Symantec Endpoint Protection 11.0

Terminal Server and Citrix Best Practices White Paper

Contents

Scope

This white paper focuses strictly on providing guidance on how to successfully deploy the Symantec Endpoint Protection 11.0 protection components to a Microsoft Terminal Server or Citrix Presentation Server. It also provides guidance on recovering from potential issues that may arise during the deployment and a list of useful online resources. This white paper does <u>not</u> cover deploying Symantec Endpoint Protection 11.0 to workstation, other more general administration concerns or Citrix server best practice in general; for guidance on these topics, please refer to the relevant product documentation. Note also, to date the content of this document has only been validated with the US English versions of Citrix Presentation Server 4.5 running on Microsoft Windows Server 2003 and Symantec Endpoint Protection 11.0 MR2.

Executive Summary

The aim of this whitepaper is to show that Symantec Endpoint Protection can function correctly on terminal servers and where necessary document any changes required to the Symantec Endpoint Protection architecture in order to improve performance or reliability on those terminal servers. The findings of this white paper are already helping to shape the future direction for SEP functionality on Citrix and Terminal servers.

What is Windows Terminal Services

The terminal server component of Windows Server allows remote clients and devices to access and use Windows Server desktops and applications. These devices can be Windows, Macintosh or Linux workstations as well as wireless devices, laptops, set top boxes or potentially any device with a network connection. When Terminal Services is activated on a windows server, users can connect to a virtual desktop on the server and all applications are executed on the server, instead of the client device.

Conceptually, the design is similar to using PCAnywhere, VNC or any other remote control product. However, by running a special kernel, a windows terminal server is able to support multiple users connecting to the server simultaneously – each running their own virtual desktop. A single server can potentially support dozens, if not hundreds or even thousands of simultaneous users.

What is Citrix Presentation Server

Citrix Presentation Server, a member of the Citrix Delivery Center product family, is an end-to-end Windows application delivery system that offers both client-side and server-side application virtualization, for optimal application performance and flexible delivery options. With the secure application architecture, organizations can centralize applications and data in secure data centers, reducing costs of management and support, increasing data security, and ensuring fast, reliable performance.

Presentation Server allows IT departments to deliver secure applications as a service, providing on-demand access to users while affording the flexibility to leverage future application architectures.

What is Symantec Endpoint Protection (SEP) 11.0?

Symantec Endpoint Protection 11.0 combines Symantec Antivirus with advanced threat prevention to deliver unmatched defence against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single agent and management console, increasing protection and helping lower total cost of ownership.

Specifically, Symantec Endpoint Protection 11.0 provides the following protection technologies:

- Antivirus and Antispyware

- Firewall

- Intrusion Prevention (both Network and Host based)

- Device Control

- Network Access Control (optional add-on)

The core components required to run a centrally managed Symantec Endpoint Protection 11.0 environment include:

- Symantec Endpoint Protection client (on each machine you wish to protect)

- Symantec Endpoint Protection Manager (a web server, utilising Microsoft IIS and Apache Tomcat)

- Database (by default, the SEPM automatically installs an embedded database, based upon Sybase Adaptive Server Anywhere version 9)

- Symantec Endpoint Protection Manager console (Java-based, can be run from anywhere with network access to the Manager)

Running Symantec Endpoint Protection on Terminal Servers

Symantec Endpoint Protection client will run acceptably on Windows Terminal Servers; however there are a few modifications than can be made in order to optimise the overall user experience.

AntiVirus and AntiSpyware protection
The following recommendations should be taken into account:
Configure Auto-Protect to:

- Scan when a file is modified

- Disable network scanning

Centralized Exceptions
It is recommended to:

- Exclude the pagefile

- Exclude the print spooler folder

- If the server is a license server, exclude the license server folder and databases

Some server administrators may wish to exclude their users roaming profiles and/or "My Documents" folders from being scanned for security risks. While this will improve performance, Symantec would not recommend this approach – in practice this is generally the location in which security risks are discovered.

Scheduled Scans
If a scheduled scan is required then it should be run out of hours in order to minimise user impact. In addition, ActiveScans when new definitions arrive and startup scans should not be run as they could place unnecessary load on the terminal server during business hours.

