SEP 12.1
Best Practices in a Virtual Environment

The document is intended to capture the complete set of best practices for installation and configuration of SEP in a virtual environment.

1 Table of Contents

Contents

2 General Advice

2.1 Upgrade to the latest version

SEP 12.1 includes greatly increased performance and security for virtual environments. To take advantage of the increased performance and security you should be sure to upgrade all your virtual clients to SEP 12.1.

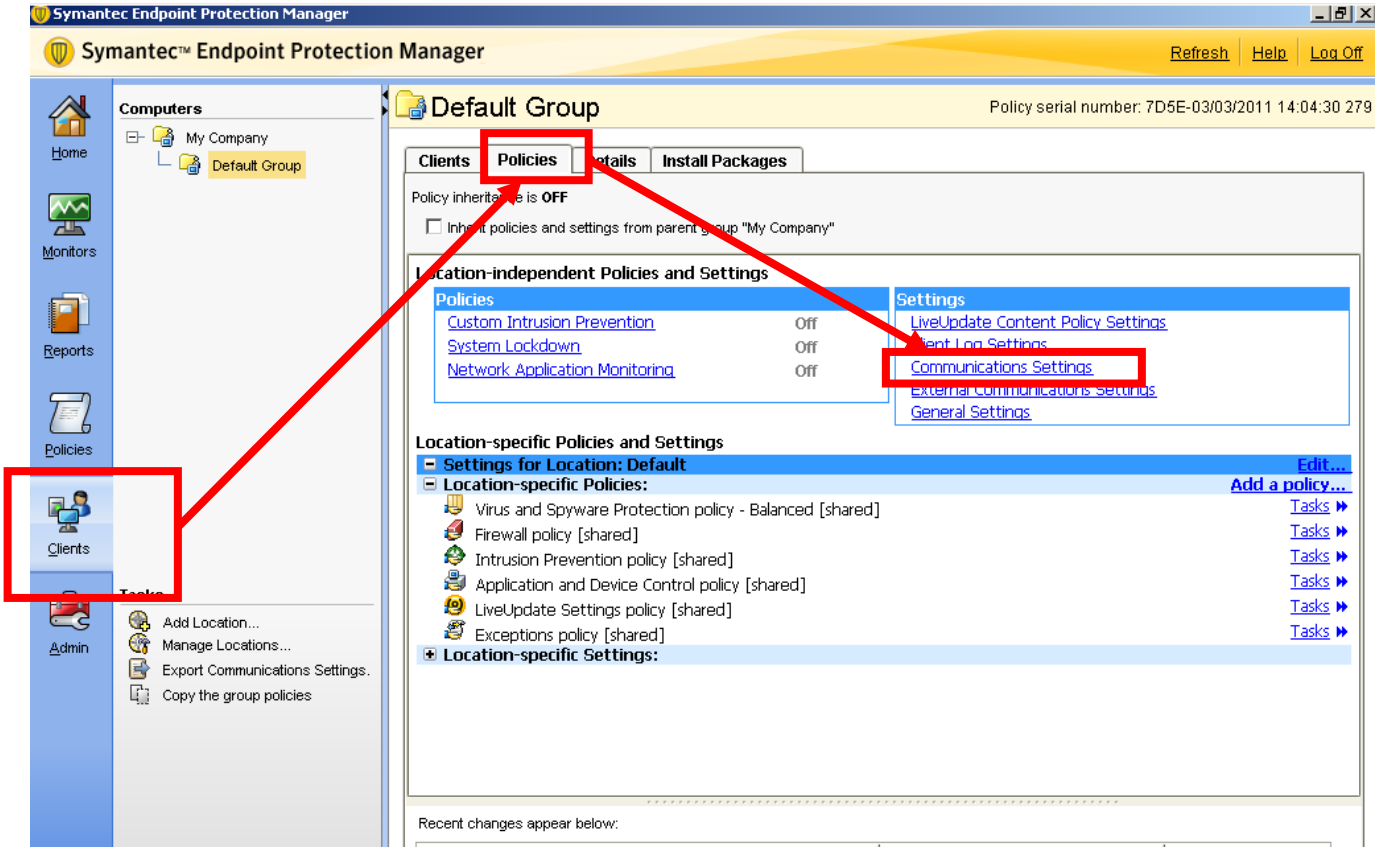
2.2 Client Grouping

Virtual machines should be put in separate SEP policy groups to allow for proper configuration of the virtual clients. The Virtual Client Tagging feature in SEP 12.1 can be used to search for virtual clients in your existing groups. You can then export the list of virtual clients and group them accordingly.

