

Sendmail 8.11.1 Release Notes

HP-UX 11.0 and 11i v1



Manufacturing Part Number: 5991-5503

May 2006

U.S.A.

© Copyright 2006 Hewlett-Packard Development Company L.P.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

U.S. Government License

Proprietary computer software. Valid license from HP 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.

Copyright Notice

Copyright © 2006 Hewlett-Packard Development Company L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Trademark Notices

UNIX is a registered trademark of The Open Group.

1. New and Changed Features

New Features	7
Changed Features	24
Removed Features	25

2. Installation Information

Compatibility with Previous Versions	28
System Requirements	29
Installing Sendmail 8.11.1	30

3. Documentation

Sendmail Information	34
----------------------------	----

4. Known Problems, Limitations, and Fixes

Known Problems and Workarounds	36
Limitations	38
Defects Closed in Sendmail 8.11.1	39

Contents

1 New and Changed Features

Sendmail 8.11.1 is available on HP-UX 11.0 and 11i platforms as a web upgrade. This version offers various new features and enhancements that enable your mail system to handle high volumes of mail with ease. It also offers new anti-spamming features, which provide granular and

finer control over existing functions implemented by Sendmail and other agents. This version of Sendmail is a dual stack implementation of IPv4 and IPv6.

IMPORTANT

Read the “Known Problems” section on page 30, before installing Sendmail 8.11.1.

New Features

The following new features have been added in Sendmail 8.11.1:

IMPORTANT

The entries in the `sendmail.cf` file preceded by a '#' (hash) are commented by default.

- Multiple Queue Directories

This feature facilitates the parallel processing of mail by spreading process loads across multiple disks, thereby improving queue performance, which is impacted by the number of entries in the queue directories. Unix files take a long time to open when number of entries in the directories exceed 1000.

NOTE

In order to use multiple directories, the `QueueDirectory` option in the `sendmail.cf` file needs to be supplied with a value ending with `*`.

For example, in the configuration file, if you specify:

```
O QueueDirectory=/var/spool/mqueue/g*
```

All the directories or links to directories that begin with 'g' will be used. If there are five directories, g1, g2, g3, g4, and g5, Sendmail will use all the five directories when the Sendmail daemon is restarted. The mails are randomly assigned to the queue directories. The queue directory structure should not be changed when Sendmail is running.

Individual flushing of the mail queues can also be done by specifying the following in command line:

```
sendmail -q -O QueueDirectory=/var/spool/mqueue/g1  
sendmail -q -O QueueDirectory=/var/spool/mqueue/g3
```

A new queue file naming system is also introduced in this release. The algorithm used to name files ensures that the names will be unique for 60 years. The queued items can be moved between queues with ease.

- Enhanced Status codes as defined by RFC 2034

This feature provides an official SMTP extension to deliver the Enhanced Mail System Codes for messages. These system codes have been derived from RFC 1893. In the earlier versions of Sendmail, messages during SMTP sessions were represented in 3-digit numeric codes like "550 Host Unknown", "220 Service Ready" etc.

The new system builds on existing 3-digit codes with three parts, each separated by a dot. For example, "2.1.1" or "5.1.2", where the first digit denotes whether the response was good, bad or incomplete, the second digit denotes the type of error (e.g., mail system error, command syntax error), and the third digit denotes supplementary information, if any.

The following are the three classes of return status:

a) 2.X.X

Success

The message was delivered.

b) 4.X.X

Persistent Transient Failure

Some temporary event (perhaps a full disk drive) could have caused the mail transfer to fail, but sending the same message in the future may be successful.

c) 5.X.X

Permanent Failure

This message cannot be delivered. The headers of the message or format could be wrong.

RFC 1893 specifies an explicit set of values for the second and third digits (or groups of digits) of the returned status as well. "4.3.1" would mean the server temporarily rejected the message because its disks are full. "5.7.2" means the mail was bounced because it was sent to a list that the sender is not authorized to send the mail.

- DaemonPortOptions

This option can be used to customize the daemon's SMTP service. The default value for the field 'Family' is 'inet' even if DaemonPortOptions is not defined or value for the 'Family' is not specified in the DaemonPortOptions setup.

By default, the `DaemonPortOptions` appears in the `sendmail.cf` file as:

- O `DaemonPortOptions=Name=MTA, Family=inet`
- O `DaemonPortOptions=Port=587, Name=MSA, M=E`

NOTE

For more information on MSA, refer to “Spam Control using Message Submission Agent” section below.

The fields currently supported by Sendmail for `DaemonPortOptions` are:

1. `Family` = `inet`, `inet6`
2. `Address` = IP address or hostname
3. `Port` = Port number/name
4. `Listen` = Listen queue size
5. `M(Modifiers - Flags)` = The flags are listed below:

- a - necessitate authentication
- b - bind to interface through which mail has been received
- c - perform hostname canonification on the message
- f - necessitate fully qualified hostname
- h - use the interface name for the outgoing HELO command
- C - do not perform hostname canonification on the message
- E - do not allow ETRN
- u - disable fully qualified address for From: address

6. `SendBufSize` = Send buffer size
7. `RcvBufSize` = Receive buffer size
8. `Name` = Name of the agent(MTA or MSA)

The default value in the `sendmail.cf` file is: `M=E` for MSA.

