

Symantec Endpoint Protection 12.1.2

Virtualization Best Practices

Date Published:

30 November 2012

Document Version:

1.1



Table of Contents

Purpose	3
1 General Advice	3
1.1 Upgrade to the latest version	3
1.2 Grouping Virtual Clients in SEPM	3
2 Configuring Content Updates	5
2.1 Updating Virus Definitions directly from the SEPM	5
2.2 Updating Virus Definitions Using a LiveUpdate Policy	7
3 Configuring Scheduled Scans	8
3.1 Use active scans instead of full scan	8
3.2 Enable Scan Randomization	8
3.3 Enable Shared Insight Cache	10
3.3.1 Network-based Shared Insight Cache	11
3.3.2 vShield-enabled Shared Insight Cache	12
4 Excluding Base Images using Virtual Image Exception	14
4.1 Monitoring a base image for security threats	15
5 Non-persistent VDI	16
5.1 Identify Non-persistent VDI Clients	16
5.2 Disable Scheduled Scans	17
5.3 Content Updates	17

Purpose

The document provides best practices for installation and configuration of Symantec Endpoint Protection (SEP) in a virtual environment

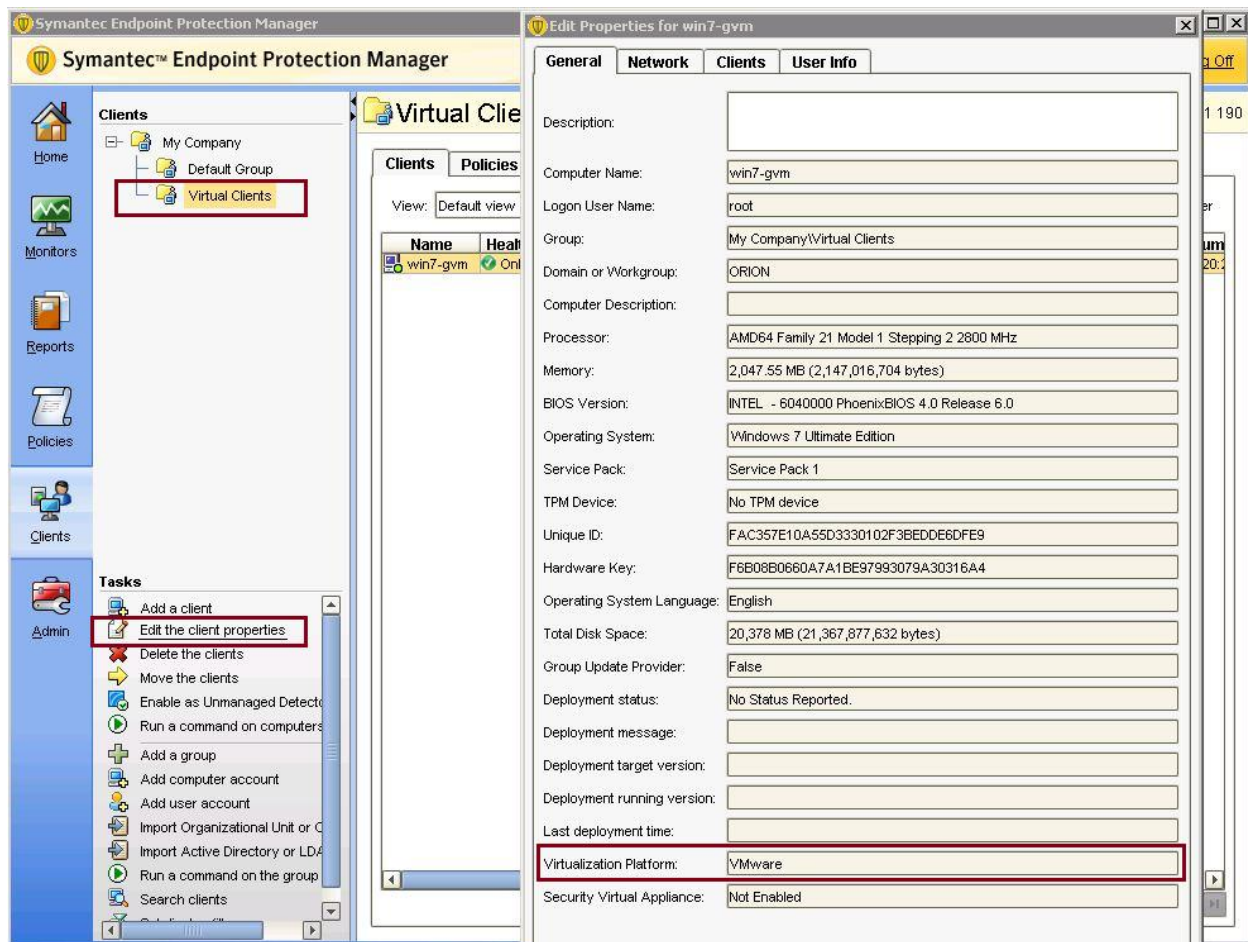
1 General Advice

1.1 Upgrade to the latest version

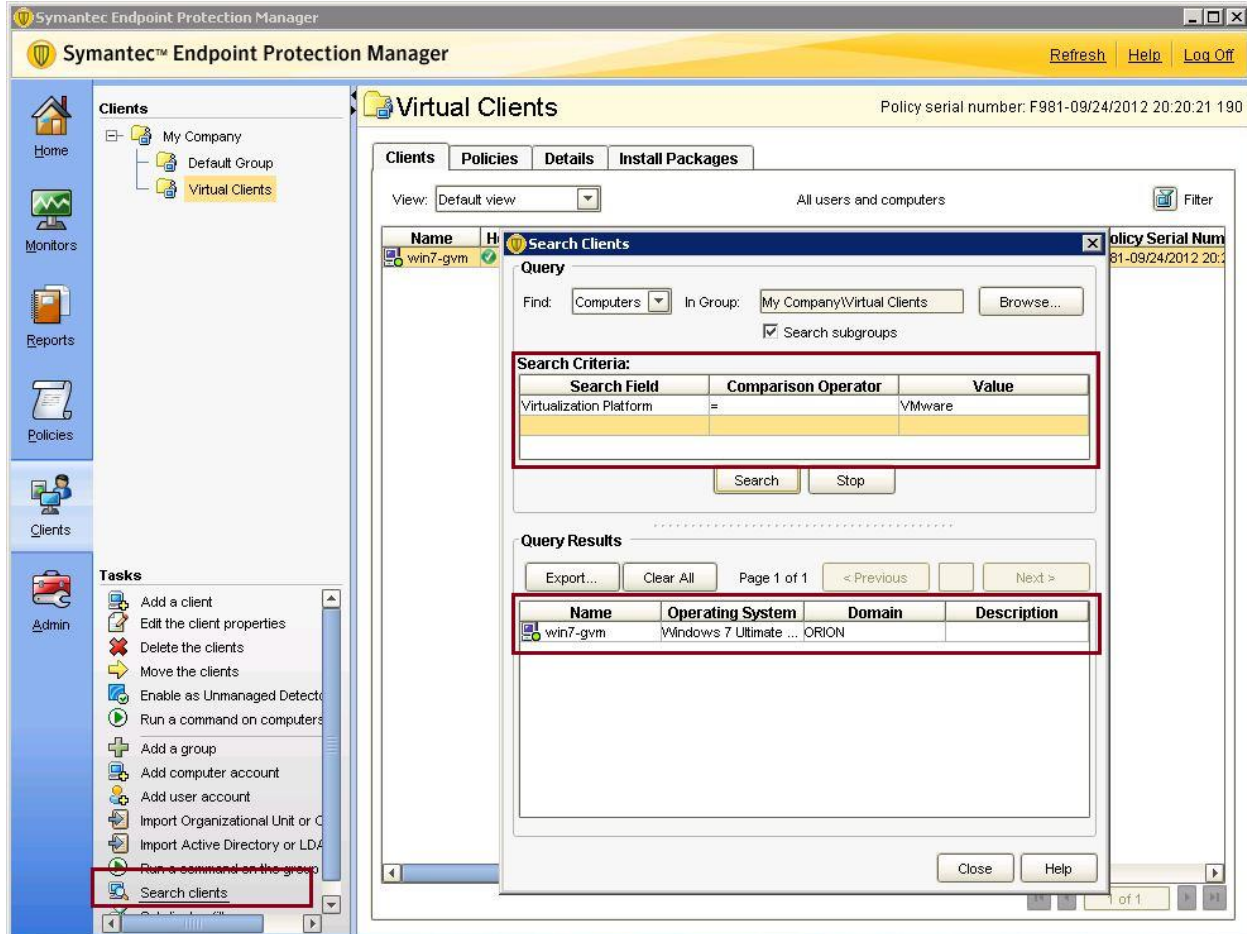
Symantec Endpoint Protection 12.1.2 includes increased performance and security for virtual environments. To take advantage of the increased performance and security you should upgrade all your virtual clients to SEP 12.1.2.

1.2 Grouping Virtual Clients in SEPM

Virtual machines should be put in separate SEP policy groups to allow for proper configuration of the virtual clients. Symantec Endpoint Protection Manager (SEPM) can identify the platform that virtual machines run on. SEPM can identify the VMware vSphere, Microsoft HyperV and Citrix Zen Desktops platforms.



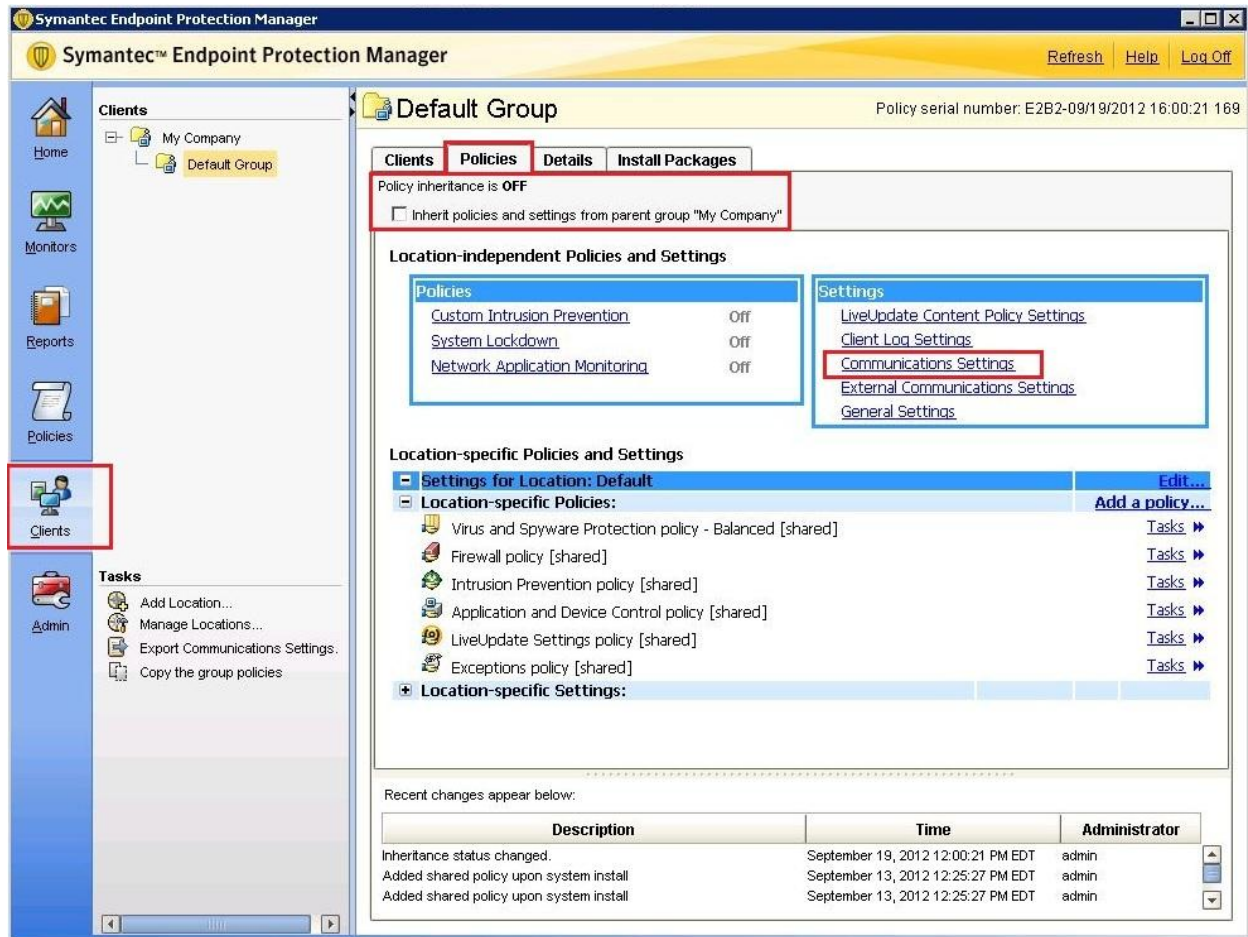
You can use the platform to search for virtual clients. You can then export the list of virtual clients and group them accordingly.



