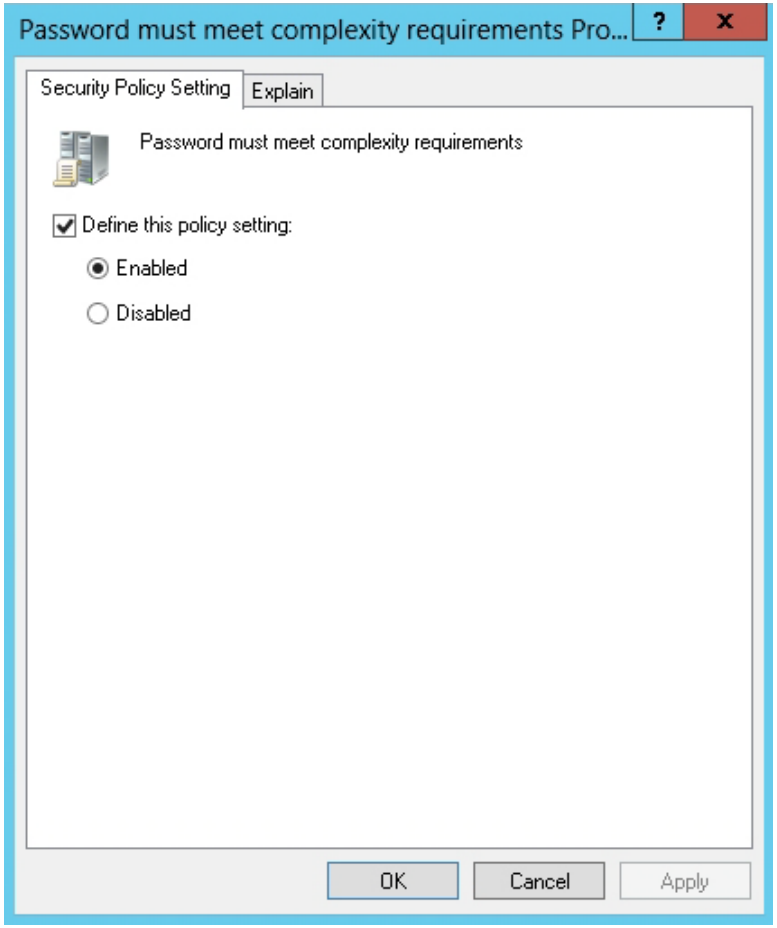
Password Policy Settings



Viewing the Enforce password history

© 2013 John Wiley & Sons, Inc.

