



PRODUCT BULLETIN NO. 2866

CONFIGURING EPOLICY ORCHESTRATOR 3.0 AND MCAFEE 8.0i WITH CISCO CALLMANAGER

Cisco® CallManager runs on a Windows2000 server. An important administrative task for server management is antivirus software. Enterprise tools such as ePolicy Orchestrator from McAfee have been developed to ensure antivirus software is effective across an entire enterprise. These tools can inventory, audit, and bring into compliance machines across an enterprise. Cisco Systems® has supported McAfee antivirus software running co-resident on Cisco CallManager for some time. Cisco now supports McAfee ePolicy Orchestrator agent running on Cisco CallManager servers.

This document outlines the procedures to configure McAfee ePolicy Orchestrator (ePO) 3.5 and McAfee 8.0i on a Cisco CallManager Media Convergence Server (MCS). This document assumes ePO agent and McAfee are installed on the Cisco CallManager server and that ePolicy Orchestrator is installed on a separate machine.

The high-level steps for setting up the ePO server and workstation policies for the Cisco CallManager servers follow:

1. Disable ScriptScan.
2. Disable Trace File Scanning.
3. Disable Scanning for Windows Protected Files.
4. Disable Heuristics Scanning.

The high-level steps for scheduling a reoccurring scan of a Cisco CallManager server follow:

1. Disable Inheriting of policies.
2. Set the scan to run during off-peak hours.
3. Exclude Trace File Scanning.
4. Exclude scanning of Windows Protected Files.
5. Disable Heuristics Scanning and set the maximum system usage to 10 percent.

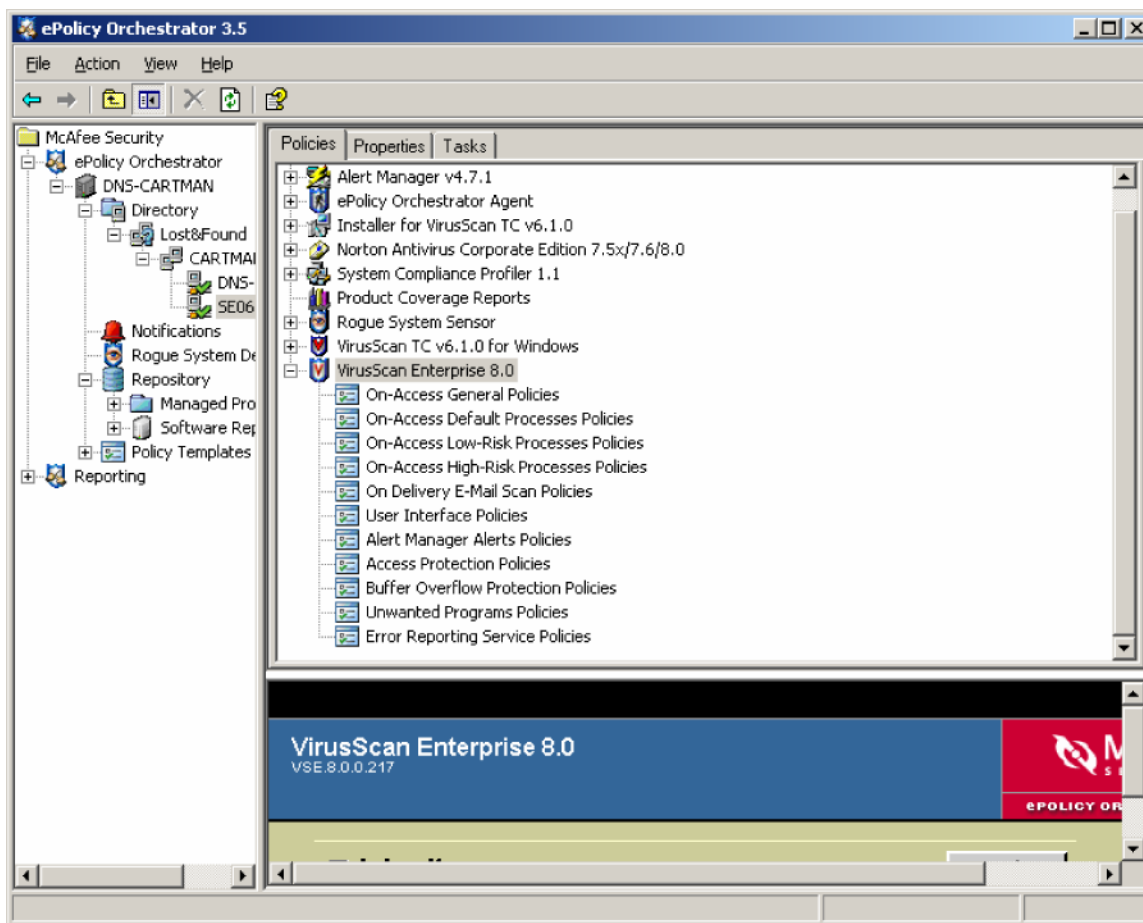
If these steps are not followed correctly, system performance and call-processing capabilities could be impacted.

EPO CONFIGURATION

The following steps modify the policy configuration with ePO (Figure 1).