2 Configuring Content Updates

2.1 Updating Virus Definitions directly from the SEPM

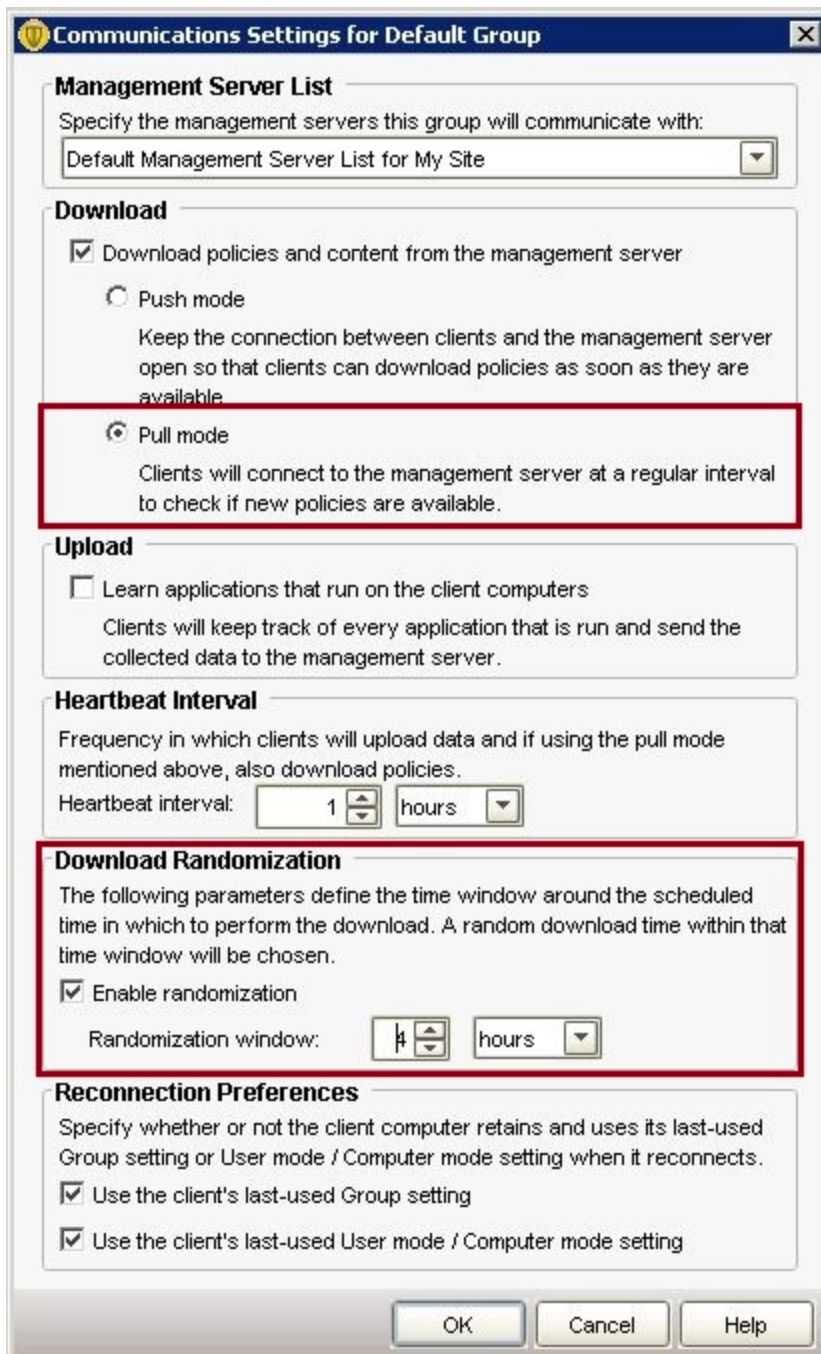
Symantec Endpoint Protection includes a randomization feature in the Communications Settings for clients that optimize performance in a virtual environment. These settings are configured via the communications settings within any group.



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. Enable the “Enable randomization” option.



Communications Settings for Default Group

Management Server List
Specify the management servers this group will communicate with:
Default Management Server List for My Site

Download
☒ Download policies and content from the management server
☐ Push mode
Keep the connection between clients and the management server open so that clients can download policies as soon as they are available.
☒ Pull mode
Clients will connect to the management server at a regular interval to check if new policies are available.

Upload
☐ Learn applications that run on the client computers
Clients will keep track of every application that is run and send the collected data to the management server.

Heartbeat Interval
Frequency in which clients will upload data and if using the pull mode mentioned above, also download policies.
Heartbeat interval: 1 hours

Download Randomization
The following parameters define the time window around the scheduled time in which to perform the download. A random download time within that time window will be chosen.
☒ Enable randomization
Randomization window: 4 hours

Reconnection Preferences
Specify whether or not the client computer retains and uses its last-used Group setting or User mode / Computer mode setting when it reconnects.
☒ Use the client's last-used Group setting
☒ Use the client's last-used User mode / Computer mode setting

OK Cancel Help

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.

