FORTRA

User Guide

Powertech Antivirus 6.4 (6.3.0 Endpoint)

Copyright Terms and Conditions

202505220734

Table of Contents

Welcome to Powertech Antivirus

Powertech Antivirus allows you to protect your AIX and Linux servers from the threats of viruses, worms, and malware using the industry-leading Trellix scanning engine. Powertech Antivirus can run continuously as a service that automatically scans files as they are opened or closed—a process called *On-Access Scanning*. For additional protection, scans can also be run explicitly for a file or directory when required using *On-Demand Scanning*.

The status of Endpoints on your network can be monitored and updated with the latest virus definitions directly from your browser using Powertech Antivirus Server running on Fortra Application Hub. The virus definitions from Trellix can be acquired directly by the Endpoints themselves or transferred through a local DAT file repository. Scan results and other Endpoint activity are reported in Powertech Antivirus Server and easily accessible with search, sorting, and filtering features. Scan results are also available in reports and activity can also be monitored using notifications.

Powertech Antivirus offers all the essential tools needed to ensure that your systems are protected from the latest threats.

Powered by Trellix

IMPORTANT: McAfee is now Trellix.

Trellix's preeminent staff backs each new update of the virus-scanning engine and release of virus definition .DAT files. Their worldwide virus research team develops daily updates for the virus definition .DAT files, leaving you confident that your server is well protected from attack. Powertech Antivirus incorporates the latest generation of Trellix's scanning engine, in turn making Powertech Antivirus a mature product backed by battle-tested technology, advanced heuristic analysis, and generic detection and cleaning.

- Scans a single file or directory
- Scans within compressed files
- Decompresses and scans files within containers such as ZIP, RAR, etc.
- Detects and cleans macro and script viruses
- Detects and cleans encrypted and polymorphic viruses
- Detects and cleans viruses in executable files, OLE compound documents, and PDFs
- Detects and removes "Trojan horses", worms, and many other types of malicious software (malware)
- Upgrades easily to new scanning technology
- Includes technology to combat the latest and future threats
- Support for many more Packed Executable formats in which known malware is often re-packaged for obfuscation purposes
- Specific detection and reporting of files compressed or packaged with known suspicious applications
- Enhancements to enable scanning of non-standard ZIP archives

Learning more about viruses

Viruses can corrupt or destroy data, they spread rapidly, and they can make your computers unusable. We strongly recommend that you do not experiment with real viruses.

Implementing Powertech Antivirus

The topics in this section describe how to begin using Powertech Antivirus.

By the end of this section, you will know how to:

- Update to the latest Virus Definitions from Trellix. See Updating Virus Definitions.
- Develop an approach to scanning your systems efficiently. See Preparing to Scan.
- Configure systems to be scanned when accessed (on-access scanning). See On-Access Scanning.
- Scan files and directories explicitly (on-demand scanning). See On-Demand Scanning.
- Schedule DAT file updates and virus scans. See Scheduling Updates and Scans.
- View and manage files that have been quarantined as a result of scanning actions. See Managing Quarantined Files.
- Configure notifications to be sent from Powertech Antivirus. See Notifications.
- Create custom reports that include consolidated on-access and on-demand scanning statistics. See Reporting.
- Use Powertech Antivirus's Interactive Fortra Application Hub features. See Powertech Antivirus and Fortra Application Hub.
- Use the functionality of the Powertech Antivirus application within Fortra Application Hub with IBM i Endpoints. See Registering IBM i Endpoints.

NOTE: See the Powertech Antivirus *Installation Guide* on the Fortra Support Portal for instructions on installing the Powertech Antivirus web server and Endpoints, and integrating Powertech Antivirus with Fortra Application Hub.

Updating Virus Definitions

Virus Definitions (DAT files) from Trellix can be downloaded onto a single local server (DAT file repository) and deployed automatically or manually via HTTPS (HTTP over TLS) or FTP to Endpoints on your network via Powertech Antivirus Server. Powertech Antivirus also allows you to schedule updates and monitor the status of connected Endpoints. Endpoints without a connection to Powertech Antivirus Server can also be configured to acquire DAT file updates from the local repository. Virus definitions can also be transferred to an air-gapped server using physical media.

The following instructions guide you through the process of configuring a local DAT file repository and keeping Endpoints updated with the latest virus definitions from Trellix.

> **NOTE:** Powertech Antivirus Server validates DAT updates before Endpoints are able to use them. For details, see 181

Updating virus definitions using a local DAT file repository

This method of updating virus definitions allows you to update the latest DAT files onto a local server, and then use Powertech Antivirus Server to distribute the DAT files to Endpoints on your network via HTTP or FTP. Only the single server running Powertech Antivirus Server needs access to Trellix for downloading DAT Files.

Install Powertech Antivirus on the server you would like to use as the DAT file repository, and connect the Endpoints you intend to scan. See the *Powertech Antivirus Installation Guide* for details on installing and connecting to Fortra Application Hub, and adding Endpoints.

Once configured, the status of Endpoints can be monitored using Powertech Antivirus within Fortra Application Hub's Home page.

The following instructions guide you through the process of:

- Configuring a local DAT file repository with automatic updates;
- Configuring a signed Certificate Authority (if required); and
- Updating DAT files on Endpoints manually using the Powertech Antivirus application in Fortra Application Hub.

To configure a local DAT file repository and schedule updates

1. Open Powertech Antivirus application in Fortra Application Hub.
2. In the Navigation Pane, choose **Settings > Repository** to open the Settings > Repository page.
3. Toggle Virus Definition (DAT) Repository Common Settings (top toggle) to **On**. Set the frequency of updates and whether to automatically update Endpoints.
4. Choose the type of file server:
   - If you intend to use an HTTPS file server, toggle Virus Definition (DAT) Repository Common Settings to **On**. Then, set the maximum number of Endpoints to be updated concurrently, and the port.

     IMPORTANT: All Endpoints must be able to access the port specified for the HTTPS service.

   - If you intend to use an FTP file server, toggle Virus Definition (DAT) Repository FTP Service Settings to **On**.

     See also: Settings > Repository.
5. Click **Save**.

While not required for normal operations, you can use --ftp, --wget, --curl, or --avget to connect to Powertech Antivirus Server's DAT repository service. For example, the following can be used to update DAT files using the Powertech Antivirus internal tool `avget` with self-signed certificates and the ptavrepo provided through the Powertech Antivirus application in Fortra Application Hub:

```
/opt/sgav/avupdate --ftp
ftp://yourusername:yourpassword@yoursite/downloads/av
/opt/sgav/avupdate --ftp --passive --ptavrepo
ftp://yourptavserverhost:21
/opt/sgav/avupdate --avget --ptavrepo
https://yourptavserverhost:8023
```

NOTE: Specifying `--ptavrepo` doesn't require the /current folder since the version will be read from the Powertech Antivirus DAT Repository service.

Configuring a signed certificate authority for DAT file updates

By default, the Powertech Antivirus Service uses a self-signed certificate to ensure secure TLS data transfer between the repository and Endpoints. Alternatively, you can use your own

trusted certificate issued by a third-party certificate authority (CA) to secure the DAT repository HTTPS file server.

If you do not have a signed certificate, the Powertech Antivirus service generates a self-signed certificate.

> NOTE: A certificate should only be provided if you are using your signed certificate authority. Do not provide a self-signed certificate.

1. Locate your certificate and key files on Powertech Antivirus Server.
2. If the certificate and key both have ".pem" file name suffixes, rename the certificate to "cert.pem" and the key to "key.pem". (If the certificate and key file name suffixes are ".crt" and ".key", no file renaming is required.)
3. Place the certificate and key files into following folder, replacing the existing files:
   Linux: /opt/ptavwebsvc/PTAVService/certs
4. Restart the Powertech Antivirus Service.
   Linux: "PTAVServer"

To update DAT files on Endpoints manually using Powertech Antivirus Server

If you set the Powertech Antivirus Settings to update Endpoints automatically when DAT files are available, connected Endpoints will be updated automatically based on your settings. You can also use the following method to update DAT files on Endpoints manually.

1. On the Powertech Antivirus navigation pane, click **Endpoints**.
2. Check the Endpoints you would like to update.
3. Click **Update DAT Files**.

Updating virus definitions from Linux Endpoints directly

If Endpoints on your network do not allow Powertech Antivirus Integration Service connections to the Powertech Antivirus service (for example, for unregistered and/or older/unsupported operating systems), you can still download the latest DAT updates from your local DAT file repository by specifying the "current" folder with the `avupdate` command.

To use this method, you must configure the HTTPS file server with a genuine certificate because the HTTPS download process (curl/wget) for legacy Endpoints does not allow self-signed certificates in `avupdate`. (See Configuring a signed certificate authority for DAT file .)

Trellix updates virus definitions every day and you should schedule the update process to run daily. To start the update, either change to the product directory or type the full path to the `avupdate` command, and specify the current folder:

EXAMPLE:

```
cd /opt/sgav
./avupdate --curl https://yourserver.yourco.com:8023/current
```

or

```
/opt/sgav/avupdate --curl
https://yourserver.yourco.com:8023/current
```

or

```
/opt/sgav/avupdate --avget https://myinsitehost:8023/current
```

The update process must be run by a root user. This is to prevent the product from accidentally (or maliciously) being disabled by deleting its files.

Updating virus definitions from IBM i Endpoints directly

Please see the section Integrating with Powertech Antivirus Server in the Powertech Antivirus for IBM i User Guide.

Updating virus definitions on air-gapped servers

If your Powertech Antivirus Server is not connected to the internet, you can load the latest virus definitions using physical media, such as a USB thumb drive. To do so:

1. Create a new folder called `datimport` in `/opt/ptavwebsvc/PTAVService` if it does not exist already. During the DAT update procedure, before referring to Trellix for DAT updates, Powertech Antivirus first checks for the presence of this folder.
2. On a system with Internet access, download the latest required virus definition (DAT) files from Trellix and save them to a tmp folder. These files are available at http://update.nai.com/products/commonupdater/.
   Files needed:
   - oem.ini
   - gdeltaavv.ini
   - avvdat.ini
   - *.zip file referenced in oem.ini
   - Incremental updates: All *.gem files. No need for these if running a standard full update (using Powertech Antivirus Server or avupdate --full). If the incremental update fails, a full update is performed using the .zip file.

3. Copy the DAT files from the tmp folder to transferable media, such as a thumb drive. Once copied, the DAT files can be deleted from the tmp folder.
4. Copy the DAT files to `/opt/ptavwebsvc/PTAVService/datimport` on the air-gapped server:

   > **NOTE:** If the Powertech Antivirus Service was allowed, it may have connected to Trellix and acquired the latest DAT files. If so, delete the contents of the datrepo folder and restart the Powertech Antivirus Service from the control panel. It is preferable to not allow the Powertech Antivirus Service before creating the datimport folder.

5. Open the Powertech Antivirus application in Fortra Application Hub, and in the Navigation pane, choose **Settings > Repository**.
6. Click **Save** to prompt the Powertech Antivirus Service to process the files.
7. Install Powertech Antivirus on the air-gapped server and register the Endpoint(s) in Fortra Application Hub. To use the Marketplace to install Powertech Antivirus on Endpoints, copy the Linux and AIX license files to the Fortra Application Hub server for the Endpoint deployment.
8. In Fortra Application Hub, open Powertech Antivirus and choose **Endpoints**.
9. Select the Endpoint and click **Update DAT Files**.

Notes

Trellix updates virus definitions every day and you should run avupdate every day.

- To schedule using cron, run command `crontab -e` to edit the crontab file using the vi editor. Position the cursor to the end and type i to insert a line.
  1. Type the following (on one line) to schedule the job to run every day at 6pm (18):

     ```
     0 18 * * * /opt/sgav/avupdate --curl
     https://yourserver.yourco.com:8023/current >
     /opt/sgav/log/avupdate.out
     ```

  2. On AIX, to see the cron log, run `tail /var/adm/cron/log`.
  3. On Linux, to see the cron log, run `tail /var/log/syslog`.

  For more information about scheduling using cron, run `man crontab`. See also Scheduling Updates and Scans.

- The exit status of the avupdate command can be used to check the result of the DAT update. Exit values are:

    - `0` Process completed successfully.
    - `1` An error occurred.
- The DAT decompression option (--decomp) can be used to ensure the virus definitions are saved in an optimal format for fast initialization. This has the most effect when a full update is requested, or when one occurs through an inability to patch incrementally.

Preparing to Scan

As is the case with many capable software products, Powertech Antivirus can occupy excessive system resources if care is not taken during deployment. In this section, you will learn the key concepts needed to plan the most appropriate scanning approach for your environment.

In this section you will learn:

- An overview of Powertech Antivirus' two scanning methods: On-Demand and On-Access.
- How to target potential threats
- Tuning parameters and configuration methods that can be used to limit resource consumption

On-Demand vs. On-Access scanning

Powertech Antivirus' two scanning methods can be used separately or in tandem to address all potential threats on your systems.

Using On-Demand Scanning

On-Demand scanning is run ‘on-demand’, that is, when started manually, or when scheduled.

This can be done in a few ways:

- Invoking the **avscan** command from the command line on the Unix Endpoint.
- Invoking the **avscan** command in a scheduler (such as cron) on the Unix Endpoint.
- Invoking the On-Demand Scan options using Powertech Antivirus Server web browser console.

To run an On-Demand scan from the command line or from a scheduler, you must pass the configuration for the scan using the parameters of the command. See avscan command.

To run an On-Demand scan from Powertech Antivirus Server, you must:

1. Open Fortra Application Hub, select Powertech Antivirus, and create an On-Demand Configuration.
2. On the Endpoints page, for an Endpoint, check the Endpoint and choose **Run Scan**.
3. In the Run Scan page, choose the Configuration and then **Save and Run** or **Run**.

Using On-Access Scanning

On-access scanning is ‘real-time’ scanning. Essentially, you set a configuration that includes several directories that you wish to continually scan. You can then decide whether to scan when a file is opened or when a file is opened and closed. This runs continually as a service.

When applications open files that require scanning, there is a delay while the system completes the scan. For most files, the scanning takes only a fraction of a second. However, large files, archive files, and compressed files can take several seconds or minutes. Once a file has been scanned by the on-access service, the scan result is stored in a cache for the file system if the file system cache has been enabled for the service. The cache is consulted the next time the file is accessed, and if it has not been modified, it will not require scanning again and access will be faster. The cache is cleared completely upon on-access service exit, update of virus definitions, or significant changes to service configuration. Individual items in the cache are also subject to size and time-to-live constraints and are configured in the service configuration. Archive scanning takes additional CPU resources and can be disabled. Many viruses come in the form of .zip archive files.

On-Access scanning can be configured locally or using Powertech Antivirus Server.

Local configuration

Set the [avsvc] stanza in the config.ini file located in /opt/sgav

[avsvc] is *only* for the on-access scan service. If you change the defaults in here, you must reload or restart the avsvc service depending on which default has been changed.

Powertech Antivirus Server configuration

You can create an on-access configuration within Powertech Antivirus Server and deploy it to the Unix Endpoint. When you change the configuration in Powertech Antivirus Server, the config.ini file is overwritten on the target Unix Endpoint and the service is reloaded. You can only have one on-access configuration running at any one time.

What should I scan?

Fortra can provide guidelines and technical details regarding the operation of Powertech Antivirus; however, every organization's networks are different, and security requirements vary across organizations. It is ultimately the responsibility of the system administrator and/or security officer to understand the details and purpose of the various filesystems to be scanned, and to decide how to employ Powertech Antivirus's capabilities to accommodate the security needs of the organization.

On-Access Scanning

On-Access Scanning refers to the process of scanning files as they are accessed by users of the system. Powertech Antivirus includes a service, avsvc, that allows you to do this.

On-Access Scanning can be started and stopped for Endpoints, both individually and in groups, using Powertech Antivirus Server. To manage On-Access Scanning from the command line, see the avsvcctl command.

WARNING: Prior to scanning, ensure you have acquired the latest virus definitions from Trellix (see Updating Virus Definitions). If you attempt to scan without updating to the latest virus definitions, Powertech Antivirus will perform the scan, but without the code required to identify the latest threats.

On-Access Scanning with Powertech Antivirus Server

To use Powertech Antivirus Server for On-Access Scanning, first install Powertech Antivirus Server, and connect the Endpoints you intend to scan. See the *Powertech Antivirus Installation Guide* for details on installing and connecting Powertech Antivirus Server and adding Endpoints.

To run On-Access scans using Powertech Antivirus Server

1. Open Fortra Application Hub and choose **Powertech Antivirus**. From the Navigation pane, choose **Configurations**. Review the On-Access Configurations to confirm one exists that you want to use for your scan. See Configurations page. To add a new On-Access Configuration, choose **Add > On-Access Configuration** and define one to meet your requirements. (See New On-Access Configuration pane).
2. On the Powertech Antivirus Navigation pane, choose **Endpoints**.
3. Ensure the virus definition DAT files are up-to-date on the Endpoints you want to scan. See Updating Virus Definitions.
4. Use the check box to the left of the Endpoint listing to specify the Endpoints you want to scan. Additional buttons appear on the top of the page with a yellow background.
5. Click **Start**. A message appears indicating On-Access scanning is starting.
6. Click **Activity Status** to open the Activity Status page, where you can monitor the status of submitted On-Access Scanning requests.
7. If the Start action failed on one or more Endpoints, you can rerun the request on failed Endpoints only by clicking ⋮ **(Show Actions) > Rerun On-Access Service Config on Failed Endpoints**.

On-Demand Scanning

On-demand scanning refers to the process of explicitly scanning a file or directory for viruses. An on-demand scan is typically initiated at a scheduled time. When an on-demand scan is initiated, Powertech Antivirus processes all of the files in the specified directories for viruses and provides a report of scanning activities.

On-access and on-demand scanning can be run simultaneously. Any user can use the avscan command, but you must have *RX authority to files in order to scan or otherwise see them. You can clean or quarantine files without *RWX authority, but will not be able to view the folder including the files. For this reason, it is recommended that full system scans be run by a root user.

To scan the file system for viruses and malicious code, you can use Powertech Antivirus Server or the `avscan` command. See avscan command for a the list of avscan options.

> WARNING: Prior to scanning, ensure you have acquired the latest virus definitions from Trellix (see Updating Virus Definitions). If you attempt to scan without updating to the latest virus definitions, Powertech Antivirus will perform the scan, but without the code required to identify the latest threats.

> **NOTE:** To use on-access scanning, see On-Access Scanning.

On-Demand Scanning with Powertech Antivirus Server

To use Powertech Antivirus Server for On-Demand Scanning, first install Powertech Antivirus Server, and connect the Endpoints you intend to scan. See the *Powertech Antivirus Installation Guide* for details on installing and connecting Powertech Antivirus Server and adding Endpoints.

To run On-Demand scans using Powertech Antivirus Server

1. Open Fortra Application Hub and choose **Powertech Antivirus**. From the Navigation pane, choose **Configurations**. Review the On-Demand Configurations to confirm one exists that you want to use for your scan. See Configurations page. To add a new On-Demand Configuration, choose **Add > On-Demand Configuration** and define one to meet your requirements. (See New/Edit/Duplicate On-Demand Configuration pane).
2. On the Powertech Antivirus Navigation pane, choose **Endpoints**.
3. Ensure the virus definition DAT files are up-to-date on the Endpoints you want to scan. See Updating Virus Definitions.

4. Use the check box to the left of the Endpoint listing to specify the Endpoints you want to scan. Additional buttons appear on the top of the page with a yellow background.
5. Click **Run Scan**. The Run Scan page appears.
6. For On-Demand Configuration, select the desired Configuration and choose **Run** to run the scan. If you would like to change the Configuration settings prior to running the scan:
    a. Make the desired Configuration changes.
    b. Click **Save and Run**. The Save Configuration page appears. The new settings will be saved as an additional Configuration, or will be overwritten.
    c. Change the name. If you do not change the name, you will be prompted to overwrite the chosen Configuration with your new settings.
    d. Click **Save and Continue** to save the new Configuration and run the scan.

Scheduling Updates and Scans

Fortra recommends updating the Powertech Antivirus DAT files daily to ensure the latest virus definitions are always being employed for On-Access scans. Updating daily also ensures all On-Demand scans are using the latest virus definitions. Fortra recommends weekly scans for systems that depend on On-Demand scanning. The following instructions describe how to schedule these events so they occur automatically.

> **NOTE:** You can use Powertech Antivirus Server to schedule virus definition updates on connected Endpoints. See Updating Virus Definitions.

Scheduling Scans with Powertech Antivirus Server

Powertech Antivirus makes it easy to schedule recurring On-Demand scans. To do so:

1. On the Powertech Antivirus Navigation Pane, choose **Scheduled Scans**.
2. Click **Add**. The New Scheduled Scan pane appears.
3. Where prompted, enter a name and description for the scheduled scan, and select the desired Configuration.
4. In the Endpoints section, enter the Endpoint aliases of the Endpoints you would like to include in the scheduled scan, separated by a semicolon.
5. Click the Scheduler toggle to display the schedule settings.
6. Select the desired day/time/month that the scan should occur. For example, to scan daily at noon, you would select the following:
7. Click **Save** to confirm your settings and enable the scheduled scan.

Scheduling Scans on the Endpoint

1. Make sure Powertech Antivirus for Linux is licensed and installed.
2. Run the command `crontab -e`
3. Cronjobs work as follows: *(minute) (hour) (day) (month) (day of the week) command to execute*.

   > **EXAMPLE:**
   > The following command will run every Saturday at 1 am.
   > `0 1 * * 6 /opt/sgav/avscan`

4. Write the cronjob that you would like followed by the command you would like to execute.
    - The command to update the DAT is **/opt/sgav/avupdate**
    - The command to run the scan is **/opt/sgav/avscan**

    > **NOTE:** You can add any of the parameters for avscan to the command. See avscan command for a the list of avscan options.

5. Save the file.
6. The cron log is located at:
    - Linux: **/var/log/syslog**
    - AIX: **/var/adm/cron/log**

    > **EXAMPLE:**
    > Cronjob for DAT file update at 7 pm everyday
    > `0 19 * * * /opt/sgav/avupdate`
    >
    > Cronjob for Avscan that runs on Sunday at 1 pm and Quarantines files in /opt/sgav/log/avscan.log
    > `0 13 * * 7 /opt/sgav/avscan --quar > /opt/sgav/log/avscan.out`

Managing Quarantined Files

Powertech Antivirus allows you to easily view and manage files that have been quarantined as a result of On-Demand Scanning or On-Access Scanning.

The option to quarantine files (set to 'off' by default) can be set in the Configuration used for the scan. See On-Access Configuration pane, On-Demand Configuration pane.

See also avsvc command, avscan command, and avconfig command.

To view, delete, or restore quarantined files

1. From the Navigation Pane, choose **Endpoints**. The Endpoints page appears. If a virus scan has resulted in quarantined files, "Quarantined: *Number of files*" appears in the Endpoint's row.
2. For an Endpoint with quarantined files, click ⋮ **> Manage Quarantine**. The Quarantined Files page appears. This page displays a list of all quarantined files along with the original file path (where the infected files were found).
3. Use the check boxes to the left of the virus paths to select the files you want to delete or restore. A yellow bar appears at the top of the page with additional options.
4. Choose **Delete** to remove the selected files, or **Restore** to replace them to their original location.

> **NOTE:** If you restore a file that has been detected by Powertech Antivirus without adjusting either the file or detection procedure (by, for example, cleaning the file or updating virus definitions), it will continue to be flagged and quarantined by Powertech Antivirus' scans.

Notifications

Notifications can be sent from several points in Powertech Antivirus, including on-demand scanning and on-access scanning. Scheduled emails can also be sent for status updates.

Notifications can also be set up using Configurations in Powertech Antivirus Server in the Fortra Application Hub web browser interface. See Configuration Properties pane.

Notification configuration

Three sections of Powertech Antivirus' config.ini are used for notification configuration: [avsvc], [avscan], and [notify].

```
[avsvc]
...
notify=mark,keith
...

[avscan]
notify=mark,sysadmin
[notify]
default.cmd=${PTAV_HOME}/notify-example.sh
default.options=none
mark.cmd=/bin/mail -s 'PTAV notification' mark.elf@northpole.com
mark.options=virus,quarantine
keith.cmd=/bin/mail -s 'PTAV notification'
kris.kringle@northpole.com
keith.options=all
sysadmin.cmd=/bin/mail -s 'PTAV notification' sysadmin@northpole.com
sysadmin.options=none
```

The [avscan] and [avsvc] sections have a `notify` parameter. Default is blank. The notify parameter can be a comma-separated list to indicate the notifiers from the [notify] section that are to be called.

For avsvc, the notify parameter specifies which notifiers will be called. For avscan, the notify parameter specifies the *default* notifiers that will be called, unless overridden on the command-line.