Tamper Protection
There are no tamper protection recommendations for a server just running Terminal Services

Network Threat Protection
Although it is not recommended to run Network Threat Protection on terminal servers, it is entirely possible to do so. The default Symantec Endpoint Protection rule set will allow all terminal services functions to work correctly. However, it should be noted that if a custom rule set is created, the following services and ports should be allowed:

Process name	Local Port	Remote Port	Inbound/Outbound	Description
Svchost.exe	3389	1024-5000	Inbound	RDP Connection

General Information about Symantec Endpoint Protection and user processes
At all times, terminal server administrators should bear in mind that running SEP client on their terminal servers will not protect the client computer from threats. Depending on the terminal solution being used, Symantec has a separate solution for these (most could run SEP, others may

require SEP for XP Embedded) and you should discuss the requirement with your Symantec partner, SE or account manager.

Image Name	User Name	CPU	Mem Usage
ccApp.exe	Anon002	00	1,348 K
ccApp.exe	Anon004	00	1,352 K
ccApp.exe	Anon008	00	688 K
ccApp.exe	Anon007	00	1,356 K
ccApp.exe	Anon009	00	1,356 K
ccApp.exe	Anon006	00	1,348 K
ccApp.exe	Anon001	00	1,348 K
ccApp.exe	Anon005	00	736 K
ccApp.exe *32	Administrator	00	740 K
ccSvcHst.exe *32	SYSTEM	00	2,584 K
SmaService.exe	LOCAL SERVICE	00	11,728 K
Smc.exe	SYSTEM	00	8,956 K
SmcGui.exe	SYSTEM	00	4,256 K
SmcGui.exe	Administrator	00	3,804 K
SmcGui.exe	Anon002	00	3,704 K
SmcGui.exe	SYSTEM	00	3,804 K
SmcGui.exe	Anon008	00	3,712 K
SmcGui.exe	Anon003	00	3,528 K
SmcGui.exe	Anon006	00	3,244 K
SmcGui.exe	Anon005	00	3,828 K
smss.exe	SYSTEM	00	308 K
spoolsv.exe	SYSTEM	00	6,456 K
pnagent.exe	Anon006	00	9,692 K
pnagent.exe *32	Administrator	00	3,044 K
ProtectionUtilSurrogate.exe	Anon002	00	13,500 K
ProtectionUtilSurrogate.exe	Anon004	00	7,224 K
ProtectionUtilSurrogate.exe	SYSTEM	00	7,004 K
ProtectionUtilSurrogate.exe	Anon008	00	13,500 K
ProtectionUtilSurrogate.exe	Anon003	02	13,508 K
ProtectionUtilSurrogate.exe	SYSTEM	02	13,500 K
ProtectionUtilSurrogate.exe	Anon006	02	13,704 K
ProtectionUtilSurrogate.exe *32	Administrator	02	7,452 K
RadeObj.exe	Anon004	00	1,968 K
RadeObj.exe	Anon008	00	5,212 K

Figure 1 - SEP Processes running on Terminal Servers

When running SEP client on terminal servers, you will notice that multiple instances of both SmcGui.exe and ccApp.exe are running. In addition, on 64 bit terminal servers you will also see ProtectionUtilSurrogate.exe running per user. This is normal behaviour and should not cause problems in small deployments or remote administration scenarios. However, under certain circumstances and depending on the number of sessions in use, this can cause the CPU utilisation to spike to 100% and large amount of extra memory to be used. Although these processes are required for a fully working SEP client installation, they can be prevented from loading on terminal servers with minimal effect to the end user. For details on how to do this, please see Appendix D.

Although SEP client can be configured to support multiple users with individual policies, in a terminal server environment, this will manifest itself in a different way than would be imagined. If a user is logged onto the console of the server, then all remote users will be given the same policy. If there is no console user, then all users will receive the policy of the first logged in user. Symantec are working to change this so that the feature works correctly on terminal servers, but this behaviour is expected at this moment in time.

Extra considerations for Symantec Endpoint Protection on Citrix products

As with Windows Terminal services, Symantec Endpoint Protection runs without major issue on Citrix environments as long as all previous recommendations are taken into account. In addition, certain components of the application may however cause issues. These can vary from an incorrectly configured firewall component blocking traffic to the Tamper Protection module causing issues with certain health checking components of Citrix.

