helpsystems

User Guide
Powertech Antivirus
5.1

Copyright Terms and Conditions

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 McAfee 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*. Scan results are available in reports and activity can be monitored using notifications.

Powertech Antivirus is easy to keep current with the latest virus definitions from McAfee and software updates directly from HelpSystems. It offers all the essential tools needed to ensure that your systems are protected from the latest threats.

Powered by McAfee

McAfee'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 McAfee'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.

The Virus Information Library on the AVERT Anti-Virus Research Site https://home.mcafee.com/virusinfo contains detailed information about thousands of viruses.

Implementing Powertech Antivirus

The topics in this section describe how to install Powertech Antivirus and begin scanning systems.

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

- Install Powertech Antivirus and connect it to HelpSystems Insite.
- Update to the latest Virus Definitions from McAfee.
- Configure systems to be scanned when accessed (on-access scanning).
- Scan files and directories explicitly (on-demand scanning).
- Use Powertech Antivirus's Interactive Insite features.

Installation

The following are general system requirements and may vary depending on the nature of your environment.

Minimum System Requirements

Linux

- AWS2
- CentOS 7.x Intel 64-bit
- Mint 18
- Oracle 7.x Intel 64-bit
- RHEL 7.x Intel 64-bit
- RHEL 7.2 Power Linux Big Endian
- RHEL 7.1 Power Linux Little Endian (and later)
- SLES 12 & 15 Intel 64-bit
- SLES 12 Power Linux Little Endian
- Ubuntu 16.04 Intel 64-bit
- Approximately 300MB disk space

AIX

- IBM AIX 7.1 TL4
- IBM AIX 7.2 TL0
- Approximately 300MB disk space

Compatibility with HelpSystems Insite

To use HelpSystems Insite to access your products through a web browser, you must meet the following browser and/or operating system requirements.

Hardware Type	Minimum Browser and/or OS Requirements
Desktop/Laptop	Firefox 11 or higher Chrome 21 or higher Internet Explorer 11 Safari 6.1 or higher Microsoft Edge
Mobile Device	iOS: Browsers on iOS 8 or higher Android: OS 4.4 or higher using Chrome Windows: OS 10 using Edge
IBM i	V7R1 or higher operating system

For more details, see the *Insite User Guide* on the HelpSystems website.

Installing or updating

1. Download the Powertech Antivirus install file for your operating system from the HelpSystems Community Portal. If you're a new user, you should have received an email message containing the download link. If you don't have it, contact your Regional Manager.

    > **NOTE:** AIX users: Powertech Antivirus can be installed using the `rpm` command or using SMIT (System Management Interface Tool). Using either method, first change to the directory where the file is located (i.e. cd /home).

2. Unzip the download file, then place the rpm file, or deb file for Ubuntu, on the host machine.

    If you are updating Powertech Antivirus, you will run the product installer over the existing installation. By default, the update folder is the same as the one used for your original Powertech Antivirus installation. (If your current installation uses a different install path, that path can be provided with the --prefix option.) Before updating, backup any user data.

    Once the update is complete, a new license file will need to be placed in the installation folder. The existing license.xml file should be removed. Make sure to keep a copy of license.xml if a rollback to the previous version is needed.

    > **NOTE:** If you are updating and need to identify the version that is currently installed, run the following command: **/opt/sgav/avsvcinfo**

Installing or Updating with RPM

Use the following instructions to install or update Powertech Antivirus with RPM.

To install or update on Red Hat, SLES, or AIX with RPM

Run the following command to install:

```
rpm --install <rpm-file-name>
```

where <rpm-file-name> is the name of the .rpm installation file.

By default, the product will install to the /opt/sgav directory which will be created if it does not exist. To install to a different directory, use the --prefix option. For example:

```
rpm --install <rpm-file-name> --prefix /home/sgav
```

will install to the /home/sgav directory.

Run the following command to update:

```
rpm --upgrade <rpm-file-name>
```

where <rpm-file-name> is the name of the latest version of the .rpm installation file.

If you have installed to an alternate prefix, you must specify the prefix when upgrading if you want the new version installed there as well:

```
rpm --upgrade <rpm-file-name> --prefix /home/sgav
```

To install or update on Ubuntu with DEB

To install on Ubuntu, run the following command:

```
dpkg -i <file-name>
```

where <file-name> is the name of the product .deb file.

To uninstall on Red Hat and SLES, run the following command:

```
rpm -e sgav
```

To uninstall on Ubuntu, run the following command:

```
dpkg -r sgav
```

AIX Only: Installing or Updating using SMIT (System Management Interface Tool)

To install or update using SMIT, run the following command:

```
smit install_software
```

Type the directory where the .rpm file is stored in the INPUT device field, and type `sgav` for SOFTWARE to install as shown below:

> **NOTE:** Users performing an update—If the latest version of Powertech Antivirus is in the same folder as the previous version, use F4 to list the packages that match sgav. Choose sgav-5.0.0.

```
                            SOFTWARE to install


Move cursor to desired item and press F7. Use arrow keys to scroll.
    ONE OR MORE items can be selected.
Press Enter AFTER making all selections.


    sgav                                                   ALL

        @@R:sgav-5.0.0-705 5.0.0-705
        @@R:sgav-4.3.0-602 4.3.0-602
```

Install Software

1. Type or select values in entry fields.
2. Press Enter AFTER making all desired changes.

[Entry Fields]

```
* INPUT device / directory for software            /home
* SOFTWARE to install                              [sgav-5.0.0-705 sgav-
5.0.0-705  > +
PREVIEW only? (install operation will NOT occur)   no                   +
COMMIT software updates?                           yes                  +
SAVE replaced files?                               no                   +
AUTOMATICALLY install requisite software?          yes                  +
EXTEND file systems if space needed?               yes                  +
OVERWRITE same or newer versions?                  no                   +
VERIFY install and check file sizes?               no                   +
Include corresponding LANGUAGE filesets?           yes                  +
DETAILED output?                                   no                   +
Process multiple volumes?                          yes                  +
ACCEPT new license agreements?                     no                   +
Preview new LICENSE agreements?                    no                   +
WPAR Management
```

```
Perform Operation in Global Environment         yes                    +
Perform Operation on Detached WPARs             no                     +
Detached WPAR Names                         [_all_wpars]          +
Remount Installation Device in WPARs            yes                    +
Alternate WPAR Installation Device              []
F1=Help           F2=Refresh        F3=Cancel         F4=List
F5=Reset          F6=Command        F7=Edit           F8=Image
F9=Shell          F10=Exit          Enter=Do
```

3. When the installation is complete, the following screen will appear. Ensure the Command status is `OK`.

```
                          COMMAND STATUS
        Command: OK              stdout: yes              stderr: no
```

Before command completion, additional instructions may appear below.

```
installp: The specified device /home/root
is not a valid device or file.
geninstall -I "a -cgNQqwX -J"  -Z   -d /home -f File 2>&1

File:
R:sgav-5.0.0-705
Validating RPM package selections ...
Please wait...
sgav                          #################################################
```

Licensing

After your purchase, you will receive an email from HelpSystems with your license code attached. To license the software:

1. Save the attached file to the /opt/sgav directory (or wherever the product was installed).
2. Rename the file to "license".

