Enabling Mac clients to download LiveUpdate content using the Apache Web server as a reverse proxy

Article ID: HOWTO85034 | **Created**: 2013-08-06 | **Updated**: 2014-03-20

How To for Endpoint Protection 12.1 12.1 RU4, Network Access Control 12.1 12.1 RU4, Endpoint Protection 12.1 12.1 RU4a

In Symantec Endpoint Protection (SEP) 12.1.4 (12.1 RU4) and later, you have at least two options for downloading LiveUpdate (LU) content to SEP for Mac clients.

1. Use Symantec LiveUpdate Administrator 2.x (LUA 2.x). This is the best option for installations with larger numbers of Macintosh computers.
2. For smaller installations, configuring the Apache Web server as a reverse proxy works well. This enables the Apache Web server installed along with Symantec Endpoint Protection Manager (SEPM) to download and cache the LU content for Mac clients locally whenever new content is published. This results in saving of external network bandwidth.

Below are the instructions to set up the Apache Web server in SEPM to allow SEP for Mac clients to download LiveUpdate (LU) content via the Web server. Please note that this solution enables the SEPM to act as a cache: it does not process Mac definitions into .dax files as it does with Windows content. It does not enable SEP for Mac clients to update from a Group Update Provider (GUP).

Note: You can only make these configuration changes on the enterprise version of SEP. These instructions do not apply to Symantec Endpoint Protection Small Business Edition (SEP SBE).

Configure Apache Web server in SEPM

Take the following steps to configure Apache Web server to serve as a reverse proxy:

1. Stop `semwebsrv` (SEPM Webserver) and `semsrv` (SEPM).

2. Create a **`cache-root`** folder under your SEPM installation folder. The result, using the default path, is:

   ```
   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\cache-root
   ```

   If your SEPM installation uses a different path, place the cache-root folder under

   ```
   %Your SEPM_Install_Folder%\apache
   ```

   Ensure that the account running SEPM Webserver has full control on this folder.

3. Verify if the below mentioned files are present in the following folder:

   ```
   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
   ```

```
Manager\apache\modules
```

```
mod_cache.so, mod_disk_cache.so, mod_proxy.so,
mod_proxy_http.so, mod_setenvif.so
```

4. If the files are not present in the mentioned location, please copy the files from the DVD or downloaded installation folder: `\Resource\Apache-ReverseProxy`
   to
   `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\modules`

   Note: If the files are not present at the above mentioned location on the DVD, please refer to the section "Security and Compatibility" for more details.

5. Make a backup of the original configuration file:

   1. Go to `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf\`
   2. Copy `httpd.conf` to `httpd-orig.conf`

6. Add the following lines to the end of `httpd.conf`. Replace the local path in the text below with the actual path of your SEPM installation.

```
# SEPM_APACHE_AS_PROXY_START Preserve this line to maintain
configuration across SEPM upgrades
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule cache_module modules/mod_cache.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule setenvif_module modules/mod_setenvif.so


<IfModule mod_proxy.c>
  <IfModule mod_cache.c>
    <IfModule mod_disk_cache.c>
        <IfModule mod_setenvif.c>
          SetEnvIf Request_URI "/luproxy/" dolog
          SetEnvIf Request_URI "/luproxy/.*_livetri.zip" no-
cache
          CustomLog "|| bin/rotatelogs.exe logs/access-%Z.log
25M" common env=dolog
        </IfModule>
        ProxyPass /luproxy/
http://liveupdate.symantecliveupdate.com/ retry=0 smax=0
ttl=60
        CacheRoot "C:/Program Files (x86)/Symantec/Symantec
Endpoint Protection Manager/apache/cache-root"
        CacheEnable disk /luproxy/
        CacheDirLevels 1
        CacheDirLength 5
        #allow downloads up to 1 GB
        CacheMaxFileSize 1000000000
    </IfModule>
   </IfModule>
</IfModule>
# SEPM_APACHE_AS_PROXY_END Preserve this line to maintain
configuration across SEPM upgrades
```

7. Start `semwebsrv` (SEPM Webserver) and `semsrv` (SEPM).

8. Test that the proxy server is running by downloading an LU file:

   Click **Start > Run**, and then type **`http://localhost:8014/luproxy/masttri.zip`** and press **Enter**.