3 Configuring Content Updates

3.1 Updating Virus Definitions directly from the SEPM

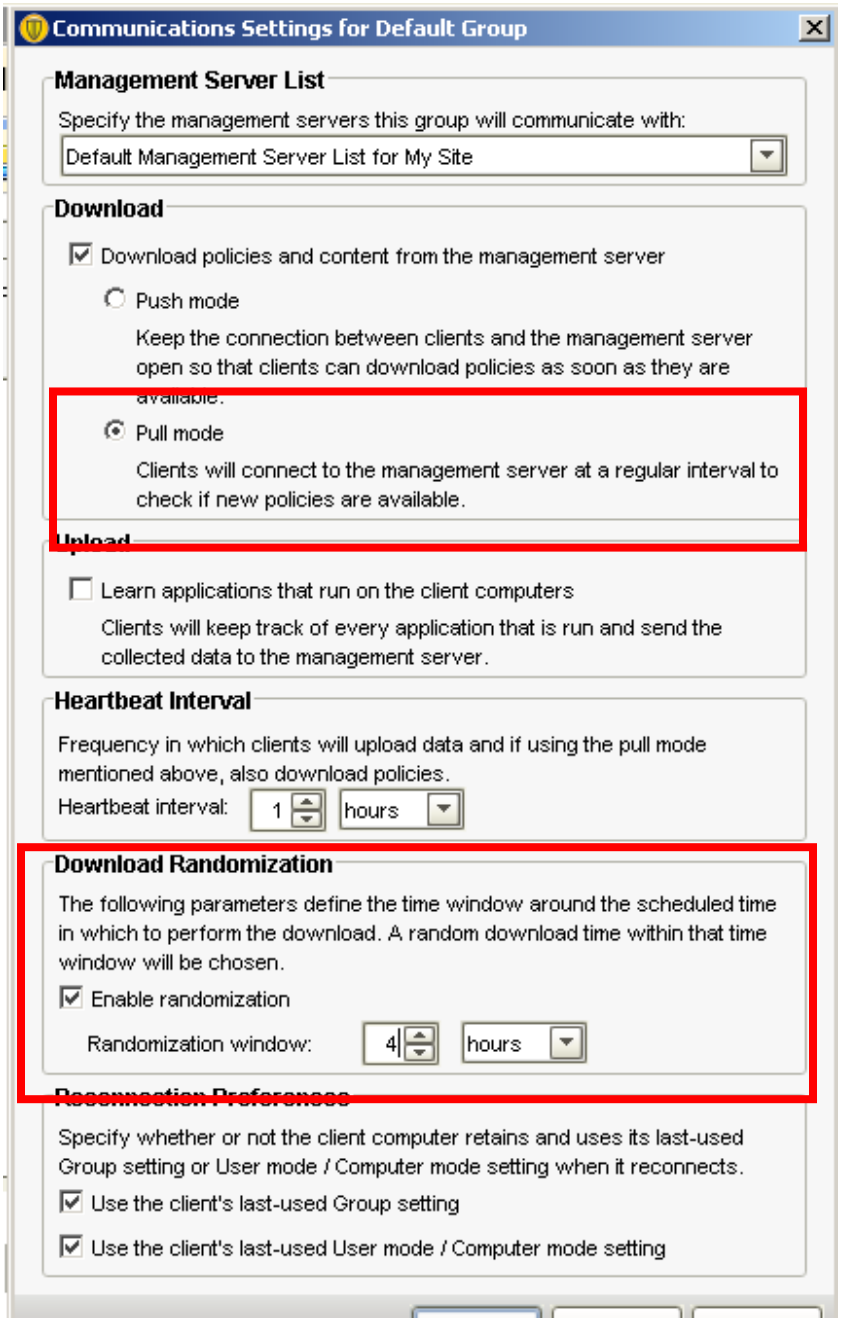
Symantec Endpoint Protection 11 Maintenance Release 3 and above include a randomization feature to the Communications Settings for clients which will optimize performance in a virtual environment. These settings are configured via the communications settings within any group.