Connecting Powertech Antivirus to HelpSystems Insite

In order to use HelpSystems Insite to monitor and manage endpoints, you need to register Powertech Antivirus on the endpoint using the Insite Integration Service. To do so:

1. Install HelpSystems Insite, including the Powertech Antivirus module (an option within the Insite installation wizard). The Insite download is available at the HelpSystems Community Portal. You can reference instructions for installing, licensing, and configuring Insite on the Insite download page.
2. Open Insite in your web browser.

3. Whitelist the Insite Powertech Antivirus service.
    a. Go to **Settings > Products** and check **Insite Powertech Antivirus Service**.
    b. Click **Whitelist**.
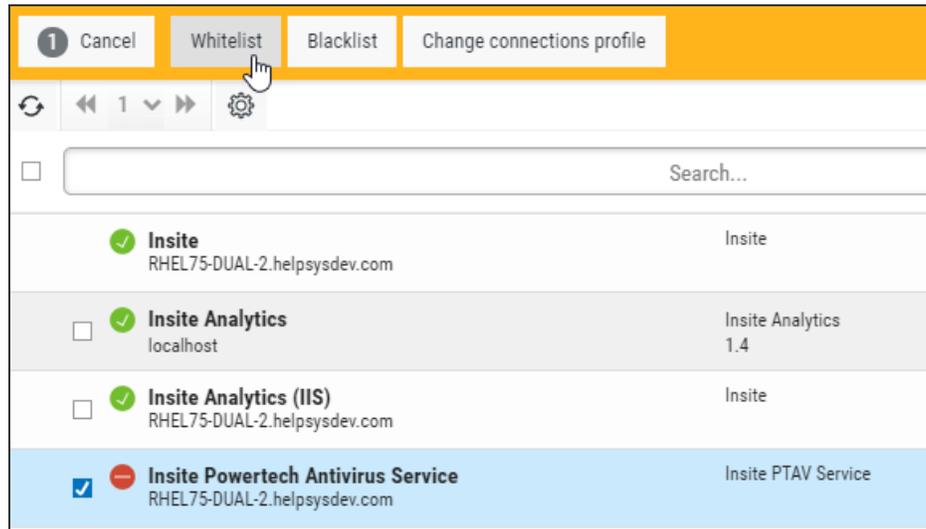
4. Copy your Insite Service API Key. To do so:
    a. Go to **Settings > Integration Service Admin**.

    b. For the key, choose ⋮ (Show Actions) > Copy.
5. On the endpoint:
    a. Go to the Integration Service folder using command `cd /opt/sgav/integration`
    b. Run the registration command `register.sh` with the required parameters, pasting the Server Key you have copied for -k.
        Required Parameters:

        ```
        -k|--key)       Server Key
        -s|--server)    Fully Qualified Domain Name
        ```

        Optional Parameters:

        ```
        -p|--port)      Server Port [default=8998]
        -a|--alias)     Alias Name
        -c|--client)    Client IP/DNS Name
        -f|--folder)    Client Install Path
        ```

        EXAMPLE: `./register.sh -k ad24embc-517u-43f1-80a8-68446a2f0e8d -s myinsiteserver.mydomain.com`

6. Return to Insite and choose **Powertech Antivirus > Connection Settings**. The server you have added appears in the list. Its status is New ○, indicating the endpoint has not been Whitelisted. Whitelisting an endpoint is required to indicate the endpoint should be allowed to communicate with the Insite server.

7. To approve the registered endpoint, click ⋮ (**Show Actions) > Whitelist**. Doing this:
   - Allows the Powertech Antivirus Service to connect to Insite's Integration Service.
   - Triggers the Integration Service to start sending health check requests to the endpoint system.

   > **NOTE**: Servers can also be whitelisted by checking the server and selecting **Whitelist** at the top of the screen.

   Insite now lists the endpoint's status as critical 🔴, indicating the endpoint is not responding to health checks.

8. Run the following command on the endpoint system (in *ptav-home*/integration) to begin responding to health check requests sent by Insite.

   ./avinsitectl start

   > **NOTE**: The command above starts the service once, but does not "enable" it to run after reboot. To also automatically start after reboot, use the command:
   >
   > **./avinsitectl enable**

   Insite now lists the endpoint's status as good ✅, indicating it is now responding to health check requests.

9. Repeat steps 2-6 for additional servers you would like to register and scan. See Using Powertech Antivirus with HelpSystems Insite for more details.

See the HelpSystems Insite User Guide for more details on setting up and using HelpSystems Insite.

Port/Server Configuration

This is the mapping of the services HelpSystems Insite and Powertech Antivirus run and the ports used. The ports shown are default ports. If they are already in use during the installation, a different port is used.

The following ports must be open in order for Insite to function:

- 8998: HTTP port used for product registration (can be selectively enabled in firewall)
- 3030: Insite web port
- 9092: Communication port

The remaining ports are only used for local communication under a single server Insite installation.

Single server configuration
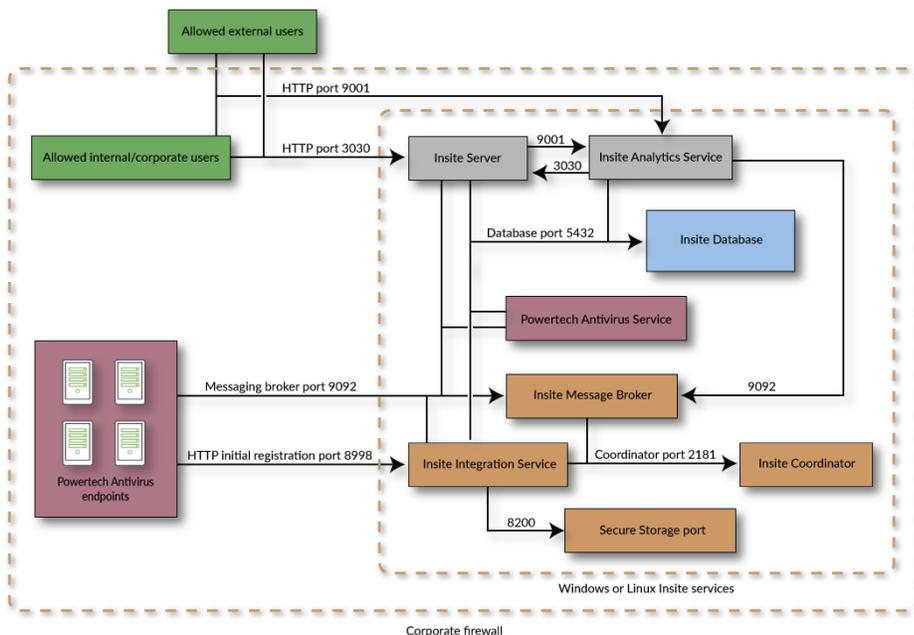
Dual server configuration

For a dual server installation, the database port (5432 by default) also needs to be open.