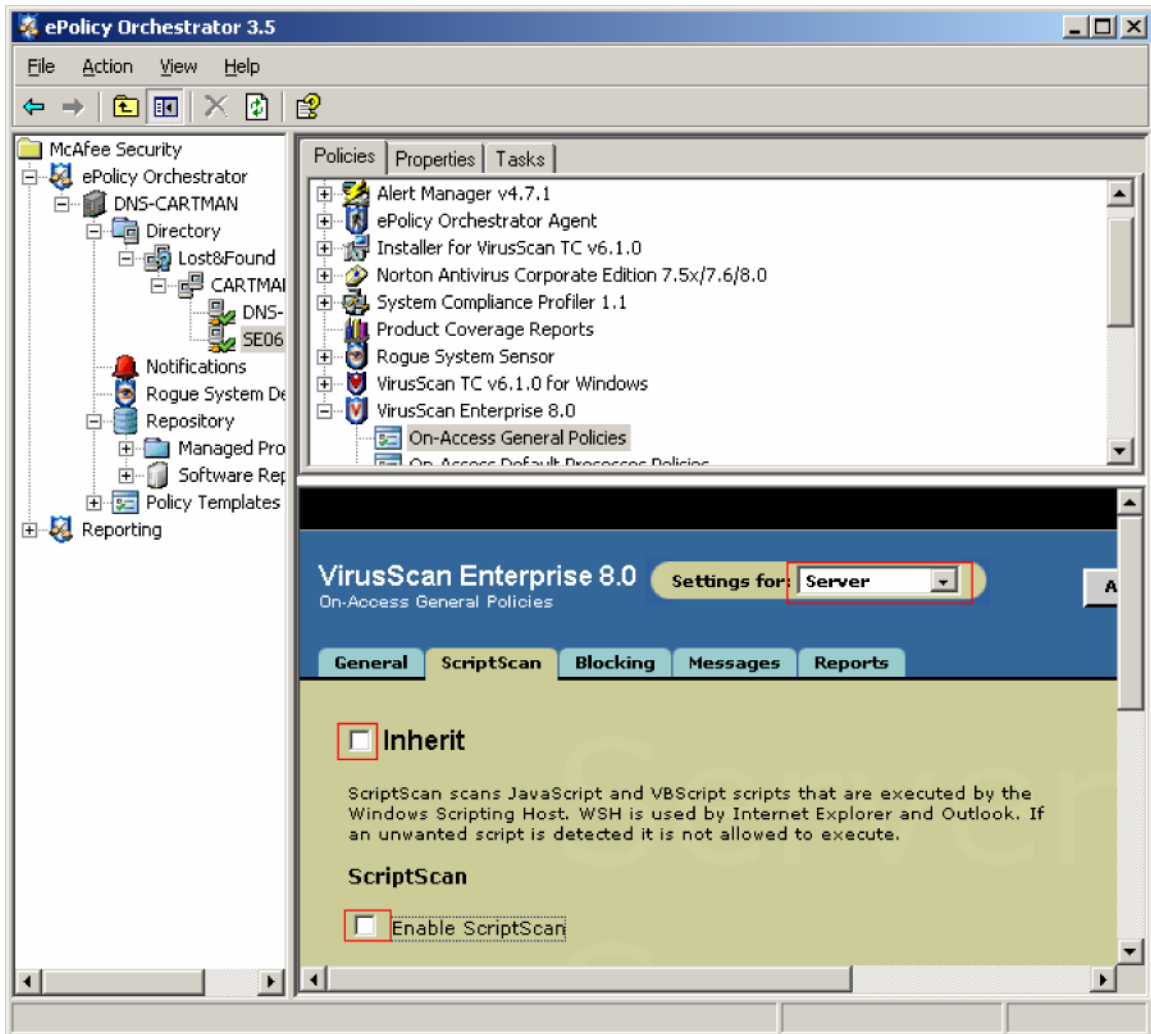
1. Open ePO and log in.
2. Expand Directory, Lost&Found, and the Server Group.
3. Select the Cisco CallManager server.
4. In the right window pane, select the Policies tab and Expand the VirusScan Enterprise 8.0 Policy group.