Password Policy Settings



Viewing the Complexity requirements

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

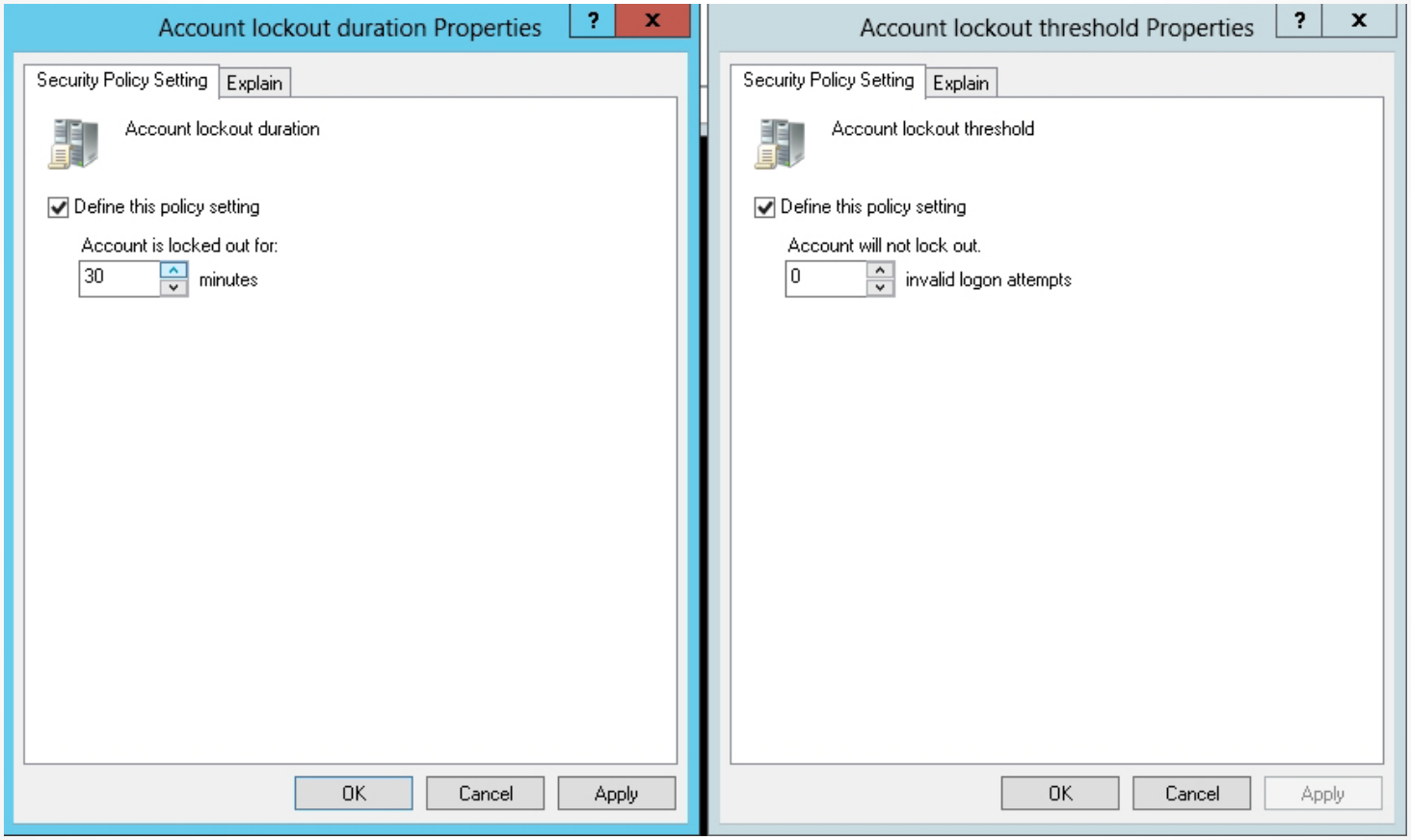
Configuring Account Lockout Settings

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.

© 2013 John Wiley & Sons, Inc.