Updating Virus Definitions

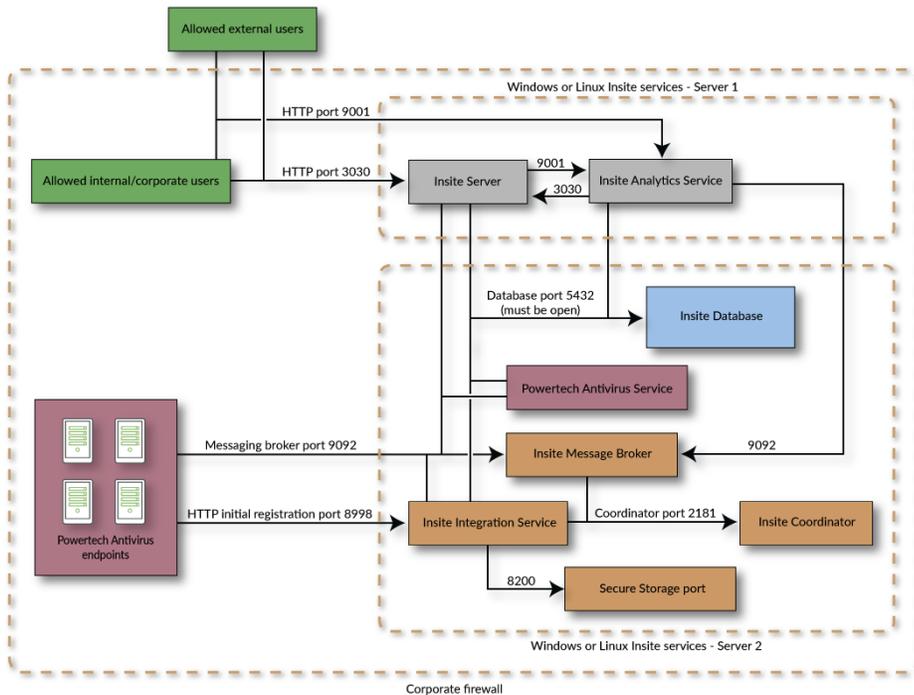After installation you will need to download the latest virus definitions from McAfee before you can perform scanning operations. By default, Powertech Antivirus can download the files using CURL. (Default download settings can be overridden using the --path, --ftp, --wget, or --curl options. See [avupdate command](#).)

> **NOTE:** McAfee is removing support for FTP access on May 31, 2019.

McAfee 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:

```
cd /opt/sgav
./avupdate
```

or

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

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.

Notes

McAfee 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 (18):

```
0 18 * * * /opt/sgav/avupdate > /opt/sgav/log/avupdate.out
```

On AIX, to see the cron log, run `tail /var/adm/cron/log`.

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](#).

```
exit status
```

This command returns the following exit values:

0 Process completed successfully.

1 An error occurred.

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.

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. Use the `avsvcctl` command to start, stop, and manage the other functions of the service as described below.

Commands to troubleshoot on-access scanning can be found in the avsvccfg Command and avsvcinfo Command.

> **WARNING:** Prior to scanning, ensure you have acquired the latest virus definitions from McAfee (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.

avsvcctl 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 install the service control file, if necessary. This option can only be run by the root user.

```
disable
```

Prevent the anti-virus service from starting during system boot. 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

avsvc

Exit Status

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

avsvc command

Use this command to troubleshoot on-access scanning. For more troubleshooting options, see avsvccfg Command and avsvcinfo 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. See Commands below.

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.

```
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. 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
```

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=300
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.

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. Please note many viruses come in the form of .zip archive files.

Troubleshooting

If a virus was not detected in a particular file, verify your virus definitions 'know' about the suspected virus. Check the McAfee virus information library at https://home.mcafee.com/virusinfo.

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'
```

See Also

[avupdate](#)

[avscan](#)

[avsvcctl](#)

Exit Status

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

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.

To scan the file system for viruses and malicious code, use the `avscan` command.

> **NOTE:** To use on-access scanning, use the `avsvc` command. See [On-Access Scanning](#).

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.

> **WARNING:** Prior to scanning, ensure you have acquired the latest virus definitions from McAfee (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.

avscan command

Syntax

```
avscan [ -r ] [--ignorelinks] [ --noheuristics ] [ --
nomacros ] [ --pup ] [ --mime ] [ --noarc ] [ --exeonly ] [ --
exclude {file(s):directorie(s) } ] [ --maxwait seconds ] [ --timeout
seconds ] [ --delay microseconds ] [ --clean ] [ --quar ] [ --cmd
<"command-string"> ] [ --notify <"notifiers"> ] [ --loglevel level ]
[ --quiet ] [ --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 encountered and you have not specified the `--clean` or `--quar` flags, the `avscan` command prints the infections to the output stream and the infected file remains unchanged. To have the command clean or quarantine infections you need to specify either the `--clean` or `--quar` options (or both). Please note if a file cannot be cleaned it is deleted unless the `--quar` option is 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
```

Linux

```
bash-4.2# ./avscan -r --pup /home/user/sgavData
Powertech Antivirus Scan 5.0.0-705
Started: Friday Mar 01 03:26 PM

Initializing ...

McAfee 6000 engine, DAT level 9182 (03/01/19)

Path . . . . . . : /home/user/sgavData
Recurse  . . . . : Yes
Archives . . . . : Yes
Files  . . . . . : All
Links  . . . . . : Yes
Heuristics . . . : Yes
Clean  . . . . . : No
Quarantine . . . : No
Macros . . . . . : Yes
Programs . . . . : Yes
MIME . . . . . . : No
Max wait . . . . : 0
Timeout. . . . . : 0
Delay. . . . . . : 0
Notify . . . . . :
Log level  . . . : 99

/home/user/sgavData
/home/user/sgavData/dir_1
/home/user/sgavData/dir_1/simplefile.log [6]  OK
/home/user/sgavData/dir_2
/home/user/sgavData/dir_2/simplefile.log [6]  OK
/home/user/sgavData/eicar-file.txt [68] .......VIRUS: /home/user/sgavData/eicar-file.txt is INFECTED (1) with 'EICAR test file'!
/home/user/sgavData/eicarpuo-file.bin [62] ........VIRUS: /home/user/sgavData/eicarpuo-file.bin is INFECTED (2) with 'EICAR PUO test file'!
/home/user/sgavData/emptyfile_1.txt [0]  OK
/home/user/sgavData/myscript.sh [37] ......... OK
/home/user/sgavData/regularfile.txt [27] ......... OK
7 files scanned, 2 infected, 0 skipped, 0 error(s), 0 cleaned, 0 deleted, 0 quarantined.
Completed: Friday Mar 01 03:27 PM, duration 23s
bash-4.2#
```

AIX

```
bash-4.2# ./avscan -r /home/user/sgavData
Powertech Antivirus Scan 5.0.0-705
Started: Friday Mar 01 03:20 PM

Initializing ...