   If your SEPM Apache web server uses a different port than 8014, replace 8014 with your actual port number in the above URL.

9. The LU download requests to the Apache web server are logged in a separate log file:

   ```
   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
   Manager\apache\logs\access-%Z.log
   ```

Update LiveUpdate policy for Mac clients to point to new LiveUpdate server

Take the following steps to update your LiveUpdate policy for Mac clients for your desired groups. Once the policy is updated, Mac clients will point to the newly configured Apache Web server for downloading LU content.

1. Within the SEPM, click **Policies > LiveUpdate**. On the LiveUpdate Settings tab, double-click the LiveUpdate Settings policy that applies to your desired groups.

2. Click **Use a specified internal LiveUpdate Server** under **Mac Settings > Server Settings** and specify the name "SEPM HTTP LU Proxy," with the corresponding URL: `http://<ServerIP or ServerName>:8014/luproxy`

   If your SEPM Apache web server uses a different port that 8014, replace 8014 with your actual port number in the above URL.

3. Add Symantec LiveUpdate server as a fallback mechanism (this is optional, because this is always a fallback option). Use the following address:

   ```
   http://liveupdate.symantecliveupdate.com
   ```

4. Enable download randomization under **Mac Settings > Schedule**. If the option is not greyed out, check **Randomize the start time**. This prevents the Apache web server from getting overloaded at certain times in a day.

Managing Cache file size

To manage the size of your cache file, take the following steps.

1. Verify if the `htcacheclean.exe` file is present in the following folder:

   ```
   C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
   Manager\apache\bin
   ```

2. If the file is not present in the mentioned location, copy `htcacheclean.exe` from the `\Resource\Apache-ReverseProxy` folder on your DVD to:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
Manager\apache\bin
```

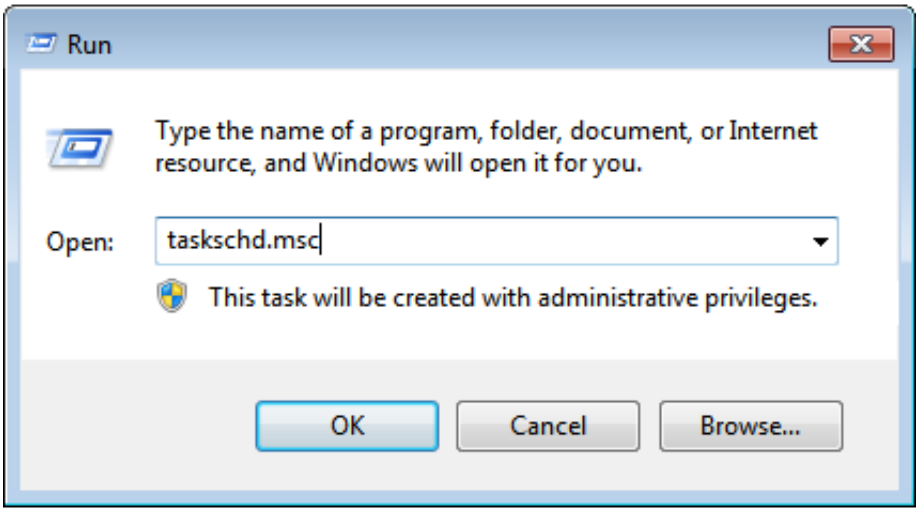
3. Run the following command from an account having full access rights on the `cache-root` folder:

```
htcacheclean -n -t -d1440 -l1024M -p"C:/Program Files
(x86)/Symantec/Symantec Endpoint Protection
Manager/apache/cache-root"
```

This will run the `htcacheclean` tool in daemon mode. The cache cleaning will be done on a daily interval. The maximum cache size allowed on disk is 1 GB.

To automatically start the `htcacheclean` daemon every time Windows starts, take the following steps.

1. Hold down the Windows key on your keyboard and press the letter **R** to open the **Run** dialog and then type `taskschd.msc` and click **OK**.



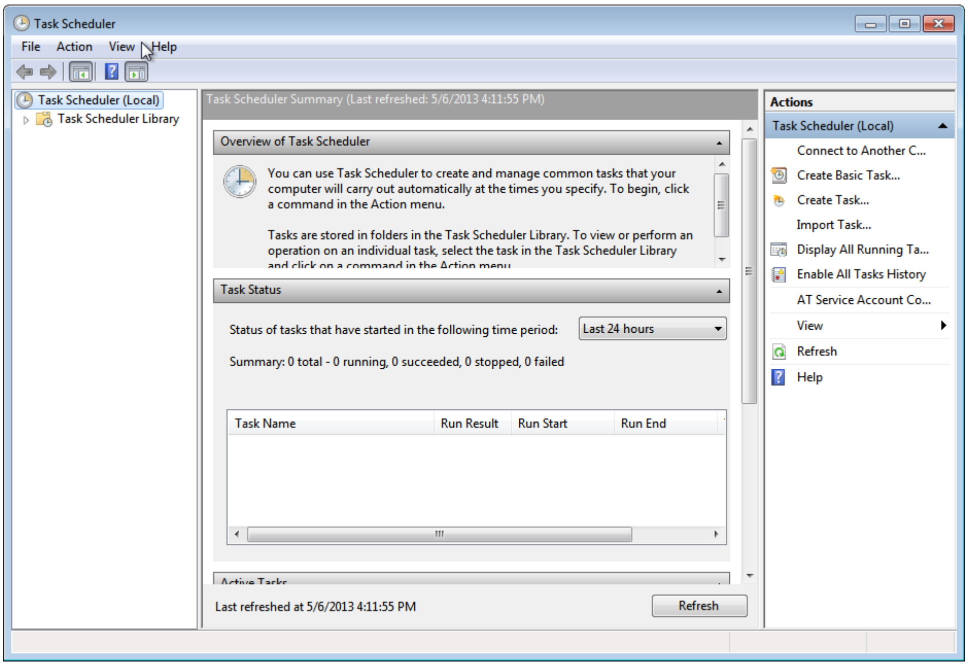
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: taskschd.msc

This task will be created with administrative privileges.

2. In the Task Scheduler, click on the **Create Basic Task…** action on the right side of the dialog:



Task Scheduler Summary (Last refreshed: 5/6/2013 4:11:55 PM)

Overview of Task Scheduler

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Task Status

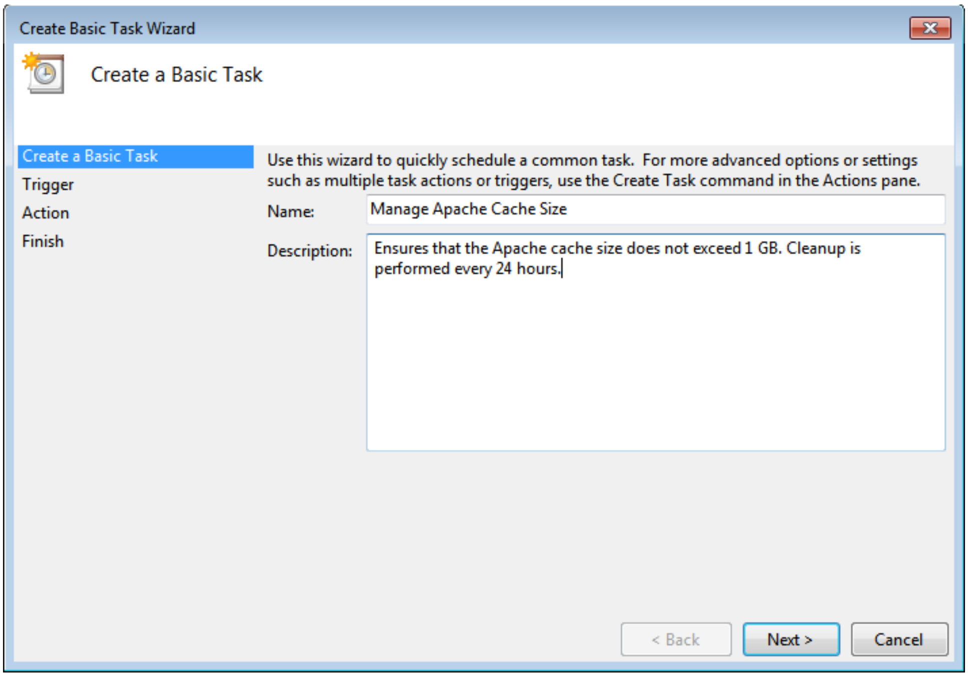
Status of tasks that have started in the following time period: Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

Task Name	Run Result	Run Start	Run End

Last refreshed at 5/6/2013 4:11:55 PM

3. Name the new task, give it a description such as "Manage Apache Cache Size," and click **Next>**:

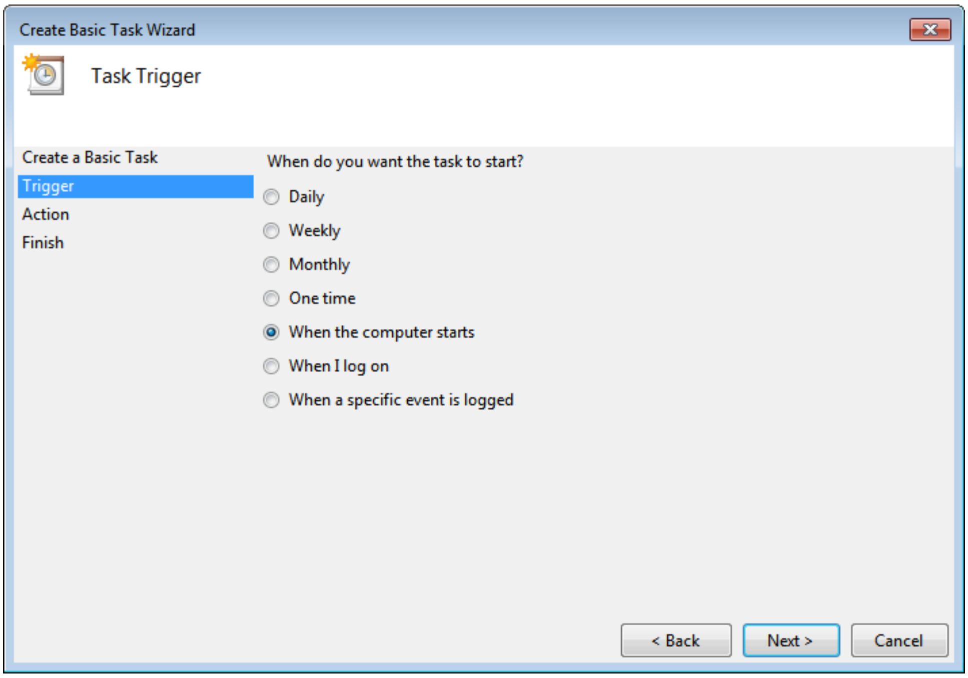


Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: Manage Apache Cache Size

Description: Ensures that the Apache cache size does not exceed 1 GB. Cleanup is performed every 24 hours.

