

ADVANTECH

# McAfee® ePolicy Orchestrator® 5.1.1 Change Control

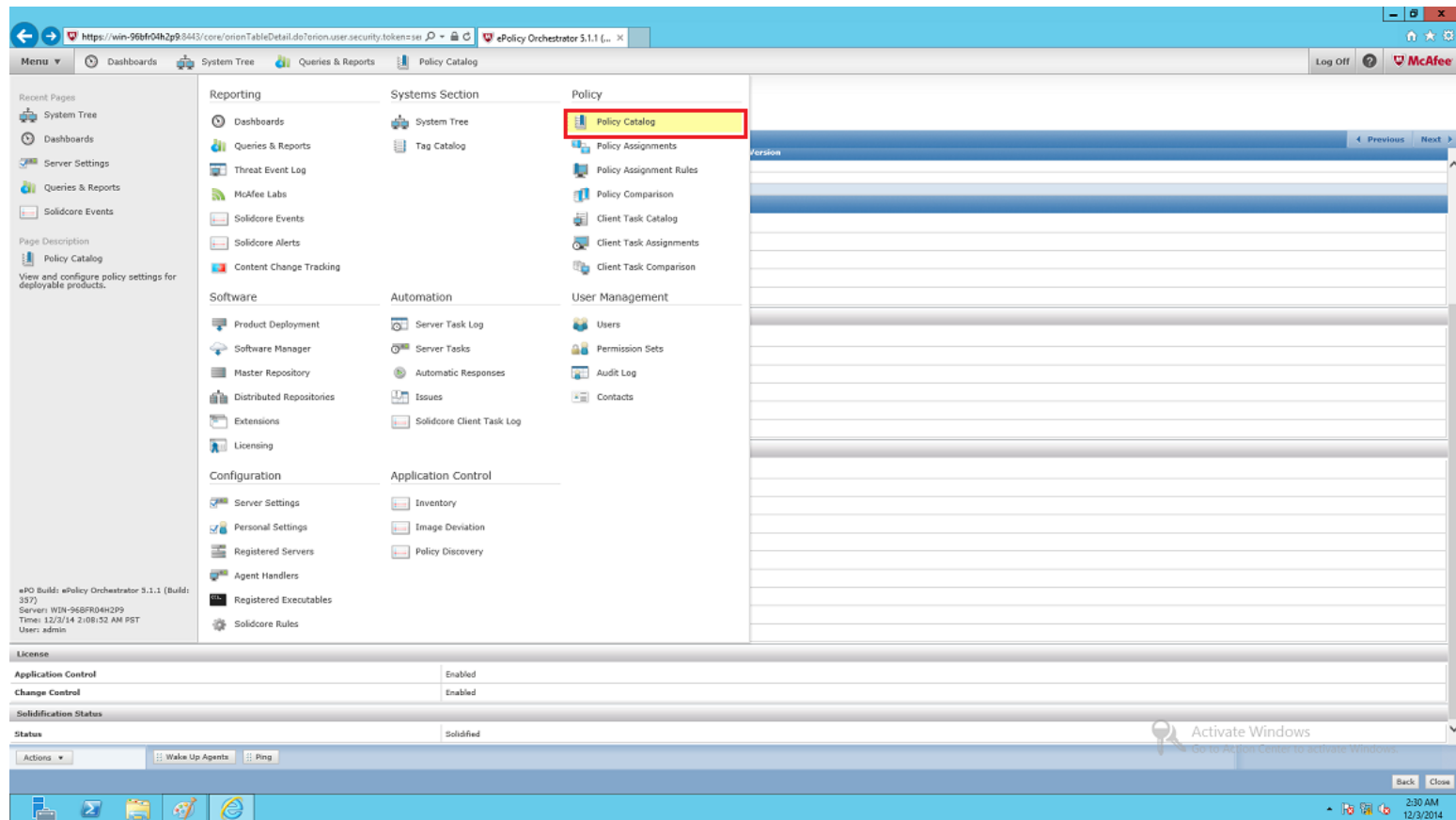
Release 1.1  
2016/5/31

# Released Date

- 2016/05/31

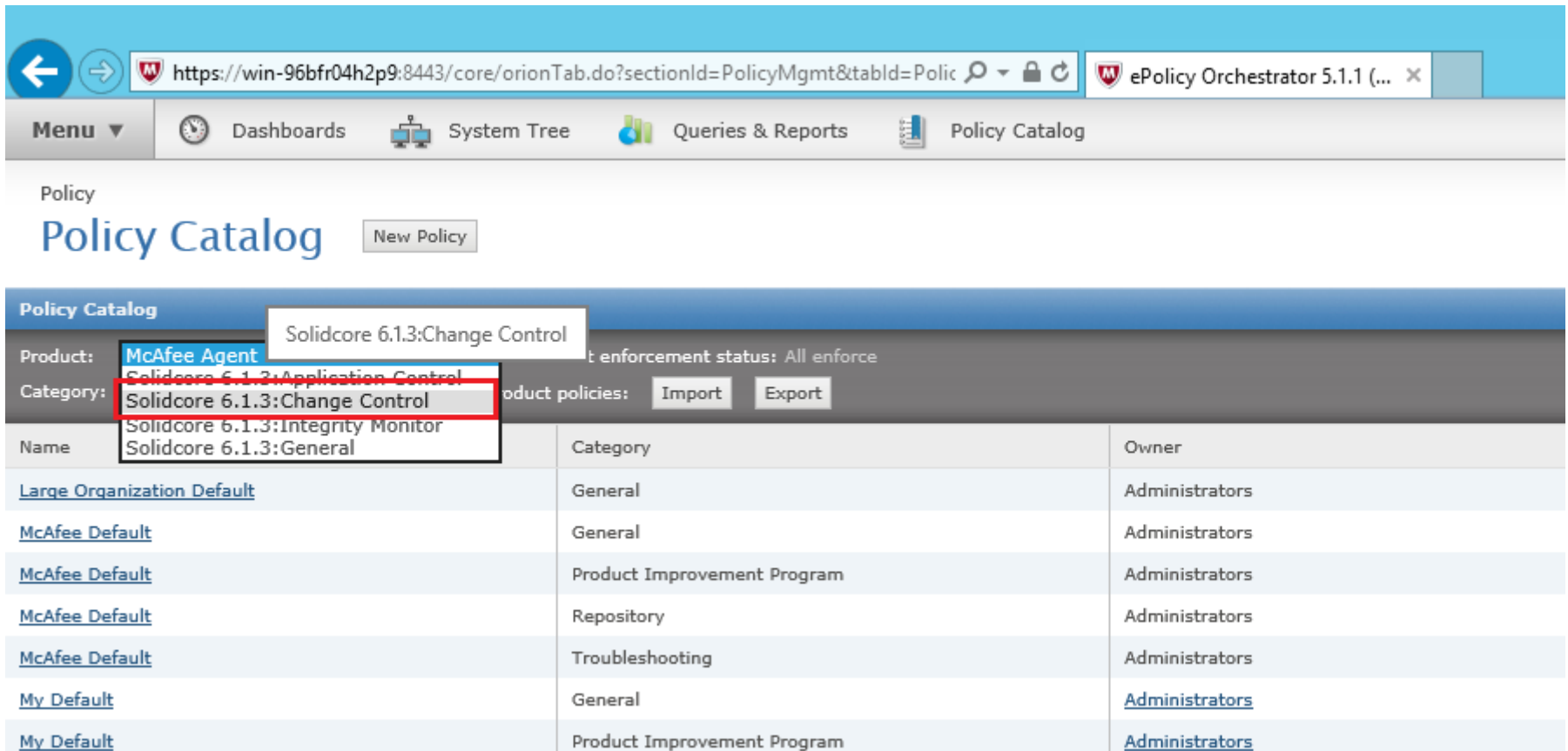
# Enable Change Control

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



# Enable Change Control

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



Policy Catalog

Product: McAfee Agent  
Category: Solidcore 6.1.3:Change Control

Product policies: Import Export

Name	Category	Owner
<a href="#">Large Organization Default</a>	General	Administrators
<a href="#">McAfee Default</a>	General	Administrators
<a href="#">McAfee Default</a>	Product Improvement Program	Administrators
<a href="#">McAfee Default</a>	Repository	Administrators
<a href="#">McAfee Default</a>	Troubleshooting	Administrators
<a href="#">My Default</a>	General	<a href="#">Administrators</a>
<a href="#">My Default</a>	Product Improvement Program	<a href="#">Administrators</a>

