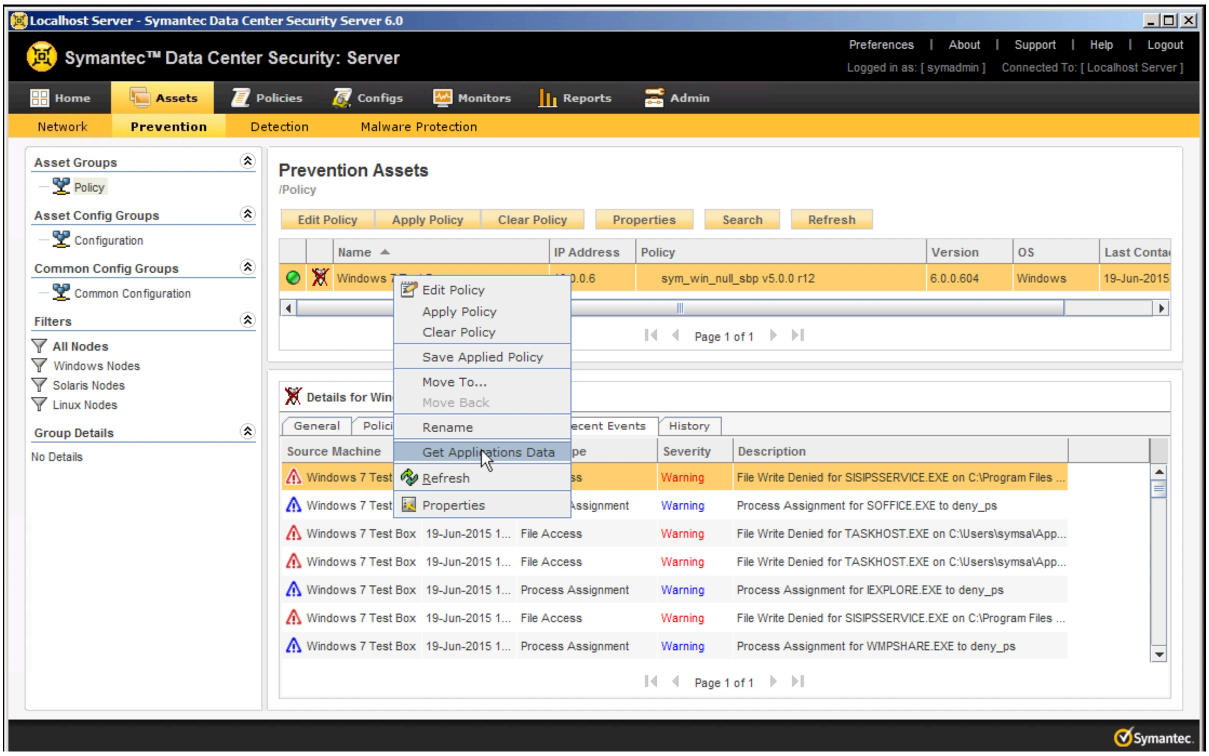
DCS Application Whitelisting Guide

June 18, 2015

1. Select the asset that you wish to begin application whitelisting and begin an inventory of software by right clicking and selecting Get applications data.

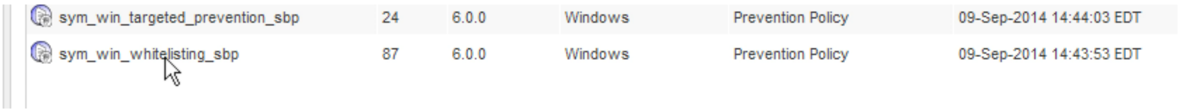


Prevention Assets
/Policy

		Name	IP Address	Policy	Version	OS	Last Conta
●		Windows 7	0.0.6	sym_win_null_sbp v5.0.0 r12	6.0.0.604	Windows	19-Jun-2015

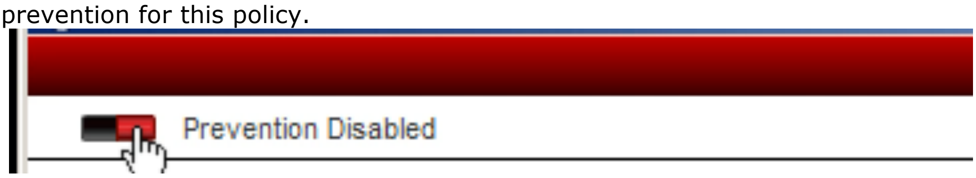
Source Machine		pe	Severity	Description
Windows 7 Test		ss	Warning	File Write Denied for SISIPSSERVICE.EXE on C:\Program Files ...
Windows 7 Test		Assignment	Warning	Process Assignment for SOFFICE.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for TASKHOST.EXE on C:\Users\symsa\App...
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for TASKHOST.EXE on C:\Users\symsa\App...
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for SISIPSSERVICE.EXE on C:\Program Files ...
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for WMPSHARE.EXE to deny_ps

2. Navigate to the policies tab and locate the sym_win_whitelisting policy. Copy it to the local workspace folder and rename it to your desired policy name. After complete, drag the policy to the required Workspace folder.

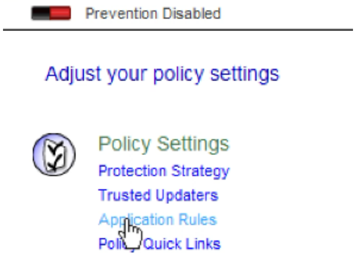


sym_win_targeted_prevention_sbp	24	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:44:03 EDT
sym_win_whitelisting_sbp	87	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:43:53 EDT