In addition to the AntiVirus and AntiSpyware exclusions for standard terminal servers, the following exclusions are recommended for Citrix servers:

- Citrix program files folder

- Citrix configuration database if present on the server

It is recommended that the following process is excluded from Tamper Protection on Citrix servers, as it is known to cause problems:

- ctxcpusched.exe – for more details on this process and how to create an exclusion for it,

  please refer to Appendix E.

As per terminal servers, if you wish to run the SEP firewall on a Citrix server then it is possible to do so without any issue using the default rule set in SEP 11.0 MR2 and beyond. If, however you wish to create a custom rule set for Citrix then the following processes and communications ports should be taken into account:

Process name	Local Port	Remote Port	Direction	Description
Svchost.exe	TCP/3389	TCP/1024-5000	Inbound	RDP Connection
ntoskrnl.exe	TCP/80	TCP/1024-5000	Inbound	Default port for unsecured Web Interface web servers and or TCP+HTTP browsing (XML port) and or Citrix Secure Gateway Secure Ticket Authority (STA) unsecured port.
	TCP/443			Default port for Citrix Secure Gateway, SSL Relay Service, Citrix ICA connections using SSL+HTTPS browsing and secure connections to a Citrix Web Interface web server) This is the only port that is needed to be open on an external

Process name	Local Port	Remote Port	Direction	Description
				firewall for secure connections to a Citrix Presentation Server environment utilizing the Citrix Secure Gateway technology.
Svchost.exe	TCP/1494	TCP/1024-5000	Inbound	Default ICA port, this can be changed if necessary. This port is not necessary to be open on the external firewall if you will be utilizing Citrix Secure Gateway for Windows.
ImaSrv.exe	TCP/2512 (on Farm Master) 1024-5000 (on Remote server)	TCP/1024-5000 (for Farm Master) TCP/2512 (on Remote Server)	Inbound	Citrix server to server communications
ImaSrv.exe	TCP/2513	TCP/1024-5000	Inbound	Citrix Management Console for Presentation Server 4.0 communication to the Citrix IMA Data Store
lmgrd.exe	TCP/27000	TCP/1024-5000	Inbound	Citrix Access Suite License Server and the License Manager daemon communicate over this port
CITRIX.exe	Dynamic by default, but configurable, see Appendix F	TCP/1024-5000	Inbound	Citrix Licensing Server wrapper
Svchost.exe	TCP/1024-5000	TCP/27000 & Dynamic, depends on CITRIX.exe configuration	Outbound	Allows Citrix servers to communicate with a Citrix license server
mmc.exe	TCP/1024-5000	Dynamic	Outbound	Allows Citrix management console to communicate with Citrix servers
ConfigMgrSvr.exe	Dynamic	TCP/1024-5000	Inbound	Allows Citrix management console to communicate with Citrix servers
Dllhost.exe	Dynamic	TCP/1024-5000	Inbound	Allows Citrix management console to communicate with Citrix servers

Process name	Local Port	Remote Port	Direction	Description
Mfcom.exe	Dynamic	TCP/1024-5000	Inbound	Allows Citrix management console to communicate with Citrix servers
SmaService.exe	Dynamic	TCP/1024-5000	Inbound	Allows Citrix management console to communicate with Citrix servers
XTE.exe	TCP/2598	TCP/1024-5000	Inbound	ICA session w/ Session Reliability client-to-server communications. This port is only used when Session Reliability is enabled.

In the case of services that use dynamic ports on servers, it is recommended that a host group be used that contains the IP addresses of the Citrix servers in your organisation. This group has been pre-created in the provided firewall policy, you simply need to add your Citrix server addresses to it.

It should be noted that administrators will only see multiple instances of SmcGui.exe, ccApp.exe and ProtectionUtilSurrogate.exe if they are publishing a full server desktop via Citrix. If published applications are used solely then there will be no multiple instances of these processes and there is no requirement to follow the steps in Appendix D.

Using Symantec Endpoint Protection Manager on Terminal Servers

While it is possible to run the Symantec Endpoint Protection Manager on a terminal server, it is not recommended if the terminal server is to be hosting a large number of terminal sessions due to the performance overhead of the Manager services, particularly when updating definitions and running the Java console.

If you wish to install the Symantec Endpoint Protection Manager on a terminal server, there are no specific recommendations for doing this, please refer to the installation PDF on the Symantec Endpoint Protection 11.0 CD1.