# Enable Change Control

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

The screenshot shows the ePolicy Orchestrator 5.1.1 interface. The browser address bar displays the URL: `https://win-96bfr04h2p9:8443/PolicyMgmt/PolicyCatalog.do?prodID=SOLIDCORE_M`. The navigation menu includes: Menu, Dashboards, System Tree, Queries & Reports, and Policy Catalog. The main content area is titled "Policy Catalog" and features a "New Policy" button highlighted with a red box. Below this, there are filters for "Product: Solidcore 6.1.3:Change Control" and "Category: All", along with "Import" and "Export" buttons. A table lists existing policies:

Name	Category	Owner
<a href="#">Blank Template</a>	Change Control Rules (Unix)	Administrators
<a href="#">Blank Template</a>	Change Control Rules (Windows)	Administrators
<a href="#">McAfee Default</a>	Change Control Rules (Unix)	Administrators
<a href="#">McAfee Default</a>	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 x

Notes:  
▾

Click "OK" to save this policy

OK Cancel

# Enable Change Control

- Click defined policy

Policy Catalog

Product: Solidcore 6.1.3:Change Control Product enforcement status: All enforce

Category: Change Control Rules (Windows) Product policies: Import Export

Name	Owner	Assignments	Rule Assignments	Actions
<a href="#">Blank Template</a>	Administrators	None	None	<a href="#">Duplicate</a>
<a href="#">McAfee Default</a>	Administrators	<a href="#">1 assignment</a>	None	<a href="#">Duplicate</a>
<a href="#">test_policy</a>	<a href="#">Administrators</a>	None	None	<a href="#">Rename</a>   <a href="#">Duplicate</a>   <a href="#">Delete</a>   <a href="#">Export</a>   <a href="#">S</a>

# Enable Change Control

- To click "Add" on Write Protect File tab

The screenshot displays the ePolicy Orchestrator 5.1.1 web interface. The browser address bar shows the URL: <https://win-96bfr04h2p9:8443/PolicyMgmt/PolicySettings.do?langID=0409&poID=45>. The navigation menu includes 'Menu', 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. The main content area is titled 'Policy Catalog' and shows a breadcrumb path: 'Solidcore 6.1.3:Change Control > Change Control Rules (Windows) > test\_policy'. Below this, there are tabs for 'Read Protect', 'Write Protect File', 'Write Protect Registry', 'Updaters', and 'Trusted Users'. The 'Write Protect File' tab is active and highlighted with a red box. A table with columns 'Filter' and 'File' is visible, and a red arrow points from the 'File' column to the 'Add' button, which is also highlighted with a red box. Other buttons 'Edit' and 'Remove' are also present.



# 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.cfa is included, then foo.cfa will be considered as included.

File:

Include  Exclude

# Enable Change Control

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

The screenshot shows the ePolicy Orchestrator 5.1.1 web interface. The browser address bar displays the URL: <https://win-96bfr04h2p9:8443/PolicyMgmt/PolicySettings.do?langID=0409&polID=45>. The navigation menu includes Dashboard, System Tree, Queries & Reports, and Policy Catalog. The main content area is titled 'Policy Catalog' and shows the path: Solidcore 6.1.3:Change Control > Change Control Rules (Windows) > test\_policy. The 'Write Protect File' tab is selected, showing a table with the following content:

Filter	File
Include	c:\test.txt

Buttons for 'Add', 'Edit', and 'Remove' are visible on the right side of the table.

