## Lesson 17: Configuring Security Policies

MOAC 70-410: Installing and Configuring Windows Server 2012



WILEY

## Overview

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

# 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.

# **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.

# 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.

### Planning and Configuring an Audit Policy

File Action View Help ← ➡ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲	Grou	ip Policy Management Editor	<b>— — X</b>
<ul> <li>✓ Computer Configuration</li> <li>✓ Policies</li> <li>▷ Software Settings</li> <li>✓ Windows Settings</li> <li>▷ Name Resolution Policy</li> <li>ⓒ Scripts (Startup/Shutdown)</li> <li>✓ Security Settings</li> <li>▷ Account Policies</li> <li>✓ Local Policies</li> <li>✓ Local Policy</li> <li>▷ ✓ Rights Assignment</li> <li>▷ ✓ Event Log</li> <li>▷ ✓ Restricted Groups</li> </ul>	< III >	Policy         Audit account logon events         Audit account management         Audit directory service access         Audit logon events         Audit object access         Audit policy change         Audit privilege use         Audit system events	Policy Setting Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined
<	>	< III	>

Audit Policies in the Default Domain Policy

# 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.

# **Event Categories**

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

### **Configure an Audit Policy**

Audit directory service access Properties ? ×
Security Policy Setting Explain
Audit directory service access
Define these policy settings
Audit these attempts:
☐ Failure
OK Cancel Apply

The Properties sheet for a policy setting

### Configure an Active Directory Object for Auditing

r			Ad	vanced Securi	ity Settings for Oliver Cox	(	_ <b>D</b> X
Own Per For	ner: rmissions additional i liting entrie	Domain Admins Auditing nformation, doubl	(ADATUM\D Effective A e-click an au	omain Admins) ccess dit entry. To mod	<u>C</u> hange dify an audit entry, select the er	ntry and click Edit (if availab	le).
	Туре	Principal		Access	Inherited from	Applies to	
88. 88.	Success Success	Everyone Everyone			DC=adatum,DC=local DC=adatum,DC=local	Descendant Organization Descendant Organization	al Unit obje al Unit obje
	A <u>d</u> d	<u>R</u> emove	View			Rest	tore defaults
C	)isable <u>i</u> nhe	ritance					
						OK Cancel	Apply

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

© 2013 John Wiley & Sons, Inc.

### Configure an Active Directory Object for Auditing

R.		Auditing Entry for Oliver Cox		x
Principal: Type: Applies to	Users (ADATUM\Users) Select a principal Success This object and all descendant objects	▼ ▼		
Permissio	ns:			
	Full control	Create all child objects		
	✓ List contents	Create mc-net-isee-90211-GroupPolicy objects		
	Write all properties	Delete ms-net-ieee-80211-GroupPolicy objects		
		Create ms-net-ieee-8023-GroupPolicy objects		
	Delete subtree	Delete ms-net-ieee-8023-GroupPolicy objects		
	✓ Read permissions	Allowed to authenticate		
	Modify permissions	Change password		
	Modify owner	Receive as		
	All validated writes	Reset password		
	All extended rights	Send as		
Properties	5			
	Read all properties	Read msDS-PrimaryComputer		
	✓ Write all properties	✓ Write msDS-PrimaryComputer		~
		ОК	Cano	el

The Auditing Entry dialog box for an object

### Configure an Active Directory Object for Auditing

		Advanced Secu	rity Settings for Users		_ <b>D</b> X
Name:	C:\Users				
Owner:	SYSTEM	ge			
Permissi	ons Auditing I	ffective Access			
For additi Auditing	onal information, double- entries:	click an audit entry. To modi	fy an audit entry, select the entry	and click Edit (if availab	le).
Туре	e Principal	Access	Inherited from	Applies to	
👗 Fail	ocox (ADATUM\ocox	) Modify	None	This folder, subfol	ders and files
Add	Remove	Edit			
Disable	inheritance				
Replac	e all child object auditing e	ntries with inheritable auditi	ing entries from this object		
				OK Cancel	Apply

#### A new auditing entry in the Advanced Security Settings dialog box

© 2013 John Wiley & Sons, Inc.