The [notify] section has a pair of *name*.cmd and *name*.options values. The *name* is the key used in the notify value in the upper sections.

The default for a non-configured *name.cmd* is nothing, the default for a non-configured *name.options* is none.

If a name cannot be resolved to command and options at run-time, that notifier is not run.

The cmd value is the name of a script to be called that receives notification information through environment variables and standard input.

The options value determines which events cause notifications to occur. This can be a comma-separated list from: *none, all, started, ended, error, timeout, virus, quarantine, delete, repair*. The values *none* and *all* trump all others, in that order. Empty options default to *none*, meaning the notifier will not run.

avconfig tool

There is a standalone tool for configuring all three sections:

```
Powertech Antivirus configuration tool v6.0.0-705.
(c) Copyright Fortra, 2021. All rights reserved. Licensed material,
property of Fortra.

Usage: ./avconfig [-d] [-h | -V | -C <params> | -U <params>]
-h        help
-d        debug
-V        validate config.ini
-C        create by overriding default settings
-U        create by overriding current settings
<params>  --<section> name=value ...
          e.g. --avsvc mime=yes programs=yes --avscan notify=default
```

The tool is for administrators and the -V, -C, and -U options require the user to be logged in as root.

For example, create a default configuration file:

```
avconfig -C
```

To override that default configuration:

```
avconfig -C --avscan notify=default --avsvc notify=default,other
mime=yes --notify hello.cmd=/usr/local/bin/hello.sh
hello.options=all
```

results in:

```
[avsvc]
access=open
```

```
include=/
exclude=/dev
threads=6
maxwait=300
delay=0
nice=0
clean=yes
cleanfail=quarantine
heuristic=yes
macro=yes
programs=no
archives=yes
files=dft
mime=yes
mount=
fsexcl=
notify=default,other
fscache=yes
fscacheage=0
fscacheidle=0
fscachesize=0

[avscan]
notify=default

[notify]
default.cmd=${PTAV_HOME}/notify-example.sh
default.options=none
hello.cmd=/usr/local/bin/hello.sh
hello.options=all
```

And to further override that configuration:

```
avconfig -U --avscan notify=hello --avsvc notify=default,hello
```

results in:

```
[avsvc]
access=open
include=/
exclude=/dev
threads=6
maxwait=300
delay=0
nice=0
clean=yes
cleanfail=quarantine
```

```
heuristic=yes
macro=yes
programs=no
archives=yes
files=dft
mime=yes
mount=
fsexcl=
notify=default,hello
fscache=yes
fscacheage=0
fscacheidle=0
fscachesize=0

[avscan]
notify=hello

[notify]
default.cmd=${PTAV_HOME}/notify-example.sh
default.options=none
hello.cmd=/usr/local/bin/hello.sh
hello.options=all
```

> **NOTE:** Use escape characters to prevent configuration text from being expanded by the shell prior to it being received by avconfig. So, to configure the default command:
> `avconfig -U --notify default.cmd=\${PTAV_HOME}/notify-example.sh default.options=none`

To upgrade a configuration file that does not have the new default notifier, use update with no parameters:

```
avconfig -U
```

Notification Messages

Messages mostly mirror the log messages that are related to file scanning:

- started
  - “avsvc running with pid *pid*”
    - Occurs after load of DATs, at the same time we tell the service controller we are “ready.”

- ended
  - “avsvc with pid *pid* stopped”
    - Also includes avsvcinfo output.
    - This is a 'best effort' message—Powertech Antivirus is in the process of shutting down at this point and discards any pending notifications not already in progress.
    - Powertech Antivirus attempts to wait for the notifier completion result, but a service controller or user could terminate before that happens.
- error
  - “quarantine of infected file failed for *file*"
  - “delete of infected file failed for *file*”
  - “File ‘*file*’ not scanned, code *code [reason]* ”
- timeout
  - “Timed out while scanning file '*file*’”
    - Based on the value "maxwait=<value>"
- virus
  - “VIRUS: '*file*’ is INFECTED with *virus*”
    - EICAR files will trigger this.
    - Note that Powertech Antivirus only sends this event when a virus is detected, and not when access is granted to it through a cached result (i.e. you will *not* see it for the log message “VIRUS granted access to infected file ‘/*file*’”).
- quarantine
  - “quarantined file *file*”
    - Based on the value "cleanfail=quarantine"
- delete
  - “file *file* deleted”
    - Based on the value "cleanfail=delete"
- repair
  - “Infected file ‘*file*’ *[action] (code [code])*”

Notification Action

When executed, the notification command will receive notification text on standard input. A sample notification script, notify-example.sh, is available in the installation directory.

The following environment variables will be available at runtime:

`PTAV_HOME`

The product installation directory.

`PTAV_VERSION`

The version of the antivirus software.

`PTAV_ENGINE`

The antivirus engine version and database level.

`PTAV_DAT_AGE`

The age, in days, of the antivirus database.

`PTAV_NOTIFICATION`

The notification event name (started, ended, error, timeout, virus, quarantine, deletion or repair).

`PTAV_HOSTNAME`

The hostname, as reported by uname.

Examples

To revert to product defaults:

```
avconfig -C
```

To create a configuration file based on product defaults and override the default avsvc settings for clean and macro options:

```
avconfig -C --avsvc clean=no macro=no
```

To extend that example to specify settings for notify for both avsvc and avscan, and include some notification configuration:

```
avconfig -C --avsvc clean=no macro=no notify=default --avscan
notify=default,mailme --notify mailme.cmd=\${PTAV_HOME}/notify-
example.sh mailme.options=started,ended
```

To change the current configuration to set the avsvc threads value:

```
avconfig -U --avsvc threads=8
```

Security

Administrative privileges are required to change the configuration file. At runtime, it must be owned by root and not writable by group or other.

The notification command runs as root. A process executes the command without any further checks. The directory is changed to “/” prior to running the command.

The on-access portion of the server identifies any viruses executed by the notification script. Note that this is not possible during service exit (the “ended” notification).

See Also

avconfig command

Reporting

Powertech Antivirus allows you to create reports that include consolidated on-access and on-demand scanning statistics. Reports can be customized to include a specific time range, filtered to include specific data, and sorted in the desired order. Reports can also be scheduled to run automatically at predetermined times, and the generated PDF can be automatically distributed to a list of recipients over email.

Creating reports

1. On the Powertech Antivirus Navigation Pane, click **Reports**. The Reports page appears.
2. To create an On-Access report, choose **Add > On-Access Report**. To create an On-Demand report, choose **Add > On-Demand Report**. To create an Endpoint Status report, choose **Add > Endpoint Status Report**. To create a Threat report, choose **Add > Threat Report**. Use the available options to define the contents, recipients, and scheduling of the report. The options available for On-Access Reports and On-Demand Reports are similar. See New/Edit On-Access Report pane, New/Edit On-Demand Report pane , New/Edit Endpoint Status Report pane or New/Edit Threat Report pane (depending on your selection) for details.

   > **NOTE:** To deliver reports to the email addresses specified in the recipients list, an email server must be configured on the Email Settings page.

3. Click **Save**. The Reports page appears, which displays the newly created report, as well as any existing reports.
   - You can track report generation using the Activity Status page.
   - To view the report output in Powertech Antivirus Server, on the Reports page, click **(Show Actions) > View** for a report. You can use the arrows at the top of each column to change the sort order.
   - Reports are delivered to the specified recipients over email as PDF attachments.

Powertech Antivirus Server and Fortra Application Hub

Powertech Antivirus Server offers a browser-based user interface that allows you to efficiently monitor and manage Powertech Antivirus on endpoints accross your network, and to provision DAT updates to those endpoints. Powertech Antivirus Server leverages Fortra Application Hub, Fortra's cross-product user interface and deployment platform.

> **NOTE:** To begin using Fortra Application Hub with Powertech Antivirus, see the *Fortra Application Hub Installation Guide* and the Powertech Antivirus Installation Guide.

The following provides an overview for how to manage Powertech Antivirus endpoints using Powertech Antivirus Server. See also the Fortra Application Hub User Guide, for general information about using Fortra Application Hub.

Sort, Search, and Filter settings

The Endpoints page, Connection Settings page, Activity Status page, and Activity Details page include settings that allow you to choose how to sort the existing list items, what type of data will be searched when you do a search, and how to filter the list.

> **NOTE:** All search results are accompanied by a unique URL. To save search results, simply bookmark or otherwise record the URL located in your browser's address bar. This URL can then be used to reference the results later. The results will appear in the same sort order.

Search Filter Categories

These settings allow you to define the categories you would like to search by, and submit the text search query.

- Click  to display the filter categories (specific to the page being viewed), then check the categories that should be included in search results. A full search is used if no category is checked.
- Begin typing into the Search field to find all list items from the selected categories that include the specified text. A text search queries all items in the category selected for all servers shown.

Show in List

These settings allow you to specify the list items you would like to show.

- Click **Show in List** to display a list of possible statuses (for example, the Endpoint status or connection status).
- Check the statuses you would like to display in the list.

The status categories selected are shown as follows:

- Click  to remove the category from the list.
- Click **Clear All** to remove all status categories.

> **NOTE:** See Tags in the Endpoints page topic for information on the Tags drop-down menu.

Sort By

These settings allow you to identify the category of list items you would like to sort, and change the sort order.

- Click next to **Sort By: *[category]*** to sort the list by the chosen category.
- Click  or  to invert the sort order (from high-to-low or from low-to-high, respectively).

> **NOTE:** Sorting information, including the column the list is currently sorted by and the sorting direction, is available in your browser's address bar. For example, a URL that includes "sort/**alias**/dir/**1**" indicates the list is sorted by *alias*, *low to high*. A URL that includes "sort/**alias**/dir/**0**" indicates the list is sorted by *alias*, *high to low*.

Fields

These settings allow you to specify the attributes of the row items you would like to show.

- Click **Fields** to display the field data categories that represent the various attributes of each row item. Each option represents a column in the list.
- Check the fields you would like to display in the list.

Save Filter

These settings allow you to save a custom filter configuration for use later, and specify the default filter configuration.

- Click **Save Filter** to activate a text field, which allows you to name the current filter configuration for use later.
- Check **Default**, if you want to set this filter configuration to the default one.
- Click **Save** to save the filter configuration for use later. The next time you click this button, the custom filter appears in the list.

Selecting Connections or Configurations

The Connection Settings page and Configuration page allow you to apply actions to multiple Connections/Configurations at once. To do so, select the check boxes to the left of the aliases. Additional buttons appear at the top of the page.

Connection Options

- **Remove Connections.** Choose this option to remove the selected connections from Powertech Antivirus Server.
- **Allow.** Choose this option to allow the selected connections to indicate the selected Endpoints should be allowed to communicate with Powertech Antivirus Server.
- **Block.** Choose this option to block the selected connections to indicate the selected Endpoints should not be allowed to communicate with Powertech Antivirus Server.
- **Cancel.** Choose this option to remove selection and dismiss the multi-select buttons.

See also Connection Settings page.

Configuration Options

- **Cancel.** Choose **Cancel** to de-select the selected Configurations.
- **Delete.** Choose **Delete** to remove the selected Configurations.
- **Update Endpoints (On-Access only).** Choose **Update Endpoints** to restore the assigned Configuration settings. This could be used, for example, if settings have been changed directly on the Endpoint itself that should be restored to match the Configuration settings assigned to the Endpoint in Powertech Antivirus.

See Configurations page and Endpoints page.

Anti-Ransomware

Ransomware is malicious software (malware) that employs encryption to hold a victim's information at ransom. In a ransomware attack, data is encrypted, which prevents access to it, and the attacker demands a ransom payment in return for decrypting the files.

How Powertech Antivirus Prevents Ransomware Attacks

Powertech Antivirus prevents ransomware attacks by detecting and alerting for potential ransomware attacks, and can also be configured to automatically take action when an attack is detected.

Powertech Antivirus helps protect against ransomware attacks in two ways:

1. The APEX (Access Pattern and Encryption Activity eXtended) detection method evaluates patterns in NetServer access to the Integrated File System (IFS). When APEX detects suspicious encryption activity, this suspicion level is compared to two thresholds:
    - a Message Threshold, which defines when a warning message is sent to the Powertech Antivirus message queue; and
    - a Block Threshold, which defines when the accessing user is blocked.
2. Canary files can be defined. A canary file is a decoy file placed within the IFS by the system administrator. If a user attempts to modify, rename or delete a canary file, the user will be blocked immediately.

IMPORTANT: Anti-ransomware functionality is only available on IBM i Endpoints.

Registering IBM i Endpoints

You can use the functionality of Powertech Antivirus Server for IBM i Endpoints.

During registration, Powertech Antivirus Server's address must be specified. It is recommended that user specify it as a full qualified domain name.

To register your Powertech Antivirus for IBM i 8.07 (and above) client with Powertech Antivirus Server, complete the steps in all sections below, in order:

On the IBM i

1. Sign on to the IBM i with a user profile that has *IOSYSCFG special authority.
2. Ensure the name used for Powertech Antivirus Server can be resolved to an IP address. Resolution can be achieved with DNS or a combination of a TCP host table entry and an entry in the /etc/hosts file.

   IMPORTANT: It is recommended that Powertech Antivirus Server parameter is specified as a fully qualified domain name rather than as a numerical IP address. If no DNS entry exists for Powertech Antivirus Server system, or if DNS is not configured on the IBM i endpoint, use these instructions: Setting-up Non-DNS name resolution on IBM i Endpoints before continuing.

3. Run **call qp2term**.
4. From the qp2term command line, run **cd /standguard/webclient/integration**.
5. Run **./register.sh -k *<API key copied from Powertech Antivirus Server - Settings > Endpoint Registration user interface>* -s *<Powertech Antivirus Server fully qualified host name>* -c *<your IBM i system name>***.

   EXAMPLE: ./register.sh -k fb0229ee-1518-4bfa-8ff2-ec733a803c98 -s MY_PTAV_SERVER.ACME.COM -c MyIBMi
   Where:
   - API key from Powertech Antivirus Server is fb0229ee-1518-4bfa-8ff2-ec733a803c98
   - the fully qualified domain name of Powertech Antivirus Server system is "MY_PTAV_SERVER.ACME.COM"
   - IBM i Endpoint name is MyIBMi

> **NOTE:** You can find the API key on the Endpoint Registration page of the Powertech Antivirus application in Fortra Application Hub.

6. Press **F3** to exit the qp2term environment.

In Powertech Antivirus Server

Your IBM i Endpoint should now appear within Powertech Antivirus Server. To allow the connection to be made from the Endpoint, complete the following steps in the Powertech Antivirus application.

1. Navigate to the Connection Settings page.
2. If the IBM i system is not displayed, clear all filters.
3. Click ⋮ **(Show Actions)** next to the IBM i Endpoint.
4. Select **Allow**.

After Registering

Start the job that connects the IBM i Endpoint to Powertech Antivirus Server by completing the following steps on the IBM i:

1. Run **ADDLIBLE STANDGUARD**.
2. Run **AVINSITE *RESTART**. The user profile running this command needs *USE authority to user profile STANDGUARD.
3. Only for systems where Powertech Antivirus for IBM i has been updated from R08M06 to R08M07, do the following steps:
   a. Sign on to an interactive session on the IBM i.
   b. Run the command:
   edtf '/standguard/webclient/integration/config/server.toml'
   c. Insert the following lines at the end of the file:
   [ibmistatuscheck]
   interval = 5
   d. Press F3 twice.
   e. You can now start the AVINSITE job.

Managing the AVINSITE Job

If needed, you can manage the connection between the Endpoint and Powertech Antivirus Server by using the AVINSITE job that runs in subsystem QSYSWRK. The user profile

running the AVINSITE command needs *USE authority to user profile STANDGUARD. Use **STANDGUARD/AVINSITE** on the IBM i with one of the following options:

***START** Starts the job that connects to Powertech AntivirusServer.

***STOP** Ends the job that connects to Powertech Antivirus Server.

***STATUS** Displays the status of the connection to Powertech Antivirus Server.

***RESTART** Restarts the connection to Powertech Antivirus Server.

***AUTOSTART** Adds an autostart job entry to the QSYSWRK subsystem so AVINSITE starts automatically when the system IPLs. This option can also be used to remove the autostart entry. In the following example, the autostart entry is added: **AVINSITE OPTION(*AUTOSTART) VALUE(*YES)**

To view the local Powertech Antivirus Server/IBM i Endpoint log, run the command:

dspf '/standguard/webclient/integration/log/avinsite.log'

Reference

The topics in this section provide detailed information regarding:

- The available Commands within the Powertech Antivirus product.
- The use of Powertech Antivirus within Powertech Antivirus Server User Interface.
- Additional configuration and validation procedures that are listed in the Appendix.

Powertech Antivirus Commands

This section describes the availability and use of the following Powertech Antivirus commands.

- avconfig - Antivirus service configuration helper
- avinsitectl - Antivirus integration service helper
- avsvc - Server to monitor file systems for viruses and malicious code
- avsvcctl - Powertech Antivirus service helper
- avsvcinfo - Queries the anti-virus service
- avscan - Scans the specified file or directory for viruses and malicious code
- avsysinfo - Provision of system and environment information
- avupdate - Updates virus definitions

avconfig command

Name

avconfig - Antivirus service configuration helper.

Synopsis

avconfig [-d] [-q] [-h | -V | -C <*parameter list*> | -U <*parameter list*>]

<parameter_list>:= <*parameter* 1> [<*parameter* 2> <*parameter* 3> ...]

<parameter>:= --section_name parameter_name=parameter_value

Description

The avconfig command can be used to validate and modify the configuration file, config.ini, for the antivirus tools.

The configuration file consists of three sections:

- [avsvc] for the antivirus service
- [avscan] for the on-demand scanner
- [notify] section which describes notification methods that can be used by either tool.

Configuration options for avsvc are described in the avsvc manual page.

Configuration options for avscan are described in the avscan manual page.

The <params> argument is a space-separated list of section names and option settings. Section names must be preceded by two hyphens. They must precede the setting names. Setting name and setting value must be separated by an equals sign, with the setting name being specified first. Examples are given below.

Root privilege is required to perform operations on the configuration file.

Options

`-d`Include debug output. This must be the first parameter.

`-q` Suppress output of product banner

`-h`Show this man page.

`-V`Produce a validation report for the current config.ini file.

`-C` <params>

Create a new configuration file by overriding the product defaults.

`-U` <params>

Create a new configuration file by overriding the current settings in config.ini.

Notification Support

The [notify] section of the configuration file defines commands and options for the notifiers requested in the [avscan] and [avsvc] section. Note that notify names should be in lowercase.

A notifier **name** is configured through **name.cmd** and **name.options** lines in the [notify] section of the configuration file.

The **name.cmd** parameter is used to specify the name of an executable file that is to perform the notification. The **name.options** parameter is used to specify the notification events that are to be sent. This is a comma-separated list containing one or more of:

`none`

Notifications disabled.

`all`

All notification events will occur.

`started`

Service or program start.

`ended`

Service or program end.

`error`

Errors reported during scanning.

`timeout`

Timeouts that occur during scanning.

`virus`

Virus detected.

`quarantine`

File has been quarantined.

`delete`

File has been deleted.

`repair`

File has been repaired.

Notification Action

When executed, the notification command will receive notification text on standard input. A sample notification script, **notify-example.sh**, is available in the installation directory.

The following environment variables will be available at runtime:

`PTAV_HOME`

The product installation directory.

`PTAV_VERSION`

The version of the antivirus software.

`PTAV_ENGINE`

The antivirus engine version and database level.

`PTAV_DAT_AGE`

The age, in days, of the antivirus database.

`PTAV_NOTIFICATION`

The notification event name (started, ended, error, timeout, virus, quarantine, deletion or repair).

`PTAV_HOSTNAME`

The hostname, as reported by uname.

Examples

EXAMPLE: To revert to product defaults:

```
avconfig -C
```

EXAMPLE: To create a configuration file based on product details and override the default avsvc settings for clean and macro options:

```
avconfig -C --avsvc clean=no macro=no
```

EXAMPLE: To extend that example to specify settings for notify for both avsvc and avscan, and include some notification configuration:

```
avconfig -C --avsvc clean=no macro=no notify=default --avscan
notify=default,mailme --notify mailme.cmd=\${PTAV_HOME}/notify-
example.sh mailme.options=started,ended
```

EXAMPLE: To change the current configuration to set the avsvc threads value:

```
avconfig -U --avsvc threads=8
```

See also: avsvc and avscan.

Changes to On-Access Scanning

In order for changes to on-access scanning to take effect, the on-scan service must be restarted in order to reload the settings.

To change the on-access scan settings to exlude directory /db2 and its subdirecctories from scanning and immediately effect the change, run the following commands:

```
avconfig -U --avsvc exclude=/db2

avsvcctl reload
```

Exit Status

On success, 0 is returned, a non-zero failure code otherwise.

avinsitectl command

Name

avinsitectl - Antivirus integration service helper.

Synopsis

avinsitectl [status | log | install | uninstall | enable | disable | start | stop | restart | reload | help]

Description

The avinsitectl command can be used to control and monitor the antivirus integration service.

Options

`status`

Shows the running status of the antivirus integration service.

`log`

Display the latest entries in the avinsite.log file.

`install`

Register the antivirus integration service with the operating system. Note that this will overwrite any system configuration already in place. This option can only be run by the root user.

`uninstall`

Deregister the antivirus integration service in the operating system. Note that this will also stop the service and disable it from starting at boot. This option can only be run by the root user.

`enable`

Set the antivirus integration service to start during system boot. Note that this will register the service with the operating system, if necessary. This option can only be run by the root user.

`disable`

Prevent the antivirus integration service from starting during system boot. This option can only be run by the root user.

`start`

Start the antivirus integration service. Note that this will register the service with the operating system, if necessary. This option can only be run by the root user.

`stop`

Stop the antivirus integration service. This option can only be run by the root user.

`restart`

Restart the antivirus integration service. Note that this will register the service with the operating system, if necessary. This option can only be run by the root user.

`reload`

Reload (reconfigure) a running instance of the antivirus integration service. This option can only be run by the root user.

`help`

Show the manual page.

Exit Status

On success, 0 is returned, a non-zero failure code otherwise.

avsvc command

Name

avsvc - Server to monitor file systems for viruses and malicious code.

Synopsys

```
avsvc [-h] [-V] [-D] [-d] [-c command]
```

Description

The avsvc server provides on-access scanning for viruses and malicious code.

The server should not be started directly, use the avsvcctl command to control the service.

Options

`-h`Show this manual page.

`-V`Parse configuration files to produce a validation report. The program will subsequently exit.

`-D`Do not daemonize the server. The default is to daemonize.

`-d`Run in foreground debug mode. Log messages at INFO level and higher are shown in the terminal screen. DEBUG level is enabled, and all log messages are sent to the log file: log/avsvc.log. This option should only be used if directed by a support representative.

`-c` command

Ask that a running server perform an operation.

Server Configuration

The server takes configuration from the file config.ini which can be found in the product install directory. The configuration options are contained in the [avsvc] group.

Configuration will be re-read if the service is sent a SIGHUP signal.

Service Settings

These settings are in the [avsvc] group. The avconfig command can be used to manipulate this file.

`access`

On-access scanning type. Valid values are `open`, which will result in files being scanned when users attempt to open the file, `opnclo`, which will result in files being scanned when users attempt to open or close the file, or `none`, which will disable on-access scanning. The default is `open`.

`include`

A colon-delimited list of path names to be included for on-access scanning. A file that exists below any of those path names will be subject to scanning unless the file path name is covered by an exclude path.

`exclude`

A colon-delimited list of path names to be excluded from on-access scanning. The exclude paths take precedence over include paths. A file that exists below any of those path names will not be subject to scanning.

> **NOTE:** `Exclude` does not support wildcard characters.

`threads`

The number of threads to be allocated for use by the on-access scanner. This can be an integer value between 2 and 32. The default is 6. The service must be restarted to change this value.

`maxwait`

The maximum amount of time in seconds the scanner should spend scanning a single file or archive before timing out. After the specified number of seconds, the file is allowed to be opened and the file's scan status remains unchanged. This can be an integer value between 0 and 3600. A value of `0` disables the timeout. The default is 300 seconds.

`delay`

The amount of time in microseconds the scanner should pause with each progress beat from a scanning operation. This can be used as a simple CPU limiting technique for certain use cases. It should not be enabled when operating system files are included in the monitoring paths. This can be an integer value between 0 and 999999. The default value of `0` disables the feature.

`nice`

Sets the runtime scheduling priority of the service. This can be a value between -20 (highest priority) and 19 (lowest priority). The default is 0 (no change in priority). The service must be restarted to change this value.

