Release Notes for LISTSERV® Version 14.5

3/2/2006 4:25 PM

IMPORTANT: LISTSERV 14.5 requires a version 14.5 LAK!

You must obtain and install a LISTSERV version 14.5 product LAK prior to upgrading your server, or LISTSERV will not start after the upgrade.

More information

Go directly to the table of contents

Product Manager's Message

With all the controversy and concerns surrounding the possible introduction of pay-for-send e-mail, we felt that an early release of the LISTSERV 15.0 deliverability improvements would help familiarize everyone with DomainKeys, SPF, Sender ID and other authentication technology. When implemented correctly, these authentication tools can improve your "deliverability," making it less likely that your legitimate messages be erroneously caught in spam filters. As we expect major ISPs to "tighten up" their spam filters in the coming months, we advise all customers to carefully review the Deliverability Assessment report now accessible through the web interface, and at least prepare for the addition of DomainKeys signatures to outbound messages.

But let's first take a pragmatic look at the pay-for-send controversy. Will it really happen? Will only the largest and wealthiest companies be able to reach out to their customers, leaving non-profits and academia out in the cold? I am confident that none of this will happen, for two simple reasons. First, while it is true that a lot of people support the idea of charging for e-mail, they do so because they have read in the press that it will end spam. But, if you read the articles in question carefully, you will see that this is the journalist's opinion, or at best the opinion of an industry watcher. Neither AOL nor anyone in the e-mail industry has claimed that an e-mail fee could so much as reduce spam, let alone eliminate it. We did not make any such claims because we know that today's spammers are oozing cash and would wait in line to buy their way past spam filters with hard currency if that were to become an option. They have worked very hard on their ROI and can absolutely afford a quarter of a cent per message and still make money. The truth is that modern spam "offerings," such as offshore pharmacy, are very profitable. Today's spammers are richer than most legitimate businesses and can afford to pay more for e-mail stamps than the local concert hall or sport accessory store.

The second reason I am not worried about pay-for-send is that the proposed fee is exorbitant, and a market economy does not tolerate that for long. Authenticating L-Soft's modest hosting service would cost up to $15 million per year. No matter how you look at it, this is an outrageous figure. It is many times our hosting revenues, thousands of times reasonable actual costs, in fact it reads like a figure out of a dot-boom business plan.

We can do better with technology based on open standards, but, alas, not today. The open standard community was taken by surprise and will need some time to recoup and extend current protocols to provide reputation and certification services. Meanwhile, everybody who opposes pay-for-send needs to become familiar with the technology that we have today, and deploy it not just as a vote of confidence, but because it provides concrete benefits today. This is where 14.5 comes into the picture, with DomainKeys support (previously released as an open beta for 14.4), and a comprehensive Deliverability Assessment report that analyzes DomainKeys, SPF, Sender ID and DNS registrations and makes detailed suggestions for improvement. Another reason to try out the Deliverability Assessment is that it is

built with the upcoming 15.0 interface, and now is the ideal time to send us any comments that you might have. Unfortunately, the 15.0 navigation and a few other minor functions had to be disabled to make the screens work with 14.5.

Looking ahead, I see two more steps to the first genuinely effective, reputation-based spam prevention tools. The first is a revised DKIM specification supporting reputation and certification services (DKIM is an Internet standardization effort combining DomainKeys and Identified Internet Mail). I expect this to be a simple technology update; for L-Soft customers, it will just mean a new version of LISTSERV to install. This will create a framework for the second step – the emergence of reputation/certification services on a level playing field, with competition keeping prices to reasonable levels. I envision two complementary business models for these services. On the one hand, companies like Dun & Bradstreet could provide e-mail reputation ratings in addition to other financial data, a service that e-mail receivers could purchase in order to help filter out spam from their mailboxes. Companies like VeriSign, on the other hand, could sell reputation certificates to senders, a service that e-mail receivers could access for free. Receivers would choose which reputation providers (of either type) they want to use to screen incoming mail. Because almost everyone would be able to afford certification, almost every message would be certified and bypass spam filters. The spam filters in turn would be able to screen messages more carefully, and in particular it would probably be acceptable to put the occasional non-certified messages through quarantine, allowing more time for spam sources to be identified and listed.

Getting back to 14.5, we also decided to expedite the release of another 15.0 feature, unixODBC support. With MySQL now playing in the same league as “big name” databases, and unixODBC included with major Linux distributions, this feature was an ideal candidate for early release. There was a (small) price to pay, though: we have not had the time to test unixODBC support with other databases than MySQL. So, for now, we recommend the native OCI and CLI interfaces for Oracle and DB2.

