L-Soft international, Inc.

The LISTSERV Anti-Virus Station (AVS)

LISTSERV® 17.5

November 2024

L-Soft's manuals for LISTSERV are available at http://www.lsoft.com/manuals .

L-Soft invites feedback on its manuals. Please feel free to send your comments by e-mail to: MANUALS@LSOFT.COM

Contents

The LISTSERV Anti-Virus Station (AVS) **1**
1 Introduction **1**
1.1 Target audience 1
1.2 What you will need 1
1.2.1 Operating system for Anti-Virus Stations 1
1.2.2 Operating system for primary LISTSERV servers 2
1.2.3 Supported LISTSERV versions 2
1.2.4 Minimum hardware requirements for the AVS 2
1.2.5 Supported Windows Defender versions 2
1.2.6 SMTP mail requirements 3
1.2.7 Obtaining product license activation keys (LAKs) 3
1.3 Scope of this document 3
2 Tasks **3**
2.1 Installation and configuration 3
2.2 Testing 5
2.3 Running the AVS in production 6
3 Reference **6**
3.1 Using bracketed IP address in AV_STATION= 6
3.2 Uptime and connectivity 7
3.3 Glossary of terms used 7

About This Manual

Every effort has been made to ensure that this document is an accurate representation of the functionality of LISTSERV®. As with every software application, development continues after the documentation has gone to press, so small inconsistencies may occur. We would appreciate any feedback on this manual. Send comments by e-mail to: MANUALS@LSOFT.COM

The following documentation conventions have been used in this manual:

- Quotations from the screen will appear in italics enclosed within quotation marks.
- Clickable buttons will appear in bold.
- Clickable links will appear in bold.
- Directory names, commands, and examples of editing program files will appear in Courier New font.
- Emphasized words or phrases will be underlined.
- Hyperlinks, actual or fictitious, will be underlined unless they are part of a screen shot or direct quotation from the screen.

Some screen captures have been cropped and annotated for emphasis or descriptive purposes.

The LISTSERV Anti-Virus Station (AVS)

1 Introduction

AVS stands for "Anti-Virus Station". An AVS is a specially-licensed LISTSERV machine that is employed as an external anti-virus scanner for other LISTSERV machines that do not currently support an internal AV scanning.

At its original release, LISTSERV Version 1.8e (14.0) supported real-time anti-virus scanning of all messages sent to mailing lists running under LISTSERV Classic or LISTSERV Classic HPO on Windows NT/2000/XP and Linux servers. This was possible through a now-canceled partner agreement with a major anti-virus software vendor. Recognizing that some customers were unwilling to install a third-party anti-virus only for the purpose of scanning LISTSERV messages, LISTSERV 16.0 and following for Windows has also supported anti-virus scanning natively via the Windows Defender Anti-Virus, which is part of modern versions of the Windows Server operating system.

Thus, the LISTSERV Anti-Virus Station provides comprehensive virus protection for sites running LISTSERV on operating systems not currently supported by LISTSERV's built-in anti-virus scanner. The AVS works by having the production LISTSERV system (called the "primary" system) forward messages to a separate system, the AVS, on which they are scanned. The AVS is a Windows Server system (2016 or later) running Windows, Windows Defender Antivirus (which ships with Windows Server 2016 and later) and a special, limited capacity version of LISTSERV. All the virus scanning functions become available, with the following exceptions:

- Scanning of DISTRIBUTE jobs (other than postings to mailing lists) is not available. Simply submit DISTRIBUTE jobs requiring virus scanning to the AVS instead.

- Documents downloaded using the web interface are not scanned for viruses.

1.1 Target audience

Administrators of LISTSERV Classic and LISTSERV Classic HPO sites running on operating systems other than Windows, who wish to take advantage of LISTSERV’s on-the-fly anti-virus scanning feature.

1.2 What you will need

There are several classes of requirements for the AVS. These include operating system, LISTSERV version, minimum hardware, Windows Defender version, and SMTP mail. Also, license keys are required for the LISTSERV products.

1.2.1 Operating system for Anti-Virus Stations

The AVS itself must run under the Microsoft Windows operating system.

Minimum supported Microsoft Windows OS: Windows Server 2016 or later.

1.2.2 Operating system for primary LISTSERV servers

Any operating system platform that is supported by L-Soft for the LISTSERV product is acceptable. See the LISTSERV Operating System Support page for details.

1.2.3 Supported LISTSERV versions

Either LISTSERV Classic or LISTSERV Classic HPO, is required. The AVS does not work with LISTSERV Lite, which does not include the AV scan feature.

