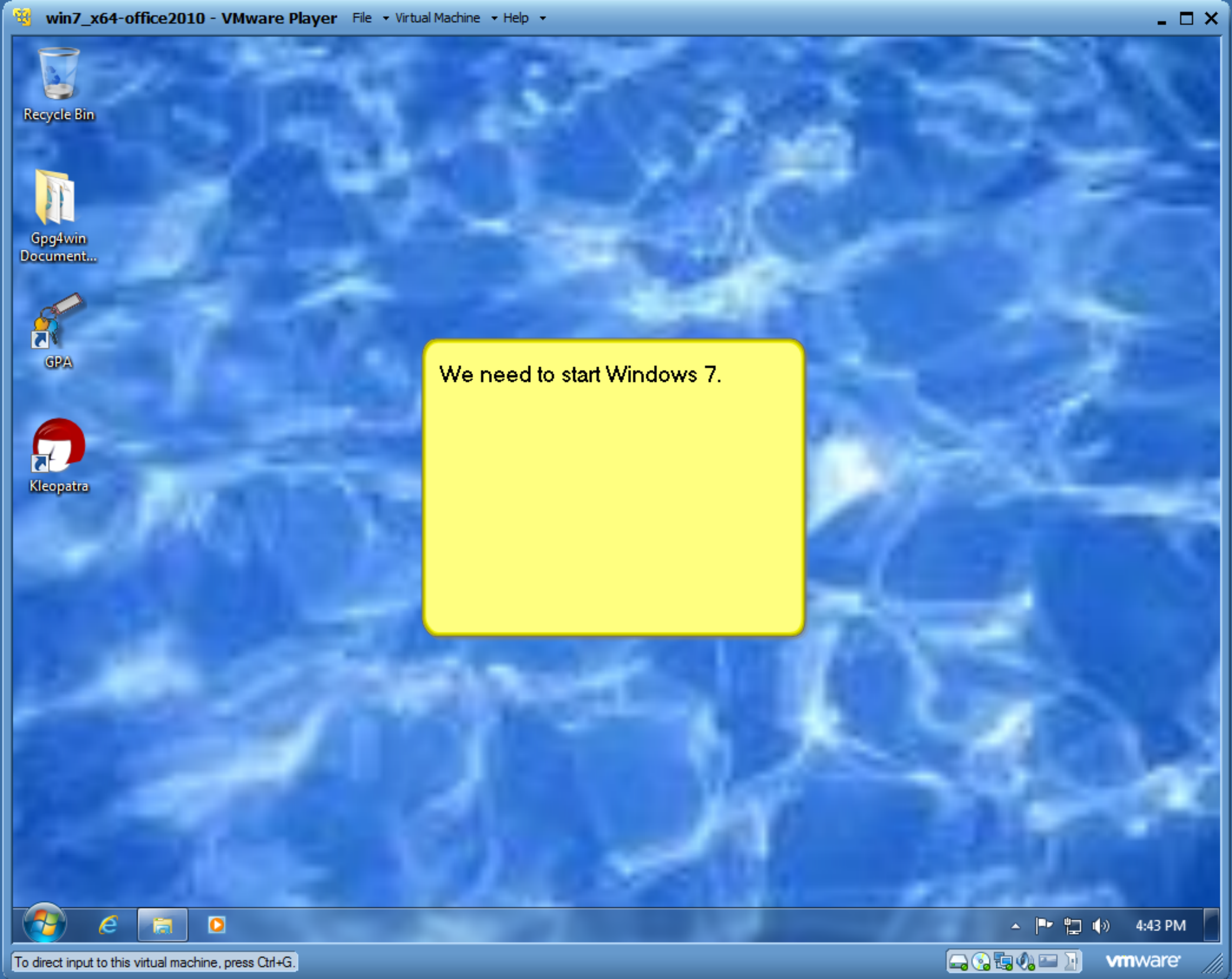
How to use the Microsoft Security Compliance Manger to measure best practice against a baseline.

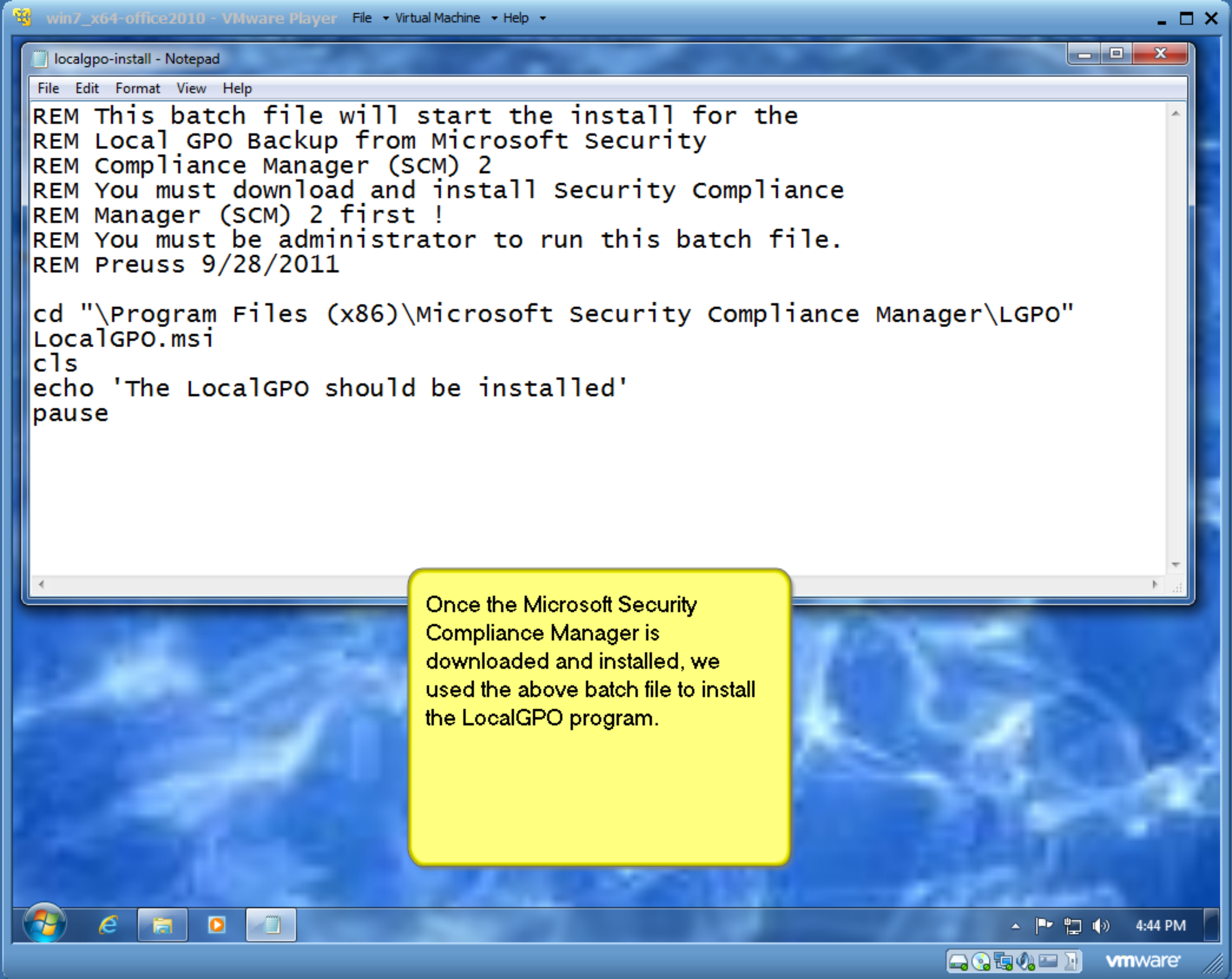
This document uses the Microsoft Security Compliance Manager (SCM) 2 version 2.0.20.0 library 1.0.71901 and Microsoft Windows 7 x64. This demo installs the local GPO backup program for import to the Security Compliance Manager. The Security Compliance Manager is used to compare the local Group Policy Object to the selected baseline (best practice).

Preuss
9/29/2011



We need to start Windows 7.