# Enable Change Control

- To click "Add" on Write Protect Registry tab

The screenshot displays the ePolicy Orchestrator 5.1.1 web interface. The browser address bar shows the URL: <https://win-96bfr04h2p9:8443/PolicyMgmt/PolicySettings.do?langID=0409&polID=45>. The navigation menu includes Dashboard, System Tree, Queries & Reports, and Policy Catalog. The main content area is titled "Policy Catalog" and shows a breadcrumb path: "Solidcore 6.1.3:Change Control > Change Control Rules (Windows) > test\_policy". Below this, there are several tabs: "Read Protect", "Write Protect File", "Write Protect Registry" (which is highlighted with a red box), "Updaters", and "Trusted Users". The "Write Protect Registry" tab is active, showing a table with columns "Filter" and "Registry". On the right side of the table, there are three buttons: "Add", "Edit", and "Remove". The "Add" button is highlighted with a red box, and a red arrow points from the "Write Protect Registry" tab to it. The left sidebar shows "Rule Groups" with a search box and "My Rules" listed below.

# 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:

Include  Exclude

# Enable Change Control

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

The screenshot shows the ePolicy Orchestrator 5.1.1 interface. The browser address bar displays the URL: <https://win-96bf04h2p98443/PolicyMgmt/PolicySettings.do?langID=0409&polID=45>. The page title is "Policy Catalog". The breadcrumb navigation shows: "Solidcore 6.1.3: Change Control > Change Control Rules (Windows) > test\_policy". The "Write Protect Registry" tab is active, showing a "Filter" section with "Registry" selected. A table lists a rule: "Include HKEY\_LOCAL\_MACHINE\BCD00000000\Description". To the right of the table are "Add", "Edit", and "Remove" buttons. At the bottom right, there is an "Activate Windows" watermark and a taskbar with a "Save" button highlighted in red. A red arrow points from the "Save" button in the taskbar to the "Save" button in the interface.

# Enable Change Control

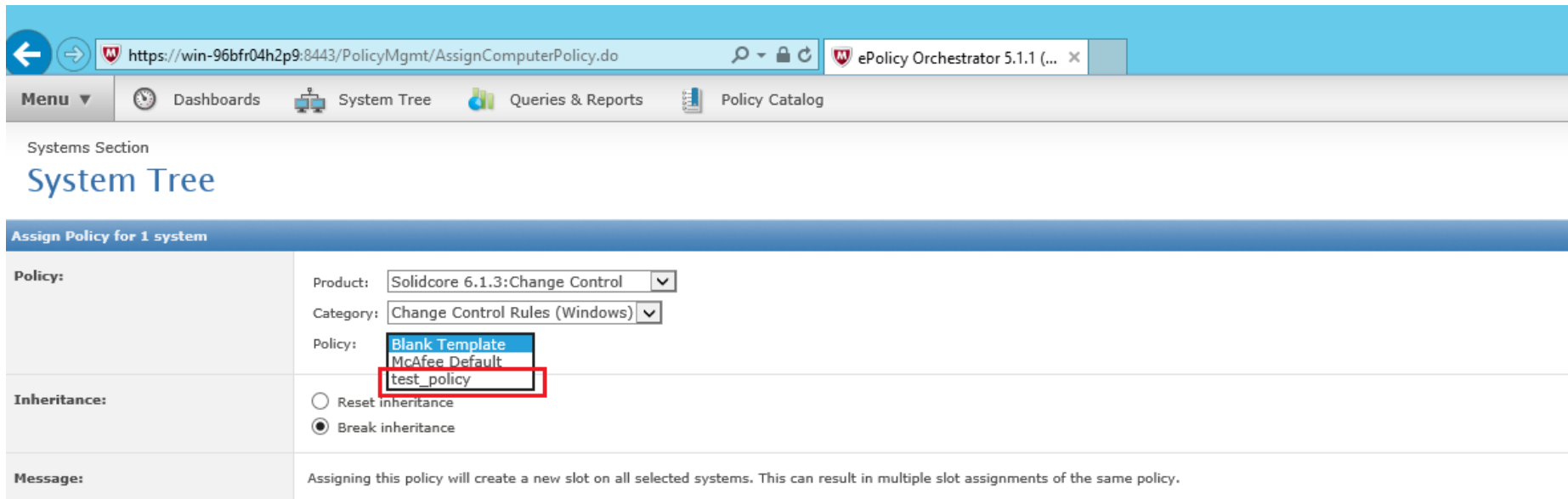
- To check client computer, and to run "Set Policy & Inheritance" from Actions → Agent

