Lesson 17: Configuring Security Policies

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 6.2: Configure Security Policies
- Configuring Security Policies Using Group Policy
- Configuring Local Users and Groups
- Configuring User Account Control

© 2013 John Wiley & Sons, Inc.

Configuring Security Policies Using Group Policy

Lesson 17: Configuring Security Policies

© 2013 John Wiley & Sons, Inc.

Configuring Security Policies Using Group Policy

- One of the primary aims of Group Policy is to provide centralized management of security settings for users and computers.
- Most of the settings that pertain to security are found in the Windows Settings folder within the Computer Configuration node of a Group Policy object (GPO).
- You can use security settings to govern how users are authenticated to the network, the resources they are permitted to use, group membership policies, and events related to user and group actions recorded in the event logs.

© 2013 John Wiley & Sons, Inc.

Defining Local Policies

- **Local Policies** enable administrators to set user privileges on the local computer to govern what users can do on the computer and determine if the system should track them in an event log.
- **Auditing** is tracking events that take place on the local computer.
- The Local Policies node of a GPO has three subordinate nodes: **User Rights Assignment**, **Security Options**, and **Audit Policy**.

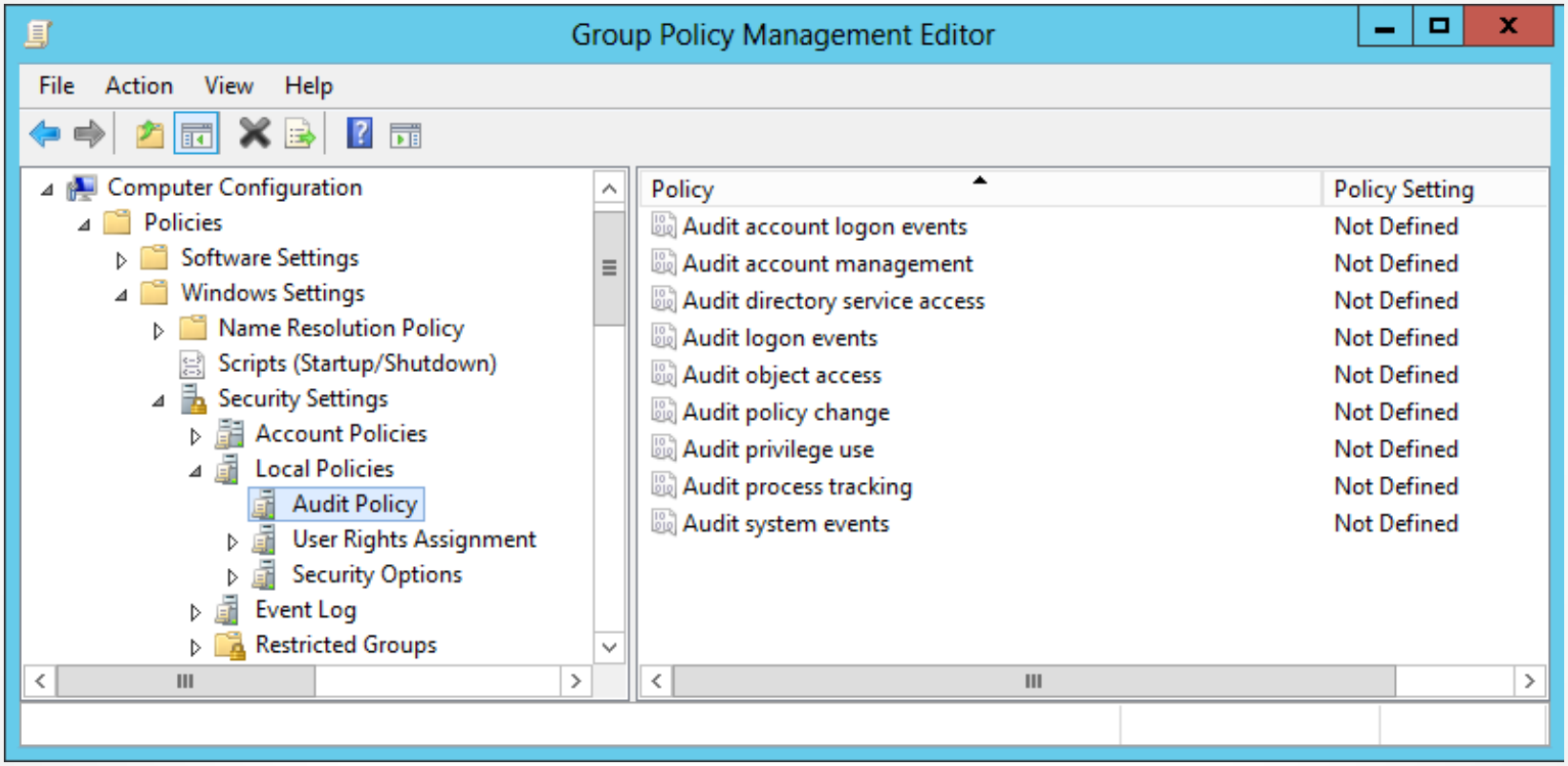
© 2013 John Wiley & Sons, Inc.

Planning and Configuring an Audit Policy

- The Audit Policy section of a GPO enables administrators to log successful and failed security events, such as logon events, account access, and object access.
- You can use auditing to track both user activities and system activities.
- Planning to audit requires that you determine the computers to be audited and the types of events you wish to track.

© 2013 John Wiley & Sons, Inc.

Planning and Configuring an Audit Policy



Audit Policies in the Default Domain Policy

© 2013 John Wiley & Sons, Inc.

Planning and Configuring an Audit Policy

The following guidelines can help you to plan your audit policy:

- Audit only pertinent items.
- Archive security logs to provide a documented history.
- Configure the size of your security logs carefully.

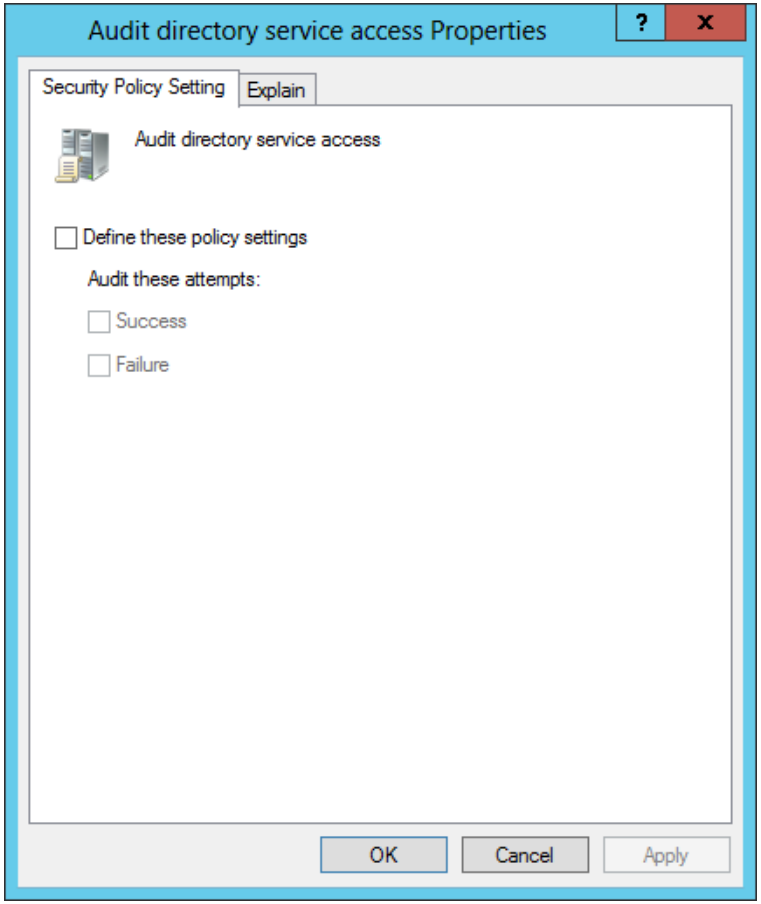
© 2013 John Wiley & Sons, Inc.

Event Categories

- System events
- Policy change events
- Account management events
- Logon events
- Account logon events

© 2013 John Wiley & Sons, Inc.