CONTENTS

Applying LISTSERV 14.5

SECURITY

WA Security Alert

A number of buffer overruns were found in the WA CGI stage for all platforms after the release of LISTSERV 14.4. This discovery triggered a full code audit and overhaul of WA for LISTSERV 14.5.

As a result, L-Soft *strongly recommends* that all LISTSERV 14.4 sites upgrade to 14.5, and particularly ensure that their existing production WA CGI script be updated with the current WA version.

The vunerabilities were found and graciously reported by Peter Winter-Smith of Next Generation Security Software, Ltd. (www.ngssoftware.com). We thank Mr. Winter-Smith for his contribution and patience with us as we took steps to eliminate these problems.

USABILITY

Support for DomainKeys Message Signing

This feature is not available in LISTSERV Lite.

Starting with version 14.5, LISTSERV supports DomainKeys for outbound mail as described in the Internet draft draft-delany-domainkeys-base-03 .

Additionally, LISTSERV HPO for Windows, Linux-x86, and FreeBSD incorporates a DomainKeys Accelerator for faster signing of messages. The accelerator requires an Intel or AMD processor with SSE2 support. If SSE2 support is not detected, LISTSERV will not enable the DomainKeys Accelerator and will log the following message at start time:

```
>23 Feb 2006 14:26:43 DomainKeys Accelerator disabled:
>23 Feb 2006 14:26:43 -> Processor lacks SSE2 support
```

Setting up LISTSERV to use DomainKeys

Please see the supplementary document *Using LISTSERV with DomainKeys*. It is necessary to configure LISTSERV appropriately before the following new features can be used.

Using DomainKeys with Mailing Lists

- If DomainKeys support has been enabled in the configuration, LISTSERV will sign all outbound messages for mailing lists, including administrative messages, welcome messages, etc.

- "`Misc-Options= NO_DKIM_SIGNATURE`" can be added in the list header (or made the system default via the DEFAULT_MISC_OPTIONS configuration variable) to override this.

- Incoming DomainKeys or DKIM signatures submitted to a mailing list will be removed unless "`Misc-Options= KEEP_DKIM_SIGNATURE`" is set in the list configuration. This is necessary because these signatures almost never match after the message has been processed. The worst thing that could possibly happen to your deliverability is a DomainKeys signature that does not match and causes the message to be flagged as suspicious.

The KEEP_DKIM_SIGNATURE option is experimental and not meant for general use. As DomainKeys is specified today, signatures DO NOT survive posting to mailing lists (LISTSERV or otherwise), so LISTSERV removes them by default to avoid triggering alerts for subscribers on systems that have implemented the client side of DomainKeys. The DKIM specification may be more robust in this respect, but even DKIM signatures will probably not survive when posted through a mailing list. Use the KEEP_DKIM_SIGNATURE option at your own risk.

If desired, either or both options can be specified for all lists via the DEFAULT_MISC_OPTIONS= site configuration variable.

Using DomainKeys in DISTRIBUTE Jobs

A new `DKIM=NO|YES` option has been added to DISTRIBUTE (default: NO). This will fail if running a LISTSERV version without DomainKeys support, but otherwise it always succeeds. Messages originating from domains for which LISTSERV has been configured to sign will be signed, while those originating from other domains won't be.

Using DomainKeys to Sign Other Types of Messages

Once you have become comfortable with DomainKeys signatures, you may want to have LISTSERV sign *every* message that it generates, regardless of its source. Setting `DKIM_SIGN_ALL=1` in the site configuration file tells LISTSERV to try to sign every message for which it has a suitable private key, as defined in the DKIM_SIGN configuration parameter (see *Using LISTSERV with DomainKeys* for details). For example:

VM	`DKIM_SIGN_ALL = 1`
VMS:	`DKIM_SIGN_ALL "1"`
unix:	`DKIM_SIGN_ALL=1` `export DKIM_SIGN_ALL`
Win:	`DKIM_SIGN_ALL=1`

Restrictions and Implementation Choices

- LISTSERV will not sign messages that already have a DomainKeys signature. Double DomainKeys signatures are disallowed in most cases and, even when allowed, there is a risk that they may not be handled correctly by all implementations. This does not apply if the incoming DomainKeys signature has been discarded (for example, a mailing list without "`Misc-Options=KEEP_DKIM_SIGNATURE`"). In that case, the message can be signed without risk of false positive.