Conclusion

In conclusion, it can be seen that Symantec Endpoint Protection client will work on terminal and Citrix servers when installed "out of the box." However there are a number of product and configuration optimisations that can be made in order to drastically improve reliability and performance in this particular environment.

Future versions of Symantec Endpoint Protection are already in development and there are many changes being made to the code to provide better optimisation in terminal services environments. Until these enhancements are realised, the steps in this whitepaper will provide the same performance benefits.

All the steps in this whitepaper have already been performed on several large Citrix deployments on Symantec customer sites and all participants have been extremely impressed at the performance benefits that these modifications bring about.

Appendix A: Testing Methodology

During the authoring of this whitepaper, the following environment was built:

Figure 2 - Terminal Services Testing Environment

- CITRIX32 – a 32 bit Windows 2003 Server running Citrix Presentation Server 4.5 – member of the farm "Citrix Farm"
- CITRIX64 – a 64 bit Windows 2003 Server running Citrix Presentation Server 4.5 – member of the farm "Citrix Farm"
- WTS32 – a 32 bit Windows 2003 Server running Terminal Services in application mode
- WTS64 – a 64 bit Windows 2003 Server running Terminal Services in application mode
- SYMDC – a 32 bit Windows 2003 Domain Controller for the Domain: SYMCTEST
- SEPM – a 32 bit Windows 2003 Member Server running Symantec Endpoint Protection Manager
- XPCLIENT – a 32 bit Windows XP Client Computer, running ICA Client and Remote Desktop

As can be seen from the diagram above, a domain "SYMCTEST" was established – all servers and clients were members of this domain during testing. Both Citrix servers were joined to the same Citrix Farm – "CitrixFarm." CITRIX64 served as the Farm master. For the purpose of testing, anonymous access to Citrix applications was configured. Common business applications, such as Microsoft Word and Excel were installed onto the Citrix servers and were published through the Citrix Web Interface. In addition, a full desktop was also published.

Symantec Endpoint Protection Manager was installed onto the server "SEPM." Packages were then created for servers and deployed from the console. The Windows firewall was turned off on all servers, as the SEP firewall was used, initially with the default firewall policy from MR2 and later with a custom developed policy.

Using the client XPCLIENT, multiple remote desktop sessions were established to each Windows Terminal Server and performance and task manager processes were observed. In the same way, 10 anonymous sessions were established to each Citrix server – separate tests were performed for published applications and the published desktop. In both cases, task manager was observed from a console connection.

Changes were then made to the clients on the servers and re-testing was performed to see the difference in performance and processes that were loaded. Each change was made separately, then tested.

Once process and AntiVirus and AntiSpyware optimisation was complete, work was started on the firewall ruleset, with an initial ruleset being put in place that allowed all communication to and from the domain controller and blocked and logged all further traffic. Rules were then created per each block rule that allowed the Citrix and Terminal Server processes until there were no more blocked requests related to Citrix or Terminal Services processes. All tests were then re-run with

this new ruleset in use to confirm overall functionality. In addition, Citrix farm administration tasks were also performed from each Citrix server to ensure that server to server communications were still working correctly.

Once all performance changes and testing had been completed, functionality tests were run against the SEP clients running on the servers to prove that core functionality had not been affected by the changes put in place. Virus detections still occurred and users were notified, clients were able to be managed from the management console, and would accept commands and update content and policies successfully.

Appendix B: Key Processes on Windows Terminal Services

The following additional processes can be seen running on a Windows terminal server running SEP Client:

Process name	Per User	Vendor	Description
Smc.exe	No	Symantec	Symantec Management Component – connects SEP client to SEPM
SmcGui.exe	Yes	Symantec	Provides the tray icon for SEP and monitors network traffic
ccApp.exe	Yes	Symantec	Provides email scanning for SEP client
ccSvcHost.exe	No	Symantec	Event Manager component
Rtvscan.exe	No	Symantec	Real Time Virus Scanning component
SymCorpUI.exe	Only when opened	Symantec	The Symantec Endpoint Protection client GUI
Lserver.exe	No	Microsoft	Terminal Server Licensing component (if server is a license server)

In addition, on 64 bit servers, the following processes are present:

Process name	Per User	Vendor	Description
ProtectionUtilSurrogate.exe	Yes	Symantec	This component allows the 64 bit SmcGui process to access 32bit processes, such as RtvScan and SymCorpUI

Appendix C: Key Processes on Citrix products

The following additional processes may be seen running on a Windows terminal server running
Citrix Presentation Server & SEP Client:

Process name	Per User	Vendor	Description
Smc.exe	No	Symantec	Symantec Management Component – connects SEP client to SEPM
SmcGui.exe	Yes	Symantec	Provides the tray icon for SEP and monitors network traffic
ccApp.exe	Yes	Symantec	Provides email scanning for SEP client
ccSvcHost.exe	No	Symantec	Event Manager component
Rtvscan.exe	No	Symantec	Real Time Virus Scanning component
SymCorpUI.exe	Only when opened	Symantec	The Symantec Endpoint Protection client GUI
Lserver.exe	No	Microsoft	Terminal Server Licensing component (if server is a license server)
CITRIX.exe	No	Citrix	Citrix License Server wrapper (if server is a Citrix License Server)
CdfSvc.exe	No	Citrix	Diagnostic Facility COM Server – manages diagnostic facility tracing when used to diagnose problems with the Citrix server
cdmsvc.exe	No	Citrix	Handles the mapping of client drives and peripherals within ICA sessions
Citrix_GTLicensingProv.exe	No	Citrix	Provides information and notifications regarding licensing events on the license server (if server is a Citrix License Server)
ConfigMgrSvr.exe	No	Citrix	Citrix Configuration Management Server
CpSvc.exe	No	Citrix	Citrix Print Manager Service – handles the creation of printers and driver usage within Citrix sessions
ctxcpushed.exe	No	Citrix	Citrix CPU Utilization Mgmt/Resource

Process name	Per User	Vendor	Description
			Mgmt – Used in Enterprise and Platinum editions to manage server resource consumption
CtxSFOSvc.exe	No	Citrix	Citrix Virtual Memory Optimisation – Used in Enterprise and Platinum editions to rebase DLL's in order to free up server memory
ctxwmisvc.exe	No	Citrix	Citrix WMI Service – used to provide the Citrix WMI classes for information and management purposes
encsvc.exe	No	Citrix	Citrix Encryption Service – Handles encryption between the client device and the Citrix server
HCAService.exe	No	Citrix	Citrix Health Monitoring and Recovery – Provides health monitoring and recovery services in the event problems occur
icabar.exe	No	Citrix	Citrix Systems Toolbar
IMAAdvanceSrv.exe	No	Citrix	Citrix Services Manager - Allows the components of Presentation server to interact with the operating system
ImaSrv.exe	No	Citrix	Citrix Independent Management Architecture – provides management services within the Citrix farm
lmgrd.exe	No	Macrovision Corporation	Citrix Licensing – Handles allocation of licenses on the license server (if server is a Citrix License Server)
mfcom.exe	No	Citrix	Citrix MFCOM service – Provides COM services which allow remote connections of the management consoles
pnagent.exe	Yes	Citrix	Citrix ICA Client Program Neighbourhood Agent
RadeObj.exe	Yes	Citrix	Citrix Streaming Client Session COM Server
RadeSvc.exe	No	Citrix	Citrix Streaming Service – used in Enterprise and Platinum versions to

Process name	Per User	Vendor	Description
			manage the Citrix Streaming Client when streaming applications
SmaService.exe	No	Citrix	Citrix SMA Service – Monitors the event log and Citrix WMI to raise alerts in the Access Suite console or Access Management console
ssonsvr.exe	Yes	Citrix	Citrix Program Neighbourhood and Single Sign on Agent
Tomcat.exe	No	Alexandria Software Consulting	Citrix License Management Console – provides the web-based interface for licensing administration
wfshell.exe	Yes	Citrix	Citrix WinFrame Shell – seamless windows engine shell
XTE.exe	No	Citrix	Citrix XTE Server - Handles SSL Relay and Session Reliability functionality

In addition, on 64 bit servers, the following processes are present:

Process name	Per User	Vendor	Description
ProtectionUtilSurrogate.exe	Yes	Symantec	This component allows the 64 bit SmcGui process to access 32bit processes, such as RtvScan and SymCorpUI

Appendix D: Preventing SmcGui, ProtectionUtilSurrogate and ccApp running for all users

In a default installation of SEP client, the following processes will run per user and can take up to 20MB of RAM per session:

Process name
SmcGui.exe
ProtectionUtilSurrogate.exe
ccApp.exe

Symantec is working on a long term solution that would only require one of these applications to be running at all times (ccApp) and with minimal memory usage (CPU utilisation with multiple instances of SmcGui is already better in MR3 and MR2 than MR1), however in the meantime there is a workaround.