`clean`

Specifies if the engine should attempt to remove the virus from the file. If the file cannot be cleaned, the cleanfail option provides a secondary choice. Set to `yes` to enable, or `no` to disable. The default is `yes`.

`cleanfail`

Action if not cleaned. Valid values are `quarantine`, `delete`, `none`. The default is `quarantine`. Quarantined files are stored under /Quarantined.

`heuristic`

Include heuristic analysis to find new viruses. When you use heuristic analysis the scanning engine employs heuristic technology to detect potentially unknown viruses in executable files (programs). Without this option, the engine can only find viruses that are already known and identified in the current virus definition files. Valid values are `yes`, `no`. The default is `yes`.

`macro`

Specifies if you want to treat embedded macros that have code resembling a virus as if they were viruses. This parameter is similar to Heuristic analysis but scans for new viruses in compound document formats; for example, Microsoft OLE formats such as Word documents. Valid values are `yes`, `no`. The default is `yes`.

`programs`

Specifies if you want scanning activities to include detection of some widely available applications, such as password crackers or remote access utilities that can be used maliciously or pose a security threat. Valid values are `yes`, `no`. The default is `no`.

`archives`

Specifies if you want scanning activities to include archive files. Archive files contain embedded files and usually end with one of the following extensions: .ZIP, .TAR, .CAB, .LZH, .JAR and .UUE. This option will also permit scanning of MSCompress files. Valid values are `yes`, no. The default is `yes`.

`files`

Specifies the type of files to include in scanning activities. Valid values are `dft`, `all`, `allmacro`. The default is `dft` which means to scan only the file types that are most susceptible to virus infection. The value `all` will scan all files, the slowest option but which provides the best protection, and `allmacro` which will expand scanning activities to include an examination of files to determine if they contain known macro viruses, faster than the all option.

`mime`

Specifies if you want scan inside MIME-encoded files, UU-encoded files, XX-encoded files and BinHex files. Valid values are `yes`, `no`. The default is `no`. Note that to enable this option, the files option must be set to all.

`mount`

[Linux only] A colon-delimited list of mount points for filesystems that are to be monitored for on-access scanning. This option is for Linux only, and is not supported on RHEL 6. It provides the means to explicitly set which filesystems will be monitored by fanotify(7). The default is an empty list. Note that filesystems will only be monitored if their type does not appear in the internal list of known unsupported filesystem types and is not part of fsexcl configuration. Note also that the decision to scan a file will still be subject to include and exclude criteria.

`fsexcl`

A colon-delimited list of filesystem type names that are to be excluded from monitoring. The default is an empty list. Note that the decision to scan a file will still be subject to include and exclude criteria.

On Linux, this is used to limit which filesystems will be monitored by fanotify(7), and complements the internal list of filesystem types that we know cannot be monitored. The names are those from the third column of /proc/mounts, see proc(5).

On AIX, the names are those from the first column of /etc/vfs, see vfs(4). The name remote can be used to select all names in /etc/vfs that are marked as remote.

`notify`

A comma-delimited list of notifier names to be used to report events. See the avconfig page for more information on notifiers.

Filesystem Cache Configuration

The filesystem cache is used to increase performance by reducing the need to repeatedly scan files that have not changed since the last time they were scanned. The options for this feature are set using these values: fscache, fscacheage, fscacheidle, and fscachesize.

Note that expiry of cache data occurs hourly. The procedure prunes the cache using one or more of fscacheage, fscacheidle, and fscachesize parameters, if enabled, and in that order.

`fscache`

The filesystem cache is used to increase performance by reducing the need to repeatedly scan files that have not changed since the last time they were scanned. Note that expiry of cache data occurs hourly. The procedure prunes the cache using one or more of fscacheage, fsacheidle amd fscachesize parameters, if enabled, and in that order. Also note that cache operations are much faster if fscacheage, fscacheidle and fscachesize are all set to 0.

Set to `yes` to enable, or `no` to disable the cache. The default is `yes`.

`fscacheage`

A time to live for an unchanged object in the cache. If the object record has not been re-scanned in that time, it will be removed from the cache. This is expressed in minutes, and can be an integer value between 0 and 999999. The default is `0`, which disables the feature.

`fscacheidle`

A time to live for a cache object that has not been re-scanned (changed) or queried (hit). This is expressed in minutes, and can be an integer value between 0 and 999999. The default is `0`, which disables the feature.

`fscachesize`

A maximum size for a single filesystem cache. There is one cache per filesystem.The cache expiry operation will reduce the cache to this maximum size, expelling oldest unchanged objects first. This is expressed as the number of files in the cache, and can be an integer value between 0 and 999999999. The default is `0`, which disables the feature.

Example Server Configuration

```
[avsvc]
access=open
include=/
exclude=/dev:/run
threads=8
maxwait=120
clean=yes
cleanfail=quarantine
programs=yes
archives=no
fscache=yes
fscachesize=1000000
```

Logging Configuration

Logging is controlled through the file zlog-avsvc.conf in the product directory.

The config rules are used when the server is run with the -V option.

The debug rules are used when the server is run with the -d option.

Otherwise the avsvc rules are used.

For more information on zlog, visit https://hardysimpson.github.io/zlog/UsersGuide-EN.html.

Commands

The avsvc executable can also be used to request information or operations from a running server, through use of the -c option. The following commands are available:

`status`

Show the status of the server: running or inactive. The exit code will be 0 for a running server, or 1 if it is inactive.

`info`

Show versions, virus handling counts and internal server statistics.

See also: avupdate, avscan, avsvcctl and avconfig.

Exit Status

On success, 0 is returned, a non-zero failure code otherwise.

Performance Considerations

When applications open files that require scanning, there is a delay while the system completes the scan. For most files, the scanning takes only a fraction of a second. However, large files, archive files, and compressed files can take several seconds or minutes.

Once a file has been scanned by the on-access service, the scan result is stored in a cache for the file system if the file system cache has been enabled for the service. The cache is consulted the next time the file is accessed, and if it has not been modified, it will not require scanning again and access will be faster. The cache is cleared completely upon on-access service exit, update of virus definitions, or significant changes to service configuration. Individual items in the cache are also subject to size and time-to-live constraints and are configured in the service configuration.

Archive scanning takes additional CPU resources, and can be disabled. Many viruses come in the form of .zip archive files.

Recommendations

- Virus definitions are released daily. Be sure to keep the database up-to-date using the avupdate tool (see Updating Virus Definitions).

- Java runtimes contain many .jar files that can take a long time to scan. This can cause a noticeable delay when starting Java applications. Consider running a simple file access command to pre-load scan results for these files into the service cache after a virus database update, service restart, or other live configuration change.

For example:

```
find /usr -type f -name \*.jar -exec file {} \; >/dev/null
```

Example Messages

The following log messages are from the on-access service log (avsvc.log).

1. Example of an infected file being detected, unable to be cleaned, and quarantined (clean=yes, cleanfail=quarantine):

   ```
   2018-04-20 15:21:19 WARN [39998:avsutil.c:640] VIRUS:
   '/mnt/extra/testing/eicar.com' is INFECTED with 'EICAR test
   file'
   2018-04-20 15:21:19 WARN [39998:avsutil.c:369] quarantined file
   /mnt/extra/testing/eicar.com
   ```

2. Example of an infected file being detected, unable to be cleaned, and removed (clean=yes, cleanfail=delete):

   ```
   2018-04-20 15:17:29 WARN [39998:avsutil.c:640] VIRUS:
   '/mnt/extra/testing/eicar.com' is INFECTED with 'EICAR test
   file'
   2018-04-20 15:17:29 INFO [39998:avsutil.c:382] file
   /mnt/extra/testing/eicar.com deleted
   ```

3. Example of an infected file being detected twice in report-only mode (clean=no). The second message indicates it was not scanned on the second file access, the cached value was used:

   ```
   2018-04-20 15:19:42 WARN [39998:avsutil.c:640] VIRUS:
   '/mnt/extra/testing/eicar.com' is INFECTED with 'EICAR test
   file'
   ```

avsvcctl command

The avsvc server provides on-access scanning for viruses and malicious code. The server is not running after first installation. Server configuration should be decided, and then the server started and (optionally) enabled to start at boot. You can also use the `avsvcctl` command to start, stop, and manage the other functions of the service.

On-Access Scanning can be started and stopped for Endpoints, both individually and in groups, using Powertech Antivirus Server. For details, see On-Access-Scanning with Powertech Antivirus Server.

Find commands to troubleshoot on-access scanning in avsvcinfo command, and avsvc command.

Name

`avsvcctl` - Powertech Antivirus service helper.

Synopsis

```
avsvcctl [status | statistics | log | install | uninstall | enable |
disable | start | stop | restart | reload | help]
```

Description

The `avsvcctl` command can be used to control and monitor the anti-virus service.

Options

`-j`

Show the output in JSON format, where possible. Currently this is only supported for status and statistics commands.

`status`

Shows the running status of the anti-virus service.

`statistics`

Show scanning performance measures for the service.

`log`

Display the latest entries in the avsvc.log file.

`install`

Install the anti-virus service control file into the system area. Note that this will overwrite anything already in place. This option can only be run by the root user.

`uninstall`

Remove the anti-virus service control file from the system area. Note that this will also stop the service and disable it from starting at boot. This option can only be run by the root user.

`enable`

Set the anti-virus service to start during system boot. Note that this will register the service with the operating system, if necessary. Note on Solaris, this command will also start the service if it is not already running. This option can only be run by the root user.

`disable`

Prevent the anti-virus service from starting during system boot. Note on Solaris, this command will also stop the service. This option can only be run by the root user.

`start`

Start the anti-virus service. Note that this will install the anti-virus service control file, if necessary. This option can only be run by the root user.

`stop`

Stop the anti-virus service. This option can only be run by the root user.

`restart`

Restart the anti-virus service. Note that this will install the service control file, if necessary. This option can only be run by the root user.

`reload`

Reload (reconfigure) the anti-virus service. This option can only be run by the root user.

`help`

Show this manual page.

See Also

avupdate command

avscan command

Exit Status

On success, 0 is returned, a non-zero failure code otherwise.

avsvcinfo command

Name

avsvcinfo - Query the anti-virus service.

Synopsis

avsvcinfo [-j | -r | -h]

Description

The avsvcinfo command can be used to retrieve runtime status, configuration and performance statistics from the anti-virus service.

> **NOTE:** This command is used for on-access scanning only.

Options

Without options, an abbreviated summary of configuration and performance is shown.

`-q`Show the summary and details of quarantined files. You must be root to see quarantined files.

`-j`Show complete configuration, status and performance data in JSON format.

`-r`Reset performance statistics. This can only be run by the root user.

`-h`Show this manual page.

See Also

avsvc command

avsvcctl command

Exit Status

The command returns 0.

avscan command

Syntax

```
avscan [ -r ] [--ignorelinks] [ --noheuristics ] [ --
nomacros ] [ --pup ] [ --mime ] [ --[no]arc ] [ --exeonly ] [ --
exclude {file(s):directorie(s) } ] [ --maxwait seconds ] [ --timeout
seconds ] [ --delay microseconds ] [ --scanthreads threads ] [ --
clean ] [ --quar ] [ --cmd <"command-string"> ] [ --notify
<"notifiers"> ] [ --loglevel level ] [ --quiet ] [ --notscanned ] [
--version ] [--help] file1:file2:dir1:dir2 ...
```

Description

The `avscan` command scans the specified file or directory for viruses and malicious code.

When an infection is found, prints a message to the output stream and the infected file remains unchanged. To have the command clean or quarantine infected files you need to specify either the `--clean` or `--quar` options (or both). If a file cannot be cleaned, it will be deleted, unless the `--quar` option is also specified.

If you specify the `-r` flag, the `avscan` command descends the specified directories recursively. If no file or directory is specified, the `avscan` command scans the current directory without descending subdirectories. For example:

```
./avscan
```

Will simply scan the current directory. To scan a specific file or directory recursively, use the following:

```
./avscan -r /home/testuser
```

You can use wildcards in file names:

```
./avscan /home/usr*
```

To send the output stream to a log file, use the redirection symbol:

```
./avscan > mylog.txt
```

Options

`-r`

Descends directories recursively.

`--ignorelinks`

Ignore all symbolic links that are found during the scan. This is the default behavior. This option is here for reasons of backwards compatibility.

`--noignorelinks`

Follow all symbolic links found during the scan.

`--noheuristics`

Do not use heuristic analysis when scanning files. The scanning engine normally employs heuristic technology to detect new viruses in executable files in addition to its normal scanning. Without heuristics, the engine can only find viruses that are already known. Heuristics slows scanning performance and increases paranoia. Default is to use heuristics, so `--noheuristics` will turn this feature off.

`--nomacros`

Do not scan compound documents for macros viruses. This parameter is similar to heuristics but scans for new viruses in compound document formats; for example Microsoft OLE formats such as Word documents. Default is to scan for macro viruses, so `--nomacros` will turn this feature off.

`--pup`

Detect potentially unwanted programs. Some widely available applications, such as password crackers or remote-access utilities can be used maliciously or can pose a security threat. If you set this parameter, the product scans for such files.

Default is to *not* scan for Potentially Unwanted Programs, so `--pup` will turn this feature on.

`--mime`

Scan for viruses in MIME-encoded files, UU-encoded files, XX-encoded files and BinHex files, and files in TNEF and IMC formats. This parameter reduces scanning performance.

Default is to not scan these types of files so --mime will turn this feature on.

`--arc`

Scan within archives (.zip, .jar, .rar, etc).The term "archive" also refers to disk images, installers underpinned by archive formats, mime attachments and other complex files that include embedded elements. Many archive files (especially jar files) can drastically increase scanning time. You may want to scan archives on a weekly basis, for example.

The default is not to scan within archives.

`--noarc`

Do not scan within archives (.zip, .jar, .rar, etc). This is the default behavior. This option is here for reasons of backwards compatibility.

`--exeonly`

Do not scan non-executable files (.txt, etc). Default is to scan all files (recommended), so `--exeonly` will scan executable files only.

`--exclude <file1:file2:directory1:directory2:...>`

Excludes the specified files and/or directories from scanning.

> **NOTE:** If your exclude string contains wildcard characters you need to surround the string in quotes (i.e. --exclude "/excluded-file*")

> **EXAMPLE:**
> `avscan --exclude /home/usr1:/home/usr2`
> will exclude both the /home/usr1 and /home/usr2 directories.

> **NOTE:** /proc, /sys (Linux) and /Quarantined do not need to be excluded on the command-line. A recursive scan will not walk into those directories unless those paths are explicitly requested for scanning.

`--maxwait <seconds>`

Specifies the maximum number of seconds to spend scanning any one file. After the number of seconds has elapsed the product assumes the file is OK and proceeds with the next file. It can be an integer value between 0 and 99999. The default is 300 seconds. A value of 0 disables the feature (files are scanned completely).

`--timeout <seconds>`

Specifies the maximum number of seconds the avscan command will execute before returning. After the number of seconds has elapsed, the command will end without scanning any remaining file(s). The return code will indicate a timeout has occurred.

It can be an integer value between 0 and 999999. The default value of 0 disables the timeout.

`--delay <microseconds>`

The amount of time in microseconds the scanner should pause with each progress beat from a scanning operation. This can be used as a simple CPU limiting technique. It can be an integer value between 0 and 999999. The default value of 0 disables the feature.

`--scanthreads <threads>`

The number of scanning threads to allocate for concurrent scanning of files. This can reduce overall scanning time for scanning many files on systems with mutiple CPUs. It can be an integer value between 1 and 16. The default value is 1 thread.

`--clean`

Clean infected files by repairing the infection. Most infections cannot be cleaned.

> **WARNING:** If the file cannot be cleaned it will be deleted (unless the `--quar` option is specified).

`--quar`

Quarantine the infected files by moving them to the /Quarantined directory. When `--quar` and `--clean` are both specified, the product attempts to clean the file first, and if unsuccessful moves the file to the quarantine directory. If neither `-clean` or `--quar` are specified, no actions are taken on infected files. This is the default.

`--cmd <"command string">`

Runs the specified command string when infections are found, passing the file name as a parameter. This allows a user-written script to perform actions such as alerting an administrator. This file will be a live infected file, and in no way should the script attempt to read it. The intention is to allow you to process the file name. You may want to implement a procedure to notify and administrator, for example. If the file remains after the command returns it will be deleted.

```
--notify <"notifiers">
```

Notify those notifiers in the comma separated list which are defined in the [notify] section of config.ini. This list will override the list defined by the config.ini avscan:notify parameter. Note that notify names should be lowercase.

See Notification Support in avconfig command.

```
--loglevel <level>
```

Specifies the number of directory levels that will be printed in the output listing. The default is 99.

```
--quiet
```

Prints minimal information to the output stream, useful for parsing the output file.

```
--notscanned
```

When used in conjunction with the quiet option, this enables the additional reporting of errors, timeouts and skipped files.

```
--version
```

Prints the program version and build information, then exits.

Skipped Files

Files may be skipped (i.e. not scanned, or only partially scanned) for the following reasons:

```
aborted
```

Scanning of the file was aborted, typically due to a timeout or resource issue.

`archive`

The archive file was not scanned because archive scanning is disabled.

`broken link`

The file is a link that points to nowhere.

`circular link`

The file is a link that would create a loop in the scanning tree.

`corrupted`

The file, or one or more of the files inside an archive file, is corrupt and was not scanned.

`encrypted`

The file, or one or more of the files inside an archive file, is encrypted and could not be scanned.

`link`

The file is a link and was not followed because the option to follow links is not enabled.

`nesting limit reached`

Nesting refers to an archive file containing an archive file that contains a further archive file and so on. One or more archive files inside the top-level archive had too many levels of nesting and was not fully scanned.

`not executable`

The file, or one or more of the files inside an archive, is not considered executable and was not scanned. This can occur when the exeonly option is used, or when the engine scans a container expecting to find an executable file - and one does not exist.

`not accessible`

The scanner could not access the file for reading or writing.

`not readable`

The scanner could not open the file for reading.

`non-regular file`

The file is a special file that cannot be scanned, i.e. a Unix domain socket, pipe, FIFO, block or character device file.

`settings`

The file was not scanned due to the scanning options employed. Note that it is not currently possible to determine whether the options pup, mime, macro or heuristics would product a different scan result, so those options are unlikely to trigger this skip code.

`timeout`

The file was not completely scanned due to the time allowed via the maxwait setting.

`unsupported object type`

The file, or one or more of the files inside an archive, is of an unexpected type and cannot be scanned. An example of this would be a path name, that was originally determined to be a file, has been changed to a directory in the interval between the scanner finding it and attempting to scan it.

Scan Summary

At the end of a scan, a set of statistics are presented. These statistics include file counts, infection activity, error counts and a summary of file skip reasons.

Scan Statistics

`files scanned`

The number of files inspected fully. This does not include skipped files, archives including skipped files, or files that encounted errors during scanning.

`infected`

The number of files that were determined to be infected.

`skipped`

The number of files that were reported as skipped during scanning. This count includes archives that contained skipped files.

`errors`

The number of errors encountered during scanning files, resulting in the files not being scanned, removed or quarantined.

`cleaned`

The number of infections that were successfully cleaned.

`deleted`

The number of files that were deleted because cleaning attempts failed.

`quarantined`

The number of files that were successfully moved to quarantine.

Skip Statistics

`link(s)`

The number of links, cyclic links and broken links that were skipped.

`archives`

The number of archive files or other containers that were skipped, due to archive scanning being disabled.

`settings`

The number of files skipped due to settings other than archive scanning. This count includes the files skipped as not executable (e.g. when the exeonly option is in use).

`no-access`

The number of files skipped because they were not readable or writable.

`encrypted`

The number of files skipped because they were determined to be encrypted. If archive scanning is enabled, this includes the number of archives containing encrypted files.

`corrupt`

The number of files skipped because they were determined to be corrupted. If archive scanning is enabled, this includes the number of archives containing corrupt files.

`timeout(s)`

The number of files that encountered a timeout during scanning, through the maxwait configuration option.

`other`

The number of files skipped for any other reason. This includes nesting limits, special files, and unsupported file types.

Examples

EXAMPLE: `avscan`
Scans all files in the current directory.

EXAMPLE: `avscan -r /`
Scans all files in the current directory and all sub-directories.

EXAMPLE: `avscan -r / --clean --quar`
Scans all files on the system and if an infection is found, the file is cleaned. If cleaning fails, the file is moved to the /Quarantined directory.

EXAMPLE: `avscan -r / --clean --quar > avscan.out`
Scans all files on the system and if an infection is found, the file is cleaned. If cleaning fails, the file is moved to the /Quarantined directory. Sends all output to the avscan.log file in the home or current directory.

If the file cannot be found, try the default path name: `/opt/sgav/avscan.log`.

EXAMPLE: `avscan -r / --scanthreads 4`
Scans all files on the system, using up to 4 threads to improve throughput and reduce the time for the complete scan.

EXAMPLE: `avscan -r / --quiet --notscanned`
Scans all files on the system, reporting only files that are infected, skipped, or encountered errors during scanning.

Notes

If the file cannot be found try the default path name: /opt/sgav/avscan.

To schedule a scan using cron, run command `crontab -e` to edit the crontab file using the vi editor. Position the cursor to the end and type i to insert a line. Type the following line to schedule the job to run every day at 1am. This example will scan the home directories and time out after 4 hours:

```
0 1 * * * /opt/sgav/avscan -r /home --timeout 864000 --clean --quar
> /opt/sgav/log/avscan.out
```

To see the cron log, run `tail /var/adm/cron/logtail /var/log/syslog`. For more information about scheduling using cron, run `man crontab`.

Exit status

The four exit status values that can be returned are:

`0` Process completed successfully. No virus(es) detected.

`1`Process completed, but one or more files were not scanned due to an error.

`2` Timeout reached (`--timeout` parameter) or scan interrupted.

`3` One or more virus infections were found.

Performance Considerations

On-demand scanning of the entire file system can be a very long running, CPU-intensive process. The time required to complete a full scan depends upon several factors, including the speed of the processor, the contention of CPU resources with other jobs, and the number and types of files to scan.

At the expense of scanning time, the impact of the on-demand scan on other jobs in the system can be lessened by the following:

- Use of nice(1) to downgrade the scheduling priority of the task
- Use of the delay option to yield CPU time at regular intervals

Recommendations

- Schedule scan tasks to run during off-peak hours.
- If you are not using on-access scanning, then run a full scan once per day if possible.
- Virus definitions are released daily. Be sure to keep the database up to date using the avupdate tool.
- Exclude /dev and optical media mount paths from your scan using the exclude path option. It is no longer necessary to exclude /proc and /sys as these paths are automatically excluded for recursive scans.
- Enable on-access scanning to reduce or eliminate the need for on-demand scanning.
- Review the scan reports to understand the length of time to scan specific directories.

avsysinfo command

This command provides system and environment information needed to help support personnel diagnose errors in the Powertech Antivirus application.

avupdate command

Name

avupdate - Update Virus Definitions.

Synopsis

avupdate [options] [path]

Description

The avupdate command downloads (or copies) virus definition files from a remote location and applies them to the product. Trellix updates virus definitions every day and you should run the avupdate command every day. By default, files will be retrieved from Trellix's HTTP server (https://update.nai.com/products/commonupdater) using curl.

This can be overridden using the --path, --ftp, --wget or --curl options (see below).

To start the update, either change to the product directory or type the full path to the avupdate command:

```
/opt/sgav/avupdate
```

The update process must be run by a root user. This is to prevent a non-root user from accidentally (or maliciously) tampering with the files.

Once started, progress messages will appear as follows:

```
Powertech Antivirus DAT update 5.0.0 starting
Tuesday, Mar 05 19 04:20:23 PM
Source=http://update.nai.com/products/commonupdater
curl http://update.nai.com/products/commonupdater/oem.ini ...
Success!
Remote DAT level is 9186
Local DAT level is 9136
Performing incremental update...
curl http://update.nai.com/products/commonupdater/gdeltaavv.ini ...
Success!
Running full update...
curl http://update.nai.com/products/commonupdater/avvdat-9186.zip
```

```
...
Success!
Expanding avvdat-9186.zip ...
```

Options

`--path`

Specifies the path to use to download the files. Use this option to obtain DATs file from a local or network path.

`--ftp`

Files will be downloaded using the system 'ftp' client. When using FTP, the path argument must be a URL:

ftp://user:password@host:port/directory

If the user and password are not specified, they default to anonymous. If port is not specified it defaults to 21. If directory is not specified, it defaults to '/'. Command output will be sent to log/ftplog.txt.

The following defaults are used unless otherwise specified:

- User: anonymous
- Port: 21
- Directory: /

If neither --path or --ftp is specified the files are retrieved using curl.

`--curl`

Files will be downloaded using the system 'curl' client:

`/usr/bin/curl or /usr/local/bin/curl.`

This is the default option if none of --path, --ftp or --wget options are specified.

