



Hewlett Packard
Enterprise

HP-UX Sendmail 8.15.2 Release Notes

Part Number: 869799-002
Published: April 2017

Legal Notices

© Copyright 2001, 2017 Hewlett Packard Enterprise Development LP.

The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing here should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Links to third-party websites take you outside the HPE website. HPE has no control over and is not responsible for information outside HPE.com. Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Acknowledgements

UNIX® is a registered trademark of The Open Group.

Copyright (c) 1990, 2013 Oracle and/or its affiliates. All rights reserved.

Copyright (c) 1995, 1996 The President and Fellows of Harvard University. All rights reserved.

Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved.

Copyright 1998-2015 The OpenLDAP Foundation, All rights reserved.

Copyright (c) 1998-2014 Proofpoint, Inc. All rights reserved.

Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

Contents

Sendmail 8.15.2 Release Notes.....	3
Announcement.....	3
What is in This Version.....	3
Sendmail 8.15.2 Features.....	3
Removed Features.....	5
Installation requirements and procedure for Sendmail.....	5
Migrating from Sendmail 8.13.3 to Sendmail 8.15.2.....	6
Known Problems.....	6
Documentation.....	6
Man Pages.....	6
Product Documentation.....	7
RFCs Supported by Sendmail 8.15.2.....	7
License Information.....	7
Defects Fixed in This Release.....	8
Defects Fixed in the HP-UX 11i v3 Operating System.....	8
Source code availability.....	8

Sendmail 8.15.2 Release Notes

This document discusses the new and changed features in the Sendmail 8.15.2 software. It also describes how to install Sendmail 8.15.2.

This document addresses the following topics:

- [Announcement](#) on page 3
- [What is in This Version](#) on page 3
- [Sendmail 8.15.2 Features](#) on page 3
- [Removed Features](#) on page 5
- [Installation requirements and procedure for Sendmail](#) on page 5
- [Migrating from Sendmail 8.13.3 to Sendmail 8.15.2](#) on page 6
- [Known Problems](#) on page 6
- [Documentation](#) on page 6
- [Defects Fixed in This Release](#) on page 8

Announcement

Sendmail is an implementation of SMTP protocol for transmitting email. HP-UX Sendmail 8.15.2.x is based on Open Source [Sendmail 8.15.2](#).

Sendmail 8.15.2 for HP-UX 11i v3 can be downloaded at <http://www.hpe.com/support/softwaredepot>.

What is in This Version

A new version of Sendmail 8.15.2 is made available on HP-UX 11i v3.

Sendmail 8.15.2 Features

Sendmail 8.15.2 includes the following new features:

- Security enhancements
 - Sendmail generates **DHParameters** of 2048 bit prime by default.
 - The option **CertFingerprintAlgorithm** sets the finger-print algorithm (digest) to use for the presented certificate.

If the option is not set, `md5` is used and the macro contains the certificate fingerprint. If the option is explicitly set, the specified algorithm (for example, `sha1`) is used and the macro `${cert_fp}` contains the certificate fingerprint.
 - The options **ServerSSLOptions** and **ClientSSLOptions** can be used to set SSL options for the server and client side respectively. See **SL_CTX_set_options** (3) for a list.

NOTE:

This change turns on **SSL_OP_NO_SSLv2** and **SSL_OP_NO_TICKET** for the client.

- The option **CipherList** sets the list of ciphers for **STARTTLS**.
- The options `ClientCertFile`, `ClientKeyFile`, `ServerCertFile` and `ServerKeyFile` can take a second file name.

These must be separated from the first with a comma (do not use any spaces) to set up a second certificate or key pair.

- This can be used to have certificates of different types, for example, RSA and DSA.
 - SSLv2 and SSLv3 are not supported. RFC 4507-style session tickets are not supported.
 - Anti-Spam control
 - Militer, the mail filter, supports the new call back functions:
 - **xxfi_negotiate()**

is used to dynamically (at runtime) determine the available protocol actions and features of the MTA, and also to specify which of these a militer wants to use.

