McAfee® ePolicy Orchestrator® 5.1.1 Change Control

Release 1.1

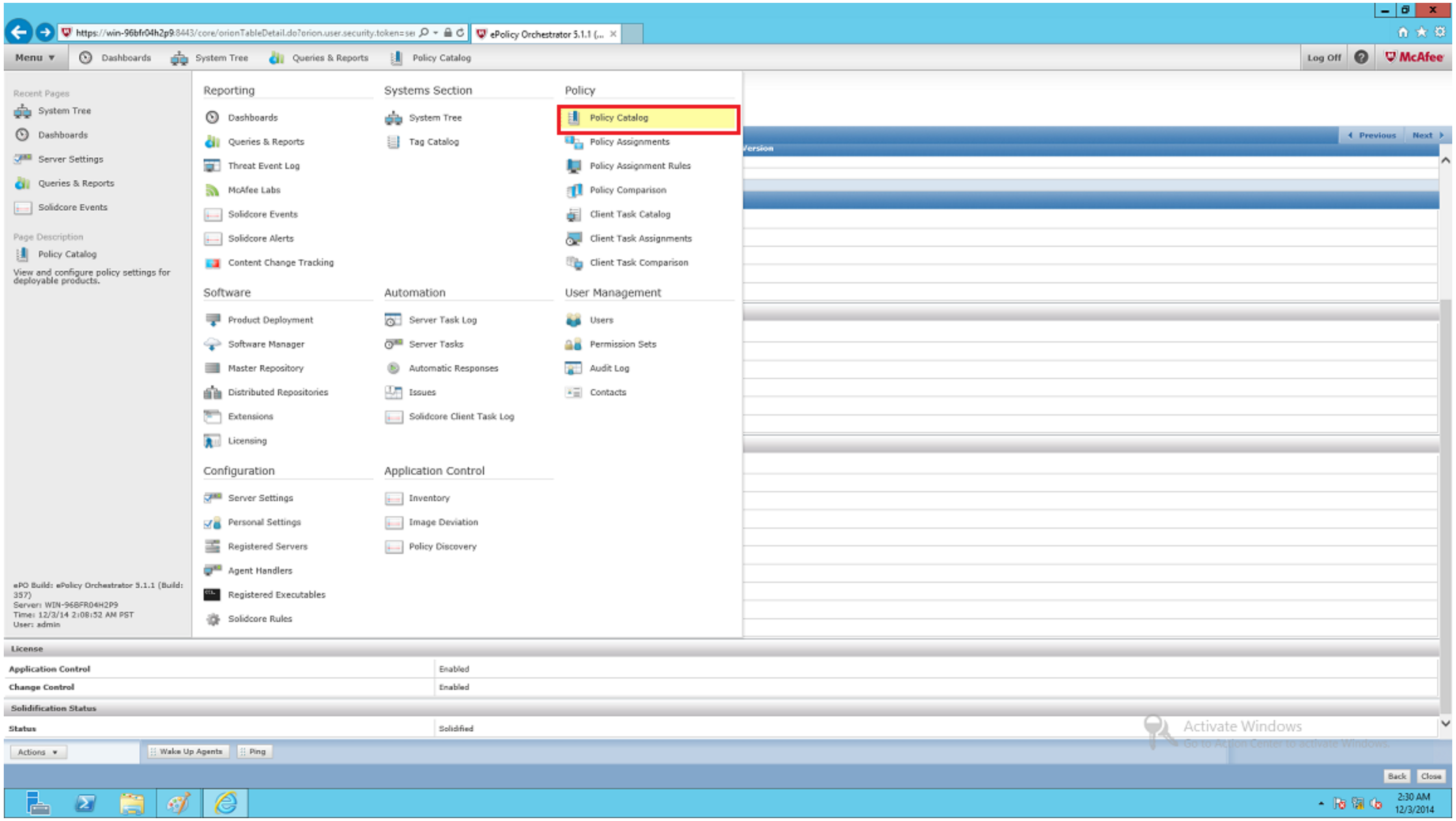
2016/5/31

Released Date

- 2016/05/31

Enable Change Control

- To click "Policy Catalog" from "Menu→Policy"



ePO Build: ePolicy Orchestrator 5.1.1 (Build: 357)
Server: WIN-96BFR04H2P9
Time: 12/3/14 2:08:52 AM PST
User: admin

License

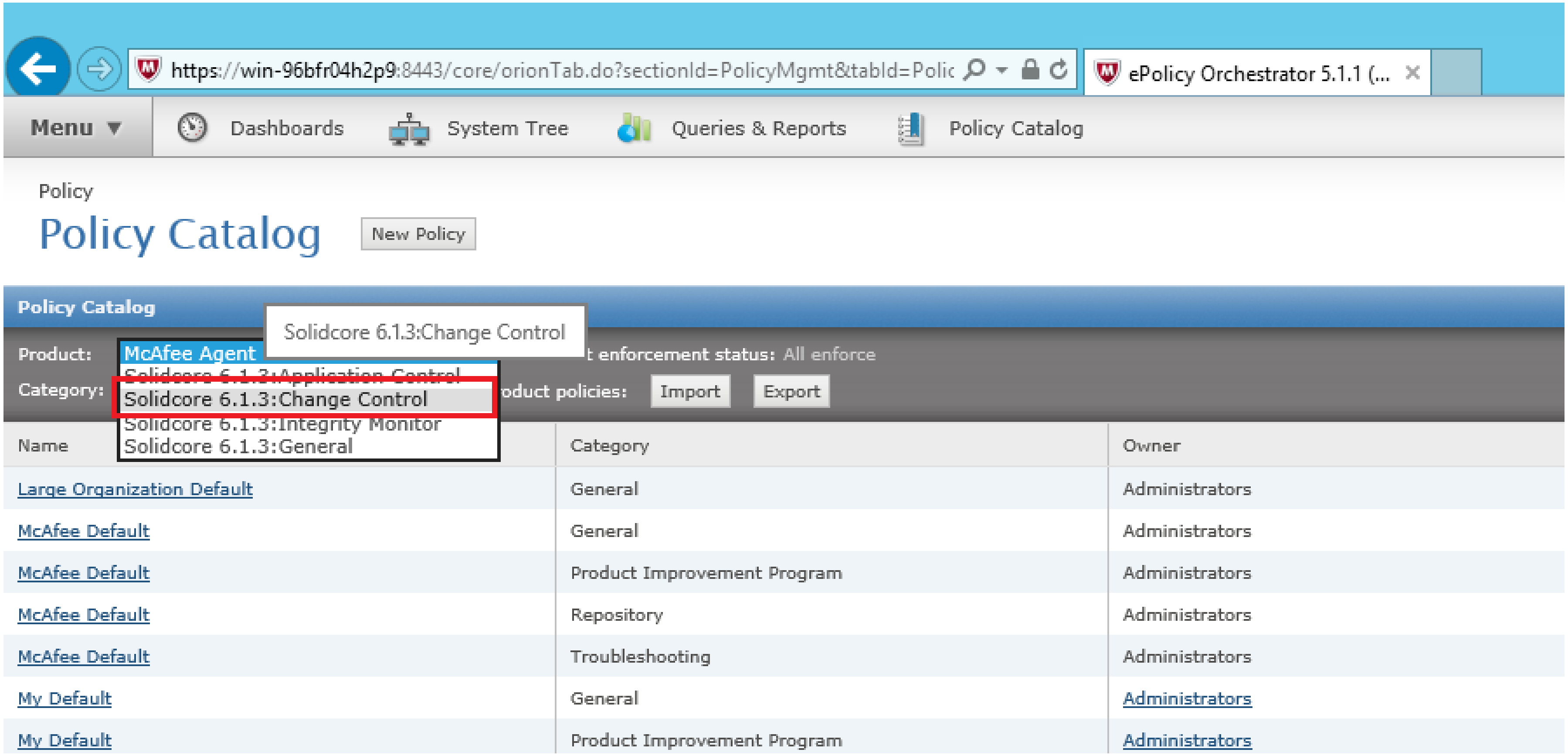
Application Control	Enabled
Change Control	Enabled

Solidification Status

Status	Solidified

Enable Change Control

- To select "Solidcore 6.1.3:Change Control" from Product drop-list


https://win-96bfr04h2p9:8443/core/orionTab.do?sectionId=PolicyMgmt&tabId=Polic
ePolicy Orchestrator 5.1.1 (...
Menu ▼
Dashboards
System Tree
Queries & Reports
Policy Catalog
New Policy
Import
Export

Policy

Policy Catalog

Policy Catalog

Product: McAfee Agent

Solidcore 6.1.3:Application Control
Solidcore 6.1.3:Change Control
Solidcore 6.1.3:Integrity Monitor
Solidcore 6.1.3:General

Solidcore 6.1.3:Change Control

Category:

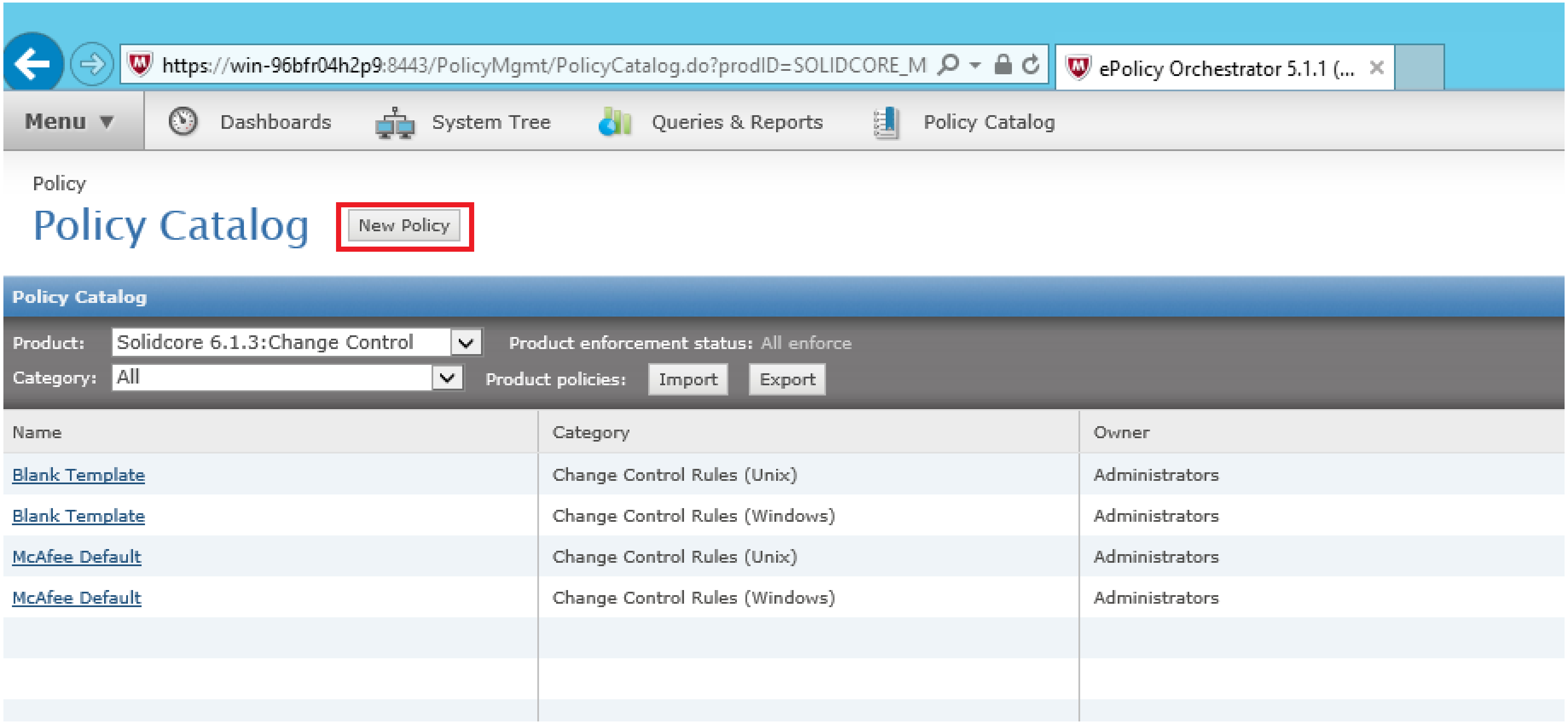
t enforcement status: All enforce

oduct policies: Import Export

Name	Category	Owner
Large Organization Default	General	Administrators
McAfee Default	General	Administrators
McAfee Default	Product Improvement Program	Administrators
McAfee Default	Repository	Administrators
McAfee Default	Troubleshooting	Administrators
My Default	General	Administrators
My Default	Product Improvement Program	Administrators

Enable Change Control

- To click "New Policy" for create a test policy



https://win-96bfr04h2p9:8443/PolicyMgmt/PolicyCatalog.do?prodID=SOLIDCORE_M
ePolicy Orchestrator 5.1.1 (...
Menu ▼
Dashboards
System Tree
Queries & Reports
Policy Catalog
Policy
Policy Catalog
New Policy
Policy Catalog
Product enforcement status: All enforce
Product policies:
Import
Export

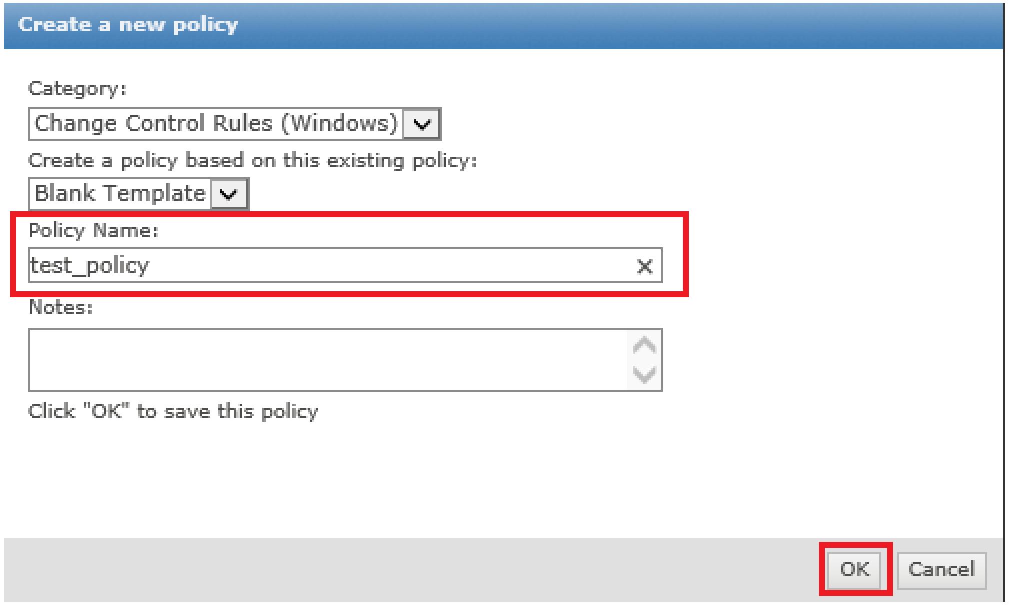
Product: Solidcore 6.1.3:Change Control

Category: All

Name	Category	Owner
Blank Template	Change Control Rules (Unix)	Administrators
Blank Template	Change Control Rules (Windows)	Administrators
McAfee Default	Change Control Rules (Unix)	Administrators
McAfee Default	Change Control Rules (Windows)	Administrators

Enable Change Control

- To fill in Policy Name and to click "OK"



Create a new policy

Category:

Change Control Rules (Windows)

Create a policy based on this existing policy:

Blank Template

Policy Name:

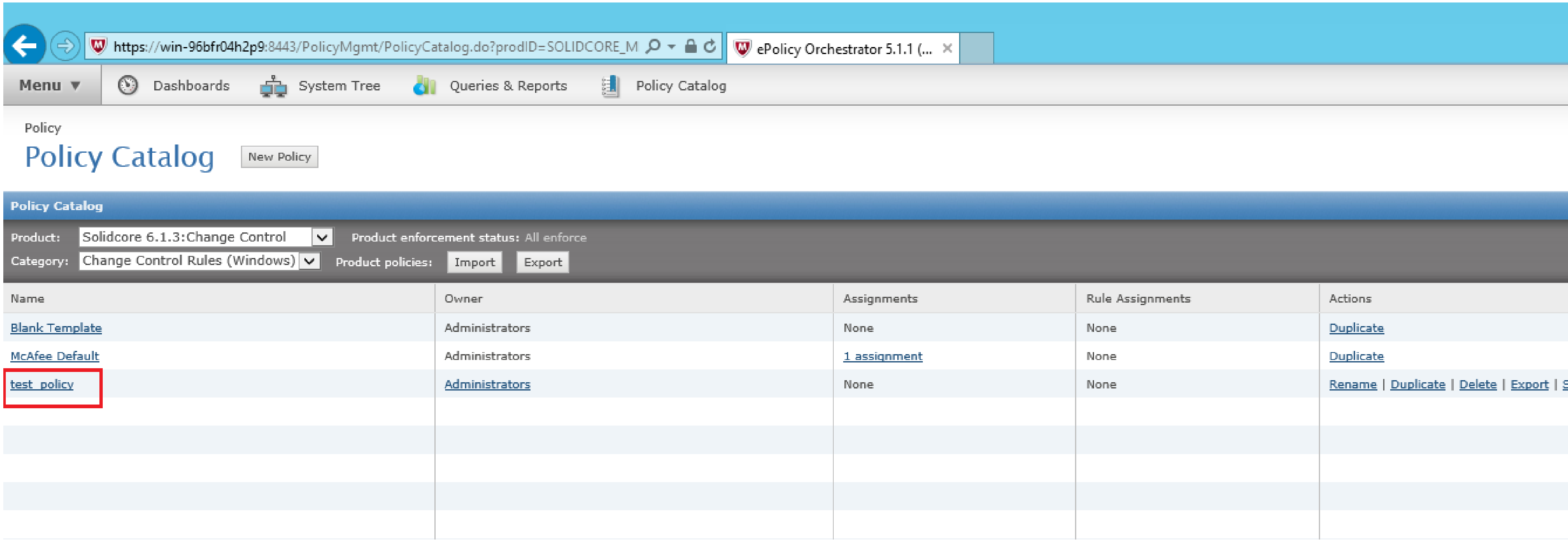
test_policy

Notes:

Click "OK" to save this policy

Enable Change Control

- Click defined policy


https://win-96bfr04h2p9:8443/PolicyMgmt/PolicyCatalog.do?prodID=SOLIDCORE_M
ePolicy Orchestrator 5.1.1 (...
Menu ▼
Dashboards
System Tree
Queries & Reports
Policy Catalog
Policy
New Policy
Import
Export

Policy Catalog

Policy Catalog

Product: Solidcore 6.1.3:Change Control

Product enforcement status: All enforce

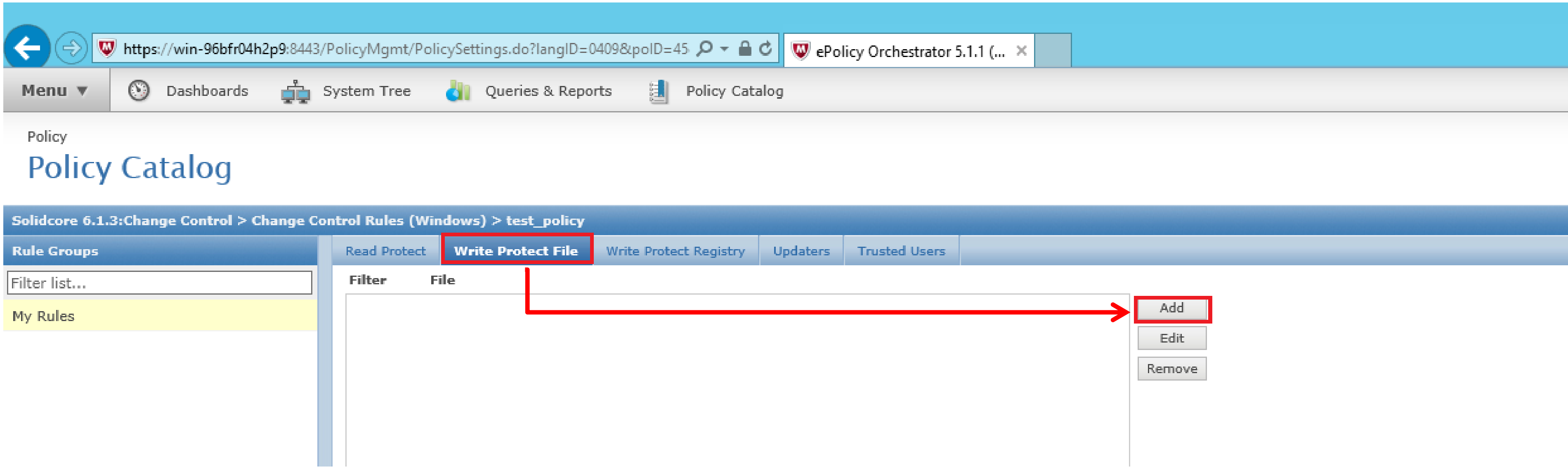
Category: Change Control Rules (Windows)

Product policies:

Name	Owner	Assignments	Rule Assignments	Actions
Blank Template	Administrators	None	None	Duplicate
McAfee Default	Administrators	1 assignment	None	Duplicate
test_policy	Administrators	None	None	Rename | Duplicate | Delete | Export | S

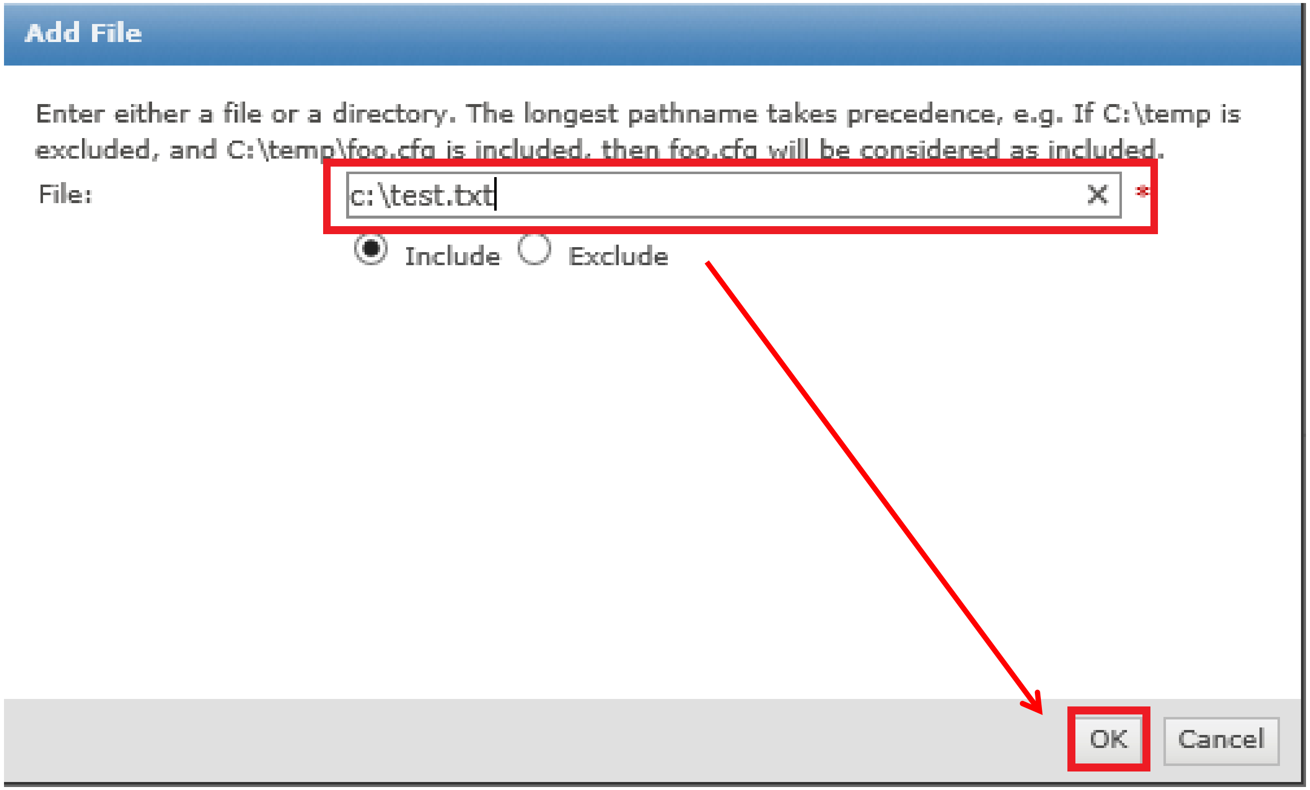
Enable Change Control

- To click "Add" on Write Protect File tab



Enable Change Control

- To fill in File Name with Include and to click "OK"



Add File

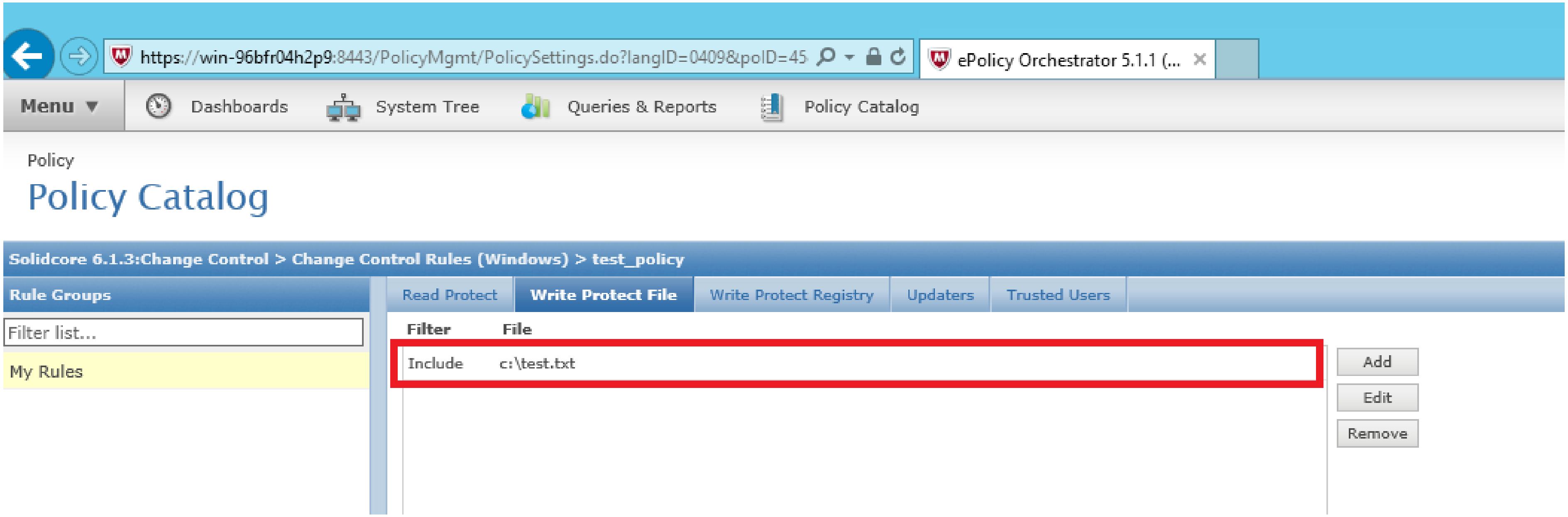
Enter either a file or a directory. The longest pathname takes precedence, e.g. If C:\temp is excluded, and C:\temp\foo.cfg is included, then foo.cfg will be considered as included.