Account Lockout Policies



Viewing account lockout policies

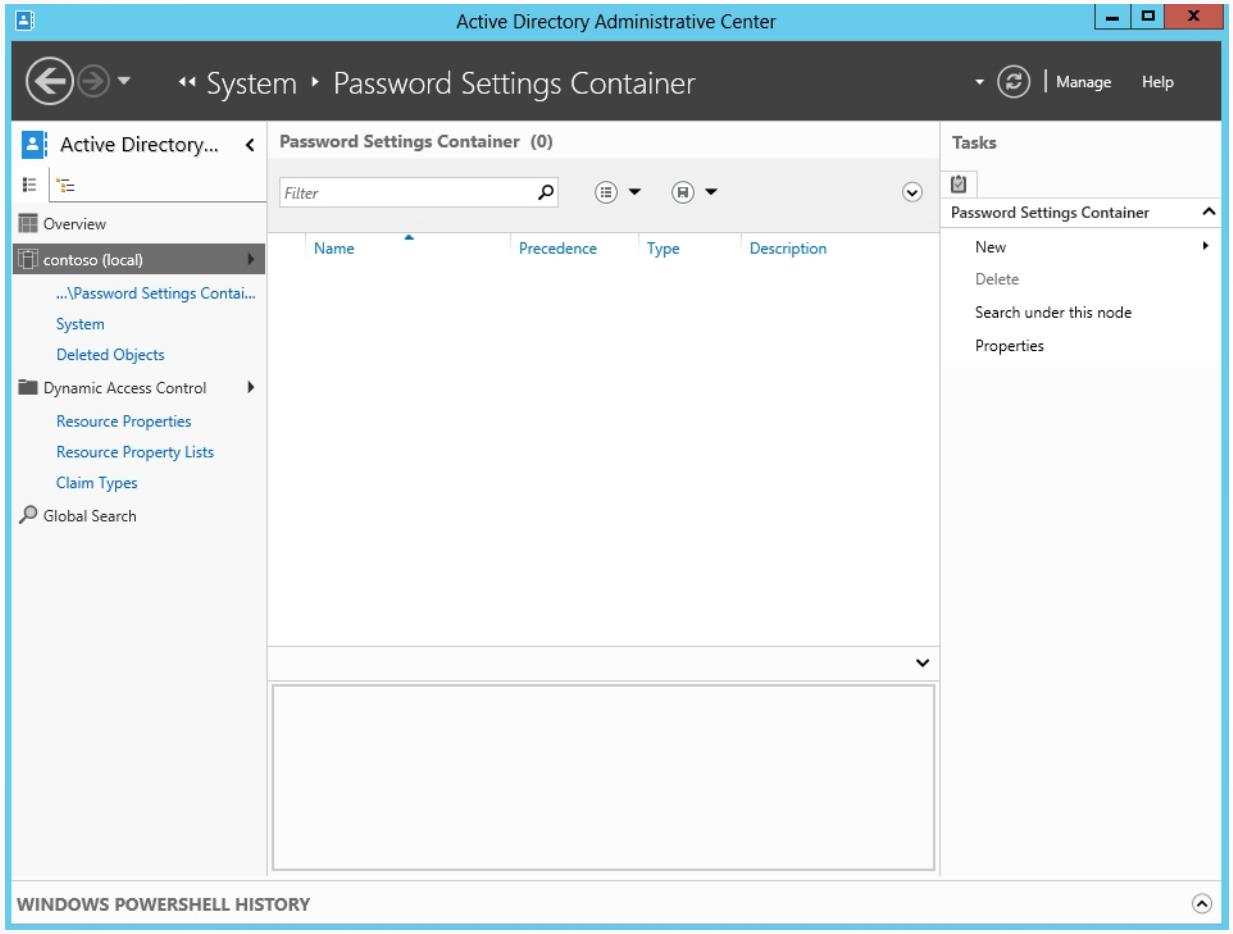
© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

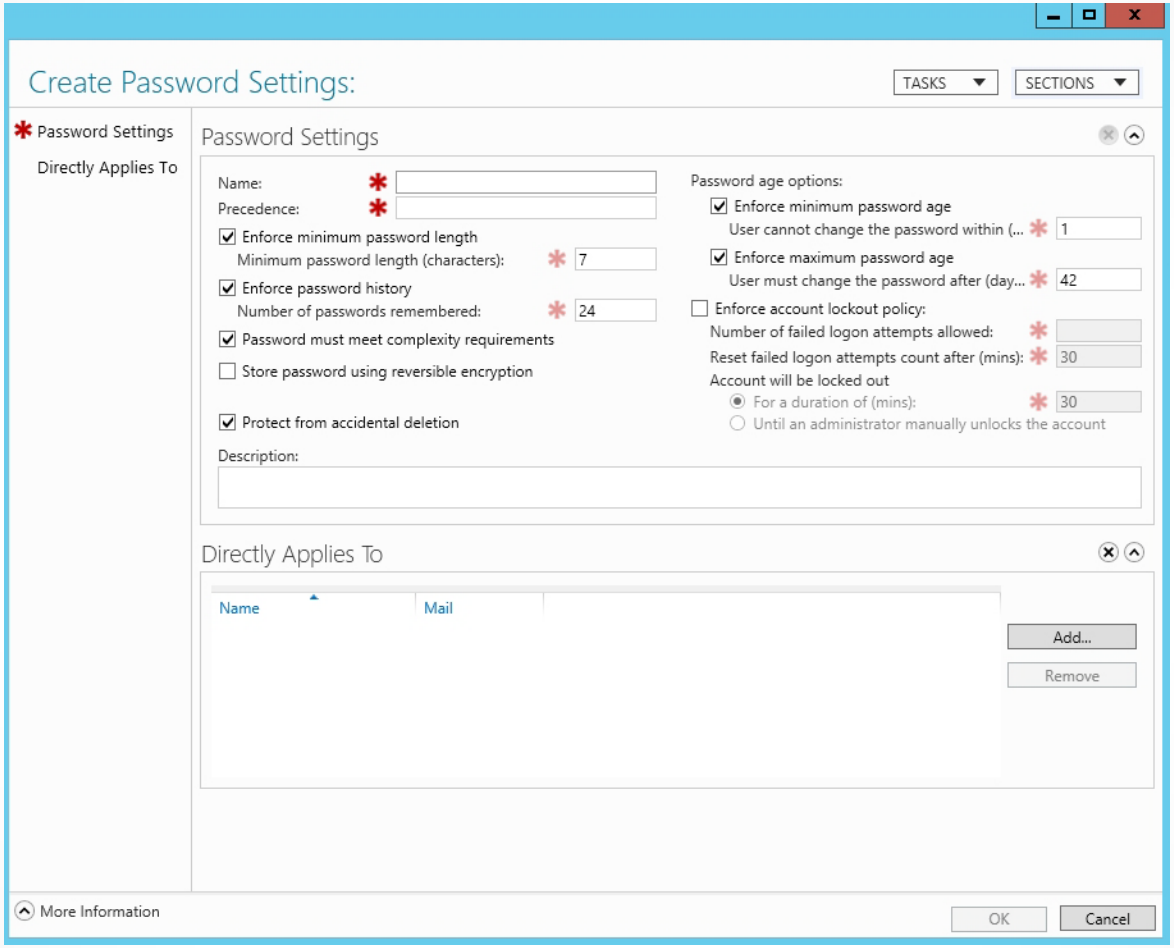
Create and Configure Password Settings Container



