FORTRA

Powertech Antivirus
for IBM i
8.09

User Guide

Table of Contents

Welcome to Powertech Antivirus for IBM i

Welcome to Powertech Antivirus for IBM i – the award-winning native antivirus solution for IBM i. Developed with the unique features of IBM i in mind, Powertech Antivirus for IBM i offers all of the power and protection of the industry-leading Trellix scanning engine found on other platforms while meeting the specific needs of IBM i systems.

You'll find Powertech Antivirus for IBM i easy to use in either graphical or green screen modes and a breeze to keep current with the latest virus definitions directly from Trellix and software updates from Fortra. With Powertech Antivirus for IBM i, you have the essential tools to ensure that your IBM i system is protected from the threats of viruses, worms, and malware.

> **IMPORTANT:** Trellix was formerly known as McAfee.

Viruses and IBM i

Viruses stored on the IBM i present a serious risk to your network and your data. In most cases, your IBM i system can be "seen" by every computer in your network. If an infected file is executed by any of these computers, that computer becomes infected, which in turn can launch new attacks against the rest of the network and even back to the IBM i itself. These attacks can render computers and the network inoperable.

A running virus has access to all of the same resources as the user that launched the virus. Consequently, if an administrator-level user becomes infected then the virus has access to all the same resources as that user (everything). Viruses can alter, copy, delete, and run commands against IBM i files, programs and libraries. With respect to IBM i, a virus could spread to other systems and partitions through the use of network shares and the Integrated File System (IFS).

Many DOS and Unix commands will execute against an IBM i system. The DEL command, for example, can be used to delete files on a user's local C drive as well as IBM i files and libraries. Likewise, the COPY command can be used to copy files. A running virus can execute these and other dangerous system commands against a network drive mapped to the IBM i, causing serious damage. Viruses can also execute commands using FTP scripts, and access IBM i data via ODBC drivers stored on the infected computer.

There are many ways a virus can make its way to an IBM i: A mapped drive, the CD/DVD drive, an FTP script, sharing files and programs with other computers, vendors and business

partners are just a few examples. The best policy is to not try and "outguess" all of the possibilities – virus writers are always improving their code to take advantage of all the latest technologies.

How does the Trellix virus scanning engine work?

The Trellix virus-scanning engine is a complex data analyzer. The exact process of analysis depends on the object (often a file) being scanned and the type of viruses being sought. However, the following stages describe the general approach that the virus-scanning engine uses.

Identifying the type of the object

This stage determines which type of object is being scanned. Files that contain executable code, for example, need to be scanned.

Different types of files in Microsoft Windows systems, for example, are distinguished by their file extensions, such as .EXE and .TXT. However, any file can be renamed to hide its true identity, so the contents of the file must first be determined.

Each type of object requires its own special processing. If the type cannot be infected with a virus, no further scanning needs to be done. For example, a picture stored in a file of bitmap format cannot be infected.

Decoding the object

This stage decodes the contents of the object, so that the virus scanner "understands" what it is looking at. For example, a compressed Zip file cannot be interpreted until it has been expanded back to its original contents. The same applies to non-compressed files too. For example, the engine must decode a Microsoft Word document (.DOC) file to find any macro viruses.

File decoding can become quite complex when a file contains further encoded files. For example, a Zip archive file might contain a mixture of other archives and document files. After the engine decodes the original Zip file, the engine must also decode and separately scan the files inside.

Looking for the virus

This complex stage of virus scanning is controlled by the virus definition (DAT) files. The scan.dat file contains thousands of different drivers. Each driver has detailed instructions on how to find a particular virus or type of virus.

The engine can find a simple virus by starting from a known place in the file, then searching for its virus signature. Often, the engine needs to search only a small part of a file to determine that the file is free from viruses.

A virus signature is a sequence of characters that uniquely identify the virus, such as a message that the virus may display on the screen, or a fragment of computer code. Care is taken when choosing these signatures to avoid falsely detecting viruses inside clean files. More complex viruses avoid detection with simple signature scanning by using two popular techniques:

Encryption – The data inside the virus is encrypted so that antivirus scanners cannot see the messages or computer code of the virus. When the virus is activated, it converts itself into a working version, then executes.

Polymorphism – This process is similar to encryption, except that when the virus replicates itself, it changes its appearance.

Using heuristic analysis

Using only virus signatures, the engine cannot detect a new virus because its signature is not yet known. Therefore the engine can use an additional technique for heuristic analysis.

Programs, documents, or email messages that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients, or use other means to replicate themselves. The engine analyzes the program code to detect these kinds of computer instructions. The engine also searches for "legitimate" non-virus-like behavior, such as prompting the user before taking action, and thereby avoids raising false alarms.

By using these techniques, the engine can detect many new viruses.

Calculating the checksum

This stage exactly identifies the virus. The engine performs a mathematical calculation over the virus data to produce a unique number for the checksum. The engine compares this checksum against previously calculated values in one of the DAT files (scan.dat) to identify the virus exactly.

Cleaning

This stage cleans the object. Usually, the engine can clean an infected file satisfactorily. However, some viruses can alter or destroy data to an extent where a file cannot be fixed. The engine can easily clean macro viruses by erasing the macro from the infected document.

Executable viruses are more complex. The engine must restore the original path of execution through the program so that the virus does not become active. For example, a virus might append itself to the end of an executable program file. To run, the virus must divert the path

of execution away from the original code to itself. After becoming active, the virus redirects the path of execution to the original code to avoid suspicion. The engine can disable this virus by removing the diversion to the virus code. To clean the file, the engine then erases the virus code.

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.

Powertech Antivirus for IBM i Features

Powertech Antivirus for IBM i includes the following features.

Powered by Trellix

> **IMPORTANT:** McAfee is now Trellix.

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

- Scans within compressed files
- Decompresses and scans files compressed in packages such as PKZip, .LHA, and .ARJ
- Detects and cleans macro and script viruses
- Detects and cleans encrypted and polymorphic viruses
- Detects and cleans new viruses in executable files and OLE compound documents
- 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

Exit Program Integration

Powertech Antivirus for IBM i uses exit points to perform its job. See the IBM i Operating System Integration section. Starting in version 8.09, Powertech Antivirus for IBM i can share those exit points with other solutions.

See Overview of Exit Program Integration.

IBM i Operating System Integration

Supports IBM i Scanning Features

Starting with V5R3, IBM integrated virus scanning support into the operating system. Powertech Antivirus for IBM i fully supports these features. The result is better security and substantially lower overhead when compared to other platforms and file systems. The following table lists some of the ways the operating system has integrated virus scanning:

NetServer (mapped drives)	Files that are opened and modified from mapped drives are scanned for viruses. The operating system will not allow infected files to be opened, thus preventing a virus from spreading to other PC clients.
open()	The open() API is used by applications to open stream files in the IFS. IBM i can be configured to call Powertech Antivirus for IBM i to scan files before allowing them to be opened (on-access scanning). The operating system will not allow applications to open stream files that are infected with a virus.
Save (SAV) command	The SAV command is used to backup the files in the IFS. There are new parameters on the SAV command to specify if you want to scan files before saving to media, and if you want to save infected files (default is *NO).
Restore (RST) command	Files that are restored to the IFS (including vendor application files) will be marked as requiring a scan before they can be first used.
Copy (CPY) command	The CPY command is used to copy IFS files. The CPY command will not copy files that are infected with a virus.
Check Object Integrity (CHGOBJITG)	The CHKOBJITG command will report on any files in the IFS that have failed a scan.

System audit journal (QAUDJRN)	The system audit journal records virus scanning and cleaning activity.
System values (QSCANFS and QSCANFSCTL)	QSCANFS controls if virus scanning is enabled (default is ON). QSCANFSCTL provides options to tune scanning performance.
File-level scanning attributes	See following discussion

About IBM i File Scanning Attributes

Figure 1 shows the attributes of a file that has never been scanned. This information can be seen using the Work with Object Links (WRKLNK) command and then option 8 next to a stream file.
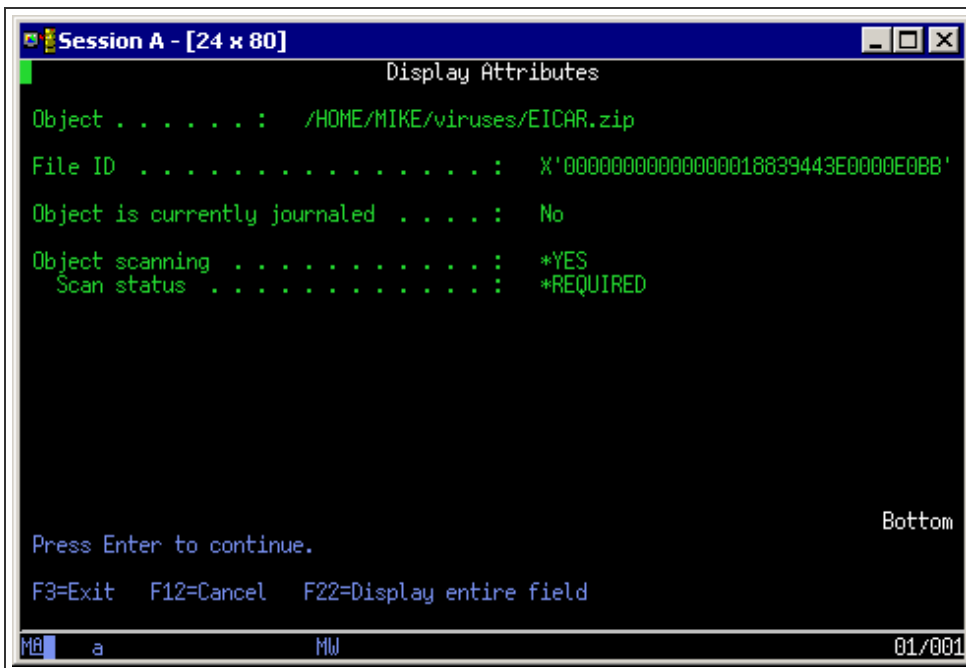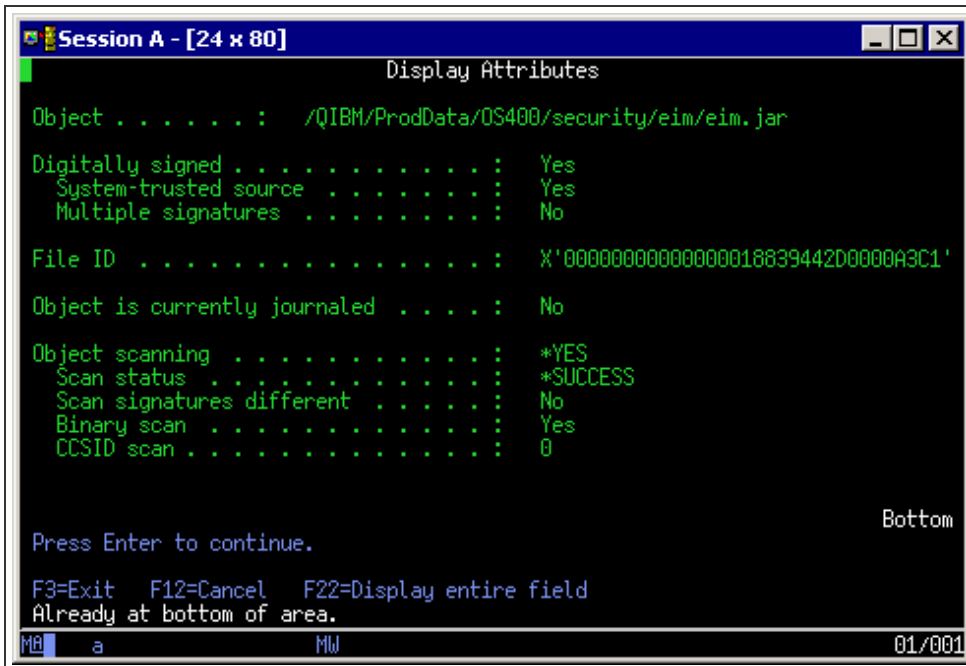
Figure 1. This screen shows attributes of a file that has never been scanned.

Press page down several times to see the scan information. In this example the file is enabled for scanning and the file will be scanned before it is next opened (Scan status = *REQUIRED). All files in the Root, QOpenSys and User-defined file systems have these default values.

Figure 2 shows the attributes of a file that has been scanned with Powertech Antivirus for IBM i. This file is not infected (Scan status = *SUCCESS) and the file will not be scanned again unless it is changed or the virus definitions are updated (Scan signatures different = No).

Figure 2. This screen shows attributes of a file that has been scanned.

When you run on-access scanning, Powertech Antivirus for IBM i knows not to scan this file because nothing has changed that would allow this file to be infected. The result is on most days a full system scan can run in minutes instead of hours or days. Think of it as a "scan changed objects" command.

Figure 3 shows the attributes of a file after a virus has been detected. Powertech Antivirus for IBM i has updated the >Scan status= to *FAILURE. The operating system logs the error in the system audit journal and messages are generated. Finally, IBM i will not allow any application to open or copy a file that has failed a scan.

Figure 3. This screen shows attributes of a file after a virus has been detected.

On-Access Scanning

Powertech Antivirus for IBM i provides real-time protection against virus threats by scanning files dynamically, as they are opened. You can separately enable on-access scanning for file server accesses (NetServer mapped drives, FTP) and 5250 environments (host-based applications, like Java, Websphere, etc).

The operating system uses the file scan information to avoid having to scan files that have not changed and have already been scanned (see discussion on the previous page). The result is the first user to open the file will wait for the scan, while subsequent accesses to that file (by that user or any other user) will not cause the file to be scanned again. Only when the file has changed, or when new virus definitions are updated, will the file be scanned again.

See On-Access Scanning.

On-Demand Scanning

Powertech Antivirus for IBM i provides on-demand scanning which allows you to scan all or part of the system at scheduled times. You can configure the directories to scan and the schedules at which to run the scan. This allows you to configure scanning to run during off-peak times to reduce the CPU impact on other applications. Once a file has been scanned using on-demand scanning, the file will not need to be scanned when accessed (no on-access overhead for that file) unless

the file has changed or the virus definitions are updated. This allows you to use off-peak times to "pre-scan" files that rarely change, thus reducing the CPU overhead of on-access scanning and improved balancing of scanning workload.

See On-Demand Scanning.

Anti-Ransomware

Powertech Antivirus prevents ransomware attacks by detecting and alerting system administrators of potential ransomware threats, and can also be configured to automatically take action when a threat is detected.

See Anti-Ransomware.

Scans Native Scanning SMTP Mail

Powertech Antivirus for IBM i can scan inbound and outbound email messages passing through the IBM i SMTP server. Powertech Antivirus for IBM i can perform virus scanning on emails before they reach your PC clients (or customers).

Object Integrity Scanning

Powertech Antivirus for IBM i scans the IBM i Operating System (and user libraries) for objects that have been tampered with and have the potential to cause serious harm to the operating system or bypass all security entirely. For more information about object integrity scanning, see Object Integrity Scanning.

Scans Files on Guest Operating System Partitions

Powertech Antivirus for IBM i can scan files on Linux and AIX guest partitions using the Network File System (NFS). By creating scheduled scan tasks to scan NFS mountable volumes on guest partitions, you can reduce the time, effort and costs associated with installing and configuring multiple stand-alone antivirus applications on each partition. A single installation of Powertech Antivirus for IBM i on the host partition can be used to ensure all of your Linux and AIX partitions are free of viruses, trojans, worms, malware and spyware.

Automatic Download of Virus Definitions

Powertech Antivirus for IBM i ensures you always have the latest protection against current virus threats by automatically downloading virus definition files from Trellix. By keeping the virus definition files up-to-date automatically, Powertech Antivirus for IBM i protects you from the new virus threats that occur each day. Automatic updating can be scheduled to run automatically, and CL commands are provided to integrate within your own nightly batch processes.

Built-in Scheduling

Built on Fortra's proven experience with IBM i administration, security, and automation, Powertech Antivirus for IBM i was designed from the ground up as a secure, automated antivirus solution that prevents headaches, not gives you new ones. Powertech Antivirus for IBM i provides automatic scheduling and updating of virus definitions, product enhancements, and scanning tasks that you create. By automating these tasks you can rest assured that Powertech Antivirus for IBM i is providing reliable, around-the-clock protection.

Network-Enabled

Powertech Antivirus for IBM i can retrieve virus definitions and program updates from either an HTTP server, an FTP server, or a shared local network path. The path can be located on another IBM i server or partition, a Windows file server, or any network path of your choice. This allows you to use one IBM i server or partition to download the virus definitions (from Trellix's HTTP server) and the remaining servers or partitions can retrieve their virus definition files from the shared network folder.

Logging

Powertech Antivirus for IBM i provides several logging features that you can use to monitor the application's activity:

- Messages are logged to the message queue AVMSGQ. You can view the message queue manually as needed, or use third-party monitoring tools to automate the monitoring of this queue and alert you to viruses and failed downloads via your email, cell phone, or pager.
- Scan reports provide detailed information about the directories scanned, infections found and cleaning/quarantining activity.
- All changes made to Powertech Antivirus for IBM i's automation files are recorded in the AVJRN journal, recording all changes made to the product, who made them and when they were altered.
- Virus scanning activity is recorded in the system audit journal, providing a secure audit trail of virus activity within the system.

Using Powertech Antivirus for IBM i

The information in this section describes how to configure and operate Powertech Antivirus for IBM i.

In this section you will learn how to:

- Acquire and use the latest virus definition (DAT files) from Trellix. See Updating Virus Definitions.
- Configure and initiate scans of all or part of your system at scheduled times. See On-Demand scanning.
- Configure and implement real-time protection against virus threats by scanning files dynamically, as they are opened. See On-Access Scanning.
- Detecting and alert for potential ransomware attacks. See Anti-Ransomware.
- Scan electronic mail messages passing through the IBM i Mail Server Framework (MSF) for viruses and malicious programs.. See Email Scanning.
- Detect potentially dangerous changes to the operating system. See Object Integrity Scanning.
- Limit scans to changed objects only. See Limiting Scans to Changed Objects.
- Quarantine threats in a secured area, out of harm's way. See Quarantine.
- Address potential threats. See Addressing a Potential Threat.
- Scan Domino mail and databases for viruses and malicious code. See Powertech Antivirus for IBM i for Domino.
- Monitor Powertech Antivirus for IBM i messages logged to the AVMSGQ. See Monitoring.

Updating Virus Definitions

Trellix releases virus definition updates every day. To ensure your system is protected against the latest virus threats, you must implement automatic updating of virus definition files.

Setup

To ensure your system is always protected against the latest virus threats, perform the following tasks. The remainder of this section covers each step in more detail.

1. Configure automatic update settings.
2. Run the update process to ensure automatic update is working.
3. Troubleshoot any problems as necessary.

4. Schedule the automatic update process to run daily.

5. Monitor the process for potential problems.

To configure automatic update settings

From the Setup menu, choose option **2**. Or, type the command **STANDGUARD/AVCHGUPDA** and press **F4**. See Change Automatic Update Attributes (AVCHGUPDA) for details.

> **NOTE:** You must run the command as a user with *ALLOBJ and *SECADM authority (such as QSECOFR).

Example

To schedule an automatic upgrade to run once per week:

AVCHGUPDA FROM(*WGET) WGET(*DFT) SCHEDULE(*DAILY) SCHEDDAYS(*WED) SCHEDTIME(083000)

To manually run an upgrade, choose option 20 from the Main Menu or type the command AVRUNUPD and press Enter.

AVRUNUPD OUTPUT(*)

Sample Report

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

* DAT Update Log                                              *

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *



Wed Mar 20 10:08:20 2019



Current version is 0



* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

```
* Getting INI files                                          *

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *



2019-03-20 15:08:20
URL:http://update.nai.com/products/commonupdater/oem.ini [2034/2034]
-> "oem.ini" [1]
2019-03-20 15:08:20
URL:http://update.nai.com/products/commonupdater/gdeltaavv.ini
[2153/2153] -> "gdeltaavv.ini" [1]
Remote version is 9200



* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

* Getting full DAT files                                     *

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *



2019-03-20 15:09:33
URL:http://update.nai.com/products/commonupdater/avvdat-9200.zip
[105343128/105343128] -> "avvdat-9200.zip" [1]



* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

* Extracting DAT files                                       *

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *



Archive:  avvdat-9200.zip

inflating: avvclean.dat

inflating: avvnames.dat

inflating: avvscan.dat

inflating: legal.txt
```

```
avvnames.dat - OK

avvscan.dat - OK

avvclean.dat - OK



************************************************************
* Replacing datfiles                                      *
************************************************************

Copying 'avvnames.dat' to '/StandGuard/dat/avvnames.dat'
Copying 'avvclean.dat' to '/StandGuard/dat/avvclean.dat'
Copying 'avvscan.dat' to '/StandGuard/dat/avvscan.dat'
Copying 'oem.ini' to '/StandGuard/dat/oem.ini'

DAT files successfully updated to 9200



************************************************************
* DAT Update   Success                                    *
************************************************************
```

Troubleshooting

- Use menu option 10 to work with logs.
- Review the log for error messages.