- DomainKeys can be used to sign mail-merge messages; however, in this case, LISTSERV's Embedded Mail Merge (EMM) feature MUST be enabled (even if you are using LSMTP). Using EMM is the only way to guarantee that the signing engine will see the exact text being sent to the recipient, and that the signature will match.

New Deliverability Assessment Tool

As spam filters become more and more aggressive, there is a growing risk for legitimate email to be blocked or relegated to spam folders. LISTSERV's new Deliverability Assessment tool will analyze your LISTSERV and DNS configurations and compare them to "best practices," giving you concrete advice on improving your deliverability.

The tool offers the following tests based on the return address hostname and the IP address of the originating server:

- DomainKeys: Yahoo! is the most significant proponent of the DomainKeys system, which is a public key/private key certification process. The public key for a given domain is stored in DNS and the corresponding private key is used to sign mail originating from that domain. The Yahoo!Mail web client displays a small notification for recipients that tells the user whether or not the mail is so certified. Other clients may have similar DomainKeys features.

- Sender Policy Framework (SPF): SPF is an open certification protocol that is also DNS-based. Sites using SPF to verify mail origination perform a DNS lookup to verify that the sending server is authorized to originate mail for the given domain. AOL, Pobox.Com, and GMail are possibly the largest SPF users at this time.

- Sender ID: SenderID is a closed certification protocol, also using DNS authentication-certification, being backed by Microsoft primarily for its Hotmail and MSN services.

- Domain Name Service test: Deliverability Assessment will also check DNS for the presence of A (address), MX (mail-exchanger), and PTR (reverse lookup) records for the hostname being assessed. Many email providers require at least an A record, and many also require a PTR record, to certify that mail is actually originating from the host it claims to be coming from.

Each test response is self-documented and, where appropriate, contains links to external resources describing the protocol in question. Test results are displayed with large green, orange, and red icons to help the administrator quickly zero in on problem areas.

The Deliverability Assessment tool can be reached from the Server Management Main Page.

New DEFAULT_MISC_OPTIONS Site Configuration Setting

A DEFAULT_MISC_OPTIONS variable is now available for use in the site configuration file. When populated with one or more of the available values for the Misc-Options= list header keyword, it sets a default for all lists that do not already have a Misc-Options= setting. If a list has a Misc-Options= keyword, the site-level setting is normally overridden. For instance, if you have (using Windows site.cfg for an example)

```
DEFAULT_MISC_OPTIONS=IGNORE_EMAIL_CASE
```

and a given list has

```
* Misc-Options= RESPECT_EMAIL_CASE
```

then the list-level option overrides the site-level option.

You may also prefix options in DEFAULT_MISC_OPTIONS with either a plus or minus sign (no space between the +/- sign and the name of the option). As before, an unprefixed option is active if the list owner did not specify the corresponding option in the list's "Misc-Options=" keyword, and is otherwise ignored.

An option prefixed with a plus sign is always active, for every list. There is no way for the list owner to turn it off. Therefore, if we modified our example above to read

```
DEFAULT_MISC_OPTIONS=+IGNORE_EMAIL_CASE
```

then that would always override any list-level setting.

Likewise, an option prefixed with a minus signed is prohibited and will be ignored if specified in the list header. Therefore something like

```
DEFAULT_MISC_OPTIONS=-NO_SPAM_CHECK
```

would disallow list owners from disabling the spam check for their list by setting "Misc-Options= NO_SPAM_CHECK".

DOCUMENTED RESTRICTION: Using the plus and minus prefixes together for the same option (for instance, "`DEFAULT_MISC_OPTIONS=+-NO_SPAM_CHECK`") will produce unpredictable results and is not supported.

Multiple options for DEFAULT_MISC_OPTIONS are specified in the usual space-separated manner.

Examples:

VM	`DEFAULT_MISC_OPTIONS = '+IGNORE_EMAIL_CASE SUPPRESS_APPROVED_BY'`
VMS:	`DEFAULT_MISC_OPTIONS "+IGNORE_EMAIL_CASE SUPPRESS_APPROVED_BY"`
unix:	`DEFAULT_MISC_OPTIONS="+IGNORE_EMAIL_CASE SUPPRESS_APPROVED_BY"` `export DEFAULT_MISC_OPTIONS`
Win:	`DEFAULT_MISC_OPTIONS=+IGNORE_EMAIL_CASE SUPPRESS_APPROVED_BY`

New IETF_SUBJECT_TAG Setting for "Misc-Options=" List Header Keyword

It is now possible to add subject tags to IETF headers (that is, for users who are set to the IETFHDR personal option). However, as this can be considered a violation of the practice for IETF-style headers, it can be prevented site-wide by the site administrator if desired.