File: c:\test.txt *

● Include ○ Exclude

Enable Change Control

- To fill in File Name with Include and to click "OK"



https://win-96bfr04h2p9:8443/PolicyMgmt/PolicySettings.do?langID=0409&polD=45
ePolicy Orchestrator 5.1.1 (...
Menu
Dashboards
System Tree
Queries & Reports
Policy Catalog
Policy

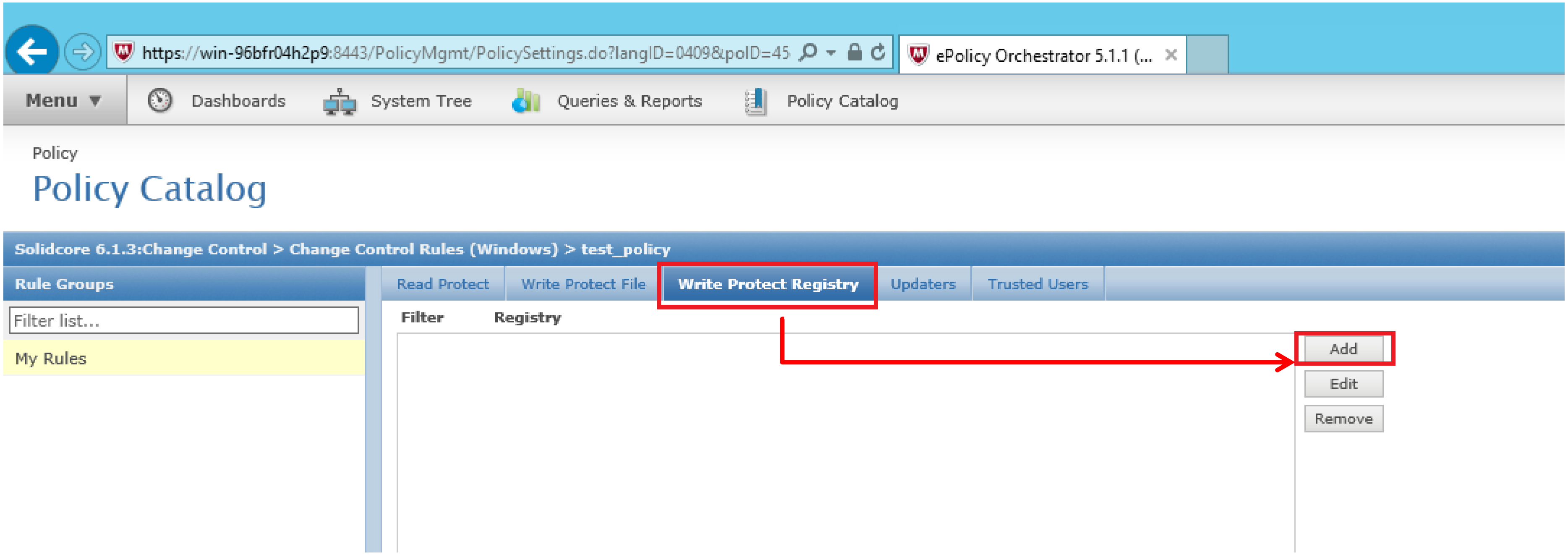
Policy Catalog

Solidcore 6.1.3:Change Control > Change Control Rules (Windows) > test_policy

Filter	File
Include	c:\test.txt

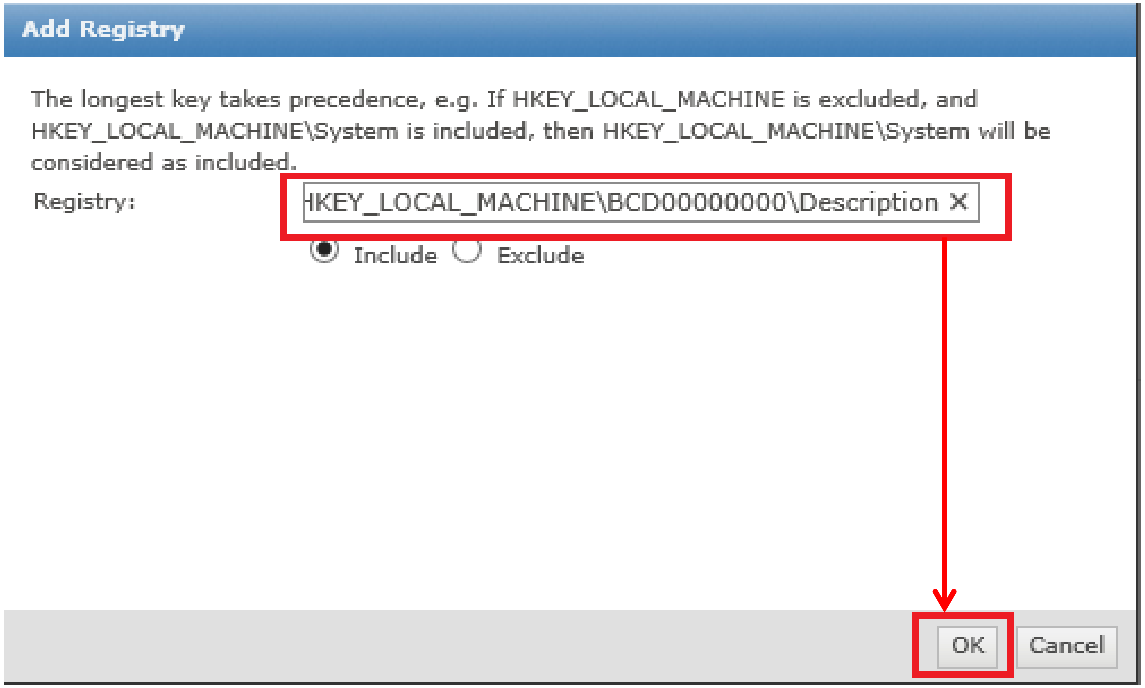
Enable Change Control

- To click "Add" on Write Protect Registry tab



Enable Change Control

- To fill in Registry Value with Include and to click "OK", then to click "Save"



Add Registry

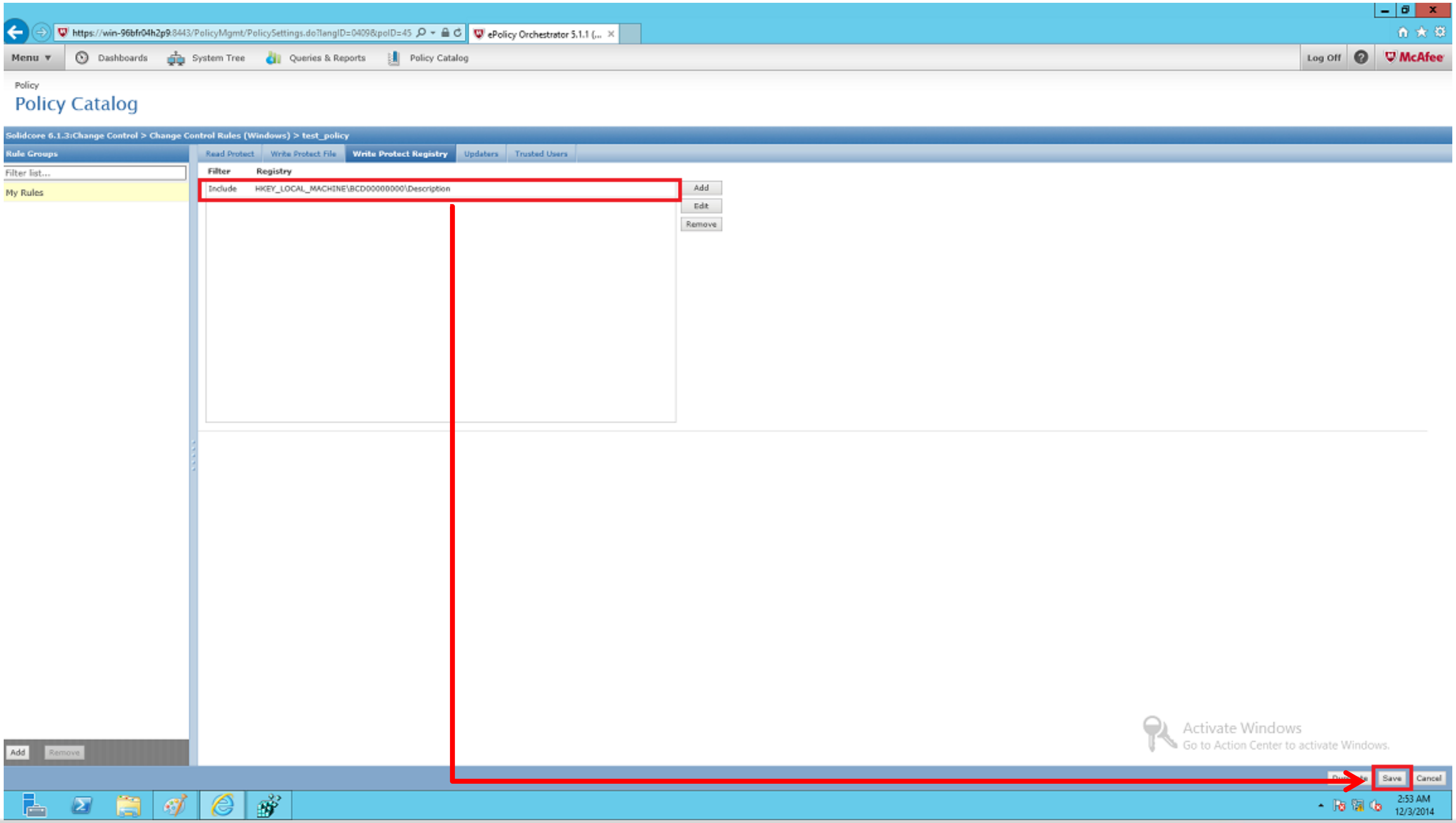
The longest key takes precedence, e.g. If HKEY_LOCAL_MACHINE is excluded, and HKEY_LOCAL_MACHINE\System is included, then HKEY_LOCAL_MACHINE\System will be considered as included.