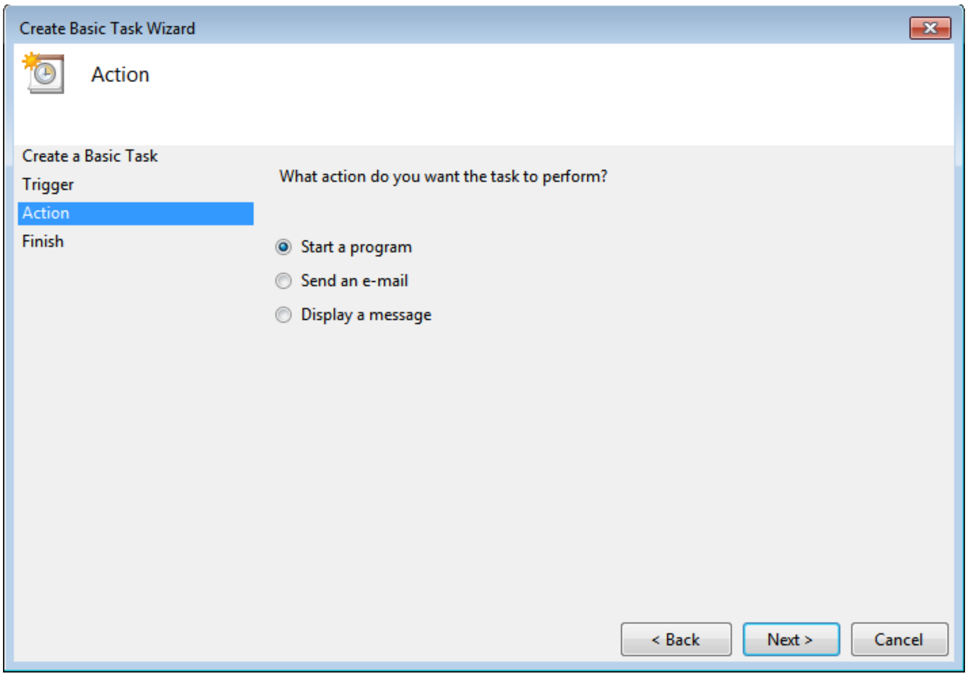
4. Set the trigger so that the task runs every time Windows starts. In the Task Trigger dialog box, click **When the computer starts**, and then click **Next>**:



When do you want the task to start?

○ Daily
○ Weekly
○ Monthly
○ One time
● When the computer starts
○ When I log on
○ When a specific event is logged

5. In the Action dialog box, click **Start a program**, and then click **Next>**:



Create Basic Task Wizard

Action

- Create a Basic Task
- Trigger
- Action
- Finish

What action do you want the task to perform?

● Start a program

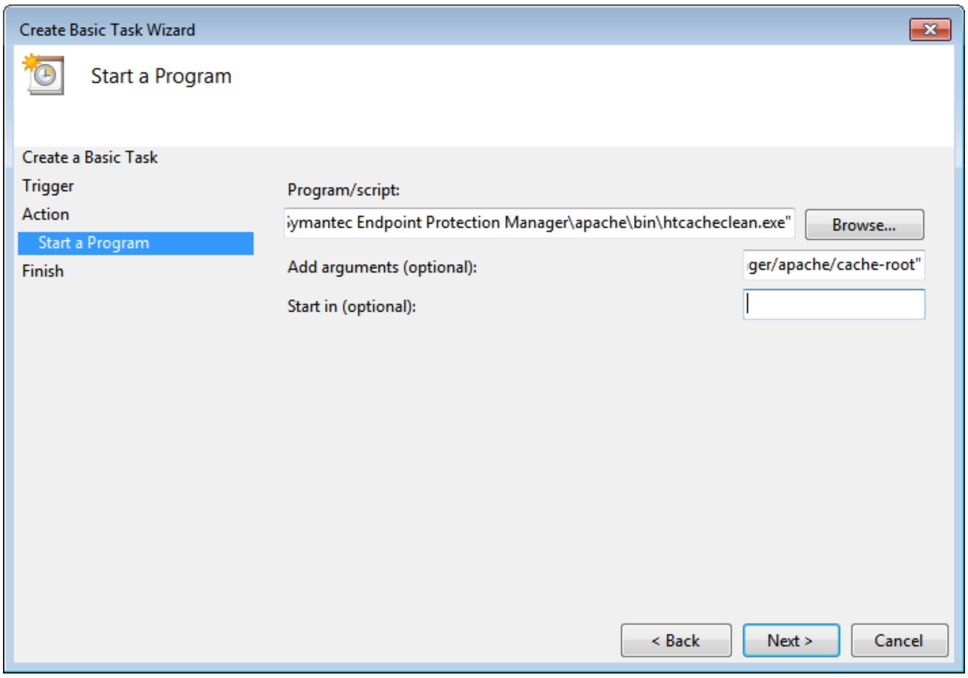
○ Send an e-mail

○ Display a message

6. Enter the full path to the `htcacheclean` utility as the Program/script name, with the optional arguments of

