helpsystems

User Guide
Powertech Antivirus
5.4.2




Copyright Terms and Conditions

202104070939

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*.

The status of endpoints on your network can be monitored and updated with the latest virus definitions directly from your browser using Insite. The virus definitions from McAfee can be acquired directly by the endpoints themselves or transferred through a local DAT file repository. Scan results and other endpoint activity is reported in Insite and easily accessible with search, sorting, and filtering features. Scan results are also available in reports and activity can also be monitored using notifications.

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

Powered by 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 Insite.
- Update to the latest Virus Definitions from McAfee.
- Develop an approach to scanning your systems efficiently
- 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.

Installing Powertech Antivirus

Use the following instructions to install Powertech Antivirus

> **NOTE:** If you intend to install Powertech Antivirus to an air-gapped system, see Air-Gapped Installation of Insite and Powertech Antivirus.

Before You Begin

Read this section before you install Powertech Antivirus.

System Requirements

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

Linux

- Supported Linux OS Versions:
  - Amazon 2
  - IBM LinuxONE and Linux on IBM Z for supported SLES, RHEL, and Ubuntu operating systems
  - IBM Linux on Power Big Endian for RHEL 7
  - IBM Linux on Power Little Endian for supported RHEL and SUSE operating systems
  - MINT 18
  - Red Hat Enterprise Linux 6, 7, and 8
  - CentOS 7
  - Debian 8
  - Oracle 7

  - Suse Enterprise Linux 12 and 15
  - Ubuntu 16.04, 18.04, and 20.04
- Approximately 1.2 GB disk space in /opt, 1.5 GB is recommended

AIX

- IBM AIX 7.1 TL4+
- IBM AIX 7.2
- Approximately 1.5 GB disk space in /opt, 2 GB is recommended

Solaris

- Approximately 1.5 GB disk space in /opt, 2 GB is recommended

Compatibility with Insite

To use 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 Powertech Antivirus with Insite

> **NOTE:** If you are installing on an RHEL system configured to use FIPS mode, skip to Installing or Updating Powertech Antivirus Manually below.

Insite allows you to easily install Powertech Antivirus on one or more endpoints with little manual configuration required. To do so:

1. Install 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 the Deployment Manager, choose ***NIX Servers**.
   - If you are adding a single server, click **Add**. Enter the required server information in the New *NIX Server pane and click **Save**.
   - To import multiple endpoints, create a CSV import file with the required server information. The import file should have 2 or 4 columns in format: hostname, alias, user, password (with fully qualified hostname and alias required). After you have created the import file:
     a. Choose **Import > Upload *NIX Servers**.
     b. Select **Choose File** to select the .csv file with the server information.
     c. Configure authentication details and click **OK**. See Upload *NIX Servers pane for more information.
3. In the Navigation Pane, choose **Products**.
4. In the Powertech Antivirus for AIX / Linux box, click **(Show Actions)** and select **Install**.
5. Select the servers and click **Add**. The servers begin receiving the endpoint install file. When that task completes, the endpoint is registered and then allowed with Powertech Antivirus.
6. In the Navigation Pane, go to **Powertech Antivirus** and select **Endpoints**. Check servers in the list to enable the available actions, which appear at the top of the screen. To set a selection of checked endpoints to automatically restart Powertech Antivirus after a reboot, choose **Enable Autostart**.

After you have installed, see Updating Virus Definitions to configure Powertech Antivirus to scan using the latest virus definition DAT files from McAfee.

Installing or Updating Powertech Antivirus Manually

Follow these instructions to install Powertech Antivirus on individual endpoints.

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. 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

Follow these instructions to install or update Powertech Antivirus with RPM.

To install or update on Red Hat (non-FIPS mode), 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.

> **NOTE:**
> If your RHEL system is configured to use FIPS mode, run the following command to install:
>
> ```
> rpm --install --nodigest --nofiledigest <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:

To completely remove Powertech Antivirus:

```
dpkg -P sgav
```

To remove Powertech Antivirus, but leave configuration files:

```
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                       ##################################################
```

Connecting Powertech Antivirus to Insite

Use the following procedure to connect Powertech Antivirus to Insite after manually installing Powertech Antivirus on an endpoint. In order to use Insite to monitor and manage endpoints, you need to register Powertech Antivirus on the endpoint using the Insite Integration Service.

1. Install 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.

   > **NOTE:** The Insite Powertech Antivirus Service is allowed automatically.

3. Copy your Insite Service API Key. To do so:
   a. Go to **Settings > Integration Service Admin**.
   b. For the key, choose (**Show Actions**) **> Copy**.
4. On the endpoint:
   a. Go to the Integration Service folder using command **`cd ptav-home/integration`** (`opt/sgav/integration` by default).
   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`

5. 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 allowed. Allowing an endpoint is required to indicate the endpoint should be allowed to communicate with the Insite server.

6. To approve the registered endpoint, click (**Show Actions**) **> Allow**. 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 allowed by checking the server and selecting **Allowed** at the top of the screen.

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

   NOTE: Each endpoint needs to be able to resolve to a domain name.

7. 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.

8. Repeat steps 2-7 for additional servers you would like to register and scan. See Using Powertech Antivirus with Insite for more details.

After you have installed, see Updating Virus Definitions to configure Powertech Antivirus to scan using the latest virus definition DAT files from McAfee.

> **NOTE:** See the Insite User Guide for more details on setting up and using Insite.

Licensing

After your purchase, you will receive an email from HelpSystems with your license code attached. You can apply the license directly to the endpoint, or add it using Insite. Using Insite allows you to apply a license to several endpoints simultaneously.

To manually license Powertech Antivirus directly on an endpoint

1. Rename the file to "license" (no extension).
2. Save the attached file to the /opt/sgav directory (or wherever the product was installed).

To license Powertech Antivirus endpoints using Insite

> **NOTE:** Licensing with Insite is a feature of Powertech Antivirus 5.4 and later.

1. Connect Powertech Antivirus to Insite.
2. In the Navigation Pane, click **Licenses**. The Licenses screen appears.
3. Click **Add**. The Add License dialog box appears.
4. Click **Choose File**. Navigate to the license file sent via email from HelpSystems.
5. Select the license file and click **Open**. Repeat the previous two steps for additional license files.
6. Click **Add**. The license file is added to the license list.
7. In the Navigation Pane, click **Endpoints**. The Endpoints screen appears.
8. Use the check boxes to select the endpoints you would like to license, and click **Allocate License**. The Allocate License dialog box appears.
9. Choose the license you would like to allocate from the License drop-down list, and click **Allocate**.

After You Are Done

Congratulations! Powertech Antivirus is now installed. Read the following for additional information regarding port configuration.

Port/Server Configuration

This is the mapping of the services 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 following port is used by Insite's Deployment Manager for product updates. It can be blocked when not in use.

- 22: SSH port

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

9001 on the Insite Analytics Service is used by:

- Allowed internal/corporate users
- Allowed external users
- The Insite Server

3030 on the Insite Server is used by:

- Allowed internal/corporate users
- Allowed external users
- The Insite Analytics Service

5432 on the Insite Database is used by:

- The Insite Server
- The Insite Analytics Service
- The Powertech Antivirus Service
- The Insite Integration Service

9092 on the Insite Message Broker is used by:

- The Insite Server
- The Insite Analytics Service
- The Powertech Antivirus Service
- Powertech Antivirus endpoints
- The Insite Integration Service

2181 on the Insite Coordinator port is used by:

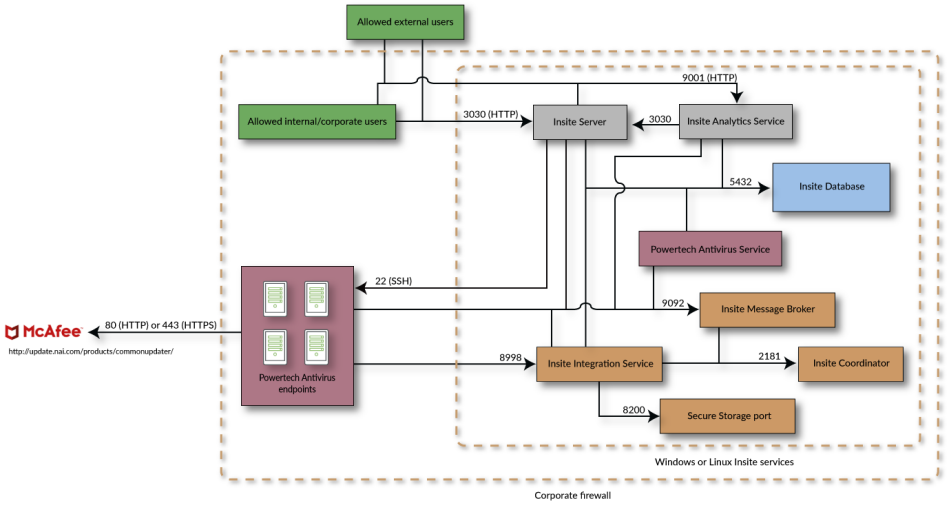
- The Insite Message Broker
- The Insite Integration Service

8023 (HTTP) on the Powertech Antivirus Service is used by the Powertech Antivirus endpoints when updating virus definitions via the DAT File Repository.

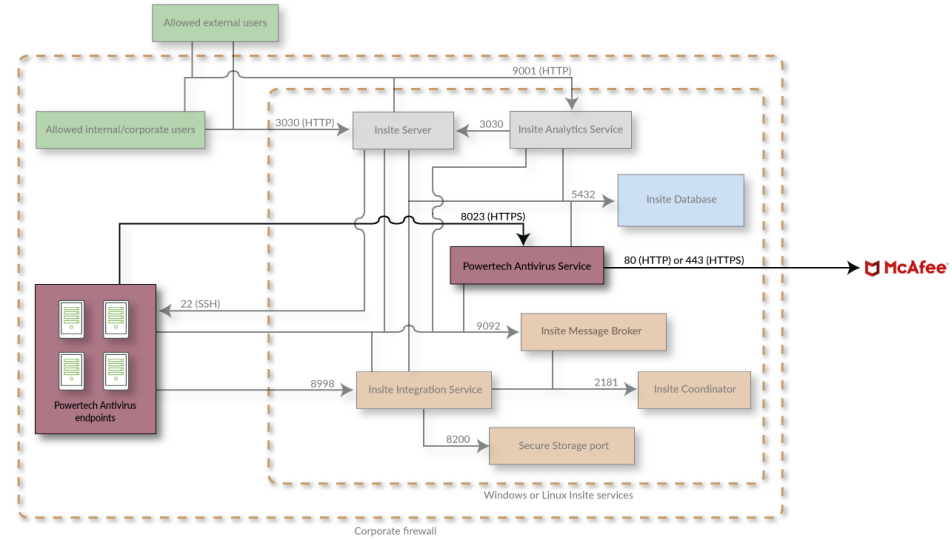
8998 on the Insite Integration Service is used by the Powertech Antivirus endpoints (initial registration).

8200 on the Secure Storage port is used by the Insite Integration Service.

Single Server Configuration (default)

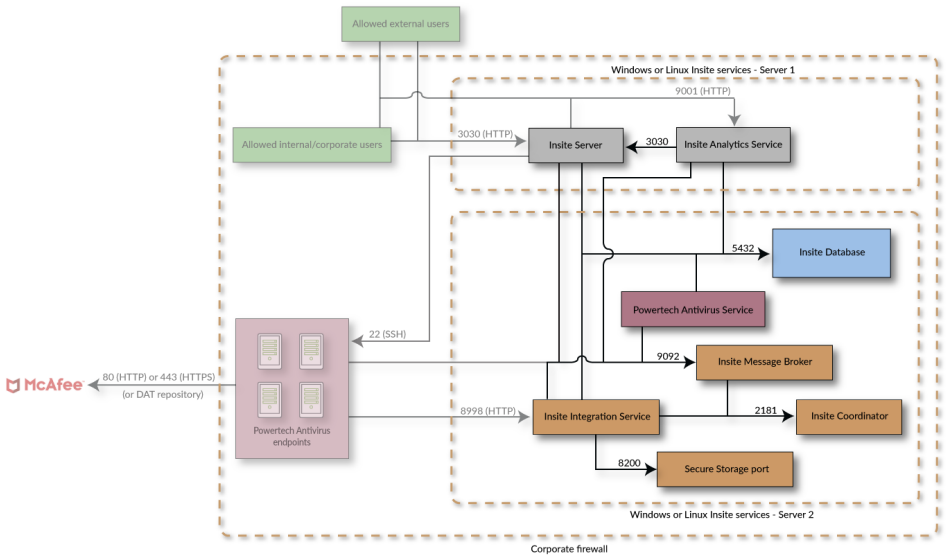


Single Server Configuration (DAT repository)



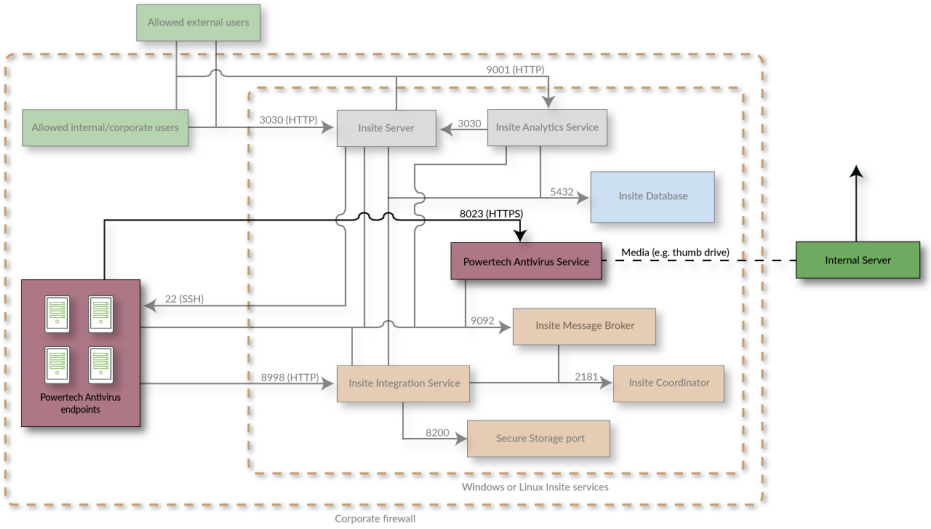
Dual Server Configuration

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



Air-Gapped Configuration

See also Updating virus definitions on air-gapped servers.



