NAME

postconf - Postfix configuration parameters

SYNOPSIS

postconf *parameter ...*

postconf -e "*parameter=value*" ...

DESCRIPTION

The Postfix main.cf configuration file specifies parameters that control the operation of the Postfix mail system. Typically the file contains only a small subset of all parameters; parameters not specified are left at their default values.

The general format of the main.cf file is as follows:

- Each logical line has the form "parameter = value". Whitespace around the "=" is ignored, as is whitespace at the end of a logical line.
- Empty lines and whitespace-only lines are ignored, as are lines whose first non-whitespace character is a '#'.
- A logical line starts with non-whitespace text. A line that starts with whitespace continues a logical line.
- A parameter value may refer to other parameters.
  - The expressions "$name" and "${name}" are recursively replaced with the value of the named parameter. An undefined parameter value is replaced with the empty value.
  - The expressions "${name?value}" and "${name?{value}}" are replaced with "value" when "$name" is non-empty. These forms are supported with Postfix versions >= 2.2 and >= 3.0, respectively.
  - The expressions "${name:value}" and "${name:{value}}" are replaced with "value" when "$name" is empty. These forms are supported with Postfix versions >= 2.2 and >= 3.0, respectively.
  - The expression "${name?{value1}:{value2}}" is replaced with "value1" when "$name" is non-empty, and with "value2" when "$name" is empty. The "{}" is required for "value1", optional for "value2". This form is supported with Postfix versions >= 3.0.
  - The first item inside "${...}" may be a logical expression of the form: "{value3} == {value4}". Besides the "==" (equality) operator Postfix supports "!=" (inequality), "<", "<=", ">=", and ">". The comparison is numerical when both operands are all digits, otherwise the comparison is lexicographical. These forms are supported with Postfix versions >= 3.0.
  - Each "value" is subject to recursive named parameter and logical expression evaluation, except where noted.
  - Whitespace before or after each "{value}" is ignored.
  - Specify "$$" to produce a single "$" character.
  - The legacy form "$(...)" is equivalent to the preferred form "${...}".
- When the same parameter is defined multiple times, only the last instance is remembered.
- Otherwise, the order of main.cf parameter definitions does not matter.

The remainder of this document is a description of all Postfix configuration parameters. Default values are shown after the parameter name in parentheses, and can be looked up with the "**postconf -d**" command.

Note: this is not an invitation to make changes to Postfix configuration parameters. Unnecessary changes can impair the operation of the mail system.

2bounce_notice_recipient (default: postmaster)
The recipient of undeliverable mail that cannot be returned to the sender. This feature is enabled with the notify_classes parameter.

access_map_defer_code (default: 450)
The numerical Postfix SMTP server response code for an **access(5)** map "defer" action, including "defer_if_permit" or "defer_if_reject". Prior to Postfix 2.6, the response is hard-coded as "450".

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.6 and later.

access_map_reject_code (default: 554)
The numerical Postfix SMTP server response code for an **access(5)** map "reject" action.

Do not change this unless you have a complete understanding of RFC 5321.

address_verify_cache_cleanup_interval (default: 12h)
The amount of time between **verify(8)** address verification database cleanup runs. This feature requires that the database supports the "delete" and "sequence" operators. Specify a zero interval to disable database cleanup.

After each database cleanup run, the **verify(8)** daemon logs the number of entries that were retained and dropped. A cleanup run is logged as "partial" when the daemon terminates early after "**postfix reload**", "**postfix stop**", or no requests for $max_idle seconds.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.7.

address_verify_default_transport (default: $default_transport)
Overrides the default_transport parameter setting for address verification probes.

This feature is available in Postfix 2.1 and later.

address_verify_local_transport (default: $local_transport)
Overrides the local_transport parameter setting for address verification probes.

This feature is available in Postfix 2.1 and later.

address_verify_map (default: see postconf −d output)
Lookup table for persistent address verification status storage. The table is maintained by the **verify(8)** service, and is opened before the process releases privileges.

The lookup table is persistent by default (Postfix 2.7 and later). Specify an empty table name to keep the information in volatile memory which is lost after "**postfix reload**" or "**postfix stop**". This is the default with Postfix version 2.6 and earlier.

Specify a location in a file system that will not fill up. If the database becomes corrupted, the world comes to an end. To recover delete (NOT: truncate) the file and do "**postfix reload**".

Postfix daemon processes do not use root privileges when opening this file (Postfix 2.5 and later). The file must therefore be stored under a Postfix-owned directory such as the data_directory. As a migration aid, an attempt to open the file under a non-Postfix directory is redirected to the Postfix-owned data_directory, and a warning is logged.

Examples:

```
address_verify_map = hash:/var/lib/postfix/verify
address_verify_map = btree:/var/lib/postfix/verify
```

This feature is available in Postfix 2.1 and later.

address_verify_negative_cache (default: yes)
Enable caching of failed address verification probe results. When this feature is enabled, the cache may pollute quickly with garbage. When this feature is disabled, Postfix will generate an address probe for every lookup.

This feature is available in Postfix 2.1 and later.

address_verify_negative_expire_time (default: 3d)
The time after which a failed probe expires from the address verification cache.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.1 and later.

address_verify_negative_refresh_time (default: 3h)
The time after which a failed address verification probe needs to be refreshed.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.1 and later.

address_verify_pending_request_limit (default: see postconf −d output)
A safety limit that prevents address verification requests from overwhelming the Postfix queue. By default, the number of pending requests is limited to 1/4 of the active queue maximum size (qmgr_message_active_limit). The queue manager enforces the limit by tempfailing requests that exceed the limit. This affects only unknown addresses and inactive addresses that have expired, because the **verify(8)** daemon automatically refreshes an active address before it expires.

This feature is available in Postfix 3.1 and later.

address_verify_poll_count (default: normal: 3, overload: 1)
How many times to query the **verify(8)** service for the completion of an address verification request in progress.

By default, the Postfix SMTP server polls the **verify(8)** service up to three times under non-overload conditions, and only once when under overload. With Postfix version 2.5 and earlier, the SMTP server always polls the **verify(8)** service up to three times by default.

Specify 1 to implement a crude form of greylisting, that is, always defer the first delivery request for a new address.

Examples:

```
# Postfix <= 2.6 default
address_verify_poll_count = 3
# Poor man's greylisting
address_verify_poll_count = 1
```

This feature is available in Postfix 2.1 and later.

address_verify_poll_delay (default: 3s)
The delay between queries for the completion of an address verification request in progress.

The default polling delay is 3 seconds.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.1 and later.

address_verify_positive_expire_time (default: 31d)
The time after which a successful probe expires from the address verification cache.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.1 and later.

address_verify_positive_refresh_time (default: 7d)
The time after which a successful address verification probe needs to be refreshed. The address verification status is not updated when the probe fails (optimistic caching).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.1 and later.

address_verify_relay_transport (default: $relay_transport)
Overrides the relay_transport parameter setting for address verification probes.

This feature is available in Postfix 2.1 and later.

address_verify_relayhost (default: $relayhost)
Overrides the relayhost parameter setting for address verification probes. This information can be overruled with the **transport(5)** table.

This feature is available in Postfix 2.1 and later.

address_verify_sender (default: $double_bounce_sender)
The sender address to use in address verification probes; prior to Postfix 2.5 the default was "postmaster". To avoid problems with address probes that are sent in response to address probes, the Postfix SMTP server excludes the probe sender address from all SMTPD access blocks.

Specify an empty value (address_verify_sender =) or <> if you want to use the null sender address. Beware, some sites reject mail from <>, even though RFCs require that such addresses be accepted.

Examples:

```
address_verify_sender = <>
address_verify_sender = postmaster@my.domain
```

This feature is available in Postfix 2.1 and later.

address_verify_sender_dependent_default_transport_maps (default: $sender_dependent_default_transport_maps)
Overrides the sender_dependent_default_transport_maps parameter setting for address verification probes.

This feature is available in Postfix 2.7 and later.

address_verify_sender_dependent_relayhost_maps (default: $sender_dependent_relayhost_maps)
Overrides the sender_dependent_relayhost_maps parameter setting for address verification probes.

This feature is available in Postfix 2.3 and later.

address_verify_sender_ttl (default: 0s)
The time between changes in the time-dependent portion of address verification probe sender addresses. The time-dependent portion is appended to the localpart of the address specified with the address_verify_sender parameter. This feature is ignored when the probe sender addresses is the null sender, i.e. the address_verify_sender value is empty or <>.

Historically, the probe sender address was fixed. This has caused such addresses to end up on spammer mailing lists, and has resulted in wasted network and processing resources.

To enable time-dependent probe sender addresses, specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Specify a value of at least several hours, to avoid problems with senders that use greylisting. Avoid nice TTL values, to make the result less predictable. Time units are: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.9 and later.

address_verify_service_name (default: verify)
The name of the **verify(8)** address verification service. This service maintains the status of sender and/or recipient address verification probes, and generates probes on request by other Postfix processes.

address_verify_transport_maps (default: $transport_maps)
Overrides the transport_maps parameter setting for address verification probes.

This feature is available in Postfix 2.1 and later.

address_verify_virtual_transport (default: $virtual_transport)
Overrides the virtual_transport parameter setting for address verification probes.

This feature is available in Postfix 2.1 and later.

alias_database (default: see postconf −d output)

The alias databases for **local(8)** delivery that are updated with "**newaliases**" or with "**sendmail -bi**".

This is a separate configuration parameter because not all the tables specified with $alias_maps have to be local files.

Examples:

```
alias_database = hash:/etc/aliases
alias_database = hash:/etc/mail/aliases
```

alias_maps (default: see postconf −d output)

The alias databases that are used for **local(8)** delivery. See **aliases(5)** for syntax details. Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found. Note: these lookups are recursive.

The default list is system dependent. On systems with NIS, the default is to search the local alias database, then the NIS alias database.

If you change the alias database, run "**postalias /etc/aliases**" (or wherever your system stores the mail alias file), or simply run "**newaliases**" to build the necessary DBM or DB file.

The **local(8)** delivery agent disallows regular expression substitution of $1 etc. in alias_maps, because that would open a security hole.

The **local(8)** delivery agent will silently ignore requests to use the **proxymap(8)** server within alias_maps. Instead it will open the table directly. Before Postfix version 2.2, the **local(8)** delivery agent will terminate with a fatal error.

Examples:

```
alias_maps = hash:/etc/aliases, nis:mail.aliases
alias_maps = hash:/etc/aliases
```

allow_mail_to_commands (default: alias, forward)

Restrict **local(8)** mail delivery to external commands. The default is to disallow delivery to "|command" in :include: files (see **aliases(5)** for the text that defines this terminology).

Specify zero or more of: **alias**, **forward** or **include**, in order to allow commands in **aliases(5)**, :include: files, respectively.

Example:

```
allow_mail_to_commands = alias,forward,include
```

allow_mail_to_files (default: alias, forward)

Restrict **local(8)** mail delivery to external files. The default is to disallow "/file/name" destinations in :include: files (see **aliases(5)** for the text that defines this terminology).

Specify zero or more of: **alias**, **forward** or **include**, in order to allow "/file/name" destinations in **aliases(5)**, files and in :include: files, respectively.

Example:

```
allow_mail_to_files = alias,forward,include
```

allow_min_user (default: no)

Allow a sender or recipient address to have ‘-’ as the first character. By default, this is not allowed, to avoid accidents with software that passes email addresses via the command line. Such software would not be able to distinguish a malicious address from a bona fide command-line option. Although this can be prevented by inserting a "--" option terminator into the command line, this is difficult to enforce consistently and globally.

As of Postfix version 2.5, this feature is implemented by trivial-**rewrite**(8). With earlier versions this feature was implemented by **qmgr(8)** and was limited to recipient addresses only.

allow_percent_hack (default: yes)

Enable the rewriting of the form "user%domain" to "user@domain". This is enabled by default.

Note: as of Postfix version 2.2, message header address rewriting happens only when one of the following conditions is true:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

Example:

```
allow_percent_hack = no
```

allow_untrusted_routing (default: no)

Forward mail with sender-specified routing (user[@%!]remote[@%!]site) from untrusted clients to destinations matching $relay_domains.

By default, this feature is turned off. This closes a nasty open relay loophole where a backup MX host can be tricked into forwarding junk mail to a primary MX host which then spams it out to the world.

This parameter also controls if non-local addresses with sender-specified routing can match Postfix access tables. By default, such addresses cannot match Postfix access tables, because the address is ambiguous.

alternate_config_directories (default: empty)

A list of non-default Postfix configuration directories that may be specified with "-c config_directory" on the command line, or via the MAIL_CONFIG environment parameter.

This list must be specified in the default Postfix configuration directory, and is used by set-gid Postfix commands such as **postqueue(1)** and **postdrop(1)**.

always_add_missing_headers (default: no)

Always add (Resent-) From:, To:, Date: or Message-ID: headers when not present. Postfix 2.6 and later add these headers only when clients match the local_header_rewrite_clients parameter setting. Earlier Postfix versions always add these headers; this may break DKIM signatures that cover non-existent headers. The undisclosed_recipients_header parameter setting determines whether a To: header will be added.

always_bcc (default: empty)

Optional address that receives a "blind carbon copy" of each message that is received by the Postfix mail system.

Note: with Postfix 2.3 and later the BCC address is added as if it was specified with NOTIFY=NONE. The sender will not be notified when the BCC address is undeliverable, as long as all down-stream software implements RFC 3461.

Note: with Postfix 2.2 and earlier the sender will be notified when the BCC address is undeliverable.

Note: automatic BCC recipients are produced only for new mail. To avoid mailer loops, automatic BCC recipients are not generated after Postfix forwards mail internally, or after Postfix generates mail itself.

anvil_rate_time_unit (default: 60s)

The time unit over which client connection rates and other rates are calculated.

This feature is implemented by the **anvil(8)** service which is available in Postfix version 2.2 and later.

The default interval is relatively short. Because of the high frequency of updates, the **anvil(8)** server uses volatile memory only. Thus, information is lost whenever the process terminates.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

anvil_status_update_time (default: 600s)

How frequently the **anvil(8)** connection and rate limiting server logs peak usage information.

This feature is available in Postfix 2.2 and later.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

append_at_myorigin (default: yes)

With locally submitted mail, append the string "@$myorigin" to mail addresses without domain information. With remotely submitted mail, append the string "@$remote_header_rewrite_domain" instead.

Note 1: this feature is enabled by default and must not be turned off. Postfix does not support domain-less addresses.

Note 2: with Postfix version 2.2, message header address rewriting happens only when one of the following conditions is true:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

append_dot_mydomain (default: Postfix >= 3.0: no, Postfix < 3.0: yes)

With locally submitted mail, append the string ".$mydomain" to addresses that have no ".domain" information. With remotely submitted mail, append the string ".$remote_header_rewrite_domain" instead.

Note 1: this feature is enabled by default. If disabled, users will not be able to send mail to "user@partial-domainname" but will have to specify full domain names instead.

Note 2: with Postfix version 2.2, message header address rewriting happens only when one of the following conditions is true:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

application_event_drain_time (default: 100s)

How long the **postkick(1)** command waits for a request to enter the Postfix daemon process input buffer before giving up.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.1 and later.

authorized_flush_users (default: static:anyone)

List of users who are authorized to flush the queue.

By default, all users are allowed to flush the queue. Access is always granted if the invoking user is the super-user or the $mail_owner user. Otherwise, the real UID of the process is looked up in the system password file, and access is granted only if the corresponding login name is on the access list. The username "unknown" is used for processes whose real UID is not found in the password file.

Specify a list of user names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. The list is matched left to right, and the search stops on the first match. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

This feature is available in Postfix 2.2 and later.

authorized_mailq_users (default: static:anyone)

List of users who are authorized to view the queue.

By default, all users are allowed to view the queue. Access is always granted if the invoking user is the super-user or the $mail_owner user. Otherwise, the real UID of the process is looked up in the system password file, and access is granted only if the corresponding login name is on the access list. The username "unknown" is used for processes whose real UID is not found in the password file.

Specify a list of user names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. The list is matched left to right, and the search stops on the first match. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a user name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

This feature is available in Postfix 2.2 and later.

authorized_submit_users (default: static:anyone)

List of users who are authorized to submit mail with the **sendmail(1)** command (and with the privileged **postdrop(1)** helper command).

By default, all users are allowed to submit mail. Otherwise, the real UID of the process is looked up in the system password file, and access is granted only if the corresponding login name is on the access list. The username "unknown" is used for processes whose real UID is not found in the password file. To deny mail submission access to all users specify an empty list.

Specify a list of user names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. The list is matched left to right, and the search stops on the first match. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a user name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Example:

```
authorized_submit_users = !www, static:all
```

This feature is available in Postfix 2.2 and later.

authorized_verp_clients (default: $mynetworks)

What remote SMTP clients are allowed to specify the XVERP command. This command requests that mail be delivered one recipient at a time with a per recipient return address.

By default, only trusted clients are allowed to specify XVERP.

This parameter was introduced with Postfix version 1.1. Postfix version 2.1 renamed this parameter to smtpd_authorized_verp_clients and changed the default to none.

Specify a list of network/netmask patterns, separated by commas and/or whitespace. The mask specifies the number of bits in the network part of a host address. You can also specify hostnames or .domain names (the initial dot causes the domain to match any name below it), "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note: IP version 6 address information must be specified inside [] in the authorized_verp_clients value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

backwards_bounce_logfile_compatibility (default: yes)

Produce additional **bounce(8)** logfile records that can be read by Postfix versions before 2.0. The current and more extensible "name = value" format is needed in order to implement more sophisticated functionality.

This feature is available in Postfix 2.1 and later.

berkeley_db_create_buffer_size (default: 16777216)
The per-table I/O buffer size for programs that create Berkeley DB hash or btree tables. Specify a byte count.

This feature is available in Postfix 2.0 and later.

berkeley_db_read_buffer_size (default: 131072)
The per-table I/O buffer size for programs that read Berkeley DB hash or btree tables. Specify a byte count.

This feature is available in Postfix 2.0 and later.

best_mx_transport (default: empty)
Where the Postfix SMTP client should deliver mail when it detects a "mail loops back to myself" error condition. This happens when the local MTA is the best SMTP mail exchanger for a destination not listed in $mydestination, $inet_interfaces, $proxy_interfaces, $virtual_alias_domains, or $virtual_mailbox_domains. By default, the Postfix SMTP client returns such mail as undeliverable.

Specify, for example, "best_mx_transport = local" to pass the mail from the Postfix SMTP client to the **local(8)** delivery agent. You can specify any message delivery "transport" or "transport:nexthop" that is defined in the master.cf file. See the **transport(5)** manual page for the syntax and meaning of "transport" or "transport:nexthop".

However, this feature is expensive because it ties up a Postfix SMTP client process while the **local(8)** delivery agent is doing its work. It is more efficient (for Postfix) to list all hosted domains in a table or database.

biff (default: yes)
Whether or not to use the local biff service. This service sends "new mail" notifications to users who have requested new mail notification with the UNIX command "biff y".

For compatibility reasons this feature is on by default. On systems with lots of interactive users, the biff service can be a performance drain. Specify "biff = no" in main.cf to disable.

body_checks (default: empty)
Optional lookup tables for content inspection as specified in the **body_checks(5)** manual page.

Note: with Postfix versions before 2.0, these rules inspect all content after the primary message headers.

body_checks_size_limit (default: 51200)
How much text in a message body segment (or attachment, if you prefer to use that term) is subjected to body_checks inspection. The amount of text is limited to avoid scanning huge attachments.

This feature is available in Postfix 2.0 and later.

bounce_notice_recipient (default: postmaster)
The recipient of postmaster notifications with the message headers of mail that Postfix did not deliver and of SMTP conversation transcripts of mail that Postfix did not receive. This feature is enabled with the notify_classes parameter.

bounce_queue_lifetime (default: 5d)
Consider a bounce message as undeliverable, when delivery fails with a temporary error, and the time in the queue has reached the bounce_queue_lifetime limit. By default, this limit is the same as for regular mail.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is d (days).

Specify 0 when mail delivery should be tried only once.

This feature is available in Postfix 2.1 and later.

bounce_service_name (default: bounce)
The name of the **bounce(8)** service. This service maintains a record of failed delivery attempts and generates non-delivery notifications.

This feature is available in Postfix 2.0 and later.

bounce_size_limit (default: 50000)

The maximal amount of original message text that is sent in a non-delivery notification. Specify a byte count. A message is returned as either message/rfc822 (the complete original) or as text/rfc822-headers (the headers only). With Postfix version 2.4 and earlier, a message is always returned as message/rfc822 and is truncated when it exceeds the size limit.

Notes:

- If you increase this limit, then you should increase the mime_nesting_limit value proportionally.
- Be careful when making changes. Excessively large values will result in the loss of non-delivery notifications, when a bounce message size exceeds a local or remote MTA's message size limit.

bounce_template_file (default: empty)

Pathname of a configuration file with bounce message templates. These override the built-in templates of delivery status notification (DSN) messages for undeliverable mail, for delayed mail, successful delivery, or delivery verification. The **bounce(5)** manual page describes how to edit and test template files.

Template message body text may contain $name references to Postfix configuration parameters. The result of $name expansion can be previewed with "**postconf -b** *file_name*" before the file is placed into the Postfix configuration directory.

This feature is available in Postfix 2.3 and later.

broken_sasl_auth_clients (default: no)

Enable interoperability with remote SMTP clients that implement an obsolete version of the AUTH command (RFC 4954). Examples of such clients are MicroSoft Outlook Express version 4 and MicroSoft Exchange version 5.0.

Specify "broken_sasl_auth_clients = yes" to have Postfix advertise AUTH support in a non-standard way.

canonical_classes (default: envelope_sender, envelope_recipient, header_sender, header_recipient)

What addresses are subject to canonical_maps address mapping. By default, canonical_maps address mapping is applied to envelope sender and recipient addresses, and to header sender and header recipient addresses.

Specify one or more of: envelope_sender, envelope_recipient, header_sender, header_recipient

This feature is available in Postfix 2.2 and later.

canonical_maps (default: empty)

Optional address mapping lookup tables for message headers and envelopes. The mapping is applied to both sender and recipient addresses, in both envelopes and in headers, as controlled with the canonical_classes parameter. This is typically used to clean up dirty addresses from legacy mail systems, or to replace login names by Firstname.Lastname. The table format and lookups are documented in **canonical(5)**. For an overview of Postfix address manipulations see the ADDRESS_REWRITING_README document.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found. Note: these lookups are recursive.

If you use this feature, run "**postmap /etc/postfix/canonical**" to build the necessary DBM or DB file after every change. The changes will become visible after a minute or so. Use "**postfix reload**" to eliminate the delay.

Note: with Postfix version 2.2, message header address mapping happens only when message header address rewriting is enabled:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

Examples:

```
canonical_maps = dbm:/etc/postfix/canonical
canonical_maps = hash:/etc/postfix/canonical
```

cleanup_service_name (default: cleanup)
The name of the **cleanup(8)** service. This service rewrites addresses into the standard form, and performs **canonical(5)** address mapping and **virtual(5)** aliasing.

This feature is available in Postfix 2.0 and later.

command_directory (default: see postconf −d output)
The location of all postfix administrative commands.

command_execution_directory (default: empty)
The **local(8)** delivery agent working directory for delivery to external command. Failure to change directory causes the delivery to be deferred.

The following $name expansions are done on command_execution_directory before the directory is changed. Expansion happens in the context of the delivery request. The result of $name expansion is filtered with the character set that is specified with the execution_directory_expansion_filter parameter.

$user The recipient's username.

$shell The recipient's login shell pathname.

$home The recipient's home directory.

$recipient
The full recipient address.

$extension
The optional recipient address extension.

$domain
The recipient domain.

$local The entire recipient localpart.

$recipient_delimiter
The address extension delimiter that was found in the recipient address (Postfix 2.11 and later), or the system-wide recipient address extension delimiter (Postfix 2.10 and earlier).

${name?value}
Expands to *value* when *$name* is non-empty.

${name:value}
Expands to *value* when *$name* is empty.

Instead of $name you can also specify ${name} or $(name).

This feature is available in Postfix 2.2 and later.

command_expansion_filter (default: see postconf −d output)
Restrict the characters that the **local(8)** delivery agent allows in $name expansions of $mailbox_command and $command_execution_directory. Characters outside the allowed set are replaced by underscores.

command_time_limit (default: 1000s)
Time limit for delivery to external commands. This limit is used by the **local(8)** delivery agent, and is the default time limit for delivery by the **pipe(8)** delivery agent.

Note: if you set this time limit to a large value you must update the global ipc_timeout parameter as well.

compatibility_level (default: 0)
A safety net that causes Postfix to run with backwards-compatible default settings after an upgrade to a newer Postfix version.

With backwards compatibility turned on (the main.cf compatibility_level value is less than the Postfix built-

in value), Postfix looks for settings that are left at their implicit default value, and logs a message when a backwards-compatible default setting is required.

```
using backwards-compatible default setting name=value
to [accept a specific client request]

using backwards-compatible default setting name=value
to [enable specific Postfix behavior]
```

See COMPATIBILITY_README for specific message details. If such a message is logged in the context of a legitimate request, the system administrator should make the backwards-compatible setting permanent in main.cf or master.cf, for example:

```
# postconf name=value
# postfix reload
```

When no more backwards-compatible settings need to be made permanent, the administrator should turn off backwards compatibility by updating the compatibility_level setting in main.cf:

```
# postconf compatibility_level=N
# postfix reload
```

For *N* specify the number that is logged in your **postfix(1)** warning message:

```
warning: To disable backwards compatibility use "postconf
compatibility_level=N" and "postfix reload"
```

This feature is available in Postfix 3.0 and later.

config_directory (default: see postconf −d output)

The default location of the Postfix main.cf and master.cf configuration files. This can be overruled via the following mechanisms:

- The MAIL_CONFIG environment variable (daemon processes and commands).
- The "-c" command-line option (commands only).

With Postfix command that run with set-gid privileges, a config_directory override requires either root privileges, or it requires that the directory is listed with the alternate_config_directories parameter in the default main.cf file.

confirm_delay_cleared (default: no)

After sending a "your message is delayed" notification, inform the sender when the delay clears up. This can result in a sudden burst of notifications at the end of a prolonged network outage, and is therefore disabled by default.

See also: delay_warning_time.

This feature is available in Postfix 3.0 and later.

connection_cache_protocol_timeout (default: 5s)

Time limit for connection cache connect, send or receive operations. The time limit is enforced in the client.

This feature is available in Postfix 2.3 and later.

connection_cache_service_name (default: scache)

The name of the **scache(8)** connection cache service. This service maintains a limited pool of cached sessions.

This feature is available in Postfix 2.2 and later.

connection_cache_status_update_time (default: 600s)

How frequently the **scache(8)** server logs usage statistics with connection cache hit and miss rates for logical destinations and for physical endpoints.

connection_cache_ttl_limit (default: 2s)

The maximal time-to-live value that the **scache(8)** connection cache server allows. Requests that specify a larger TTL will be stored with the maximum allowed TTL. The purpose of this additional control is to protect the infrastructure against careless people. The cache TTL is already bounded by $max_idle.

content_filter (default: empty)

After the message is queued, send the entire message to the specified *transport:destination*. The *transport* name specifies the first field of a mail delivery agent definition in master.cf; the syntax of the next-hop *destination* is described in the manual page of the corresponding delivery agent. More information about external content filters is in the Postfix FILTER_README file.

Notes:

- This setting has lower precedence than a FILTER action that is specified in an **access(5)**, **header_checks(5)** or **body_checks(5)** table.
- The meaning of an empty next-hop filter *destination* is version dependent. Postfix 2.7 and later will use the recipient domain; earlier versions will use $myhostname. Specify "default_filter_nexthop = $myhostname" for compatibility with Postfix 2.6 or earlier, or specify a content_filter value with an explicit next-hop *destination*.

cyrus_sasl_config_path (default: empty)

Search path for Cyrus SASL application configuration files, currently used only to locate the $smtpd_sasl_path.conf file. Specify zero or more directories separated by a colon character, or an empty value to use Cyrus SASL's built-in search path.

This feature is available in Postfix 2.5 and later when compiled with Cyrus SASL 2.1.22 or later.

daemon_directory (default: see postconf −d output)

The directory with Postfix support programs and daemon programs. These should not be invoked directly by humans. The directory must be owned by root.

daemon_table_open_error_is_fatal (default: no)

How a Postfix daemon process handles errors while opening lookup tables: gradual degradation or immediate termination.

no (default)
: Gradual degradation: a daemon process logs a message of type "error" and continues execution with reduced functionality. Features that do not depend on the unavailable table will work normally, while features that depend on the table will result in a type "warning" message.
When the notify_classes parameter value contains the "data" class, the Postfix SMTP server and client will report transcripts of sessions with an error because a table is unavailable.

yes (historical behavior)
: Immediate termination: a daemon process logs a type "fatal" message and terminates immediately. This option reduces the number of possible code paths through Postfix, and may therefore be slightly more secure than the default.

For the sake of sanity, the number of type "error" messages is limited to 13 over the lifetime of a daemon process.

This feature is available in Postfix 2.9 and later.

daemon_timeout (default: 18000s)

How much time a Postfix daemon process may take to handle a request before it is terminated by a built-in watchdog timer.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

data_directory (default: see postconf −d output)

The directory with Postfix-writable data files (for example: caches, pseudo-random numbers). This directory must be owned by the mail_owner account, and must not be shared with non-Postfix software.

This feature is available in Postfix 2.5 and later.

debug_peer_level (default: 2)

The increment in verbose logging level when a remote client or server matches a pattern in the debug_peer_list parameter.

debug_peer_list (default: empty)

Optional list of remote client or server hostname or network address patterns that cause the verbose logging level to increase by the amount specified in $debug_peer_level.

Specify domain names, network/netmask patterns, "/file/name" patterns or "type:table" lookup tables. The right-hand side result from "type:table" lookups is ignored.

Pattern matching of domain names is controlled by the presence or absence of "debug_peer_list" in the parent_domain_matches_subdomains parameter value.

Examples:

```
debug_peer_list = 127.0.0.1
debug_peer_list = example.com
```

debugger_command (default: empty)

The external command to execute when a Postfix daemon program is invoked with the -D option.

Use "command .. & sleep 5" so that the debugger can attach before the process marches on. If you use an X-based debugger, be sure to set up your XAUTHORITY environment variable before starting Postfix.

Note: the command is subject to $name expansion, before it is passed to the default command interpreter. Specify "$$" to produce a single "$" character.

Example:

```
debugger_command =
PATH=/usr/bin:/usr/X11R6/bin
ddd $daemon_directory/$process_name $process_id & sleep 5
```

default_database_type (default: see postconf −d output)

The default database type for use in **newaliases(1)**, **postalias(1)** and **postmap(1)** commands. On many UNIX systems the default type is either **dbm** or **hash**. The default setting is frozen when the Postfix system is built.

Examples:

```
default_database_type = hash
default_database_type = dbm
```

default_delivery_slot_cost (default: 5)

How often the Postfix queue manager’s scheduler is allowed to preempt delivery of one message with another.

Each transport maintains a so-called "available delivery slot counter" for each message. One message can be preempted by another one when the other message can be delivered using no more delivery slots (i.e., invocations of delivery agents) than the current message counter has accumulated (or will eventually accumulate - see about slot loans below). This parameter controls how often is the counter incremented - it happens after each default_delivery_slot_cost recipients have been delivered.

The cost of 0 is used to disable the preempting scheduling completely. The minimum value the scheduling algorithm can use is 2 - use it if you want to maximize the message throughput rate. Although there is no maximum, it doesn’t make much sense to use values above say 50.

The only reason why the value of 2 is not the default is the way this parameter affects the delivery of mailing-list mail. In the worst case, their delivery can take somewhere between (cost+1/cost) and (cost/cost-1) times more than if the preemptive scheduler was disabled. The default value of 5 turns out to provide reasonable message response times while making sure the mailing-list deliveries are not extended by more than 20-25 percent even in the worst case.

Use *transport*_delivery_slot_cost to specify a transport-specific override, where *transport* is the master.cf

name of the message delivery transport.

Examples:

```
default_delivery_slot_cost = 0
default_delivery_slot_cost = 2
```

default_delivery_slot_discount (default: 50)

The default value for transport-specific _delivery_slot_discount settings.

This parameter speeds up the moment when a message preemption can happen. Instead of waiting until the full amount of delivery slots required is available, the preemption can happen when transport_delivery_slot_discount percent of the required amount plus transport_delivery_slot_loan still remains to be accumulated. Note that the full amount will still have to be accumulated before another preemption can take place later.

Use *transport*_delivery_slot_discount to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_delivery_slot_loan (default: 3)

The default value for transport-specific _delivery_slot_loan settings.

This parameter speeds up the moment when a message preemption can happen. Instead of waiting until the full amount of delivery slots required is available, the preemption can happen when transport_delivery_slot_discount percent of the required amount plus transport_delivery_slot_loan still remains to be accumulated. Note that the full amount will still have to be accumulated before another preemption can take place later.

Use *transport*_delivery_slot_loan to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_delivery_status_filter (default: empty)

Optional filter to replace the delivery status code or explanatory text of successful or unsuccessful deliveries. This does not allow the replacement of a successful status code (2.X.X) with an unsuccessful status code (4.X.X or 5.X.X) or vice versa.

The following parameters can be used to implement a filter for specific delivery agents: lmtp_delivery_status_filter, local_delivery_status_filter, pipe_delivery_status_filter, smtp_delivery_status_filter or virtual_delivery_status_filter. These parameters support the same filter syntax as described here.

Specify zero or more "type:table" lookup table names, separated by comma or whitespace. For each successful or unsuccessful delivery to a recipient, the tables are queried in the specified order with one line of text that is structured as follows:

enhanced-status-code SPACE explanatory-text

The first table match wins. The lookup result must have the same structure as the query, a successful status code (2.X.X) must be replaced with a successful status code, an unsuccessful status code (4.X.X or 5.X.X) must be replaced with an unsuccessful status code, and the explanatory text field must be non-empty. Other results will result in a warning.

Example 1: convert specific soft TLS errors into hard errors, by overriding the first number in the enhanced status code.

```
/etc/postfix/main.cf:
smtp_delivery_status_filter = pcre:/etc/postfix/smtp_dsn_filter

/etc/postfix/smtp_dsn_filter:
/^4(\.\d+\.\d+ TLS is required, but host \S+ refused to start TLS: .+)/
5$1
/^4(\.\d+\.\d+ TLS is required, but was not offered by host .+)/
5$1
# Do not change the following into hard bounces. They may
# result from a local configuration problem.
```

```
# 4.\d+.\d+ TLS is required, but our TLS engine is unavailable
# 4.\d+.\d+ TLS is required, but unavailable
# 4.\d+.\d+ Cannot start TLS: handshake failure
```

Example 2: censor the per-recipient delivery status text so that it does not reveal the destination command or filename when a remote sender requests confirmation of successful delivery.

```
/etc/postfix/main.cf:
local_delivery_status_filter = pcre:/etc/postfix/local_dsn_filter

/etc/postfix/local_dsn_filter:
/^(2\S+ delivered to file).+/ $1
/^(2\S+ delivered to command).+/ $1
```

Notes:

- This feature will NOT override the soft_bounce safety net.
- This feature will change the enhanced status code and text that is logged to the maillog file, and that is reported to the sender in delivery confirmation or non-delivery notifications.

This feature is available in Postfix 3.0 and later.

default_destination_concurrency_failed_cohort_limit (default: 1)

How many pseudo-cohorts must suffer connection or handshake failure before a specific destination is considered unavailable (and further delivery is suspended). Specify zero to disable this feature. A destination's pseudo-cohort failure count is reset each time a delivery completes without connection or handshake failure for that specific destination.

A pseudo-cohort is the number of deliveries equal to a destination's delivery concurrency.

Use *transport*_destination_concurrency_failed_cohort_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

This feature is available in Postfix 2.5. The default setting is compatible with earlier Postfix versions.

default_destination_concurrency_limit (default: 20)

The default maximal number of parallel deliveries to the same destination. This is the default limit for delivery via the **lmtp(8)**, **pipe(8)**, **smtp(8)** and **virtual(8)** delivery agents. With per-destination recipient limit > 1, a destination is a domain, otherwise it is a recipient.

Use *transport*_destination_concurrency_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_destination_concurrency_negative_feedback (default: 1)

The per-destination amount of delivery concurrency negative feedback, after a delivery completes with a connection or handshake failure. Feedback values are in the range 0..1 inclusive. With negative feedback, concurrency is decremented at the beginning of a sequence of length 1/feedback. This is unlike positive feedback, where concurrency is incremented at the end of a sequence of length 1/feedback.

As of Postfix version 2.5, negative feedback cannot reduce delivery concurrency to zero. Instead, a destination is marked dead (further delivery suspended) after the failed pseudo-cohort count reaches $default_destination_concurrency_failed_cohort_limit (or $*transport*_destination_concurrency_failed_cohort_limit). To make the scheduler completely immune to connection or handshake failures, specify a zero feedback value and a zero failed pseudo-cohort limit.

Specify one of the following forms:

number

number / *number*

Constant feedback. The value must be in the range 0..1 inclusive. The default setting of "1" is compatible with Postfix versions before 2.5, where a destination's delivery concurrency is throttled down to zero (and further delivery suspended) after a single failed pseudo-cohort.

number / concurrency
: Variable feedback of "*number* / (delivery concurrency)". The*number* must be in the range 0..1 inclusive. With *number* equal to "1", a destination's delivery concurrency is decremented by 1 after each failed pseudo-cohort.

A pseudo-cohort is the number of deliveries equal to a destination's delivery concurrency.

Use *transport*_destination_concurrency_negative_feedback to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

This feature is available in Postfix 2.5. The default setting is compatible with earlier Postfix versions.

default_destination_concurrency_positive_feedback (default: 1)

The per-destination amount of delivery concurrency positive feedback, after a delivery completes without connection or handshake failure. Feedback values are in the range 0..1 inclusive. The concurrency increases until it reaches the per-destination maximal concurrency limit. With positive feedback, concurrency is incremented at the end of a sequence with length 1/feedback. This is unlike negative feedback, where concurrency is decremented at the start of a sequence of length 1/feedback.

Specify one of the following forms:

number

number / *number*
: Constant feedback. The value must be in the range 0..1 inclusive. The default setting of "1" is compatible with Postfix versions before 2.5, where a destination's delivery concurrency doubles after each successful pseudo-cohort.

number / concurrency
: Variable feedback of "*number* / (delivery concurrency)". The*number* must be in the range 0..1 inclusive. With *number* equal to "1", a destination's delivery concurrency is incremented by 1 after each successful pseudo-cohort.

A pseudo-cohort is the number of deliveries equal to a destination's delivery concurrency.

Use *transport*_destination_concurrency_positive_feedback to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

This feature is available in Postfix 2.5 and later.

default_destination_rate_delay (default: 0s)

The default amount of delay that is inserted between individual deliveries to the same destination; the resulting behavior depends on the value of the corresponding per-destination recipient limit.

- With a corresponding per-destination recipient limit > 1, the rate delay specifies the time between deliveries to the *same domain*. Different domains are delivered in parallel, subject to the process limits specified in master.cf.
- With a corresponding per-destination recipient limit equal to 1, the rate delay specifies the time between deliveries to the *same recipient*. Different recipients are delivered in parallel, subject to the process limits specified in master.cf.

To enable the delay, specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

NOTE: the delay is enforced by the queue manager. The delay timer state does not survive "**postfix reload**" or "**postfix stop**".

Use *transport*_destination_rate_delay to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

NOTE: with a non-zero _destination_rate_delay, specify a *transport*_destination_concurrency_failed_cohort_limit of 10 or more to prevent Postfix from deferring all mail for the same destination after only one connection or handshake error.

This feature is available in Postfix 2.5 and later.

default_destination_recipient_limit (default: 50)

The default maximal number of recipients per message delivery. This is the default limit for delivery via the **lmtp(8)**, **pipe(8)**, **smtp(8)** and **virtual(8)** delivery agents.

Setting this parameter to a value of 1 affects email deliveries as follows:

- It changes the meaning of the corresponding per-destination concurrency limit, from concurrency of deliveries to the *same domain* into concurrency of deliveries to the *same recipient*. Different recipients are delivered in parallel, subject to the process limits specified in master.cf.
- It changes the meaning of the corresponding per-destination rate delay, from the delay between deliveries to the *same domain* into the delay between deliveries to the *same recipient*. Again, different recipients are delivered in parallel, subject to the process limits specified in master.cf.
- It changes the meaning of other corresponding per-destination settings in a similar manner, from settings for delivery to the *same domain* into settings for delivery to the *same recipient*.

Use *transport*_destination_recipient_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_extra_recipient_limit (default: 1000)

The default value for the extra per-transport limit imposed on the number of in-memory recipients. This extra recipient space is reserved for the cases when the Postfix queue manager's scheduler preempts one message with another and suddenly needs some extra recipients slots for the chosen message in order to avoid performance degradation.

Use *transport*_extra_recipient_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_filter_nexthop (default: empty)

When a content_filter or FILTER request specifies no explicit next-hop destination, use $default_filter_nexthop instead; when that value is empty, use the domain in the recipient address. Specify "default_filter_nexthop = $myhostname" for compatibility with Postfix version 2.6 and earlier, or specify an explicit next-hop destination with each content_filter value or FILTER action.

This feature is available in Postfix 2.7 and later.

default_minimum_delivery_slots (default: 3)

How many recipients a message must have in order to invoke the Postfix queue manager's scheduling algorithm at all. Messages which would never accumulate at least this many delivery slots (subject to slot cost parameter as well) are never preempted.

Use *transport*_minimum_delivery_slots to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_privs (default: nobody)

The default rights used by the **local(8)** delivery agent for delivery to external file or command. These rights are used when delivery is requested from an **aliases(5)** file that is owned by **root**, or when delivery is done on behalf of **root**. **DO NOT SPECIFY A PRIVILEGED USER OR THE POSTFIX OWNER**.

default_process_limit (default: 100)

The default maximal number of Postfix child processes that provide a given service. This limit can be overruled for specific services in the master.cf file.

default_rbl_reply (default: see postconf −d output)

The default Postfix SMTP server response template for a request that is rejected by an RBL-based restriction. This template can be overruled by specific entries in the optional rbl_reply_maps lookup table.