Opening the Password Settings Container

© 2013 John Wiley & Sons, Inc.

Create and Configure Password Settings Container



Creating a New Password Settings Container

© 2013 John Wiley & Sons, Inc.

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
```

© 2013 John Wiley & Sons, Inc.

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.

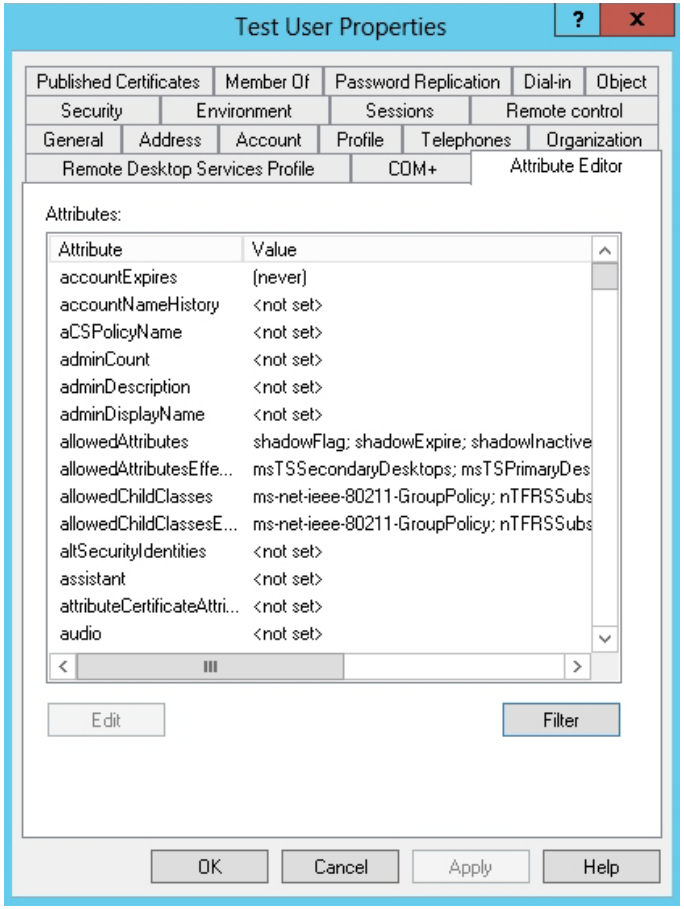
© 2013 John Wiley & Sons, Inc.

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.