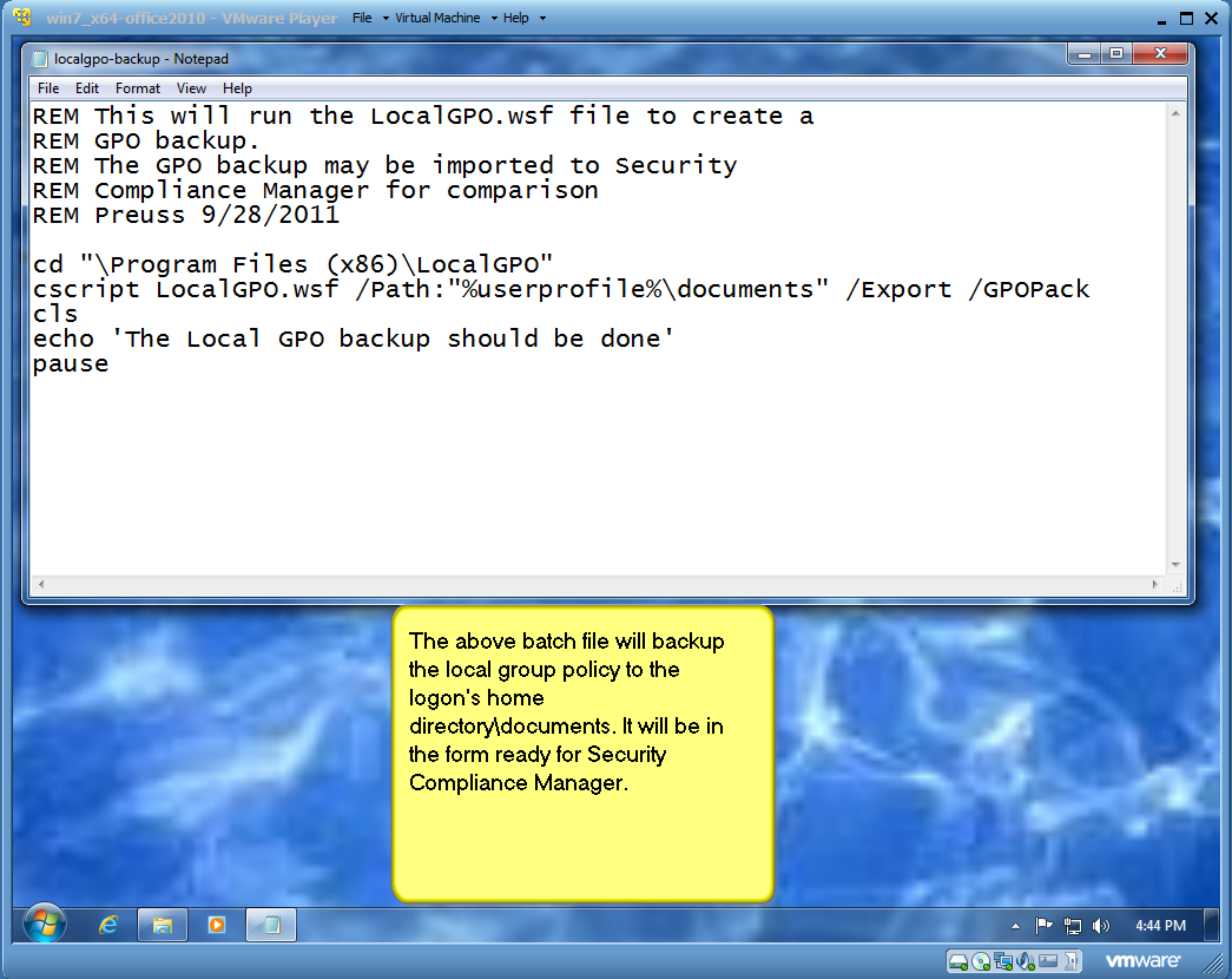
To direct input to this virtual machine, press Ctrl+G.


win7_x64-office2010 - VMware Player
File
Virtual Machine
Help
localgpo-install - Notepad
File
Edit
Format
View
Help
4:44 PM
vmware

```
REM This batch file will start the install for the
REM Local GPO Backup from Microsoft Security
REM Compliance Manager (SCM) 2
REM You must download and install Security Compliance
REM Manager (SCM) 2 first !
REM You must be administrator to run this batch file.
REM Preuss 9/28/2011

cd "\Program Files (x86)\Microsoft Security Compliance Manager\LGPO"
LocalGPO.msi
cls
echo 'The LocalGPO should be installed'
pause
```

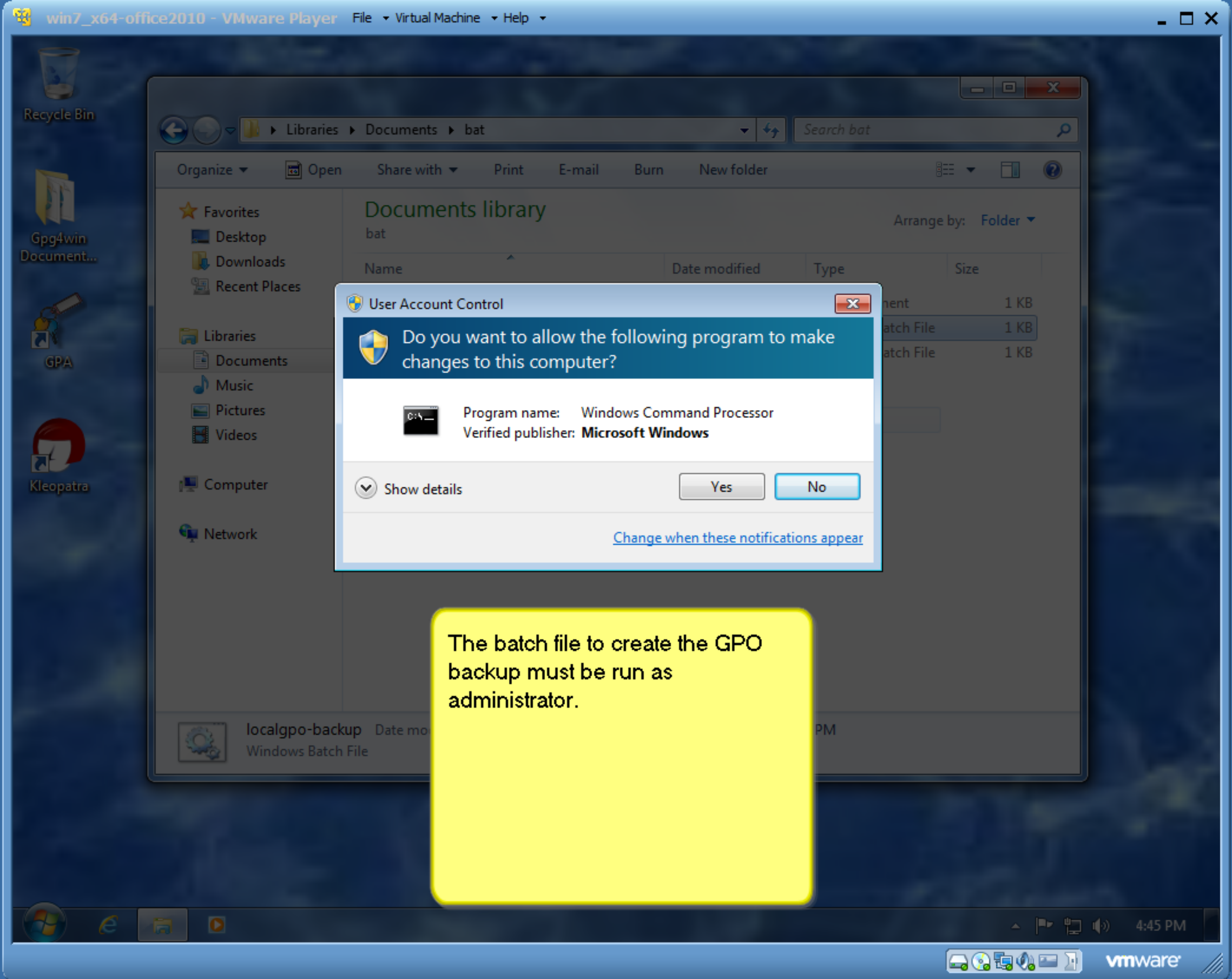
Once the Microsoft Security Compliance Manager is downloaded and installed, we used the above batch file to install the LocalGPO program.


win7_x64-office2010 - VMware Player
File
Virtual Machine
Help
localgpo-backup - Notepad
File
Edit
Format
View
Help
4:44 PM
vmware

```
REM This will run the LocalGPO.wsf file to create a
REM GPO backup.
REM The GPO backup may be imported to Security
REM Compliance Manager for comparison
REM Preuss 9/28/2011

cd "\Program Files (x86)\LocalGPO"
cscript LocalGPO.wsf /Path:"%userprofile%\documents" /Export /GPOPack
cls
echo 'The Local GPO backup should be done'
pause
```

The above batch file will backup the local group policy to the logon's home directory\documents. It will be in the form ready for Security Compliance Manager.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**