Recommendations

- Schedule the update process to run daily. The job doesn't consume much CPU resources and could be run during the day if necessary. Approximate run time should be less than 10 minutes, providing there are no network problems or delays.
- The automatic update job AVUPDATE runs under the STANDGUARD profile. If you decide to schedule the command outside the product, you will need to ensure either the STANDGUARD profile is used or a profile with *ALLOBJ authority. STANDGUARD does not have *ALLOBJ authority but works because it is the owner of the virus definition files. Public has only read authority, so if you do not use STANDGUARD you will need *ALLOBJ authority.

- Monitor the messages in the AVMSGQ to ensure an ongoing problem is noticed and remedied as soon as possible. Do not allow a connectivity problem to go unresolved or the virus definition files will become quickly outdated and will not provide adequate protection against new viruses.
- Do not hardcode the IP address of UPDATE.NAI.COM in any scripts or firewalls. The IP address of UPDATE.NAI.COM changes frequently.

Using a PC to Download Virus Definitions

Powertech Antivirus for IBM i provides everything you need to reliably download virus definitions automatically from Trellix's HTTP server. The process utilizes "micro-updates" to minimize the size and time required to download the full virus definition files. However if you would rather implement you own procedures for supplying the virus definition files then you will need to do the following:

1. Download the required files from Trellix's HTTP server.
2. Make the files available to Powertech Antivirus for IBM i. Files can br retrieved from an FTP server, a local path, or a network path.
3. Some method of monitoring the process to ensure it is always working (recommended).

Firewall Configuration

In order to acquire Trellix virus definition updates, the system's firewall must be configured to allow them. Virus updates are acquired either directly from Trellix, or from a server configured to host the virus definitions for the local network. In either, you must configure the firewall of the system receiving the virus definitions from Trellix to allow HTTP downloads from http://update.nai.com.

Download DAT files using A Windows PC

You can use a PowerShell script to download the DAT files (PowerShell is built into Windows 10).

1. Copy the following text into Notepad and save the file as "getdats.ps1" into an empty directory:

```
$url = 'http://update.nai.com/products/commonupdater/'
Invoke-WebRequest $url'oem.ini' -OutFile 'oem.ini'
Invoke-WebRequest $url'gdeltaavv.ini' -OutFile 'gdeltaavv.ini'
$site = Invoke-WebRequest -UseBasicParsing -Uri $url
$table = $site.links | ?{ $_.href.ToLower().Contains('avvdat-') } | sort
href -desc | select href -first 1
```

```
$filename = $table.href.ToString()
Invoke-WebRequest $url$filename -OutFile $filename
Expand-Archive -Force $filename .
Get-ChildItem $Path -Recurse | Where-Object {($_.Name -like '*-*') -and
($_.LastWriteTime -lt (Get-Date).AddDays(-2))} | Remove-Item -Recurse
```

2. Copy the following text into Notepad and save the file as "getdats.bat"

```
@ECHO OFF
PowerShell.exe -NoProfile -ExecutionPolicy Bypass -Command "&
'./getdats.ps1'"
```

3. Open a command window and execute the batch file getdats.bat. This will execute the Powershell script to download and extract the appropriate .zip file from Trellix's HTTP server into the current directory. Once completed the directory will be as follows:

```
06/19/2019  08:25 AM    <DIR>          .
06/19/2019  08:25 AM    <DIR>          ..
06/19/2019  07:00 AM          833,041 avvclean.dat
06/19/2019  08:24 AM      121,669,129 avvdat-9292.zip
06/19/2019  08:24 AM          730,425 avvnames.dat
06/19/2019  07:00 AM      102,055,422 avvscan.dat
06/19/2019  08:23 AM            2,151 gdeltaavv.ini
04/29/2019  12:22 PM               89 getdats.bat
06/19/2019  08:40 AM              606 getdats.ps1
06/19/2019  07:00 AM            8,170 legal.txt
06/19/2019  08:23 AM            2,034 oem.ini
         7 File(s)     104,520,459 bytes
```

4. Schedule the batch file to be executed once a day, every day. You can use any scheduler to do this, including the Windows Task Scheduler included with Windows. Ensure the working directory of the action is set to the directory of the getdats.bat file. For example, if the getdats.bat file's full path is `C:\Fortra\PTAV-i\getdats.bat`, specify `C:\Fortra\PTAV-i` as the working directory.
   If you use Windows Task Scheduler, you can configure the working directory as follows:

   a. Double-click the task to display its Properties.

   b. Choose the Actions tab.

   c. Select the 'Start a program' action and click **Edit**.

   d. Enter the working directory in the field 'Start in (optional)'. (Note: Do not put the value in quotation marks.)

   e. Click **OK**, then **OK** again.

> **NOTE:** A method of monitoring the above process to ensure it is continuously running is recommended.

Making DAT files available to Powertech Antivirus for IBM i

Now that you have the virus definition files listed on the previous page in a directory on your network, the next step is to configure Powertech Antivirus for IBM i to retrieve the files from an alternate source. There are two main methods:

- Put the files onto an internal FTP server, and set Powertech Antivirus for IBM i to download them via FTP.
- Share the files over a file share from a Windows server, configure the QNTC file system on the IBM i to include the file share, and configure Powertech Antivirus for IBM i to download them via the *PATH method.

These methods are described below.

Using FTP

1. Identify an internal Windows or Linux system that is configured as an FTP server.
2. Verify that you can connect from the IBM i to that server using FTP using the command `ftp` *xx.xx.xx.xx*, where "xx.xx.xx.xx" is the IP address of the server. If you can connect, so can Powertech Antivirus for IBM i.
3. Identify the folder on the server that is shared via FTP. There is at least one directory that the FTP server shares (for example, a "C:\FTP Files" directory).
4. Place the files that you downloaded previously into that directory.
5. Use the STANDGUARD/AVCHGUPDA command to set the Transfer Method to *FTP, change the FTP Location to the address of the FTP server, and to specify the FTP user and password.

> **EXAMPLE:**
> `AVCHGUPDA FROM(*FTP) FTP(`*IP-address/directory*`) FTPUSER(`*user*`)`
> `FTPPWD(`*password*`).`

Be sure to add the path to the end of the server's address. If the DAT files are located in the user's home or root directory, then specify / after the address.

Retrieving the DAT Files Using a Network Share

1. Identify an internal Windows PC or Windows server that is configured to share files.

2. Place the files that you downloaded previously into the shared directory on the Windows system.

3. Configure the QNTC file system on the IBM i so that the file share from the Windows system is mounted. The QNTC file system makes shared files on a Windows system visible in an IFS. The configuration of the QNTC file system is described in the following IBM document: How to access file shares from IBM i using QNTC.

4. Once the QNTC file system has been configured, determine the directory (path) of the Windows file share in the IFS of the IBM i.

5. Use the STANDGUARD/AVCHGUPDA command to change the Transfer Method to *PATH and the Path to the IFS path that you determined in the preceding step.

> **EXAMPLE:**
> `AVCHGUPDA FROM(*PATH) PATH(/QNTC/`*server-name/share-name*`)`

On-Demand Scanning

On-Demand scanning is the process of explicitly scanning a file or directory for viruses. Typically, an on-demand scan is initiated at a scheduled time to scan all or part of the system. When you initiate an on-demand scan, Powertech Antivirus for IBM i processes all of the files in the specified directories for viruses and provides a report of scanning activities.

Powertech Antivirus for IBM i can only track scan status for files in the Root, QOpenSys, and UDFS file systems. Files in other file systems, such as QDLS do not contain this information and consequently will be scanned every time.

On-Demand scanning is usually a long-running process. To minimize the time required to complete a scan, Powertech Antivirus for IBM i does not have to scan files that have already been scanned at the current virus definition level, unless the file has changed. Then as each file is scanned, Powertech Antivirus for IBM i records the scan information with the file. This information can be seen using the WRKLNK command and then option 8 next to the file. For a brief discussion about this, see the About IBM i file scanning attributes section in Powertech Antivirus for IBM i Features.

As Powertech Antivirus for IBM i scans files, the scan status is updated with either *SUCCESS or *FAILURE. Files with *SUCCESS status will not be scanned again until either the file data has changed or the virus definitions have been updated. Finally, the operating system will not allow files marked as *FAILURE to be opened (thus preventing the virus from spreading).

IMPORTANT: To scan all IFS files regardless of their respective object authority, the On-Demand scan should be performed under a user profile that has *ALLOBJ and *JOBCTL special authorities. The user profile must also be enrolled in the system distribution directory.
This applies to:

- The Powertech Antivirus Scan (AVSCAN) command: Run, or submit to run under a user profile that has *ALLOBJ and *JOBCTL if you want to ensure that all objects in the specified directory tree are scanned

- The Run Scan Task (AVRUNTSK) command: Run, or submit to run under a user profile that has *ALLOBJ and *JOBCTL if you want to ensure that all objects in the specified directory tree are scanned.

- When Configure Scan Task (AVCFGTSK) is used to configure recurring scans, the scans are configured as scheduled jobs in the IBM i job scheduler. The scheduled job will be initially configured to run under the user profile that executed the AVCFGTSK command.

> **EXAMPLE:** If user PMUELLER runs the AVCFGTSK command and configures recurring scans within it, an AVRUNTSK scheduled job is created that is configured to run under PMUELLER. In this case, profile PMUELLER must have *ALLOBJ and *JOBCTL special authorities to ensure that the scan will be able to scan all files in the specified directory tree.

Configuring, Scheduling, and Initiating an On-Demand scan

1. From the Main Menu, choose option **50**, Setup Menu (or type AVCHGA at the command line and press F4).

2. Choose option **6**, Virus Scan Tasks.

3. Here, you can use the available fields to create a scan configuration and schedule scans. See Configure Scan Task (AVCFGTSK) Command for complete details. Press F10 to see all parameters. Powertech Antivirus for IBM i is also pre-configured with the *SYS task, which scans the entire system with recommended settings. To use the pre-configured task, press F4 to see the list of tasks. Type *SYS and press Enter.

```
                    Configure Scan Task (AVCFGTSK)

 Type choices, press Enter.

 Task name  . . . . . . . . . . >  *SYS_____
 Objects:                       _
   Name . . . . . . . . . . . .   '/'_____
 _____
   Directory subtree  . . . . .   *ALL        *NONE, *ALL
                + for more values _
 Omit . . . . . . . . . . . . .   '/QOPT'_____

 _____
                + for more values  _____

 _____
 Heuristic analysis . . . . . .   *YES        *NO, *YES, *SAME
 Macro analysis . . . . . . . .   *YES        *NO, *YES, *SAME
 Potentially unwanted programs .   *NO         *NO, *YES, *SAME
 Scan archives  . . . . . . . .   *YES        *NO, *YES, *SAME
 Clean infected files . . . . .   *YES        *YES, *NO, *SAME
 Clean failure action . . . . .   *QRN        *QRN, *DELETE, *NONE, *SAME
                                                          More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

4. Press Enter to confirm changes and return to the Powertech Antivirus Setup Menu.

5. Press F3 to return to the Main Menu.

6. Choose option **1**. The Submit Job panel appears.

```
                   _      Submit Job (SBMJOB)

 Type choices, press Enter.

 Command to run . . . . . . . . >  AVRUNTSK TASK(*SYS) OUTPUT(*TASK)_____
 _____
 _____
 _____
 _____
 _____
 _____  ...
 Job name . . . . . . . . . . . >  AVRUNTSK     Name, *JOBD

                       Additional Parameters

 Schedule date  . . . . . . . . >  *CURRENT     Date, *CURRENT, *MONTHSTR...
 Schedule time  . . . . . . . . >  *CURRENT     Time, *CURRENT


                                                            Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

7. In the 'Command to run' field, the Run AV Scan Task (AVRUNTSK) Command has already been entered (by default) and set to use the included *SYS configuration. Replace this parameter as needed if you have created your own configuration. Add additional parameters as required if you would like to override certain values of the selected configuration.

> **EXAMPLE:**
> The following command configures the system task to scan the entire IFS for viruses, clean infected files, quarantine files that cannot be cleaned, and excludes scanning of the CD-ROM drive. The task will start every Saturday at 1am:
> ```
> AVCFGTSK TASK(*SYS) OBJ(('/' *ALL)) OMIT('/QOPT') CLEAN
> (*YES) CLEANFAIL(*QRN) RUNPTY(99) SCHEDULE (*WEEKLY)
> SCHEDDAY(*SAT) SCHEDTIME(010000)
> ```

8. Review the additional job parameters and make adjustments as necessary, then press Enter to submit the scan job.

Performance Considerations

On-Demand scanning of the entire Integrated File System can be a very long running CPU-intensive process. The time required to complete a full scan depends upon several factors:

- The speed of the processor
- The contention of CPU resources with other jobs
- The number and types of files to scan
- If any of the files are located in the /QOPT optical file system
- If virus definitions have changed since the last scan. When virus definitions are updated, the scan information for all files previously scanned becomes outdated. An update of virus definitions will require files to be re-scanned the next time they are accessed (if on-access scanning is enabled) and with the next on-demand scan. If virus definitions have not changed, then only files that have been changed will be scanned and the scanning process will be substantially faster.

NOTE: Powertech Antivirus for IBM i ignores symbolic links since they are not actually directories or files, but rather links to other directories or files. Symbolic links can point to a directory that is also a symbolic link pointing back to the first directory, creating a recursive circle of links. Powertech Antivirus for IBM i ignores symbolic links in order to prevent the possibility of this endless loop that would continually scan the same files or directories.

Troubleshooting

- If for some reason you need to cancel a long-running scan task, restarting the task will pick up where it left off except for QDLS files. QDLS files do not contain scan information and will be scanned every time.

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, so the first full scan after new definitions are downloaded will take substantially longer than other days.
- Exclude QOPT from scanning. QOPT is the IBM i CD-ROM/DVD drive(s). Scanning files in QOPT is substantially slower than local files. You can exclude QOPT by specifying OMIT(>/QOPT=) on the AVCFGTSK command.

- 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.

- Do not run commands AVCFGTSK , AVRUNTSK or AVSCAN under STANDGUARD profile. STANDGUARD does not have sufficient authority to perform a full system scan.

- Use the Timeout feature of scan tasks to limit the number of minutes a scan task can run. For more information, .

Sample report

The following report is an example of an on-demand scan report. Reports can be viewed using Main menu option 10.

```
Saturday, Nov 13 01:37 PM

Job . . . . . : QPADEV0001 MIKE        013887
Start path  . : /home/mike
Quarantine  . : /quarantined
Files . . . . : *ALL
Heuristics  . : *YES
Macro analysis: *YES
Programs  . . : *NO
Archives  . . : *YES
Clean . . . . : *YES
Clean fail  . : *QRN
Files . . . . : *ALL
Engine version: 4.4.00
DAT version . : 4406 (09-Nov-18)

   Time       Seconds   Directory
========   ========   =========================
13:40:42     120.8   /home/mike/test

13:40:47    < 0.1   /home/mike/com/Fortra/standguard/av

13:40:47      2.5   /home/mike/com/Fortra/standguard

13:40:47      2.5   /home/mike/com/Fortra

13:40:47      2.5   /home/mike/com

13:40:48      0.5   /home/mike/resources
```

```
        ERROR: 3546 Cannot open file /home/mike/viruses/EICAR.zip,
Object mar
ked as a scan failure!

13:40:49        0.5   /home/mike/viruses


13:40:49       124.4  /home/mike
0 virus(es) found!

# Files:
  Processed . : 25
  Scanned . . : 24
  OK  . . . . : 24
  Infected  . : 0
  Cleaned . . : 0
  Moved . . . : 0
  Deleted . . : 0

Warnings  . . : 0
Errors  . . . : 1

Completed at Saturday, Nov 13 01:40 PM
25 files processed in 220 seconds (0.11 files/sec)
```

On-Access Scanning

On-Access scanning refers to the process of scanning files as they are accessed and changed. To minimize the impact on performance, the operating system stores scan information with each file as they are opened. This process does not increase any storage use and typically requires less than a second for most files. The first user to access the file will cause a scan to occur, but subsequent accesses by that user (or any other user) will not trigger a scan unless the file contents have changed.

Powertech Antivirus for IBM i requires the use of a server job (AVSVR) running in the QSYSWRK subsystem to be active at all times. During installation, this job is configured to start automatically every time you start your system. If this job is ended for any reason then scanning is disabled. We strongly recommend that you implement procedures to monitor this job to ensure is it always running and restart the job as necessary. For monitoring suggestions, see Monitoring.
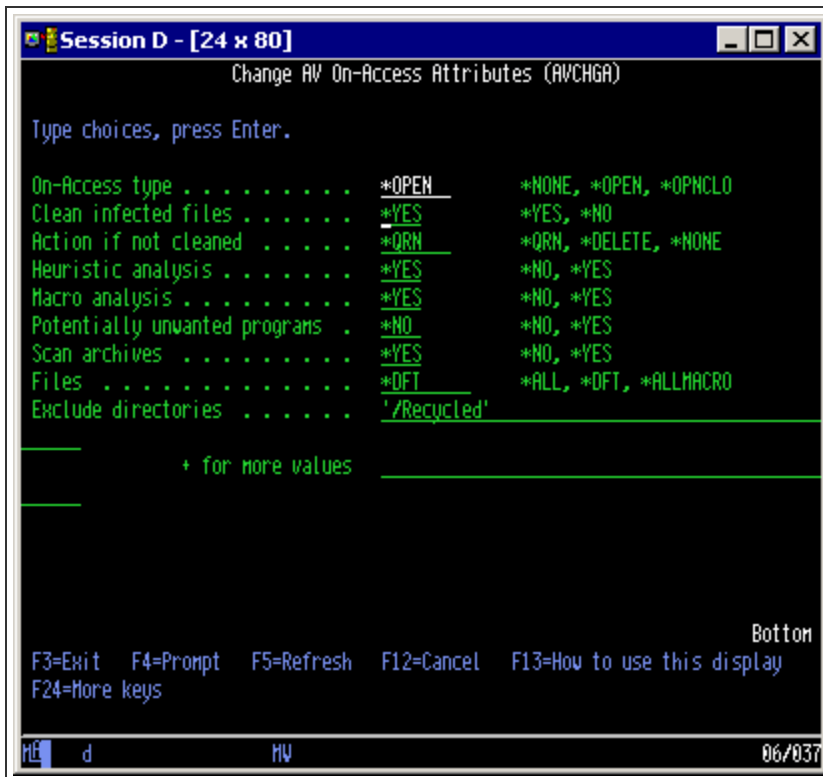
As files are scanned, IBM i updates the scan status information with the file. If the file is marked as infected, the operating system will not allow the file to be opened.

Requirements

You must have *ALLOBJ, *JOBCTL, and *SECADM authority to configure on-access scanning.

Setup

1. To view or modify on-access settings, choose Setup Menu option **1**, or type **AVCHGA** at the command line and press **F4**.
2. Press PAGE DOWN for additional options.

```
Session D - [24 x 80]                                    _ □ ✕
                   Change AV On-Access Attributes (AVCHGA)

 Type choices, press Enter.

 On-Access type . . . . . . . . .   *OPEN        *NONE, *OPEN, *OPNCLO
 Clean infected files . . . . . .   *YES         *YES, *NO
 Action if not cleaned  . . . . .   *QRN         *QRN, *DELETE, *NONE
 Heuristic analysis . . . . . . .   *YES         *NO, *YES
 Macro analysis . . . . . . . . .   *YES         *NO, *YES
 Potentially unwanted programs  .   *NO          *NO, *YES
 Scan archives  . . . . . . . . .   *YES         *NO, *YES
 Files  . . . . . . . . . . . . .   *DFT         *ALL, *DFT, *ALLMACRO
 Exclude directories  . . . . . .   '/Recycled'

                    + for more values

                                                              Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

 MA    d              MW                                         06/037
```

3. Configure scanning attributes as needed for your security policy. See Change AV On-Access Attributes (AVCHGA) command for details.

System Values

There are two system values that control when the operating system calls upon Powertech Antivirus for IBM i to scan a file: QSCANFS and QSCANFSCTL. You can access these settings by choosing option 4 from the Powertech Antivirus for IBM i Support Menu.

Scan file systems (QSCANFS)

Do not set this value to *NONE unless you want to disable all on-access and on-demand virus scanning.

QSCANFS identifies which file systems will be scanned using on-access scanning. The only supported value is *ROOTOPNUD. Only files in the Root, QopenSys and UDFS file systems support on-access scanning. Other file systems, such as QDLS, do not support on-access scanning and must be scanned using on-demand scanning.