The screenshot shows the ePolicy Orchestrator 5.1.1.1 interface. The browser address bar displays the URL: <https://win-96bf04h2p9.8443/cors/orionTab.do?sectionId=ComputerMgmt&tabId=1>. The interface includes a navigation menu with options like Dashboards, System Tree, Queries & Reports, and Policy Catalog. The main area is titled "System Tree" and shows a table of systems. The table has columns for System Name, Managed State, Tags, IP Address, User Name, and Last Communication. One system, "TEST-PC", is selected. A context menu is open over the selected system, with the "Set Policy & Inheritance" option highlighted. Other options in the menu include Deploy Agents, Modify Policies on a Single System, Modify Tasks on a Single System, Run Client Task Now, Set Description, Show Agent Log, Show Client Events, Show Threat Events, Transfer Systems, Update Now, and Wake Up Agents. The bottom status bar shows "System Tree Actions" and "1 of 1 selected".

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



The screenshot shows the ePolicy Orchestrator 5.1.1 interface. The browser address bar displays the URL: <https://win-96bfr04h2p9:8443/PolicyMgmt/AssignComputerPolicy.do>. The navigation menu includes: Menu, Dashboards, System Tree, Queries & Reports, and Policy Catalog. The current page is titled "Systems Section" and "System Tree".

The main content area is titled "Assign Policy for 1 system" and contains the following form fields:

- Policy:**
  - Product: Solidcore 6.1.3:Change Control
  - Category: Change Control Rules (Windows)
  - Policy: A dropdown menu is open, showing three options: "Blank Template", "McAfee Default", and "test\_policy". The "test\_policy" option is highlighted with a red box.
- 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**"

The screenshot shows the ePolicy Orchestrator 3.1.1 interface. The main window is titled "System Tree" and displays the "Assign Policy for 1 system" dialog box. The dialog box has the following fields:

- 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.

The "Break inheritance" radio button is highlighted with a red box, and a red arrow points from it to the "Save" button in the bottom right corner of the dialog box. The "Save" button is also highlighted with a red box. The Windows taskbar at the bottom shows the time as 2:55 AM on 12/3/2014.



# Enable Change Control

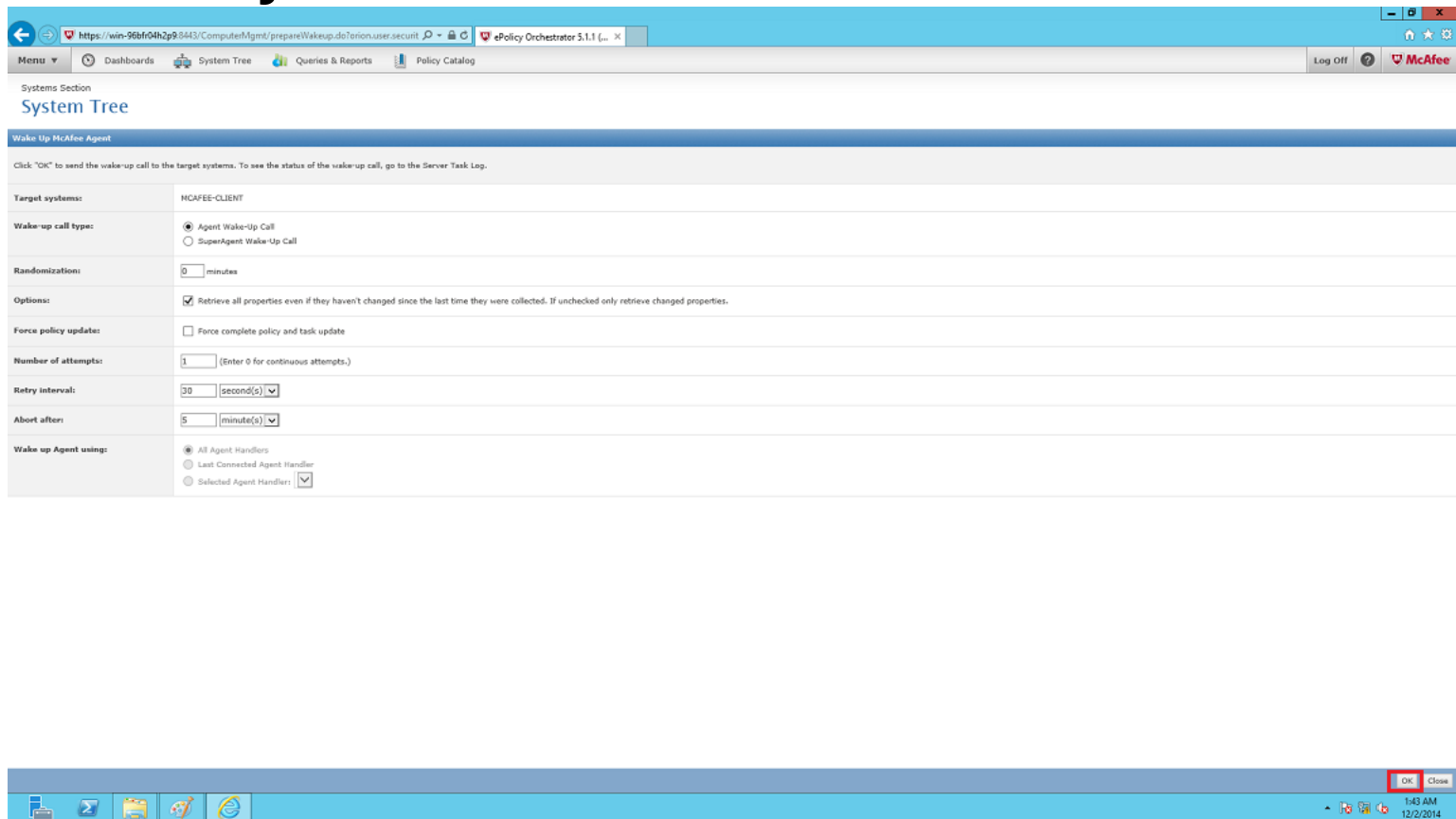
- To click "**Wake Up Agents**" and click "**OK**" for apply Policy that we just created