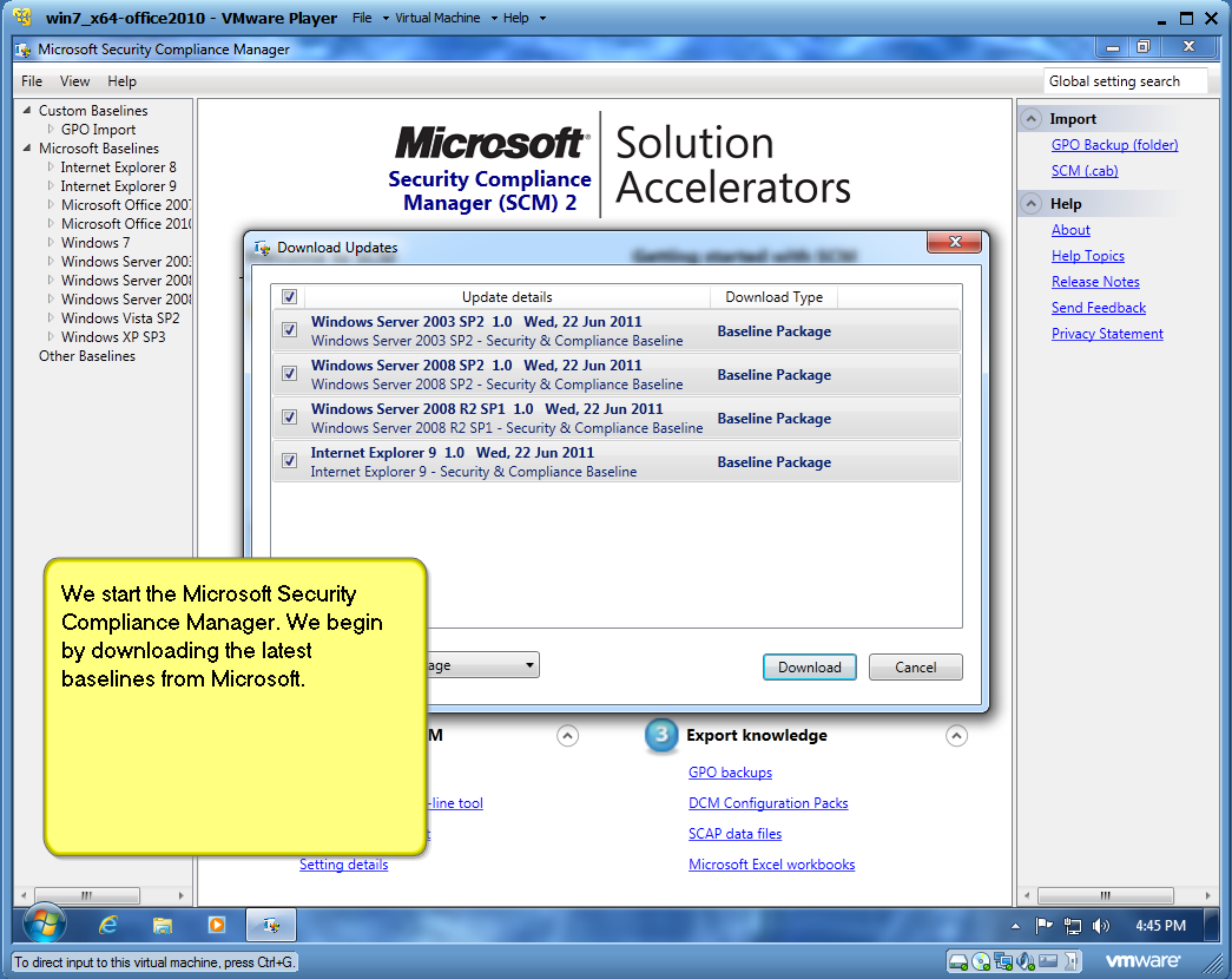
Show details

Yes

No

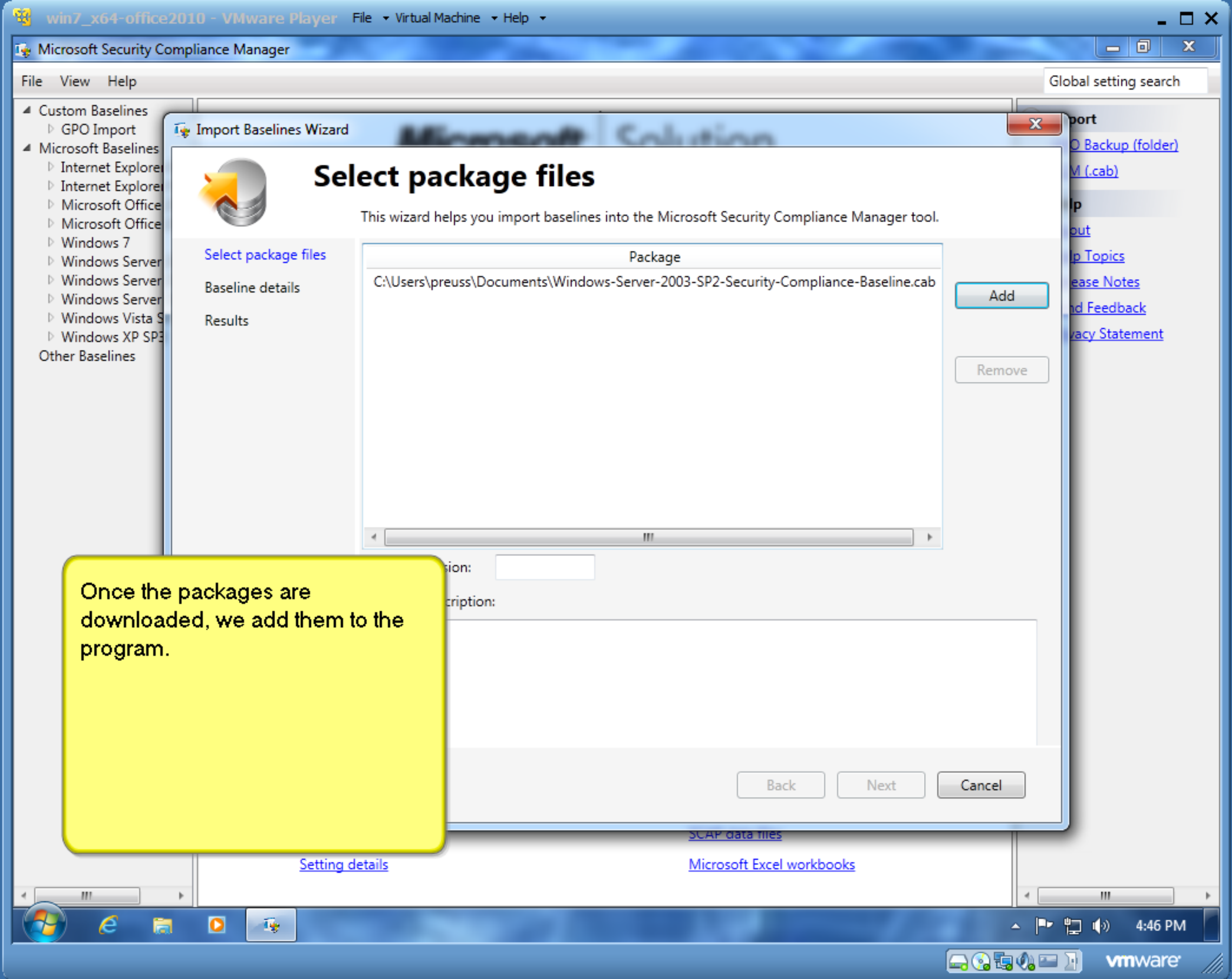
Change when these notifications appear

The batch file to create the GPO backup must be run as administrator.



☑	Update details	Download Type
☑	**Windows Server 2003 SP2 1.0 Wed, 22 Jun 2011** Windows Server 2003 SP2 - Security & Compliance Baseline	**Baseline Package**
☑	**Windows Server 2008 SP2 1.0 Wed, 22 Jun 2011** Windows Server 2008 SP2 - Security & Compliance Baseline	**Baseline Package**
☑	**Windows Server 2008 R2 SP1 1.0 Wed, 22 Jun 2011** Windows Server 2008 R2 SP1 - Security & Compliance Baseline	**Baseline Package**
☑	**Internet Explorer 9 1.0 Wed, 22 Jun 2011** Internet Explorer 9 - Security & Compliance Baseline	**Baseline Package**

We start the Microsoft Security Compliance Manager. We begin by downloading the latest baselines from Microsoft.