Scan file systems control (QSCANFSCTL)

QSCANFSCTL provides several options to balance security and performance. One or more of the following values may be specified. The default value is *NONE, however when Powertech Antivirus for IBM i is installed we change this setting to *FSVRONLY.

*FSVRONLY — Only accesses through the file servers will be scanned. For example, accesses through Network File System will be scanned as well as other file server methods. If this is not specified, all accesses will be scanned (5250 access will be scanned).

*USEOCOATR — The system will use the specification of the "object change only" attribute to only scan the object if it has been modified. If this is not specified, this "object change only" attribute will not be used, and the object will be scanned after it is modified and when virus definitions have changed. Using *USEOCOATR can make on-demand scans run considerably faster by not scanning files that have not changed. However, be aware this value may allow a virus to hide in a file indefinitely. Use with caution.

*ERRFAIL — If there are errors when attempting to scan a file (the AVSVR job is not running, for example), the operating system will not allow the file to be opened. If this value is not specified, the system will allow the file to be opened and treat it as if the object was not scanned.

Be careful using *ERRFAIL if the file can not be scanned for any reason (if the AVSVR job is not running, for example) the operating system will not allow any stream files to be opened.

*NOPOSTRST — After objects are restored, they will not be scanned just because they were restored. In general, it may be dangerous to restore objects without scanning them at least once. It is best to use this option only when you know that the objects were scanned before they were saved or they came from a trusted source.

IBM i Directory and File Scan Attributes

Each directory in the supported file systems has a value to control the scanning attribute for files created in that directory. As new files are created, they inherit the setting on their parent directory. You can view the directory settings using WRKLNK and IBM i Navigator. By default, all directories and files are configured to be scanned.

To change all files in a directory to not be scanned using on-access scanning, run the command CHGATR OBJ('/path/*') ATR(*SCAN) VALUE(*NO) SUBTREE(*ALL) , where path is the name of the directory you want to change.

When you use the AVCHGA command the scan attributes are updated automatically so normally you do not need to perform the CHGATR command. This information is provided in case you want to modify scan attributes outside the product (when you create a new directory, for example).

Anti-Ransomware

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

How Powertech Antivirus Prevents Ransomware Attacks

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

Powertech Antivirus helps protect against ransomware attacks in two ways:

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

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

2. Canary files can be defined. A canary file is a decoy file placed within the IFS by the system administrator. If a defined canary file is modified, renamed, or deleted, it will immediately block the user.

Using Anti-Ransomware

Use the following steps to activate and configure anti-ransomware.

Activating/De-Activating Anti-Ransomware Protection

1. From the Powertech Antivirus Main Menu, choose option **50**, Setup Menu, then option **10**, Anti-Ransomware Settings. The Powertech Anti-Ransomware Menu appears.

2. To activate and deactivate anti-ransomware protection, choose option **50**, Activate/Deactivate Anti-Ransomware. The Activate/Deactivate Anti-Ransomware (AVACTAR) panel appears. Note that it will not be activated/deactivated until the QSERVER subsystem is restarted.

Configuring Anti-Ransomware

1. From the Powertech Antivirus Main Menu, choose option **50**, Setup Menu, then option **10**, Anti-Ransomware Settings. The Powertech Anti-Ransomware Menu appears.

2. Choose option **1** to open the Configure APEX Thresholds (AVCFGTHR) panel.

    a. For Send Message on Threshold, specify the threshold value to be used to determine when a message will be sent, warning of a possible ransomware attack. The message is sent to message queue AVMSGQ.

    b. For Block User on Threshold, specify the threshold value to be used to determine when a user will be blocked, in response to a possible ransomware attack. A message is sent to message queue AVMSGQ and the user is blocked within User Overrides.

3. Press **F3** to return to the Anti-Ransomware menu and choose option **2**, Work with APEX Directory Exclusions. The Work with Directory Exclusions (AVWRKDIR) panel appears.

    a. Define the directories that will not be protected by Powertech Antivirus for IBM i Anti-Ransomware.

    b. Note that an override does not apply to sub-directories; it only applies to the directory specified.

4. Press **F3** to return to the Anti-Ransomware menu and choose option **3**, Work with APEX User Overrides. The Work with User Overrides (AVWRKUSR) panel appears.

    Use this option to manage users in relation to anti-ransomware protection. You can define a different message and block thresholds for specific users and also define if a user is currently blocked. When a user is automatically blocked by the anti-ransomware protection, the user will have an entry within User Overrides.

5. Press **F3** to return to the Anti-Ransomware menu and choose option **10**, Work with Canary Files. The Work with Canary Files panel appears.
    Use this option to define decoy files you have created within the Integrated File System (IFS), which should result in the immediate blocking of a user if modified, renamed, or deleted. This will be actioned, if active, even if the canary file is within a directory that has a Directory Override, excluding it from anti-ransomware protection.

> **NOTE:** Anti-Ransomware detection will not work if files are already encrypted. As an alternative, place canary files into encrypted directories.

Email Scanning

Powertech Antivirus for IBM i includes the ability to scan electronic mail messages passing through the IBM i Mail Server Framework (MSF) for viruses and malicious programs. If you are using the IBM i SMTP server, Powertech Antivirus for IBM i can perform virus scanning on emails before they reach your PC clients.

Features

- Scans IBM i SMTP email at the server
- Scans inside archive files such as .ZIP, .JAR, etc.
- Detects header exploits and malformed MIME
- Redirects infected or suspicious email to an Administrator

Scans SMTP Email at the server

Powertech Antivirus for IBM i scans email messages passing through the IBM i Mail Server Framework looking for known viruses as well as code that could be malicious. This means it can protect against known viruses, but most importantly, potentially against unknown viruses and/or malicious code. This is crucial as an unknown virus could be a one-off piece of code, developed specifically to break into your network.

Scans compressed and encoded messages

Powertech Antivirus for IBM i scans deep inside attachments to detect viruses buried in multiple levels of encoding and compression. Powertech Antivirus for IBM i decodes BINHEX, UUENCODE and XXENCODE, MIME (BASE64 and quoted-printable), TNEF, and IMC attachments. Files compressed with PKZIP,ZIP2EXE, ARJ, ARJ2EXE, JAR, LHA, LHA2EXE, TAR, GZIP, UNIX PACK, and MS Compression methods are also effectively scanned. Powertech Antivirus for IBM i even scans files with multiple compression levels; for example, a ZIP file that has also been compressed with LZEXE and ARJ, then zipped again, and so on.

Detects header exploits and malformed MIME

MIME headers specify things such as the subject line, date, or filename. By specifying a well-crafted string, a skilled hacker could execute arbitrary code on the target machines. Such vulnerabilities are prone to exploitation for penetrating remote networks or for delivery of viruses and worms. This vulnerability allows attached executable files to be run when a message is simply viewed. Several common viruses make use of this exploit, including W32/Badtrans@MM, W32/Nimda.gen@MM, and W32/Klez.gen@MM. Powertech Antivirus for IBM i detects these header exploit tactics and blocks these messages from reaching your desktop clients, where the virus is able to execute.

Redirects infected or suspicious email to an Administrator

When a known virus, potentially malicious program, or an email using a MIME header exploit is detected, Powertech Antivirus for IBM i can either redirect the mail to an administrator or simply delete the mail without forwarding. In either case, a message is logged to the AVMSGQ for real-time monitoring purposes and the AVLOG file for a more permanent audit trail.

Setup

To activate Powertech Antivirus for IBM i scanning of SMTP messages passing through the IBM i Mail Server Framework, choose option 4 from the Setup menu or type the command STANDGUARD/AVCHGSMTPA and press F4.

```
                    Change SMTP AV Attributes (AVCHGSMTPA)

Type choices, press Enter.

Scan SMTP mail . . . . . . . . .   *YES          *SAME, *YES, *NO
How to handle infected mail:
  Action . . . . . . . . . . . .   *FORWARD      *SAME, *DELETE, *FORWARD
  Forward address  . . . . . . .   admin@mycompany.com
```

Scan SMTP mail (SCANSMPT)

*YES activates scanning of mail. *NO deactivates mail scanning. Note: *IOSYSCFG authority is required to change this setting.

How to handle infected mail

The Action (ACTION) specifies how you want the infected mail to be handled. *FORWARD will forward infected mail to the specified forward address. Provide the address in the Forward address field. The infected mail will forwarded and not be delivered to the intended recipients. *DELETE will simply delete the mail without forwarding. In either case a message is logged to STANDGUARD/AVMSGQ with information about the infection and the action taken.

Figure 1 shows an example of an infected mail item that Powertech Antivirus for IBM i forwarded to the administrator. The original email is attached so it can be examined in its original form if necessary.

Be very careful opening these attachments. The email from Powertech Antivirus for IBM i can be opened safely, but the attachment is the original message and is a virus.
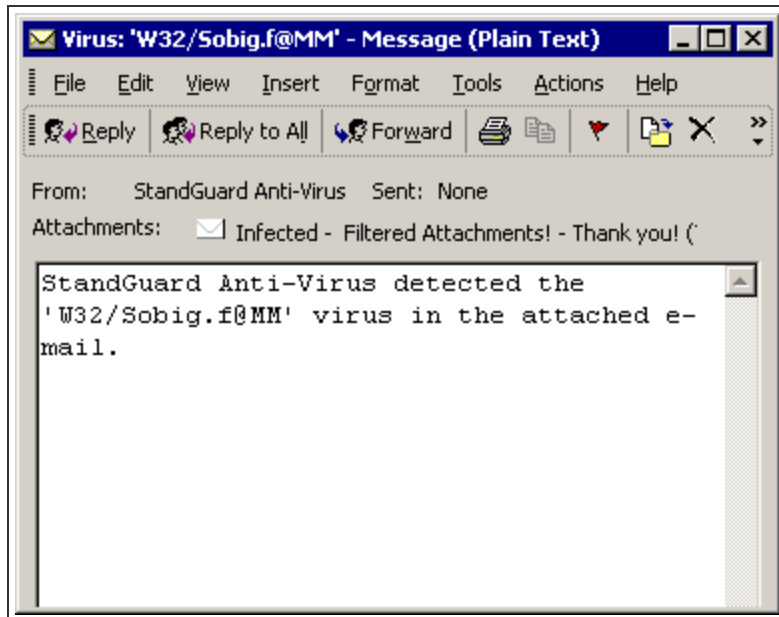
Troubleshooting

- Use the Support Menu option 2, and locate the job that processed the email item. There may be many jobs to choose from or the job may have completed. Look in the joblogs for any error messages.

- If you do not want mail scanned, turn off mail scanning (using Setup Menu option 4, or the AVCHGSMTPA command).

- The exit point used to scan mail is QIBM_QZMFMSF_SEC_AUT. Under rare circumstances should you not be able to disable mail scanning using the recommended procedures, then use WRKREGINF QIBM_QZMF_SEC_AUT and remove exit program AVSMTPX. Then restart MSF (ENDMSF, STRMSF). That will end the connection between the mail server and Powertech Antivirus for IBM i.

- Restart MSF using ENDMSF and STRMSF commands.

Recommendations

- Consider using SMTP filters to filter out messages with certain types of harmful attachments. For more information about SMTP filters, see Filtering email to prevent virus proliferation.

- Keep virus definitions up to date. See Updating Virus Definitions.

Object Integrity Scanning

Powertech Antivirus for IBM i can detect potentially dangerous changes to the operating system, and for user programs that have the potential to cause serious harm to the operating system and bypass security. Powertech Antivirus for IBM i Object Integrity scanning can:

- Detect changes to IBM provided operating system objects
- Detect if libraries or commands have been tampered with
- Detect user programs that have been patched into fooling the operating system to allow it to bypass security and system integrity
- Optionally retranslate patched program, reinstating the operating system's ability to enforce its security and object integrity protection with these programs

We recommend you run an object integrity scan:

- After someone has restored programs to your system
- After someone has used dedicated service tools (DST)
- After you install a product from a new ISV and at least periodically after updates from established ISVs
- Periodically to check if anyone has changed any system objects

Digital Signature Checking

Beginning in V5R1, IBM started signing the operating system as a way of officially marking objects as originating from IBM and as a means of detecting when unauthorized changes occur to system objects. A digital signature can be used to show proof of origin and detect tampering.

Figure 1 shows an example of digital signatures. There are tens of thousands of digital signatures on the system. A digital signature does not prevent an object from being modified or tampered with – but it can be used to determine if an object has been changed.

```
Session A - [24 x 80]                                      _ □ ✕
File  Edit  View  Communication  Actions  Window  Help
                    Display Program Information
                                                  Display 4 of 7
Program  . . . . . . . :    QSYCHOVN    Library . . . . . . . :   QSYS
Owner  . . . . . . . . :    QSYS
Program attribute  . . :    CPPLE
Detail . . . . . . . . :    *SRVPGM


Type options, press Enter.
  5=Display


      Service
Opt   Program    Library    Signature
  _   QSYGENCM   QSYS       D8E2E8C7C5D5C3D44040404040404040
  _   QP0LGS1    QSYS       D8D7F0D3C7E2F14040404040404040
  _   QSYCODEUTL QSYS       D8E2E8C3D6C4C5E4E3D3404040404040
  _   QSYCLEANUP QSYS       D8E2E8C3D3C5C1D5E4D74040404040
  _   QC2UTIL1   QSYS       CB1F803582C31AC25B4DCBDD1B6D0948
  _   QYPPRI370  QSYS       D8E8D7D7D9E3F3F7F040404040404040
  _   QLEAVI     QSYS       44F70FABA08585397BDF0CF195F82EC1
                                                       Bottom
F3=Exit  F4=Prompt  F11=Display character signature  F12=Cancel  F17=Top
F18=Bottom

MA    a                                               14/003
```

Figure 1 - IBM i Digital Signatures

Whenever an object is changed, the digital signature is invalidated. The object may continue to run, but not in a way that was intended by the signer (IBM, in this case). Powertech Antivirus for IBM i uses application program interfaces (APIs) provided by IBM to verify the signature of these objects that have been digitally signed.

Patched programs

A potentially, and very serious, security risk is user programs that have been patched to fool the operating system into allowing them to bypass all system security levels. Allowing system state programs provided by someone other than IBM represents a potential integrity risk to your system. At best these programs may be using interfaces or directly manipulating the internals of the objects that IBM is free to change at any time. The results of such a change could be a failed application, an unstable system, or even a damaged system that needs to be reinstalled. At worst, they could be rogue programs that are bypassing the auditing and integrity of your system to steal information or intentionally damage it.

Powertech Antivirus for IBM i can detect patched programs, and optionally retranslate them to remove the patch. Retranslating will in most cases cause the program to fail. We recommend running the object integrity scan with the translate option set to *NO, then review the output of the command to see what programs were detected. Contact the owner and/or

administrator of the programs to obtain proper versions of the programs. If proper versions cannot be obtained, you can add the program(s) to an exclusions list. Exclude the program only when you trust the vendor/owner of the program at the expense of bypassing operating system integrity and security.

Setup

To setup object integrity scanning:

1. On the Main Menu, choose option **50**, Setup Menu.
2. Choose option 5, Object Integrity Scan Tasks (or type AVCFGITGT at the command line).
3. Press F9 to see all parameters. See Configure Integrity Scan Task (AVCFGITGT) for details.
4. Configure parameters as needed and press Enter.

Examples

1. Check all operating system libraries, ensure all objects are signed and have valid signatures, schedule the task to run automatically on Fridays at 1:00AM:
   ```
   AVCFGITGT TASK(*SYS) TYPE(*LIB) LIB(*IBM) CHKSIG(*ALL) FRCCRT
   (*NO) SCHEDULE(*WEEKLY) SCHEDDAY(*FRI) SCHEDTIME(010000)
   ```
2. Check all user libraries for patched programs, verify digital signatures of objects that have been signed, schedule the task to run automatically on Mondays, Wednesdays and Fridays at 11:00PM.
   ```
   AVCFGITGT TASK(*ALLUSR) TYPE(*LIB) LIB(*ALLUSR) CHKSIG(*SIGNED)
   FRCCRT(*NO) SCHEDULE(*DAILY) SCHEDDAYS(*MON *WED *FRI)
   SCHEDTIME(230000)
   ```

Recommendations

- Most IBM commands duplicated from a release prior to V5R2 will be logged as violations. These commands should be deleted and re-created using the CRTDUPOBJ (Create duplicate object) command each time a new release is loaded.
- Running an Object Integrity Scan requires *AUDIT special authority. Sign on as QSECOFR when changing the object integrity scanning schedule.
- The command may take a long time to run because of the scans and calculations it performs. You should run it at a tim e when your system is not busy.

- Most objects in user libraries are not signed. Using CHKSIG(*ALL) on user libraries will log an error for every object in the library - probably not what you want. All IBM objects are signed, so use CHKSIG(*ALL) on all IBM libraries, and CHKSIG (*SIGNED) on user libraries that are not signed.

Sample Report

The following lists a sample Object Integrity scanning report. The sample shows a scan of libraries for QSYS and QIWA* libraries for illustration purposes only.

```
Time . . . . . . . . . . . : Wednesday, Nov 10 01:02 PM
Job. . . . . . . . . . . . : AVRUNITG   MIKE       013640
Task name. . . . . . . . . : *SYS
Task type. . . . . . . . . : *LIB
Libraries. . . . . . . . . : QSYS
                             QIWA*
Check signatures . . . . : *ALL
Force program creation . : *NO
Exclusions . . . . . . . . : *NONE

  Time     Library
======== ==========
13:02:58  *                       (System integrity)
QVFYOBJRST system value does not verify object signatures during
restore at its current setting.

13:07:30  QSYS
        The runnable object QEZAST type *PGM has been tampered
with.
        The object QWSACCDS type *PGM has a digital signature that
is not valid.

13:16:25  QIWA2
        The object CFGACCWEB2 type *CMD can be signed but does not
have a digital signature.
        The object ENDACCWEB2 type *CMD can be signed but does not
have a digital signature.
        The object RMVACCWEB2 type *CMD can be signed but does not
have a digital signature.
        The object STRACCWEB2 type *CMD can be signed but does not
have a digital signature.

6 violation(s) found!
```

Error messages

The following list shows the most common error messages that may appear on the report:

Message ID	Error message text
CPF9EA7	QVFYOBJRST system value does not verify object signatures during restore at its current setting.
	The object has a digital signature that is not valid.
	The domain is not correct for the object type.
	The runnable object has been tampered with.
	The library protection attribute is set incorrectly.
CPFB722	The object can be signed but does not have a digital signature
	The object cannot be checked, it is in debug mode, saved with storage freed, or compressed.
	The object has not been converted to RISC format.
CPFB749	Object signature operation ended abnormally. &1 objects attempted, &2 objects successfully processed.

Scanning Unchanged Objects

When Powertech Antivirus for IBM i is requested to scan a file, it first checks to determine if the file has been scanned before and if the scan can be skipped for that file. By default, the scan is skipped if all of the following are true:

- The file has been scanned before
- The file has not been modified since the last scan
- The version of the virus definitions used for the last scan is identical with the current version
- For an On-Demand scan, the scan command or scan definition have not been parameterized to force scanning of already-scanned files

In this section, we will refer to the action of scanning a file's contents for malware for a file that was previously scanned, as *file rescan*.

Forcing file rescans

To enforce the re-scanning of files that were scanned previously, specify a `FORCE` parameter (on the scan command, or the definition used for the scan) of either `*CHGONLY`, `*NOSCAN`, or `*ALL`. (See the F1 help for that parameter for additional information).

> NOTE: When the `FORCE` parameter is set to one of the above values, Powertech Antivirus for IBM i scans files even if:
> - The file has been scanned before
> - The file has not been modified since the last scan
> - The version of the virus definitions has not changed since the last scan

Preventing File Rescans after Virus Definition Updates

When an object has been scanned before and has not changed, but the version of the virus definitions has changed, by default, scans result in file rescans. This behavior can be changed to reduce scan times and scan overhead.

To prevent file rescans after virus definition updates, you need to:

- Configure the Integrated File Systems
- Configure the scan task

These steps are described below. They can be performed at any time and do not need to be performed immediately after installation.

> NOTE: If both Powertech Antivirus for IBM i and Powertech Encryption for IBM i are installed on this system, and if the IFS encryption functionality of Powertech Encryption for IBM i is used or is planned to be used, the following steps must not be performed, as they would interfere with IFS encryption.

Configuring the Operating System for Changes-Only Scans

To configure the Integrated File System to prevent file rescans after virus definition updates:

- Ensure that system value QSCANFSCTL includes the value *USEOCOATR

Perform the following steps:

a. Execute the command:
   CALL QCMD

b. Press F11 to display the full-screen command-line.

c. Execute the following commands.