Figure 1. ePolicy Orchestrator 3.5



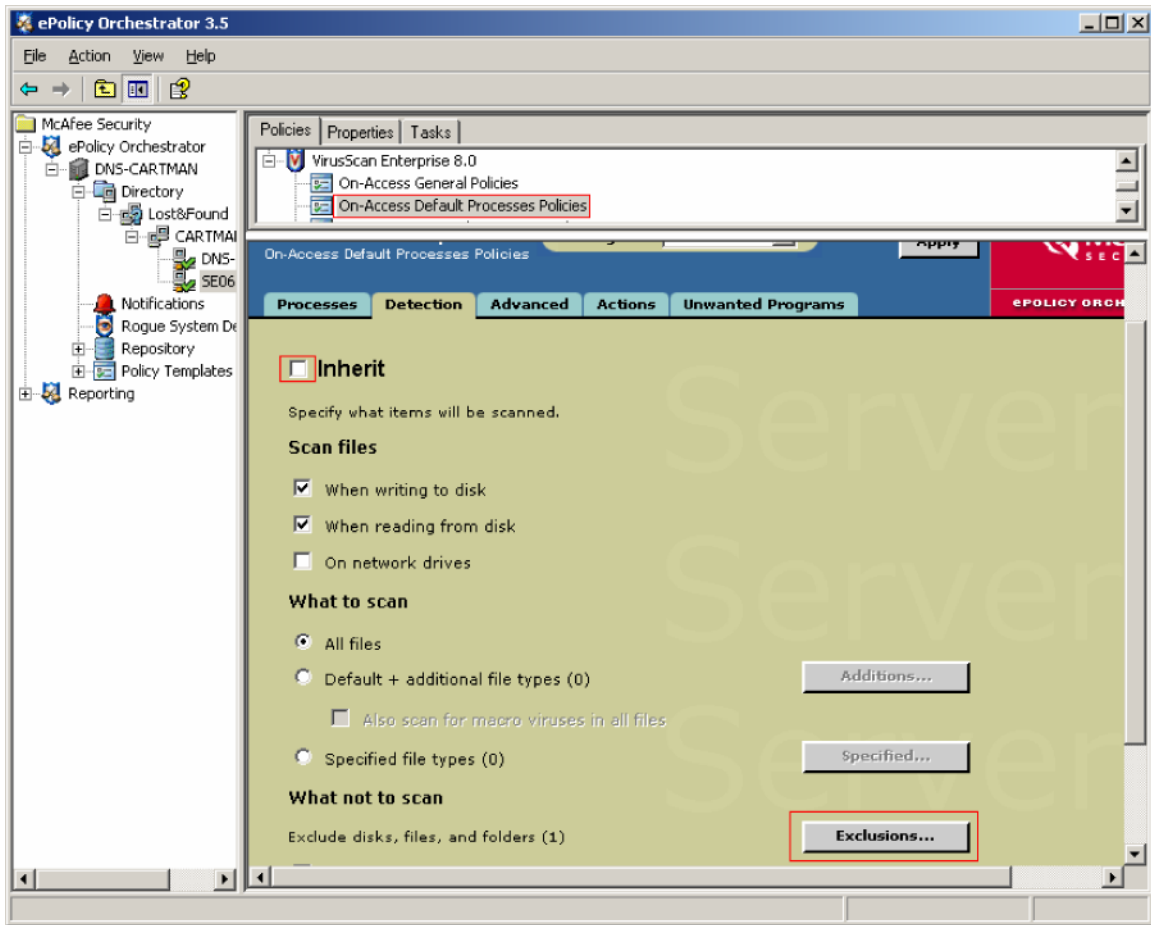
5. Select On-Access General Policies. The window pane shown in Figure 2 will refresh with Configuration Options.
6. In the Settings for: drop-down menu, select Server.
7. Select the Script Scan tab from the Configuration Choices menu.
8. In the Script Scan tab, uncheck Inherit and then uncheck the Enable ScriptScan check box.

Figure 2. VirusScan Enterprise 8.0 Server Settings



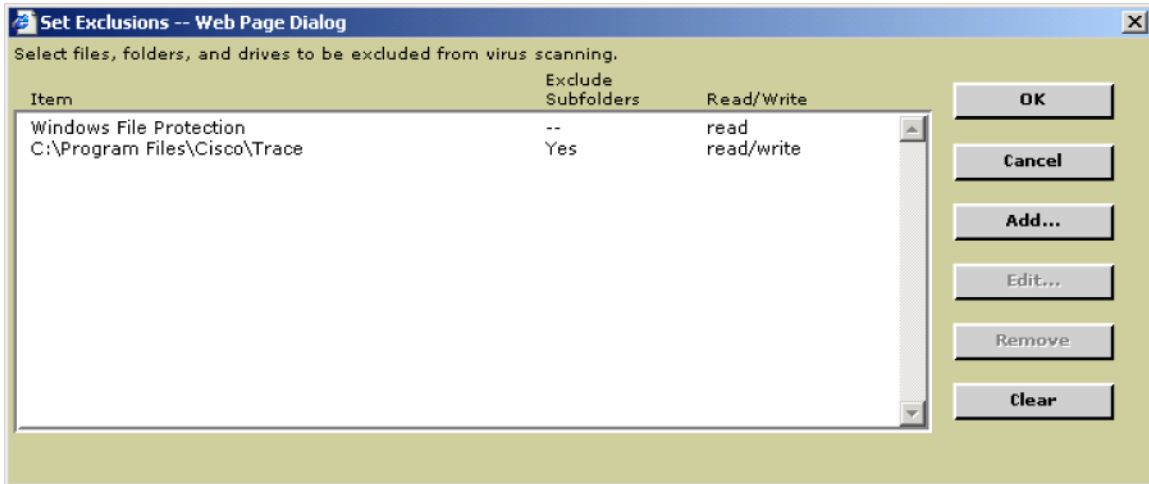
9. Repeat this process for the Workstation selection in the Settings for: drop-down menu.
10. Next, Click on On-Access Default Processes Policies.
11. Select Server in the Settings for: drop-down menu.
12. Click on the Detection tab.
13. Uncheck the Inherit check box and click on the Exclusions button.

Figure 3. Default Detection Properties



14. The files and folders shown in Figure 4 should be excluded from On-Access scanning.

Figure 4. Scan Exclude List



15. To add the files and folders, Click the Add button and type the text shown in Figure 5, clicking OK after each addition. Also exclude all Windows protected files as in Figure 6. Be sure to check the Exclude Subfolders check box.