- `ClientPortOptions`

This option is similar to the `DaemonPortOptions` but is meant only for outgoing connections.

The steps to set this option are same as those for the `DaemonPortOptions` except that the option name `ClientPortOptions` should be specified instead of `DaemonPortOptions`.

By default, it appears in the `sendmail.cf` file as:

```
#0 ClientPortOptions=Address=0.0.0.0
```

- **IPv6 Support**

A new option value ‘inet6’ for the field “Family” in `DaemonPortOptions` to enable IPv6 functionality has been added.

To enable IPv6, set the `DaemonPortOptions` in the `sendmail.cf` configuration file as:

```
O DaemonPortOptions=Port=smtp, Name=MTA, Family=inet6
```

```
O DaemonPortOptions=Port=587, Name=MTA, M=E, Family=inet6
```

This will accept both IPv4 and IPv6 addresses.

- **Spam Control using Message Submission Agent (RFC 2476)**

Message Submission Protocol is a means for MUAs to introduce new messages into the message transfer agent routing network. Messages being submitted by MUAs, in some cases, may be unfinished. Unfinished messages need to be completed by the MSA before submitting to the MTA. It also helps in implementing authenticated submission, including off-site submission by authorized users such as travellers.

The messages received on port 587 are regarded as "submitted messages". MSAs may implement message rejection rules, i.e. if an MSA is unable to determine a return path for the submitting user, from a valid MAIL FROM, a valid source IP address, or based on authenticated identity, then the MSA will immediately reject the message, as it gives the user and MUA direct feedback.

Sendmail 8.11.1 supports RFC 2476, a protocol for message submission. The anti-spam rulesets have been enhanced to improve the anti-spam capabilities. The RFC proposes a new standard for the Message Submission Agent (MSA). This is designed to replace the more general-purpose mail transfer agent (MTA) as the first service to which a Mail User Agent (MUA) connects to deliver a mail message. The RFC also describes how the usual protocols for SMTP service should be tightened up at the point where mail enters the

system, rather than being routed from one site to another. Sendmail 8.11.1 also serves as a powerful tool to authenticate and control mail messages.

By default, MSA is defined in the `sendmail.cf` file as:

```
O DaemonPortOptions=Name=MSA, Port=587, M=E
```

where Port 587 is reserved for email message submission.

A Message Submission Agent still uses all of the same rulesets for processing the message (and therefore still allows message rejection via the `check_*` rulesets). In accordance with the RFC, the MSA will ensure that all domains in the envelope are fully qualified if the message is relayed to another MTA. It will also enforce the normal address syntax rules and log error messages. In addition to the above, you can request authentication before the messages are accepted by MSA by using the `M=a` modifier in the `DaemonPortOptions`.

NOTE

MSA can be turned off in the `sendmail.cf` file using the option, `'no_default_msa'` in `gen_cf`. For more information, refer to “`no_default_msa`” option below.

The `XUSR SMTP` command as well as the `'-U'` (initial user submission) command line option are deprecated. Mail user agents are expected to start using MSA for initial user message submission from now onwards. XUSR may be removed in future releases. The next release of sendmail will assume that any message submitted from the command line is an initial user submission and act accordingly.

- **Generating the Configuration File**

`gen_cf` is a UNIX shell script, which is installed in the directory `'/usr/newconfig/etc/mail/cf/cf'`. This script cannot be copied to a different directory and executed, as it uses the macros defined in the `'/usr/newconfig/etc/mail/cf'` directory to generate `sendmail.cf` file.

This script provides many options that will enable a specific ruleset. The input file for this script will be the `*.m4` files defined in the `/usr/newconfig/etc/mail/cf` directory. The user can specify the output file and later incorporate site-specific changes (if any) in the output file.

NOTE

The output file generated by `gen_cf`, `sendmail.cf.gen` can be later copied or moved to `/etc/mail/sendmail.cf` file.

In addition to the options provided in Sendmail 8.9.3 release, the following new options have been added in the `gen_cf` script:

1. `dnsbl`

This new DNS-based black list option replaces ‘`rbl`’, the RealtimeBlackhole List feature that was included in Sendmail 8.9.3 release. The `rbl` option is deprecated now. `dnsbl` option avoids the possible confusion between RealtimeBlackhole List and other DNS-based Blacklist servers like ORBS. It takes the name of the Blacklist server and also an optional rejection message as arguments.

`dnsbl` can be included multiple times in the `sendmail.cf` file, thereby allowing sites to subscribe to multiple Blacklist servers. The Blacklist server verifies the IP address of the incoming connection and rejects all the SMTP commands if the address is blacklisted. An error message is also displayed.

2. `delay_checks`

This option delays the anti-spam checks by Sendmail until it issues the SMTP RCPT command. Mails from certain addresses that might have been blocked by other anti-spam checks are received. In these cases, deferred checks are not done.