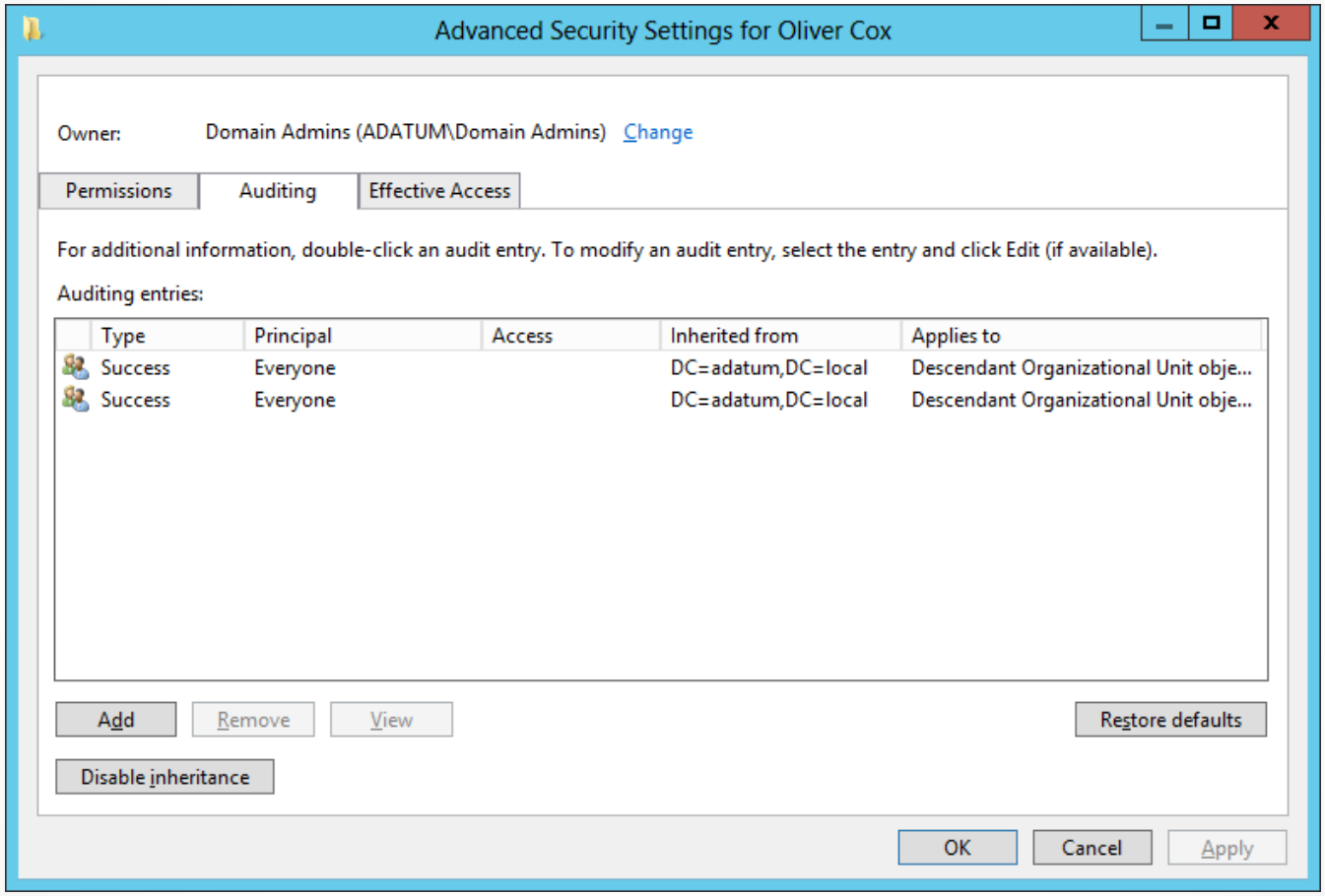
Configure an Audit Policy



The Properties sheet for a policy setting

© 2013 John Wiley & Sons, Inc.

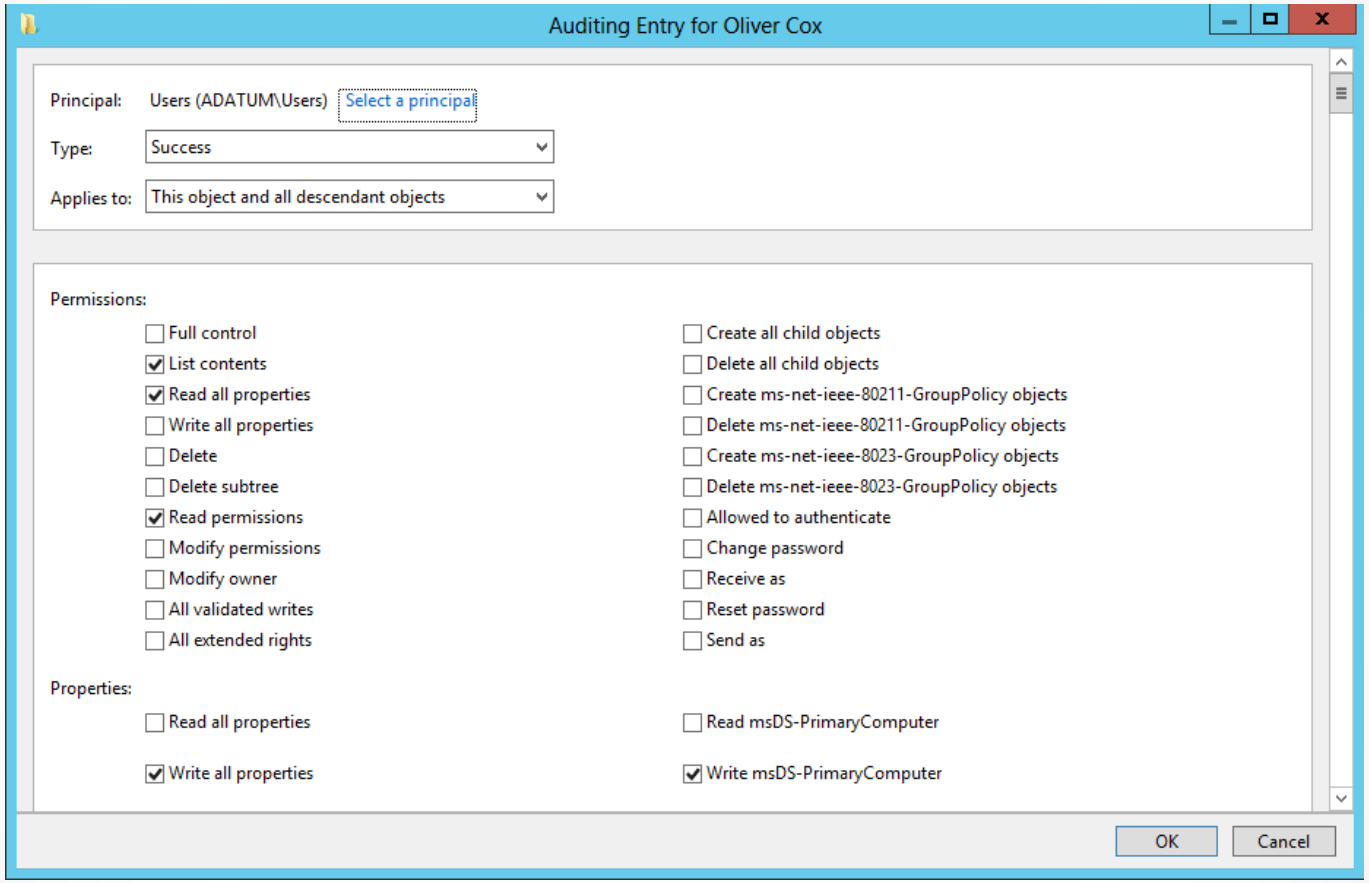
Configure an Active Directory Object for Auditing



The Auditing tab of an object's Advanced Security Settings dialog box

© 2013 John Wiley & Sons, Inc.

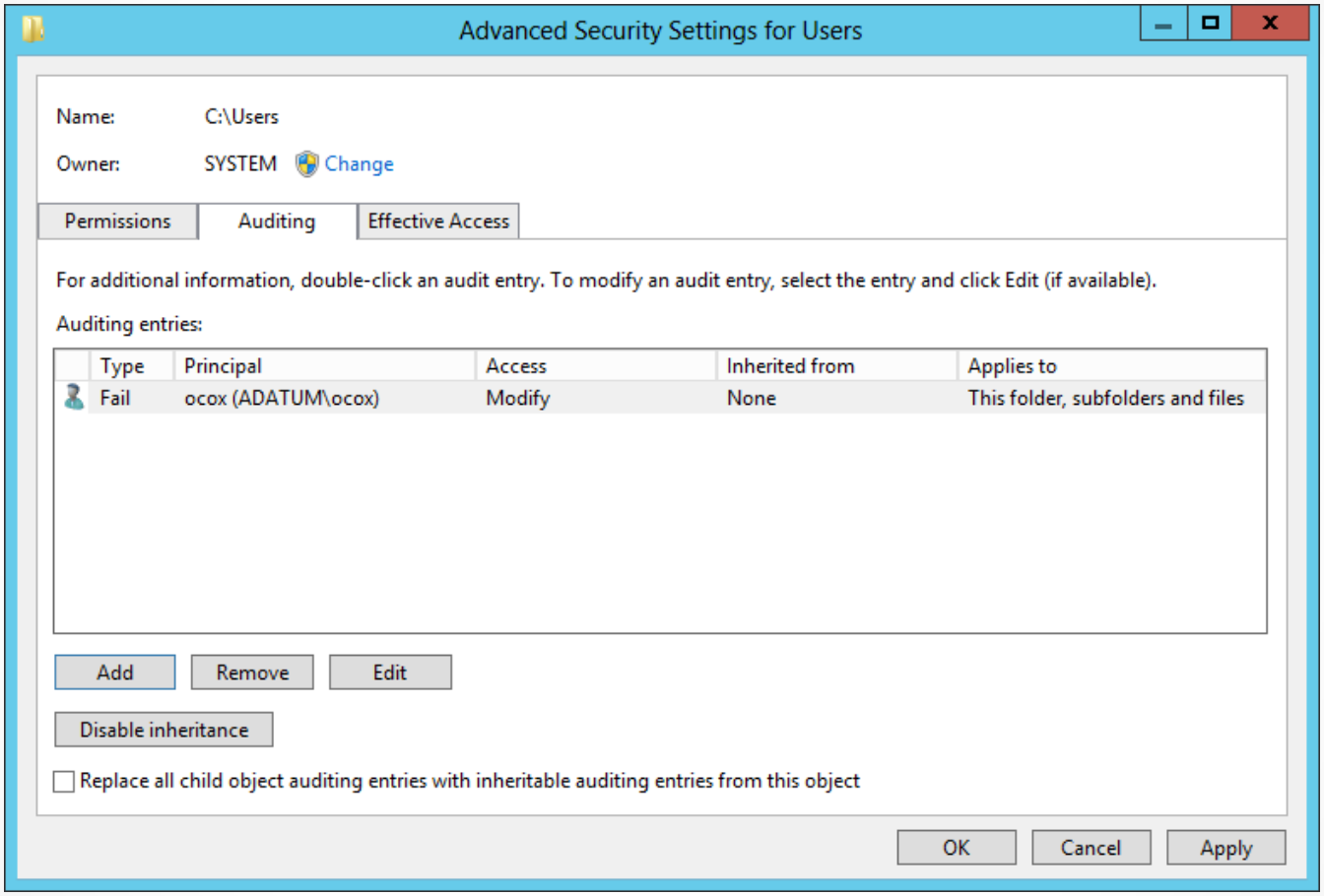
Configure an Active Directory Object for Auditing



The Auditing Entry dialog box for an object

© 2013 John Wiley & Sons, Inc.