This feature is available in Postfix 2.0 and later.

The template is subject to exactly one level of $name substitution:

$client The client hostname and IP address, formatted as name[address].

$client_address
The client IP address.

$client_name
The client hostname or "unknown". See reject_unknown_client_hostname for more details.

$reverse_client_name
The client hostname from address->name lookup, or "unknown". See reject_unknown_reverse_client_hostname for more details.

$helo_name
The hostname given in HELO or EHLO command or empty string.

$rbl_class
The blacklisted entity type: Client host, Helo command, Sender address, or Recipient address.

$rbl_code
The numerical SMTP response code, as specified with the maps_rbl_reject_code configuration parameter. Note: The numerical SMTP response code is required, and must appear at the start of the reply. With Postfix version 2.3 and later this information may be followed by an RFC 3463 enhanced status code.

$rbl_domain
The RBL domain where $rbl_what is blacklisted.

$rbl_reason
The reason why $rbl_what is blacklisted, or an empty string.

$rbl_what
The entity that is blacklisted (an IP address, a hostname, a domain name, or an email address whose domain was blacklisted).

$recipient
The recipient address or <> in case of the null address.

$recipient_domain
The recipient domain or empty string.

$recipient_name
The recipient address localpart or <> in case of null address.

$sender
The sender address or <> in case of the null address.

$sender_domain
The sender domain or empty string.

$sender_name
The sender address localpart or <> in case of the null address.

${name?text}
Expands to ‘text’ if $name is not empty.

${name:text}
Expands to ‘text’ if $name is empty.

Instead of $name you can also specify ${name} or $(name).

Note: when an enhanced status code is specified in an RBL reply template, it is subject to modification. The following transformations are needed when the same RBL reply template is used for client, helo, sender, or recipient access restrictions.

- When rejecting a sender address, the Postfix SMTP server will transform a recipient DSN status (e.g., 4.1.1-4.1.6) into the corresponding sender DSN status, and vice versa.

- When rejecting non-address information (such as the HELO command argument or the client hostname/address), the Postfix SMTP server will transform a sender or recipient DSN status into a generic non-address DSN status (e.g., 4.0.0).

default_recipient_limit (default: 20000)

The default per-transport upper limit on the number of in-memory recipients. These limits take priority over the global qmgr_message_recipient_limit after the message has been assigned to the respective transports. See also default_extra_recipient_limit and qmgr_message_recipient_minimum.

Use *transport*_recipient_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

default_recipient_refill_delay (default: 5s)

The default per-transport maximum delay between recipients refills. When not all message recipients fit into the memory at once, keep loading more of them at least once every this many seconds. This is used to make sure the recipients are refilled in timely manner even when $default_recipient_refill_limit is too high for too slow deliveries.

Use *transport*_recipient_refill_delay to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

This feature is available in Postfix 2.4 and later.

default_recipient_refill_limit (default: 100)

The default per-transport limit on the number of recipients refilled at once. When not all message recipients fit into the memory at once, keep loading more of them in batches of at least this many at a time. See also $default_recipient_refill_delay, which may result in recipient batches lower than this when this limit is too high for too slow deliveries.

Use *transport*_recipient_refill_limit to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport.

This feature is available in Postfix 2.4 and later.

default_transport (default: smtp)

The default mail delivery transport and next-hop destination for destinations that do not match $mydestination, $inet_interfaces, $proxy_interfaces, $virtual_alias_domains, $virtual_mailbox_domains, or $relay_domains. This information can be overruled with the sender_dependent_default_transport_maps parameter and with the **transport(5)** table.

In order of decreasing precedence, the nexthop destination is taken from $sender_dependent_default_transport_maps, $default_transport, $sender_dependent_relayhost_maps, $relayhost, or from the recipient domain.

Specify a string of the form *transport:nexthop*, where *transport* is the name of a mail delivery transport defined in master.cf. The*:ne xthop* destination is optional; its syntax is documented in the manual page of the corresponding delivery agent.

Example:

```
default_transport = uucp:relayhostname
```

default_transport_rate_delay (default: 0s)

The default amount of delay that is inserted between individual deliveries over the same message delivery transport, regardless of destination. If non-zero, all deliveries over the same message delivery transport will happen one at a time.

Use *transport*_transport_rate_delay to specify a transport-specific override, where the initial *transport* is the master.cf name of the message delivery transport.

Example: throttle outbound SMTP mail to at most 3 deliveries per minute.

```
/etc/postfix/main.cf:
smtp_transport_rate_delay = 20s
```

To enable the delay, specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

NOTE: the delay is enforced by the queue manager.

This feature is available in Postfix 3.1 and later.

default_verp_delimiters (default: +=)

The two default VERP delimiter characters. These are used when no explicit delimiters are specified with the SMTP XVERP command or with the "**sendmail -V**" command-line option. Specify characters that are allowed by the verp_delimiter_filter setting.

This feature is available in Postfix 1.1 and later.

defer_code (default: 450)

The numerical Postfix SMTP server response code when a remote SMTP client request is rejected by the "defer" restriction.

Do not change this unless you have a complete understanding of RFC 5321.

defer_service_name (default: defer)

The name of the defer service. This service is implemented by the **bounce(8)** daemon and maintains a record of failed delivery attempts and generates non-delivery notifications.

This feature is available in Postfix 2.0 and later.

defer_transports (default: empty)

The names of message delivery transports that should not deliver mail unless someone issues "**sendmail -q**" or equivalent. Specify zero or more names of mail delivery transports names that appear in the first field of master.cf.

Example:

```
defer_transports = smtp
```

delay_logging_resolution_limit (default: 2)

The maximal number of digits after the decimal point when logging sub-second delay values. Specify a number in the range 0..6.

Large delay values are rounded off to an integral number seconds; delay values below the delay_logging_resolution_limit are logged as "0", and delay values under 100s are logged with at most two-digit precision.

The format of the "delays=a/b/c/d" logging is as follows:

- a = time from message arrival to last active queue entry
- b = time from last active queue entry to connection setup
- c = time in connection setup, including DNS, EHLO and STARTTLS
- d = time in message transmission

This feature is available in Postfix 2.3 and later.

delay_notice_recipient (default: postmaster)

The recipient of postmaster notifications with the message headers of mail that cannot be delivered within $delay_warning_time time units.

See also: delay_warning_time, notify_classes.

delay_warning_time (default: 0h)

The time after which the sender receives a copy of the message headers of mail that is still queued. The confirm_delay_cleared parameter controls sender notification when the delay clears up.

To enable this feature, specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is h (hours).

See also: delay_notice_recipient, notify_classes, confirm_delay_cleared.

deliver_lock_attempts (default: 20)
The maximal number of attempts to acquire an exclusive lock on a mailbox file or **bounce(8)** logfile.

deliver_lock_delay (default: 1s)
The time between attempts to acquire an exclusive lock on a mailbox file or **bounce(8)** logfile.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

destination_concurrency_feedback_debug (default: no)
Make the queue manager's feedback algorithm verbose for performance analysis purposes.

This feature is available in Postfix 2.5 and later.

detect_8bit_encoding_header (default: yes)
Automatically detect 8BITMIME body content by looking at Content-Transfer-Encoding: message headers; historically, this behavior was hard-coded to be "always on".

This feature is available in Postfix 2.5 and later.

disable_dns_lookups (default: no)
Disable DNS lookups in the Postfix SMTP and LMTP clients. When disabled, hosts are looked up with the getaddrinfo() system library routine which normally also looks in /etc/hosts. As of Postfix 2.11, this parameter is deprecated; use smtp_dns_support_level instead.

DNS lookups are enabled by default.

disable_mime_input_processing (default: no)
Turn off MIME processing while receiving mail. This means that no special treatment is given to Content-Type: message headers, and that all text after the initial message headers is considered to be part of the message body.

This feature is available in Postfix 2.0 and later.

Mime input processing is enabled by default, and is needed in order to recognize MIME headers in message content.

disable_mime_output_conversion (default: no)
Disable the conversion of 8BITMIME format to 7BIT format. Mime output conversion is needed when the destination does not advertise 8BITMIME support.

This feature is available in Postfix 2.0 and later.

disable_verp_bounces (default: no)
Disable sending one bounce report per recipient.

The default, one per recipient, is what ezmlm needs.

This feature is available in Postfix 1.1 and later.

disable_vrfy_command (default: no)
Disable the SMTP VRFY command. This stops some techniques used to harvest email addresses.

Example:

```
disable_vrfy_command = no
```

dns_ncache_ttl_fix_enable (default: no)
Enable a workaround for future libc incompatibility. The Postfix implementation of RFC 2308 negative reply caching relies on the promise that res_query() and res_search() invoke res_send(), which returns the server response in an application buffer even if the requested record does not exist. If this promise is broken, specify "yes" to enable a workaround for DNS reputation lookups.

This feature is available in Postfix 3.1 and later.

dnsblog_reply_delay (default: 0s)
A debugging aid to artificially delay DNS responses.

This feature is available in Postfix 2.8.

dnsblog_service_name (default: dnsblog)
The name of the **dnsblog(8)** service entry in master.cf. This service performs DNS white/blacklist lookups.

This feature is available in Postfix 2.8 and later.

dont_remove (default: 0)
Don't remove queue files and save them to the "saved" mail queue. This is a debugging aid. To inspect the envelope information and content of a Postfix queue file, use the **postcat(1)** command.

double_bounce_sender (default: double−bounce)
The sender address of postmaster notifications that are generated by the mail system. All mail to this address is silently discarded, in order to terminate mail bounce loops.

duplicate_filter_limit (default: 1000)
The maximal number of addresses remembered by the address duplicate filter for **aliases(5)** or **virtual(5)** alias expansion, or for **showq(8)** queue displays.

empty_address_default_transport_maps_lookup_key (default: <>)
The sender_dependent_default_transport_maps search string that will be used instead of the null sender address.

This feature is available in Postfix 2.7 and later.

empty_address_recipient (default: MAILER−DAEMON)
The recipient of mail addressed to the null address. Postfix does not accept such addresses in SMTP commands, but they may still be created locally as the result of configuration or software error.

empty_address_relayhost_maps_lookup_key (default: <>)
The sender_dependent_relayhost_maps search string that will be used instead of the null sender address.

This feature is available in Postfix 2.5 and later. With earlier versions, sender_dependent_relayhost_maps lookups were skipped for the null sender address.

enable_errors_to (default: no)
Report mail delivery errors to the address specified with the non-standard Errors-To: message header, instead of the envelope sender address (this feature is removed with Postfix version 2.2, is turned off by default with Postfix version 2.1, and is always turned on with older Postfix versions).

enable_long_queue_ids (default: no)
Enable long, non-repeating, queue IDs (queue file names). The benefit of non-repeating names is simpler logfile analysis and easier queue migration (there is no need to run "postsuper" to change queue file names that don't match their message file inode number).

Note: see below for how to convert long queue file names to Postfix <= 2.8.

Changing the parameter value to "yes" has the following effects:

- Existing queue file names are not affected.
- New queue files are created with names such as 3Pt2mN2VXxznjll. These are encoded in a 52-character alphabet that contains digits (0-9), upper-case letters (B-Z) and lower-case letters (b-z). For safety reasons the vowels (AEIOUaeiou) are excluded from the alphabet. The name format is: 6 or more characters for the time in seconds, 4 characters for the time in microseconds, the 'z'; the remainder is the file inode number encoded in the first 51 characters of the 52-character alphabet.
- New messages have a Message-ID header with *queueID@myhostname*.
- The mailq (postqueue -p) output has a wider Queue ID column. The number of whitespace-separated fields is not changed.

- The hash_queue_depth algorithm uses the first characters of the queue file creation time in microseconds, after conversion into hexadecimal representation. This produces the same queue hashing behavior as if the queue file name was created with "enable_long_queue_ids = no".

Changing the parameter value to "no" has the following effects:

- Existing long queue file names are renamed to the short form (while running "postfix reload" or "postsuper").
- New queue files are created with names such as C3CD21F3E90 from a hexadecimal alphabet that contains digits (0-9) and upper-case letters (A-F). The name format is: 5 characters for the time in microseconds; the remainder is the file inode number.
- New messages have a Message-ID header with *YYYYMMDDHHMMSS.queueid@myhostname*, where *YYYYMMDDHHMMSS* are the year, month, day, hour, minute and second.
- The mailq (postqueue -p) output has the same format as with Postfix <= 2.8.
- The hash_queue_depth algorithm uses the first characters of the queue file name, with the hexadecimal representation of the file creation time in microseconds.

Before migration to Postfix <= 2.8, the following commands are required to convert long queue file names into short names:

```
# postfix stop
# postconf enable_long_queue_ids=no
# postsuper
```

Repeat the postsuper command until it reports no more queue file name changes.

This feature is available in Postfix 2.9 and later.

enable_original_recipient (default: yes)

Enable support for the X-Original-To message header. This header is needed for multi-recipient mailboxes.

When this parameter is set to yes, the **cleanup(8)** daemon performs duplicate elimination on distinct pairs of (original recipient, rewritten recipient), and generates non-empty original recipient queue file records.

When this parameter is set to no, the **cleanup(8)** daemon performs duplicate elimination on the rewritten recipient address only, and generates empty original recipient queue file records.

This feature is available in Postfix 2.1 and later. With Postfix version 2.0, support for the X-Original-To message header is always turned on. Postfix versions before 2.0 have no support for the X-Original-To message header.

error_notice_recipient (default: postmaster)

The recipient of postmaster notifications about mail delivery problems that are caused by policy, resource, software or protocol errors. These notifications are enabled with the notify_classes parameter.

error_service_name (default: error)

The name of the **error(8)** pseudo delivery agent. This service always returns mail as undeliverable.

This feature is available in Postfix 2.0 and later.

execution_directory_expansion_filter (default: see postconf −d output)

Restrict the characters that the **local(8)** delivery agent allows in $name expansions of $command_execution_directory. Characters outside the allowed set are replaced by underscores.

This feature is available in Postfix 2.2 and later.

expand_owner_alias (default: no)

When delivering to an alias "aliasname" that has an "owner-aliasname" companion alias, set the envelope sender address to the expansion of the "owner-aliasname" alias. Normally, Postfix sets the envelope sender address to the name of the "owner-aliasname" alias.

export_environment (default: see postconf −d output)

The list of environment variables that a Postfix process will export to non-Postfix processes. The TZ variable is needed for sane time keeping on System-V-ish systems.

Specify a list of names and/or name=value pairs, separated by whitespace or comma. Specify "{ name=value }" to protect whitespace or comma in parameter values (whitespace after "{" and before "}" is ignored). The form name=value is supported with Postfix version 2.1 and later; the use of {} is supported with Postfix 3.0 and later.

Example:

```
export_environment = TZ PATH=/bin:/usr/bin
```

extract_recipient_limit (default: 10240)

The maximal number of recipient addresses that Postfix will extract from message headers when mail is submitted with "**sendmail -t**".

This feature was removed in Postfix version 2.1.

fallback_relay (default: empty)

Optional list of relay hosts for SMTP destinations that can't be found or that are unreachable. With Postfix 2.3 this parameter is renamed to smtp_fallback_relay.

By default, mail is returned to the sender when a destination is not found, and delivery is deferred when a destination is unreachable.

The fallback relays must be SMTP destinations. Specify a domain, host, host:port, [host]:port, [address] or [address]:port; the form [host] turns off MX lookups. If you specify multiple SMTP destinations, Postfix will try them in the specified order.

Note: before Postfix 2.2, do not use the fallback_relay feature when relaying mail for a backup or primary MX domain. Mail would loop between the Postfix MX host and the fallback_relay host when the final destination is unavailable.

- In main.cf specify "relay_transport = relay",
- In master.cf specify "-o fallback_relay =" (i.e., empty) at the end of the relay entry.
- In transport maps, specify "relay:*nexthop*..." as the right-hand side for backup or primary MX domain entries.

Postfix version 2.2 and later will not use the fallback_relay feature for destinations that it is MX host for.

fallback_transport (default: empty)

Optional message delivery transport that the **local(8)** delivery agent should use for names that are not found in the **aliases(5)** or UNIX password database.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

fallback_transport_maps (default: empty)

Optional lookup tables with per-recipient message delivery transports for recipients that the **local(8)** delivery agent could not find in the **aliases(5)** or UNIX password database.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

For safety reasons, this feature does not allow $number substitutions in regular expression maps.

This feature is available in Postfix 2.3 and later.

fast_flush_domains (default: $relay_domains)

Optional list of destinations that are eligible for per-destination logfiles with mail that is queued to those destinations.

By default, Postfix maintains "fast flush" logfiles only for destinations that the Postfix SMTP server is willing to relay to (i.e. the default is: "fast_flush_domains = $relay_domains"; see the relay_domains parameter in the **postconf(5)** manual).

Specify a list of hosts or domains, "/file/name" patterns or "type:table" lookup tables, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when the domain or its parent domain appears as lookup key.

Pattern matching of domain names is controlled by the presence or absence of "fast_flush_domains" in the parent_domain_matches_subdomains parameter value.

Specify "fast_flush_domains =" (i.e., empty) to disable the feature altogether.

fast_flush_purge_time (default: 7d)
The time after which an empty per-destination "fast flush" logfile is deleted.

You can specify the time as a number, or as a number followed by a letter that indicates the time unit: s=seconds, m=minutes, h=hours, d=days, w=weeks. The default time unit is days.

fast_flush_refresh_time (default: 12h)
The time after which a non-empty but unread per-destination "fast flush" logfile needs to be refreshed. The contents of a logfile are refreshed by requesting delivery of all messages listed in the logfile.

You can specify the time as a number, or as a number followed by a letter that indicates the time unit: s=seconds, m=minutes, h=hours, d=days, w=weeks. The default time unit is hours.

fault_injection_code (default: 0)
Force specific internal tests to fail, to test the handling of errors that are difficult to reproduce otherwise.

flush_service_name (default: flush)
The name of the **flush(8)** service. This service maintains per-destination logfiles with the queue file names of mail that is queued for those destinations.

This feature is available in Postfix 2.0 and later.

fork_attempts (default: 5)
The maximal number of attempts to fork() a child process.

fork_delay (default: 1s)
The delay between attempts to fork() a child process.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

forward_expansion_filter (default: see postconf −d output)
Restrict the characters that the **local(8)** delivery agent allows in $name expansions of $forward_path. Characters outside the allowed set are replaced by underscores.

forward_path (default: see postconf −d output)
The **local(8)** delivery agent search list for finding a .forward file with user-specified delivery methods. The first file that is found is used.

The following $name expansions are done on forward_path before the search actually happens. The result of $name expansion is filtered with the character set that is specified with the forward_expansion_filter parameter.

$user The recipient’s username.

$shell The recipient’s login shell pathname.

$home The recipient’s home directory.

$recipient
The full recipient address.

$extension
The optional recipient address extension.

$domain
The recipient domain.

$local The entire recipient localpart.

$recipient_delimiter
The address extension delimiter that was found in the recipient address (Postfix 2.11 and later), or the system-wide recipient address extension delimiter (Postfix 2.10 and earlier).

${name?value}
Expands to *value* when *$name* is non-empty.

${name:value}
Expands to *value* when *$name* is empty.

Instead of $name you can also specify ${name} or $(name).

Examples:

```
forward_path = /var/forward/$user
forward_path =
/var/forward/$user/.forward$recipient_delimiter$extension,
/var/forward/$user/.forward
```

frozen_delivered_to (default: yes)
Update the **local(8)** delivery agent's idea of the Delivered-To: address (see prepend_delivered_header) only once, at the start of a delivery attempt; do not update the Delivered-To: address while expanding aliases or .forward files.

This feature is available in Postfix 2.3 and later. With older Postfix releases, the behavior is as if this parameter is set to "no". The old setting can be expensive with deeply nested aliases or .forward files. When an alias or .forward file changes the Delivered-To: address, it ties up one queue file and one cleanup process instance while mail is being forwarded.

hash_queue_depth (default: 1)
The number of subdirectory levels for queue directories listed with the hash_queue_names parameter. Queue hashing is implemented by creating one or more levels of directories with one-character names. Originally, these directory names were equal to the first characters of the queue file name, with the hexadecimal representation of the file creation time in microseconds.

With long queue file names, queue hashing produces the same results as with short names. The file creation time in microseconds is converted into hexadecimal form before the result is used for queue hashing. The base 16 encoding gives finer control over the number of subdirectories than is possible with the base 52 encoding of long queue file names.

After changing the hash_queue_names or hash_queue_depth parameter, execute the command "**postfix reload**".

hash_queue_names (default: deferred, defer)
The names of queue directories that are split across multiple subdirectory levels.

Before Postfix version 2.2, the default list of hashed queues was significantly larger. Claims about improvements in file system technology suggest that hashing of the incoming and active queues is no longer needed. Fewer hashed directories speed up the time needed to restart Postfix.

After changing the hash_queue_names or hash_queue_depth parameter, execute the command "**postfix reload**".

header_address_token_limit (default: 10240)
The maximal number of address tokens are allowed in an address message header. Information that exceeds the limit is discarded. The limit is enforced by the **cleanup(8)** server.

header_checks (default: empty)
Optional lookup tables for content inspection of primary non-MIME message headers, as specified in the **header_checks(5)** manual page.

header_size_limit (default: 102400)
The maximal amount of memory in bytes for storing a message header. If a header is larger, the excess is discarded. The limit is enforced by the **cleanup(8)** server.

helpful_warnings (default: yes)
Log warnings about problematic configuration settings, and provide helpful suggestions.

This feature is available in Postfix 2.0 and later.

home_mailbox (default: empty)
Optional pathname of a mailbox file relative to a **local(8)** user's home directory.

Specify a pathname ending in "/" for qmail-style delivery.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

Examples:

```
home_mailbox = Mailbox
home_mailbox = Maildir/
```

hopcount_limit (default: 50)
The maximal number of Received: message headers that is allowed in the primary message headers. A message that exceeds the limit is bounced, in order to stop a mailer loop.

html_directory (default: see postconf −d output)
The location of Postfix HTML files that describe how to build, configure or operate a specific Postfix subsystem or feature.

ignore_mx_lookup_error (default: no)
Ignore DNS MX lookups that produce no response. By default, the Postfix SMTP client defers delivery and tries again after some delay. This behavior is required by the SMTP standard.

Specify "ignore_mx_lookup_error = yes" to force a DNS A record lookup instead. This violates the SMTP standard and can result in mis-delivery of mail.

import_environment (default: see postconf −d output)
The list of environment parameters that a Postfix process will import from a non-Postfix parent process. Examples of relevant parameters:

TZ Needed for sane time keeping on most System-V-ish systems.

DISPLAY
Needed for debugging Postfix daemons with an X-windows debugger.

XAUTHORITY
Needed for debugging Postfix daemons with an X-windows debugger.

MAIL_CONFIG
Needed to make "**postfix -c**" work.

Specify a list of names and/or name=value pairs, separated by whitespace or comma. Specify "{ name=value }" to protect whitespace or comma in parameter values (whitespace after "{" and before "}" is ignored). The form name=value is supported with Postfix version 2.1 and later; the use of {} is supported with Postfix 3.0 and later.

in_flow_delay (default: 1s)
Time to pause before accepting a new message, when the message arrival rate exceeds the message delivery rate. This feature is turned on by default (it's disabled on SCO UNIX due to an SCO bug).

With the default 100 Postfix SMTP server process limit, "in_flow_delay = 1s" limits the mail inflow to 100 messages per second above the number of messages delivered per second.

Specify 0 to disable the feature. Valid delays are 0..10.

inet_interfaces (default: all)

The network interface addresses that this mail system receives mail on. Specify "all" to receive mail on all network interfaces (default), and "loopback-only" to receive mail on loopback network interfaces only (Postfix version 2.2 and later). The parameter also controls delivery of mail to user@[ip.address].

Note 1: you need to stop and start Postfix when this parameter changes.

Note 2: address information may be enclosed inside [], but this form is not required here.

When inet_interfaces specifies just one IPv4 and/or IPv6 address that is not a loopback address, the Postfix SMTP client will use this address as the IP source address for outbound mail. Support for IPv6 is available in Postfix version 2.2 and later.

On a multi-homed firewall with separate Postfix instances listening on the "inside" and "outside" interfaces, this can prevent each instance from being able to reach remote SMTP servers on the "other side" of the firewall. Setting smtp_bind_address to 0.0.0.0 avoids the potential problem for IPv4, and setting smtp_bind_address6 to :: solves the problem for IPv6.

A better solution for multi-homed firewalls is to leave inet_interfaces at the default value and instead use explicit IP addresses in the master.cf SMTP server definitions. This preserves the Postfix SMTP client's loop detection, by ensuring that each side of the firewall knows that the other IP address is still the same host. Setting $inet_interfaces to a single IPv4 and/or IPV6 address is primarily useful with virtual hosting of domains on secondary IP addresses, when each IP address serves a different domain (and has a different $myhostname setting).

See also the proxy_interfaces parameter, for network addresses that are forwarded to Postfix by way of a proxy or address translator.

Examples:

```
inet_interfaces = all (DEFAULT)
inet_interfaces = loopback-only (Postfix version 2.2 and later)
inet_interfaces = 127.0.0.1
inet_interfaces = 127.0.0.1, [::1] (Postfix version 2.2 and later)
inet_interfaces = 192.168.1.2, 127.0.0.1
```

inet_protocols (default: all)

The Internet protocols Postfix will attempt to use when making or accepting connections. Specify one or more of "ipv4" or "ipv6", separated by whitespace or commas. The form "all" is equivalent to "ipv4, ipv6" or "ipv4", depending on whether the operating system implements IPv6.

With Postfix 2.8 and earlier the default is "ipv4". For backwards compatibility with these releases, the Postfix 2.9 and later upgrade procedure appends an explicit "inet_protocols = ipv4" setting to main.cf when no explicit setting is present. This compatibility workaround will be phased out as IPv6 deployment becomes more common.

This feature is available in Postfix 2.2 and later.

Note: you MUST stop and start Postfix after changing this parameter.

On systems that pre-date IPV6_V6ONLY support (RFC 3493), an IPv6 server will also accept IPv4 connections, even when IPv4 is turned off with the inet_protocols parameter. On systems with IPV6_V6ONLY support, Postfix will use separate server sockets for IPv6 and IPv4, and each will accept only connections for the corresponding protocol.

When IPv4 support is enabled via the inet_protocols parameter, Postfix will look up DNS type A records, and will convert IPv4-in-IPv6 client IP addresses (::ffff:1.2.3.4) to their original IPv4 form (1.2.3.4). The latter is needed on hosts that pre-date IPV6_V6ONLY support (RFC 3493).

When IPv6 support is enabled via the inet_protocols parameter, Postfix will do DNS type AAAA record

lookups.

When both IPv4 and IPv6 support are enabled, the Postfix SMTP client will choose the protocol as specified with the smtp_address_preference parameter. Postfix versions before 2.8 attempt to connect via IPv6 before attempting to use IPv4.

Examples:

```
inet_protocols = ipv4
inet_protocols = all (DEFAULT)
inet_protocols = ipv6
inet_protocols = ipv4, ipv6
```

initial_destination_concurrency (default: 5)

The initial per-destination concurrency level for parallel delivery to the same destination. With per-destination recipient limit > 1, a destination is a domain, otherwise it is a recipient.

Use *transport*_initial_destination_concurrency to specify a transport-specific override, where *transport* is the master.cf name of the message delivery transport (Postfix 2.5 and later).

Warning: with concurrency of 1, one bad message can be enough to block all mail to a site.

internal_mail_filter_classes (default: empty)

What categories of Postfix-generated mail are subject to before-queue content inspection by non_smtpd_milters, header_checks and body_checks. Specify zero or more of the following, separated by whitespace or comma.

bounce Inspect the content of delivery status notifications.

notify Inspect the content of postmaster notifications by the **smtp(8)** and **smtpd(8)** processes.

NOTE: It's generally not safe to enable content inspection of Postfix-generated email messages. The user is warned.

This feature is available in Postfix 2.3 and later.

invalid_hostname_reject_code (default: 501)

The numerical Postfix SMTP server response code when the client HELO or EHLO command parameter is rejected by the reject_invalid_helo_hostname restriction.

Do not change this unless you have a complete understanding of RFC 5321.

ipc_idle (default: version dependent)

The time after which a client closes an idle internal communication channel. The purpose is to allow Postfix daemon processes to terminate voluntarily after they become idle. This is used, for example, by the Postfix address resolving and rewriting clients.

With Postfix 2.4 the default value was reduced from 100s to 5s.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

ipc_timeout (default: 3600s)

The time limit for sending or receiving information over an internal communication channel. The purpose is to break out of deadlock situations. If the time limit is exceeded the software aborts with a fatal error.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

ipc_ttl (default: 1000s)

The time after which a client closes an active internal communication channel. The purpose is to allow Postfix daemon processes to terminate voluntarily after reaching their client limit. This is used, for example, by the Postfix address resolving and rewriting clients.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.1 and later.

line_length_limit (default: 2048)
Upon input, long lines are chopped up into pieces of at most this length; upon delivery, long lines are reconstructed.

lmdb_map_size (default: 16777216)
The initial OpenLDAP LMDB database size limit in bytes. Each time a database becomes full, its size limit is doubled.

This feature is available in Postfix 2.11 and later.

lmtp_address_preference (default: ipv6)
The LMTP-specific version of the smtp_address_preference configuration parameter. See there for details.

This feature is available in Postfix 2.8 and later.

lmtp_address_verify_target (default: rcpt)
The LMTP-specific version of the smtp_address_verify_target configuration parameter. See there for details.

This feature is available in Postfix 3.0 and later.

lmtp_assume_final (default: no)
When a remote LMTP server announces no DSN support, assume that the server performs final delivery, and send "delivered" delivery status notifications instead of "relayed". The default setting is backwards compatible to avoid the infinitesimal possibility of breaking existing LMTP-based content filters.

lmtp_bind_address (default: empty)
The LMTP-specific version of the smtp_bind_address configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_bind_address6 (default: empty)
The LMTP-specific version of the smtp_bind_address6 configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_body_checks (default: empty)
The LMTP-specific version of the smtp_body_checks configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_cache_connection (default: yes)
Keep Postfix LMTP client connections open for up to $max_idle seconds. When the LMTP client receives a request for the same connection the connection is reused.

This parameter is available in Postfix version 2.2 and earlier. With Postfix version 2.3 and later, see lmtp_connection_cache_on_demand, lmtp_connection_cache_destinations, or lmtp_connection_reuse_time_limit.

The effectiveness of cached connections will be determined by the number of remote LMTP servers in use, and the concurrency limit specified for the Postfix LMTP client. Cached connections are closed under any of the following conditions:

- The Postfix LMTP client idle time limit is reached. This limit is specified with the Postfix max_idle configuration parameter.
- A delivery request specifies a different destination than the one currently cached.
- The per-process limit on the number of delivery requests is reached. This limit is specified with the Postfix max_use configuration parameter.
- Upon the onset of another delivery request, the remote LMTP server associated with the current session does not respond to the RSET command.

Most of these limitations have been with the Postfix a connection cache that is shared among multiple LMTP client programs.

lmtp_cname_overrides_servername (default: yes)
The LMTP-specific version of the smtp_cname_overrides_servername configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_connect_timeout (default: 0s)
The Postfix LMTP client time limit for completing a TCP connection, or zero (use the operating system built-in time limit). When no connection can be made within the deadline, the LMTP client tries the next address on the mail exchanger list.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

Example:

```
lmtp_connect_timeout = 30s
```

lmtp_connection_cache_destinations (default: empty)
The LMTP-specific version of the smtp_connection_cache_destinations configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_connection_cache_on_demand (default: yes)
The LMTP-specific version of the smtp_connection_cache_on_demand configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_connection_cache_time_limit (default: 2s)
The LMTP-specific version of the smtp_connection_cache_time_limit configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_connection_reuse_count_limit (default: 0)
The LMTP-specific version of the smtp_connection_reuse_count_limit configuration parameter. See there for details.

This feature is available in Postfix 2.11 and later.

lmtp_connection_reuse_time_limit (default: 300s)
The LMTP-specific version of the smtp_connection_reuse_time_limit configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_data_done_timeout (default: 600s)
The Postfix LMTP client time limit for sending the LMTP ".", and for receiving the remote LMTP server response. When no response is received within the deadline, a warning is logged that the mail may be delivered multiple times.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_data_init_timeout (default: 120s)
The Postfix LMTP client time limit for sending the LMTP DATA command, and for receiving the remote LMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_data_xfer_timeout (default: 180s)
The Postfix LMTP client time limit for sending the LMTP message content. When the connection stalls for more than $lmtp_data_xfer_timeout the LMTP client terminates the transfer.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_defer_if_no_mx_address_found (default: no)
The LMTP-specific version of the smtp_defer_if_no_mx_address_found configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_delivery_status_filter (default: empty)
The LMTP-specific version of the smtp_delivery_status_filter configuration parameter. See there for details.

This feature is available in Postfix 3.0 and later.

lmtp_destination_concurrency_limit (default: $default_destination_concurrency_limit)
The maximal number of parallel deliveries to the same destination via the lmtp message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

lmtp_destination_recipient_limit (default: $default_destination_recipient_limit)
The maximal number of recipients per message for the lmtp message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

Setting this parameter to a value of 1 changes the meaning of lmtp_destination_concurrency_limit from concurrency per domain into concurrency per recipient.

lmtp_discard_lhlo_keyword_address_maps (default: empty)
Lookup tables, indexed by the remote LMTP server address, with case insensitive lists of LHLO keywords (pipelining, starttls, auth, etc.) that the Postfix LMTP client will ignore in the LHLO response from a remote LMTP server. See lmtp_discard_lhlo_keywords for details. The table is not indexed by hostname for consistency with smtpd_discard_ehlo_keyword_address_maps.

This feature is available in Postfix 2.3 and later.

lmtp_discard_lhlo_keywords (default: empty)
A case insensitive list of LHLO keywords (pipelining, starttls, auth, etc.) that the Postfix LMTP client will ignore in the LHLO response from a remote LMTP server.

This feature is available in Postfix 2.3 and later.

Notes:

- Specify the **silent-discard** pseudo keyword to prevent this action from being logged.
- Use the lmtp_discard_lhlo_keyword_address_maps feature to discard LHLO keywords selectively.

lmtp_dns_reply_filter (default: empty)
Optional filter for Postfix LMTP client DNS lookup results. See smtp_dns_reply_filter for details including an example.

This feature is available in Postfix 3.0 and later.

lmtp_dns_resolver_options (default: empty)
The LMTP-specific version of the smtp_dns_resolver_options configuration parameter. See there for details.

This feature is available in Postfix 2.8 and later.

lmtp_dns_support_level (default: empty)
The LMTP-specific version of the smtp_dns_support_level configuration parameter. See there for details.

This feature is available in Postfix 2.11 and later.

lmtp_enforce_tls (default: no)
The LMTP-specific version of the smtp_enforce_tls configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_fallback_relay (default: empty)
Optional list of relay hosts for LMTP destinations that can't be found or that are unreachable. In main.cf elements are separated by whitespace or commas.

By default, mail is returned to the sender when a destination is not found, and delivery is deferred when a destination is unreachable.

The fallback relays must be TCP destinations, specified without a leading "inet:" prefix. Specify a host or host:port. Since MX lookups do not apply with LMTP, there is no need to use the "[host]" or "[host]:port" forms. If you specify multiple LMTP destinations, Postfix will try them in the specified order.

This feature is available in Postfix 3.1 and later.

lmtp_generic_maps (default: empty)
The LMTP-specific version of the smtp_generic_maps configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_header_checks (default: empty)
The LMTP-specific version of the smtp_header_checks configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_host_lookup (default: dns)
The LMTP-specific version of the smtp_host_lookup configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_lhlo_name (default: $myhostname)
The hostname to send in the LMTP LHLO command.

The default value is the machine hostname. Specify a hostname or [ip.add.re.ss].

This information can be specified in the main.cf file for all LMTP clients, or it can be specified in the master.cf file for a specific client, for example:

```
/etc/postfix/master.cf:
mylmtp ... lmtp -o lmtp_lhlo_name=foo.bar.com
```

This feature is available in Postfix 2.3 and later.

lmtp_lhlo_timeout (default: 300s)
The Postfix LMTP client time limit for sending the LHLO command, and for receiving the initial remote LMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_line_length_limit (default: 990)
The LMTP-specific version of the smtp_line_length_limit configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_mail_timeout (default: 300s)
The Postfix LMTP client time limit for sending the MAIL FROM command, and for receiving the remote LMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_mime_header_checks (default: empty)
The LMTP-specific version of the smtp_mime_header_checks configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_mx_address_limit (default: 5)
The LMTP-specific version of the smtp_mx_address_limit configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_mx_session_limit (default: 2)
The LMTP-specific version of the smtp_mx_session_limit configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_nested_header_checks (default: empty)
The LMTP-specific version of the smtp_nested_header_checks configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_per_record_deadline (default: no)
The LMTP-specific version of the smtp_per_record_deadline configuration parameter. See there for details.

This feature is available in Postfix 2.9 and later.

lmtp_pix_workaround_delay_time (default: 10s)
The LMTP-specific version of the smtp_pix_workaround_delay_time configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_pix_workaround_maps (default: empty)
The LMTP-specific version of the smtp_pix_workaround_maps configuration parameter. See there for details.

This feature is available in Postfix 2.4 and later.

lmtp_pix_workaround_threshold_time (default: 500s)
The LMTP-specific version of the smtp_pix_workaround_threshold_time configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_pix_workarounds (default: empty)
The LMTP-specific version of the smtp_pix_workaround configuration parameter. See there for details.

This feature is available in Postfix 2.4 and later.

lmtp_quit_timeout (default: 300s)
The Postfix LMTP client time limit for sending the QUIT command, and for receiving the remote LMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_quote_rfc821_envelope (default: yes)
The LMTP-specific version of the smtp_quote_rfc821_envelope configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_randomize_addresses (default: yes)
The LMTP-specific version of the smtp_randomize_addresses configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_rcpt_timeout (default: 300s)
The Postfix LMTP client time limit for sending the RCPT TO command, and for receiving the remote LMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_reply_filter (default: empty)
The LMTP-specific version of the smtp_reply_filter configuration parameter. See there for details.

This feature is available in Postfix 2.7 and later.

lmtp_rset_timeout (default: 20s)
The Postfix LMTP client time limit for sending the RSET command, and for receiving the remote LMTP server response. The LMTP client sends RSET in order to finish a recipient address probe, or to verify that a cached connection is still alive.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

lmtp_sasl_auth_cache_name (default: empty)
The LMTP-specific version of the smtp_sasl_auth_cache_name configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_sasl_auth_cache_time (default: 90d)
The LMTP-specific version of the smtp_sasl_auth_cache_time configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_sasl_auth_enable (default: no)
Enable SASL authentication in the Postfix LMTP client.

lmtp_sasl_auth_soft_bounce (default: yes)
The LMTP-specific version of the smtp_sasl_auth_soft_bounce configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_sasl_mechanism_filter (default: empty)
The LMTP-specific version of the smtp_sasl_mechanism_filter configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_sasl_password_maps (default: empty)
Optional Postfix LMTP client lookup tables with one username:password entry per host or domain. If a remote host or domain has no username:password entry, then the Postfix LMTP client will not attempt to authenticate to the remote host.

lmtp_sasl_path (default: empty)
Implementation-specific information that is passed through to the SASL plug-in implementation that is selected with **lmtp_sasl_type**. Typically this specifies the name of a configuration file or rendezvous point.

This feature is available in Postfix 2.3 and later.

lmtp_sasl_security_options (default: noplaintext, noanonymous)
SASL security options; as of Postfix 2.3 the list of available features depends on the SASL client implementation that is selected with **lmtp_sasl_type**.

The following security features are defined for the **cyrus** client SASL implementation:

noplaintext
Disallow authentication methods that use plaintext passwords.

noactive
Disallow authentication methods that are vulnerable to non-dictionary active attacks.

nodictionary
Disallow authentication methods that are vulnerable to passive dictionary attack.

noanonymous
Disallow anonymous logins.

Example:

```
lmtp_sasl_security_options = noplaintext
```

lmtp_sasl_tls_security_options (default: $lmtp_sasl_security_options)
The LMTP-specific version of the smtp_sasl_tls_security_options configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_sasl_tls_verified_security_options (default: $lmtp_sasl_tls_security_options)
The LMTP-specific version of the smtp_sasl_tls_verified_security_options configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_sasl_type (default: cyrus)
The SASL plug-in type that the Postfix LMTP client should use for authentication. The available types are listed with the "**postconf -A**" command.

This feature is available in Postfix 2.3 and later.

lmtp_send_dummy_mail_auth (default: no)
The LMTP-specific version of the smtp_send_dummy_mail_auth configuration parameter. See there for details.

This feature is available in Postfix 2.9 and later.

lmtp_send_xforward_command (default: no)
Send an XFORWARD command to the remote LMTP server when the LMTP LHLO server response announces XFORWARD support. This allows an **lmtp(8)** delivery agent, used for content filter message injection, to forward the name, address, protocol and HELO name of the original client to the content filter and downstream queuing LMTP server. Before you change the value to yes, it is best to make sure that your content filter supports this command.

This feature is available in Postfix 2.1 and later.

lmtp_sender_dependent_authentication (default: no)
The LMTP-specific version of the smtp_sender_dependent_authentication configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_skip_5xx_greeting (default: yes)
The LMTP-specific version of the smtp_skip_5xx_greeting configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_skip_quit_response (default: no)
Wait for the response to the LMTP QUIT command.

lmtp_starttls_timeout (default: 300s)
The LMTP-specific version of the smtp_starttls_timeout configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tcp_port (default: 24)
The default TCP port that the Postfix LMTP client connects to.

lmtp_tls_CAfile (default: empty)
The LMTP-specific version of the smtp_tls_CAfile configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_CApath (default: empty)
The LMTP-specific version of the smtp_tls_CApath configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_block_early_mail_reply (default: empty)
The LMTP-specific version of the smtp_tls_block_early_mail_reply configuration parameter. See there for details.

This feature is available in Postfix 2.7 and later.

lmtp_tls_cert_file (default: empty)
The LMTP-specific version of the smtp_tls_cert_file configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_ciphers (default: medium)
The LMTP-specific version of the smtp_tls_ciphers configuration parameter. See there for details.