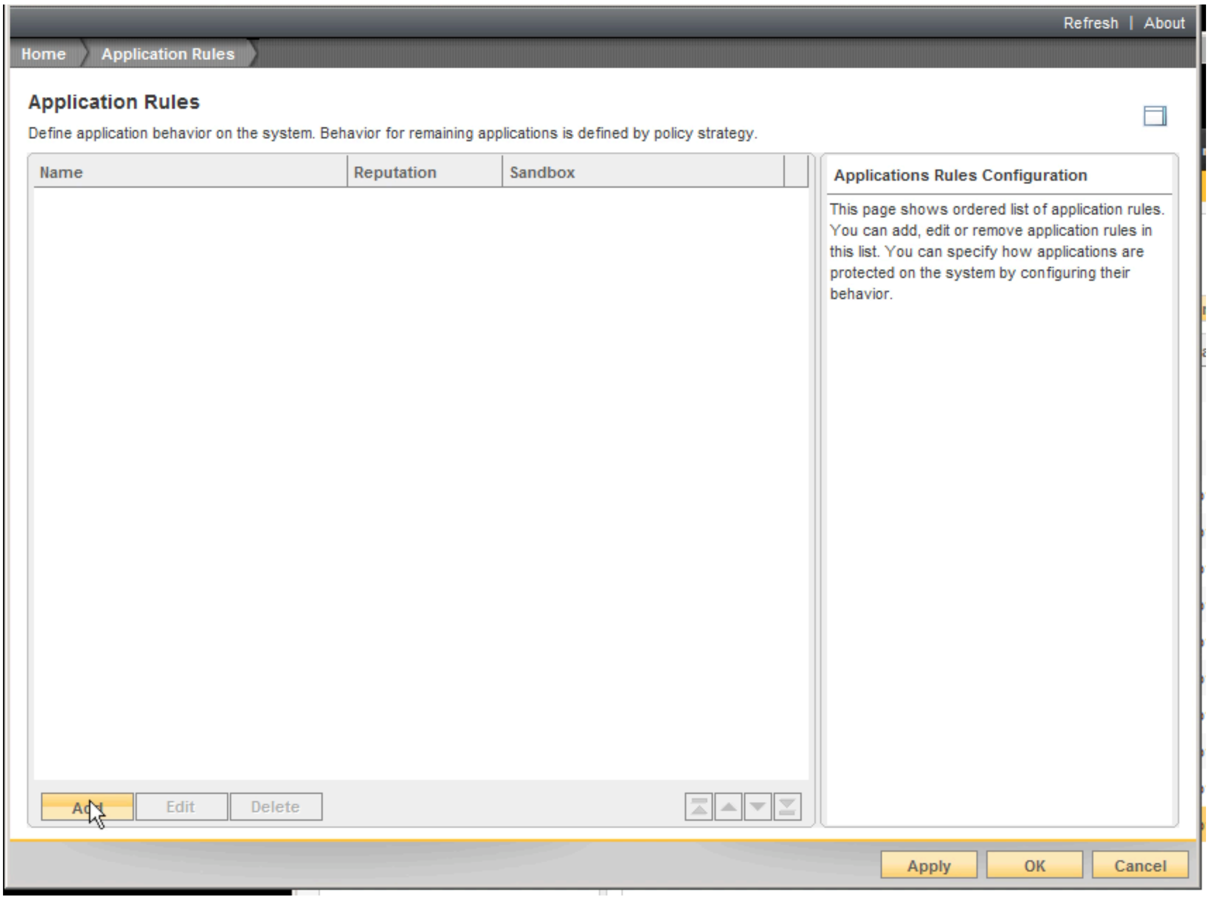
3. Navigate to the required Workspace folder and open the new policy and immediately disable prevention for this policy.



4. Select Application Rules.



5. Click add.



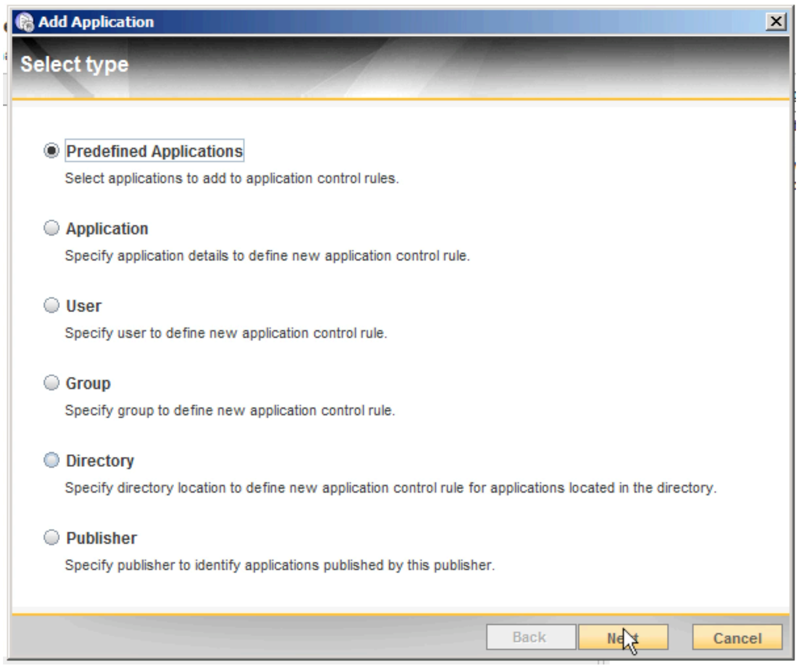
Application Rules

Define application behavior on the system. Behavior for remaining applications is defined by policy strategy.

Applications Rules Configuration

This page shows ordered list of application rules. You can add, edit or remove application rules in this list. You can specify how applications are protected on the system by configuring their behavior.

6. Select predefined applications and click next.



Add Application

Select type

● Predefined Applications
Select applications to add to application control rules.

○ Application
Specify application details to define new application control rule.