Registry: HKEY_LOCAL_MACHINE\BCD00000000\Description

● Include ○ Exclude

Enable Change Control

- To fill in Registry Value with Include and to click "OK", then to click "Save"



https://win-96bfr04h2p9:8443/PolicyMgmt/PolicySettings.do?langID=0409&polD=45

Policy

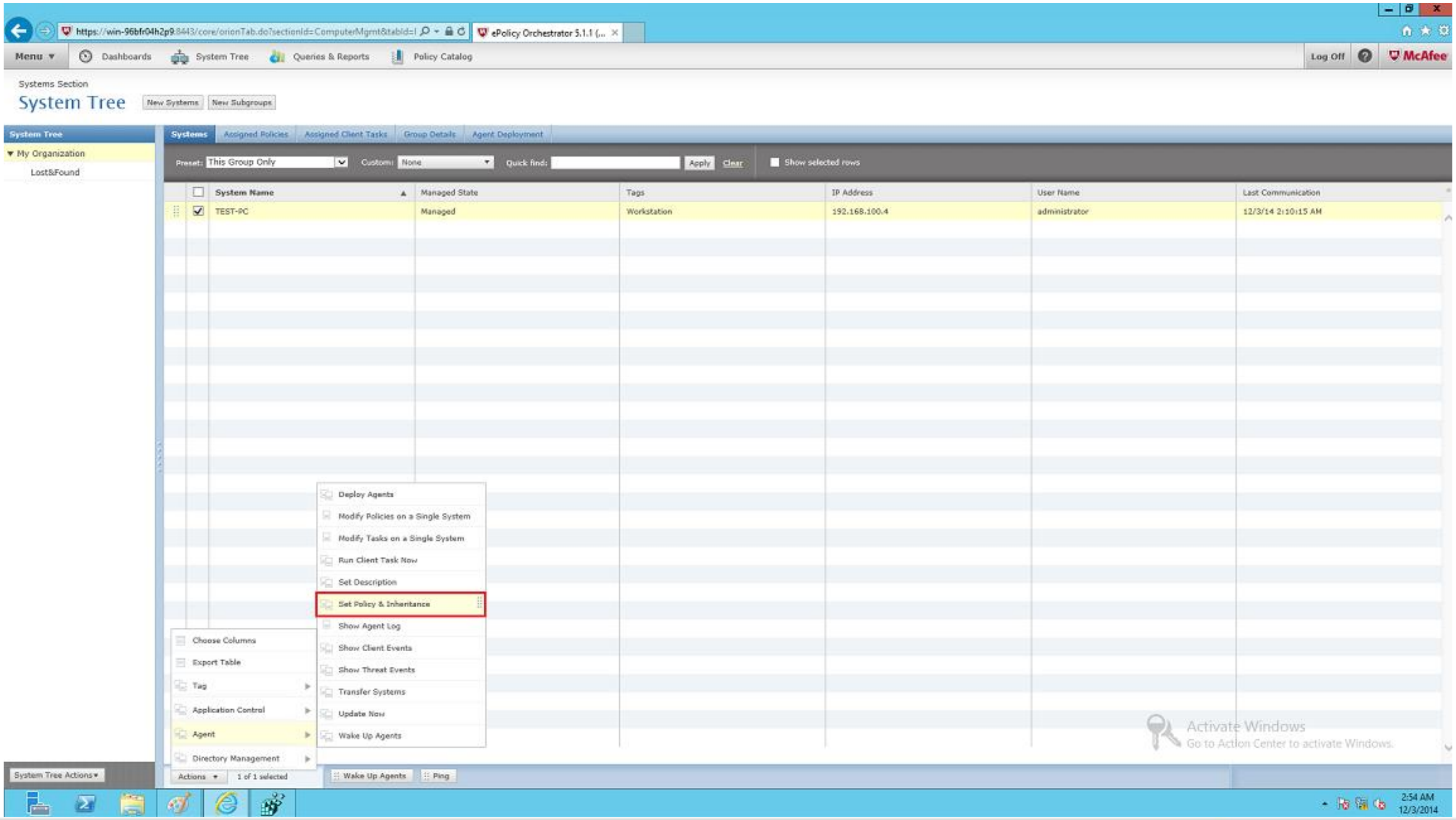
Policy Catalog

Solidcore 6.1.3:Change Control > Change Control Rules (Windows) > test_policy

Filter	Registry
Include	HKEY_LOCAL_MACHINE\BCD00000000\Description

Enable Change Control

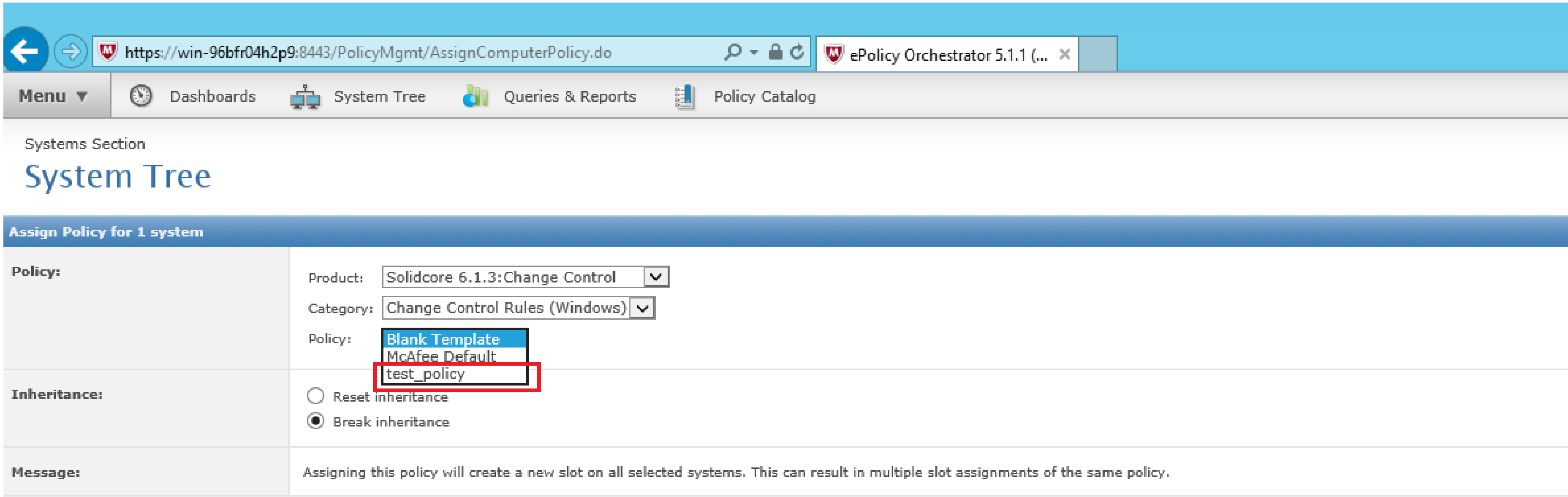
- To check client computer, and to run "Set Policy & Inheritance" from Actions→Agent



	System Name	Managed State	Tags	IP Address	User Name	Last Communication
☑	TEST-PC	Managed	Workstation	192.168.100.4	administrator	12/3/14 2:10:15 AM

Enable Change Control

- To select “test_policy" from Policy drop-list


https://win-96bfr04h2p9:8443/PolicyMgmt/AssignComputerPolicy.do
ePolicy Orchestrator 5.1.1 (...
Menu ▼
Dashboards
System Tree
Queries & Reports
Policy Catalog