On Solaris, we also look for:

`/opt/csw/bin/curl` and `/usr/sfw/bin/curl`.

On AIX, we also look for:

`/opt/freeware/bin/curl`

Command output will be sent to:

`log/curl.log`.

`--wget`

Files will be downloaded using the system 'wget' client:

`/usr/bin/wget`.

On Solaris, we also look for:

`/opt/csw/bin/wget` and `/usr/sfw/bin/wget`

On AIX we also look for:

`/opt/freeware/bin/wget`

Command output will be sent to:

`log/wget.log`.

To specify additional parameters to the wget command, enclose the path and options in quotes (e.g. "ftp://ftp.nai.com/CommonUpdater --tries=10". Be sure to specify at least one space between the path and wget options).

`--avget`

Files will be downloaded using the product 'avget' client, if it is available on this platform. Command output will be sent to log/avget.log.

`--full`

Performs a full update of virus definitions instead of an incremental update. Incremental updates transfer fewer bytes, and therefore faster download times.

A full update will always transfer the complete set (approximately 150MB, subject to change).

`--cmd <"command-string">`

Runs the specified command string after a successful update of virus definitions. This can be useful to execute a user written script to perform additional processing as needed.

`--passive`

Runs the FTP process using passive mode.

`--sscert`

Passes options to curl, avget, or wget to have them avoid checks for self-signed server certificates.

`--force`

Forces an update of the virus definitions even if the files are already up to date.

`--decomp`

When an update is to be applied, this causes a rewrite of the virus definition files to an optimal format for faster initialization time.

`--savepath <path>`

Copies the virus definitions to the specified path after a successful update. Example: avupdate --savepath /dat

To save the output of the avupdate command to a log file, use the redirection operator:
`/opt/sgav/avupdate > /home/logs/avupdate_log.txt`

`--version`

Prints the program version and build information, then exits.

`--Path`

Specifies the path to use to download the files. Default is http://update.nai.com/products/commonupdater (subject to change). --curl is the default option if --path, --ftp, or --wget options are not specified.

`--ptavrepo`

Indicates the path is a Powertech Antivirus DAT repository. When called via Powertech Antivirus Server request, the command references the root file server path and resolves the DAT level subfolder dynamically.

Example:

```
./avupdate --ptavrepo https://myreposerver.mydomain.com:8023
```

A similar command could be employed from a command shell:

```
./avupdate --ptavrepo https://myreposerver.mydomain.com:8023
```

`--help`

Displays help text.

Examples

```
/opt/sgav/avupdate

/opt/sgav/avupdate --decomp --https

/opt/sgav/avupdate --decomp --full --force

/opt/sgav/avupdate --wget

/opt/sgav/avupdate --path /tmp/datfiles

/opt/sgav/avupdate --curl
http://update.nai.com/products/commonupdater

/opt/sgav/avupdate --ftp ftp://myuser:mypass@mysite/downloads/av
```

```
/opt/sgav/avupdate   --avget  --sscert  --ptavrepo
https://ptavwebservice:8023
```

Notes

Trellix updates virus definitions every day and you should run avupdate every day. To schedule using cron, run command "crontab -e" to edit the crontab file using the vi editor. Position the cursor to the end and type i to insert a line. Type the following line to schedule the job to run everyday at 6pm (17):

```
0 17  * * * /opt/sgav/avupdate > /opt/sgav/log/avupdate.out.
```

To see the cron log, run "tail /var/adm/cron/log". For more information about scheduling using cron, run "man crontab"

Exit Status

This command returns the following exit values:

0 Process completed successfully.

1 An error occurred.

See Also

Scheduling Updates and Scans

Powertech Antivirus Server User Interface

The topics in this section describe Powertech Antivirus Server user interface.

NOTE:

- To connect Powertech Antivirus to Fortra Application Hub, see the *Fortra Application Hub Installation Guide*.
- See Powertech Antivirus Server and Fortra Application Hub.

Activity Details

This page includes detailed information about Powertech Antivirus activity. See also Activity Status.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Logging > Activity Status**. Click a record in the list.

Identifying the Activity Status

In Progress. Indicates there is at least one item in the request that is in progress.

Failed. Indicates no item in the request is In Progress, and at least one item in the request has failed.

Successful. Indicates all items in the request ended successfully.

Canceled. Indicates Endpoint scanning has been canceled.

Options

Close

Select **Close** to dismiss the page and return to the Activity Status page.

Activity Status

This page allows you to reference status information about requests sent to Powertech Antivirus endpoints, and cancel scans. The list indicates the progress status of each scan request, one of four statuses with their count, the request time, and time the request was completed. The list also includes the status of reports.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Logging > Activity Status**.

Identifying the Status

In Progress. Indicates there is at least one item in the request that is in progress.

Failed. Indicates no item in the request is in progress, and at least one item in the request has failed.

Successful. Indicates all items in the request ended successfully.

Canceled. Indicates the request has been canceled.

Options

> **NOTE:** Options are available for scan requests only, not reports.

(Show Actions)

Select this to show a menu with the following options:

- **View Details.** Click **View Details** for a request to open the Activity Details page, where you can view the status of all Endpoints included in the update request.
- **Rerun All Endpoints.** (Virus Scan requests only) Choose this option to scan all Endpoints included in the original scan request.
- **Rerun on Failed/Cancelled Endpoints.** (Virus scans only) Choose this option to scan all Endpoints in the original Virus Scan request that failed or were canceled.

- **Rerun on Failed Endpoints.** (AND for DAT Level update requests, AND for Configuration update requests, AND for On-Access Service Requests) Choose this option to send a new configuration update request for all Endpoints in the original request that failed.
- **Cancel Request.** Click **Cancel** to stop the scan.

Selected Requests

Select one or more requests using the check box to the left of each request in the list. When you do so, the following options appear in a yellow Show Actions menu bar at the top of the screen. This menu bar allows for changes to multiple requests simultaneously.

- **Cancel.** Choose **Cancel** to dismiss the Show Actions menu.
- **Cancel Request.** Choose **Cancel Request** to stop the request processing for the selected requests, and cancel them.

Add License

To learn how to add and allocate a license to one or more Endpoints, see the *Powertech Antivirus Installation Guide*.

This dialog box allows you to choose a Powertech Antivirus license file to be added to your system. This pane is only for Linux/AIX Endpoint licenses. IBM i licenses are handled by Fortra Application Hub or directly on the Endpoints.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Licenses**. Click **Add**.

Options

Add

1. Click **Upload License File** to open an Explorer window where you can select the license file that was attached to an email delivered from Fortra.
2. Select the license file and click **Open**.
3. On the Add License dialog, click **Add** to assign this license to the system.

Allocate License

To learn how to allocate a license to one or more Endpoints, see the *Powertech Antivirus Installation Guide*.

This dialog box allows you to choose a Powertech Antivirus license file to be allocated to an Endpoint.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Endpoints**. Choose ⋮ for an Endpoint and select **Allocate**.

Options

Allocate

Choose a license file and select **Allocate** to allocate it to the selected Endpoint. In order to allocate a Powertech Antivirus license, it must first be added. See Add License.

Cancel

Click **Cancel** to dismiss the dialog box without allocating a license.

Anti-Ransomware Configurations

> **NOTE:** For an overview of Anti-Ransomware, see Anti-Ransomware.

The Anti-Ransomware Configurations option allows you to add, edit and delete specific configurations of Anti-Ransomware settings.

These unique settings can then be applied to individual IBM i Endpoints. This gives you complete control over the Anti-Ransomware configuration for each Endpoint in your network.

The Anti-Ransomware Configurations panel shows the configurations that have already been defined and displays the following information:

- **Name**: The unique name by which the Anti-Ransomware Configuration is identified.
- **Description**: A textual description of the Anti-Ransomware Configuration.
- **Number of Endpoints**: The number of Endpoints to which this Anti-Ransomware Configuration is currently applied.

How to Get There

In the Powertech Antivirus Navigation Pane choose **Anti-Ransomware** > **Configurations**.

> **NOTE:** See also: Preferences > IBM i Anti-Ransomware Configuration.

Options

Search

These settings allow you to choose the type of data that will be queried when you do a search. You can search by Name, Description or both.

- Click the Search down arrow to open the search settings.
- By default, both Name and Description are selected. Click next to an option to deselect it from the search mechanism.

Searching

A search box is available near the top of your browser window. Type into the Search box to find all items that include the specified text. Be sure the text you are searching for is in the same category selected for "Search By" in the settings (see above). A text search queries all items in the category selected for all servers shown.

All search results that match the entered criteria are displayed in the Configuration list.

> TIP: Click '**x**' in the search box to clear the entered criteria and return to the full list of Anti-Ransomware Configurations.

Add

Click the **+ADD** button to open a New Configuration panel into which the details of a new Anti-Ransomware Configuration can be entered. See New Anti-Ransomware Configuration for more information.

Other options

Click the ⋮ Action button against each Anti-Ransomware Configuration to open a pop-up menu which provides access to options allowing you to edit the existing properties, update the associated Endpoints, duplicate or delete the configuration.

Click in the ☐ Selection box to the left of an Anti-Ransomware Configuration to be able to update the associated Endpoints for the selection or delete the configuration.

> TIP: Click in the ☐ Selection box in the Configurations Header bar to select all Anti-Ransomware Configurations.

Edit Existing Properties

When using the ⋮ Action button against an Anti-Ransomware Configuration, select **Properties** from the pop-up menu to open the Edit Configuration panel. From here the properties of the selected configuration can be amended. See Edit Anti-Ransomware Configurations for more information.

Update Endpoints

When using the ⋮ Action button against an Anti-Ransomware Configuration, select **Update Endpoints** from the pop-up menu to update all of the Endpoints that have been assigned this Anti-Ransomware Configuration.

> **NOTE:** Updating Endpoints can also be invoked when using the ☐ Selection box option. Click in the selection box against the required Endpoint(s) and then click **Update Endpoints** from the Configurations header bar.

Duplicate Configuration

When using the ⋮ Action button against an Anti-Ransomware Configuration, select **Duplicate** from the pop-up menu to open the Duplicate Configuration panel. From here the properties of the selected configuration are duplicated and can be amended as required to create a new configuration. This allows you to quickly create multiple Anti-Ransomware Configurations, where only a few options may change. See Edit Anti-Ransomware Configurations for more information.

Anti-Ransomware Blocked Users

The Anti-Ransomware Blocked Users panel shows all of the users that have been blocked by the anti-ransomware functionality from using any file server functionality on an Endpoint.

The Blocked Users panel allows you to unblock users who have been prevented from accessing a specific IBM i Endpoint.

The following information is displayed:

- **User**: Displays the name of the blocked user
- **Endpoint**: Displays the name of the Endpoint from which the user is blocked
- **Block Time**: The date and timestamp at which the user was blocked
- **Block Origin**: The method by which the user was blocked

How to Get There

In the Powertech Antivirus Navigation Pane choose **Anti-Ransomware** > **Blocked Users**.

Navigation

The following navigation options are available:

- By default, up to 10 rows of blocked users are displayed in reverse alphanumerical order. The display order can be reversed by clicking 

. The display changes to show those blocked users, in numerical-alphabetical order. The arrow next to **User** changes direction to provide a visual representation of the sequence order.
- To display more than 10 Blocked Users on a page click **Rows per page** in the footer of the panel and from the drop-down menu select the new value from 25, 50 or 100 rows.
- To display further pages of Blocked Users (if available) use the arrows in the bottom-right corner of the panel to move forwards and backwards through the list.

Options

Search

These settings allow you to choose the blocked user data that will be queried when you do a search. You can search by User, Endpoint or both:

- Click the Search down arrow to open the search settings.
- By default, both User and Endpoint are selected. Click next to an option to deselect it from the search mechanism.

Searching

A search box is available near the top of your browser window. Type into the Search box to find all items that include the specified text. Be sure the text you are searching for is in the same category selected for "Search By" in the settings (see above). A text search queries all items in the category selected for all servers shown.

All search results that match the entered criteria being entered are displayed in the Blocked User list.

Other Options

Block Origin

The main display allows you to only show blocked users with a specific block origin. By default, users with any block origin value are displayed.

Click **Block Origin: All** to display a drop-down menu that can be used to select one (or any combination) of:

- **Server Configuration**: The configuration of the IBM i Endpoint server caused the user to be blocked
- **Local Configuration**: The local configuration settings of the IBM i Endpoint server caused the user to be blocked
- **Detection**: The user was blocked due to breaking an Anti-Ransomware threshold or was attempting to amend a canary file.

Blocked User Selection

Click the Action button against each Blocked User to open a Properties pane allowing you to unblock the user from the selected Endpoint.

Click in the Selection box to the left of a Blocked User to be able to unblock the user for the selected Endpoint. An option to Unblock the selection is then displayed in the header bar.

TIP: Click in the ☐ Selection box in the Blocked Users Header bar to select all Blocked Users.

For either selection option, click **Unblock** to open a prompt where you can either confirm the unblock action or cancel it.

Anti-Ransomware Endpoints

The Anti-Ransomware Endpoints panel shows all of the IBM i Endpoints that are available to have an Anti-Ransomware specific Configuration applied.

The Endpoint panel allows you to assign and update the Anti-Ransomware Configuration that is applied to each Endpoint (if required).

The following information is displayed:

- **Alias**: Displays the name by which the Endpoint has been defined
- **Configuration**: If applicable, displays the name of the Anti-Ransomware Configuration currently assigned to the Endpoint

How to Get There

In the Powertech Antivirus Navigation Pane choose **Anti-Ransomware** > **Endpoints**.

Navigation

The following navigation options are available:

- By default, up to 10 rows of Endpoints are displayed in status order, critical Endpoints first. The display order can be reversed by clicking 

. The display changes to show those Endpoints in an OK status first. The arrow next to Status changes direction to provide a visual representation of the sequence order.
- To display more than 10 Endpoint rows on a page click **Rows per page** in the footer of the panel and from the drop-down menu select the new value from 25, 50 or 100 rows.
- To display further pages of Endpoints (if available) use the arrows in the bottom-right corner of the panel to move forwards and backwards through the list.

Options

Search

These settings allow you to choose the Endpoint data that will be queried when you do a search. You can search by Alias, Status Message or both.

- Click the Search down arrow to open the search settings.
- By default, both Alias and Status Message are selected. Click next to an option to deselect it from the search mechanism.

Searching

A search box is available near the top of your browser window. Type into the Search box to find all items that include the specified text. Be sure the text you are searching for is in the same category selected for "Search By" in the settings (see above). A text search queries all items in the category selected for all servers shown.

All search results that match the entered criteria being entered are displayed in the Endpoint list.

Other options

Configuration

The main display allows you to only show Endpoints with a configuration applied. By default, Endpoints with any configuration are displayed.

Click **Configuration: All** to display a drop-down menu that can be used to select one (or any combination) of defined configurations:

Click the Action button against each Endpoint to open a Properties pane containing editing options.

Click in the Selection box to the left of an Endpoint to be able to update the associated configuration for the selection or assign a new configuration to the Endpoint.

> TIP: Click in the Selection box in the Configurations Header bar to select all Anti-Ransomware Configurations.

Update Configuration

Use the **Update Configuration** option to refresh an Endpoint with an amended anti-ransomware configuration, changed using the Edit Configuration options. This allows you to update multiple Endpoints with a new configuration with just a single click.

To update the configuration of an Endpoint:

1. Click in the ☐ Selection box to the left of the required Endpoint(s) for update.
2. Click **Update Configuration**. A message stating that the selected Endpoint(s) will be updated in the background is displayed in the panel.

IMPORTANT: This option is only applicable to Endpoints that have an anti-ransomware configuration applied.

Anti-Ransomware Endpoint Properties pane

The Anti-Ransomware Endpoint Properties pane displays the Endpoint Alias and Configuration details of the selected Endpoint. From this pane it is possible to assign a different Configuration to an Endpoint.

To open the Endpoint Properties pane:

1. From the Anti-Ransomware Endpoints page, click the ⋮ Actions button against an Endpoint to open a pop-up menu.
2. Click **Properties** to open the Properties pane.
3. The **Alias** field displays the name of the Endpoint. This cannot be changed from this pane.
4. The **Configuration** field shows the current configuration applied to the Endpoint. Click in this field to display a drop-down menu from which an alternative Configuration can be assigned.
5. Click **Save**.

Assign Anti-Ransomware Configuration

Use the **Assign Configuration** option to apply an already defined Anti-Ransomware Configuration to an existing Endpoint. This allows you to apply an Anti-Ransomware Configuration to multiple Endpoints with just a single click.

To assign the configuration of an Endpoint:

1. Click in the ☐ Selection box to the left of the required Endpoint(s) to select for assignment.
2. Click **Assign Configuration**. The Assign Configuration window is displayed.
3. From the drop-down menu, select the anti-ransomware configuration to be applied to the selected Endpoint(s).
4. Click **Assign**.

Change Configuration dialog box

Use this dialog box to change the Configuration assigned to the selected Endpoints.

How to Get There

Select one or more Endpoints on the Endpoints page and choose **Change Configuration**.

Options

Configuration; Local Configuration • Primary • Default • *[other configurations]*

Choose a Configuration to assign to the Endpoints that are currently selected.

Configurations are collections of scan and notification settings that can be added and managed using the Configurations page. You can use this drop-down to assign a Configuration to the Endpoints. If you choose the Primary Configuration, a future change to the Configuration that is set as Primary will also update the Endpoint's Configuration. A Configuration can be assigned to Primary using the Set as Primary toggle switch in its Configuration Properties on the Edit On-Access Configuration pane.

A Configuration can also be changed for an Endpoint using the Endpoint Properties pane.

Cancel • Change

Choose **Cancel** to dismiss the dialog box without changing a Configuration. Click **Change** to change the Endpoint to the selected Configuration.

Connection Settings

The Connection Settings page indicates the connection status of Endpoints.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Connection Settings**.

Or, on the Home page, click **View** for an item in the Connections Status section.

Identifying the Connection Status

Ok. The system is responding to health check requests from Powertech Antivirus Server.

New. System not yet allowed. In order to communicate with Powertech Antivirus Server, the system must be allowed.

Critical. The system is not responding to health checks. You can use **./avinsitectl status** to ensure the Integration Service is running on the Endpoint system.

Blocked. The system has been blocked, indicating it is not allowed to communicate with Powertech Antivirus Server.

Options

[Advanced Search and Filtering options]

See Sort, Search, and Filter Settings in Powertech Antivirus Server and Fortra Application Hub .

(Show Actions)

Uncheck all rows to show this button on the right side of each row. Select it to show a menu with the following options:

- **Properties.** Click Properties for a Connection to open the Connection Properties pane, where you can configure settings for the Endpoint.
- **Block.** Choose this option to block the Connection, preventing communication with Powertech Antivirus Server.

- **Remove Connection.** Choose this option to remove the Connection from Powertech Antivirus Server.

You can apply settings to one or more Connections by selecting them using the check boxes to the left of the Connection name. See Selecting Connections or Configurations in Powertech Antivirus Server and Fortra Application Hub.

Connection Properties pane

The Connection Properties settings allow you to identify Endpoint connection status details and manage the connection.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Connection Settings** and click a connection in the list.

Options

Actions

Click **Actions** to open a submenu with the following connection management options:

- **Block.** Choose this option to block the connection, preventing communication with Powertech Antivirus Server.
- **Remove Connection.** Choose this option to remove the connection from Powertech Antivirus Server.
- **Close.** Choose this option to close the submenu.

Status

Connection Status

The status of the connection. Green indicates the connection is Ok. Red indicates a critical status, meaning the system is not responding to health check requests from Powertech Antivirus Server.

Registration

Indicates the registration status of the connection. Green indicates the status is Ok. Red indicates the connection is not registered.

TLS Certificate

Indicates the status of the TLS certificate along with its expiration date. Green  indicates the certificate is valid. Red  indicates the certificate is expired.

Product Connection

Host Address

The host address of the product connection.

Alias

How the system is displayed in the connection settings list.

Configuration

Installation Location

This is the path of the Integration directory on the Endpoint system.

Configurations

The Configuration page allows you to add or update On-Access and On-Demand Configurations. Configurations define the parameters used by Powertech Antivirus to facilitate scanning.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Configurations**.

Options

Search

These settings allow you to choose how to sort the existing list items, what type of data will be searched when you do a search, and how to filter the list.

- Click **(Settings)** to open the sort, search, and filter settings.
- Select how you want the status list sorted (Sort By). Click your selection again to change the sort order to ascending or descending .

  > **NOTE:** Sorting information, including the column the list is currently sorted by and the sorting direction, is available in your browser's address bar. For example, a URL that includes "sort/**alias**/dir/**1**" indicates the list is sorted by *alias*, *low to high*. A URL that includes "sort/**alias**/dir/**0**" indicates the list is sorted by *alias*, *high to low*.

- Select the list category that will be used for searching (Search By).
- Select the Endpoint Statuses you would like to show in the list (Show In List).
- Select the filtering you want used (Filter By). You can choose to see all the list items, or you can select a specific type.
- Click **(Close)** to close the settings.

Searching

A search field appears near the top of your browser window. Type into the Search field to find all items that include the specified text. Be sure the text you are searching for is in the same category selected for "Search By" in the Sort, Search, and Filter settings (see above). A text search queries all items in the category selected for all servers shown.

> **NOTE:** All search results are accompanied by a unique URL. To save search results, simply bookmark or otherwise record the URL located in your browser's address bar. This URL can then be used to reference the results later. The results will appear in the same sort order.

Add

Opens the New On-Access Configuration pane or New/Edit/Duplicate On-Demand Configuration pane, where you can define a new Configuration.

(Show Actions)

Select this to show a menu with the following options:

- **Properties.** Click Properties to open the New On-Access Configuration pane or New/Edit/Duplicate On-Demand Configuration pane, where you can update settings for the Configuration.
- **Update Endpoints (On-Access Only).** Choose this option to update the Endpoint to restore the assigned Configuration settings.
- **Duplicate.** Choose this option to duplicate the Configuration.
- **Delete.** Deletes the selected Configuration. You are prompted to confirm.

Selected Configurations

Select one or more Configurations using the check box to the left of each Configuration in the list. See Selecting Connections or Configurations in Powertech Antivirus Server and Fortra Application Hub. When you select a check box, the following options appear at the top of the screen:

Delete Anti-Ransomware Configuration

When you choose to delete one or more Anti-Ransomware Configurations, Endpoints assigned to the Configurations being deleted must be reassigned to a new Configuration.

To delete an Anti-Ransomware Configuration

1. Click the ⋮ Action button against the Anti-Ransomware Configuration to be deleted.
2. Select **Delete** from the pop-up menu to open a confirmation prompt. If there are any Endpoints that have been assigned this Anti-Ransomware Configuration, you will need to assign each Endpoint to a configuration other than the one you want to delete, before the deletion can be completed.
3. Once done, click **Delete** to complete the action.

> **NOTE:** Anti-Ransomware Configurations can also be deleted when using the ☐ Selection box option. Click in the selection box against the required Anti-Ransomware Configuration and then click **Delete** from the Configurations header bar.

Delete Configuration dialog box

When you choose to delete one or more Configurations, Endpoints assigned to the Configurations being deleted will be reassigned to a new Configuration. This dialog box allows you to select the Configuration that will be assigned to Endpoints currently assigned to the Configuration being deleted.

Endpoints assigned to Primary will be set to the Default Configuration.

> **NOTE:** If you delete the Primary Configuration, Endpoints that are assigned to Primary will be set to the Default Configuration. Endpoints that have been assigned to the Configuration in a static sense (rather than dynamic), will be assigned to the Configuration chosen from the Configuration drop-down menu. See also Endpoint Properties pane.

How to Get There

Select one or more Configurations on the Configurations page and choose Delete. Or, delete a Configuration using the ⋮ Show Actions submenu.

Options

Configuration; Local Configuration • Primary • Default • *[other configurations]*

Choose a Configuration to assign to the Endpoints currently assigned to the Configuration being deleted.

Cancel • Delete

Choose **Cancel** to dismiss the dialog box without deleting a Configuration. Click **Delete** to remove the Configuration and reassign Endpoints accordingly.

Edit Anti-ransomware Configuration

Follow these instructions to edit the settings within an existing Anti-Ransomware Configuration:

1. From the Anti-Ransomware Configurations panel click on the Action button at the end of the line of the configuration that you want to edit.
2. From the pop-up menu , select **Properties**. The Edit Configuration panel is displayed.

Edit Default Message Threshold For Users

You can amend the following settings:

- Use the slider control to turn off (or on) the ability to Send Messages to the Powertech Antivirus message queue.
- If already set (or if you have you have just activated the Send Messages option), you can over-type (or enter) a new Threshold value for which messages are sent to the Powertech Antivirus message queue.