Figure 5. Trace Files Exclusion

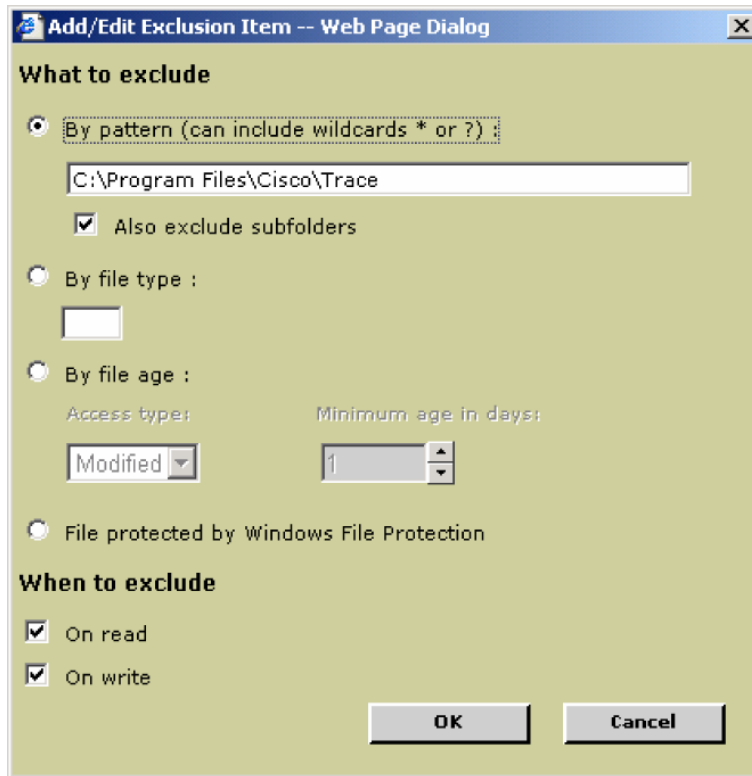
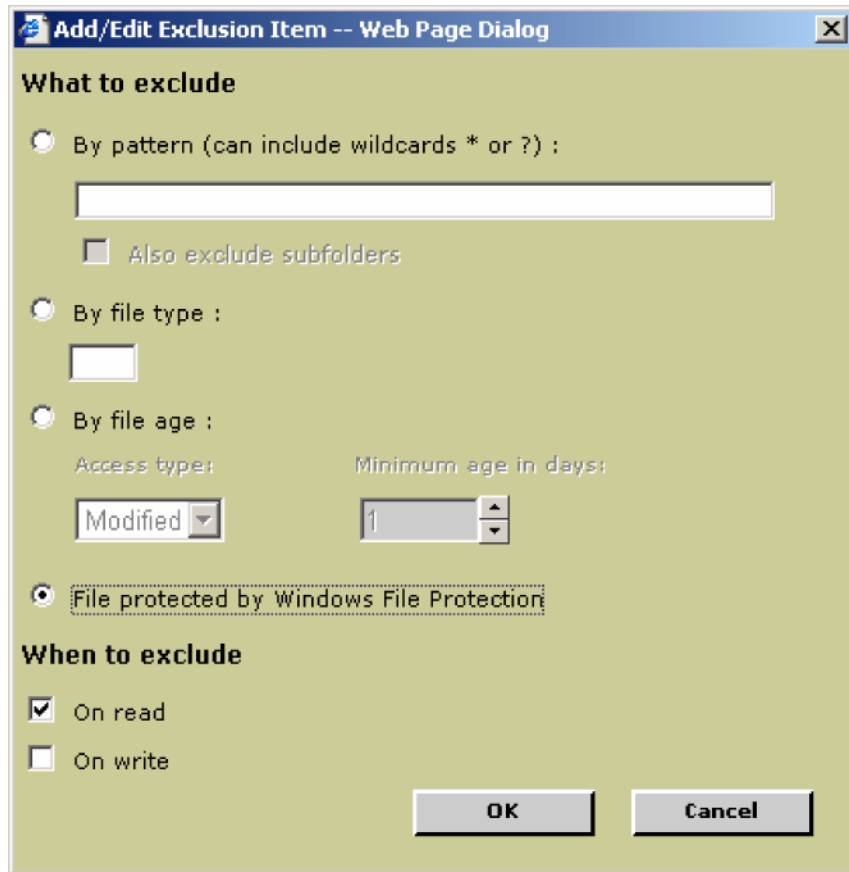
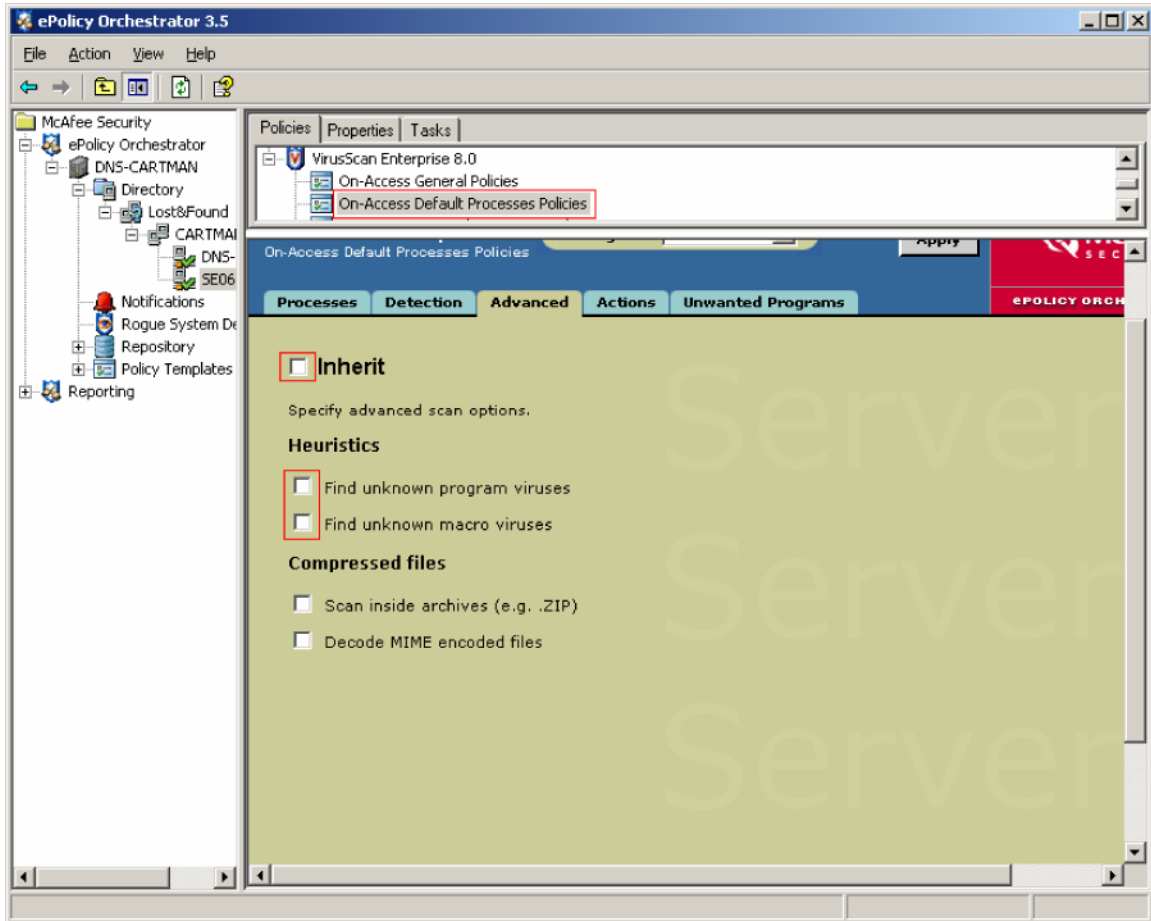