By using `delay_checks`, the rulesets `check_mail` and `check_relay` will not be called when a client connects or issues a MAIL command, respectively. Instead, those rulesets will be called by the `check_rcpt` ruleset; they will be skipped if a sender has been authenticated using a "trusted" mechanism, i.e. one that is defined via the list of AuthMechanisms. If `check_mail` returns an error, the RCPT TO command will be rejected with that error. If it returns some other result starting with `$#`, then `check_relay` will be skipped. If the sender address (or a part of it) is listed in the access map and it has a RHS of OK or RELAY, then `check_relay` will be skipped.

3. `relay_mail_from`

This option can be used to facilitate relaying through a user's machine. The sender's name, which is listed as "RELAY" in the access map (tagged with From:) can be specified using this option. The domain portion of the mail sender is also checked, when the optional argument 'domain' is provided.

4. ldap_routing

This option can be used to implement the ldap-based email recipient routing. This provides a method for re-routing addresses with a domain portion in class {LdapRoute} to either a different mail host or to a different address.

NOTE

For more information, refer to "LDAP-based Routing" section.

5. no_default_msa

This option can be used to generate the configuration file without 'DaemonPortOptions' option for Message Submission Agent (MSA) daemon. The `sendmail.cf` configuration file will not contain the following line:

```
O DaemonPortOptions=Port=587, Name=MSA, M=E
```

6. receive_only

This option generates a `sendmail.cf` file with a new set of rules called 'check_compat'. You can only receive mail messages, but cannot send them. Two new flags have been added in `/etc/rc.config.d/mailservs` file. They are:

a. SENDMAIL_RECVONLY

This flag must be set to '1' in order to use "receive_only" feature.

b. SENDMAIL_SENDOONLY

This flag may not be set to any value.

NOTE

Sendmail 8.11.1 depot will install the `mailservs` file will be in `/usr/newconfig/etc/rc.config.d`. You need to manually move this file to `/etc/rc.config.d/` in order to use this feature.

The priorities for these flags are defined in the
/usr/newconfig/etc/rc.config.d/mailservs file.

7. send_only

This option generates a sendmail.cf file without the
'check_compat' ruleset. You can only send mail messages, but
cannot receive them.

The SENDMAIL_SENDOONLY flag in
/etc/rc.config.d/mailservs file must be set to '1' in order to
use 'send_only' feature.

- SMTP Authentication based on RFC 2554

This version of Sendmail supports SMTP AUTH as defined in RFC
2554 (SMTP Service Extension for Authentication), which is based
on SASL (Simple Authentication and Security Layer - RFC 2222).
SMTP authentication provides a robust tool to control relaying with
maximum flexibility.

The authentication protocol exchange consists of a series of server
challenges (otherwise known as a ready response) and client answers
that are specific to the authentication mechanism.

The AUTH parameter to the MAIL FROM command is set as:

```
MAIL FROM: from-addr AUTH=addr-spec
```

The addr-spec contains the identity that submitted the message to
the delivery system. If the server trusts the authenticated identity of
the client to assert that the message was originally submitted by the
supplied addr-spec, then the server must supply the same addr-spec
in an AUTH parameter when relaying the message to any server
that supports the AUTH extension.

The list of authentication mechanisms for AUTH can be specified in
the option, AuthMechanisms in the sendmail.cf file. By default, it
appears in the sendmail.cf file as:

```
#O AuthMechanisms=GSSAPI KERBEROS_V4 DIGEST-MD5 CRAM-MD5
```

A new option to set AUTH parameter in MAIL FROM command has
been added in the sendmail.cf file. By default, this appears as:

```
#O AuthOptions
```

If this option is set to 'A', the AUTH= parameter for the MAIL FROM command will be issued only when authentication succeeds.

DaemonPortOptions has one sub-option called 'modifiers' (M), one of which is 'a'. This instructs the daemon to necessitate authentication for all connections to it.

By default, it appears in the sendmail.cf file as:

```
#O DefaultAuthInfo=/etc/mail/default-auth-info
```

The DefaultAuthInfo option sets the filename which contains the authentication information for outgoing connections by default. It must contain the authorization id (userid), the authentication id (authid), the password (plain text), and the realm to use, each on a separate line. This information must be readable only by root (or the trusted user). If no realm is specified, \$j will be used.

- Virtual Hosting

This version of Sendmail imposes better control over virtusertable, which provides a domain-specific form of aliasing and also allows multiple domains to be hosted on a single machine.

With this feature, users can have their own domain names and receive mails using these domain names with a single host. You are required to obtain a new (available) domain name and set up name servers for that domain. Then, you must configure MX records for your new domain.

NOTE

You must know how to setup DNS before implementing this feature. For information on setting up DNS, refer to "Installing and Administering Internet Services" manual, posted on <http://docs.hp.com>.

The following steps describe how to set up virtual hosting:

1. Assume 'mydomain.com' as the new domain name. If the mail server which serves the new domain name has a full time connection to the internet, include the following line in the db.domain file.

```
mydomain.com. IN MX 10 mymailserver.mydomain.com.
```

Otherwise, you will need to have another machine to queue mails for your domain. Include the following lines in the db.domain file:

```
mydomain.com. IN MX 10 mymailserver.mydomain.com.  
mydomain.com. IN MX 20  
othermailserver.otherdomain.com.
```

Now, you must setup Sendmail.