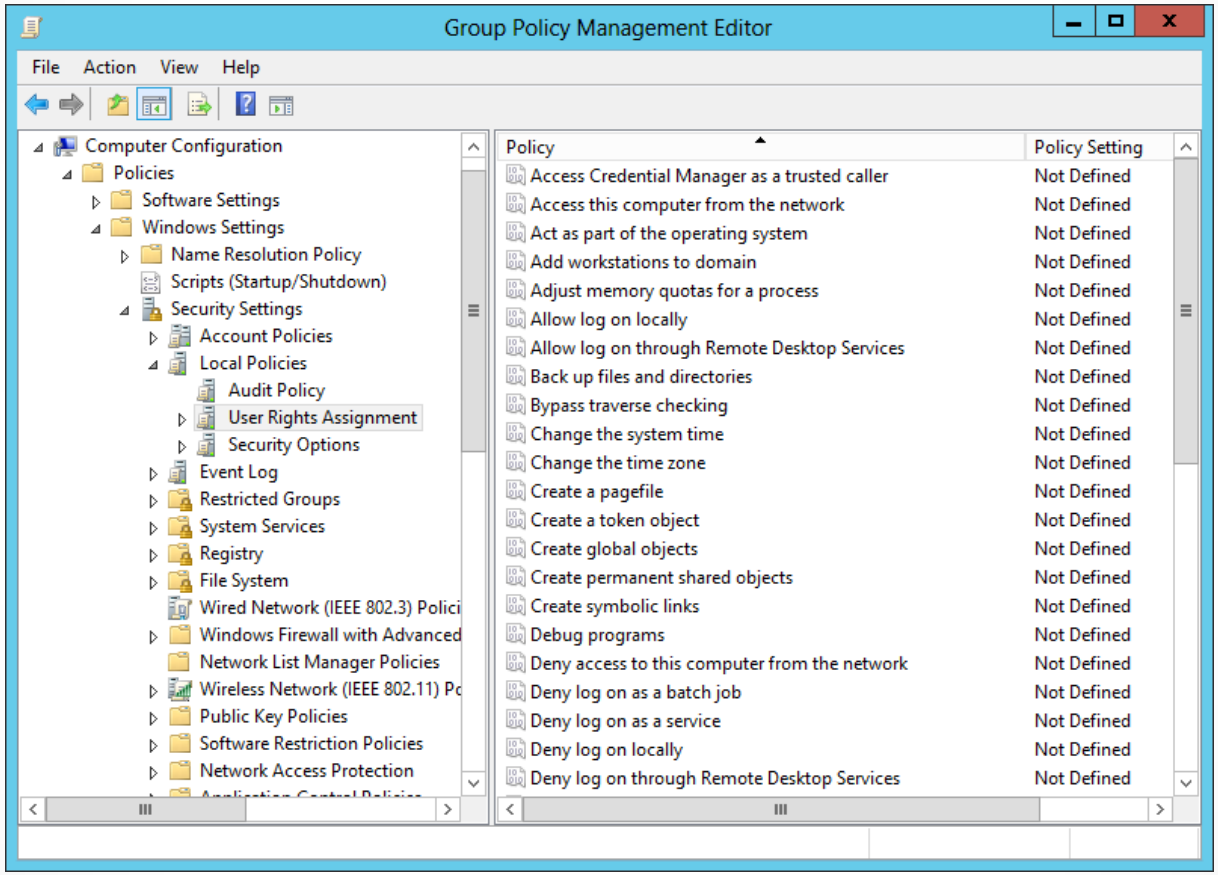
Configure an Active Directory Object for Auditing



A new auditing entry in the Advanced Security Settings dialog box

© 2013 John Wiley & Sons, Inc.

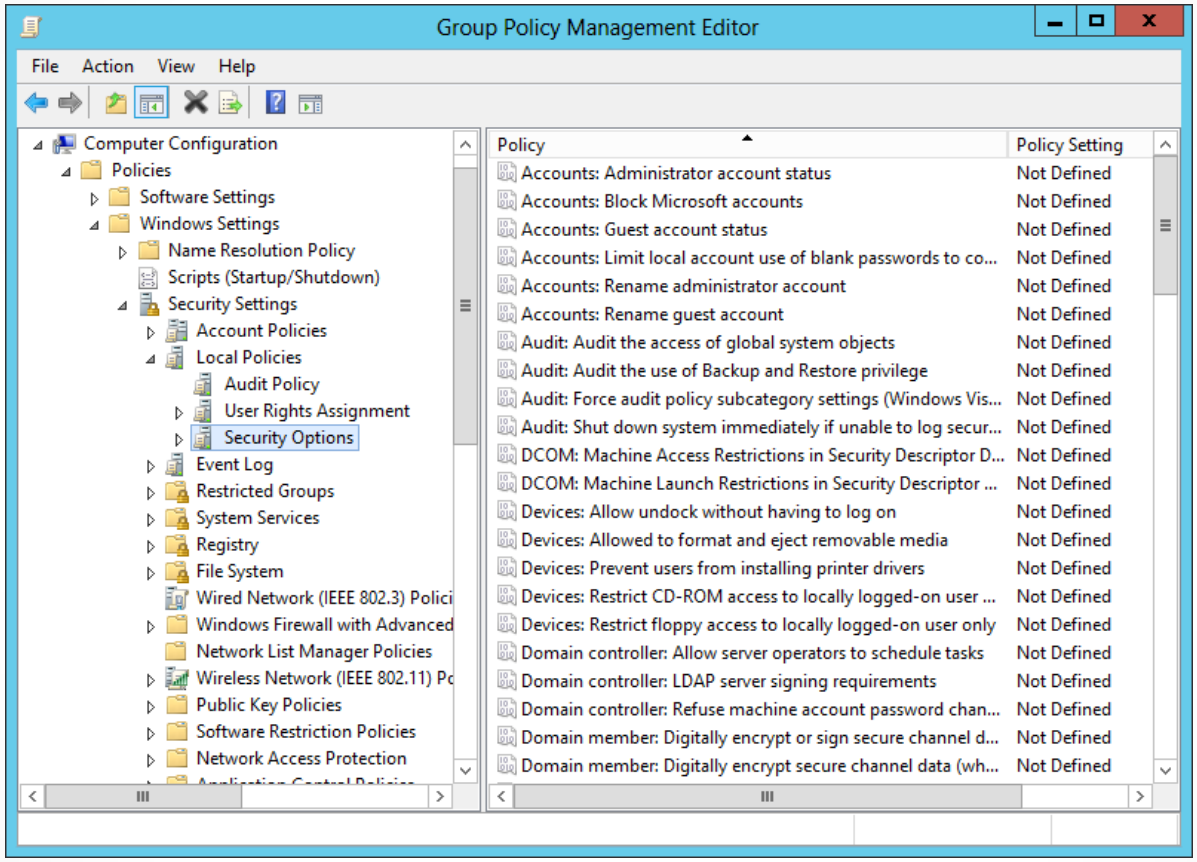
Assigning User Rights



User rights assignment settings in a Group Policy object

© 2013 John Wiley & Sons, Inc.

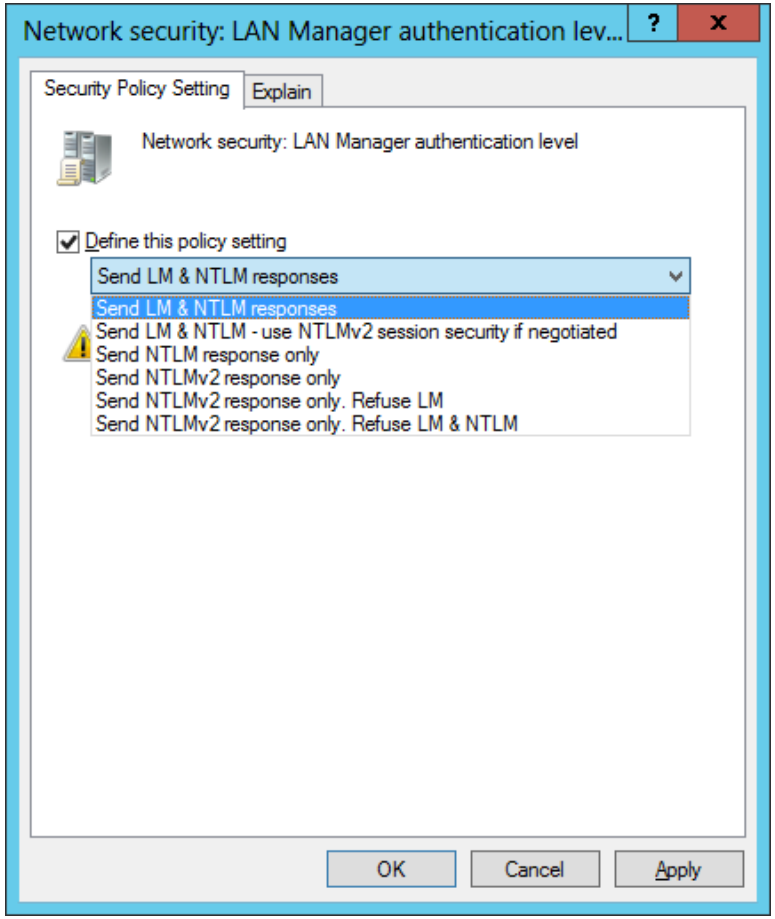
Configuring Security Options



The Security Options node in a GPO

© 2013 John Wiley & Sons, Inc.