Adding "Misc-Options= IETFHDR_SUBJECT_TAG" causes the IETFHDR option to always include subject tags (by default, they do not include any subject tags).

The IETFHDR_SUBJECT_TAG option can be disallowed by the site administrator by setting

VM	`DEFAULT_MISC_OPTIONS = '-IETF_SUBJECT_TAG'`
VMS:	`DEFAULT_MISC_OPTIONS "-IETF_SUBJECT_TAG"`
unix:	`DEFAULT_MISC_OPTIONS="-IETF_SUBJECT_TAG"` `export DEFAULT_MISC_OPTIONS`
Win:	`DEFAULT_MISC_OPTIONS=-IETF_SUBJECT_TAG`

as described in the preceding section.

New SUBJECTHDR_SEQUENCE Setting for "Misc-Options=" List Header Keyword

For LISTSERV 14.5, it is possible for each list posting to have a sequence number attributed to it, which can be seen by subscribers who are set to the SUBJECTHDR personal option. This new feature is enabled by adding "Misc-Options= SUBJECTHDR_SEQUENCE" to the list header. It can be enabled by default for all lists on the server by adding SUBJECTHDR_SEQUENCE to DEFAULT_MISC_OPTIONS. The format of the new subject tag is

[listname - number]

For example:

```
Subject: [TEST - 256] Test of SUBJECTHDR_SEQUENCE
```

where 'number' is a sequence number, starting from 1 and increasing.

The "Subject-Tag=" list header keyword is still used to change the text of the subject tag.

RFC2369 Headers Now Supported for List Postings

Support has been added for RFC2369, which calls for the use of message headers such as "List-Help", "List-Subscribe", and "List-Unsubscribe". A list posting using these headers will look like this:

```
Date: Fri, 21 Oct 2005 14:21:03 -0500
Reply-To: Test list <TEST@LISTSERV.EXAMPLE.COM>
Sender: Test list <TEST@LISTSERV.EXAMPLE.COM>
From: Some User <someuser@EXAMPLE.COM>
Subject: What's all this RFC2369 stuff?
To: TEST@LISTSERV.EXAMPLE.COM
Precedence: list
List-Help: <http://listserv.example.com/scripts/wa.exe?LIST=TEST>,
           <mailto:LISTSERV.EXAMPLE.COM?body=INFO+TEST>
List-Unsubscribe: <mailto:TEST-unsubscribe-request@LISTSERV.EXAMPLE.COM>
List-Subscribe: <mailto:TEST-subscribe-request@LISTSERV.EXAMPLE.COM>
List-Owner: <mailto:TEST-request@LISTSERV.EXAMPLE.COM>
List-Archive: <http://listserv.example.com/scripts/wa.exe?LIST=TEST>

I was curious about these new headers, can someone enlighten me?
```

RFC2369 support is activated by default and supplies all of the headers specified in the standard except "List-Post:", which L-Soft considers to be redundant.

In compliance with RFC2369, LISTSERV discards any pre-existing List-xxx tags.

RFC2369 compliance can be disabled using:

```
* Misc-Options= NO_RFC2369
```

and this can also be specified in the site-wide DEFAULT_MISC_OPTIONS variable. When RFC2369 support is disabled, you get the old behavior; that is, the tags are neither added nor removed.

unixODBC Support for MySQL

LISTSERV 14.5 for unix now supports MySQL databases accessed via unixODBC as datastores. The prerequisite for this support is that unixODBC *must* be installed on the unix machine that is running LISTSERV.

The LISTSERV implementation is similar to that for CLI, except that the prefixes are UODBC instead of CLI. You define UODBC_DSN and so on in your configuration, and you use "DBMS= UODBC" or just "DBMS= Yes" in your lists and DISTRIBUTE jobs. For instance, the site configuration for a unixODBC datasource called GREEN would look like this:

```
UODBC_DSN="GREEN"
UODBC_UID="..."
UODBC_AUTH="..."
```

```
export UODBC_DSN UODBC_UID UODBC_AUTH
```

(Replace the ellipses with appropriate DBMS-specific authentication information.)