TIP: Position the mouse pointer in the Threshold Value field to display increase and decrease arrows which can be used to adjust the value from directly within the field.

Edit Message Threshold Overrides for Users

You can amend the following settings:

- If Message Threshold Overrides have already been created for specific users you can amend them by clicking the Action button next to the user name. You can then:
  - **Edit User Override**: Allows you to change the User name and/or the Message Threshold value. You can also use the slider control to turn off (or on) the ability to Send Messages to the Powertech Antivirus message queue for this user. Click **OK** to confirm the change.
  - **Remove User Override**: Click to delete the override for the selected user.
- Click **Add Override** to create a new user message override for this configuration.

TIP: Position the mouse pointer in the Threshold Value field to display increase and decrease arrows which can be used to adjust the value from directly within the field.

Edit Blocked Threshold for Users

You can amend the following settings:

- If Block Threshold Overrides have already been created for specific users you can amend them by clicking the ⋮ Action button next to the user name. You can then:
  - **Edit User Override**: Allows you to change the User name and/or the Block Threshold value. You can also use the  slider control to turn off (or on) the ability to Never Block this user. Click **OK** to confirm the change.
  - **Remove User Override**: Click to delete the override for the selected user.
- Click **Add Override** to create a new block threshold override for this configuration.

TIP: Position the mouse pointer in the Threshold Value field to display increase and decrease arrows which can be used to adjust the value from directly within the field.

Edit Exclude Paths

You can amend the following settings:

- If Exclude Paths have already been created you can amend them by clicking the ⋮ Action button next to the directory path. You can then:
  - **Edit Exclude Path**: Allows you to change the current directory path entry. Click **OK** to confirm the change.
  - **Remove Exclude Path**: Click to delete the excluded directory path.
- Click **Add Exclude Path** to create a new excluded directory path for this configuration.

Edit Canary Files

You can amend the following settings:

- If Exclude Paths have already been created you can amend them by clicking the ⋮ Action button next to the directory path. You can then:
  - **Edit Exclude Path**: Allows you to change the current Canary File path entry. Click **OK** to confirm the change.
  - **Remove Exclude Path**: Click to delete the Canary File path entry.
- Click **Add File Path** to create a new Canary File path for this configuration.

Edit Blocked Users

You can amend the following settings:

- If Blocked Users have already been created you can amend them by clicking the Action button next to the directory path. You can then:
  - **Edit Blocked User**: Allows you to change the current Blocked User entry. Click **OK** to confirm the change.
  - **Remove Blocked User**: Click to delete the Canary File path entry.
- Click **Add File Path** to create a new Canary File path for this configuration.

Endpoints

The Endpoints page indicates the status of registered Endpoints and allows you to manage the Powertech Antivirus Service, which allows you to run On-Demand scans and update virus definitions on Endpoints. This list excludes Endpoints that have not been allowed, as well as Endpoints that have been blocked. (See Connection Settings page for details.)

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Endpoints**.

Or, on the Home page, click **View** for an item in the Endpoints Status section.

Search

Type alphanumeric characters into the search box to find and display endpoints with these sequential characters in any of the endpoint attributes. Click ▼ to the left of the Search box, to display a list of criteria by which to restrict the search. The following criteria are available:

- Alias
- Address
- Configuration
- Endpoint OS
- License
- On-Access Service Status
- IBM i: On-Access
- IBM i: AVSVR Status

By default, all attributes are selected. Use the check boxes to select the criteria that are assigned to the Endpoints you would like to include in the search.

Filters

The following filter options can be used to restrict the display to the endpoints that meet the selected criteria.

Whenever any of the Status, Tags, or Custom options are updated, it is possible to save the selection as a new filter. Click 💾 to open a Save window, where you can provide a name for the new filter and specify whether it should be the default view when opening the Endpoints

page. Once named, click **Save**. This filter will now be available for selection every time the Endpoints page is displayed.

Endpoint Status

By default, all endpoint statuses are selected. Click ▼ in the Status box to display a drop-down menu with the following statuses:

Ok. No issues found.

Warning. No major issues found, but warnings reported.

Critical. Issues found. Action required.

Down. The Endpoint did not respond to the last health check request.

Use the check boxes to select the statuses that are assigned to the Endpoints you would like to display in the Endpoints list.. Multiple selections are permitted.

Tags

Use the Tags drop-down list to specify the Endpoints you would like to display in the Endpoints list.

- Click **Tags** to open the drop-down list. This list includes all tags that have been defined. Tags can be defined and assigned to Endpoints in the Endpoint Properties pane, or in the Manage Tags dialog box (available from the Endpoints screen).
- Type in the ***Search*** field to display only tags that include the submitted text.
- Use the check boxes to select the tags that are assigned to the Endpoints you would like to display in the Endpoints list.
- Use the "No tags" check box to display Endpoints that have no tag assigned.

Custom

Use the Custom Filter to apply additional criteria to the selection of endpoints. The default selection is None. The following custom criteria can be applied:

- None
- License Expired Endpoints

- License Expiring Endpoints (10 days)
- Local Configuration
- On-Access Service - Stopped
- On-Access Service Autostart - Disabled
- Running Scans
- Unlicensed Endpoints
- IBM i: AVSVR Status - Inactive
- IBM i: On-Access - Active
- IBM i: On-Access - Inactive

Use the check boxes to select the custom criteria that are assigned to the Endpoints you would like to display in the Endpoints list.

Options

(Show Actions)

Select this to show a menu with the following options. The options shown vary depending on the operating system of the Endpoint:

- **Properties.** Opens the Endpoint Properties pane, where you can identify Endpoint status details and license information, modify the Endpoint alias, and perform additional actions.
- **Run Scan.** Opens the Run Scan page, where you can make final adjustments to the Configuration being used and run the scan.
- **Update DAT Files.** Choose this option to update the virus definitions (DAT files) on the Endpoint.
- **Start.** Starts the On-Access service and performs and installs the anti-virus service control file into the system area if needed.
- **Stop.** Stops the On-Access service.
- **Enable Autostart.** Configures Powertech Antivirus to start on future reboots of the Endpoint. Install is performed if needed.
- **Disable Autostart.** Configures Powertech Antivirus to not start on future reboots of the Endpoint.
- **Restart.** Restarts selected Endpoints. Selected Endpoints that are not running are also started. Install is performed if needed.
- **Manage Quarantine.** If quarantined files exist for an Endpoint, this option is available. Choose this option to open the Quarantined Files page, where you can view and manage quarantined files.

- **Allocate License.** Choose this option to allocate the license to the selected Endpoint.
- **Remove License.** Choose this option to remove the license from the selected Endpoint.

Select All; Select All On Page • Select All Across Page

Check this box to select all on the page or across pages. Use the adjacent drop-down list to indicate the action to be taken when checking this Select All check box.

- Choose **Select All On Page** to indicate this check box should select all Endpoints on the current page only.
- Choose **Select All Across Pages** to indicate this check box should select all Endpoints, including all Endpoints listed on subsequent pages.

Selected Endpoints

Select one or more Endpoints using the check box to the left of each Endpoint in the list. When you do so, many of the same options described above, and additional configuration options, appear in a yellow Show Actions menu bar at the top of the screen. This menu bar allows for changes to multiple Endpoints simultaneously.

The options shown vary depending on the operating system of the Endpoint. The additional configuration options, other than those described in Show Actions are:

- **Assign Configuration.** Choose this option to assign a Configuration to the Endpoint.
- **Update Configuration.** Choose this option to update the Configuration on the Endpoint in order to restore the current Configuration settings.
- **Manage Tags.** Choose this option to open the Manage Tags dialog box. This dialog box allows you to assign tags to the selected Endpoints, remove tags from the selected Endpoints, create new tags, or delete existing tags. Tags that are assigned to Endpoints can be used to filter the Endpoint list on the Endpoints page.
  - Green tags (

) are already assigned to all selected Endpoints. Gray tags (

) are assigned to one or more of the selected Endpoints. Click a gray tag to assign it to all selected Endpoints.
  - To assign an existing tag to all selected Endpoints, type the tag text and press enter. Or, click ▾ to display the list of existing tags, then click a tag in the list, or press the down arrow key until the tag is highlighted and press Enter, to assign it to all selected Endpoints.
  - To create a new tag, type the desired tag text and press Enter. (If the tag already exists, it will be assigned to all selected Endpoints.)
  - **Cancel.** Dismiss the Manage Tags dialog box without making changes.

- **Apply.** Assign blue tags to all Endpoints. Delete any existing tags from the selected Endpoints that were removed on the Manage Tags dialog.

> **NOTE:** Tags assigned to an Endpoint are listed in the Endpoint description on the Endpoints page.

Tags can also be managed and assigned for an Endpoint in the Endpoint Properties pane.

Endpoint Properties pane

The Endpoints Properties settings allow you to identify Endpoint status details and license information, modify the Endpoint alias, and perform additional actions.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Endpoints** and click an Endpoint in the list.

Field Descriptions

The fields displayed vary depending on the operating system of the Endpoint.

Status

Shows how the Endpoint responded to the most recent health check. See Endpoints page for a description of the primary statuses.

Alias

How the system is displayed in the Endpoint settings list.

Configuration

Configurations are collections of scan and notification settings that can be added and managed using the Configurations page. You can use this drop-down to assign a Configuration to the Endpoint. If you choose the Primary Configuration, a future change to the Configuration that is set as Primary will also update the Endpoint's Configuration. A Configuration can be assigned to Primary using the Set as Primary toggle switch in its Configuration Properties.

Tags

This option allows you to assign tags to the Endpoint, remove tags from the Endpoint, create new tags, or delete existing tags. Tags that are assigned to Endpoints can be used to filter the Endpoint list on the Endpoints page. See Tags in the Endpoints page topic.

- Type in the "Search" field to display a list of existing tags that include the submitted text. Then, click a tag, or press the down arrow key until the tag is highlighted and press Enter, to assign it to the Endpoint.
- To create a new tag, type the desired tag text in the "Search" field and press Enter.
- Click  to remove the tag from the Endpoint.

Powertech Antivirus Version

The version of Powertech Antivirus installed on the Endpoint.

Powertech Antivirus Engine

The Trellix scan engine used for virus scanning.

DAT Level

The virus definition (DAT file) level currently being used for virus scans.

On-Access Service

Current status of the On-Access Service.

On-Access Service Auto-Start

Whether the On-Access Service is configured to restart if the Endpoint is rebooted.

OS Name • OS Version • OS Release • OS Machine • Host Address

Endpoint system details including the host address of the product connection.

License

On Linux/AIX Endpoints
: Displays Endpoint license information as shown on the License Properties pane.

On IBM i Endpoints
: Displays the license and system information from the IBM i.

Product License (on IBM i Endpoints)

Displays product license information for IBM i Endpoints. The Product License is the license that enables all product functionality.

Support License (on IBM i Endpoints)

Displays support license information for IBM i Endpoints. The Support License is the license that enables the product to download DAT updates (virus definitions).

Options

These options are only available for Linux and AIX Endpoints.

Actions

- **Start.** Starts the On-Access service and performs and installs the anti-virus service control file into the system area if needed.
- **Stop.** Stops the On-Access service.
- **Enable Autostart.** Configures Powertech Antivirus to start on future reboots of the Endpoint. Install is performed if needed.
- **Disable Autostart.** Configures Powertech Antivirus to not start on future reboots of the Endpoint.
- **Restart.** Restarts selected Endpoints. Selected Endpoints that are not running are also started. Install is performed if needed.
- **Manage Quarantine.** If quarantined files exist for an Endpoint, this option is available. Choose this option to open the Quarantined Files page, where you can view and manage quarantined files.

- **Allocate License.** Choose this option to allocate the license to the selected Endpoint.
- **Remove License.** Choose this option to remove the license from the selected Endpoint.
- **Close.** Choose **Close** to dismiss the Actions menu.

Endpoint Registration

The Endpoint Registration page allows you to identify the status of the API key required for Endpoint registration. It also allows you to copy, edit, enable/disable, and regenerate the API key.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Settings > Endpoint Registration**.

Options

API Key

Click ⋮ to show a menu with the following actions:

- **Copy Key To Clipboard.** Copies the API key to the clipboard.
- **Enable/Disable Key.** API keys are enabled by default. You can disable an API key if it is not needed. When Require API Key is set to On, the API key must be enabled in order to add Endpoints.
- **Regenerate Key.** This option regenerates the API key. This action may be required if the old key has been compromised, or as part of, for example, a security policy that requires the key to be regenerated periodically.
- **Edit Key.** Opens the Edit API Key dialog where you can manually edit the API Key.

Require API Key

When off, Endpoints can register without an API key or with any properly formatted UUID/API key (less secure).

Require Approval of New Endpoints

When off, Endpoints are automatically approved (Allowed) on the Connection Settings list after registration (less secure).

Powertech Antivirus Home

The Powertech Antivirus Home page displays the Endpoint Status of systems being scanned and the Connection Status of Powertech Antivirus installations with Powertech Antivirus Server.

How to Get There

In the Navigation Pane for Powertech Antivirus, choose **Home**.

Endpoints Status

These indicators allow you to quickly identify the number of Endpoints at each status level, and navigate to the Endpoints page filtered to include a list of Endpoints at the status level indicated.

Ok. Indicates the number of Endpoints with no warnings or connection issues. Click **View** to open the Endpoints page with the list of Endpoints filtered by "Endpoint Status - Ok."

Warning. Indicates the number of Endpoints with warnings. Click **View** to open the Endpoints page with the list of Endpoints filtered by "Endpoint Status - Warning."

Critical. Indicates the number of Endpoints whose status is Critical. Click **View** to open the Endpoints page with the list of Endpoints filtered by "Endpoint Status - Critical."

Running Scans. Indicates the number of scans that are currently running on connected Endpoints.

Outdated DAT Level

Indicates the number of Endpoints that have outdated virus definitions. For information on updating virus definitions on Endpoints, see Updating Virus Definitions.

Connections Status

These indicators allow you to quickly identify the number of connections between Powertech Antivirus Server and Endpoints at each status level, and navigate to the Connection Settings page filtered to include the list of connections at the status level indicated.

Ok. Indicates the number of systems responding to health check requests from Powertech Antivirus Server. Click **View** to open the Connection Settings page with connections filtered by "Connection - Ok."

Critical. This indicates the number of connections that are not responding to health check requests from Powertech Antivirus Server. Click **View** to open the Connection Settings page with connections filtered by "Connection - Critical."

To be Allowed. This indicates the number of new connections that have not yet been allowed. Click **View** to open the Connection Settings page with connections filtered by "To be Allowed."

Options

Refresh

Refreshes the Home page with the latest status for connections and Endpoints.

View

Click View for a status indicator to open more details in the respective Endpoints page or Connection Settings page.

License Properties pane

This pane displays information about the selected license, including information regarding legacy licenses. This pane is only for Linux/AIX Endpoint licenses. IBM i licenses are handled by Fortra Application Hub or directly on the Endpoints.

> **NOTE:** All information is not available for all licenses.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Licenses**. Click a license in the list.

Field Descriptions

Product

The name of the product and product version.

Signature

The first 10 letters of the license signature.

Mac

The Mac address being used for the license, always 00:00:00:00:00:00.

Expires

Allocated/Count

Licenses may include this field to indicate how many Endpoints the license can be installed on. 'Allocated' is the number of Endpoints currently allocated to this license. 'Count' is the Endpoint capacity of the license.

Generated

Licenses may include this field to indicate when the license was created.

Licenses page

To learn how to allocate a license to one or more Endpoints, see the *Powertech Antivirus Installation Guide*.

This page displays a list of Powertech Antivirus licenses on your system, and allows you to add manage licenses. This page is only for Linux/AIX Endpoint licenses. IBM i licenses are handled by Fortra Application Hub or directly on the Endpoints.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Licenses**.

Options

Add

Opens the Add License dialog box, where you can choose a license file to add.

Logging > Diagnostics

The Logging > Diagnostics page includes information helpful for diagnosing and troubleshooting potential issues.

This information is divided into the following sections:

- **Status:** Gives high-level system information (memory, date/time).
- **Java Properties:** Displays Java information and properties.
- **Environment Variables:** Displays your environment variables.
- **Threads:** Lists all used threads.

Identifying the Status of Powertech Antivirus Services

 The service is active and functioning properly.

 The service is inactive.

How to Get There

From the Powertech Antivirus Navigation Pane, choose **Logging > Diagnostics**.

Options

Diagnostics tab

Refresh

Refreshes the page with the latest logging and diagnostic information.

Logs tab

Refresh

Reloads the display to show the most current log information.

Clear Log

Reloads the display with the log data removed.

Download Logs

Downloads the log data to your local machine in .zip format.

Choose Log

Allows you to choosefrom the available log files:

- ptavws.log
- hsconnect.log
- tomcat.catalina.log
- tomcat.localhost.log
- tomcat.manager.log
- tomcat.host-manager.log

The ptavws.log includes all java related entries that would be found in hsconnect.log, in addition to any log output from the following projects:

- com.helpsystems
- org.springframework
- org.hibernate
- org.apache.kafka
- org.quartz
- net.sf.jasperreports
- org.apache.commons

These help diagnose issues related to the database, communication between services and Endpoints, scheduling, reporting, and others.

The hsconnect.log includes only java related log output from the com.helpsystems.hsconnect project. These entries are focused on communication between services and Endpoints.

(Settings)

Opens the Logging Settings, where you can select the detail of the logging messages for Powertech Antivirus.

Logging Settings

The Logging Settings pane allows you to select the level of logging you want to see.

How to Get There

In the Navigation Pane, choose **Logging > Diagnostics** to open the Logging > Diagnostics page. Choose the **Logs** tab and click  .

Options

Info • Debug • Trace

Select the level of message logging to be used for Powertech Antivirus. You can choose from three levels. "Info" has the least amount of detail; "Trace" has the most.

> **NOTE:** Selecting "Trace" will have an impact on your server performance.

Save • Cancel

Choose **Save** to confirm your logging settings. Choose **Cancel** to dismiss the pane without making changes.

New/Edit Anti-Ransomware Configuration pane

Use these settings to create and configure an Anti-Ransomware Configuration, which can be used by Powertech Antivirus to protect Endpoints from the ongoing threat of ransomware.

How to Get There

In the Anti-Ransomware Configuration Properties pane, choose **+Add**.

Options

Name

Enter a unique name for the configuration you are defining.

Description

Enter a textual description that identifies the purpose of the configuration.

APEX Thresholds

The APEX (Access Pattern and Encryption Activity eXtended) detection method evaluates patterns in NetServer access to the Integrated File System (IFS). When APEX detects suspicious encryption activity, this suspicion level is compared to two thresholds:

- a Message Threshold, which defines when a warning message is sent to the Powertech Antivirus message queue; and
- a Block Threshold, which defines when the accessing user is blocked.

Default Message Threshold For Users

This section is used to set the thresholds to determine when messages are sent to the Powertech Antivirus message queue to warn of a possible ransomware attack on the Endpoint to which this configuration is applied.

The default setting for new configurations is to **Never Send Messages**. This means that even in the event of a possible ransomware attack no messages will be sen to the Antivrus message queue.

Click the  slider control to change the default setting to **Send Messages**. A field allowing the entry of a Threshold Value is displayed.

Enter a value between 1 and 100 to represent the level at which messages are sent to the Antivirus message queue.

> **IMPORTANT:** The lower this value is, the more likely it is that a message may be sent in error, i.e. a false positive. The higher this value is, the less likely it is that a message may be sent in error, but more likely that a ransomware attack may go unreported.

Message Threshold Overrides for Users

This option allows you to set an override value (different from the default threshold) to be applied to specific users. For example, you can set a higher threshold for a trusted user account or for that account to Never Send Messages.

Add Override

Click **Add Override** to open the Add Override window.

1. Enter the **User name** for which this message override will be applied.
2. Leave the slider control set to Never Send Messages so that messages will never be sent from this user account or click the slider control and enter a new message threshold (different from the default setting) that will apply to this user account.
3. Click **Add** to create and apply the message override to the user account.

Once defined, message threshold overrides for users are listed in this section. From here they can be edited and deleted.

Default Block Threshold for Users

This section is used to set the thresholds to determine when a user is blocked from the Endpoint to which this configuration is applied, in response to a possible ransomware attack.

The default setting for new configurations is to **Never Block Users**. This means that even in the event of a possible ransomware attack no user accounts will be blocked.

Click the  slider control to change the default setting to **Block Users**. A field allowing the entry of a Threshold Value is displayed.

Enter a value between 1 and 100 to represent the level at which user accounts will be blocked from the Endpoint to which this configuration is applied. The value represents the number of files being encrypted that Powertech Antivirus detects. The relationship is as follows:

- Powertech Antivirus considers file encryptions performed within the last 5 minutes.
- Each encryption of a file adds to a score.
- The score starts at 0 and can reach a maximum of 100.

The following table shows how the number of file encryptions maps to the score:

Number of Files Encrypted	Scoring Impact
1	-6
2	14
3	32
4	46
5	57
6	66
7	73
8	78
9	83
10	86
11	89
12	92
13	94
14	95
15	96
16	97
17	98
18	98
19	99
20+	100

IMPORTANT: The lower this value is, the more likely it is that a user may be blocked in error, i.e. a false positive. The higher this value is, the less likely it is that a user may be blocked in error, but more likely that a ransomware attack may go unreported.

Block Threshold Overrides for Users

This option allows you to set an override value (different from the default threshold) to be applied to specific users. For example, you can set a higher threshold for a trusted user account or for that account to Never Be Blocked.

Add Override

Click **Add Override** to open the Add Override window.

1. Enter the **User name** for which this block override will be applied.
2. Leave the slider control set to Never Block Users so that this user account will never be blocked or click the slider control and enter a new threshold (different from the default setting) that will apply to this user account.
3. Click **Add** to create the block user override to the user account.

Once defined, block threshold overrides for users are listed in this section. From here they can be edited and deleted.

APEX Exclude Paths

The section allows you to define and maintain the directories that are excluded from being detected by the APEX detection engine.

Add Exclude Path

Click **Add Exclude Path** to open the Add Exclude Path window into which the directory paths to be excluded can be entered.

1. Type the directory path into the window in the following format; for example; /windows/tmp
2. Click **Add** to confirm the directory exclusion.

TIP: Click **Enter** to add further entries to this exclusion path before clicking **Add**.

Once defined, Apex Exclude Paths are listed in this section. From here they can be edited and deleted.

Canary Files

A Canary File is a fake file that is placed amongst real files in order to aid in the early detection of unauthorized data access, copying or modification, which are likely scenarios associated with a ransomware attack.

A canary file can be placed by a user among real files, enabling Powertech Antivirus to detect additional signs of ransomware activity. Whenever a process writes to a canary file, it is immediately considered suspicious, as any legitimate application or user would not access these files. A user will be blocked if they try to tamper with a canary file, for example, if the user tries to update the contents of the file or rename/delete the file.

Canary files can be added to directories that have been overridden to exclude from analysis, to allow some protection for those directories.

IMPORTANT: We recommend that you add canary files to the root directory of vulnerable shares and to critical directories.
The command:
STANDGUARD/AVCRTTEST TYPE(*CANARY) FILE(<path>)
can be used to create a canary file.
Alternatively, any file that is copied to the IFS or created there can be used.

Add File Path

Click **Add Canary File Path** to open the Add File Path window into which the directory paths to be excluded can be entered.

1. Type the directory path and file name into the window in the following format; for example; /windows/tmp/test.jpg
2. Click **Add** to confirm the addition of the canary file.

TIP: Click **Enter** to add further entries to this exclusion path before clicking **Add**.

Once defined, Canary File Paths are listed in this section. From here they can be edited and deleted.

Blocked Users

The Blocked Users section allows you to define, as part of this configuration, which user profiles are blocked from accessing file servers, namely the IBM i NetServer TCP server and Integrated File System host server.

Add Blocked User

Click **Add User** to open the Add Blocked User window into which the user profiles to be blocked can be entered.

1. Type the name of the user profile to be blocked.
2. Click **Add** to confirm the addition of the user profile.

Once defined, Blocked Users are listed in this section. From here they can be edited and deleted.

Save • Cancel

Click **Save** to save the configuration settings. Click **Cancel** to dismiss the pane without making changes.

New/Edit On-Access Report pane

These settings allow you to define the criteria to be used for creating On-Access scanning reports.

> **NOTE:** For details on how to create a report, see Reporting.

How to Get There

In the Reports page, choose **Add > On-Access Report**.

Options

Save • Cancel

Click **Save** to save the report settings. Click **Cancel** to dismiss the pane without making changes.

Type; On-Access Scan Summary • On-Access Scan Daily Summary

From this drop-down list, choose **On-Access Scan Summary** if you would like to define a report that includes an aggregation of all scans for a given period of time. Choose **On-Access Scan Daily Summary** if you would like to define a report that includes a daily aggregation of scans for a given period of days.