Contacting Us

For additional resources, or to contact Technical Support, visit the HelpSystems Community Portal at https://community.helpsystems.com.

Updating Virus Definitions

Virus Definitions (DAT files) from McAfee can be downloaded onto a single local server (DAT file repository) and deployed automatically or manually via HTTP or FTP to endpoints on your network via Insite. Insite also allows you to schedule updates and monitor the status of connected endpoints.

Endpoints without a connection to Insite can also be configured to acquire DAT file updates from the local repository. Virus definitions can also be transferred to an air-gapped server using physical media.

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

> **NOTE:** Powertech Antivirus validates DAT updates before endpoints are able to use them. For details, see DAT file validation.

Updating virus definitions using a local DAT file repository

This method of updating virus definitions allows you to update the latest DAT files onto a local server, and then use the Insite PTAV Service to distribute the DAT files to endpoints on your network via HTTP or FTP. Only the single server running the Insite PTAV Service needs access to McAfee for downloading DAT Files.

Install the Insite PTAV Service on the server you would like to use as the DAT file repository, and connect the endpoints you intend to scan. See Connecting Powertech Antivirus to Insite for details on installing and connecting Insite, and adding endpoints. See also Port/Server Configuration for port mapping details.

Once configured, the status of endpoints can be monitored on Powertech Antivirus for Insite's Home screen.

The following instructions guide you through the process of:

- Configuring a local DAT file repository with automatic updates
- Configuring a signed Certificate Authority (if required)
- Updating DAT files on endpoints manually using Insite

To configure a local DAT file repository and schedule updates

1. Open Insite.
2. In the Navigation Pane, choose **Settings** to open the Powertech Antivirus Settings screen.
3. Toggle Virus Definition (DAT) Repository Common Settings to **On**. Set the frequency of updates and whether to automatically update endpoints.
4. Choose the type of file server:
   - If you intend to use an HTTP file server, toggle Virus Definition (DAT) Repository HTTP Service Settings to **On**. Then, set the maximum number of endpoints to be updated concurrently, and the port.
   - > **IMPORTANT:** The port specified for the HTTP service must be accessible by all endpoints.
   - If you intend to use an FTP file server, toggle Virus Definition (DAT) Repository FTP Service Settings to **On**.

     See also: Powertech Antivirus Settings screen.
5. Click **Save**.

You can use --ftp, --wget, --curl, or --avget to connect to the Insite PTAV DAT repository service. For example, the following can be used to update DAT files using the PTAV internal tool `avget` with self-signed certificates and the ptavrepo provided through Insite:

```
/opt/sgav/avupdate --ftp
ftp://yourusername:yourpassword@yoursite/downloads/av
/opt/sgav/avupdate --ftp --ptavrepo https://your-helpsystems-one-
host:21
/opt/sgav/avupdate --avget --ptavrepo https://your-helpsystems-one-
host:8023
```

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

Configuring a signed certificate authority for DAT file updates

By default, the PTAV Service uses a self-signed certificate to ensure secure TLS data transfer between the repository and endpoints. Alternatively, you can use your own trusted certificate issued by a third-party certificate authority (CA) to secure the DAT repository HTTP file server.

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

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

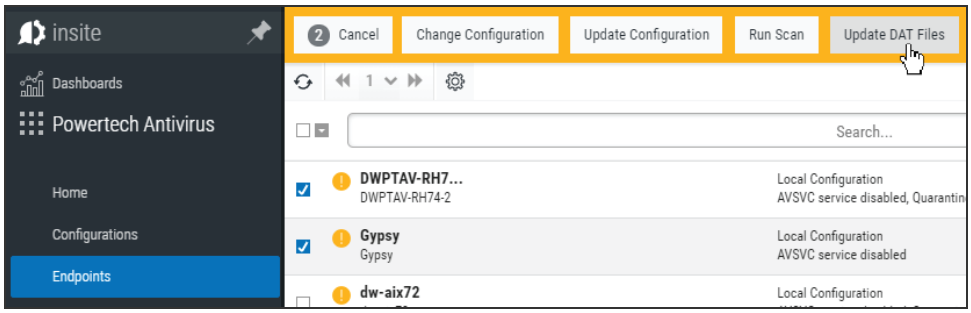
1. Locate your certificate and key files.
2. If the certificate and key both have ".pem" file name suffixes, rename the certificate to "cert.pem" and the key to "key.pem". (If the certificate and key file name suffixes are ".crt" and ".key", no file renaming is required.)
3. Place the certificate and key files into following folder, replacing the existing files:
    a. Windows: \Help Systems\HelpSystems Insite\PTAVService\certs
    b. Linux: /opt/insite/PTAVService/certs
4. Restart the Insite Powertech Antivirus Service.
    a. Windows: "InsitePTAVService"
    b. Linux: "HelpSystemsInsitePTAVServer"

To update DAT files on endpoints manually using Insite

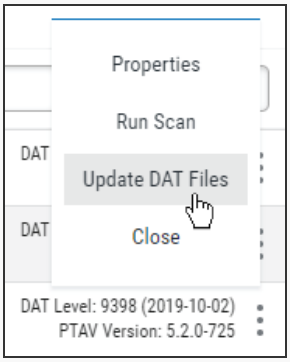
If you set the Powertech Antivirus Settings to update endpoints automatically when DAT files are available, connected endpoints will be updated automatically based on your settings. You can also use the following method to update DAT files on endpoints manually.

1. On the Powertech Antivirus navigation pane, click **Endpoints**.
2. Check the endpoints you would like to update.

3. Click **Update DAT Files**.



NOTE: Alternatively, to update a single endpoint, you can also choose **> Update DAT Files**.



Updating virus definitions from endpoints directly

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

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

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, and specify the current folder:

EXAMPLE:

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

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

Updating virus definitions on air-gapped servers

If an endpoint is not connected to the network, you can load the latest virus definitions using physical media such as a USB thumb drive. To do so:

1. Install Insite and the Powertech Antivirus module as described under Air-gapped Installation of Insite and Powertech Antivirus.
2. Create a new folder called `datimport` in `/opt/insite/PTAVService` if it does not exist already. During the DAT update procedure, before referring to McAfee for DAT updates, Powertech Antivirus first checks for the presence of this folder.
3. On a system with Internet access, download the latest virus definition (DAT) files from McAfee available at http://update.nai.com/products/commonupdater/. Save them to a tmp folder.
4. Copy the DAT files from the tmp folder to transferable media, such as a thumb drive. Once copied, the DAT files can be deleted from the tmp folder.
5. Copy the DAT files to `/opt/insite/PTAVService/datimport` on the air-gapped server.

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

6. Open Insite, and in the Navigation pane, choose **Settings**.
7. Click **Save** to process the files.
8. Open Insite, and in the Navigation pane, choose **Products**.
9. Select Insite Powertech Antivirus Service and click **Allow**.
10. Install Powertech Antivirus on the air-gapped server and register the endpoint in Insite. To use the Deployment Manager to install Powertech Antivirus on endpoints, copy the Linux and AIX license files to the Insite server for the endpoint deploy. See Installation.
11. In Insite, open Powertech Antivirus and choose **Endpoints**.
12. Select the endpoint and click **Update DAT Files**.

See also: Air-Gapped Configuration for a diagram of port mappings.

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 (on one line) to schedule the job to run every day at 6pm (18):

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

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.

Preparing to Scan

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

In this section you will learn:

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

On-Demand vs. On-Access scanning

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

Using On-Demand Scanning

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

This can be done in a few ways:

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

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

In order to run an On-Demand scan from Insite, you must:

1. Open Insite and create an On-Demand Configuration.
2. On the Endpoints screen, for an endpoint, check the endpoint and choose **Run Scan**.
3. In the Run Scan screen, choose the Configuration and then **Save and Run** or **Run**.

Using On-Access Scanning

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

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

On-Access scanning can be configured locally (on the UNIX endpoint) or using Insite.

Local configuration

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

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

Insite configuration

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

What should I scan?

As a Unix system administrator, you should know your own systems. If you don't know what filesystems are used for in your Unix system, then you should educate yourself and find out. Helpsystems cannot tell you what and what not to scan, we can only provide guidelines.

On-Access Scanning

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

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

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

On-Access Scanning with Insite

To use Insite for On-Access Scanning, first install Insite with the Insite PTAV Service, and connect the endpoints you intend to scan. See Connecting Powertech Antivirus to Insite for details on installing and connecting Insite, and adding endpoints.

To run On-Access scans using Insite

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

On-Demand Scanning

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

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

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

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

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

On-Demand Scanning with Insite

To use Insite for On-Demand Scanning, first install Insite with the Insite PTAV Service, and connect the endpoints you intend to scan. See Connecting Powertech Antivirus to Insite for details on installing and connecting Insite, and adding endpoints.

To run On-Demand scans using Insite

1. Open Insite and choose **Powertech Antivirus**. From the Navigation pane, choose **Configurations**. Review the On-Demand Configurations to confirm one exists that you want to use for your scan. See Configurations screen. To add a new On-Demand Configuration, choose **Add > On-Demand Configuration** and define one to meet your requirements. (See New On-Demand Configuration pane).
2. On the Insite Navigation pane, choose **Endpoints**.
3. Ensure the virus definition DAT files are up-to-date on the endpoints you want to scan. See Updating Virus Definitions.
4. Use the check box to the left of the endpoint listing to specify the endpoints you want to scan. Additional buttons appear on the top of the screen with a yellow background.
5. Click **Run Scan**. The Run Scan screen appears.
6. For On-Demand Configuration, select the desired Configuration and choose **Run** to run the scan. If you would like to change the Configuration settings prior to running the scan:
    a. Make the desired Configuration changes.
    b. Click **Save and Run**. The Save Configuration page appears. The new settings will be saved as an additional Configuration, or will be overwritten.
    c. Change the name. If you do not change the name, you will be prompted to overwrite the chosen Configuration with your new settings.
    d. Click **Save and Continue** to save the new Configuration and run the scan.

Scheduling updates and scans

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.

> **NOTE:** You can use Insite to schedule virus definition updates on connected endpoints. See Updating virus definitions.

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
> ```

Managing Quarantined Files

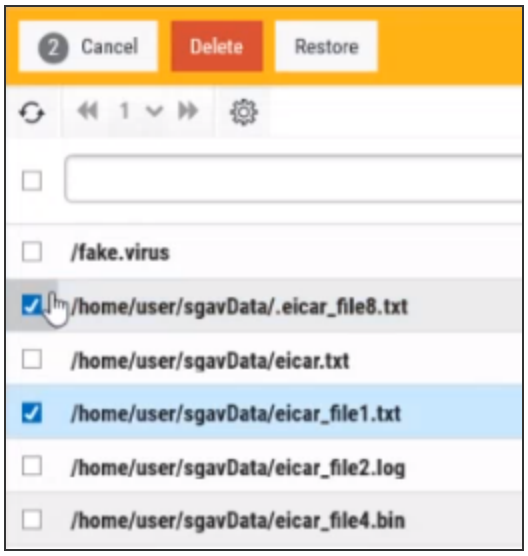
Powertech Antivirus allows you to easily view and manage files that have been quarantined as a result of On-Demand Scanning or On-Access Scanning.

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

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

To view, delete, or restore quarantined files

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



4. Choose **Delete** to remove the selected files, or **Restore** to replace them to their original location.

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

Notifications

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

Notifications can also be set up using Configurations in 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*’”
    - Based on the value "maxwait=<value>"
- virus
  - “VIRUS: '*file*’ is INFECTED with *virus*”
    - EICAR files will trigger this.
    - Note that Powertech Antivirus only sends this event when a virus is detected, and not when access is granted to it through a cached result (i.e. you will *not* see it for the log message “VIRUS granted access to infected file ‘/*file*’”).
- quarantine
  - “quarantined file *file*”
    - Based on the value "cleanfail=quarantine"
- delete
  - “file *file* deleted”
    - Based on the value "cleanfail=delete"
- repair
  - “Infected file ‘*file*’ *[action] (code [code])*”

Notification Action

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

The following environment variables will be available at runtime:

`PTAV_HOME`

The product installation directory.

`PTAV_VERSION`

The version of the antivirus software.

