What's New in LISTSERV® Version 17.5

20 November 2024
(Minor revisions 4 Feb 2024)

LISTSERV 17.5 includes all known fixes, patches and between-release enhancements since the original release of LISTSERV 17.0 up to 20 November 2024. There are several bug fixes and enhancements in LISTSERV itself, and there are also changes and fixes to the WA CGI for the web interface as well as the web and mail templates.

This level-set release is categorized as a **"must-have"** upgrade for organizations running LISTSERV Version 17.0 as it contains new features for securing the web interface, including CAPTCHA integration and rate-limiting to prevent botnets from maliciously entering thousands of subscription requests by bypassing the web interface and connecting directly to WA.

IMPORTANT: LISTSERV 17.5 requires a valid version 17.5 LAK!
This Level Set also requires valid Maintenance expiring on 20 November 2024 or later!

You must FIRST obtain and install a LISTSERV version 17.5 product LAK and (for sites with perpetual licensing) an appropriate maintenance LAK, or LISTSERV will not start after the upgrade.

More Information

Supported Operating Systems

Table of Contents

[Security] New CAPTCHA Support

CAPTCHA solutions allow a web page to require users to pass some test before they can access the functionality of the page, with the idea that humans will be better able to pass these tests than bots. If you've ever been asked to click on photos that contained motorcycles or traffic lights when you tried to log in to a site, then you've encountered a CAPTCHA.

By making it difficult for bots to access the pages, securing a site via CAPTCHA makes it less attractive as a target for bot-based attacks and decreases the chance that such attacks will be effective.

Starting with 17.5, LISTSERV has built-in support for several CAPTCHA-type solutions, which can be used to secure access to the public login, new password request and subscription functions. While older LISTSERV versions had limited support for CAPTCHA, this could not be used to secure LISTSERV against bot-based subscription requests that bypass the web interface altogether and make calls directly to WA. This has been changed in LISTSERV 17.5, and now, if this feature is enabled, all login, new password and subscription requests must be validated using CAPTCHA, making it much more difficult for bot-based requests to get through.

At present, LISTSERV can integrate with three of the most popular CAPTCHA solutions: reCAPTCHA, hCaptcha and Cloudflare Turnstile.

Please note, for Unix, the captcha.php file that makes the feature work REQUIRES PHP version 8 at minimum.

Please note, for Windows, the captcha.aspx file that makes the feature work REQUIRES ASP.NET to be installed on the server.

The relevant settings can be found under Server Administration/Site Configuration under the Web Interface tab.

To set up a CAPTCHA solution for your LISTSERV site, follow these steps:

Step 1: You can configure a secret LISTSERV Captcha Badge to use by itself, or with other CAPTCHA solutions. This is done at the site level (either in SITE.CFG or via the web interface) using the **WWW_CAPTCHA_BADGE** setting.

If defined, the login, new password and subscription screens *will not* accept any requests without this badge or key. **This prevents bots from bypassing any CAPTCHA challenge** since they will not know what the secret badge is.

This secret badge can also be used without a CAPTCHA solution but will be less effective as the badge won't be protected by CAPTCHA and the bots could, in theory, be able to retrieve it from the source code of the web page.

The secret badge can be **any alphanumeric combination of letters and numbers.** It *cannot* contain spaces or other special characters. For maximum security, we **recommend** using a randomly generated string. It will not be necessary for any administrators, list owners or users to type in the code manually. For example, let us assume you choose a badge code of "3A444B6". If configuring this via the web interface, you would find the **WWW_CAPTCHA_BADGE** setting under Server Administration/Site Configuration/Web Interface. Type the value 3A444B6 (or your preferred badge) into the text box, then click the Update button at the bottom of the page.

If preferred, the value can also be configured manually via the site-level configuration files.

For Windows (site.cfg):

```
WWW_CAPTCHA_BADGE=3A444B6
```

For unix (go.user):

```
WWW_CAPTCHA_BADGE="3A444B6"
export WWW_CAPTCHA_BADGE
```

Note that, as always, setting the value manually in either site.cfg or go.user requires the LISTSERV server to be restarted for the change to be recognized.

