



Confidence in a connected world.

Symantec Endpoint Protection 11.0

Securing Virtual Environments Best Practices White Paper

Updated 7/20/2010

Securing Virtual Environments with Symantec Endpoint Protection

Content

- Scope 3**
- Executive Summary 3**
- What is Virtualization 3**
 - Supported Virtualization Platforms 3
- What is Symantec Endpoint Protection 4**
- Best Practices for Symantec Endpoint Protection Clients in a Virtual Environment 4**
 - Best Practices for Security Overview 4
 - Best Practices for Performance Overview 5
 - Randomizing Virus Definition Updates 5
 - Randomizing Scans 5
 - Updating Virus Definitions directly from the SEPM 6
 - Updating Virus Definitions Using LiveUpdate 8
 - Scheduled Scans 9
- Best Practices for Symantec Endpoint Protection Manager on a guest system 9**
- Appendix A: Licensing 10
- Appendix B: Looking Forward – VMsafe 10

Securing Virtual Environments

Scope

This White Paper provides an overview on Best Practices when running Symantec Endpoint Protection in a virtual environment, and offers an overview of what factors to consider when using Symantec Endpoint Protection in virtual environments.

It does not give specific sizing guidelines, as many factors can influence performance of multiple guest hosts in a virtual environment.

Note: In certain configurations or environments, Symantec Endpoint Protection might not be the recommended solution to maintain security. For example, Symantec Critical System Protection might be the preferred solution for a locked down VDI workstation or similar guest operating system. Please contact a Symantec Sales Engineer or Consultant if you have questions about your particular environment.

This White Paper addresses cases where Symantec Endpoint Protection is considered the proper solution for securing a virtual environment.

Executive Summary

Symantec Endpoint Protection 11.0 fully supports, virtual environments. This White Paper provides an overview of the most common considerations when running Symantec Endpoint Protection in virtual environments. It describes specific points about how to secure virtual environments while maintaining acceptable performance of guest systems.

What is Virtualization

Virtualization is the abstraction and simulation of resources. Platform virtualization/Virtual Machines (VMs) are software simulations of physical machines. Virtualization enables more than one running operating system per physical machine. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.

Symantec Endpoint Protection components run in virtual systems just as on physical hardware, although you may need to slightly increase basic hardware requirements for the physical system account for overhead due to running multiple virtual environments concurrently.

Supported Virtualization Platforms

The following Virtualization Platforms are supported by Symantec Endpoint Protection 11.0

- VMWare (WS 5.0, GSX 3.2, and ESX 2.5, ESX 3.x)
- Microsoft Virtual Server 2005
- Hyper-V

Note: this list is current as of the date of this white paper's publication. For a current list of support platforms, please refer to: <http://service1.symantec.com/support/ent-security.nsf/docid/2008121812110848>

What is Symantec Endpoint Protection

Symantec Endpoint Protection 11.0 combines Symantec Antivirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops, servers and **guest hosts in a virtual environment**. 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, utilizing 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)

Best Practices for Symantec Endpoint Protection Clients in a Virtual Environment

The main considerations when running Symantec Endpoint Protection in a virtual environment are the same as running on physical hardware: **Security and Performance**. The following Best Practices address how to ensure security for a virtual environment while maintaining performance and stability.

Best Practices for Security Overview

Symantec Endpoint Protection protects Windows-based operating systems, and must be installed on each instance of Windows to ensure protection. For example, if an administrator runs a Windows-based host with multiple Windows-based guest virtual machines, each discrete Windows instance must have Symantec Endpoint Protection installed to avoid any security gaps.

In general, the default settings for Symantec Endpoint Protection are appropriate to ensure the security of a guest operating system.

Securing Virtual Environments

Best Practices for Performance Overview

When running Symantec Endpoint Protection in a virtual environment, consider how multiple guest systems can impact hardware resources on a host system. This is especially true when routine tasks happen simultaneously on multiple guest systems. Due to extremely high I/O, the following tasks are examples that can degrade performance if run on multiple guest systems simultaneously.