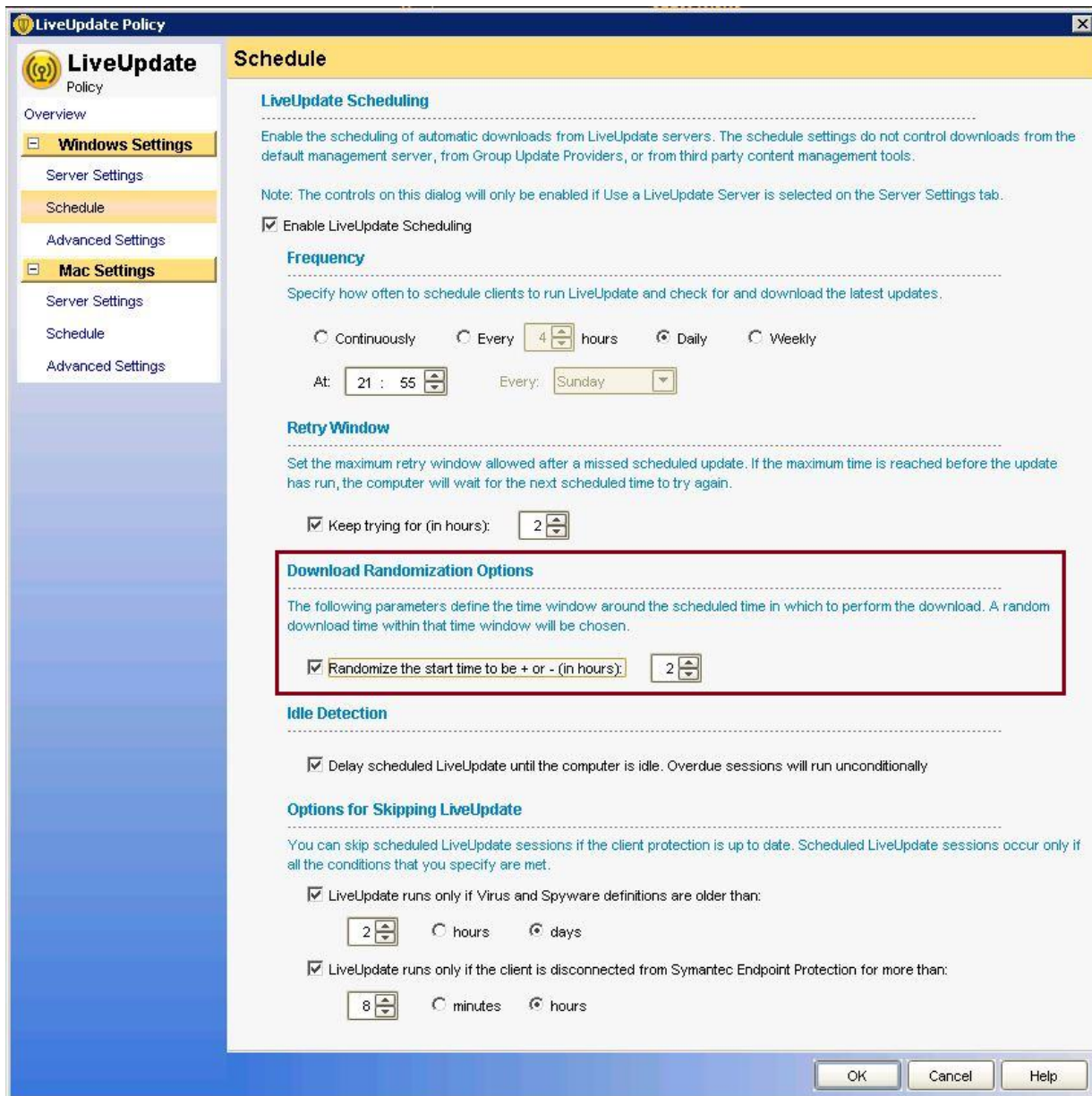
For large scale virtual environments (1000 or more clients) Symantec recommends a heartbeat interval of 1 hour and a download randomization window of at least 2 hours.

2.2 Updating Virus Definitions Using a LiveUpdate Policy

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

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

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. Enable "Use a LiveUpdate Server."
5. In the Schedule dialog box, enable scheduling and configure a schedule during non-peak times.
6. Enable "Download Randomization Options".



LiveUpdate Policy

Policy

Overview

Windows Settings

Server Settings

Schedule

Advanced Settings

Mac Settings

Server Settings

Schedule

Advanced Settings

Schedule

LiveUpdate Scheduling

Enable the scheduling of automatic downloads from LiveUpdate servers. The schedule settings do not control downloads from the default management server, from Group Update Providers, or from third party content management tools.

Note: The controls on this dialog will only be enabled if Use a LiveUpdate Server is selected on the Server Settings tab.

☒ Enable LiveUpdate Scheduling

Frequency

Specify how often to schedule clients to run LiveUpdate and check for and download the latest updates.

☐ Continuously ☐ Every hours ☒ Daily ☐ Weekly

At: : Every:

Retry Window

Set the maximum retry window allowed after a missed scheduled update. If the maximum time is reached before the update has run, the computer will wait for the next scheduled time to try again.

☒ Keep trying for (in hours):

Download Randomization Options

The following parameters define the time window around the scheduled time in which to perform the download. A random download time within that time window will be chosen.

☒ Randomize the start time to be + or - (in hours):

Idle Detection

☒ Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally

Options for Skipping LiveUpdate

You can skip scheduled LiveUpdate sessions if the client protection is up to date. Scheduled LiveUpdate sessions occur only if all the conditions that you specify are met.

☒ LiveUpdate runs only if Virus and Spyware definitions are older than:

☐ hours ☒ days

☒ LiveUpdate runs only if the client is disconnected from Symantec Endpoint Protection for more than:

☐ minutes ☒ hours

OK Cancel Help

3 Configuring Scheduled Scans

3.1 Use active scans instead of full scan

With the increased security capabilities of SEP, Symantec recommends that you configure scheduled scans as active scans instead of full scans. Active scans scan currently running processes as well as critical system areas and result in a small amount of system activity compared to full scans. Full scans are not required to secure the system.

3.2 Enable Scan Randomization

Scheduled scans should be configured to run when activity in the environment is low to minimize the impact. Additionally the scan start time should be randomized over the longest possible window. For virtual environments Symantec recommends at least a 12-hour scan window. For environments where it is critical to minimize the impact of the scan this duration can be configured to run for up to an entire week.

Virus and Spyware Protection Policy

Policy

Overview

Windows Settings

Scheduled Scans:

Administrator-Defined Scans

Protection Technology:

Auto-Protect

Download Protection

SONAR

Early Launch Anti-Malware Driver

Email Scans:

Internet Email Auto-Protect

Microsoft Outlook Auto-Protect

Lotus Notes Auto-Protect

Advanced Options:

Global Scan Options

Quarantine

Miscellaneous

Mac Settings

Scheduled Scans:

Administrator-Defined Scans

Protection Technology:

Auto-Protect

Advanced Options:

Miscellaneous

Edit Scheduled Scan

Operating System: Windows

Scan name: Scheduled Scan for Virtual Clients

Description:

Scan Details

Insight Lookup

Schedule

Actions

Notifications

Scanning Schedule

Specify how often the scan should run:

Scan: ☐ Daily ☒ Weekly ☐ Monthly

At: 19 : 30

On: Saturday

Scan Duration

☐ Scan until finished (recommended to optimize scan performance)

☒ Scan for up to: 12 hours

☒ Randomize scan start time within this period (recommended in VMs)

Missed Scheduled Scans

Specify the retry interval in case the computer is off or unable to start the scan at the scheduled time.

☐ Retry the scan within: 3 days

OK

Cancel

Help

3.3 Enable Shared Insight Cache

If you configure your virtual clients to run scheduled full scans then you should install Shared Insight Cache.

Shared Insight Cache improves performance in virtual infrastructures. Files that Symantec Endpoint Protection clients have determined to be clean are added to the cache. The subsequent scans that use the same virus definitions version can ignore the files that are in the Shared Insight Cache. Shared Insight Cache is used only for scheduled and manual scans.

Shared Insight Cache uses a voting system. After a client uses the latest content to scan a file and determines that it is clean, the client submits a vote to the cache. If the file is not clean, the client does not submit a vote. When the vote count for a file is greater than or equal to the vote count threshold, then Shared Insight Cache considers the file clean. When another client subsequently needs to scan the same file, that client first queries Shared Insight Cache. If the file is marked clean for their current content, then the client does not scan that file. When a client sends a vote to Shared Insight Cache, the cache checks the version of content that the client used to scan the file. If the client does not have the latest content, Shared Insight Cache ignores the vote. If newer content is available, the newer content becomes the latest known content and Shared Insight sets the vote count back to one.

