Using Antivirus Software in an Interplay and MediaCentral Environment

Support for Symantec™ Endpoint v12.1.x

Overview

Avid Interplay Production v2.x and v3.x supports the following components of Symantec™ Endpoint v12.1.x:

- Antivirus
- Antispyware

The following features are not supported:

- Proactive Threat Protection
- Network Threat Protection

In addition, Interplay has not been qualified with the Firewall component of Symantec Endpoint.

You can install Symantec v12.1.x on Interplay clients and servers if you follow the installation procedure described in this document. Note that Avid ISIS also supports Symantec v12.1.x with the same installation restrictions.

MediaCentral Platform Services and AntiVirus Software

Antivirus is not required on the MediaCentral servers due to the nature of the Linux operating system and the data that is passed from the MediaCentral client to the MediaCentral server. Avid recommends that no other application be loaded on the MediaCentral server to ensure optimal performance.

Avid Interplay Engine and Antivirus Software

Antivirus software containing autoscanning (real-time scan) features can interfere with the operation of the Interplay Engine. For example, an antivirus program might lock the database files. You can install and configure antivirus software on the Interplay Engine, but you need to disable real-time scanning on the Interplay database folders. Any scheduled file scans also need to exclude these folders.

By default, all database folders are contained in D:\Workgroup_Databases, which is represented by the hidden administrative share \\<Servername>\WG_Database$.

Exclude the D:\Workgroup_Databases folders from any antivirus scanning.

File deletion protection utilities also consume system resources and could interfere with the proper operation of the Interplay Engine. These utilities automatically back up any files that are deleted, even temporary files created and deleted by the Interplay Engine. This consumes a large amount of disk space.

Installing Symantec v12.1.x on Interplay Servers and Clients

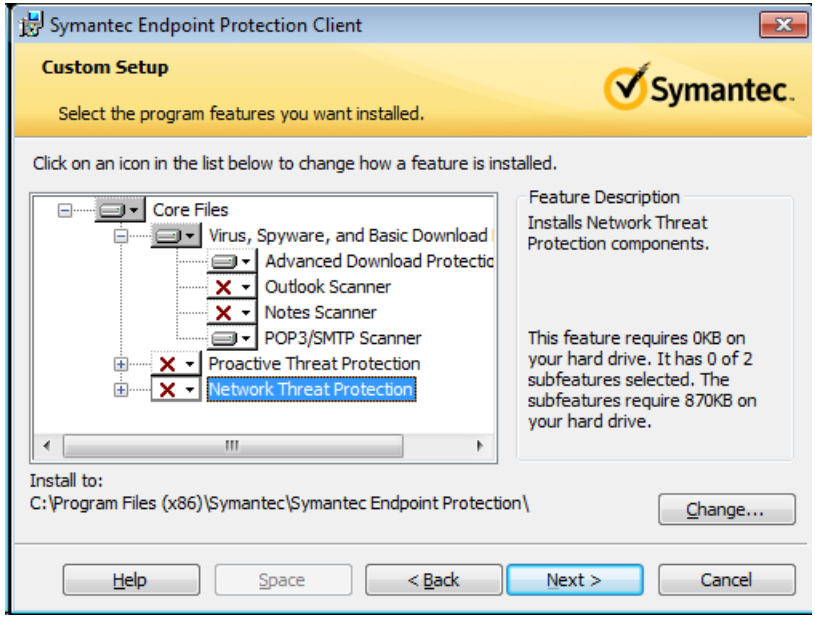
The following procedure identifies the Symantec options that you should disable during an installation.

To install Symantec v12.1.x:

1. If you are upgrading an existing Symantec installation, open the application and take note of the exclusion folders you are using. You will want to exclude the same folders for the v12.1.x installation.
2. If you are upgrading a Symantec11.x installation, use the Windows Add/Remove Programs feature to uninstall the 11.x version. See “Upgrading from Symantec 11.x” on page 5.
3. Open the Symantec v12.1.x installer and double-click the setup.exe file.
4. Click Next to move past the Welcome page.
5. On the License Agreement page, click the radio button “I accept the terms in the license agreement” and click Next.
6. In the Client Type window, select “unmanaged client” and click Next.
7. In the Setup Type window, select the radio button for “Custom” and click Next.
8. In the Custom Setup window, click on the Plus icon to expand the folder for “Virus, Spyware and Basic Download.”