- Virus Definition Updates
- Scheduled Scans

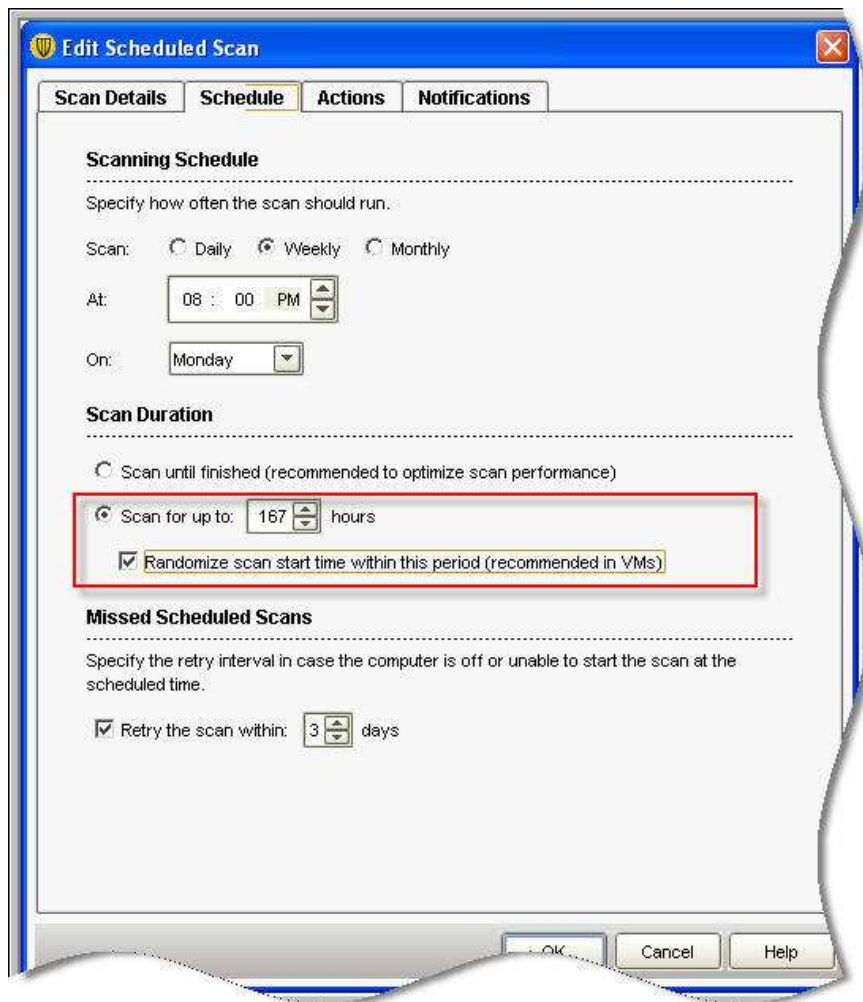
Symantec recommends using **randomization** to minimize the impact on hardware resources when these tasks occur. Randomization ensures each client on a guest system does not run a scheduled scan or update virus definitions at the same time.

Randomizing Virus Definition Updates

Symantec Endpoint Protection clients can update their virus definitions either directly from the Symantec Endpoint Protection Management server or by running the LiveUpdate component on the client to download virus definitions.

Randomizing Scans

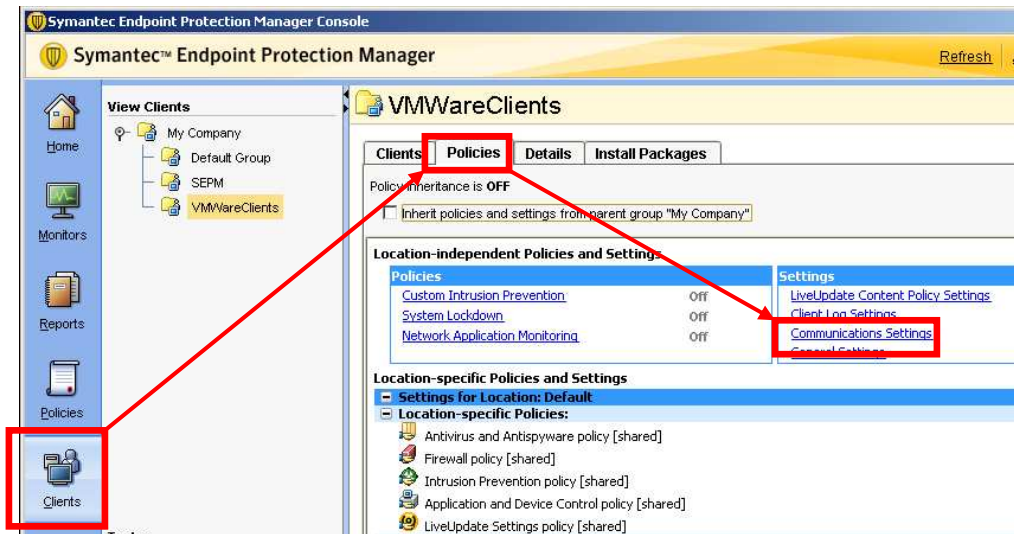
SEP RU6a includes a scan randomization feature designed to ease the load on the host machine by running scans at different times. This feature is especially useful in virtual machine environments helping to reduce the overall load at any given time on the host computer. The need for this feature arose from potential performance and bottleneck issues when scans would start and run simultaneously on host machines running multiple VMs. This feature corrects that bottleneck and ensures scans are not started simultaneously in multiple VM environments thus greatly improving overall performance. The Amber release will include Idle time and Scan Less features further improving performance of scanning VM environments. More information on these Amber features will become available in the coming months.