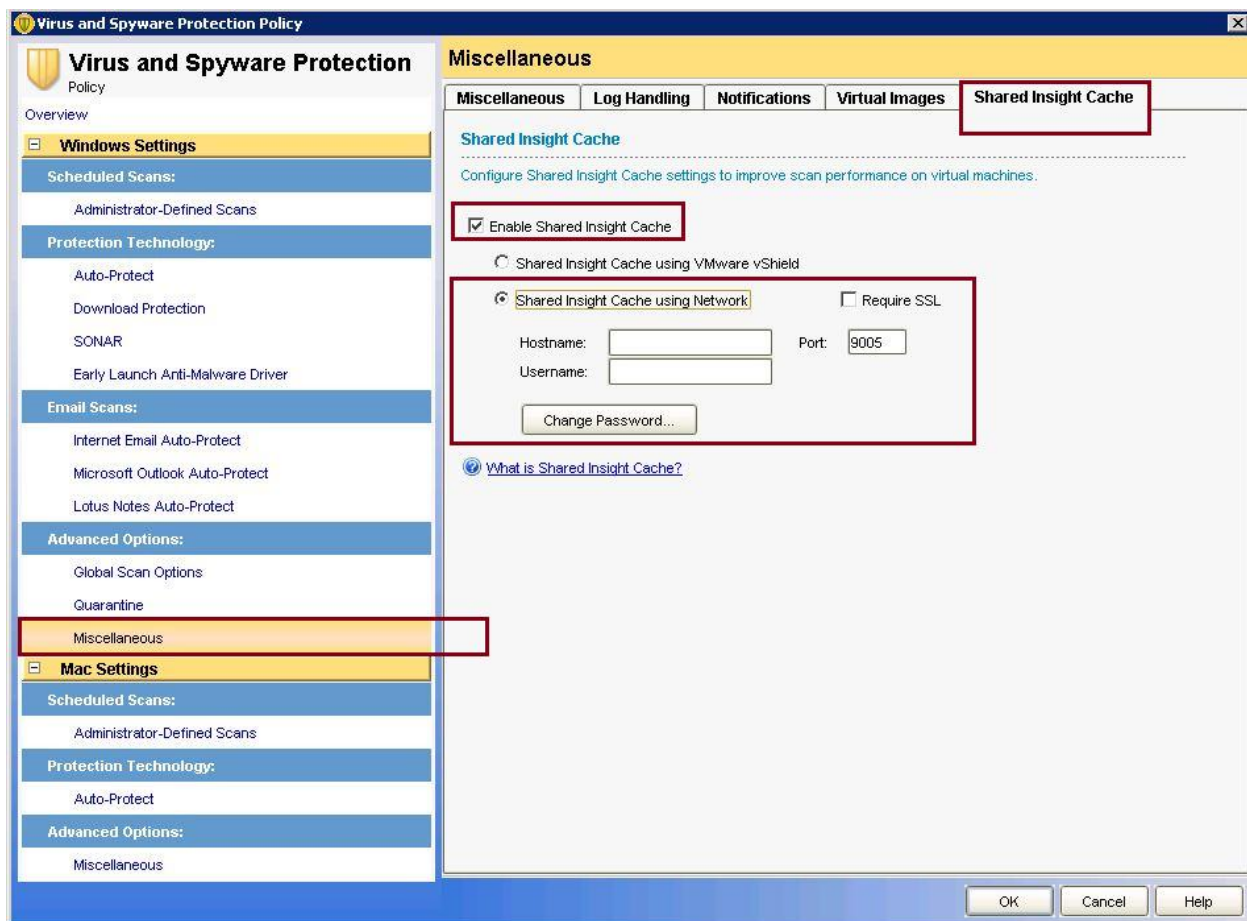
Shared Insight Cache can reduce the impact of full scans by up to 80%. The performance gain from the shared cache is not significant for environments where only active scans are run. Between operating system files, common applications, and common data files there is often significant overlap across systems. The shared cache allows clients to leverage the work already done by other clients in the environment.

3.3.1 Network-based Shared Insight Cache

Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache to reduce scan loads. Network-based Shared Insight Cache requires a dedicated server or virtual machine. Communication between the cache server and the SEP clients happens over an HTTP connection. For optimal security you should configure SSL on the connection and use the username/password authentication option.

To install and configure the Network-based Shared Insight Cache, refer to the topic: “Installing and using a network-based Shared Insight Cache” in the [Symantec Endpoint Protection 12.1.2 Installation & Administration Guide](#).

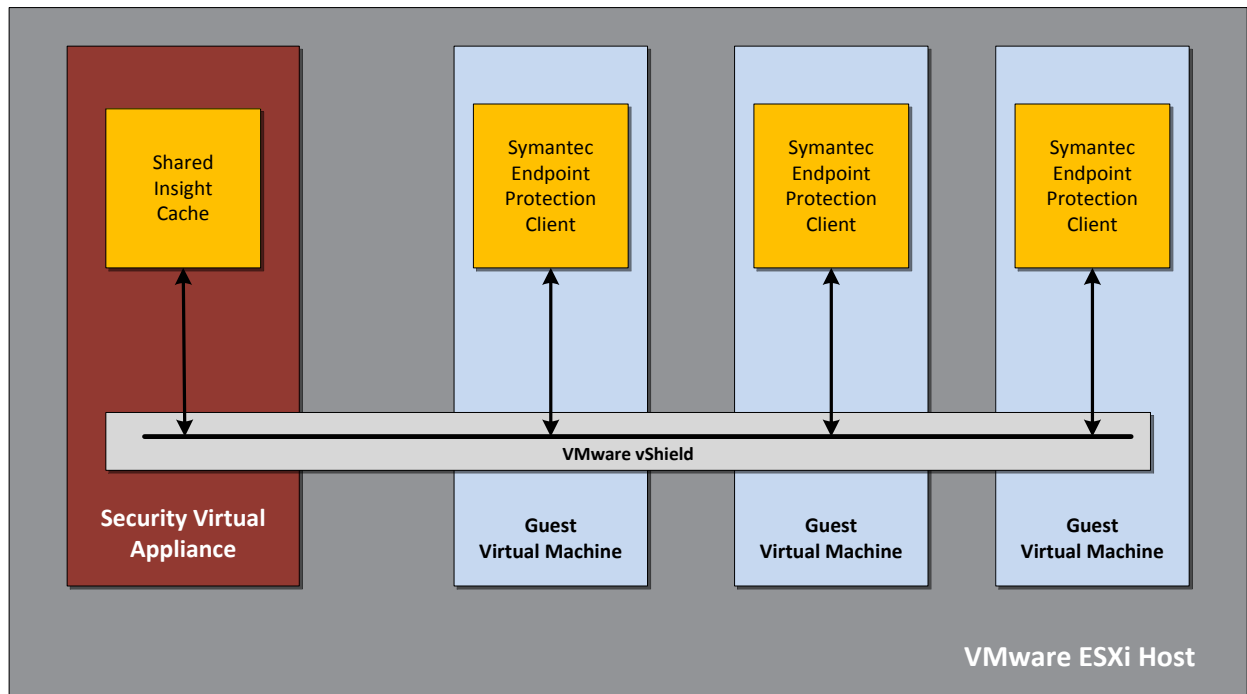
Note: Network-based Shared Insight Cache is only recommended for virtual clients. The feature may be used with physical clients if desired but the network impact may be significant. In most cases physical clients are dispersed across the network. It may be difficult to ensure that communications between the network-based Shared Insight Cache and physical clients are not traversing long distances on the network.