> NOTE: In both commands, replace *A_USER* with a user profile that has *ALLOBJ special authority.

```
SBMJOB CMD(CHGATR OBJ(/) ATR(*CRTOBJSCAN) VALUE(*CHGONLY)
   SUBTREE(*ALL))
   JOB(CHGATTR1)
   USER(A_USER)
   JOBMSGQFL(*WRAP)


SBMJOB CMD(CHGATR OBJ(/) ATR(*SCAN) VALUE(*CHGONLY)
   SUBTREE(*ALL))
   JOB(CHGATTR2)
   USER(A_USER)
   JOBMSGQFL(*WRAP)
```

d. Wait for the submitted jobs CHGATTR1 and CHGATTR2 to complete.

> NOTE: A high number of CPFA0AD "Function not supported by file system" messages may appear in the job logs of the submitted jobs. This is normal and not an indication of an issue.

On-Access scanning, if used, will immediately benefit from the above steps, and gain the performance benefits resulting from it. In contrast, On-Demand scans only benefit if they are parameterized accordingly. This is described in the following subsection.

Configuring the Scan Task

To configure a scan that does not perform file rescans after virus definition updates:

- Ensure that the `FORCE` parameter of the scan contains neither the value `*ALL` nor the value `*CHGONLY`.

  > NOTE: The default setting for this parameter is `*NONE`.

> NOTE: The duration of the first scan run on a system is not affected by these settings, as at that point no files have been previously scanned. Only subsequent scans will be impacted by the above changes.

Combining Different Scan Types

Different scan settings represent different tradeoffs between detection capability, scan duration, and overhead. Settings that prevent file rescans after virus definition updates reduce scan times, but also prevent the detection of malware, for which signatures are only contained in more recent virus definitions.

One way of dealing with the conflicting requirements of detection vs. performance is to combine different scan types. For instance, depending on these requirements, the following may be a useful combination of scan types:

- Nightly on-demand scans Monday through Friday, that avoid file rescans after virus definition updates, to ensure total scan duration is limited and does not overlap with bath processes. The `FORCE` parameter on the scan definition is set to `*NONE`.
- A weekend scan that does perform file rescans after virus definition updates, to ensure files are scanned with the latest virus definitions, if at a delay. The `FORCE` parameter is set to `*ALL`.

Quarantine

Powertech Antivirus for IBM i provides a secured area where infected files are moved to and out of harm's way. When a file has been quarantined, the file has not been deleted but access to the file is prevented. The infected file is moved to the '/Quarantined' directory.

Setup

Powertech Antivirus for IBM i automatically builds the path for the infected file inside the '/Quarantined' directory. For example, if an infected file is found in '/home/docs/mydoc.doc', then the infected file is moved to '/Quarantined/home/docs/mydoc.doc'. No setup is necessary.

Managing

You can view the files in the quarantine directory using the command WRKLNK '/Quarantined/*', or Option 12 from the Main Menu.

Troubleshooting

If for some (rare) reason you need to unlock an infected file, disable on-access scanning using the command AVCHGA ACCESS(*NONE), then run CHGATR OBJ ('/home/mike/myfile.exe') ATR(*SCAN) VALUE(*NO). That will turn off scanning of the file and allow the file to be opened. Contact Fortra Technical Support, if needed.

Recommendations

If you want to delete a folder in 'Quarantined', use 2 to change, then 9 to 'Recursive delete'

Addressing a Potential Threat

If Powertech Antivirus for IBM i identifies a virus or malware on your system, do the following to address the potential threat:

1. Ensure you are using the latest DAT files by running a manual update. To do so, Submit the command: **STANDGUARD/AVRUNUPD**.
2. Isolate the threat:
    -   Run full scans on other hardware/computers etc. to ensure the malware has not spread any further.
    -   Run an On-Demand Scan with all Scan Settings enabled.
        -   Objects:
        -   Name . . . . '/'
        -   Heuristic analysis . . . . *YES
        -   Macro analysis . . . . *YES
        -   Potentially unwanted programs . *YES
        -   Scan archives . . . . *YES
        -   Files . . . . *ALL
        -   Force . . . . *ALL
    -   If you wish to review all the scan details after the scan has run, change the Logging Level to *DETAILED.
    -   If you want the scan to run in its entirety, ensure the Timeout minutes parameter is set to *NONE.
        Be aware that running a full scan may affect performance.
3. Determine if the virus or threat was found in a critical folder.
    -   The Quarantined folder can be found under the AVMENU, option 12 (Work with quarantined files).
    -   For reference, the path name within the Quarantined folder reflects the actual path name where the infected object was found. By leaving the path name structure in place, even after you delete the infected object, you have a history of folders that have been infected.

4. Investigate the threat.

   - Investigate to see if the object was legitimate and somehow got infected, or if it was a fraudulent object that was inserted maliciously into the folder. If it was legitimate, and may be needed in the future, you will need to recover it from a valid source. If it was a fraudulent object, you won't need to recreate it.Investigate how the object was infected and identify possible users who may be at risk.

     - Which users have access to this object?
     - Are their PCs running up to date antivirus software?
     - Try to work out when it hit the IFS, and therefore, possibly, where it came from.

5. Delete the infected object as soon as is possible. As a reminder, **you should never save or replicate the /QUARANTINED directory**.

6. Closely review scans for the next few days or weeks. If a PC or other system that connects to the IBM i system is infected and this is not caught, it is possible for the infected file to get transferred to the system again.

Overview of Exit Program Integration

Powertech Antivirus for IBM i uses IBM i exit points for file scanning. The File Server exit point allows only a single exit point solution to use the exit point at one time. Exit program integration is an advanced functionality, introduced in Powertech Antivirus for IBM i version 8.09, that allows overcoming this File Server exit point limitation. The integration uses a single exit program for the File Server exit point, which then calls other programs as if they were exit programs directly assigned to the exit point.

Exit program integration provided with Powertech Antivirus for IBM i includes the following exit points:

- The File Server exit point
- The Integrated File System Scan on Open exit point
- The Integrated File System Scan on Close exit point

> IMPORTANT: Exit program integration is automatically installed and configured with a first installation of Powertech Antivirus for IBM i. If you have Powertech Antivirus for IBM i version 8.05-8.08 and enabled the anti-ransomware functionality before an upgrade, you must manually enable exit program integration by removing then re-adding the anti-ransomware exit program from the Anti-Ransomware Menu.

Exit Program Sequencing

Exit program integration allows you to control the order of how the exit programs are called. Exit programs can prevent the following two exit program groups from being called:

1. The exit programs of Fortra products that support exit program integration, which are called first. Between the products, the order of how the exit programs are called is determined programatically and cannot be customized.

2. Other exit programs, which are called next. You can specify the order between these programs.

> NOTE: Any of the exit programs on this chain can stop the processing of the other exit programs further down the chain.

Exit Program Integration and Other Solutions Using Exit Points

Powertech Encryption for IBM i

Powertech Encryption for IBM i version 4.0 and higher will automatically configure exit point integration for co-use between Powertech Encryption for IBM i and Powertech Antivirus for IBM i.

Powertech Exit Point Manager for IBM i

Please refer to this article for information and instructions for using Exit Program Integration with Powertech Antivirus for IBM i.

Other Solutions' Configuration

Other solutions from Fortra and third-party providers can also use exit point integration. To add the exit program for another solution into the integration, follow these steps:

1. Use the Work with Exit Program Integration (WRKEXTPGM) Command to add an exit program to a specific exit point.

2. Under "exit program for which product," select one of the "NON-FORTRA" entries.

3. Under "Product," specify the exit program library and name.

Powertech Antivirus for IBM i for Domino

Powertech Antivirus for IBM i for Domino is an optional licensed feature that provides the ability to scan Domino mail and databases for viruses and malicious code. The following instructions explain how to install this optional product feature.

Requirements

1. Domino 6.5.6 or later
2. You must have previously completed installing the Powertech Antivirus for IBM i base feature. For these instructions, see About the Installation Process.
3. You will need to end and restart the Domino server during the installation process.

Installing

See Domino Installation Instructions to install the module on the IBM i, then proceed with the following.

Install the code to the Domino server

In the following instructions, replace server-name with the name of the Domino server you want to install the code to. You can see a list of Domino server names using the command WRKDOMSVR. The Domino server must be ended for the product to be installed.

1. Run the following command to end the server, then wait for the server to end before continuing with the next step.
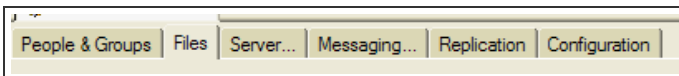   **ENDDOMSVR SERVER(server-name)**

   Run the following command to install the code to the server:

   STANDGUARD/AVDOINS SERVER(server-name) OPTION(*INSTALL)

   Finally, start the Domino server:

   STRDOMSVR SERVER(server-name)
2. **Sign the Powertech Antivirus for IBM i databases.** Open the Domino Administrator client and go to the Files Tab.


   Choose Templates Only from the Show Me: Drop down list.

   Highlight the SGAV Template databases in the list of templates shown.

Once highlighted open the Databases section on the right side of the Administration pane and choose Sign. Make sure to uncheck Update existing signatures only and choose to sign with the Active User's ID (if a trusted Administrator ID, and the ID going to be used for installation) or with the Active Server's ID. Choose OK after selecting the options to sign the databases with a trusted ID in your Domino environment.
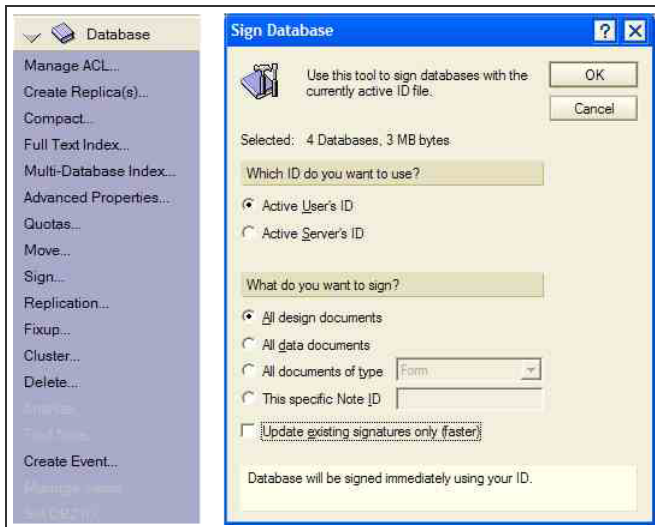
3. **Verify Agent authority.**

   Since the Powertech Antivirus for IBM i databases have many agents that run, the ID you used for signing, Server or Administrator ID, should also have the rights to Run unrestricted methods and operations. This is found in the Security Tab of the Current Server Document.


   Click on the Security tab. Verify LocalDomainAdmins is specified for "Run unrestricted methods and operations" as shown below.

Programmability Restrictions	Who can –
Run unrestricted methods and operations:	LocalDomainAdmins, LocalDomainServers
Sign agents to run on behalf of someone else:	
Sign agents to run on behalf of the invoker of the agent:	
Run restricted LotusScript/Java agents:	
Run Simple and Formula agents:	
Sign script libraries to run on behalf of someone else:	
Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Run restricted Java/Javascript/COM:	
Run unrestricted Java/Javascript/COM:	

4. **Completing the installation.**

   A. Open the Notes client, and choose File>Database>Open.

   B. In the 'Server' field, type or choose your server name. In the 'Filename' field, type SGAVINST.NTF, click Open.

   C. When the Installation form appears, choose Install.
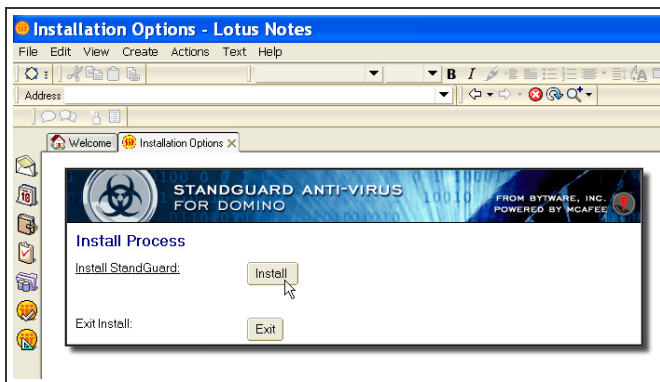
5. When the installation process is completed, choose Exit.
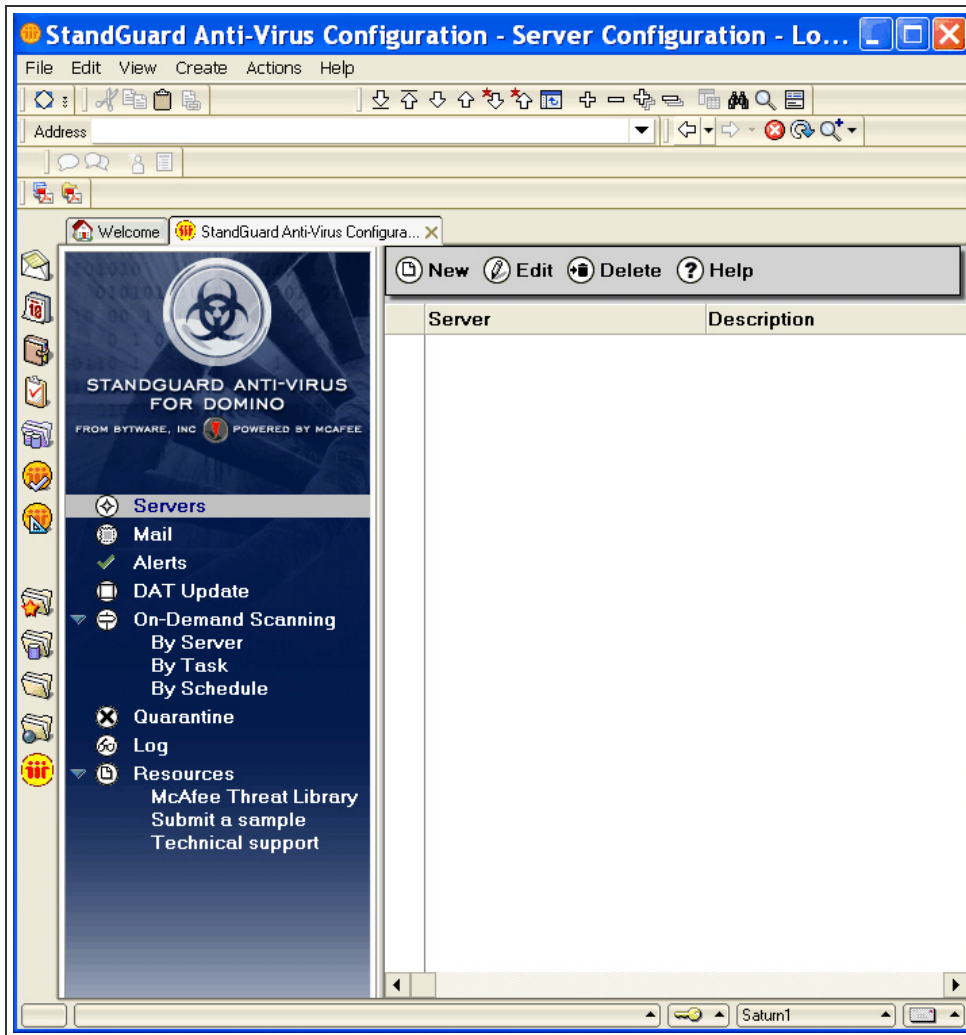
Starting

To start the application:

1. Open the Notes client and choose File>Database>Open.

2. In the 'Server' field, type or choose your server name.

3. Scroll to the directory SGAV and open it.

4. Select database Powertech Antivirus for IBM i Configuration and click Open.
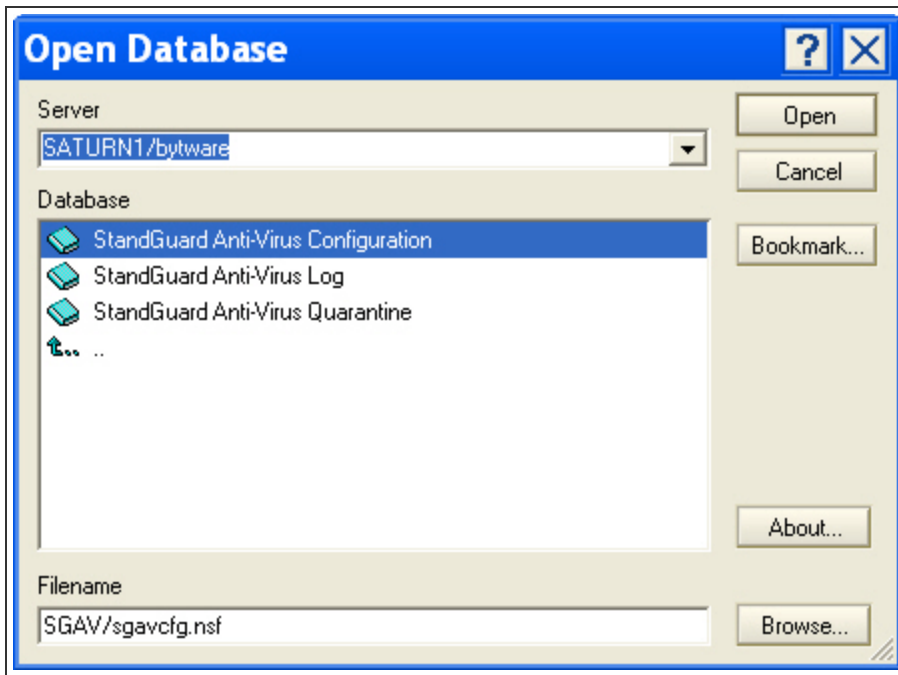
The main application screen will appear as shown below.

Setup

Server Configuration

The first step that must be performed is to create a server configuration document. The server configuration document specifies configuration information for each Domino server that is protected by Powertech Antivirus for IBM i. In the navigator, click on Servers, then click New (in the toolbar).
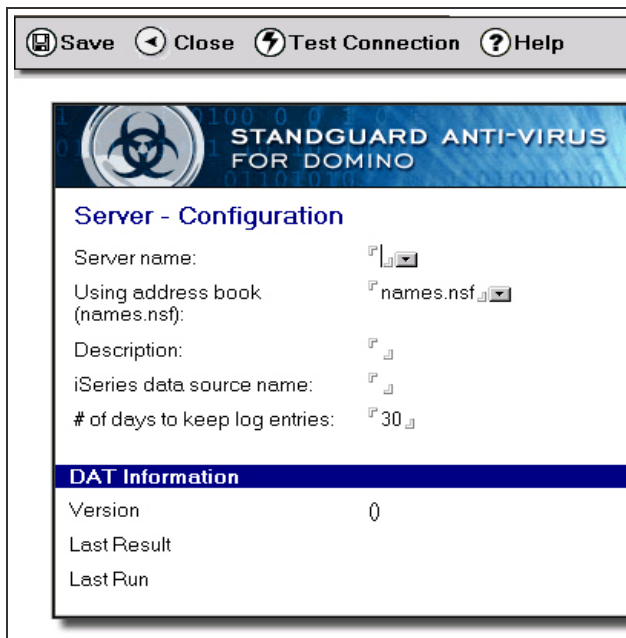
Server name (required)

Specifies the name of the server protected by Powertech Antivirus for IBM i. Choose the Server name using the drop down list to the right of the server name field.

Address book

Specifies the address book used to lookup the server name (typically names.nsf)

Description

The optional description for the server.

IBM i data source name

The name of the IBM i data source used to access the server (typically *LOCAL). When working with multiple servers, the data source name is used to access remote servers, and can be viewed using the WRKRDBDIRE command. After changing the data source name, press the Test Connection button to verify the connection.

Number of days to keep log entries

Specifies the number of days log entries are retained before being purged (automatically).

DAT Information

These values cannot be edited directly, and are updated by the product whenever the DAT update process retrieves updated files (typically once per day).

Version

Specifies the version of the DAT files.

Last result

Specifies the last result of the DAT Update process for the server.

Last run

Specifies the time the DAT Update process was last run.

When you have finished entering information, click Save, then Close.

Mail Configuration

The Mail configuration document specifies configuration settings the product uses to scan mail attachments on a particular server. There is one configuration document for each server.