Updating Virus Definitions directly from the SEPM

Symantec Endpoint Protection 11 Maintenance Release 3 introduced a randomization feature to the Communications Settings for clients which will optimize performance in a virtual environment. These settings are configured via the communications settings within any group.

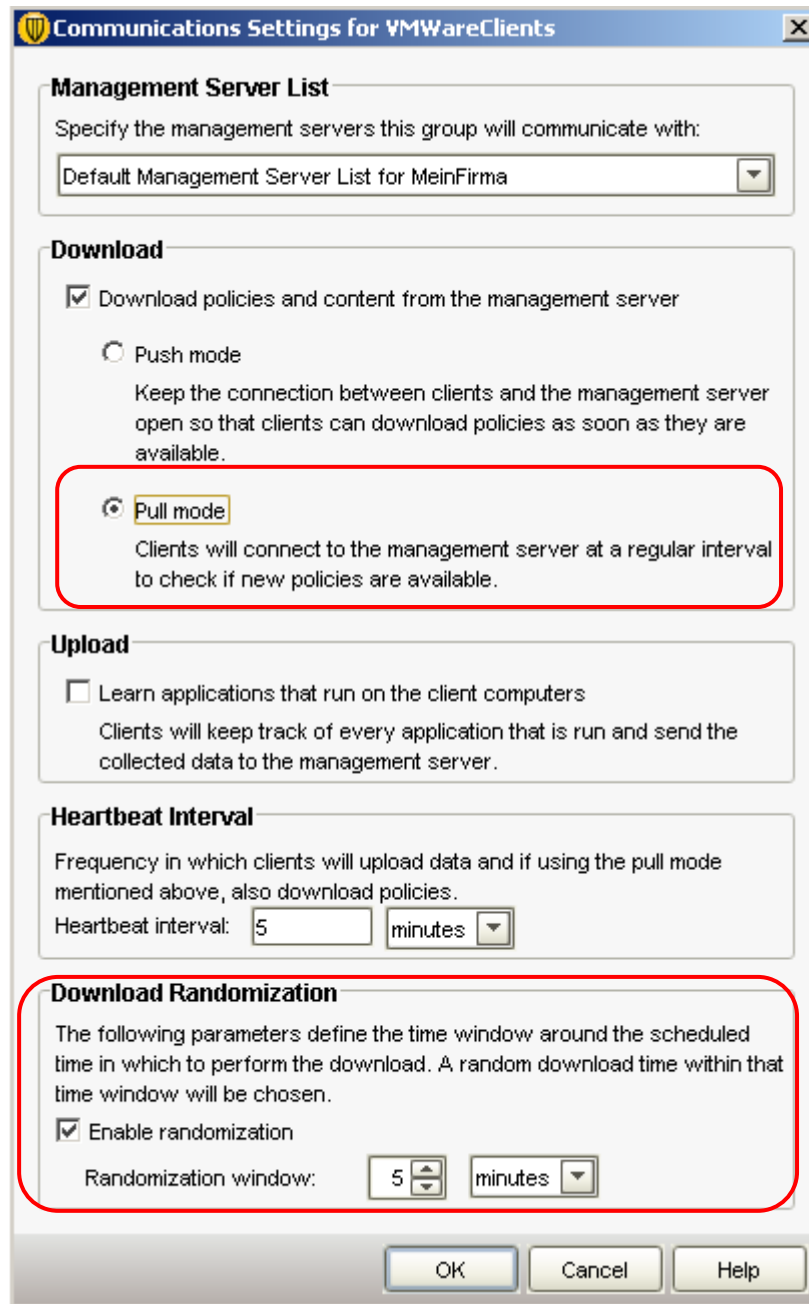
Securing Virtual Environments



Note: Uncheck the box next to “Inherit policies and settings from parent group” to configure the Group specific settings.