3.3.2 vShield-enabled Shared Insight Cache

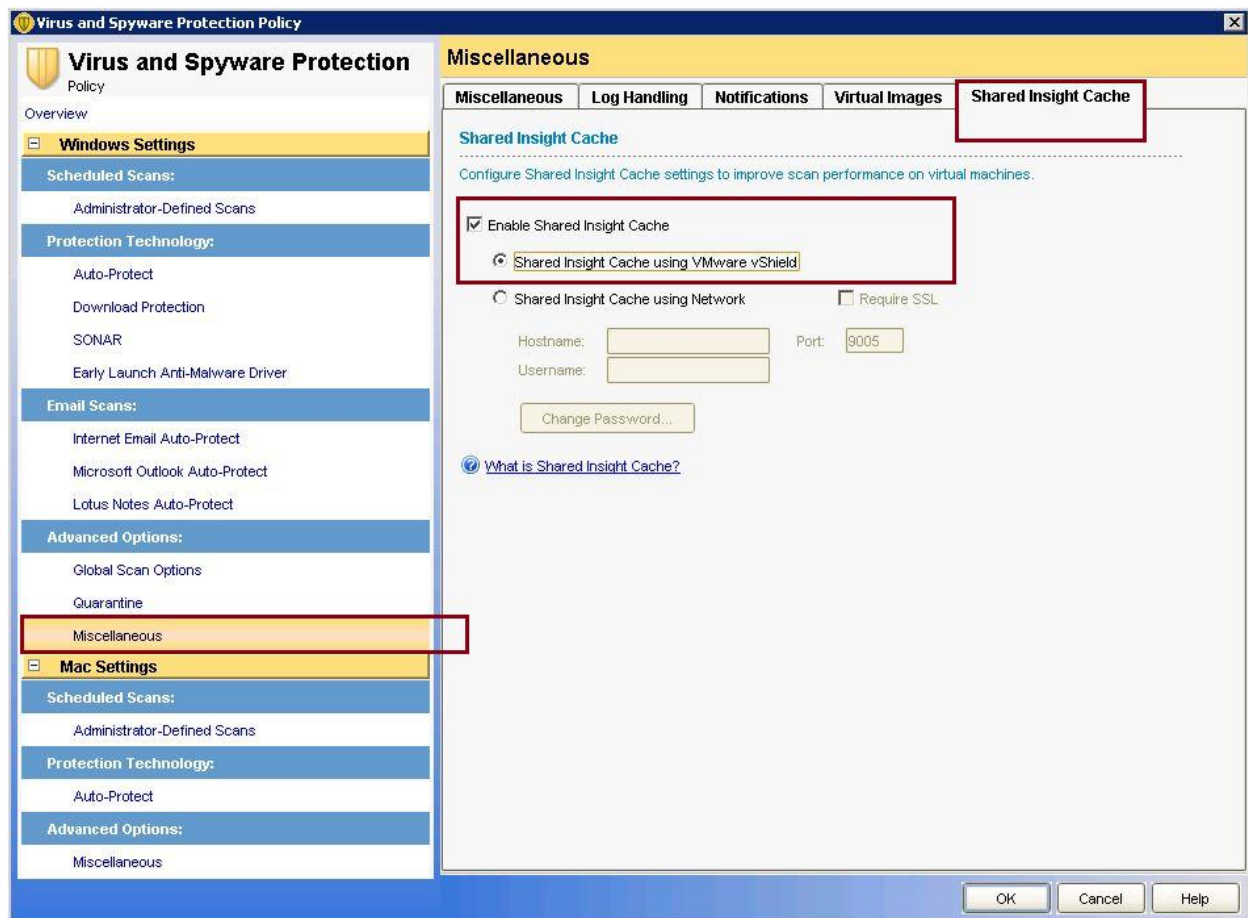
Virtual clients in a VMware vShield infrastructure can use a vShield-enabled Shared Insight Cache to reduce scan loads. A vShield-enabled Shared Insight Cache runs in a Symantec Endpoint Protection Security Virtual Appliance. You must install the appliance so that Windows-based Guest Virtual Machines (GVMs) can use VMware vShield Endpoint to access the Shared Insight Cache.

Note: You must install a Security Virtual Appliance on each ESX/ESXi host where you want the GVMs to access Shared Insight Cache.



To install and configure the vShield-enabled Shared Insight Cache, refer to the topic: “Installing a Security Virtual Appliance and using a vShield-enabled Shared Insight Cache” in the [Symantec Endpoint Protection 12.1.2 Installation & Administration Guide](#).