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”



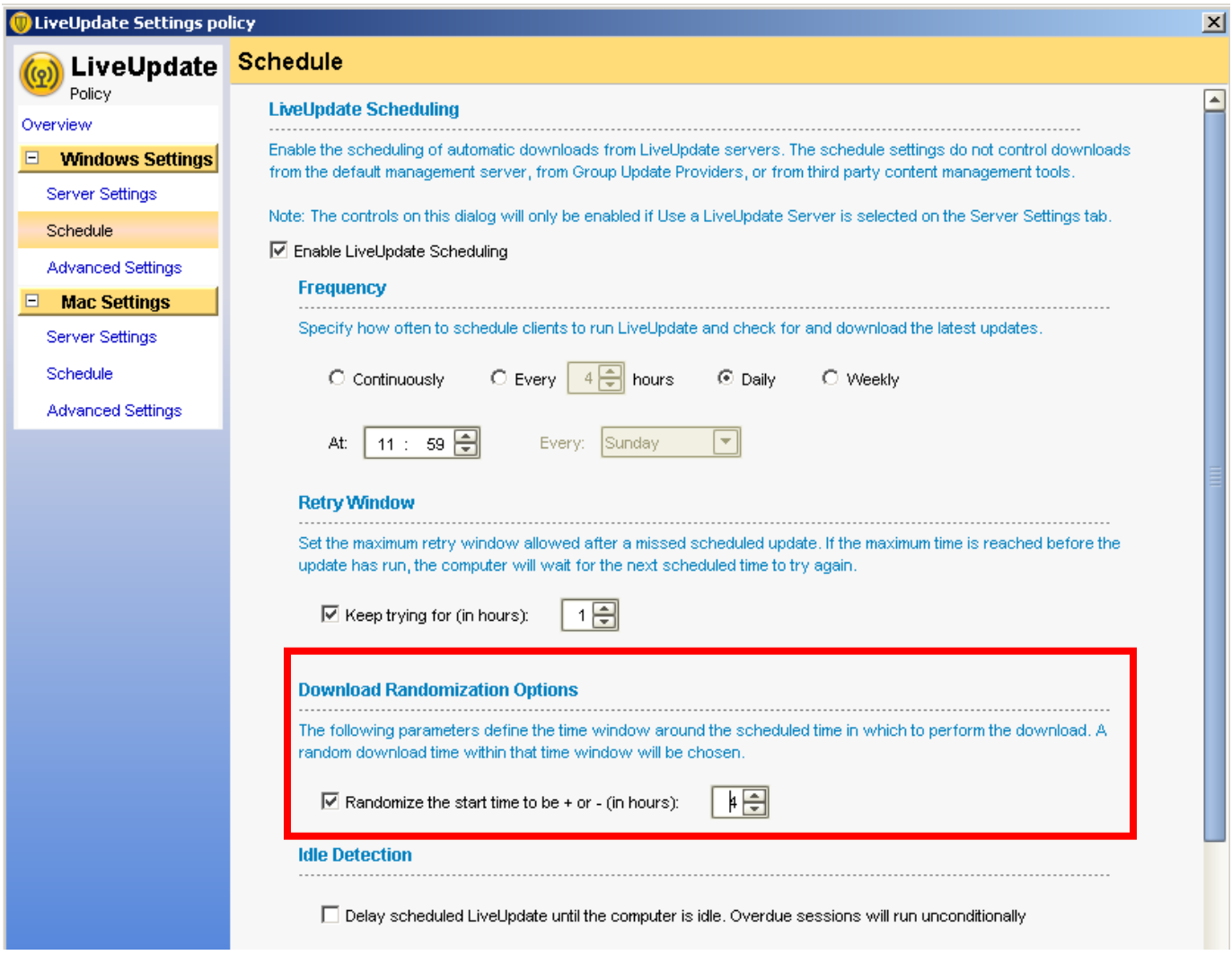
Note: Depending on the number of clients in the virtual environment, consider increasing the heartbeat interval as needed. Additionally, if the time at which clients update virus definitions causes a performance impact, consider increasing the randomization window as needed.