In the following Communication Settings dialog box, make the following changes as shown below:

1. Configure clients to use “Pull Mode”
2. Place a check in the “Enable randomization”



Note: Depending on the number of clients in the virtual environment, consider increasing the heartbeat interval as needed. Additionally, if the time at which clients update virus definitions causes a performance impact, consider increasing the randomization window as needed.

Updating Virus Definitions Using LiveUpdate

Alternatively, clients can be configured to run LiveUpdate to download Virus Definitions directly from Symantec. To prevent many clients from updating Virus Definitions simultaneously, Symantec recommends that you randomize the LiveUpdate schedule.

To configure clients to run LiveUpdate with a randomized schedule, configure the LiveUpdate Settings policy as follows:

Securing Virtual Environments

1. In the Symantec Endpoint Protection Manager, select the Policy Page and then select LiveUpdate
2. Open or create a LiveUpdate Settings policy for editing.
3. In the Server Settings dialog box uncheck “Download Definitions from management server” unless the randomization setting has been enabled in the client group’s communication settings.
4. Make sure there is a check next to “Use a LiveUpdate Server.”
5. In the Schedule dialogue enable scheduling and configure a schedule during non peak times
6. Make sure there is a check box next to “randomize the start time”

Scheduled Scans

Scheduled scans require consideration in a virtual environment due to the potential for performance degradation. How often and when scheduled scans should be run will depend on security policies in your organizations.

The following Knowledge Base articles apply to Scheduled Scan tuning in general and should be considered when configuring scheduled scans for guest systems:

Ensure Scan Tuning options are set for “Best Application Performance”:

<http://service1.symantec.com/support/ent-security.nsf/docid/2008082509323748>

Consider using multithreading during scheduled scans:

<http://service1.symantec.com/support/ent-security.nsf/docid/2005062813030748>

Consider utilizing the resumable scan feature:

<http://service1.symantec.com/support/ent-security.nsf/docid/2005062806252148>

Note: the specific options that are appropriate will depend on your environment.

Additionally, Symantec recommends dividing up guest clients in different groups with different scheduled scan times to avoid performance degradation. Also, consider scanning compressed files one or two levels deep (instead of default 3).

Best Practices for Symantec Endpoint Protection Manager on a guest system

When running a Symantec Endpoint Protection Manager in a guest host, ensure the Symantec Endpoint Protection Manager guest operating system has at least two virtual CPUs and that CPU throttling is disabled in ESX.

Furthermore, Symantec recommends following the same recommendations noted above for running multiple guest systems. The previously discussed settings establish how clients communicate with the manager and how the clients receive content from the manager, both of which affect how much CPU and Disk I/O the manager requires. Simultaneous content downloads can severely affect performance of a host virtual environment.

In summary, Symantec recommends configuring clients to communicate with the Symantec Endpoint Protection Manager in Pull Mode and enabling randomization for content downloads in the Communications Settings.

Securing Virtual Environments

Appendices

Appendix A: Licensing

Section 17.2 in the End User License Agreement states that each running instance of Symantec Endpoint Protection Client requires a license. This includes a running instance that exists due to cloning a virtual system. The exact wording is as follows:

17.2. Notwithstanding anything to the contrary contained in this License Agreement, if the Licensed Software is Symantec Endpoint Protection, each running instance (physical and/or virtual) of such Software must be licensed. You create an “instance” of software by executing the software’s setup or install procedure. You also create an “instance” of software by duplicating an existing instance. References to software include “instances” of the software. You “run an instance” of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.

Appendix B: Looking Forward – VMSafe

VMSafe is an API provided by VMWare to enhance security in virtual environments. Symantec is partnering with VMWare to leverage this technology to improve security and performance of virtual environments.

For more information please refer to VMWare’s VMSafe website:

<http://www.vmware.com/technology/security/vmsafe/partnerships.html>

This White Paper will be updated as more information about Symantec’s VMSafe technology is made available.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 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 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.