Name • Description

A name and description for the report you are defining.

Time Range; Last 60 Min...Custom

From this drop-down list, choose the time period to include. Scans within this time range will be included in the report. Choose **Custom** to specify a start and end time.

Endpoints

Use this filter field to specify the Endpoints you would like to include in the report. For example enter "xyz" to select all Endpoints that contain "xyz" in their alias. You can use multiple filters, separated by a semicolon.

Leave the filter blank to gather data for all Endpoints.

Tags

Endpoints to include on the report can also be selected by the use of assigned tags.

Enter the name of the Endpoint tag that you want to include on the report. Multiple tags can be included. Click ▼ in the Tags field to open the Search facility. Type alphanumeric characters to begin searching for endpoint tags. Click 'Add xx' (where xx is the name of the tag) to select the tag for the report.

> TIP: Any selected tags can be removed from selection by clicking the 'x' next to the tag name.

Leave the Tags field empty to gather data for all endpoints.

Tags Selection Logic

Tags Selection Logic can be applied to the selected tags using OR or AND boolean logic. Use the Toggle switch to select between OR and AND.

- **OR** Filtered endpoints should have any (at least one) of the selected tags assigned
- **AND** Filtered endpoints should have all of the selected tags assigned

> NOTE: Tags Selection Logic is OR by default.

> IMPORTANT: The generated report will only include data for endpoints filtered according to the specified Alias and Tags filters.

Preview Endpoints

Click **Preview Endpoints** to open a display showing the list of endpoints, specified by the selections in alias and tag filters, that will be included on the report when it is generated.

Recipients; Email • Add

Enter an email address and click **Add** to include the email in the list of recipients. When email is properly configured in the Email Settings page, upon report generation, the included recipients will receive an email with a PDF attachment of the report.

Scheduler; Off • On

This setting allows you to run the report instance on a schedule automatically. Toggle to **Off** to disable, or **On** to enable, the automatic generation and distribution of reports. When set to On, the following fields appear, which allow you to define the frequency and timing of automatic report generation.

Repeat; Monthly • Daily • Day of Week

From this list, choose how often you would like to repeat the process of report generation and distribution.

- **Monthly; Day of Month; First Day • Last Day • Custom**

  From this list, choose the day of the month the report should be generated and distributed, first or last. To specify a different day, or list of days, choose **Custom**. With custom selected, specify one or more days of the month. For multiple days, separate each day with a semicolon.
- **Daily**

  Choose this option to run the report each day, at the specified time.
- **Day of Week; list of days**

  Select the days the report should run.

Time

Click this field to specify the hour (0-24) and minute (00-60) of the day the reports should be generated and distributed. Use the arrows adjacent to the hour field to increment by hour. Use the arrows adjacent to the minute field to increment by five minute intervals.

New/Edit On-Demand Report pane

These settings allow you to define the criteria to be used for creating On-Demand scanning reports.

> **NOTE:** For details on how to create a report, see Reporting.

How to Get There

In the Reports page, choose **Add > On-Demand Report**.

Options

Save • Cancel

Click **Save** to save the report settings. Click **Cancel** to dismiss the pane without making changes.

Type; On-Demand Scan Summary • On-Demand Scan Daily Summary • On-Demand Scan History

From this drop-down list, choose **On-Demand Scan Summary** if you would like to define a report that includes an aggregation of all scans for a given period of time. Choose **On-Demand Scan Daily Summary** if you would like to define a report that includes a daily aggregation of scans for a given period of days. Choose **On-Demand Scan History** to define a report that includes a detailed history for On-Demand Scans with additional sorting options.

Name • Description

A name and description for the report you are defining.

Time Range; Last 60 Min...Custom

From this drop-down list, choose the time period to include. Scans within this time range will be included in the report. Choose **Custom** to specify a start and end time.

Endpoints

Use this filter field to specify the Endpoints you would like to include in the report. For example enter "xyz" to select all Endpoints that contain "xyz" in their alias. You can use multiple filters, separated by a semicolon.

Leave the filter blank to gather data for all Endpoints.

Tags

Endpoints to include on the report can also be selected by the use of assigned tags.

Enter the name of the Endpoint tag that you want to include on the report. Multiple tags can be included. Click ▼ in the Tags field to open the Search facility. Type alphanumeric characters to begin searching for endpoint tags. Click 'Add xx' (where xx is the name of the tag) to select the tag for the report.

> TIP: Any selected tags can be removed from selection by clicking the 'x' next to the tag name.

Leave the Tags field empty to gather data for all endpoints.

Tags Selection Logic

Tags Selection Logic can be applied to the selected tags using OR or AND boolean logic. Use the Toggle switch to select between OR and AND.

- **OR** Filtered endpoints should have any (at least one) of the selected tags assigned
- **AND** Filtered endpoints should have all of the selected tags assigned

> NOTE: Tags Selection Logic is OR by default.

> IMPORTANT: The generated report will only include data for endpoints filtered according to the specified Alias and Tags filters.

Preview Endpoints

Click **Preview Endpoints** to open a display showing the filtered list of endpoints, specified by the selections in alias and tag filters, that will be included on the report when it is generated.

Recipients; Email • Add

Enter an email address and click **Add** to include the email in the list of recipients. When email is properly configured in the Email Settings page, upon report generation, the included recipients will receive an email with a PDF attachment of the report.

Scheduler; Off • On

This setting allows you to run the report instance on a schedule automatically. Toggle to **Off** to disable, or **On** to enable, the automatic generation and distribution of reports. When set to On, the following fields appear, which allow you to define the frequency and timing of automatic report generation.

Repeat; Monthly • Daily • Day of Week

From this list, choose how often you would like to repeat the process of report generation and distribution.

- **Monthly; Day of Month; First Day • Last Day • Custom**

  From this list, choose the day of the month the report should be generated and distributed, first or last. To specify a different day, or list of days, choose **Custom**. With custom selected, specify one or more days of the month. For multiple days, separate each day with a semicolon.
- **Daily**

  Choose this option to run the report each day, at the specified time.
- **Day of Week; list of days**

  Select the days the report should run.

Time

Click this field to specify the hour (0-24) and minute (00-60) of the day the reports should be generated and distributed. Use the arrows adjacent to the hour field to increment by hour. Use the arrows adjacent to the minute field to increment by five minute intervals.

Sorting; Sort by: Endpoint • Scan Started Timestamp • Status

From this list, choose how the report details should be sorted. Choose **Endpoint** to sort alphabetically by Endpoint alias. Choose Scan Started Timestamp to sort chronologically,

from earliest to latest based on the timestamp of each scan. Choose Status to sort based on each scan's reported status.

New/Edit Endpoint Status Report pane

These settings allow you to define the criteria to be used for creating an Endpoint Status report.

The Endpoint Status report lists the Endpoints with useful status information.

> **NOTE:** For details on how to create a report, see Reporting.

How to Get There

In the Reports page, choose **Add > Endpoint Status Report**.

Options

Save • Cancel

Click **Save** to save the report settings. Click **Cancel** to dismiss the pane without making changes.

Name • Description

A name and description for the report you are defining.

Columns

- **Basic Values**: These are always included in the Endpoint Status report:
  - Endpoint name
  - Status
  - Operating System
  - Powertech Antivirus version installed
  - Dat level
  - Address

    - Quarantined files
    - Tags
- **Configuration Values**: Select this option to additionally include the following on the report:
    - Configuration type
    - On-Access Info
- **License Values**: Select this option to additionally include the following on the report:
    - License Info

Endpoints

Use this filter field to specify the Endpoints you would like to include in the report. For example enter "xyz" to select all Endpoints that contain "xyz" in their alias. You can use multiple filters, separated by a semicolon.

Leave the filter blank to gather data for all Endpoints.

Tags

Endpoints to include on the report can also be selected by the use of assigned tags.

Enter the name of the Endpoint tag that you want to include on the report. Multiple tags can be included. Click ▼ in the Tags field to open the Search facility. Type alphanumeric characters to begin searching for endpoint tags. Click 'Add xx' (where xx is the name of the tag) to select the tag for the report.

> TIP: Any selected tags can be removed from selection by clicking the 'x' next to the tag name.

Leave the Tags field empty to gather data for all endpoints.

Tags Selection Logic

Tags Selection Logic can be applied to the selected tags using OR or AND boolean logic. Use the Toggle switch to select between OR and AND.

- **OR** Filtered endpoints should have any (at least one) of the selected tags assigned
- **AND** Filtered endpoints should have all of the selected tags assigned

> **NOTE:** Tags Selection Logic is OR by default.

IMPORTANT: The generated report will only include data for endpoints filtered according to the specified Alias and Tags filters.

Preview Endpoints

Click **Preview Endpoints** to open a display showing the list of endpoints, specified by the selections in alias and tag filters, that will be included on the report when it is generated.

Recipients; Email • Add

Enter an email address and click **Add** to include the email in the list of recipients. When email is properly configured in the Email Settings page, upon report generation, the included recipients will receive an email with a PDF attachment of the report.

Scheduler; Off • On

This setting allows you to run the report instance on a schedule automatically. Toggle to **Off** to disable, or **On** to enable, the automatic generation and distribution of reports. When set to On, the following fields appear, which allow you to define the frequency and timing of automatic report generation.

Repeat; Monthly • Daily • Day of Week

From this list, choose how often you would like to repeat the process of report generation and distribution.

- **Monthly; Day of Month; First Day • Last Day • Custom**

  From this list, choose the day of the month the report should be generated and distributed, first or last. To specify a different day, or list of days, choose **Custom**. With custom selected, specify one or more days of the month. For multiple days, separate each day with a semicolon.
- **Daily**

  Choose this option to run the report each day, at the specified time.
- **Day of Week; list of days**

  Select the days the report should run.

Time

Click this field to specify the hour (0-24) and minute (00-60) of the day the reports should be generated and distributed. Use the arrows adjacent to the hour field to increment by hour. Use the arrows adjacent to the minute field to increment by five minute intervals.

New/Edit Threat Report pane

These settings allow you to define the criteria to be used for creating a Threat report.

The Threat report contains a list of all the viruses detected upon the defined criteria and when viewed displays:

- **Endpoint Name**: The name of the endpoint on which the threat was detected
- **Threat**: The type of threat detected
- **Infected Filename**: The name of the infected file on the endpoint
- **Infection Name**: The name of the threat
- **Action Taken**: The action taken against the threat
- **Detection Type**: The detection type used to identify the threat
- **Detected**: Time and date stamp of when the treat was detected

> **NOTE:** For details on how to create a report, see Reporting.

How to Get There

In the Reports page, choose **Add > Threat Report**.

Options

Save • Cancel

Click **Save** to save the report settings. Click **Cancel** to dismiss the pane without making changes.

Name • Description

A name and description for the report you are defining.

Time Range; Last 60 Min...Custom

From this drop-down list, choose the time period to include. Scans within this time range will be included in the report. Choose **Custom** to specify a start and end time.

Endpoints

Use this filter field to specify the Endpoints you would like to include in the report. For example enter "xyz" to select all Endpoints that contain "xyz" in their alias. You can use multiple filters, separated by a semicolon.

Leave the filter blank to gather data for all Endpoints.

Tags

Endpoints to include on the report can also be selected by the use of assigned tags.

Enter the name of the Endpoint tag that you want to include on the report. Multiple tags can be included. Click ▼ in the Tags field to open the Search facility. Type alphanumeric characters to begin searching for endpoint tags. Click 'Add xx' (where xx is the name of the tag) to select the tag for the report.

> TIP: Any selected tags can be removed from selection by clicking the 'x' next to the tag name.

Leave the Tags field empty to gather data for all endpoints.

Tags Selection Logic

Tags Selection Logic can be applied to the selected tags using OR or AND boolean logic. Use the Toggle switch to select between OR and AND.

- **OR** Filtered endpoints should have any (at least one) of the selected tags assigned
- **AND** Filtered endpoints should have all of the selected tags assigned

> NOTE: Tags Selection Logic is OR by default.

> IMPORTANT: The generated report will only include data for endpoints filtered according to the specified Alias and Tags filters.

Preview Endpoints

Click **Preview Endpoints** to open a display showing the list of endpoints, specified by the selections in alias and tag filters, that will be included on the report when it is generated.

Recipients; Email • Add

Enter an email address and click **Add** to include the email in the list of recipients. When email is properly configured in the Email Settings page, upon report generation, the included recipients will receive an email with a PDF attachment of the report.

Scheduler; Off • On

This setting allows you to run the report instance on a schedule automatically. Toggle to **Off** to disable, or **On** to enable, the automatic generation and distribution of reports. When set to On, the following fields appear, which allow you to define the frequency and timing of automatic report generation.

Repeat; Monthly • Daily • Day of Week

From this list, choose how often you would like to repeat the process of report generation and distribution.

- **Monthly; Day of Month; First Day • Last Day • Custom**

  From this list, choose the day of the month the report should be generated and distributed, first or last. To specify a different day, or list of days, choose **Custom**. With custom selected, specify one or more days of the month. For multiple days, separate each day with a semicolon.
- **Daily**

  Choose this option to run the report each day, at the specified time.
- **Day of Week; list of days**

  Select the days the report should run.

Time

Click this field to specify the hour (0-24) and minute (00-60) of the day the reports should be generated and distributed. Use the arrows adjacent to the hour field to increment by hour. Use the arrows adjacent to the minute field to increment by five minute intervals.

New/Edit Notification pane

Use these settings to configure email notifications, which can be triggered by specified Powertech Antivirus events. Notifications can be configured for both on-access scanning and on-demand scanning.

How to Get There

In the Configuration Properties pane, choose **Add Notification**.

Options

Save • Cancel

Click **Save** to save the notification settings. Click **Cancel** to dismiss the pane without making changes.

Name

A name for the notification you are defining. The notification name is case sensitive and must be lower case.

Events

Select one or more of the events in this list that will trigger the notification. These are the same options that can be selected using the avconfig command. See Notification Support in avconfig command.

Command

Enter the command string here to specify, for example, the email addresses that should receive the notification when triggered. For more information, see Notifications.

Notify Options; On-Access Service • On-Demand Scanner

Choose **On-Access Service** to activate selected notifications for on-access scanning (AVSVC). Choose **On-Demand Service** to activate selected notifications for on-demand scanning (AVSCAN). Notifications will not be sent for events unless they are also checked in the list above.

> **NOTE:** Notification settings are the only on-demand scanning configuration options supported by Powertech Antivirus Server. When you save a set of configuration options in Powertech Antivirus Server, the existing config.ini configuration settings file is overwritten.

New/Edit Scheduled Scan pane

This topic describes the options on the New/Edit Scheduled Scan pane. These settings allow you to create a new Scheduled Scan, or modify an existing one. For information on how to schedule scans, see Scheduling Updates and Scans.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Scheduled Scans**. On the Scheduled Scans page, choose **Add** to define a new Scheduled Scan. Or, click within an existing scan's row to open the Edit Scheduled Scan pane, where you can modify an existing Scheduled Scan.

Options

Save • Cancel

Click **Save** to save the Scheduled Scan. Click **Cancel** to dismiss the pane without making changes.

Name • Description

A name and description for the Scheduled Scan you are defining.

Choose On-Demand Configuration

The On-Demand Configuration you would like to use for the Scheduled Scan. More details about the available Configurations can be found on the Configurations page.

Endpoints

The Endpoint aliases to scan, separated by semicolons.

Tags

Endpoints to include in the scan also be selected by the use of assigned tags.

Enter the name of the Endpoint tag that you want to include in the scan. Multiple tags can be included. Click ▼ in the Tags field to open the Search facility. Type alphanumeric characters

to begin searching for endpoint tags. Click 'Add xx' (where xx is the name of the tag) to select the tag for the scan.

TIP: Any selected tags can be removed from selection by clicking the 'x' next to the tag name.

Leave the Tags field empty to run the scan for all endpoints.

Tags Selection Logic

Tags Selection Logic can be applied to the selected tags using OR or AND boolean logic. Use the Toggle switch to select between OR and AND.

- **OR** Filtered endpoints should have any (at least one) of the selected tags assigned
- **AND** Filtered endpoints should have all of the selected tags assigned

NOTE: Tags Selection Logic is OR by default.

IMPORTANT: The generated scan will only apply to endpoints filtered according to the specified Alias and Tags filters.

Preview Endpoints

Click **Preview Endpoints** to open a display showing the list of endpoints, specified by the selections in alias and tag filters, that will be included in the scan when it is run.

Scheduler; Off • On

Toggle to Off to disable the Scheduled Scan. Toggle to **On** to display scheduling options.

Repeat • Day of Month • Time

Use these options to specify the frequency of the Scheduled Scan, by month, daily, or day of week. If monthly, you can specify a day of the month. In the Time fields, specify the hour and minute the scan should run on the days specified.

New/Edit/Duplicate On-Access Configuration pane

The New/Edit/Duplicate On-Access Configuration pane allows you to set configuration options, including notification settings, for on-access scanning.

How to Get There

- To create a new Configuration, on the Configurations page, choose **Add > On-Access Configuration**.
- To create a new Configuration starting with the settings of an existing Configuration, on the Configurations page, for an existing On-Access Configuration, click > **Properties**.
- To edit an existing Configuration, on the Configurations page, for an existing On-Access Configuration, click > **Properties**.

Options

Actions

Click **Actions** to open a submenu with the following connection management options:

- **Duplicate.** Choose this option to duplicate the configuration.
- **Delete.** Opens the Delete Configuration dialog box, where you are prompted to specify a new Configuration for Endpoints assigned to the Configuration you are deleting.
- **Close.** Choose this option to close the submenu.

Name • Description

The name and description of the configuration.

Set as Primary; Off • On

Endpoints set to the Primary Configuration (see Endpoint Properties pane) inherit the settings of the Configuration that is set as Primary. Toggle this switch to **On** to indicate that you would like to set Endpoints currently assigned to the Primary Configuration to the Configuration you are editing. When you click **Save**, the number of Endpoints that will change

is indicated and you are prompted to confirm. Toggle this switch to **Off** to indicate that you would like to set Endpoints assigned to the Primary Configuration to the Default Configuration. The Configuration that is currently set to Primary is indicated in the Configurations page.

Common Settings

On-access scanning Type; File Open • File Open and Close • Disable

File Open specifies that files should be scanned when users attempt to open the file. **File Open and Close** specifies that files should be scanned during file open and after file close. **Disable** disables on-access scanning.

Exclude Paths

A colon-delimited list of path names to be excluded from on-access scanning. The exclude paths take precedence over include paths. A file that exists within any of these path names will not be subject to scanning.

Resources

File Clean

Specifies if the engine should attempt to remove the virus from the file. If the file cannot be cleaned, the cleanfail option provides a secondary choice. Set to yes to enable, or no to disable. The default is yes.

File Clean Fail; Quarantine • Delete • No Action

Action if not cleaned. The default is quarantine. Quarantined files are stored under /Quarantined.

Heuristic Analysis

Include heuristic analysis to find new viruses. When you use heuristic analysis the scanning engine employs heuristic technology to detect potentially unknown viruses in executable files (programs). Without this option, the engine can only find viruses that are already known and identified in the current virus definition files. Valid values are On, Off. The default is On.

Macro

Specifies if you want to treat embedded macros that have code resembling a virus as if they were viruses. This parameter is similar to Heuristic analysis but scans for new viruses in compound document formats; for example, Microsoft OLE formats such as Word documents. Valid values are On, Off. The default is On.

Programs

Specifies if you want scanning activities to include detection of some widely available applications, such as password crackers or remote access utilities that can be used maliciously or pose a security threat. Valid values are On, Off. The default is Off.

Archive Files

Specifies if you want scanning activities to include archive files. Archive files contain embedded files and usually end with one of the following extensions: .ZIP, .TAR, .CAB, .LZH, .JAR and .UUE. This option will also permit scanning of MSCompress files. Valid values are On, Off. The default is Off.

File Types; Most Susceptible to Infection • All Files • Examine Files for Known Macro Viruses

Specifies the type of files to include in scanning activities. The default is Most Susceptible to Infection. All Files will scan all files, the slowest option but which provides the best protection. Examine Files for Known Macro Viruses will expand scanning activities to include an examination of files to determine if they contain known macro viruses, faster than the All Files option.

Mime

Specifies if you want to scan inside MIME-encoded files, UU-encoded files, XX-encoded files and BinHex files. The default is Off. Note that to enable this option, the File Types option must be set to all.

Linux/Unix Only

Include Paths

A colon-delimited list of path names to be included for on-access scanning. A file that exists within any of the path names specified will be subject to scanning unless the file path name is specified as an Exclude Path.

Filesystem Mount Points

This option is for Linux only. A colon-delimited list of mount points for filesystems that are to be monitored for on-access scanning. It provides the means to explicitly set which filesystems will be monitored by fanotify(7). The default is an empty list. Note that filesystems will only be monitored if their type does not appear in the internal list of known unsupported filesystem types and is not part of fsexcl configuration. Note also that the decision to scan a file will still be subject to include and exclude criteria.

Exclude Filesystem Type Names

A colon-delimited list of filesystem type names that are to be excluded from monitoring. The default is an empty list. Note that the decision to scan a file will still be subject to include and exclude criteria.

On Linux, this is used to limit which filesystems will be monitored by fanotify(7), and complements the internal list of filesystem types that we know cannot be monitored. The names are those from the third column of /proc/mounts, see proc(5).

On AIX, the names are those from the first column of /etc/vfs, see vfs(4). The name remote can be used to select all names in /etc/vfs that are marked as remote.

Resources

Thread Allocation

The number of threads to be allocated for use by the on-access scanner. This can be an integer value between 2 and 32. The default is 6. The service must be restarted to change this value.

Max Wait Before Timeout

The maximum amount of time in seconds the scanner should spend scanning a single file or archive before timing out. After the specified number of seconds, the file is allowed to be opened and the file's scan status remains unchanged. This can be an integer value between 0 and 3600. A value of 0 disables the timeout. The default is 300 seconds.

Delay Scan Process

The amount of time in microseconds the scanner should pause with each progress beat from a scanning operation. This can be used as a simple CPU limiting technique for certain use cases. It should not be enabled when operating system files are included in the monitoring paths. This can be an integer value between 0 and 999999. The default value of 0 disables the feature.

Runtime Scheduling Priority

Sets the runtime scheduling priority of the service. This can be a value between -20 (highest priority) and 19 (lowest priority). The default is 0 (no change in priority). The service must be restarted to change this value.

Filesystem Caching

Cache

Set to On to enable, or Off to disable the cache. The default is On.

Max Age

A time to live for an unchanged object in the cache. If the object record has not been re-scanned in that time, it will be removed from the cache. This is expressed in minutes, and can be an integer value between 0 and 999999. The default is 0, which disables the feature. Toggle to On to display a text field where you can specify the number of minutes.

Max Idle

A time to live for a cache object that has not been re-scanned (changed) or queried (hit). This is expressed in minutes, and can be an integer value between 0 and 999999. The default is 0, which disables the feature. Toggle to On to display a text field where you can specify the number of minutes.

Max Size

A maximum size for a single filesystem cache. There is one cache per filesystem. The cache expiry operation will reduce the cache to this maximum size, expelling oldest unchanged objects first. This is expressed as the number of files in the cache, and can be an integer value between 0 and 999999999. The default is 0, which disables the feature. Toggle to On to display a text field where you can specify the number of files.

Notifications

Add Notification

Choose this option to open the New/Edit Notification pane, where you can define a new Notification.

(Show Actions)

Select this for a Notification to show a menu with the following options:

- **Edit Notification.** Opens the New/Edit Notification pane, where you can edit the Notification.
- **Remove Notification.** Deletes the Notification.
- **Close.** Choose **Close** to dismiss the Show Actions menu.

IBM i Only

Timeout

The period of time (in seconds) after which a connection to the IBM i is considered to have failed. The default value is 30.

Log Level

Specifies the amount of information logged to the avsvr.log file. The following options are available:

- 0 - Disabled
- 1 - Infections, cleaning and quarantine (default value)
- 2 - Everything from level 1 and file names
- 3 - Everything from level 2 and job names

New/Edit/Duplicate On-Demand Configuration pane

The New/Edit/Duplicate On-Demand Configuration pane allows you to set configuration options, including notification settings, for on-demand scanning.

How to Get There

- To create a new Configuration, on the Configurations page, choose **Add > On-Demand Configuration**.
- To create a new Configuration starting with the settings of an existing Configuration, on the Configurations page, for an existing On-Demand Configuration, click  **> Properties**.
- To edit an existing Configuration, on the Configurations page, for an existing On-Demand Configuration, click **> Properties**.