McAfee 6000 engine, DAT level 9182 (03/01/19)

Path . . . . . : /home/user/sgavData
Recurse  . . . : Yes
Archives . . . : Yes
Files  . . . . : All
Links  . . . . : Yes
Heuristics . . : Yes
Clean  . . . . : No
Quarantine . . : No
Macros . . . . : Yes
Programs . . . : No
MIME . . . . . : No
Max wait . . . : 0
Timeout. . . . : 0
Delay. . . . . : 0
Notify . . . . :
Log level  . . : 99

/home/user/sgavData
/home/user/sgavData/dir_1
/home/user/sgavData/dir_1/simplefile.log [6]  OK
/home/user/sgavData/dir_2
/home/user/sgavData/dir_2/simplefile.log [6]  OK
/home/user/sgavData/emptyfile_1.txt [0]  OK
/home/user/sgavData/myscript.sh [37] ......... OK
/home/user/sgavData/regularfile.txt [27] ......... OK
5 files scanned, 0 infected, 0 skipped, 0 error(s), 0 cleaned, 0 deleted, 0 quarantined.
Completed: Friday Mar 01 03:21 PM, duration 23s
bash-4.2#
```

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 only directories recursively, as specified by the pattern File...|Directory....

```
--ignorelinks
```

Ignore all symbolic links. By default, the command follows all symbolic links during the scan. This parameter instructs the command to ignore any symbolic links it finds.

```
--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. By default the `avscan` command will scan for macro viruses. Use the `--nomacros` option to turn this feature off.

```
--pup
```

Scan for 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.

```
--mime
```

Scan for viruses in MIME-encoded files, UU-encoded files, XX-encoded files and BinHex files, and files in TNEF and IMC formats. By default, the product does not scan these types of files. This parameter reduces scanning performance.

```
--noarc
```

Do not scan within archives (.zip, .jar, .rar, etc). Default is to scan archives.

```
--quiet
```

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

```
--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. For example:

`avscan --exclude /home/usr1:/home/usr2` will exclude the `/home/usr1` and `/home/usr2` directories. You can specify a maximum of 100 files and directories to exclude using this parameter.

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

```
--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. There is no default for this parameter (files are scanned completely). Use this option cautiously.

```
--timeout <seconds>
```

Specifies the maximum number of seconds the `avscan` command 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.

```
--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.

```
--clean
```

Clean infected files by repairing the infection. Please note 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.

```
--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. Please note 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 <"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. See Notification Support.

```
--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.

```
--version
```

Prints the program version and build information, then exits.

Examples

```
avscan
```

Scans all files in the current directory.

```
avscan -r /
```

Scans all files in the current directory and all sub-directories.

```
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 /Quarantine directory.

```
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 /Quarantine 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`.

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
```

This command returns the following exit values:

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).

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

Troubleshooting

If a virus was not detected in a particular file, verify your virus definitions 'know' about the suspected virus. Check the McAfee virus information library at https://home.mcafee.com/virusinfo.

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 /proc, /dev, /sys and optical media mount paths from your scan using the exclude path option.
- 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.

Scheduling updates and scans

HelpSystems recommends updating the Powertech Antivirus DAT files daily, and running scans weekly. The following instructions describe how to schedule these events so they occur automatically.

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 listed under Options (in the Scanning section of this document) to the command.

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
> ```

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 the Insite web browser interface. See Configuration Properties pane.

Notification configuration

Two sections of Powertech Antivirus's config.ini are used for notification configuration: [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 an 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 v5.0.0-705.
(c) Copyright HelpSystems, 2019. All rights reserved. Licensed
material, property of HelpSystems.

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*'"
    - This can be tested via the maxwait option.

- 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*"
    - Tested via cleanfail=quarantine.
- delete
  - "file *file* deleted"
    - This can be tested via cleanfail=delete.
  - "Infected file '*file*' deleted *code [code]*"
    - TODO: I think there is a macro document that triggers this one?
- 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).

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](#)

Powertech Antivirus and HelpSystems Insite

The HelpSystems Insite web browser interface provides an efficient, interactive method to monitor and manage Powertech Antivirus on endpoints across your network.

> **NOTE:** To begin using Insite with Powertech Antivirus, see [HelpSystems Insite Setup](#).

Using Insite with Powertech Antivirus

The following provides an overview for how to manage Powertech Antivirus using your web browser. For general details about using HelpSystems Insite, see the [HelpSystems Insite User Guide](#).

Sort, Search, and Filter settings

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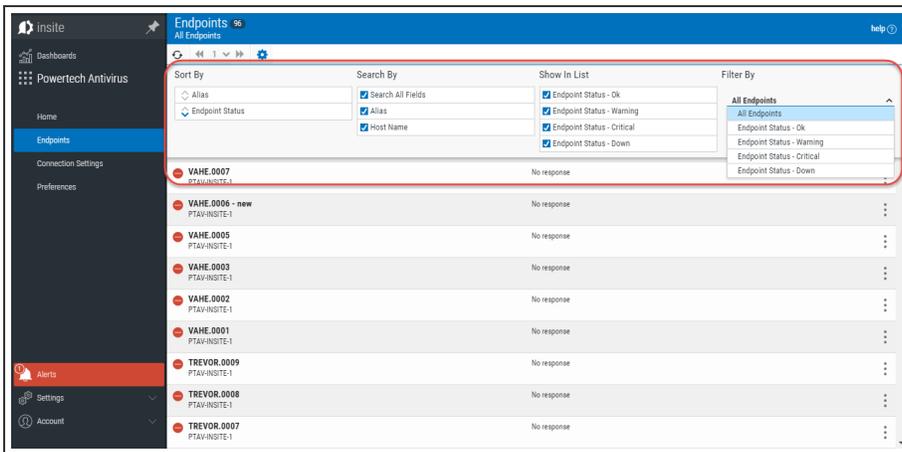
- Click ⚙ **(Settings)** to open the sort, search, and filter settings.
- Select how you want the status list sorted (Sort By). Click your selection again to change the sort order to ascending ⌃ or descending ⌄.

> **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 box appears near the top of your browser window. Type into Insite's 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 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.

# Navigation Pane and Select Products Pane

The Navigation Pane includes management tools for Powertech Antivirus. When open, it is located on the left side of your browser window.

Click ![pin icon] to allow the Navigation Pane to minimize. Click ![pin icon] to pin the Navigation Pane open, so its contents remain visible.

Click ![grid icon] to open or close the Select Product Pane.

Selecting Multiple Connections or Configurations

The Connection Settings screen and Configuration screen 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 screen.
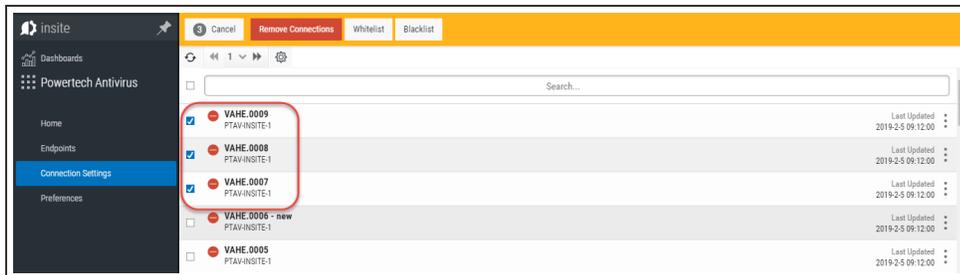
Connection Options

- **Remove Connections.** Choose this option to remove the selected connections from Insite.
- **Whitelist.** Choose this option to whitelist the selected connections to indicate the selected endpoints should be allowed to communicate with the Insite server.
- **Blacklist.** Choose this option to blacklist the selected connections to indicate the selected endpoints should not be allowed to communicate with the Insite server.
- **Cancel.** Choose this option to remove selection and dismiss the multi-select buttons.