The generic-hpux10.mc file in /usr/newconfig/etc/mail/cf/cf/generic.mc is used for generating the configuration file. In the generic-hpux10.mc file, the version id string and the DOMAIN () flag can be modified to contain 'mydomain.com'.

2. Create a file mydomain.com.m4 in /usr/newconfig/etc/mail/cf/domain/ directory. This file must be similar to the /usr/newconfig/etc/mail/cf/domain/generic.m4 file, with the version id containing 'mydomain.com'.
3. Generate the sendmail.cf.gen file using gen_cf utility with 'virtusertable' option and move this file to /etc/mail/sendmail.cf.

NOTE

For more information on gen_cf, read the "Generating the Configuration File" section above.

4. Create the virtusertable in /etc/mail directory. A sample virtusertable may look like:

```
joe@mydomain.com      jschmoe  
jane@mydomain.com      jdoe@othercompany.com  
@mydomain.com          jschmoe
```

In the first example, the address joe@mydomain.com will be mapped to the local user jschmoe, jane@mydomain.com to the remote user jdoe@othercompany.com, and any other address in mydomain.com will also be mapped to jschmoe.

5. Build the virtusertable database file in the command line as follows:


```
# makemap dbm /etc/mail/virtusertable <  
/etc/mail/virtusertable
```

If you wish to reverse-map local users for out-bound mail, you will need to generate `sendmail.cf` file with ‘genericstable’ option in addition to ‘virtusertable’ option.

You must generate the genericstable similar to the virtusertable, but with the entries reversed.

Example:

```
jschmoe                                joe@yourdomain.com
```

6. Add your domain name to `/etc/mail/sendmail.cw` file.

7. Kill and Restart Sendmail.

Now you should be able to receive mails at `mydomain.com`.

IMPORTANT

‘Virtual Hosting’ feature provides better support for ISPs that offer queueing services to dial-up customers as queue-runs no longer wait for the dial-up server connection attempts to time out.

- **LDAP-based Routing**

This feature can be used to implement the LDAP-based re-routing. This provides a method to re-route addresses with a domain portion in class {LDAPRoute} to either a different mail host or a different address. The domains can be added to the class {LDAPRoute} as given in the examples below.

Ensure that you setup a domain for LDAP routing. Assume that your domain is “`yyy.com`”. Add the following line in the `sendmail.cf` file:

```
C{LDAPRoute}yyy.com
```

or

```
F{LDAPRoute}/etc/mail/ldap-domain-file
```

where `/etc/mail/ldap-domain-file` contains the domains.

The LDAPDefaultSpec option in the `sendmail.cf` file sets the default LDAP map specification. This needs to be set before defining LDAP maps. The settings will be used for all LDAP maps unless they are specified in the individual map specification ('K' command). By default, it appears in `sendmail.cf` file as follows:

```
O LDAPDefaultSpec=-h localhost
```

`localhost` can be replaced by your LDAP server name.

The following are the switches commonly used by most applications:

1. 'b' - ldap search base

"Directory" in ldap "tree" where the search begins. For example,

```
-b "o=hp.com"
```

2. 'd' - bindDN

The BindDN parameter is used to specify the DN value for the LDAP bind request. For example,

```
-d"cn=ldap://:389,dc=edat104,dc=atl,dc=hp,dc=com"
```

3. 'h' - ldap servers

Space separated string of servers which support ldap at your site. For example,

```
-h "ldap1.hp.com ldap2.hp.com"
```

4. 'p' - port numbers

Port numbers where ldap service is available. For example,

```
-p 33333
```

5. 'k' - ldap search string (key)

String that defines how a ldap map takes its input value and initiates an ldap search. For example,

```
-k (&(ObjectClass=mailrecipient) (mail=%0))
```

6. 'v' - ldap attribute

Value that replaces the origin string in the map. In most cases, this will be the rfc822 email address. For example,

```
-v mailroutingaddress
```

The ldap maps are defined in the configuration file as:

```
Kldap -l -v mailHost -k  
(&(objectClass=inetLocalMailRecipient)  
(mailLocalAddress=%0))  
  
Kldapmra ldap -l -v mailRoutingAddress -k  
(&(objectClass=inetLocalMailRecipient)  
(mailLocalAddress=%0))
```

where

mailLocalAddress is the RFC 822 compliant email address of the recipient,

mailHost is the fully-qualified host name of the MTA that is the final SMTP destination of the message to the recipient,

and, mailRoutingAddress is the RFC 822 address to be used when routing messages to the SMTP MTA of the recipient.

- New Option Value for QueueSortOrder - Filename

This new option value alleviates your task of sorting the queue by opening each queue file to get the host and time information. The queue files need not be opened and read each time, when they are run. As a result, the queue processing becomes faster.

This option can be set in the sendmail.cf file as:

```
O QueueSortOrder=Filename
```

- New Option Value for Privacy Options - nobodyreturn

This new option value instructs Sendmail to ignore the body of the original message, when notifying the delivery status of the message.