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

3.2 Updating Virus Definitions Using 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 with 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. 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”



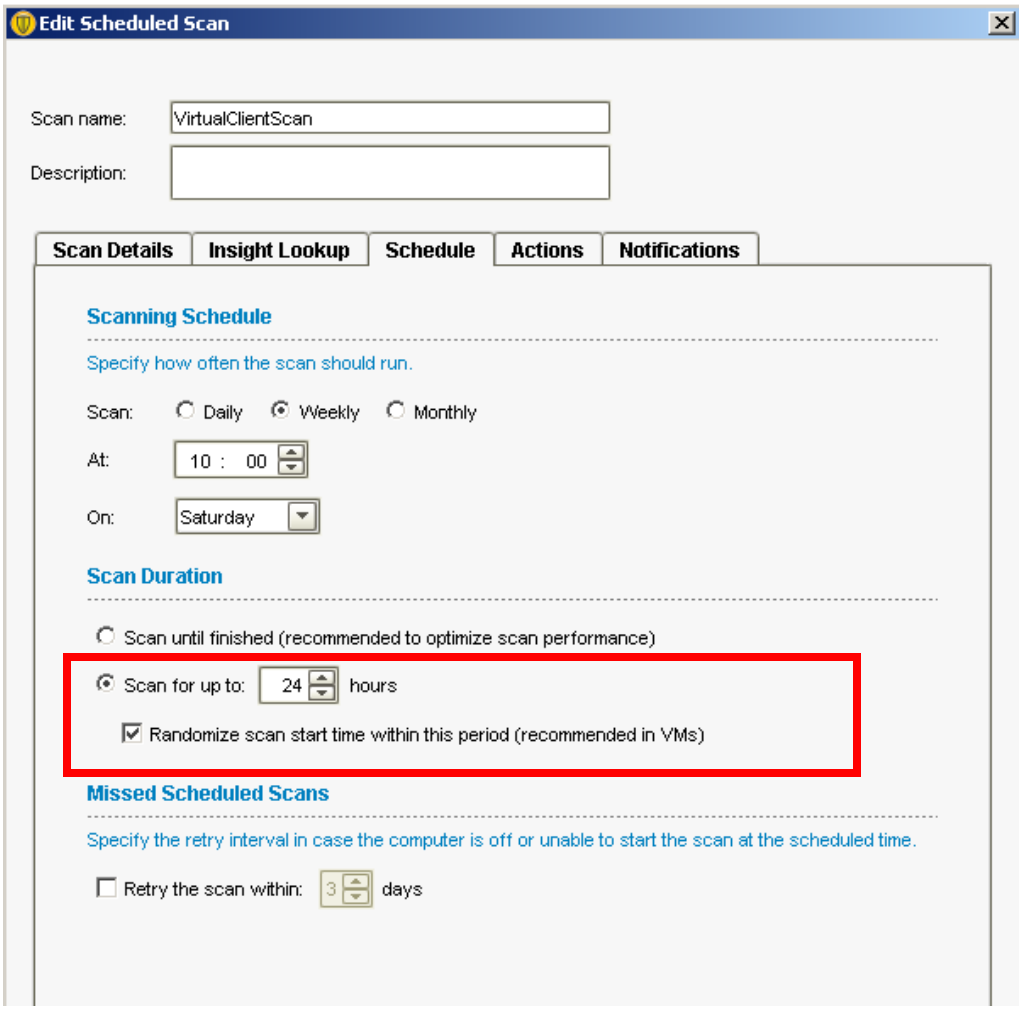
4 Configuring Scheduled Scans

4.1 Use active scan instead of full scan

With the increased security capabilities of SEP 12.1 Symantec recommends scheduled scans be configured as active scans instead of full scans. Active scans will scan currently running processes as well as critical system areas and result in a small amount of system activity when compared to full scans. Full scans are not required to secure the system.