`PTAV_ENGINE`

The antivirus engine version and database level.

`PTAV_DAT_AGE`

The age, in days, of the antivirus database.

`PTAV_NOTIFICATION`

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

Examples

To revert to product defaults:

```
avconfig -C
```

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

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

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

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

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

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

Security

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

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

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

See Also

avconfig command

Reporting

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

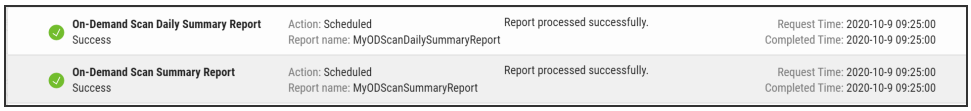
Creating reports

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

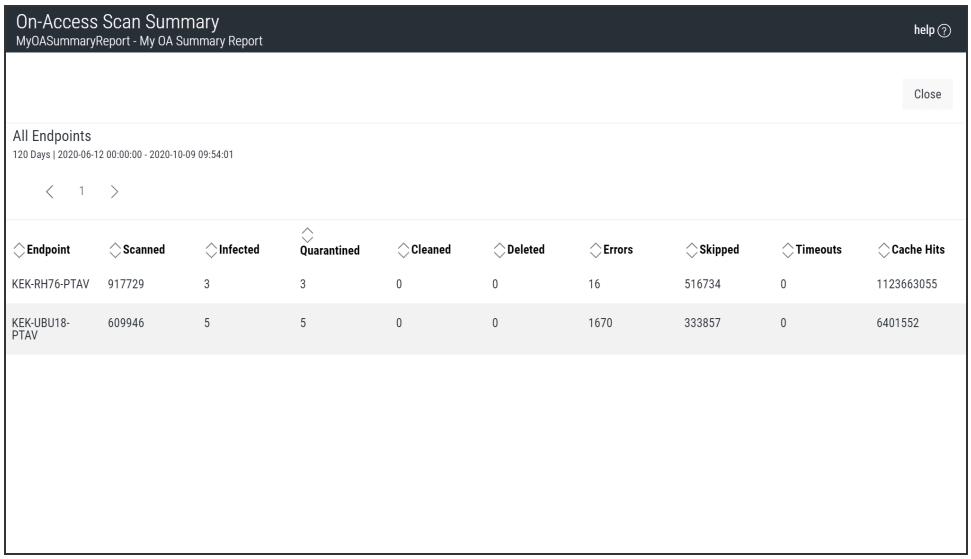
   > **NOTE:** In order to deliver reports to the email addresses specified in the recipients list, an email server must be configured on the Email Settings screen.

3. Click **Save**. The Reports screen appears, which displays the newly created report, as well as any existing reports.

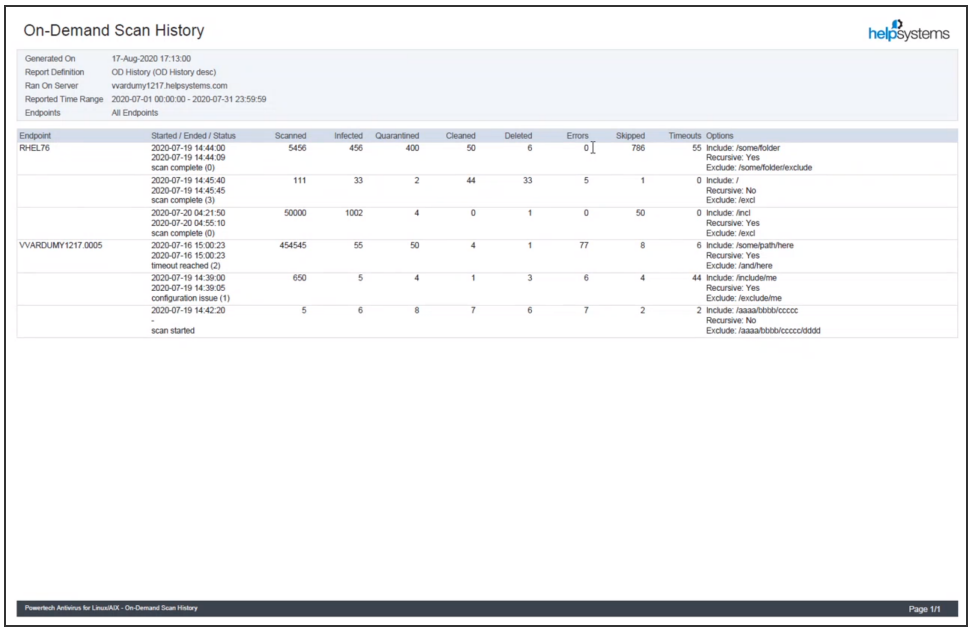
- You can track report generation using the Activity Status screen.



- To view the report output in Insite, on the Reports screen, click **(Show Actions) > View** for a report. You can use the arrows at the top of each column to change the sort order.



- Reports are delivered to the specified recipients over email as PDF attachments.



Powertech Antivirus and Insite

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

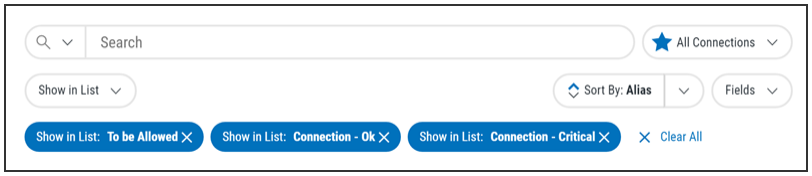
NOTE: To begin using Insite with Powertech Antivirus, see Insite Setup.

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 Insite, see the Insite User Guide.

Sort, Search, and Filter settings

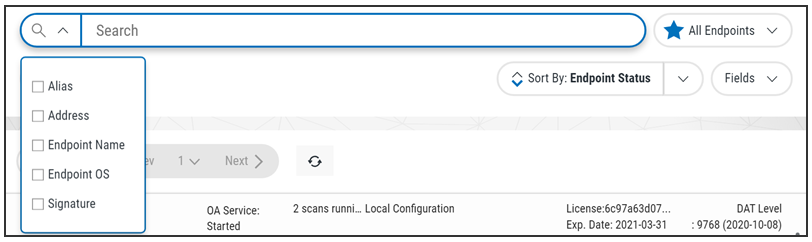
The Endpoints screen, Connection Settings screen, Activity Status screen, and Activity Details screen include settings that allow you to choose how to sort the existing list items, what type of data will be searched when you do a search, and how to filter the list.



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

[Search Filter Categories; Search]

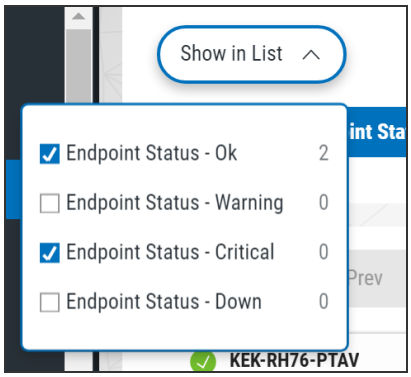
These settings allow you to define the categories you would like to search by, and submit the text search query.



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

Show in List

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



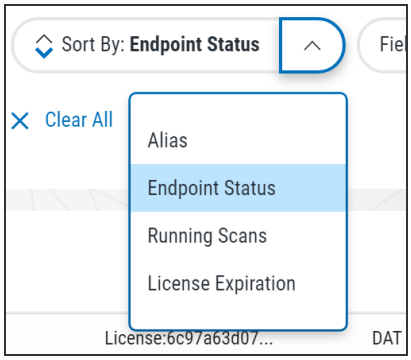
- Click **Show in List** to display a list of possible statuses (for example, the endpoint status or connection status).
- Check the statuses you would like to display in the list.

The status categories selected are shown as follows:

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

Sort By

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

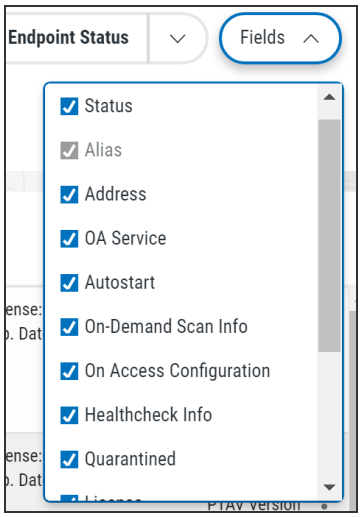


- Click ⌄ next to **Sort By:** ***[category]*** to sort the list by the chosen category.
- Click ⌃ or ⌃ to invert the sort order (from high-to-low or from low-to-high, respectively).

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

Fields

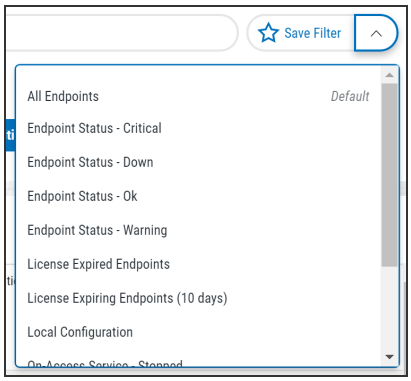
These settings allow you to specify the attributes of the row items you would like to show.



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

Save Filter

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



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

Navigation Pane and Select Products Pane

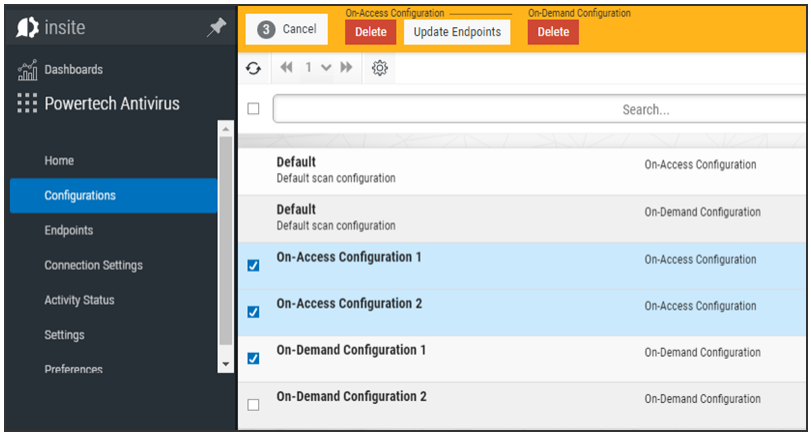
The Navigation Pane includes management tools for Powertech Antivirus. When open, it is located on the left side of your browser window.

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

Click  to open or close the Select Product Pane.

Selecting 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.
- **Allow.** Choose this option to allow the selected connections to indicate the selected endpoints should be allowed to communicate with the Insite server.
- **Block.** Choose this option to block 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 (On-Access only).** Choose **Update Endpoints** to restore the assigned Configuration settings. This could be used, for example, if settings have been changed directly on the endpoint itself that should be restored to match the Configuration settings assigned to the endpoint in Powertech Antivirus.

See 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

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.

NOTE: `Exclude` does not support wildcard characters.

```
threads
```

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

```
maxwait
```

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

```
delay
```

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

```
nice
```

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

```
clean
```

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

```
cleanfail
```

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

```
heuristic
```

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

```
macro
```

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

```
programs
```

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

```
archives
```

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

```
files
```

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

```
mime
```

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

```
mount
```

[Linux only] A colon-delimited list of mount points for filesystems that are to be monitored for on-access scanning. This option is for Linux only. 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'
```

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

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

On-Access Scanning can be started and stopped for endpoints, both individually and in groups, using Insite. For details, see On-Access-Scanning with Insite.

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

Name

`avsvcctl` - Powertech Antivirus service helper.

Synopsis

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

Description

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

Options

```
-j
```

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

```
status
```

Shows the running status of the anti-virus service.

```
statistics
```

Show scanning performance measures for the service.

```
log
```

Display the latest entries in the avsvc.log file.

```
install
```

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

```
uninstall
```

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

```
enable
```

Set the anti-virus service to start during system boot. Note that this will 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

avupdate

avscan

Exit Status

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

avsvcinfo command

Name

avsvcinfo - Query the anti-virus service.

Synopsis

avsvcinfo [-j | -r | -h]

Description

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

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

Options

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

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

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

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

`-h` Show this manual page.

See Also

avsvc

avsvcctl

Exit Status

The command returns 0.

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.

The avscan command scans the specified files and/or directories for viruses and malicious code. When an infection is found, prints a message to the output stream and the infected file remains unchanged. To have the command clean or quarantine infected files you need to specify either the `--clean` or `--quar` options (or both). Please note if a file cannot be cleaned it will be deleted unless the `--quar` option is also specified.

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

```
./avscan
```

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

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

You can use wildcards in file names:

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

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

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

Options

```
-r
```

Descends directories recursively.

```
--ignorelinks
```

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

```
--noignorelinks
```

Follow all symbolic links found during the scan.

```
--noheuristics
```

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

```
--nomacros
```

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

```
--pup
```

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

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

```
--mime
```

Scan for viruses in MIME-encoded files, UU-encoded files, XX-encoded files and BinHex files, and files in TNEF and IMC formats. This parameter reduces scanning performance. Default is to not scan these types of files so --mime will turn this feature on.