This feature is available in Postfix 2.6 and later.

lmtp_tls_dcert_file (default: empty)
The LMTP-specific version of the smtp_tls_dcert_file configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_dkey_file (default: $lmtp_tls_dcert_file)
The LMTP-specific version of the smtp_tls_dkey_file configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_eccert_file (default: empty)
The LMTP-specific version of the smtp_tls_eccert_file configuration parameter. See there for details.

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

lmtp_tls_eckey_file (default: empty)
The LMTP-specific version of the smtp_tls_eckey_file configuration parameter. See there for details.

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

lmtp_tls_enforce_peername (default: yes)
The LMTP-specific version of the smtp_tls_enforce_peername configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_exclude_ciphers (default: empty)
The LMTP-specific version of the smtp_tls_exclude_ciphers configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_fingerprint_cert_match (default: empty)
The LMTP-specific version of the smtp_tls_fingerprint_cert_match configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_tls_fingerprint_digest (default: md5)
The LMTP-specific version of the smtp_tls_fingerprint_digest configuration parameter. See there for details.

This feature is available in Postfix 2.5 and later.

lmtp_tls_force_insecure_host_tlsa_lookup (default: no)
The LMTP-specific version of the smtp_tls_force_insecure_host_tlsa_lookup configuration parameter. See there for details.

This feature is available in Postfix 2.11 and later.

lmtp_tls_key_file (default: $lmtp_tls_cert_file)
The LMTP-specific version of the smtp_tls_key_file configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_loglevel (default: 0)
The LMTP-specific version of the smtp_tls_loglevel configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_mandatory_ciphers (default: medium)
The LMTP-specific version of the smtp_tls_mandatory_ciphers configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_mandatory_exclude_ciphers (default: empty)
The LMTP-specific version of the smtp_tls_mandatory_exclude_ciphers configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_mandatory_protocols (default: !SSLv2, !SSLv3)
The LMTP-specific version of the smtp_tls_mandatory_protocols configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_note_starttls_offer (default: no)
The LMTP-specific version of the smtp_tls_note_starttls_offer configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_per_site (default: empty)
The LMTP-specific version of the smtp_tls_per_site configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_policy_maps (default: empty)
The LMTP-specific version of the smtp_tls_policy_maps configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_protocols (default: !SSLv2, !SSLv3)
The LMTP-specific version of the smtp_tls_protocols configuration parameter. See there for details.

This feature is available in Postfix 2.6 and later.

lmtp_tls_scert_verifydepth (default: 9)
The LMTP-specific version of the smtp_tls_scert_verifydepth configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_secure_cert_match (default: nexthop)
The LMTP-specific version of the smtp_tls_secure_cert_match configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_security_level (default: empty)
The LMTP-specific version of the smtp_tls_security_level configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_session_cache_database (default: empty)
The LMTP-specific version of the smtp_tls_session_cache_database configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_session_cache_timeout (default: 3600s)
The LMTP-specific version of the smtp_tls_session_cache_timeout configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_tls_trust_anchor_file (default: empty)
The LMTP-specific version of the smtp_tls_trust_anchor_file configuration parameter. See there for details.

This feature is available in Postfix 2.11 and later.

lmtp_tls_verify_cert_match (default: hostname)
The LMTP-specific version of the smtp_tls_verify_cert_match configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_use_tls (default: no)
The LMTP-specific version of the smtp_use_tls configuration parameter. See there for details.

This feature is available in Postfix 2.3 and later.

lmtp_xforward_timeout (default: 300s)
The Postfix LMTP client time limit for sending the XFORWARD command, and for receiving the remote LMTP server response.

In case of problems the client does NOT try the next address on the mail exchanger list.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.1 and later.

local_command_shell (default: empty)
Optional shell program for **local(8)** delivery to non-Postfix command. By default, non-Postfix commands are executed directly; commands are given to given to the default shell (typically, /bin/sh) only when they contain shell meta characters or shell built-in commands.

"sendmail's restricted shell" (smrsh) is what most people will use in order to restrict what programs can be run from e.g. .forward files (smrsh is part of the Sendmail distribution).

Note: when a shell program is specified, it is invoked even when the command contains no shell built-in commands or meta characters.

Example:

```
local_command_shell = /some/where/smrsh -c
local_command_shell = /bin/bash -c
```

local_delivery_status_filter (default: $default_delivery_status_filter)
Optional filter for the **local(8)** delivery agent to change the status code or explanatory text of successful or unsuccessful deliveries. See default_delivery_status_filter for details.

This feature is available in Postfix 3.0 and later.

local_destination_concurrency_limit (default: 2)
The maximal number of parallel deliveries via the local mail delivery transport to the same recipient (when "local_destination_recipient_limit = 1") or the maximal number of parallel deliveries to the same local domain (when "local_destination_recipient_limit > 1"). This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

A low limit of 2 is recommended, just in case someone has an expensive shell command in a .forward file or in an alias (e.g., a mailing list manager). You don't want to run lots of those at the same time.

local_destination_recipient_limit (default: 1)
The maximal number of recipients per message delivery via the local mail delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

Setting this parameter to a value > 1 changes the meaning of local_destination_concurrency_limit from concurrency per recipient into concurrency per domain.

local_header_rewrite_clients (default: permit_inet_interfaces)

Rewrite message header addresses in mail from these clients and update incomplete addresses with the domain name in $myorigin or $mydomain; either don't rewrite message headers from other clients at all, or rewrite message headers and update incomplete addresses with the domain specified in the remote_header_rewrite_domain parameter.

See the append_at_myorigin and append_dot_mydomain parameters for details of how domain names are appended to incomplete addresses.

Specify a list of zero or more of the following:

permit_inet_interfaces

Append the domain name in $myorigin or $mydomain when the client IP address matches $inet_interfaces. This is enabled by default.

permit_mynetworks

Append the domain name in $myorigin or $mydomain when the client IP address matches any network or network address listed in $mynetworks. This setting will not prevent remote mail header address rewriting when mail from a remote client is forwarded by a neighboring system.

permit_sasl_authenticated

Append the domain name in $myorigin or $mydomain when the client is successfully authenticated via the RFC 4954 (AUTH) protocol.

permit_tls_clientcerts

Append the domain name in $myorigin or $mydomain when the remote SMTP client TLS certificate fingerprint or public key fingerprint (Postfix 2.9 and later) is listed in $relay_clientcerts. The fingerprint digest algorithm is configurable via the smtpd_tls_fingerprint_digest parameter (hard-coded as md5 prior to Postfix version 2.5).

permit_tls_all_clientcerts

Append the domain name in $myorigin or $mydomain when the remote SMTP client TLS certificate is successfully verified, regardless of whether it is listed on the server, and regardless of the certifying authority.

check_address_map *type:table*

type:table

Append the domain name in $myorigin or $mydomain when the client IP address matches the specified lookup table. The lookup result is ignored, and no subnet lookup is done. This is suitable for, e.g., pop-before-smtp lookup tables.

Examples:

The Postfix < 2.2 backwards compatible setting: always rewrite message headers, and always append my own domain to incomplete header addresses.

```
local_header_rewrite_clients = static:all
```

The purist (and default) setting: rewrite headers only in mail from Postfix sendmail and in SMTP mail from this machine.

```
local_header_rewrite_clients = permit_inet_interfaces
```

The intermediate setting: rewrite header addresses and append $myorigin or $mydomain information only with mail from Postfix sendmail, from local clients, or from authorized SMTP clients.

Note: this setting will not prevent remote mail header address rewriting when mail from a remote client is forwarded by a neighboring system.

```
local_header_rewrite_clients = permit_mynetworks,
permit_sasl_authenticated permit_tls_clientcerts
```

```
check_address_map hash:/etc/postfix/pop-before-smtp
```

local_recipient_maps (default: proxy:unix:passwd.byname $alias_maps)

Lookup tables with all names or addresses of local recipients: a recipient address is local when its domain matches $mydestination, $inet_interfaces or $proxy_interfaces. Specify @domain as a wild-card for domains that do not have a valid recipient list. Technically, tables listed with $local_recipient_maps are used as lists: Postfix needs to know only if a lookup string is found or not, but it does not use the result from table lookup.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

If this parameter is non-empty (the default), then the Postfix SMTP server will reject mail for unknown local users.

To turn off local recipient checking in the Postfix SMTP server, specify "local_recipient_maps =" (i.e. empty).

The default setting assumes that you use the default Postfix local delivery agent for local delivery. You need to update the local_recipient_maps setting if:

- You redefine the local delivery agent in master.cf.
- You redefine the "local_transport" setting in main.cf.
- You use the "luser_relay", "mailbox_transport", or "fallback_transport" feature of the Postfix **local(8)** delivery agent.

Details are described in the LOCAL_RECIPIENT_README file.

Beware: if the Postfix SMTP server runs chrooted, you need to access the passwd file via the **proxymap(8)** service, in order to overcome chroot access restrictions. The alternative, maintaining a copy of the system password file in the chroot jail is not practical.

Examples:

```
local_recipient_maps =
```

local_transport (default: local:$myhostname)

The default mail delivery transport and next-hop destination for final delivery to domains listed with mydestination, and for [ipaddress] destinations that match $inet_interfaces or $proxy_interfaces. This information can be overruled with the **transport(5)** table.

By default, local mail is delivered to the transport called "local", which is just the name of a service that is defined the master.cf file.

Specify a string of the form *transport:nexthop*, where *transport* is the name of a mail delivery transport defined in master.cf. The*:ne xthop* destination is optional; its syntax is documented in the manual page of the corresponding delivery agent.

Beware: if you override the default local delivery agent then you need to review the LOCAL_RECIPIENT_README document, otherwise the SMTP server may reject mail for local recipients.

luser_relay (default: empty)

Optional catch-all destination for unknown **local(8)** recipients. By default, mail for unknown recipients in domains that match $mydestination, $inet_interfaces or $proxy_interfaces is returned as undeliverable.

The following $name expansions are done on luser_relay:

$domain
The recipient domain.

$extension
The recipient address extension.

$home The recipient's home directory.

$local The entire recipient address localpart.

$recipient
The full recipient address.

$recipient_delimiter
The address extension delimiter that was found in the recipient address (Postfix 2.11 and later), or the system-wide recipient address extension delimiter (Postfix 2.10 and earlier).

$shell The recipient's login shell.

$user The recipient username.

${name?value}
Expands to *value* when *$name* has a non-empty value.

${name:value}
Expands to *value* when *$name* has an empty value.

Instead of $name you can also specify ${name} or $(name).

Note: luser_relay works only for the Postfix **local(8)** delivery agent.

Note: if you use this feature for accounts not in the UNIX password file, then you must specify "local_recipient_maps =" (i.e. empty) in the main.cf file, otherwise the Postfix SMTP server will reject mail for non-UNIX accounts with "User unknown in local recipient table".

Examples:

```
luser_relay = $user@other.host
luser_relay = $local@other.host
luser_relay = admin+$local
```

mail_name (default: Postfix)
The mail system name that is displayed in Received: headers, in the SMTP greeting banner, and in bounced mail.

mail_owner (default: postfix)
The UNIX system account that owns the Postfix queue and most Postfix daemon processes. Specify the name of an unprivileged user account that does not share a user or group ID with other accounts, and that owns no other files or processes on the system. In particular, don't specify nobody or daemon. PLEASE USE A DEDICATED USER ID AND GROUP ID.

When this parameter value is changed you need to re-run "**postfix set-permissions**" (with Postfix version 2.0 and earlier: "**/etc/postfix/post-install set-permissions**".

mail_release_date (default: see postconf −d output)
The Postfix release date, in "YYYYMMDD" format.

mail_spool_directory (default: see postconf −d output)
The directory where **local(8)** UNIX-style mailboxes are kept. The default setting depends on the system type. Specify a name ending in / for maildir-style delivery.

Note: maildir delivery is done with the privileges of the recipient. If you use the mail_spool_directory setting for maildir style delivery, then you must create the top-level maildir directory in advance. Postfix will not create it.

Examples:

```
mail_spool_directory = /var/mail
mail_spool_directory = /var/spool/mail
```

mail_version (default: see postconf −d output)
The version of the mail system. Stable releases are named *major.minor.patchlevel*. Experimental releases also include the release date. The version string can be used in, for example, the SMTP greeting banner.

mailbox_command (default: empty)

Optional external command that the **local(8)** delivery agent should use for mailbox delivery. The command is run with the user ID and the primary group ID privileges of the recipient. Exception: command delivery for root executes with $default_privs privileges. This is not a problem, because 1) mail for root should always be aliased to a real user and 2) don't log in as root, use "su" instead.

The following environment variables are exported to the command:

CLIENT_ADDRESS
Remote client network address. Available in Postfix version 2.2 and later.

CLIENT_HELO
Remote client EHLO command parameter. Available in Postfix version 2.2 and later.

CLIENT_HOSTNAME
Remote client hostname. Available in Postfix version 2.2 and later.

CLIENT_PROTOCOL
Remote client protocol. Available in Postfix version 2.2 and later.

DOMAIN
The domain part of the recipient address.

EXTENSION
The optional address extension.

HOME
The recipient home directory.

LOCAL
The recipient address localpart.

LOGNAME
The recipient's username.

ORIGINAL_RECIPIENT
The entire recipient address, before any address rewriting or aliasing.

RECIPIENT
The full recipient address.

SASL_METHOD
SASL authentication method specified in the remote client AUTH command. Available in Postfix version 2.2 and later.

SASL_SENDER
SASL sender address specified in the remote client MAIL FROM command. Available in Postfix version 2.2 and later.

SASL_USER
SASL username specified in the remote client AUTH command. Available in Postfix version 2.2 and later.

SENDER
The full sender address.

SHELL
The recipient's login shell.

USER The recipient username.

Unlike other Postfix configuration parameters, the mailbox_command parameter is not subjected to $name substitutions. This is to make it easier to specify shell syntax (see example below).

If you can, avoid shell meta characters because they will force Postfix to run an expensive shell process. If you're delivering via Procmail then running a shell won't make a noticeable difference in the total cost.

Note: if you use the mailbox_command feature to deliver mail system-wide, you must set up an alias that forwards mail for root to a real user.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

Examples:

```
mailbox_command = /some/where/procmail
mailbox_command = /some/where/procmail -a "$EXTENSION"
mailbox_command = /some/where/maildrop -d "$USER"
-f "$SENDER" "$EXTENSION"
```

mailbox_command_maps (default: empty)

Optional lookup tables with per-recipient external commands to use for **local(8)** mailbox delivery. Behavior is as with mailbox_command.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

mailbox_delivery_lock (default: see postconf −d output)

How to lock a UNIX-style **local(8)** mailbox before attempting delivery. For a list of available file locking methods, use the "**postconf -l**" command.

This setting is ignored with **maildir** style delivery, because such deliveries are safe without explicit locks.

Note: The **dotlock** method requires that the recipient UID or GID has write access to the parent directory of the mailbox file.

Note: the default setting of this parameter is system dependent.

mailbox_size_limit (default: 51200000)

The maximal size of any **local(8)** individual mailbox or maildir file, or zero (no limit). In fact, this limits the size of any file that is written to upon local delivery, including files written by external commands that are executed by the **local(8)** delivery agent.

This limit must not be smaller than the message size limit.

mailbox_transport (default: empty)

Optional message delivery transport that the **local(8)** delivery agent should use for mailbox delivery to all local recipients, whether or not they are found in the UNIX passwd database.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

mailbox_transport_maps (default: empty)

Optional lookup tables with per-recipient message delivery transports to use for **local(8)** mailbox delivery, whether or not the recipients are found in the UNIX passwd database.

The precedence of **local(8)** delivery features from high to low is: aliases, .forward files, mailbox_transport_maps, mailbox_transport, mailbox_command_maps, mailbox_command, home_mailbox, mail_spool_directory, fallback_transport_maps, fallback_transport and luser_relay.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

For safety reasons, this feature does not allow $number substitutions in regular expression maps.

This feature is available in Postfix 2.3 and later.

mailq_path (default: see postconf −d output)
Sendmail compatibility feature that specifies where the Postfix **mailq(1)** command is installed. This command can be used to list the Postfix mail queue.

manpage_directory (default: see postconf −d output)
Where the Postfix manual pages are installed.

maps_rbl_domains (default: empty)
Obsolete feature: use the reject_rbl_client feature instead.

maps_rbl_reject_code (default: 554)
The numerical Postfix SMTP server response code when a remote SMTP client request is blocked by the reject_rbl_client, reject_rhsbl_client, reject_rhsbl_reverse_client, reject_rhsbl_sender or reject_rhsbl_recipient restriction.

Do not change this unless you have a complete understanding of RFC 5321.

masquerade_classes (default: envelope_sender, header_sender, header_recipient)
What addresses are subject to address masquerading.

By default, address masquerading is limited to envelope sender addresses, and to header sender and header recipient addresses. This allows you to use address masquerading on a mail gateway while still being able to forward mail to users on individual machines.

Specify zero or more of: envelope_sender, envelope_recipient, header_sender, header_recipient

masquerade_domains (default: empty)
Optional list of domains whose subdomain structure will be stripped off in email addresses.

The list is processed left to right, and processing stops at the first match. Thus,

```
masquerade_domains = foo.example.com example.com
```

strips "user@any.thing.foo.example.com" to "user@foo.example.com", but strips "user@any.thing.else.example.com" to "user@example.com".

A domain name prefixed with ! means do not masquerade this domain or its subdomains. Thus,

```
masquerade_domains = !foo.example.com example.com
```

does not change "user@any.thing.foo.example.com" or "user@foo.example.com", but strips "user@any.thing.else.example.com" to "user@example.com".

Note: with Postfix version 2.2, message header address masquerading happens only when message header address rewriting is enabled:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

Example:

```
masquerade_domains = $mydomain
```

masquerade_exceptions (default: empty)
Optional list of user names that are not subjected to address masquerading, even when their address matches $masquerade_domains.

By default, address masquerading makes no exceptions.

Specify a list of user names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. The list is matched left to right, and the search stops on the first match. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a

name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Examples:

```
masquerade_exceptions = root, mailer-daemon
masquerade_exceptions = root
```

master_service_disable (default: empty)

Selectively disable **master(8)** listener ports by service type or by service name and type. Specify a list of service types ("inet", "unix", "fifo", or "pass") or "name/type" tuples, where "name" is the first field of a master.cf entry and "type" is a service type. As with other Postfix matchlists, a search stops at the first match. Specify "!pattern" to exclude a service from the list. By default, all **master(8)** listener ports are enabled.

Note: this feature does not support "/file/name" or "type:table" patterns, nor does it support wildcards such as "*" or "all". This is intentional.

Examples:

```
# With Postfix 2.6..2.10 use '.' instead of '/'.
# Turn on all master(8)
listener ports (the default).
master_service_disable =
# Turn off only the main SMTP listener port.
master_service_disable = smtp/inet
# Turn off all TCP/IP listener ports.
master_service_disable = inet
# Turn off all TCP/IP listener ports except "foo".
master_service_disable = !foo/inet, inet
```

This feature is available in Postfix 2.6 and later.

max_idle (default: 100s)

The maximum amount of time that an idle Postfix daemon process waits for an incoming connection before terminating voluntarily. This parameter is ignored by the Postfix queue manager and by other long-lived Postfix daemon processes.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

max_use (default: 100)

The maximal number of incoming connections that a Postfix daemon process will service before terminating voluntarily. This parameter is ignored by the Postfix queue manager and by other long-lived Postfix daemon processes.

maximal_backoff_time (default: 4000s)

The maximal time between attempts to deliver a deferred message.

This parameter should be set to a value greater than or equal to $minimal_backoff_time. See also $queue_run_delay.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

maximal_queue_lifetime (default: 5d)

Consider a message as undeliverable, when delivery fails with a temporary error, and the time in the queue has reached the maximal_queue_lifetime limit.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is d (days).

Specify 0 when mail delivery should be tried only once.

message_drop_headers (default: bcc, content−length, resent−bcc, return−path)

Names of message headers that the **cleanup(8)** daemon will remove after applying **header_checks(5)** and before invoking Milter applications. The default setting is compatible with Postfix < 3.0.

Specify a list of header names, separated by comma or space. Names are matched in a case-insensitive

manner. The list of supported header names is limited only by available memory.

This feature is available in Postfix 3.0 and later.

message_reject_characters (default: empty)

The set of characters that Postfix will reject in message content. The usual C-like escape sequences are recognized: \a \b \f \n \r \t \v *ddd* (up to three octal digits) and \\.

Note 1: this feature does not recognize text that requires MIME decoding. It inspects raw message content, just like header_checks and body_checks.

Note 2: this feature is disabled with "receive_override_options = no_header_body_checks".

Example:

```
message_reject_characters = \0
```

This feature is available in Postfix 2.3 and later.

message_size_limit (default: 10240000)

The maximal size in bytes of a message, including envelope information.

Note: be careful when making changes. Excessively small values will result in the loss of non-delivery notifications, when a bounce message size exceeds the local or remote MTA's message size limit.

message_strip_characters (default: empty)

The set of characters that Postfix will remove from message content. The usual C-like escape sequences are recognized: \a \b \f \n \r \t \v *ddd* (up to three octal digits) and \\.

Note 1: this feature does not recognize text that requires MIME decoding. It inspects raw message content, just like header_checks and body_checks.

Note 2: this feature is disabled with "receive_override_options = no_header_body_checks".

Example:

```
message_strip_characters = \0
```

This feature is available in Postfix 2.3 and later.

meta_directory (default: see 'postconf −d' output)

The location of non-executable files that are shared among multiple Postfix instances, such as postfix-files, dynamicmaps.cf, and the multi-instance template files main.cf.proto and master.cf.proto. This directory should contain only Postfix-related files. Typically, the meta_directory parameter has the same default as the config_directory parameter (/etc/postfix or /usr/local/etc/postfix).

For backwards compatibility with Postfix versions 2.6..2.11, specify "meta_directory = $daemon_directory" in main.cf before installing or upgrading Postfix, or specify "meta_directory = /path/name" on the "make makefiles", "make install" or "make upgrade" command line.

This feature is available in Postfix 3.0 and later.

milter_command_timeout (default: 30s)

The time limit for sending an SMTP command to a Milter (mail filter) application, and for receiving the response.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.3 and later.

milter_connect_macros (default: see postconf −d output)

The macros that are sent to Milter (mail filter) applications after completion of an SMTP connection. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_connect_timeout (default: 30s)
The time limit for connecting to a Milter (mail filter) application, and for negotiating protocol options.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.3 and later.

milter_content_timeout (default: 300s)
The time limit for sending message content to a Milter (mail filter) application, and for receiving the response.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.3 and later.

milter_data_macros (default: see postconf −d output)
The macros that are sent to version 4 or higher Milter (mail filter) applications after the SMTP DATA command. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_default_action (default: tempfail)
The default action when a Milter (mail filter) application is unavailable or mis-configured. Specify one of the following:

accept Proceed as if the mail filter was not present.

reject Reject all further commands in this session with a permanent status code.

tempfail
Reject all further commands in this session with a temporary status code.

quarantine
Like "accept", but freeze the message in the "hold" queue. Available with Postfix 2.6 and later.

This feature is available in Postfix 2.3 and later.

milter_end_of_data_macros (default: see postconf −d output)
The macros that are sent to Milter (mail filter) applications after the message end-of-data. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_end_of_header_macros (default: see postconf −d output)
The macros that are sent to Milter (mail filter) applications after the end of the message header. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.5 and later.

milter_header_checks (default: empty)
Optional lookup tables for content inspection of message headers that are produced by Milter applications. See the **header_checks(5)** manual page available actions. Currently, PREPEND is not implemented.

The following example sends all mail that is marked as SPAM to a spam handling machine. Note that matches are case-insensitive by default.

```
/etc/postfix/main.cf:
milter_header_checks = pcre:/etc/postfix/milter_header_checks

/etc/postfix/milter_header_checks:
/^X-SPAM-FLAG:\s+YES/ FILTER mysmtp:sanitizer.example.com:25
```

The milter_header_checks mechanism could also be used for whitelisting. For example it could be used to

skip heavy content inspection for DKIM-signed mail from known friendly domains.

This feature is available in Postfix 2.7, and as an optional patch for Postfix 2.6.

milter_helo_macros (default: see postconf −d output)
The macros that are sent to Milter (mail filter) applications after the SMTP HELO or EHLO command. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_macro_daemon_name (default: $myhostname)
The {daemon_name} macro value for Milter (mail filter) applications. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_macro_defaults (default: empty)
Optional list of *name=value* pairs that specify default values for arbitrary macros that Postfix may send to Milter applications. These defaults are used when there is no corresponding information from the message delivery context.

Specify *name=value* or *{name}=value* pairs separated by comma or whitespace. Enclose a pair in "{}" when a value contains comma or whitespace (this form ignores whitespace after the enclosing "{", around the "=", and before the enclosing "}").

This feature is available in Postfix 3.1 and later.

milter_macro_v (default: $mail_name $mail_version)
The {v} macro value for Milter (mail filter) applications. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_mail_macros (default: see postconf −d output)
The macros that are sent to Milter (mail filter) applications after the SMTP MAIL FROM command. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_protocol (default: 6)
The mail filter protocol version and optional protocol extensions for communication with a Milter application; prior to Postfix 2.6 the default protocol is 2. Postfix sends this version number during the initial protocol handshake. It should match the version number that is expected by the mail filter application (or by its Milter library).

Protocol versions:

2 Use Sendmail 8 mail filter protocol version 2 (default with Sendmail version 8.11 .. 8.13 and Postfix version 2.3 .. 2.5).

3 Use Sendmail 8 mail filter protocol version 3.

4 Use Sendmail 8 mail filter protocol version 4.

6 Use Sendmail 8 mail filter protocol version 6 (default with Sendmail version 8.14 and Postfix version 2.6).

Protocol extensions:

no_header_reply
Specify this when the Milter application will not reply for each individual message header.

This feature is available in Postfix 2.3 and later.

milter_rcpt_macros (default: see postconf −d output)
The macros that are sent to Milter (mail filter) applications after the SMTP RCPT TO command. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

milter_unknown_command_macros (default: see postconf −d output)
The macros that are sent to version 3 or higher Milter (mail filter) applications after an unknown SMTP command. See MILTER_README for a list of available macro names and their meanings.

This feature is available in Postfix 2.3 and later.

mime_boundary_length_limit (default: 2048)
The maximal length of MIME multipart boundary strings. The MIME processor is unable to distinguish between boundary strings that do not differ in the first $mime_boundary_length_limit characters.

This feature is available in Postfix 2.0 and later.

mime_header_checks (default: $header_checks)
Optional lookup tables for content inspection of MIME related message headers, as described in the **header_checks(5)** manual page.

This feature is available in Postfix 2.0 and later.

mime_nesting_limit (default: 100)
The maximal recursion level that the MIME processor will handle. Postfix refuses mail that is nested deeper than the specified limit.

This feature is available in Postfix 2.0 and later.

minimal_backoff_time (default: 300s)
The minimal time between attempts to deliver a deferred message; prior to Postfix 2.4 the default value was 1000s.

This parameter also limits the time an unreachable destination is kept in the short-term, in-memory, destination status cache.

This parameter should be set greater than or equal to $queue_run_delay. See also $maximal_backoff_time.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

multi_instance_directories (default: empty)
An optional list of non-default Postfix configuration directories; these directories belong to additional Postfix instances that share the Postfix executable files and documentation with the default Postfix instance, and that are started, stopped, etc., together with the default Postfix instance. Specify a list of pathnames separated by comma or whitespace.

When $multi_instance_directories is empty, the **postfix(1)** command runs in single-instance mode and operates on a single Postfix instance only. Otherwise, the **postfix(1)** command runs in multi-instance mode and invokes the multi-instance manager specified with the multi_instance_wrapper parameter. The multi-instance manager in turn executes **postfix(1)** commands for the default instance and for all Postfix instances in $multi_instance_directories.

Currently, this parameter setting is ignored except for the default main.cf file.

This feature is available in Postfix 2.6 and later.

multi_instance_enable (default: no)
Allow this Postfix instance to be started, stopped, etc., by a multi-instance manager. By default, new instances are created in a safe state that prevents them from being started inadvertently. This parameter is reserved for the multi-instance manager.

This feature is available in Postfix 2.6 and later.

multi_instance_group (default: empty)
The optional instance group name of this Postfix instance. A group identifies closely-related Postfix instances that the multi-instance manager can start, stop, etc., as a unit. This parameter is reserved for the multi-instance manager.

This feature is available in Postfix 2.6 and later.

multi_instance_name (default: empty)
The optional instance name of this Postfix instance. This name becomes also the default value for the syslog_name parameter.

This feature is available in Postfix 2.6 and later.

multi_instance_wrapper (default: empty)
The pathname of a multi-instance manager command that the **postfix(1)** command invokes when the multi_instance_directories parameter value is non-empty. The pathname may be followed by initial command arguments separated by whitespace; shell metacharacters such as quotes are not supported in this context.

The **postfix(1)** command invokes the manager command with the **postfix(1)** non-option command arguments on the manager command line, and with all installation configuration parameters exported into the manager command process environment. The manager command in turn invokes the **postfix(1)** command for individual Postfix instances as "postfix -c *config_directory command*".

This feature is available in Postfix 2.6 and later.

multi_recipient_bounce_reject_code (default: 550)
The numerical Postfix SMTP server response code when a remote SMTP client request is blocked by the reject_multi_recipient_bounce restriction.

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.1 and later.

mydestination (default: $myhostname, localhost.$mydomain, localhost)
The list of domains that are delivered via the $local_transport mail delivery transport. By default this is the Postfix **local(8)** delivery agent which looks up all recipients in /etc/passwd and /etc/aliases. The SMTP server validates recipient addresses with $local_recipient_maps and rejects non-existent recipients. See also the local domain class in the ADDRESS_CLASS_README file.

The default mydestination value specifies names for the local machine only. On a mail domain gateway, you should also include $mydomain.

The $local_transport delivery method is also selected for mail addressed to user@[the.net.work.address] of the mail system (the IP addresses specified with the inet_interfaces and proxy_interfaces parameters).

Warnings:

- Do not specify the names of virtual domains - those domains are specified elsewhere. See VIRTUAL_README for more information.
- Do not specify the names of domains that this machine is backup MX host for. See STANDARD_CONFIGURATION_README for how to set up backup MX hosts.
- By default, the Postfix SMTP server rejects mail for recipients not listed with the local_recipient_maps parameter. See the **postconf(5)** manual for a description of the local_recipient_maps and unknown_local_recipient_reject_code parameters.

Specify a list of host or domain names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace.

Examples:

```
mydestination = $myhostname, localhost.$mydomain $mydomain
mydestination = $myhostname, localhost.$mydomain www.$mydomain, ftp.$mydomain
```

mydomain (default: see postconf −d output)
The internet domain name of this mail system. The default is to use $myhostname minus the first component, or "localdomain" (Postfix 2.3 and later). $mydomain is used as a default value for many other configuration parameters.

Example:

```
mydomain = domain.tld
```

myhostname (default: see postconf −d output)

The internet hostname of this mail system. The default is to use the fully-qualified domain name (FQDN) from gethostname(), or to use the non-FQDN result from gethostname() and append ".$mydomain". $myhostname is used as a default value for many other configuration parameters.

Example:

```
myhostname = host.example.com
```

mynetworks (default: see postconf −d output)

The list of "trusted" remote SMTP clients that have more privileges than "strangers".

In particular, "trusted" SMTP clients are allowed to relay mail through Postfix. See the smtpd_relay_restrictions parameter description in the **postconf(5)** manual.

You can specify the list of "trusted" network addresses by hand or you can let Postfix do it for you (which is the default). See the description of the mynetworks_style parameter for more information.

If you specify the mynetworks list by hand, Postfix ignores the mynetworks_style setting.

Specify a list of network addresses or network/netmask patterns, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace.

The netmask specifies the number of bits in the network part of a host address. You can also specify "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored).

The list is matched left to right, and the search stops on the first match. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note 1: Pattern matching of domain names is controlled by the or absence of "mynetworks" in the parent_domain_matches_subdomains parameter value.

Note 2: IP version 6 address information must be specified inside [] in the mynetworks value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

Examples:

```
mynetworks = 127.0.0.0/8 168.100.189.0/28
mynetworks = !192.168.0.1, 192.168.0.0/28
mynetworks = 127.0.0.0/8 168.100.189.0/28 [::1]/128 [2001:240:587::]/64
mynetworks = $config_directory/mynetworks
mynetworks = hash:/etc/postfix/network_table
```

mynetworks_style (default: Postfix >= 3.0: host, Postfix < 3.0: subnet)

The method to generate the default value for the mynetworks parameter. This is the list of trusted networks for relay access control etc.

- Specify "mynetworks_style = host" when Postfix should "trust" only the local machine.
- Specify "mynetworks_style = subnet" when Postfix should "trust" remote SMTP clients in the same IP subnetworks as the local machine. On Linux, this works correctly only with interfaces specified with the "ifconfig" command.
- Specify "mynetworks_style = class" when Postfix should "trust" remote SMTP clients in the same IP class A/B/C networks as the local machine. Caution: this may cause Postfix to "trust" your entire provider’s network. Instead, specify an explicit mynetworks list by hand, as described with the mynetworks configuration parameter.

myorigin (default: $myhostname)
The domain name that locally-posted mail appears to come from, and that locally posted mail is delivered to. The default, $myhostname, is adequate for small sites. If you run a domain with multiple machines, you should (1) change this to $mydomain and (2) set up a domain-wide alias database that aliases each user to user@that.users.mailhost.

Example:

```
myorigin = $mydomain
```

nested_header_checks (default: $header_checks)
Optional lookup tables for content inspection of non-MIME message headers in attached messages, as described in the **header_checks(5)** manual page.

This feature is available in Postfix 2.0 and later.

newaliases_path (default: see postconf −d output)
Sendmail compatibility feature that specifies the location of the **newaliases(1)** command. This command can be used to rebuild the **local(8) aliases(5)** database.

non_fqdn_reject_code (default: 504)
The numerical Postfix SMTP server reply code when a client request is rejected by the reject_non_fqdn_helo_hostname, reject_non_fqdn_sender or reject_non_fqdn_recipient restriction.

non_smtpd_milters (default: empty)
A list of Milter (mail filter) applications for new mail that does not arrive via the Postfix **smtpd(8)** server. This includes local submission via the **sendmail(1)** command line, new mail that arrives via the Postfix **qmqpd(8)** server, and old mail that is re-injected into the queue with "postsuper -r". Specify space or comma as separator. See the MILTER_README document for details.

This feature is available in Postfix 2.3 and later.

notify_classes (default: resource, software)
The list of error classes that are reported to the postmaster. The default is to report only the most serious problems. The paranoid may wish to turn on the policy (UCE and mail relaying) and protocol error (broken mail software) reports.

NOTE: postmaster notifications may contain confidential information such as SASL passwords or message content. It is the system administrator's responsibility to treat such information with care.

The error classes are:

bounce (also implies **2bounce**)
Send the postmaster copies of the headers of bounced mail, and send transcripts of SMTP sessions when Postfix rejects mail. The notification is sent to the address specified with the bounce_notice_recipient configuration parameter (default: postmaster).

2bounce
Send undeliverable bounced mail to the postmaster. The notification is sent to the address specified with the 2bounce_notice_recipient configuration parameter (default: postmaster).

data Send the postmaster a transcript of the SMTP session with an error because a critical data file was unavailable. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).
This feature is available in Postfix 2.9 and later.

delay Send the postmaster copies of the headers of delayed mail (see delay_warning_time). The notification is sent to the address specified with the delay_notice_recipient configuration parameter (default: postmaster).

policy Send the postmaster a transcript of the SMTP session when a client request was rejected because of (UCE) policy. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

protocol
Send the postmaster a transcript of the SMTP session in case of client or server protocol errors. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

resource
Inform the postmaster of mail not delivered due to resource problems. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

software
Inform the postmaster of mail not delivered due to software problems. The notification is sent to the address specified with the error_notice_recipient configuration parameter (default: postmaster).

Examples:

```
notify_classes = bounce, delay, policy, protocol, resource, software
notify_classes = 2bounce, resource, software
```

nullmx_reject_code (default: 556)
The numerical reply code when the Postfix SMTP server rejects a sender or recipient address because its domain has a nullmx DNS record (an MX record with an empty hostname). This is one of the possible replies from the restrictions reject_unknown_sender_domain and reject_unknown_recipient_domain.

This feature is available in Postfix 3.0 and later.

openssl_path (default: openssl)
The location of the OpenSSL command line program **openssl(1)**. This is used by the "**postfix tls**" command to create private keys, certificate signing requests, self-signed certificates, and to compute public key digests for DANE TLSA records. In multi-instance environments, this parameter is always determined from the configuration of the default Postfix instance.

Example:

```
/etc/postfix/main.cf:
# NetBSD pkgsrc:
openssl_path = /usr/pkg/bin/openssl
# Local build:
openssl_path = /usr/local/bin/openssl
```

This feature is available in Postfix 3.1 and later.

owner_request_special (default: yes)
Give special treatment to owner-listname and listname-request address localparts: don't split such addresses when the recipient_delimiter is set to "-". This feature is useful for mailing lists.

parent_domain_matches_subdomains (default: see postconf −d output)
A list of Postfix features where the pattern "example.com" also matches subdomains of example.com, instead of requiring an explicit ".example.com" pattern. This is planned backwards compatibility: eventually, all Postfix features are expected to require explicit ".example.com" style patterns when you really want to match subdomains.

The following Postfix feature names are supported.

Postfix version 1.0 and later
debug_peer_list, fast_flush_domains, mynetworks, permit_mx_backup_networks, relay_domains, transport_maps

Postfix version 1.1 and later
qmqpd_authorized_clients, smtpd_access_maps,

Postfix version 2.8 and later
postscreen_access_list

Postfix version 3.0 and later
smtpd_client_event_limit_exceptions

permit_mx_backup_networks (default: empty)
Restrict the use of the permit_mx_backup SMTP access feature to only domains whose primary MX hosts match the listed networks. The parameter value syntax is the same as with the mynetworks parameter; note, however, that the default value is empty.

Pattern matching of domain names is controlled by the presence or absence of "permit_mx_backup_networks" in the parent_domain_matches_subdomains parameter value.

pickup_service_name (default: pickup)
The name of the **pickup(8)** service. This service picks up local mail submissions from the Postfix maildrop queue.

This feature is available in Postfix 2.0 and later.

pipe_delivery_status_filter (default: $default_delivery_status_filter)
Optional filter for the **pipe(8)** delivery agent to change the delivery status code or explanatory text of successful or unsuccessful deliveries. See default_delivery_status_filter for details.

This feature is available in Postfix 3.0 and later.

plaintext_reject_code (default: 450)
The numerical Postfix SMTP server response code when a request is rejected by the **reject_plaintext_session** restriction.

This feature is available in Postfix 2.3 and later.

postmulti_control_commands (default: reload flush)
The **postfix(1)** commands that the **postmulti(1)** instance manager treats as "control" commands, that operate on running instances. For these commands, disabled instances are skipped.

This feature is available in Postfix 2.6 and later.

postmulti_start_commands (default: start)
The **postfix(1)** commands that the **postmulti(1)** instance manager treats as "start" commands. For these commands, disabled instances are "checked" rather than "started", and failure to "start" a member instance of an instance group will abort the start-up of later instances.

This feature is available in Postfix 2.6 and later.

postmulti_stop_commands (default: see postconf −d output)
The **postfix(1)** commands that the **postmulti(1)** instance manager treats as "stop" commands. For these commands, disabled instances are skipped, and enabled instances are processed in reverse order.

This feature is available in Postfix 2.6 and later.

postscreen_access_list (default: permit_mynetworks)
Permanent white/blacklist for remote SMTP client IP addresses. **postscreen(8)** searches this list immediately after a remote SMTP client connects. Specify a comma- or whitespace-separated list of commands (in upper or lower case) or lookup tables. The search stops upon the first command that fires for the client IP address.

permit_mynetworks
Whitelist the client and terminate the search if the client IP address matches $mynetworks. Do not subject the client to any before/after 220 greeting tests. Pass the connection immediately to a Postfix SMTP server process.
Pattern matching of domain names is controlled by the presence or absence of "postscreen_access_list" in the parent_domain_matches_subdomains parameter value.

type:table
Query the specified lookup table. Each table lookup result is an access list, except that access lists inside a table cannot specify type:table entries.
To discourage the use of hash, btree, etc. tables, there is no support for substring matching like

smtpd(8). Use CIDR tables instead.

permit
Whitelist the client and terminate the search. Do not subject the client to any before/after 220 greeting tests. Pass the connection immediately to a Postfix SMTP server process.

reject Blacklist the client and terminate the search. Subject the client to the action configured with the postscreen_blacklist_action configuration parameter.

dunno All **postscreen(8)** access lists implicitly have this command at the end.
When **dunno** is executed inside a lookup table, return from the lookup table and evaluate the next command.
When **dunno** is executed outside a lookup table, terminate the search, and subject the client to the configured before/after 220 greeting tests.

Example:

```
/etc/postfix/main.cf:
postscreen_access_list = permit_mynetworks,
cidr:/etc/postfix/postscreen_access.cidr
postscreen_blacklist_action = enforce

/etc/postfix/postscreen_access.cidr:
# Rules are evaluated in the order as specified.
# Blacklist 192.168.* except 192.168.0.1.
192.168.0.1 dunno
192.168.0.0/16 reject
```

This feature is available in Postfix 2.8.

postscreen_bare_newline_action (default: ignore)
The action that **postscreen(8)** takes when a remote SMTP client sends a bare newline character, that is, a newline not preceded by carriage return. Specify one of the following:

ignore Ignore the failure of this test. Allow other tests to complete. Do *not* repeat this test before some the result from some other test expires. This option is useful for testing and collecting statistics without blocking mail permanently.

enforce
Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects.

This feature is available in Postfix 2.8.

postscreen_bare_newline_enable (default: no)
Enable "bare newline" SMTP protocol tests in the **postscreen(8)** server. These tests are expensive: a remote SMTP client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

This feature is available in Postfix 2.8.

postscreen_bare_newline_ttl (default: 30d)
The amount of time that **postscreen(8)** will use the result from a successful "bare newline" SMTP protocol test. During this time, the client IP address is excluded from this test. The default is long because a remote SMTP client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_blacklist_action (default: ignore)

The action that **postscreen(8)** takes when a remote SMTP client is permanently blacklisted with the postscreen_access_list parameter. Specify one of the following:

ignore (default)
: Ignore this result. Allow other tests to complete. Repeat this test the next time the client connects. This option is useful for testing and collecting statistics without blocking mail.

enforce
: Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop
: Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects.