LISTSERV version 16.0-2017a is required at minimum. LISTSERV 16.0-2017a has a build date of 28 Feb 2017. ***However, L-Soft STRONGLY RECOMMENDS that all customers should upgrade LISTSERV to the generally-available version, LISTSERV 17.5.***

Maintenance is required. Sites that do not have maintenance contracts with L-Soft will not be able to run the AVS.

If you are unsure what version of LISTSERV you are running, issue a SHOW VERSION command to LISTSERV, or view the Server Dashboard. The output in both cases will include the LISTSERV build date.

1.2.4 Minimum hardware requirements for the AVS

The AVS hardware requirements vary depending on how the machine is used. The AVS is not resource intensive and does not need to run on a dedicated server; you can use an existing server or an unused, previous generation system. Microsoft's minimum requirements for current Windows Server systems are

- 1.4GHz 64-bit processor with at least 2 cores
- 2GB RAM
- 32GB system partition
- 1Gbit PCI Express NIC

You will need to enable the Windows Desktop Experience in order to install Windows Defender Anti-Virus as a server feature. This is why 2GB RAM is required at minimum.

If you plan to run other applications on the machine, or post DISTRIBUTE jobs through the AVS as mentioned above, then your minimum hardware requirements will escalate accordingly.

AVS is supported on virtualized Windows Server 2016 (or later) systems (for instance running under Hyper-V or in commercial cloud services such as Azure or AWS). It is not necessary to have a physical machine.

1.2.5 Supported Windows Defender versions

At this writing, the supported Windows Defender version is 1.359.770.0. This changes several times daily as Windows Update installs updated signature files, so your installed version will likely be higher.

To determine the version of Windows Defender running on any given Windows Server machine, check Settings -> Update & Security -> Windows Defender, and scroll to the bottom. Look for "Antivirus Definition". This is the version code LISTSERV displays in a "SHOW VERSION" or "RELEASE" command response, e.g.,

```
Virus database version:      2022-02-23 09:33:06 (1.359.770.0)
```

1.2.6 SMTP mail requirements

The AVS machine communicates with its primary servers (and vice versa) using SMTP e-mail. This requires that the AVS machine must have a working SMTP server installed and running that understands how to pass mail to LISTSERV.

Under Microsoft Windows, this means that the SMTPL.EXE "listener" service (provided with LISTSERV) must be installed on the AVS. No other Windows SMTP implementations are supported as they do not have knowledge of LISTSERV and cannot be used to pass mail to LISTSERV. Further, if the SMTPL.EXE "listener" service is used, an external machine must be used to handle LISTSERV's outbound mail, as the SMTPL.EXE service is designed to handle inbound mail only.

Please see the LISTSERV installation instructions for more information on setting up your SMTP mailer.

1.2.7 Obtaining product license activation keys (LAKs)

LISTSERV (including both the AVS machine and any primary servers) requires license keys, which can be obtained from your L-Soft sales representative. Keys are operating-system specific, so be sure to clearly specify the operating system for each key.

Please do not contact the product support department for license keys; only the sales department may issue LAKs.

1.3 Scope of this document

This document will explain how to install and configure the LISTSERV Anti-Virus Server (AVS) for LISTSERV sites running operating systems without LISTSERV native support for anti-virus scanning. It does not include instructions on installing LISTSERV. Installation guides, FAQs, and other documentation for LISTSERV can be found at http://www.lsoft.com/manuals .

2 Tasks

Tasks related to AVS installation include installation and configuration; testing; and running the AVS in production.

2.1 Installation and configuration

The AVS is configured and installed as follows:

1. Upgrade the primary LISTSERV system to the latest version (see the installation guide for your operating system platform for upgrade instructions).

2. Select hardware and operating system for the AVS system.

3. Obtain license activation keys (LAKs) for the AVS from your L-Soft sales representative.

4. Download and install LISTSERV 17.5 on the AVS system, using the LAKs obtained in step 3. The AVS does not require a web interface, although you should consider installing it for your convenience in managing the server.

5. Choose a "secret word" for the AVS. In this example, we will use the word SECRET. For authentication purposes, the secret word is incorporated into all AVS jobs sent from the primary server to the AVS and back again. If the secret word found in a given AVS job does not match the secret word you have chosen, the AVS job is discarded. This prevents random LISTSERV sites from using your AVS without permission.