This option can be set in the sendmail.cf file as:

```
O PrivacyOptions=nobodyreturn
```

- Configuration Options

The following are the new or enhanced configuration options available in Sendmail 8.11.1:

1. Timeout.*

- a. The total time spent in satisfying a socket control request can be set using the 'Timeout.control' option. The default setting for this option is:

```
#O Timeout.control=2m
```

- b. The resolver's transmission time interval (in seconds) can be set using the 'Timeout.resolver.retrans' option. This option sets the 'Timeout.resolver.retrans.first', which sets the resolver's transmission time interval (in seconds) for the first attempt to deliver a message. It also sets the 'Timeout.resolver.retrans.normal' option. The default setting for this option is:

```
#O Timeout.resolver.retrans=5s
```

```
#O Timeout.resolver.retrans.first=5s
```

```
#O Timeout.resolver.retrans.normal=5s
```

- c. The frequency of resolver query retransmission can be set using the 'Timeout.resolver.retrans.normal' option. This option sets the 'Timeout.resolver.retry.first' option for the first attempt to deliver a message. It also sets the 'Timeout.resolver.retry.normal' option for all resolver lookups except for the first delivery attempt. The default setting for this option is:

```
#O Timeout.resolver.retry=4
```

```
#O Timeout.resolver.retry.first=4
```

```
#O Timeout.resolver.retry.normal=4
```

2. DataFileBufferSize

This option can be used to control the maximum size of a memory-buffered data (df) file before a disk-based file is used. The default setting for this option is:

```
#O DataFileBufferSize=4096
```

3. XscriptFileBufferSize

This option can be used to control the maximum size of a memory-buffered (xf) transcript before a disk-based file is used. The default setting for this option is:

```
#O XscriptFileBufferSize=4096
```

4. MaxAliasRecursion

The maximum depth of an alias recursion can be specified in the `sendmail.cf` file using this option. The default setting for this option is:

```
#O MaxAliasRecursion=10
```

5. PidFile

The location of the ProcessId (Pid) file can be defined using this option. The default setting for this option is:

```
#O PidFile=/etc/mail/sendmail.pid
```

`/etc/mail/sendmail.pid` will be taken as the default file, if this option is not set. If you choose a directory other than `/etc/mail` for the pidfile, please ensure that the directory has proper write permissions as those of `/etc/mail`.

6. ProcessTitlePrefix

The prefix string for the process title shown in ‘ps’ listings can be specified using this option. By default, this option is commented. For example, if you set this option in the `sendmail.cf` file as:

```
#O ProcessTitlePrefix=HPUX_Sendmail-8.11.1
```

The command ‘`ps -ef | grep sendmail | grep -v grep`’ might show ‘`sendmail: HPUX_Sendmail-8.11.1: accepting connections`’ in the output.

7. TrustedUser

This option can be used to specify a user, who can own important files instead of root. This option necessitates ‘`fchown`’. The default setting for this option is:

```
#O TrustedUser=root
```

8. MaxMimeHeaderLength

The size of the MIME headers and parameters within those headers can be set using this option. This can also be used to protect Mail User Agents (MUA) from buffer overflow attacks. The default setting for this option is:

```
#O MaxMimeHeaderLength=10
```

9. DeadLetterDrop

This option can be used to specify the location of the system-wide dead.letter file, which was formerly hardcoded to /var/tmp/dead.letter. The default setting for this option in this version is:

```
O DeadLetterDrop=/var/tmp/dead.letter
```

Please note that Sendmail will not save mails anywhere if this option is not set at all.

- **Command Line Options**

The following are the new or enhanced command line options available in Sendmail 8.11.1:

1. **-G**

This option indicates that the message being submitted by the command line is meant only for relaying and not for gateway submission. This implies that the message will be rejected if the addresses are not fully qualified and canonification will not be performed on the message.

NOTE

Mail User Agents (MUA) begin with "-G" to indicate that the message submission is relayed.

2. **-L**

This option can be used to set the identifier in syslog messages to a supplied tag.

Example:

```
/usr/sbin/sendmail -bd -L HP-Sendmail-8.11.1
```

HP-Sendmail-8.11.1 line is added to all the lines in /var/adm/syslog/mail.log file.

3. **-C**

This option in "praliases" can be used to specify an alternate sendmail configuration file used for finding the alias file.

4. **-p** (for 'mailstats')

This command can be used to print the output information in program-readable mode and reset the statistics file.

5. Three new options are added in "makemap". They are:
 - a. "-C" to accept an alternate sendmail configuration file used to find the 'TrustedUser' option.
 - b. "-u" to dump (unmap) a database.
 - c. "-e" to allow empty values.

NOTE

For information on makemap, refer to makemap (1m) manual page.