Step 2: Sign up for the CAPTCHA service of your choice. Then copy and paste the unique site key into one of the following, depending on the service you're using.

- **WWW_CLOUDFLARE_SITEKEY** for Cloudflare Turnstile, or
- **WWW_HCAPTCHA_SITEKEY** for hCaptcha, or
- **WWW_RECAPTCHA_SITEKEY** for reCAPTCHA.

The ***_SITEKEY** values above may also be configured in site.cfg or go.user, in the same format as shown above for **WWW_CAPTCHA_BADGE**.

NOTE: LISTSERV does not support Google ReCAPTCHA v3. If using Google ReCAPTCHA, you MUST use ReCAPTCHA v2, preferably the check-box option.

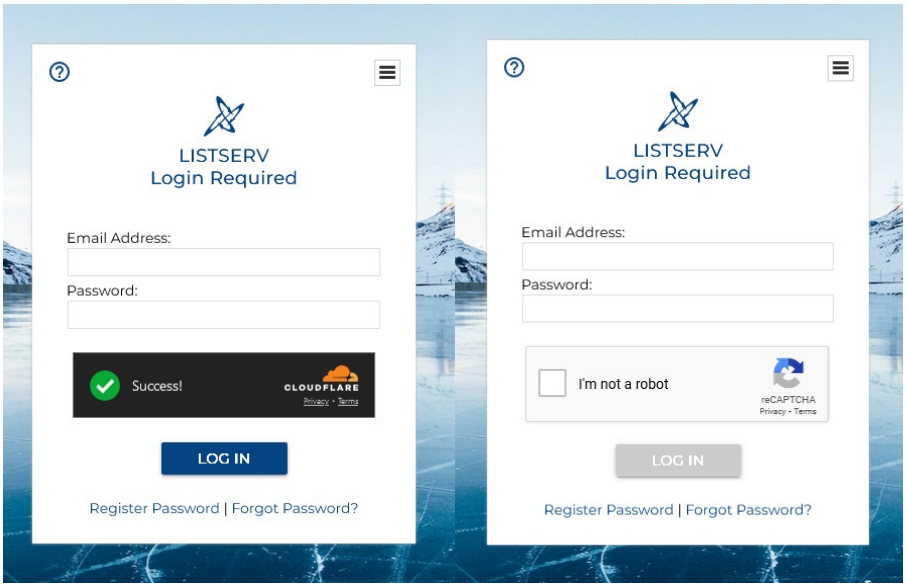
Step 3: In the **WWW_ARCHIVE_DIR** location (look under Server Administration/Site Configuration to find this setting), there should be a subfolder named "captcha". In this location, edit the file named **default.keys** and update it with your LISTSERV domain name, your LISTSERV Captcha Badge from above and your unique secret key. ***Note that the secret key is always different from the site key, so double-check that you are using the right key in the right place.*** Then save this edited file in the same directory under the name **captcha.keys**. The data in the file is in XML format:

```
<config>
  <script>https://listserv.example.com/scripts/wa.exe</script>
  <badge></badge>
  <recaptchaSecretKey></recaptchaSecretKey>
  <hcaptchaSecretKey></hcaptchaSecretKey>
  <cloudflareSecretKey></cloudflareSecretKey>
</config>
```

Step 4: Find the **WWW_CAPTCHA_VENDOR** setting on the site configuration screen, and use the pulldown menu to select your desired CAPTCHA solution. **If this is not set, then no CAPTCHA solution will be used.** *Don't set this until all other steps have been completed,* or else the login, new password and subscription pages will stop working.

Once you have saved your new configuration settings, the public login, new password and subscription screens will automatically use the CAPTCHA solution of your choice, and by defining a secret LISTSERV Captcha Badge, bots will be unable to bypass the CAPTCHA validation, offering the best protection against abuse of your forms.