6. Add `AV_SECRET_WORD=SECRET` to the LISTSERV configuration on the AVS. Restart LISTSERV on the AVS.

Example:

Windows: (site.cfg)	`AV_SECRET_WORD=SECRET`

7. Add `AV_SECRET_WORD` as above (same value) to the LISTSERV configuration of the primary LISTSERV system. In addition, set `AV_STATION` to the hostname of the AVS system, and restart the primary LISTSERV instance. For the purpose of example we will assume that the AVS system is named AVS.EXAMPLE.COM in DNS.

OS-specific examples:

Unix:
(go.user)
	`AV_SECRET_WORD="SECRET"`
	`AV_STATION="AVS.EXAMPLE.COM"`
	`export AV_SECRET_WORD AV_STATION`

z/VM: (LOCAL SYSVARS)	`AV_SECRET_WORD = 'secret'` `AV_STATION = 'AVS.EXAMPLE.COM'`

NOTE: `AV_SECRET_WORD` should contain only characters that are not reserved or otherwise have special meaning to the operating system shell. Specifically we are aware that "&" should not be used under unix. It is L-Soft's recommendation that the value of `AV_SECRET_WORD` be chosen strictly from the set of all alphanumeric characters (A-Z, a-z, 0-9) plus dash, underscore, and period. The use of other characters in `AV_SECRET_WORD` may result in errors such as

```
20 Nov 2024 02:22:22 Processing file 37472 from
MAILER@LISTSERV.EXAMPLE.COM

-> Invalid AV signature.
```

(from the LISTSERV console log).

2.2 Testing

After installing the AVS, it should first be tested before running it in production.

For a basic test of the AVS, send a message to a mailing list and watch the logs of the primary and AVS servers. The message should go through the AVS for scanning and come back.

A set of standard anti-virus test files is made available by EICAR and can be used to test the AVS. These files are described and are available at http://www.eicar.org/anti_virus_test_file.htm. The files are NOT viral in nature, but note that in order to download them, local anti-virus scanning may need to be turned off, as most anti-virus suites will (as designed) quarantine the EICAR test files.

On the primary server, the LISTSERV log will contain entries like the following:

```
20 Nov 2024 17:13:18 Processing file 0326 from MAILER@LISTSERV.EXAMPLE.COM
-> Forwarding to AV Station.
20 Nov 2024 17:13:19 Processing file 0328 from MAILER@LISTSERV.EXAMPLE.COM
20 Nov 2024 17:13:20 -> Rejected:
* Your posting to the TEST list has been rejected because it contains the
* 'EICAR_Test_File' virus in attachment 'eicar.com'. You are strongly advised
* to check your computer for viruses as soon as possible!
20 Nov 2024 17:13:20 Sent information mail to nathan@EXAMPLE.COM
```

On the AVS the corresponding log entries would look like this:

```
20 Nov 2024 17:13:11 Processing file 0022 from MAILER@AVS.EXAMPLE.COM
20 Nov 2024 17:13:11 From LISTSERV@LISTSERV.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
CLASS=M
20 Nov 2024 17:13:11 Rescheduled as: 0023
20 Nov 2024 17:13:11 Processing file 0023 from LISTSERV@AVS.EXAMPLE.COM
20 Nov 2024 17:13:11 From LISTSERV@LISTSERV.EXAMPLE.COM: X-AV SCAN
TEST@LISTSERV.EXAMPLE.COM 1
20 Nov 2024 17:13:12 >>> Error X'01100011' running virus scanner <<<
20 Nov 2024 17:13:12 -> Severity: Warning
20 Nov 2024 17:13:12 -> Facility: Virus detection system
20 Nov 2024 17:13:12 -> Abstract: Virus detected
20 Nov 2024 17:13:12 Virus found: EICAR_Test_File
20 Nov 2024 17:13:12 >>> Error X'01100011' scanning message for viruses <<<
20 Nov 2024 17:13:12 -> Severity: Warning
20 Nov 2024 17:13:12 -> Facility: Virus detection system
20 Nov 2024 17:13:12 -> Abstract: Virus detected
```

If there is no virus found during the scan, the log entries are much simpler. Here is a sample primary server log for a virus-free message:

```
20 Nov 2024 09:58:44 Processing file 0510 from MAILER@LISTSERV.EXAMPLE.COM
-> Forwarding to AV Station.
20 Nov 2024 09:58:46 Processing file 0512 from MAILER@LISTSERV.EXAMPLE.COM
20 Nov 2024 09:58:46 Processing mail from nathan@EXAMPLE.COM for TEST
20 Nov 2024 09:58:46 Rebuilding HTML page for TEST...
```

and here is the corresponding AVS log:

```
20 Nov 2024 09:59:27 Processing file 0034 from MAILER@AVS.EXAMPLE.COM
20 Nov 2024 09:59:28 From LISTSERV@LISTSERV.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
CLASS=M
20 Nov 2024 09:59:28 Rescheduled as: 0035
20 Nov 2024 09:59:28 Processing file 0035 from LISTSERV@AVS.EXAMPLE.COM
20 Nov 2024 09:59:28 From LISTSERV@LISTSERV.EXAMPLE.COM: X-AV SCAN
TEST@LISTSERV.EXAMPLE.COM 1
```

(If the AV scan is clear, no further information is written to the AVS log.)