Options

Actions

Click **Actions** to open a submenu with the following connection management options:

- **Duplicate.** Choose this option to duplicate the configuration.
- **Delete.** Opens the Delete Configuration dialog box, where you are prompted to specify a new Configuration for Endpoints assigned to the Configuration you are deleting.
- **Close.** Choose this option to close the submenu.

Name • Description

The name and description of the configuration.

Set as Primary

Endpoints set to the Primary Configuration (see Endpoint Properties pane) inherit the settings of the Configuration that is set as Primary. Toggle this switch to **On** to indicate that you would like to set Endpoints currently assigned to the Primary Configuration to the Configuration you are editing. When you click **Save**, the number of Endpoints that will change is indicated and you are prompted to confirm. Toggle this switch to **Off** to indicate that you

would like to set Endpoints assigned to the Primary Configuration to the Default Configuration. The Configuration that is currently set to Primary is indicated in the Configurations page.

Common

Include

A required colon-delimited list of path names to be included for on-demand scanning. A file that exists within any of the path names specified will be subject to scanning unless the file path name is specified as an Exclude Path. IBM i Endpoints support single paths only.

Exclude

A colon-delimited list of path names to be excluded from on-demand scanning. The exclude paths take precedence over include paths. A file that exists within any of these path names will not be subject to scanning.

Recursive

If set to **On**, the scan descends the specified directories recursively. If set to **Off**, the current directory is scanned without descending subdirectories.

Heuristic Analysis

Include heuristic analysis to find new viruses. If set to **On**, Powertech Antivirus employs heuristic technology to detect potentially unknown viruses in executable files (programs). If set to **Off**, the engine can only find viruses that are already known and identified in the current virus definition files.

Macro

If set to **On**, Powertech Antivirus treats embedded macros that have code resembling a virus as if they are viruses. This parameter is similar to Heuristic analysis but scans for new viruses in compound document formats; for example, Microsoft OLE formats such as Word documents. If set to **Off**, embedded macros that have code resembling a virus are not treated as viruses.

Programs

If set to **On**, Powertech Antivirus detects some widely available applications, such as password crackers or remote access utilities that can be used maliciously or pose a security threat. If set to **Off**, these applications are not detected.

Archive Files

If set to **On**, Powertech Antivirus includes archive files. Archive files contain embedded files and usually end with one of the following extensions: .ZIP, .TAR, .CAB, .LZH, .JAR and .UUE. This option will also permit scanning of MSCompress files. If set to **Off**, archive file types are not scanned.

Clean

If set to **On**, Powertech Antivirus cleans infected files by repairing the infection. Most infections cannot be cleaned.

> WARNING: If the file cannot be cleaned, it will be deleted (unless Quarantine is set to **On**).

Quarantine

If set to **On**, Powertech Antivirus quarantines the infected files by moving them to the /Quarantined directory. When Quarantine and Clean are both On, Powertech Antivirus attempts to clean the file first, and if unsuccessful, moves the file to the quarantine directory. If they are both off, no actions are taken on infected files.

Timeout

Specifies the maximum number of seconds the scan will execute in total. After the number of seconds has elapsed, the command will end without scanning any remaining files. The return code will indicate a timeout has occurred. For IBM i Endpoints, the seconds you enter are converted to minutes.

Linux/Unix Only

Mime

If set to **On**, Powertech Antivirus scans inside MIME-encoded files, UU-encoded files, XX-encoded files, and BinHex files. If set to **Off**, Powertech Antivirus does not scan inside these types of files. This parameter reduces scanning performance.

Log Level

Specifies the number of directory levels that will be printed in the output listing. The default is 99.

Ignore Links

If set to **On**, the scan ignores all symbolic links. If set to **Off**, symbolic links are scanned.

Scan Only EXE Files

If set to **On**, Powertech Antivirus scans executable files only. The scan engine uses the file extension alone to determine whether the file is an executable. If set to **Off**, Powertech Antivirus scans all files regardless of the file extension.

Command

Runs the specified command string when infections are found, passing the file name as a parameter. This allows a user-written script to perform actions such as alerting an administrator. This file will be a live infected file, and in no way should the script attempt to read it. The intention is to allow you to process the file name. You may want to implement a procedure to notify an administrator, for example. Scripts must have execute permissions in order to be run.

Notify

Notify those notifiers in the comma separated list, which are defined in the [notify] section of config.ini. This list will override the list defined by the config.ini avscan:notify parameter. See Notification Support in avconfig command.

Max Wait

Specifies the maximum number of seconds to spend scanning any one file. After the number of seconds has elapsed the product assumes the file is OK and proceeds with the next file. The default is 300. Use this option cautiously.

Delay Scan Progress

The amount of time in microseconds the scanner should pause with each progress beat from a scanning operation. This can be used as a simple CPU limiting technique. It can be an integer value between 0 and 999999. The default value of 0 disables the feature.

Quiet

Prints minimal information to the output stream, useful for parsing the output file.

Scan Threads

The number of threads used of scan files concurrently. Between 1 and 16 threads can be specified for this parameter. The default setting is 1.

IBM i Only

File Types

Specifies the types of files to scan. The options are:

- Most Susceptible to Infection
- All files
- Examine Files for Known Macro Viruses

Force rescan of scanned files

Specifies if the objects scan settings should be overridden. The options are:

- Do not force rescan
- Rescan all files

- If file's "Object scanning" attribute is *NO
- If file's "Object scanning" attribute is *CHGONLY

Restart

If set to **On**, the system will restart the scan from a previous timeout. If set to **Off**, the system will not restart the scan.

Run Priority

The CPU priority for the AVSVR job scan thread. Values between 11 (the highest priority) and 99 (the lowest priority) are permitted. The default setting is 50.

Log Level

Determines the level of logging for the on-demand scanning configuration. The possible options are:

- Summary
- Detailed
- Full

Preferences

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Settings > Preferences**.

Options

Dark Mode

Use the toggle switch to change the main display between Light and Dark Mode. The default setting is Off. The left-hand menu can be switched between Light and Dark Mode using the preferences within Fortra Application Hub.

Auto-Refresh; on • off

When on, Powertech Antivirus refreshes the Home page with the latest status for connections and Endpoints. Enter a number into the adjacent text field to specify the refresh interval, in minutes. When off, the Home page does not automatically refresh.

IBM i Anti-Ransomware Configuration; on • off

When on, Powertech Antivirus allows the use of IBM i Anti-Ransomware Configurations.

Quarantined Files page

This page displays a list of quarantined files on the server, including the original file paths. Quarantined files are files that have been flagged as infected by Powertech Antivirus and moved into Powertech Antivirus' quarantined files directory.

How to Get There

On the Endpoints page, choose ⋮ for an Endpoint and select **Manage Quarantine**.

Options

Delete • Restore

Check one or more quarantined files using the check boxes to the left of the file list. Or, click ⋮ to the right of each quarantined file. These buttons appear at the top of the page. Choose **Delete** to remove the selected files. You are asked to confirm the file delete. If the file is not a virus, or has been cleaned, you can choose **Restore** to replace the file to its original location.

> NOTE: If you restore a file that has been detected by Powertech Antivirus without adjusting either the file or detection procedure (by, for example, cleaning the file or updating virus definitions), it will continue to be flagged and quarantined by Powertech Antivirus' scans.

Reports

This page allows you to add and manage Reports. The list of Reports includes the Report Name, Description, Scheduled info (if configured), Type, quantity of recipients, and date the Report was last run.

> **NOTE:** For details on how to create a report, see Reporting.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Reports**.

Options

Filter

By default, defined reports of all types are shown on the Reports page.

Click ▼ in the **TYPE: ALL** box to open a drop-down menu of available report type options. Select report types on this menu to include them on the Reports page display. Multiple selections are permitted. Any report type not selected will not be visible on this page, until the default setting of ALL is restored. The following report types are available for selection:

- On-Demand Scan Summary
- On-Demand Scan Daily Summary
- On-Demand Scan History
- On-Access Scan Summary
- On-Access Scan Daily Summary
- Endpoint Status
- Threats

Add; Add On-Access Report • Add On-Demand Report • Add Endpoint Status Report • Add Threats Report

Choose Add On-Access Report to open the New On-Access Report pane, which allows you to define a new On-Access Report. Choose Add On-Demand Report to open the New On-Demand Report pane, which allows you to define a new On-Demand Report. Choose Add Endpoint Status Report to open the New Endpoint Status Report pane, which allows you to

define a new Endpoint Status Report. Choose Add Threat Report to open the New Threats Report pane, which allows you to define a new Threat Report.

(Show Actions)

IMPORTANT: If you upgraded from Powertech Antivirus version 5.4.1 (Insite) or 6.0 (Powertech Antivirus Server (Fortra Application Hub): Starting in version 6.1, the **Run** action and button are renamed to **E-mail**. There is no change to functionality.

Select **Show Actions** to see a menu with the following options:

- **Properties.** Choose Properties to view the New/Edit On-Access Report pane , New/Edit On-Demand Report pane, New/Edit Endpoint Status Report pane or New/Edit Threat Report (depending on the type of report), where you can edit the report configuration.
- **E-mail.** Choose this option to run the report, generate a PDF report of the output, and e-mail the PDF to recipients specified in the report definition. The E-mail option is presented only if e-mail recipients have been specified in the report definition.
- **Download**. Choose Download to generate and immediately download PDF reports from the user interface.
- **View.** Choose View to run the report and view the report output. This is the same data that appears in the respective PDF report delivered to the specified recipients (if any).
- **Delete.** Choose this option to delete the report from the database.

Selected Reports

Select one or more reports using the check box to the left of each report in the list. When you do so, the following options appear in a yellow Show Actions menu bar at the top of the page. This menu bar allows for changes to multiple reports simultaneously.

- **Cancel.** Choose **Cancel** to dismiss the Show Actions menu.
- **Delete.** Choose this option to delete the selected reports from the database.
- **E-mail.** Choose this option to e-mail the PDF report to recipients specified in the report definition.

Roles

User access to Fortra Application Hub and its products can be secured through the use of Roles, which are collections of authorities that define a user's permissions for managed systems and products.

> **NOTE:** For general help and guidance on the use of Roles within Fortra Application Hub, see Roles.

This section describes the use of Roles specifically within Powertech Antivirus.

Creating a new Role for Powertech Antivirus

1. Open **Fortra Application Hub**.
2. From the left-hand navigation menu, click **User Security**.
3. From the User Security menu bar click **Roles**. The list of currently defined Roles is displayed.
4. Click **Add**.
5. Enter a **Name** and **Description** for the new Role, select the **Security Group** and the **User Level**. These options are covered in the Fortra Application Hub online help.
6. In the '**Authorized To**' section, and after you have specified the access levels for Dashboards, Application Manager and Fortra Application Hub (also covered in the Fortra Application Hub online help, click to enable and then expand the Powertech Antivirus option.
7. If you have multiple instances of Powertech Antivirus running on Fortra Application Hub, select the one for which you want to create the new role and expand the selection. The following areas of Powertech Antivirus can have role levels assigned:
    - **Home Page**
    - **Endpoints**
    - **Reports**
    - **Scheduled Scans**
    - **Anti-Ransomware**
    - **Settings**
    - **Activity Status**
    - **Diagnostics and Logging**

> **NOTE:** For all the above areas (except Home and Endpoints) the Role can have the following assignations:
>
> - **View** - The user can only see (and not amend) items on the Powertech Antivirus User Interface.
> - **Full Access** - The user has all the view permissions but can additionally edit any content within the chosen area.

For the Home page, role access is either enabled or disabled.

For Endpoints the role assignations can be one of:

- **View** - The user can only see (and not amend) Endpoint items on the Powertech Antivirus User Interface
- **Full Access** - The user has all the view permissions but can additionally edit any content within Endpoints
- **Full Access (no Scan Notification Commands)** - This role provides access to all elements of the endpoints and scan configurations User Interface with the exception of the notifications area. Notifications run as root on an endpoint and access to this User Interface should be restricted to highly trusted administrators.

8. Once all the assignations for the role have been set, click **Save**. The Role will now be available for selection in the

Editing a Role

1. From the main Roles display window, click the **Actions** ⋮ button next to the Role that you want to edit.
2. Click **Edit**.

The available options are the same as when Creating a new Role.

Run Scan page

These settings allow you to confirm your Configuration choices prior to running an On-Demand scan.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Endpoints**. On the Endpoints page, for an Endpoint, choose  **> Run Scan**. Or, select one or more Endpoints and select **Run Scan** from the options at the top of the page.

Or, in the Endpoint Properties pane, click **Actions > Run Scan**.

Options

Configuration

From this drop-down menu, choose the On-Demand Configuration you would like to use for the scan. When you choose a Configuration, its settings appear in the options below.

More details about the available Configurations can be found on the Configurations page.

[Configuration Options]

The options in this section are identical to the options in the New/Edit/Duplicate On-Demand Configuration pane.

Run

Runs the scan on the selected Endpoints using the Configuration options you have selected.

Save and Run

Opens the Save Configuration page, where you can save your Configuration settings into a new Configuration record or overwrite the existing Configuration with the new settings.

Cancel

Choose this option to dismiss the Run Scan page without running a scan.

Save Configuration

This page allows you to save a new Configuration record, or overwrite an existing one, using the settings from the Run Scan page.

How to Get There

On the Run Scan page, click **Save and Run**.

Options

Name • Description

This is the name and description of the Configuration to be saved. Upon arrival, these settings reflect what was previously selected in the Run Scan page.

Save and Continue

Choose this option to save the Configuration. If you have not changed the name, you will be prompted to overwrite the existing Configuration. If you have changed the name, a new Configuration will be created using the new name and the existing Configuration will not be changed.

Cancel

Choose this option to dismiss the page without saving a Configuration.

Scheduled Scans page

This page lists existing Scheduled Scans. It allows you to create, find/search, and run Scheduled On-Demand Scans. For information on how to schedule scans, see Scheduling Updates and Scans.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Scheduled Scans**.

Options

(Cancel • Delete • Run)

When you check one or more Scheduled Scans, these options appear at the top of the page.

Cancel

Removes selection from checked Scheduled Scans.

Delete

Deletes selected Scheduled Scans.

Run

Runs selected Scheduled Scans. The status of Scheduled Scans can be monitored on the Activity Status page.

Add

Opens the New Scheduled Scan pane, where you can define a new Scheduled Scan.

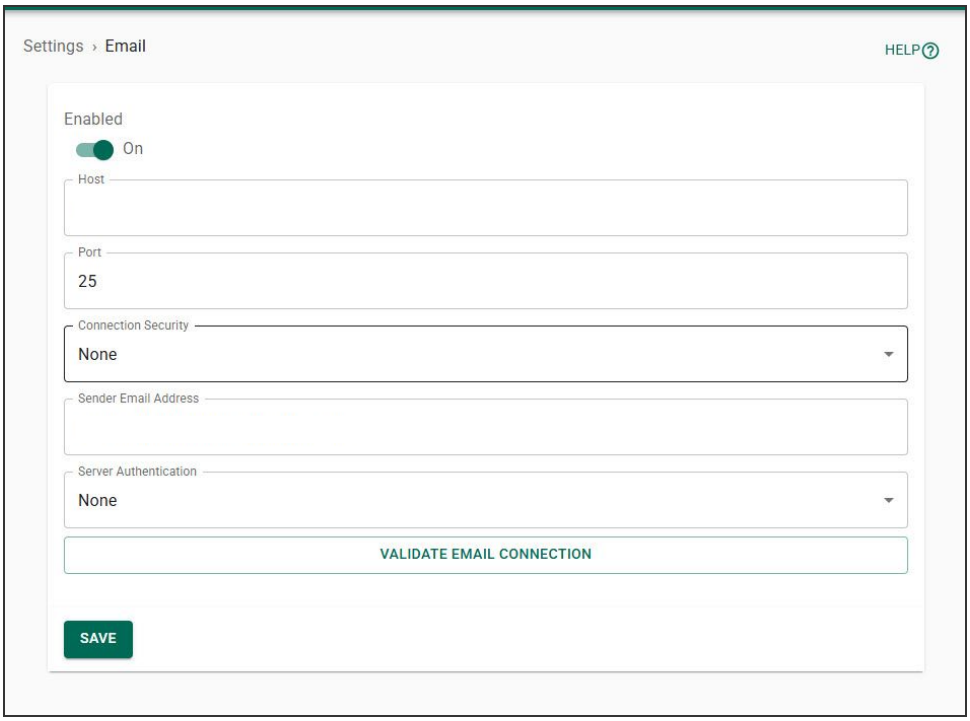
(Show Actions)

Opens a submenu for the Scheduled Scan with the following scheduling management options:

- **Properties.** Opens the Edit Scheduled Scan pane, which allows you to edit the Scheduled Scan.
- **Run.** Runs selected Scheduled Scan. The status of Scheduled Scans can be monitored on the Activity Status page.
- **Delete.** Deletes the Scheduled Scan definition.

Settings > Email

When a recipient's email address has been added to a report's definition (On-Access Report, On-Demand Report, Endpoint Status Report and/or Threat Report), they can be sent a PDF of the report via email. Use these settings to configure the required email settings.



How to Get There

In the Powertech Antivirus Navigation Pane, choose **Email Settings**.

Options

Enabled; Off • On

Toggle this switch to **Off** to disable email messages, or **On** to enable them.

Host

This is the host name of your email server.

Port

This is the port used by your email server.

Connection Security

Use the drop-down menu to select the option controlling connection security. The following choices are available:

- None (this is the default)
- START/TLS
- SSL/TLS

Sender Email Address

This is the email address that will appear in the "From" field of the recipient's message.

Server Authentication

Use the drop-down menu to select the method of server authentication to be used.

- None (this is the default)
- Username and password. The following fields become available:
  - Username
  - Password
- Office 365. The following fields become available:
  - Client ID
  - Client Secret
  - Username
  - Tenant ID

Validate Email Connection

Use this button to test the email server connection. If the server requires validation, the specified User Name and Password or Office 365 Credentials are tested.

Settings > Repository

Trellix virus definitions (DAT file) updates can be applied to Powertech Antivirus Endpoints from an internal DAT file repository using an HTTP or FTP file server. The file server is secured using TLS and runs in FTPS mode ensuring that data transfer is always secure.

This page allows you to configure the Virus Definition Repository settings.

How to Get There

In the Powertech Antivirus Navigation Pane, choose **Settings**.

Options

Virus Definition (DAT) Repository Common Settings

Off • On

The Powertech Antivirus Service will download DAT files for internal repository that can be shared. **Off** disables the Powertech Antivirus Service Repository. **On** enables it.

Use HTTPS; On • Off

When Powertech Antivirus's HTTP Proxy Server setting is on, you can toggle this setting to **On** to download virus definition DAT files using the secure HTTPS server offered by Trellix (https://update.nai.com/products/commonupdater). HTTPS uses Transport Layer Security (TLS) (formerly known as Secure Sockets Layer (SSL)) to encrypt the transaction.

When this setting is **Off**, and Use HTTP Proxy Server is on, Powertech Antivirus uses Trellix's HTTP server for DAT file downloads (http://update.nai.com/products/commonupdater).

DAT Update Frequency

This setting controls the frequency the Powertech Antivirus Service checks for DAT Updates, from 5-1440 minutes. Default is 60.

HTTP Proxy Server; On • Off

This option allows you to configure the DAT Repository Trellix download process to use a proxy server rather than directly accessing the Trellix Server. Set to **On** to use a proxy server and add the proxy server address (for example, https://dns_name:port; https://ip_address:port; http://dns_name:port; http://ip_address:port). Set to **Off** to configure Powertech Antivirus to access the Trellix server directly.

If you have configured the proxy server address and change the setting to Off, the address will be restored when turned On.

Automatically update Endpoints when DAT Updates are available; On • Off

Set this to **On** to check for DAT file updates automatically at the frequency indicated above. Set to **Off** to disable automatic DAT file updates.

Virus Definition (DAT) Repository HTTP Service Settings

Off • On

If set to **On**, the Powertech Antivirus Service will run an HTTP file server for the DAT File Repository. **Off** disables the HTTP file server.

Max Concurrent Endpoint Updates

This is the maximum concurrent DAT updates allowed within a request (10-200). Default is 32.

Port

The port used for the DAT file server.

Virus Definition (DAT) Repository FTP Service Settings

Off • On

If set to **On**, the Powertech Antivirus Service will run an FTP file server for the DAT File Repository. **Off** disables the FTP file server.

By default, Linux prevents programs from accessing ports lower than 1024. To allow our FTP server to use port 21, run the following commands:

```
setcap CAP_NET_BIND_SERVICE=+eip /opt/ptavwebsvc/PTAVService/ptavsvc

modprobe ip_conntrack_ftp
```

IMPORTANT: After running the `setcap` and `modprobe` commands you must restart the Powertech Antivirus Service.

TIP: We recommend that you register 'ip_conntrack_ftp' so that it is automatically loaded after a system boot. To do this, create a file, such as:

```
/etc/modules-load.d/ip_conntrack_ftp.conf
```

and put ip_conntrack.ftp within this file.

NOTE: It may be necessary to repeat the `setcap` command and restart the Powertech Antivirus Service after an upgrade of Powertech Antivirus, as the extended attributes for ptavsvc may get overwritten.

Appendix

The topics in this section include additional configuration and validation options for Powertech Antivirus.

Additional Information for Amazon Linux

Powertech Antivirus support and maintenance costs are calculated as a percentage of the total per instance cost of the deployment.

Powertech Antivirus is licensed per running copy of the Amazon Linux2 OS. Size or deployment model of the instance is not a factor.

> **NOTE:** In the case of an instance failure, a new EC2 instance must be created, the Powertech Antivirus RPM file must be re-installed, and the license applied as listed in the *Powertech Antivirus Installation Guide*.

The links below will point to you frequently asked questions and additional information on deploying Powertech Antivirus in your AWS environment:

AWS Identity and Access Management

AWS deployment options

AWS disaster recovery information

AWS event handling

AWS region high availability

Auto scaling groups information

Availability Zone continuity information

Compare AWS support plan options

Creating security groups for your VPC

EC2 Instance type information (under "Instance types")

How to create IAM Aws roles

How to manage service limits on AWS

Information on AWS Certificate Manager

Information on AWS Limit Manager

Information on AWS encryption options

Mitigating AZ failures

Multi AZ deployment information

Planning for disaster recovery on AWS

Tracking status of your instances

Working with AWS credentials

Configuring a Local Repository for Virus Definitions

A local repository allows you to scan a system without connecting to an outside port. If you suspect a system has been compromised, use a local repository to help ensure an infection remains contained.

To configure a local repository for virus definitions, follow these steps:

1. Download your repository.

   TIP:
   To manually download oem.ini and the virus definition archive package to your local server:

   a. wget -O oem.ini http://update.nai.com/products/commonupdater/oem.ini

   b. wget -N http://update.nai.com/products/commonupdater/*.zip

      Trellix stores the latest 2 zip files in this folder. Ensure you have a process to manage this folder (i.e. purge old zip files) if this will be run as a cron job or scheduled event, as this folder could fill up quickly.

2. Transfer oem.ini and the latest avvdat-*xxxx*.zip file to an empty directory on the remote server where Powertech Antivirus is installed (e.g. /home/user/dat).
3. Run `avupdate` with the path option.

   EXAMPLE:
   ```
   /opt/sgav/avupdate --path /home/user/dat
   ```

DAT File Validation

DAT updates are validated by Powertech Antivirus before Endpoints can use them, whether downloaded from Trellix or copied from the air-gapped "datimport" folder.

The validation method is triggered automatically once the download process has completed. A message is logged to indicate the validation routine is running.

If any errors are discovered:

- The folder in the datrepo that contains the invalid DAT files will be deleted.
- An error will be written into the datinfo file, which will then appear on the home page.
- The datinfo file will not be updated to reflect the download (i.e. the current, valid version will remain the "current" version in the file and will be used by Endpoints).
- Information on the files that must be validated can be found in the "oem.ini" file as follows:
    - The "[AVV-ZIP]" section contains the name and md5 hash of the DAT update zip file (i.e. "avvdat-nnnn.zip").
    - The "[AVV-Incremental]" section contains the name and md5 hash of the file that contains information required for incremental updates (the file is generally called "gdeltaavv.ini" but we check for the filename here in case it changes).
    - The "[GEM-MD5]" section contains the name and md5 hash for every gem file that needs to be downloaded.
- The validation method reports an error under the following conditions:
    - The "oem.ini" file is missing.
    - The "avvdat.ini" file is missing.
    - The "avvdat-nnnn.zip" file is missing.
    - The md5 hash of the "avvdat-nnnn.zip" file is incorrect.
    - The incremental file ("gdeltaavv.ini" or whatever filename is specified in oem.ini) is missing.
    - The md5 hash of the incremental file is incorrect.
    - One or more gem files is missing.
    - The md5 hash of one or more gem files is incorrect.
- The validation method returns an error for the first error that it finds. It does not process further if an error has been found.
- If any unexpected files are found in the download folder, they are ignored.