For example, these are sites that have been secured using the Cloudflare Turnstile service and the reCAPTCHA service:



[Usability] New Support for "List-Unsubscribe-Post:" headers

Beginning with Version 17.5, LISTSERV supports RFC 8058, "Signaling One-Click Functionality for List Email Headers". This allows the recipient ISP to place a one-click unsubscribe button in their customers' email clients for compliant messages, providing customers with an unambiguous way to unsubscribe from mailing lists. Certain large ISPs, e.g., Gmail and Yahoo!, are now requiring that external mailers provide this feature.

In order to activate this feature and generate RFC 8058-compliant List-Unsubscribe-Post: headers for a given mailing list, LISTSERV **requires** that the list use Mail-Merge (i.e., the list must be set explicitly to "Mail-Merge= Yes"). It is impossible to generate a unique per-address List-Unsubscribe-Post: header for non-mail-merge messages since the information is not available to the BSMTP mail generator. Therefore, the use of mail-merge is required for this feature to work.

The headers are generated automatically, without need for any special configuration once mail-merge is enabled for a list. Note that even though the "List-Unsubscribe-Post" mail header is present, individual ISPs can still choose whether or not to make the "Unsubscribe" button available in their email clients depending on the characteristics, reputation and traffic of your email lists. The absence of an "Unsubscribe" button in the email client does not mean that the "List-Unsubscribe-Post" header is missing.

[Security] New Command Rate Limit Feature

To protect against DoS and other abusive behavior, L-Soft has implemented a command rate limit feature. The following configuration variables are available:

```
RATE_LIMIT_LOGIN
RATE_LIMIT_OK
RATE_LIMIT_PW
RATE_LIMIT_SUBSCRIBE
```

The format is:

```
limit[/[qty]unit]
```

If limit = 0, the feature is disabled. If qty is omitted, it defaults to 1 unit. The supported units are S (Second), M (Minute), H (Hour) and D (Day). The default unit is Seconds. These settings do not require a full restart, assuming that they are set in the web interface, just a configuration reload. As shipped, the defaults are:

LOGIN	10/S
OK	10/S
PW	10/M
SUBSCRIBE	50/H

If the rate is exceeded, LISTSERV responds with the following templated message and does not execute the command.

```
>>> MSG_RATE_LIMIT_EXCEEDED Command rate limit exceeded
Rate limit exceeded, try again later.
```

Please note that the values are cumulative per server and *not* per user. This may lead to situations where legitimate logins/subscriptions are denied due to the rate limit being exceeded. To solve this problem, it is recommended that a CAPTCHA solution be implemented as explained above. At minimum, adding a CAPTCHA_BADGE will prevent bots from bypassing the web interface CGI and flooding the server with requests.

[Usability] 'X-ms-reactions: disallow' Header Support

A number of customers have asked for assistance in preventing emoji responses (or as Microsoft puts it, "reactions") to mailing lists. L-Soft has added support for the (documented) Microsoft version of emoji responses in LISTSERV 17.5, which is handled automatically for all outbound list mail only. This is done by adding a header

```
x-ms-reactions: disallow
```

to the outbound message headers. According to Microsoft, if this header is present, attempts to react to the email will be rejected and will fail (in Exchange Online) and the entry point to react to the mail will be greyed out (in Outlook on the Web and Outlook for Windows, with support for other Outlook clients to be added later).

Unfortunately, providing direction to disallow emoji responses from Gmail is not well documented at this time, and no native mitigation has been provided.

This feature is hard-coded ON and cannot be disabled.

[Security] OK Cookie Size Increased to 48 Bits

Beginning with Version 17.5, LISTSERV OK "cookies" are generated 48 bits in length. The cookie processor will continue to accept the 32-bit cookies created by older builds (you need not worry about invalidating cookies created just prior to an upgrade).

Strictly speaking, it was unlikely the existing 32-bit cookies were vulnerable to cracking attempts, as a brute-force attempt to do so would have required ca. 25k WA launches per second (40µs per WA session plus LISTSERV interaction time). The new 48-bit cookies would require ca. 1.6 billion WA launches per second for a similar brute-force attempt. This is because cookies expire after 48 hours, so trying to brute-force a password change was likely impossible before and is even more unlikely now.