See also Connection Settings screen.

Configuration Options

- **Cancel.** Choose **Cancel** to de-select the selected Configurations.
- **Delete.** Choose **Delete** to remove the selected Configurations.
- **Update Endpoints.** 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 also Configurations screen.

Reference
Powertech Antivirus Commands

This section describes Powertech Antivirus' commands.

avconfig command

Name

avconfig - Antivirus service configuration helper.

Synopsis

avconfig [-d] [-h | -V | -C <params> | -U <params>]

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, and a [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. 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.

−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.

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.

See Also

[Notifications](#)

[avsvc](#)

[avscan](#)

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

See On-Access Scanning.

avsvccfg command

Name

avsvccfg - Powertech Antivirus service configuration helper.

Synopsis

```
avsvccfg [validate | create | update | help]
```

Description

The avsvccfg command can be used to validate and modify the [avsvc] section of the configuration file, config.ini, for the anti virus service.

> **NOTE:** This command has been superseded by the more powerful avconfig tool.

Configuration options are described in the avsvc manual page. Root privilege is required to perform operations on the configuration file.

Options

```
validate
```

Produce a validation report of the current contents of config.ini.

```
create
```

Overwrite the configuration file with the supplied parameters, merged with the default settings.

> **EXAMPLE:**
> To revert to default settings:
> ```
> avsvccfg create
> ```
> To override default settings for clean and macro options:
> ```
> avsvccfg create clean=no,macro=no
> ```

```
update
```

Overwrite the configuration file with the supplied parameters, merged with the current settings.

> **EXAMPLE:**
> To change exclude and programs options:
> ```
> avsvccfg update exclude=/dev:/run,programs=yes
> ```

```
help
```

Show man page with this information.

See Also

[avsvc](#)

Exit Status

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

avsvcctl command

See [On-Access Scanning](#).

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

avsvcctl

Exit Status

The command returns 0.

avscan command

See On-Demand Scanning.

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. McAfee updates virus definitions every day and you should run the avupdate command every day. By default, files will be retrieved from McAfee's HTTP server (http://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. This is the default option if none of --path, --ftp or --wget options are specified. Command output will be sent to log/curl.log.

```
--wget
```

Files will be downloaded using the system 'wget' client, /usr/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).

```
--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.

```
--force
```

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

```
--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.

```
--help
```

Displays help text.

Example

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

Notes

McAfee 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](#)

HelpSystems Insite Web UI

The topics in this section describe the Powertech Antivirus-specific elements of HelpSystems Insite.

> **NOTE:**
> - To connect Powertech Antivirus to HelpSystems Insite, see Connecting Powertech Antivirus to HelpSystems Insite.
> - See also Using Insite with Powertech Antivirus.
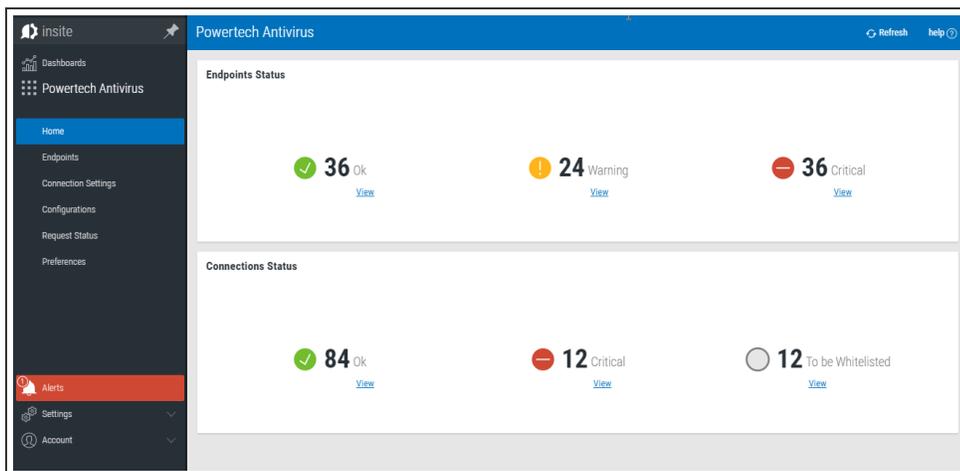
Home screen

How to get there

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

What it does

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

Endpoint Status

These indicators allow you to quickly identify the number of endpoints at each status level, and navigate to the Endpoints screen 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 screen with the list of endpoints filtered by "Endpoint Status - Ok."

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

Connection Status

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

✅ **Ok.** Indicates the number of systems responding to health check requests from Insite. Click **View** to open the Connection Settings screen with connections filtered by "Connection - Ok."

🔴 **Critical.** This indicates the number of connections that are not responding to health check requests from Insite. Click **View** to open the Connections screen with connections filtered by "Connection - Critical."

⚪ **To be Whitelisted.** This indicates the number of new connections that have not yet been whitelisted. Click **View** to open the Connections screen with connections filtered by "To be Whitelisted."

Endpoints screen

How to get there

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

What it does

The Endpoints screen indicates the status of registered endpoints. This list excludes endpoints that have not been whitelisted, as well as endpoint that have been blacklisted. (See Connection Settings screen for details.)

Identifying the Endpoint Status

✅ **Good.** 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.

Options

⋮ **(Show Actions)**

Select this to show a menu with the following options

- **Properties.** Click Properties for an Endpoint to open the Endpoint Properties pane, where you can configure settings for the Endpoint.
- **Update Endpoint Configuration.** Choose this option to update the Configuration on the endpoint in order to restore the current Configuration settings.
- **Close.** Choose **Close** to dismiss the Actions menu.

Selected Endpoints

Select one or more Endpoints using the check box to the left of each Endpoint in the list. When you do so, the following options appear at the top of the screen.
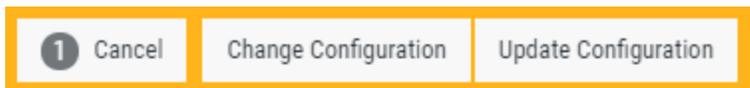
Endpoint Properties pane
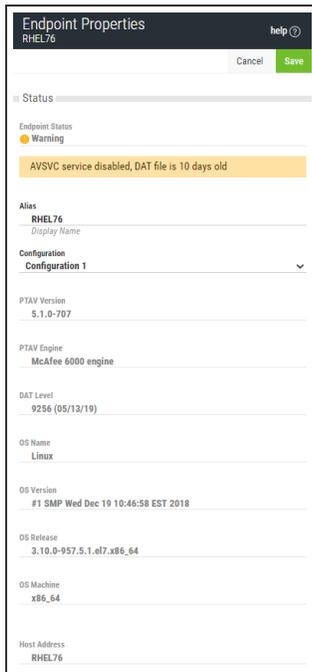
How to get there

In the Insite Navigation Pane, choose **Endpoints** and click an endpoint in the list.