This feature is available in Postfix 2.8.

postscreen_cache_cleanup_interval (default: 12h)

The amount of time between **postscreen(8)** cache cleanup runs. Cache cleanup increases the load on the cache database and should therefore not be run frequently. This feature requires that the cache database supports the "delete" and "sequence" operators. Specify a zero interval to disable cache cleanup.

After each cache cleanup run, the **postscreen(8)** daemon logs the number of entries that were retained and dropped. A cleanup run is logged as "partial" when the daemon terminates early after "**postfix reload**", "**postfix stop**", or no requests for $max_idle seconds.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_cache_map (default: btree:$data_directory/postscreen_cache)

Persistent storage for the **postscreen(8)** server decisions.

To share a **postscreen(8)** cache between multiple **postscreen(8)** instances, use "postscreen_cache_map = proxy:btree:/path/to/file". This requires Postfix version 2.9 or later; earlier **proxymap(8)** implementations don't support cache cleanup. For an alternative approach see the **memcache_table(5)** manpage.

This feature is available in Postfix 2.8.

postscreen_cache_retention_time (default: 7d)

The amount of time that **postscreen(8)** will cache an expired temporary whitelist entry before it is removed. This prevents clients from being logged as "NEW" just because their cache entry expired an hour ago. It also prevents the cache from filling up with clients that passed some deep protocol test once and never came back.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_client_connection_count_limit (default: $smtpd_client_connection_count_limit)

How many simultaneous connections any remote SMTP client is allowed to have with the **postscreen(8)** daemon. By default, this limit is the same as with the Postfix SMTP server. Note that the triage process can take several seconds, with the time spent in postscreen_greet_wait delay, and with the time spent talking to the **postscreen(8)** built-in dummy SMTP protocol engine.

This feature is available in Postfix 2.8.

postscreen_command_count_limit (default: 20)

The limit on the total number of commands per SMTP session for **postscreen(8)**'s built-in SMTP protocol engine. This SMTP engine defers or rejects all attempts to deliver mail, therefore there is no need to enforce separate limits on the number of junk commands and error commands.

This feature is available in Postfix 2.8.

postscreen_command_filter (default: $smtpd_command_filter)
A mechanism to transform commands from remote SMTP clients. See smtpd_command_filter for further details.

This feature is available in Postfix 2.8 and later.

postscreen_command_time_limit (default: normal: 300s, overload: 10s)
The time limit to read an entire command line with **postscreen(8)**'s built-in SMTP protocol engine.

This feature is available in Postfix 2.8.

postscreen_disable_vrfy_command (default: $disable_vrfy_command)
Disable the SMTP VRFY command in the **postscreen(8)** daemon. See disable_vrfy_command for details.

This feature is available in Postfix 2.8.

postscreen_discard_ehlo_keyword_address_maps (default: $smtpd_discard_ehlo_keyword_address_maps)
Lookup tables, indexed by the remote SMTP client address, with case insensitive lists of EHLO keywords (pipelining, starttls, auth, etc.) that the **postscreen(8)** server will not send in the EHLO response to a remote SMTP client. See smtpd_discard_ehlo_keywords for details. The table is not searched by hostname for robustness reasons.

This feature is available in Postfix 2.8 and later.

postscreen_discard_ehlo_keywords (default: $smtpd_discard_ehlo_keywords)
A case insensitive list of EHLO keywords (pipelining, starttls, auth, etc.) that the **postscreen(8)** server will not send in the EHLO response to a remote SMTP client. See smtpd_discard_ehlo_keywords for details.

This feature is available in Postfix 2.8 and later.

postscreen_dnsbl_action (default: ignore)
The action that **postscreen(8)** takes when a remote SMTP client's combined DNSBL score is equal to or greater than a threshold (as defined with the postscreen_dnsbl_sites and postscreen_dnsbl_threshold parameters). Specify one of the following:

ignore (default)
Ignore the failure of this test. Allow other tests to complete. Repeat this test the next time the client connects. This option is useful for testing and collecting statistics without blocking mail.

enforce
Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects.

This feature is available in Postfix 2.8.

postscreen_dnsbl_max_ttl (default: ${postscreen_dnsbl_ttl?{$postscreen_dnsbl_ttl}:{1}}h)
The maximum amount of time that **postscreen(8)** will use the result from a successful DNS-based reputation test before a client IP address is required to pass that test again. If the DNS reply specifies a shorter TTL value, that value will be used unless it would be smaller than postscreen_dnsbl_min_ttl.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 3.1. The default setting is backwards-compatible with older Postfix versions.

postscreen_dnsbl_min_ttl (default: 60s)
The minimum amount of time that **postscreen(8)** will use the result from a successful DNS-based reputation test before a client IP address is required to pass that test again. If the DNS reply specifies a larger TTL value, that value will be used unless it would be larger than postscreen_dnsbl_max_ttl.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time

unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 3.1.

postscreen_dnsbl_reply_map (default: empty)

A mapping from actual DNSBL domain name which includes a secret password, to the DNSBL domain name that postscreen will reply with when it rejects mail. When no mapping is found, the actual DNSBL domain will be used.

For maximal stability it is best to use a file that is read into memory such as pcre:, regexp: or texthash: (texthash: is similar to hash:, except a) there is no need to run **postmap(1)** before the file can be used, and b) texthash: does not detect changes after the file is read).

Example:

```
/etc/postfix/main.cf:
postscreen_dnsbl_reply_map = texthash:/etc/postfix/dnsbl_reply

/etc/postfix/dnsbl_reply:
secret.zen.spamhaus.org zen.spamhaus.org
```

This feature is available in Postfix 2.8.

postscreen_dnsbl_sites (default: empty)

Optional list of DNS white/blacklist domains, filters and weight factors. When the list is non-empty, the **dnsblog(8)** daemon will query these domains with the IP addresses of remote SMTP clients, and **postscreen(8)** will update an SMTP client's DNSBL score with each non-error reply.

Caution: when postscreen rejects mail, it replies with the DNSBL domain name. Use the postscreen_dnsbl_reply_map feature to hide "password" information in DNSBL domain names.

When a client's score is equal to or greater than the threshold specified with postscreen_dnsbl_threshold, **postscreen(8)** can drop the connection with the remote SMTP client.

Specify a list of domain=filter*weight entries, separated by comma or whitespace.

- When no "=filter" is specified, **postscreen(8)** will use any non-error DNSBL reply. Otherwise, **postscreen(8)** uses only DNSBL replies that match the filter. The filter has the form d.d.d.d, where each d is a number, or a pattern inside [] that contains one or more ";"-separated numbers or number..number ranges.
- When no "*weight" is specified, **postscreen(8)** increments the remote SMTP client's DNSBL score by 1. Otherwise, the weight must be an integral number, and **postscreen(8)** adds the specified weight to the remote SMTP client's DNSBL score. Specify a negative number for whitelisting.
- When one postscreen_dnsbl_sites entry produces multiple DNSBL responses, **postscreen(8)** applies the weight at most once.

Examples:

To use example.com as a high-confidence blocklist, and to block mail with example.net and example.org only when both agree:

```
postscreen_dnsbl_threshold = 2
postscreen_dnsbl_sites = example.com*2, example.net, example.org
```

To filter only DNSBL replies containing 127.0.0.4:

```
postscreen_dnsbl_sites = example.com=127.0.0.4
```

This feature is available in Postfix 2.8.

postscreen_dnsbl_threshold (default: 1)

The inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score as defined with the postscreen_dnsbl_sites parameter.

This feature is available in Postfix 2.8.

postscreen_dnsbl_timeout (default: 10s)
The time limit for DNSBL or DNSWL lookups. This is separate from the timeouts in the **dnsblog(8)** daemon which are defined by system **resolver(3)** routines.

This feature is available in Postfix 3.0.

postscreen_dnsbl_ttl (default: 1h)
The amount of time that **postscreen(8)** will use the result from a successful DNS-based reputation test before a client IP address is required to pass that test again.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8-3.0. It was replaced by postscreen_dnsbl_max_ttl in Postfix 3.1.

postscreen_dnsbl_whitelist_threshold (default: 0)
Allow a remote SMTP client to skip "before" and "after 220 greeting" protocol tests, based on its combined DNSBL score as defined with the postscreen_dnsbl_sites parameter.

Specify a negative value to enable this feature. When a client passes the postscreen_dnsbl_whitelist_threshold without having failed other tests, all pending or disabled tests are flagged as completed with a time-to-live value equal to postscreen_dnsbl_ttl. When a test was already completed, its time-to-live value is updated if it was less than postscreen_dnsbl_ttl.

This feature is available in Postfix 2.11.

postscreen_enforce_tls (default: $smtpd_enforce_tls)
Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption. See smtpd_postscreen_enforce_tls for details.

This feature is available in Postfix 2.8 and later. Preferably, use postscreen_tls_security_level instead.

postscreen_expansion_filter (default: see postconf −d output)
List of characters that are permitted in postscreen_reject_footer attribute expansions. See smtpd_expansion_filter for further details.

This feature is available in Postfix 2.8 and later.

postscreen_forbidden_commands (default: $smtpd_forbidden_commands)
List of commands that the **postscreen(8)** server considers in violation of the SMTP protocol. See smtpd_forbidden_commands for syntax, and postscreen_non_smtp_command_action for possible actions.

This feature is available in Postfix 2.8.

postscreen_greet_action (default: ignore)
The action that **postscreen(8)** takes when a remote SMTP client speaks before its turn within the time specified with the postscreen_greet_wait parameter. Specify one of the following:

ignore (default)
Ignore the failure of this test. Allow other tests to complete. Repeat this test the next time the client connects. This option is useful for testing and collecting statistics without blocking mail.

enforce
Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects.

In either case, **postscreen(8)** will not whitelist the remote SMTP client IP address.

This feature is available in Postfix 2.8.

postscreen_greet_banner (default: $smtpd_banner)
The *text* in the optional "220-*text*..." server response that **postscreen(8)** sends ahead of the real Postfix SMTP server's "220 text..." response, in an attempt to confuse bad SMTP clients so that they speak before

their turn (pre-greet). Specify an empty value to disable this feature.

This feature is available in Postfix 2.8.

postscreen_greet_ttl (default: 1d)
The amount of time that **postscreen(8)** will use the result from a successful PREGREET test. During this time, the client IP address is excluded from this test. The default is relatively short, because a good client can immediately talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_greet_wait (default: normal: 6s, overload: 2s)
The amount of time that **postscreen(8)** will wait for an SMTP client to send a command before its turn, and for DNS blocklist lookup results to arrive (default: up to 2 seconds under stress, up to 6 seconds otherwise).

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_helo_required (default: $smtpd_helo_required)
Require that a remote SMTP client sends HELO or EHLO before commencing a MAIL transaction.

This feature is available in Postfix 2.8.

postscreen_non_smtp_command_action (default: drop)
The action that **postscreen(8)** takes when a remote SMTP client sends non-SMTP commands as specified with the postscreen_forbidden_commands parameter. Specify one of the following:

ignore Ignore the failure of this test. Allow other tests to complete. Do *not* repeat this test before some the result from some other test expires. This option is useful for testing and collecting statistics without blocking mail permanently.

enforce
Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects. This action is the same as with the Postfix SMTP server's smtpd_forbidden_commands feature.

This feature is available in Postfix 2.8.

postscreen_non_smtp_command_enable (default: no)
Enable "non-SMTP command" tests in the **postscreen(8)** server. These tests are expensive: a client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

This feature is available in Postfix 2.8.

postscreen_non_smtp_command_ttl (default: 30d)
The amount of time that **postscreen(8)** will use the result from a successful "non_smtp_command" SMTP protocol test. During this time, the client IP address is excluded from this test. The default is long because a client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_pipelining_action (default: enforce)
The action that **postscreen(8)** takes when a remote SMTP client sends multiple commands instead of sending one command and waiting for the server to respond. Specify one of the following:

ignore Ignore the failure of this test. Allow other tests to complete. Do *not* repeat this test before some the result from some other test expires. This option is useful for testing and collecting statistics without blocking mail permanently.

enforce
Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the helo/sender/recipient information. Repeat this test the next time the client connects.

drop Drop the connection immediately with a 521 SMTP reply. Repeat this test the next time the client connects.

This feature is available in Postfix 2.8.

postscreen_pipelining_enable (default: no)
Enable "pipelining" SMTP protocol tests in the **postscreen(8)** server. These tests are expensive: a good client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

This feature is available in Postfix 2.8.

postscreen_pipelining_ttl (default: 30d)
The amount of time that **postscreen(8)** will use the result from a successful "pipelining" SMTP protocol test. During this time, the client IP address is excluded from this test. The default is long because a good client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_post_queue_limit (default: $default_process_limit)
The number of clients that can be waiting for service from a real Postfix SMTP server process. When this queue is full, all clients will receive a 421 response.

This feature is available in Postfix 2.8.

postscreen_pre_queue_limit (default: $default_process_limit)
The number of non-whitelisted clients that can be waiting for a decision whether they will receive service from a real Postfix SMTP server process. When this queue is full, all non-whitelisted clients will receive a 421 response.

This feature is available in Postfix 2.8.

postscreen_reject_footer (default: $smtpd_reject_footer)
Optional information that is appended after a 4XX or 5XX **postscreen(8)** server response. See smtpd_reject_footer for further details.

This feature is available in Postfix 2.8 and later.

postscreen_tls_security_level (default: $smtpd_tls_security_level)
The SMTP TLS security level for the **postscreen(8)** server; when a non-empty value is specified, this overrides the obsolete parameters postscreen_use_tls and postscreen_enforce_tls. See smtpd_tls_security_level for details.

This feature is available in Postfix 2.8 and later.

postscreen_upstream_proxy_protocol (default: empty)
The name of the proxy protocol used by an optional before-postscreen proxy agent. When a proxy agent is used, this protocol conveys local and remote address and port information. Specify "postscreen_upstream_proxy_protocol = haproxy" to enable the haproxy protocol.

This feature is available in Postfix 2.10 and later.

postscreen_upstream_proxy_timeout (default: 5s)
The time limit for the proxy protocol specified with the postscreen_upstream_proxy_protocol parameter.

This feature is available in Postfix 2.10 and later.

postscreen_use_tls (default: $smtpd_use_tls)

Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

This feature is available in Postfix 2.8 and later. Preferably, use postscreen_tls_security_level instead.

postscreen_watchdog_timeout (default: 10s)

How much time a **postscreen(8)** process may take to respond to a remote SMTP client command or to perform a cache operation before it is terminated by a built-in watchdog timer. This is a safety mechanism that prevents **postscreen(8)** from becoming non-responsive due to a bug in Postfix itself or in system software. To avoid false alarms and unnecessary cache corruption this limit cannot be set under 10s.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

postscreen_whitelist_interfaces (default: static:all)

A list of local **postscreen(8)** server IP addresses where a non-whitelisted remote SMTP client can obtain **postscreen(8)**'s temporary whitelist status. This status is required before the client can talk to a Postfix SMTP server process. By default, a client can obtain **postscreen(8)**'s whitelist status on any local **postscreen(8)** server IP address.

When **postscreen(8)** listens on both primary and backup MX addresses, the postscreen_whitelist_interfaces parameter can be configured to give the temporary whitelist status only when a client connects to a primary MX address. Once a client is whitelisted it can talk to a Postfix SMTP server on any address. Thus, clients that connect only to backup MX addresses will never become whitelisted, and will never be allowed to talk to a Postfix SMTP server process.

Specify a list of network addresses or network/netmask patterns, separated by commas and/or whitespace. The netmask specifies the number of bits in the network part of a host address. Continue long lines by starting the next line with whitespace.

You can also specify "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored).

The list is matched left to right, and the search stops on the first match. Specify "!pattern" to exclude an address or network block from the list.

Note: IP version 6 address information must be specified inside [] in the postscreen_whitelist_interfaces value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

Example:

```
/etc/postfix/main.cf:
# Don't whitelist connections to the backup IP address.
postscreen_whitelist_interfaces = !168.100.189.8, static:all
```

This feature is available in Postfix 2.9 and later.

prepend_delivered_header (default: command, file, forward)

The message delivery contexts where the Postfix **local(8)** delivery agent prepends a Delivered-To: message header with the address that the mail was delivered to. This information is used for mail delivery loop detection.

By default, the Postfix local delivery agent prepends a Delivered-To: header when forwarding mail and when delivering to file (mailbox) and command. Turning off the Delivered-To: header when forwarding mail is not recommended.

Specify zero or more of **forward**, **file**, or **command**.

Example:

```
prepend_delivered_header = forward
```

process_id (read−only)
The process ID of a Postfix command or daemon process.

process_id_directory (default: pid)
The location of Postfix PID files relative to $queue_directory. This is a read-only parameter.

process_name (read−only)
The process name of a Postfix command or daemon process.

propagate_unmatched_extensions (default: canonical, virtual)
What address lookup tables copy an address extension from the lookup key to the lookup result.

For example, with a **virtual(5)** mapping of "*joe@example.com => joe.user@example.net*", the address "*joe+foo@example.com*" would rewrite to "*joe.user+foo@example.net*".

Specify zero or more of **canonical**, **virtual**, **alias**, **forward**, **include** or **generic**. These cause address extension propagation with **canonical(5)**, **virtual(5)**, and **aliases(5)** maps, with **local(8)** **smtp(8)** generic maps, respectively.

Note: enabling this feature for types other than **canonical** and **virtual** is likely to cause problems when mail is forwarded to other sites, especially with mail that is sent to a mailing list exploder address.

Examples:

```
propagate_unmatched_extensions = canonical, virtual, alias,
forward, include
propagate_unmatched_extensions = canonical, virtual
```

proxy_interfaces (default: empty)
The network interface addresses that this mail system receives mail on by way of a proxy or network address translation unit.

This feature is available in Postfix 2.0 and later.

You must specify your "outside" proxy/NAT addresses when your system is a backup MX host for other domains, otherwise mail delivery loops will happen when the primary MX host is down.

Example:

```
proxy_interfaces = 1.2.3.4
```

proxy_read_maps (default: see postconf −d output)
The lookup tables that the **proxymap(8)** server is allowed to access for the read-only service.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Table references that don't begin with proxy: are ignored.

This feature is available in Postfix 2.0 and later.

proxy_write_maps (default: see postconf −d output)
The lookup tables that the **proxymap(8)** server is allowed to access for the read-write service. Postfix-owned local database files should be stored under the Postfix-owned data_directory. Table references that don't begin with proxy: are ignored.

This feature is available in Postfix 2.5 and later.

proxymap_service_name (default: proxymap)
The name of the proxymap read-only table lookup service. This service is normally implemented by the **proxymap(8)** daemon.

This feature is available in Postfix 2.6 and later.

proxywrite_service_name (default: proxywrite)
The name of the proxywrite read-write table lookup service. This service is normally implemented by the **proxymap(8)** daemon.

This feature is available in Postfix 2.6 and later.

qmgr_clog_warn_time (default: 300s)
The minimal delay between warnings that a specific destination is clogging up the Postfix active queue. Specify 0 to disable.

This feature is enabled with the helpful_warnings parameter.

This feature is available in Postfix 2.0 and later.

qmgr_daemon_timeout (default: 1000s)
How much time a Postfix queue manager process may take to handle a request before it is terminated by a built-in watchdog timer.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.8 and later.

qmgr_fudge_factor (default: 100)
Obsolete feature: the percentage of delivery resources that a busy mail system will use up for delivery of a large mailing list message.

This feature exists only in the **oqmgr(8)** old queue manager. The current queue manager solves the problem in a better way.

qmgr_ipc_timeout (default: 60s)
The time limit for the queue manager to send or receive information over an internal communication channel. The purpose is to break out of deadlock situations. If the time limit is exceeded the software either retries or aborts the operation.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.8 and later.

qmgr_message_active_limit (default: 20000)
The maximal number of messages in the active queue.

qmgr_message_recipient_limit (default: 20000)
The maximal number of recipients held in memory by the Postfix queue manager, and the maximal size of the short-term, in-memory "dead" destination status cache.

qmgr_message_recipient_minimum (default: 10)
The minimal number of in-memory recipients for any message. This takes priority over any other in-memory recipient limits (i.e., the global qmgr_message_recipient_limit and the per transport _recipient_limit) if necessary. The minimum value allowed for this parameter is 1.

qmqpd_authorized_clients (default: empty)
What remote QMQP clients are allowed to connect to the Postfix QMQP server port.

By default, no client is allowed to use the service. This is because the QMQP server will relay mail to any destination.

Specify a list of client patterns. A list pattern specifies a host name, a domain name, an internet address, or a network/mask pattern, where the mask specifies the number of bits in the network part. When a pattern specifies a file name, its contents are substituted for the file name; when a pattern is a "type:table" table specification, table lookup is used instead.

Patterns are separated by whitespace and/or commas. In order to reverse the result, precede a pattern with an exclamation point (!). The form "!/file/name" is supported only in Postfix version 2.4 and later.

Pattern matching of domain names is controlled by the presence or absence of "qmqpd_authorized_clients" in the parent_domain_matches_subdomains parameter value.

Example:

```
qmqpd_authorized_clients = !192.168.0.1, 192.168.0.0/24
```

qmqpd_client_port_logging (default: no)
Enable logging of the remote QMQP client port in addition to the hostname and IP address. The logging format is "host[address]:port".

This feature is available in Postfix 2.5 and later.

qmqpd_error_delay (default: 1s)
How long the Postfix QMQP server will pause before sending a negative reply to the remote QMQP client. The purpose is to slow down confused or malicious clients.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

qmqpd_timeout (default: 300s)
The time limit for sending or receiving information over the network. If a read or write operation blocks for more than $qmqpd_timeout seconds the Postfix QMQP server gives up and disconnects.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

queue_directory (default: see postconf −d output)
The location of the Postfix top-level queue directory. This is the root directory of Postfix daemon processes that run chrooted.

queue_file_attribute_count_limit (default: 100)
The maximal number of (name=value) attributes that may be stored in a Postfix queue file. The limit is enforced by the **cleanup(8)** server.

This feature is available in Postfix 2.0 and later.

queue_minfree (default: 0)
The minimal amount of free space in bytes in the queue file system that is needed to receive mail. This is currently used by the Postfix SMTP server to decide if it will accept any mail at all.

By default, the Postfix SMTP server rejects MAIL FROM commands when the amount of free space is less than 1.5*$message_size_limit (Postfix version 2.1 and later). To specify a higher minimum free space limit, specify a queue_minfree value that is at least 1.5*$message_size_limit.

With Postfix versions 2.0 and earlier, a queue_minfree value of zero means there is no minimum required amount of free space.

queue_run_delay (default: 300s)
The time between deferred queue scans by the queue manager; prior to Postfix 2.4 the default value was 1000s.

This parameter should be set less than or equal to $minimal_backoff_time. See also $maximal_backoff_time.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

queue_service_name (default: qmgr)
The name of the **qmgr(8)** service. This service manages the Postfix queue and schedules delivery requests.

This feature is available in Postfix 2.0 and later.

rbl_reply_maps (default: empty)
Optional lookup tables with RBL response templates. The tables are indexed by the RBL domain name. By default, Postfix uses the default template as specified with the default_rbl_reply configuration parameter. See there for a discussion of the syntax of RBL reply templates.

This feature is available in Postfix 2.0 and later.

readme_directory (default: see postconf −d output)
The location of Postfix README files that describe how to build, configure or operate a specific Postfix subsystem or feature.

receive_override_options (default: empty)

Enable or disable recipient validation, built-in content filtering, or address mapping. Typically, these are specified in master.cf as command-line arguments for the **smtpd(8)**, **qmqpd(8)** or **pickup(8)** daemons.

Specify zero or more of the following options. The options override main.cf settings and are either implemented by **smtpd(8)**, **qmqpd(8)**, or **pickup(8)** themselves, or they are forwarded to the cleanup server.

no_unknown_recipient_checks
: Do not try to reject unknown recipients (SMTP server only). This is typically specified AFTER an external content filter.

no_address_mappings
: Disable canonical address mapping, virtual alias map expansion, address masquerading, and automatic BCC (blind carbon-copy) recipients. This is typically specified BEFORE an external content filter.

no_header_body_checks
: Disable header/body_checks. This is typically specified AFTER an external content filter.

no_milters
: Disable Milter (mail filter) applications. This is typically specified AFTER an external content filter.

Note: when the "BEFORE content filter" receive_override_options setting is specified in the main.cf file, specify the "AFTER content filter" receive_override_options setting in master.cf (and vice versa).

Examples:

```
receive_override_options =
no_unknown_recipient_checks, no_header_body_checks
receive_override_options = no_address_mappings
```

This feature is available in Postfix 2.1 and later.

recipient_bcc_maps (default: empty)

Optional BCC (blind carbon-copy) address lookup tables, indexed by recipient address. The BCC address (multiple results are not supported) is added when mail enters from outside of Postfix.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

The table search order is as follows:

- Look up the "user+extension@domain.tld" address including the optional address extension.
- Look up the "user@domain.tld" address without the optional address extension.
- Look up the "user+extension" address local part when the recipient domain equals $myorigin, $mydestination, $inet_interfaces or $proxy_interfaces.
- Look up the "user" address local part when the recipient domain equals $myorigin, $mydestination, $inet_interfaces or $proxy_interfaces.
- Look up the "@domain.tld" part.

Note: with Postfix 2.3 and later the BCC address is added as if it was specified with NOTIFY=NONE. The sender will not be notified when the BCC address is undeliverable, as long as all down-stream software implements RFC 3461.

Note: with Postfix 2.2 and earlier the sender will unconditionally be notified when the BCC address is undeliverable.

Note: automatic BCC recipients are produced only for new mail. To avoid mailer loops, automatic BCC recipients are not generated after Postfix forwards mail internally, or after Postfix generates mail itself.

Example:

```
recipient_bcc_maps = hash:/etc/postfix/recipient_bcc
```

After a change, run "**postmap /etc/postfix/recipient_bcc**".

This feature is available in Postfix 2.1 and later.

recipient_canonical_classes (default: envelope_recipient, header_recipient)

What addresses are subject to recipient_canonical_maps address mapping. By default, recipient_canonical_maps address mapping is applied to envelope recipient addresses, and to header recipient addresses.

Specify one or more of: envelope_recipient, header_recipient

This feature is available in Postfix 2.2 and later.

recipient_canonical_maps (default: empty)

Optional address mapping lookup tables for envelope and header recipient addresses. The table format and lookups are documented in **canonical(5)**.

Note: $recipient_canonical_maps is processed before $canonical_maps.

Example:

```
recipient_canonical_maps = hash:/etc/postfix/recipient_canonical
```

recipient_delimiter (default: empty)

The set of characters that can separate a user name from its extension (example: user+foo), or a .forward file name from its extension (example: .forward+foo). Basically, the software tries user+foo and .forward+foo before trying user and .forward. This implementation recognizes one delimiter character and one extension per email address or .forward file name.

When the recipient_delimiter set contains multiple characters (Postfix 2.11 and later), a user name or .forward file name is separated from its extension by the first character that matches the recipient_delimiter set.

See **canonical(5)**, **local(8)**, **relocated(5)** and **virtual(5)** for the effects of recipient_delimiter on lookups in aliases, canonical, virtual, and relocated maps, and see the propagate_unmatched_extensions parameter for propagating an extension from one email address to another.

When used in command_execution_directory, forward_path, or luser_relay, ${recipient_delimiter} is replaced with the actual recipient delimiter that was found in the recipient email address (Postfix 2.11 and later), or it is replaced with the main.cf recipient_delimiter parameter value (Postfix 2.10 and earlier).

The recipient_delimiter is not applied to the mailer-daemon address, the postmaster address, or the double-bounce address. With the default "owner_request_special = yes" setting, the recipient_delimiter is also not applied to addresses with the special "owner-" prefix or the special "-request" suffix.

Examples:

```
# Handle Postfix-style extensions.
recipient_delimiter = +
```

```
# Handle both Postfix and qmail extensions (Postfix 2.11 and later).
recipient_delimiter = +-
```

```
# Use .forward for mail without address extension, and for mail with
# an unrecognized address extension.
forward_path = $home/.forward${recipient_delimiter}${extension},
$home/.forward
```

reject_code (default: 554)

The numerical Postfix SMTP server response code when a remote SMTP client request is rejected by the "reject" restriction.

Do not change this unless you have a complete understanding of RFC 5321.

reject_tempfail_action (default: defer_if_permit)

The Postfix SMTP server's action when a reject-type restriction fails due to a temporary error condition. Specify "defer" to defer the remote SMTP client request immediately. With the default "defer_if_permit" action, the Postfix SMTP server continues to look for opportunities to reject mail, and defers the client

request only if it would otherwise be accepted.

For finer control, see: unverified_recipient_tempfail_action, unverified_sender_tempfail_action, unknown_address_tempfail_action, and unknown_helo_hostname_tempfail_action.

This feature is available in Postfix 2.6 and later.

relay_clientcerts (default: empty)

List of tables with remote SMTP client-certificate fingerprints or public key fingerprints (Postfix 2.9 and later) for which the Postfix SMTP server will allow access with the permit_tls_clientcerts feature. The fingerprint digest algorithm is configurable via the smtpd_tls_fingerprint_digest parameter (hard-coded as md5 prior to Postfix version 2.5).

Postfix lookup tables are in the form of (key, value) pairs. Since we only need the key, the value can be chosen freely, e.g. the name of the user or host: D7:04:2F:A7:0B:8C:A5:21:FA:31:77:E1:41:8A:EE:80 lutzpc.at.home

Example:

```
relay_clientcerts = hash:/etc/postfix/relay_clientcerts
```

For more fine-grained control, use check_ccert_access to select an appropriate **access(5)** policy for each client. See RESTRICTION_CLASS_README.

Note: Postfix 2.9.0-2.9.5 computed the public key fingerprint incorrectly. To use public-key fingerprints, upgrade to Postfix 2.9.6 or later.

This feature is available with Postfix version 2.2.

relay_destination_concurrency_limit (default: $default_destination_concurrency_limit)

The maximal number of parallel deliveries to the same destination via the relay message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

This feature is available in Postfix 2.0 and later.

relay_destination_recipient_limit (default: $default_destination_recipient_limit)

The maximal number of recipients per message for the relay message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

Setting this parameter to a value of 1 changes the meaning of relay_destination_concurrency_limit from concurrency per domain into concurrency per recipient.

This feature is available in Postfix 2.0 and later.

relay_domains (default: Postfix >= 3.0: empty, Postfix < 3.0: $mydestination)

What destination domains (and subdomains thereof) this system will relay mail to. For details about how the relay_domains value is used, see the description of the permit_auth_destination and reject_unauth_destination SMTP recipient restrictions.

Domains that match $relay_domains are delivered with the $relay_transport mail delivery transport. The SMTP server validates recipient addresses with $relay_recipient_maps and rejects non-existent recipients. See also the relay domains address class in the ADDRESS_CLASS_README file.

Note: Postfix will not automatically forward mail for domains that list this system as their primary or backup MX host. See the permit_mx_backup restriction in the **postconf(5)** manual page.

Specify a list of host or domain names, "/file/name" patterns or "type:table" lookup tables, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a (parent) domain appears as lookup key. Specify "!pattern" to exclude a domain from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Pattern matching of domain names is controlled by the presence or absence of "relay_domains" in the parent_domain_matches_subdomains parameter value.

relay_domains_reject_code (default: 554)

The numerical Postfix SMTP server response code when a client request is rejected by the reject_unauth_destination recipient restriction.

Do not change this unless you have a complete understanding of RFC 5321.

relay_recipient_maps (default: empty)

Optional lookup tables with all valid addresses in the domains that match $relay_domains. Specify @domain as a wild-card for domains that have no valid recipient list, and become a source of backscatter mail: Postfix accepts spam for non-existent recipients and then floods innocent people with undeliverable mail. Technically, tables listed with $relay_recipient_maps are used as lists: Postfix needs to know only if a lookup string is found or not, but it does not use the result from table lookup.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

If this parameter is non-empty, then the Postfix SMTP server will reject mail to unknown relay users. This feature is off by default.

See also the relay domains address class in the ADDRESS_CLASS_README file.

Example:

```
relay_recipient_maps = hash:/etc/postfix/relay_recipients
```

This feature is available in Postfix 2.0 and later.

relay_transport (default: relay)

The default mail delivery transport and next-hop destination for remote delivery to domains listed with $relay_domains. In order of decreasing precedence, the nexthop destination is taken from $relay_transport, $sender_dependent_relayhost_maps, $relayhost, or from the recipient domain. This information can be overruled with the **transport(5)** table.

Specify a string of the form *transport:nexthop*, where *transport* is the name of a mail delivery transport defined in master.cf. The*:ne xthop* destination is optional; its syntax is documented in the manual page of the corresponding delivery agent.

See also the relay domains address class in the ADDRESS_CLASS_README file.

This feature is available in Postfix 2.0 and later.

relayhost (default: empty)

The next-hop destination of non-local mail; overrides non-local domains in recipient addresses. This information is overruled with relay_transport, sender_dependent_default_transport_maps, default_transport, sender_dependent_relayhost_maps and with the **transport(5)** table.

On an intranet, specify the organizational domain name. If your internal DNS uses no MX records, specify the name of the intranet gateway host instead.

In the case of SMTP, specify a domain name, hostname, hostname:port, [hostname]:port, [hostaddress] or [hostaddress]:port. The form [hostname] turns off MX lookups.

If you’re connected via UUCP, see the UUCP_README file for useful information.

Examples:

```
relayhost = $mydomain
relayhost = [gateway.example.com]
relayhost = uucphost
relayhost = [an.ip.add.ress]
```

relocated_maps (default: empty)

Optional lookup tables with new contact information for users or domains that no longer exist. The table format and lookups are documented in **relocated(5)**.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be

searched in the specified order until a match is found.

If you use this feature, run "**postmap /etc/postfix/relocated**" to build the necessary DBM or DB file after change, then "**postfix reload**" to make the changes visible.

Examples:

```
relocated_maps = dbm:/etc/postfix/relocated
relocated_maps = hash:/etc/postfix/relocated
```

remote_header_rewrite_domain (default: empty)

Don't rewrite message headers from remote clients at all when this parameter is empty; otherwise, rewrite message headers and append the specified domain name to incomplete addresses. The local_header_rewrite_clients parameter controls what clients Postfix considers local.

Examples:

The safe setting: append "domain.invalid" to incomplete header addresses from remote SMTP clients, so that those addresses cannot be confused with local addresses.

```
remote_header_rewrite_domain = domain.invalid
```

The default, purist, setting: don't rewrite headers from remote clients at all.

```
remote_header_rewrite_domain =
```

require_home_directory (default: no)

Require that a **local(8)** recipient's home directory exists before mail delivery is attempted. By default this test is disabled. It can be useful for environments that import home directories to the mail server (IMPORTING HOME DIRECTORIES IS NOT RECOMMENDED).

reset_owner_alias (default: no)

Reset the **local(8)** delivery agent's idea of the owner-alias attribute, when delivering mail to a child alias that does not have its own owner alias.

This feature is available in Postfix 2.8 and later. With older Postfix releases, the behavior is as if this parameter is set to "yes".

As documented in **aliases(5)**, when an alias *name* has a companion alias named owner-*name*, delivery errors will be reported to the owner alias instead of the sender. This configuration is recommended for mailing lists.

A less known property of the owner alias is that it also forces the **local(8)** delivery agent to write local and remote addresses from alias expansion to a new queue file, instead of attempting to deliver mail to local addresses as soon as they come out of alias expansion.

Writing local addresses from alias expansion to a new queue file allows for robust handling of temporary delivery errors: errors with one local member have no effect on deliveries to other members of the list. On the other hand, delivery to local addresses as soon as they come out of alias expansion is fragile: a temporary error with one local address from alias expansion will cause the entire alias to be expanded repeatedly until the error goes away, or until the message expires in the queue. In that case, a problem with one list member results in multiple message deliveries to other list members.

The default behavior of Postfix 2.8 and later is to keep the owner-alias attribute of the parent alias, when delivering mail to a child alias that does not have its own owner alias. Then, local addresses from that child alias will be written to a new queue file, and a temporary error with one local address will not affect delivery to other mailing list members.

Unfortunately, older Postfix releases reset the owner-alias attribute when delivering mail to a child alias that does not have its own owner alias. The **local(8)** delivery agent then attempts to deliver local addresses as soon as they come out of child alias expansion. If delivery to any address from child alias expansion fails with a temporary error condition, the entire mailing list may be expanded repeatedly until the mail expires in the queue, resulting in multiple deliveries of the same message to mailing list members.

resolve_dequoted_address (default: yes)
Resolve a recipient address safely instead of correctly, by looking inside quotes.

By default, the Postfix address resolver does not quote the address localpart as per RFC 822, so that additional @ or % or ! operators remain visible. This behavior is safe but it is also technically incorrect.

If you specify "resolve_dequoted_address = no", then the Postfix resolver will not know about additional @ etc. operators in the address localpart. This opens opportunities for obscure mail relay attacks with user@domain@domain addresses when Postfix provides backup MX service for Sendmail systems.

resolve_null_domain (default: no)
Resolve an address that ends in the "@" null domain as if the local hostname were specified, instead of rejecting the address as invalid.

This feature is available in Postfix 2.1 and later. Earlier versions always resolve the null domain as the local hostname.

The Postfix SMTP server uses this feature to reject mail from or to addresses that end in the "@" null domain, and from addresses that rewrite into a form that ends in the "@" null domain.

resolve_numeric_domain (default: no)
Resolve "user@ipaddress" as "user@[ipaddress]", instead of rejecting the address as invalid.

This feature is available in Postfix 2.3 and later.

rewrite_service_name (default: rewrite)
The name of the address rewriting service. This service rewrites addresses to standard form and resolves them to a (delivery method, next-hop host, recipient) triple.

This feature is available in Postfix 2.0 and later.

sample_directory (default: /etc/postfix)
The name of the directory with example Postfix configuration files. Starting with Postfix 2.1, these files have been replaced with the **postconf(5)** manual page.

send_cyrus_sasl_authzid (default: no)
When authenticating to a remote SMTP or LMTP server with the default setting "no", send no SASL authoriZation ID (authzid); send only the SASL authentiCation ID (authcid) plus the authcid's password.

The non-default setting "yes" enables the behavior of older Postfix versions. These always send a SASL authzid that is equal to the SASL authcid, but this causes interoperability problems with some SMTP servers.

This feature is available in Postfix 2.4.4 and later.

sender_based_routing (default: no)
This parameter should not be used. It was replaced by sender_dependent_relayhost_maps in Postfix version 2.3.

sender_bcc_maps (default: empty)
Optional BCC (blind carbon-copy) address lookup tables, indexed by sender address. The BCC address (multiple results are not supported) is added when mail enters from outside of Postfix.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

The table search order is as follows:

- Look up the "user+extension@domain.tld" address including the optional address extension.
- Look up the "user@domain.tld" address without the optional address extension.
- Look up the "user+extension" address local part when the sender domain equals $myorigin, $mydestination, $inet_interfaces or $proxy_interfaces.
- Look up the "user" address local part when the sender domain equals $myorigin, $mydestination, $inet_interfaces or $proxy_interfaces.

- Look up the "@domain.tld" part.

Note: with Postfix 2.3 and later the BCC address is added as if it was specified with NOTIFY=NONE. The sender will not be notified when the BCC address is undeliverable, as long as all down-stream software implements RFC 3461.

Note: with Postfix 2.2 and earlier the sender will be notified when the BCC address is undeliverable.

Note: automatic BCC recipients are produced only for new mail. To avoid mailer loops, automatic BCC recipients are not generated after Postfix forwards mail internally, or after Postfix generates mail itself.

Example:

```
sender_bcc_maps = hash:/etc/postfix/sender_bcc
```

After a change, run "**postmap /etc/postfix/sender_bcc**".

This feature is available in Postfix 2.1 and later.

sender_canonical_classes (default: envelope_sender, header_sender)

What addresses are subject to sender_canonical_maps address mapping. By default, sender_canonical_maps address mapping is applied to envelope sender addresses, and to header sender addresses.

Specify one or more of: envelope_sender, header_sender

This feature is available in Postfix 2.2 and later.

sender_canonical_maps (default: empty)

Optional address mapping lookup tables for envelope and header sender addresses. The table format and lookups are documented in **canonical(5)**.

Example: you want to rewrite the SENDER address "user@ugly.domain" to "user@pretty.domain", while still being able to send mail to the RECIPIENT address "user@ugly.domain".

Note: $sender_canonical_maps is processed before $canonical_maps.