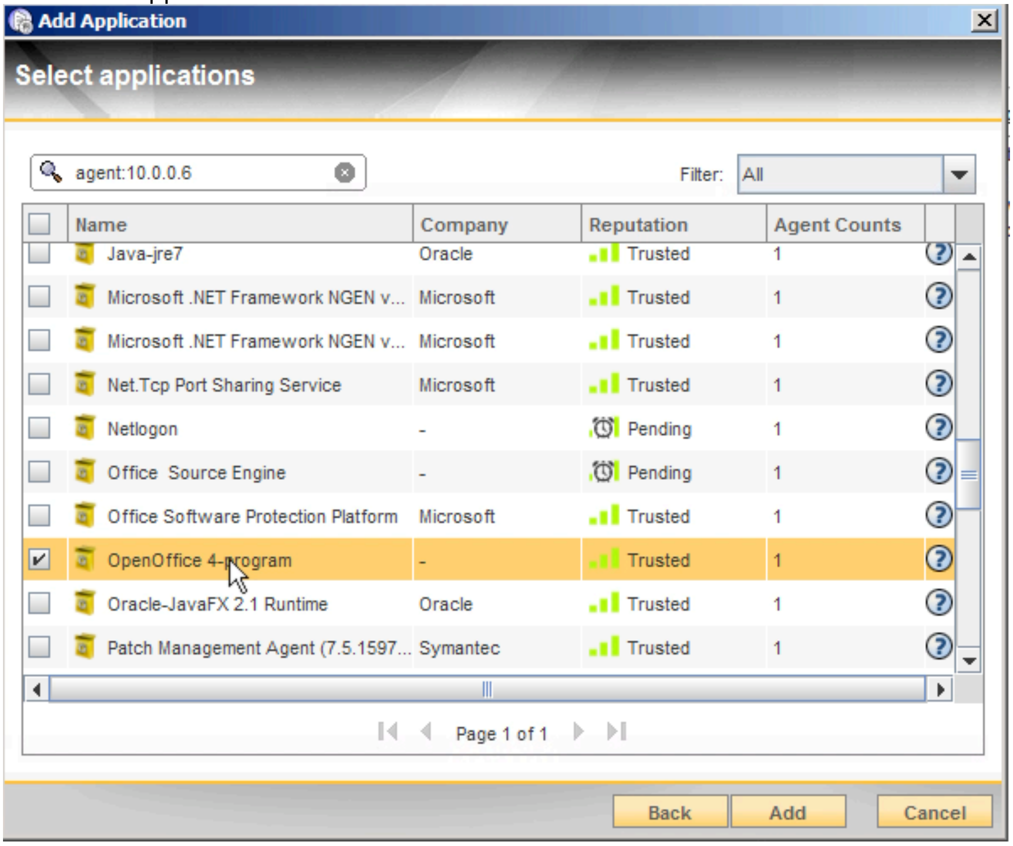
○ User
Specify user to define new application control rule.

○ Group
Specify group to define new application control rule.

○ Directory
Specify directory location to define new application control rule for applications located in the directory.

○ Publisher
Specify publisher to identify applications published by this publisher.

7. Type agent:%IP_ADDRESS% in the search bar to filer the list of applications to only those installed on the client you are whitelisting. In this example, OpenOffice is selected. Click Add to create the application rule.



Add Application

Select applications

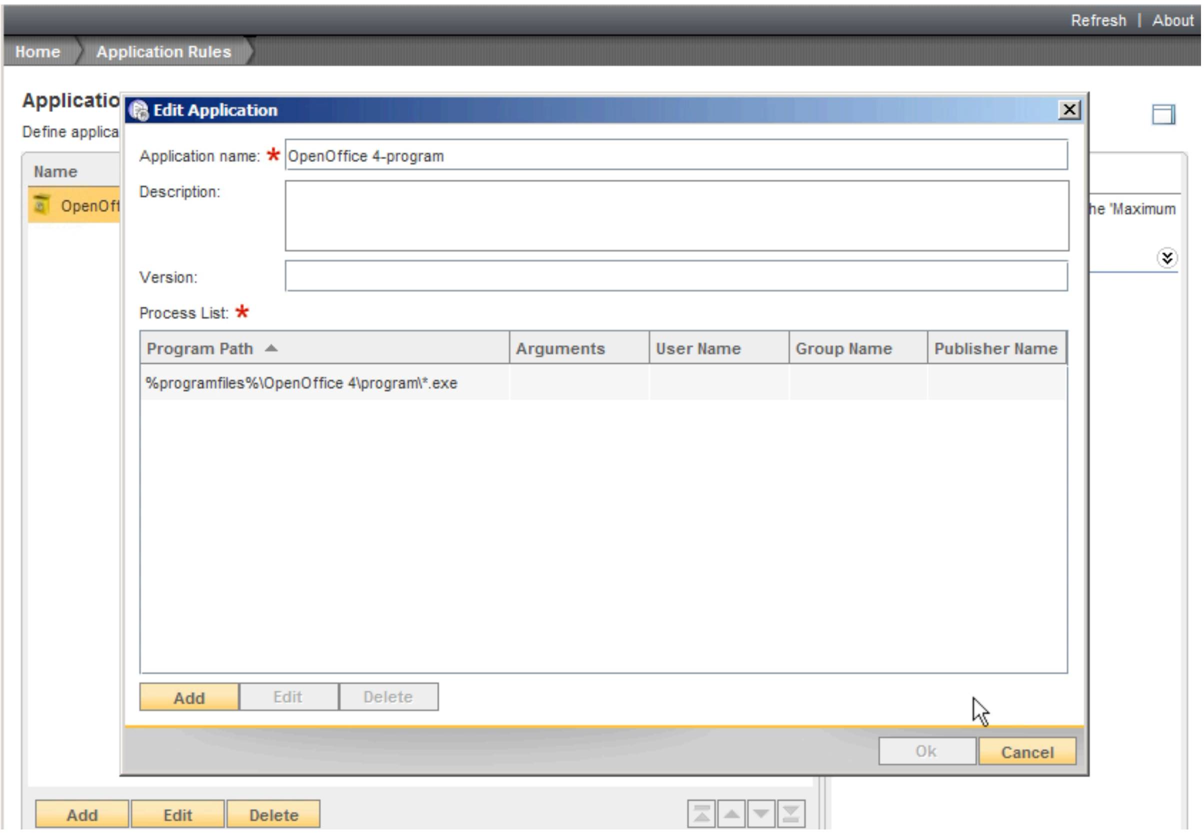
agent:10.0.0.6

Filter: All

□	Name	Company	Reputation	Agent Counts
□	Java-jre7	Oracle	Trusted	1
□	Microsoft .NET Framework NGEN v...	Microsoft	Trusted	1
□	Microsoft .NET Framework NGEN v...	Microsoft	Trusted	1
□	Net.Tcp Port Sharing Service	Microsoft	Trusted	1
□	Netlogon	-	Pending	1
□	Office Source Engine	-	Pending	1
□	Office Software Protection Platform	Microsoft	Trusted	1
☑	OpenOffice 4-program	-	Trusted	1
□	Oracle-JavaFX 2.1 Runtime	Oracle	Trusted	1
□	Patch Management Agent (7.5.1597...	Symantec	Trusted	1