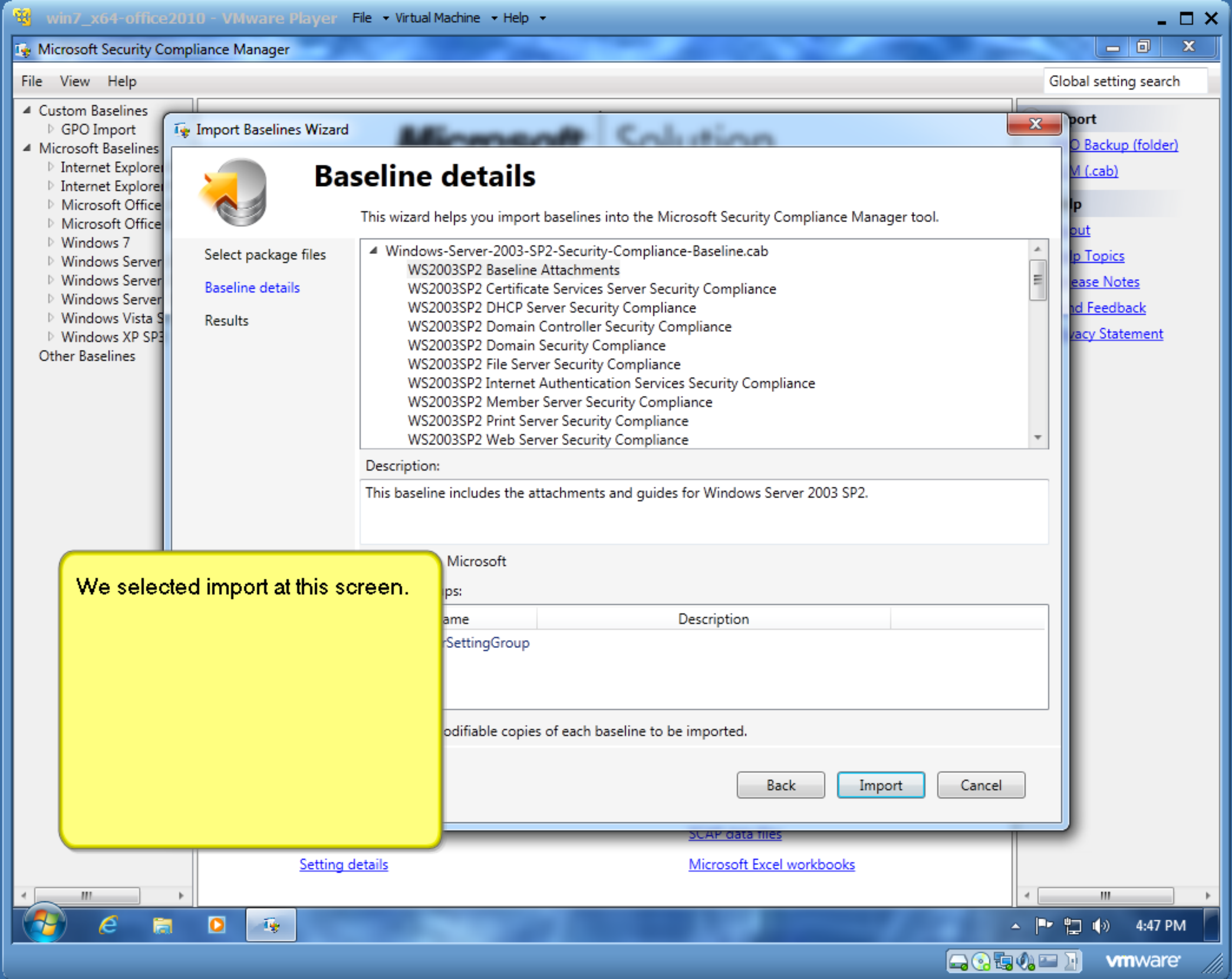


Select package files

This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.

C:\Users\preuss\Documents\Windows-Server-2003-SP2-Security-Compliance-Baseline.cab

Once the packages are downloaded, we add them to the program.



Baseline details

This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.

- Windows-Server-2003-SP2-Security-Compliance-Baseline.cab
  - WS2003SP2 Baseline Attachments
  - WS2003SP2 Certificate Services Server Security Compliance
  - WS2003SP2 DHCP Server Security Compliance
  - WS2003SP2 Domain Controller Security Compliance
  - WS2003SP2 Domain Security Compliance
  - WS2003SP2 File Server Security Compliance
  - WS2003SP2 Internet Authentication Services Security Compliance
  - WS2003SP2 Member Server Security Compliance
  - WS2003SP2 Print Server Security Compliance
  - WS2003SP2 Web Server Security Compliance

Description:

This baseline includes the attachments and guides for Windows Server 2003 SP2.

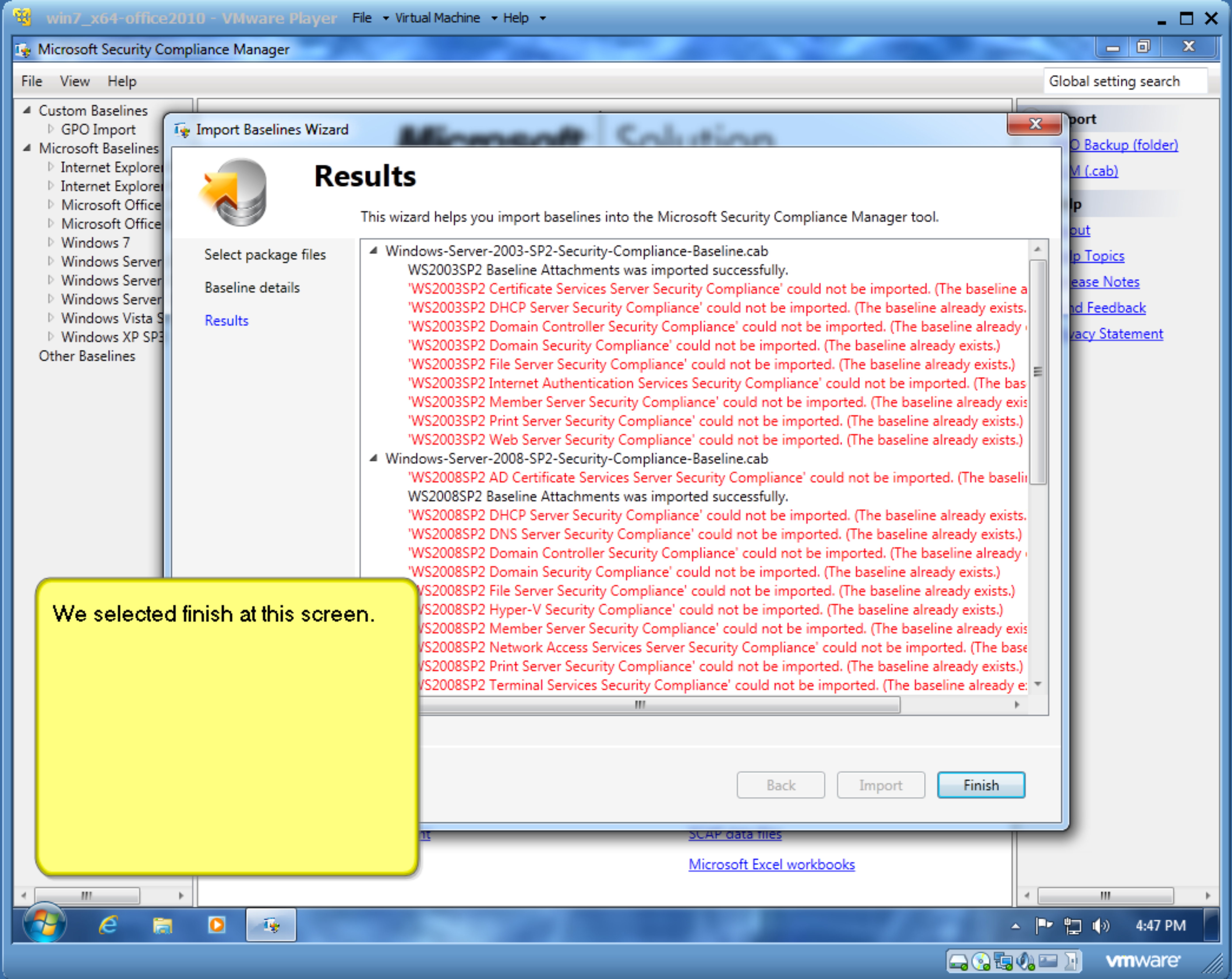
Microsoft

ps:

ame	Description
SettingGroup	

odifiable copies of each baseline to be imported.

We selected import at this screen.