- Other Features

In addition to the above, Sendmail 8.11.1 offers the following features:

1. Finer spam control by using tags for the LHS of the access map

You can now tag entries in the access map based on their type. Three tags are available. They are:

- a. Connect: connection information (\${client_addr}, \${client_name})
- b. From: sender
- c. To: recipient

If the required item is looked up in a map, it will be tried with the corresponding tag in front, then without any tag (as fallback to enable backward compatibility). For example,

```
From: spammer@some.dom    REJECT
To: friend.domain         RELAY
Connect: friend.domain    OK
Connect.from.domain       RELAY
From: good@another.dom    OK
From: another.dom         REJECT
```

Changed Features

The following changes have been made in version 8.11.1 of Sendmail:

- The error code returned for unrecognized parameters to the SMTP mail and RCPT commands is changed from 501 to 555 as per RFC 1869.
- The configuration file (`sendmail.cf`) version number is incremented to 9.
- Aliases with no right hand side are provided with ‘missing value’ warnings, when ‘newaliases’ is run instead of making an attempt to deliver the mail messages to an alias.
- A new mailer flag, ‘F=%’ is included in this release. Mailers, which have this flag will not attempt to deliver the message to the initial recipient. Those mails will be queued up. The queued messages are selected using one of the -qI/-qR/-qS queue run modifiers or an ETRN request and then delivered to the recipient.
- The [hostname] is added to class ‘w’ for the names of all interfaces unless DontProbeInterfaces option is set. This is useful for sending mails to hosts, which have dynamically assigned names.
- All numbered rulesets have been named in this release. They can still be accessed by their numbers. For example, Scanonify=3 instead of S3; SRecurse =97 instead of S97.
- A ‘/Quit’ command to address the test mode is added. This command can be used to exit from the address test mode.
- The SMTP commands are not processed when the SMTP connection drops. This prevents a remote system from flooding the connection with commands and also disconnecting. In the earlier releases, all buffered commands were processed by the server.
- Purgestat and sendmail ‘-bH’ options delete only expired files in the host status database, which have exceeded the values set by Timeout.hoststatus.
- Terminating and restarting the sendmail daemon may not be instantaneous.

Removed Features

There are no removed features in this release of Sendmail.

New and Changed Features

Removed Features

2 **Installation Information**

Read this chapter before installing version 8.11.1 of Sendmail.

Compatibility with Previous Versions

Customers currently using any 8.x version of Sendmail do not need to modify their configuration file. It is compatible with this release of Sendmail. However, it is highly recommended to use the Sendmail 8.11.1 configuration file (.cf) version9 delivered with this release in order to effectively use the new features and changes incorporated in this version.

System Requirements

To install Sendmail 8.11.1, you must have the following system components:

- Hewlett-Packard 9000 Computer
- HP-UX operating system Version 11.0 or 11i.

Installing Sendmail 8.11.1

The pre-installation requirements for Sendmail 8.11.1 are same as those for Sendmail 8.9.3. This release of Sendmail is available as a web upgrade on HP-UX 11.x platform. The web upgrade depot will be posted on www.software.hp.com from where you can download the installable version.

NOTE

The IPv6-enabled version of Sendmail 8.11.1 is compatible only with 11i platform.

You need to run the following command to install Sendmail 8.11.1:

```
swinstall -s "<destination path>"
```

where <destination path> is the absolute path where you downloaded the Sendmail web upgrade depot.

The web upgrade version of Sendmail 8.11.1 is now available for use.

Please note that Sendmail 8.9.3, delivered as a part of HP-UX 11.x is also installed on the system.

"enable_inet sendmail" is the command used to enable the Sendmail web upgrade that you installed on your system as specified above. The Sendmail 8.11.1 web upgrade depot takes care of the enabling process automatically.

Upon installation of this depot, it is strongly recommended that administrators run the following commands:

- /usr/sbin/newaliases
- /usr/sbin/mailstats (if the mail statistics file is already existing)

If administrators choose to collect the mail statistics in future, mailstats needs to be run immediately after creating the mail statistics file.

The administrators are recommended to take necessary action based on the notification messages.

NOTE

If you want to install a patch or revert back to the previous version, you need to disable Sendmail 8.11.1 by running the command `"/usr/bin/enable_inet -r sendmail"` in the command line to revert back to Sendmail 8.9.3.

Please note that you will not be able to use the new options incorporated in this release, if you wish to revert back to Sendmail 8.9.3.

When you upgrade a HP-UX 11.0 operating system containing Sendmail 8.11.1 webupgrade to a HP-UX 11i operating system, Sendmail 8.11.1 is overwritten with Sendmail 8.9.3 which is the version available with the 11i core operating system. Now, if you want to obtain the latest version of Sendmail, you must install Sendmail 8.11.1 webupgrade on the HP-UX 11i operating system.

3 Documentation

The following product documentation is available for Sendmail 8.11.1:

Sendmail Information

Sendmail 8.11.1 documentation is available through its man pages. Table 3-1 lists and describes the man pages distributed with Sendmail 8.11.1.

Table 3-1 **Man Pages**

Man Page	Description
killsm.1m	Kills the sendmail daemon.
mailq.1	Prints a summary of the mail messages queued for future delivery.
mailstats.1	Prints mail traffic statistics.
makemap.1m	Creates the database maps for sendmail.
praliases.1	Prints system-wide sendmail aliases.
sendmail.1m	Sends a message to one or more recipients or addresses, routing the message through necessary networks.