```
--arc
```

Scan within archives (.zip, .jar, .rar, etc). Many archive files (especially jar files) can drastically increase scanning time. You may want to scan archives on a weekly basis, for example. The default is not to scan within archives.

```
--noarc
```

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

```
--exeonly
```

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

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

Excludes the specified files and/or directories from scanning. If your exclude string contains wildcard characters you need to surround the string in quotes (i.e. --exclude "/excluded-file*")

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

NOTE: 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. It can be an integer value between 0 and 99999. The default is 300 seconds. A value of 0 disables the feature (files are scanned completely).

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

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

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

```
--delay <microseconds>
```

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

```
--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. This is the default.

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

Runs the specified command string when infections are found, passing the file name as a parameter. This allows a user-written script to perform actions such as alerting an administrator. 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 and administrator, for example. If the file remains after the command returns it will be deleted.

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

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

See Notification Support.

```
--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.

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).

```
--avget
```

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

```
--full
```

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

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

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

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

```
--passive
```

Runs the FTP process using passive mode.

```
--sscert
```

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

```
--force
```

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

```
--savepath <path>
```

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

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

```
--version
```

Prints the program version and build information, then exits.

```
--Path
```

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

```
--ptavrepo
```

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

Example:

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

A similar command could be employed from a command shell:

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