You will also see entries like this, approximately once each hour:

```
20 Nov 2024 17:00:07 From LISTSERV@AVS.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
20 Nov 2024 17:00:07 Rescheduled as: 0323
20 Nov 2024 17:00:07 Processing file 0323 from LISTSERV@LISTSERV.EXAMPLE.COM
20 Nov 2024 17:00:07 From LISTSERV@AVS.EXAMPLE.COM: X-AV STATS
> 1-FFE5B86C-6A0D2560 200302 6 0 0
```

This is normal. In a standard non-AVS LISTSERV installation, where Windows Defender is installed on the same machine with LISTSERV, anti-virus statistics are normally gathered in the background and this sort of job would not be seen. When using an AVS, the work is actually being done by Windows Defender on the AVS, and periodically the AVS sends updated statistics to the primary server. These are the statistics used by the Anti-Virus Statistics section of LISTSERV's web administration interface.

2.3 Running the AVS in production

One AVS can serve multiple primary servers, but they must all have valid L-Soft maintenance. It is the maintenance LAK of the primary server that determines whether the AVS is used. If the AVS LAK expires, the AVS will also stop working. Normally, the AVS and primary systems will have maintenance keys with the same expiration date.

As noted above, the AVS and primary server(s) will communicate with each other to update statistics counters and other informational data. Eventually — the process may take up to a day — the Windows Defender virus database version will be shown on the RELEASE command, and virus statistics will update.

3 Reference

3.1 Using bracketed IP address in AV_STATION=

Under some circumstances it may be necessary to refer to the AVS by its IP address rather than by a fully-qualified domain name (FQDN).

In this case it is necessary that the IP address be bracketed, as in the following examples:

Windows: (site.cfg)	`AV_STATION=[192.168.254.3]`
Unix: (go.user)	`AV_STATION="[192.168.254.3]"`

VM: (LOCAL SYSVARS)	`AV_STATION = '[192.168.254.3]'`

Bracketed IPs should be used only if it is not possible to identify the AVS with an FQDN, for example, if a firewall exists between the AVS and the primary server(s). ***Wherever possible, use of an FQDN in the AV_STATION= setting is strongly recommended.***

3.2 Uptime and connectivity

In order to use the AVS, LISTSERV depends on being able to send and receive email from the AVS machine. Thus it is vitally important that the AVS machine have as close to 100% uptime as possible, and that the AVS machine not be prone to dropping out of DNS unexpectedly, or be installed behind a "flaky" router or firewall that makes connectivity to the machine problematic.

It should be carefully noted that any mailings sent to the LISTSERV server during a period when the AVS is unreachable will be delayed until the AVS is back online. Should AVS messages from the primary server to the AVS machine be bounced or otherwise lost, the postings they contain will also be lost. LISTSERV will not retry AVS submissions and there is no way to requeue them short of reposting them.

If the AVS must be stopped for any reason, it is **strongly recommended** that any and all primary servers which use the AVS be stopped first. This will help prevent mail loss in the event that the AVS downtime is longer than expected.

When changing the name or network address of the AVS machine, it is **extremely important** to ensure that the primary server(s) will still be able to exchange mail with the AVS after the change, for the reasons noted above. Also, imposing a firewall between the AVS and its primary server(s) should be done carefully, again ensuring that the flow of mail between the machines not be impeded.

3.3 Glossary of terms used

AVS: Anti-Virus Station

FQDN: Fully-Qualified Domain Name, for instance, listserv.example.com .

LAK: License Activation Key

NIC: Network interface card

Primary server: A LISTSERV production server that is configured to use an AVS for anti-virus scanning.

Change Log:

20040512-001	Reserved or special characters should not be used in AV_SECRET_WORD setting
20040707-001	14.3
20050601-001	14.4
20060224-001	14.5
20070620-001	15.0
20090401-001	16.0
20220222-001	17.0
20241115-001	17.5