McAfee® ePolicy Orchestrator® 5.1.1 Change Control

Release 1.1 2016/5/31



Released Date

2016/05/31



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

	//eeeo/esiaeTableDatail.de7eciae.com	uteinen On Ad Mar of		- 0 ×
Menu v 🕥 Dashboards 👘	System Tree A Queries & Reports	Policy Catalog	Strator 3.1.1 (A	
Recent Pages	Reporting O Dashboards	Systems Section	Policy Policy Cetalog	
O Dashboards	谢 Queries & Reports	Tag Catalog	Policy Assignments	
Server Settings	Threat Event Log		Policy Assignment Rules	^ ^ ^
Queries & Reports	MoAfee Labs		Policy Comparison	
Solidcore Events	Solidcore Events		🚛 Client Task Catalog	
Page Description	Solidcore Alerts		👼 Client Task Assignments	
View and configure policy settings for	Content Change Tracking		n Client Task Comparison	
deptoyable products.	Software	Automation	User Management	
	Product Deployment	Server Task Log	👪 Users	
	🐢 Software Manager	Om Server Tasks	🔒 Permission Sets	
	Master Repository	Automatic Responses	📰 Audit Log	
	Distributed Repositories	Issues	Contacts	
	Extensions	Solidcore Client Task Log		
	Licensing			
	Configuration	Application Control		
	Server Settings	inventory		
	📲 Personal Settings	iii Image Deviation		
	Registered Servers	Policy Discovery		
	🚛 Agent Handlers			
ePO Build: ePolicy Orchestrator 5.1.1 (Build: 357) Server: WIN-968FR04H2P9	Registered Executables			
Time: 12/3/14 2:08:52 AM PST User: admin	🎲 Solidcore Rules			
License				
Application Control		Enabled		
Change Control		Enabled		
Solidification Status		Solidified		🔾 Activate Windows 🗸
Actions •	Agenta 🗄 Ping			Go to Action Center to activate Windows.
				Back Close
📥 🛛 🗎 🍕				 ► 16 10 12/3/2014

Enabling an Intelligent Planet

AD\ANTECH

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

+ ttps://win-96bfr04h2p9:8443/core/orion	Tab.do?sectionId=PolicyMgmt&tabId=Polic 🔎 👻 🕻	🖉 ePolicy Orchestrator 5.1.1 (🗙
Menu 🔻 🕥 Dashboards 🚔 System Tre	ee 🍓 Queries & Reports 🔢 Policy Catalog	
Policy Policy Catalog New Policy		
Policy Catalog Solidcore 6.1.3:Change Contro		
Product: McAfee Agent Category: Category: Cate	t enforcement status: All enforce	
Solidcore 6.1.3:Change Control Solidcore 6.1.3:Integrity Monitor		
Name Solidcore 6.1.3:General	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

Enabling an Intelligent Planet

AD\ANTECH

To click "New Policy" for create a test policy

← → 👿 https://win-96bfr04h2p9:8443/PolicyMgm	it/PolicyCatalog.do?prodID=SOLIDCORE_M 🔎 – 🔒 🖒 🤇	🖉 ePolicy Orchestrator 5.1.1 (🗙
Menu 🔻 🛞 Dashboards 🚔 System Tre	e 🎳 Queries & Reports 📃 Policy Catalog	
Policy Policy Catalog New Policy		
Policy Catalog		
Product: Solidcore 6.1.3:Change Control V Pro	duct enforcement status: All enforce	
Category: All Produ	ct policies: Import Export	
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



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:		
	\sim	
Click "OK" to save this policy		
		OK Cancel



Click defined policy

	atalog.do?prodID=SOLIDCORE_M 🔎 🗕 🖒 👿 ePolicy Orch	nestrator 5.1.1 (×		
Menu 🔻 🕥 Dashboards 🚔 System Tree 🎳	Queries & Reports 🔡 Policy Catalog			
Policy Policy Catalog New Policy				
Policy Catalog				
Product: Solidcore 6.1.3:Change Control Product enford Category: Change Control Rules (Windows) Product policies:	rement status: All enforce			
Name	Owner	Assignments	Rule Assignments	Actions
Blank Template	Administrators	None	None	Duplicate
McAfee Default	Administrators	<u>1 assignment</u>	None	Duplicate
test policy	Administrators	None	None	Rename Duplicate Delete Export S



To click "Add" on Write Protect File tab

< ∋	https://win-96bfr04h	2p9 :8443/PolicyMgmt/Po	blicySettings.do?langID=0409&	9&poID=45 🔎 – 🗎 🔿 👿 ePolicy Orchestrator 5.1.1 (🗙	
Menu 🔻	🕥 Dashboards	System Tree	谢 Queries & Reports	Policy Catalog	
Policy Policy	Catalog				
Solidcore 6.1.3	Change Control > C	hange Control Bules (W	indows) > test noticy		

bondeore organistendinge control y change et	ond of functs ()	maons) / cest_pone;						
Rule Groups	Read Protect	Write Protect File	Write Protect Registry	Updaters	Trusted Users			
Filter list	Filter	File					_	
My Rules						 >	Add	
							Edit	
							Remove	