It is possible to connect to all kinds of databases (as opposed to MySQL only) using unixODBC, but at this time L-Soft does not formally support the use of databases other than MySQL with unixODBC. We would be interested in hearing the results of tests conducted in the field with other DBMS products and would be willing to consider adding support based on those results.

For more information on setting up unixODBC to work with LISTSERV, please see the Developer's Guide to LISTSERV.

New Loopcheck= Default

In LISTSERV 14.5, the new loopcheck heuristic defaults to "Loopcheck= Normal" (which is itself a new option to that keyword setting) if there is no explicit "Loopcheck=" setting in the list header. This is a backward-compatible change that eliminates from the default test suite the test that results in the error *"Sender:", "From:" or "Reply-To:" field pointing to the list*.

L-Soft has decided to change the default in 14.5 to eliminate this test because the kinds of loops it was designed to prevent no longer occur on a typical discussion list; most MTAs that were responsible for them have long since been fixed. On the other hand, there are still exceptions, and this test remains the only reliable way to catch these kinds of loops. To put things in perspective, whenever you post something to a discussion list and you, the poster, receive a notice that the mailbox does not exist, it is a signal that the list may be at risk for this type of loop. Nowadays, this almost never happens, but there are still lists where it does. In addition, the larger the list, the higher the risk.

If you don't want to lose this test when 14.5 is installed on your server, you should add "Loopcheck= Full" to your list header(s) prior to the upgrade. You may also set this value at the site level with the new DEFAULT_LOOPCHECK site configuration variable; for example,

VM	`DEFAULT_LOOPCHECK = 'FULL'`
VMS:	`DEFAULT_LOOPCHECK "FULL"`
unix:	`DEFAULT_LOOPCHECK="FULL"` `export DEFAULT_LOOPCHECK`
Win:	`DEFAULT_LOOPCHECK=FULL`

This setting may then be overridden at the list level if desired. The default value is NORMAL.

In the future, it is anticipated that other tests found to be obsolete will be moved from the "Normal" suite to the "Full" suite, for the same backward compatibility.

New Embedded Mail-Merge (EMM) Default

In LISTSERV 14.5, the Embedded Mail-Merge (EMM) feature introduced in LISTSERV 14.4 is now the default. This is necessary in order to enable all LISTSERV sites to create DomainKeys signatures.

Given the high performance of EMM, this change is unlikely to have any noticeable impact for the average site. Very high-volume LSMTP sites or sites running older hardware may notice performance degradation, and if so, will need either to re-tune their servers or to revert to the old default.

To switch back to the pre-14.5 default (or to set it explicitly before upgrading to LISTSERV 14.5), set

VM:	`EMBEDDED_MAIL_MERGE = 0`
VMS:	`EMBEDDED_MAIL_MERGE "0"`
unix:	`EMBEDDED_MAIL_MERGE=0` `export EMBEDDED_MAIL_MERGE`
Win:	`EMBEDDED_MAIL_MERGE=0`

in LISTSERV's site configuration file and restart the server. Please remember that disabling Embedded Mail-Merge will also disable your server's ability to generate DomainKeys signatures.

WEB INTERFACE - WA

Current Version

LISTSERV 14.5 requires that the Web interface (commonly known as "wa") is version 2.3.42 R1559 or later. To determine what version of "wa" you currently have running, browse to http://yourserver/path-to-wa/wa?DEBUG-SHOW-VERSION for unix, or http://yourserver/path-to-wa/wa.exe?DEBUG-SHOW-VERSION for Windows and OpenVMS).

Other WA Improvements

- The privacy token <[login to unmask]> that hides email addresses in displayed postings for publicly-viewable lists is now a link to the login page.
- Most if not all national language encoding problems for subject lines in WA have been fixed.
- A problem that caused duplicate listings to be displayed in the list-level table of contents has been fixed.
- A problem that would cause WA to display a "Log In" link when the user was already logged in on pages that did not require authentication has been fixed.
- The web posting interface has been rewritten to a considerable extent and should be more user-friendly.

OTHER

Miscellaneous Changes and Fixes

The following miscellaneous fixes and changes are included in LISTSERV 14.5.

- The site-level variable USE_LSMTP_MAIL_MERGE is obsolete and deprecated as of this version. Sites that use it should use EMBEDDED_MAIL_MERGE instead.
- The original release of LISTSERV 14.4 (and possibly earlier) used an incorrect MIME boundary in generated bounces. This has been fixed.
- The LANGUAGE template in a list's WWWTPL file did not always reset when the Language= keyword setting was changed. This has been fixed.
- LMail-formatted "soft" bounces did not result in a SOFTBOUNCE record being written when using NOLIST changelogs. This has been fixed.
- Maintenance expiration messages have been made more consistent.