### Assigning User Rights

File       Action       View       Help <ul> <li>Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Soripts (Startup/Shutdown)</li> <li>Socripts (Startup/Shutdown)</li></ul>	G	rou	ip Policy Management Editor	_		x	
Image: Security Settings       Policy       Policy Setting         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Security Settings         Image: Security Settings       Image: Security Settings       Image: Security Settings       Image: Settings         Image: Setting Setting Security Settings       Image: Setting Settings       Image: Settings       Image: Settings         Image: Setting Setting Setting Setting Setting Setting Setting Settings       Image: Settings       Image: S	File Action View Help						
Image: Computer Configuration	🗢 🄿 🔁 🔜 🔒 🛛 🖬						
Image: Policies       Policies       Not Defined         Image: Policies       Image: Policies       Not Defined	🔺 👰 Computer Configuration	^	Policy	Policy Se	tting		^
Software Settings       Access this computer from the network       Not Defined         Mindows Settings       Act as part of the operating system       Not Defined         Scripts (Startup/Shutdown)       Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Act as part of the operating system       Not Defined         Audit Policy       Back up files and directories       Not Defined         Act as pagefile       Not Defined       Not Defined         System Services       Create a pagefile       Not Defined         System Services       Create a pagefile       Not Defined         Security Windows Firewall with Advanced       Create symbolic links       Not Defined         Security Windows Firewall with Advanced       Deny acce	⊿ 🧮 Policies		B Access Credential Manager as a trusted caller	Not Defi	ned		
Image: Windows Settings       Not Defined         Image: Windows Settings       Image: Act as part of the operating system       Not Defined         Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Act as part of the operating system       Not Defined         Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Act as part of the operating system       Not Defined         Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Not Defined         Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Not Defined       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Not Defined       Image: Scripts (Startup/Shutdown)       Not Defined       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Startup/Shutdown)       Image: Scripts (Start	Software Settings		🔯 Access this computer from the network	Not Defi	ned		
Name Resolution Policy       Add workstations to domain       Not Defined         Scripts (Startup/Shutdown)       Addust memory quotas for a process       Not Defined         Account Policies       Allow log on locally       Not Defined         Audit Policy       Allow log on through Remote Desktop Services       Not Defined         Audit Policy       Security Options       Back up files and directories       Not Defined         Security Options       Change the system time       Not Defined         System Services       Create a pagefile       Not Defined         System Services       Create a loken object       Not Defined         Wired Network (IEEE 802.3) Policies       Create global objects       Not Defined         Wireless Network (IEEE 802.11) Pc       Debug programs       Not Defined         Deny log on as a batch job       Not Defined       Deny log on as a service       Not Defined         Deny log on locally       Not Defined       Deny log on locally       Not Defined	⊿ 🚞 Windows Settings		📖 Act as part of the operating system	Not Defi	ned		
Scripts (Startup/Shutdown)       Adjust memory quotas for a process       Not Defined         Account Policies       Allow log on locally       Not Defined         Account Policies       Allow log on through Remote Desktop Services       Not Defined         Audit Policy       Back up files and directories       Not Defined         Change the system time       Not Defined         Create global objects       Not Defined         Create global objects       Not Defined         Create global objects       Not Defined         Create symbolic links       Not Defined         Create symbolic links       Not Defined         Deny log on as a bach job       Not Defined         Deny log on as a service       Not Defined         Deny log on loc	Name Resolution Policy		📓 Add workstations to domain	Not Defi	ned		
▲       Security Settings       ■         ▲       Account Policies       Allow log on locally       Not Defined         ▲       Local Policies       Not Defined       ■         ▲       User Rights Assignment       ■       ■       Back up files and directories       Not Defined         ●       User Rights Assignment       ■       ■       Not Defined       ■         >       Security Options       ■       Change the system time       Not Defined         >       ■       Restricted Groups       ■       Change the time zone       Not Defined         >       ■       Registry       Create a pagefile       Not Defined         >       ■       Network (IEEE 802.3) Polici       ■       Create global objects       Not Defined         >       ■       Windows Firewall with Advanced       ■       Debug programs       Not Defined         >       ■       Windows Firewall with Advanced       ■       Debug log on as a batch job       Not Defined         >       ■       So	Scripts (Startup/Shutdown)		📓 Adjust memory quotas for a process	Not Defi	ned		
Account Policies       Allow log on through Remote Desktop Services       Not Defined         Audit Policy       Audit Policy       Back up files and directories       Not Defined         Back up files and directories       Not Defined       Not Defined         Back up files and directories       Not Defined         Change the time zone       Not Defined         Create a pagefile       Not Defined         Create a token object       Not Defined         Create global objects       Not Defined         Create symbolic links       Not Defined         Create symbolic links       Not Defined         Debug programs       Not Defined         Deny log on as a batch job       Not Defined         Deny log on as a service       Not Defined         Deny log on locally       Not Defined <td>Security Settings</td> <td>≡</td> <td>📓 Allow log on locally</td> <td>Not Defi</td> <td>ned</td> <td></td> <td>≡</td>	Security Settings	≡	📓 Allow log on locally	Not Defi	ned		≡