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





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

	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 Co	ntrol Rules (Windows) > test_policy	
Rule Groups	Read Protect Write Protect File Write Protect Registry Updaters Trusted Users	
Filter list	Filter File	
My Rules	Include c:\test.txt	Add
		Edit Remove



• To click "Add" on Write Protect Registry tab

()	https://win-96bfr04h2p9:844	3/PolicyMgmt/Po	blicySettings.do?langlD	=0409&poID=45 🔎 → 🔒 (👌 👿 ePoli	icy Orchestrator 5.1.1 (🗙	
Menu 🔻	🕥 Dashboards 📫	System Tree	Uueries & Re	ports 📃 Policy Cata	log		
Policy Policy	Catalog						
Solidcore 6.1.	3:Change Control > Change	Control Rules (W	indows) > test_polic	y			
Rule Groups		Read Protect	Write Protect File	Write Protect Registry	Updaters	Trusted Users	
Filter list		Filter	Registry	1			
My Rules							Add
							Edit
							Remove



 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: IKEY_LOCAL_MACHINE\BCD0000000\Description × Include C Exclude
OK Cancel



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

	Palia Martin Falia Falia a Tana D. Milian D. K. O A			Ĺ	- 0 x
Menu v 🔘 Dashboards 🚠	System Tree	ePolicy Orchestrator 5.1.1 (, ×		Log Off 🔞	₩ McAfee
Policy	en i Gad				
Policy Catalog					
Solidcore 6.1.3:Change Control > Change Co	ontrol Rules (Windows) > test_policy				
Rule Groups Filter list	Read Protect Write Protect File Write Protect Registry Filter Registry	Updaters Trusted Users			
My Rules	Include HKEY_LOCAL_MACHINE\BCD0000000\/Description		Add		
			Edit		
			HEINUYE		
				Activate Windows	
Add Remove				Go to Action Center to activate Window	#5.
					Save Cancel
📥 🛛 🚞 🍕	6 💣			- Re 19 0	2:53 AM 12/3/2014



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

nu 🔻 🕥 Dashboar	ds 📸 System Tree 🏼 🍓 Q	aueries & Reports 🔛 Policy Catalog				Log Off 🔮 🤍 McJ
tems Section						
stem Tree	New Systems New Subgroups					
m Tree	Systems Assigned Policies	Assigned Client Tasks Group Details Agent Deployment				
Organization	Preset: This Group Only	Customi None 🔻 Duick find:	Apply Cleare	Show selected rows		
ost&Found					Tax and the	
	System Name	Managed State	Tags	IP Address	User Name	Last Communication
	:: (M) (ESLAC	manageo	renasation	19210010014	auministrator	22/014 21/010 AM
	4					
		C Deploy Agents				
		R Modify Policies on a Single System				
		📃 Modify Tasks on a Single System				
		Run Client Task Now				
		Set Description				
		Set Policy & Inheritance				
		Show Agent Log				
	Choose Columna	Show Clant Eventa				
	📃 Export Table	Con Show Threat Events				
	Sig Tag	Contractor Sustaine				
	C Application Control	Transfer by seeins				
	C'i sout	Contraction of the second				Activate Windows
	The open	Wake up Agents			1 0.7	Go to Action Center to activate Windows.
	Directory Management	>				



To select "test_policy" from Policy drop-list

← → 👽 https://win-96bfr04h2p	9:8443/PolicyMgmt/AssignComputerPolicy.do $\mathcal{P} - \stackrel{\frown}{=} \stackrel{\bullet}{\mathcal{O}} ePolicy Orchestrator 5.1.1 (imes and its second seco$
Menu v 🕥 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
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.



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

		L	- 8 ×
+ (=) V https://win-96bfr04b	4h2p92443/Policy.Mgmt/AssignComputePolicy.do 🔎 = 🗎 🖒 🕎 ePolicy Orchestrator 5.1.1 (,,, ×		∩ ★ Ø
Menu v 🕥 Dashboards	r 🚋 System Tree 🏼 🏭 Queries & Reports 🔢 Policy Catalog	Log Off 🔮	♥ McAfee
Systems Section			
Arrian Balicy for Lowtern			
Policy			
	rrödutti <u>Solidoze o.l.s.Champic ultitoti v</u> Categori (Dango Catrito Rules (Windows) √		
	Policy: Itest_policy		
Inheritance:	Reset inhertance Break inhertance		
Messager	Assigning this policy will create new slot on all selected systems. This can result in multiple slot assignments of the same policy.		
		Activate Window Go to Action Center to activo Mindow	05.
			Save Close
🖆 🖉 🔚		- He Sai G	3 12/3/2014