To access the Mail configuration documents, go to the main application display, then click on Mail, then New or Edit (in the toolbar).
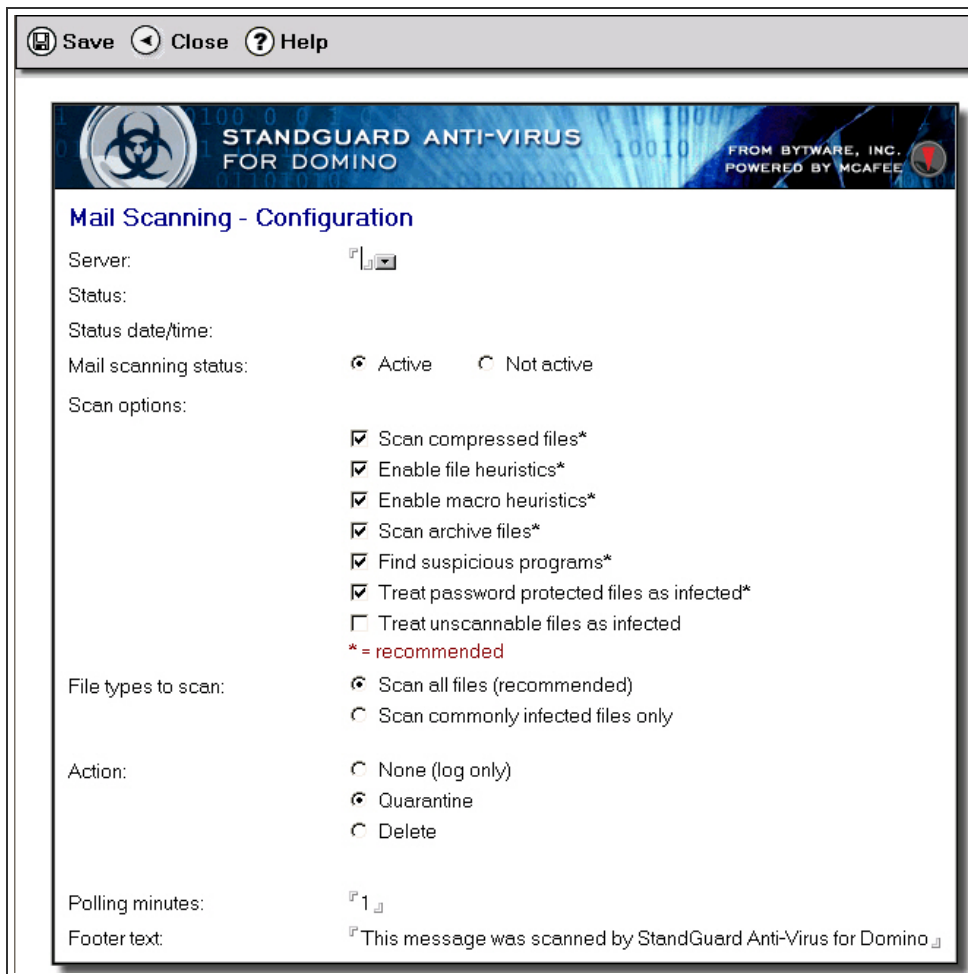
Server (required)

Specifies the name of the server for which mail scanning is being configured. Choose the Server name using the drop down list to the right of the server name field.

Status

Specifies the status of the mail scanning server task AVDOMSVR.

Status date/time

Specifies the time the status was last updated. Typically this is the time the AVDOMSVR last started. The AVDOMSVR server task usually restarts every day, whenever DAT files are updated.

Mail scanning status

The active status of the mail scanning. Choose one of the following:

Active (recommended)

Mail scanning is currently active for the server. All mail with attachments will be scanned for viruses and malicious code, using the scan options below.

Not active

Mail scanning is currently not active for the server. Use this setting to turn off mail scanning.

Scan options

Specifies the options that will be used to scan mail.

Scan compressed files (recommended)

Decompress executable files before scanning. Many programs use executable compressors to make the distribution file smaller, for example, PKLite. Unfortunately, packaged files can contain viruses that are compressed. You can use this parameter to decompress these files (in memory) and scan the internal image for viruses.

Enable file heuristics (recommended)

Use heuristic scanning to detect executable files that have code resembling malware.

Enable macro heuristics (recommended)

Use heuristic scanning to detect unknown macro viruses.

Scan archive files (recommended)

Decompress multi file archives before scanning. This parameter tells the product to scan inside archive formats. The list of formats includes ARJ, LHA, PKARC, PKZIP, RAR, TAR and WinACE files, and also BZIP and Zcompress single file compression. The list is frequently updated. Archive formats store a number of files within a single file. For example, a scan of a single .ZIP file results in many files being scanned.

Find suspicious programs (recommended)

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

Treat password proteced files as infected (recommended)

The product can scan password protected files by employing password cracking techniques. The techniques can crack most passwords, but if the password cannot be cracked, the product can treat the file as if it was infected. Many infected mail messages contain password protected files.

Treat unscannable files as infected

If a file cannot be scanned for some other reason, whether to treat the file as infected.

File types to scan

Specifies the types of file attachments that will be scanned.

Scan all files (recommended)

All file types, regardless of extension, will be scanned.

Scan commonly infected files only

Only file types that are known to contain viruses and/or malicious code are scanned.

Action

Specifies the action to perform whenever an infection is detected.

None (log only)

A message is logged in the log database, but no further action is taken.

Quarantine

Themail item is left in themail.box as dead mail and not routed to the recipient. A message is logged in the log database.

Delete

Themail item is deleted and not routed to the recipient. A message is logged in the log database.
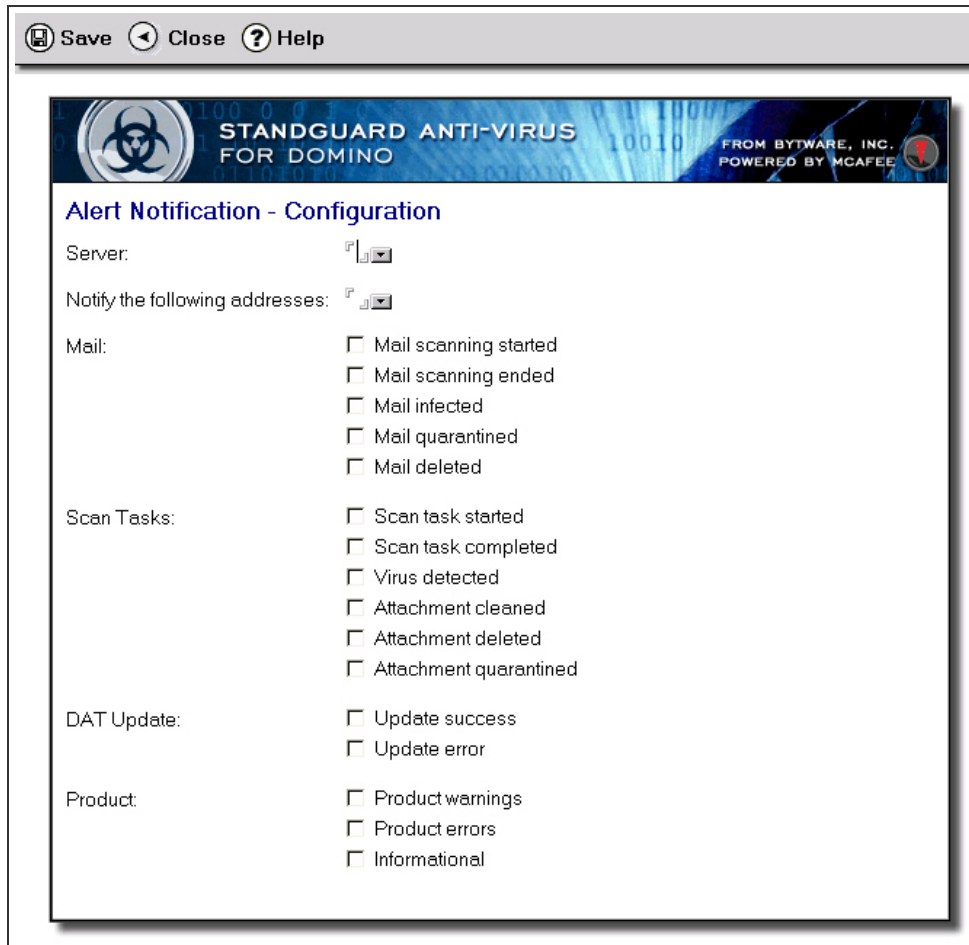
Footer text

Specifies the text to append to the bottom of mail that has been scanned and verified successfully.

When you have finished entering information, click Save, then Close.

Alert Configuration

Being notified when a potential threat is detected is an important part of protecting your environment. Alert documents specify who will be notified by email when important events occur. Alert documents are required if you want to receive alerts about various product activities and events.

To access the Alert configuration documents, go to the main application display, then click on Alerts, then New or Edit (in the toolbar).

Server (required)

Specifies the name of the server for which the alert monitor is being configured.

Notify the following addresses (required)

Specifies the email addresses of the recipient(s) to receive the alert.

Mail

Mail scanning started

Choose this option to be notified when mail scanning is activated for the server.

Mail scanning ended

Choose this option to be notified when mail scanning is ended for the server.

Mail infected

Choose this option to be notified when mail scanning detects an infected attachment.

Mail quarantined

Choose this option to be notified when mail scanning quarantines an infected mail document.

Mail deleted

Choose this option to be notified when mail scanning deletes an infected mail document.

Scan tasks

Scan task started

Choose this option to be notified when a scan task has started.

Scan task completed

Choose this option to be notified when a scan task has completed.

Virus detected

Choose this option to be notified when a scan task detects an infected document attachment.

Attachment cleaned

Choose this option to be notified when a scan task cleans an infected document attachment.

Attachment deleted

Choose this option to be notified when a scan task deletes an infected document attachment.

Attachment quarantined

Choose this option to be notified when a scan task quarantines an infected document attachment.

DAT Update

Update success

Choose this option to be notified when the DAT update process retrieves new virus definition files successfully.

Update error

Choose this option to be notified when the DAT update process fails to retrieve new virus definition files.

Product

Warnings

Choose this option to be notified when warning events occur.

Errors

Choose this option to be notified when error events occur.

Informational

Choose this option to be notified when informational events occur.

When you have finished entering information, click Save, then Close.

DAT Update Configuration

DAT Update is where you specify how and when the product will download new virus definitions. In addition, you can specify scheduling options to choose when the files will be downloaded at regular, recurring intervals. It is recommended that you download new DAT files every day.

To access the DAT Update configuration documents, go to the main application display, then click on DAT Update, then Edit (in the toolbar).

Server (required)

Specifies the name of the server for which the DAT Update is being configured.

DAT Version

Specifies the version and date of the virus definitions that are currently installed.

Transfer method

FTP (using defaults)

Choose this option to retrieve the virus definitions using FTP and the default FTP server (ftp.nai.com).

FTP (Custom)

Choose this option to retrieve the virus definitions using your own FTP server.

Path

Choose this option to retrieve the virus definitions using a path on your local network.

FTP Options

If you chose FTP as the transfer method, the following options allow you to further define the FTP parameters.

FTP Passive

Choose this option to use passive FTP, or select No to use active FTP. Turn this on if you want your server to establish the data connection to the FTP site instead of the site establishing the data connection to your server. This is recommended for most FTP sites, and it is absolutely necessary for some firewall and gateway configurations and when you get failed data channel errors. Note, however, that not all FTP sites support passive mode.

FTP Path

If you chose FTP (Custom) as the transfer method, specify the server and path name in the format //server name/path. If the files are located in the root path, you must end the server name with the root path name. For example: //192.168.1.1/.

FTP User and Password

If you chose FTP (Custom) as the transfer method, specify the FTP user name and password that will be used to log into the FTP server and retrieve the files.

Path Options

Directory

If you chose Path as the transfer method, specify the network path name where the dat files are located.

Schedule Options

Specifies the time when automatic updates will run.

None

Do not schedule the DAT Update process to run.

Daily

Run the DAT Update process every day. Choose the desired days and time you want to run the process.

Weekly

Run the DAT Update process once per week. Choose the desired day and time you want to run the process.

Monthly

Run the DAT Update process once per month (not recommended).

Retrieve only

Specifies if the new files will be retrieved but not installed.

Save extra copy

Specifies the additional path where the new files will be saved. Use this option if you have one system or partition downloading the files and want to copy the files to an additional location where the remaining systems can access them over the local network.

Run command after update

Specifies a system command to run after a successful download of new files. You could run a system command to save the information to tape, or notify an administrator, for example.

When you have finished entering information, click Save, then Close.

On-Demand Scanning - Configuration

On-Demand scanning documents specify how and when the product will scan Domino databases for infected attachments and malicious code. This scanning process is referred to as a scan task. You should create On-Demand scan tasks to perform scanning and cleaning activities on a recurring scheduled basis.
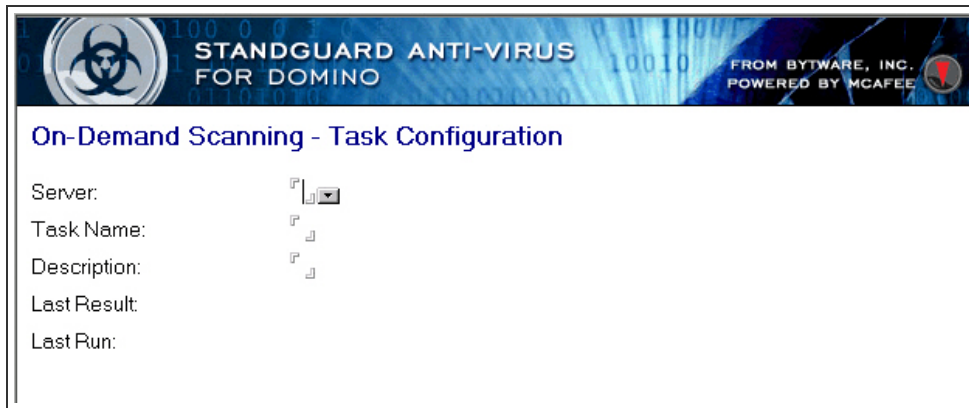
Server (required)

Specifies the name of the server for which the scan task is being configured.

Task name (required)

Specifies the short name of the task (8 characters or less). This name is used to create the job schedule entry, and to submit the scan task process to the system (job name).

Description

Specifies the optional descriptive name for the task.

Last result

The result from the last time the scan task was run is shown for your information. More detailed information can be seen using Log application.

Starting directory or database name (required)

Specifies the directory or database name where scanning will start. To specify the server's data directory, type and asterisk '*'. Directory or database names must be relative to the Domino server directory path.

Databases to omit from scan

Specifies the directory and database names to omit from scanning. Separate multiple values using comma's ",".

Skip files larger than

Specifies the maximum size of databases to scan. Databases larger than this size will not be scanned, for performance reasons. Specify 0 to scan all databases regardless of size.

Scan Options

Specifies the option that will be used to scan databases.

Scan compressed files (recommended)

Decompress executable files before scanning. Many programs use executable compressors to make the distribution file smaller, for example, PKLite. Unfortunately, packaged files can contain viruses that are compressed. You can use this parameter to decompress these files (in memory) and scan the internal image for viruses.

Enable file heuristics (recommended)

Use heuristic scanning to detect executable files that have code resembling malware.

Find suspicious programs

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

Scan archive files (recommended)

Decompress multi file archives before scanning. This parameter tells the product to scan inside archive formats. The list of formats includes ARJ, LHA, PKARC, PKZIP, RAR, TAR and WinACE files, and also BZIP and Zcompress single file compression. The list is frequently updated. Archive formats store a number of files within a single file. For example, a scan of a single .ZIP file results in many files being scanned.

Incremental scan

Select this option to scan only documents that have been created or changed since the last time the scan task was ran.

Macro analysis

Use heuristic scanning to detect unknown macro viruses.

File types to scan

Specifies the types of file attachments that will be scanned.

Scan all files (recommended)

All file types, regardless of extension, will be scanned.

Scan commonly infected files only (faster)

Only file types that are known to contain viruses and/or malicious code are scanned.

Run priority

Specifies the run priority for the job. Run priority is a value, ranging from 21 (highest priority) through 99 (lowest priority), that represents the priority at which the job competes for the processing unit relative to other jobs that are active at the same time. This value represents

the relative (not the absolute) importance of the job. For example, a job with a run priority of 25 is not twice as important as one with a run priority of 50.

Timeout

Specifies the number of minutes before the operation will timeout. Use this option to limit the number of minutes the task will run. The task will scan as many databases and attachments as possible within the time period before ending. The next time the task starts it will resume where it previously left off. If the task completes all files before timing out, it will start at the specified starting directory the next time it runs.

When an infection is found

Specifies the action the product will take when an infection is found.

Log and continue

An entry is logged to the log database, and no other actions are performed.

Clean attachment

An entry is logged to the log database, and the product will attempt to remove the infection from the attachment. If the infection cannot be removed, the 'If clean fails' action is performed.

Quarantine attachment

An entry is logged to the log database, and the product will move the infected attachment to the Quarantine database.

Delete attachment

An entry is logged to the log database, and the product will remove the infected attachment from the document.

If clean fails

If the above action is Clean attachment, this option specifies what action to perform if the attachment cannot be cleaned.

Quarantine attachment

An entry is logged to the log database, and the product will move the infected attachment to the Quarantine database.

Delete attachment

An entry is logged to the log database, and the product will remove the infected attachment from the document.

Schedule

Specifies the time when the task will run. When you specify a schedule, the product schedules the task using the ADDJOBSCDE command.

Once

Run the task once.

Daily

Run the task on the specified week days. Choose the desired days and time you want to run the process.

Monthly

Run the task once per month. Choose the desired day and time you want to run the process.

Logging

Specifies the type of information to record to the scan log. If you select >All files, detailed information about each file attachment in each database is recorded to the scan log.

When you have finished entering information, click Save, then Close.

Resources

McAfee Threat Library

Previously, choosing this option opened the McAfee Threat Library page. This option is no longer functional.

Submit a sample

Choose this option to go to Avert® Labs WebImmune. Here you can submit potentially infected files to WebImmune for analysis. You will receive information about your files, including solutions and real time fixes, if required.

Technical Support

Choose this option to go to the Fortra Support page where you can get online technical assistance, product updates, tips, advice, and support requests. You can speak directly with Fortra technical support specialists, and most questions can be answered online.

Monitoring

Fortra strongly recommends that you monitor the Powertech Antivirus for IBM i messages logged to the AVMSGQ to ensure an ongoing problem is noticed and remedied as soon as possible.

You can monitor the AVMSGQ message queue manually, or to insure timely notification, automate the monitoring with one of Fortra's products.

As important as it is to install antivirus protection on your server, it is equally important to know when problems occur. Important events that you need to monitor are:

1. When Powertech Antivirus for IBM i detected and removed a virus,
2. If virus definition files could not be retrieved; and
3. If the AVSVR job is ended or not running.

In addition, you could monitor other events, such as if a scan ended abnormally or did not run at all.

Manually monitoring the AVMSGQ message queue

To monitor the AVMSGQ manually, run the following command:

CHGMSGQ MSGQ(STANDGUARD/AVMSGQ) DLVRY(*BREAK) SEV(90)

Note: You will need to run this command each time you sign on, or automate the command into an initial sign-on program.

Automated monitoring of the AVMSGQ message queue

If you are using a monitor product, we recommend you monitor the AVMSGQ message queue for messages of severity 90 and higher. Add an action to page you or send emails to a list of operators or administrators.

In a multiple-system/partition environment, distribute the monitor to each system running Powertech Antivirus for IBM i.

We recommend you create an additional monitor to check for the absence of the completion message by a specific time. This will alert you to conditions where the automatic process is not starting, possibly due to a problem with the job schedule entry or job queue. In a multiple-system/partition environment, a monitor product can ensure all systems/partitions have reported the update process started and completed successfully, and notify an administrator with exceptions.

We recommend monitoring for the following messages:

Message ID	Message Text
AVC0305	&4 file(s)scanned in &6. &5 viruses found,&2 file(s)skipped, &3 error(s)
AVC1001	&1 violations found
AVE0105	Error(s)occurred running task '&1'. See messages in job &4/&3/&2
AVE0106	Task 'System virus scan task' completed with errors
AVE0107	Task '&23' completed with warnings. 0 viruses found , &4 file(s)scanned OK but &6 file(s)were not scanned due to errors
AVE0131	FILE …. IS INFECTED WITH
AVE0139	&13 virus(es)found. &6 file(s)not scanned due to errors

Message ID	Message Text
AVE0207	Error(s) occurred updating virus definitions.
AVI0601	WARNING: Virus definitions are older than 7 days
AVI9903	Powertech Anti-Virus support will end in &1 day(s)
AVI9904	Powertech Anti-Virus activation ends in &1 days
AVI9905	Powertech Anti-Virus E-mail scanning will end in &1 days
AVI9906	Powertech Anti-Virus on-access scanning will end in &1 days
BYT9901	License invalid or expired. Press Help for more information

Reference

The following includes a comprehensive reference of Powertech Antivirus for IBM i's functions.

Change Automatic Update Attributes (AVCHGUPDA)

> **NOTE:** See also Updating Virus Definitions.

Transfer method (FROM)

Specifies the transfer method that will be used to retrieve the new virus definition files.

*WGET The files will be downloaded using WGET, a utility that retrieves files using the HTTP protocol. This is the default setting.

*FTP The data will be downloaded using the IBM i FTP client. Please note that Trellix does not provide a FTP server. This option can be used to retrieve virus definitions from an internal server, for example.