Page 1 of 1

8. Double click the new application rule to review the contents.



Application name: * OpenOffice 4-program

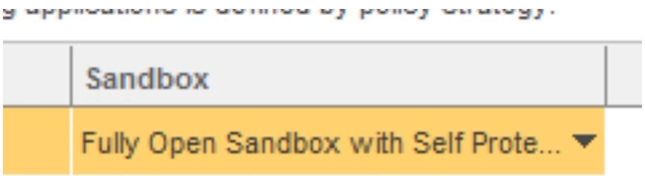
Description:

Version:

Process List: *

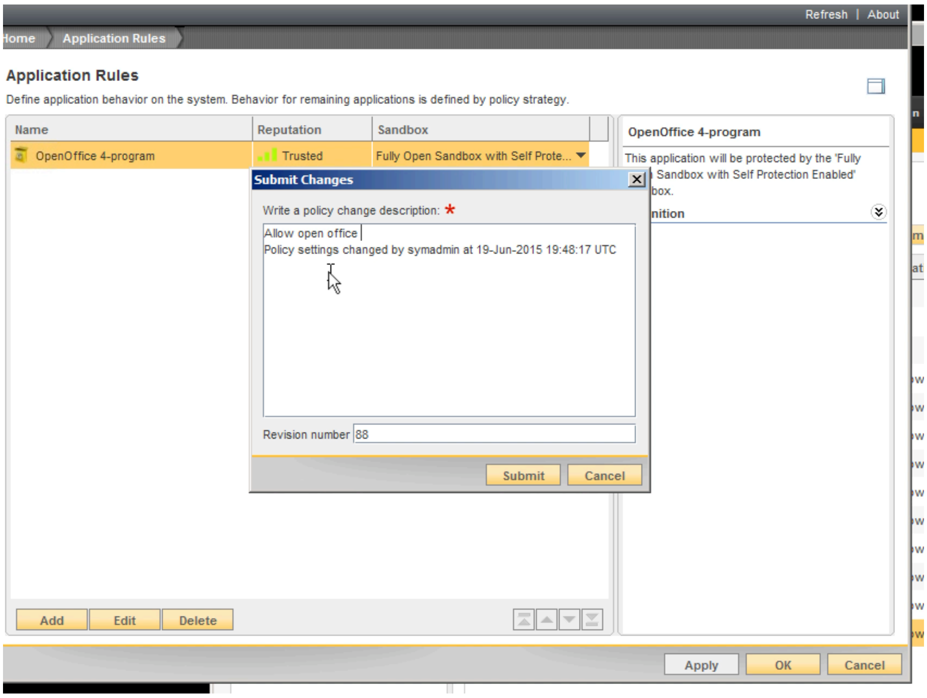
Program Path	Arguments	User Name	Group Name	Publisher Name
%programfiles%\OpenOffice 4\program\*.exe				

9. Change the sandbox type to “Fully open sandbox with self protection enabled”.



Sandbox
Fully Open Sandbox with Self Prote...

10. Commit change by selecting Apply and type the relevant notes. Click Submit and then click OK to exit the policy editing window.



Application Rules

Define application behavior on the system. Behavior for remaining applications is defined by policy strategy.

Name	Reputation	Sandbox
OpenOffice 4-program	Trusted	Fully Open Sandbox with Self Prote...

OpenOffice 4-program

This application will be protected by the 'Fully … Sandbox with Self Protection Enabled' …box.