Image: A unit Policy       Image: A unit Policy       Image: Back up files and directories       Not Defined         Image: A unit Policy       Image: Back up files and directories       Not Defined         Image: A unit Policy       Image: Back up files and directories       Not Defined         Image: Back up files       Not Defined         Image: Back up files <td>Account Policies</td> <td></td> <td>📓 Allow log on through Remote Desktop Services</td> <td>Not Defi</td> <td>ned</td> <td></td> <td></td>	Account Policies		📓 Allow log on through Remote Desktop Services	Not Defi	ned		
Audit Policy       Bypass traverse checking       Not Defined         Change the time zone       Not Defined         Bypass traverse checking       Not Defined         Bypass traverse checking       Not Defined         Create a pagefile       Not Defined         Create global objects       Not Defined         Create global objects       Not Defined         Create symbolic links       Not Defined         Create symbolic links       Not Defined         Deny access to this computer from the network       Not Defined         Deny log on as a batch job       Not Defined         Deny log on as a service       Not Defined         Deny log on locally       Not Defined         Deny log on through Remote Desktop Services       Not Defined	⊿ j Local Policies		Back up files and directories	Not Defi	ned		
Image: Security Options       Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change the system time       Not Defined         Image: Security Options       Image: Change: Change the system time       Not Defined         Image: Security Options       Image: Change: Change	Audit Policy		Bypass traverse checking	Not Defi	ned		
Image: Security Options       Image: Security Options         Image: Security Options       Not Defined         Image: Security Options       Not Defined     <	Ser Rights Assignment		B Change the system time	Not Defi	ned		
>       Event Log       Not Defined         >       Restricted Groups       System Services       Not Defined         >       Registry       Not Defined       System Services         >       File System       Create a boken objects       Not Defined         Wired Network (IEEE 802.3) Polici       Create global objects       Not Defined         >       Wired Network (IEEE 802.3) Polici       Create symbolic links       Not Defined         >       Wireless Network (IEEE 802.1) Policies       Debug programs       Not Defined         >       Wireless Network (IEEE 802.1) Policies       Deny access to this computer from the network       Not Defined         >       Software Restriction Policies       Deny log on as a batch job       Not Defined         >       Network Access Protection       Deny log on locally       Not Defined         >       Network Access Protection       Deny log on through Remote Desktop Services       Not Defined	Security Options		📓 Change the time zone	Not Defi	ned		
Image: Section of Oddps       Image: Section of Oddps         Image: Section of Oddps       Image: Section of Oddps <td>Event Log</td> <td></td> <td>Create a pagefile</td> <td>Not Defi</td> <td>ned</td> <td></td> <td></td>	Event Log		Create a pagefile	Not Defi	ned		
Image: Sector Services       Image: Sector Services       Not Defined         Image: Sector Services       Image: Sector Services       Not Defined         Image: Sector Services       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined         Image: Sector Sector Defined       Image: Sector Sector Defined       Image: Sector Sector Defined	Kesticted Gloups		Create a token object	Not Defi	ned		
Image: Sector Sector Policies       Image: Sector Policies         Image: Sector Policies       Image: Sector Policies         Image: Sector Policies       Image: Sector Policies         Image: Sector Policies       Image: Policies         Image: Policies	B Registry		Create global objects	Not Defi	ned		
Wired Network (IEEE 802.3) Polici         Wired Network (IEEE 802.3) Polici         Windows Firewall with Advanced         Windows Firewall with Advanced         Wireless Network (IEEE 802.1) Pc         Wireless Network (IEEE 802.1) Pc         Public Key Policies         Software Restriction Policies         Network Access Protection         Network Access Protection	► File System		Create permanent shared objects	Not Defi	ned		
Windows Firewall with Advanced       Debug programs       Not Defined         Windows Firewall with Advanced       Debug programs       Not Defined         Wireless Network List Manager Policies       Deny log on as a batch job       Not Defined         Public Key Policies       Deny log on as a batch job       Not Defined         Software Restriction Policies       Deny log on locally       Not Defined         Network Access Protection       Deny log on through Remote Desktop Services       Not Defined	Wired Network (IEEE 802.3) Polici		Create symbolic links	Not Defi	ned		
Network List Manager Policies         Network Access Protection         Network Access Protection         Network Control Policies         Network Access Protection         Network Access Protection	Windows Firewall with Advanced		B Debug programs	Not Defi	ned		
Image: Section of the section of t	Network List Manager Policies		Deny access to this computer from the network	Not Defi	ned		
Public Key Policies     Software Restriction	Wireless Network (IEEE 802.11) Po		Denv log on as a batch job	Not Defi	ned		
Software Restriction Policies     Software Restriction Policies     Software Restriction Policies     Software Restriction     Software Restr	Public Key Policies		Deny log on as a service	Not Defi	ned		
Network Access Protection     Services     Not Defined     Services     Not Defined     Services     Not Defined     Services     Not Defined	Software Restriction Policies		B Deny log on locally	Not Defi	ned		
Image: State of the state o	Network Access Protection		Denv log on through Remote Desktop Services	Not Defi	ned		_
	Analization Control Deligion	×				>	~
						-	-