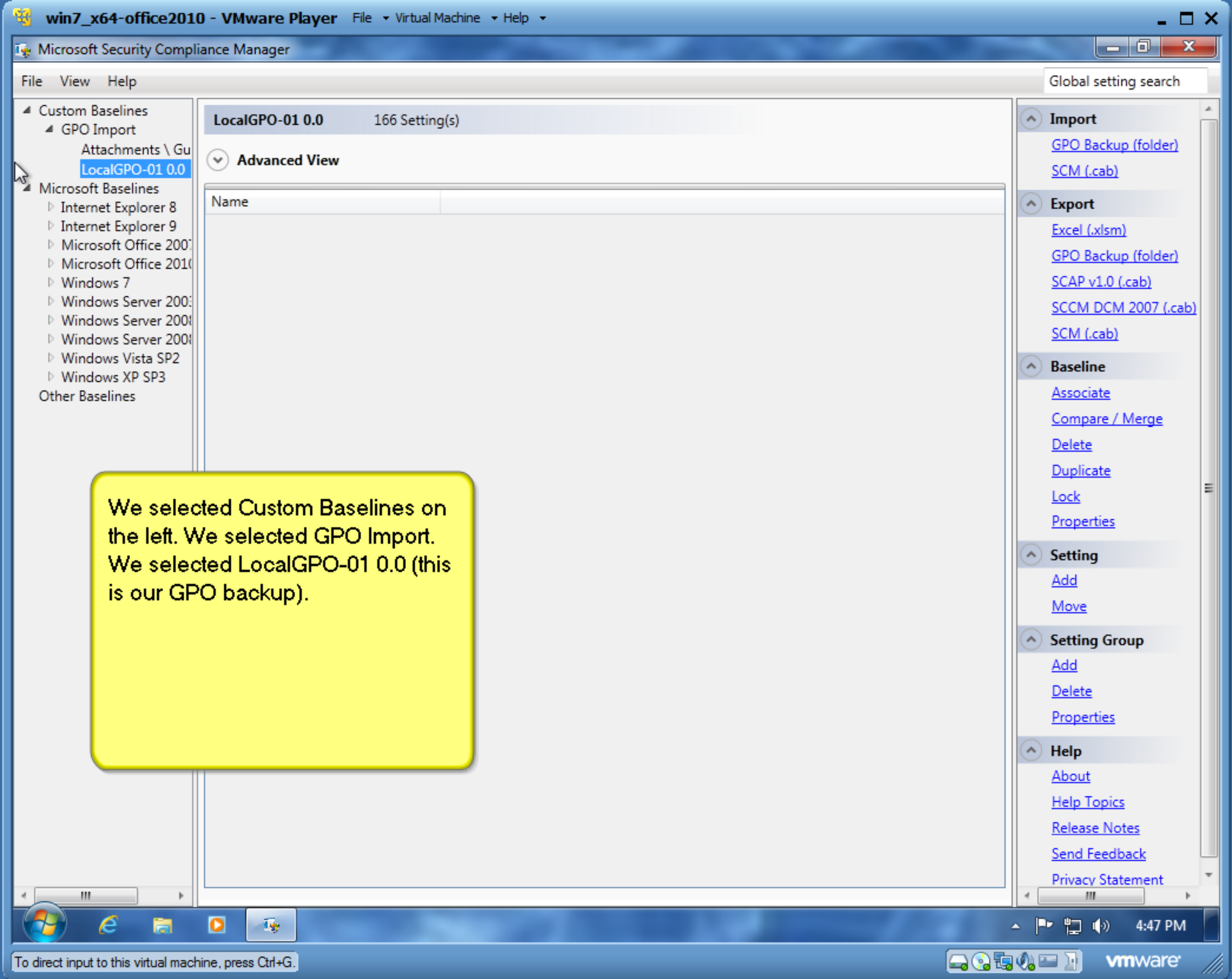


Results

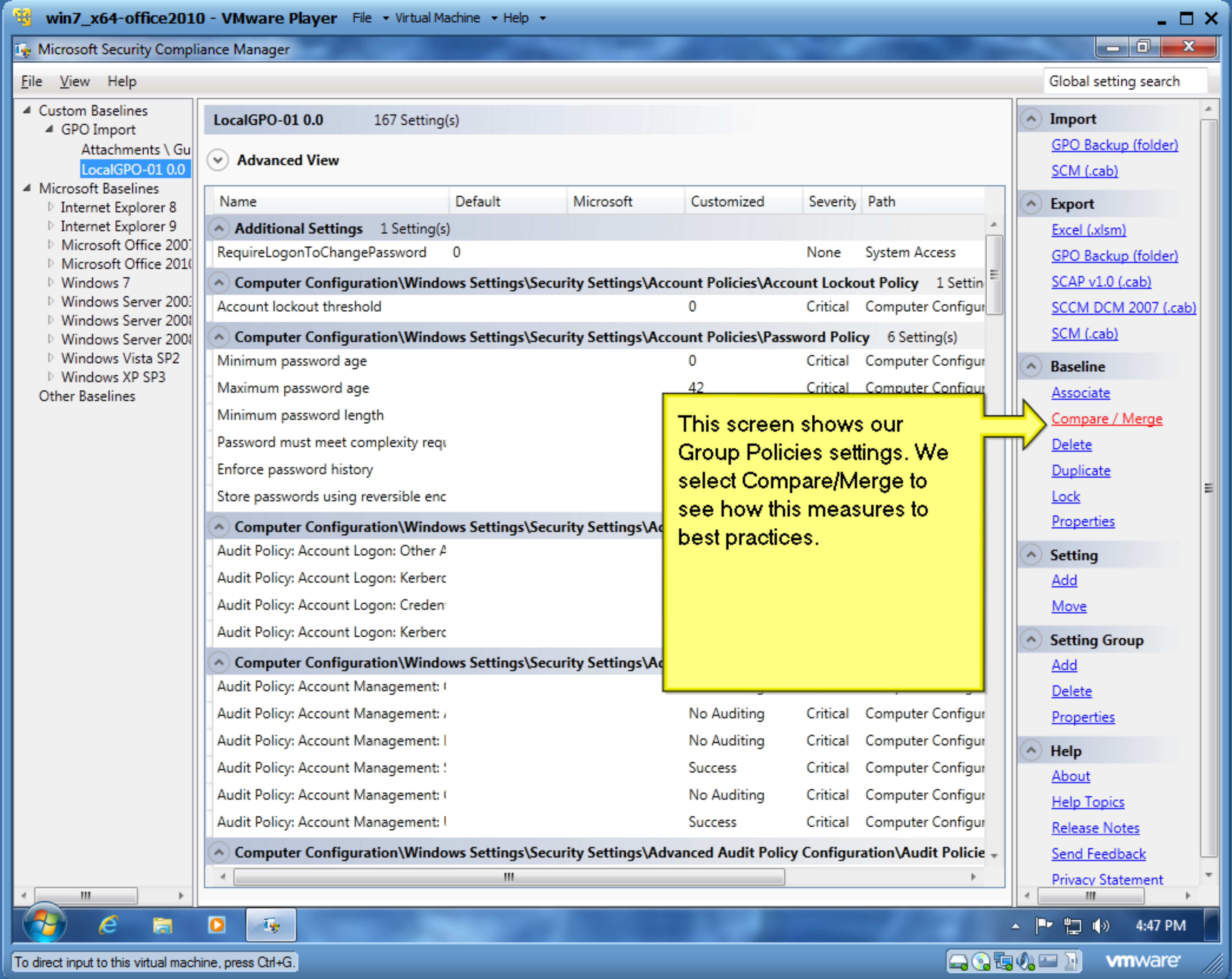
This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.

```
◢ Windows-Server-2003-SP2-Security-Compliance-Baseline.cab
    WS2003SP2 Baseline Attachments was imported successfully.
    'WS2003SP2 Certificate Services Server Security Compliance' could not be imported. (The baseline a
    'WS2003SP2 DHCP Server Security Compliance' could not be imported. (The baseline already exists.
    'WS2003SP2 Domain Controller Security Compliance' could not be imported. (The baseline already
    'WS2003SP2 Domain Security Compliance' could not be imported. (The baseline already exists.)
    'WS2003SP2 File Server Security Compliance' could not be imported. (The baseline already exists.)
    'WS2003SP2 Internet Authentication Services Security Compliance' could not be imported. (The bas
    'WS2003SP2 Member Server Security Compliance' could not be imported. (The baseline already exis
    'WS2003SP2 Print Server Security Compliance' could not be imported. (The baseline already exists.)
    'WS2003SP2 Web Server Security Compliance' could not be imported. (The baseline already exists.)
◢ Windows-Server-2008-SP2-Security-Compliance-Baseline.cab
    'WS2008SP2 AD Certificate Services Server Security Compliance' could not be imported. (The baseli
    WS2008SP2 Baseline Attachments was imported successfully.
    'WS2008SP2 DHCP Server Security Compliance' could not be imported. (The baseline already exists.
    'WS2008SP2 DNS Server Security Compliance' could not be imported. (The baseline already exists.)
    'WS2008SP2 Domain Controller Security Compliance' could not be imported. (The baseline already
    'WS2008SP2 Domain Security Compliance' could not be imported. (The baseline already exists.)
    'S2008SP2 File Server Security Compliance' could not be imported. (The baseline already exists.)
    'S2008SP2 Hyper-V Security Compliance' could not be imported. (The baseline already exists.)
    'S2008SP2 Member Server Security Compliance' could not be imported. (The baseline already exis
    'S2008SP2 Network Access Services Server Security Compliance' could not be imported. (The base
    'S2008SP2 Print Server Security Compliance' could not be imported. (The baseline already exists.)
    'S2008SP2 Terminal Services Security Compliance' could not be imported. (The baseline already e:
```

We selected finish at this screen.



We selected Custom Baselines on the left. We selected GPO Import. We selected LocalGPO-01 0.0 (this is our GPO backup).