Submit Changes

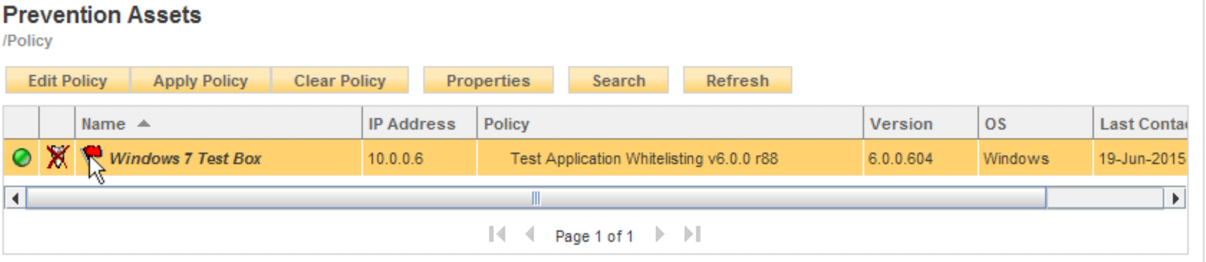
Write a policy change description: *

Allow open office

Policy settings changed by symadmin at 19-Jun-2015 19:48:17 UTC

Revision number 88

11. Apply newly modified policy to required assets and ensure the policy is applied.

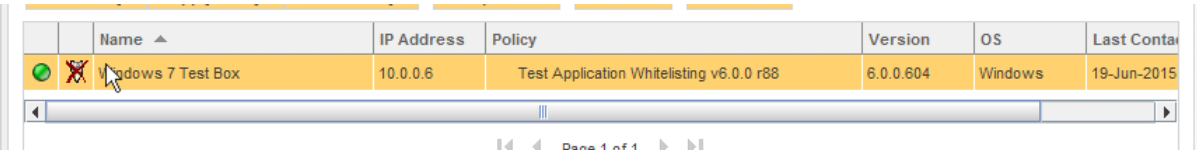


Prevention Assets

/Policy

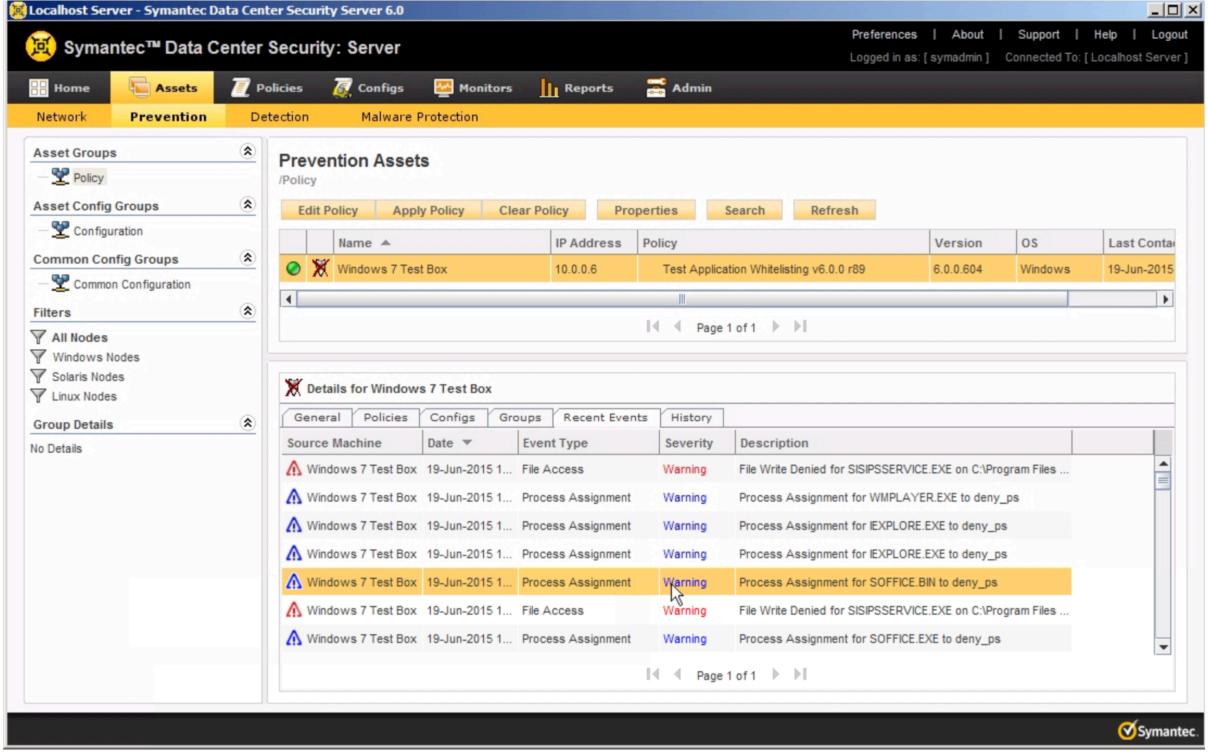
		Name	IP Address	Policy	Version	OS	Last Conta
●	☒	Windows 7 Test Box	10.0.0.6	Test Application Whitelisting v6.0.0 r88	6.0.0.604	Windows	19-Jun-2015

Absence of red flag indicates policy has been applied successfully.



		Name	IP Address	Policy	Version	OS	Last Conta
●	☒	Windows 7 Test Box	10.0.0.6	Test Application Whitelisting v6.0.0 r88	6.0.0.604	Windows	19-Jun-2015

12. Test the new whitelisting policy for a period of time before enabling prevention by logging in to the required asset and working normally for a while. This will generate events in the management console. After some time, log in to the management server and select the assets tab. In the lower right section of the interface, select the recent events tab. This will display the detections. Detections in blue will be denied and be red once prevention has been enabled.



Prevention Assets
/Policy

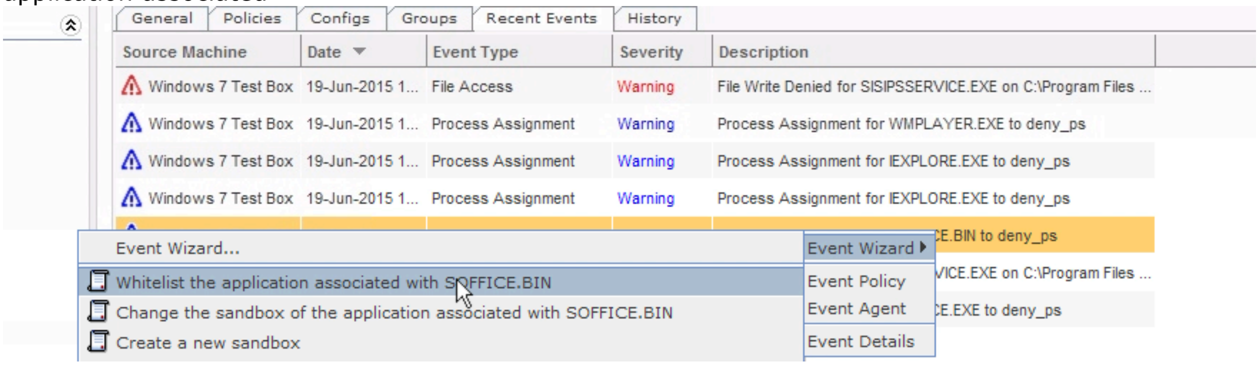
		Name	IP Address	Policy	Version	OS	Last Conta
●		Windows 7 Test Box	10.0.0.6	Test Application Whitelisting v6.0.0 r89	6.0.0.604	Windows	19-Jun-2015

Details for Windows 7 Test Box

Source Machine	Date	Event Type	Severity	Description
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for SISIPSSERVICE.EXE on C:\Program Files ...
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for WMPLAYER.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for SOFFICE.BIN to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for SISIPSSERVICE.EXE on C:\Program Files ...
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for SOFFICE.EXE to deny_ps