```
--help
```

Displays help text.

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

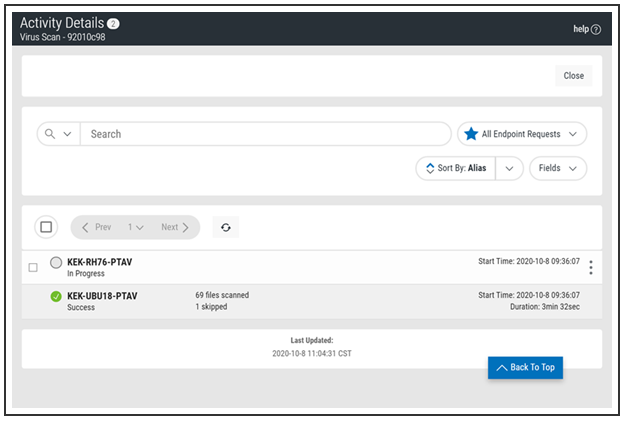
Insite Web UI

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

NOTE:

- To connect Powertech Antivirus to Insite, see Connecting Powertech Antivirus to Insite.
- See also Using Insite with Powertech Antivirus.

Activity Details screen



How to get there

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

Identifying the Activity Status

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

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

Successful. Indicates all items in the request ended successfully.

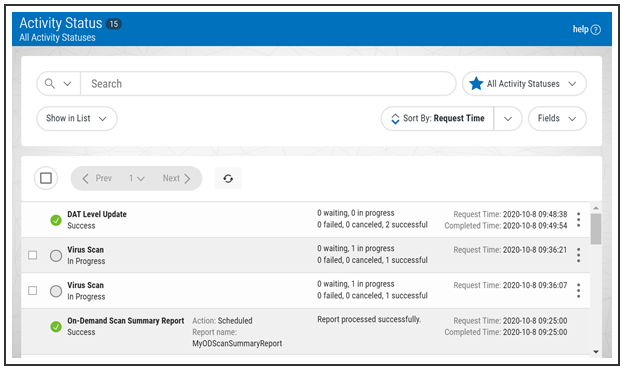
Canceled. Indicates endpoint scanning has been canceled.

Options

Close

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

Activity Status screen



How to get there

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

What it does

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

Identifying the Status

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

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

Successful. Indicates all items in the request ended successfully.

Canceled. Indicates the request has been canceled.

Options

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

(Show Actions)

Select this to show a menu with the following options:

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

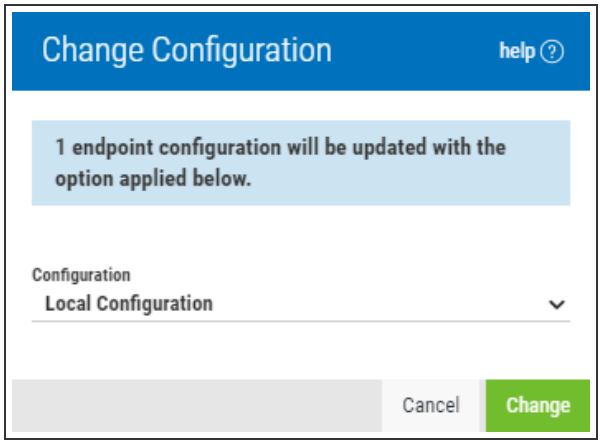
- **Rerun DAT Level Update on Failed Endpoints.** (DAT Level Update requests only) Choose this option to update all endpoints in the original DAT Level Update request that failed.
- **Rerun Config Update on Failed Endpoints.** (Configuration update requests only) Choose this option to send a new configuration update request for all endpoints in the original request that failed.
- **Rerun On-Access Service Configuration on Failed Endpoints.** (On-Access Service requests only) Choose this option to send a new On-Access Service Config request for all endpoints in the original request that failed.
- **Cancel Scan.** Click **Cancel** Scan to stop the scan.
- **Close.** Choose **Close** to dismiss the Actions menu.

Selected Requests

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

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

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.

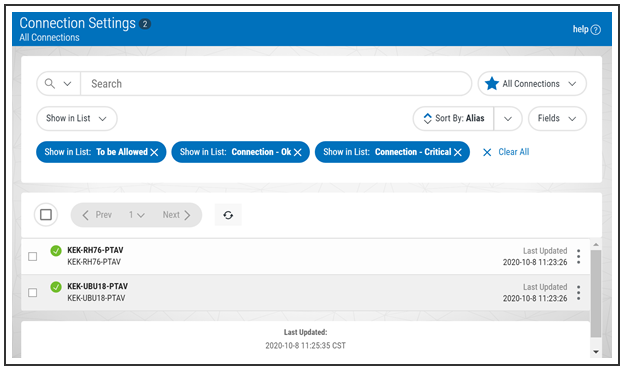
Configurations are collections of scan and notification settings that can be added and managed using the Configurations screen. You can use this drop-down to assign a Configuration to the endpoints. If you choose the Primary Configuration, a future change to the Configuration that is set as Primary will 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.

Connection Settings screen



How to get there

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

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

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 allowed. In order to communicate with Insite, the system must be allowed.

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

Blocked. The system has been blocked, indicating it is not allowed to communicate with the Insite server.

Options

[Advanced Search and Filtering options]

See Sort, Search, and Filter Settings.

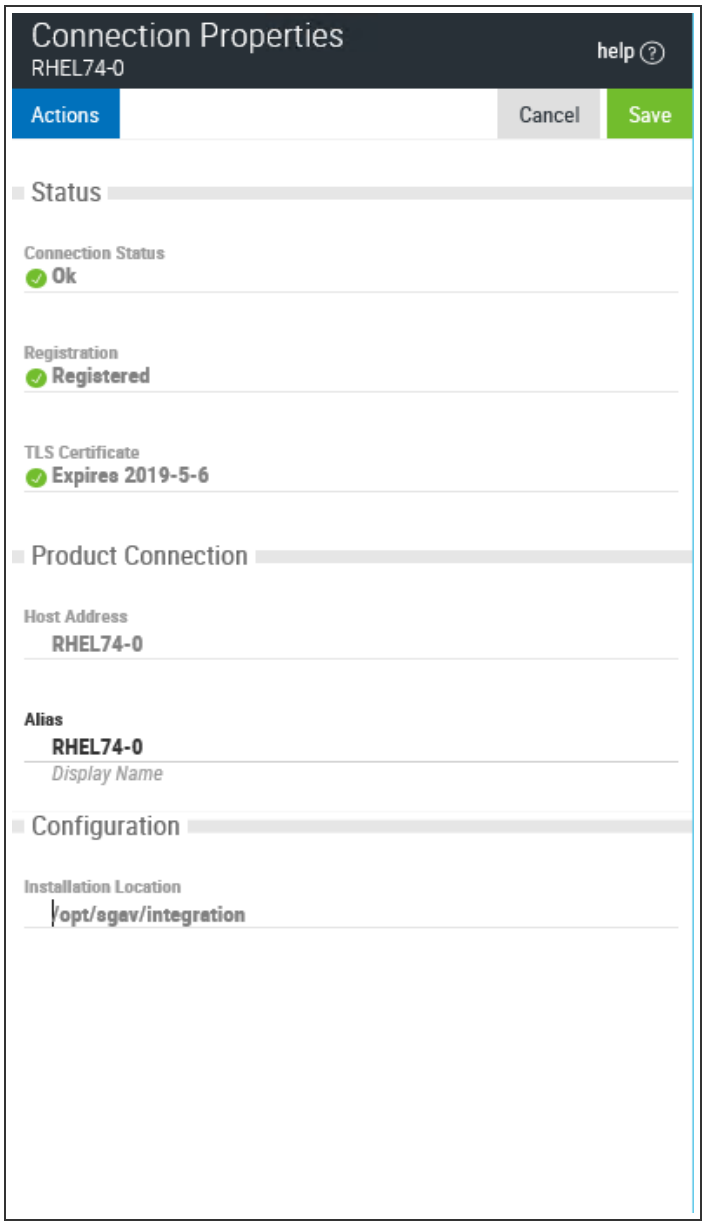
 (Show Actions)

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

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

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

- **Block.** Choose this option to block the connection, preventing communication with the Insite server.
- **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 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

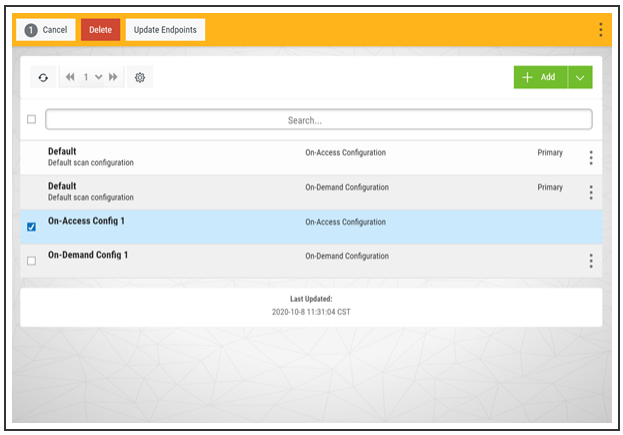
How the system is displayed in the connection settings list.

Configuration

Installation Location

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

Configurations screen



How to get there

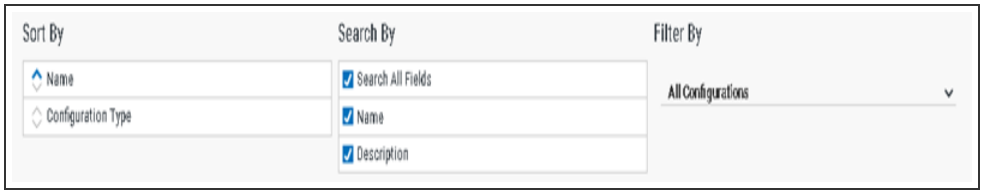
In the Insite Navigation Pane, choose **Configurations**.

What it does

The Configuration Screen allows you to add or update On-Access and On-Demand Configurations.

Options

Search



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

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

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

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

Searching

A search 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.

Add

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

(Show Actions)

Select this to show a menu with the following options:

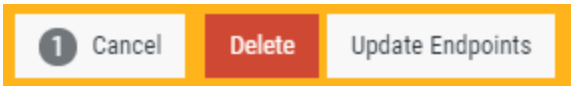
- **Properties.** Click Properties to open the New On-Access Configuration pane or New On-Demand Configuration pane, where you can update settings for the Configuration.
- **Update Endpoints (On-Access Only).** Choose this option to update the endpoint to restore the assigned Configuration settings.
- **Duplicate.** Choose this option to duplicate the Configuration.
- **Delete.** Deletes the selected Configuration. You are prompted to confirm.
- **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. If both an On-Access Configuration and On-Demand Configuration are included in your selection

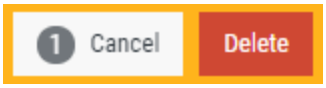
Selected Configurations

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.

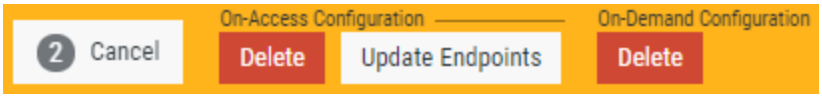
On-Access Configuration



On-Demand Configuration

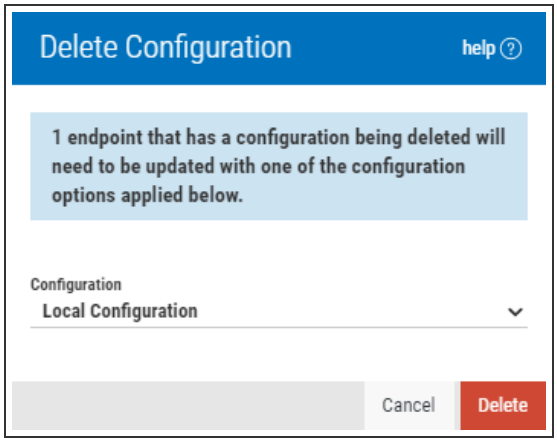


On-Access and On-Demand Configurations



In this scenario, the action taken applies only to selected Configurations of the type indicated.

Delete Configuration dialog box



How to get there

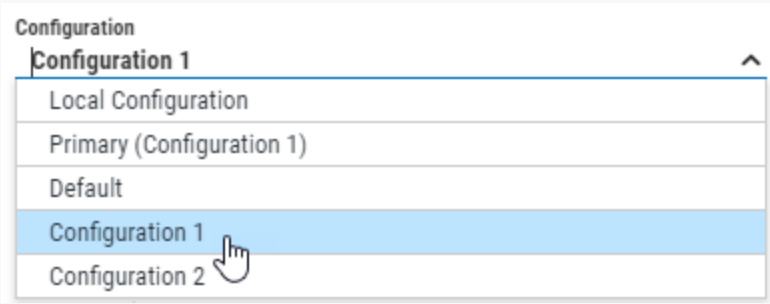
Select one or more Configurations on the Configurations screen and choose Delete. Or, delete a Configuration using the ⋮ Show Actions submenu.

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.



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.

Email Settings screen

How to get there

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

What it does

When a recipient's email address has been added to a report's definition (see New On-Access Report pane and New On-Demand Report pane), they can be sent a PDF of the report via email. Use these

settings to configure the required email settings.

Options

Enabled; Off • On
Toggle this switch to **Off** to disable email messages, or **On** to enable them.

Host
This is the host name of your email server.

Port
This is the port used by your email server.

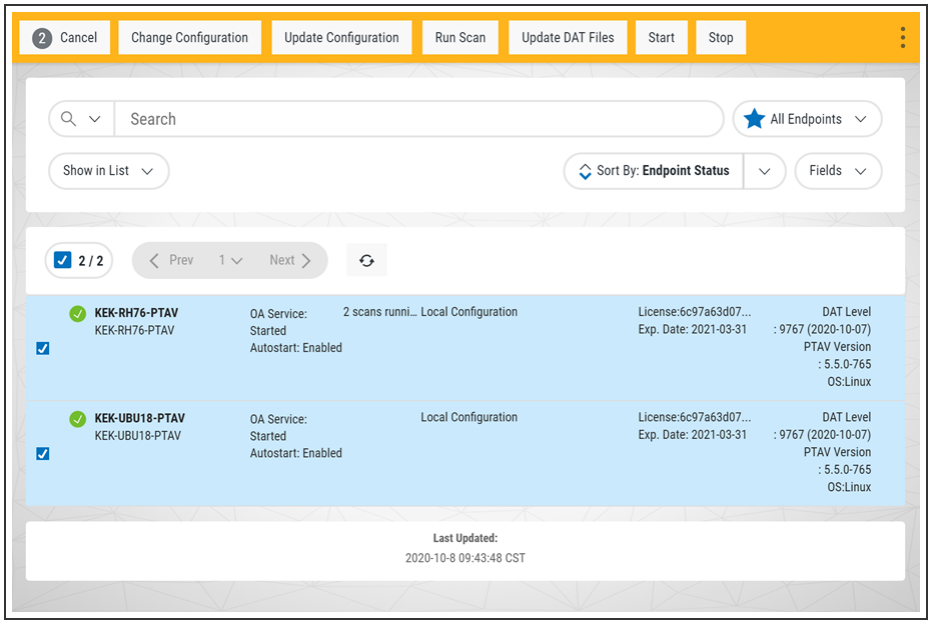
Use SSL/TLS with Email; Off • On
Toggle to **On** to secure email correspondence with TLS, or **Off** to disable TLS.

Sender Email Address
This is the email address that will appear in the "From" field of the recipient's message.

Server Requires Validation; Off • On
Toggle to **Off** to specify that server validation is not required. Toggle to **On** to enable the User Name and Password fields. Use these fields to specify credentials for your email server, if your email server requires a User Name and Password. Use the **Validate Email Connection** button at the top of the screen to test the connection.

Validate Email Connection
Use this button to test the email server connection. If the server requires validation, the specified User Name and Password is tested.

Endpoints screen



How to get there

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

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

What it does

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

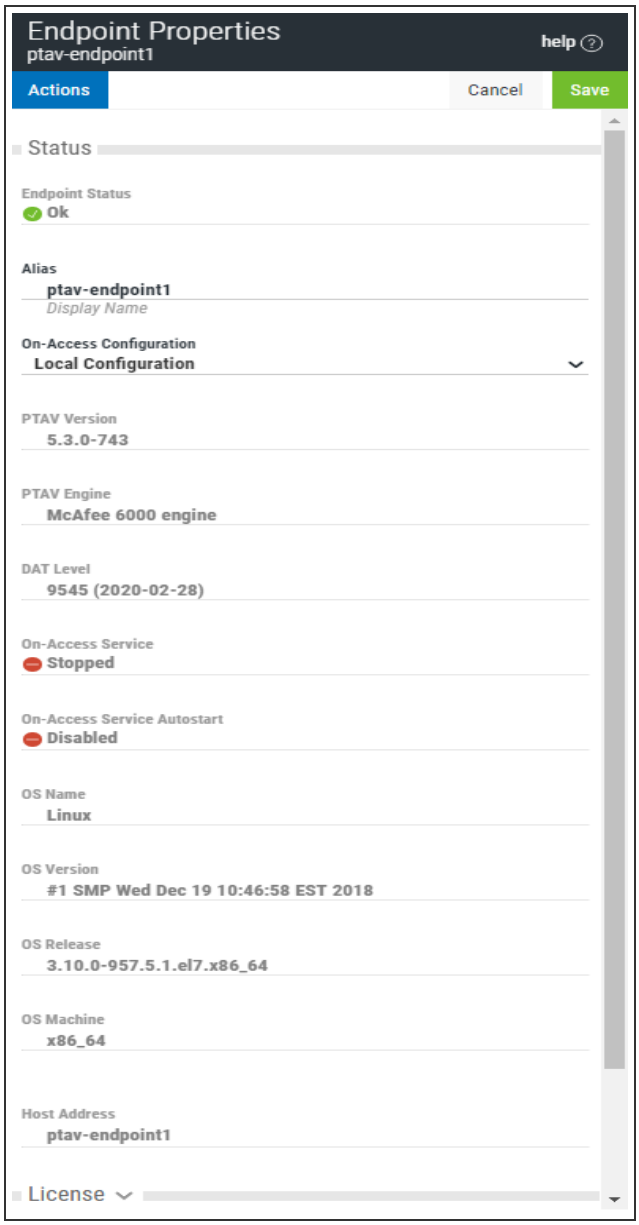
Select this to show a menu with the following options:

- **Change Configuration.** Choose this option to change the Configuration on the endpoint.
- **Update Configuration.** Choose this option to update the Configuration on the endpoint in order to restore the current Configuration settings.