*PATH The data will be retrieved from a network path. The path option is typically used in a network environment where you have one or more IBM i servers downloading from an FTP site and saving to a local path. This improves performance and security by using one IBM i server or partition to download the files to a secured share. The remaining servers or partitions can use this option to access the files over the local network.

Path (PATH)

Specifies the network path name that will be used to retrieve the virus definition files. This option applies only if the FROM keyword is *PATH. Use this option when you have another server or partition saving the files to a network path.

> **WGET string (WGET)** Specifies the base directory followed by any optional WGET parameters. This option applies only if the FROM keyword is *WGET.

> ***DFT** The files will be downloaded from http://update.nai.com/products/commonupdater.

> **WGET string** Specify the wget base directory followed by optional parameters. For example: `http://update.nai.com/products/commonupdater --verbose`

FTP location (FTP)

Specifies the host name and path that will be used to obtain the information. This option applies only when the FROM keyword is *FTP. To use a port other than the standard port 21, type a colon and the port number after the host name. For example: `ftp.myserver.com:2121` to use port 2121.

> NOTE: The system must be able to access the FTP site through any firewalls.

> **location-name** Specify the host name and path in the format domain/path.

FTP User (FTPUSR)

Specifies the remote user name to use when logging into the FTP server.

> ***ANONYMOUS** The user 'anonymous' will be used.
> **user-name** Specify the user name to use for the FTP login.

FTP Password (FTPPWD)

The password is stored unencrypted in file AVUPDATE, which has public *EXCLUDE authority. However, the password is sent to the FTP server unencrypted.

Specifies the password for the remote user name when logging into the FTP server. This parameter applies only when the FTP User (FTPUSER) is not *ANONYMOUS.

Schedule (SCHEDULE)

Specifies the type of scheduling for the command or process.

> ***DAILY** Run the update every day (recommended).

*WEEKLY Run the update once per week.
*MONTHLY Run the update once per month.
*NONE When you specify a schedule and press Enter, the product adds the job schedule entry AVUPDATE using the ADDJOBSCDE command. The job runs as user STANDGUARD.

Automatic update is disabled. This setting is not recommended unless you choose to handle automatic updating outside the product.

Day, Days, Time Specifies the specific time period for the automatic update process to run, depending on the choice selected for Schedule. For more information on the values allowed for these parameters, press Help.

Change On-Access Attributes (AVCHGA) Command

The AVCHGA command allows you to configure the settings for on-access scanning.

On-Access type (ACCESS)

*NONE On-Access scanning is disabled.

*OPEN Scan files during open processing if: 1) The file has never been scanned, or 2) The file has been modified since the last time it was scanned, or 3) The virus definitions have been updated since the last time it was scanned.

*OPNCLO Files will be scanned as they are opened and after they have been closed.

> NOTE: Close scanning occurs only when the last job has closed the file. If multiple jobs have a file open, the file will be scanned only when the last job has closed the file.

Clean infected files (CLEAN)

Specifies if the engine should remove the virus from the file ("clean"). If a file cannot be cleaned, the CLEANFAIL parameter provides a secondary choice.

*YES Attempt to remove viruses from infected files.
*NO Do not attempt to clean infected files.

Action if not cleaned (CLEANFAIL)

*QRN Move the infected file to the /Quarantied directory. The open of the file will be prevented. For more information see Quarantine.

*DELETE Delete the infected file. The open of the file will be prevented.

*NONE No action is performed. The open of the file will be prevented.

Heuristic analysis (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.

*YES Include heuristic analysis to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.
*NO Do not use heuristic analysis.

Macro analysis (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.

You can use both Macro Analysis and Heuristic Analysis as parameters, and the engine determines which heuristics to implement based on the file type.

*YES Include macro analysis to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.
*NO Do not use macro analysis.

Potentially unwanted programs (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.

*NO Do not scan for potentially unwanted programs.
*YES Scan for potentially unwanted programs.

Scan archives (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.

*YES Scan archive files to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.
*NO Do not scan archive files.

Files (FILES)

Specifies the types of files to include in scanning activities.

*DFT Scan only file types that are most susceptible to virus infection. This option safely narrows the scope of scan operations to files that are susceptible to virus infection and reduces the amount of time devoted to scanning files.

*ALL Scan all files. This attribute slows the engine's performance, but offers you the best protection against infection.

*ALLMACRO Expands scanning activities to include an examination of all files to determine if they contain known macro viruses. This attribute slows the engine's performance but offers you the best protection against infection from macro viruses. This option is faster than the *ALL files option, which examines every file for program viruses and macro viruses.

Exclude Directories (EXCL)

Even if a directory is omitted from on-access scanning, Powertech Antivirus for IBM i will still scan the directory if it is included in an on-demand scan task.

Specifies the list of directories to exclude from on-access scanning. Domino data directories are a good choice here, since Domino is known to have problems when it cannot open infected files. To exclude a single file, use the command **CHGATR OBJ(_file-name_) ATR (*SCAN) VALUE(*NO)**, where file-name is the fully qualified path of the object you want to exclude from scanning).

The maximum path length is 4096.

> TIP: To extend the command prompt, enter an ampersand (&) in the first position of the field, followed by a blank, and press Enter. Repeat this until the field is long enough, up to an additional 512 characters.
> To go beyond this size, the command needs to be entered without the prompt by using CALL QCMD and pressing F11.

Timeout (TIMEOUT)

Specifies the maximum number of seconds the product will spend scanning any one particular file during an on-access scan. After the specified number of seconds, the file is allowed to be opened and the file's scan status remains unchanged. The default setting is 30 (seconds).

Logging level (LOGLVL)

Specifies the amount of information logged to the avsvr.log file. Settings 2 and 3 can be used for troubleshooting but are not recommended for long term use as the log file can grow very large, and reduces scanning performance.

*NONE No information is logged.
1 Infections and actions about file cleaning and quarantine.

2 Everything from level 1 and file names.
3 Everything from level 2 and job names.

Configure Canary Files (AVCFGCNY)

The configure canary files (AVCFGCNY) command allows users to change the canary file settings. This command allows the user to add, change, and remove canary files.

```
                  Configure Canary Files (AVCFGCNY)

Type choices, press Enter.

Canary file  . . . . . . . . . . >  '/qgpl/encryptme'
Enabled  . . . . . . . . . . .     *YES          Name, *SAME, *YES, *NO







                                                           Bottom
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

How to Get There

Call command **AVCFGCNY**. Or, choose option **2** for a canary file on the Work with Canary Files screen.

Options

Canary File (CANARY)

Specify the filename and path of the canary file.

The possible values are:

Canary File Enter the filename and path of the canary file.

Enabled (ENABLED)

Specify the whether the canary file is enabled.

The possible values are:

*YES The canary file is enabled.
*NO The canary file is not enabled.

Delete canary files (DELETE)
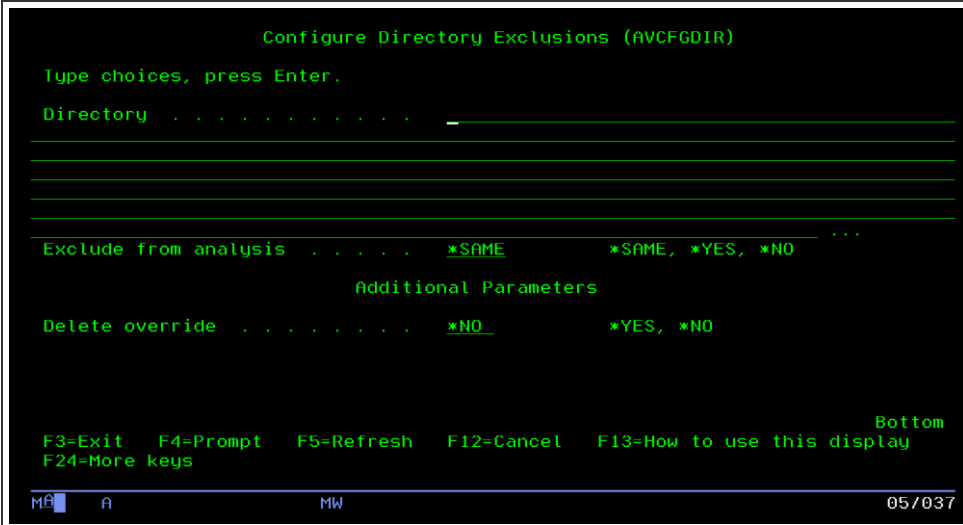
Specify whether to delete the canary files.

The possible values are:

*YES The canary file is deleted.
*NO The canary file is not deleted.

Configure Directory Exclusions (AVCFGDIR)

The configure directory exclusions (AVCFGDIR) command allows users to configure APEX directory exclusions. This command allows the user to add, change, and remove APEX directory exclusions.

```
              Configure Directory Exclusions (AVCFGDIR)
  Type choices, press Enter.

  Directory  . . . . . . . . . .   _

  _____
  _____
  _____
  _____
  _____
  _____   ...
  Exclude from analysis  . . . . .   *SAME          *SAME, *YES, *NO

                      Additional Parameters

  Delete override  . . . . . . . .   *NO            *YES, *NO



                                                        Bottom
  F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
  F24=More keys
  MA    A             MW                                    05/037
```

How to Get There

Call command **AVCFGDIR**. Or, choose option **2** for a user on the Work with Directory Exclusions (AVWRKDIR) screen.

Options

Directory (DIR)

Specify the directory being overridden.
> The possible values are:

> **Directory** Enter the path of the directory being overridden.

Exclude (EXCLUDE)

Specify the exclude.
> The possible values are:

> ***YES** The directory is excluded from analysis.
> ***NO** The directory is not excluded from analysis.

Delete directory overrides (DELETE)

Specify whether to delete the directory overrides.
> The possible values are:

> ***YES** The directory override is deleted.
> ***NO** The directory override is not deleted.

Configure Integrity Scan Task (AVCFGITGT)

The AVCFGITGT command allows you to configure the settings for an object integrity scanning task. Object integrity tasks scan the operating system for missing and invalid signatures, and user libraries for patched programs.

Task name

Specifies the name or description of the task. The task name is used to configure and run tasks. To change an existing task, press F4 and type the name of the task you want to change, then press Enter. To create a new task, type the name of the task you want to create and press Enter.

> ***SYS** The system default task.

> **task-name** Specify the name of a task to create or use.

Task type

Specifies the type of object integrity scanning task.

> ***LIB** Library object integrity task

> ***USER** User object integrity task

Libraries

Specifies the libraries of the objects to check integrity.

> ***IBM** All libraries in the auxiliary storage pools (ASPs) defined by the ASP device (ASPDEV) parameter which are saved and restored using the SAVLIB and RSTLIB CL commands with *IBM specified for the Library (LIB) parameter are shown.

> ***ALLUSR** All libraries with names that do not begin with the letter Q except for the following:

>> #CGULIB #DSULIB #SEULIB
>> #COBLIB #RPGLIB
>> #DFULIB #SDALIB

> Although the following libraries with names that begin with the letter Q are provided by IBM, they typically contain user data that changes frequently. Therefore, these libraries are also considered user libraries:

>> QDSNX QRCLxxxxx QUSRIJS QUSRVxRxMx
>> QGPL QSRVAGT QUSRINFSKR
>> QGPL38 QSYS2 QUSRNOTES
>> QMGTC QSYS2xxxxx QUSROND
>> QMGTC2 QS36F QUSRPOSGS

generic-name

Specify the generic name of the objects to be shown. A generic name is specified as a character string that contains one or more characters followed by an asterisk (*). A generic name specifies objects that have names with the same prefix as the generic object name for which you have some authority (except exclude (*EXCLUDE) authority).

> **library name** Specify the name of the library to be scanned.

> **Users** Specifies the list of users to check integrity. Objects owned by the specified users are checked.

generic-name Specify the generic name of the objects to be shown. A generic name is specified as a character string that contains one or more characters followed by an asterisk (*). A generic name specifies objects that have names with the same prefix as the generic object name for which you have some authority (except exclude (*EXCLUDE) authority).

user name Specify the name of the user to be scanned.

Omit

The list of objects to exclude from scanning.

If you are working with library scan tasks, specify the library name you want to exclude. For example, ABCLIB will exclude library ABCLIB. ABC* will exclude all libraries starting with ABC.

If you are working with user scan tasks, specify the user name you want to exclude. For example, USER1 will exclude user USER1. USER* will exclude all users starting with USER.

To exclude an object from checking, specify the QSYS.LIB path name of the object. For example, to exclude PGM1 from LIBA, specify /QSYS.LIB/LIBA.LIB/PGM1.PGM.

Check signatures

The digital signatures of objects that can be signed will be checked.

Most objects in user libraries are not signed. Using CHKSIG(*ALL) on user libraries will log an error for every object in the library -- probably not what you want. All IBM objects are signed, so use CHKSIG(*ALL) on all IBM libraries, and CHKSIG(*SIGNED) on user libraries that are not signed.

***SIGNED** Objects with digital signatures are checked. Any object with a signature that is not valid will be logged.

***ALL** All objects that can be digitally signed are checked. Any object that can be signed but has no signature will be logged. Any object with a signature that is not valid will be logged. Use this option with LIB(*IBM) to ensure there are no unsigned objects in IBM libraries.

Force program re-creation

Specifies whether re-creation of patched programs is forced.

To be eligible for re-creation, OPM programs must have all observability and ILE programs must have all observable creation data. Use the Display Program (DSPPGM) command to determine whether a program is observable or has all observable creation data. Unobservable creation data cannot be used by CHGPGM.

*NO Patched programs will not be recreated.
*YES Patched programs will be recreated.

Output

Specifies where output from program should be sent.

* The output is sent to the display. If the job is a batch job, the output is spooled to an output queue.
*LOGFILE The output is sent to an IFS stream file in the logs directory.
*PRINT The output is spooled to an output queue.

Schedule

Specifies the type of scheduling for the command or process.

*NONE Do not schedule the command or process to run.
*DAILY Run the command or process every day.
*WEEKLY Run the command or process on the same day once per week.
*MONTHLY Run the command or process on the same day each month.

Days

Specifies the days to perform the task.

*SUN Sundays
*MON Mondays
*TUE Tuesdays
*WED Wednesdays
*THR Thursdays
*FRI Fridays
*SAT Saturdays

Day

Specifies the day of the week to perform the task.

*SUN Sundays
*MON Mondays
*TUE Tuesdays
*WED Wednesdays
*THR Thursdays
*FRI Fridays
*SAT Saturdays

Day

Specifies the day of the month (1 - 31) to perform the task.

Schedule time Specifies the time perform the task.

Run priority Specifies the run priority for the job. Run priority is a value, ranging from 1 (highest priority) through 99 (lowest priority), that represents the priority at which the job competes for the processing unit relative to other jobs that are active at the same time. This value represents the relative (not the absolute) importance of the job. For example, a job with a run priority of 25 is not twice as important as one with a run priority of 50.

Delete

Specifies to delete the record or job.

> ***YES** The record or job will be deleted.
> ***NO** Do not delete the record or job.

Configure Scan Task (AVCFGTSK) Command

Restrictions

The user running the command must either have *ALLOBJ authority OR have *RX authority to all files and directories referenced on the OBJ parameter, and *RWX authority for cleaning of any viruses. We recommend running the command under a profile with *ALLOBJ authority to ensure complete scanning and cleaning. The Integrated File System does not recognize adopted authorities. Therefore, you cannot use the command in a CL program that adopts authority. The actual job user must have the required authorities to properly scan files.

Parameters

Task name (TASK)

Specifies the name or description of the task. The task name is used to configure and run tasks. To change an existing task, press F4 and type the name of the task you want to change, then press Enter. To create a new task, type the name of the task you want to create and press Enter.

> ***SYS** The system default task.
> **task-name** Specify the name of a task to create or use.

Objects (OBJ)

This is the object (starting path or filename) to scan.

Examples:

The following file systems are always excluded from scanning (even if they are specified in the starting path). This may not be a complete list. In general, only local file systems can be scanned (not network files).

- QSYS.LIB
- QNTC
- QFileSvr.400
- QTCPTMM
1. To scan the entire Integrated File System, specify '/'.
2. To scan only the /QIBM directory, specify '/QIBM'.

Directory subtree (SUBTREE)

Specifies if files contained in subfolders relative to the starting path are scanned.

*ALL Files within subfolders of the starting path will be scanned. If the subfolders also contain subfolders, they will also be scanned, and so on. If you want to exclude a folder within a subfolder, see the Exclude paths (EXCL) parameter.

*NONE To exclude directories within the subtree use the following OMIT parameter. Do not scan subfolders. If the subfolders contain additional files and folders, they will not be scanned.

Omit (OMIT)

Specifies the list of directories to exclude from scanning.

Heuristic analysis (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.

*YES Include heuristic analysis to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.

*NO Do not use heuristic analysis.

Macro analysis (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.

You can use both Macro analysis and Heuristic analysis as parameters, and the engine determines which heuristics to implement based on the file type.

> ***YES** Include macro analysis to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.
> ***NO** Do not use macro analysis.

Potentially unwanted programs (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.

> ***NO** Do not scan for potentially unwanted programs.
> ***YES** Scan for potentially unwanted programs.

Scan archives (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.

> ***YES** Scan archive files to find new viruses. This attribute slows the engine's performance and consumes additional processor resources.
> ***NO** Do not scan archive files.

Clean infected files (CLEAN)

Specifies if the engine should remove the virus from the file ("clean"). If a file cannot be cleaned, the Clean failure action (CLEANFAIL) parameter provides a secondary choice.

> ***YES** Clean the infected file(s) by removing the virus.
> ***NO** Do not clean infected files.

Clean failure action (CLEANFAIL)

Specifies the secondary action if the file cannot be cleaned.

> ***QRN** Move or create a link in the quarantine folder to the infected file. Whether a link is created or the file is moved depends on the file system where the virus was found. For more information about quarantining files see Quarantine.

*DELETE Delete the file. These files are first overwritten with zeros, made zero length and then deleted using an operating system call. Therefore, you cannot undelete these files.

*NONE No action is performed. Use this option with caution as any viruses that are found and cannot be cleaned are left in place and still present a threat.

Files (FILES)

Specifies the types of files to include in scanning activities.

*ALL Scan all files. This attribute slows the engine's performance, but offers you the best protection against infection.

*DFT Scan only file types that are most susceptible to virus infection. This option safely narrows the scope of scan operations to files that are susceptible to virus infection and reduces the amount of time devoted to scanning files.

*ALLMACRO Expands scanning activities to include an examination of all files to determine if they contain known macro viruses. This attribute slows the engine's performance but offers you the best protection against infection from macro viruses. This option is faster than the *ALL files option, which examines every file for program viruses and macro viruses.

Force (FORCE)

Specifies if you want to recognize or override the object's scan settings when performing this scan. The object's scan settings can be seen using the **WRKLNK** command and choosing option 8 to view the object's attributes as seen below:

```
Object scanning . . . . . . . . . . . : *YES
Scan status . . . . . . . . . . . . . : *SUCCESS
Scan signatures different . . . . . : No
Binary scan . . . . . . . . . . . . . : Yes
CCSID scan . . . . . . . . . . . . . : 0
```

The scan settings for an object can be changed using the **CHGATR ATTR(*SCAN)** command.

*NONE The object's scan settings will be utilized. This is the default. Objects set to 'Object scanning *NO' will not be scanned. Objects set to 'Object scanning *CHGONLY' will not be scanned unless the object has changed ('Scan status *REQUIRED').

*ALL All files will be scanned regardless of the 'Object scanning' parameter, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES'). This option can be useful to periodically scan objects that would normally be skipped from scanning.

*NOSCAN Files that have been configured with 'Object scanning *NO' will be scanned, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES').

*CHGONLY Files that have been configured with 'Object scanning *CHGONLY' will be scanned even though the object has not changed, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES').

Output (OUTPUT)

Specifies where output from the program should be sent.

*LOGFILE The output is sent to an IFS stream file in the logs directory.
*PRINT The output is spooled to an output queue.

Schedule (SCHEDULE)

Specifies when to schedule the task. When you specify a schedule and press Enter, the product schedules the job AVRUNTSK using the ADDJOBSCHDE command.

*NONE Do not schedule the command or process to run. Tasks that are configured but not scheduled need to be run manually using the AVRUNTSK command.
*DAILY Run the command or process every day.
*WEEKLY Run the command or process on the same day once per week.
*MONTHLY Run the command or process on the same day each month.

Additional Parameters

The following parameters appear when you prompt the command and press F9 for All parameters.

Days (SCHEDDAYS)

Specifies the days to perform the task.

*ALL Schedule the task to run every day.
*SUN Schedule the task to run every Sunday.
*MON Schedule the task to run every Monday.
*TUE Schedule the task to run every Tuesday.
*WED Schedule the task to run every Wednesday.
*THR Schedule the task to run every Thursday.
*FRI Schedule the task to run every Friday.
*SAT Schedule the task to run every Saturday.

Time (SCHEDTIME)

Specifies the time to run the task.

Run priority (RUNPTY)

Specifies the job run priority for the task. The value can be in the range of 11 - 99, where 11 is the highest priority and 99 is the lowest. 99 will have the least impact on other jobs but will take longer to run.

Logging level (LOGLVL)

Specifies the number of directory levels listed in the scan log.

>***DETAILED** Detailed information is logged. Detailed logging contains more information than *SUMMARY but less than *FULL.
>***SUMMARY** Summary information is logged.
>***FULL** All information is logged.

Timeout minutes (TIMEOUT)

Specifies the number of minutes the scan task will run before the operation times out. Use this option to limit the time for long-running scan tasks to complete. Incomplete scan tasks will automatically resume scanning from the last directory on the next run of the task. For example, if a complete scan requires 8 hours but is configured with a 240 minute timeout (and is scheduled to run daily), then you will get a complete scan every other day.

>***NONE** The task will run as long as necessary to completion without timing out.
>**minutes** The task will time out after the specified number of minutes. Note: The timeout is checked after each directory is scanned and will not timeout in the middle of a directory. Therefore, the task may run longer than the specified number of minutes as needed to establish a directory boundary.

Host (HOST)

Specifies the name of the NFS host where the files are stored. Use this option to scan files and directories on Linux and AIX partitions. To use this option you must export the root directory on the specified host with read/write and allow root access (no_root_squash). When you specify a host name, the root file system will be mounted using the Network File System (NFS) to a temporary directory, the files and directories will be scanned, and the file system unmounted. You can determine the host name using the DSPNWSD command.

>***LOCAL** The start path is located on the local file system.
>**hostname** The start path is located on the specified NFS host. You must have *ALLOBJ authority for this option to work correctly.

Delete (DELETE)
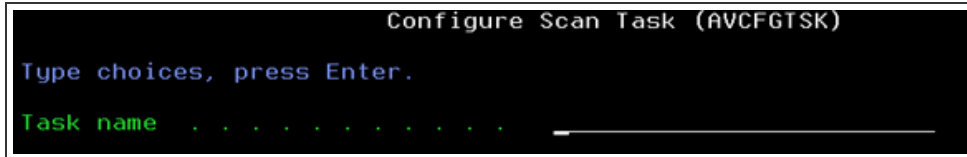
Specifies if you want to delete or change the task.

*NO The task will be changed or created.
*YES The task will be deleted. All other parameters except the task name are ignored.

NOTE:
At the beginning of 'Configure Scan Task' (AVCFGTSK) there is the option to submit a 'Task name'.