5. 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.

© 2013 John Wiley & Sons, Inc.

View the msDS-ResultantPSO Attribute



Viewing user attributes

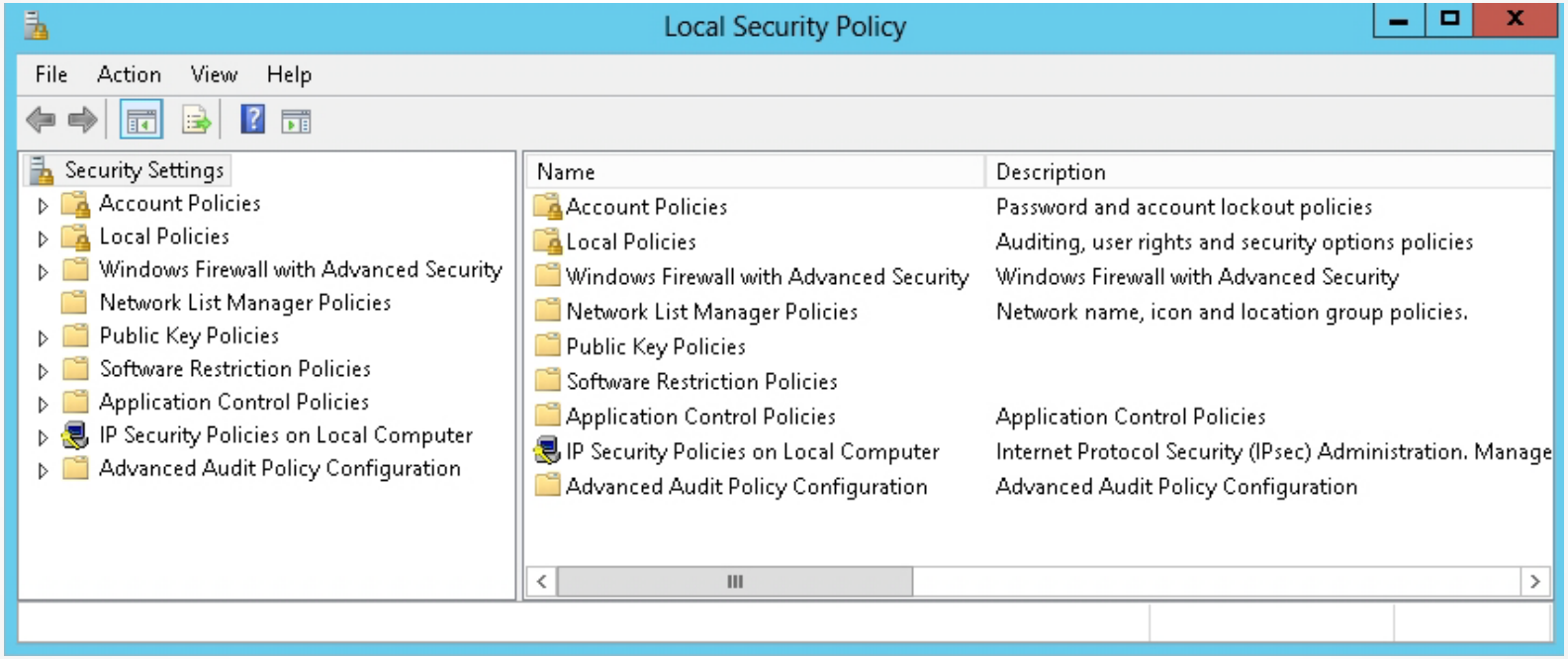
© 2013 John Wiley & Sons, Inc.

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

© 2013 John Wiley & Sons, Inc.

Local Security Policy Console



Opening the Local Security Policy

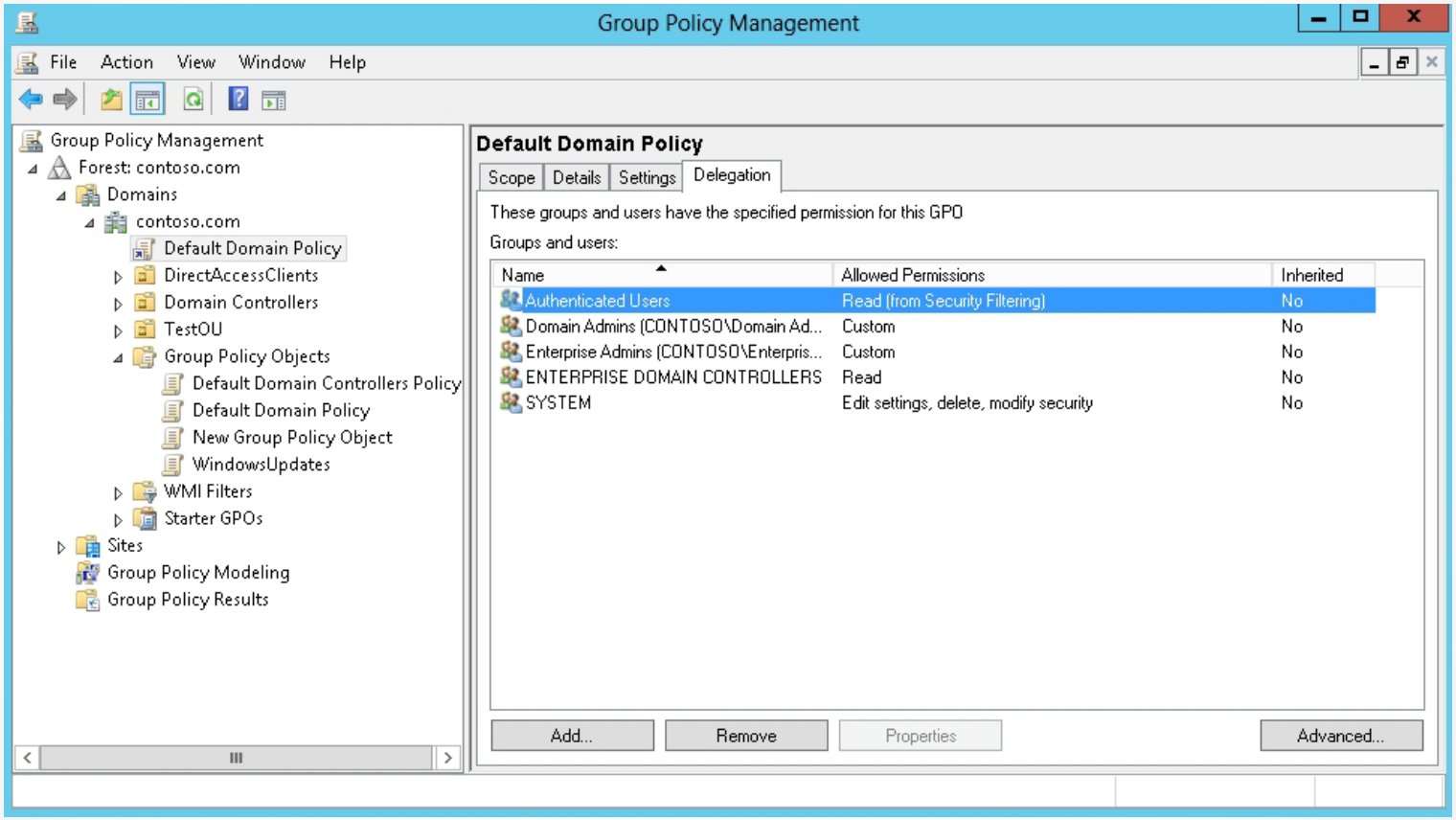
© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