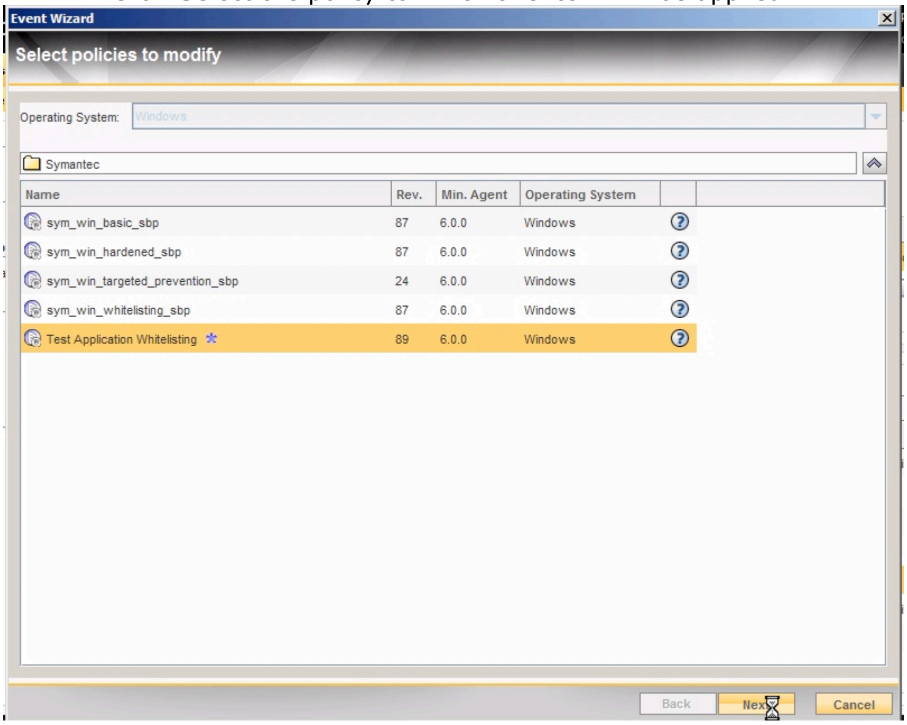
13. Sometimes, gathering application data is not sufficient for an effective whitelisting policy, and you may review the processes that will be blocked/fine tune application rules before enabling prevent to ensure that allowed processes are not blocked. For example, although the get application data option was able to detect the executable data for Open Office (*.exe), it was unable to detect SOFFICE.BIN, a required binary file for the application to run. To effectively allow the application to be whitelisted, simply add another entry to the application rules in the whitelisting policy. To whitelist an application, simply right click and select "Event Wizard" and then "Whitelist the application associated with %FILENAME%".

13.a Right click application detected for deny and click event wizard->whitelist the application associated



Source Machine	Date	Event Type	Severity	Description
Windows 7 Test Box	19-Jun-2015 1...	File Access	Warning	File Write Denied for SISIPSSERVICE.EXE on C:\Program Files ...
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for WMPLAYER.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps
Windows 7 Test Box	19-Jun-2015 1...	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps
				E.BIN to deny_ps
				VICE.EXE on C:\Program Files ...
				E.EXE to deny_ps

13.b Select the policy to which this item will be applied.

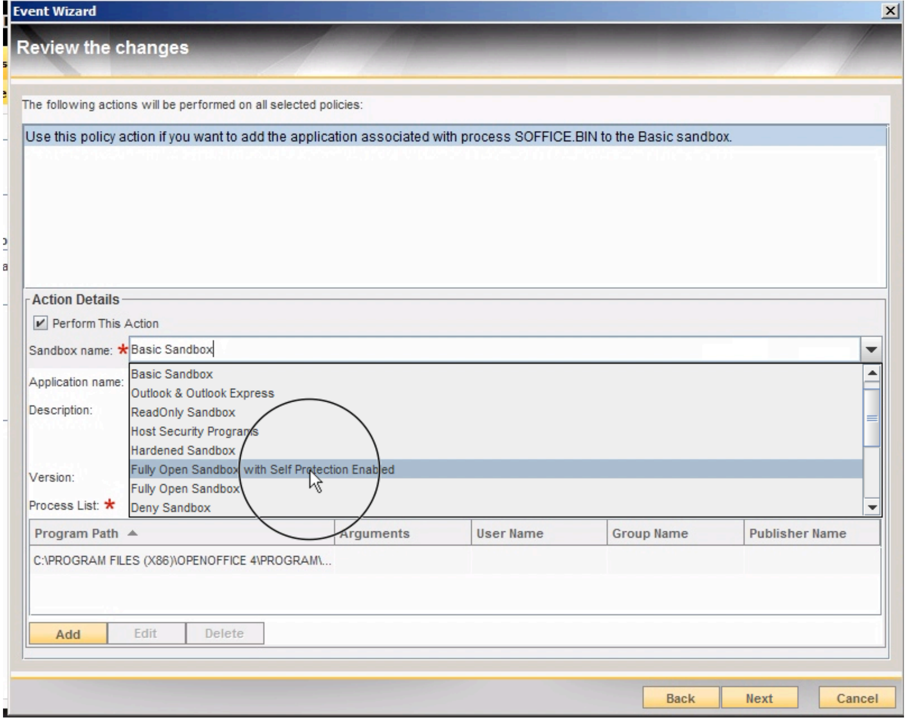


Operating System: Windows

Symantec

Name	Rev.	Min. Agent	Operating System
sym_win_basic_sbp	87	6.0.0	Windows
sym_win_hardened_sbp	87	6.0.0	Windows
sym_win_targeted_prevention_sbp	24	6.0.0	Windows
sym_win_whitelisting_sbp	87	6.0.0	Windows
Test Application Whitelisting *	89	6.0.0	Windows

13. c Select fully open sandbox with self protection enabled. Click next.



Event Wizard

Review the changes

The following actions will be performed on all selected policies:

Use this policy action if you want to add the application associated with process SOFFICE.BIN to the Basic sandbox.