4.2 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.



4.3 Configure the Shared Insight Cache Server if running full scans

If you configure your virtual clients to run scheduled full scans then you should install the Shared Insight Cache Server. The cache server can reduce the impact of full scans by up to 80%. The performance gain from cache server is not significant for environments where only active scans are run.

The Shared Insight Cache Server allows clients to share scan results so that identical files only need to be scanned once across all the clients. Between operating system files, common applications, and common data files there is often significant overlap across systems. The cache server allows clients to leverage the work already done by other clients in the environment.

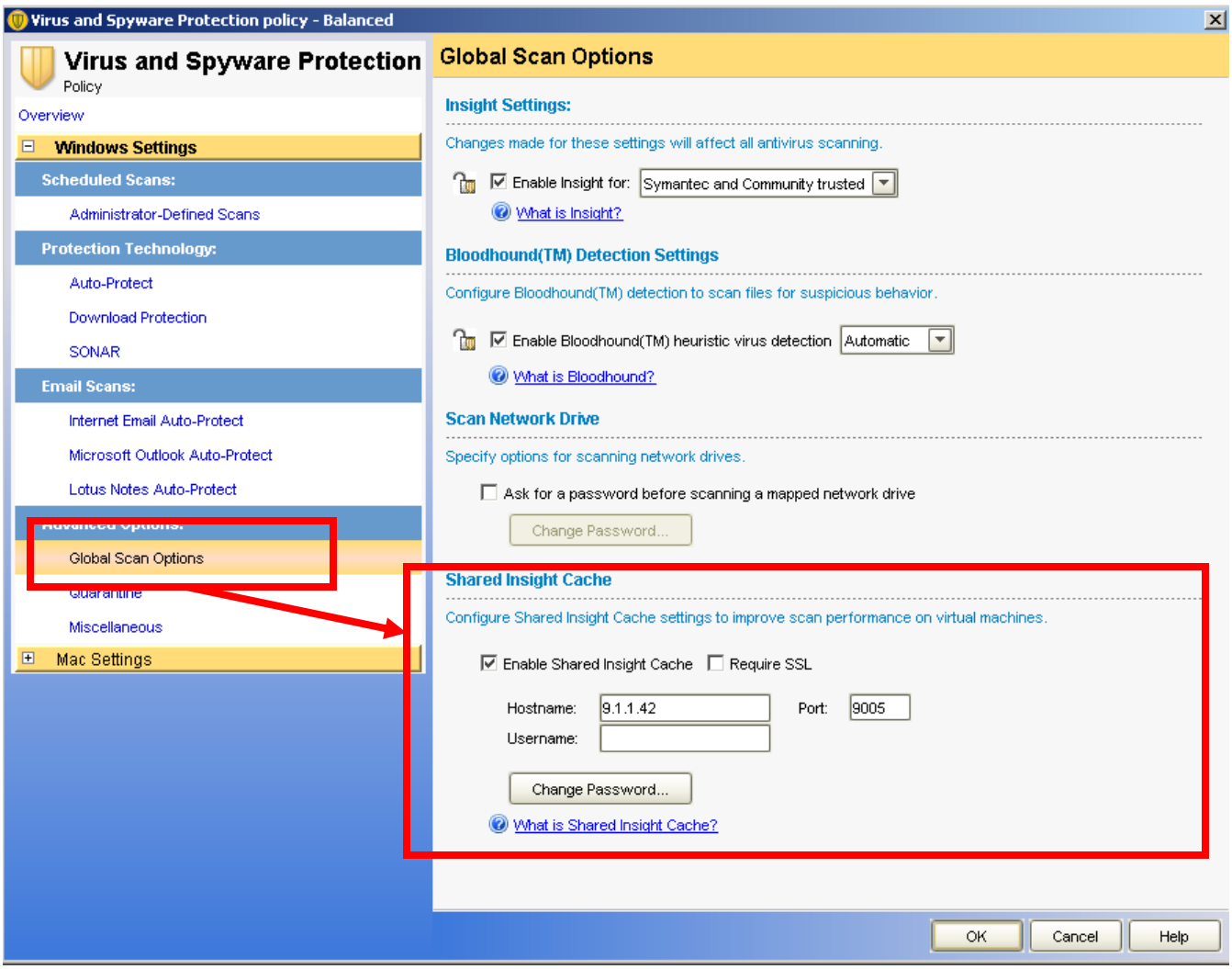
4.3.1 Cache Server System Requirements

The Shared Insight Cache Server runs on a dedicated server or virtual machine and requires the following:

- Windows Server 2008 32 or 64 bit, 64 bit is recommended for best performance
- 30 GB of total disk space
- CPU requirements
    - For less than 100 clients a single core CPU is acceptable
    - For more than 100 clients two CPU cores are recommended
- RAM requirements are dependent on the number of clients in the environment
    - 2 GB for less than 100 clients.
    - 4 GB for 100-1000 clients.
    - 8 GB for over 1000 clients.

4.3.2 Cache Server Configuration

Communication between the cache server and the SEP clients happens over a HTTP connection. For optimal security you should configure SSL on the connection and use the username/password authentication option. To install and configure the cache server please read the Shared Insight Cache administration guide found in the /Tools/SharedInsightCache folder on the SEP DVD. To enable Shared Insight Cache in the client AV policy and enable the feature on the global scan options page, see picture below.



4.3.3 Deciding how many cache servers to install

The following should be considered when deciding where to install the cache server and how many to install:

- Since the calls to the cache server happen over the network it is best to install the cache server in on the same VM cluster as the clients. Cache server connections over long network distances will produce unwanted network traffic and could potentially impact scan times.
- If you have multiple VM clusters in different locations separate cache servers should be used for each location.
- If you have SEP client policies separated into multiple lines of business you may want to install separate cache servers for each line of business to maximize content overlap between systems.

- The Shared Insight Cache Server supports up to 1500 concurrently scanning clients. If you are using scan randomization the cache server can support 1500 clients per hour of the randomization window up to a maximum of 24,000 clients.

    1. Example 1: In an environment running 6 hour randomization window 9,000 clients can be supported on a single cache server.
    2. Example 2: In an environment running 12 hour randomization window 18,000 clients can be supported on a single cache server.
    3. Example 3: In an environment running 16 hour randomization window 24,000 clients can be supported on a single cache server.
    4. Example 4: In an environment running 24 hour randomization window 24,000 clients can be supported on a single cache server.