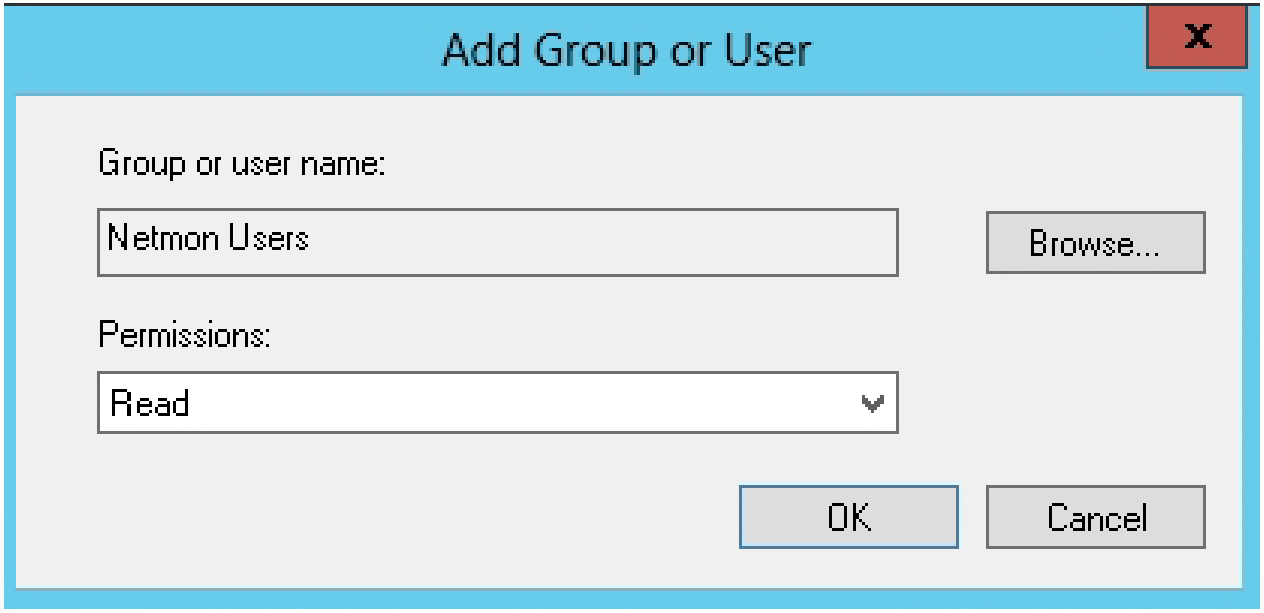
Manage GPO Permissions



Displaying the Delegation tab

© 2013 John Wiley & Sons, Inc.

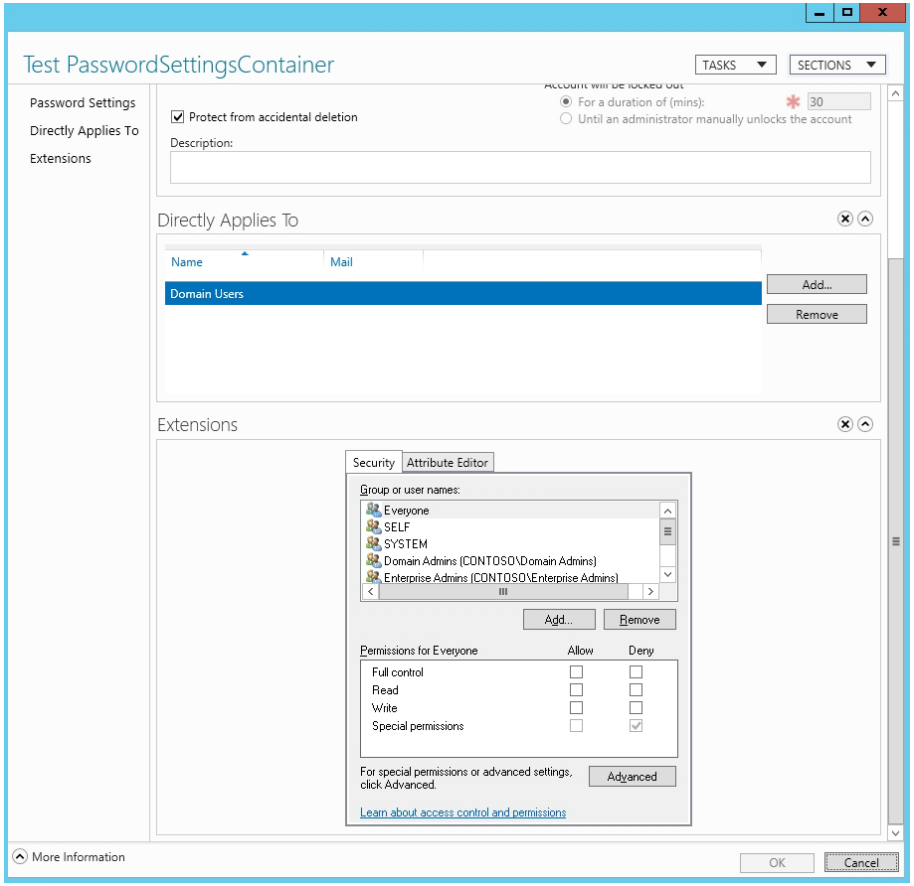
Manage GPO Permissions



Assigning permissions to a GPO

© 2013 John Wiley & Sons, Inc.

Manage Password Settings Object Permissions



Viewing the users and groups that have access to the PSO

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.

© 2013 John Wiley & Sons, Inc.

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.