Action Details

☑ Perform This Action

Sandbox name: * Basic Sandbox

Application name:

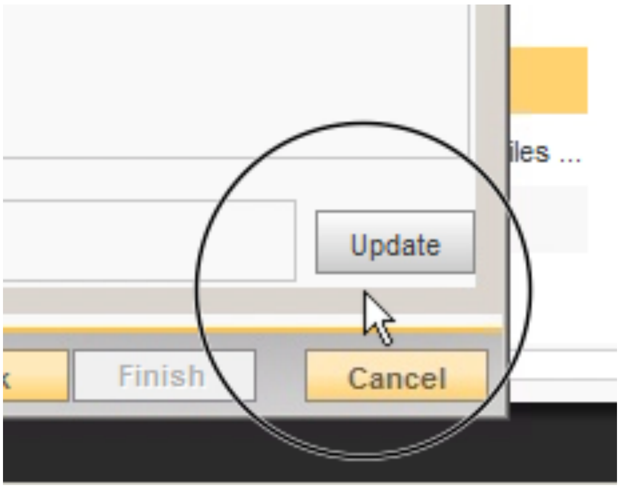
Description:

Version:

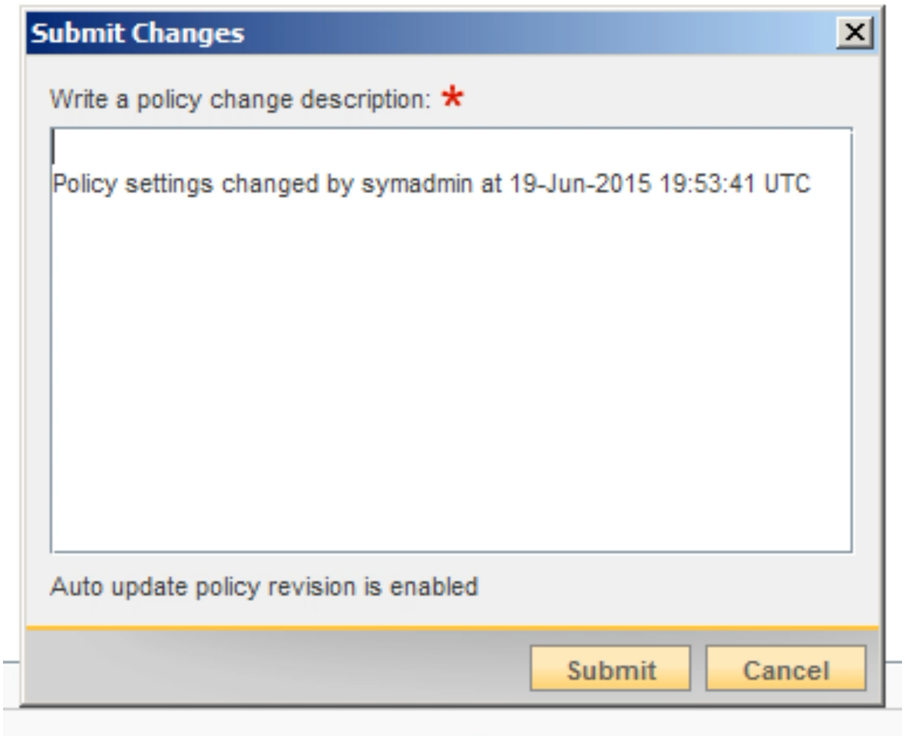
Process List: *

Program Path	Arguments	User Name	Group Name	Publisher Name
C:\PROGRAM FILES (X86)\OPENOFFICE 4\PROGRAM\...				

13. d Click update.



13. e Commit change by clicking submit.



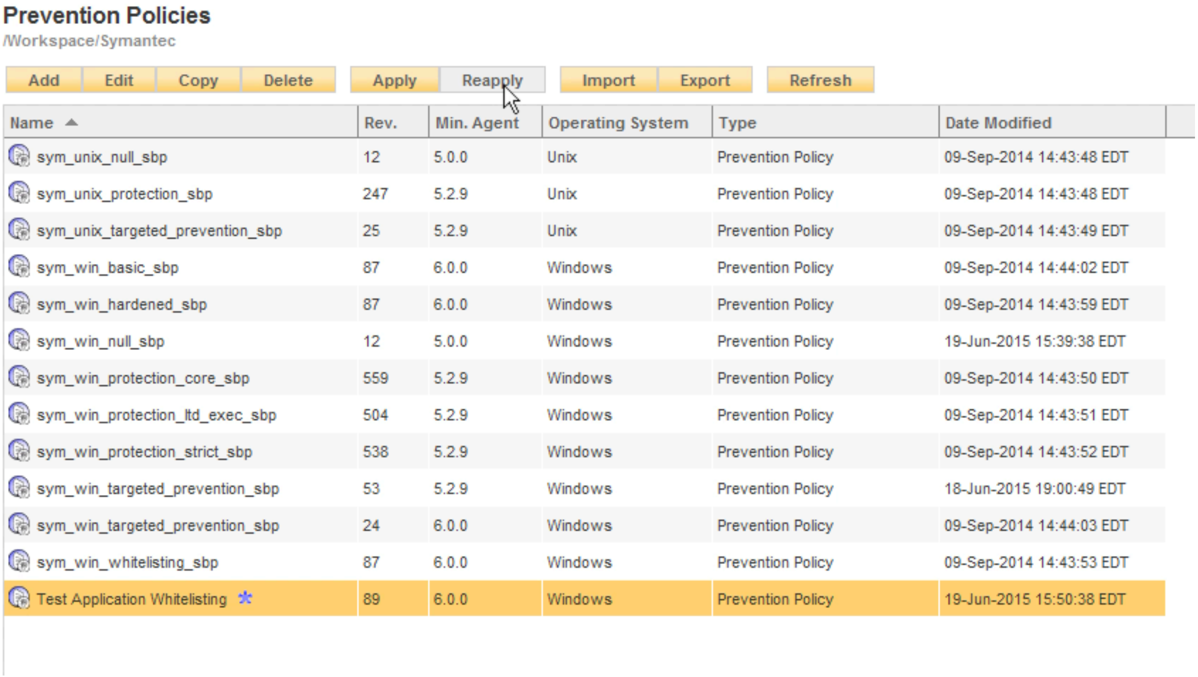
Submit Changes

Write a policy change description: *

Policy settings changed by symadmin at 19-Jun-2015 19:53:41 UTC

Auto update policy revision is enabled

13. f In the policies window, select newly modified policy and click reapply to launch the Reapply Policy Wizard.