User rights assignment settings in a Group Policy object

### **Configuring Security Options**

G	rou	ip Policy Management Editor	_ □	x
File Action View Help				
🔺 👰 Computer Configuration	^	Policy	Policy Setting	^
⊿ 🚞 Policies		🔯 Accounts: Administrator account status	Not Defined	
Software Settings		🗟 Accounts: Block Microsoft accounts	Not Defined	
⊿ <sup>™</sup> Windows Settings		🔯 Accounts: Guest account status	Not Defined	≡
Name Resolution Policy		📓 Accounts: Limit local account use of blank passwords to co	Not Defined	
Scripts (Startup/Shutdown)		🔯 Accounts: Rename administrator account	Not Defined	
⊿ Security Settings	≡	🐻 Accounts: Rename guest account	Not Defined	
Account Policies		🐻 Audit: Audit the access of global system objects	Not Defined	
⊿ i Local Policies		📓 Audit: Audit the use of Backup and Restore privilege	Not Defined	
Audit Policy		🐻 Audit: Force audit policy subcategory settings (Windows Vis	Not Defined	
Security Ontions		🐻 Audit: Shut down system immediately if unable to log secur	Not Defined	
Event Log		DCOM: Machine Access Restrictions in Security Descriptor D	Not Defined	
Event Log Bestricted Groups		B DCOM: Machine Launch Restrictions in Security Descriptor	Not Defined	
N System Services		Devices: Allow undock without having to log on	Not Defined	
N Registry		Devices: Allowed to format and eject removable media	Not Defined	
⊳ 📑 File System		Devices: Prevent users from installing printer drivers	Not Defined	
Wired Network (IEEE 802.3) Polici		Devices: Restrict CD-ROM access to locally logged-on user	Not Defined	
Windows Firewall with Advanced		Devices: Restrict floppy access to locally logged-on user only	Not Defined	
Network List Manager Policies		Domain controller: Allow server operators to schedule tasks	Not Defined	
Wireless Network (IEEE 802.11) Percent Statement Percent Pe		Domain controller: LDAP server signing requirements	Not Defined	
Public Key Policies		Domain controller: Refuse machine account password chan	Not Defined	
Software Restriction Policies		Domain member: Digitally encrypt or sign secure channel d	Not Defined	
Network Access Protection	H	Domain member: Digitally encrypt secure channel data (wh	Not Defined	
Andientics Control Delivies	~	<pre></pre>		>

The Security Options node in a GPO

### **Configuring Security Options**

Network security: LAN Manager authentication lev	?	x
Security Policy Setting Explain		
Network security: LAN Manager authentication level		
☑ Define this policy setting		
Send LM & NTLM responses	×	
Send LM & NTLM responses Send LM & NTLM - use NTLMv2 session security if negotiated Send NTLM response only Send NTLMv2 response only Send NTLMv2 response only. Refuse LM Send NTLMv2 response only. Refuse LM & NTLM		
OK Cancel	App	bly

