L-Soft international, Inc.

The LISTSERV Anti-Virus Station (AVS)

LISTSERV® 15.0

June 2007

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. L-Soft international, Inc. does not endorse or approve the use of any of the product names or trademarks appearing in this document.

Some of L-Soft's manuals for LISTSERV are available in ASCII-text format from LISTSERV and in PDF at ftp://ftp.lsoft.com/. Many are also available on the World Wide Web at http://www.lsoft.com/manuals/index.html .

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

Contents

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. The message body and any inline uuencoded binaries and MIME attachments in those messages are scanned by submitting them to the F-Secure Anti-Virus scanning engine, which is installed on the LISTSERV machine. The F-Secure Anti-Virus scanning engine is made available at no extra charge through a partner agreement between L-Soft international, Inc., and F-Secure Corporation, to L-Soft's customers who purchase LISTSERV maintenance.

Since F-Secure Anti-Virus was and is currently available only for Windows and Linux-x86 systems, this meant that until now only Windows and Linux-x86 systems could be protected by the new AV scanning feature. L-Soft recognized from the beginning of its partnership with F-Secure that this situation would have to be remedied so that all LISTSERV platforms could be protected, and so the LISTSERV Anti-Virus Station was created.

The LISTSERV Anti-Virus Station is a new product providing comprehensive virus protection for sites running LISTSERV on operating systems not currently supported by F-Secure. 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 NT/2000 system running FSAV 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 and Linux, 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, F-Secure Anti-Virus version, and SMTP mail. Also, license keys are required for the LISTSERV and FSAV 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 2000 Professional or Server, with Service Pack 3 applied, or later, on Intel hardware.

Please note that the LISTSERV Anti-Virus Station is not currently available for Linux.

Support for further operating systems will depend upon future F-Secure Anti-Virus support for those platforms.

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 14.0 is required at minimum, but does not support the latest F-Secure Anti-Virus software. In order to use the latest FSAV software, LISTSERV version 15.0 is required at minimum.

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

LISTSERV 1.8e (14.0), released in May 2002, and later revisions and releases, are the only AVS-supported LISTSERV versions, both for the AVS itself and for the primary systems that use it. At this writing, the current LISTSERV version is LISTSERV 15.0-2007a, released in February 2007.

LISTSERV 1.8d and earlier are not AVS-aware and must be upgraded to be able to take advantage of the LISTSERV AVS feature.

If you are unsure what version of LISTSERV you are running, issue a SHOW VERSION command to LISTSERV.

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. However, the absolute minimum requirement is a Pentium-class machine with 128-256M RAM, a 4GB or larger IDE disk, and a NIC with sufficient bandwidth to handle network requests.

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.

1.2.5 Supported F-Secure Anti-Virus (FSAV) versions

At this writing, the supported FSAV version is:

Operating System	LISTSERV 14.3, 14.4, 14.5	LISTSERV 15.0 or later
Windows 2000/2003 Server	FSAV 5.52	FSAV 5.52 or 7.00
Windows 2000/XP	FSAV 5.44	FSAV 5.44 or 7.00

The requirement to run the AVS under the Microsoft Windows operating system stems from two important points:

- The Windows version of FSAV currently supported by L-Soft has three independent virus-scanning engines, whereas the Linux version currently supported by L-Soft has only one.

- The Windows version of FSAV has a simpler, fast, incremental method of automatically updating virus signature databases (with the included BackWeb or F-Secure Automatic Updates utility). FSAV for Linux relies on cron running an ftp of the entire virus signature database, which is slow.

FSAV kits are available for download at

USA main site: ftp://www.lsoft.com/f-secure/
Europe mirror: ftp://www.lsoft.se/f-secure/

These kits require an FSAV license key to install (see section 1.2.7).

Installation instructions for FSAV with LISTSERV are found at http://www.lsoft.com/manuals/fsav-install.html , and a LISTSERV-FSAV FAQ is found at http://www.lsoft.com/manuals/f-secure-faq.stm .

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[1]. 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.

[1] L-Soft's legacy LSMTP mailer is also supported for this purpose, but the product is no longer available for new installations and is no longer being maintained.