What it does

The Endpoints Properties settings allow you to identify endpoint status details and modify the endpoint alias.

Options

Status

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

### Product Connection

Host Address
The host address of the product connection.

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 screen. 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.

Connection Settings screen
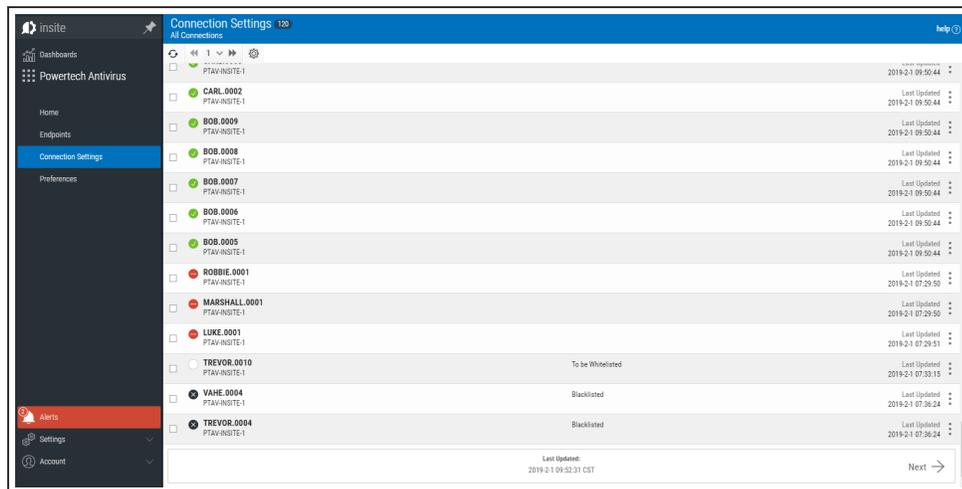
How to get there

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

What it does

The Connection Settings screen indicates the connection status of endpoints.

Identifying the Connection Status

✅ **Ok.** The system is responding to health check requests from Insite.

⭕ **New.** System not yet whitelisted. In order to communicate with Insite, the system must be whitelisted.

🔴 **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.

❌ **Blacklisted.** The system has been blacklisted, indicating it is not allowed to communicate with the Insite server.

Options

 (Show Actions)

Select this 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.
- **Blacklist.** Choose this option to blacklist the Connection, preventing communication with the Insite server.
- **Remove Connection.** Choose this option to remove the Connection from Insite.
- **Close.** Choose **Close** to dismiss the Actions menu.

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 Multiple Connections or Configurations.

Connection Properties pane
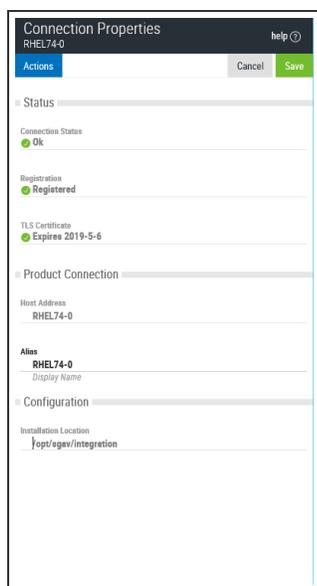
How to get there

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

What it does

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

Options

Actions

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

- **Blacklist.** Choose this option to blacklist the connection, preventing communication with the Insite server.
- **Renew Certificate.** Choose this option to renew the TLS certificate. The server's Connection Status must be Ok in order for this option to function.
- **Remove Connection.** Choose this option to remove the connection from Insite.
- **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 Insite.

Registration

Indicates the registration status of the connection. Green indicates the status is Ok. Red indicates the connection is not registered. See HelpSystems Insite Setup for details on registering the endpoint.

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

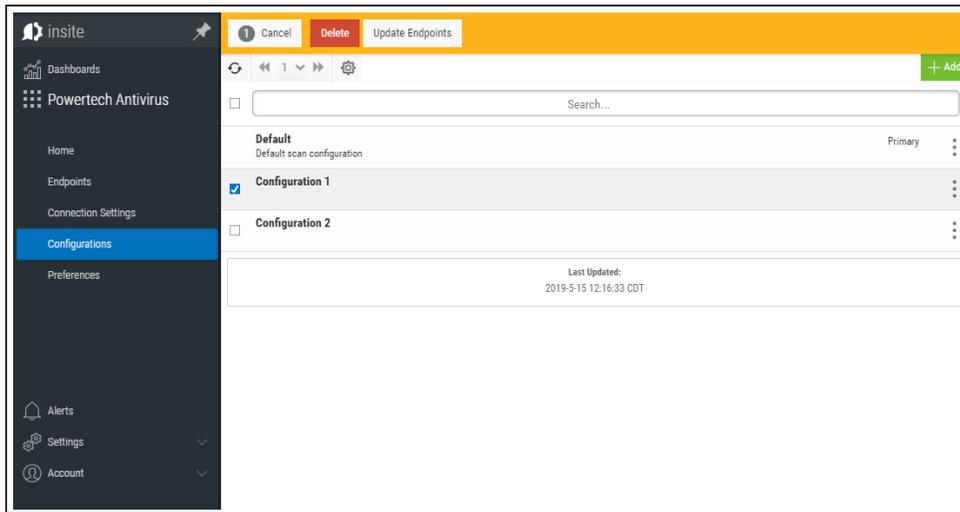The host address of the product connection.

Alias

How the system is displayed in the connection settings list.

Configuration

Installation Location

This is the path of the Insite Integration directory on the endpoint system.

Configurations screen

How to get there

In the Insite Navigation Pane, choose **Configurations**.

What it does

The Configuration Screen allows you to add or update Configurations. See also Configuration Properties pane.

Options

Add

Choose **Add** to open the New 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 Configuration Properties pane, where you can update settings for the Configuration.
- **Update Endpoints.** Choose this option to update the endpoint to restore the assigned Configuration settings.
- **Duplicate.** Choose this option to duplicate the Configuration.
- **Close.** Choose **Close** to dismiss the Show Actions menu.

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 Multiple Connections.

Selected Configurations

Select one or more Configurations using the check box to the left of each Configuration in the list. When you do so, the following options appear at the top of the screen.
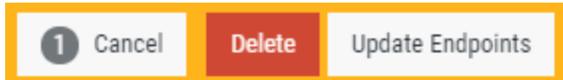
Configuration Properties/New Configuration pane
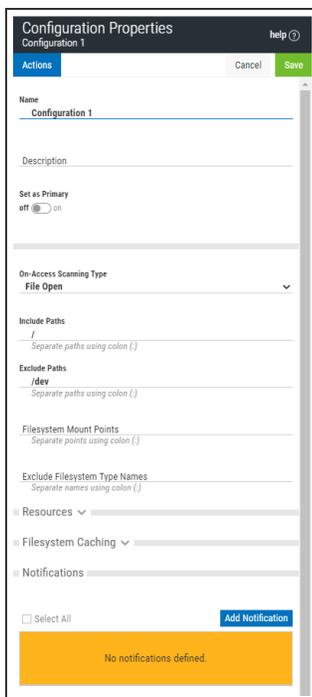
How to get there

In the Insite Navigation Pane, choose **Configurations** and click a Configuration in the list.