[Usability] Unicode Support for Content-Filter Template

The CONTENT_FILTER mail template, which allows for scanning inbound emails for unwanted text strings, now supports the use of Unicode characters. For instance, prior to this change, LISTSERV was unable to parse rules such as the following:

```
>>> CONTENT_FILTER
.CS UTF-8
Subject: 撤回
Action: DISCARD Chinese "recall" message
Subject: 谢绝
Action: DISCARD Chinese "decline" message
```

These rules now work as expected.

[Security] Introducing Support for SAML

Please note that L-Soft Development is still working on this feature. LISTSERV 17.5 contains the code necessary for SAML integration, but Development is still working on the scripts for integration. When the scripts are ready for release, a separate notice will be issued. We anticipate this release no later than 1Q 2025, but it will likely be sooner.

LISTSERV's SSO SAML support will improve user authentication by allowing single sign-on integration through the Security Assertion Markup Language (SAML) protocol. This feature integrates LISTSERV with existing identify providers (IdPs), facilitating a unified login experience and authentication process across multiple platforms.

How it works:

When a user attempts to login to LISTSERV's web interface, the Service Provider (SP) sends a SAML request to the Identity Provider (IdP) of choice. After the IdP authenticates the user's identity, it sends a SAML assertion back to the SP, containing an attribute that corresponds to the user's email address. This email address will then be used by LISTSERV's SAML support to generate a login token for the underlying user and grant the user access to the resources.

[Bug/Improvement] [Linux] Fix for Integration with Newer Versions of unixODBC

A non-backward compatible change appeared in unixODBC after the rollout of Red Hat Enterprise Linux 8 (and other distributions using the Linux 4.x kernel) and the newer versions of unixODBC which were shipped with them. This change did not affect all Linux customers, but has become more urgent with more recent versions of Linux. The issue was carefully reviewed by development and has been fixed in LISTSERV 17.5.

It should be noted that the MySQL and MariaDB connectors shipped by default with Red Hat 9 and similar variants will still crash if TRACE is enabled. This is due to a buffer overrun in the

version of unixODBC shipped with those distributions, which was from 2020. A newer version of unixODBC from 2022 contains a fix for this problem, should customers experience it.

LISTSERV 17.5 Changes for WA

The current WA version at the version 17.5 release is "17.5 (Build Date: 19 November 2024)".

WA continues to undergo improvements and optimizations. L-Soft also continues to quash XSS and similar vulnerabilities as they are reported. Because these issues remain exploitable in older versions of WA, L-Soft will not discuss the specific changes made in this regard, other than to state that all those vulnerabilities that have been found during the course of a comprehensive code review have been fixed in the current release of WA.

[Security] Support for SameSite Cookie attribute

New in LISTSERV 17.5, this configuration variable defines the **SameSite** attribute for LISTSERV login cookies, which controls whether or not a cookie is sent with cross-site requests. The possible values are Strict, Lax and None.

The configuration variable controlling this is **WWW_COOKIE_SAMESITE**. It can be set in the web interface by going to Server Administration/Site Configuration/Web Interface.

The default value is **Strict**, which means that the cookie is only sent for same-site requests.

The other possible values are **Lax** and **None**. We **strongly recommend** that the default value be used.

Important: If considering whether to lower the cookie security level, we **strongly recommend** that the implications of setting the SameSite attribute to Lax or None are clearly understood. While it is beyond the scope of this document to delve into the intricacies of the HTTP SameSite attribute, we recommend reading the Internet Draft standard draft-ietf-httpbis-rfc6265bis-15 (in particular 5.6.7.1. "Strict" and "Lax" enforcement) or an article such as https://web.dev/articles/samesite-cookies-explained, which explains the concept of the attribute and the implications for setting it to the various values.