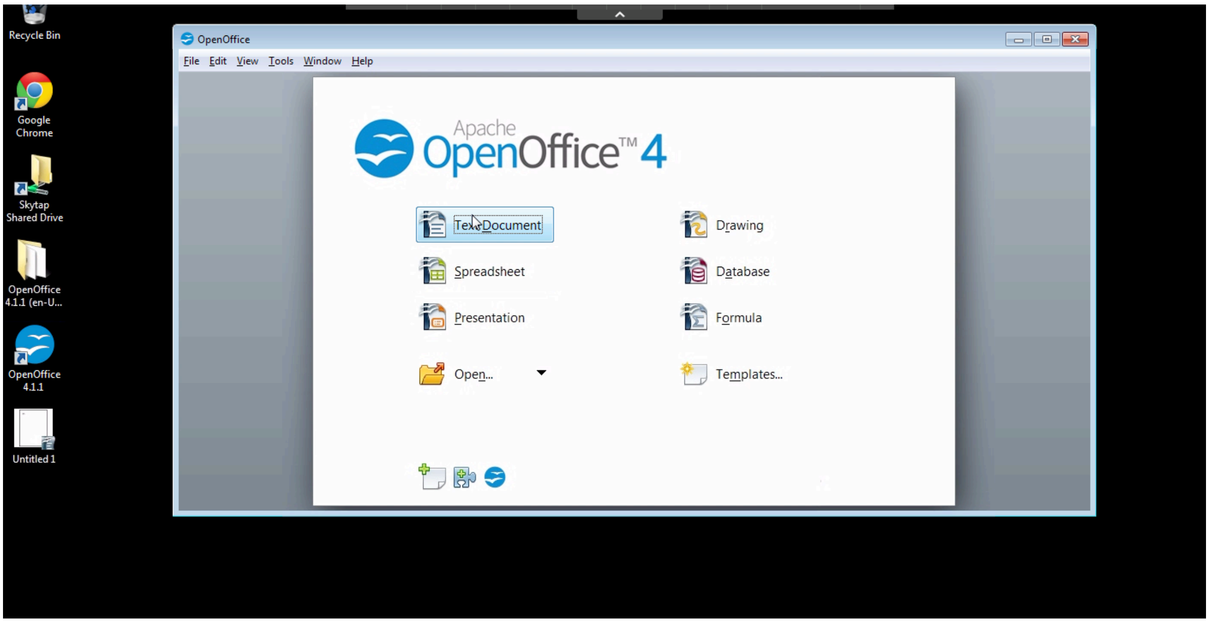


Prevention Policies

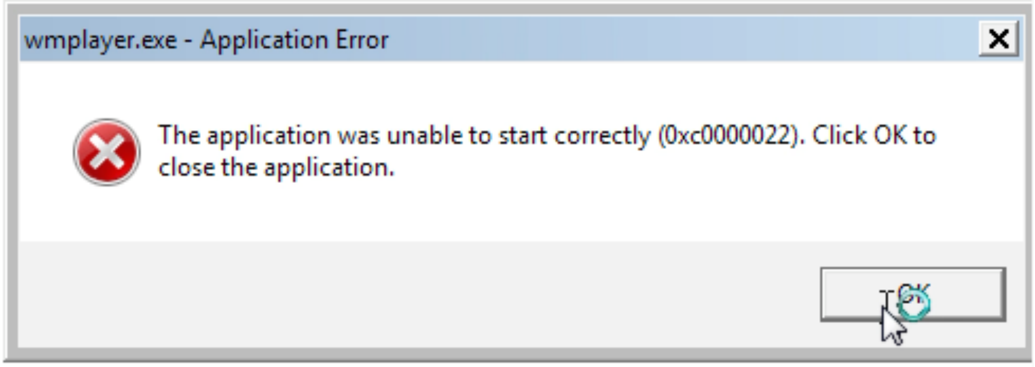
/Workspace/Symantec

Name	Rev.	Min. Agent	Operating System	Type	Date Modified
sym_unix_null_sbp	12	5.0.0	Unix	Prevention Policy	09-Sep-2014 14:43:48 EDT
sym_unix_protection_sbp	247	5.2.9	Unix	Prevention Policy	09-Sep-2014 14:43:48 EDT
sym_unix_targeted_prevention_sbp	25	5.2.9	Unix	Prevention Policy	09-Sep-2014 14:43:49 EDT
sym_win_basic_sbp	87	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:44:02 EDT
sym_win_hardened_sbp	87	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:43:59 EDT
sym_win_null_sbp	12	5.0.0	Windows	Prevention Policy	19-Jun-2015 15:39:38 EDT
sym_win_protection_core_sbp	559	5.2.9	Windows	Prevention Policy	09-Sep-2014 14:43:50 EDT
sym_win_protection_ltd_exec_sbp	504	5.2.9	Windows	Prevention Policy	09-Sep-2014 14:43:51 EDT
sym_win_protection_strict_sbp	538	5.2.9	Windows	Prevention Policy	09-Sep-2014 14:43:52 EDT
sym_win_targeted_prevention_sbp	53	5.2.9	Windows	Prevention Policy	18-Jun-2015 19:00:49 EDT
sym_win_targeted_prevention_sbp	24	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:44:03 EDT
sym_win_whitelisting_sbp	87	6.0.0	Windows	Prevention Policy	09-Sep-2014 14:43:53 EDT
Test Application Whitelisting *	89	6.0.0	Windows	Prevention Policy	19-Jun-2015 15:50:38 EDT

13. g Open office launches successfully without generation warnings in the management console after new whitelist items have been applied.



13. h After enabling prevention for the policy, only the whitelisted items will run. Non-permitted applications will fail to execute (e.g. Windows Media Player)


wmplayer.exe - Application Error

The application was unable to start correctly (0xc0000022). Click OK to close the application.