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

enu v 🕥 Dashboards	Hh2p938443/core/ononTab.do/sectionId=Compute	entigmt Statistical D + B C Policy Orchestra ports	tor 3.1.1 (×			Log Off 🔗 🤍 Med
systems Section	New Systems New Subgroups					
tem Tree y Organization	Systems Assigned Policies Assigned Cliv Preset: This Group Only	ent Tasks Group Details Agent Deployment	Ample Class	Show selected rows		
Lost&Found	System Name	Managed State	Taps	IP Address	User Name	Last Communication
	H MCAFEE-CLIENT	Managed	Workstation	192.168.100.2	administrator	12/3/14 2:10:15 AM
	3					
						Activate Windows
						Go to Action Center to activate windows.
n Tree Actions *	Actions • 1 of 1 selected # Wa	ake Up Agents 🗄 Ping				



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

C 🗇 🛡 https://win-96bfr04h2p	88443/ComputerMgmt/prepareWakeup.do?onion.user.securit 🔎 = 🖴 🖸 🐺 ePolicy Orchestrator 5.1.1 ("			∩ ★ ©
Menu 🔻 🕥 Dashboards	💑 System Tree 🍓 Queries & Reports 🔢 Policy Catalog	Log Off	0	♥ McAfee
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 sakerup call, go to the Server Task Log.			
Target systems:	NCAFEE-CLIENT			
Wake-up call type:	Apent Wale-Up Call SuperApent Wale-Up Call			
Randomization:	0 minutas			
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 © for continuous attempts.)			
Retry interval:	30 [second(s)]			
Abort after:	5 minute(s)			
Wake up Agent using:	Al Agent Handlers Land Connected Agent Handler Selected Agent Handler:			

	ОК Сом
📕 🛛 🚞 🍕 🙆	 ▶8 3 (a) 1×8 AM ▶10 3 (b) 1×12/2/14





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





Solidcore Events

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

							- 0	x
	3/ComputerMgmt/showManagedSystemHor	ne.do?orior 🔎 = 🔒 🖉 🦞 ePolicy Orches	strator 5.1.1 (×				0	★ ₽
Menu 🔻 🕥 Dashboards 📫	System Tree 🏾 🎳 Queries & Reports	Policy Catalog					Log Off 🕜 🤍 Mc	Afee
Recent Pages	Reporting	Systems Section	Policy					
System Tree	🕥 Dashboards	📩 System Tree	Policy Catalog					
Policy Catalog	谢 Queries & Reports	Tag Catalog	Policy Assignments					
O Dashboards	Threat Event Log		Noticy Assignment Rules	Show selected				
Server Settings	McAfee Labs		1 Policy Comparison	IP	Address	User Name	Last Communication	
Queries & Reports	Solidcore Events		Client Task Catalog	15	92.168.100.4	administrator	12/3/14 2:10:15 AM	~
Page Description	Solidcore Alerts		灵 Client Task Assignments					
Solidcore Events	Content Change Tracking		🐚 Client Task Comparison					
events.	Software	Automation	User Management					
	Product Deployment	Separ Task Lon	22 Uters					
	Software Manager	Server Tasks	A Remission Sets					
	Master Repository	Automatic Responses	audit Los					
	Distributed Reportanian		Contractor					
	Distributed Repusitories	Calidana Client Tark Lan	Contacts					
	Extensions	Solidcore Client Task Log						
	Licensing							
	Configuration	Application Control						
	Server Settings	inventory						
	Personal Settings	Image Deviation						
	Registered Servers	Policy Discovery						
	💭 Magent Handlers							
ePO Build: ePolicy Orchestrator 5.1.1 (Build: 357)	Registered Executables							
Time: 12/3/14 2:56:49 AM PST User: admin	Solidcore Rules							
							AAGe of except	
						Go to Act	e WINDOWS Ion Center to activate Windows.	~
System Tree Actions Act	ions 🔻 1 items	Jp Agents # Ping						
							- Ris 🕼 🕼 3:00	AM 2014

Enabling an Intelligent Planet

AD\ANTECH

Solidcore Events

Solidcore Events will be used to record and audit

						- 0 ×
(C) 🔍 🔍 https://win-96bfr0	4h2p9:8443/core/orionTab.do?sectionId=orion.report&tab	bld=scor: 🔎 👻 🖨 🖉 🤠 ePolicy Orchestrator 5.1.1	(×			n 🛧 0
Menu 🔻 🕥 Dashboards	s 🚓 System Tree 🍓 Queries & Reports	Policy Catalog				Log Off 😧 🤍 McAfee
Reporting						
Solidcore Event	s					
System Tree	Filter					
My Organization	Time Filter			System Tree Filter This G	iroup Only	
	Advanced Filters					
	Solidcore Events					Options 🔻
	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	Di\Sleepervexe	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	
	1					
					Act	ivate Windows
	Select all in this page	I pages			Got	o Action Center to activate Windows
	Actions *					
						The Street 3:02 AM
	14 G					* 1 3 149 12 12/3/2014