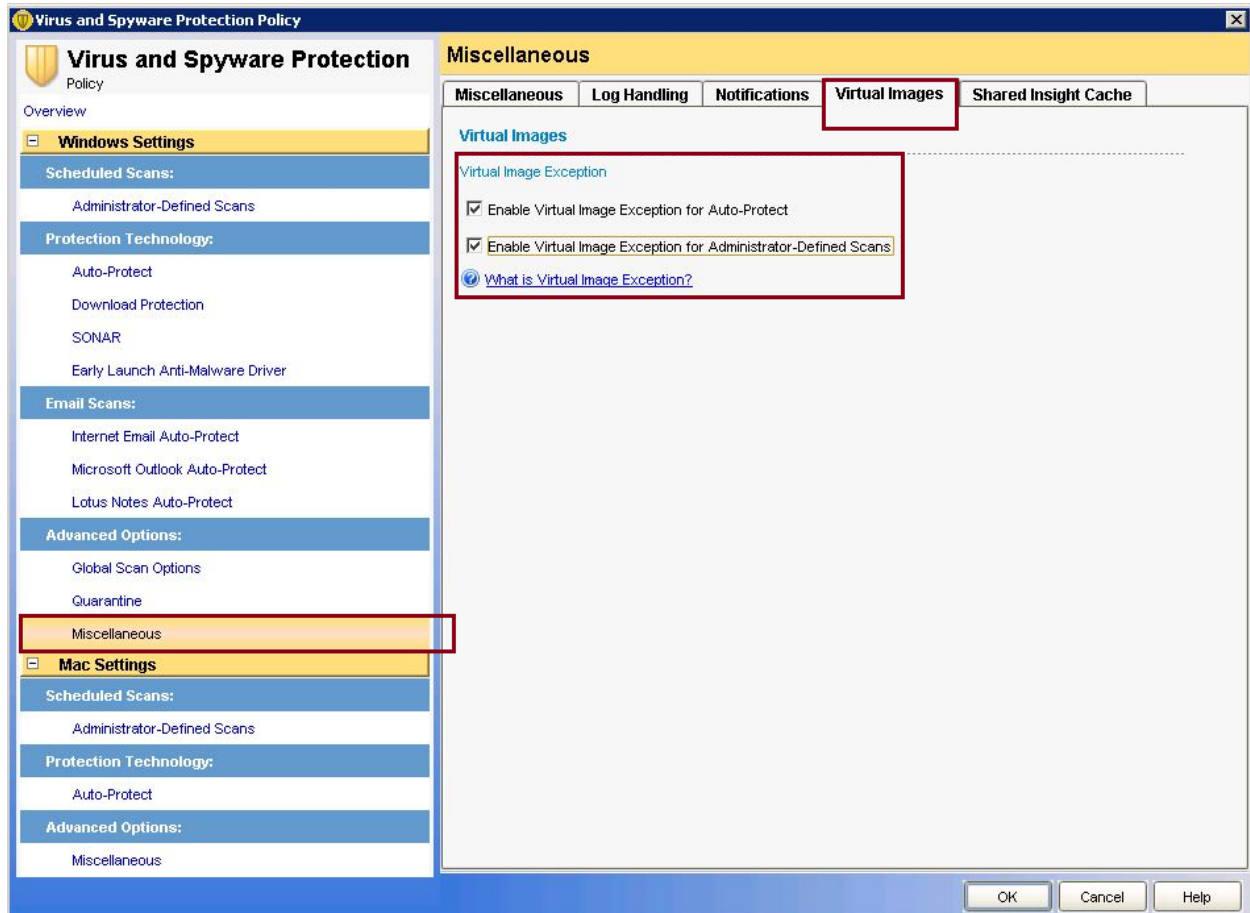
Note: Symantec supports the use of the Security Virtual Appliance only in VMware ESX/ESXi infrastructures.



4 Excluding Base Images using Virtual Image Exception

The Virtual Image Exception feature provides the ability exclude base image files from scanning. This feature involves four steps:

1. Install SEP client in the image and run a full scan to insure the image is not infected.
2. Run the virtual image exception tool against the image prior to deployment to the end user.
3. Remove the tool from the image.
4. Enable virtual image exception in the SEP Virus and Spyware Protection policy. See picture below.



You should use this tool on all images that are deployed in the virtual environment to increase performance of Auto-Protect and scheduled and on-demand scans.

If you are considering installing Shared Insight Cache in your environment you should run the Virtual Image Exception tool with the --hash option to prep the image for the Shared Insight Cache. This will make the Shared Insight Cache run optimally the first time the client scans.

Note: Changing the Windows SID after running the tool will invalidate the data on Windows XP and Windows 2003 operating systems. If you change the Windows SID you must run the tool after changing the value. Windows 2008, Vista, and 7 are not affected by this issue.

Note: You must install the SEP client before you run the Virtual Image Exception tool.

4.1 Monitoring a base image for security threats

As a security best practice Symantec recommends monitoring excluded base images for latent threats. To do this you should run one copy of each excluded image in its default state and use a separate SEP policy with virtual image exception disabled to monitor for threats. If a threat is discovered in an excluded image there are two remediation options.

1. Run the virtual image exception tool using the --clear option to remove the exclusion for the file in question. This needs to be run on each affected client.
2. Disable the virtual image exception feature in the Virus and Spyware Protection policy and scan the systems. After the scan runs and the files are remediated you can re-enable the virtual image exception feature in the policy.