```
-n -t -d1440 -l1024M -p"C:/Program Files (x86)/Symantec/Symantec Endpoint Protection Manager/apache/cache-root"
```

and then click **Next>**.



Create Basic Task Wizard

Start a Program

- Create a Basic Task
- Trigger
- Action
- Start a Program
- Finish

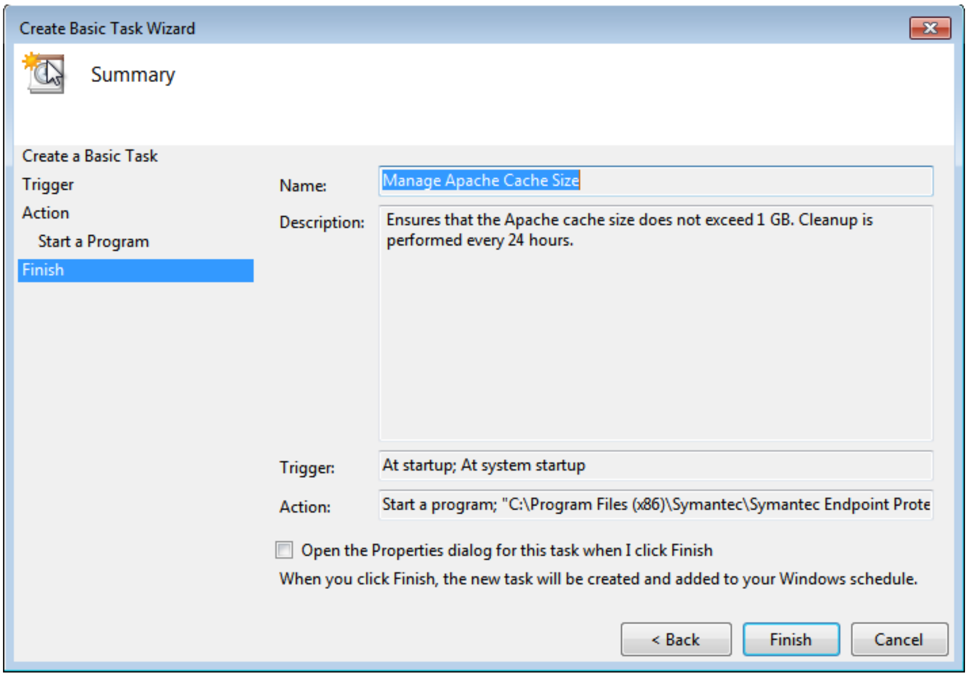
Program/script:

ymantec Endpoint Protection Manager\apache\bin\htcacheclean.exe"

Add arguments (optional): ger/apache/cache-root"

Start in (optional):

7. Click **Finish** to complete adding the scheduled task:



Name: Manage Apache Cache Size

Description: Ensures that the Apache cache size does not exceed 1 GB. Cleanup is performed every 24 hours.

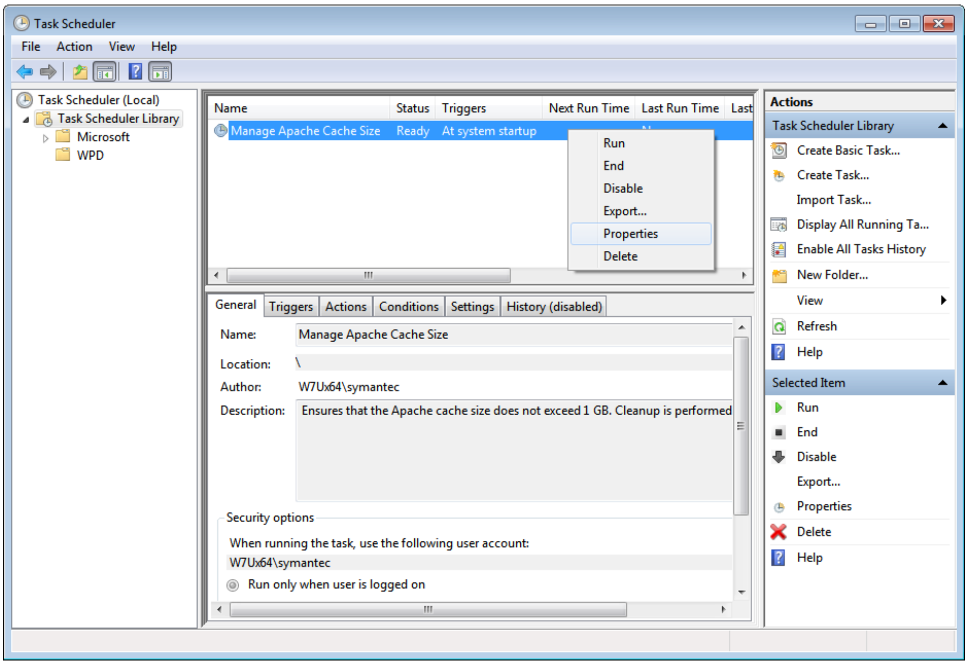
Trigger: At startup; At system startup

Action: Start a program; "C:\Program Files (x86)\Symantec\Symantec Endpoint Prote

□ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

8. The task should now appear in your Task Scheduler Library. Right-click on the task and then click **Properties**:



Manage Apache Cache Size Ready At system startup

Name: Manage Apache Cache Size

Location: \

Author: W7Ux64\symantec

Description: Ensures that the Apache cache size does not exceed 1 GB. Cleanup is performed

