helpsystems

Getting the Most Out of Your Powertech Antivirus Trial

Congratulations on starting the journey toward a more secure business and IT infrastructure. This guide was designed to ensure you have the knowledge and support you need to make the most of your trial of the Powertech Antivirus solution. With this software in place over a 30-day period, you'll have access to all the latest virus definitions to help you complete native virus scanning on your server environment and ward off threats.

Getting Started

Installation and Licensing

If you haven't yet installed your trial of Powertech Antivirus, you can refer to this online manual, where you'll find the command you need to run depending on your environment. The manual also includes information about how to license the solution.

Two Types of Scans

On-Demand Scan

On-demand scans are scheduled or can be run ad-hoc from the command line. It can scan all files, or it can scan particular files and directories based on the paths and options provided with the command.

The time it takes for the first scan to complete will vary based on the components of your unique IT environment. This includes factors such as file sizes, the number of files, and more. Because the amount of time this first scan will take is unknown, we recommend running it during a planned maintenance window or low usage hours.

There are many tuning options available to adjust the scan to your unique environment. The scan will run as fast as possible unless the parameters are set to utilize a lower level of resources. Excluding certain directories also affects scanning time. For example, usually all database data files are excluded unless it is a maintenance window. It is recommended to perform your initial scan with archive files excluded (zip,jar,war,tar) to minimize the time spent on the initial scan operation.

You'll want to establish a baseline speed during this first scan. The scan defaults to running as quickly as possible, so if the baseline scan takes too many hours, reassess and prioritize what's being scanned. If timeliness isn't as large a concern, the permitted CPU usage should be lowered, enabling the scan to occur in the background while still leaving enough power for normal day to day tasks to be completed.

Once your baseline scan is complete, we recommend saving full system scans for planned maintenance windows or weekends, depending on your business and when your users are most active. If you have a 24/7 server environment, try planning your scans during ad-hoc maintenance windows or lower usage times.

On-Access Scan

When enabled, an on-access scan is designed to check for malware hidden in files when they are accessed by users or programmatic services while they are read or written to disk. A cache feature can improve performance and reduce system resources. Every time you read or write a file to disk, Powertech Antivirus scans that file. If the file was previously scanned clean and hasn't been modified since the last scan, the cache setting will reduce CPU impact by not scanning the file until it changes again.

Getting the Most out of Your Trial

Testing the Antivirus Solution

After initial configuration, you'll want to test the system to ensure that everything is working properly. The European Institute for Computer Antivirus Research (EICAR) has developed an anti-malware test file that contains a virus signature, but is not actually a harmful virus. It enables you to make sure that your scans are hitting the correct file systems, inclusions/exclusions are working, and that notifications are activated and going to the correct place.

Excluding Files or Folders

If you're scanning a database, you generally don't want to scan your live files since they are constantly changing. These can be handled with an on-demand scan during off hours.

Below are two other types of files that can be scanned intermittently:

- **Archive files** include file types such as zip, jar, and tar files which are very CPU intensive to scan due to their size or the number of files in question. You might even see a scan is still going 24 –

72 hours after it started, which is often how your windows PC performs antivirus scans in the background. Because of this, archive files are best handled during off hours. You can manage these situations by adjusting your settings specific to these file types so they are only scanned during specific time periods. You may also want to run multiple scheduled scans, one excluding archives and another scanning the archive file directories.

- **Database files** are constantly being used or changed. They are often skipped during scans because they will be locked down and unavailable to users during the evaluation. Adjust your settings to scan these high-use files during off hours when they're not needed.

Downloading Virus Definitions for Offline Machines

You may have machines not connected to the Internet that require scanning. However, you can still get regular updates for this equipment. One option is to designate another internet facing signature to access an external repository. From there, you can move the updates into the network from that system. Alternatively, you can provide the update to the antivirus systems from an internal web server, ftp server, or by indicating a directory path. The directory can be a local disk, or a network mounted filesystem.

You can learn more about Powertech Antivirus and other HelpSystems solutions in the Community Portal.