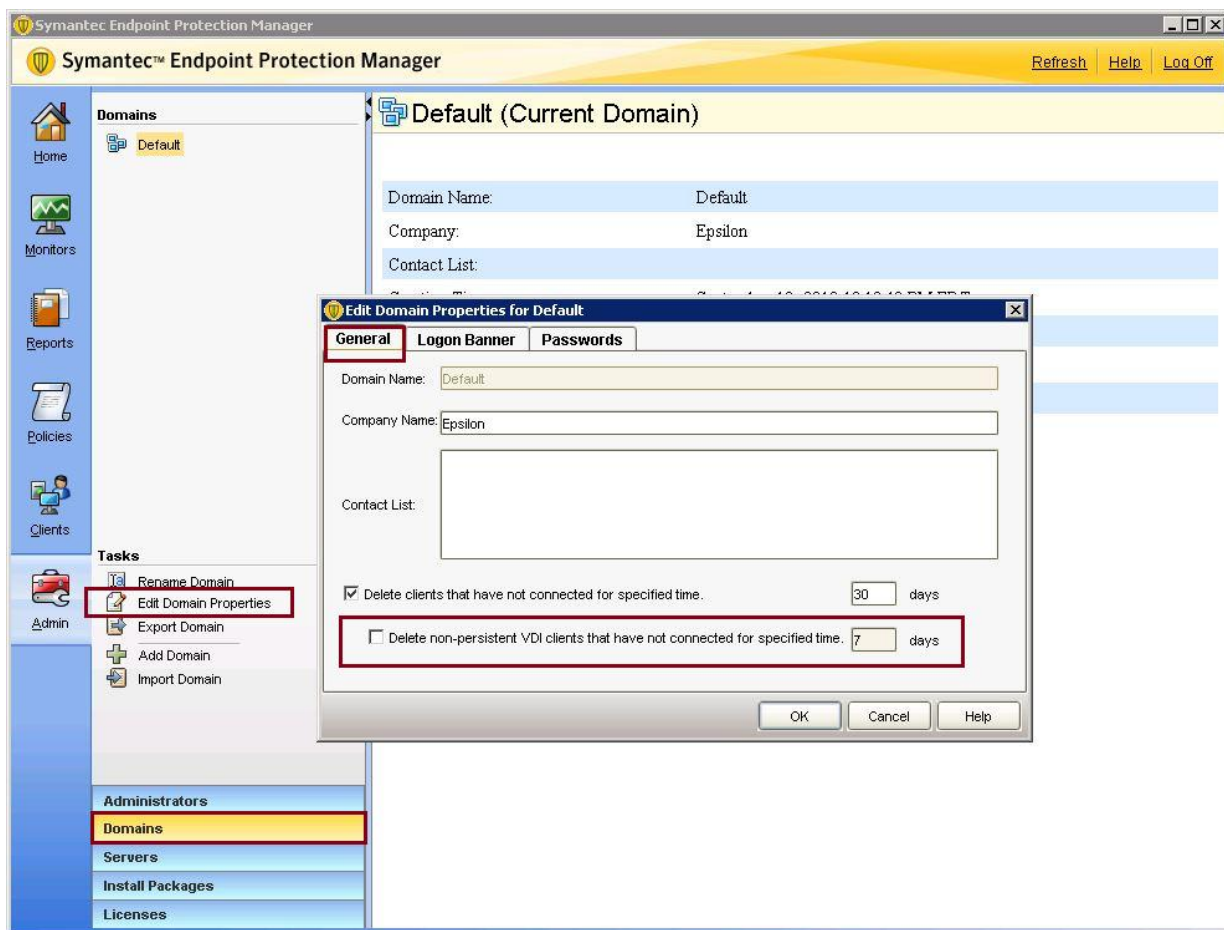
5 Non-persistent VDI

A non-persistent VDI is a VM where typically the VM is created on the fly from a gold master/linked clone when a user logs in. When the user logs out, the VM is deleted and its resources are released. If you are running a non-persistent VDI setup then you should consider the following additional items.

5.1 Identify Non-persistent VDI Clients

A common problem with non-persistent VDI is the case of orphaned clients. Each time a VM is created, the SEP client registers with SEPM. Since the client is active only for the duration of the user's work day, this fills up the SEPM database with entries for clients that are no longer around. Additionally, while the orphaned clients are in the SEPM database, they use up a client license.

You can configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. You can then configure a separate purge interval in Symantec Endpoint Protection for the offline guest virtual machines (GVMs) in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period. This feature makes it simpler to manage the non-persistent GVMs in Symantec Endpoint Protection Manager.



To install and configure the non-persistent VDI clients, refer to the topic: “Non-persistent Virtual Desktop Infrastructures” in the [Symantec Endpoint Protection 12.1.2 Installation & Administration Guide](#).

5.2 Disable Scheduled Scans

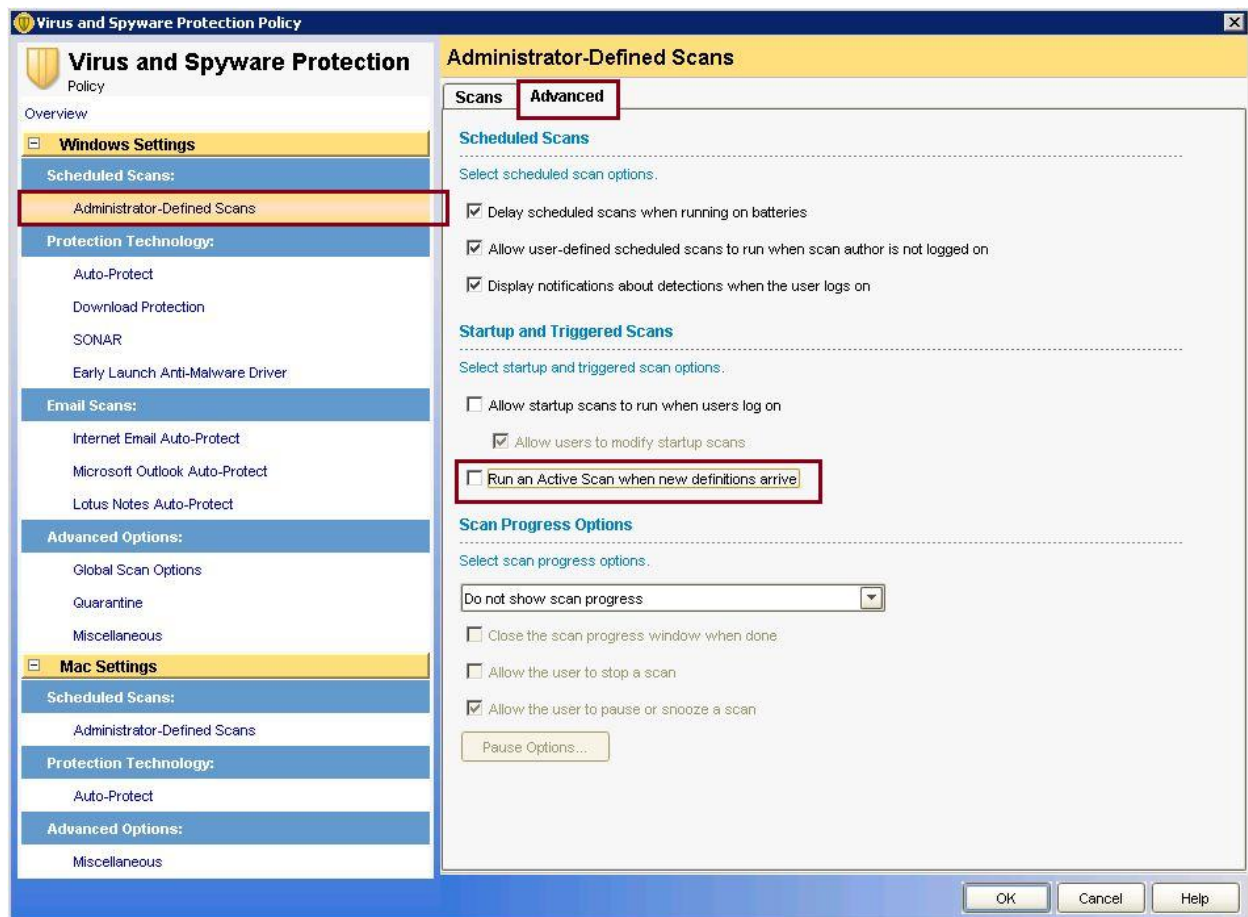
Disable all scheduled scans in non-persistent VDI environments. Scheduled scans are not needed because the image is refreshed with each log in.

5.3 Content Updates

Make sure that you update the definitions as part of the base image update process. This will make sure that when the images are cloned the definitions are as close to current as possible.

Configure the client policy to use SEPM or a GUP to get content. Make sure there are enough deltas saved on the SEPM to ensure that the content download for any given update is not a full download. This means the number of deltas kept should be more than the number of days between image refreshes. So if you plan to refresh your image and update the definitions in the image once a month then you should keep at least 45 days of deltas.

The default settings will run an active scan with each definition update. This is not needed in a non-persistent VDI environment. This setting should be disabled, see picture below.



NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com

Copyright © 2012 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.