[Security] New Default Login Cookie Duration

In LISTSERV 17.5, to improve security, the default login cookie duration has been changed to SESSION and is enforced for all users on the LISTSERV site. This means that rather than a login cookie with a specific expiration date and time, the new login cookie is only valid for as long as

the browser session is active, after which the cookie will no longer be valid, and the user will need to log in again.

While not recommended, this behavior can be overridden by modifying the DEFAULTS template under Server Administration/Web Templates. The relevant lines look as follows:

```
+******************** Login Cookie Expiration ********************
+*
+* SESSION - end of browser session
+* m - minutes (60m)
+* d - days (30d)
+* w - weeks (1w)
+* M - months (12M)
+* y - years (2y)
+* 0 - never expires
+*
+* Defines expiration but allows users to change setting through
personal preferences
+SEP COOKIE_EXPIRATION SESSION
+* Defines expiration and forces all users to use this setting (SESSION
by default)
+SE EXPIRECOOKIE_OVERRIDE SESSION
```

The COOKIE_EXPIRATION setting sets the default for all users but allows them to select their own preferred cookie duration on the Preferences screen. If you wanted to change the default login cookie expiration to 60m instead of SESSION, you can enter +SEP COOKIE_EXPIRATION 60m.

The EXPIRECOOKIE_OVERRIDE setting forces all users, regardless of the setting that they have selected on the Preferences screen, to use the login cookie duration entered. Again, if you wanted to change the enforced login cookie duration to 60m instead of SESSION, you can enter +SE EXPIRECOOKIE_OVERRIDE 60m. If you don't want to enforce a specific login cookie duration and wish to allow individual users to select their own cookie duration on the Preferences screen, you can enter +SE EXPIRECOOKIE_OVERRIDE 0.

[Security] New Option to Hide X and Y Tokens from All URLs

In LISTSERV 17.5, as an extra security measure to prevent the accidental disclosure of active X and Y tokens, site administrators can choose to remove the X and Y tokens from all URLs. This setting can be enabled by modifying the DEFAULTS template under Server Administration/Web Templates. The relevant lines look as follows:

```
+* Hides OPTXY from all URLs as an extra security measure
+*
+* 0 - Do not hide
+* 1 - Hide (if you're using LISTSERV together with LISTSERV Maestro,
make sure that your Maestro version is 11.0-8 or later)
+*
```

```
+SE HIDEOPTXY 0
+*
+BB &+HIDEOPTXY;
+SE OPTXY
+EB
```

To hide the X and Y tokens from all URLs, enter +SE HIDEOPTXY 1.

Important: If you are using LISTSERV together with LISTSERV Maestro, make sure that your LISTSERV Maestro version is 11.0-8 or later before enabling this setting. If you are not using LISTSERV Maestro, you can enable this setting without restrictions.

[Security] New Option to Suppress Page-Specific Parameters from Being Submitted During the Login Process

As an extra security measure, site administrators can also choose to suppress page-specific parameters from being submitted during the login process. To enable this feature, modify the DEFAULTS template under Server Administration/Web Templates. The relevant lines look as follows:

```
+* Suppresses page-specific parameters from being submitted during the
login process as an extra security measure
+*
+* 0 - Include page-specific parameters
+* 1 - Suppress page-specific parameters
+*
+SE NOLOGINPARAMETERS 0
```

To suppress all page-specific parameters from being submitted during the login process, you can enter +SE NOLOGINPARAMETERS 1.

[Usability] Modernized Mail Templates and Confirmation Emails

In LISTSERV 17.5, the most common confirmation and informational emails have been simplified and modernized. In addition, these confirmation emails are now in HTML format by default. You can preview or change the format of the confirmation messages by going to Server Administration/Mail Templates and using the pulldown menu under Template Style. The color scheme and look of the HTML mail template comes directly from your site customization settings, so if you were to change the color scheme of your LISTSERV site and add a custom logo, all of those customizations will carry through to the default HTML template automatically.