The screenshot displays the McAfee ePolicy Orchestrator 3.1.1 web interface. The main content area shows a table of systems under the 'Systems' tab. The table has the following columns: System Name, Managed State, Tags, IP Address, User Name, and Last Communication. One system, 'MCAFFEE-CLIENT', is selected and highlighted in yellow. Below the table, the 'System Tree Actions' menu is open, and the 'Wake Up Agents' option is highlighted with a red box. The bottom status bar shows the time as 2:56 AM on 12/3/2014.

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

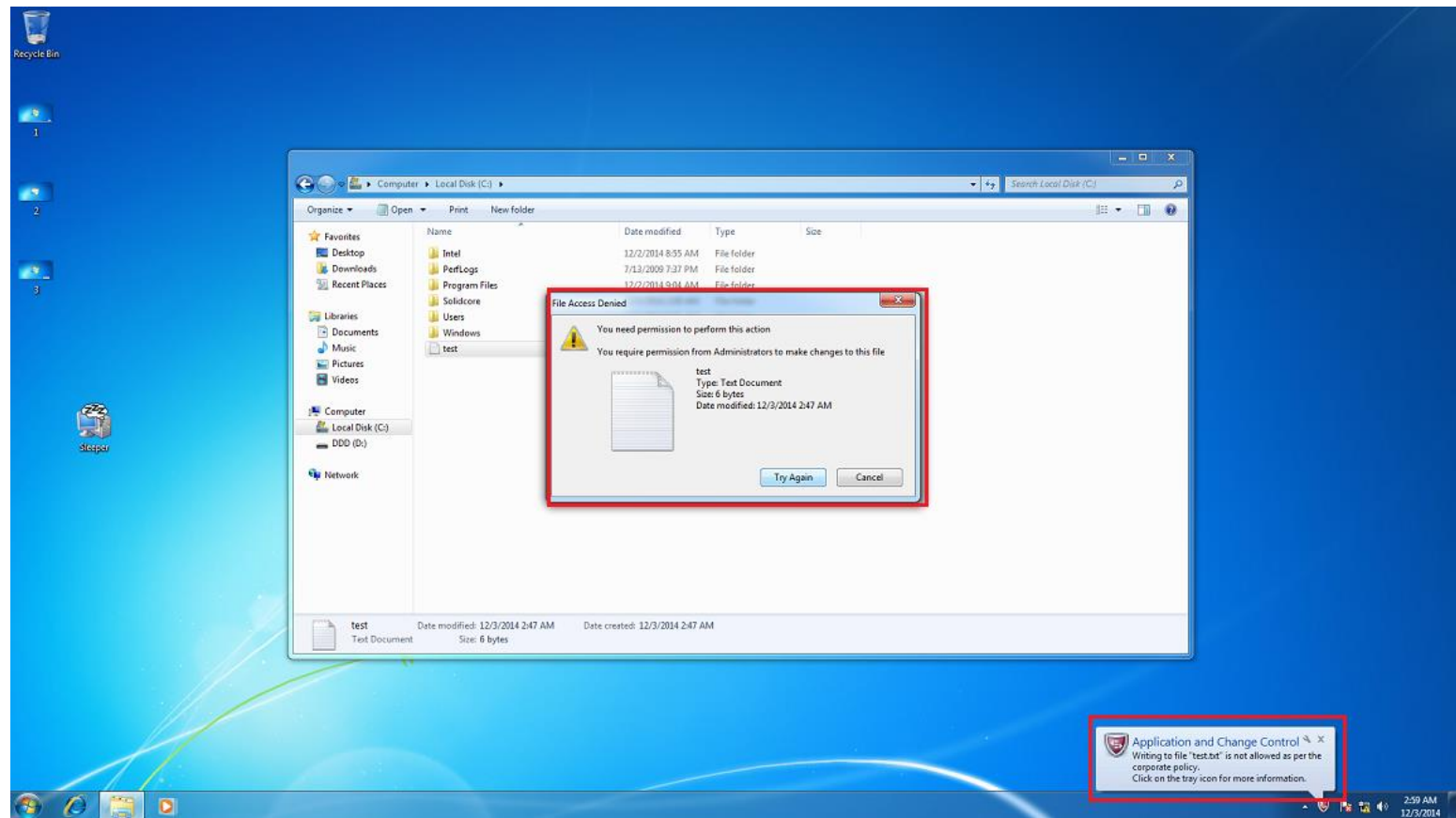
# Enable Change Control

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



# Enable Change Control

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



# Solidcore Events

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

The screenshot displays the ePolicy Orchestrator 5.1.1 web interface. The 'Reporting' section in the left-hand menu is expanded, and the 'Solidcore Events' option is highlighted with a red rectangle. The main content area shows a table with the following data:

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