This enables more flexibility than hardcoding these flags in the **xxfi_flags** field of the **smfiDesc** structure.
 - **xxfi_data()** is available, so milters can act on the DATA command.
 - **xxfi_unknown()** is available, so milters can receive unknown SMTP commands.
 - The new return code **SMFIS_SKIP** can be used in the **xxfi_body()** callback to skip over further body chunks, and redirect to the **xxfi_eom()** callback.

This is useful if a militer can make a decision based on the body chunks it already received without reading the entire rest of the body and the militer wants to invoke functions that are only available from the **xxfi_eom()** callback.
 - Require Reverse DNS (**require_rdns**) to reject messages from SMTP clients IP addresses that do not have proper reverse DNS.
 - Block Bad Helo (**block_bad_helo**) to reject messages from SMTP clients which provide a HELO/EHLO argument which is either unqualified or is one of our own names (the server name instead of the client name).
 - Bad MX (**badmx**) to reject envelope sender addresses (MAIL) whose domain part resolves to a "bad" MX record.
 - New named config file rule **check_eom** which is called at the end of a message, its parameter is the size of the message.
- If the macro `{addr_type}` indicates that the current address is a header address it also distinguishes between recipient and sender addresses (as it is done for envelope addresses).
- The macro **check_relay** is set, the value is accessible by all transactions in the same SMTP session.
 - The **SharedMemoryKeyFile** option: If shared memory support is enabled, the MTA can be prompted to select a shared memory key itself by setting **SharedMemoryKey** to `-1` and specifying a file where to store the selected key.
 - Newer DNS map options: `-B`: Specify a domain that is always appended to queries. `-z`: Specify the delimiter at which to cut off the result of a query if it is too long. `-Z`: specify the maximum number of entries to be concatenated to form the result of a lookup.
 - The operator `r` for the **arith** map to return a random number.
 - The macros **SMTP_MAILER_LL** and **RELAY_MAILER_LL**, that are used to override the maximum line length of the SMTP mailers.
 - The option **relaytofulladdress** for **access_db** to allow entries in the access map to be of the form `To:user@example.com RELAY`
 - A new mailer flag **!** is available to suppress an MH hack that drops an explicit **From:** header if it is the same as what Sendmail would generate.
 - 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. For example, `sendmail -C new.cf -bC` performs a syntax or consistency check of `new.cf` (`sendmail.cf` or `submit.cf`).
 - Allow local (not just TCP) socket connections to the server, for example, `O DaemonPortOptions=Family=local, Addr=/var/mta/server.sock` can be used.
 - `dnsbl` and `enhdnsbl` can discard or quarantine messages from blacklisted clients as second argument.

- The option **UseCompressedIPv6Addresses** to select between compressed and uncompressed IPv6 addresses. By default, Sendmail supports uncompressed IPv6 addresses. If **UseCompressedIPv6Addresses** is set to select compressed IPv6 Address.
- Allow connections from `IPv6:0:0:0:0:0:0:0:1` to relay again.
- If shared memory is used and the **RunAsUser** option is set, the owner and group of the shared memory segment is set to the ids specified. **RunAsUser** and the access mode is set to `0660` to allow for updates by Sendmail processes.
- If DSN support is disabled in `access_db`, the related **ESMTP** parameters for **MAIL** and **RCPT** should be rejected.

Sendmail 8.15.2 includes these new options:

- The new sub options for **DaemonPortOptions** to set them individually per daemon socket: **DeliveryMode** **DeliveryMode refuseLA RefuseLA delayLA DelayLA queueLA QueueLA children** **MaxDaemonChildren**
- The **HeloName** option to set the name for the `HELO/EHLO` command (instead of `$j`).
- The **SoftBounce** option (if set), issue temporary errors (`4xy`) instead of permanent errors (`5xy`). This can be useful during the testing of a new configuration to avoid erroneous bouncing of mails.
- The **MaxNOOPCommands** option to override default of 20 for the number of "useless" commands before the SMTP server will slow down responding.
- New Privacy Options **noactualrecipient** to avoid putting X-Actual-Recipient lines in DSNs revealing the actual account that addresses map to.
- The sub options **eah** and **data** to specify the list of macros a Milter should receive at those stages in the SMTP dialogue.
- The option **MaxQueueAge** is set to a value greater than zero. Entries are retried during a queue run only on maximum retries which are doubled for each attempt. The maximum retry time is limited by the specified value.
- The **DontBlameSendmail** option **GroupReadableDefaultAuthInfoFile** to relax requirement for `DefaultAuthInfo` file.
- The **StatusFile** option is set to the **StatusFile** (`StatusFile=/etc/mail/statistics`), `mailstats` command print mail traffic statistics. If it is not set, `mailstats` command will display `No statistics file located`
- If **Timeout.resolver.retrans** is set to a value larger than 20, the **resolver.retry** is set to 1 for `gethostbyaddr()` lookups.
- The `-do` option used to set a timeout for communication with socket map servers.
- The `-K` option for LDAP maps to replace %1 through %9 in the lookup key with the LDAP escaped contents of the arguments specified in the map lookup.

Removed Features

Sendmail 8.15.2 does not include the following features:

- Support for IPv4-mapped IPv6 addresses to prevent the MTA from using a mapped address over a legitimate IPv6 address, and to enforce semantics over an IPv6 connection.
- The mailer flag `I` is removed.
- The default domain `blackholes.mail-abuse.org` for `dnsbl` and `enhdnsbl` is no longer available.

Installation requirements and procedure for Sendmail

For a detailed information on all the installation requirements and procedure for Sendmail version 8.15.2, see [SMail815](#).

Migrating from Sendmail 8.13.3 to Sendmail 8.15.2

Upgrade from Sendmail 8.13.3 to Sendmail 8.15.2 will continue to work as is, with the configuration files of Sendmail 8.13.3.

Users have to make appropriate changes to configuration files to make use of the new features in 8.15.2. For this, re-generate `sendmail.cf` with the `gen_cf` utility.

Known Problems

These are the known problems in Sendmail 8.15.2:

- You must use the `O DaemonPortOptions=Name=NoMTA, Addr=127.0.0.1, M=E`, in `submit.mc` to avoid problems with host name resolution for the localhost. This is because many systems do not resolve localhost to 127.0.0.1 (or `::1` for IPv6). If you do not use IPv4 addresses and use only IPv6 addresses, you must complete the following steps to change the `/usr/newconfig/etc/mail/cf/cf/submit.mc`

Procedure

1. Change `[127.0.0.1]` to `[IPv6:::1]` in the `submit.mc` file as follows:

```
FEATURE('msp', '[IPv6:::1]') dnl for Compressed IPv6 Address
```

or

```
FEATURE('msp', '[IPv6:0:0:0:0:0:0:0:1]') dnl for UnCompressed IPv6 Address.
```

2. Run the following commands to regenerate the `submit.cf` file:

```
# cd /usr/newconfig/etc/mail/cf/cf/
```

```
# ./gen_cf
```

3. Select the option “6: Generate `submit.cf`” in the main menu of the `gen_cf` script.
4. Copy the `/usr/newconfig/etc/mail/cf/cf/submit.cf.gen` file to `/etc/mail/submit.cf`.
5. To start the Sendmail daemon, run the following command at the HP-UX prompt:

```
/sbin/init.d/sendmail start
```

Documentation

These sections discuss the Sendmail 8.15.2 documentation:

Man Pages

Table 1: Description of man pages distributed with the Sendmail 8.15.2 depot

Man Page	Description
<code>killsm.1m</code>	Kills the sendmail daemon.
<code>mailq.1</code>	Prints a summary of the mail messages queued for future delivery.
<code>mailstats.1</code>	Prints mail traffic statistics.
<code>makemap.1m</code>	Creates database maps for Sendmail.
<code>praliases.1</code>	Prints system-wide sendmail aliases.