- The new list deletion feature added in the original release of LISTSERV 14.4 did not always delete the list's archive directory. This has been fixed.

- Nested HTML mail templates caused occasional problems. This has been fixed.

- It was possible for users to be spam-quarantined regardless of their whitelist status because LISTSERV's older anti-spam measures were being taken without reference to the whitelist. This has been changed in 14.5, and the old spam filter now goes through the whitelist before registering an event, which in turn is based on the combined score of both whitelist and blacklist in the same manner as with the new spam filter. However, as the old spam filter lacks a TO context or a bounce flag, only the FROM lists are checked.

Important OS support information

L-Soft formally supports FreeBSD (Intel) and Linux (S/390) since LISTSERV 14.0 (1.8e). A comprehensive list of operating systems (and versions) under which LISTSERV is supported can be found at:

http://www.lsoft.com/products/listserv_os.asp

The following operating systems are no longer supported:

- Windows NT 4.0
- Windows 95/98/Me
- BSDi (Intel)
- IRIX (MIPS)
- Solaris-x86 (Intel)

Sites running these operating systems should migrate to a different operating system. Please contact your sales representative for further information.

Sites running the Windows 95 shareware should note that their licenses will not activate the product under Windows XP. Please contact your sales representative for alternatives if you are planning to upgrade to Windows XP (optionally you may migrate to the LISTSERV Lite Free Edition). Sites running the Windows 95 Lite Free Edition can simply upgrade to the Windows NT/2000/XP LISTSERV Lite Free Edition. You may also elect to continue running LISTSERV under Windows 95/98/Me, but there will be no further new versions or fixes for that platform.

Applying LISTSERV 14.5

IMPORTANT: Install your LISTSERV 14.5 product LAK before upgrading! A valid product LAK (License Activation Key) with "REL=14.5" must be installed before upgrading or LISTSERV will not start after the upgrade.

If you have not received a LISTSERV 14.5 product LAK, please contact your sales representative or SALES@LSOFT.COM before upgrading!

To find out if you can upgrade to LISTSERV 14.5 with your current license key, please issue a SHOW LICENSE command to LISTSERV and examine the response. It will be similar to this:

```
License type:       Permanent
Expiration date:    None - perpetual license
Maintenance until:  1 March 2006, serial number MNT-XYZ-1
Capacity:           Unlimited
```

```
Version:            14.5
Serial number:      XYZ-1
Build date:         15 Feb 2006
```

Your license key will be valid for the 14.5 upgrade if your current LAK is for version **14.5 or higher.**

Sites running LISTSERV 14.4 may use the LAK input tool in the Web Administration interface to apply and check their new LAK before upgrading.

The installation kits found on L-Soft's web site can be used either to install a new copy of LISTSERV or to upgrade an existing installation. To download LISTSERV 14.5, simply go to L-Soft's Web site and download an evaluation copy of LISTSERV or LISTSERV Lite, then follow the installation instructions for your operating system. The kits can be found at:

http://www.lsoft.com/download/listserv.asp

http://www.lsoft.com/download/listservlite.asp

SPECIAL NOTES

1. This document does not include upgrade instructions. Please see the installation guide specific to your OS platform for upgrade instructions.

VMS: http://www.lsoft.com/manuals/1.8e/vmsinst.html

unix: http://www.lsoft.com/manuals/1.8e/unixinst.html

Windows: http://www.lsoft.com/manuals/1.8e/ntinst.html

VM sites currently at the 1.8e or 14.x level should download ftp://ftp.lsoft.com/listserv/vm/upd145.hex and install it per the "Fixes and Upgrades" section of ftp://ftp.lsoft.com/listserv/vm/00-read.me . VM sites currently at the 1.8d or earlier level must first upgrade to 1.8e (LISTSERV 14) before applying this level set fix.

2. The unix kit now only requires a single download. You do not need to download a common.tar.Z file as in previous versions, as those files are now included in the single OS-specific installation file.

3. LISTSERV version 14.5 is available only for operating systems currently supported by L-Soft. When browsing FTP.LSOFT.COM, you may find installation kits for other operating systems, such as Ultrix or SunOS 4.x, but these kits will be based on older versions and/or code bases. L-Soft no longer has development systems for unsupported operating systems and is not in a position to compile LISTSERV 14.5 for these systems.