At the bottom of the interface, there is a system tray with the date and time: 3:00 AM 12/3/2014. An 'Activate Windows' watermark is also visible in the bottom right corner.

# Solidcore Events

- Solidcore Events will be used to record and audit

The screenshot shows the McAfee ePolicy Orchestrator 5.1.1 interface. The main content area displays a table of Solidcore Events. The table has the following columns: Event Generated Time, System Name, Object Name, Event Display Name, User Name, and Actions. The table is highlighted with a red border.

Event Generated Time	System Name	Object Name	Event Display Name	User Name	Actions
<input type="checkbox"/> Dec 3, 2014 2:17:46 AM Pacific Standard Time	MCAFFEE-CLIENT	c:\users\administrator\desktop\sleeper.exe	Execution Denied	MCAFFEEDEMO\Administrator	
<input type="checkbox"/> Dec 3, 2014 2:16:21 AM Pacific Standard Time	MCAFFEE-CLIENT	D:\sleeper.exe	Execution Denied	MCAFFEEDEMO\Administrator	
<input type="checkbox"/> Dec 3, 2014 2:08:37 AM Pacific Standard Time	MCAFFEE-CLIENT	admin status	Command Executed	MCAFFEEDEMO\Administrator	
<input type="checkbox"/> Dec 3, 2014 2:03:36 AM Pacific Standard Time	MCAFFEE-CLIENT		Started Enabled mode		
<input type="checkbox"/> Dec 3, 2014 2:03:36 AM Pacific Standard Time	MCAFFEE-CLIENT	C:\pagefile.sys	File Solidified	unknown	