Technical white paper

Antivirus Software Support

Windows-based HP thin clients

Table of contents

Overview

The purpose of this white paper is to list the configuration details and support for industry-standard antivirus software on Windows-based HP thin clients.

Thin clients are protected by a write filter that prevents from application-specific information writing to the flash. Therefore, antivirus software is not required on thin clients. If you are required to use antivirus software by your company, this paper provides setup instructions.

Symantec Endpoint Protection

Windows Embedded Standard 7 setup

Note
Symantec Endpoint Protection does not work properly with Enhanced Write Filter (EWF), because EWF does not use exclusions. HP recommends using File-Based Write Filter (FBWF) with the Registry Filter.

Preparation

1. Verify the system requirements specified by Symantec Corporation.
2. Download **Symantec Endpoint Protection** to a local computer.
3. Copy the program to a USB flash drive or any network location.
4. Select **Symantec_Endpoint_Protection_<version>.MP4.Full_Installation_EN.exe** to extract all files that are necessary for installation.

   Note
   A new folder is created under the name `Symantec_Endpoint_Protection_<version>.MP4.Full_Installation_EN` in the root directory of the USB flash drive.

5. Log on to the thin client as an administrator.
6. Disable the write filter. After the thin client restarts, log on as an administrator again.
7. Connect the USB flash drive to the thin client.

Deployment

1. In the `Symantec_Endpoint_Protection_<version>.MP4.Full_Installation_EN` folder, double-click **setup.exe**.
2. Select **Install Symantec Endpoint Protection**, and then select **Next**.
3. Accept the EULA, and then select **Next**.
4. Select **Next**, and then select **Install**.
5. If a warning appears, select **OK**.
6. The installation takes several minutes. Select **Next** to finish the installation.
7. In the configuration menu, select a configuration:

   If you are deploying the program to fewer than 100 clients, select **Default Configuration**, and then select **Next**.

   – or –

   If you are deploying the program to more than 100 clients, select **Custom Configuration**, and then click to open the submenu. The SQL Server client tools must be installed on the same server as Symantec Endpoint Protection Manager. Make sure that the tools are selected, and specify the folder where they are to be installed in the appropriate box. Then, select **Next**.
8. Select number of thin clients, and then select **Next**.
9. If you are a first-time user, select **Install my first site as target**, and then select **Next**.
10. Verify the configuration, and then select **Next**.
11. Select the database.

    For multiple sites or servers or for large numbers of thin clients, select **Microsoft SQL Server database**, and then select **Next**.

    – or –

    Select **Default embedded database**, and then select **Next**.

    – or –

    Select **Create a new database**, and then select **Next**.

Account creation

On this screen, create a system administrator account.

1. Enter any necessary information, including email and password, to enable Symantec Endpoint Protection, and then select **Next**.
2. Select **Send test email**, and verify that you received a Symantec Endpoint Protection Manager Test Message, which means the system is working correctly.
3. After this email is received, select **Next**.

LiveUpdate

1. Select whether to submit anonymous system and usage information to Symantec, and then select **Next**.
2. After LiveUpdate finishes, re-enable the write filter and restart the system to save your configuration.

Write filter exclusions

The installer automatically creates file and registry exclusions for FBWF.

1. Select **Exclusion List** to verify that all required parameters are present. See the following lists. You can add your own write filter exclusions, if necessary.

   Note
   Symantec Endpoint Protection automatically adds some items to the exclusion list. Some of the registry keys might not exist on the thin client's system.

   Windows Embedded Standard 7E 32-bit file exclusions

   - Program Data\Symantec
   - Users\All Users\Symantec
   - Program files\Symantec
   - Program files\common files\Symantec Shared

   Windows Embedded Standard 7P 64-bit file exclusions

   - Program Data\Symantec
   - Users\All Users\Symantec
   - Program files(x86)\Symantec
   - Program files(x86)\common files\Symantec
   - Program files\common files\Symantec Shared

   Registry key exclusions for FBWF

   - HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection
   - HKLM\SYSTEM\CurrentControlSet\Services\SepMasterService
   - HKLM\SYSTEM\CurrentControlSet\services\NAVENG
   - HKLM\SYSTEM\CurrentControlSet\services\NAVEX15
   - HKLM\SYSTEM\CurrentControlSet\services\SNAC
   - HKLM\SYSTEM\CurrentControlSet\services\SRTSP
   - HKLM\SYSTEM\CurrentControlSet\services\SRTSPX
   - HKLM\SYSTEM\CurrentControlSet\services\SYMNETS
   - HKLM\SYSTEM\CurrentControlSet\services\SYMTDI
   - HKLM\SYSTEM\CurrentControlSet\services\SYMTDIV
   - HKLM\SYSTEM\CurrentControlSet\services\SepMasterServiceMig
   - HKLM\SYSTEM\CurrentControlSet\services\SyDvCtrl
   - HKLM\SYSTEM\CurrentControlSet\services\SymEFASI
   - HKLM\SYSTEM\CurrentControlSet\services\SymELAM
   - HKLM\SYSTEM\CurrentControlSet\services\SymEPSecFlt
   - HKLM\SYSTEM\CurrentControlSet\services\SymEvent
   - HKLM\SYSTEM\CurrentControlSet\services\SymIRON
   - HKLM\SYSTEM\CurrentControlSet\services\SysPlant
   - HKLM\SYSTEM\CurrentControlSet\services\Teefer2

- HKLM\SYSTEM\CurrentControlSet\services\ccSettings_{GUID}

Windows Embedded Standard 7E 32-bit file exclusions

- HKLM\SOFTWARE\Symantec\SharedDefs
- HKLM\SOFTWARE\Symantec\Symantec AntiVirus
- HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection
- HKLM\SYSTEM\CurrentControlSet\services\BHDrvx86
- HKLM\SYSTEM\CurrentControlSet\services\IDSVia86
- HKLM\SYSTEM\CurrentControlSet\services\IDSxpa86

Windows Embedded Standard 7P 64-bit file exclusions

- HKLM\SOFTWARE\Wow6432Node\Symantec\SharedDefs
- HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec AntiVirus
- HKLM\SYSTEM\CurrentControlSet\services\BHDrvx64
- HKLM\SYSTEM\CurrentControlSet\services\IDSVia64
- HKLM\SYSTEM\CurrentControlSet\services\IDSxpa64
- HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection

2. Restart the thin client, and then re-enable the write filter.

Windows Defender

Note
Microsoft does not support Windows Defender on the Windows Embedded Standard 7E 32-bit operating system.

Windows Embedded Standard 7 setup

Windows Defender is included and enabled by default on all HP thin clients that are based on the Windows Embedded Standard 7P 64-bit operating system. For more information on how to defend your computer using Windows Defender, go to the following websites:

https://www.microsoft.com/security/portal/definitions/adl.aspx

https://support.microsoft.com/en-us/help/17464/windows-defender-help-protect-computer

Windows 10 IoT Enterprise setup

Windows Defender is included and enabled by default on HP thin clients that are based on the Windows 10 IoT Enterprise operating system. When you start the thin client for the first time, Windows Defender is on and actively scans your computer for any malicious software or viruses. For more information on how to defend your computer using Windows Defender, go to the following website:

https://support.microsoft.com/en-us/help/17464/windows-defender-help-protect-computer

For more information

For more information about Windows-based HP thin clients, go to the following resources:

- http://www.hp.com/go/bizsupport (Search for your thin client model. For documentation, select **Manuals**.)
- http://www.hp.com/go/thinclient

Sign up for updates
hp.com/go/getupdated

First Edition: October 2016

Document Part Number: 917704-001