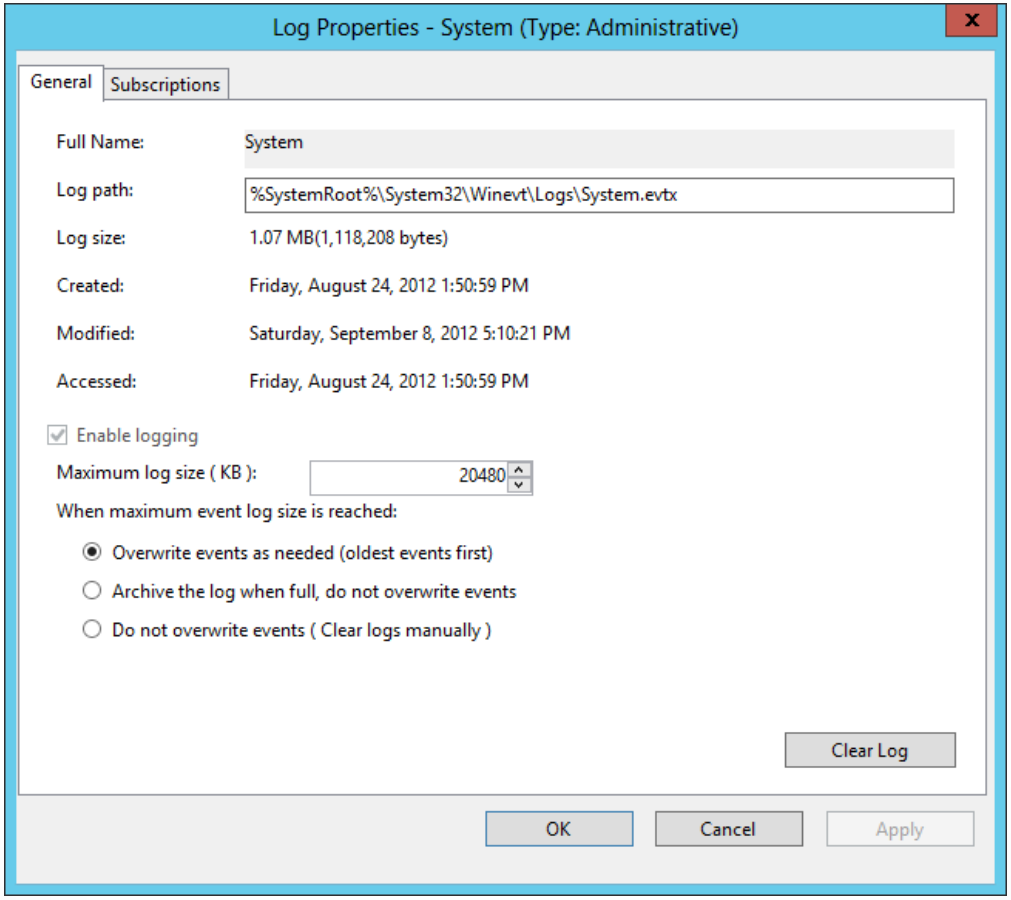
Configuring Security Options



The Network security: LAN Manager authentication level security option

© 2013 John Wiley & Sons, Inc.

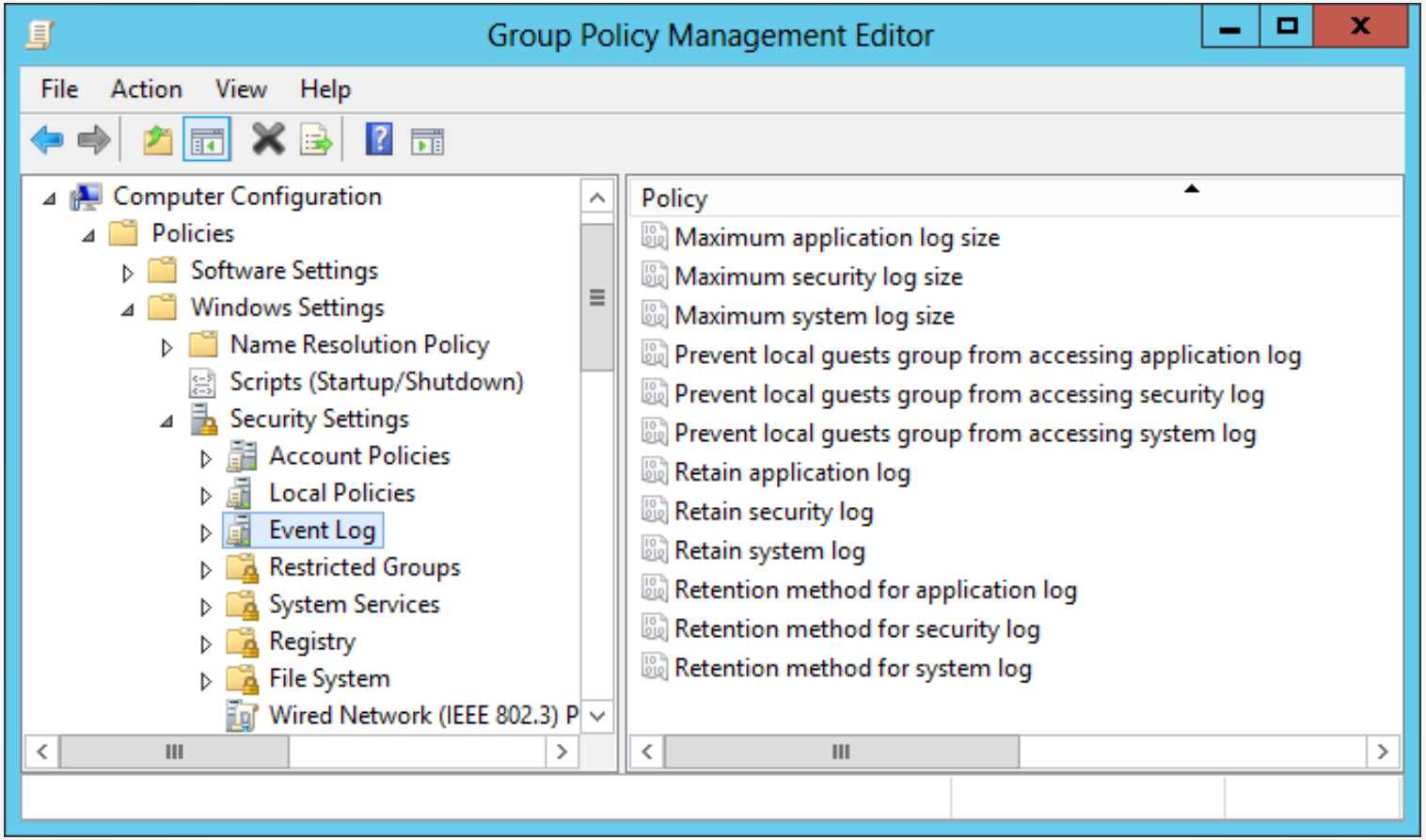
Customizing Event Log Policies



The Properties sheet for an event log in the Event Viewer console

© 2013 John Wiley & Sons, Inc.

Customizing Event Log Policies



Policies in the Event Log node of a GPO

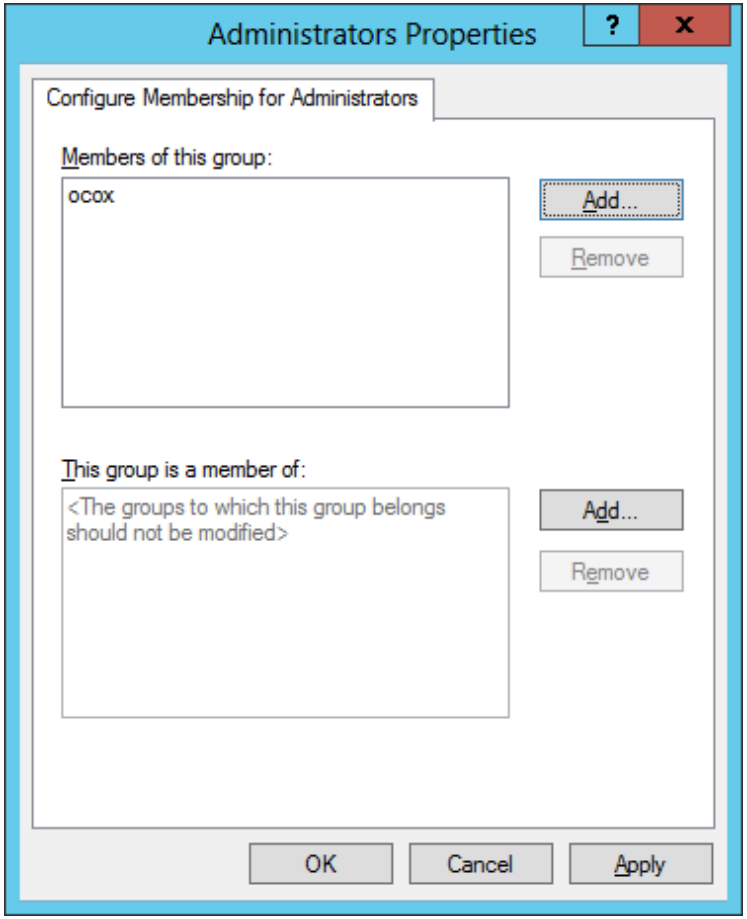
© 2013 John Wiley & Sons, Inc.