Figure 6. Windows Protected Files Exclusion



16. Next click the Advanced tab. Uncheck Inherit and any boxes that are checked so it looks like the window shown in Figure 7.

Figure 7. Advanced Tab



17. Click Apply to write the changes.

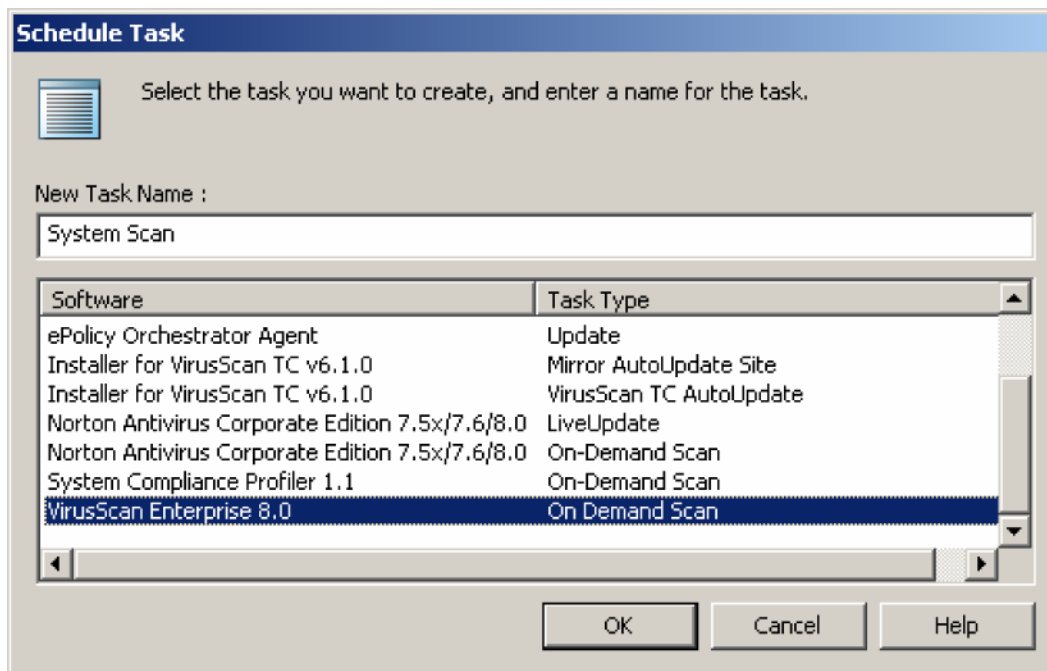
18. Repeat steps 13–18 for the Workstation selection in the Settings for: drop-down menu.