The following RFCs have been implemented in Sendmail 8.11.1:

- RFC 821
- RFC 822
- RFC 2821
- RFC 2033
- RFC 2034
- RFC 2222
- RFC 2476
- RFC 2487
- RFC 2505
- RFC 2553
- RFC 2554

4 Known Problems, Limitations, and Fixes

This chapter discusses the known problems, workarounds, fixes, and defects closed in this release of Sendmail.

Known Problems and Workarounds

The following are the known problems in this release of Sendmail:

- Sendmail uses `identd`, an optional authentication tool to find the user id for a given connection established with a remote machine. `identd` invokes some kernel services which hold the system resources for a long time. This affects the performance of Sendmail when there are large number of active TCP connections. The system appears hung during this timeframe.

In order to resolve this problem, do the following:

1. Disable `identd` by modifying the following entry in the `sendmail.cf` file:

```
#O Timeout.ident=5s
as
O Timeout.ident=0s
```

Now you need to kill and restart Sendmail.

2. To disable `identd`, perform the following steps:
 - a. Edit the `/etc/inetd.conf` file and comment out the `ident` line by placing a `#` in the first column as follows:

```
#ident stream tcp wait bin /usr/sbin/identd identd
```
 - b. Force `inetd` to re-read the `inetd.conf` file by executing `'/usr/sbin/inetd -c'` in the command line.

NOTE

`identd` is not distributed with this release of Sendmail. However if the system already contains an `identd`, you may encounter the above problem.

-
- If you specify a new location/file for the `PidFile` option in the `sendmail.cf` file and try killing Sendmail, the new file which does not contain any entries will be read by Sendmail instead of the default one. Therefore, Sendmail will not be killed. When you try restarting Sendmail, an error message is displayed.

In order to resolve this problem, kill Sendmail before changing the PidFile option in the sendmail.cf file. You can then start Sendmail after making the changes in the sendmail.cf file. By doing this, the Pids will be written to the new file.

- Sendmail used to add other user's address in "Diagnostic-code" in warning messages under abnormal conditions, when the server connections are reset in the data phase. The email queue warning is returned to the sender with the Diagnostic-Code including an incorrect address.

A workaround for this problem has been provided with this release. In such cases, no address will be added in the Diagnostic-Code line in the warning messages.

Limitations

The following are the limitations and fixes in Sendmail 8.11.1:

- If the LDAP server is used to resolve aliases and the LDAP server happens to be a IPv6 server, Sendmail-8.11.1 will be unable to use LDAP. However it will work if the LDAP server is IPv4.
- In order to use both IPv4 and IPv6 features, a machine should have dual stack.
- `identd`, the tool used by Sendmail to authenticate and find the user id for a given connection established with a remote machine will be available in the future releases with appropriate defect fixes.
- The command used to revert back to the previous version of Sendmail (i.e., 8.9.3), `“/usr/sbin/enable_inet -r sendmail”` must not be executed in the directory `“/usr/contrib/sendmail/save_custom/”` or any of its sub-directories.

Defects Closed in Sendmail 8.11.1

Table 4-1 and Table 4-2 list and describe the defects fixed in Sendmail 8.11.1 for the following releases:

- HP-UX 11.0
 - Version 1 (B.11.00.01.001)
 - Version 2 (B.11.00.01.002)
 - Version 3 (B.11.00.01.003)
 - Version 4 (B.11.00.01.004)
 - Version 5 (B.11.00.01.005)
 - Version 8 (B.11.00.01.008)

NOTE

The Sendmail HP-UX 11.0 releases B.11.00.01.006 and B.11.00.01.007 were intermediate releases. You may not find these release names mentioned in any documentation available with B.11.00.01.008 because they did not provide a complete solution.

- HP-UX 11i
 - Version 1 (B.11.11.01.001)
 - Version 2 (B.11.11.01.002)
 - Version 3 (B.11.11.01.003)
 - Version 4 (B.11.11.01.004)
 - Version 5 (B.11.11.01.005)
 - Version 6 (B.11.11.01.006)

Table 4-1 Defect Fixes in HP-UX 11.0 and 11i

Defect #	Description
CR JAGaa30867	Site hiding for local delivery

Table 4-1 Defect Fixes in HP-UX 11.0 and 11i (Continued)

Defect #	Description
CR JAGaa31678	Sendmail 10.20 patch PHNE_11395 removes UUCP rule.
CR JAGaa30793	UUCP mails fails due to an MX record configuration problem
CR JAGaa30300	There is no X400/Openmail gateway functionality support in Sendmail 8.7 configuration file.
CR JAGaa27019	Sendmail 8.x does not support /etc/hosts.smtp files, Sendmail 5.6.5 does.
CR JAGaa31389	Support the old functionality of DL macro in Sendmail 8.8.6.
CR JAGaa30262	rev-alias file is not supported.
CR JAGaa31569	UUCP address includes to.uucp.relay and other unnecessary information at the end of the legitimate address.
CR JAGaa27057	UUCP problems with ISP because of \$: (user) delivery agent.
CR JAGab46861	Sendmail PHNE_10099 does not send mail relay with dns in nsswitch.con.
CR JAGaa31589	Sendmail 8.8.6 does not send mail to local domain only, but to relay.
CR JAGaa31401	Interoperability problem of Sendmail 8.8.6 with Openmail to be fixed.
CR JAGaa31152	Sendmail won't deliver mail file, wrongly thinks shell is bad.
CR JAGaa30335	Makemap does not add YP_LAST_MODIFIED and YP_MASTER_MAP into dbm database.
CR JAGaa73105	The relative shared library path in /usr/bin/chkey is incorrect.