Table Continued

Man Page	Description
sendmail.1m	Sends a message to one or more recipients or addresses, routing the message through necessary networks.
identd.1m	Specifies the TCP/IP IDENT protocol server.

Product Documentation

For more information on Sendmail, see the **HP-UX Mailing Services Administrator's Guide** at: <http://www.hpe.com/info/hpux-networking-docs-11iv3>.

RFCs Supported by Sendmail 8.15.2

These are the RFCs supported by Sendmail 8.15.2:

- RFC 821 (*Simple Mail Transfer Protocol*)
- RFC 822 (*STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES*)
- RFC 974 (*Mail routing and the domain system*)
- RFC 1123 (*Requirements for Internet Hosts - Application and Support*)
- RFC 1652 (*SMTP Service Extension for 8bit-MIMEtransport*)
- RFC 1869 (*SMTP Service Extensions*)
- RFC 1870 (*SMTP Service Extension for Message Size Declaration*)
- RFC 1891 (*SMTP Service Extension for Delivery Status Notifications*)
- RFC 1892 (*The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages*)
- RFC 1893 (*Enhanced Mail System Status Codes*)
- RFC 1894 (*Extensible Message Format for Delivery Status Notifications*)
- RFC 1985 (*SMTP Service Extension for Remote Message Queue Starting*)
- RFC 2033 (*Local Mail Transfer Protocol*)
- RFC 2034 (*SMTP Service Extension for Returning Enhanced Error Codes*)
- RFC 2045 (*Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*)
- RFC 2222 (*Simple Authentication and Security Layer (SASL)*)
- RFC 2476 (*Message Submission*)
- RFC 2487 (*SMTP Service Extension for Secure SMTP over TLS*)
- RFC 2505 (*Anti-Spam Recommendations for SMTP MTAs*)
- RFC 2553 (*Basic Socket Interface Extensions for IPv6*)
- RFC 2554 (*SMTP Service Extension for Authentication*)
- RFC 2821 (*Simple Mail Transfer Protocol*)
- RFC 2822 (*Internet Message Format*)
- RFC 2852 (*Deliver By SMTP Service Extension*)
- RFC 2920 (*SMTP Service Extension for Command Pipelining*)
- RFC 3848 (*ESMTP and LMTP Transmission Types Registration*)
- RFC 6176 (*Prohibiting Secure Sockets Layer (SSL) Version 2.0*)

License Information

For detailed license information, see the following files that are delivered with Sendmail 8.15.2:

Sendmail : /usr/share/doc/Sendmail/Sendmail.LICENSE

Berkeley DB : /usr/share/doc/Sendmail/BerkeleyDB.LICENSE

Cyrus SASL : /usr/share/doc/Sendmail/CyrusSASL.LICENSE

Defects Fixed in This Release

This section discusses the defects fixed in Sendmail 8.15.2 in the HP-UX 11i v3 operating system.

- [Defects Fixed in the HP-UX 11i v3 Operating System](#) on page 8

Defects Fixed in the HP-UX 11i v3 Operating System

Table 2: Defects fixed in Sendmail 8.15.2 running on the HP-UX 11i v3 operating system

Identifier	Description
Defects Fixed in Sendmail 8.15.2 (C.8.15.2.1)	
QXCR1001453731	Upgrade/Re-install or <code>gen_cf -f</code> incorrectly assigns <code>group bin</code> to <code>aliases.db</code> .
QXCR1001490035	Vulnerability CVE-2014-3956 in Sendmail C.8.13.3.5 for HP-UX.
Defect Fixed in Sendmail 8.15.2 (C.8.15.2.3)	
QXCR1001520862	Sendmail C.8.15.2.1 does not start the sendmail service during installation.

Source code availability

The source code for HP-UX Sendmail 8.15.2 and dependencies can be downloaded from this location: <https://hpe.com/software/opensource> (Open Source Software > Software Products > Operating Systems).