In order to prevent SmcGui and ProtectionUtilSurrogate (on 64 bit servers) from loading with each user session, complete the following steps for pre-MR3 clients:

Step	Process	Complete
1	Logon to the server you wish to configure with an administrator account	☐
2	Click Start, Run and type "smc –stop" then click OK. Enter a password if prompted. Wait for the shield to disappear from the system tray	☐
3	Browse to the SEP Client installation location (normally C:\Program Files\Symantec\Symantec Endpoint Protection)	☐
4	Find the file SmcGui.exe and right click it	☐
5	Click Rename	☐
6	Rename the file "xSmcGui.exe" press Enter	☐
7	Click File, New and select Text Document	☐
8	Call the document "SmcGui.exe" press Enter	☐
9	At the prompt to change the file extension, click Yes Rename ☒ ⚠ If you change a file name extension, the file may become unusable. Are you sure you want to change it? [Yes] [No]	☐
10	Click Start, Run and type "smc –start" then click OK. You will notice from Task Manager that SMC starts as SYSTEM, but SmcGui does not load.	☐
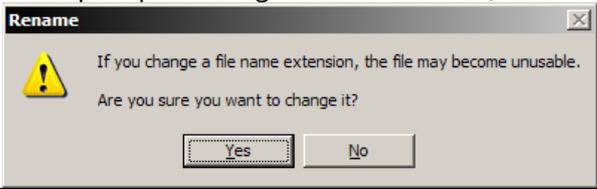
For MR3 clients only, please use the following steps:

Step	Process	Complete
1	Logon to the server you wish to configure with an administrator account	☐
2	Click Start, Run and type "regedit" then click OK	☐
3	Browse to HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC	☐
4	Find the entry LaunchSmcGui and change it from DWORD 1 to DWORD 0	☐

To further optimise memory, you can prevent ccApp from loading by following the instructions below:

Step	Process	Complete
1	Logon to the server you wish to configure with an administrator account	☐

2	Click Start, Run and type "regedit" then click OK	
3	Browse to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (for 64bit servers this is HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run)	
4	Find the entry ccApp and delete it	

From this point onwards, SmcGui.exe, ProtectionUtilSurrogate.exe (on 64 bit servers) and ccApp.exe will no longer load for any new user sessions. There may however still be instances of ccApp.exe already running on the server that have not been closed. You can either kill these tasks from Task Manager or wait for the user to log off – ccApp.exe will close and will not be re-launched at the next logon.

The following is a list of the features that are lost after implementation of this workaround:
Disabling ccApp:

- Internet Email Scanning

Disabling SmcGui

- Tray icon and Tray Icon menu
    - Open Symantec Endpoint Protection
    - Enable/Disable Symantec Endpoint Protection
    - Update Policy
    - Re-Authenticate User (SNAC Only)
- Firewall and AV status
    - Tool Tips
    - Balloons
    - Firewall prompts (packets will be dropped)
- Creation of a user's private log directory
- AV Definitions dialogs:
    - Definitions out-of-date
    - Definitions corrupt
    - Definitions missing
- Startup Scans
- Floppy disk detection on shutdown
- Reboot prompts. Reboots will happen without prompting, identical to what happens when there is no logged in user.
- Screen saver detection for firewall rules that use the Screen Saver state

Appendix E: Tamper Protection

In certain circumstances, if SEP is configured to notify the user of Tamper Protection violations, you will see the following dialog box when SEP is installed onto 32 bit Citrix servers. You will not see this notification on 64 bit servers as Tamper Protection is currently not supported on 64 bit servers.
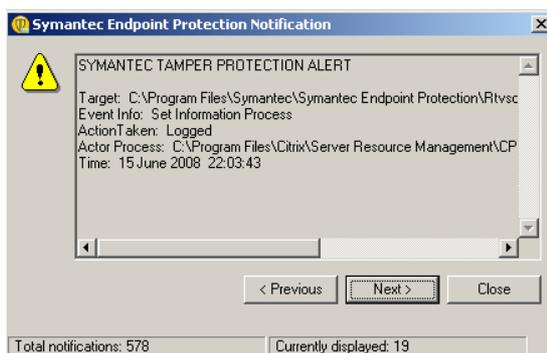
Figure 3 - Tamper Protection Alert for Citrix CPU Management process