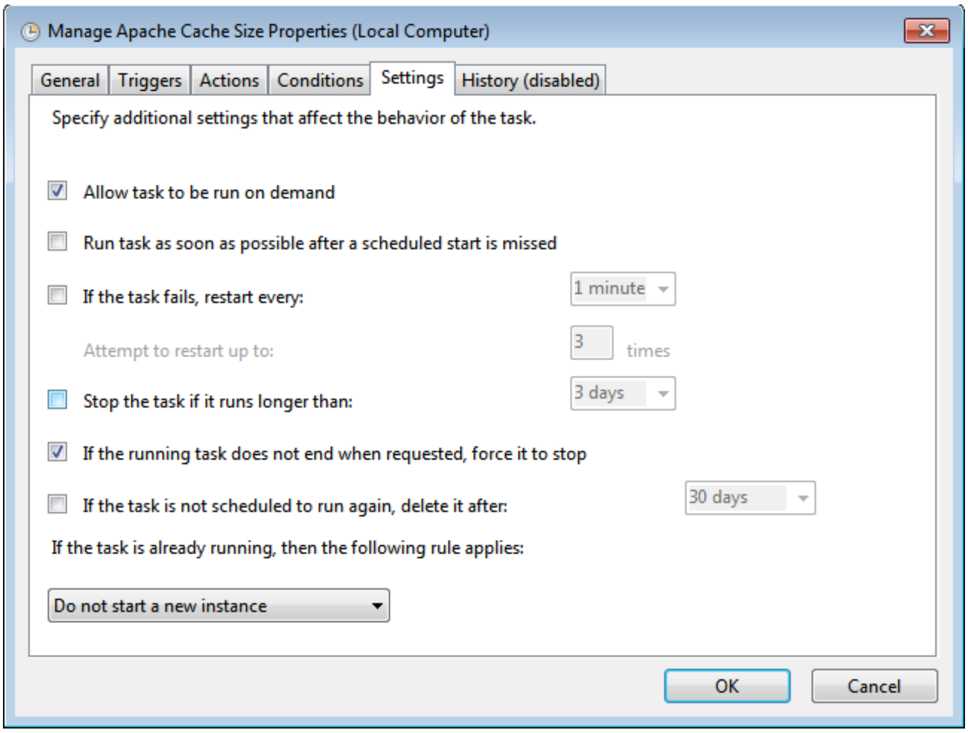
Security options

When running the task, use the following user account:

W7Ux64\symantec

○ Run only when user is logged on

9. Go to the Settings tab and click to clear **Stop the task if it runs longer than:**, and click **OK**:



Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

□ Stop the task if it runs longer than: 3 days

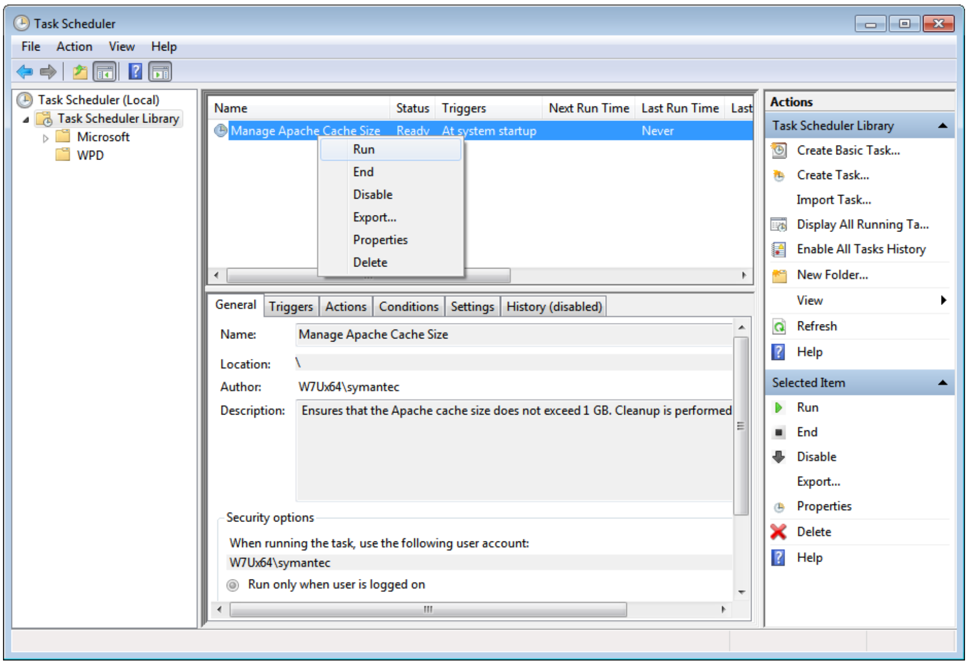
☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

10. Run the task now, because it will not run again until the system is restarted. In the Task Scheduler, right-click on the **"Manage Apache Cache Size"** task, and then click **Run**.



Name	Status	Triggers	Next Run Time	Last Run Time	Last
Manage Apache Cache Size	Ready	At system startup		Never	

Name: Manage Apache Cache Size

Location: \

Author: W7Ux64\symantec

Description: Ensures that the Apache cache size does not exceed 1 GB. Cleanup is performed

Security options

When running the task, use the following user account:

W7Ux64\symantec

○ Run only when user is logged on

Note: Ensure that the user account running the task has full control on this folder:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
Manager\apache\cache-root
```