[Usability] New TCPGUI_PUBLIC_IPADDR Site Configuration Variable

LISTSERV 17.5 contains a new site configuration variable for LISTSERV sites running in virtual (cloud) services such as Microsoft Azure and Amazon AWS (but not limited to those services). Typically, a virtual server is assigned a non-routable internal IP address belonging to one of the three private class ranges, as opposed to a routable IP address facing the public Internet. This provides security for operations being conducted strictly within the cloud that have no reason to allow general access from the Internet.

For a virtual machine running LISTSERV, a static external IP is required in order for mail and web traffic to reach the server. In Azure (for example) this is done by obtaining Public IP Prefixes which contain a block of external IP addresses, and assigning one of the IPs in the block thus obtained to the virtual machine running LISTSERV.

This is all well and good for SMTP mail, but the LISTSERV web interface will be listening on the internal (private) address by default (the existing **TCPGUI_IPADDR** configuration variable MUST be set to the internal address in order for WA to talk to LISTSERV). In order to tell the web interface to listen to the external (public) IP address, the new configuration variable **TCPGUI_PUBLIC_IPADDR** is used. We recommend that the variable be configured manually in the site-level configuration file, as follows:

For Windows (site.cfg):

```
TCPGUI_PUBLIC_IPADDR=aaa.bbb.ccc.ddd
```

For unix (go.user):

```
TCPGUI_PUBLIC_IPADDR="aaa.bbb.ccc.ddd"
export TCPGUI_PUBLIC_IPADDR
```

Where "aaa.bbb.ccc.ddd" is the *public-facing* IP address, e.g., for Windows,

```
TCPGUI_PUBLIC_IPADDR=1.2.3.4
```

Or for unix,

```
TCPGUI_PUBLIC_IPADDR="1.2.3.4"
Export TCPGUI_PUBLIC_IPADDR
```

If this variable is set manually in the site.cfg or go.user file after the LISTSERV server has been installed and is running, it will require a restart of the LISTSERV service to pick up the change.

If the variable is set in the web interface, it will require only a reload of the configuration.

[HPO] Improvement: Page Loading Delay under HPO Has Been Eliminated

After the release of LISTSERV 17.0, some HPO customers noticed a delay of 2-3 seconds while loading just about any page of the LISTSERV web interface. This was traced to HPO

optimization code in the WA CGI that was not executing properly. This issue was fixed, and customers who have installed the newer WA have reported that the delays have disappeared, and page loading is now nearly instantaneous. The version of WA shipped with LISTSERV 17.5 has this fix.

Important Reminder: Windows Defender Anti-Virus Replaces F-Secure Anti-Virus

- As of 31 Mar 2022, native support for F-Secure Server Security and F-Secure Linux Security were dropped.

- Windows Defender Anti-Virus is fully supported natively by LISTSERV 17.0 and following for Windows Servers.

- Anti-virus for LISTSERV on Unix platforms is supported exclusively through the LISTSERV AVS. For more information about the LISTSERV AVS, please contact your sales representative.

- There remains no intent to make this functionality available in the Lite version of the product.

Applying LISTSERV 17.5

IMPORTANT: If you are upgrading **to** any level of LISTSERV 17.x **from** LISTSERV 16.5 or earlier, please **STOP NOW** and read the LISTSERV 17.0 release notes (yes, we do mean the **17.0** release notes) before applying either LISTSERV 17.5 or any LISTSERV 17.5 level set release. **In particular,** you should read the section **Preliminary Setup for Upgrades in the LISTSERV 17.0 release notes** before attempting to upgrade from LISTSERV 16.x to LISTSERV 17.0 or later.

If you are already running 17.0 and are upgrading to 17.5, the above does not apply to you and you may continue.

IMPORTANT: Install (or ensure that it is installed) your LISTSERV 17.5 product LAK before upgrading! A valid product LAK (License Activation Key) with "REL=17.5" must be installed before upgrading or LISTSERV will not start after the upgrade.

Also, a valid maintenance LAK expiring no earlier than **20 November 2024** is required in order to apply this release.*

If you have not received a LISTSERV 17.5 product LAK, please contact your sales representative or sales@lsoft.com before upgrading!