Systems Section

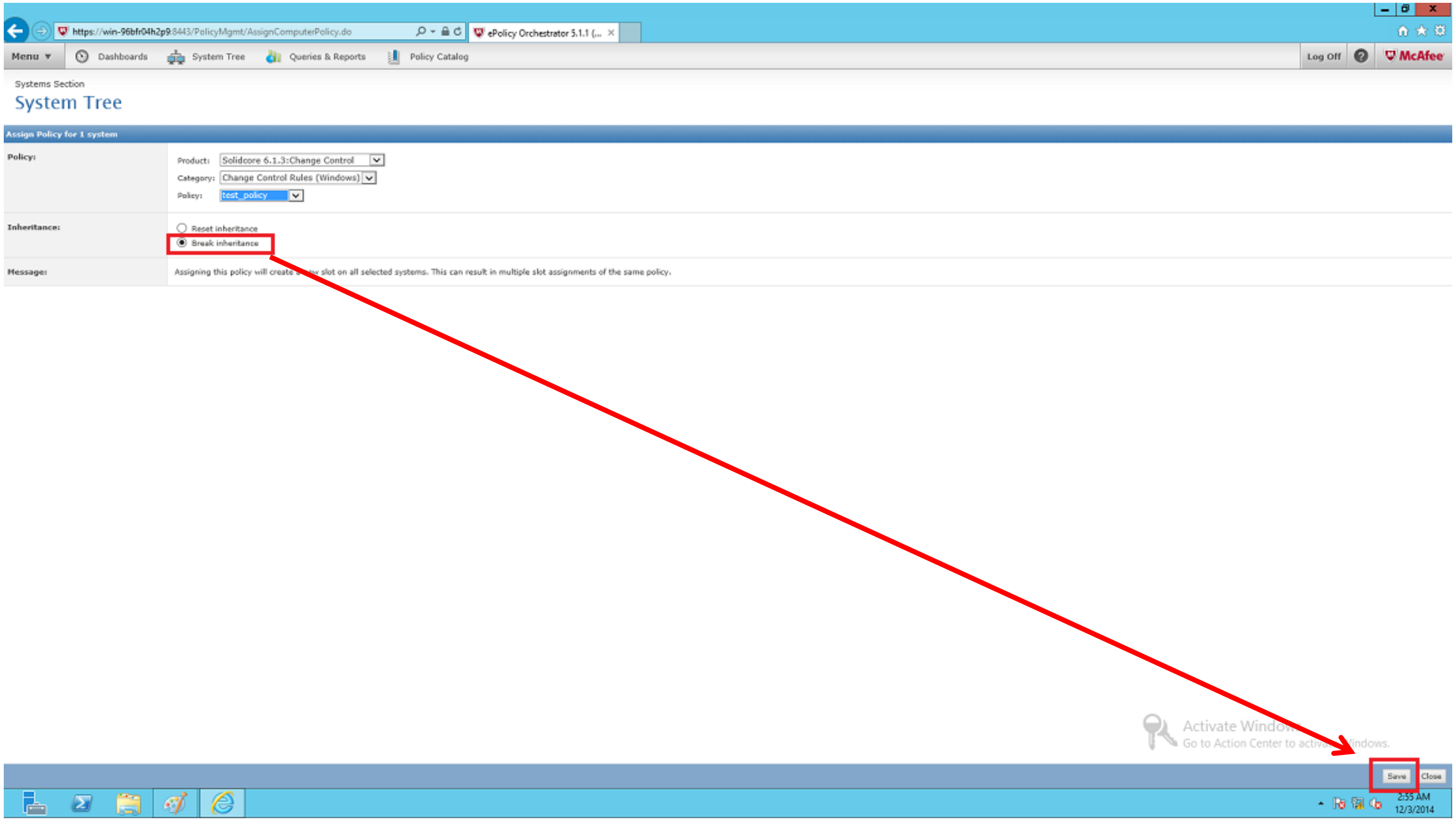
System Tree

Assign Policy for 1 system

Policy:	Product: Solidcore 6.1.3:Change Control Category: Change Control Rules (Windows) Policy: Blank Template McAfee Default test_policy
Inheritance:	○ Reset inheritance ● Break inheritance
Message:	Assigning this policy will create a new slot on all selected systems. This can result in multiple slot assignments of the same policy.

Enable Change Control

- Inheritance is choose "Break inheritance", and to click "Save"

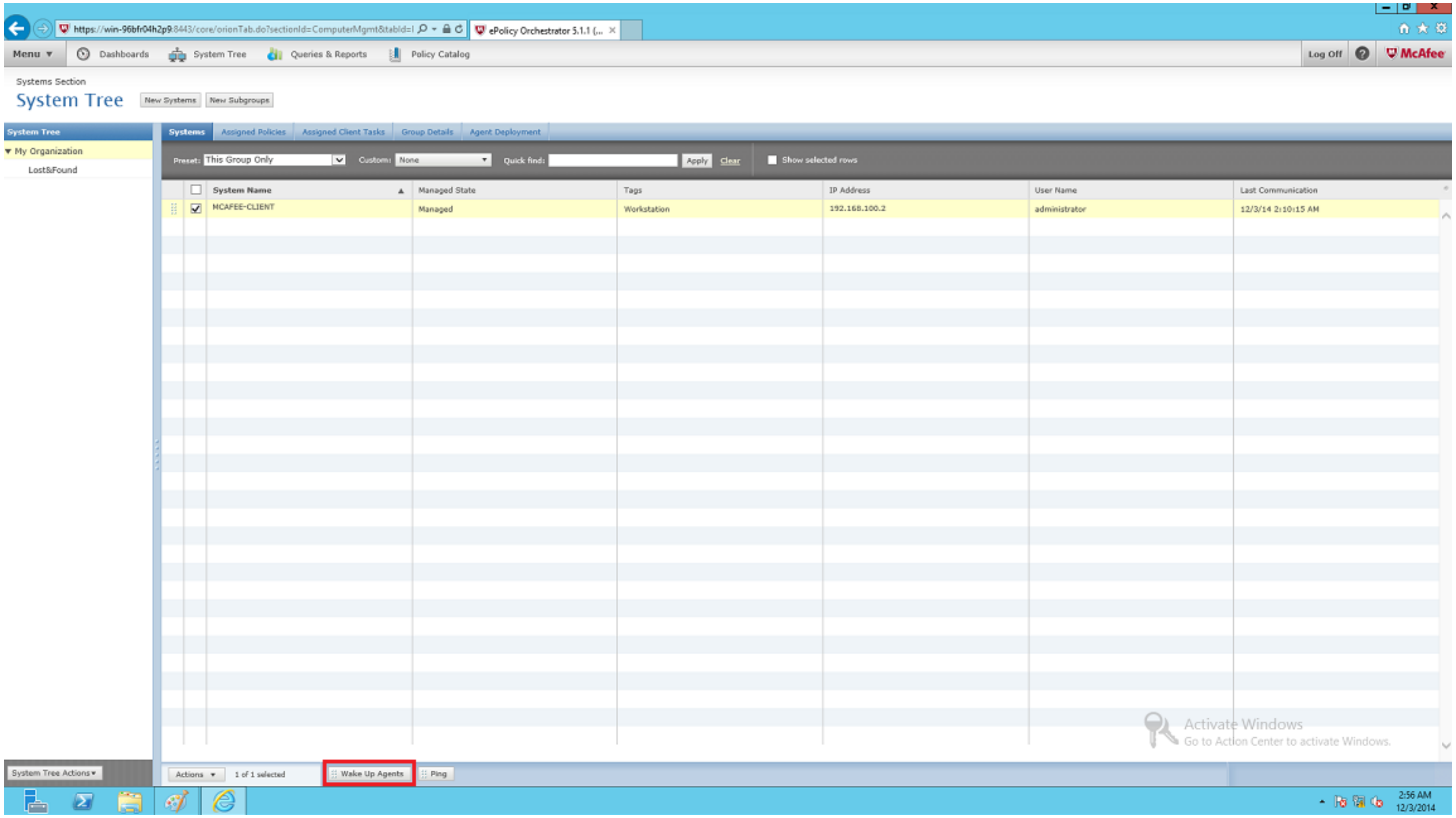


Assign Policy for 1 system

Policy:	Product: Solidcore 6.1.3:Change Control Category: Change Control Rules (Windows) Policy: test_policy
Inheritance:	○ Reset inheritance ● Break inheritance
Message:	Assigning this policy will create a new slot on all selected systems. This can result in multiple slot assignments of the same policy.