Example:

```
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

sender_dependent_default_transport_maps (default: empty)

A sender-dependent override for the global default_transport parameter setting. The tables are searched by the envelope sender address and @domain. A lookup result of DUNNO terminates the search without overriding the global default_transport parameter setting. This information is overruled with the **transport(5)** table.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

Note: this overrides default_transport, not transport_maps, and therefore the expected syntax is that of default_transport, not the syntax of transport_maps. Specifically, this does not support the transport_maps syntax for null transport, null nexthop, or null email addresses.

For safety reasons, this feature does not allow $number substitutions in regular expression maps.

This feature is available in Postfix 2.7 and later.

sender_dependent_relayhost_maps (default: empty)

A sender-dependent override for the global relayhost parameter setting. The tables are searched by the envelope sender address and @domain. A lookup result of DUNNO terminates the search without overriding the global relayhost parameter setting (Postfix 2.6 and later). This information is overruled with relay_transport, sender_dependent_default_transport_maps, default_transport and with the **transport(5)** table.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

For safety reasons, this feature does not allow $number substitutions in regular expression maps.

This feature is available in Postfix 2.3 and later.

sendmail_fix_line_endings (default: always)
Controls how the Postfix sendmail command converts email message line endings from <CR><LF> into UNIX format (<LF>).

always Always convert message lines ending in <CR><LF>. This setting is the default with Postfix 2.9 and later.

strict Convert message lines ending in <CR><LF> only if the first input line ends in <CR><LF>. This setting is backwards-compatible with Postfix 2.8 and earlier.

never Never convert message lines ending in <CR><LF>. This setting exists for completeness only.

This feature is available in Postfix 2.9 and later.

sendmail_path (default: see postconf −d output)
A Sendmail compatibility feature that specifies the location of the Postfix **sendmail(1)** command. This command can be used to submit mail into the Postfix queue.

service_throttle_time (default: 60s)
How long the Postfix **master(8)** waits before forking a server that appears to be malfunctioning.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

setgid_group (default: postdrop)
The group ownership of set-gid Postfix commands and of group-writable Postfix directories. When this parameter value is changed you need to re-run "**postfix set-permissions**" (with Postfix version 2.0 and earlier: "**/etc/postfix/post-install set-permissions**".

shlib_directory (default: see 'postconf −d' output)
The location of Postfix dynamically-linked libraries (libpostfix-*.so), and the default location of Postfix database plugins (postfix-*.so) that have a relative pathname in the dynamicmaps.cf file. The shlib_directory parameter defaults to "no" when Postfix dynamically-linked libraries and database plugins are disabled at compile time, otherwise it typically defaults to /usr/lib/postfix or /usr/local/lib/postfix.

Notes:

- The directory specified with shlib_directory should contain only Postfix-related files. Postfix dynamically-linked libraries and database plugins should not be installed in a "public" system directory such as /usr/lib or /usr/local/lib. Linking Postfix dynamically-linked library files or database plugins into non-Postfix programs is not supported. Postfix dynamically-linked libraries and database plugins implement a Postfix-internal API that changes without maintaining compatibility.
- You can change the shlib_directory value after Postfix is built. However, you may have to run ldconfig or equivalent to prevent Postfix programs from failing because the libpostfix-*.so files are not found. No ldconfig command is needed if you keep the libpostfix-*.so files in the compiled-in default $shlib_directory location.

This feature is available in Postfix 3.0 and later.

show_user_unknown_table_name (default: yes)
Display the name of the recipient table in the "User unknown" responses. The extra detail makes trouble shooting easier but also reveals information that is nobody elses business.

This feature is available in Postfix 2.0 and later.

showq_service_name (default: showq)
The name of the **showq(8)** service. This service produces mail queue status reports.

This feature is available in Postfix 2.0 and later.

smtp_address_preference (default: any)
The address type ("ipv6", "ipv4" or "any") that the Postfix SMTP client will try first, when a destination has IPv6 and IPv4 addresses with equal MX preference. This feature has no effect unless the inet_protocols setting enables both IPv4 and IPv6.

Postfix SMTP client address preference has evolved. With Postfix 2.8 the default is "ipv6"; earlier implementations are hard-coded to prefer IPv6 over IPv4.

Notes for mail delivery between sites that have both IPv4 and IPv6 connectivity:

- The setting "smtp_address_preference = ipv6" is unsafe. It can fail to deliver mail when there is an outage that affects IPv6, while the destination is still reachable over IPv4.
- The setting "smtp_address_preference = any" is safe. With this, mail will eventually be delivered even if there is an outage that affects IPv6 or IPv4, as long as it does not affect both.

This feature is available in Postfix 2.8 and later.

smtp_address_verify_target (default: rcpt)

In the context of email address verification, the SMTP protocol stage that determines whether an email address is deliverable. Specify one of "rcpt" or "data". The latter is needed with remote SMTP servers that reject recipients after the DATA command. Use transport_maps to apply this feature selectively:

```
/etc/postfix/main.cf:
transport_maps = hash:/etc/postfix/transport

/etc/postfix/transport:
smtp-domain-that-verifies-after-data smtp-data-target:
lmtp-domain-that-verifies-after-data lmtp-data-target:

/etc/postfix/master.cf:
smtp-data-target unix - - n - - smtp
-o smtp_address_verify_target=data
lmtp-data-target unix - - n - - lmtp
-o lmtp_address_verify_target=data
```

Unselective use of the "data" target does no harm, but will result in unnecessary "lost connection after DATA" events at remote SMTP/LMTP servers.

This feature is available in Postfix 3.0 and later.

smtp_always_send_ehlo (default: yes)

Always send EHLO at the start of an SMTP session.

With "smtp_always_send_ehlo = no", the Postfix SMTP client sends EHLO only when the word "ESMTP" appears in the server greeting banner (example: 220 spike.porcupine.org ESMTP Postfix).

smtp_bind_address (default: empty)

An optional numerical network address that the Postfix SMTP client should bind to when making an IPv4 connection.

This can be specified in the main.cf file for all SMTP clients, or it can be specified in the master.cf file for a specific client, for example:

```
/etc/postfix/master.cf:
smtp ... smtp -o smtp_bind_address=11.22.33.44
```

Note 1: when inet_interfaces specifies no more than one IPv4 address, and that address is a non-loopback address, it is automatically used as the smtp_bind_address. This supports virtual IP hosting, but can be a problem on multi-homed firewalls. See the inet_interfaces documentation for more detail.

Note 2: address information may be enclosed inside [], but this form is not required here.

smtp_bind_address6 (default: empty)

An optional numerical network address that the Postfix SMTP client should bind to when making an IPv6 connection.

This feature is available in Postfix 2.2 and later.

This can be specified in the main.cf file for all SMTP clients, or it can be specified in the master.cf file for a specific client, for example:

```
/etc/postfix/master.cf:
smtp ... smtp -o smtp_bind_address6=1:2:3:4:5:6:7:8
```

Note 1: when inet_interfaces specifies no more than one IPv6 address, and that address is a non-loopback address, it is automatically used as the smtp_bind_address6. This supports virtual IP hosting, but can be a problem on multi-homed firewalls. See the inet_interfaces documentation for more detail.

Note 2: address information may be enclosed inside [], but this form is not recommended here.

smtp_body_checks (default: empty)

Restricted **body_checks(5)** tables for the Postfix SMTP client. These tables are searched while mail is being delivered. Actions that change the delivery time or destination are not available.

This feature is available in Postfix 2.5 and later.

smtp_cname_overrides_servername (default: version dependent)

When the remote SMTP servername is a DNS CNAME, replace the servername with the result from CNAME expansion for the purpose of logging, SASL password lookup, TLS policy decisions, or TLS certificate verification. The value "no" hardens Postfix smtp_tls_per_site hostname-based policies against false hostname information in DNS CNAME records, and makes SASL password file lookups more predictable. This is the default setting as of Postfix 2.3.

When DNS CNAME records are validated with secure DNS lookups (smtp_dns_support_level = dnssec), they are always allowed to override the above servername (Postfix 2.11 and later).

This feature is available in Postfix 2.2.9 and later.

smtp_connect_timeout (default: 30s)

The Postfix SMTP client time limit for completing a TCP connection, or zero (use the operating system built-in time limit).

When no connection can be made within the deadline, the Postfix SMTP client tries the next address on the mail exchanger list. Specify 0 to disable the time limit (i.e. use whatever timeout is implemented by the operating system).

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_connection_cache_destinations (default: empty)

Permanently enable SMTP connection caching for the specified destinations. With SMTP connection caching, a connection is not closed immediately after completion of a mail transaction. Instead, the connection is kept open for up to $smtp_connection_cache_time_limit seconds. This allows connections to be reused for other deliveries, and can improve mail delivery performance.

Specify a comma or white space separated list of destinations or pseudo-destinations:

- if mail is sent without a relay host: a domain name (the right-hand side of an email address, without the [] around a numeric IP address),
- if mail is sent via a relay host: a relay host name (without [] or non-default TCP port), as specified in main.cf or in the transport map,
- if mail is sent via a UNIX-domain socket: a pathname (without the unix: prefix),
- a /file/name with domain names and/or relay host names as defined above,
- a "type:table" with domain names and/or relay host names on the left-hand side. The right-hand side result from "type:table" lookups is ignored.

This feature is available in Postfix 2.2 and later.

smtp_connection_cache_on_demand (default: yes)

Temporarily enable SMTP connection caching while a destination has a high volume of mail in the active queue. With SMTP connection caching, a connection is not closed immediately after completion of a mail transaction. Instead, the connection is kept open for up to $smtp_connection_cache_time_limit seconds. This allows connections to be reused for other deliveries, and can improve mail delivery performance.

This feature is available in Postfix 2.2 and later.

smtp_connection_cache_time_limit (default: 2s)
When SMTP connection caching is enabled, the amount of time that an unused SMTP client socket is kept open before it is closed. Do not specify larger values without permission from the remote sites.

This feature is available in Postfix 2.2 and later.

smtp_connection_reuse_count_limit (default: 0)
When SMTP connection caching is enabled, the number of times that an SMTP session may be reused before it is closed, or zero (no limit). With a reuse count limit of N, a connection is used up to N+1 times.

NOTE: This feature is unsafe. When a high-volume destination has multiple inbound MTAs, then the slowest inbound MTA will attract the most connections to that destination. This limitation does not exist with the smtp_connection_reuse_time_limit feature.

This feature is available in Postfix 2.11.

smtp_connection_reuse_time_limit (default: 300s)
The amount of time during which Postfix will use an SMTP connection repeatedly. The timer starts when the connection is initiated (i.e. it includes the connect, greeting and helo latency, in addition to the latencies of subsequent mail delivery transactions).

This feature addresses a performance stability problem with remote SMTP servers. This problem is not specific to Postfix: it can happen when any MTA sends large amounts of SMTP email to a site that has multiple MX hosts.

The problem starts when one of a set of MX hosts becomes slower than the rest. Even though SMTP clients connect to fast and slow MX hosts with equal probability, the slow MX host ends up with more simultaneous inbound connections than the faster MX hosts, because the slow MX host needs more time to serve each client request.

The slow MX host becomes a connection attractor. If one MX host becomes N times slower than the rest, it dominates mail delivery latency unless there are more than N fast MX hosts to counter the effect. And if the number of MX hosts is smaller than N, the mail delivery latency becomes effectively that of the slowest MX host divided by the total number of MX hosts.

The solution uses connection caching in a way that differs from Postfix version 2.2. By limiting the amount of time during which a connection can be used repeatedly (instead of limiting the number of deliveries over that connection), Postfix not only restores fairness in the distribution of simultaneous connections across a set of MX hosts, it also favors deliveries over connections that perform well, which is exactly what we want.

The default reuse time limit, 300s, is comparable to the various smtp transaction timeouts which are fair estimates of maximum excess latency for a slow delivery. Note that hosts may accept thousands of messages over a single connection within the default connection reuse time limit. This number is much larger than the default Postfix version 2.2 limit of 10 messages per cached connection. It may prove necessary to lower the limit to avoid interoperability issues with MTAs that exhibit bugs when many messages are delivered via a single connection. A lower reuse time limit risks losing the benefit of connection reuse when the average connection and mail delivery latency exceeds the reuse time limit.

This feature is available in Postfix 2.3 and later.

smtp_data_done_timeout (default: 600s)
The Postfix SMTP client time limit for sending the SMTP ".", and for receiving the remote SMTP server response.

When no response is received within the deadline, a warning is logged that the mail may be delivered multiple times.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_data_init_timeout (default: 120s)
The Postfix SMTP client time limit for sending the SMTP DATA command, and for receiving the remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_data_xfer_timeout (default: 180s)
The Postfix SMTP client time limit for sending the SMTP message content. When the connection makes no progress for more than $smtp_data_xfer_timeout seconds the Postfix SMTP client terminates the transfer.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_defer_if_no_mx_address_found (default: no)
Defer mail delivery when no MX record resolves to an IP address.

The default (no) is to return the mail as undeliverable. With older Postfix versions the default was to keep trying to deliver the mail until someone fixed the MX record or until the mail was too old.

Note: the Postfix SMTP client always ignores MX records with equal or worse preference than the local MTA itself.

This feature is available in Postfix 2.1 and later.

smtp_delivery_status_filter (default: $default_delivery_status_filter)
Optional filter for the **smtp(8)** delivery agent to change the delivery status code or explanatory text of successful or unsuccessful deliveries. See default_delivery_status_filter for details.

NOTE: This feature modifies Postfix SMTP client error or non-error messages that may or may not be derived from remote SMTP server responses. In contrast, the smtp_reply_filter feature modifies remote SMTP server responses only.

smtp_destination_concurrency_limit (default: $default_destination_concurrency_limit)
The maximal number of parallel deliveries to the same destination via the smtp message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

smtp_destination_recipient_limit (default: $default_destination_recipient_limit)
The maximal number of recipients per message for the smtp message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

Setting this parameter to a value of 1 changes the meaning of smtp_destination_concurrency_limit from concurrency per domain into concurrency per recipient.

smtp_discard_ehlo_keyword_address_maps (default: empty)
Lookup tables, indexed by the remote SMTP server address, with case insensitive lists of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP client will ignore in the EHLO response from a remote SMTP server. See smtp_discard_ehlo_keywords for details. The table is not indexed by hostname for consistency with smtpd_discard_ehlo_keyword_address_maps.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

This feature is available in Postfix 2.2 and later.

smtp_discard_ehlo_keywords (default: empty)
A case insensitive list of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP client will ignore in the EHLO response from a remote SMTP server.

This feature is available in Postfix 2.2 and later.

Notes:

- Specify the **silent-discard** pseudo keyword to prevent this action from being logged.

- Use the smtp_discard_ehlo_keyword_address_maps feature to discard EHLO keywords selectively.

smtp_dns_reply_filter (default: empty)

Optional filter for Postfix SMTP client DNS lookup results. Specify zero or more lookup tables. The lookup tables are searched in the given order for a match with the DNS lookup result, converted to the following form:

name ttl class type preference value

The *class* field is always "IN", the *preference* field exists only for MX records, the names of hosts, domains, etc. end in ".", and those names are in ASCII form (xn--mumble form in the case of UTF8 names).

When a match is found, the table lookup result specifies an action. By default, the table query and the action name are case-insensitive. Currently, only the **IGNORE** action is implemented.

Notes:

- Postfix DNS reply filters have no effect on implicit DNS lookups through nsswitch.conf or equivalent mechanisms.
- The Postfix SMTP/LMTP client uses smtp_dns_reply_filter and lmtp_dns_reply_filter only to discover a remote SMTP or LMTP service (record types MX, A, AAAAA, and TLSA). These lookups are also made to implement the features reject_unverified_sender and reject_unverified_recipient.
- The Postfix SMTP/LMTP client defers mail delivery when a filter removes all lookup results from a successful query.
- Postfix SMTP server uses smtpd_dns_reply_filter only to look up MX, A, AAAAA, and TXT records to implement the features reject_unknown_helo_hostname, reject_unknown_sender_domain, reject_unknown_recipient_domain, reject_rbl_*, and reject_rhsbl_*.
- The Postfix SMTP server logs a warning or defers mail delivery when a filter removes all lookup results from a successful query.

Example: ignore Google AAAA records in Postfix SMTP client DNS lookups, because Google sometimes hard-rejects mail from IPv6 clients with valid PTR etc. records.

```
/etc/postfix/main.cf:
smtp_dns_reply_filter = pcre:/etc/postfix/smtp_dns_reply_filter

/etc/postfix/smtp_dns_reply_filter:
# /domain ttl IN AAAA address/ action, all case-insensitive.
# Note: the domain name ends in ".".
/^\S+\.google\.com\.\s+\S+\s+\S+\s+AAAA\s+/ IGNORE
```

This feature is available in Postfix 3.0 and later.

smtp_dns_resolver_options (default: empty)

DNS Resolver options for the Postfix SMTP client. Specify zero or more of the following options, separated by comma or whitespace. Option names are case-sensitive. Some options refer to domain names that are specified in the file /etc/resolv.conf or equivalent.

res_defnames

Append the current domain name to single-component names (those that do not contain a "." character). This can produce incorrect results, and is the hard-coded behavior prior to Postfix 2.8.

res_dnsrch

Search for host names in the current domain and in parent domains. This can produce incorrect results and is therefore not recommended.

This feature is available in Postfix 2.8 and later.

smtp_dns_support_level (default: empty)

Level of DNS support in the Postfix SMTP client. With "smtp_dns_support_level" left at its empty default value, the legacy "disable_dns_lookups" parameter controls whether DNS is enabled in the Postfix SMTP client, otherwise the legacy parameter is ignored.

Specify one of the following:

disabled

Disable DNS lookups. No MX lookups are performed and hostname to address lookups are unconditionally "native". This setting is not appropriate for hosts that deliver mail to the public Internet. Some obsolete how-to documents recommend disabling DNS lookups in some configurations with content_filters. This is no longer required and strongly discouraged.

enabled

Enable DNS lookups. Nexthop destination domains not enclosed in "[]" will be subject to MX lookups. If "dns" and "native" are included in the "smtp_host_lookup" parameter value, DNS will be queried first to resolve MX-host A records, followed by "native" lookups if no answer is found in DNS.

dnssec Enable DNSSEC lookups. The "dnssec" setting differs from the "enabled" setting above in the following ways:

- Any MX lookups will set RES_USE_DNSSEC and RES_USE_EDNS0 to request DNSSEC-validated responses. If the MX response is DNSSEC-validated the corresponding hostnames are considered validated.
- The address lookups of validated hostnames are also validated, (provided of course "smtp_host_lookup" includes "dns", see below).
- Temporary failures in DNSSEC-enabled hostname-to-address resolution block any "native" lookups. Additional "native" lookups only happen when DNSSEC lookups hard-fail (NODATA or NXDOMAIN).

The Postfix SMTP client considers non-MX "[nexthop]" and "[nexthop]:port" destinations equivalent to statically-validated MX records of the form "nexthop. IN MX 0 nexthop." Therefore, with "dnssec" support turned on, validated hostname-to-address lookups apply to the nexthop domain of any "[nexthop]" or "[nexthop]:port" destination. This is also true for LMTP "inet:host" and "inet:host:port" destinations, as LMTP hostnames are never subject to MX lookups.

The "dnssec" setting is recommended only if you plan to use the dane or dane-only TLS security level, otherwise enabling DNSSEC support in Postfix offers no additional security. Postfix DNSSEC support relies on an upstream recursive nameserver that validates DNSSEC signatures. Such a DNS server will always filter out forged DNS responses, even when Postfix itself is not configured to use DNSSEC.

When using Postfix DANE support the "smtp_host_lookup" parameter should include "dns", as DANE is not applicable to hosts resolved via "native" lookups.

As mentioned above, Postfix is not a validating stub resolver; it relies on the system's configured DNSSEC-validating recursive nameserver to perform all DNSSEC validation. Since this nameserver's DNSSEC-validated responses will be fully trusted, it is strongly recommended that the MTA host have a local DNSSEC-validating recursive caching nameserver listening on a loopback address, and be configured to use only this nameserver for all lookups. Otherwise, Postfix may remain subject to man-in-the-middle attacks that forge responses from the recursive nameserver

DNSSEC support requires a version of Postfix compiled against a reasonably-modern DNS **resolver(3)** library that implements the RES_USE_DNSSEC and RES_USE_EDNS0 resolver options.

This feature is available in Postfix 2.11 and later.

smtp_enforce_tls (default: no)

Enforcement mode: require that remote SMTP servers use TLS encryption, and never send mail in the clear. This also requires that the remote SMTP server hostname matches the information in the remote server certificate, and that the remote SMTP server certificate was issued by a CA that is trusted by the

Postfix SMTP client. If the certificate doesn't verify or the hostname doesn't match, delivery is deferred and mail stays in the queue.

The server hostname is matched against all names provided as dNSNames in the SubjectAlternativeName. If no dNSNames are specified, the CommonName is checked. The behavior may be changed with the smtp_tls_enforce_peername option.

This option is useful only if you are definitely sure that you will only connect to servers that support RFC 2487 _and_ that provide valid server certificates. Typical use is for clients that send all their email to a dedicated mailhub.

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtp_tls_security_level instead.

smtp_fallback_relay (default: $fallback_relay)

Optional list of relay hosts for SMTP destinations that can't be found or that are unreachable. With Postfix 2.2 and earlier this parameter is called fallback_relay.

By default, mail is returned to the sender when a destination is not found, and delivery is deferred when a destination is unreachable.

With bulk email deliveries, it can be beneficial to run the fallback relay MTA on the same host, so that it can reuse the sender IP address. This speeds up deliveries that are delayed by IP-based reputation systems (greylist, etc.).

The fallback relays must be SMTP destinations. Specify a domain, host, host:port, [host]:port, [address] or [address]:port; the form [host] turns off MX lookups. If you specify multiple SMTP destinations, Postfix will try them in the specified order.

To prevent mailer loops between MX hosts and fall-back hosts, Postfix version 2.2 and later will not use the fallback relays for destinations that it is MX host for (assuming DNS lookup is turned on).

smtp_generic_maps (default: empty)

Optional lookup tables that perform address rewriting in the Postfix SMTP client, typically to transform a locally valid address into a globally valid address when sending mail across the Internet. This is needed when the local machine does not have its own Internet domain name, but uses something like *localdomain.local* instead.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

The table format and lookups are documented in **generic(5)**; examples are shown in the ADDRESS_REWRITING_README and STANDARD_CONFIGURATION_README documents.

This feature is available in Postfix 2.2 and later.

smtp_header_checks (default: empty)

Restricted **header_checks(5)** tables for the Postfix SMTP client. These tables are searched while mail is being delivered. Actions that change the delivery time or destination are not available.

This feature is available in Postfix 2.5 and later.

smtp_helo_name (default: $myhostname)

The hostname to send in the SMTP HELO or EHLO command.

The default value is the machine hostname. Specify a hostname or [ip.add.re.ss].

This information can be specified in the main.cf file for all SMTP clients, or it can be specified in the master.cf file for a specific client, for example:

```
/etc/postfix/master.cf:
mysmtp ... smtp -o smtp_helo_name=foo.bar.com
```

This feature is available in Postfix 2.0 and later.

smtp_helo_timeout (default: 300s)
The Postfix SMTP client time limit for sending the HELO or EHLO command, and for receiving the initial remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_host_lookup (default: dns)
What mechanisms the Postfix SMTP client uses to look up a host's IP address. This parameter is ignored when DNS lookups are disabled (see: disable_dns_lookups and smtp_dns_support_level). The "dns" mechanism is always tried before "native" if both are listed.

Specify one of the following:

dns Hosts can be found in the DNS (preferred).

native Use the native naming service only (nsswitch.conf, or equivalent mechanism).

dns, native
Use the native service for hosts not found in the DNS.

This feature is available in Postfix 2.1 and later.

smtp_line_length_limit (default: 998)
The maximal length of message header and body lines that Postfix will send via SMTP. This limit does not include the <CR><LF> at the end of each line. Longer lines are broken by inserting "<CR><LF><SPACE>", to minimize the damage to MIME formatted mail.

The Postfix limit of 998 characters not including <CR><LF> is consistent with the SMTP limit of 1000 characters including <CR><LF>. The Postfix limit was 990 with Postfix 2.8 and earlier.

smtp_mail_timeout (default: 300s)
The Postfix SMTP client time limit for sending the MAIL FROM command, and for receiving the remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_mime_header_checks (default: empty)
Restricted **mime_header_checks(5)** tables for the Postfix SMTP client. These tables are searched while mail is being delivered. Actions that change the delivery time or destination are not available.

This feature is available in Postfix 2.5 and later.

smtp_mx_address_limit (default: 5)
The maximal number of MX (mail exchanger) IP addresses that can result from Postfix SMTP client mail exchanger lookups, or zero (no limit). Prior to Postfix version 2.3, this limit was disabled by default.

This feature is available in Postfix 2.1 and later.

smtp_mx_session_limit (default: 2)
The maximal number of SMTP sessions per delivery request before the Postfix SMTP client gives up or delivers to a fall-back relay host, or zero (no limit). This restriction ignores sessions that fail to complete the SMTP initial handshake (Postfix version 2.2 and earlier) or that fail to complete the EHLO and TLS handshake (Postfix version 2.3 and later).

This feature is available in Postfix 2.1 and later.

smtp_nested_header_checks (default: empty)
Restricted **nested_header_checks(5)** tables for the Postfix SMTP client. These tables are searched while mail is being delivered. Actions that change the delivery time or destination are not available.

This feature is available in Postfix 2.5 and later.

smtp_never_send_ehlo (default: no)
Never send EHLO at the start of an SMTP session. See also the smtp_always_send_ehlo parameter.

smtp_per_record_deadline (default: no)
Change the behavior of the smtp_*_timeout time limits, from a time limit per read or write system call, to a time limit to send or receive a complete record (an SMTP command line, SMTP response line, SMTP message content line, or TLS protocol message). This limits the impact from hostile peers that trickle data one byte at a time.

Note: when per-record deadlines are enabled, a short timeout may cause problems with TLS over very slow network connections. The reasons are that a TLS protocol message can be up to 16 kbytes long (with TLSv1), and that an entire TLS protocol message must be sent or received within the per-record deadline.

This feature is available in Postfix 2.9 and later. With older Postfix releases, the behavior is as if this parameter is set to "no".

smtp_pix_workaround_delay_time (default: 10s)
How long the Postfix SMTP client pauses before sending ".<CR><LF>" in order to work around the PIX firewall "<CR><LF>.<CR><LF>" bug.

Choosing a too short time makes this workaround ineffective when sending large messages over slow network connections.

smtp_pix_workaround_maps (default: empty)
Lookup tables, indexed by the remote SMTP server address, with per-destination workarounds for CISCO PIX firewall bugs. The table is not indexed by hostname for consistency with smtp_discard_ehlo_keyword_address_maps.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

This feature is available in Postfix 2.4 and later.

smtp_pix_workaround_threshold_time (default: 500s)
How long a message must be queued before the Postfix SMTP client turns on the PIX firewall "<CR><LF>.<CR><LF>" bug workaround for delivery through firewalls with "smtp fixup" mode turned on.

By default, the workaround is turned off for mail that is queued for less than 500 seconds. In other words, the workaround is normally turned off for the first delivery attempt.

Specify 0 to enable the PIX firewall "<CR><LF>.<CR><LF>" bug workaround upon the first delivery attempt.

smtp_pix_workarounds (default: disable_esmtp, delay_dotcrlf)
A list that specifies zero or more workarounds for CISCO PIX firewall bugs. These workarounds are implemented by the Postfix SMTP client. Workaround names are separated by comma or space, and are case insensitive. This parameter setting can be overruled with per-destination smtp_pix_workaround_maps settings.

delay_dotcrlf
Insert a delay before sending ".<CR><LF>" after the end of the message content. The delay is subject to the smtp_pix_workaround_delay_time and smtp_pix_workaround_threshold_time parameter settings.

disable_esmtp
Disable all extended SMTP commands: send HELO instead of EHLO.

This feature is available in Postfix 2.4 and later. The default settings are backwards compatible with earlier Postfix versions.

smtp_quit_timeout (default: 300s)
The Postfix SMTP client time limit for sending the QUIT command, and for receiving the remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_quote_rfc821_envelope (default: yes)
Quote addresses in Postfix SMTP client MAIL FROM and RCPT TO commands as required by RFC 5321. This includes putting quotes around an address localpart that ends in ".".

The default is to comply with RFC 5321. If you have to send mail to a broken SMTP server, configure a special SMTP client in master.cf:

```
/etc/postfix/master.cf:
broken-smtp . . . smtp -o smtp_quote_rfc821_envelope=no
```

and route mail for the destination in question to the "broken-smtp" message delivery with a **transport(5)** table.

This feature is available in Postfix 2.1 and later.

smtp_randomize_addresses (default: yes)
Randomize the order of equal-preference MX host addresses. This is a performance feature of the Postfix SMTP client.

smtp_rcpt_timeout (default: 300s)
The Postfix SMTP client time limit for sending the SMTP RCPT TO command, and for receiving the remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtp_reply_filter (default: empty)
A mechanism to transform replies from remote SMTP servers one line at a time. This is a last-resort tool to work around server replies that break interoperability with the Postfix SMTP client. Other uses involve fault injection to test Postfix's handling of invalid responses.

Notes:

- In the case of a multi-line reply, the Postfix SMTP client uses the final reply line's numerical SMTP reply code and enhanced status code.
- The numerical SMTP reply code (XYZ) takes precedence over the enhanced status code (X.Y.Z). When the enhanced status code initial digit differs from the SMTP reply code initial digit, or when no enhanced status code is present, the Postfix SMTP client uses a generic enhanced status code (X.0.0) instead.

Specify the name of a "type:table" lookup table. The search string is a single SMTP reply line as received from the remote SMTP server, except that the trailing <CR><LF> are removed. When the lookup succeeds, the result replaces the single SMTP reply line.

Examples:

```
/etc/postfix/main.cf:
smtp_reply_filter = pcre:/etc/postfix/reply_filter
```

```
/etc/postfix/reply_filter:
# Transform garbage into "250-filler..." so that it looks like
# one line from a multi-line reply. It does not matter what we
# substitute here as long it has the right syntax. The Postfix
# SMTP client will use the final line's numerical SMTP reply
# code and enhanced status code.
!/^([2-5][0-9][0-9]($|[- ]))/ 250-filler for garbage
```

This feature is available in Postfix 2.7.

smtp_rset_timeout (default: 20s)
The Postfix SMTP client time limit for sending the RSET command, and for receiving the remote SMTP server response. The SMTP client sends RSET in order to finish a recipient address probe, or to verify that a cached session is still usable.

This feature is available in Postfix 2.1 and later.

smtp_sasl_auth_cache_name (default: empty)

An optional table to prevent repeated SASL authentication failures with the same remote SMTP server hostname, username and password. Each table (key, value) pair contains a server name, a username and password, and the full server response. This information is stored when a remote SMTP server rejects an authentication attempt with a 535 reply code. As long as the smtp_sasl_password_maps information does no change, and as long as the smtp_sasl_auth_cache_name information does not expire (see smtp_sasl_auth_cache_time) the Postfix SMTP client avoids SASL authentication attempts with the same server, username and password, and instead bounces or defers mail as controlled with the smtp_sasl_auth_soft_bounce configuration parameter.

Use a per-destination delivery concurrency of 1 (for example, "smtp_destination_concurrency_limit = 1", "relay_destination_concurrency_limit = 1", etc.), otherwise multiple delivery agents may experience a login failure at the same time.

The table must be accessed via the proxywrite service, i.e. the map name must start with "proxy:". The table should be stored under the directory specified with the data_directory parameter.

This feature uses cryptographic hashing to protect plain-text passwords, and requires that Postfix is compiled with TLS support.

Example:

```
smtp_sasl_auth_cache_name = proxy:btree:/var/lib/postfix/sasl_auth_cache
```

This feature is available in Postfix 2.5 and later.

smtp_sasl_auth_cache_time (default: 90d)

The maximal age of an smtp_sasl_auth_cache_name entry before it is removed.

This feature is available in Postfix 2.5 and later.

smtp_sasl_auth_enable (default: no)

Enable SASL authentication in the Postfix SMTP client. By default, the Postfix SMTP client uses no authentication.

Example:

```
smtp_sasl_auth_enable = yes
```

smtp_sasl_auth_soft_bounce (default: yes)

When a remote SMTP server rejects a SASL authentication request with a 535 reply code, defer mail delivery instead of returning mail as undeliverable. The latter behavior was hard-coded prior to Postfix version 2.5.

Note: the setting "yes" overrides the global soft_bounce parameter, but the setting "no" does not.

Example:

```
# Default as of Postfix 2.5
smtp_sasl_auth_soft_bounce = yes
# The old hard-coded default
smtp_sasl_auth_soft_bounce = no
```

This feature is available in Postfix 2.5 and later.

smtp_sasl_mechanism_filter (default: empty)

If non-empty, a Postfix SMTP client filter for the remote SMTP server’s list of offered SASL mechanisms. Different client and server implementations may support different mechanism lists; by default, the Postfix SMTP client will use the intersection of the two. smtp_sasl_mechanism_filter specifies an optional third mechanism list to intersect with.

Specify mechanism names, "/file/name" patterns or "type:table" lookup tables. The right-hand side result from "type:table" lookups is ignored. Specify "!pattern" to exclude a mechanism name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

This feature is available in Postfix 2.2 and later.

Examples:

```
smtp_sasl_mechanism_filter = plain, login
smtp_sasl_mechanism_filter = /etc/postfix/smtp_mechs
smtp_sasl_mechanism_filter = !gssapi, !login, static:rest
```

smtp_sasl_password_maps (default: empty)

Optional Postfix SMTP client lookup tables with one username:password entry per sender, remote hostname or next-hop domain. Per-sender lookup is done only when sender-dependent authentication is enabled. If no username:password entry is found, then the Postfix SMTP client will not attempt to authenticate to the remote host.

The Postfix SMTP client opens the lookup table before going to chroot jail, so you can leave the password file in /etc/postfix.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

smtp_sasl_path (default: empty)

Implementation-specific information that the Postfix SMTP client passes through to the SASL plug-in implementation that is selected with **smtp_sasl_type**. Typically this specifies the name of a configuration file or rendezvous point.

This feature is available in Postfix 2.3 and later.

smtp_sasl_security_options (default: noplaintext, noanonymous)

Postfix SMTP client SASL security options; as of Postfix 2.3 the list of available features depends on the SASL client implementation that is selected with **smtp_sasl_type**.

The following security features are defined for the **cyrus** client SASL implementation:

Specify zero or more of the following:

noplaintext
: Disallow methods that use plaintext passwords.

noactive
: Disallow methods subject to active (non-dictionary) attack.

nodictionary
: Disallow methods subject to passive (dictionary) attack.

noanonymous
: Disallow methods that allow anonymous authentication.

mutual_auth
: Only allow methods that provide mutual authentication (not available with SASL version 1).

Example:

```
smtp_sasl_security_options = noplaintext
```

smtp_sasl_tls_security_options (default: $smtp_sasl_security_options)

The SASL authentication security options that the Postfix SMTP client uses for TLS encrypted SMTP sessions.

This feature is available in Postfix 2.2 and later.

smtp_sasl_tls_verified_security_options (default: $smtp_sasl_tls_security_options)

The SASL authentication security options that the Postfix SMTP client uses for TLS encrypted SMTP sessions with a verified server certificate.

When mail is sent to the public MX host for the recipient’s domain, server certificates are by default optional, and delivery proceeds even if certificate verification fails. For delivery via a submission service that requires SASL authentication, it may be appropriate to send plaintext passwords only when the connection to the server is strongly encrypted **and** the server identity is verified.

The smtp_sasl_tls_verified_security_options parameter makes it possible to only enable plaintext mechanisms when a secure connection to the server is available. Submission servers subject to this policy must either have verifiable certificates or offer suitable non-plaintext SASL mechanisms.

This feature is available in Postfix 2.6 and later.

smtp_sasl_type (default: cyrus)
The SASL plug-in type that the Postfix SMTP client should use for authentication. The available types are listed with the "**postconf -A**" command.

This feature is available in Postfix 2.3 and later.

smtp_send_dummy_mail_auth (default: no)
Whether or not to append the "AUTH=<>" option to the MAIL FROM command in SASL-authenticated SMTP sessions. The default is not to send this, to avoid problems with broken remote SMTP servers. Before Postfix 2.9 the behavior is as if "smtp_send_dummy_mail_auth = yes".

This feature is available in Postfix 2.9 and later.

smtp_send_xforward_command (default: no)
Send the non-standard XFORWARD command when the Postfix SMTP server EHLO response announces XFORWARD support.

This allows a Postfix SMTP delivery agent, used for injecting mail into a content filter, to forward the name, address, protocol and HELO name of the original client to the content filter and downstream queuing SMTP server. This can produce more useful logging than localhost[127.0.0.1] etc.

This feature is available in Postfix 2.1 and later.

smtp_sender_dependent_authentication (default: no)
Enable sender-dependent authentication in the Postfix SMTP client; this is available only with SASL authentication, and disables SMTP connection caching to ensure that mail from different senders will use the appropriate credentials.

This feature is available in Postfix 2.3 and later.

smtp_skip_4xx_greeting (default: yes)
Skip SMTP servers that greet with a 4XX status code (go away, try again later).

By default, the Postfix SMTP client moves on the next mail exchanger. Specify "smtp_skip_4xx_greeting = no" if Postfix should defer delivery immediately.

This feature is available in Postfix 2.0 and earlier. Later Postfix versions always skip remote SMTP servers that greet with a 4XX status code.

smtp_skip_5xx_greeting (default: yes)
Skip remote SMTP servers that greet with a 5XX status code.

By default, the Postfix SMTP client moves on the next mail exchanger. Specify "smtp_skip_5xx_greeting = no" if Postfix should bounce the mail immediately. Caution: the latter behavior appears to contradict RFC 2821.

smtp_skip_quit_response (default: yes)
Do not wait for the response to the SMTP QUIT command.

smtp_starttls_timeout (default: 300s)
Time limit for Postfix SMTP client write and read operations during TLS startup and shutdown handshake procedures.

This feature is available in Postfix 2.2 and later.

smtp_tls_CAfile (default: empty)
A file containing CA certificates of root CAs trusted to sign either remote SMTP server certificates or intermediate CA certificates. These are loaded into memory before the **smtp(8)** client enters the chroot jail. If the number of trusted roots is large, consider using smtp_tls_CApath instead, but note that the latter directory must be present in the chroot jail if the **smtp(8)** client is chrooted. This file may also be used to

augment the client certificate trust chain, but it is best to include all the required certificates directly in $smtp_tls_cert_file.

Specify "smtp_tls_CAfile = /path/to/system_CA_file" to use ONLY the system-supplied default Certification Authority certificates.

Specify "tls_append_default_CA = no" to prevent Postfix from appending the system-supplied default CAs and trusting third-party certificates.

Example:

```
smtp_tls_CAfile = /etc/postfix/CAcert.pem
```

This feature is available in Postfix 2.2 and later.

smtp_tls_CApath (default: empty)

Directory with PEM format Certification Authority certificates that the Postfix SMTP client uses to verify a remote SMTP server certificate. Don’t forget to create the necessary "hash" links with, for example, "$OPENSSL_HOME/bin/c_rehash /etc/postfix/certs".

To use this option in chroot mode, this directory (or a copy) must be inside the chroot jail.

Specify "smtp_tls_CApath = /path/to/system_CA_directory" to use ONLY the system-supplied default Certification Authority certificates.

Specify "tls_append_default_CA = no" to prevent Postfix from appending the system-supplied default CAs and trusting third-party certificates.

Example:

```
smtp_tls_CApath = /etc/postfix/certs
```

This feature is available in Postfix 2.2 and later.

smtp_tls_block_early_mail_reply (default: no)

Try to detect a mail hijacking attack based on a TLS protocol vulnerability (CVE-2009-3555), where an attacker prepends malicious HELO, MAIL, RCPT, DATA commands to a Postfix SMTP client TLS session. The attack would succeed with non-Postfix SMTP servers that reply to the malicious HELO, MAIL, RCPT, DATA commands after negotiating the Postfix SMTP client TLS session.

This feature is available in Postfix 2.7.

smtp_tls_cert_file (default: empty)

File with the Postfix SMTP client RSA certificate in PEM format. This file may also contain the Postfix SMTP client private RSA key, and these may be the same as the Postfix SMTP server RSA certificate and key file.

Do not configure client certificates unless you **must** present client TLS certificates to one or more servers. Client certificates are not usually needed, and can cause problems in configurations that work well without them. The recommended setting is to let the defaults stand:

```
smtp_tls_cert_file =
smtp_tls_key_file =
smtp_tls_dcert_file =
smtp_tls_dkey_file =
smtp_tls_eccert_file =
smtp_tls_eckey_file =
```

The best way to use the default settings is to comment out the above parameters in main.cf if present.

To enable remote SMTP servers to verify the Postfix SMTP client certificate, the issuing CA certificates must be made available to the server. You should include the required certificates in the client certificate file, the client certificate first, then the issuing CA(s) (bottom-up order).

Example: the certificate for "client.example.com" was issued by "intermediate CA" which itself has a certificate issued by "root CA". Create the client.pem file with "cat client_cert.pem intermediate_CA.pem

root_CA.pem > client.pem".

If you also want to verify remote SMTP server certificates issued by these CAs, you can add the CA certificates to the smtp_tls_CAfile, in which case it is not necessary to have them in the smtp_tls_cert_file, smtp_tls_dcert_file or smtp_tls_eccert_file.

A certificate supplied here must be usable as an SSL client certificate and hence pass the "openssl verify -purpose sslclient ..." test.

Example:

```
smtp_tls_cert_file = /etc/postfix/client.pem
```

This feature is available in Postfix 2.2 and later.

smtp_tls_cipherlist (default: empty)

Obsolete Postfix < 2.3 control for the Postfix SMTP client TLS cipher list. As this feature applies to all TLS security levels, it is easy to create interoperability problems by choosing a non-default cipher list. Do not use a non-default TLS cipher list on hosts that deliver email to the public Internet: you will be unable to send email to servers that only support the ciphers you exclude. Using a restricted cipher list may be more appropriate for an internal MTA, where one can exert some control over the TLS software and settings of the peer servers.

Note: do not use "" quotes around the parameter value.

This feature is available in Postfix version 2.2. It is not used with Postfix 2.3 and later; use smtp_tls_mandatory_ciphers instead.

smtp_tls_ciphers (default: medium)

The minimum TLS cipher grade that the Postfix SMTP client will use with opportunistic TLS encryption. Cipher types listed in smtp_tls_exclude_ciphers are excluded from the base definition of the selected cipher grade. The default value is "medium" for Postfix releases after the middle of 2015, "export" for older releases.

When TLS is mandatory the cipher grade is chosen via the smtp_tls_mandatory_ciphers configuration parameter, see there for syntax details. See smtp_tls_policy_maps for information on how to configure ciphers on a per-destination basis.

This feature is available in Postfix 2.6 and later. With earlier Postfix releases only the smtp_tls_mandatory_ciphers parameter is implemented, and opportunistic TLS always uses "export" or better (i.e. all) ciphers.

smtp_tls_dane_insecure_mx_policy (default: dane)

The TLS policy for MX hosts with "secure" TLSA records when the nexthop destination security level is **dane**, but the MX record was found via an "insecure" MX lookup. The choices are:

may The TLSA records will be ignored and TLS will be optional. If the MX host does not appear to support STARTTLS, or the STARTTLS handshake fails, mail may be sent in the clear.

encrypt
The TLSA records will signal a requirement to use TLS. While TLS encryption will be required, authentication will not be performed.

dane (default)
The TLSA records will be used just as with "secure" MX records. TLS encryption will be required, and, if at least one of the TLSA records is "usable", authentication will be required. When authentication succeeds, it will be logged only as "Trusted", not "Verified", because the MX host name could have been forged.
Though with "insecure" MX records an active attacker can compromise SMTP transport security by returning forged MX records, such attacks are "tamper-evident" since any forged MX hostnames will be recorded in the mail logs. Attackers who place a high value staying hidden may be deterred from forging MX records.

This feature is available in Postfix 3.1 and later. The **may** policy is backwards-compatible with earlier

Postfix versions.

smtp_tls_dcert_file (default: empty)
File with the Postfix SMTP client DSA certificate in PEM format. This file may also contain the Postfix SMTP client private DSA key.

See the discussion under smtp_tls_cert_file for more details.

Example:

```
smtp_tls_dcert_file = /etc/postfix/client-dsa.pem
```

This feature is available in Postfix 2.2 and later.

smtp_tls_dkey_file (default: $smtp_tls_dcert_file)
File with the Postfix SMTP client DSA private key in PEM format. This file may be combined with the Postfix SMTP client DSA certificate file specified with $smtp_tls_dcert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

This feature is available in Postfix 2.2 and later.

smtp_tls_eccert_file (default: empty)
File with the Postfix SMTP client ECDSA certificate in PEM format. This file may also contain the Postfix SMTP client ECDSA private key.

See the discussion under smtp_tls_cert_file for more details.

Example:

```
smtp_tls_eccert_file = /etc/postfix/ecdsa-ccert.pem
```

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

smtp_tls_eckey_file (default: $smtp_tls_eccert_file)
File with the Postfix SMTP client ECDSA private key in PEM format. This file may be combined with the Postfix SMTP client ECDSA certificate file specified with $smtp_tls_eccert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

smtp_tls_enforce_peername (default: yes)
With mandatory TLS encryption, require that the remote SMTP server hostname matches the information in the remote SMTP server certificate. As of RFC 2487 the requirements for hostname checking for MTA clients are not specified.

This option can be set to "no" to disable strict peer name checking. This setting has no effect on sessions that are controlled via the smtp_tls_per_site table.

Disabling the hostname verification can make sense in closed environment where special CAs are created. If not used carefully, this option opens the danger of a "man-in-the-middle" attack (the CommonName of this attacker will be logged).

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtp_tls_security_level instead.

smtp_tls_exclude_ciphers (default: empty)
List of ciphers or cipher types to exclude from the Postfix SMTP client cipher list at all TLS security levels. This is not an OpenSSL cipherlist, it is a simple list separated by whitespace and/or commas. The elements are a single cipher, or one or more "+" separated cipher properties, in which case only ciphers matching **all** the properties are excluded.

Examples (some of these will cause problems):

```
smtp_tls_exclude_ciphers = aNULL
smtp_tls_exclude_ciphers = MD5, DES
smtp_tls_exclude_ciphers = DES+MD5
smtp_tls_exclude_ciphers = AES256-SHA, DES-CBC3-MD5
smtp_tls_exclude_ciphers = kEDH+aRSA
```

The first setting, disables anonymous ciphers. The next setting disables ciphers that use the MD5 digest algorithm or the (single) DES encryption algorithm. The next setting disables ciphers that use MD5 and DES together. The next setting disables the two ciphers "AES256-SHA" and "DES-CBC3-MD5". The last setting disables ciphers that use "EDH" key exchange with RSA authentication.

This feature is available in Postfix 2.3 and later.

smtp_tls_fingerprint_cert_match (default: empty)

List of acceptable remote SMTP server certificate fingerprints for the "fingerprint" TLS security level (**smtp_tls_security_level** = fingerprint). At this security level, Certification Authorities are not used, and certificate expiration times are ignored. Instead, server certificates are verified directly via their certificate fingerprint or public key fingerprint (Postfix 2.9 and later). The fingerprint is a message digest of the server certificate (or public key). The digest algorithm is selected via the **smtp_tls_fingerprint_digest** parameter.

When an **smtp_tls_policy_maps** table entry specifies the "fingerprint" security level, any "match" attributes in that entry specify the list of valid fingerprints for the corresponding destination. Multiple fingerprints can be combined with a "|" delimiter in a single match attribute, or multiple match attributes can be employed.

Example: Certificate fingerprint verification with internal mailhub. Two matching fingerprints are listed. The relayhost may be multiple physical hosts behind a load-balancer, each with its own private/public key and self-signed certificate. Alternatively, a single relayhost may be in the process of switching from one set of private/public keys to another, and both keys are trusted just prior to the transition.