Table 4-1 Defect Fixes in HP-UX 11.0 and 11i (Continued)

Defect #	Description
CR JAGad58227	NIS PLUS is not enabled in Sendmail 8.9.
CR JAGaa27122	Sendmail execution (<code>sendmail -b</code>) can take upto 20 minutes to execute.
CR JAGaa30304	Use HP-UX/SUN switch instead of <code>service.switch</code> .
CR JAGac07212	Sendmail leaves 0-byte file in <code>/var/tmp</code> .
CR JAGab13472	When sending mail and accidentally specifying a host that does not exist, the message will be deferred. The user will not find out about this for four hours.
CR JAGaa30185	Starting mail daemon has warning and system was forced to use short name.
CR JAGab15526	Errors seen after <code>boot: /sbin/rc</code> . Failed to read <code>row/col</code> in console.
CR JAGa31082	Sendmail 10.20 with PHNE_9624 has problems with DBM files.
CR JAGab46785	Sendmail cant send to Error-To: specified in the message if the unknown user is at a remote host.
CR JAGaa31466	ER: PHNE_10496 installation requires the <code>/etc/nsswitch.conf</code> file.
CR JAGaa27064	The <code>expand_alias</code> command failed to expand aliases for hosts that have MX records but not A or CNAME records.
CR JAGab13472	Message delivery deferred when a user specified a no-existent host.
CR JAGab11180	The subject field of a message having Japanese characters in it, garbled when the user tried sending the message using Sendmail.

Table 4-1 Defect Fixes in HP-UX 11.0 and 11i (Continued)

Defect #	Description
CR JAGad01838	Sendmail created a file of size 10MB in /var/tmp for every DB access. This affected the performance of Sendmail.
CR JAGac78493	Sendmail 8.9.3 exited when loaded heavily, without generating any error or core file.
CR JAGad00187	Sendmail failed to use /etc/hosts file for host lookup when DNS server was down.
CR JAGac68812	The usage of the -f option was wrongly documented in Sendmail manpage.
CR JAGac47219	The gen_cf script option I set the promiscuous relay wrongly in the configuration file generated by Sendmail.
CR JAGad96395	When a user enables or disables the web upgrade version of Sendmail, swverify on the sendmail patch shows error.
CR JAGae01215	gen_cf fails to include the TrustAuthMech class macro in the generated Sendmail configuration file.
CR JAGae31789	Sendmail does not log transient (name server timeout) error messages while processing the mail queue.
CR JAGae33040	Under certain conditions, Sendmail or its associated utilities may not operate properly.
CR JAGae48326	Under certain circumstances, Sendmail does not process the mail queue properly.
CR JAGae33308	Under certain conditions, Sendmail does not terminate/restart properly.
CR JAGae52734	In some cases, smrsh does not operate properly.

Table 4-1 Defect Fixes in HP-UX 11.0 and 11i (Continued)

Defect #	Description
CR JAGae52730	When name server times out, Sendmail retries instantly due to wrong interpretation of the retransmission timeout value.
CR JAGae56930	If you set the resolver retransmission timeout value to a value greater than 20 seconds in the sendmail configuration file, sendmail fails to resolve the client's hostname.
CR JAGae58098	In some cases, sendmail does parse mail headers properly.
CR JAGae67325	Sendmail does not parse the headers properly.
CR JAGae63329	In some cases, Sendmail allows illegal relaying.
CR JAGae77457	The webupgrade (11.00: Revision B.11.00.01.003, 11i: Revision B.11.11.01.004) contains incorrect manpages.
CR JAGae91741	In some circumstances, Sendmail does not parse headers properly.
CR JAGae92668	In some circumstances, Sendmail does not parse rulesets properly.
CR JAGae96186	In the Sendmail address test mode, creation of a class macro is not functioning properly.
CR JAGae96227	Sendmail is not operating properly in the address test mode.
CR JAGaf96078	Under certain circumstances, Sendmail does not handle timeouts properly.

Table 4-2 Defect Fixes Applicable Only to HP-UX 11i

Defect #	Description
CR JAGad47118	IPv6 changes for Sendmail 8.11.1 on HP-UX.
CR JAGae29033	In a non-IPv6 HP-UX 11i system, Sendmail-8.11 does not use the available MX record to resolve the domain name, if the "A" record is not configured.
CR JAGae63788	Sendmail logs the transient error messages to the terminal when sendmail is unable to resolve the address of the host using the name service.