Enable Change Control

- To click "Wake Up Agents" and click "OK" for apply Policy that we just created



Systems Section

System Tree

▾ My Organization
Lost&Found

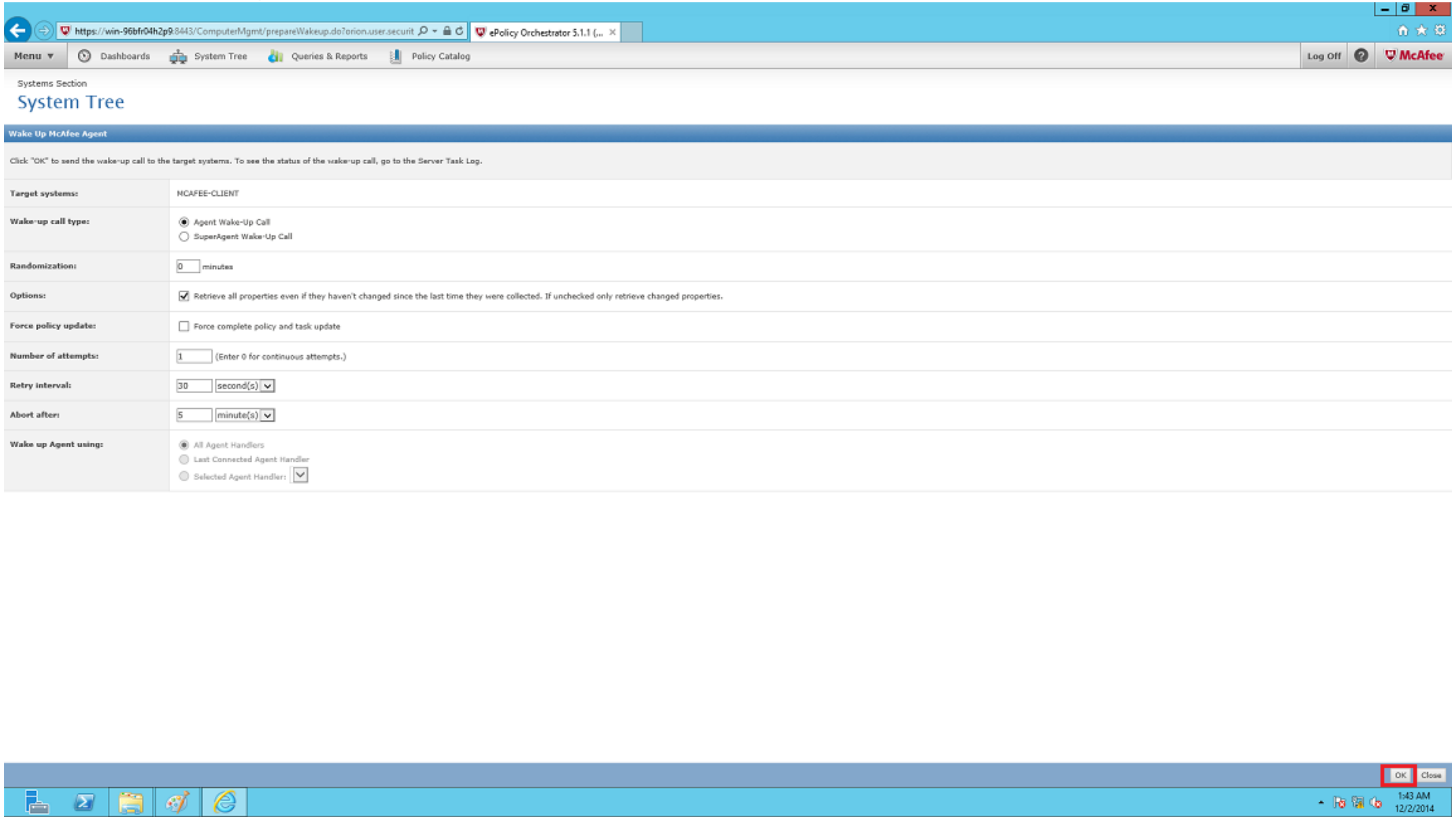
Preset: This Group Only Custom: None Quick find: ☐ Show selected rows

☐	System Name ▲	Managed State	Tags	IP Address	User Name	Last Communication
☑	MCAFEE-CLIENT	Managed	Workstation	192.168.100.2	administrator	12/3/14 2:10:15 AM

1 of 1 selected

Enable Change Control

- To click "Wake Up Agents" and click "OK" for apply Policy that we just created


https://win-96bfr04h2p9:8443/ComputerMgmt/prepareWakeup.do?orion.user.securit
ePolicy Orchestrator 5.1.1 (...
Menu
Dashboards
System Tree
Queries & Reports
Policy Catalog
Log Off
McAfee
OK
Close
1:43 AM
12/2/2014

Systems Section

System Tree

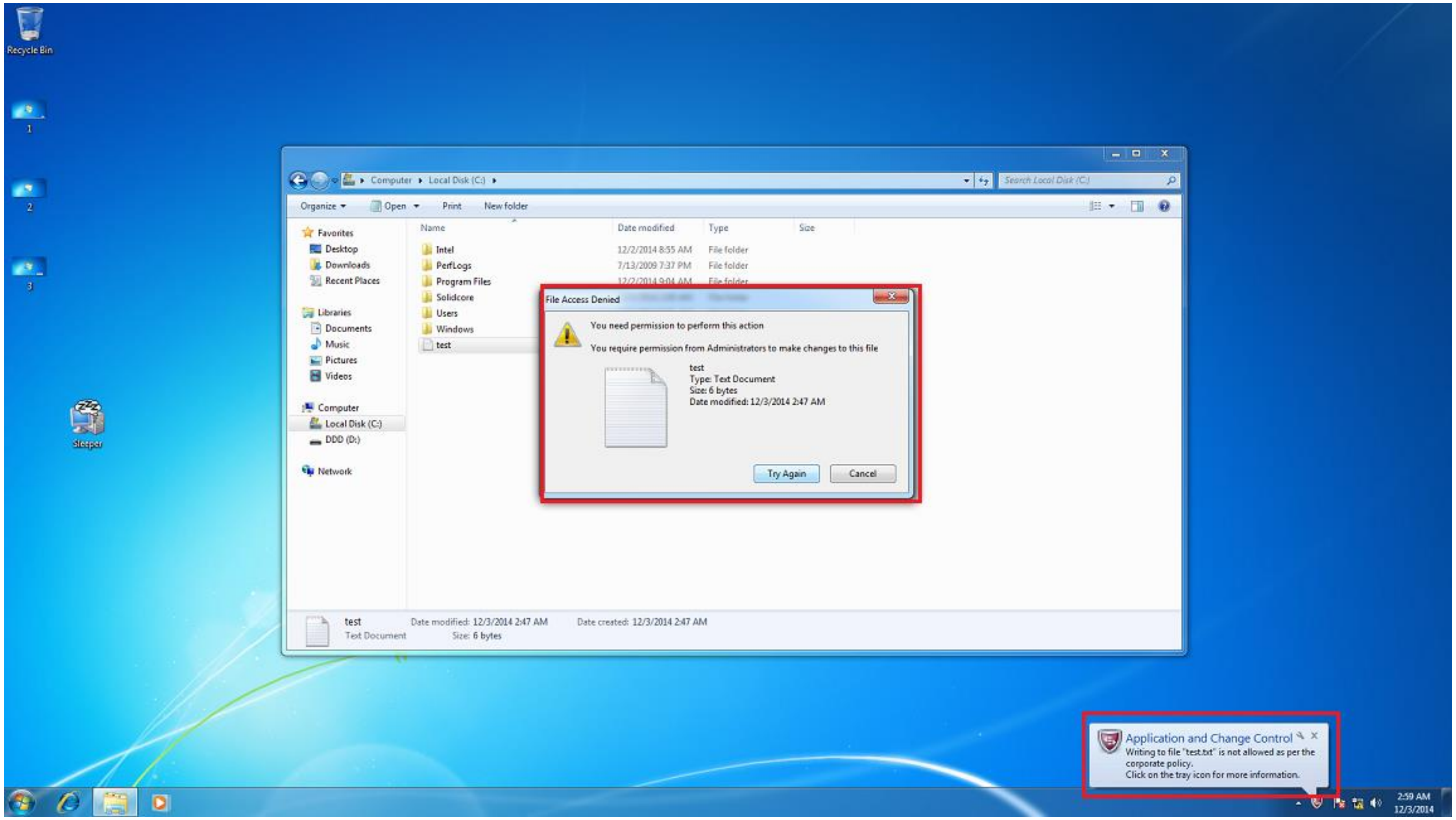
Wake Up McAfee Agent

Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call, go to the Server Task Log.