```
relayhost = [mailhub.example.com]
smtp_tls_security_level = fingerprint
smtp_tls_fingerprint_digest = md5
smtp_tls_fingerprint_cert_match =
3D:95:34:51:24:66:33:B9:D2:40:99:C0:C1:17:0B:D1
EC:3B:2D:B0:5B:B1:FB:6D:20:A3:9D:72:F6:8D:12:35
```

Example: Certificate fingerprint verification with selected destinations. As in the example above, we show two matching fingerprints:

```
/etc/postfix/main.cf:
smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
smtp_tls_fingerprint_digest = md5

/etc/postfix/tls_policy:
example.com fingerprint
match=3D:95:34:51:24:66:33:B9:D2:40:99:C0:C1:17:0B:D1
match=EC:3B:2D:B0:5B:B1:FB:6D:20:A3:9D:72:F6:8D:12:35
```

This feature is available in Postfix 2.5 and later.

smtp_tls_fingerprint_digest (default: md5)

The message digest algorithm used to construct remote SMTP server certificate fingerprints. At the "fingerprint" TLS security level (**smtp_tls_security_level** = fingerprint), the server certificate is verified by directly matching its certificate fingerprint or its public key fingerprint (Postfix 2.9 and later). The fingerprint is the message digest of the server certificate (or its public key) using the selected algorithm. With a digest algorithm resistant to "second pre-image" attacks, it is not feasible to create a new public key and a matching certificate (or public/private key-pair) that has the same fingerprint.

The default algorithm is **md5**; this is consistent with the backwards compatible setting of the digest used to verify client certificates in the SMTP server.

The best practice algorithm is now **sha1**. Recent advances in hash function cryptanalysis have led to md5

being deprecated in favor of sha1. However, as long as there are no known "second pre-image" attacks against md5, its use in this context can still be considered safe.

While additional digest algorithms are often available with OpenSSL's libcrypto, only those used by libssl in SSL cipher suites are available to Postfix. For now this means just md5 or sha1.

To find the fingerprint of a specific certificate file, with a specific digest algorithm, run:

```
$ openssl x509 -noout -fingerprint -digest -in certfile.pem
```

The text to the right of "=" sign is the desired fingerprint. For example:

```
$ openssl x509 -noout -fingerprint -sha1 -in cert.pem
SHA1 Fingerprint=D4:6A:AB:19:24:79:F8:32:BB:A6:CB:66:82:C0:8E:9B:EE:29:A8:1
```

To extract the public key fingerprint from an X.509 certificate, you need to extract the public key from the certificate and compute the appropriate digest of its DER (ASN.1) encoding. With OpenSSL the "-pubkey" option of the "x509" command extracts the public key always in "PEM" format. We pipe the result to another OpenSSL command that converts the key to DER and then to the "dgst" command to compute the fingerprint.

The actual command to transform the key to DER format depends on the version of OpenSSL used. With OpenSSL 1.0.0 and later, the "pkey" command supports all key types. With OpenSSL 0.9.8 and earlier, the key type is always RSA (nobody uses DSA, and EC keys are not fully supported by 0.9.8), so the "rsa" command is used.

```
# OpenSSL 1.0 with all certificates and SHA-1 fingerprints.
$ openssl x509 -in cert.pem -noout -pubkey |
openssl pkey -pubin -outform DER |
openssl dgst -sha1 -c
(stdin)= 64:3f:1f:f6:e5:1e:d4:2a:56:8b:fc:09:1a:61:98:b5:bc:7c:60:58
```

```
# OpenSSL 0.9.8 with RSA certificates and MD5 fingerprints.
$ openssl x509 -in cert.pem -noout -pubkey |
openssl rsa -pubin -outform DER |
openssl dgst -md5 -c
(stdin)= f4:62:60:f6:12:8f:d5:8d:28:4d:13:a7:db:b2:ff:50
```

The Postfix SMTP server and client log the peer (leaf) certificate fingerprint and public key fingerprint when the TLS loglevel is 2 or higher.

Note: Postfix 2.9.0-2.9.5 computed the public key fingerprint incorrectly. To use public-key fingerprints, upgrade to Postfix 2.9.6 or later.

This feature is available in Postfix 2.5 and later.

smtp_tls_force_insecure_host_tlsa_lookup (default: no)

Lookup the associated DANE TLSA RRset even when a hostname is not an alias and its address records lie in an unsigned zone. This is unlikely to ever yield DNSSEC validated results, since child zones of unsigned zones are also unsigned in the absence of DLV or locally configured non-root trust-anchors. We anticipate that such mechanisms will not be used for just the "_tcp" subdomain of a host. Suppressing the TLSA RRset lookup reduces latency and avoids potential interoperability problems with nameservers for unsigned zones that are not prepared to handle the new TLSA RRset.

This feature is available in Postfix 2.11.

smtp_tls_key_file (default: $smtp_tls_cert_file)

File with the Postfix SMTP client RSA private key in PEM format. This file may be combined with the Postfix SMTP client RSA certificate file specified with $smtp_tls_cert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

Example:

```
smtp_tls_key_file = $smtp_tls_cert_file
```

This feature is available in Postfix 2.2 and later.

smtp_tls_loglevel (default: 0)

Enable additional Postfix SMTP client logging of TLS activity. Each logging level also includes the information that is logged at a lower logging level.

0 Disable logging of TLS activity.

1 Log only a summary message on TLS handshake completion - no logging of remote SMTP server certificate trust-chain verification errors if server certificate verification is not required. With Postfix 2.8 and earlier, log the summary message and unconditionally log trust-chain verification errors.

2 Also log levels during TLS negotiation.

3 Also log hexadecimal and ASCII dump of TLS negotiation process.

4 Also log hexadecimal and ASCII dump of complete transmission after STARTTLS.

Do not use "smtp_tls_loglevel = 2" or higher except in case of problems. Use of loglevel 4 is strongly discouraged.

This feature is available in Postfix 2.2 and later.

smtp_tls_mandatory_ciphers (default: medium)

The minimum TLS cipher grade that the Postfix SMTP client will use with mandatory TLS encryption. The default value "medium" is suitable for most destinations with which you may want to enforce TLS, and is beyond the reach of today’s cryptanalytic methods. See smtp_tls_policy_maps for information on how to configure ciphers on a per-destination basis.

The following cipher grades are supported:

export Enable "EXPORT" grade or better OpenSSL ciphers. The underlying cipherlist is specified via the tls_export_cipherlist configuration parameter, which you are strongly encouraged to not change. This choice is insecure and SHOULD NOT be used.

low Enable "LOW" grade or better OpenSSL ciphers. The underlying cipherlist is specified via the tls_low_cipherlist configuration parameter, which you are strongly encouraged to not change. This choice is insecure and SHOULD NOT be used.

medium
Enable "MEDIUM" grade or better OpenSSL ciphers. The underlying cipherlist is specified via the tls_medium_cipherlist configuration parameter, which you are strongly encouraged to not change.

high Enable only "HIGH" grade OpenSSL ciphers. This setting may be appropriate when all mandatory TLS destinations (e.g. when all mail is routed to a suitably capable relayhost) support at least one "HIGH" grade cipher. The underlying cipherlist is specified via the tls_high_cipherlist configuration parameter, which you are strongly encouraged to not change.

null Enable only the "NULL" OpenSSL ciphers, these provide authentication without encryption. This setting is only appropriate in the rare case that all servers are prepared to use NULL ciphers (not normally enabled in TLS servers). A plausible use-case is an LMTP server listening on a UNIX-domain socket that is configured to support "NULL" ciphers. The underlying cipherlist is specified via the tls_null_cipherlist configuration parameter, which you are strongly encouraged to not change.

The underlying cipherlists for grades other than "null" include anonymous ciphers, but these are automatically filtered out if the Postfix SMTP client is configured to verify server certificates. You are very unlikely to need to take any steps to exclude anonymous ciphers, they are excluded automatically as necessary. If you must exclude anonymous ciphers at the "may" or "encrypt" security levels, when the Postfix SMTP client does not need or use peer certificates, set "smtp_tls_exclude_ciphers = aNULL". To exclude anonymous ciphers only when TLS is enforced, set "smtp_tls_mandatory_exclude_ciphers = aNULL".

This feature is available in Postfix 2.3 and later.

smtp_tls_mandatory_exclude_ciphers (default: empty)

Additional list of ciphers or cipher types to exclude from the Postfix SMTP client cipher list at mandatory TLS security levels. This list works in addition to the exclusions listed with smtp_tls_exclude_ciphers (see there for syntax details).

Starting with Postfix 2.6, the mandatory cipher exclusions can be specified on a per-destination basis via the TLS policy "exclude" attribute. See smtp_tls_policy_maps for notes and examples.

This feature is available in Postfix 2.3 and later.

smtp_tls_mandatory_protocols (default: !SSLv2, !SSLv3)

List of SSL/TLS protocols that the Postfix SMTP client will use with mandatory TLS encryption. In main.cf the values are separated by whitespace, commas or colons. In the policy table "protocols" attribute (see smtp_tls_policy_maps) the only valid separator is colon. An empty value means allow all protocols. The valid protocol names, (see \fBfBSSL_get_version(3)), are "SSLv2", "SSLv3" and "TLSv1". The default value is "!SSLv2, !SSLv3" for Postfix releases after the middle of 2015, "!SSLv2" for older releases.

With Postfix >= 2.5 the parameter syntax was expanded to support protocol exclusions. One can explicitly exclude "SSLv2" by setting "smtp_tls_mandatory_protocols = !SSLv2". To exclude both "SSLv2" and "SSLv3" set "smtp_tls_mandatory_protocols = !SSLv2, !SSLv3". Listing the protocols to include, rather than protocols to exclude, is supported, but not recommended. The exclusion form more closely matches the underlying OpenSSL interface semantics.

The range of protocols advertised by an SSL/TLS client must be contiguous. When a protocol version is enabled, disabling any higher version implicitly disables all versions above that higher version. Thus, for example (assuming the OpenSSL library supports both SSLv2 and SSLv3):

```
smtp_tls_mandatory_protocols = !SSLv2, !TLSv1
```

also disables any protocols version higher than TLSv1 leaving only "SSLv3" enabled.

Note: As of OpenSSL 1.0.1 two new protocols are defined, "TLSv1.1" and "TLSv1.2". When Postfix <= 2.5 is linked against OpenSSL 1.0.1 or later, these, or any other new protocol versions, cannot be disabled except by also disabling "TLSv1" (typically leaving just "SSLv3"). The latest patch levels of Postfix >= 2.6, and all versions of Postfix >= 2.10 can explicitly disable support for "TLSv1.1" or "TLSv1.2".

OpenSSL 1.1.1 introduces support for "TLSv1.3". With Postfix >= 3.4 (or patch releases >= 3.0.14, 3.1.10, 3.2.7 and 3.3.2) this can be disabled, if need be, via "!TLSv1.3".

At the dane and dane-only security levels, when usable TLSA records are obtained for the remote SMTP server, the Postfix SMTP client is obligated to include the SNI TLS extension in its SSL client hello message. This may help the remote SMTP server live up to its promise to provide a certificate that matches its TLSA records. Since TLS extensions require TLS 1.0 or later, the Postfix SMTP client must disable "SSLv2" and "SSLv3" when SNI is required. If you use "dane" or "dane-only" do not disable TLSv1, except perhaps via the policy table for destinations which you are sure will support "TLSv1.1" or "TLSv1.2".

See the documentation of the smtp_tls_policy_maps parameter and TLS_README for more information about security levels.

Example:

```
# Preferred syntax with Postfix >= 2.5:
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
# Legacy syntax:
smtp_tls_mandatory_protocols = TLSv1
```

This feature is available in Postfix 2.3 and later.

smtp_tls_note_starttls_offer (default: no)

Log the hostname of a remote SMTP server that offers STARTTLS, when TLS is not already enabled for that server.

The logfile record looks like:

```
postfix/smtp[pid]: Host offered STARTTLS: [name.of.host]
```

This feature is available in Postfix 2.2 and later.

smtp_tls_per_site (default: empty)

Optional lookup tables with the Postfix SMTP client TLS usage policy by next-hop destination and by remote SMTP server hostname. When both lookups succeed, the more specific per-site policy (NONE, MUST, etc) overrides the less specific one (MAY), and the more secure per-site policy (MUST, etc) overrides the less secure one (NONE). With Postfix 2.3 and later smtp_tls_per_site is strongly discouraged: use smtp_tls_policy_maps instead.

Use of the bare hostname as the per-site table lookup key is discouraged. Always use the full destination nexthop (enclosed in [] with a possible ":port" suffix). A recipient domain or MX-enabled transport nexthop with no port suffix may look like a bare hostname, but is still a suitable *destination*.

Specify a next-hop destination or server hostname on the left-hand side; no wildcards are allowed. The next-hop destination is either the recipient domain, or the destination specified with a **transport(5)** table, the relayhost parameter, or the relay_transport parameter. On the right hand side specify one of the following keywords:

NONE Don't use TLS at all. This overrides a less specific **MAY** lookup result from the alternate host or next-hop lookup key, and overrides the global smtp_use_tls, smtp_enforce_tls, and smtp_tls_enforce_peername settings.

MAY Try to use TLS if the server announces support, otherwise use the unencrypted connection. This has less precedence than a more specific result (including **NONE**) from the alternate host or next-hop lookup key, and has less precedence than the more specific global "smtp_enforce_tls = yes" or "smtp_tls_enforce_peername = yes".

MUST_NOPEERMATCH
Require TLS encryption, but do not require that the remote SMTP server hostname matches the information in the remote SMTP server certificate, or that the server certificate was issued by a trusted CA. This overrides a less secure **NONE** or a less specific **MAY** lookup result from the alternate host or next-hop lookup key, and overrides the global smtp_use_tls, smtp_enforce_tls and smtp_tls_enforce_peername settings.

MUST Require TLS encryption, require that the remote SMTP server hostname matches the information in the remote SMTP server certificate, and require that the remote SMTP server certificate was issued by a trusted CA. This overrides a less secure **NONE** and **MUST_NOPEERMATCH** or a less specific **MAY** lookup result from the alternate host or next-hop lookup key, and overrides the global smtp_use_tls, smtp_enforce_tls and smtp_tls_enforce_peername settings.

The above keywords correspond to the "none", "may", "encrypt" and "verify" security levels for the new smtp_tls_security_level parameter introduced in Postfix 2.3. Starting with Postfix 2.3, and independently of how the policy is specified, the smtp_tls_mandatory_ciphers and smtp_tls_mandatory_protocols parameters apply when TLS encryption is mandatory. Connections for which encryption is optional typically enable all "export" grade and better ciphers (see smtp_tls_ciphers and smtp_tls_protocols).

As long as no secure DNS lookup mechanism is available, false hostnames in MX or CNAME responses can change the server hostname that Postfix uses for TLS policy lookup and server certificate verification. Even with a perfect match between the server hostname and the server certificate, there is no guarantee that Postfix is connected to the right server. See TLS_README (Closing a DNS loophole with obsolete per-site TLS policies) for a possible work-around.

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtp_tls_policy_maps instead.

smtp_tls_policy_maps (default: empty)

Optional lookup tables with the Postfix SMTP client TLS security policy by next-hop destination; when a non-empty value is specified, this overrides the obsolete smtp_tls_per_site parameter. See TLS_README for a more detailed discussion of TLS security levels.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

The TLS policy table is indexed by the full next-hop destination, which is either the recipient domain, or the verbatim next-hop specified in the transport table, $local_transport, $virtual_transport, $relay_transport or $default_transport. This includes any enclosing square brackets and any non-default destination server port suffix. The LMTP socket type prefix (inet: or unix:) is not included in the lookup key.

Only the next-hop domain, or $myhostname with LMTP over UNIX-domain sockets, is used as the nexthop name for certificate verification. The port and any enclosing square brackets are used in the table lookup key, but are not used for server name verification.

When the lookup key is a domain name without enclosing square brackets or any *:port* suffix (typically the recipient domain), and the full domain is not found in the table, just as with the **transport(5)** table, the parent domain starting with a leading "." is matched recursively. This allows one to specify a security policy for a recipient domain and all its sub-domains.

The lookup result is a security level, followed by an optional list of whitespace and/or comma separated name=value attributes that override related main.cf settings. The TLS security levels in order of increasing security are:

none No TLS. No additional attributes are supported at this level.

may Opportunistic TLS. Since sending in the clear is acceptable, demanding stronger than default TLS security merely reduces interoperability. The optional "ciphers", "exclude" and "protocols" attributes (available for opportunistic TLS with Postfix >= 2.6) override the "smtp_tls_ciphers", "smtp_tls_exclude_ciphers" and "smtp_tls_protocols" configuration parameters. When opportunistic TLS handshakes fail, Postfix retries the connection with TLS disabled. This allows mail delivery to sites with non-interoperable TLS implementations.

encrypt
Mandatory TLS encryption. At this level and higher, the optional "protocols" attribute overrides the main.cf smtp_tls_mandatory_protocols parameter, the optional "ciphers" attribute overrides the main.cf smtp_tls_mandatory_ciphers parameter, and the optional "exclude" attribute (Postfix >= 2.6) overrides the main.cf smtp_tls_mandatory_exclude_ciphers parameter. In the policy table, multiple protocols or excluded ciphers must be separated by colons, as attribute values may not contain whitespace or commas.

dane Opportunistic DANE TLS. The TLS policy for the destination is obtained via TLSA records in DNSSEC. If no TLSA records are found, the effective security level used is may. If TLSA records are found, but none are usable, the effective security level is encrypt. When usable TLSA records are obtained for the remote SMTP server, the server certificate must match the TLSA records. RFC 6698 (DANE) TLS authentication and DNSSEC support is available with Postfix 2.11 and later.

dane-only
Mandatory DANE TLS. The TLS policy for the destination is obtained via TLSA records in DNSSEC. If no TLSA records are found, or none are usable, no connection is made to the server. When usable TLSA records are obtained for the remote SMTP server, the server certificate must match the TLSA records. RFC 6698 (DANE) TLS authentication and DNSSEC support is available with Postfix 2.11 and later.

fingerprint
Certificate fingerprint verification. Available with Postfix 2.5 and later. At this security level, there are no trusted Certification Authorities. The certificate trust chain, expiration date, ... are not checked. Instead, the optional**match** attrib ute, or else the main.cf

smtp_tls_fingerprint_cert_match parameter, lists the certificate fingerprints or the public key fingerprint (Postfix 2.9 and later) of the valid server certificate. The digest algorithm used to calculate the fingerprint is selected by the **smtp_tls_fingerprint_digest** parameter. Multiple fingerprints can be combined with a "|" delimiter in a single match attribute, or multiple match attributes can be employed. The ":" character is not used as a delimiter as it occurs between each pair of fingerprint (hexadecimal) digits.

verify Mandatory TLS verification. At this security level, DNS MX lookups are trusted to be secure enough, and the name verified in the server certificate is usually obtained indirectly via unauthenticated DNS MX lookups. The optional "match" attribute overrides the main.cf smtp_tls_verify_cert_match parameter. In the policy table, multiple match patterns and strategies must be separated by colons. In practice explicit control over matching is more common with the "secure" policy, described below.

secure Secure-channel TLS. At this security level, DNS MX lookups, though potentially used to determine the candidate next-hop gateway IP addresses, are **not** trusted to be secure enough for TLS peername verification. Instead, the default name verified in the server certificate is obtained directly from the next-hop, or is explicitly specified via the optional **match** attribute which overrides the main.cf smtp_tls_secure_cert_match parameter. In the policy table, multiple match patterns and strategies must be separated by colons. The match attribute is most useful when multiple domains are supported by common server, the policy entries for additional domains specify matching rules for the primary domain certificate. While transport table overrides routing the secondary domains to the primary nexthop also allow secure verification, they risk delivery to the wrong destination when domains change hands or are re-assigned to new gateways. With the "match" attribute approach, routing is not perturbed, and mail is deferred if verification of a new MX host fails.

Example:

```
/etc/postfix/main.cf:
smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
# Postfix 2.5 and later
smtp_tls_fingerprint_digest = md5

/etc/postfix/tls_policy:
example.edu none
example.mil may
example.gov encrypt protocols=TLSv1
example.com verify ciphers=high
example.net secure
[mail.example.org]:587 secure match=nexthop
# Postfix 2.5 and later
[thumb.example.org] fingerprint
match=EC:3B:2D:B0:5B:B1:FB:6D:20:A3:9D:72:F6:8D:12:35
match=3D:95:34:51:24:66:33:B9:D2:40:99:C0:C1:17:0B:D1
```

Note: The **hostname** strategy if listed in a non-default setting of smtp_tls_secure_cert_match or in the **match** attribute in the policy table can render the **secure** level vulnerable to DNS forgery. Do not use the **hostname** strategy for secure-channel configurations in environments where DNS security is not assured.

This feature is available in Postfix 2.3 and later.

smtp_tls_protocols (default: !SSLv2, !SSLv3)

List of TLS protocols that the Postfix SMTP client will exclude or include with opportunistic TLS encryption. The default value is "!SSLv2, !SSLv3" for Postfix releases after the middle of 2015, "!SSLv2" for older releases. Before Postfix 2.6, the Postfix SMTP client would use all protocols with opportunistic TLS.

In main.cf the values are separated by whitespace, commas or colons. In the policy table (see smtp_tls_policy_maps) the only valid separator is colon. An empty value means allow all protocols. The valid protocol names, (see \fBfBSSL_get_version(3)), are "SSLv2", "SSLv3" and "TLSv1".

The range of protocols advertised by an SSL/TLS client must be contiguous. When a protocol version is enabled, disabling any higher version implicitly disables all versions above that higher version. Thus, for example (assuming the OpenSSL library supports both SSLv2 and SSLv3):

```
smtp_tls_protocols = !SSLv2, !TLSv1
```

also disables any protocols version higher than TLSv1 leaving only "SSLv3" enabled.

Note: As of OpenSSL 1.0.1 two new protocols are defined, "TLSv1.1" and "TLSv1.2". The latest patch levels of Postfix >= 2.6, and all versions of Postfix >= 2.10 can explicitly disable support for "TLSv1.1" or "TLSv1.2"

OpenSSL 1.1.1 introduces support for "TLSv1.3". With Postfix >= 3.4 (or patch releases >= 3.0.14, 3.1.10, 3.2.7 and 3.3.2) this can be disabled, if need be, via "!TLSv1.3".

To include a protocol list its name, to exclude it, prefix the name with a "!" character. To exclude SSLv2 for opportunistic TLS set "smtp_tls_protocols = !SSLv2". To exclude both "SSLv2" and "SSLv3" set "smtp_tls_protocols = !SSLv2, !SSLv3". Explicitly listing the protocols to include, rather than protocols to exclude, is supported, but not recommended. The exclusion form more closely matches the underlying OpenSSL interface semantics.

Example:

```
# TLSv1 or better:
smtp_tls_protocols = !SSLv2, !SSLv3
```

This feature is available in Postfix 2.6 and later.

smtp_tls_scert_verifydepth (default: 9)

The verification depth for remote SMTP server certificates. A depth of 1 is sufficient if the issuing CA is listed in a local CA file.

The default verification depth is 9 (the OpenSSL default) for compatibility with earlier Postfix behavior. Prior to Postfix 2.5, the default value was 5, but the limit was not actually enforced. If you have set this to a lower non-default value, certificates with longer trust chains may now fail to verify. Certificate chains with 1 or 2 CAs are common, deeper chains are more rare and any number between 5 and 9 should suffice in practice. You can choose a lower number if, for example, you trust certificates directly signed by an issuing CA but not any CAs it delegates to.

This feature is available in Postfix 2.2 and later.

smtp_tls_secure_cert_match (default: nexthop, dot−nexthop)

How the Postfix SMTP client verifies the server certificate peername for the "secure" TLS security level. In a "secure" TLS policy table ($smtp_tls_policy_maps) entry the optional "match" attribute overrides this main.cf setting.

This parameter specifies one or more patterns or strategies separated by commas, whitespace or colons. In the policy table the only valid separator is the colon character.

For a description of the pattern and strategy syntax see the smtp_tls_verify_cert_match parameter. The "hostname" strategy should be avoided in this context, as in the absence of a secure global DNS, using the results of MX lookups in certificate verification is not immune to active (man-in-the-middle) attacks on DNS.

Sample main.cf setting:

```
smtp_tls_secure_cert_match = nexthop
```

Sample policy table override:

```
example.net secure match=example.com:.example.com
.example.net secure match=example.com:.example.com
```

This feature is available in Postfix 2.3 and later.

smtp_tls_security_level (default: empty)

The default SMTP TLS security level for the Postfix SMTP client; when a non-empty value is specified, this overrides the obsolete parameters smtp_use_tls, smtp_enforce_tls, and smtp_tls_enforce_peername.

Specify one of the following security levels:

none No TLS. TLS will not be used unless enabled for specific destinations via smtp_tls_policy_maps.

may Opportunistic TLS. Use TLS if this is supported by the remote SMTP server, otherwise use plaintext. Since sending in the clear is acceptable, demanding stronger than default TLS security merely reduces interoperability. The "smtp_tls_ciphers" and "smtp_tls_protocols" (Postfix >= 2.6) configuration parameters provide control over the protocols and cipher grade used with opportunistic TLS. With earlier releases the opportunistic TLS cipher grade is always "export" and no protocols are disabled. When TLS handshakes fail, the connection is retried with TLS disabled. This allows mail delivery to sites with non-interoperable TLS implementations.

encrypt

Mandatory TLS encryption. Since a minimum level of security is intended, it is reasonable to be specific about sufficiently secure protocol versions and ciphers. At this security level and higher, the main.cf parameters smtp_tls_mandatory_protocols and smtp_tls_mandatory_ciphers specify the TLS protocols and minimum cipher grade which the administrator considers secure enough for mandatory encrypted sessions. This security level is not an appropriate default for systems delivering mail to the Internet.

dane Opportunistic DANE TLS. At this security level, the TLS policy for the destination is obtained via DNSSEC. For TLSA policy to be in effect, the destination domain's containing DNS zone must be signed and the Postfix SMTP client's operating system must be configured to send its DNS queries to a recursive DNS nameserver that is able to validate the signed records. Each MX host's DNS zone should also be signed, and should publish DANE TLSA (RFC 6698) records that specify how that MX host's TLS certificate is to be verified. TLSA records do not preempt the normal SMTP MX host selection algorithm, if some MX hosts support TLSA and others do not, TLS security will vary from delivery to delivery. It is up to the domain owner to configure their MX hosts and their DNS sensibly. To configure the Postfix SMTP client for DNSSEC lookups see the documentation for the smtp_dns_support_level main.cf parameter. When DNSSEC-validated TLSA records are not found the effective tls security level is "may". When TLSA records are found, but are all unusable the effective security level is "encrypt". For purposes of protocol and cipher selection, the "dane" security level is treated like a "mandatory" TLS security level, and weak ciphers and protocols are disabled. Since DANE authenticates server certificates the "aNULL" cipher-suites are transparently excluded at this level, no need to configure this manually. RFC 6698 (DANE) TLS authentication is available with Postfix 2.11 and later.

dane-only

Mandatory DANE TLS. This is just like "dane" above, but DANE TLSA authentication is required. There is no fallback to "may" or "encrypt" when TLSA records are missing or unusable. RFC 6698 (DANE) TLS authentication is available with Postfix 2.11 and later.

fingerprint

Certificate fingerprint verification. At this security level, there are no trusted Certification Authorities. The certificate trust chain, expiration date, etc., are not checked. Instead, the **smtp_tls_fingerprint_cert_match** parameter lists the certificate fingerprint or public key fingerprint (Postfix 2.9 and later) of the valid server certificate. The digest algorithm used to calculate the fingerprint is selected by the **smtp_tls_fingerprint_digest** parameter. Available with Postfix 2.5 and later.

verify Mandatory TLS verification. At this security level, DNS MX lookups are trusted to be secure enough, and the name verified in the server certificate is usually obtained indirectly via unauthenticated DNS MX lookups. The smtp_tls_verify_cert_match parameter controls how the server name is verified. In practice explicit control over matching is more common at the "secure" level, described below. This security level is not an appropriate default for systems delivering mail to the Internet.

secure Secure-channel TLS. At this security level, DNS MX lookups, though potentially used to determine the candidate next-hop gateway IP addresses, are **not** trusted to be secure enough for TLS peername verification. Instead, the default name verified in the server certificate is obtained from the next-hop domain as specified in the smtp_tls_secure_cert_match configuration parameter. The default matching rule is that a server certificate matches when its name is equal to or is a subdomain of the nexthop domain. This security level is not an appropriate default for systems delivering mail to the Internet.

Examples:

```
# No TLS. Formerly: smtp_use_tls=no and smtp_enforce_tls=no.
smtp_tls_security_level = none

# Opportunistic TLS.
smtp_tls_security_level = may
# Postfix >= 2.6:
# Do not tweak opportunistic ciphers or protocol unless it is essential
# to do so (if a security vulnerability is found in the SSL library that
# can be mitigated by disabling a particular protocol or raising the
# cipher grade from "export" to "low" or "medium").
smtp_tls_ciphers = export
smtp_tls_protocols = !SSLv2, !SSLv3

# Mandatory (high-grade) TLS encryption.
smtp_tls_security_level = encrypt
smtp_tls_mandatory_ciphers = high

# Mandatory TLS verification of hostname or nexthop domain.
smtp_tls_security_level = verify
smtp_tls_mandatory_ciphers = high
smtp_tls_verify_cert_match = hostname, nexthop, dot-nexthop

# Secure channel TLS with exact nexthop name match.
smtp_tls_security_level = secure
smtp_tls_mandatory_protocols = TLSv1
smtp_tls_mandatory_ciphers = high
smtp_tls_secure_cert_match = nexthop

# Certificate fingerprint verification (Postfix >= 2.5).
# The CA-less "fingerprint" security level only scales to a limited
# number of destinations. As a global default rather than a per-site
# setting, this is practical when mail for all recipients is sent
# to a central mail hub.
relayhost = [mailhub.example.com]
smtp_tls_security_level = fingerprint
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtp_tls_mandatory_ciphers = high
smtp_tls_fingerprint_cert_match =
3D:95:34:51:24:66:33:B9:D2:40:99:C0:C1:17:0B:D1
EC:3B:2D:B0:5B:B1:FB:6D:20:A3:9D:72:F6:8D:12:35
```

This feature is available in Postfix 2.3 and later.

smtp_tls_session_cache_database (default: empty)

Name of the file containing the optional Postfix SMTP client TLS session cache. Specify a database type that supports enumeration, such as **btree** or **sdbm**; there is no need to support concurrent access. The file is created if it does not exist. The **smtp(8)** daemon does not use this parameter directly, rather the cache is implemented indirectly in the **tlsmgr(8)** daemon. This means that per-smtp-instance master.cf overrides of this parameter are not effective. Note, that each of the cache databases supported by **tlsmgr(8)** daemon: $smtpd_tls_session_cache_database, $smtp_tls_session_cache_database (and with Postfix 2.3 and later

$lmtp_tls_session_cache_database), needs to be stored separately. It is not at this time possible to store multiple caches in a single database.

Note: **dbm** databases are not suitable. TLS session objects are too large.

As of version 2.5, Postfix no longer uses root privileges when opening this file. The file should now be stored under the Postfix-owned data_directory. As a migration aid, an attempt to open the file under a non-Postfix directory is redirected to the Postfix-owned data_directory, and a warning is logged.

Example:

```
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_scache
```

This feature is available in Postfix 2.2 and later.

smtp_tls_session_cache_timeout (default: 3600s)

The expiration time of Postfix SMTP client TLS session cache information. A cache cleanup is performed periodically every $smtp_tls_session_cache_timeout seconds. As with $smtp_tls_session_cache_database, this parameter is implemented in the **tlsmgr(8)** daemon and therefore per-smtp-instance master.cf overrides are not possible.

As of Postfix 2.11 this setting cannot exceed 100 days. If set <= 0, session caching is disabled. If set to a positive value less than 2 minutes, the minimum value of 2 minutes is used instead.

This feature is available in Postfix 2.2 and later.

smtp_tls_trust_anchor_file (default: empty)

Zero or more PEM-format files with trust-anchor certificates and/or public keys. If the parameter is not empty the root CAs in CAfile and CApath are no longer trusted. Rather, the Postfix SMTP client will only trust certificate-chains signed by one of the trust-anchors contained in the chosen files. The specified trust-anchor certificates and public keys are not subject to expiration, and need not be (self-signed) root CAs. They may, if desired, be intermediate certificates. Therefore, these certificates also may be found "in the middle" of the trust chain presented by the remote SMTP server, and any untrusted issuing parent certificates will be ignored. Specify a list of pathnames separated by comma or whitespace.

Whether specified in main.cf, or on a per-destination basis, the trust-anchor PEM file must be accessible to the Postfix SMTP client in the chroot jail if applicable. The trust-anchor file should contain only certificates and public keys, no private key material, and must be readable by the non-privileged $mail_owner user. This allows destinations to be bound to a set of specific CAs or public keys without trusting the same CAs for all destinations.

The main.cf parameter supports single-purpose Postfix installations that send mail to a fixed set of SMTP peers. At most sites, if trust-anchor files are used at all, they will be specified on a per-destination basis via the "tafile" attribute of the "verify" and "secure" levels in smtp_tls_policy_maps.

The underlying mechanism is in support of RFC 6698 (DANE TLSA), which defines mechanisms for a client to securely determine server TLS certificates via DNS.

If you want your trust anchors to be public keys, with OpenSSL you can extract a single PEM public key from a PEM X.509 file containing a single certificate, as follows:

```
$ openssl x509 -in cert.pem -out ta-key.pem -noout -pubkey
```

This feature is available in Postfix 2.11 and later.

smtp_tls_verify_cert_match (default: hostname)

How the Postfix SMTP client verifies the server certificate peername for the "verify" TLS security level. In a "verify" TLS policy table ($smtp_tls_policy_maps) entry the optional "match" attribute overrides this main.cf setting.

This parameter specifies one or more patterns or strategies separated by commas, whitespace or colons. In the policy table the only valid separator is the colon character.

Patterns specify domain names, or domain name suffixes:

example.com
: Match the *example.com* domain, i.e. one of the names the server certificate must be *example.com*, upper and lower case distinctions are ignored.

.example.com
: Match subdomains of the *example.com* domain, i.e. match a name in the server certificate that consists of a non-zero number of labels followed by a *.example.com* suffix. Case distinctions are ignored.

Strategies specify a transformation from the next-hop domain to the expected name in the server certificate:

nexthop
: Match against the next-hop domain, which is either the recipient domain, or the transport next-hop configured for the domain stripped of any optional socket type prefix, enclosing square brackets and trailing port. When MX lookups are not suppressed, this is the original nexthop domain prior to the MX lookup, not the result of the MX lookup. For LMTP delivery via UNIX-domain sockets, the verified next-hop name is $myhostname. This strategy is suitable for use with the "secure" policy. Case is ignored.

dot-nexthop
: As above, but match server certificate names that are subdomains of the next-hop domain. Case is ignored.

hostname
: Match against the hostname of the server, often obtained via an unauthenticated DNS MX lookup. For LMTP delivery via UNIX-domain sockets, the verified name is $myhostname. This matches the verification strategy of the "MUST" keyword in the obsolete smtp_tls_per_site table, and is suitable for use with the "verify" security level. When the next-hop name is enclosed in square brackets to suppress MX lookups, the "hostname" strategy is the same as the "nexthop" strategy. Case is ignored.

Sample main.cf setting:

```
smtp_tls_verify_cert_match = hostname, nexthop, dot-nexthop
```

Sample policy table override:

```
example.com verify match=hostname:nexthop
.example.com verify match=example.com:.example.com:hostname
```

This feature is available in Postfix 2.3 and later.

smtp_tls_wrappermode (default: no)
: Request that the Postfix SMTP client connects using the legacy SMTPS protocol instead of using the STARTTLS command.

  This mode requires "smtp_tls_security_level = encrypt" or stronger.

  Example: deliver all remote mail via a provider’s server "mail.example.com".