The Network security: LAN Manager authentication level security option

### **Customizing Event Log Policies**

		Log Properties - System (Type: Administrative)	x
General	Subscriptions		
Full N	lame:	System	
Log p	ath:	%SystemRoot%\System32\Winevt\Logs\System.evtx	]
Log s	ize:	1.07 MB(1,118,208 bytes)	
Creat	ed:	Friday, August 24, 2012 1:50:59 PM	
Modi	fied:	Saturday, September 8, 2012 5:10:21 PM	
Acces	sed:	Friday, August 24, 2012 1:50:59 PM	
🗹 Ena	able logging		
Maxir	num log size ( Kl	B): 20480 😴	
When	ı maximum even	nt log size is reached:	
۲	Overwrite even	ts as needed (oldest events first)	
0	Archive the log	y when full, do not overwrite events	
0	Do not overwri	te events ( Clear logs manually )	
			.
		Clear Log	
		OK Cancel Apply	
			_

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

### **Customizing Event Log Policies**



Policies in the Event Log node of a GPO

# **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.

### **Restricted Groups**

Administrators Properti	es ? X
Configure Membership for Administrators	
Members of this group:	
ocox	Add
<u>This group is a member of:</u> <the belongs<br="" group="" groups="" this="" to="" which="">should not be modified&gt;</the>	A <u>d</u> d R <u>e</u> move

Group membership in the Restricted Groups policy

# 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.

### Using the Security Templates Console

emplates\C:\Users\Administrator\Docu	uments\Securi	ty\Te 🗕 🗖 🗙
Help		_ & ×
Name	Description	Actions
Workstations		C:\Users\Admini 🔺
		More Actions
< 111	>	
	emplates\C:\Users\Administrator\Doct   Help     Name   Workstations     <	Templates\C:\Users\Administrator\Documents\Securi   Help     Name   Workstations     <

The Security Templates snap-in

# 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.

# 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.

### Importing Security Templates into GPOs

Import Policy From		x
Look in: 🌗 Templates 🗸 🗸	G 🤌 📂 🖽 -	
Name • Workstations	Date modified 9/11/2012 9:16 PM	T) Se
<		>
File <u>n</u> ame:	<u>O</u> pen	
Files of type: Security Template (.inf)	✓ Cancel	
Clear this database before importing		н

The Import Policy From dialog box

# 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

# 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

# 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.

## 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.



The Make changes to your user account window

#### Add a user

Choose a password that will be easy for you to remember but hard for others to guess. If you forget, we'll show the hint.

User name	
Password	
Reenter password	
Password hint	

#### The Add a user page



The Manage Accounts window

Real Change Account	t Type
🕞 💿 🔻 🕈 🍇 « Change an Account 🕨 Change Account Type	✓ ♂ Search Control Panel
Choose a new account type for Oliver Cox Oliver Cox Local Account Password protected	
Standard Standard accounts can use most software and change syst security of this PC.	em settings that don't affect other users or the
<ul> <li>Administrator</li> <li>Administrators have complete control over the PC. They can and programs stored on the PC.</li> </ul>	an change any settings and access all of the files
Why is a standard account recommended?	
	Change Account Type Cancel

The Change Account Type window

### Create a New Local User Account with Local Users and Groups

New User ? X					
User name:					
<u>F</u> ull name:					
Description:					
Password:					
Confirm password:					
✓ User must change password at next logon					
User cannot change password					
Pass <u>w</u> ord never expires					
Account is disa <u>b</u> led					
Help Create Close					

The New User dialog box

### 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.

# 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.

### **Performing Administrative Tasks**

۲	User Account Control				
Do you want to allow the following program to make changes to this computer?					
1	Program name: System Remote Settings Verified publisher: <b>Microsoft Windows</b> File origin: Hard drive on this computer				
To continue, type an administrator password, and then click Yes.					
P	Administrator Password				
Show det	ails Yes No				

#### A UAC credential prompt

### Performing Administrative Tasks

0	User Account Control			x	
0	Do you want to allow the following program from an unknown publisher to make changes to this computer?				
	Program name: Publisher: File origin:	snagit.exe <b>Unknown</b> Network drive			
⊗ s	how details		Yes	۷o	
		<u>Cł</u>	ange when these notification	s appear	

#### A UAC elevation prompt

# 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.

### **Configure UAC Settings**



The User Account Control Settings dialog box

# 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.

# 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.

#### 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.