What it does

The Configuration Properties pane allows you to set configuration options, including notification settings, for on-access scanning. It also allows you to set notification options for on-demand scanning.

> **NOTE:** Notification settings are the only on-demand scanning configuration options supported by Insite. When you save a set of configuration options in Insite, the existing config.ini configuration settings file is overwritten.

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 screen.

On-access scanning Type; File Open • File Open and Closed • Disable

File Open specifies that files should be scanned when users attempt to open the file. **File Open and Closed** specifies that files should be scanned during file open and after file close. **Disable** disables on-access scanning.

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.

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.

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.

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 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.

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 yes, no. The default is no.

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.

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.

Change Configuration dialog box
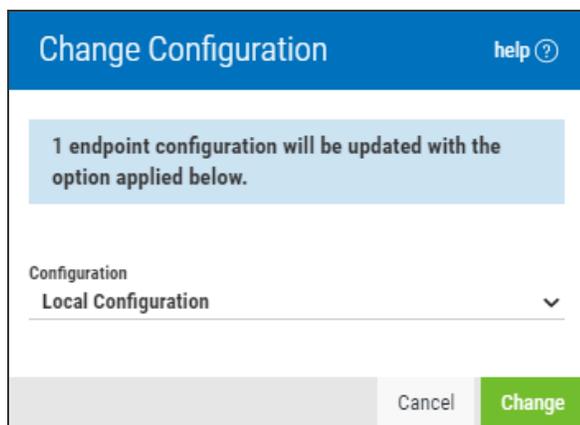
How to get there

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

What it does

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

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 screen. 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.

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.

Delete Configuration dialog box
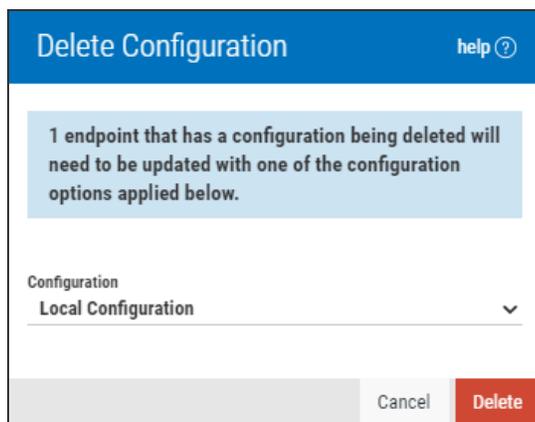
How to get there

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

What it does

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), as shown below, will be assigned to the Configuration chosen from the Configuration drop-down menu. See also Endpoint Properties pane.

Configuration

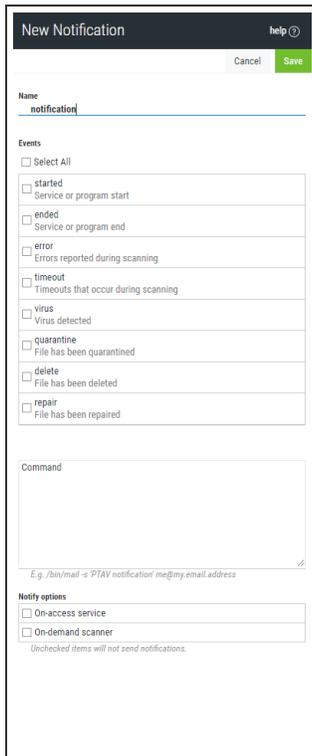| Configuration 1	^
Local Configuration	
Primary (Configuration 1)	
Default	
Configuration 1	
Configuration 2	

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.

New/Edit Notification pane

How to get there

In the Configuration Properties pane, choose **Add Notification**.

What it does

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.

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.

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 Insite. When you save a set of configuration options in Insite, the existing config.ini configuration settings file is overwritten.

Preferences screen
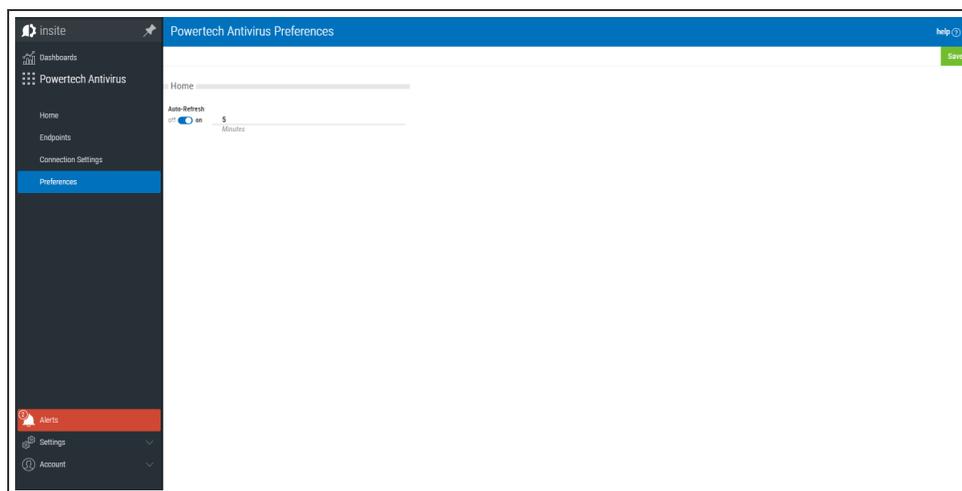
How to get there

In the Insite Navigation Pane for Powertech Antivirus, choose **Preferences**.

What it does

This screen allows you to configure the status and frequency of Powertech Antivirus's Auto-Refresh feature.

Options

Auto-Refresh; on • off.

When on, Powertech Antivirus refreshes the Home screen 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 screen does not automatically refresh.

Request Details screen

How to get there

In the Powertech Antivirus Navigation Pane, choose **Request Status**. Click ⋮ **(Show Actions)** and select **View Details**.

What it does

This screen includes the status of all endpoints included in the update request. See also Request Status screen.

Identifying the Request 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.

Options

Close

Select **Close** to dismiss the screen and return to the Request Status screen.

Request Status screen

How to get there

In the Powertech Antivirus Navigation Pane, choose **Request Status**.

What it does

This screen allows you to reference status information about requests sent to Insite's Powertech Antivirus service. The list indicates the progress status of each request, one of three statuses with their count, the request time, and time the request was completed.
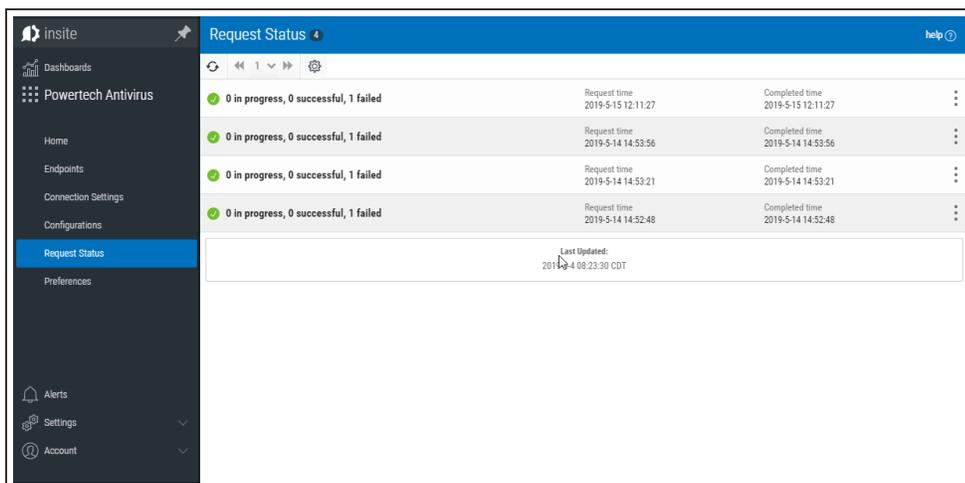
Identifying the Request Status

⚪ **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.