Restricted Groups

- The **Restricted Groups** policy setting enables an administrator to specify group membership lists.
- You can control membership in important groups, such as the local Administrators and Backup Operators groups.
- Only those users who are part of the Restricted Group membership list within the policy setting will be added to the group.

© 2013 John Wiley & Sons, Inc.

Restricted Groups



Group membership in the Restricted Groups policy

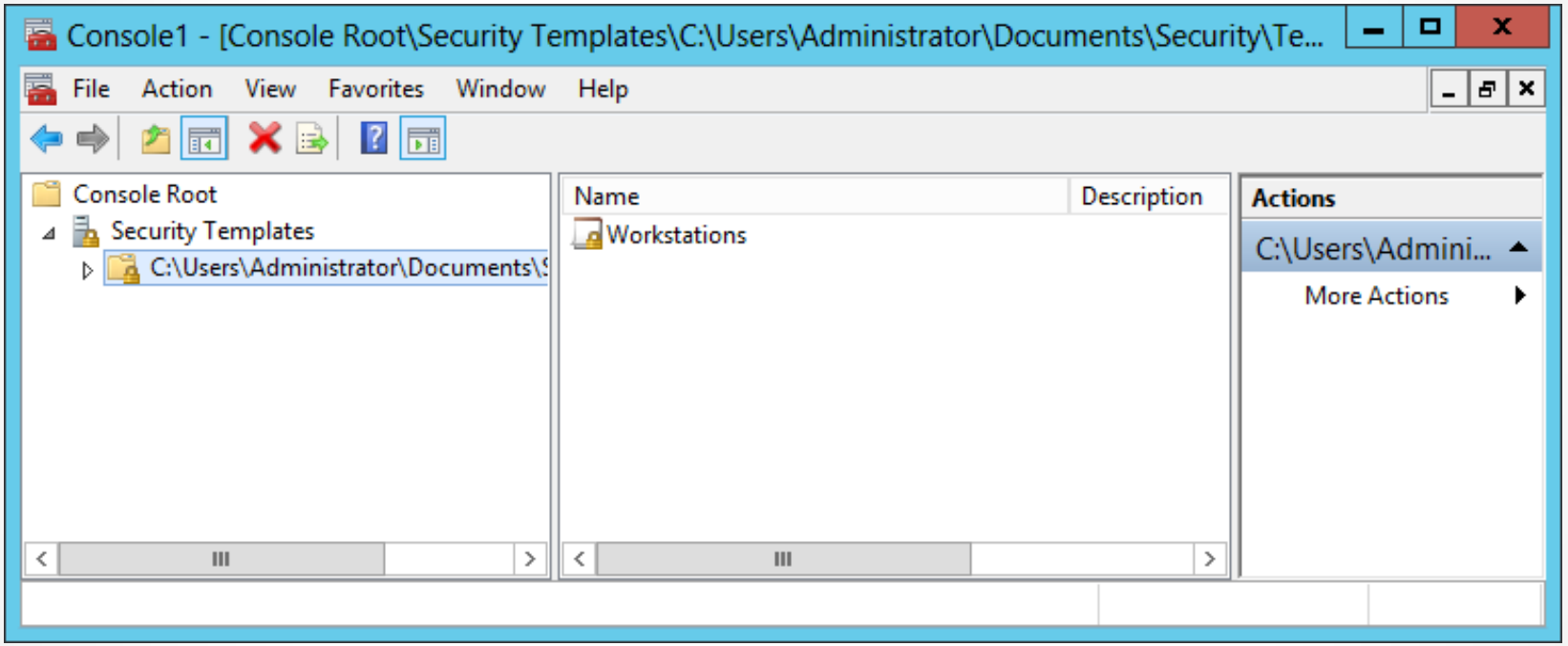
© 2013 John Wiley & Sons, Inc.

Security Templates

- A **security template** is a collection of configuration settings stored as a text file with an .inf extension.
- Can contain many of the same security parameters as group policy objects.
- Parameters are presented in a unified interface, enabling you to save your configurations as files and simplify the process of deploying them.

© 2013 John Wiley & Sons, Inc.

Using the Security Templates Console



The Security Templates snap-in

© 2013 John Wiley & Sons, Inc.

Security Template Planning

By creating templates for specific roles, administrators can apply them to multiple computers, using combinations in cases where computers perform multiple roles.

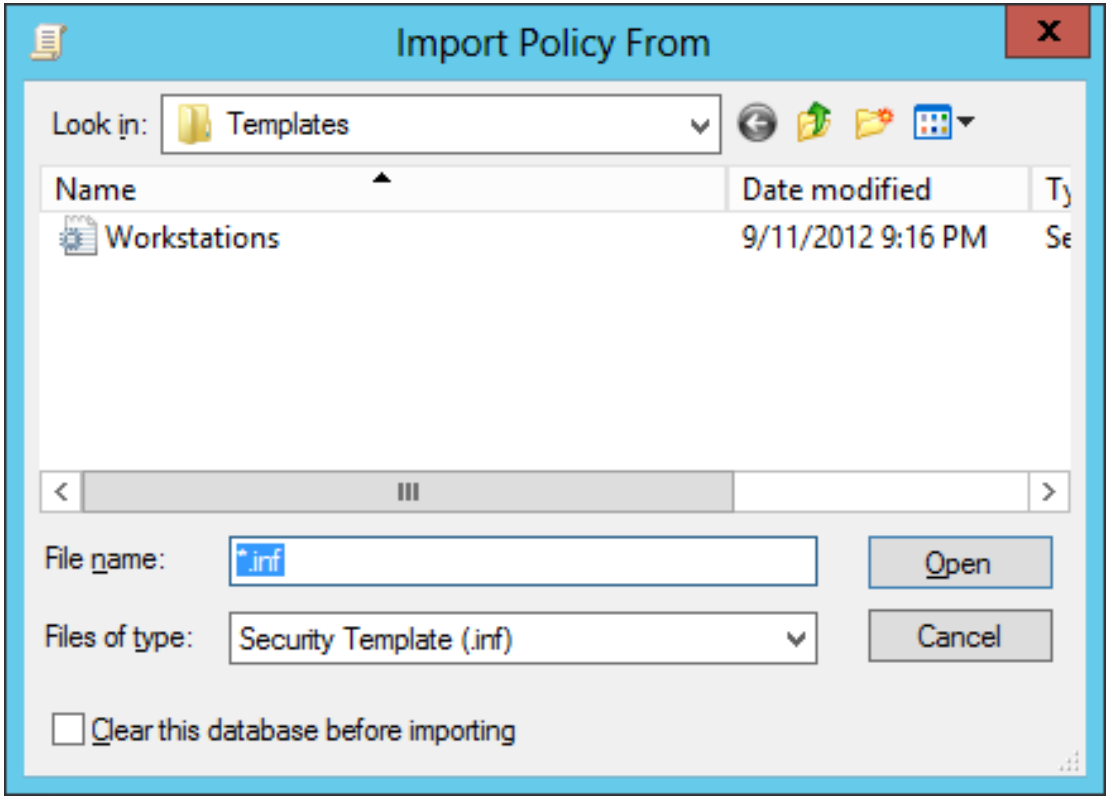
© 2013 John Wiley & Sons, Inc.

Working with Security Template Settings

- Security templates have more settings than Local Computer Policy, because a template includes options for both standalone computers and computers that are participating in a domain.
- Security templates also provide a means for configuring the permissions associated with files, folders, registry entries, and services.

© 2013 John Wiley & Sons, Inc.

Importing Security Templates into GPOs



The Import Policy From dialog box

© 2013 John Wiley & Sons, Inc.

Maintaining and Optimizing Group Policy

These are the default refresh periods for the various types of Group Policy settings:

- Set Group Policy Refresh Interval for Computers
- Set Group Policy Refresh Interval for Domain Controllers
- Set Group Policy Refresh Interval for Users

© 2013 John Wiley & Sons, Inc.

Manually Refreshing Group Policy

When you modify Group Policy settings that you wish to be immediately invoked without requiring a restart, a new logon session, or waiting for the next refresh period, you can force a manual refresh by using the **Gpupdate.exe** tool:

```
Gpupdate/target:user
Gpupdate/target:computer
```

© 2013 John Wiley & Sons, Inc.

Optimizing Group Policy Processing

When you create a GPO that contains computer or user settings, but not both, you can disable the setting area that is not configured for faster processing.

© 2013 John Wiley & Sons, Inc.

Configuring Local Users and Groups

Lesson 17: Configuring Security Policies

© 2013 John Wiley & Sons, Inc.