SYSTEM SCAN CONFIGURATION

The following steps are used if a system scan will be scheduled in ePO:

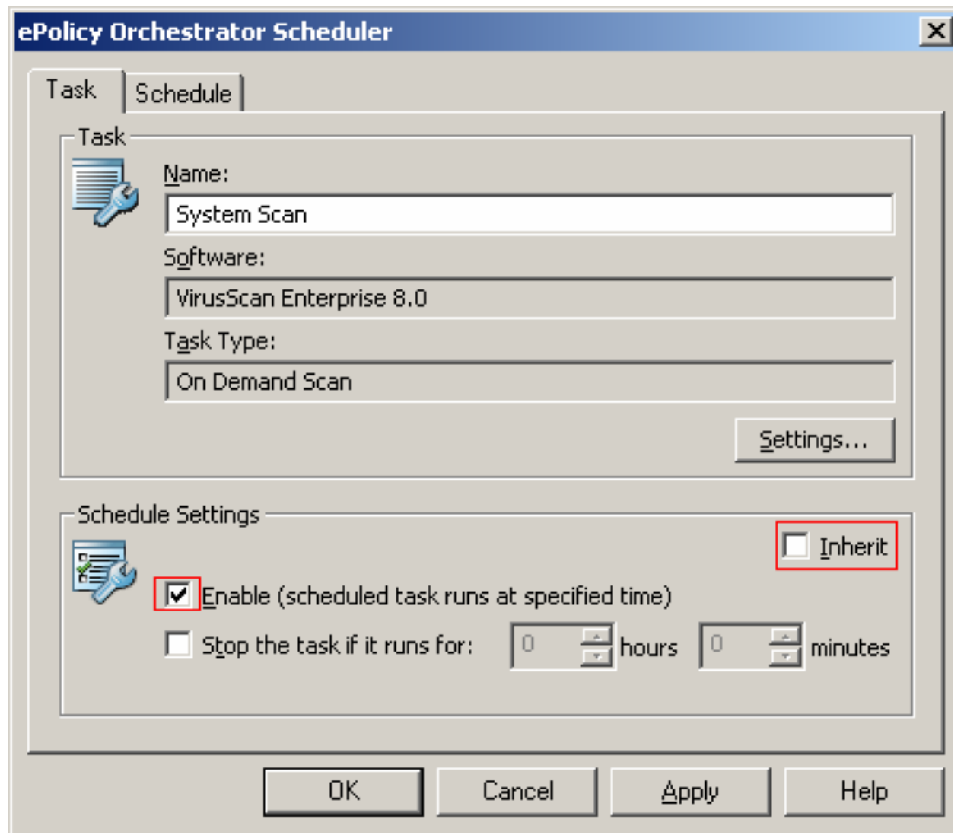
1. Select the Cisco CallManager server in the left pane, and then select the Tasks tab in the right window pane.
2. Right click in the Task pane and choose Schedule Task...
3. Name the scan task and choose VirusScan Enterprise 8.0 On-Demand Scan from the selections (Figure 8) and Click OK.

Figure 8. Scheduling System Scans



4. Uncheck the Inherit check box and check the Enable check box to enable this task (Figure 9).

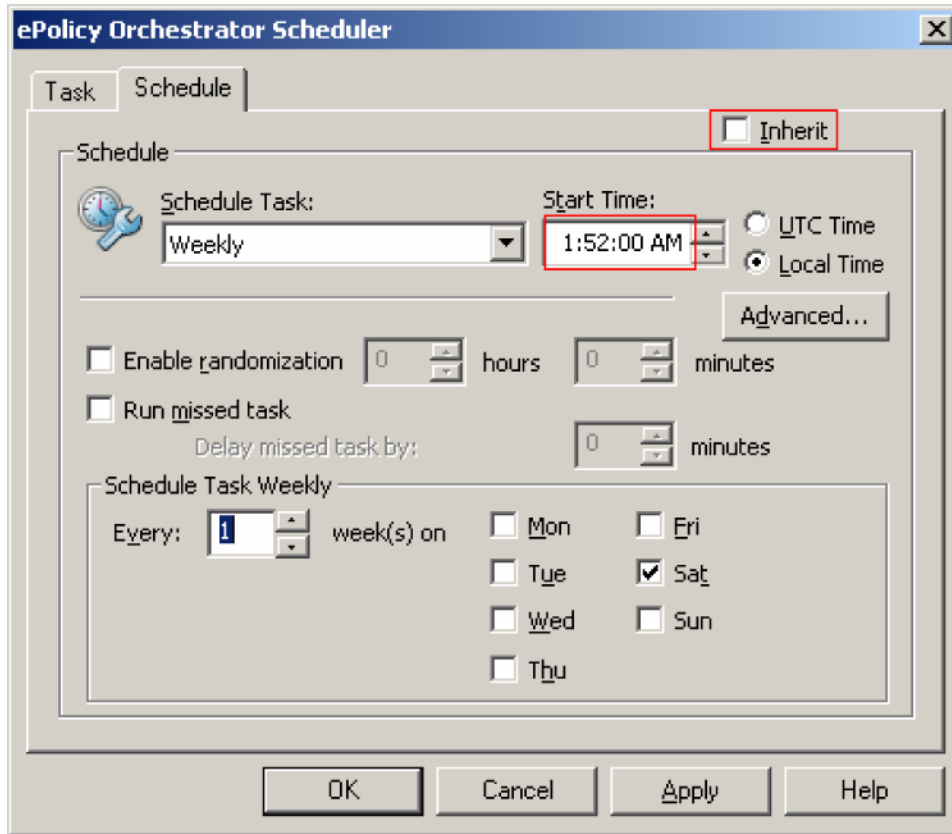
Figure 9. Schedule Settings



5. Click on the Schedule tab.

6. Uncheck the Inherit check box. Set the scan to run at off-peak hours so it does not negatively impact Cisco CallManager performance (Figure 10).