- **Run Scan.** Opens the Run Scan screen, where you can make final adjustments to the Configuration being used and run the scan.
- **Update DAT Files.** Choose this option to update the virus definitions (DAT files) on the endpoint. See Powertech Antivirus Settings for more details.
- **Start.** Starts the On-Access service and performs and installs the anti-virus service control file into the system area if needed.
- **Stop.** Stops the On-Access service.
- **Enable Autostart.** Configures Powertech Antivirus to start on future reboots of the endpoint. Install is performed if needed.
- **Disable Autostart.** Configures Powertech Antivirus to not start on future reboots of the endpoint.
- **Restart.** Restarts selected endpoints. Selected endpoints that are not running are also started. Install is performed if needed.
- **Manage Quarantine.** If quarantined files exist for an endpoint, this option is available. Choose this option to open the Quarantined Files screen, where you can view and manage quarantined files.
- **Allocate License.** Choose this option to allocate the license to the selected endpoint.
- **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 same options described above appear in a yellow Show Actions menu bar at the top of the screen. This menu bar allows for changes to multiple endpoints simultaneously.

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 license information, modify the endpoint alias, and perform additional actions.

Field Descriptions

Status

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

Alias

How the system is displayed in the endpoint settings list.

Configuration

Configurations are collections of scan and notification settings that can be added and managed using the Configurations 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.

PTAV Version

The version of Powertech Antivirus installed on the endpoint.

PTAV Engine

The McAfee scan engine used for virus scanning.

DAT Level

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

On-Access Service

Current status of the On-Access Service.

On-Access Service Auto-Start

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

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

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

License

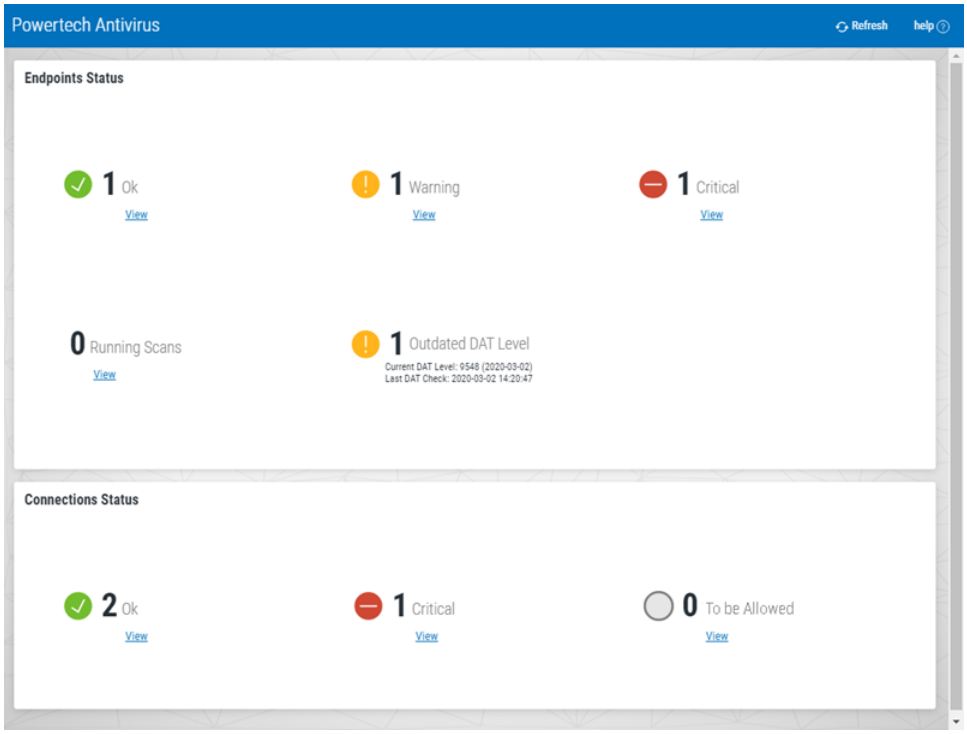
Displays endpoint license information as shown on the License Properties pane.

Options

- **Run Scan.** Opens the Run Scan screen, where you can make final adjustments to the Configuration being used and run the scan.
- **Update DAT Files.** Choose this option to update the virus definitions (DAT files) on the endpoint. See Powertech Antivirus Settings for more details.

- **Start.** Starts the On-Access service and performs and installs the anti-virus service control file into the system area if needed.
- **Stop.** Stops the On-Access service.
- **Enable Autostart.** Configures Powertech Antivirus to start on future reboots of the endpoint. Install is performed if needed.
- **Disable Autostart.** Configures Powertech Antivirus to not start on future reboots of the endpoint.
- **Restart.** Restarts selected endpoints. Selected endpoints that are not running are also started. Install is performed if needed.
- **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.

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."

Running Scans

Indicates the number of scans that are currently running on connected endpoints.

Outdated DAT Level

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

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

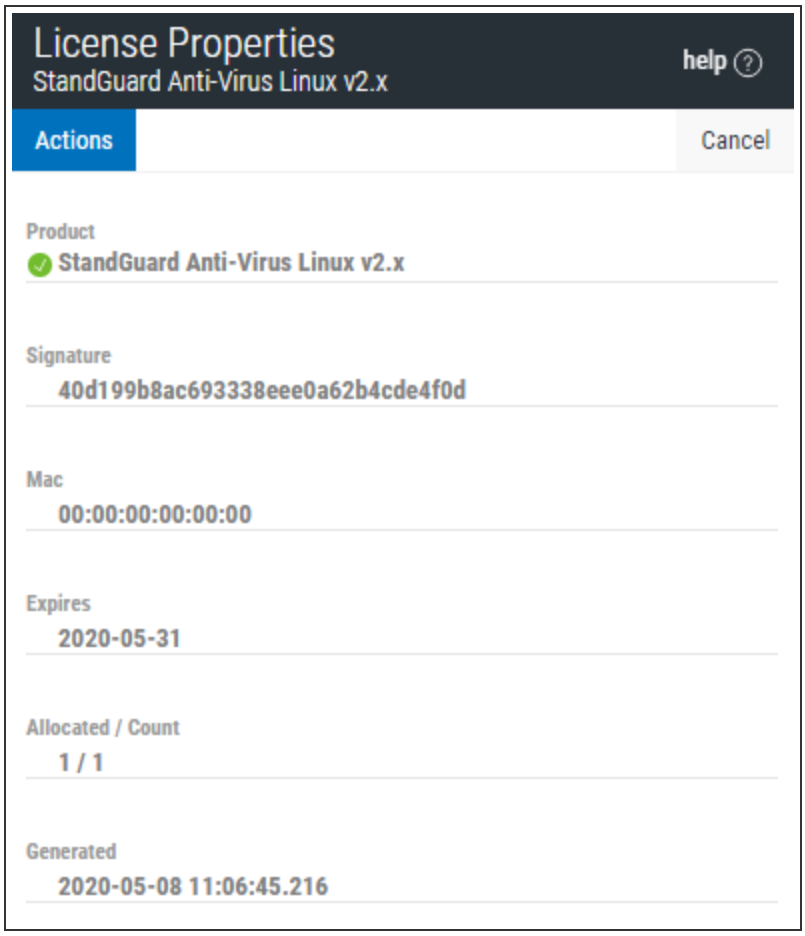
Options

Refreshes the Home screen with the latest status for connections and endpoints.

View

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

License Properties pane



How to get there

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

What it does

This screen displays information about the selected license, including information regarding legacy licenses.

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

Field Descriptions

Product

The name of the product and product version.

Signature

The first 10 letters of the license signature.

Mac

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

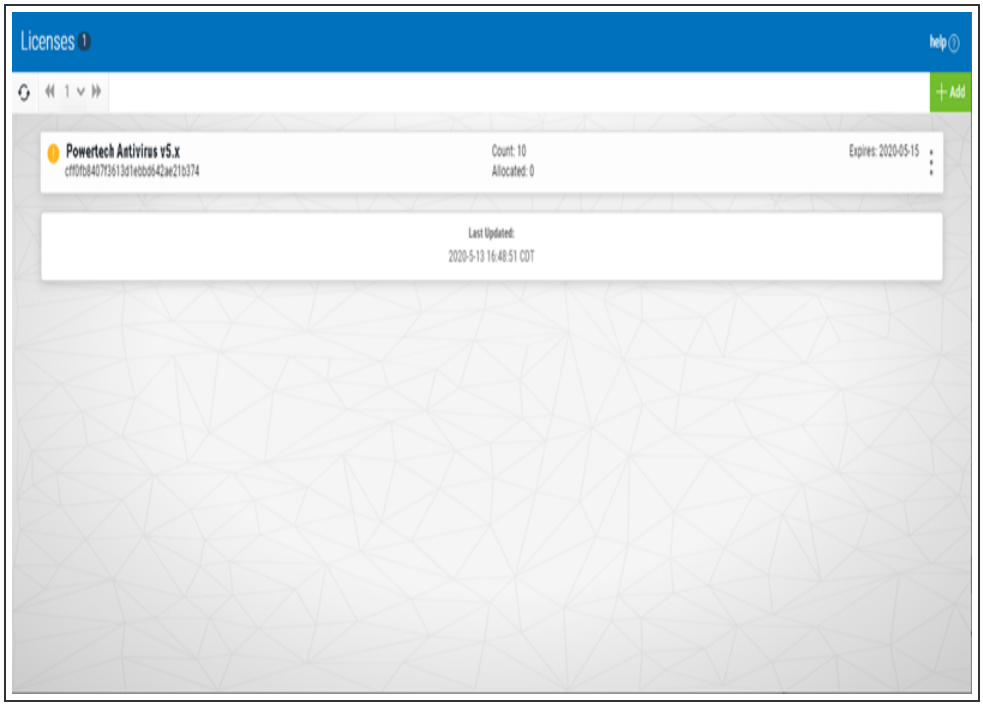
Expires

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

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

Logging/Diagnostics screen

To lear



How to get there
In the

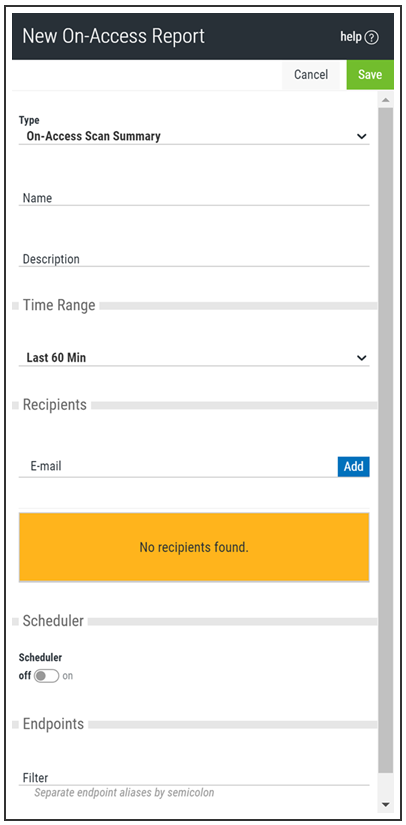
What it does
This screen displ

Options

A

New/Edit On-Access Report pane

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



How to get there

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

What it does

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

Options

Save • Cancel

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

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

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

Name • Description

A name and description for the report you are defining.

Time Range; Last 60 Min...Custom

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

Recipients; Email • Add

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

Scheduler; Off • On

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

Repeat; Monthly • Daily • Day of Week

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

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

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

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

  Select the days the report should run.

Time

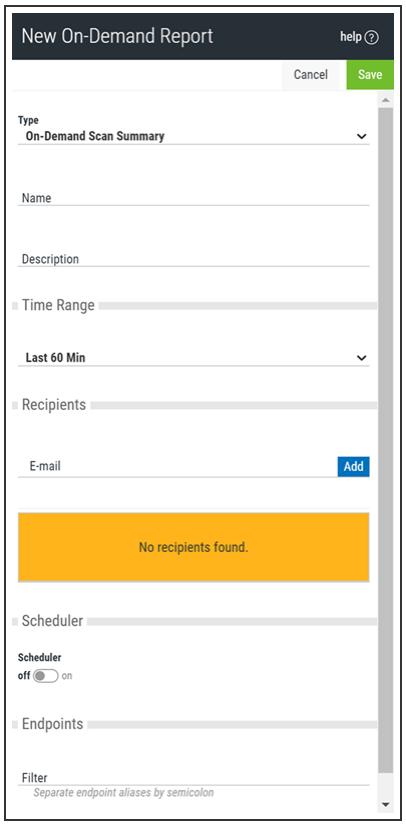
Click this field to specify the hour (0-24) and minute (00-60) of the day the reports should be generated and distributed. Use the arrows adjacent to the hour field to increment by hour. Use the arrows adjacent to the minute field to increment by five minute intervals.

Endpoints

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

New/Edit On-Demand Report pane

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



How to get there

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

What it does

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

Options

Save • Cancel

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

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

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

Name • Description

A name and description for the report you are defining.

Time Range; Last 60 Min...Custom

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

Recipients; Email • Add

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

Scheduler; Off • On

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

Repeat; Monthly • Daily • Day of Week

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

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

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

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

  Select the days the report should run.

Time

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

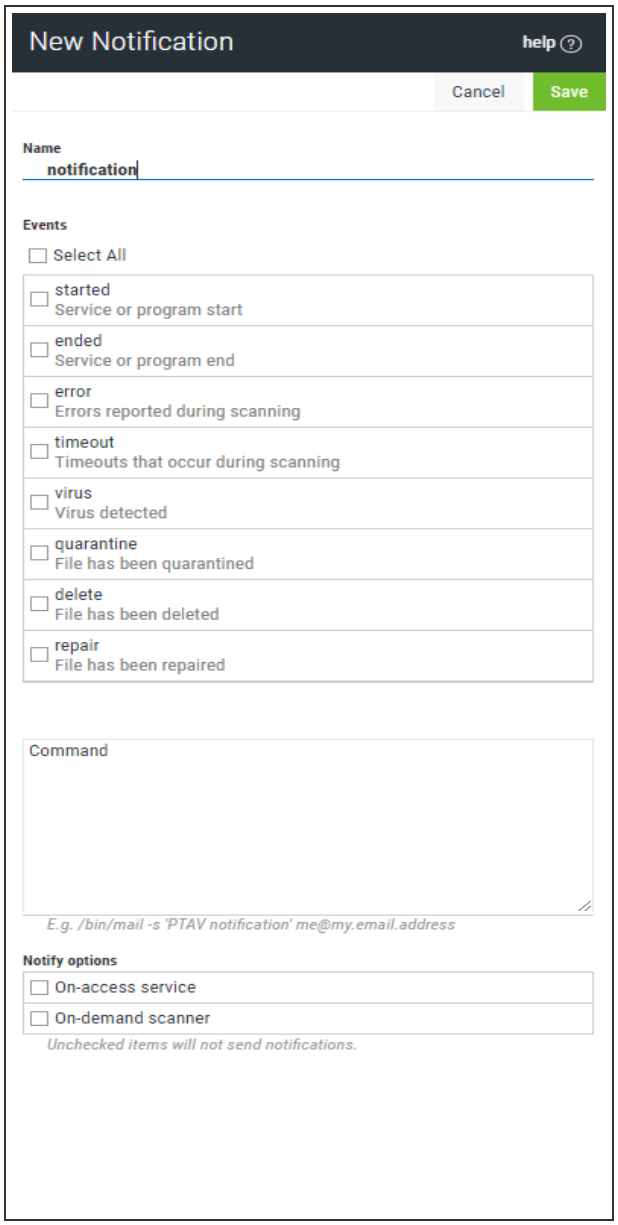
Endpoints

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

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

From this list, choose how the report details should be sorted. Choose **Endpoint** to sort alphabetically by endpoint alias. Choose Scan Started Timestamp to sort chronologically, from earliest to latest based on the timestamp of each scan. Choose Status to sort based on each scan's reported status.

New/Edit 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.

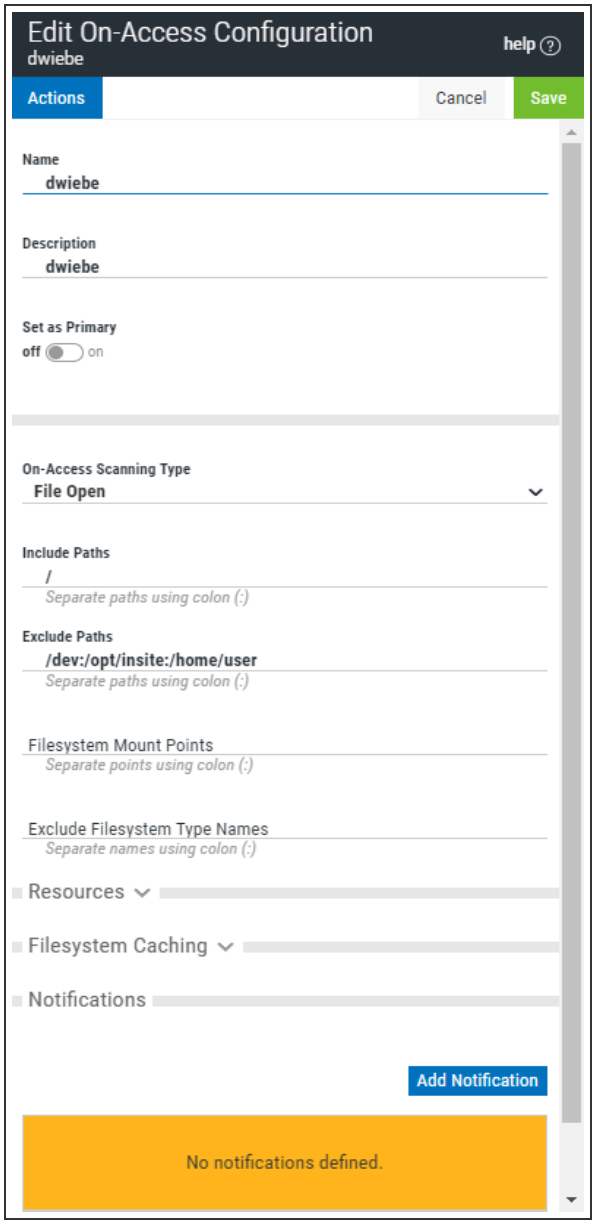
Events
Select one or more of the events in this list that will trigger the notification. These are the same options that can be selected using the avconfig command. See Notification Support.

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.

New/Edit/Duplicate On-Access Configuration pane



How to get there

- To create a new Configuration, on the Configurations screen, choose **Add > On-Access Configuration**.