Configuring Local Users and Groups

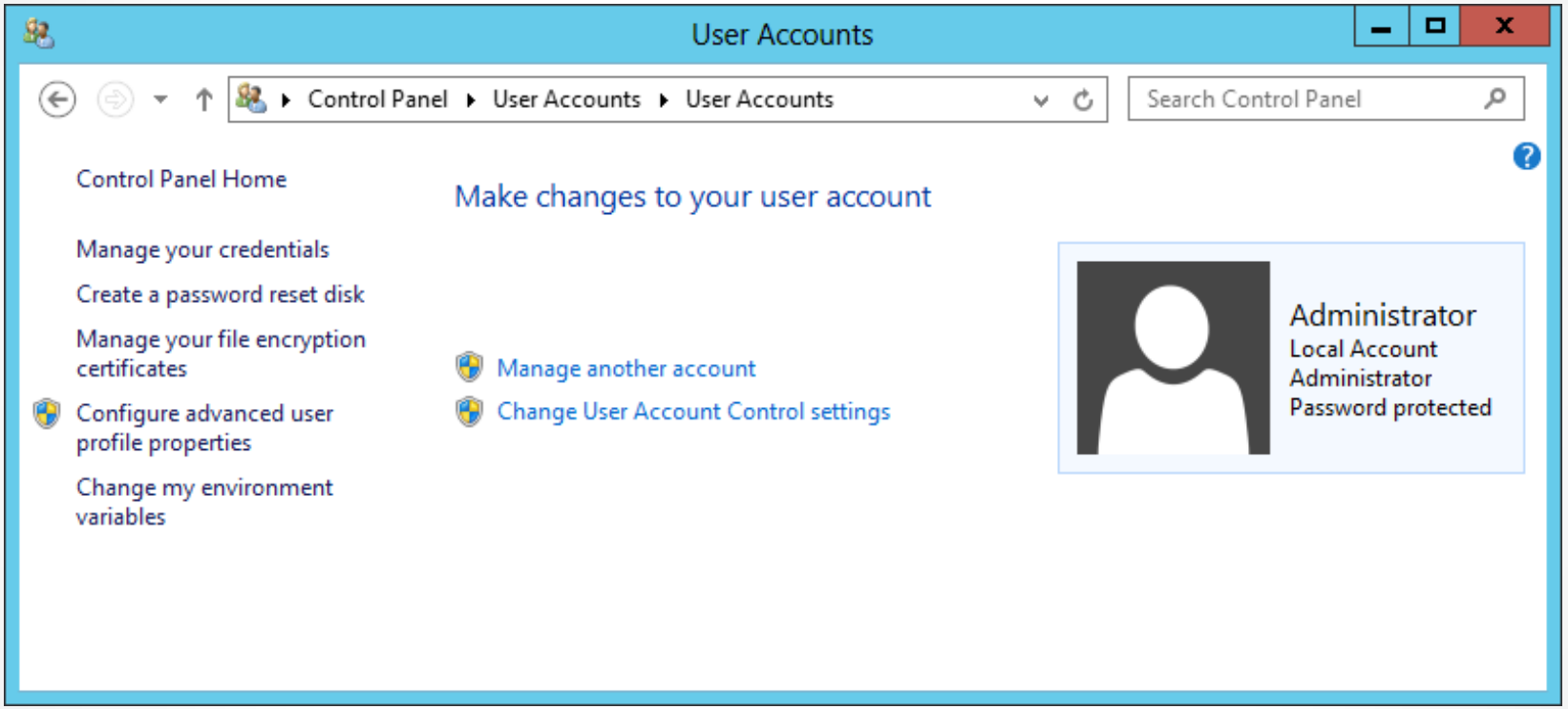
Windows Server 2012 provides two separate interfaces for creating and managing local user accounts:

- **User Accounts** control panel
- **Local Users and Groups** snap-in for MMC

Both interfaces provide access to the same Security Account Manager (SAM) where the user and group information is stored, so any changes you make using one interface will appear in the other.

© 2013 John Wiley & Sons, Inc.

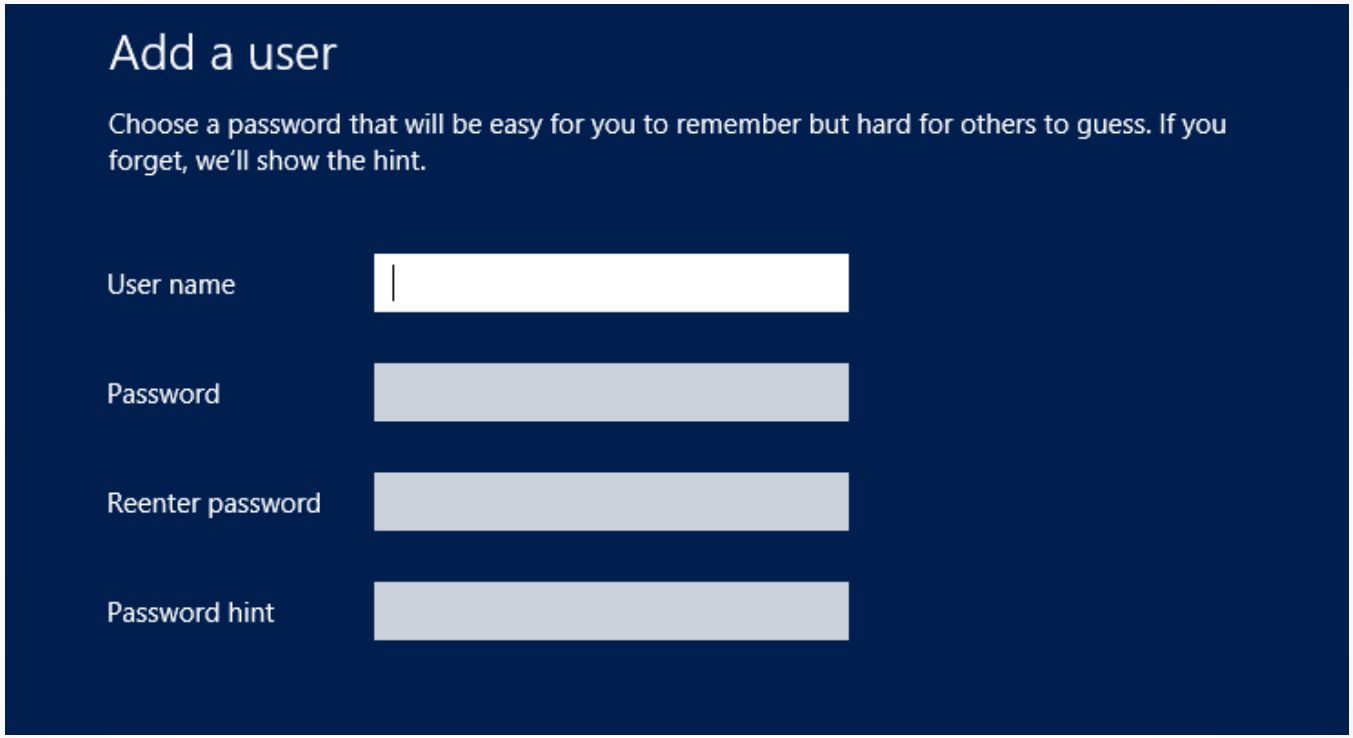
Create a New Local User Account with the Control Panel



The Make changes to your user account window

© 2013 John Wiley & Sons, Inc.

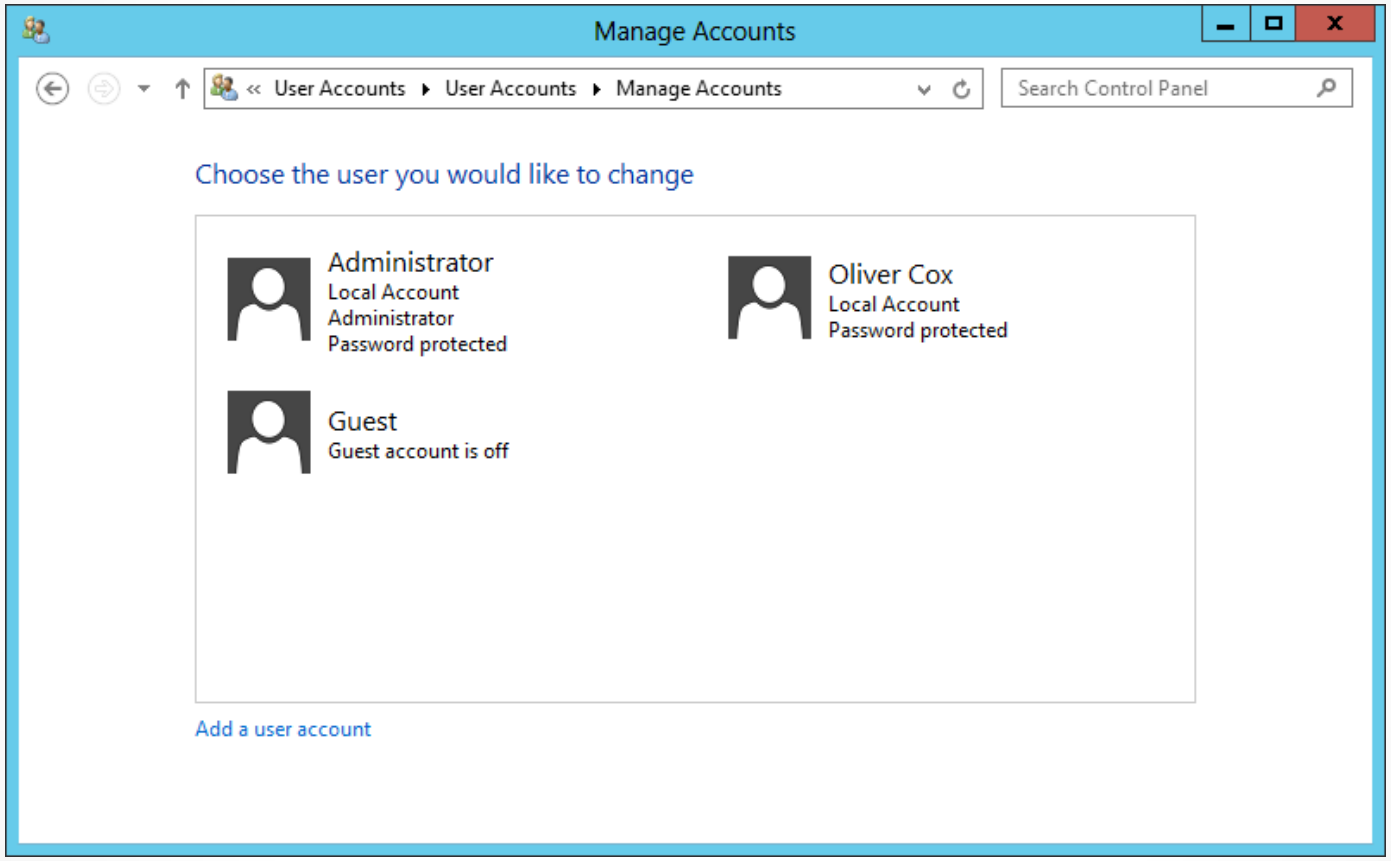
Create a New Local User Account with the Control Panel



The Add a user page

© 2013 John Wiley & Sons, Inc.