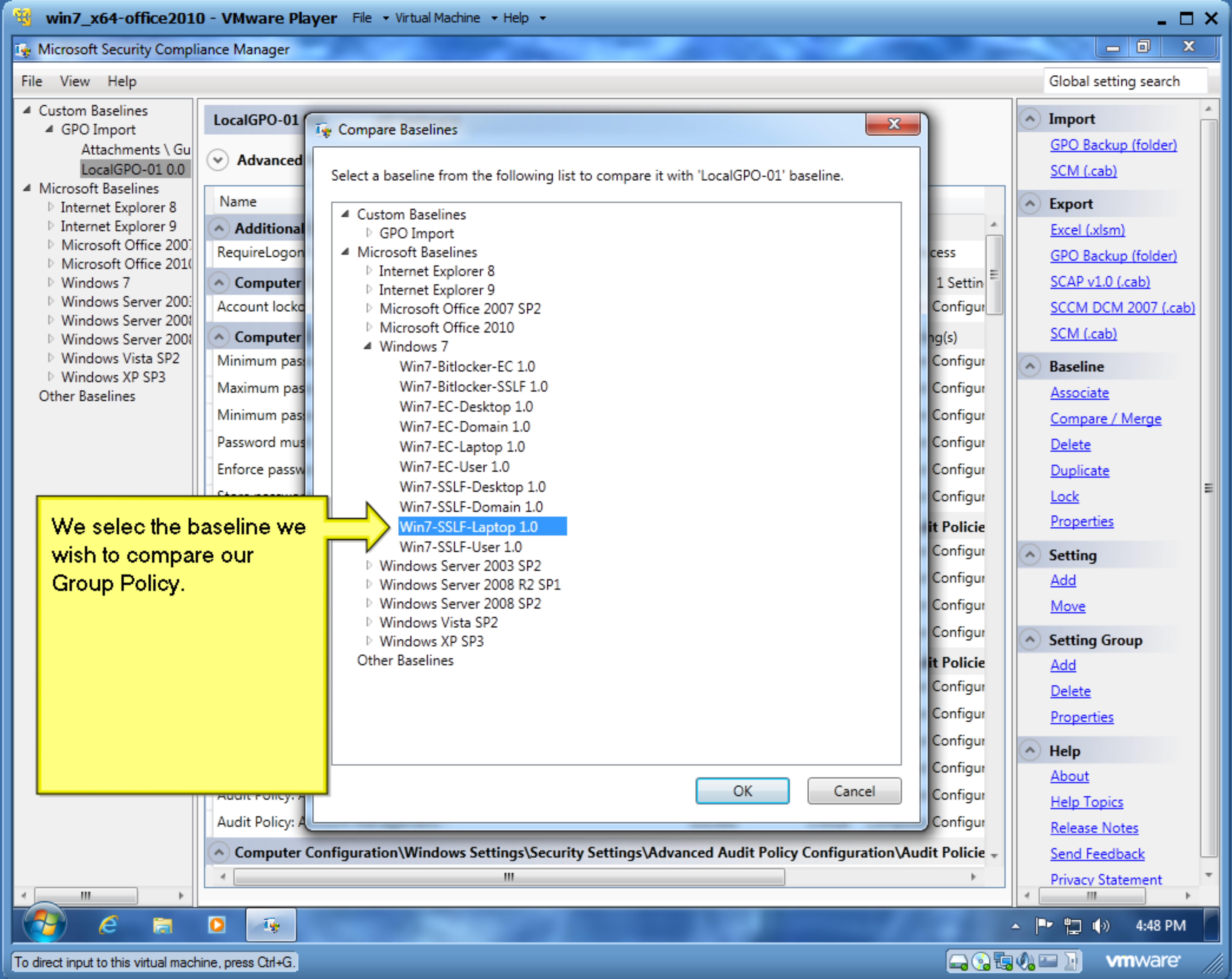


LocalGPO-01 0.0 167 Setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severity	Path
Additional Settings 1 Setting(s)					
RequireLogonToChangePassword	0			None	System Access
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy 1 Settin					
Account lockout threshold			0	Critical	Computer Configur
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy 6 Setting(s)					
Minimum password age			0	Critical	Computer Configur
Maximum password age			42	Critical	Computer Configur
Minimum password length					
Password must meet complexity requ					
Enforce password history					
Store passwords using reversible enc					
Computer Configuration\Windows Settings\Security Settings\Ad					
Audit Policy: Account Logon: Other A					
Audit Policy: Account Logon: Kerberc					
Audit Policy: Account Logon: Creden					
Audit Policy: Account Logon: Kerberc					
Computer Configuration\Windows Settings\Security Settings\Ad					
Audit Policy: Account Management:					
Audit Policy: Account Management:			No Auditing	Critical	Computer Configur
Audit Policy: Account Management:			No Auditing	Critical	Computer Configur
Audit Policy: Account Management:			Success	Critical	Computer Configur
Audit Policy: Account Management:			No Auditing	Critical	Computer Configur
Audit Policy: Account Management:			Success	Critical	Computer Configur
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policie					

This screen shows our Group Policies settings. We select Compare/Merge to see how this measures to best practices.



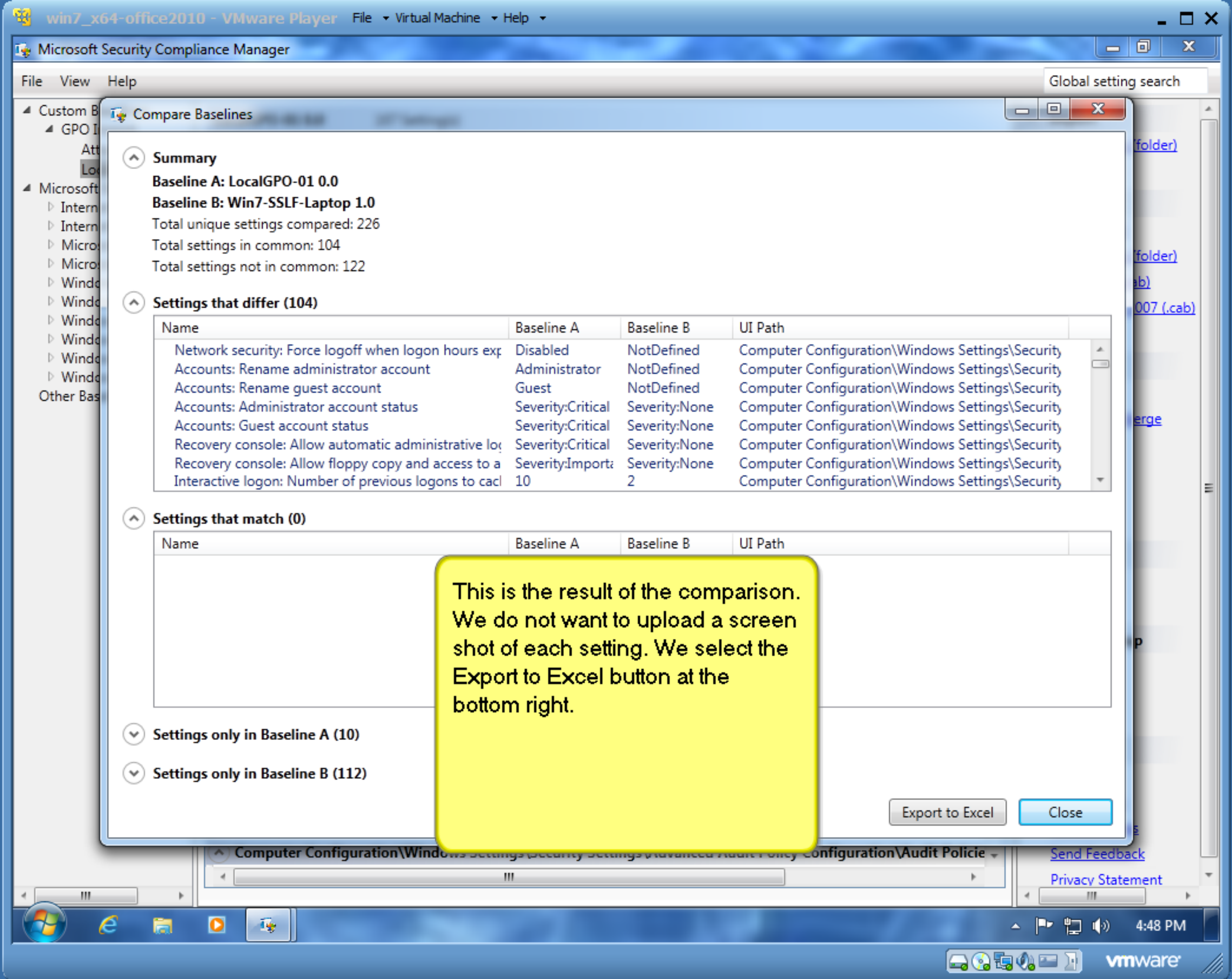
Compare Baselines

Select a baseline from the following list to compare it with 'LocalGPO-01' baseline.