To find out if you can upgrade to LISTSERV 17.5 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:   26 Nov 2025, serial number MNT-XYZ-1
Capacity:            Unlimited
Version:             17.5
Serial number:       XYZ-1
Build date:          20 Nov 2024
```

Your license key will be valid for the 17.5 upgrade if your current product LAK is for version 17.5 or higher, and your maintenance LAK is valid until at least 20 November 2024.

---

* LISTSERV Lite Free Edition installations require *only* the 17.5 product LAK, which is included in the LISTSERV Lite Free Edition kits.

Sites running LISTSERV 14.4 or later may use the LAK input tool in the web interface to apply and check their new LAK before upgrading. You can find this under Server Administration/Site Configuration/License.

The installation kits found on L-Soft's website are used either to install a new copy of LISTSERV or to upgrade an existing installation. L-Soft does not provide patch kits or dedicated upgrade kits; to upgrade to LISTSERV 17.5, simply go to L-Soft's website 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:

https://www.lsoft.com/download/listserv.asp
https://www.lsoft.com/download/listservlite.asp

All LISTSERV installation guides are found on our documentation page at:

https://www.lsoft.com/manuals

Current Supported Operating Systems

LISTSERV for Microsoft Windows	Windows 10 (64-bit only)*
	Windows 11 (64-bit only)*
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
LISTSERV for Unix	AIX 4.3 (PowerPC) and later
	Linux 3.10 and later (e.g., RH7 64-bit)
	Linux 5.x and later (e.g., RH9 64-bit)
	Linux 2.4.2 or later (S/390)
	Solaris 10 and later (SPARC)
	Solaris 10 and later (x64)
LISTSERV for VM/ESA, z/VM	(Contact L-Soft for details)

*The Pro or Enterprise editions are recommended.

LISTSERV for Windows and Unix is also known to run in virtual servers under Microsoft Azure and Amazon AWS.

Support for 32-bit Windows and Linux was withdrawn as of the release of LISTSERV 16.0-2017a. Support for Windows prior to Windows 10 and Windows Server 2016 was withdrawn when manufacturer support for those earlier versions was dropped by Microsoft.

Future LISTSERV support for all Windows products is contingent on official Microsoft support for those products. For instance, our support for LISTSERV running on Windows 10 will end on October 14, 2025. Mainstream support for Windows Server 2016 technically ended on January 11, 2022, but we will continue to support LISTSERV on Windows Server 2016 until the Extended End Date of January 12, 2027. Mainstream support for Windows Server 2019 ended on January 9, 2024, but we will continue to support LISTSERV on Windows Server 2019 until the Extended End Date of January 9, 2029.

Future LISTSERV support for all Unix products is contingent on official vendor support for those products.

Support for OpenVMS was withdrawn as of the release of LISTSERV 16.0-2017a.

A separate build for Linux 2.6 that was built on RHEL 5 was withdrawn with the release of LISTSERV 16.5-2018a.

Support for MacOS X (x86) was withdrawn as of the release of LISTSERV 17.0.

SPECIAL NOTES

Upgrade Instructions

This document does not include upgrade instructions. Please see the installation guide specific to your OS platform for upgrade instructions. Installation guides are available at:

https://www.lsoft.com/resources/manuals.asp

Supported Operating Systems

LISTSERV version 17.5 is available only for operating systems currently supported by L-Soft. L-Soft no longer maintains development systems for unsupported operating systems and is not in a position to compile LISTSERV 17.5 for those systems.

Support for GDPR Compliance

L-Soft has made available, at no charge, a comprehensive EU General Data Protection Regulation (GDPR) reporting script written in the Microsoft PowerShell scripting language, which can be used in conjunction with L-Soft's LCMD or LCMDX utilities on Microsoft Windows, Linux, and MacOS systems. For more information, please see our *GDPRSCAN Installation and Operating Guide for Windows, Linux, and MacOS* at:

https://www.lsoft.com/manuals/17.0/GDPRSCAN_Installation_and_Operating_Guide.html

end of file