```
/etc/postfix/main.cf:
# Client-side SMTPS requires "encrypt" or stronger.
smtp_tls_security_level = encrypt
smtp_tls_wrappermode = yes
# The [] suppress MX lookups.
relayhost = [mail.example.com]:465
```

  More examples are in TLS_README, including examples for older Postfix versions.

  This feature is available in Postfix 3.0 and later.

smtp_use_tls (default: no)
: Opportunistic mode: use TLS when a remote SMTP server announces STARTTLS support, otherwise send the mail in the clear. Beware: some SMTP servers offer STARTTLS even if it is not configured. With Postfix < 2.3, if the TLS handshake fails, and no other server is available, delivery is deferred and mail stays in

the queue. If this is a concern for you, use the smtp_tls_per_site feature instead.

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtp_tls_security_level instead.

smtp_xforward_timeout (default: 300s)

The Postfix SMTP client time limit for sending the XFORWARD command, and for receiving the remote SMTP server response.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.1 and later.

smtpd_authorized_verp_clients (default: $authorized_verp_clients)

What remote SMTP clients are allowed to specify the XVERP command. This command requests that mail be delivered one recipient at a time with a per recipient return address.

By default, no clients are allowed to specify XVERP.

This parameter was renamed with Postfix version 2.1. The default value is backwards compatible with Postfix version 2.0.

Specify a list of network/netmask patterns, separated by commas and/or whitespace. The mask specifies the number of bits in the network part of a host address. You can also specify hostnames or .domain names (the initial dot causes the domain to match any name below it), "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note: IP version 6 address information must be specified inside [] in the smtpd_authorized_verp_clients value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

smtpd_authorized_xclient_hosts (default: empty)

What remote SMTP clients are allowed to use the XCLIENT feature. This command overrides remote SMTP client information that is used for access control. Typical use is for SMTP-based content filters, fetchmail-like programs, or SMTP server access rule testing. See the XCLIENT_README document for details.

This feature is available in Postfix 2.1 and later.

By default, no clients are allowed to specify XCLIENT.

Specify a list of network/netmask patterns, separated by commas and/or whitespace. The mask specifies the number of bits in the network part of a host address. You can also specify hostnames or .domain names (the initial dot causes the domain to match any name below it), "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note: IP version 6 address information must be specified inside [] in the smtpd_authorized_xclient_hosts value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

smtpd_authorized_xforward_hosts (default: empty)

What remote SMTP clients are allowed to use the XFORWARD feature. This command forwards information that is used to improve logging after SMTP-based content filters. See the XFORWARD_README document for details.

This feature is available in Postfix 2.1 and later.

By default, no clients are allowed to specify XFORWARD.

Specify a list of network/netmask patterns, separated by commas and/or whitespace. The mask specifies the number of bits in the network part of a host address. You can also specify hostnames or .domain names (the initial dot causes the domain to match any name below it), "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note: IP version 6 address information must be specified inside [] in the smtpd_authorized_xforward_hosts value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

smtpd_banner (default: $myhostname ESMTP $mail_name)

The text that follows the 220 status code in the SMTP greeting banner. Some people like to see the mail version advertised. By default, Postfix shows no version.

You MUST specify $myhostname at the start of the text. This is required by the SMTP protocol.

Example:

```
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
```

smtpd_client_auth_rate_limit (default: 0)

The maximal number of AUTH commands that any client is allowed to send to this service per time unit, regardless of whether or not Postfix actually accepts those commands. The time unit is specified with the anvil_rate_time_unit configuration parameter.

By default, there is no limit on the number AUTH commands that a client may send.

To disable this feature, specify a limit of 0.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 3.1 and later.

smtpd_client_connection_count_limit (default: 50)

How many simultaneous connections any client is allowed to make to this service. By default, the limit is set to half the default process limit value.

To disable this feature, specify a limit of 0.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 2.2 and later.

smtpd_client_connection_rate_limit (default: 0)

The maximal number of connection attempts any client is allowed to make to this service per time unit. The time unit is specified with the anvil_rate_time_unit configuration parameter.

By default, a client can make as many connections per time unit as Postfix can accept.

To disable this feature, specify a limit of 0.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 2.2 and later.

Example:

```
smtpd_client_connection_rate_limit = 1000
```

smtpd_client_event_limit_exceptions (default: $mynetworks)

Clients that are excluded from smtpd_client_*_count/rate_limit restrictions. See the mynetworks parameter description for the parameter value syntax.

By default, clients in trusted networks are excluded. Specify a list of network blocks, hostnames or .domain names (the initial dot causes the domain to match any name below it).

Note: IP version 6 address information must be specified inside [] in the smtpd_client_event_limit_exceptions value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

Pattern matching of domain names is controlled by the presence or absence of "smtpd_client_event_limit_exceptions" in the parent_domain_matches_subdomains parameter value (postfix 3.0 and later).

This feature is available in Postfix 2.2 and later.

smtpd_client_message_rate_limit (default: 0)

The maximal number of message delivery requests that any client is allowed to make to this service per time unit, regardless of whether or not Postfix actually accepts those messages. The time unit is specified with the anvil_rate_time_unit configuration parameter.

By default, a client can send as many message delivery requests per time unit as Postfix can accept.

To disable this feature, specify a limit of 0.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 2.2 and later.

Example:

```
smtpd_client_message_rate_limit = 1000
```

smtpd_client_new_tls_session_rate_limit (default: 0)

The maximal number of new (i.e., uncached) TLS sessions that a remote SMTP client is allowed to negotiate with this service per time unit. The time unit is specified with the anvil_rate_time_unit configuration parameter.

By default, a remote SMTP client can negotiate as many new TLS sessions per time unit as Postfix can accept.

To disable this feature, specify a limit of 0. Otherwise, specify a limit that is at least the per-client concurrent session limit, or else legitimate client sessions may be rejected.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 2.3 and later.

Example:

```
smtpd_client_new_tls_session_rate_limit = 100
```

smtpd_client_port_logging (default: no)

Enable logging of the remote SMTP client port in addition to the hostname and IP address. The logging format is "host[address]:port".

This feature is available in Postfix 2.5 and later.

smtpd_client_recipient_rate_limit (default: 0)

The maximal number of recipient addresses that any client is allowed to send to this service per time unit, regardless of whether or not Postfix actually accepts those recipients. The time unit is specified with the anvil_rate_time_unit configuration parameter.

By default, a client can send as many recipient addresses per time unit as Postfix can accept.

To disable this feature, specify a limit of 0.

WARNING: The purpose of this feature is to limit abuse. It must not be used to regulate legitimate mail traffic.

This feature is available in Postfix 2.2 and later.

Example:

```
smtpd_client_recipient_rate_limit = 1000
```

smtpd_client_restrictions (default: empty)

Optional restrictions that the Postfix SMTP server applies in the context of a client connection request. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

The default is to allow all connection requests.

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are specific to client hostname or client network address information.

check_ccert_access *type:table*

Use the remote SMTP client certificate fingerprint or the public key fingerprint (Postfix 2.9 and later) as lookup key for the specified **access(5)** database; with Postfix version 2.2, also require that the remote SMTP client certificate is verified successfully. The fingerprint digest algorithm is configurable via the smtpd_tls_fingerprint_digest parameter (hard-coded as md5 prior to Postfix version 2.5). This feature is available with Postfix version 2.2 and later.

check_client_access *type:table*

Search the specified access database for the client hostname, parent domains, client IP address, or networks obtained by stripping least significant octets. See the **access(5)** manual page for details.

check_client_a_access *type:table*

Search the specified **access(5)** database for the IP addresses for the client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 3.0 and later.

check_client_mx_access *type:table*

Search the specified **access(5)** database for the MX hosts for the client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.7 and later.

check_client_ns_access *type:table*

Search the specified **access(5)** database for the DNS servers for the client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.7 and later.

check_reverse_client_hostname_access *type:table*

Search the specified access database for the unverified reverse client hostname, parent domains, client IP address, or networks obtained by stripping least significant octets. See the **access(5)** manual page for details. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.6 and later.

check_reverse_client_hostname_a_access *type:table*

Search the specified **access(5)** database for the IP addresses for the unverified reverse client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 3.0 and later.

check_reverse_client_hostname_mx_access *type:table*

Search the specified **access(5)** database for the MX hosts for the unverified reverse client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety

reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.7 and later.

check_reverse_client_hostname_ns_access *type:table*
Search the specified **access(5)** database for the DNS servers for the unverified reverse client hostname, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.7 and later.

check_sasl_access *type:table*
Use the remote SMTP client SASL user name as lookup key for the specified **access(5)** database. The lookup key has the form "username@domainname" when the smtpd_sasl_local_domain parameter value is non-empty. Unlike the check_client_access feature, check_sasl_access does not perform matches of parent domains or IP subnet ranges. This feature is available with Postfix version 2.11 and later.

permit_inet_interfaces
Permit the request when the client IP address matches $inet_interfaces.

permit_mynetworks
Permit the request when the client IP address matches any network or network address listed in $mynetworks.

permit_sasl_authenticated
Permit the request when the client is successfully authenticated via the RFC 4954 (AUTH) protocol.

permit_tls_all_clientcerts
Permit the request when the remote SMTP client certificate is verified successfully. This option must be used only if a special CA issues the certificates and only this CA is listed as trusted CA. Otherwise, clients with a third-party certificate would also be allowed to relay. Specify "tls_append_default_CA = no" when the trusted CA is specified with smtpd_tls_CAfile or smtpd_tls_CApath, to prevent Postfix from appending the system-supplied default CAs. This feature is available with Postfix version 2.2.

permit_tls_clientcerts
Permit the request when the remote SMTP client certificate fingerprint or public key fingerprint (Postfix 2.9 and later) is listed in $relay_clientcerts. The fingerprint digest algorithm is configurable via the smtpd_tls_fingerprint_digest parameter (hard-coded as md5 prior to Postfix version 2.5). This feature is available with Postfix version 2.2.

reject_rbl_client *rbl_domain=d.d.d.d*
Reject the request when the reversed client network address is listed with the A record "*d.d.d.d*" under *rbl_domain* (Postfix version 2.1 and later only). Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges (Postfix version 2.8 and later). If no "*=d.d.d.d*" is specified, reject the request when the reversed client network address is listed with any A record under *rbl_domain*.
The maps_rbl_reject_code parameter specifies the response code for rejected requests (default: 554), the default_rbl_reply parameter specifies the default server reply, and the rbl_reply_maps parameter specifies tables with server replies indexed by *rbl_domain*. This feature is available in Postfix 2.0 and later.

permit_dnswl_client *dnswl_domain=d.d.d.d*
Accept the request when the reversed client network address is listed with the A record "*d.d.d.d*" under *dnswl_domain*. Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges. If no "*=d.d.d.d*" is specified, accept the request when the reversed client network address is listed with any A record under *dnswl_domain*.
For safety, permit_dnswl_client is silently ignored when it would override reject_unauth_destination. The result is DEFER_IF_REJECT when whitelist lookup fails. This feature is available in Postfix 2.8 and later.

reject_rhsbl_client *rbl_domain=d.d.d.d*
Reject the request when the client hostname is listed with the A record "*d.d.d.d*" under *rbl_domain* (Postfix version 2.1 and later only). Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges (Postfix version 2.8 and later). If no "*=d.d.d.d*" is specified, reject the request when the client hostname is listed with any A record under *rbl_domain*. See the reject_rbl_client description above for additional RBL related configuration parameters. This feature is available in Postfix 2.0 and later; with Postfix version 2.8 and later, reject_rhsbl_reverse_client will usually produce better results.

permit_rhswl_client *rhswl_domain=d.d.d.d*
Accept the request when the client hostname is listed with the A record "*d.d.d.d*" under *rhswl_domain*. Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges. If no "*=d.d.d.d*" is specified, accept the request when the client hostname is listed with any A record under *rhswl_domain*.
Caution: client name whitelisting is fragile, since the client name lookup can fail due to temporary outages. Client name whitelisting should be used only to reduce false positives in e.g. DNS-based blocklists, and not for making access rule exceptions.
For safety, permit_rhswl_client is silently ignored when it would override reject_unauth_destination. The result is DEFER_IF_REJECT when whitelist lookup fails. This feature is available in Postfix 2.8 and later.

reject_rhsbl_reverse_client *rbl_domain=d.d.d.d*
Reject the request when the unverified reverse client hostname is listed with the A record "*d.d.d.d*" under *rbl_domain*. Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges. If no "*=d.d.d.d*" is specified, reject the request when the unverified reverse client hostname is listed with any A record under *rbl_domain*. See the reject_rbl_client description above for additional RBL related configuration parameters. This feature is available in Postfix 2.8 and later.

reject_unknown_client_hostname (with Postfix < 2.3: reject_unknown_client)
Reject the request when 1) the client IP address->name mapping fails, 2) the name->address mapping fails, or 3) the name->address mapping does not match the client IP address.
This is a stronger restriction than the reject_unknown_reverse_client_hostname feature, which triggers only under condition 1) above.
The unknown_client_reject_code parameter specifies the response code for rejected requests (default: 450). The reply is always 450 in case the address->name or name->address lookup failed due to a temporary problem.

reject_unknown_reverse_client_hostname
Reject the request when the client IP address has no address->name mapping.
This is a weaker restriction than the reject_unknown_client_hostname feature, which requires not only that the address->name and name->address mappings exist, but also that the two mappings reproduce the client IP address.
The unknown_client_reject_code parameter specifies the response code for rejected requests (default: 450). The reply is always 450 in case the address->name lookup failed due to a temporary problem.
This feature is available in Postfix 2.3 and later.

In addition, you can use any of the following generic restrictions. These restrictions are applicable in any SMTP command context.

check_policy_service *servername*
Query the specified policy server. See the SMTPD_POLICY_README document for details. This feature is available in Postfix 2.1 and later.

defer Defer the request. The client is told to try again later. This restriction is useful at the end of a restriction list, to make the default policy explicit.
The defer_code parameter specifies the SMTP server reply code (default: 450).

defer_if_permit
Defer the request if some later restriction would result in an explicit or implicit PERMIT action. This is useful when a blacklisting feature fails due to a temporary problem. This feature is available in Postfix version 2.1 and later.

defer_if_reject
Defer the request if some later restriction would result in a REJECT action. This is useful when a whitelisting feature fails due to a temporary problem. This feature is available in Postfix version 2.1 and later.

permit Permit the request. This restriction is useful at the end of a restriction list, to make the default policy explicit.

reject_multi_recipient_bounce
Reject the request when the envelope sender is the null address, and the message has multiple envelope recipients. This usage has rare but legitimate applications: under certain conditions, multi-recipient mail that was posted with the DSN option NOTIFY=NEVER may be forwarded with the null sender address.
Note: this restriction can only work reliably when used in smtpd_data_restrictions or smtpd_end_of_data_restrictions, because the total number of recipients is not known at an earlier stage of the SMTP conversation. Use at the RCPT stage will only reject the second etc. recipient.
The multi_recipient_bounce_reject_code parameter specifies the response code for rejected requests (default: 550). This feature is available in Postfix 2.1 and later.

reject_plaintext_session
Reject the request when the connection is not encrypted. This restriction should not be used before the client has had a chance to negotiate encryption with the AUTH or STARTTLS commands.
The plaintext_reject_code parameter specifies the response code for rejected requests (default: 450). This feature is available in Postfix 2.3 and later.

reject_unauth_pipelining
Reject the request when the client sends SMTP commands ahead of time where it is not allowed, or when the client sends SMTP commands ahead of time without knowing that Postfix actually supports ESMTP command pipelining. This stops mail from bulk mail software that improperly uses ESMTP command pipelining in order to speed up deliveries.
With Postfix 2.6 and later, the SMTP server sets a per-session flag whenever it detects illegal pipelining, including pipelined HELO or EHLO commands. The reject_unauth_pipelining feature simply tests whether the flag was set at any point in time during the session.
With older Postfix versions, reject_unauth_pipelining checks the current status of the input read queue, and its usage is not recommended in contexts other than smtpd_data_restrictions.

reject Reject the request. This restriction is useful at the end of a restriction list, to make the default policy explicit. The reject_code configuration parameter specifies the response code for rejected requests (default: 554).

sleep *seconds*
Pause for the specified number of seconds and proceed with the next restriction in the list, if any. This may stop zombie mail when used as:

```
/etc/postfix/main.cf:
smtpd_client_restrictions =
sleep 1, reject_unauth_pipelining
smtpd_delay_reject = no
```

This feature is available in Postfix 2.3.

warn_if_reject
A safety net for testing. When "warn_if_reject" is placed before a reject-type restriction, access table query, or check_policy_service query, this logs a "reject_warning" message instead of rejecting a request (when a reject-type restriction fails due to a temporary error, this logs a "reject_warning" message for any implicit "defer_if_permit" actions that would normally prevent mail from being

accepted by some later access restriction). This feature has no effect on defer_if_reject restrictions.

Other restrictions that are valid in this context:

- SMTP command specific restrictions that are described under the smtpd_helo_restrictions, smtpd_sender_restrictions or smtpd_recipient_restrictions parameters. When helo, sender or recipient restrictions are listed under smtpd_client_restrictions, they have effect only with "smtpd_delay_reject = yes", so that $smtpd_client_restrictions is evaluated at the time of the RCPT TO command.

Example:

```
smtpd_client_restrictions = permit_mynetworks, reject_unknown_client_hostname
```

smtpd_command_filter (default: empty)

A mechanism to transform commands from remote SMTP clients. This is a last-resort tool to work around client commands that break interoperability with the Postfix SMTP server. Other uses involve fault injection to test Postfix's handling of invalid commands.

Specify the name of a "type:table" lookup table. The search string is the SMTP command as received from the remote SMTP client, except that initial whitespace and the trailing <CR><LF> are removed. The result value is executed by the Postfix SMTP server.

There is no need to use smtpd_command_filter for the following cases:

- Use "resolve_numeric_domain = yes" to accept "*user@ipaddress*".
- Postfix already accepts the correct form "*user@[ipaddress]*". Use virtual_alias_maps or canonical_maps to translate these into domain names if necessary.
- Use "strict_rfc821_envelopes = no" to accept "RCPT TO:<*User Name* <*user@example.com*>>". Postfix will ignore the "*User Name*" part and deliver to the <*user@example.com*> address.

Examples of problems that can be solved with the smtpd_command_filter feature:

```
/etc/postfix/main.cf:
smtpd_command_filter = pcre:/etc/postfix/command_filter

/etc/postfix/command_filter:
# Work around clients that send malformed HELO commands.
/^HELO\s*$/ HELO domain.invalid

# Work around clients that send empty lines.
/^\s*$/ NOOP

# Work around clients that send RCPT TO:<'user@domain'>.
# WARNING: do not lose the parameters that follow the address.
/^(RCPT\s+TO:\s*<)'([^[:space:]]+)'(>.*)/ $1$2$3

# Append XVERP to MAIL FROM commands to request VERP-style delivery.
# See VERP_README for more information on how to use Postfix VERP.
/^(MAIL FROM:\s*<listname@example\.com>.*)/ $1 XVERP

# Bounce-never mail sink. Use notify_classes=bounce,resource,software
# to send bounced mail to the postmaster (with message body removed).
/^(RCPT\s+TO:\s*<.*>.*)\s+NOTIFY=\S+(.*)/ $1 NOTIFY=NEVER$2
/^(RCPT\s+TO:.*)/ $1 NOTIFY=NEVER
```

This feature is available in Postfix 2.7.

smtpd_data_restrictions (default: empty)

Optional access restrictions that the Postfix SMTP server applies in the context of the SMTP DATA command. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

This feature is available in Postfix 2.0 and later.

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are valid in this context:

- Generic restrictions that can be used in any SMTP command context, described under smtpd_client_restrictions.
- SMTP command specific restrictions described under smtpd_client_restrictions, smtpd_helo_restrictions, smtpd_sender_restrictions or smtpd_recipient_restrictions.
- However, no recipient information is available in the case of multi-recipient mail. Acting on only one recipient would be misleading, because any decision will affect all recipients equally. Acting on all recipients would require a possibly very large amount of memory, and would also be misleading for the reasons mentioned before.

Examples:

```
smtpd_data_restrictions = reject_unauth_pipelining
smtpd_data_restrictions = reject_multi_recipient_bounce
```

smtpd_delay_open_until_valid_rcpt (default: yes)

Postpone the start of an SMTP mail transaction until a valid RCPT TO command is received. Specify "no" to create a mail transaction as soon as the Postfix SMTP server receives a valid MAIL FROM command.

With sites that reject lots of mail, the default setting reduces the use of disk, CPU and memory resources. The downside is that rejected recipients are logged with NOQUEUE instead of a mail transaction ID. This complicates the logfile analysis of multi-recipient mail.

This feature is available in Postfix 2.3 and later.

smtpd_delay_reject (default: yes)

Wait until the RCPT TO command before evaluating $smtpd_client_restrictions, $smtpd_helo_restrictions and $smtpd_sender_restrictions, or wait until the ETRN command before evaluating $smtpd_client_restrictions and $smtpd_helo_restrictions.

This feature is turned on by default because some clients apparently mis-behave when the Postfix SMTP server rejects commands before RCPT TO.

The default setting has one major benefit: it allows Postfix to log recipient address information when rejecting a client name/address or sender address, so that it is possible to find out whose mail is being rejected.

smtpd_discard_ehlo_keyword_address_maps (default: empty)

Lookup tables, indexed by the remote SMTP client address, with case insensitive lists of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP server will not send in the EHLO response to a remote SMTP client. See smtpd_discard_ehlo_keywords for details. The tables are not searched by hostname for robustness reasons.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

This feature is available in Postfix 2.2 and later.

smtpd_discard_ehlo_keywords (default: empty)

A case insensitive list of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP server will not send in the EHLO response to a remote SMTP client.

This feature is available in Postfix 2.2 and later.

Notes:

- Specify the **silent-discard** pseudo keyword to prevent this action from being logged.
- Use the smtpd_discard_ehlo_keyword_address_maps feature to discard EHLO keywords selectively.

smtpd_dns_reply_filter (default: empty)
Optional filter for Postfix SMTP server DNS lookup results. See smtp_dns_reply_filter for details including an example.

This feature is available in Postfix 3.0 and later.

smtpd_end_of_data_restrictions (default: empty)
Optional access restrictions that the Postfix SMTP server applies in the context of the SMTP END-OF-DATA command. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

This feature is available in Postfix 2.2 and later.

See smtpd_data_restrictions for details and limitations.

smtpd_enforce_tls (default: no)
Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption. According to RFC 2487 this MUST NOT be applied in case of a publicly-referenced SMTP server. This option is therefore off by default.

Note 1: "smtpd_enforce_tls = yes" implies "smtpd_tls_auth_only = yes".

Note 2: when invoked via "**sendmail -bs**", Postfix will never offer STARTTLS due to insufficient privileges to access the server private key. This is intended behavior.

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtpd_tls_security_level instead.

smtpd_error_sleep_time (default: 1s)
With Postfix version 2.1 and later: the SMTP server response delay after a client has made more than $smtpd_soft_error_limit errors, and fewer than $smtpd_hard_error_limit errors, without delivering mail.

With Postfix version 2.0 and earlier: the SMTP server delay before sending a reject (4xx or 5xx) response, when the client has made fewer than $smtpd_soft_error_limit errors without delivering mail.

smtpd_etrn_restrictions (default: empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client ETRN command. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

The Postfix ETRN implementation accepts only destinations that are eligible for the Postfix "fast flush" service. See the ETRN_README file for details.

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are specific to the domain name information received with the ETRN command.

check_etrn_access *type:table*
Search the specified access database for the ETRN domain name or its parent domains. See the **access(5)** manual page for details.

Other restrictions that are valid in this context:

- Generic restrictions that can be used in any SMTP command context, described under smtpd_client_restrictions.
- SMTP command specific restrictions described under smtpd_client_restrictions and smtpd_helo_restrictions.

Example:

```
smtpd_etrn_restrictions = permit_mynetworks, reject
```

smtpd_expansion_filter (default: see postconf −d output)
What characters are allowed in $name expansions of RBL reply templates. Characters not in the allowed set are replaced by "_". Use C like escapes to specify special characters such as whitespace.

This parameter is not subjected to $parameter expansion.

This feature is available in Postfix 2.0 and later.

smtpd_forbidden_commands (default: CONNECT, GET, POST)
List of commands that cause the Postfix SMTP server to immediately terminate the session with a 221 code. This can be used to disconnect clients that obviously attempt to abuse the system. In addition to the commands listed in this parameter, commands that follow the "Label:" format of message headers will also cause a disconnect.

This feature is available in Postfix 2.2 and later.

smtpd_hard_error_limit (default: normal: 20, overload: 1)
The maximal number of errors a remote SMTP client is allowed to make without delivering mail. The Postfix SMTP server disconnects when the limit is exceeded. Normally the default limit is 20, but it changes under overload to just 1. With Postfix 2.5 and earlier, the SMTP server always allows up to 20 errors by default.

smtpd_helo_required (default: no)
Require that a remote SMTP client introduces itself with the HELO or EHLO command before sending the MAIL command or other commands that require EHLO negotiation.

Example:

```
smtpd_helo_required = yes
```

smtpd_helo_restrictions (default: empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client HELO command. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

The default is to permit everything.

Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip smtpd_helo_restrictions by not sending HELO or EHLO).

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are specific to the hostname information received with the HELO or EHLO command.

check_helo_access *type:table*
Search the specified **access(5)** database for the HELO or EHLO hostname or parent domains, and execute the corresponding action. Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip check_helo_access by not sending HELO or EHLO).

check_helo_a_access *type:table*
Search the specified **access(5)** database for the IP addresses for the HELO or EHLO hostname, and execute the corresponding action. Note 1: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. Note 2: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip check_helo_a_access by not sending HELO or EHLO). This feature is available in Postfix 3.0 and later.

check_helo_mx_access *type:table*
Search the specified **access(5)** database for the MX hosts for the HELO or EHLO hostname, and execute the corresponding action. Note 1: a result of "OK" is not allowed for safety reasons.

Instead, use DUNNO in order to exclude specific hosts from blacklists. Note 2: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip check_helo_mx_access by not sending HELO or EHLO). This feature is available in Postfix 2.1 and later.

check_helo_ns_access *type:table*
Search the specified **access(5)** database for the DNS servers for the HELO or EHLO hostname, and execute the corresponding action. Note 1: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. Note 2: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip check_helo_ns_access by not sending HELO or EHLO). This feature is available in Postfix 2.1 and later.

reject_invalid_helo_hostname (with Postfix < 2.3: reject_invalid_hostname)
Reject the request when the HELO or EHLO hostname is malformed. Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_invalid_helo_hostname by not sending HELO or EHLO).
The invalid_hostname_reject_code specifies the response code for rejected requests (default: 501).

reject_non_fqdn_helo_hostname (with Postfix < 2.3: reject_non_fqdn_hostname)
Reject the request when the HELO or EHLO hostname is not in fully-qualified domain or address literal form, as required by the RFC. Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_non_fqdn_helo_hostname by not sending HELO or EHLO).
The non_fqdn_reject_code parameter specifies the response code for rejected requests (default: 504).

reject_rhsbl_helo *rbl_domain=d.d.d.d*
Reject the request when the HELO or EHLO hostname is listed with the A record "*d.d.d.d*" under *rbl_domain* (Postfix version 2.1 and later only). Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges (Postfix version 2.8 and later). If no "*=d.d.d.d*" is specified, reject the request when the HELO or EHLO hostname is listed with any A record under *rbl_domain*. See the reject_rbl_client description for additional RBL related configuration parameters. Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_rhsbl_helo by not sending HELO or EHLO). This feature is available in Postfix 2.0 and later.

reject_unknown_helo_hostname (with Postfix < 2.3: reject_unknown_hostname)
Reject the request when the HELO or EHLO hostname has no DNS A or MX record.
The reply is specified with the unknown_hostname_reject_code parameter (default: 450) or unknown_helo_hostname_tempfail_action (default: defer_if_permit). See the respective parameter descriptions for details.
Note: specify "smtpd_helo_required = yes" to fully enforce this restriction (without "smtpd_helo_required = yes", a client can simply skip reject_unknown_helo_hostname by not sending HELO or EHLO).

Other restrictions that are valid in this context:

- Generic restrictions that can be used in any SMTP command context, described under smtpd_client_restrictions.
- Client hostname or network address specific restrictions described under smtpd_client_restrictions.
- SMTP command specific restrictions described under smtpd_sender_restrictions or smtpd_recipient_restrictions. When sender or recipient restrictions are listed under smtpd_helo_restrictions, they have effect only with "smtpd_delay_reject = yes", so that $smtpd_helo_restrictions is evaluated at the time of the RCPT TO command.

Examples:

```
smtpd_helo_restrictions = permit_mynetworks, reject_invalid_helo_hostname
```

```
smtpd_helo_restrictions = permit_mynetworks, reject_unknown_helo_hostname
```

smtpd_history_flush_threshold (default: 100)
The maximal number of lines in the Postfix SMTP server command history before it is flushed upon receipt of EHLO, RSET, or end of DATA.

smtpd_junk_command_limit (default: normal: 100, overload: 1)
The number of junk commands (NOOP, VRFY, ETRN or RSET) that a remote SMTP client can send before the Postfix SMTP server starts to increment the error counter with each junk command. The junk command count is reset after mail is delivered. See also the smtpd_error_sleep_time and smtpd_soft_error_limit configuration parameters. Normally the default limit is 100, but it changes under overload to just 1. With Postfix 2.5 and earlier, the SMTP server always allows up to 100 junk commands by default.

smtpd_log_access_permit_actions (default: empty)
Enable logging of the named "permit" actions in SMTP server access lists (by default, the SMTP server logs "reject" actions but not "permit" actions). This feature does not affect conditional actions such as "defer_if_permit".

Specify a list of "permit" action names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. The list is matched left to right, and the search stops on the first match. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a name matches a lookup key (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a name from the list.

Examples:

```
/etc/postfix/main.cf:
# Log all "permit" actions.
smtpd_log_access_permit_actions = static:all
```

```
/etc/postfix/main.cf:
# Log "permit_dnswl_client" only.
smtpd_log_access_permit_actions = permit_dnswl_client
```

This feature is available in Postfix 2.10 and later.

smtpd_milters (default: empty)
A list of Milter (mail filter) applications for new mail that arrives via the Postfix **smtpd(8)** server. Specify space or comma as separator. See the MILTER_README document for details.

This feature is available in Postfix 2.3 and later.

smtpd_noop_commands (default: empty)
List of commands that the Postfix SMTP server replies to with "250 Ok", without doing any syntax checks and without changing state. This list overrides any commands built into the Postfix SMTP server.

smtpd_null_access_lookup_key (default: <>)
The lookup key to be used in SMTP **access(5)** tables instead of the null sender address.

smtpd_peername_lookup (default: yes)
Attempt to look up the remote SMTP client hostname, and verify that the name matches the client IP address. A client name is set to "unknown" when it cannot be looked up or verified, or when name lookup is disabled. Turning off name lookup reduces delays due to DNS lookup and increases the maximal inbound delivery rate.

This feature is available in Postfix 2.3 and later.

smtpd_per_record_deadline (default: normal: no, overload: yes)
Change the behavior of the smtpd_timeout and smtpd_starttls_timeout time limits, from a time limit per read or write system call, to a time limit to send or receive a complete record (an SMTP command line, SMTP response line, SMTP message content line, or TLS protocol message). This limits the impact from hostile peers that trickle data one byte at a time.

Note: when per-record deadlines are enabled, a short timeout may cause problems with TLS over very slow network connections. The reasons are that a TLS protocol message can be up to 16 kbytes long (with TLSv1), and that an entire TLS protocol message must be sent or received within the per-record deadline.

This feature is available in Postfix 2.9 and later. With older Postfix releases, the behavior is as if this parameter is set to "no".

smtpd_policy_service_default_action (default: 451 4.3.5 Server configuration problem)
The default action when an SMTPD policy service request fails. Specify "DUNNO" to behave as if the failed SMTPD policy service request was not sent, and to continue processing other access restrictions, if any.

Limitations:

- This parameter may specify any value that would be a valid SMTPD policy server response (or **access(5)** map lookup result). An **access(5)** map or policy server in this parameter value may need to be declared in advance with a restriction_class setting.
- If the specified action invokes another check_policy_service request, that request will have the built-in default action.

This feature is available in Postfix 3.0 and later.

smtpd_policy_service_max_idle (default: 300s)
The time after which an idle SMTPD policy service connection is closed.

This feature is available in Postfix 2.1 and later.

smtpd_policy_service_max_ttl (default: 1000s)
The time after which an active SMTPD policy service connection is closed.

This feature is available in Postfix 2.1 and later.

smtpd_policy_service_policy_context (default: empty)
Optional information that the Postfix SMTP server specifies in the "policy_context" attribute of a policy service request (originally, to share the same service endpoint among multiple check_policy_service clients).

This feature is available in Postfix 3.1 and later.

smtpd_policy_service_request_limit (default: 0)
The maximal number of requests per SMTPD policy service connection, or zero (no limit). Once a connection reaches this limit, the connection is closed and the next request will be sent over a new connection. This is a workaround to avoid error-recovery delays with policy servers that cannot maintain a persistent connection.

This feature is available in Postfix 3.0 and later.

smtpd_policy_service_retry_delay (default: 1s)
The delay between attempts to resend a failed SMTPD policy service request. Specify a value greater than zero.

This feature is available in Postfix 3.0 and later.

smtpd_policy_service_timeout (default: 100s)
The time limit for connecting to, writing to, or receiving from a delegated SMTPD policy server.

This feature is available in Postfix 2.1 and later.

smtpd_policy_service_try_limit (default: 2)
The maximal number of attempts to send an SMTPD policy service request before giving up. Specify a value greater than zero.

This feature is available in Postfix 3.0 and later.

smtpd_proxy_ehlo (default: $myhostname)
How the Postfix SMTP server announces itself to the proxy filter. By default, the Postfix hostname is used.

This feature is available in Postfix 2.1 and later.

smtpd_proxy_filter (default: empty)
The hostname and TCP port of the mail filtering proxy server. The proxy receives all mail from the Postfix SMTP server, and is supposed to give the result to another Postfix SMTP server process.

Specify "host:port" or "inet:host:port" for a TCP endpoint, or "unix:pathname" for a UNIX-domain endpoint. The host can be specified as an IP address or as a symbolic name; no MX lookups are done. When no "host" or "host:" are specified, the local machine is assumed. Pathname interpretation is relative to the Postfix queue directory.

This feature is available in Postfix 2.1 and later.

The "inet:" and "unix:" prefixes are available in Postfix 2.3 and later.

smtpd_proxy_options (default: empty)
List of options that control how the Postfix SMTP server communicates with a before-queue content filter. Specify zero or more of the following, separated by comma or whitespace.

speed_adjust
Do not connect to a before-queue content filter until an entire message has been received. This reduces the number of simultaneous before-queue content filter processes.

NOTE 1: A filter must not *selectively* reject recipients of a multi-recipient message. Rejecting all recipients is OK, as is accepting all recipients.

NOTE 2: This feature increases the minimum amount of free queue space by $message_size_limit. The extra space is needed to save the message to a temporary file.

This feature is available in Postfix 2.7 and later.

smtpd_proxy_timeout (default: 100s)
The time limit for connecting to a proxy filter and for sending or receiving information. When a connection fails the client gets a generic error message while more detailed information is logged to the maillog file.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

This feature is available in Postfix 2.1 and later.

smtpd_recipient_limit (default: 1000)
The maximal number of recipients that the Postfix SMTP server accepts per message delivery request.

smtpd_recipient_overshoot_limit (default: 1000)
The number of recipients that a remote SMTP client can send in excess of the limit specified with $smtpd_recipient_limit, before the Postfix SMTP server increments the per-session error count for each excess recipient.

smtpd_recipient_restrictions (default: see postconf −d output)
Optional restrictions that the Postfix SMTP server applies in the context of a client RCPT TO command, after smtpd_relay_restrictions. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

With Postfix versions before 2.10, the rules for relay permission and spam blocking were combined under smtpd_recipient_restrictions, resulting in error-prone configuration. As of Postfix 2.10, relay permission rules are preferably implemented with smtpd_relay_restrictions, so that a permissive spam blocking policy under smtpd_recipient_restrictions will no longer result in a permissive mail relay policy.

For backwards compatibility, sites that migrate from Postfix versions before 2.10 can set smtpd_relay_restrictions to the empty value, and use smtpd_recipient_restrictions exactly as before.

IMPORTANT: Either the smtpd_relay_restrictions or the smtpd_recipient_restrictions parameter must specify at least one of the following restrictions. Otherwise Postfix will refuse to receive mail:

```
reject, reject_unauth_destination

defer, defer_if_permit, defer_unauth_destination
```

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are specific to the recipient address that is received with the RCPT TO command.

check_recipient_access *type:table*
Search the specified **access(5)** database for the resolved RCPT TO address, domain, parent domains, or localpart@, and execute the corresponding action.

check_recipient_a_access *type:table*
Search the specified **access(5)** database for the IP addresses for the RCPT TO domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 3.0 and later.

check_recipient_mx_access *type:table*
Search the specified **access(5)** database for the MX hosts for the RCPT TO domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.1 and later.

check_recipient_ns_access *type:table*
Search the specified **access(5)** database for the DNS servers for the RCPT TO domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.1 and later.

permit_auth_destination
Permit the request when one of the following is true:

- Postfix is mail forwarder: the resolved RCPT TO domain matches $relay_domains or a subdomain thereof, and the address contains no sender-specified routing (user@elsewhere@domain),
- Postfix is the final destination: the resolved RCPT TO domain matches $mydestination, $inet_interfaces, $proxy_interfaces, $virtual_alias_domains, or $virtual_mailbox_domains, and the address contains no sender-specified routing (user@elsewhere@domain).

permit_mx_backup
Permit the request when the local mail system is backup MX for the RCPT TO domain, or when the domain is an authorized destination (see permit_auth_destination for definition).

- Safety: permit_mx_backup does not accept addresses that have sender-specified routing information (example: user@elsewhere@domain).
- Safety: permit_mx_backup can be vulnerable to mis-use when access is not restricted with permit_mx_backup_networks.
- Safety: as of Postfix version 2.3, permit_mx_backup no longer accepts the address when the local mail system is primary MX for the recipient domain. Exception: permit_mx_backup accepts the address when it specifies an authorized destination (see permit_auth_destination for definition).
- Limitation: mail may be rejected in case of a temporary DNS lookup problem with Postfix prior to version 2.0.

reject_non_fqdn_recipient
Reject the request when the RCPT TO address is not in fully-qualified domain form, as required by the RFC.
The non_fqdn_reject_code parameter specifies the response code for rejected requests (default: 504).

reject_rhsbl_recipient *rbl_domain=d.d.d.d*
Reject the request when the RCPT TO domain is listed with the A record "*d.d.d.d*" under *rbl_domain* (Postfix version 2.1 and later only). Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges (Postfix version 2.8 and later). If no "=*d.d.d.d*" is specified, reject the request when the RCPT TO domain is listed with any A record under *rbl_domain*.
The maps_rbl_reject_code parameter specifies the response code for rejected requests (default: 554); the default_rbl_reply parameter specifies the default server reply; and the rbl_reply_maps parameter specifies tables with server replies indexed by *rbl_domain*. This feature is available in Postfix version 2.0 and later.

reject_unauth_destination
Reject the request unless one of the following is true:

- Postfix is mail forwarder: the resolved RCPT TO domain matches $relay_domains or a subdomain thereof, and contains no sender-specified routing (user@elsewhere@domain),
- Postfix is the final destination: the resolved RCPT TO domain matches $mydestination, $inet_interfaces, $proxy_interfaces, $virtual_alias_domains, or $virtual_mailbox_domains, and contains no sender-specified routing (user@elsewhere@domain).
  The relay_domains_reject_code parameter specifies the response code for rejected requests (default: 554).

defer_unauth_destination
Reject the same requests as reject_unauth_destination, with a non-permanent error code. This feature is available in Postfix 2.10 and later.

reject_unknown_recipient_domain
Reject the request when Postfix is not final destination for the recipient domain, and the RCPT TO domain has 1) no DNS MX and no DNS A record or 2) a malformed MX record such as a record with a zero-length MX hostname (Postfix version 2.3 and later).
The reply is specified with the unknown_address_reject_code parameter (default: 450), unknown_address_tempfail_action (default: defer_if_permit), or 556 (nullmx, Postfix 3.0 and later). See the respective parameter descriptions for details.

reject_unlisted_recipient (with Postfix version 2.0: check_recipient_maps)
Reject the request when the RCPT TO address is not listed in the list of valid recipients for its domain class. See the smtpd_reject_unlisted_recipient parameter description for details. This feature is available in Postfix 2.1 and later.

reject_unverified_recipient
Reject the request when mail to the RCPT TO address is known to bounce, or when the recipient address destination is not reachable. Address verification information is managed by the **verify(8)** server; see the ADDRESS_VERIFICATION_README file for details.
The unverified_recipient_reject_code parameter specifies the numerical response code when an address is known to bounce (default: 450, change into 550 when you are confident that it is safe to do so).
The unverified_recipient_defer_code parameter specifies the numerical response code when an address probe failed due to a temporary problem (default: 450).
The unverified_recipient_tempfail_action parameter specifies the action after address probe failure due to a temporary problem (default: defer_if_permit).
This feature is available in Postfix 2.1 and later.

Other restrictions that are valid in this context:

- Generic restrictions that can be used in any SMTP command context, described under smtpd_client_restrictions.
- SMTP command specific restrictions described under smtpd_client_restrictions, smtpd_helo_restrictions and smtpd_sender_restrictions.

Example:

```
# The Postfix before 2.10 default mail relay policy. Later Postfix
# versions implement this preferably with smtpd_relay_restrictions.
smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination
```

smtpd_reject_footer (default: empty)

Optional information that is appended after each Postfix SMTP server 4XX or 5XX response.

The following example uses "\c" at the start of the template (supported in Postfix 2.10 and later) to suppress the line break between the reply text and the footer text. With earlier Postfix versions, the footer text always begins on a new line, and the "\c" is output literally.