```
                  Configure Scan Task (AVCFGTSK)

Type choices, press Enter.

Task name  . . . . . . . . . . .    _____
```

You can create one by entering the desired name, but if you select the default (*SYS), there is a restriction: The default task name *SYS cannot be deleted, so if you select *YES for *SYS, it will not be deleted. Only 'customized' tasks named anything other than *SYS will be able to be deleted using this *YES option.

Configure User Overrides (AVCFGUSR)

The Configure User Overrides (AVCFGUSR) command allows you to specify overriding settings for the specified user. This command allows you to add, change, and remove user overrides.

When a user has been automatically blocked by the anti-ransomware software, this command can be used to re-enable their profile.

NOTE: When anti-ransomware blocks a user, the job logs for the IBM file server jobs can contain the message "The exit program does not allow you to perform the requested operation." This is NOT an error. This is anti-ransomware doing its job of blocking a user.

```
              Configure User Overrides (AVCFGUSR)

Type choices, press Enter.

User . . . . . . . . . . . . . > AWEIGOLD      Name
Send message on threshold  . . .  *DFT         Number, *NEVER, *DFT, *SAME
Block user on threshold  . . . .  *DFT         Number, *NEVER, *DFT, *SAME
User is currently blocked  . . .  *YES         *YES, *NO, *SAME

                                                                       Bottom
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

How to Get There

Call command **AVCFGUSR**. Or, choose option **2** for a user on the Work with User Overrides (AVWRKUSR) screen.

Options

User (USR)

Specify the user name, for whom the settings are being overridden.

The possible values are:

> **User** Enter the user.

Send message on threshold (MSGTHR)

Specify the threshold value to be used to determine when a message will be sent, warning of a possible ransomware attack.

The lower this value is, the more likely it is that a message may be sent in error, i.e. a false positive.

The higher this value is, the less likely it is that a message may be sent in error, but more likely that a ransomware attack may go unreported.

The possible values are:

Threshold Value Enter the threshold value.
*NEVER When *NEVER is specified a message will never be sent
*SAME When *SAME is specified, the threshold value will remain unchanged.

Block user on threshold (BLKTHR)

Specify the threshold value to be used to determine when a user will be blocked, in response to a possible ransomware attack.

The lower this value is, the more likely it is that a user may be blocked in error, i.e. a false positive.

The higher this value is, the less likely it is that a user may be blocked in error, but more likely that a ransomware attack may go unchallenged.

The possible values are:

Threshold Value Enter the threshold value.
*NEVER When *NEVER is specified a message will never be sent
*SAME When *SAME is specified, the threshold value will remain unchanged.

User is currently blocked (BLOCKED)

Specify whether the user is currently blocked.

The possible values are:

*YES The user is currently blocked.
*NO The user is not currently blocked.

Delete override (DELETE)

Specify whether to delete the user override.

The possible values are:

*YES The user override is deleted.
*NO The user override is not deleted.

Powertech Antivirus Scan (AVSCAN)

The AVSCAN command scans the Integrated File System (IFS) for viruses.

Parameters

File or Directory (OBJ)

The file or directory name to scan.

> NOTE: Note: You can see a list of files and directories on the system using the WRKLNK command. To scan a NFS mountable directory, specify the path as hostname:pathname.

/ All files and directories on the system will be scanned
file or directory The specified file or directory will be scanned.

Directory subtree (SUBTREE)

Specifies if files contained in subfolders relative to the starting path are scanned.

*ALL Files within subfolders of the starting path will be scanned. If the subfolders also contain subfolders, they will also be scanned, and so on. If you want to exclude a folder within a subfolder, see the Exclude paths (EXCL) parameter.

*NONE Do not scan subfolders. If the subfolders contain additional files and folders, they will not be scanned.

Heuristic analysis (HEURISTIC)

Include heuristic analysis to find new viruses. When you use heuristic analysis, the scanning engine employs heuristic technology to detect new viruses in executable files (programs). Without this option, the engine can only find viruses that are already known.

*YES Include heuristic analysis to find new viruses. This attribute slows the engine's performance.
*NO Do not use heuristic analysis.

Macro analysis (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. You can use both Macro Analysis and Heuristic Analysis as parameters, and the engine determines which heuristics to implement based on the file type.

*YES Include macro analysis to find new viruses. This attribute slows the engine's performance.

*NO Do not use macro analysis.

Potentially unwanted programs (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 can pose a security threat.

*NO Do not scan for potentially unwanted programs.
*YES Scan for potentially unwanted programs.

Scan archives (ARCHIVES)

Specifies if you want scanning activities to include archive files. Archive files contain imbedded files and usually end with one of the following extensions: .ZIP, .CAB, .LZH, JAR and .UUE.

This option will also permit scanning of MSCompress files, which display the ??_ extension.

*YES Scan archive files to find new viruses. This attribute slows the engine's performance.
*NO Do not scan archive files.

Scan MIME (MIME)

Specifies if you want to check files for MIME encoded content.

*YES Check files for MIME content.
*NO Do not check files for MIME content.

Clean infected files (CLEAN)

Specifies if infected files should be cleaned whenever possible.

*YES Clean infected files by removing the virus.
*NO Do not clean infected files.

Action if not cleaned (CLEANFAIL)

Specifies the action to perform on infected files that could not be cleaned.

*QRN Move the infected file to the /Quarantied directory. The open of the file will be prevented.
*DELETE Delete the infected file. The open of the file will be prevented.
*NONE No action will be performed. The open of the file will be prevented.

Scan file types (FILES)

Specifies the extension types to include in scanning activities. By default, the engine normally checks that the three-letter file extension matches one that it knows. You can use this parameter to enable the engine to scan for more extensions than are normally scanned. This is useful for clean-up operations or where a new virus affects a file type that was not previously affected. When you specify a file extension, case is not relevant. For example, "abc" is the same as "ABC", "aBC" and so on.

> ***ALL** Scan all files for new viruses. This attribute slows the engine's performance, but offers you the best protection against infection.

> ***DFT** Scan only file types that are most susceptible to virus infection. This option safely narrows the scope of scan operations to files that are susceptible to virus infection and reduces the amount of time devoted to scanning files.

> ***ALLMACRO** Expands scanning activities to include an examination of all files to determine if they contain known macro viruses. This attribute slows the engine's performance, but offers you the best protection against infection from macro viruses. This option is faster than the *ALL files option, which examines every file for program viruses and macro viruses.

Force (FORCE)

Specifies if you want to recognize or override the object's scan settings when performing this scan. The object's scan settings can be seen using the WRKLNK command and choosing option 8 to view the object's attributes as seen below:

Object scanning ....: *YES

> Scan status ....: *SUCCESS
> Scan signatures different ......: No
> Binary scan ....: Yes
> CCSID scan ....: 0

The scan settings for an object can be changed using the CHGATR ATTR(*SCAN) command.

> ***NONE** The object's scan settings will be utilized. This is the default. Objects set to 'Object scanning *NO' will not be scanned. Objects set to 'Object scanning *CHGONLY' will not be scanned unless the object has changed ('Scan status *REQUIRED').

> ***ALL** All files will be scanned regardless of the 'Object scanning' parameter, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES'). This option can be useful to periodically scan objects that would normally be skipped from scanning.

*NOSCAN Files that have been configured with 'Object scanning *NO' will be scanned, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES').

*CHGONLY Files that have been configured with 'Object scanning *CHGONLY' will be scanned even though the object has not changed, provided the virus definitions have been updated to a newer level since the object was last scanned ('Scan signatures different *YES').

Exclude files or paths (EXCL)

Specifies the list of directories (and subdirectories) to exclude from scanning. To exclude a single file, use the command CHGATR OBJ(file-name) ATR(*SCAN) VALUE(*NO), where file-name is the fully qualified path of the object you want to exclude.

*NONE All files will be scanned.

path-name Specifies the list of directories to exclude from scanning. This will exclude the specified directory and all of its subdirectories from the on-access scanning.

Logging Level (LOGLVL)

Specifies the level of detail that will be printed on the scan report.

*DETAILED Several directory levels will be printed.
*SUMMARY One directory level will be printed.
*FULL All directory levels will be printed.
1-99 Specifies the number of directory levels to print.

Output (OUTPUT)

Specifies where output from program should be sent.

* The output is sent to the display. If the job is a batch job, the output is spooled to an output queue.
path-name The output is sent to an IFS stream file.

Timeout minutes (TIMEOUT)

The time-out is applied after the scanning of each directory. If the configured time-out is reached after only some of the files in a directory have been scanned, the scanning will continue until all files in that directory have been scanned.

*NONE The operation will run as long as necessary to completion without timing out.
minutes The operation will time out after the specified number of minutes.

Restart (RESTART)

Specifies if the scan is to restart from a previous timeout.

*NO The scan will start from the specified start path.
*YES The scan will resume from the last directory of the previous start path. If the previous scan completed without timeout, then the scan will start from the specified start path.

Powertech AV Installation (AVINSTALL)

The AVINSTALL command is used to install the Powertech Antivirus for IBM i software.

```
                  PowerTech AV Installation (AVINSTALL)

 Type choices, press Enter.

 Optional part to be restored . . >  *BASE         Number, *BASE, *ALL
 Library  . . . . . . . . . . . >  *SAME         Character value, *DFT, *SAME
 Code home directory  . . . . . >  *SAME

 Show main menu . . . . . . . . >  *NO           *YES, *NO




                                                             Bottom
 F9=All parameters   F11=Keywords   F14=Command string   F24=More keys
```

How to Get There

1. After installation from a PC, sign on to the IBM i and call HSLOADMGR/HSWRKLOAD.
2. For Powertech Antivirus, enter 1.

Options

Antivirus Installation (AVINSTALL)

The AVINSTALL command is used to install the Powertech Antivirus for IBM i software.

Optional part to be restored

Specifies which optional part of the Powertech Antivirus for IBM i software is to be installed.

The possible values are:

*ALL Installs all components.
*BASE Installs the main Powertech Antivirus for IBM i software.
2 Installs the ops navigator plugin for Powertech Antivirus for IBM i.
3 Installs Powertech Antivirus for Domino.

Library

Specify a library for the Powertech Antivirus for IBM isoftware.

The possible values are:

*SAME While upgrading, this option specifies the software will be installed into a library of the same name as the existing Powertech Antivirus for IBM i library. Note: If this is a first-time installation, the *DFT value will be used.

*DFT Install the software into the default library STANDGUARD.

Code home directory

Specify a directory for the Powertech Antivirus for IBM i software.

The possible values are:

*SAME While upgrading, this option specifies the software will be installed into the same directory as the current Powertech Antivirus for IBM i Code home directory. Note: If this is a first-time installation, the *DFT value will be used.

*DFT Install the software into the default Code home directory of /standguard.

Show Main Menu

Specifies whether the Powertech Antivirus for IBM i Main Menu will be shown at the end of the installation.

The possible values are:

*YES The Main Menu will be shown at the end of the installation.
*NO The Main Menu will not be shown at the end of the installation.

Run AV Scan Task (AVRUNTSK) Command

The Run AV Scan Task (AVRUNTSK) command is used to run a scan task. If you configured the task to run on schedule, then the task will run automatically at the specified time. However if you did not schedule the task, then the AVRUNTSK command must be used to start the task manually. You can submit a scan task using option 1 on the Main menu.

Do not run AVRUNTSK (or AVSCAN) commands interactively unless you are running in a restricted state. Virus scanning is very CPU intensive and running the command interactively will likely slow down other jobs on the system.

The results of scan tasks can be seen using Main menu option 11 (Display Messages), and option 10 (Work with logs).

See On-Demand Scanning.

Work with Exit Program Integration (WRKEXTPGM) Command

The Work with Exit Program Integration (WRKEXTPGM) command is used to configure exit program integration. See Overview of Exit Program Integration.

> **IMPORTANT:**
> The command should be used only in the following two situations:
> 1. To add an exit program to one of the exit points supported by the integration, if the product does not support automatic exit point integration.
> 2. At the direction of Powertech Technical Support.

This command has no parameters and displays the Exit Program Integration screen.

```
 GSCEXTMNT.01                 Fortra IBM i Products
                            Exit Program Integration

 Type options, press Enter.
    2=Change   4=Unregister   6=Restart Server   7=WRKREGINF


                                                ---- Product Exit ----
Opt   Exit Point            Format   Product         Pgm Lib      Program
      QIBM_QPWFS_FILE_SERV  PWFS0100 ANTIVIRUS       STANDGUARD   AVRWFSX
 _    QIBM_QPWFS_FILE_SERV  PWFS0100 ENCRYPTION      CRYPTO       CRRP042

 _    QIBM_QP0L_SCAN_OPEN   SCOP0100 ANTIVIRUS       STANDGUARD   AVOAOCX




                                                               Bottom
    F3=Exit     F5=Refresh        F6=Add Exit Pgm      F12=Previous
```

License Keys

When you license Powertech Antivirus for IBM i, you will be provided two license keys. The first license key is for the use of the Powertech Antivirus for IBM i product. The second key is for the product support. If you have a partitioned system, you will need to enter these keys into each partition that is licensed for Powertech Antivirus for IBM i.

Product license key

This license key allows you to run the Powertech Antivirus for IBM i scanning programs for either a temporary or permanent term limit. For permanent usage, this key will not need to be re-entered unless your hardware changes. For temporary usage, this key will allow you to run the scanning programs until an expiration date is reached.

Domino license key

This license key allows you to run the Powertech Antivirus for Domino scanning programs for either a temporary or permanent term limit. For permanent usage, this key will not need to be re-entered unless your hardware changes. For temporary usage, this key will allow you to run the scanning programs until an expiration date is reached.

Support license key

This license key allows you to download the support files needed to keep the scanning product up-to-date with the latest virus definition files, and any program enhancements and fixes to the product. This key is provided for a temporary term, typically one (1) year. A new key will need to be entered before the expiration date to ensure you are protected against the latest virus threats.

Powertech Antivirus Menus

Main Menu

The following describes the Powertech Antivirus for IBM i Main Menu.

```
AVMENU                 Powertech Antivirus Main Menu
                                                    System:
Select one of the following:

     1. Submit a virus scan task
     2. Submit an object integrity scan task
     3. Work with scan jobs
     4. Work with job schedule entries

    10. Work with logs
    11. Display messages
    12. Work with quarantined files

    20. Download latest virus definitions (DATs)
    21. Download latest program updates (PTFs)

    50. Setup Menu
    51. Support Menu
    52. License Menu
                                                    Bottom
Selection or command
===> _
F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F10=Commands   F12=Cancel
(c) Copyright Help/Systems, LLC.              >Powered by McAfee
```

How To Get There

Type **STANDGUARD/AVMENU** (or just AVMENU) at a command line and press Enter.

Options

1. Submit a virus scan task

Select this option to submit a virus scan task. A virus scan task is a list of directories and options that control scanning parameters. A default task (named *SYS) is provided as a starting point for you to scan the entire system using recommended values. You can choose to start the scan immediately, or schedule it to run at a later time. For more information about creating, changing and running scan tasks, see On-Demand Scanning.

2. Submit an object integrity scan task

Select this option to submit an object integrity scan task. An object integrity scan task is a list of libraries and options that control an object integrity scan. A default task (named *SYS) is provided as a starting point for you to scan the entire system using recommended values. You can choose to start the scan immediately, or schedule it to run at a later time. For more information about creating, changing and running object integrity scan tasks, see Object Integrity scanning.

3. Work with scan jobs

Select this option to work with scan jobs that have been started as a result of options 1 or 2, as well as any jobs that have started automatically as a result of scheduling a scan task. To schedule a task to run automatically at recurring intervals, see On-Demand Scanning.

4. Work with job schedule entries

Select this option to work with job schedule entries that have been created as a result of configuring scan tasks and automatic updates. You can use this option to see a quick display of what jobs are scheduled to run.

10. Work with logs

Select this option to view the log files from Powertech Antivirus for IBM i activities. Log files are generated from Object Integrity Scanning, on-demand scanning, Virus Definition Updates, and Program Updates (PTF) activities (see About PTFs). You can use this display to see the results of the last automatic update or scan task.

11. Display messages

Select this option to view important messages from Powertech Antivirus for IBM i activities.

12. Work with quarantined files

Select this option to work with files that have been moved to the quarantine location. For more information about quarantine, see Quarantine.

20. Download latest virus definitions (DATs)

Select this option to download the latest virus definitions. These definitions will ensure that your virus protection is constantly updated as cures for new virus threats are published. For more information, see Updating Virus Definitions (DATs).

21. Download latest program updates (PTFs)

This option formerly (prior to version 8.2) could be used to download the latest program temporary fixes (PTFs). See About PTFs.

50. Setup Menu

Select this option to view the Powertech Antivirus Setup Menu. The Setup Menu provides the options needed to configure the product.

51. Support Menu

Select this option to view the Support Menu. The Support Menu provides many useful items for maintaining and supporting the use of the product.

52. License Menu

Select this option to view the License Menu. The License Menu provides options for maintaining and supporting the product license.

Powertech Antivirus Setup Menu

The Setup Menu provides options to configure product settings. To access the Setup menu, choose option 50 from the Main menu, or run the command GO STANDGUARD/AVSETUP.

```
AVSETUP                  Powertech Antivirus Setup Menu
                                                         System:
Select one of the following:

     1. On-access scanning
     2. Automatic virus definition updates (DATs)

     4. QMSF Mail scanning
     5. Object integrity scan tasks
     6. Virus scan tasks
     7. Change *ALLOBJ Profile

    10. Anti-Ransomware Settings

    30. Work with job schedule entries




                                                         Bottom
Selection or command
===> _
F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F10=Command Entry   F12=Cancel
```

Options

1. On-Access scanning

Select this option to enable or disable on-access scanning, and change options that affect on-access scanning performance. On-Access scanning allows you to scan files dynamically as they are opened and/or modified. For more information about on-access scanning see On-Access Scanning.

2. Automatic virus definition updates (DATs)

Select this option to schedule and configure settings for updating virus definitions. For more information about virus definitions see Updating Virus Definitions.

3. Automatic program updates (PTFs)

Select this option to schedule and configure settings for updating program temporary fixes (PTFs).

> **NOTE:** PTFs are no longer issued for product updates. See About PTFs.

4. QMSF Mail scanning

Select this option to configure settings for scanning IBM i mail. For more information, see Email Scanning.