The Centralized Exceptions policy provided with this whitepaper will exclude this process from detection; however in certain cases this exclusion may not work correctly and you will need to exclude it yourself. The only way you can do this is via the management console AFTER detection. If you would like to add the process in this manner, please follow the steps below:

Step	Process	Complete
1	Logon to the SEPM management console with an administrator account	❏
2	Click Policies, Centralized Exceptions	❏
3	If you don't already have a Centralized Exceptions policy, then either import the one with this whitepaper (follow Appendix F) or create a new one by clicking "Add a Centralized Exceptions Policy." Give the policy a suitable name and click OK, then click No to the assign the policy prompt	❏
4	Click Monitors	❏
5	Click the Logs tab	❏
6	In Log Type, select Application and Device Control	❏
7	In Log Content, select Application Control	❏
8	Click Advanced Settings >>	❏
9	In Event Type, select Tamper Protection	❏
10	Click View Log, you will be shown a list of Tamper Protection Violations	❏
11	Select an appropriate violation and at the top of the window, choose "Add File to Centralized Exceptions policy" then click Start	❏
12	Check the file to be excluded is correct	❏
13	Select all the Centralized Exceptions policies you wish to add the exception	❏

Step	Process	Complete
	to	
14	Click OK	❐
15	Click OK at the completion prompt	❐
16	Click Policies, Centralized Exceptions	❐
17	Double click the Centralized Exception policy you added the new exception to	❐
18	The policy will open, on the left hand side, click Centralized Exceptions and confirm the file is listed and has an Action of "Ignore"	❐

Appendix F: Changing the Citrix Vendor Daemon Port Number

By default, the Citrix vendor daemon uses a dynamically changing port number that changes when the license server or the CitrixLicensing service is restarted.

Consequently, the Citrix vendor daemon port is not specified anywhere. To change the port number, add parameters for the new port number and the path for the options file to the VENDOR CITRIX line in each license file, including the startup license file. The modified syntax in the license file is as follows:

VENDOR CITRIX options="C:\Program Files\Citrix\Licensing\MyFiles\CITRIX.opt" port=number

When changing the Citrix vendor daemon port number, you must change the number in every license file on the license server and all subsequent license files that you download.

To configure a static port number for the Citrix vendor daemon

Step	Process	Complete
1	Logon to the Citrix License Server with an administrative account	☐
2	Browse to the Citrix license server files location (default location is C:\Program Files\Citrix\Licensing\MyFiles)	☐
3	Remove the Read Only attribute from all license files on the server, including the startup license file	☐
4	Open a license file with any text editor	☐
5	In the license file, locate the line VENDOR CITRIX.	☐

6	Modify the line by appending the following:
	
	`options=<the path to the options file> port=<the chosen port number>`
	
	Example:
	
	`VENDOR CITRIX options="C:\Program Files\Citrix\Licensing\MyFiles\CITRIX.opt" port=27950`
		☐

7	Save the license file—ensure you keep the .lic extension	☐
8	Repeat Steps 4 through 7 for each license file on the license server	☐
9	Restart the CitrixLicensing service. You can also run the lmreread License Administration Command on the license files or force the license server to reread the license files by clicking Update license data on the License Files page of the License Management Console. Note If a TCP/IP port number is specified on the VENDOR line, the Citrix vendor daemon may not restart until all the clients close their connections to the vendor daemon.	☐

Appendix G: Supporting links and information

CITRIX: Antivirus Software Configuration Guidelines for Presentation Server
http://support.citrix.com/article/ctx114522

CITRIX: Error: SYMANTEC TAMPER PROTECTION ALERT Points to CPU Utilization Management Executables
http://support.citrix.com/article/CTX113486

CITRIX: Citrix Presentation Server Services Overview
http://support.citrix.com/article/ctx114669

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 800 745 6054.

Symantec Corporation

World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

408 517 8000

800 721 3934

www.symantec.com