More details:

- The validation routine is called both following an update from Trellix, or from the air-gapped "datimport" folder. A message appears in the log to indicate that the validation routine is running.
- If any errors are discovered when validating the download:
  - The downloaded folder is deleted.
  - An error is written into the datinfo file which then appears on the home page.
  - The datinfo file remains otherwise unchanged (i.e. the current and previous versions are unchanged; the only update is an error in the error field).
- The validation method reports an error under the following conditions:
  - The "oem.ini" file is missing.
  - The "avvdat.ini" file is missing.
  - The "avvdat-nnnn.zip" file is missing.
  - The md5 hash of the "avvdat-nnnn.zip" file is incorrect.
  - The incremental file ("gdeltaavv.ini" or whatever filename is specified in oem.ini) is missing.
  - The md5 hash of the incremental file is incorrect.
  - One or more gem file is missing.
  - The md5 hash of one or more gem files is incorrect.
- If any unexpected files are found in the download folder, they are ignored.

Syslog Configuration

Use the following information to configure Powertech Antivirus syslog logging.

Powertech Antivirus uses Zlog to send log messages to local logs and to mirror them to syslog. For information about the Zlog configuration file, see https://hardysimpson.github.io/zlog/UsersGuide-EN.html.

Log files are created in the/opt/sgav/log folder. If they are not, verify the following:

- The zlog.conf and zlog-avsvc.conf files exist
- The zlog.conf and zlog-avsvc.conf files can be read by the user
- The zlog.conf fileand zlog-avsvc.conf files do not contain typos that could cause the file to not be read correctly

> **NOTE:** The destination for the syslog messages depends on the syslog configuration of the host. By default, it may be /var/log/messages or /var/log/syslog.

Logging levels

The following severity levels are used by Powertech Antivirus:

FATAL	Fatal conditions that will cause the product to stop running.
ERROR	Serious messages that cause the product to fail or stop working.
WARN	Important messages that should be looked at (e.g. virus infections, quarantine).
NOTICE	General startup and shutdown activity, completion messages.
INFO	Detailed messages, files not scanned, etc.
DEBUG	Debug trace.

You can set the syslog log level names to which these messages are sent in the zlog configuration files. By default:

- FATAL and ERROR messages are sent to syslog at level LOG_LOCAL3.
- WARN messages are sent to LOG_LOCAL4.
- NOTICE messages are sent to LOG_LOCAL5.
- INFO and DEBUG messages are not mirrored to syslog.

Zlog configuration for the avupdate and avscan tools are defined by the avupdate and avscan rules in zlog.conf. Changes will take effect the next time these tools are run.

The avsvc server uses the avsvc rules in zlog-avsvc .conf. Changes will take effect the next time the server is started or configuration is reloaded (“avsvcctl reload”).

Possible Syslog Messages

The following are the bodies of the Powertech Antivirus messages for levels FATAL, ERROR, WARN, and NOTICE, as they would appear with the default syslog formatting:

```
PTAV FATAL another instance of %s is already running
PTAV FATAL client initialization failed
PTAV FATAL configuration failed, exiting
PTAV FATAL driver write failure, errno %d %s
PTAV FATAL error monitoring mounts, errno %d
PTAV FATAL failed to create client threadpool of size %ld, errno %d
%s
PTAV FATAL failed to create notification threadpool, errno %d %s
PTAV FATAL failed to create onaccess threadpool of size %ld, errno
%d %s
PTAV FATAL failed to ignore SIGPIPE, errno %d %s
PTAV FATAL failed to initialize monitoring
PTAV FATAL fileops: %s
PTAV FATAL no memory for event initialisation
PTAV FATAL out of memory
PTAV FATAL out of memory (array)
PTAV FATAL reporting initialization failed
PTAV FATAL unrecoverable error from device driver
PTAV ERROR avscan notifier '%s' is not configured
PTAV ERROR avsvc 'mime' configuration option has no effect unless
'files' is set to 'all'
PTAV ERROR avsvc notifier '%s' is not configured
PTAV ERROR AVUpdate failed, error %d
PTAV ERROR bad receive state %d nr %d ne %d
PTAV ERROR cannot create a configuration dictionary, error %d %s
PTAV ERROR cannot open log directory [%s], error %d %s
PTAV ERROR cannot parse configuration file '%s'
PTAV ERROR caught signal %d, crash log written to %s
PTAV ERROR Configuration failed, exiting
PTAV ERROR copy %s to %s failed, errno %d %s
PTAV ERROR could not create local listener, errno %d %s
PTAV ERROR could not get device driver version, errno %d %s
PTAV ERROR could not issue driver shutdown, errno %d %s
PTAV ERROR could not open instance lock file '%s', errno %d %s
PTAV ERROR could not open %s, errno %d %s
```

```
PTAV ERROR could not query %s, errno %d %s
PTAV ERROR could not send fanotify response, errno %d
PTAV ERROR could not send fanotify response for file '%s', errno %d
PTAV ERROR current patch index %s is invalid
PTAV ERROR DAT update failed!
PTAV ERROR DAT update failed, error %ld %s
PTAV ERROR decompression of DATs in %s failed
PTAV ERROR delete of infected file failed for %s
PTAV ERROR device driver query failed, errno %d %s
PTAV ERROR device driver version (%s) does not match service (%s)
PTAV ERROR %d exclude paths were rejected in avsvc configuration
PTAV ERROR %d include paths were rejected in avsvc configuration
PTAV ERROR discarding over-length client record (%u)
PTAV ERROR %d mount paths were rejected in avsvc configuration
PTAV ERROR driver close failed, rc %d errno %d %s
PTAV ERROR Engine failure: %s
PTAV ERROR EOVERFLOW, file too large
PTAV ERROR ERROR! cannot transfer files, neither curl or wget is
available
PTAV ERROR error creating thread
PTAV ERROR ERROR! curl not found
PTAV ERROR Error getting latest version directory from %s file.
PTAV ERROR error in client protocol, unexpected header
%02x%02x%02x%02x
PTAV ERROR error reading from device driver, errno %d %s
PTAV ERROR ERROR! See FTP log %s for details.
PTAV ERROR ERROR! See %s/%s for details.
PTAV ERROR errors were encountered, aborting configuration change
PTAV ERROR ERROR! wget not found
PTAV ERROR failed to add directory watch for '%s', errno %d %s
PTAV ERROR failed to add scan work to thread pool
PTAV ERROR failed to add scan work to thread pool, errno %d
PTAV ERROR failed to add %s to file queue, errno %d
PTAV ERROR failed to add %s to scan pool, errno %d
PTAV ERROR failed to allocate vfstypes storage
PTAV ERROR failed to allow access to file %s, errno %d %s
PTAV ERROR failed to build path for %s event on '%s'
PTAV ERROR failed to configure device driver, errno %d %s
PTAV ERROR failed to create device driver special file %s, errno %d
%s
PTAV ERROR failed to create directory %s, errno %d %s
PTAV ERROR failed to create event, errno %d %s
PTAV ERROR failed to create inotify thread, errno %d %s
PTAV ERROR failed to duplicate client fd, error %d %s
PTAV ERROR failed to fdopen file %s, errno %d %s
PTAV ERROR failed to find zip file name in %s
PTAV ERROR failed to increase max inotify watches, errno %d %s
PTAV ERROR failed to initialize device driver, errno %d %s
```

```
PTAV ERROR failed to initialize filesystem cache
PTAV ERROR failed to initialize inotify, errno %d %s
PTAV ERROR failed to initialize scan pool, erno %d %s
PTAV ERROR failed to initialize scan pool, errno %d %s
PTAV ERROR failed to initialize search pool, errno %d %s
PTAV ERROR failed to load device driver, errno %d %s
PTAV ERROR failed to locate patch with index %ld
PTAV ERROR failed to open debug file %s: %d %s
PTAV ERROR failed to open debug file %s, errno %d %s
PTAV ERROR failed to open directory %s, errno %d %s
PTAV ERROR failed to open file %s, errno %d %s
PTAV ERROR failed to open file %s for %s, errno %d %s
PTAV ERROR failed to open %s, errno %d %s
PTAV ERROR Failed to quarantine infected file '%s' - %s
PTAV ERROR failed to register tool, errno %d
PTAV ERROR failed to %s access for file %s from PID %lld, errno %d
(%s)
PTAV ERROR failed to send %s configuration to device driver, errno
%d %s
PTAV ERROR failed to set driver debug level, errno %d %s
PTAV ERROR failed to set inotify max watches, errno %d %s
PTAV ERROR failed to set inotify queue size, errno %d %s
PTAV ERROR failed to %s scan parameter list
PTAV ERROR failed to stop avexech service: %s
PTAV ERROR Failed to stop the avsvc service. You must stop it
manually before re-attempting the update.
PTAV ERROR failed to terminate device driver, errno %d %s
PTAV ERROR failed to truncate file %s, errno %d %s
PTAV ERROR failed to unload device driver, errno %d %s
PTAV ERROR fanotify_init failed %d %s
PTAV ERROR fanotify read failure, errno %d %s
PTAV ERROR fanotify write failure, rc %d, errno %d %s
PTAV ERROR FD_CLOEXEC failed %d %s
PTAV ERROR fileops: %s
PTAV ERROR ignored empty '%s' value in avsvc configuration
PTAV ERROR ignored invalid '%s' value '%s' in avsvc configuration
PTAV ERROR ignoring '%s' in notify section
PTAV ERROR inotify loop poll failed, rc=%d errno=%d
PTAV ERROR inotify queue overflow, events have been lost
PTAV ERROR invalid 'access' value '%s' in avsvc configuration
PTAV ERROR Invalid argument: %s
PTAV ERROR Invalid argument to parameter %s
PTAV ERROR invalid avsvc parameter '%s'
PTAV ERROR invalid 'cleanfail' value '%s' in avsvc configuration
PTAV ERROR invalid DATVersion %s
PTAV ERROR invalid 'delay' value '%s' in avsvc configuration
PTAV ERROR invalid 'files' value '%s' in avsvc configuration
PTAV ERROR invalid 'fscacheage' value '%s' in avsvc configuration
```

```
PTAV ERROR invalid 'fscacheidle' value '%s' in avsvc configuration
PTAV ERROR invalid 'fscachesize' value '%s' in avsvc configuration
PTAV ERROR invalid 'maxbacklog' value '%s' in avsvc configuration
PTAV ERROR invalid 'maxwait' value '%s' in avsvc configuration
PTAV ERROR invalid 'nice' value '%s' in avsvc configuration
PTAV ERROR invalid parameter '%s'
PTAV ERROR Invalid parameter %s
PTAV ERROR invalid 'thread' value '%s' in avsvc configuration
PTAV ERROR latest patch index %s is invalid
PTAV ERROR License error %d, %s, call Powertech
PTAV ERROR local listener failure, error %d %s
PTAV ERROR Malformed %s parameter
PTAV ERROR message data size %d out of range
PTAV ERROR missing DATVersion in %s
PTAV ERROR missing LastEncremental in Contents section of %s
PTAV ERROR mkdir %s failed, errno %d %s
PTAV ERROR monitoring stopped abnormally
PTAV ERROR move of %s %s to %s failed, errno %d %s
PTAV ERROR no callback registered for client connection
PTAV ERROR notifier '%s' has no command specified
PTAV ERROR Notifier '%s' is not configured
PTAV ERROR ODM initialize failure, error %d
PTAV ERROR out of memory
PTAV ERROR out of memory for buffer size %d
PTAV ERROR out of memory for mount list
PTAV ERROR out of memory for mount list (%d)
PTAV ERROR out of memory for mounts array
PTAV ERROR out of memory to handle file open event
PTAV ERROR parameter '%s' needs a value
PTAV ERROR path '%s' is invalid
PTAV ERROR permission denied, invalid message signature
PTAV ERROR Quarantine failed for %s
PTAV ERROR Quarantine failed for %s%s
PTAV ERROR Quarantine of infected file failed for %s%s
PTAV ERROR read of %s failed, errno %d %s
PTAV ERROR receive in unexpected state %d
PTAV ERROR reconfigure of monitoring parameters failed
PTAV ERROR refusing to read configuration file '%s' because %s
PTAV ERROR save directory does not exist
PTAV ERROR Scan engine failed, reason code %d.
PTAV ERROR Scan engine failed: %s.
PTAV ERROR Scan failed (error %d)
PTAV ERROR %s: command-line parse failure - %s
PTAV ERROR %s: could not start avexech service - %s
PTAV ERROR search on '%s' failed, errno %d %s
PTAV ERROR %s initialization failed, error %d
PTAV ERROR %s: initialization failure - %s
PTAV ERROR %s is not a directory
```

```
PTAV ERROR skipping '%s', configuration section not set
PTAV ERROR %s: License error %d, %s, call %s
PTAV ERROR special file %s does not have expected ownership and/or
permissions
PTAV ERROR stat of %s %s failed, errno %d %s
PTAV ERROR The parameter %s expects an argument
PTAV ERROR The parameter %s expects a value between %d and %d
PTAV ERROR the scanning engine encountered an unrecoverable error
PTAV ERROR timed out waiting for monitoring thread to start
PTAV ERROR unable to get list of filesystem mounts (/proc/mounts),
error %d %s
PTAV ERROR unable to get list of mounted filesystems, errno %d %s
PTAV ERROR unable to get number of mounted filesystems, errno %d %s
PTAV ERROR unable to get VFS details, errno %d %s
PTAV ERROR unable to locate %s tool at '%s', errno %d %s
PTAV ERROR unable to open cache dump file '%s', errno %d %s
PTAV ERROR unable to open %s, errno %d %s
PTAV ERROR unable to parse '%s' value '%s' in configuration file
PTAV ERROR unable to parse '%s' value '%s' in avsvc configuration
PTAV ERROR unable to resolve quarantine path '%s', errno %d %s
PTAV ERROR unable to set client socket options, errno %d %s
PTAV ERROR unhandled message %d from device driver
PTAV ERROR unknown configuration section %s
PTAV ERROR unknown device driver action %d
PTAV ERROR unknown notify option '%s' for '%s'
PTAV ERROR unlink %s failed, errno %d file path has changed to %s
PTAV ERROR unlink %s failed, errno %d realpath: %s
PTAV ERROR unlink %s failed, errno %d %s
PTAV ERROR unsupported parameter '%s', use avconfig
PTAV ERROR unzip of %s failed
PTAV ERROR write of %s failed, errno %d %s
PTAV NOTICE avscan completed: %lld files scanned, %lld infected,
%lld skipped, %lld error(s), %lld cleaned, %lld deleted, %lld
quarantined. %s.
PTAV NOTICE avscan starting
PTAV NOTICE built-in unsupported filesystem types: %s
PTAV NOTICE DAT files updated to %d
PTAV NOTICE DAT levels the same, nothing to do!
PTAV NOTICE fileops: %s
PTAV NOTICE filesystems (by mount point):
PTAV NOTICE monitored filesystems:
PTAV NOTICE monitoring disabled, no filesystems monitored
PTAV NOTICE Notifying avinsite service...
PTAV NOTICE not starting monitoring - access is set to none
PTAV NOTICE on-access scanning is disabled
PTAV NOTICE Restarting avsvc service...
PTAV NOTICE Scan queue size overridden to %d
PTAV NOTICE Scan queue size override too high, maximum is %d
```

```
PTAV NOTICE %s DAT update %s starting
PTAV NOTICE %s %d engine, DAT level %d (%s)
PTAV NOTICE %s %s is being reconfigured
PTAV NOTICE %s %s is shutting down
PTAV NOTICE %s starting
PTAV NOTICE Starting %s %s v%s at %.24s.
PTAV NOTICE Stopping avsvc service...
PTAV NOTICE supported filesystems:
PTAV NOTICE the 'mount' option is not supported on this platform
PTAV WARN cache clear attempt by non-root user %lld
PTAV WARN cache dump attempt by non-root user %lld
PTAV WARN cannot open directory %s, errno %d %s
PTAV WARN cannot remove %s, errno %d %s
PTAV WARN chown %lld:%lld of %s failed, errno %d %s
PTAV WARN command %s execution failed: %s
PTAV WARN command '%s' wait failed: %s
PTAV WARN configuration load failed
PTAV WARN could not increase max open file limit to %d, errno %d %s
PTAV WARN Deleted infected file '%s'
PTAV WARN Delete of infected file failed for file %s with error=%d
%s
PTAV WARN Disabling script command: error %d while scanning '%s'
PTAV WARN Disabling script command '%s': errno=%d
PTAV WARN Disabling script command: '%s' is infected
PTAV WARN Disabling script command '%s': not found or not executable
PTAV WARN Disabling script command: '%s' %s
PTAV WARN Disabling script command: timeout reached while scanning
'%s'
PTAV WARN driver debug control attempt by non-root user %lld
PTAV WARN failed to add fanotify mark for path '%s', errno %d %s
PTAV WARN Failed to close quarantine lock fd, errno %d %s
PTAV WARN failed to get driver event stats, errno %d %s
PTAV WARN failed to get driver queue stats, errno %d %s
PTAV WARN failed to read DAT version
PTAV WARN failed to report event statistics, error %d
PTAV WARN failed to report virus event for file '%s'
PTAV WARN failed to reset driver queue stats, errno %d %s
PTAV WARN failed to restart event statistics timer, error %d
PTAV WARN failed to set shutdown handler, errno %d %s
PTAV WARN failed to start avexech service: %s
PTAV WARN failed to start event report timer, error %d
PTAV WARN failed to watch directory %s
PTAV WARN fileops: %s
PTAV WARN Infected file '%s' cleaned %s
PTAV WARN Infected file '%s' deleted %s
PTAV WARN Infected file '%s' repaired (%s)
PTAV WARN %llu filesystem events missed in the last %d seconds
PTAV WARN log reconfigure failed
```

```
PTAV WARN log reconfigure with file '%s' failed because %s
PTAV WARN lost event on wd %d mask %x len %d name %s
PTAV WARN no filesystems are being monitored after reconfiguration
PTAV WARN no filesystems are being monitored after refresh
PTAV WARN notifier %s execution failed: %s
PTAV WARN notifier %s returned code %d (errno %d)
PTAV WARN notifier %s wait failed: %s
PTAV WARN pid deregister failed, errno %d %s
PTAV WARN pid register failed, errno %d %s
PTAV WARN product is not licensed: error %d (%s)
PTAV WARN Quarantined file %s
PTAV WARN Quarantined infected file '%s'
PTAV WARN Quarantine directory '%s' not found
PTAV WARN reconfiguration of monitored filesystems failed,
monitoring is in an undefined state
PTAV WARN refresh of monitored filesystems failed, monitoring is in
an undefined state
PTAV WARN rejecting unauthorized client connection from uid %lld pid
%lld %s
PTAV WARN Script failed: return code=%d. script=%s
PTAV WARN stats reset attempt by non-root user %lld
PTAV WARN trace control attempt by non-root user %lld
PTAV WARN Unable to get current working directory, errno %d
PTAV WARN unable to set process priority to %ld, errno %d %s
PTAV WARN unrecognised client command %u
PTAV WARN virus definitions are %d days old
PTAV WARN VIRUS: %s is INFECTED (%d) with '%s'!
PTAV WARN VIRUS: %s is INFECTED with '%s'!
PTAV WARN VIRUS: '%s' is INFECTED with '%s'
PTAV WARN VIRUS: %s (%s) is INFECTED with '%s'!
```

The AIX device driver will send the following messages to syslog using the "kern" facility:

```
PTAV ERROR an instance of the driver already exists
PTAV ERROR bad receive state %d nr %d ne %d
PTAV ERROR driver failed to initialize, error %d
PTAV ERROR driver termination failed, error %d
PTAV ERROR failed to pin device driver, rc %d
PTAV ERROR failed to register close extension, rc %d %s
PTAV ERROR failed to register close extension, rc %d %s %d %x
PTAV ERROR fskv_reg failed, error %d
PTAV ERROR fskv_unreg failure, error %d
PTAV ERROR message length %u too large
PTAV ERROR out of memory for outq buffer, size %d
PTAV ERROR receive in unexpected state %d
PTAV ERROR timeout waiting for callouts to complete
PTAV ERROR uiomove failed rc %d
```

```
PTAV ERROR unpinning failed, err %d
PTAV WARN unhandled ioctl %x
PTAV WARN unhandled message %u
```

zlog.conf

```
[global]
strict init = false
reload conf period = 1M
buffer min = 1024
buffer max = 2MB
default format = "%m%n"
file perms = 640
fsync period = 1K

[formats]
simple = "%m%n"
normal = "%d(%F %T) %m%n"
syslog = "PTAV %V %m%n"
debug = "[%p:%F:%L] %m%n"
scan = "%d %V [%p:%F:%L] %m%n"

[rules]
# Log errors to separate log
*.ERROR                         "%E(PTAV_HOME)/log/error.log", 1MB;
normal

# avscan logging

#avscan.*   >stdout

avscan.INFO                     "%E(PTAV_HOME)/log/avscan.log", 10MB
* 3 ~

"%E(PTAV_HOME)/log/avscan.log.#r"; scan

# avupdate logging

avupdate.*                      >stdout
avupdate.*                      "%E(PTAV_HOME)/log/avupdate.log", 1MB; normal

# syslog output

avscan.=FATAL                   >syslog, LOG_LOCAL3; syslog
avscan.=ERROR                   >syslog, LOG_LOCAL3; syslog
avscan.=WARN                    >syslog, LOG_LOCAL4; syslog
```

```
avscan.=NOTICE                  >syslog, LOG_LOCAL5; syslog

avupdate.=FATAL                 >syslog, LOG_LOCAL3; syslog
avupdate.=ERROR                 >syslog, LOG_LOCAL3; syslog
avupdate.=WARN                  >syslog, LOG_LOCAL4; syslog
avupdate.=NOTICE                >syslog, LOG_LOCAL5; syslog
```

Notes on the default configuration:

- The value of “%E(PTAV_HOME)” is resolved at run-time to be the installation directory, typically /opt/sgav.
- Errors from avscan and avupdate tools are sent to error.log.
- Messages at INFO level and above from avscan are sent to avscan.log
- Messages at all levels from avupdate are sent to standard out and mirrored to avupdate.log.
- Messages at FATAL, ERROR, WARN, and NOTICE for both tools are mirrored to syslog using the syslog levels shown.
- error.log and avupdate.log are truncated once their size reaches 1MB.
- avscan.log is rotated once its size reaches 10MB. Up to three historical logs are kept.
- To prevent mirroring to syslog, comment-out all lines that have “>syslog” in the rule destination.

zlog-avsvc.conf

```
[global]
strict init = true
reload conf period = 0
file perms = 640
default format = "%V %v %m%n"

[formats]
normal = "%d %V [%p:%F:%L] %m%n"
abbrev = "%V %m %n"
plain = "%m %n"
syslog = "PTAV %V %m%n"

[rules]
# config rules used for configuration validation mode
config.=FATAL  >stdout; abbrev
config.=ERROR  >stdout; abbrev
config.=NOTICE >stdout; abbrev
```

```
config.=WARN   >stdout; abbrev
config.=INFO   >stderr; plain
config.*     "%E(PTAV_HOME)/log/avsvc.log",30MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal

# debug rules used in foreground debug mode
debug.INFO   >stderr; abbrev
debug.*      "%E(PTAV_HOME)/log/avsvc.log",30MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal

# avsvc rules used in daemon mode
avsvc.INFO  "%E(PTAV_HOME)/log/avsvc.log",30MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal
#avsvc.*    "%E(PTAV_HOME)/log/avsvc.log",30MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal

# syslog output, daemon mode
avsvc.=FATAL   >syslog, LOG_LOCAL3; syslog
avsvc.=ERROR   >syslog, LOG_LOCAL3; syslog
avsvc.=WARN    >syslog, LOG_LOCAL4; syslog
avsvc.=NOTICE  >syslog, LOG_LOCAL5; syslog
```

Notes on the default configuration:

- A copy of all messages, including debug statements, are sent to avsvc.log.
- The running server will log messages including and above INFO level to avsvc.log, maximum size 10MB, with up to three files of rotation.
- The running server will also log messages including and above NOTICE to syslog.
- To prevent mirroring to syslog, comment-out all lines that have “>syslog” in the rule destination.
- Debug trace may be obtained by swapping the avsvc rules:

```
# avsvc rules used in daemon mode
#avsvc.INFO    "%E(PTAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal
avsvc.*        "%E(PTAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(PTAV_
HOME)/log/avsvc.log.#r"; normal
```

Contacting Fortra

Please contact Fortra for questions or to receive information about Powertech Antivirus. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the Fortra Support Portal at https://support.fortra.com.