Options

⋮

(Show Actions)

Select this to show a menu with the following options:

- **View Details.** Click **View Details** for a request to open the <u>Request Details screen</u>, where you can view the status of all endpoints included in the update request.
- **Close.** Choose **Close** to dismiss the Actions menu.

Appendix

The topics in this section include additional information about Powertech Antivirus.

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 <u>http://update.nai.com/products/commonupdater/oem.ini</u>
   > b. wget -N <u>http://update.nai.com/products/commonupdater/*.zip</u>
   >   McAfee 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`

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 <u>https://hardysimpson.github.io/zlog/UsersGuide-EN.html</u>.

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 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 ignore SIGUSR1, errno %d %s
PTAV FATAL failed to initialize monitoring
PTAV FATAL failed to install SIGUSR2 handler, errno %d %s
PTAV FATAL no memory for event initialisation
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 code %d.
PTAV ERROR bad receive state %d nr %d ne %d
PTAV ERROR Cannot clear %s, not a subdir within %s
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 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 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 DAT update 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 EOVERFLOW, file too large
PTAV ERROR error creating thread
PTAV ERROR Error getting DATVersion from oem.ini 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 failed to add scan work to thread pool
PTAV ERROR failed to allocate vfstypes storage
PTAV ERROR failed to allow access to file %s, errno %d %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 event, 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 initialize device driver, errno %d %s
PTAV ERROR failed to initialize filesystem cache
PTAV ERROR failed to load device driver, errno %d %s
PTAV ERROR failed to open file %s, errno %d %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 %s scan parameter list
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 ignored empty '%s' value in configuration file
PTAV ERROR ignored invalid '%s' value '%s' in configuration file
PTAV ERROR ignoring '%s' in notify section
PTAV ERROR invalid 'access' value '%s' in avsvc configuration
PTAV ERROR invalid avsvc parameter '%s'
PTAV ERROR invalid 'cleanfail' value '%s' in avsvc configuration
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 'thread' value '%s' in avsvc configuration
PTAV ERROR licensing error %d, contact PowerTech
PTAV ERROR local listener failure, error %d %s
PTAV ERROR message data size %d out of range
PTAV ERROR mkdir %s failed, errno %d %s
PTAV ERROR no callback registered for client connection
PTAV ERROR notifier '%s' has no command specified
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 permission denied, invalid message signature
PTAV ERROR quarantine of infected file failed for %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\n
PTAV ERROR Scan engine failed, reason code %d.
PTAV ERROR Scan engine failed: %s.
PTAV ERROR Scan failed (error %d)
PTAV ERROR skipping '%s'
PTAV ERROR special file %s does not have expected ownership and/or
permissions
PTAV ERROR the scanning engine encountered an unrecoverable error
PTAV ERROR timed out waiting for monitoring thread to start
PTAV ERROR Unable to apply incrementals on this build (switching to
full update)
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 /proc/mounts, errno %d %s
PTAV ERROR unable to parse '%s' value '%s' in configuration file
PTAV ERROR unable to resolve quarantine path '%s', errno %d %s
PTAV ERROR unable to set client socket options, errno %d %s
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 %s
PTAV ERROR unsupported parameter '%s', use avconfig
PTAV ERROR Unzip failed, see log file %s/unzip.txt for details.
PTAV NOTICE avscan starting
PTAV NOTICE DAT files updated to %d
PTAV NOTICE DAT levels the same, nothing to do!
PTAV NOTICE McAfee %d engine, DAT level %d (%s)
PTAV NOTICE Restarting avsvc service...
PTAV NOTICE %s DAT update %s starting
PTAV NOTICE Starting %s %s v%s at %.24s.
PTAV NOTICE Stopping avsvc service...
PTAV WARN cache clear attempt by non-root user %lld
PTAV WARN cache dump attempt by non-root user %lld
PTAV WARN chown %lld:%lld of %s failed, errno %d %s
PTAV WARN configuration load failed
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: 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 get driver queue stats, errno %d %s
PTAV WARN failed to reset driver queue stats, errno %d %s
PTAV WARN log reconfigure failed
PTAV WARN log reconfigure with file '%s' failed because %s
PTAV WARN no filesystems are being monitored after reconfiguration
PTAV WARN no filesystems are being monitored after refresh
PTAV WARN notifier %s returned code %d (errno %d)
PTAV WARN product is not licensed: error %d (%s)
PTAV WARN quarantined file %s
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 stats reset attempt by non-root user %lld
PTAV WARN unable to set process priority to %ld, errno %d %s
PTAV WARN unhandled message %d from device driver
PTAV WARN unrecognised client command %u
PTAV WARN virus definitions are %d days old
PTAV WARN VIRUS: '%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 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 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
rotate lock file = /tmp/zlog.lock
```

```
default format = "%m%n"
# Log file permissions: 660 = -rw-rw----
file perms = 660
fsync period = 1K

[formats]
simple = "%m%n"
normal = "%d(%F %T) %m%n"
syslog = "SGAV %V %m%n"
debug = "[%p:%F:%L] %m%n"

[rules]
# Log errors to separate log
*.ERROR                         "%E(SGAV_HOME)/log/error.log", 1MB;
normal

# avupdate logging

avupdate.*                 >stdout
avupdate.*                 "%E(SGAV_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(SGAV_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 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.
- 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 = 644
default format = "%V %v %m%n"

[formats]
normal = "%d %V [%p:%F:%L] %m%n"
abbrev = "%V %m %n"
plain = "%m %n"
syslog = "SGAV %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(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
HOME)/log/avsvc.log.#r"; normal

# debug rules used in foreground debug mode
debug.INFO   >stderr; abbrev
debug.*      "%E(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
HOME)/log/avsvc.log.#r"; normal

# avsvc rules used in daemon mode
avsvc.INFO  "%E(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
HOME)/log/avsvc.log.#r"; normal
#avsvc.*     "%E(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
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:

- When the server is requested to validate the config.ini configuration file ("avsvccfg validate"), the messages for everything including and above INFO level are sent to the screen. 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(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
HOME)/log/avsvc.log.#r"; normal
avsvc.*        "%E(SGAV_HOME)/log/avsvc.log",10MB * 3 ~ "%E(SGAV_
HOME)/log/avsvc.log.#r"; normal
```

Technical Support

To contact Powertech Customer Support, visit http://www.helpsystems.com/powertech/technical-support.