- Custom Baselines
  - GPO Import
- Microsoft Baselines
  - Internet Explorer 8
  - Internet Explorer 9
  - Microsoft Office 2007 SP2
  - Microsoft Office 2010
  - Windows 7
    - Win7-Bitlocker-EC 1.0
    - Win7-Bitlocker-SSLF 1.0
    - Win7-EC-Desktop 1.0
    - Win7-EC-Domain 1.0
    - Win7-EC-Laptop 1.0
    - Win7-EC-User 1.0
    - Win7-SSLF-Desktop 1.0
    - Win7-SSLF-Domain 1.0
    - Win7-SSLF-Laptop 1.0
    - Win7-SSLF-User 1.0
  - Windows Server 2003 SP2
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2
  - Windows Vista SP2
  - Windows XP SP3
- Other Baselines

OK Cancel

We selec the baseline we wish to compare our Group Policy.



Summary

Baseline A: LocalGPO-01 0.0

Baseline B: Win7-SSLF-Laptop 1.0

Total unique settings compared: 226

Total settings in common: 104

Total settings not in common: 122

Settings that differ (104)

Name	Baseline A	Baseline B	UI Path
Network security: Force logoff when logon hours exp	Disabled	NotDefined	Computer Configuration\Windows Settings\Security
Accounts: Rename administrator account	Administrator	NotDefined	Computer Configuration\Windows Settings\Security
Accounts: Rename guest account	Guest	NotDefined	Computer Configuration\Windows Settings\Security
Accounts: Administrator account status	Severity:Critical	Severity:None	Computer Configuration\Windows Settings\Security
Accounts: Guest account status	Severity:Critical	Severity:None	Computer Configuration\Windows Settings\Security
Recovery console: Allow automatic administrative lo	Severity:Critical	Severity:None	Computer Configuration\Windows Settings\Security
Recovery console: Allow floppy copy and access to a	Severity:Importa	Severity:None	Computer Configuration\Windows Settings\Security
Interactive logon: Number of previous logons to cacl	10	2	Computer Configuration\Windows Settings\Security

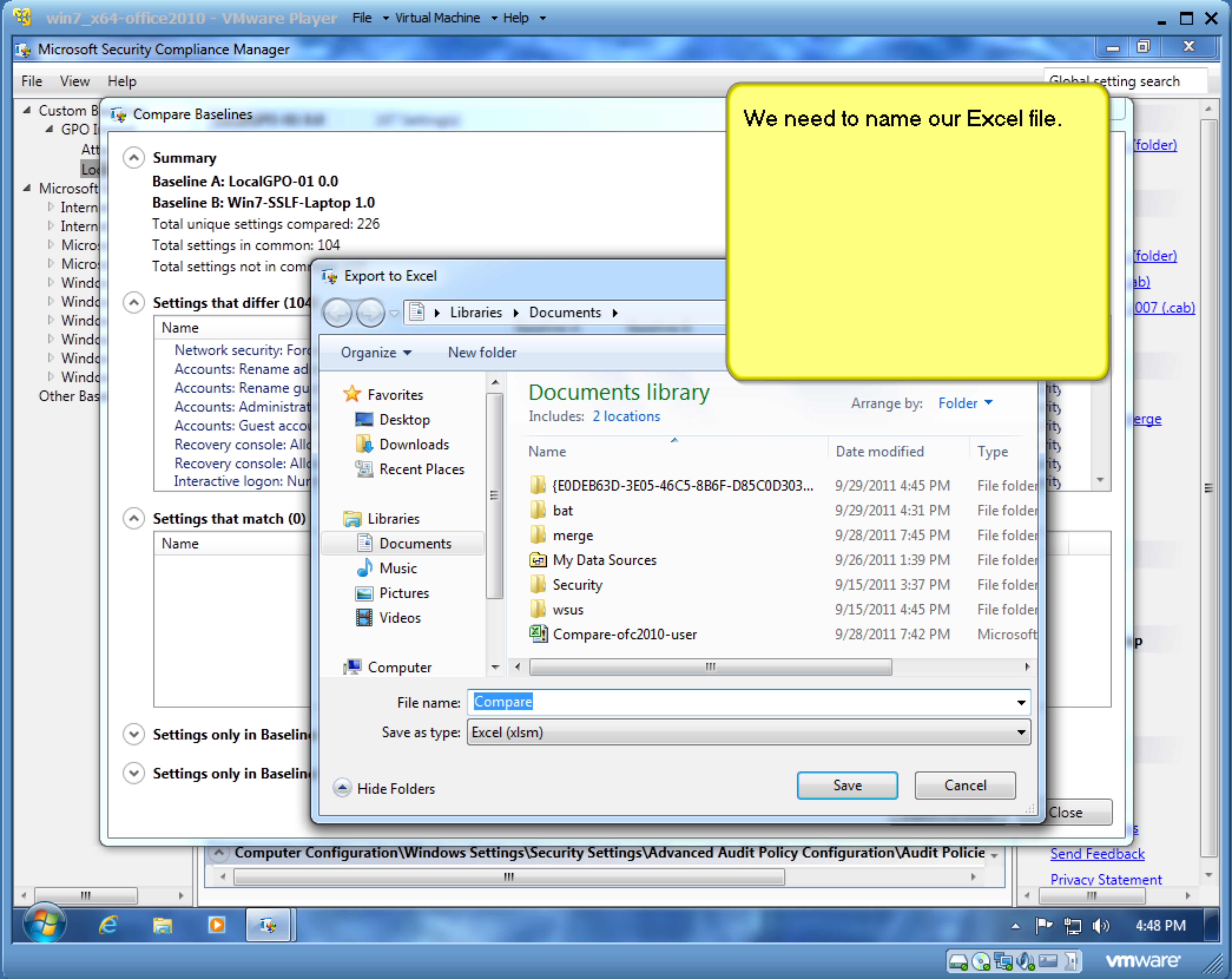
Settings that match (0)

Name	Baseline A	Baseline B	UI Path

Settings only in Baseline A (10)

Settings only in Baseline B (112)

This is the result of the comparison. We do not want to upload a screen shot of each setting. We select the Export to Excel button at the bottom right.



We need to name our Excel file.

win7_x64-office2010 - VMware Player

Microsoft Security Compliance Manager

Compare Baselines

Summary

Baseline A: LocalGPO-01 0.0

Baseline B: Win7-SSLF-Laptop 1.0

Total unique settings compared: 226

Total settings in common: 104

Total settings not in com

Settings that differ (104

Network security: For
Accounts: Rename ad
Accounts: Rename gu
Accounts: Administrat
Accounts: Guest acco
Recovery console: All
Recovery console: All
Interactive logon: Nu

Settings that match (0)

