

Overview Best Practices non-persistent VDI's with Symantec Endpoint Protection 14.x

Feature/Configuration	Description	Links
1 Client Recommendations	Client recommendations ensure that SEP clients, in non-persistent VDI environments, generate no network or disk I/O from advanced SEP features that do benefit non-persistent clients. See link and scroll to 'Client Recommendations'.	Deploy Endpoint Protection clients in non-persistent VDI environments Virtualization best practices for Endpoint Protection
2 Shared Insight Cache	Shared Insight Cache (SIC) keeps track of the files that are known to be clean. SIC can reduce the scan load by eliminating the need to rescan those files.	About Shared Insight Cache Using Symantec Endpoint Protection in virtual infrastructures
3 Purging obsolete non-persistent VDI client to free up licences	In the Symantec Endpoint Protection Manager we can configure a separate purge interval for offline non-persistent VDI's	Purging obsolete non-persistent VDI clients to free up licenses
4 Setting up the base image for non-persistent VDI's	This configures the Symantec Endpoint Protection client in the base image to indicate that it is a non-persistent virtual client.	Setting up the base image for non-persistent guest virtual machines in VDIs
5 Virtual Image Exception Tool	The Virtual Image Exception tool lets you mark base image files as safe so that scans skip those files to reduce scan loads.	About the Virtual Image Exception tool Using the Virtual Image Exception tool on a base image
6 Prepare base image for cloning (ClientSideClonePrepTool)	This document (see link) lists the best practices for cloning a Symantec Endpoint Protection (SEP) 14/14.2/14.3 client in either a physical, or virtual, environment. If you do not follow these best practices, then cloned Endpoint Protection clients will have duplicate identifiers, which will result in problems with management and inaccuracies in reporting.	Prepare Endpoint Protection clients for cloning
7 Image Maintenance	Follow these steps to the routine maintenance schedule for base images. See link and scroll down for 'Image Maintenance'.	Deploy Endpoint Protection clients in non-persistent VDI environments

1. Client Recommendations

The following configuration recommendations ensure that SEP clients, in non-persistent VDI environments, generate no network or disk I/O from advanced SEP features that do not benefit non-persistent clients.

- **Make these changes to the Communications Settings policy:**
 - Configure clients to download policies and content in Pull mode
 - Disable the option to Learn applications that run on the client computers
 - Set the Heartbeat Interval to no less than one hour
 - Enable Download Randomization, set the Randomization window for 4 hours

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

Communications Settings for Non-Persistent X

Management Server List
Specify the management servers this group will communicate with:
W2K16 Management Server List

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
☒ Let clients upload critical events immediately

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

- **Make these changes to the Virus and Spyware Protection policy:**

- Disable all scheduled scans
- Disable the option to "Allow startup scans to run when users log on" (This is disabled by default)Disable the option to "Run an Active Scan when new definitions Arrive"

Administrator-Defined Scans

Scans Advanced

Scheduled Scans

Define scans and scan schedules.

Name	Enabled	When	Description
------	---------	------	-------------

Make sure nothing is enabled

Add...

Edit...

Delete

Administrator-Defined Scans

Scans Advanced

Scheduled Scans

Select scheduled scan options.

- ☐ Delay scheduled scans when running on batteries
- ☒ Allow user-defined scheduled scans to run when scan author is not logged on

Scan Progress Options

Select scan progress options.

- Do not show scan progress
- ☐ Close the scan progress window when done
- ☐ Allow the user to stop a scan
- ☒ Allow the user to pause or snooze a scan

Pause Options...

Startup and Triggered Scans

Select startup and triggered scan options.

Note: The Scan Progress Options above are not used for startup or triggered scans.

- ☐ Allow startup scans to run when users log on
- ☒ Allow users to modify startup scans
- ☐ Run an Active Scan when new definitions arrive

2. 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.

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.

Virus and Spyware Protection Policy

Virus and Spyware Protection 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

Linux Settings

Miscellaneous

Miscellaneous

Log Handling

Notifications

Virtual Images

Shared Insight Cache

Shared Insight Cache

Configure Shared Insight Cache settings to improve scan performance on virtual machines.

