

## SENDMAIL RELEASE NOTES

This listing shows the version of the sendmail binary, the version of the sendmail configuration files, the date of release, and a summary of the changes in that release.

8.15.1/8.15.1 2014/12/06

SECURITY: Properly set the close-on-exec flag for file descriptors (except stdin, stdout, and stderr) before executing mailers.

If header rewriting fails due to a temporary map lookup failure, queue the mail for later retry instead of sending it without rewriting the header. Note: this is done while the mail is being sent and hence the transaction is aborted, which only works for SMTP/LMTP mailers hence the handling of temporary map failures is suppressed for other mailers. SMTP/LMTP servers may complain about aborted transactions when this problem occurs.

See also "DNS Lookups" in sendmail/TUNING.

Incompatible Change: Use uncompressed IPv6 addresses by default, i.e., they will not contain "::". For example, instead of ::1 it will be 0:0:0:0:0:0:0:1. This permits a zero subnet to have a more specific match, such as different map entries for IPv6:0:0 vs IPv6:0. This change requires that configuration data (including maps, files, classes, custom ruleset, etc) must use the same format, so make certain such configuration data is updated before using 8.15. As a very simple check search for patterns like 'IPv6:[0-9a-fA-F]\*:::' and 'IPv6::'. If necessary, the prior format can be retained by compiling with: APPENDEF(`conf\_sendmail\_ENVDEF', `-DIPV6\_FULL=0') in your devtools/Site/site.config.m4 file.

If debugging is turned on (-d0.14) also print the OpenSSL versions, both build time and run time (provided STARTTLS is compiled in).

If a connection to the MTA is dropped by the client before its hostname can be validated, treat it as "may be forged", so that the unvalidated hostname is not passed to a milter in xxfi\_connect().

Add a timeout for communication with socket map servers which can be specified using the -d option.

Add a compile time option HESIOD\_ALLOW\_NUMERIC\_LOGIN to allow numeric logins even if HESIOD is enabled.

The new option CertFingerprintAlgorithm specifies the fingerprint algorithm (digest) to use for the presented cert. If the option is not set, md5 is used and the macro {cert\_md5} contains the cert fingerprint.

However, if the option is set, the specified algorithm (e.g., sha1) is used and the macro {cert\_fp} contains the cert fingerprint.

That is, as long as the option is not set, the behaviour does not change, but otherwise, {cert\_md5} is superseded by {cert\_fp} even if you set CertFingerprintAlgorithm to md5.

The options ServerSSLOptions and ClientSSLOptions can be used to set SSL options for the server and client side respectively. See SSL\_CTX\_set\_options(3) for a list.

Note: this change turns on SSL\_OP\_NO\_SSLv2 and SSL\_OP\_NO\_TICKET for the client. See doc/op/op.me for details.

The option CipherList sets the list of ciphers for STARTTLS. See ciphers(1) for possible values.

Do not log "STARTTLS: internal error: tls\_verify\_cb: ssl == NULL" if a CRLFile is in use (and LogLevel is 14 or higher.)

Store a more specific TLS protocol version in \${tls\_version} instead of a generic one, e.g., TLSv1 instead of TLSv1/SSLv3.

Properly set {client\_port} value on little endian machines. Patch from Kelsey Cummings of Sonic.net.

Per RFC 3848, indicate in the Received: header whether SSL or SMTP AUTH was negotiated by setting the protocol clause to ESMTPS, ESMTPA, or ESMTPSA instead of ESMTPL.

If the 'C' flag is listed as TLSSrvOptions the requirement for the TLS server to have a cert is removed. This only works under very specific circumstances and should only be used if the consequences are understood, e.g., clients may not work with a server using this.

The options ClientCertFile, ClientKeyFile, ServerCertFile, and ServerKeyFile can take a second file name, which must be separated from the first with a comma (note: do not use any spaces) to set up a second cert/key pair. This can be used to have certs of different types, e.g., RSA and DSA.

A new map type "arpa" is available to reverse an IP (IPv4 or IPv6) address. It returns the string for the PTR lookup, but without trailing {ip6,in-addr}.arpa.

New operation mode 'C' just checks the configuration file, e.g., sendmail -C new.cf -bC will perform a basic syntax/consistency check of new.cf.

The mailer flag 'I' is deprecated and will be removed in a future version.

Allow local (not just TCP) socket connections to the server, e.g., 0 DaemonPortOptions=Family=local, Addr=/var/mta/server.sock can be used.

If the new option MaxQueueAge is set to a value greater than zero, entries in the queue will be retried during a queue run only if the individual retry time has been reached which is doubled for each attempt. The maximum retry time is limited by the specified value.

New DontBlameSendmail option GroupReadableDefaultAuthInfoFile to relax requirement for DefaultAuthInfo file.

Reset timeout after receiving a message to appropriate value if STARTTLS is in use. Based on patch by Kelsey Cummings of Sonic.net.

Report correct error messages from the LDAP library for a range of small negative return values covering those used by

#### OpenLDAP.

Fix compilation with Berkeley DB 5.0 and 6.0. Patch from Allan E Johannesen of Worcester Polytechnic Institute. CONFIG: FEATURE(`nopercenthack') takes one parameter: reject or nospecial which describes whether to disallow "%" in the local part of an address.

DEVT00LS: Fix regression in auto-detection of libraries when only shared libraries are available. Problem reported by Bryan Costales.

LIBMILTER: Mark communication socket as close-on-exec in case a user's filter starts other applications.

Based on patch from Paul Howarth.

Portability:

SunOS 5.12 has changed the API for sigwait(2) to conform with XPG7. Based on patch from Roger Faulkner of Oracle.

Deleted Files:

libsm/path.c