Target systems:	MCAFEE-CLIENT
Wake-up call type:	● Agent Wake-Up Call ○ SuperAgent Wake-Up Call
Randomization:	0 minutes
Options:	☑ Retrieve all properties even if they haven't changed since the last time they were collected. If unchecked only retrieve changed properties.
Force policy update:	□ Force complete policy and task update
Number of attempts:	1 (Enter 0 for continuous attempts.)
Retry interval:	30 second(s)
Abort after:	5 minute(s)
Wake up Agent using:	● All Agent Handlers ○ Last Connected Agent Handler ○ Selected Agent Handler:

Enable Change Control

- Then, try to delete file "C:\Test.txt" that will not be deleted



File Access Denied

You need permission to perform this action

You require permission from Administrators to make changes to this file

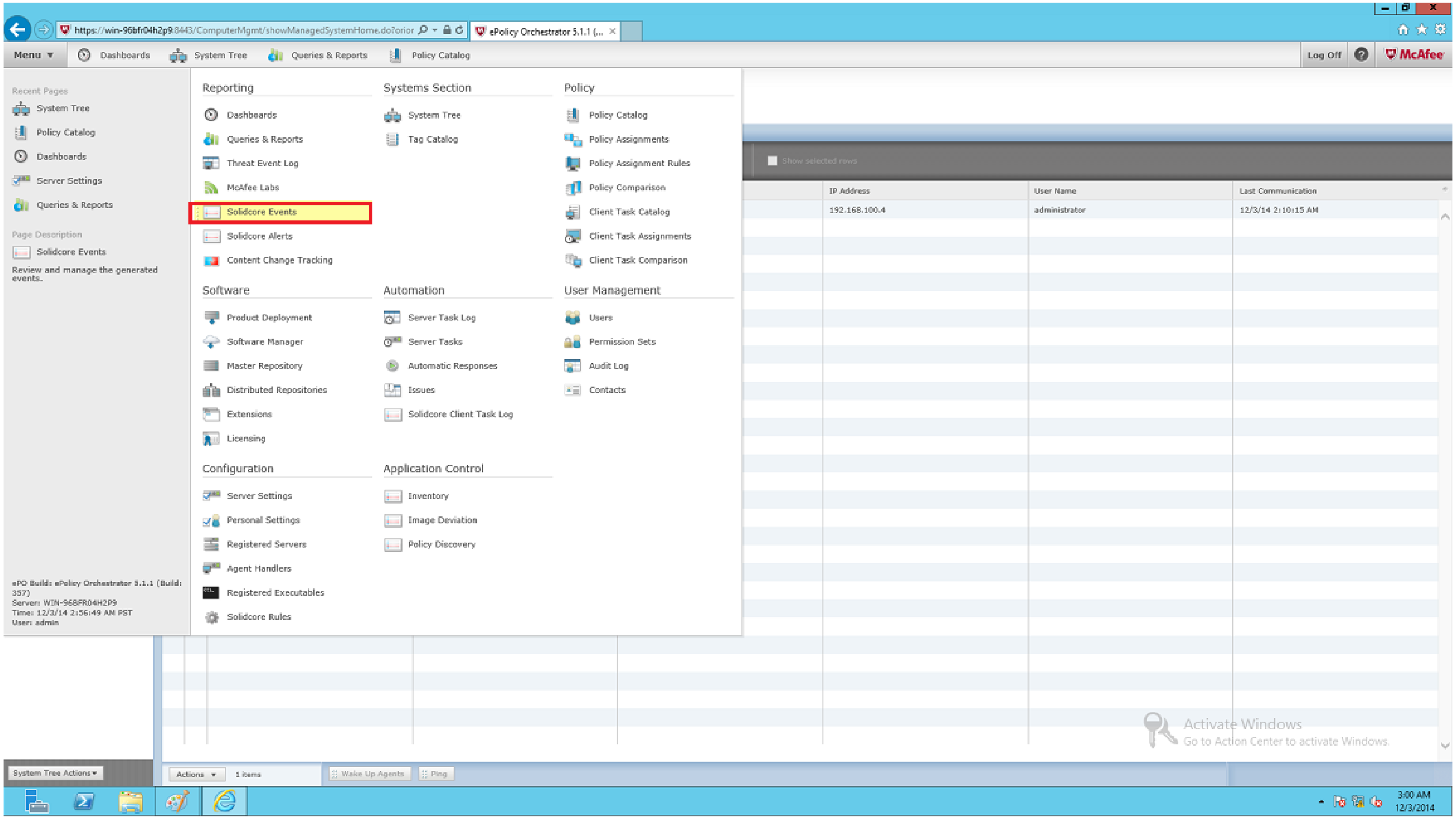
test
Type: Text Document
Size: 6 bytes
Date modified: 12/3/2014 2:47 AM

Application and Change Control

Writing to file "test.txt" is not allowed as per the corporate policy.
Click on the tray icon for more information.

Solidcore Events

- To click "Solidcore Events" from "Menu→Reporting"



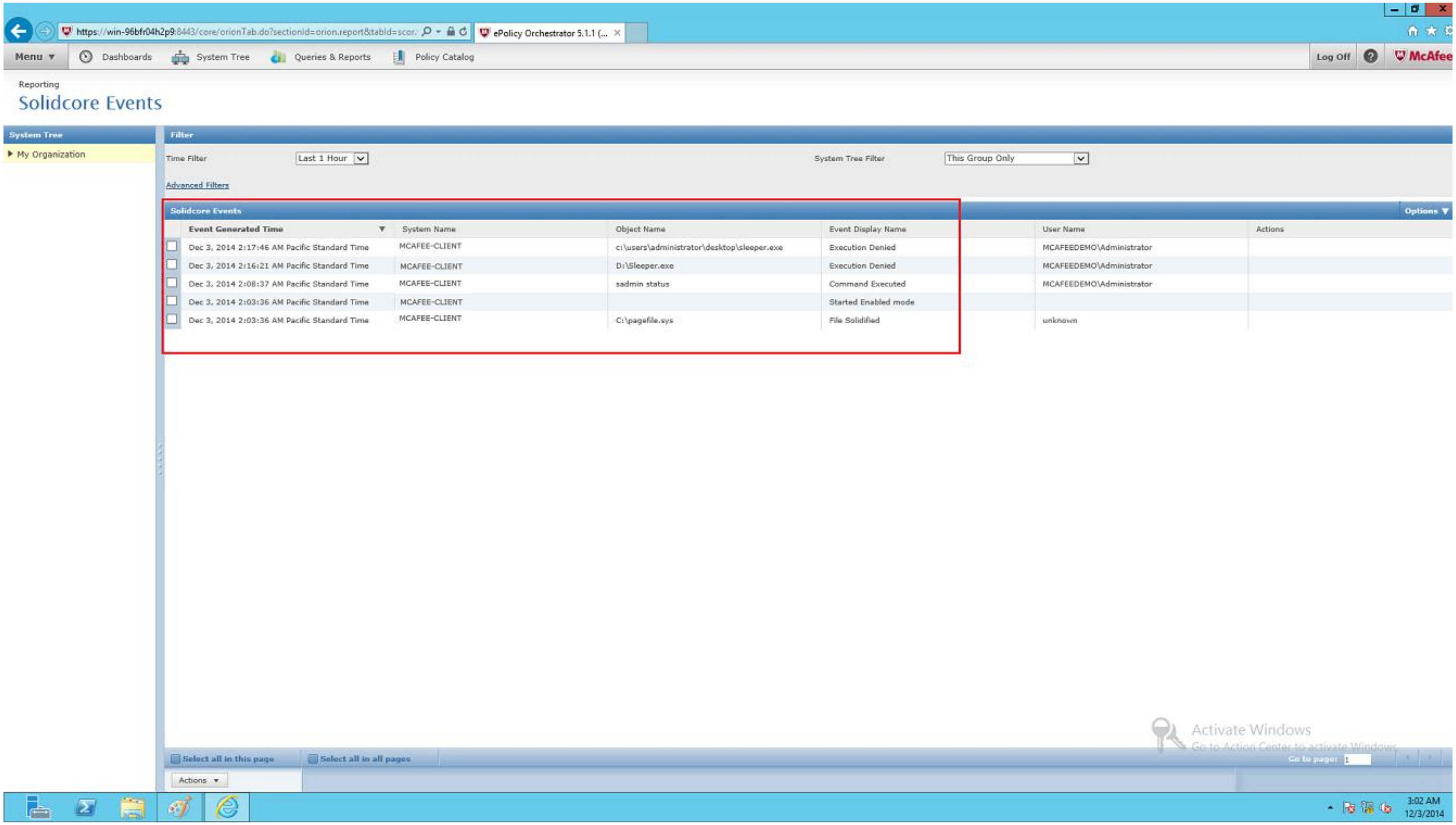
Review and manage the generated events.

IP Address	User Name	Last Communication
192.168.100.4	administrator	12/3/14 2:10:15 AM

ePO Build: ePolicy Orchestrator 5.1.1 (Build: 357)
Server: WIN-96BFR04H2P9
Time: 12/3/14 2:56:49 AM PST
User: admin

Solidcore Events

- Solidcore Events will be used to record and audit



Reporting

Solidcore Events

Time Filter: Last 1 Hour

System Tree Filter: This Group Only

Solidcore Events

	Event Generated Time	System Name	Object Name	Event Display Name	User Name	Actions
□	Dec 3, 2014 2:17:46 AM Pacific Standard Time	MCAFEE-CLIENT	c:\users\administrator\desktop\sleeper.exe	Execution Denied	MCAFEEDEMO\Administrator	
□	Dec 3, 2014 2:16:21 AM Pacific Standard Time	MCAFEE-CLIENT	D:\Sleeper.exe	Execution Denied	MCAFEEDEMO\Administrator	
□	Dec 3, 2014 2:08:37 AM Pacific Standard Time	MCAFEE-CLIENT	sadmin status	Command Executed	MCAFEEDEMO\Administrator	
□	Dec 3, 2014 2:03:36 AM Pacific Standard Time	MCAFEE-CLIENT		Started Enabled mode		
□	Dec 3, 2014 2:03:36 AM Pacific Standard Time	MCAFEE-CLIENT	C:\pagefile.sys	File Solidified	unknown	