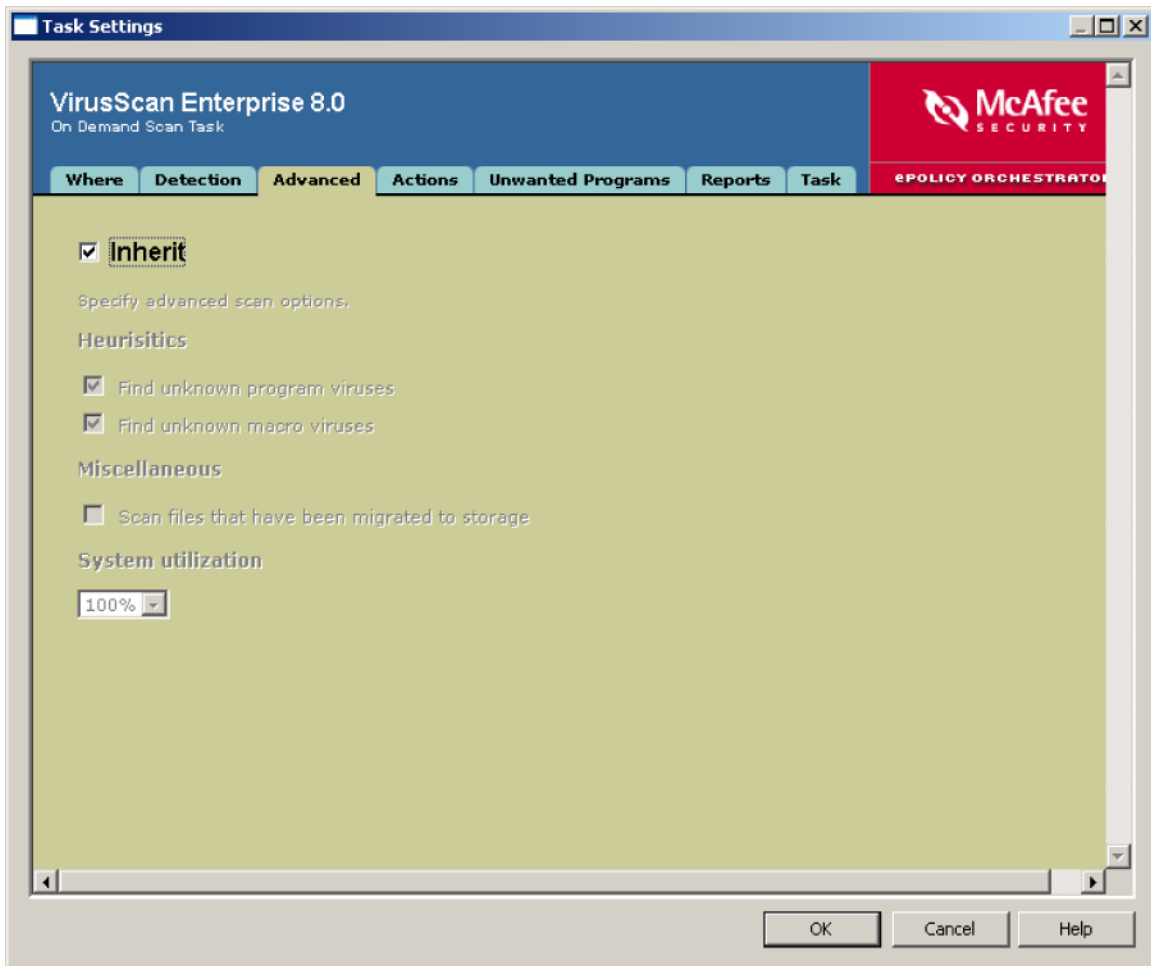
Figure 10. Scan Schedule



7. Click Apply.
8. Click on the Task tab again and select Settings.
9. Next, click on the Detection tab and uncheck Inherit.
10. Click on the Exclusions button and set the Exclusions outlined in step 16.
11. Click on the Advanced tab.