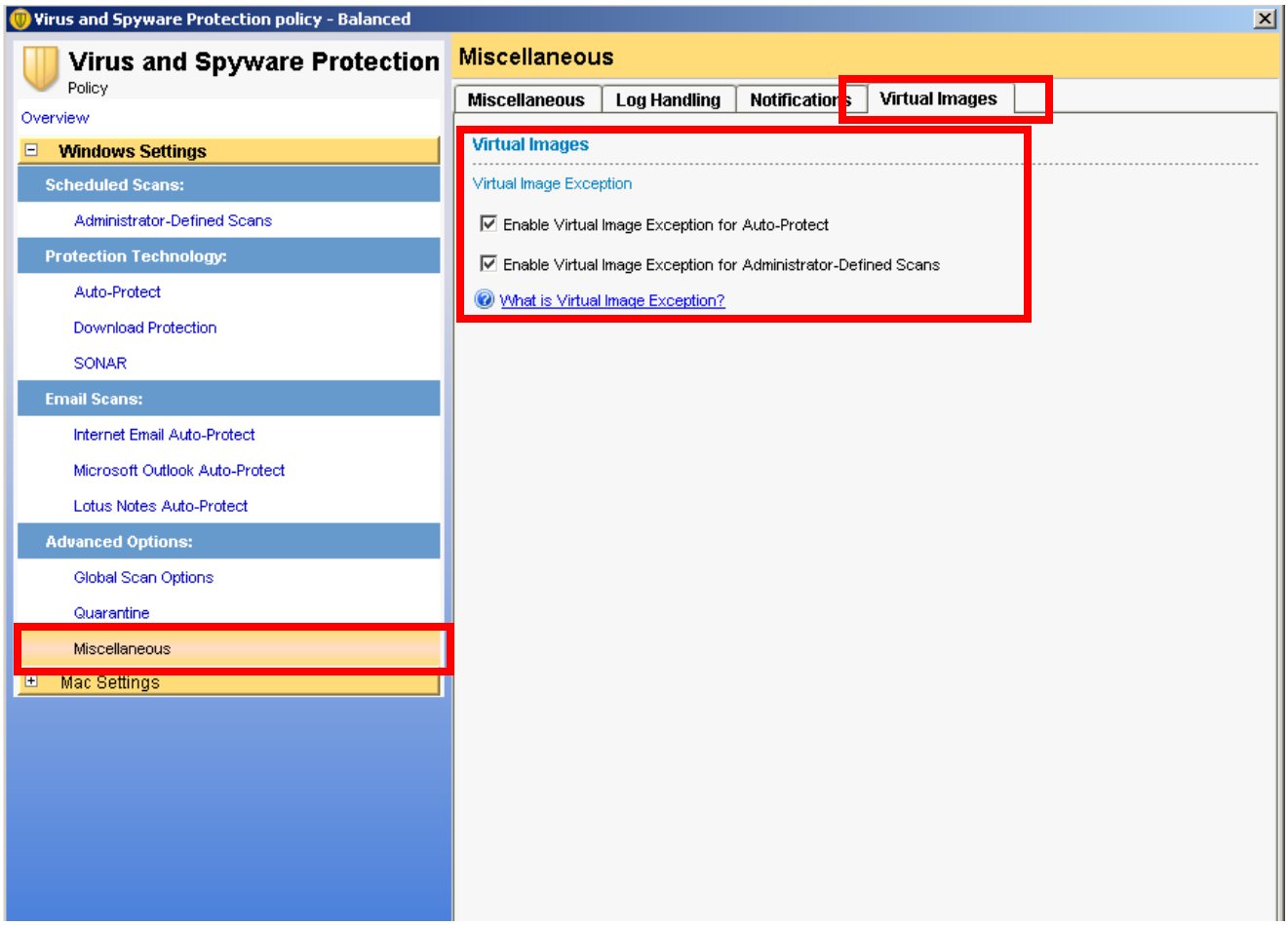
- Only one cache server IP address or hostname can be configured for each SEP policy. If you require multiple cache servers you can either split the SEP policy groups or use DNS or other load balancing methods.

Note: The Shared Insight Cache server 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 be sure the cache server to physical client communications are not traversing long distances on the network.

5 Excluding Base Images

The virtual image exception feature in SEP 12.1 includes 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. The tool and administration guide can be found on the SEP DVD in the /Tools/VirtualImageException folder.
3. Remove the tool from the image.
4. Enable virtual image exception in the SEP AV policy. See picture below.



This should be used for 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 a cache server in your environment you should run the Virtual Image Exception tool with the --hash option to prep the image for the cache server. This will make the cache server run optimally the first time the client scans.

Note: Changing the Windows SID after running the tool will invalidate the data. If you change the Windows SID you must run the tool after changing the value.

Note: The SEP client is required to be installed prior to running the Virtual Image Exception tool.

5.1 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 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 AV policy and scan the systems. After the scan runs and the file is remediated you can re-enable the virtual image exception feature in the policy.