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) and FSAV require 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 not yet supported by F-Secure Anti-Virus (FSAV). 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 version 15.0 (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 15.0 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:

Windows: (site.cfg)	AV_SECRET_WORD=SECRET AV_STATION=AVS.EXAMPLE.COM
Unix: (go.user)	AV_SECRET_WORD="SECRET" AV_STATION="AVS.EXAMPLE.COM" export AV_SECRET_WORD AV_STATION
OpenVMS: (site_config.dat)	AV_SECRET_WORD "SECRET" AV_STATION "AVS.EXAMPLE.COM"
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 Jun 2007 09:47:20 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:

```
14 Mar 2003 17:13:18 Processing file 0326 from MAILER@LISTSERV.EXAMPLE.COM
-> Forwarding to AV Station.
14 Mar 2003 17:13:19 Processing file 0328 from MAILER@LISTSERV.EXAMPLE.COM
14 Mar 2003 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!
14 Mar 2003 17:13:20 Sent information mail to nathan@EXAMPLE.COM
```

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

```
14 Mar 2003 17:13:11 Processing file 0022 from MAILER@AVS.EXAMPLE.COM
14 Mar 2003 17:13:11 From LISTSERV@LISTSERV.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
CLASS=M
14 Mar 2003 17:13:11 Rescheduled as: 0023
14 Mar 2003 17:13:11 Processing file 0023 from LISTSERV@AVS.EXAMPLE.COM
14 Mar 2003 17:13:11 From LISTSERV@LISTSERV.EXAMPLE.COM: X-AV SCAN
TEST@LISTSERV.EXAMPLE.COM 1
14 Mar 2003 17:13:12 >>> Error X'01100011' running virus scanner <<<
14 Mar 2003 17:13:12 -> Severity: Warning
14 Mar 2003 17:13:12 -> Facility: Virus detection system
14 Mar 2003 17:13:12 -> Abstract: Virus detected
14 Mar 2003 17:13:12 Virus found: EICAR_Test_File
14 Mar 2003 17:13:12 >>> Error X'01100011' scanning message for viruses <<<
14 Mar 2003 17:13:12 -> Severity: Warning
14 Mar 2003 17:13:12 -> Facility: Virus detection system
14 Mar 2003 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:

```
18 Mar 2003 09:58:44 Processing file 0510 from MAILER@LISTSERV.EXAMPLE.COM
-> Forwarding to AV Station.
18 Mar 2003 09:58:46 Processing file 0512 from MAILER@LISTSERV.EXAMPLE.COM
18 Mar 2003 09:58:46 Processing mail from nathan@EXAMPLE.COM for TEST
18 Mar 2003 09:58:46 Rebuilding HTML page for TEST...
```

and here is the corresponding AVS log:

```
18 Mar 2003 09:59:27 Processing file 0034 from MAILER@AVS.EXAMPLE.COM
18 Mar 2003 09:59:28 From LISTSERV@LISTSERV.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
CLASS=M
18 Mar 2003 09:59:28 Rescheduled as: 0035
18 Mar 2003 09:59:28 Processing file 0035 from LISTSERV@AVS.EXAMPLE.COM
18 Mar 2003 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:

```
14 Mar 2003 17:00:07 From LISTSERV@AVS.EXAMPLE.COM: X-B64 ID=X-AV.JOB ASCII
14 Mar 2003 17:00:07 Rescheduled as: 0323
14 Mar 2003 17:00:07 Processing file 0323 from LISTSERV@LISTSERV.EXAMPLE.COM
14 Mar 2003 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 FSAV 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 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 — you will see the "Secured by F-Secure" logo on your web archive pages, the F-Secure version and 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]"`
OpenVMS: (site_config.dat)	`AV_STATION "[192.168.254.3]"`
VM: (LOCAL SYSVARS)	`AV_STATION = '[192.168.254.3]'`

L-Soft does not formally support the use of bracketed IPs in place of fully-qualified domain names, but this will work 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, however, 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.

Sites running the AVS under Windows should also note that the BackWeb component of FSAV requires the ability to connect to port 80 on the F-Secure update server in order to download virus signature updates.

3.3 Glossary of terms used

AVS: Anti-Virus Station

FSAV: F-Secure Anti-Virus

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

LAK: License Activation Key

NIC: Network interface card

Primary server: A LISTSERV 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