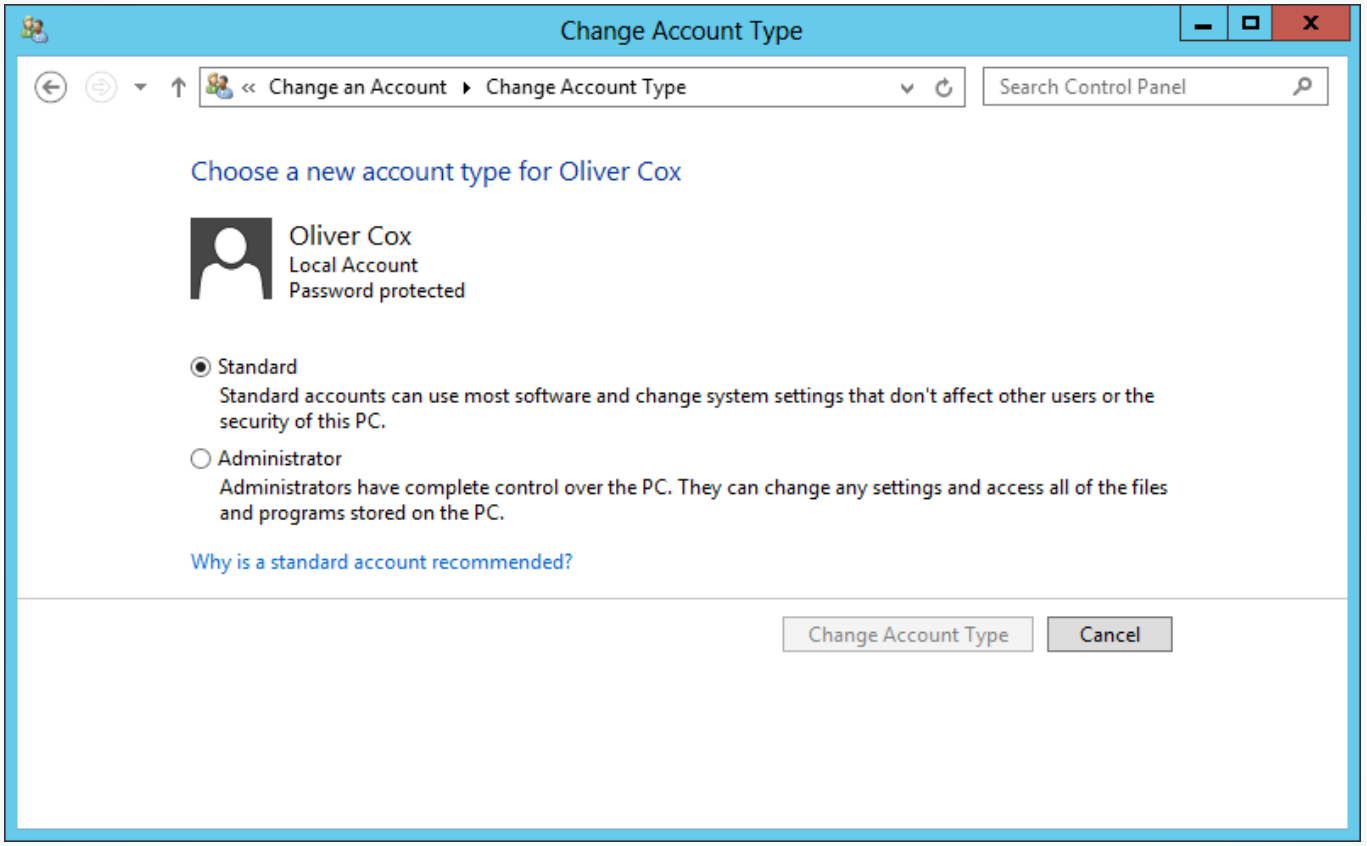
Create a New Local User Account with the Control Panel



The Manage Accounts window

© 2013 John Wiley & Sons, Inc.

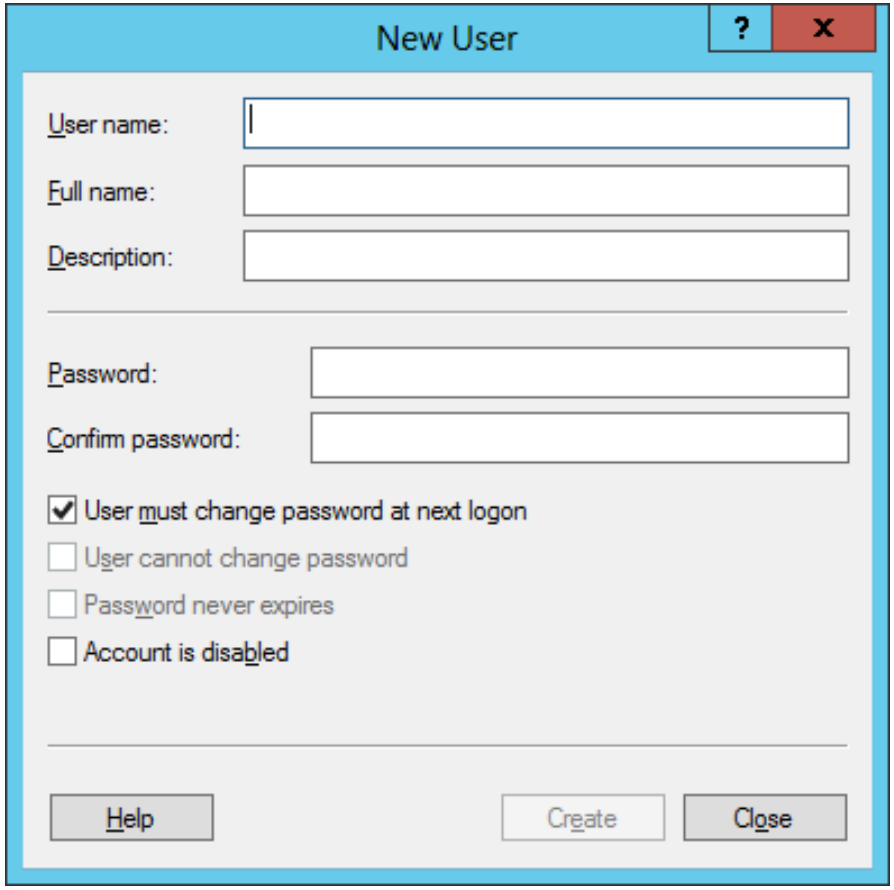
Create a New Local User Account with the Control Panel



The Change Account Type window

© 2013 John Wiley & Sons, Inc.

Create a New Local User Account with Local Users and Groups



The New User dialog box

© 2013 John Wiley & Sons, Inc.

Configuring User Account Control

Lesson 17: Configuring Security Policies

© 2013 John Wiley & Sons, Inc.

Configuring User Account Control

- **User Account Control (UAC)** is the mechanism that prevents users from accessing the system using administrative privileges unless those privileges are required to perform the task at hand.
- Administrators should only log on to a server using an account with administrative access when performing administrative tasks; however, it is often inconvenient to switch back and forth between an administrative account and standard user account.

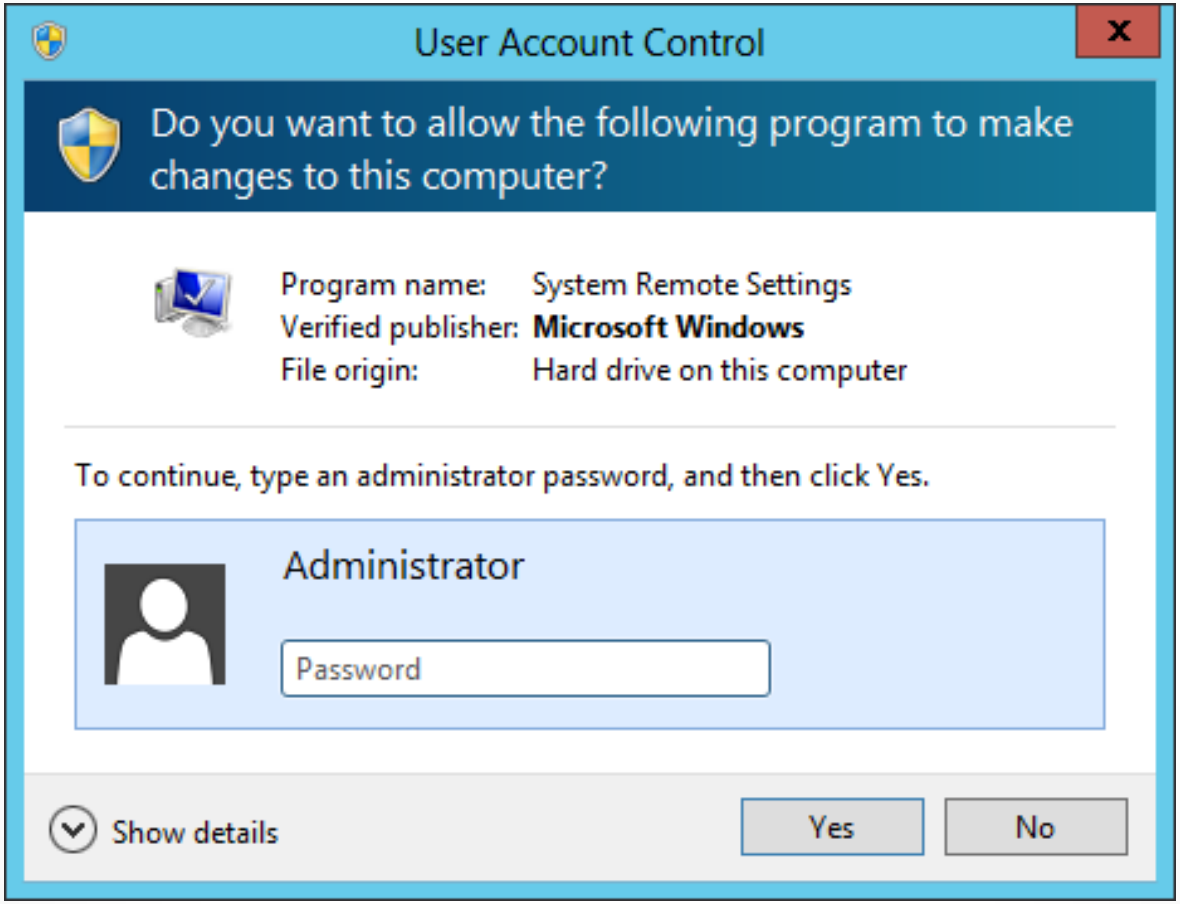
© 2013 John Wiley & Sons, Inc.