Performance and scale: this is designed for small numbers of Mac clients

This setup should be used if there are only a few Mac clients and the network connecting clients and SEPM has a good bandwidth. Assuming that each client downloads roughly 500KB of LU content on daily basis, 2000 Mac clients will result in a download of approximately 1 GB of LU content daily from the Apache Web server. For configurations having large numbers of clients, alternatives like Symantec LiveUpdate Administrator should be considered.

Security and Compatibility

1. Symantec suggests use of only Symantec-signed binaries for Apache modules that are mentioned in this article. These signed binaries are available on the SEP DVD in the following locations, for versions of SEP 12.1 RU4 and later, enterprise version only.

   - Symantec Endpoint Protection (enterprise version): Disk 1, `\Resource\Apache-ReverseProxy`
   - Symantec Network Access Control: `\Resource\Apache-ReverseProxy`

     Note that the required binaries also get installed along with Symantec Endpoint Protection Manager for versions 12.1 RU4 and above.

2. The configuration described here is applicable for SEP 12.1 and later versions. If you are using the configuration for SEP 12.1 versions earlier than SEP 12.1 RU4, the binaries are not available on the DVD. In that case, please ensure that the version of Apache module binaries you use matches the version of the Apache Web server in your SEPM installation.

3. Because new vulnerabilities may be published after the publication of this article, please check the vulnerabilities published by the Apache project for the appropriate version of Apache web server: http://httpd.apache.org/security/

Related Articles

- TECH103198   Using the LiveUpdate Administrator 2.x to download updates for Symantec Endpoint Protection for Macintosh
- TECH211972   New fixes and features in Symantec Endpoint Protection 12.1.4
- TECH131735   Will a managed Symantec Endpoint Protection for Macintosh client update virus definitions automatically from a SEPM or GUP?

Article URL http://www.symantec.com/docs/HOWTO85034