5. Object integrity scan tasks

Select this option to schedule and configure object integrity scan tasks. For more information, see Object Integrity Scanning.

6. Virus scan tasks

Select this option to schedule and configure virus scan tasks. For more information, see On-Demand Scanning.

7. Change *ALLOBJ Profile

Select this option to view or change the *ALLOBJ profile that Powertech Antivirus uses to perform tasks that require special authorities. This includes the AVSVR and AVINSITE jobs and the execution of DAT updates. The default is QSECOFR. You can use an existing profile but you must ensure the profile has *ALLOBJ, *JOBCTL, and *SECADM authority and is not disabled. A password is not required or used.

After changing the *ALLOBJ profile, the AVSVR and AVINSITE jobs will continue to run under the old *ALLOBJ profile until restarted by a DAT update, an IPL, or manually. To force the AVSVR job to run under the new profile immediately, restart the job by running the command AVENDSVR and then the command AVSTRSVR. If the AVINSITE job is active, to force it to run under the new profile immediately, restart the job by running the command AVINSITE *STOP and then the command AVINSITE *START.

> NOTE: The *ALLOBJ profile is **not** used for reading in files during scanning. Files are read in the job in which the AVSCAN or AVRUNTSK commands are run. It is the current user of those jobs that determines whether the job is authorized to files, not the *ALLOBJ profile. (For scheduled scans, the current user of the job, while it is active, is determined by the profile specified on the corresponding AVRUNTSK job scheduler entry). To guarantee that all files in the directories that are configured for a scan are scanned, ensure that the scan runs under a user profile that has *ALLOBJ special authority, or has public or private authority to all of the configured directories and the files in those directories.

> **NOTE:** If you want to create a new user profile to use as the *ALLOBJ profile, we recommend the following parameters:
>
> - PASSWORD: *NONE
>
> - Special authority (no commas, only blanks, between values): *ALLOBJ *JOBCTL *SECADM
>
> - Initial menu: *SIGNOFF
>
> - TEXT parameter value: (in single quotes): Privileged user profile for use by Powertech Antivirus for IBM i

10. Anti-Ransomware Settings

Select this option to configure Anti-Ransomware. See Powertech Antivirus Anti-Ransomware Menu.

30. Work with job schedule entries

Select this option to work with the jobs that have been scheduled as a result of changes made on this screen. Press F11 to see additional information. The jobs that may appear are as follows:

Name	Description
AVUPDATE	Run virus definition update
AVUPGRADE	Run PTF update (no longer required. See the Disabling Automatic PTF Updates section in About PTFs.)
AVRUNTSK	Run a scan task

Support Menu

The Support Menu provides useful options for maintaining and supporting the product.

```
AVSUPPORT              Powertech Antivirus Support Menu
                                                     System:
Select one of the following:

    1. Work with AVSVR jobs
    2. Work with QMSF jobs
    3. Work with job schedule entries
    4. Work with system values
    5. Work with output queue
    6. Work with IFS files
    7. Work with exit points

    20. Download latest virus definitions (DATs)
    21. Display last automatic virus definition update log (DATs)
    22. Display virus definition version

    30. Download latest program updates (PTFs)
    31. Display last automatic program updates log (PTFs)
    32. Display PTF status
                                                     Bottom
Selection or command
===> _
F1=Help    F3=Exit    F4=Prompt    F9=Retrieve    F10=Command Entry    F12=Cancel
```

How to Get There

Choose option 51 from the Main Menu. Or, run the command GO
STANDGUARD/AVSUPPORT.

Options

1. Work with AVSVR job(s)

Select this option to view the server job (AVSVR) that is currently running or has completed.
The AVSVR job must be running at all times for virus scanning to function. This option allows
you to verify the job is currently running, and to access joblogs for AVSVR jobs that have
ended.

2. Work with QMSF jobs

Select this option to work with active and completed QMSF mail server jobs. From this
display you can view joblogs to diagnose problems with mail.

3. Work with job schedule entries

Select this option to work with scheduled Powertech Antivirus for IBM i jobs. This Work with
Job Schedule Entries display allows you to change the days and times the jobs are started,
start a job to run immediately, and to view the results from the last submission. For more
information, select this option and press Help.

4. Work with system values

Select this option to work with the operating system values related to virus scanning.

5. Work with output queue

Select this option to work with the Powertech Antivirus for IBM i output queue (AVOUTQ). The Work with Output Queue display allows you to view, print and delete reports. For more information, select this option and press Help.

6. Work with IFS files

Select this option to work with files and directories in the Integrated File System (IFS). For more information, select this option and press Help.

7. Work with exit points

Select this option to work with the operating system exit points related to virus scanning.

Powertech Antivirus Anti-Ransomware Menu

The Anti-Ransomware Menu allows you to configure anti-ransomware settings.

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

```
AVRANSOM          Powertech Antivirus Anti-Ransomware Menu
                                               System:
Select one of the following:

    1. Configure APEX Default Thresholds
    2. Work with APEX Directory Exclusions
    3. Work with APEX User Overrides

   10. Work with Canary Files

   40. Work with Blocked Users

   50. Activate/Deactivate Anti-Ransomware




                                                      Bottom
Selection or command
===> _
F1=Help   F3=Exit   F4=Prompt   F9=Retrieve   F10=Command Entry   F12=Cancel
```

How to Get There

On the Powertech Antivirus Setup Menu, choose option **10**.

Options

1. Configure APEX Default Thresholds (AVCFGTHR)

Select this option to change the default APEX threshold settings for anti-ransomware detection. See the Configure APEX Thresholds (AVCFGTHR) command.

2. Work with APEX Directory Exclusions (AVWRKDIR)

Select this option to specify which directories should be ignored by the APEX detection mechanism. See the Work with Directory Exclusions (AVWRKDIR) command.

3. Work with APEX User Overrides (AVWRKUSR)

Select this option to fine-tune the APEX detection threshold values by user profile. See the Work with User Overrides (AVWRKUSR) command.

10. Work with Canary Files

Select this option to select the files to be treated as canary files by Powertech Antivirus. See the Work with Canary Files (AVWRKCNY) command.

40. Work with Blocked Users

Select this option to unblock user profiles that have been blocked by the anti-ransomware software. See the Work with Blocked Users (AVWRKBLK) command.

50. Activate/Deactivate Anti-Ransomware

Select this option to either activate or deactivate the anti-ransomware software. When activating or deactivating the anti-ransomware software, the QSERVER subsystem must be ended and restarted. This means that network services will be unavailable for a minute or so, and therefore, should be done during a period of low network activity. See the Activate/Deactivate Anti-Ransomware (AVACTAR) command.

Configure APEX Thresholds (AVCFGTHR)

The Configure APEX Thresholds (AVCFGTHR) command allows you to specify the settings that control Powertech Antivirus' anti-ransomware capabilities.

> **NOTE:** For an overview of Anti-Ransomware and configuration instructions, see <u>Anti-Ransomware</u>.

```
                    Configure APEX Thresholds (AVCFGTHR)

 Type choices, press Enter.

 Send message on threshold  . . .    *NEVER        1-100, *NEVER, *SAME
 Block user on threshold  . . . .    *NEVER        1-100, *NEVER, *SAME




                                                               Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

How to Get There

Call command **AVCFGTHR**. Or, from the Powertech Antivirus Anti-Ransomware Menu, choose option **1**.

Options

Send message on threshold (MSGTHR)

Specify the threshold value to be used to determine when a message will be sent, warning of a possible ransomware attack.

The lower this value is, the more likely it is that a message may be sent in error, i.e. a false positive.

The higher this value is, the less likely it is that a message may be sent in error, but more likely that a ransomware attack may go unreported.

The possible values are:

> **Threshold Value** Enter the threshold value.
> ***NEVER** When *NEVER is specified a message will never be sent.
> ***SAME** When *SAME is specified, the threshold value will remain unchanged.

Block user on threshold (BLKTHR)

Specify the threshold value to be used to determine when a user will be blocked, in response to a possible ransomware attack.

The lower this value is, the more likely it is that a user may be blocked in error, i.e. a false positive.

The higher this value is, the less likely it is that a user may be blocked in error, but more likely that a ransomware attack may go unchallenged.

The possible values are:

> **Threshold Value** Enter the threshold value.
> ***NEVER** When *NEVER is specified a message will never be sent.
> ***SAME** When *SAME is specified, the threshold value will remain unchanged.

Function Keys

F3 (Exit): Exits the prompt display and associated displays without running the command.

F4 (Prompt): Shows the permissible values for the entry field. If the cursor is on an entry field for a parameter of TYPE(*COMMAND) or TYPE(*CMDSTR), shows a prompt display for the command.

F5 (Refresh): Resets all parameters to their original default values.

F9 (All parameters): Shows entry fields for all parameters, including those not selected by entries on previous parameters and those not commonly used. It does not show parameters which have been defined with the selective prompt character ?-.

F11 (Keywords/Choices): Toggles between the version of the prompt display that shows possible choices and the version that shows parameter keywords.

F12 (Cancel): Cancels this display and returns to the previous menu or display.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F14 (Command string): Shows the resulting command as it would run with the parameter values currently entered.

F15 (Error messages): Shows all error messages that pertain to the command being entered.

F16 (Command complete): Indicates that all values needed have been entered, and requests the system to run the command without showing additional displays.

Work with Directory Exclusions (AVWRKDIR)

The Work with Directory Exclusions (AVWRKDIR) command allows users to maintain the directories that will be excluded from being detected by the APEX detection engine. This command's screen includes functions to add, change, display, and remove excluded directories.

A directory specified here indicates it is to be excluded from anti-ransomware protection. You can use directory exclusions to prevent false positives from blocking a user in error, for example, when an automated process transforms the files in a specific directory.

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

```
                    Powertech Antivirus              QSECOFR
                 Work with Directory Exclusions      AVWRKDIRM  D2

Type options, press Enter.
  2=Change    4=Remove    5=Display


Opt   Directory                                      Exclude
 __    /directory for encrypted files/               *YES




  F3=Exit   F5=Refresh   F6=Add   F12=Cancel
```

How to Get There

Call command **AVWRKDIR**. Or, choose option **2** on the Powertech Antivirus Anti-Ransomware Menu.

Options

2 (Change)

Opens the Configure Directory Exclusions (AVCFGDIR) screen, where you can add, change, and remove APEX directory exclusions.

4 (Remove)

Deletes the directory from the list of excluded directories.

5 (Display)

Displays directory exclusion settings.

Function Keys

F3 (Exit Program): Dismiss the screen and return to the previous screen.

F5 (Refresh Screen): Refresh the screen with current data.

F6 (Add): Opens the Configure Directory Exclusions (AVCFGDIR) screen, where you can add, change, and remove APEX directory exclusions.

F12 (Cancel): Cancels this display and returns to the previous menu or display.

Work with User Overrides (AVWRKUSR)

The Work with User Overrides (AVWRKUSR) command allows you to maintain the APEX user overrides. This command's screen includes functions to add, change, display, and remove APEX user overrides.

You can use APEX user overrides to prevent false positives from blocking a user in error, for example, when an automated process with a specific user transforms a set of files.

> NOTE: For an overview of Anti-Ransomware and configuration instructions, see Anti-Ransomware.

```
                   Powertech Antivirus          QSECOFR
                  Work with User Overrides      AVWRKUSRM  D2

   Type options, press Enter.
     2=Change    4=Remove    5=Display

                     Message    Block
   Opt  User       Threshold  Threshold
    _    USER1          10         25
    __   USER2          20         30




                                                      Bottom
   F3=Exit   F5=Refresh   F6=Add   F12=Cancel
```

How to Get There

Call command **AVWRKUSR**. Or, choose option **3** on the <u>Powertech Antivirus Anti-Ransomware Menu</u>.

Options

2 (Change)

Opens the <u>Configure User Overrides (AVCFGUSR) screen</u>, where you can add, change, and remove user overrides.

4 (Remove)

Deletes the user from the list.

5 (Display)

Displays user override settings.

Function Keys

F3 (Exit Program): Dismiss the screen and return to the previous screen.

F5 (Refresh Screen): Refresh the screen with current data.

F6 (Add): Opens the Configure User Overrides (AVCFGUSR) screen, where you can add, change, and remove user overrides.

F12 (Cancel): Cancels this display and returns to the previous menu or display.

Work with Canary Files (AVWRKCNY)

The Work with Canary Files (AVWRKCNY) command allows users to maintain the canary files. This command's screen includes functions to add, change, display, and remove canary files.

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

Canary files can be added to directories that have been overridden to exclude from analysis, to allow some protection for those directories. We recommend you add canary files to the root directory of vulnerable shares and to critical directories.

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

```
                    Powertech Antivirus
                  Work with Canary Files               AVWRKCNYM   D2

    Type options, press Enter.
      2=Change    4=Remove    5=Display


    Opt   Canary File                                    Enabled
      _     /encryptme/xgcp-mib-v1smi.my                   *YES













    F3=Exit    F5=Refresh    F6=Add    F12=Cancel

    MA*    A                                             09/002
```

How to Get There

Call command **AVWRKCNY**. Or, choose option **10** on the Powertech Antivirus Anti-Ransomware Menu.

Options

2 (Change): Opens the Configure Canary Files (AVCFGCNY) screen, where you can add, change, and remove user overrides.

4 (Remove): Deletes the directory from the list of excluded directories.

5 (Display): Displays directory settings.

Function Keys

F3 (Exit Program): Dismiss the screen and return to the previous screen.

F5 (Refresh Screen): Refresh the screen with current data.

F6 (Add): Opens the Configure Canary Files (AVCFGCNY) screen, where you can add, change, and remove canary files.
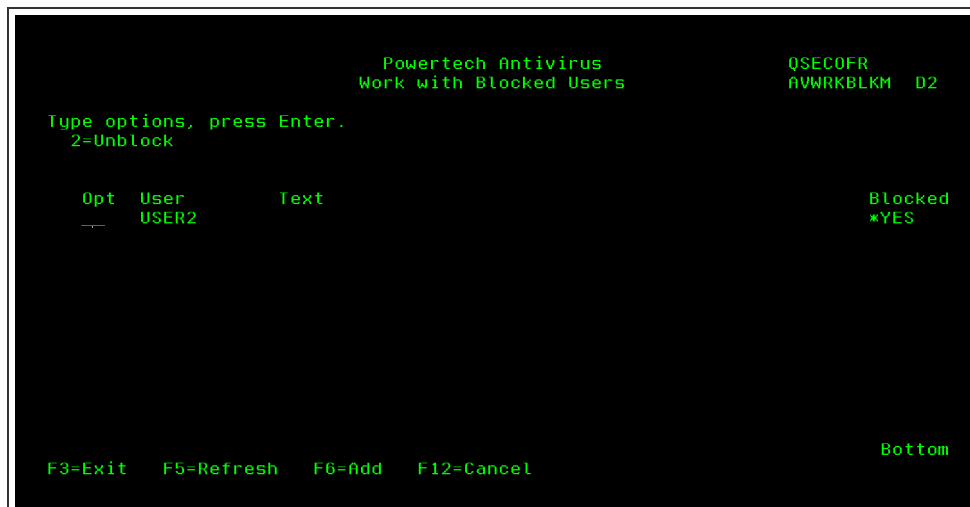
F12 (Cancel): Cancels this display and returns to the previous menu or display.

Work with Blocked Users (AVWRKBLK)

The Work with Blocked Users (AVWRKBLK) command allows you to maintain which user profiles are currently blocked.

From this screen, you can unblock user profiles that have been blocked by the anti-ransomware software.

> NOTE: For an overview of Anti-Ransomware and configuration instructions, see Anti-Ransomware.

```
                        Powertech Antivirus          QSECOFR
                       Work with Blocked Users       AVWRKBLKM  D2

          Type options, press Enter.
            2=Unblock


            Opt  User       Text                              Blocked
            __   USER2                                        *YES




                                                             Bottom
          F3=Exit   F5=Refresh   F6=Add   F12=Cancel
```

How to Get There

Call command **AVWRKBLK**. Or, choose option **40** on the Powertech Antivirus Anti-Ransomware Menu.

Options

2 (Unblock): Opens the Configure User Overrides (AVCFGUSR) screen, where you can unblock a user who is currently blocked by the anti-ransomware functionality.

Function Keys

F3 (Exit): Dismiss the screen and return to the previous screen.

F5 (Refresh): Refresh the screen with current data.

F6 (Add): Opens the Configure User Overrides (AVCFGUSR) screen, where you can add, change, and remove user overrides.
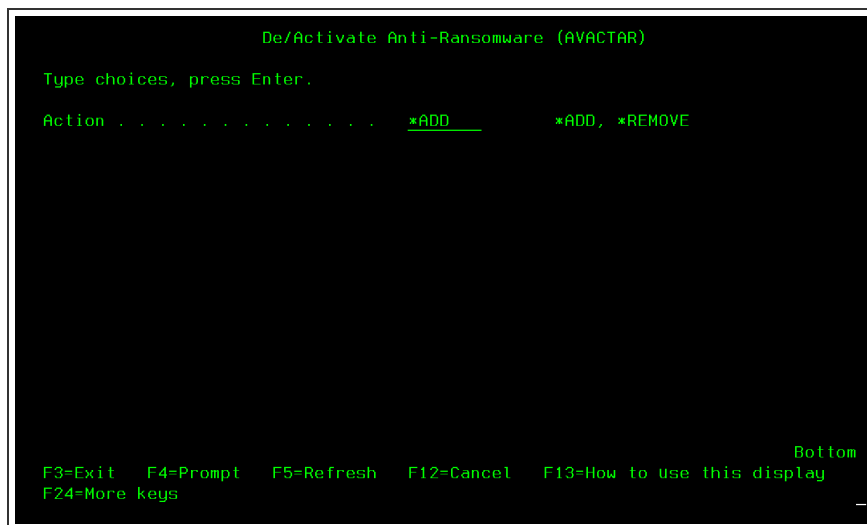
F12 (Cancel): Cancels this display and returns to the previous menu or display.

Activate/Deactivate Anti-Ransomware (AVACTAR)

The De/Activate Anti-Ransomware (AVACTAR) command allows the user to activate or deactivate the anti-ransomware software.

When activating or deactivating the anti-ransomware software, the QSERVER subsystem must be ended and restarted. This means that network services will be unavailable for a minute or so, and therefore, should be done during a period of low network activity.

> NOTE: For an overview of Anti-Ransomware and configuration instructions, see Anti-Ransomware.

```
                    De/Activate Anti-Ransomware (AVACTAR)

 Type choices, press Enter.

 Action . . . . . . . . . . . . .   *ADD        *ADD, *REMOVE




















                                                                 Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

How to Get There

Call command **AVACTAR**. Or, choose option **50** on the Powertech Antivirus Anti-Ransomware Menu.

Options

Action (ACTION)

Specify whether the anti-ransomware software is being activated or deactivated.

The possible values are:

> ***ADD** When *ADD is specified, the anti-ransomware software will be activated.
> ***REMOVE** When *REMOVE is specified, the anti-ransomware software will be deactivated.

Function Keys

F3 (Exit): Exits the prompt display and associated displays without running the command.

F4 (Prompt): Shows the permissible values for the entry field. If the cursor is on an entry field for a parameter of TYPE(*COMMAND) or TYPE(*CMDSTR), shows a prompt display for the command.

F5 (Refresh): Resets all parameters to their original default values.

F9 (All parameters): Shows entry fields for all parameters, including those not selected by entries on previous parameters and those not commonly used. It does not show parameters which have been defined with the selective prompt character ?-.

F11 (Keywords/Choices): Toggles between the version of the prompt display that shows possible choices and the version that shows parameter keywords.

F12 (Cancel): Cancels this display and returns to the previous menu or display.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F14 (Command string): Shows the resulting command as it would run with the parameter values currently entered.

F15 (Error messages): Shows all error messages that pertain to the command being entered.

F16 (Command complete): Indicates that all values needed have been entered, and requests the system to run the command without showing additional displays.

Appendix

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

About PTFs

In Powertech Antivirus for IBM i versions prior to 8.2, Fortra released Program Temporary Fixes (PTFs) and/or product enhancements that could be used to update the product much like IBM PTFs are used to update the OS. As of version 8.2, all product updates are acquired from either the Fortra Community Portal or using Fortra Application Hub or Fortra Insite, and included in the product installation process. Product updates are no longer provided as PTFs.

Disabling Automatic PTF Updates

If Powertech Antivirus for IBM i was previously configured to download and apply PTFs, remove the corresponding scheduled jobs. To do so:

1. From the Powertech Antivirus for IBM i Main Menu, choose option **4**, Work with Job Schedule Entries.

2. On the Work with Job Schedule Entries screen, use option **4** to remove any scheduled jobs that are named **AVUPGRADE**. Do not remove jobs named **AVUPDATE**.

Contacting Fortra

Please contact Fortra for questions or to receive information about Powertech Antivirus for IBM i. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

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