- To create a new Configuration starting with the settings of an existing Configuration, on the Configurations screen, for an existing On-Access Configuration, click ⋮ **> Properties**.

- To edit an existing Configuration, on the Configurations screen, for an existing On-Access Configuration, click > **Properties**.

What it does

The New/Edit/Duplicate On-Access Configuration pane allows you to set configuration options, including notification settings, for on-access scanning.

Options

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

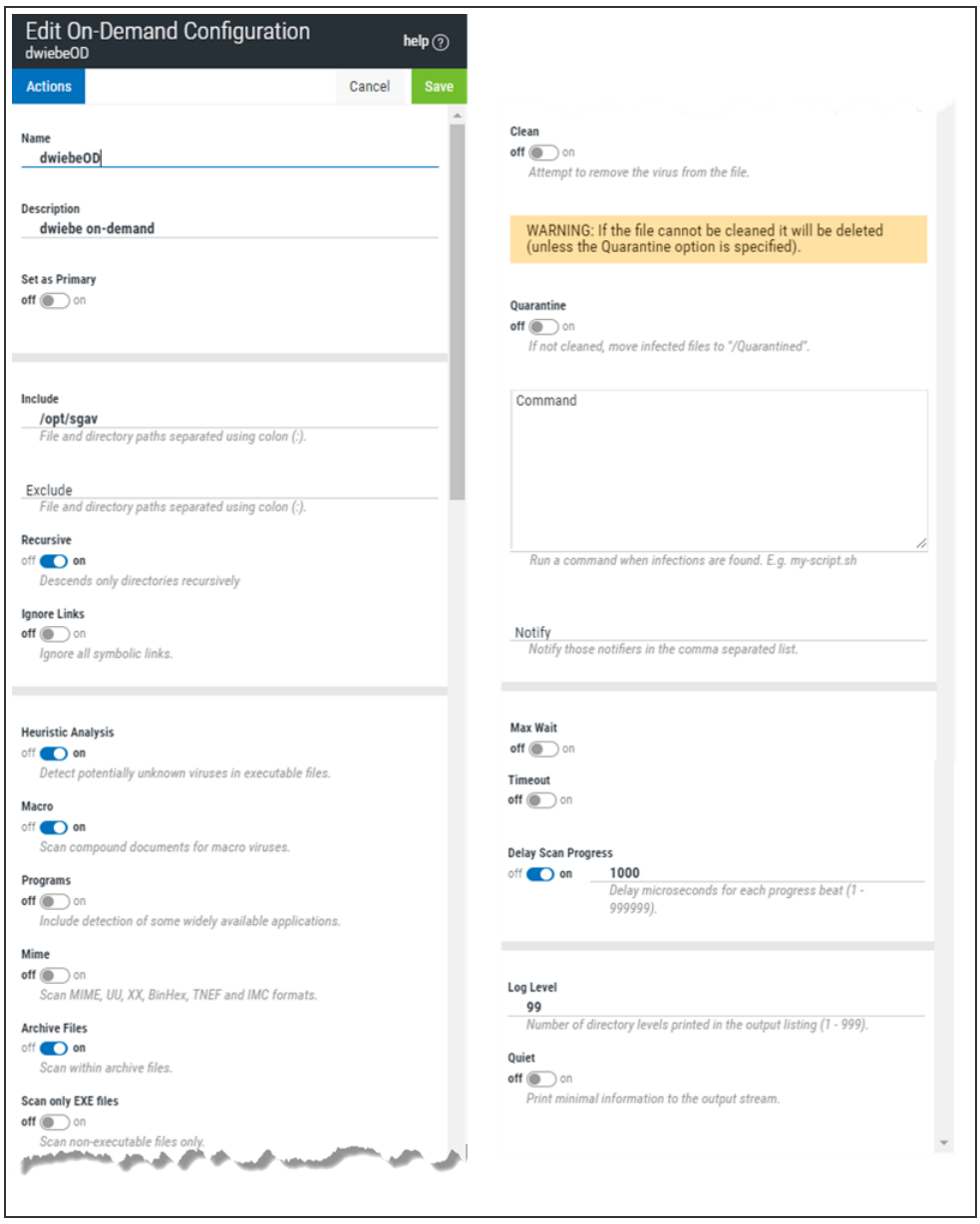
Choose this option to open the New/Edit Notification pane, where you can define a new Notification.

(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.

New/Edit/Duplicate On-Demand Configuration pane



How to get there

- To create a new Configuration, on the Configurations screen, choose **Add > On-Demand Configuration**.
- To create a new Configuration starting with the settings of an existing Configuration, on the Configurations screen, for an existing On-Demand Configuration, click ⋮ **> Properties**.

- To edit an existing Configuration, on the Configurations screen, for an existing On-Demand Configuration, click > **Properties**.

What it does

The New/Edit/Duplicate On-Demand Configuration pane allows you to set configuration options, including notification settings, for on-demand scanning.

Options

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.

Include Paths

A required colon-delimited list of path names to be included for on-demand scanning. A file that exists within any of the path names specified will be subject to scanning unless the file path name is specified as an Exclude Path.

Exclude Paths

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

Recursive

If set to **On**, the scan descends the specified directories recursively. If **Off** is specified, the current directory is scanned without descending subdirectories.

Ignore Links

If set to **On**, the scan ignores all symbolic links. If **Off**, symbolic links are scanned.

Resources

Heuristic Analysis

Include heuristic analysis to find new viruses. If set to **On**, Powertech Antivirus employs heuristic technology to detect potentially unknown viruses in executable files (programs). If set to **Off**, the engine can only find viruses that are already known and identified in the current virus definition files.

Macro

If set to **On**, Powertech Antivirus treats embedded macros that have code resembling a virus as if they are viruses. This parameter is similar to Heuristic analysis but scans for new viruses in compound document formats; for example, Microsoft OLE formats such as Word documents. Of set to **Off**, embedded macros that have code resembling a virus are not treated as viruses.

Programs

If set to **On**, Powertech Antivirus detects some widely available applications, such as password crackers or remote access utilities that can be used maliciously or pose a security threat. If set to **Off**, these applications are not detected.

Mime

If set to **On**, Powertech Antivirus scans inside MIME-encoded files, UU-encoded files, XX-encoded files, and BinHex files. If set to **Off**, Powertech Antivirus does not scan inside these types of files. This parameter reduces scanning performance.

Archive Files

If set to **On**, Powertech Antivirus includes archive files. Archive files contain embedded files and usually end with one of the following extensions: .ZIP, .TAR, .CAB, .LZH, .JAR and .UUE. This option will also permit scanning of MSCompress files. If set to **Off**, archive file types are not scanned.

Scan Only EXE Files

If set to **On**, Powertech Antivirus scans executable files only. If set to **Off**, Powertech Antivirus does not scan non-executable files (.txt, etc).

Clean

If set to **On**, Powertech Antivirus cleans 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 Quarantine is **On**.

Quarantine

If set to **On**, Powertech Antivirus quarantines the infected files by moving them to the /Quarantined directory. When Quarantine and Clean are both On, Powertech Antivirus attempts to clean the file first, and if unsuccessful, moves the file to the quarantine directory. If they are both off, no actions are taken on infected files.

Command

Runs the specified command string when infections are found, passing the file name as a parameter. This allows a user-written script to perform actions such as alerting an administrator. 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
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.

Max Wait
Specifies the maximum number of seconds to spend scanning any one file. After the number of seconds has elapsed the product assumes the file is OK and proceeds with the next file. The default is 300. Use this option cautiously.

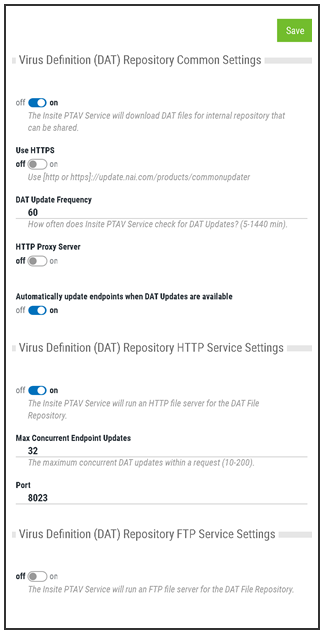
Timeout
Specifies the maximum number of seconds the scan will execute in total. After the number of seconds has elapsed, the command will end without scanning any remaining files. The return code will indicate a timeout has occurred.

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

Log 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.

Settings / Repository



How to get there

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

What it does

McAfee virus definitions (DAT file) updates can be applied to Powertech Antivirus endpoints from an internal DAT file repository using an HTTP or FTP file server. The file server is secured using TLS and runs in FTPS mode ensuring that data transfer is always secure.

This screen allows you to configure the Virus Definition Repository settings.

Options

Virus Definition (DAT) Repository Common Settings

Off • On

The Insite PTAV Service will download DAT files for internal repository that can be shared. **Off** disables the PTAV Service Repository. **On** enables it.

Use HTTPS; On • Off

When Powertech Antivirus's HTTP Proxy Server setting is on, you can toggle this setting to **On** to download virus definition DAT files using the secure HTTPS server offered by McAfee (https://update.nai.com/products/commonupdater). HTTPS uses Transport Layer Security (TLS) (formerly known as Secure Sockets Layer (SSL)) to encrypt the transaction.

When this setting is **Off**, and Use HTTP Proxy Server is on, Powertech Antivirus uses McAfee's HTTP server for DAT file downloads (http://update.nai.com/products/commonupdater).

DAT Update Frequency

This setting controls the frequency the Insite PTAV Service checks for DAT Updates, from 5-1440 minutes. Default is 60.

HTTP Proxy Server; On • Off

This option allows you to configure the DAT Repository McAfee download process to use a proxy server rather than directly accessing the McAfee Server. Set to **On** to use a proxy server and add the proxy server address (https://*dns_name* or *ip_ address*:*port*). Set to **Off** to configure Powertech Antivirus to access the McAfee server directly.

If you have configured the proxy server address and change the setting to Off, the address will be restored when turned On.

Automatically update endpoints when DAT Updates are available; On • Off

Set this to **On** to check for DAT file updates automatically at the frequency indicated above. Set to **Off** to disable automatic DAT file updates.

Virus Definition (DAT) Repository HTTP Service Settings

Off • On

If set to **On**, the Insite PTAV Service will run an HTTP file server for the DAT File Repository. **Off** disables the HTTP file server.

Max Concurrent Endpoint Updates
This is the maximum concurrent DAT updates allowed within a request (10-200). Default is 32.

Port
The port used for the DAT file server.

Virus Definition (DAT) Repository FTP Service Settings

Off • On
If set to **On**, the Insite PTAV Service will run an FTP file server for the DAT File Repository. **Off** disables the FTP file server.

By default, Linux prevents programs from accessing ports lower than 1024. To allow our FTP server to use port 21, run the following commands:

```
setcap CAP_NET_BIND_SERVICE=+eip /opt/insite/PTAVService/ptavsvc

modprobe ip_conntrack_ftp
```

Preferences screen

How to get there
In the Insite Navigation Pane for Powertech Antivirus, choose **Preferences**.

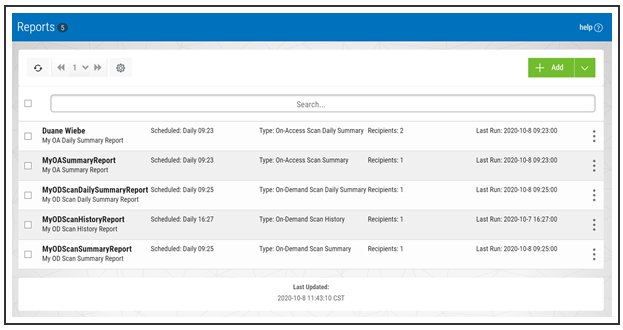
What it does
This screen allows you to configure the status and frequency of Powertech Antivirus's Auto-Refresh feature.

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.

Reports screen

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



How to get there

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

What it does

This screen allows you to add and manage Reports. The list of Reports includes the Report Name, Description, Scheduled info (if configured), Type, quantity of recipients, and date the Report was last run.

Options

Add; Add On-Access Report • Add On-Demand Report

Choose Add On-Access Report to open the New On-Access Report pane, which allows you to define a new On-Access Report. Choose Add On-Demand Report to open the New On-Demand Report pane, which allows you to define a new On-Demand Report.

(Show Actions)

Select this to show a menu with the following options:

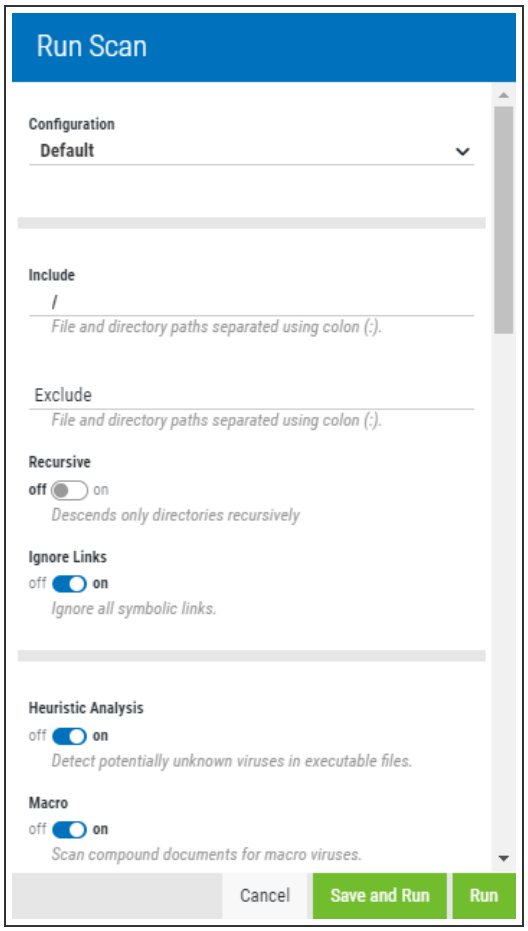
- **Properties.** Choose Properties to view the Edit On-Access Report pane or Edit On-Demand Report pane (depending on the type of report), where you can edit the report configuration.
- **Run.** Choose this option to run the report.
- **View.** Choose View to view the report output. This is the same data that appears in the respective PDF report delivered to the specified recipients (if any).
- **Delete.** Choose this option to delete the report from the database.
- **Close.** Choose **Close** to dismiss the Show Actions menu.

Selected Reports

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

- **Cancel.** Choose **Cancel** to dismiss the Show Actions menu.
- **Delete.** Choose this option to delete the selected reports from the database.
- **Run.** Choose this option to run the selected reports.

Run Scan screen



How to get there

In the Insite Navigation Pane, choose **Powertech Antivirus**, then **Endpoints**. On the Endpoints screen, for an endpoint, choose > **Run Scan**. Or, select one or more endpoints and select **Run Scan** from the options at the top of the screen.

Or, in the Endpoint Properties pane, click **Actions** > **Run Scan**.

What it does

These settings allow you to confirm your Configuration choices prior to running an On-Demand scan.

Options

Configuration
From this drop-down menu, choose the On-Demand Configuration you would like to use for the scan. When you choose a Configuration, its settings appear in the options below.

More details about the available Configurations can be found on the Configurations screen.

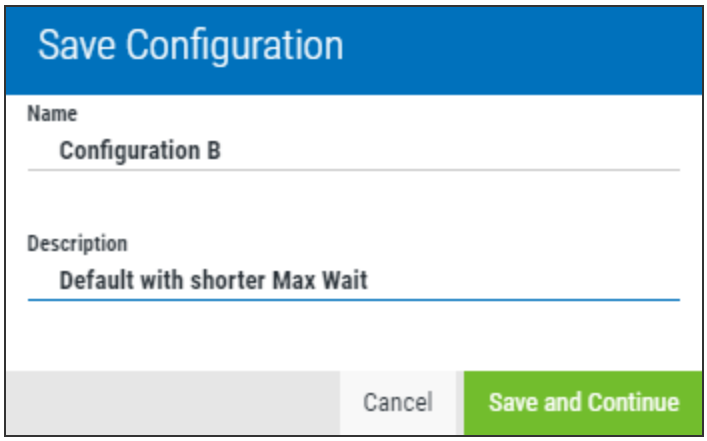
[Configuration Options]
The options in this section are identical to the options in the New/Edit/Duplicate On-Demand Configuration pane.

Run
Runs the scan on the selected endpoints using the Configuration options you have selected.

Save and Run
Opens the Save Configuration screen, where you can save your Configuration settings into a new Configuration record or overwrite the existing Configuration with the new settings.

Cancel
Choose this option to dismiss the Run Scan screen without running a scan.

Save Configuration screen



How to get there
On the Run Scan screen, click **Save and Run**.

What it does
This screen allows you to save a new Configuration record, or overwrite an existing one, using the settings from the Run Scan screen.

Options

Name • Description
This is the name and description of the Configuration to be saved. Upon arrival, these settings reflect what was previously selected in the Run Scan screen.

Save and Continue
Choose this option to save the Configuration. If you have not changed the name, you will be prompted to overwrite the existing Configuration. If you have changed the name, a new Configuration will be created using the new name and the existing Configuration will not be changed.

Cancel
Choose this option to dismiss the screen without saving a Configuration.

Appendix

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

Additional Information for Amazon Linux

Powertech Antivirus support and maintenance costs are calculated as a percentage of the total per instance cost of the deployment.

Powertech Antivirus is licensed per running copy of the Amazon Linux2 OS. Size or deployment model of the instance is not a factor.

> **NOTE:** In the case of an instance failure, a new EC2 instance must be created, the Powertech Antivirus RPM file must be re-installed, and the license applied as listed in the User guide. See Installation.

The links below will point to you frequently asked questions and additional information on deploying Powertech Antivirus in your AWS environment:

AWS Identity and Access Management

AWS deployment options

AWS disaster recovery information

AWS event handling

AWS region high availability

Auto scaling groups information

Availability Zone continuity information

Compare AWS support plan options

Creating security groups for your VPC

EC2 Instance type information (under "Instance types")

How to create IAM Aws roles

How to manage service limits on AWS

Information on AWS Certificate Manager

Information on AWS Limit Manager

Information on AWS encryption options

Mitigating AZ failures

Multi AZ deployment information

Planning for disaster recovery on AWS

Tracking status of your instances

Working with AWS credentials

Air-Gapped Installation of Insite and Powertech Antivirus

Use the following procedure to acquire, transfer, and install Insite and Powertech Antivirus on an air-gapped Windows or Linux server:

1. On a system with an Internet connection, download the following files and save them to transportable media (such as a thumb drive):
    a. The Insite installer file for your platform from the Insite Download Page
    b. The Powertech Antivirus installer file for your platform from the Powertech Antivirus Download Page
    c. "deployment.json" at https://hsinsite.s3.amazonaws.com/deployment.json
    d. "linux_deployment.json" at https://hsinsite.s3.amazonaws.com/linux_deployment.json
    e. Linux users: you also must download JRE and Postgres files from http://download.helpsystems.com/download/. During installation, Insite detects your OS and references the appropriate file from the "insite_install" folder within your installation folder. The files required depend on your OS distribution:

    JRE

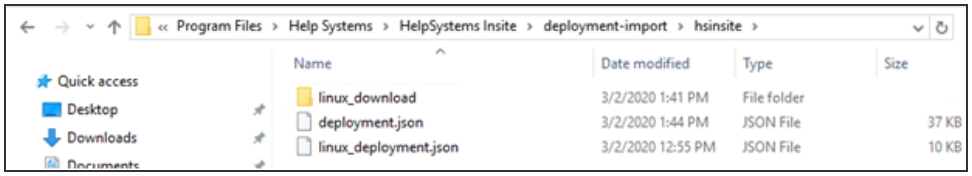
    - jre18_161-Linux-i686.tgz
    - jre18_161-Linux-ppc64.tgz
    - jre18_161-Linux-ppcle.tgz
    - jre18_161-Linux-x86_64.tgz

    Postgres Database

    - postgresql11_2-Linux-ppc64.tar.gz
    - postgresql11_2-Linux-ppc64le-suse-ssl1_1.tar.gz
    - postgresql11_2-Linux-ppc64le-suse.tar.gz
    - postgresql11_2-Linux-ppc64le-ubuntu.tar.gz
    - postgresql11_2-Linux-ppc64le.tar.gz

- postgresql11_2-Linux-x86_64-suse-ssl1_1.tar.gz
- postgresql11_2-Linux-x86_64-suse.tar.gz
- postgresql11_2-Linux-x86_64-ubuntu.tar.gz
- postgresql11_2-Linux-x86_64.tar.gz

2. Transfer the Insite installer to a temporary folder on the air-gapped server.
3. If you are installing Insite on Linux:
   a. Unpack the Insite installer using the following command:
      `tar -xzf insite_install.tgz`
   b. Place the JRE and Postgres files you downloaded into the "insite_install" folder (created when the install file is unpacked).
4. Install Insite, including the Powertech Antivirus module (an option within the Insite installation wizard). You can reference instructions for installing, licensing, and configuring Insite on the Insite download page.
5. Create the following folder:
   - Windows: `C:\Program Files\Help Systems\HelpSystems Insite\deployment-import\hsinsite\linux_download\sgav`
   - Linux: `/opt/insite/deployment-import/hsinsite/linux_download/sgav`
6. Save "deployment.json" and "linux_deployment.json" to the `hsinsite` folder you just created.



7. Copy the endpoint Powertech Antivirus installer file or files (e.g. "sgav-5.3.0-743.el7.x86_64.rpm") from your transportable media to the `sgav` folder you just created.
8. Open the following "web.properties" file in a text editor:
   - Windows: `C:\Program Files\Help Systems\HelpSystems Insite\lib`
   - Linux: `opt/insite/lib`
9. Change `use_filesystem_for_deployment=false` to `true` and save the file.
10. Restart Insite to use the new configuration files.

    Windows (`C:\Program Files\HelpSystems\HelpSystems Insite`):
    a. maintenanceStop.bat
    b. maintenanceStart.bat

    Linux:

    ```
    ./stopInsite.sh
    ./startInsite.sh
    ```

11. On Windows, open the Task Manager. Right-click "InsitePTAVService" and choose **Restart**. (The previous Linux commands restart the PTAV service automatically.)
12. Update the inbound firewall rules to ensure the ports selected during the installation procedure are open. Additional ports may need to be opened based on the Powertech Antivirus configured. For example:

- **8023** – HTTP Datrepo PTAV Service
- **21** – FTP Datrepo PTAV
- **22** – Insite Deployment Manager

13. See Updating virus definitions on air-gapped servers to acquire and load the most recent virus definition updates.

Configuring a Local Repository for Virus Definitions

A local repository allows you to scan a system without connecting to an outside port. If you suspect a system has been compromised, use a local repository to help ensure an infection remains contained.

To configure a local repository for virus definitions, follow these steps:

1. Download your repository.

   TIP:
   To manually download oem.ini and the virus definition archive package to your local server:
   a. wget -O oem.ini http://update.nai.com/products/commonupdater/oem.ini
   b. wget -N http://update.nai.com/products/commonupdater/*.zip
      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
   ```

DAT File Validation

DAT updates are validated by Powertech Antivirus before endpoints can use them, whether downloaded from McAfee or copied from the air-gapped "datimport" folder.

The validation method is triggered automatically once the download process has completed. A message is logged to indicate the validation routine is running.

If any errors are discovered:

- The folder in the datrepo that contains the invalid DAT files will be deleted.
- An error will be written into the datinfo file, which will then appear on the home page.
- The datinfo file will not be updated to reflect the download (i.e. the current, valid version will remain the "current" version in the file and will be used by endpoints).

- Information on the files that must be validated can be found in the "oem.ini" file as follows:
  - The "[AVV-ZIP]" section contains the name and md5 hash of the DAT update zip file (i.e. "avvdat-nnnn.zip").
  - The "[AVV-Incremental]" section contains the name and md5 hash of the file that contains information required for incremental updates (the file is generally called "gdeltaavv.ini" but we check for the filename here in case it changes).
  - The "[GEM-MD5]" section contains the name and md5 hash for every gem file that needs to be downloaded.
- The validation method reports an error under the following conditions:
  - The "oem.ini" file is missing.
  - The "avvdat.ini" file is missing.
  - The "avvdat-nnnn.zip" file is missing.
  - The md5 hash of the "avvdat-nnnn.zip" file is incorrect.
  - The incremental file ("gdeltaavv.ini" or whatever filename is specified in oem.ini) is missing.
  - The md5 hash of the incremental file is incorrect.
  - One or more gem files is missing.
  - The md5 hash of one or more gem files is incorrect.
- The validation method returns an error for the first error that it finds. It does not process further if an error has been found.
- If any unexpected files are found in the download folder, they are ignored.

More details:

- The validation routine is called both following an update from McAfee, or from the air-gapped "datimport" folder. A message appears in the log to indicate that the validation routine is running.
- If any errors are discovered when validating the download:
  - The downloaded folder is deleted.
  - An error is written into the datinfo file which then appears on the home page.
  - The datinfo file remains otherwise unchanged (i.e. the current and previous versions are unchanged; the only update is an error in the error field).
- The validation method reports an error under the following conditions:
  - The "oem.ini" file is missing.
  - The "avvdat.ini" file is missing.
  - The "avvdat-nnnn.zip" file is missing.
  - The md5 hash of the "avvdat-nnnn.zip" file is incorrect.
  - The incremental file ("gdeltaavv.ini" or whatever filename is specified in oem.ini) is missing.
  - The md5 hash of the incremental file is incorrect.
  - One or more gem file is missing.
  - The md5 hash of one or more gem files is incorrect.
- If any unexpected files are found in the download folder, they are ignored.

Syslog Configuration

Use the following information to configure Powertech Antivirus syslog logging.

Powertech Antivirus uses Zlog to send log messages to local logs and to mirror them to syslog. For information about the Zlog configuration file, see https://hardysimpson.github.io/zlog/UsersGuide-EN.html.

Log files are created in the/opt/sgav/log folder. If they are not, verify the following:

- The zlog.conf and zlog-avsvc.conf files exist
- The zlog.conf and zlog-avsvc.conf files can be read by the user
- The zlog.conf fileand zlog-avsvc.conf files do not contain typos that could cause the file to not be read correctly

NOTE: The destination for the syslog messages depends on the syslog configuration of the host. By default, it may be /var/log/messages or /var/log/syslog.

Logging levels

The following severity levels are used by Powertech Antivirus:

FATAL	Fatal conditions that will cause the product to stop running.
ERROR	Serious messages that cause the product to fail or stop working.
WARN	Important messages that should be looked at (e.g. virus infections, quarantine).
NOTICE	General startup and shutdown activity, completion messages.
INFO	Detailed messages, files not scanned, etc.
DEBUG	Debug trace.

You can set the syslog log level names to which these messages are sent in the zlog configuration files. By default:

- FATAL and ERROR messages are sent to syslog at level LOG_LOCAL3.
- WARN messages are sent to LOG_LOCAL4.
- NOTICE messages are sent to LOG_LOCAL5.
- INFO and DEBUG messages are not mirrored to syslog.

Zlog configuration for the avupdate and avscan tools are defined by the avupdate and avscan rules in zlog.conf. Changes will take effect the next time these tools are run.

The avsvc server uses the avsvc rules in zlog-avsvc .conf. Changes will take effect the next time the server is started or configuration is reloaded (“avsvcctl reload”).

Possible Syslog Messages

The following are the bodies of the Powertech Antivirus messages for levels FATAL, ERROR, WARN, and NOTICE, as they would appear with the default syslog formatting:

```
PTAV FATAL another instance of %s is already running
PTAV FATAL client initialization failed
PTAV FATAL configuration failed, exiting
PTAV FATAL driver write failure, errno %d %s
PTAV FATAL 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.