☒ Shared Insight Cache using Network

☐ Require SSL

Hostname:

Port:

Username:

[Change Password...](#)

 [What is Shared Insight Cache?](#)


3. Purging obsolete non-persistent VDI clients to free up licences

Over time, obsolete clients can accumulate in the Symantec Endpoint Protection Manager database. Obsolete clients are those clients that have not connected to Symantec Endpoint Protection Manager for 30 days. Symantec Endpoint Protection Manager purges obsolete clients every 30 days by default.

If you do not want to wait the same number of days to purge obsolete non-persistent clients, you can configure a separate interval for them. If you do not configure a separate interval, then offline non-persistent virtual clients are purged at the same interval that obsolete physical clients are purged.

To purge obsolete non-persistent VDI clients to free up licenses

1. In the Symantec Endpoint Protection Manager console, on the **Admin** page, click **Domains**.
2. In the **Domains** tree, click the desired domain.
3. Under **Tasks**, click **Edit Domain Properties**.
4. On the **Edit Domain Properties > General** tab, check the **Delete non-persistent VDI clients that have not connected for specified time** check box and change the days value to the desired number. **The Delete clients that have not connected for specified time** option must be checked to access the option for offline non-persistent VDI clients.
5. Click **OK**.

 Edit Domain Properties for ×

General Logon Banner Passwords

Domain Name:

Company Name:

Contact List:

☒ Delete clients that have not connected for specified time. days

☒ Delete non-persistent VDI clients that have not connected for specified time. days

☐ Upload quarantined files from the clients.

OK

Cancel

Help

4. Setting up the base image for non-persistent VDI's

- You can set your base image up to make it simpler to use Symantec Endpoint Protection Manager to manage GVMs in non-persistent virtual desktop infrastructures.

Step	Description
Step 1: Install Symantec Endpoint Protection on the base image.	For more information, see: <ul style="list-style-type: none">• Choosing a method to install the client using the Client Deployment Wizard
Step 2: Disable Tamper Protection in the management server so that you can modify the registry.	For more information, see: <ul style="list-style-type: none">• Changing Tamper Protection settings
Step 3: Make sure that Symantec Endpoint Protection Manager correctly counts the number of licenses for non-persistent virtual clients.	The advantage of non-persistent clients is that offline non-persistent clients do not count toward the number of deployed licenses. Only online clients count. To mark a virtual client as a non-persistent client, you must create a registry key in the base image. For more information, see: <ul style="list-style-type: none">• How to manage the license count for non-persistent VDI clients
Step 4: In Symantec Endpoint Protection Manager, re-enable Tamper Protection.	For more information, see: <ul style="list-style-type: none">• Changing Tamper Protection settings

5. Virtual Image Exception Tool

You can use the Virtual Image Exception tool on a base image before you build out your virtual machines. The Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your virtual desktop infrastructure.

Symantec Endpoint Protection supports the use of the Virtual Image Exception tool for managed clients and unmanaged clients

Step	Action
Step 1	On the base image, perform a full scan all of the files to ensure that the files are clean. If the Symantec Endpoint Protection client quarantines infected files, you must repair or delete the quarantined files to remove them from quarantine.
Step 2	Ensure that the client's quarantine is empty.
Step 3	Run the Virtual Image Exception tool from the command line to mark the base image files. See: <ul style="list-style-type: none">• Running the Virtual Image Exception tool• vietool
Step 4	Enable the feature in Symantec Endpoint Protection Manager so that your clients know to look for and bypass the marked files when a scan runs. See: <ul style="list-style-type: none">• Configuring Symantec Endpoint Protection to bypass the scanning of base image files
Step 5	Remove the Virtual Image Exception tool from the base image.

The Virtual Image Exception tool supports fixed, local drives. It works with the files that conform to the New Technology File System (NTFS) standard.