Performing Administrative Tasks

- When a user logs on to Windows Server 2012, the system issues a token, which indicates the user's access level.
- Whenever the system authorizes the user to perform a particular activity, it consults the token to see if the user has the required privileges.
- On a computer running Windows Server 2012 with User Account Control, a standard user still receives a standard user token, but an administrative user receives two tokens: one for standard user access and one for administrative user access.
- By default, the standard and administrative users both run using the standard user token most of the time.

© 2013 John Wiley & Sons, Inc.

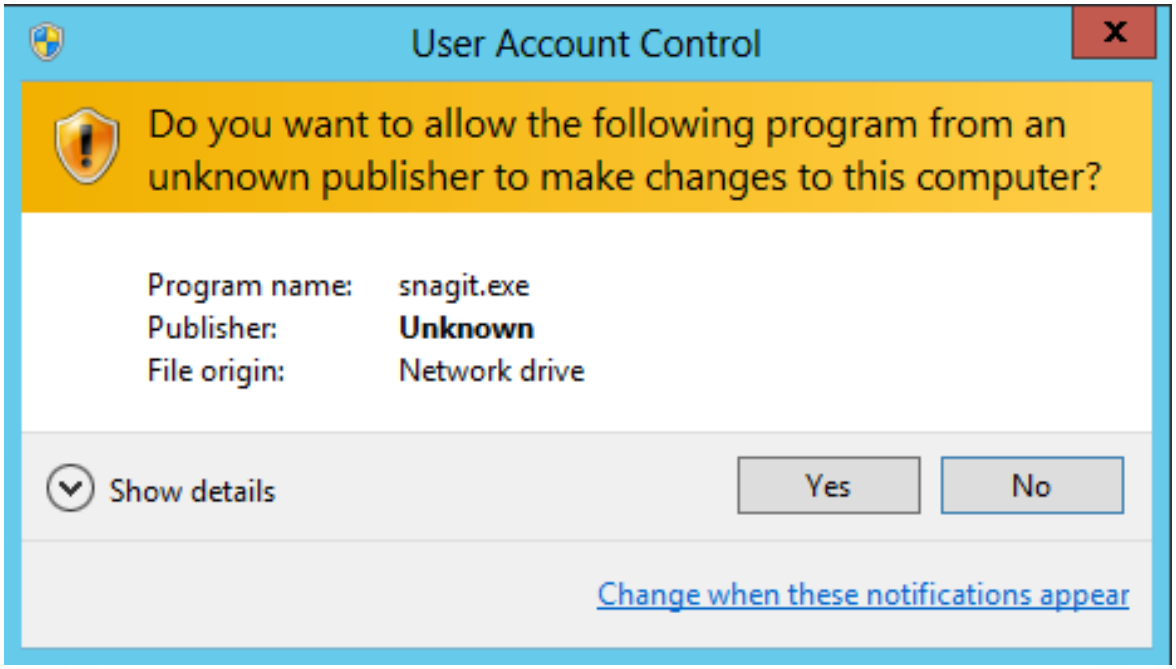
Performing Administrative Tasks



A UAC credential prompt

© 2013 John Wiley & Sons, Inc.

Performing Administrative Tasks



A UAC elevation prompt

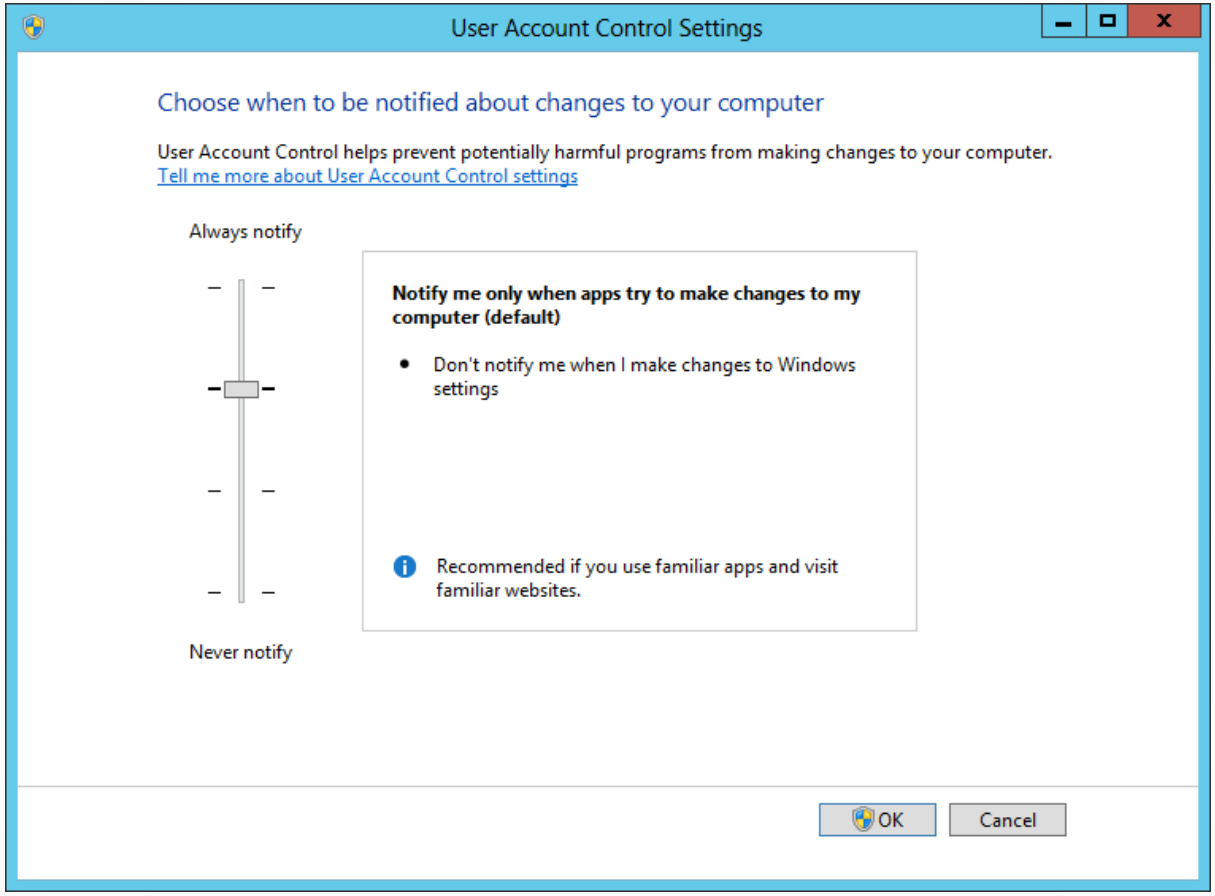
© 2013 John Wiley & Sons, Inc.

Secure Desktop

- The **secure desktop** is an alternative to the interactive user desktop that Windows normally displays.
- When an elevation or credential prompt is generated, the system switches to the secure desktop, suppressing the operation of all other desktop controls and permitting only Windows processes to interact with the prompt.
- The object of this is to prevent malware from automating a response to the elevation or credential prompt and bypassing the human reply.

© 2013 John Wiley & Sons, Inc.

Configure UAC Settings



The User Account Control Settings dialog box

© 2013 John Wiley & Sons, Inc.

Lesson Summary

- Most security-related settings are found within the Windows Settings node of the Computer Configuration node of a GPO.
- Local policy settings govern the actions users can perform on a specific computer and determine if the actions are recorded in an event log.
- Auditing can be configured to audit successes, failures, or both.
- Because audited events are recorded in the appropriate event log, it is necessary to understand the Event Log Policy setting area. This area allows control over maximum log sizes, log retention, and access rights to each log.
- Restrictions on group memberships can be accomplished using the Group Restriction Policy setting. Implementing this policy removes group members who are not part of the configured group membership list or adds group members according to a preconfigured list.

© 2013 John Wiley & Sons, Inc.

Lesson Summary

- Administrators can use security templates to configure local policies, group memberships, event log settings, and other policies.
- Computer configuration group policies are refreshed every 90 minutes by default. Domain controller group policies are refreshed every 2 minutes. These settings can be altered based on the frequency in which policy changes occur.
- When a standard user attempts to perform a task that requires administrative privileges, the system displays a credential prompt, requesting that the user supply the name and password for an account with administrative privileges.
- User Account Control is enabled by default in all Windows Server 2012 installations, but it is possible to configure its properties, or even disable it completely, using Group Policy.

© 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.