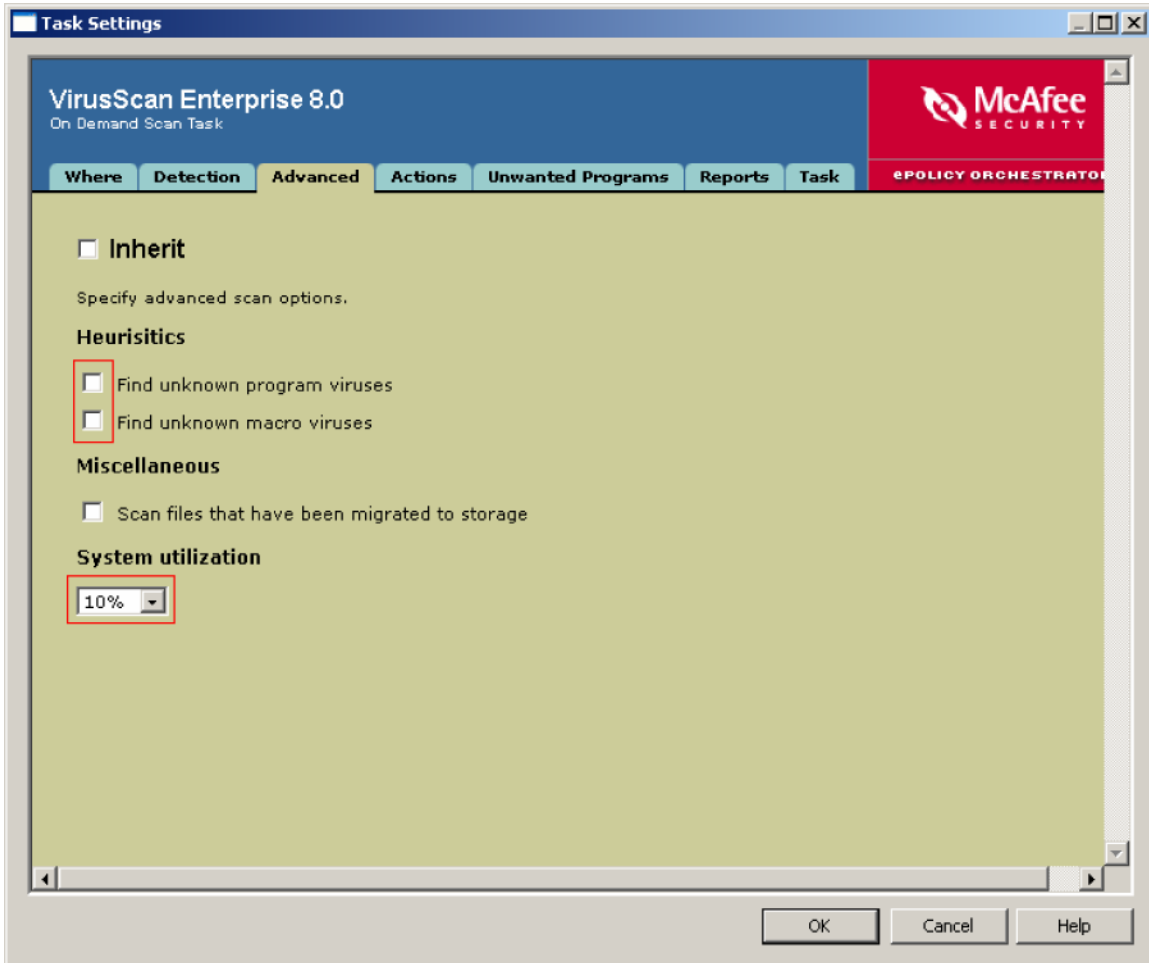
12. Figure 11 shows the default settings.

Figure 11. Default Settings



13. Change the Default setting to appear as Figure 12. and click OK.

Figure 12. Scheduled Scan Default Settings



14. Click Apply, and then OK to save the changes to the task.

Figure 13 is a screenshot of the processes loaded on the Cisco CallManager server when using ePO agent and McAfee Antivirus. Seven new processes are added to the Cisco CallManager server.

Figure 13. Windows Process Listing

Image Name	PID	CPU	CPU Time	Mem Usage
DCX500.EXE	896	00	0:00:38	122,516 K
DLLHOST.EXE	828	00	0:00:19	12,940 K
DLLHOST.EXE	924	00	0:00:00	5,896 K
explorer.exe	3368	00	0:00:23	6,120 K
FrameworkService	1064	00	0:01:29	12,864 K
inetinfo.exe	1860	00	0:01:33	35,744 K
InsertCDR.exe	2192	00	0:00:06	11,188 K
LLSSRV.EXE	1032	00	0:00:00	2,252 K
logread.exe	2476	00	0:00:01	6,204 K
LSASS.EXE	304	00	0:00:26	15,108 K
Mcshield.exe	1188	00	0:06:37	28,472 K
msdtc.exe	608	00	0:00:00	6,012 K
naPrdMgr.exe	1440	00	0:01:15	600 K
ntpd.exe	1484	00	0:00:00	3,248 K
regsvc.exe	1588	00	0:00:00	1,216 K
scardsvr.exe	1596	00	0:00:00	1,344 K
ServiceabilityR	740	00	0:00:14	23,264 K
SERVICES.EXE	292	00	0:00:11	15,372 K
shstat.exe	3488	00	0:00:04	728 K
SMSS.EXE	216	00	0:00:00	388 K
SNMP.EXE	1628	00	0:00:01	15,888 K
sqlagent.exe	2224	00	0:00:04	4,680 K
sqlmangr.exe	3536	00	0:00:00	4,732 K
sqlservr.exe	1432	00	0:04:11	183,268 K
svchost.exe	576	00	0:00:18	4,848 K
svchost.exe	996	00	0:00:00	6,580 K
svchost.exe	3656	00	0:00:00	3,768 K
sysdown.exe	1900	00	0:00:00	2,380 K
System	8	00	0:01:05	220 K
System Idle Process	0	99	38:11:56	16 K
TASKMGR.EXE	1176	00	0:00:00	2,788 K
TBMon.exe	3504	00	0:00:00	1,528 K
termsrv.exe	408	00	0:00:00	3,452 K
tomcat.exe	872	00	0:00:48	44,076 K
UpdaterUI.exe	3480	00	0:00:00	2,772 K
WsTskMgr.exe	1208	00	0:00:24	448 K
WINLOGON.EXE	236	00	0:00:13	3,048 K
WinMgmt.exe	1680	00	0:00:53	980 K

Processes: 46 CPU Usage: 0% Mem Usage: 744188K / 5837156K

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205215.ba_ETMG_SK_4.05