Settings only in Baselin

Settings only in Baselin

Export to Excel

Libraries ▸ Documents ▸

Documents library

Includes: 2 locations

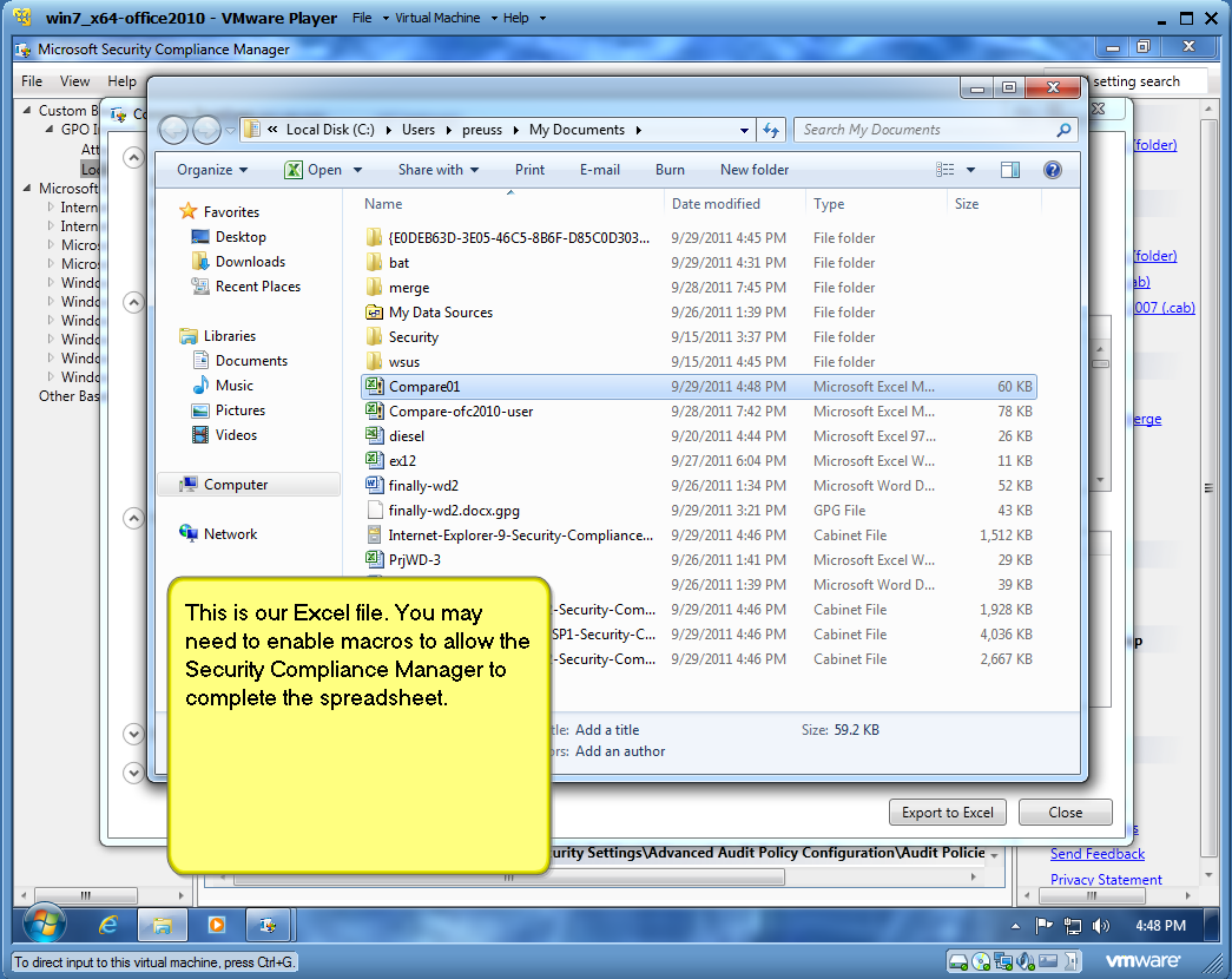
Arrange by: Folder

Name	Date modified	Type
{E0DEB63D-3E05-46C5-8B6F-D85C0D303...	9/29/2011 4:45 PM	File folder
bat	9/29/2011 4:31 PM	File folder
merge	9/28/2011 7:45 PM	File folder
My Data Sources	9/26/2011 1:39 PM	File folder
Security	9/15/2011 3:37 PM	File folder
wsus	9/15/2011 4:45 PM	File folder
Compare-ofc2010-user	9/28/2011 7:42 PM	Microsoft

File name: Compare

Save as type: Excel (xlsm)

Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policie

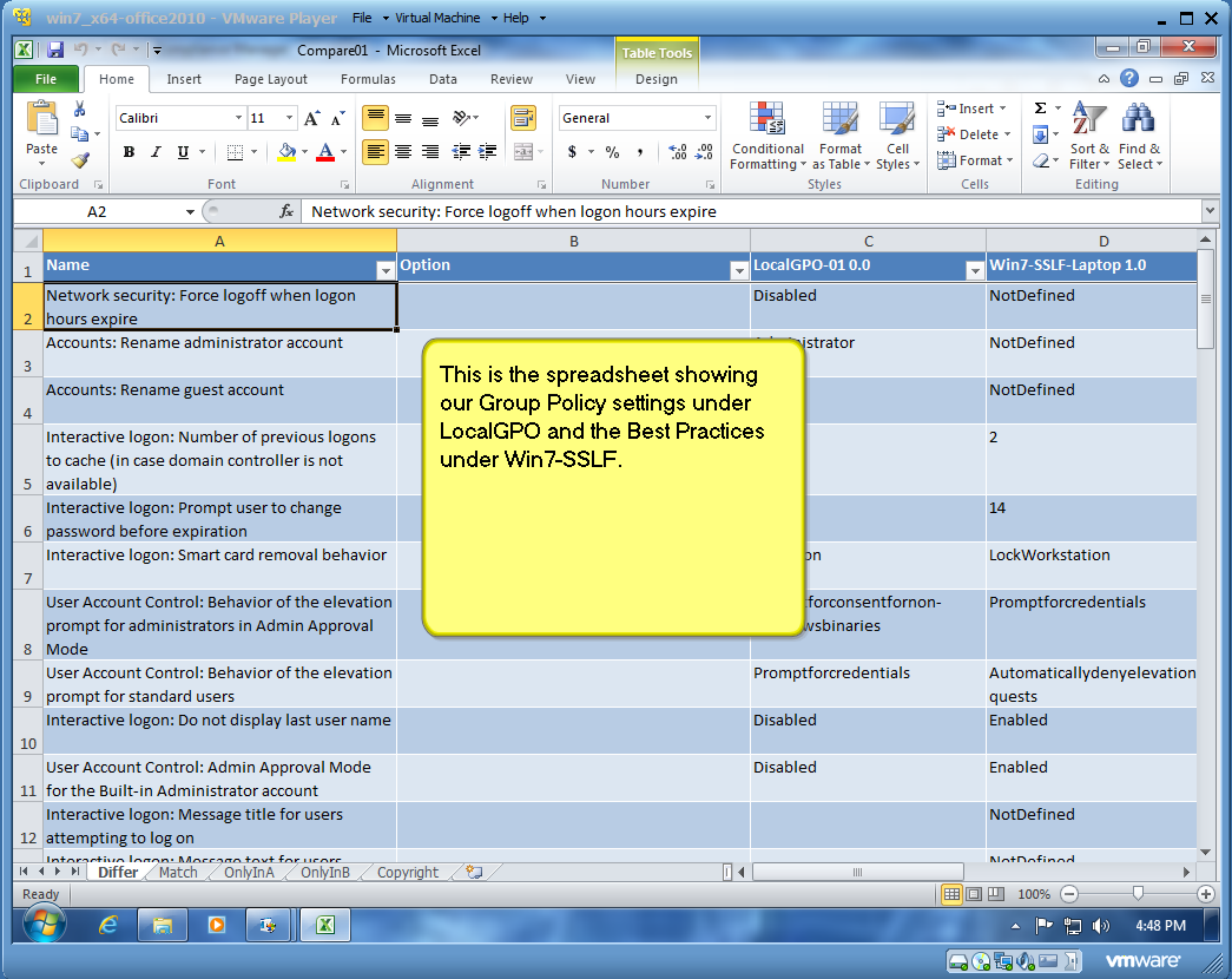


Name	Date modified	Type	Size
{E0DEB63D-3E05-46C5-8B6F-D85C0D303...	9/29/2011 4:45 PM	File folder	
bat	9/29/2011 4:31 PM	File folder	
merge	9/28/2011 7:45 PM	File folder	
My Data Sources	9/26/2011 1:39 PM	File folder	
Security	9/15/2011 3:37 PM	File folder	
wsus	9/15/2011 4:45 PM	File folder	
Compare01	9/29/2011 4:48 PM	Microsoft Excel M...	60 KB
Compare-ofc2010-user	9/28/2011 7:42 PM	Microsoft Excel M...	78 KB
diesel	9/20/2011 4:44 PM	Microsoft Excel 97...	26 KB
ex12	9/27/2011 6:04 PM	Microsoft Excel W...	11 KB
finally-wd2	9/26/2011 1:34 PM	Microsoft Word D...	52 KB
finally-wd2.docx.gpg	9/29/2011 3:21 PM	GPG File	43 KB
Internet-Explorer-9-Security-Compliance...	9/29/2011 4:46 PM	Cabinet File	1,512 KB
PrjWD-3	9/26/2011 1:41 PM	Microsoft Excel W...	29 KB
	9/26/2011 1:39 PM	Microsoft Word D...	39 KB
-Security-Com...	9/29/2011 4:46 PM	Cabinet File	1,928 KB
SP1-Security-C...	9/29/2011 4:46 PM	Cabinet File	4,036 KB
-Security-Com...	9/29/2011 4:46 PM	Cabinet File	2,667 KB

tle: Add a title
rs: Add an author
Size: 59.2 KB

urity Settings\Advanced Audit Policy Configuration\Audit Policie

This is our Excel file. You may need to enable macros to allow the Security Compliance Manager to complete the spreadsheet.



This is the spreadsheet showing our Group Policy settings under LocalGPO and the Best Practices under Win7-SSLF.

Network security: Force logoff when logon hours expire

	Name	Option	LocalGPO-01 0.0	Win7-SSLF-Laptop 1.0
2	Network security: Force logoff when logon hours expire		Disabled	NotDefined
3	Accounts: Rename administrator account		istrator	NotDefined
4	Accounts: Rename guest account			NotDefined
5	Interactive logon: Number of previous logons to cache (in case domain controller is not available)			2
6	Interactive logon: Prompt user to change password before expiration			14
7	Interactive logon: Smart card removal behavior		on	LockWorkstation
8	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode		forconsentfornon-wsbinaries	Promptforcredentials
9	User Account Control: Behavior of the elevation prompt for standard users		Promptforcredentials	Automaticallydenyelevationquests
10	Interactive logon: Do not display last user name		Disabled	Enabled
11	User Account Control: Admin Approval Mode for the Built-in Administrator account		Disabled	Enabled
12	Interactive logon: Message title for users attempting to log on			NotDefined
	Interactive logon: Message text for users			NotDefined