9. Make sure that Outlook Scanner and Notes Scanner have an “X” indicating that they will not be installed.
10. Click once on the drive icon for “Proactive Threat Protection” and select the “X” which will indicate that “the entire feature will be unavailable.”
11. Click once on the drive icon for “Network Threat Protection” and select the “X” which will indicate that “the entire feature will be unavailable.”

    The following illustration shows the final selections for the Custom Setup window.



On a Vista system, see “Installing Symantec on ISIS Clients Running Windows Vista” on page 6.

12. Click Next.
13. In the Protections Options window, make sure that Enable Auto-Protect and Run LiveUpdate are checked.
14. Check “Disable Windows Defender”.

Note that the Disable Windows Defender option is not available on Windows 2008 Server R2.

The following illustration shows the final selections for the Protection Options window.

15. Click Next.
16. (Option) In the File Reputation Data Submission window, uncheck the option and click Next.
17. (Option) In the Ready to Install the Program window, uncheck the Data collection option.
18. Click on the Install button and follow the system prompts to complete the installation.

    After the installation is completed, the Symantec installer opens the Live Update Status window and attempts to download updates to the Symantec files. If you don't have an internet connection you can cancel this portion of the installation.

On an Interplay Engine system, open the Symantec application and exclude the D:\Workgroup_Databases folders from any antivirus scanning. You must do this BEFORE Symantec performs its first scan. If you fail to do so, users may be prevented from logging into Interplay after the first scan. See "On an Interplay Engine identify the Exclusion folders before the first scan" on page 6.

Installing on an Interplay Engine Cluster

You can install Symantec v12.1.x on a cluster. Make sure you exclude the following locations from the virus scanning:

- Q:\ (Quorum disk)
- C:\Windows\Cluster
- S:\Workgroup_Databases (database)
- R:\ (MSDTC disk)

Use the following guidelines for installing on a cluster:

- Perform the Symantec installation when the node is offline using the same procedure as described in "Installing Symantec v12.1.x on Interplay Servers and Clients" on page 2.
- Bring the node online to configure Symantec and identify the exclusion folders as listed above.

It is important to configure the exclusion folders on both nodes before Symantec runs the first scan.

Installing on a Stream Server

If you are installing Symantec on an Interplay Streaming Server v2.4 and higher, exclude the folder C:\Program Files (x86)\Avid\Avid Interplay Streaming Server from scanning by virus protection software. Scanning for virus protection could cause disruptions to the Interplay Streaming Server and could cause it to shut down. For additional information on the Streaming Server, see the Interplay Software Installation and Configuration Guide.

Limitations

The following limitations exist for installing Symantec v12.1.x in an Interplay environment.

Upgrading from Symantec 11.x

There is a known issue with upgrading from Symantec EndPoint v11.x to v12.1.x. After the upgrade, the "Disable Symantec Endpoint Protection" option is grayed out on the Symantec Endpoint Protection icon in the system tray. Refer to TECH169398 on Symantec's support web page for additional information.

To avoid this problem, uninstall Symantec v11.x before you install Symantec v12.1.x. Before you perform the uninstall, open the Symantec application and take note of the exclusion folders. You will need to set up these same exclusion folders after the installation.

On an Interplay Engine identify the Exclusion folders before the first scan

On Symantec v12.1.x, if you fail to exclude the Workgroup_Database folders before the first scan, the scan can create conflicts between Symantec and the Interplay database. The result is that you cannot log into Access or the Interplay Admin tool and the system displays an error message including the text “Class not registered”.

If this problem occurs you must reinstall the Interplay Engine software. You can reinstall the Interplay Engine software over the existing installation.