More information

[System requirements for the Virtual Image Exception tool](#)

6. Prepare base image for cloning (ClientSidePrepTool)

This document lists the best practices for cloning a Symantec Endpoint Protection (SEP) 14/14.2/14.3 client in either a physical, or virtual, environment. If you do not follow these best practices, then cloned Endpoint Protection clients will have duplicate identifiers, which will result in problems with management and inaccuracies in reporting.

For Symantec Endpoint Security (SES) clients, see [Installing Symantec Agent on a client device without automatically enrolling it](#).

These instructions are for Windows clients; for Macintosh clients, see [Deploying Endpoint Protection for Mac as part of a drive image for cloning](#).

Prepare clients for cloning using ClientSideClonePrepTool

1. Install the operating system, needed applications, and all relevant patches.
2. Install the Endpoint Protection client and update with the latest available definitions.
If you prepare a version 12.1.671.4971 client installed on Windows 7 or Server 2008, disable Tamper Protection before proceeding to step 3 to avoid the continual reboot of clients created from the prepared image. For more information, see **Related Articles**.
3. In SEP 14.0 RU1 and above, turn off Application Hardening feature for this client, otherwise clone prep utility might be blocked when Hardening Enforcement policies are applied.
4. Run **ClientSideClonePrepTool.exe**. You must be logged on as a Windows administrator.

Note: For Windows 10 32-bit/64-bit, the ClientSideClonePrepTool.exe tool needs to be run with elevated privileges (e.g. "Run as administrator").

This tool removes all Symantec Endpoint Protection client identifiers and leaves the Symantec Endpoint Protection services stopped. Using this tool should be the last step in the image preparation process, before running Sysprep and/or shutting down the system. Shut down the system after running clone prep; do not restart. If the system or the Symantec Endpoint Protection client services are restarted, then new identifiers are generated and you must run the tool again before cloning.

Silently prepare clients for cloning using manual steps

The ClientSideClonePrepTool does not run silently, but you can script the following steps as a silent alternative. If you script these steps, you must [disable Tamper Protection](#) on the Symantec Endpoint Protection client.

1. Run **smc -stop**.
2. Delete all instances of sephwid.xml and communicator.dat on the file system. Possible locations:
 - o C:\
 - o C:\Program Files\Common Files\Symantec Shared\HWID\
 - o C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config
 - o C:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\PersistedData\
 - o C:\ProgramData\Symantec\Symantec Endpoint Protection\PersistedData\
 - o C:\Users\All Users\Symantec\Symantec Endpoint Protection\PersistedData
 - o C:\Windows\Temp\
 - o C:\Documents and Settings*\Local Settings\Temp\
 - o C:\Users*\AppData\Local\Temp\
3. Delete the following registry values:
 - o HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink\ForceHardwareKey
 - o HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink\HardwareID
 - o HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink\HostGUID

7. Image Maintenance

Add these steps to the routine maintenance schedule for base images. Symantec recommends that you perform these maintenance tasks at least once a week.

1. Update all applicable definitions and security content on the base image with the latest content available
2. Confirm the SEP client on the base image is able to communicate with its SEPM server(s)
3. Confirm the SEP client is using the correct VDI-specific policies
4. Before you redistribute the image:
 - Remove any temporary files associated with the SEP client, including
 - Remove hardware key information from the base image. See Prepare Endpoint Protection clients for cloning.
 - Navigate to one of the following registry keys:
 - On 32-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
 - On 64-bit systems: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\
 - Create a new subkey named **Virtualization**
 - In the Virtualization sub-key, create a key of type **DWORD** named **IsNPVDIClient** and assign it a value of 1.

Follow the general best practices below for periodic image maintenance and testing.

1. Manually upgrade the SEP client on the base image rather than using AutoUpgrade for the VM client policy groups
2. Test performance optimizations. For instance, reduced memory allocated to a VM can cause increased operating system (OS) swapping and defeat hypervisor optimizations like memory page deduplication
3. To minimize the size of the base VM image, disable the client to install cache and set content cache revisions to 1. See [About Content Cache Control](#).
4. Configure VM refreshes to occur on logoff. Set the pool of available VM's large enough so that users can easily access a running image that was updated in the background.