```
/etc/postfix/main.cf:
smtpd_reject_footer = \c. For assistance, call 800-555-0101.
Please provide the following information in your problem report:
time ($localtime), client ($client_address) and server
($server_name).
```

Server response:

```
550-5.5.1 <user@example> Recipient address rejected: User
unknown. For assistance, call 800-555-0101. Please provide the
following information in your problem report: time (Jan 4 15:42:00),
client (192.168.1.248) and server (mail1.example.com).
```

Note: the above text is meant to make it easier to find the Postfix logfile records for a failed SMTP session. The text itself is not logged to the Postfix SMTP server's maillog file.

Be sure to keep the text as short as possible. Long text may be truncated before it is logged to the remote SMTP client's maillog file, or before it is returned to the sender in a delivery status notification.

This feature supports a limited number of $name attributes in the footer text. These are replaced by their current value for the SMTP session:

client_address
: The Client IP address that is logged in the maillog file.

client_port
: The client TCP port that is logged in the maillog file.

localtime
: The server local time (Mmm dd hh:mm:ss) that is logged in the maillog file.

server_name
: The server's myhostname value. This attribute is made available for sites with multiple MTAs (perhaps behind a load-balancer), where the server name can help the server support team to quickly find the right log files.

Notes:

- NOT SUPPORTED are other attributes such as sender, recipient, or main.cf parameters.
- For safety reasons, text that does not match $smtpd_expansion_filter is censored.

This feature supports the two-character sequence \n as a request for a line break in the footer text. Postfix automatically inserts after each line break the three-digit SMTP reply code (and optional enhanced status code) from the original Postfix reject message.

To work around mail software that mis-handles multi-line replies, specify the two-character sequence \c at the start of the template. This suppresses the line break between the reply text and the footer text (Postfix 2.10 and later).

This feature is available in Postfix 2.8 and later.

smtpd_reject_unlisted_recipient (default: yes)

Request that the Postfix SMTP server rejects mail for unknown recipient addresses, even when no explicit reject_unlisted_recipient access restriction is specified. This prevents the Postfix queue from filling up with undeliverable MAILER-DAEMON messages.

An address is always considered "known" when it matches a **virtual(5)** alias or a **canonical(5)** mapping.

- The recipient domain matches $mydestination, $inet_interfaces or $proxy_interfaces, but the recipient is not listed in $local_recipient_maps, and $local_recipient_maps is not null.
- The recipient domain matches $virtual_alias_domains but the recipient is not listed in $virtual_alias_maps.
- The recipient domain matches $virtual_mailbox_domains but the recipient is not listed in $virtual_mailbox_maps, and $virtual_mailbox_maps is not null.
- The recipient domain matches $relay_domains but the recipient is not listed in $relay_recipient_maps, and $relay_recipient_maps is not null.

This feature is available in Postfix 2.1 and later.

smtpd_reject_unlisted_sender (default: no)

Request that the Postfix SMTP server rejects mail from unknown sender addresses, even when no explicit reject_unlisted_sender access restriction is specified. This can slow down an explosion of forged mail from worms or viruses.

An address is always considered "known" when it matches a **virtual(5)** alias or a **canonical(5)** mapping.

- The sender domain matches $mydestination, $inet_interfaces or $proxy_interfaces, but the sender is not listed in $local_recipient_maps, and $local_recipient_maps is not null.
- The sender domain matches $virtual_alias_domains but the sender is not listed in $virtual_alias_maps.
- The sender domain matches $virtual_mailbox_domains but the sender is not listed in $virtual_mailbox_maps, and $virtual_mailbox_maps is not null.
- The sender domain matches $relay_domains but the sender is not listed in $relay_recipient_maps, and $relay_recipient_maps is not null.

This feature is available in Postfix 2.1 and later.

smtpd_relay_restrictions (default: permit_mynetworks, permit_sasl_authenticated, defer_unauth_destination)

Access restrictions for mail relay control that the Postfix SMTP server applies in the context of the RCPT TO command, before smtpd_recipient_restrictions. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

With Postfix versions before 2.10, the rules for relay permission and spam blocking were combined under smtpd_recipient_restrictions, resulting in error-prone configuration. As of Postfix 2.10, relay permission rules are preferably implemented with smtpd_relay_restrictions, so that a permissive spam blocking policy under smtpd_recipient_restrictions will no longer result in a permissive mail relay policy.

For backwards compatibility, sites that migrate from Postfix versions before 2.10 can set smtpd_relay_restrictions to the empty value, and use smtpd_recipient_restrictions exactly as before.

By default, the Postfix SMTP server accepts:

- Mail from clients whose IP address matches $mynetworks, or:
- Mail to remote destinations that match $relay_domains, except for addresses that contain sender-specified routing (user@elsewhere@domain), or:
- Mail to local destinations that match $inet_interfaces or $proxy_interfaces, $mydestination, $virtual_alias_domains, or $virtual_mailbox_domains.

IMPORTANT: Either the smtpd_relay_restrictions or the smtpd_recipient_restrictions parameter must

specify at least one of the following restrictions. Otherwise Postfix will refuse to receive mail:

```
reject, reject_unauth_destination

defer, defer_if_permit, defer_unauth_destination
```

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. The same restrictions are available as documented under smtpd_recipient_restrictions.

This feature is available in Postix 2.10 and later.

smtpd_restriction_classes (default: empty)

User-defined aliases for groups of access restrictions. The aliases can be specified in smtpd_recipient_restrictions etc., and on the right-hand side of a Postfix **access(5)** table.

One major application is for implementing per-recipient UCE control. See the RESTRICTION_CLASS_README document for other examples.

smtpd_sasl_application_name (default: smtpd)

The application name that the Postfix SMTP server uses for SASL server initialization. This controls the name of the SASL configuration file. The default value is **smtpd**, corresponding to a SASL configuration file named **smtpd.conf**.

This feature is available in Postfix 2.1 and 2.2. With Postfix 2.3 it was renamed to smtpd_sasl_path.

smtpd_sasl_auth_enable (default: no)

Enable SASL authentication in the Postfix SMTP server. By default, the Postfix SMTP server does not use authentication.

If a remote SMTP client is authenticated, the permit_sasl_authenticated access restriction can be used to permit relay access, like this:

```
# With Postfix 2.10 and later, the mail relay policy is
# preferably specified under smtpd_relay_restrictions.
smtpd_relay_restrictions =
permit_mynetworks, permit_sasl_authenticated, ...

# With Postfix before 2.10, the relay policy can be
# specified only under smtpd_recipient_restrictions.
smtpd_recipient_restrictions =
permit_mynetworks, permit_sasl_authenticated, ...
```

To reject all SMTP connections from unauthenticated clients, specify "smtpd_delay_reject = yes" (which is the default) and use:

```
smtpd_client_restrictions = permit_sasl_authenticated, reject
```

See the SASL_README file for SASL configuration and operation details.

smtpd_sasl_authenticated_header (default: no)

Report the SASL authenticated user name in the **smtpd(8)** Received message header.

This feature is available in Postfix 2.3 and later.

smtpd_sasl_exceptions_networks (default: empty)

What remote SMTP clients the Postfix SMTP server will not offer AUTH support to.

Some clients (Netscape 4 at least) have a bug that causes them to require a login and password whenever AUTH is offered, whether it’s necessary or not. To work around this, specify, for example, $mynetworks to prevent Postfix from offering AUTH to local clients.

Specify a list of network/netmask patterns, separated by commas and/or whitespace. The mask specifies the number of bits in the network part of a host address. You can also "/file/name" or "type:table" patterns. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with

whitespace. Specify "!pattern" to exclude an address or network block from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

Note: IP version 6 address information must be specified inside [] in the smtpd_sasl_exceptions_networks value, and in files specified with "/file/name". IP version 6 addresses contain the ":" character, and would otherwise be confused with a "type:table" pattern.

Example:

```
smtpd_sasl_exceptions_networks = $mynetworks
```

This feature is available in Postfix 2.1 and later.

smtpd_sasl_local_domain (default: empty)

The name of the Postfix SMTP server's local SASL authentication realm.

By default, the local authentication realm name is the null string.

Examples:

```
smtpd_sasl_local_domain = $mydomain
smtpd_sasl_local_domain = $myhostname
```

smtpd_sasl_path (default: smtpd)

Implementation-specific information that the Postfix SMTP server passes through to the SASL plug-in implementation that is selected with **smtpd_sasl_type**. Typically this specifies the name of a configuration file or rendezvous point.

This feature is available in Postfix 2.3 and later. In earlier releases it was called **smtpd_sasl_application_name**.

smtpd_sasl_security_options (default: noanonymous)

Postfix SMTP server SASL security options; as of Postfix 2.3 the list of available features depends on the SASL server implementation that is selected with **smtpd_sasl_type**.

The following security features are defined for the **cyrus** server SASL implementation:

Restrict what authentication mechanisms the Postfix SMTP server will offer to the client. The list of available authentication mechanisms is system dependent.

Specify zero or more of the following:

noplaintext
: Disallow methods that use plaintext passwords.

noactive
: Disallow methods subject to active (non-dictionary) attack.

nodictionary
: Disallow methods subject to passive (dictionary) attack.

noanonymous
: Disallow methods that allow anonymous authentication.

forward_secrecy
: Only allow methods that support forward secrecy (Dovecot only).

mutual_auth
: Only allow methods that provide mutual authentication (not available with Cyrus SASL version 1).

By default, the Postfix SMTP server accepts plaintext passwords but not anonymous logins.

Warning: it appears that clients try authentication methods in the order as advertised by the server (e.g., PLAIN ANONYMOUS CRAM-MD5) which means that if you disable plaintext passwords, clients will log in anonymously, even when they should be able to use CRAM-MD5. So, if you disable plaintext logins, disable anonymous logins too. Postfix treats anonymous login as no authentication.

Example:

```
smtpd_sasl_security_options = noanonymous, noplaintext
```

smtpd_sasl_service (default: smtp)
The service name that is passed to the SASL plug-in that is selected with **smtpd_sasl_type** and **smtpd_sasl_path**.

This feature is available in Postfix 2.11 and later. Prior versions behave as if "**smtp**" is specified.

smtpd_sasl_tls_security_options (default: $smtpd_sasl_security_options)
The SASL authentication security options that the Postfix SMTP server uses for TLS encrypted SMTP sessions.

This feature is available in Postfix 2.2 and later.

smtpd_sasl_type (default: cyrus)
The SASL plug-in type that the Postfix SMTP server should use for authentication. The available types are listed with the "**postconf -a**" command.

This feature is available in Postfix 2.3 and later.

smtpd_sender_login_maps (default: empty)
Optional lookup table with the SASL login names that own the sender (MAIL FROM) addresses.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found. With lookups from indexed files such as DB or DBM, or from networked tables such as NIS, LDAP or SQL, the following search operations are done with a sender address of *user@domain*:

1) *user@domain*
This table lookup is always done and has the highest precedence.

2) *user* This table lookup is done only when the *domain* part of the sender address matches $myorigin, $mydestination, $inet_interfaces or $proxy_interfaces.

3) *@domain*
This table lookup is done last and has the lowest precedence.

In all cases the result of table lookup must be either "not found" or a list of SASL login names separated by comma and/or whitespace.

smtpd_sender_restrictions (default: empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client MAIL FROM command. See SMTPD_ACCESS_README, section "Delayed evaluation of SMTP access restriction lists" for a discussion of evaluation context and time.

The default is to permit everything.

Specify a list of restrictions, separated by commas and/or whitespace. Continue long lines by starting the next line with whitespace. Restrictions are applied in the order as specified; the first restriction that matches wins.

The following restrictions are specific to the sender address received with the MAIL FROM command.

check_sender_access *type:table*
Search the specified **access(5)** database for the MAIL FROM address, domain, parent domains, or localpart@, and execute the corresponding action.

check_sender_a_access *type:table*
Search the specified **access(5)** database for the IP addresses for the MAIL FROM domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 3.0 and later.

check_sender_mx_access *type:table*
Search the specified **access(5)** database for the MX hosts for the MAIL FROM domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.1 and later.

check_sender_ns_access *type:table*
Search the specified **access(5)** database for the DNS servers for the MAIL FROM domain, and execute the corresponding action. Note: a result of "OK" is not allowed for safety reasons. Instead, use DUNNO in order to exclude specific hosts from blacklists. This feature is available in Postfix 2.1 and later.

reject_authenticated_sender_login_mismatch
Enforces the reject_sender_login_mismatch restriction for authenticated clients only. This feature is available in Postfix version 2.1 and later.

reject_known_sender_login_mismatch
Apply the reject_sender_login_mismatch restriction only to MAIL FROM addresses that are known in $smtpd_sender_login_maps. This feature is available in Postfix version 2.11 and later.

reject_non_fqdn_sender
Reject the request when the MAIL FROM address is not in fully-qualified domain form, as required by the RFC.
The non_fqdn_reject_code parameter specifies the response code for rejected requests (default: 504).

reject_rhsbl_sender *rbl_domain=d.d.d.d*
Reject the request when the MAIL FROM domain is listed with the A record "*d.d.d.d*" under *rbl_domain* (Postfix version 2.1 and later only). Each "*d*" is a number, or a pattern inside "[]" that contains one or more ";"-separated numbers or number..number ranges (Postfix version 2.8 and later). If no "*=d.d.d.d*" is specified, reject the request when the MAIL FROM domain is listed with any A record under *rbl_domain*.
The maps_rbl_reject_code parameter specifies the response code for rejected requests (default: 554); the default_rbl_reply parameter specifies the default server reply; and the rbl_reply_maps parameter specifies tables with server replies indexed by *rbl_domain*. This feature is available in Postfix 2.0 and later.

reject_sender_login_mismatch
Reject the request when $smtpd_sender_login_maps specifies an owner for the MAIL FROM address, but the client is not (SASL) logged in as that MAIL FROM address owner; or when the client is (SASL) logged in, but the client login name doesn't own the MAIL FROM address according to $smtpd_sender_login_maps.

reject_unauthenticated_sender_login_mismatch
Enforces the reject_sender_login_mismatch restriction for unauthenticated clients only. This feature is available in Postfix version 2.1 and later.

reject_unknown_sender_domain
Reject the request when Postfix is not final destination for the sender address, and the MAIL FROM domain has 1) no DNS MX and no DNS A record, or 2) a malformed MX record such as a record with a zero-length MX hostname (Postfix version 2.3 and later).
The reply is specified with the unknown_address_reject_code parameter (default: 450), unknown_address_tempfail_action (default: defer_if_permit), or 550 (nullmx, Postfix 3.0 and later). See the respective parameter descriptions for details.

reject_unlisted_sender
Reject the request when the MAIL FROM address is not listed in the list of valid recipients for its domain class. See the smtpd_reject_unlisted_sender parameter description for details. This feature is available in Postfix 2.1 and later.

reject_unverified_sender

Reject the request when mail to the MAIL FROM address is known to bounce, or when the sender address destination is not reachable. Address verification information is managed by the **verify(8)** server; see the ADDRESS_VERIFICATION_README file for details.

The unverified_sender_reject_code parameter specifies the numerical response code when an address is known to bounce (default: 450, change into 550 when you are confident that it is safe to do so).

The unverified_sender_defer_code specifies the numerical response code when an address probe failed due to a temporary problem (default: 450).

The unverified_sender_tempfail_action parameter specifies the action after address probe failure due to a temporary problem (default: defer_if_permit).

This feature is available in Postfix 2.1 and later.

Other restrictions that are valid in this context:

- Generic restrictions that can be used in any SMTP command context, described under smtpd_client_restrictions.
- SMTP command specific restrictions described under smtpd_client_restrictions and smtpd_helo_restrictions.
- SMTP command specific restrictions described under smtpd_recipient_restrictions. When recipient restrictions are listed under smtpd_sender_restrictions, they have effect only with "smtpd_delay_reject = yes", so that $smtpd_sender_restrictions is evaluated at the time of the RCPT TO command.

Examples:

```
smtpd_sender_restrictions = reject_unknown_sender_domain
smtpd_sender_restrictions = reject_unknown_sender_domain,
check_sender_access hash:/etc/postfix/access
```

smtpd_service_name (default: smtpd)

The internal service that **postscreen(8)** hands off allowed connections to. In a future version there may be different classes of SMTP service.

This feature is available in Postfix 2.8.

smtpd_soft_error_limit (default: 10)

The number of errors a remote SMTP client is allowed to make without delivering mail before the Postfix SMTP server slows down all its responses.

- With Postfix version 2.1 and later, the Postfix SMTP server delays all responses by $smtpd_error_sleep_time seconds.
- With Postfix versions 2.0 and earlier, the Postfix SMTP server delays all responses by (number of errors) seconds.

smtpd_starttls_timeout (default: see postconf −d output)

The time limit for Postfix SMTP server write and read operations during TLS startup and shutdown handshake procedures. The current default value is stress-dependent. Before Postfix version 2.8, it was fixed at 300s.

This feature is available in Postfix 2.2 and later.

smtpd_timeout (default: normal: 300s, overload: 10s)

The time limit for sending a Postfix SMTP server response and for receiving a remote SMTP client request. Normally the default limit is 300s, but it changes under overload to just 10s. With Postfix 2.5 and earlier, the SMTP server always uses a time limit of 300s by default.

Note: if you set SMTP time limits to very large values you may have to update the global ipc_timeout parameter.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

smtpd_tls_CAfile (default: empty)

A file containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates. These are loaded into memory before the **smtpd(8)** server enters the chroot jail. If the number of trusted roots is large, consider using smtpd_tls_CApath instead, but note that the latter directory must be present in the chroot jail if the **smtpd(8)** server is chrooted. This file may also be used to augment the server certificate trust chain, but it is best to include all the required certificates directly in the server certificate file.

Specify "smtpd_tls_CAfile = /path/to/system_CA_file" to use ONLY the system-supplied default Certification Authority certificates.

Specify "tls_append_default_CA = no" to prevent Postfix from appending the system-supplied default CAs and trusting third-party certificates.

By default (see smtpd_tls_ask_ccert), client certificates are not requested, and smtpd_tls_CAfile should remain empty. If you do make use of client certificates, the distinguished names (DNs) of the Certification Authorities listed in smtpd_tls_CAfile are sent to the remote SMTP client in the client certificate request message. MUAs with multiple client certificates may use the list of preferred Certification Authorities to select the correct client certificate. You may want to put your "preferred" CA or CAs in this file, and install other trusted CAs in $smtpd_tls_CApath.

Example:

```
smtpd_tls_CAfile = /etc/postfix/CAcert.pem
```

This feature is available in Postfix 2.2 and later.

smtpd_tls_CApath (default: empty)

A directory containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates. Do not forget to create the necessary "hash" links with, for example, "$OPENSSL_HOME/bin/c_rehash /etc/postfix/certs". To use smtpd_tls_CApath in chroot mode, this directory (or a copy) must be inside the chroot jail.

Specify "smtpd_tls_CApath = /path/to/system_CA_directory" to use ONLY the system-supplied default Certification Authority certificates.

Specify "tls_append_default_CA = no" to prevent Postfix from appending the system-supplied default CAs and trusting third-party certificates.

By default (see smtpd_tls_ask_ccert), client certificates are not requested, and smtpd_tls_CApath should remain empty. In contrast to smtpd_tls_CAfile, DNs of Certification Authorities installed in $smtpd_tls_CApath are not included in the client certificate request message. MUAs with multiple client certificates may use the list of preferred Certification Authorities to select the correct client certificate. You may want to put your "preferred" CA or CAs in $smtpd_tls_CAfile, and install the remaining trusted CAs in $smtpd_tls_CApath.

Example:

```
smtpd_tls_CApath = /etc/postfix/certs
```

This feature is available in Postfix 2.2 and later.

smtpd_tls_always_issue_session_ids (default: yes)

Force the Postfix SMTP server to issue a TLS session id, even when TLS session caching is turned off (smtpd_tls_session_cache_database is empty). This behavior is compatible with Postfix < 2.3.

With Postfix 2.3 and later the Postfix SMTP server can disable session id generation when TLS session caching is turned off. This keeps remote SMTP clients from caching sessions that almost certainly cannot be re-used.

By default, the Postfix SMTP server always generates TLS session ids. This works around a known defect in mail client applications such as MS Outlook, and may also prevent interoperability issues with other MTAs.

Example:

```
smtpd_tls_always_issue_session_ids = no
```

This feature is available in Postfix 2.3 and later.

smtpd_tls_ask_ccert (default: no)

Ask a remote SMTP client for a client certificate. This information is needed for certificate based mail relaying with, for example, the permit_tls_clientcerts feature.

Some clients such as Netscape will either complain if no certificate is available (for the list of CAs in $smtpd_tls_CAfile) or will offer multiple client certificates to choose from. This may be annoying, so this option is "off" by default.

This feature is available in Postfix 2.2 and later.

smtpd_tls_auth_only (default: no)

When TLS encryption is optional in the Postfix SMTP server, do not announce or accept SASL authentication over unencrypted connections.

This feature is available in Postfix 2.2 and later.

smtpd_tls_ccert_verifydepth (default: 9)

The verification depth for remote SMTP client certificates. A depth of 1 is sufficient if the issuing CA is listed in a local CA file.

The default verification depth is 9 (the OpenSSL default) for compatibility with earlier Postfix behavior. Prior to Postfix 2.5, the default value was 5, but the limit was not actually enforced. If you have set this to a lower non-default value, certificates with longer trust chains may now fail to verify. Certificate chains with 1 or 2 CAs are common, deeper chains are more rare and any number between 5 and 9 should suffice in practice. You can choose a lower number if, for example, you trust certificates directly signed by an issuing CA but not any CAs it delegates to.

This feature is available in Postfix 2.2 and later.

smtpd_tls_cert_file (default: empty)

File with the Postfix SMTP server RSA certificate in PEM format. This file may also contain the Postfix SMTP server private RSA key.

Public Internet MX hosts without certificates signed by a "reputable" CA must generate, and be prepared to present to most clients, a self-signed or private-CA signed certificate. The client will not be able to authenticate the server, but unless it is running Postfix 2.3 or similar software, it will still insist on a server certificate.

For servers that are **not** public Internet MX hosts, Postfix 2.3 supports configurations with no certificates. This entails the use of just the anonymous TLS ciphers, which are not supported by typical SMTP clients. Since such clients will not, as a rule, fall back to plain text after a TLS handshake failure, the server will be unable to receive email from TLS enabled clients. To avoid accidental configurations with no certificates, Postfix 2.3 enables certificate-less operation only when the administrator explicitly sets "smtpd_tls_cert_file = none". This ensures that new Postfix configurations will not accidentally run with no certificates.

Both RSA and DSA certificates are supported. When both types are present, the cipher used determines which certificate will be presented to the client. For Netscape and OpenSSL clients without special cipher choices the RSA certificate is preferred.

To enable a remote SMTP client to verify the Postfix SMTP server certificate, the issuing CA certificates must be made available to the client. You should include the required certificates in the server certificate file, the server certificate first, then the issuing CA(s) (bottom-up order).

Example: the certificate for "server.example.com" was issued by "intermediate CA" which itself has a certificate of "root CA". Create the server.pem file with "cat server_cert.pem intermediate_CA.pem root_CA.pem > server.pem".

If you also want to verify client certificates issued by these CAs, you can add the CA certificates to the smtpd_tls_CAfile, in which case it is not necessary to have them in the smtpd_tls_cert_file or smtpd_tls_dcert_file.

A certificate supplied here must be usable as an SSL server certificate and hence pass the "openssl verify -purpose sslserver ..." test.

Example:

```
smtpd_tls_cert_file = /etc/postfix/server.pem
```

This feature is available in Postfix 2.2 and later.

smtpd_tls_cipherlist (default: empty)

Obsolete Postfix < 2.3 control for the Postfix SMTP server TLS cipher list. It is easy to create interoperability problems by choosing a non-default cipher list. Do not use a non-default TLS cipherlist for MX hosts on the public Internet. Clients that begin the TLS handshake, but are unable to agree on a common cipher, may not be able to send any email to the SMTP server. Using a restricted cipher list may be more appropriate for a dedicated MSA or an internal mailhub, where one can exert some control over the TLS software and settings of the connecting clients.

Note: do not use "" quotes around the parameter value.

This feature is available with Postfix version 2.2. It is not used with Postfix 2.3 and later; use smtpd_tls_mandatory_ciphers instead.

smtpd_tls_ciphers (default: medium)

The minimum TLS cipher grade that the Postfix SMTP server will use with opportunistic TLS encryption. Cipher types listed in smtpd_tls_exclude_ciphers are excluded from the base definition of the selected cipher grade. The default value is "medium" for Postfix releases after the middle of 2015, "export" for older releases.

When TLS is mandatory the cipher grade is chosen via the smtpd_tls_mandatory_ciphers configuration parameter, see there for syntax details.

This feature is available in Postfix 2.6 and later. With earlier Postfix releases only the smtpd_tls_mandatory_ciphers parameter is implemented, and opportunistic TLS always uses "export" or better (i.e. all) ciphers.

smtpd_tls_dcert_file (default: empty)

File with the Postfix SMTP server DSA certificate in PEM format. This file may also contain the Postfix SMTP server private DSA key.

See the discussion under smtpd_tls_cert_file for more details.

Example:

```
smtpd_tls_dcert_file = /etc/postfix/server-dsa.pem
```

This feature is available in Postfix 2.2 and later.

smtpd_tls_dh1024_param_file (default: empty)

File with DH parameters that the Postfix SMTP server should use with non-export EDH ciphers.

Instead of using the exact same parameter sets as distributed with other TLS packages, it is more secure to generate your own set of parameters with something like the following commands:

```
openssl dhparam -out /etc/postfix/dh512.pem 512
openssl dhparam -out /etc/postfix/dh1024.pem 1024
openssl dhparam -out /etc/postfix/dh2048.pem 2048
```

It is safe to share the same DH parameters between multiple Postfix instances. If you prefer, you can generate separate parameters for each instance.

If you want to take maximal advantage of ciphers that offer forward secrecy see the Getting started section of FORWARD_SECRECY_README. The full document conveniently presents all information about Postfix "perfect" forward secrecy support in one place: what forward secrecy is, how to tweak settings, and what you can expect to see when Postfix uses ciphers with forward secrecy.

Example:

```
smtpd_tls_dh1024_param_file = /etc/postfix/dh2048.pem
```

This feature is available with Postfix version 2.2.

smtpd_tls_dh512_param_file (default: empty)
File with DH parameters that the Postfix SMTP server should use with export-grade EDH ciphers. The default SMTP server cipher grade is "medium" with Postfix releases after the middle of 2015, and as a result export-grade cipher suites are by default not used.

See also the discussion under the smtpd_tls_dh1024_param_file configuration parameter.

Example:

```
smtpd_tls_dh512_param_file = /etc/postfix/dh_512.pem
```

This feature is available with Postfix version 2.2.

smtpd_tls_dkey_file (default: $smtpd_tls_dcert_file)
File with the Postfix SMTP server DSA private key in PEM format. This file may be combined with the Postfix SMTP server DSA certificate file specified with $smtpd_tls_dcert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

This feature is available in Postfix 2.2 and later.

smtpd_tls_eccert_file (default: empty)
File with the Postfix SMTP server ECDSA certificate in PEM format. This file may also contain the Postfix SMTP server private ECDSA key.

See the discussion under smtpd_tls_cert_file for more details.

Example:

```
smtpd_tls_eccert_file = /etc/postfix/ecdsa-scert.pem
```

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

smtpd_tls_eckey_file (default: $smtpd_tls_eccert_file)
File with the Postfix SMTP server ECDSA private key in PEM format. This file may be combined with the Postfix SMTP server ECDSA certificate file specified with $smtpd_tls_eccert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

This feature is available in Postfix 2.6 and later, when Postfix is compiled and linked with OpenSSL 1.0.0 or later.

smtpd_tls_eecdh_grade (default: see postconf −d output)
The Postfix SMTP server security grade for ephemeral elliptic-curve Diffie-Hellman (EECDH) key exchange.

The available choices are:

none Don’t use EECDH. Ciphers based on EECDH key exchange will be disabled. This is the default in Postfix versions 2.6 and 2.7.

strong Use EECDH with approximately 128 bits of security at a reasonable computational cost. This is the current best-practice trade-off between security and computational efficiency. This is the default in Postfix version 2.8 and later.

ultra Use EECDH with approximately 192 bits of security at computational cost that is approximately twice as high as 128 bit strength ECC. Barring significant progress in attacks on elliptic curve crypto-systems, the "strong" curve is sufficient for most users.

If you want to take maximal advantage of ciphers that offer forward secrecy see the Getting started section of FORWARD_SECRECY_README. The full document conveniently presents all information about

Postfix "perfect" forward secrecy support in one place: what forward secrecy is, how to tweak settings, and what you can expect to see when Postfix uses ciphers with forward secrecy.

This feature is available in Postfix 2.6 and later, when it is compiled and linked with OpenSSL 1.0.0 or later on platforms where EC algorithms have not been disabled by the vendor.

smtpd_tls_exclude_ciphers (default: empty)

List of ciphers or cipher types to exclude from the SMTP server cipher list at all TLS security levels. Excluding valid ciphers can create interoperability problems. DO NOT exclude ciphers unless it is essential to do so. This is not an OpenSSL cipherlist; it is a simple list separated by whitespace and/or commas. The elements are a single cipher, or one or more "+" separated cipher properties, in which case only ciphers matching **all** the properties are excluded.

Examples (some of these will cause problems):

```
smtpd_tls_exclude_ciphers = aNULL
smtpd_tls_exclude_ciphers = MD5, DES
smtpd_tls_exclude_ciphers = DES+MD5
smtpd_tls_exclude_ciphers = AES256-SHA, DES-CBC3-MD5
smtpd_tls_exclude_ciphers = kEDH+aRSA
```

The first setting disables anonymous ciphers. The next setting disables ciphers that use the MD5 digest algorithm or the (single) DES encryption algorithm. The next setting disables ciphers that use MD5 and DES together. The next setting disables the two ciphers "AES256-SHA" and "DES-CBC3-MD5". The last setting disables ciphers that use "EDH" key exchange with RSA authentication.

This feature is available in Postfix 2.3 and later.

smtpd_tls_fingerprint_digest (default: md5)

The message digest algorithm to construct remote SMTP client-certificate fingerprints or public key fingerprints (Postfix 2.9 and later) for **check_ccert_access** and **permit_tls_clientcerts**. The default algorithm is **md5**, for backwards compatibility with Postfix releases prior to 2.5.

Advances in hash function cryptanalysis have led to md5 being deprecated in favor of sha1. However, as long as there are no known "second pre-image" attacks against md5, its use in this context can still be considered safe.

While additional digest algorithms are often available with OpenSSL's libcrypto, only those used by libssl in SSL cipher suites are available to Postfix.

To find the fingerprint of a specific certificate file, with a specific digest algorithm, run:

```
$ openssl x509 -noout -fingerprint -digest -in certfile.pem
```

The text to the right of "=" sign is the desired fingerprint. For example:

```
$ openssl x509 -noout -fingerprint -sha1 -in cert.pem
SHA1 Fingerprint=D4:6A:AB:19:24:79:F8:32:BB:A6:CB:66:82:C0:8E:9B:EE:29:A8:1
```

To extract the public key fingerprint from an X.509 certificate, you need to extract the public key from the certificate and compute the appropriate digest of its DER (ASN.1) encoding. With OpenSSL the "-pubkey" option of the "x509" command extracts the public key always in "PEM" format. We pipe the result to another OpenSSL command that converts the key to DER and then to the "dgst" command to compute the fingerprint.

The actual command to transform the key to DER format depends on the version of OpenSSL used. With OpenSSL 1.0.0 and later, the "pkey" command supports all key types. With OpenSSL 0.9.8 and earlier, the key type is always RSA (nobody uses DSA, and EC keys are not fully supported by 0.9.8), so the "rsa" command is used.

```
# OpenSSL 1.0 with all certificates and SHA-1 fingerprints.
$ openssl x509 -in cert.pem -noout -pubkey |
openssl pkey -pubin -outform DER |
openssl dgst -sha1 -c
```

```
(stdin)= 64:3f:1f:f6:e5:1e:d4:2a:56:8b:fc:09:1a:61:98:b5:bc:7c:60:58

# OpenSSL 0.9.8 with RSA certificates and MD5 fingerprints.
$ openssl x509 -in cert.pem -noout -pubkey |
openssl rsa -pubin -outform DER |
openssl dgst -md5 -c
(stdin)= f4:62:60:f6:12:8f:d5:8d:28:4d:13:a7:db:b2:ff:50
```

The Postfix SMTP server and client log the peer (leaf) certificate fingerprint and public key fingerprint when the TLS loglevel is 2 or higher.

Note: Postfix 2.9.0-2.9.5 computed the public key fingerprint incorrectly. To use public-key fingerprints, upgrade to Postfix 2.9.6 or later.

Example: client-certificate access table, with sha1 fingerprints:

```
/etc/postfix/main.cf:
smtpd_tls_fingerprint_digest = sha1
smtpd_client_restrictions =
check_ccert_access hash:/etc/postfix/access,
reject
/etc/postfix/access:
# Action folded to next line...
AF:88:7C:AD:51:95:6F:36:96:F6:01:FB:2E:48:CD:AB:49:25:A2:3B
OK
85:16:78:FD:73:6E:CE:70:E0:31:5F:0D:3C:C8:6D:C4:2C:24:59:E1
permit_auth_destination
```

This feature is available in Postfix 2.5 and later.

smtpd_tls_key_file (default: $smtpd_tls_cert_file)

File with the Postfix SMTP server RSA private key in PEM format. This file may be combined with the Postfix SMTP server RSA certificate file specified with $smtpd_tls_cert_file.

The private key must be accessible without a pass-phrase, i.e. it must not be encrypted. File permissions should grant read-only access to the system superuser account ("root"), and no access to anyone else.

smtpd_tls_loglevel (default: 0)

Enable additional Postfix SMTP server logging of TLS activity. Each logging level also includes the information that is logged at a lower logging level.

0 Disable logging of TLS activity.

1 Log only a summary message on TLS handshake completion - no logging of client certificate trust-chain verification errors if client certificate verification is not required. With Postfix 2.8 and earlier, log the summary message, peer certificate summary information and unconditionally log trust-chain verification errors.

2 Also log levels during TLS negotiation.

3 Also log hexadecimal and ASCII dump of TLS negotiation process.

4 Also log hexadecimal and ASCII dump of complete transmission after STARTTLS.

Do not use "smtpd_tls_loglevel = 2" or higher except in case of problems. Use of loglevel 4 is strongly discouraged.

This feature is available in Postfix 2.2 and later.

smtpd_tls_mandatory_ciphers (default: medium)

The minimum TLS cipher grade that the Postfix SMTP server will use with mandatory TLS encryption. The default grade ("medium") is sufficiently strong that any benefit from globally restricting TLS sessions to a more stringent grade is likely negligible, especially given the fact that many implementations still do not offer any stronger ("high" grade) ciphers, while those that do, will always use "high" grade ciphers. So

insisting on "high" grade ciphers is generally counter-productive. Allowing "export" or "low" ciphers is typically not a good idea, as systems limited to just these are limited to obsolete browsers. No known SMTP clients fail to support at least one "medium" or "high" grade cipher.

The following cipher grades are supported:

export Enable "EXPORT" grade or stronger OpenSSL ciphers. The underlying cipherlist is specified via the tls_export_cipherlist configuration parameter, which you are strongly encouraged to not change. This choice is insecure and SHOULD NOT be used.

low Enable "LOW" grade or stronger OpenSSL ciphers. The underlying cipherlist is specified via the tls_low_cipherlist configuration parameter, which you are strongly encouraged to not change. This choice is insecure and SHOULD NOT be used.

medium
Enable "MEDIUM" grade or stronger OpenSSL ciphers. These use 128-bit or longer symmetric bulk-encryption keys. This is the default minimum strength for mandatory TLS encryption. The underlying cipherlist is specified via the tls_medium_cipherlist configuration parameter, which you are strongly encouraged to not change.

high Enable only "HIGH" grade OpenSSL ciphers. The underlying cipherlist is specified via the tls_high_cipherlist configuration parameter, which you are strongly encouraged to not change.

null Enable only the "NULL" OpenSSL ciphers, these provide authentication without encryption. This setting is only appropriate in the rare case that all clients are prepared to use NULL ciphers (not normally enabled in TLS clients). The underlying cipherlist is specified via the tls_null_cipherlist configuration parameter, which you are strongly encouraged to not change.

Cipher types listed in smtpd_tls_mandatory_exclude_ciphers or smtpd_tls_exclude_ciphers are excluded from the base definition of the selected cipher grade. See smtpd_tls_ciphers for cipher controls that apply to opportunistic TLS.

The underlying cipherlists for grades other than "null" include anonymous ciphers, but these are automatically filtered out if the server is configured to ask for remote SMTP client certificates. You are very unlikely to need to take any steps to exclude anonymous ciphers, they are excluded automatically as required. If you must exclude anonymous ciphers even when Postfix does not need or use peer certificates, set "smtpd_tls_exclude_ciphers = aNULL". To exclude anonymous ciphers only when TLS is enforced, set "smtpd_tls_mandatory_exclude_ciphers = aNULL".

This feature is available in Postfix 2.3 and later.

smtpd_tls_mandatory_exclude_ciphers (default: empty)
Additional list of ciphers or cipher types to exclude from the Postfix SMTP server cipher list at mandatory TLS security levels. This list works in addition to the exclusions listed with smtpd_tls_exclude_ciphers (see there for syntax details).

This feature is available in Postfix 2.3 and later.

smtpd_tls_mandatory_protocols (default: !SSLv2, !SSLv3)
The SSL/TLS protocols accepted by the Postfix SMTP server with mandatory TLS encryption. If the list is empty, the server supports all available SSL/TLS protocol versions. A non-empty value is a list of protocol names separated by whitespace, commas or colons. The supported protocol names are "SSLv2", "SSLv3" and "TLSv1", and are not case sensitive. The default value is "!SSLv2, !SSLv3" for Postfix releases after the middle of 2015, "!SSLv2" for older releases.

With Postfix >= 2.5 the parameter syntax was expanded to support protocol exclusions. One can explicitly exclude "SSLv2" by setting "smtpd_tls_mandatory_protocols = !SSLv2". To exclude both "SSLv2" and "SSLv3" set "smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3". Listing the protocols to include, rather than protocols to exclude, is supported, but not recommended. The exclusion form more closely matches the underlying OpenSSL interface semantics.

Note: As of OpenSSL 1.0.1 two new protocols are defined, "TLSv1.1" and "TLSv1.2". When Postfix <= 2.5 is linked against OpenSSL 1.0.1 or later, these, or any other new protocol versions, cannot be disabled.

The latest patch levels of Postfix >= 2.6, and all versions of Postfix >= 2.10 can disable support for "TLSv1.1" or "TLSv1.2".

OpenSSL 1.1.1 introduces support for "TLSv1.3". With Postfix >= 3.4 (or patch releases >= 3.0.14, 3.1.10, 3.2.7 and 3.3.2) this can be disabled, if need be, via "!TLSv1.3".

Example:

```
# Preferred syntax with Postfix >= 2.5:
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
# Legacy syntax:
smtpd_tls_mandatory_protocols = TLSv1
```

This feature is available in Postfix 2.3 and later.

smtpd_tls_protocols (default: !SSLv2, !SSLv3)

List of TLS protocols that the Postfix SMTP server will exclude or include with opportunistic TLS encryption. The default value is "!SSLv2, !SSLv3" for Postfix releases after the middle of 2015, empty for older releases allowing all protocols to be used with opportunistic TLS. A non-empty value is a list of protocol names separated by whitespace, commas or colons. The supported protocol names are "SSLv2", "SSLv3" and "TLSv1", and are not case sensitive.

Note: As of OpenSSL 1.0.1 two new protocols are defined, "TLSv1.1" and "TLSv1.2". The latest patch levels of Postfix >= 2.6, and all versions of Postfix >= 2.10 can disable support for "TLSv1.1" or "TLSv1.2".

OpenSSL 1.1.1 introduces support for "TLSv1.3". With Postfix >= 3.4 (or patch releases >= 3.0.14, 3.1.10, 3.2.7 and 3.3.2) this can be disabled, if need be, via "!TLSv1.3".

To include a protocol list its name, to exclude it, prefix the name with a "!" character. To exclude SSLv2 for opportunistic TLS set "smtpd_tls_protocols = !SSLv2". To exclude both "SSLv2" and "SSLv3" set "smtpd_tls_protocols = !SSLv2, !SSLv3". Explicitly listing the protocols to include, rather than protocols to exclude, is supported, but not recommended. The exclusion form more closely matches the underlying OpenSSL interface semantics.

Example:

```
smtpd_tls_protocols = !SSLv2, !SSLv3
```

This feature is available in Postfix 2.6 and later.

smtpd_tls_received_header (default: no)

Request that the Postfix SMTP server produces Received: message headers that include information about the protocol and cipher used, as well as the remote SMTP client CommonName and client certificate issuer CommonName. This is disabled by default, as the information may be modified in transit through other mail servers. Only information that was recorded by the final destination can be trusted.

This feature is available in Postfix 2.2 and later.

smtpd_tls_req_ccert (default: no)

With mandatory TLS encryption, require a trusted remote SMTP client certificate in order to allow TLS connections to proceed. This option implies "smtpd_tls_ask_ccert = yes".

When TLS encryption is optional, this setting is ignored with a warning written to the mail log.

This feature is available in Postfix 2.2 and later.

smtpd_tls_security_level (default: empty)

The SMTP TLS security level for the Postfix SMTP server; when a non-empty value is specified, this overrides the obsolete parameters smtpd_use_tls and smtpd_enforce_tls. This parameter is ignored with "smtpd_tls_wrappermode = yes".

Specify one of the following security levels:

none TLS will not be used.

may Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

encrypt
Mandatory TLS encryption: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption. According to RFC 2487 this MUST NOT be applied in case of a publicly-referenced SMTP server. Instead, this option should be used only on dedicated servers.

Note 1: the "fingerprint", "verify" and "secure" levels are not supported here. The Postfix SMTP server logs a warning and uses "encrypt" instead. To verify remote SMTP client certificates, see TLS_README for a discussion of the smtpd_tls_ask_ccert, smtpd_tls_req_ccert, and permit_tls_clientcerts features.

Note 2: The parameter setting "smtpd_tls_security_level = encrypt" implies "smtpd_tls_auth_only = yes".

Note 3: when invoked via "sendmail -bs", Postfix will never offer STARTTLS due to insufficient privileges to access the server private key. This is intended behavior.

This feature is available in Postfix 2.3 and later.

smtpd_tls_session_cache_database (default: empty)
Name of the file containing the optional Postfix SMTP server TLS session cache. Specify a database type that supports enumeration, such as **btree** or **sdbm**; there is no need to support concurrent access. The file is created if it does not exist. The **smtpd(8)** daemon does not use this parameter directly, rather the cache is implemented indirectly in the **tlsmgr(8)** daemon. This means that per-smtpd-instance master.cf overrides of this parameter are not effective. Note, that each of the cache databases supported by **tlsmgr(8)** daemon: $smtpd_tls_session_cache_database, $smtp_tls_session_cache_database (and with Postfix 2.3 and later $lmtp_tls_session_cache_database), needs to be stored separately. It is not at this time possible to store multiple caches in a single database.

Note: **dbm** databases are not suitable. TLS session objects are too large.

As of version 2.5, Postfix no longer uses root privileges when opening this file. The file should now be stored under the Postfix-owned data_directory. As a migration aid, an attempt to open the file under a non-Postfix directory is redirected to the Postfix-owned data_directory, and a warning is logged.

As of Postfix 2.11 the preferred mechanism for session resumption is RFC 5077 TLS session tickets, which don't require server-side storage. Consequently, for Postfix >= 2.11 this parameter should generally be left empty. TLS session tickets require an OpenSSL library (at least version 0.9.8h) that provides full support for this TLS extension. See also smtpd_tls_session_cache_timeout.

Example:

```
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache
```

This feature is available in Postfix 2.2 and later.

smtpd_tls_session_cache_timeout (default: 3600s)
The expiration time of Postfix SMTP server TLS session cache information. A cache cleanup is performed periodically every $smtpd_tls_session_cache_timeout seconds. As with $smtpd_tls_session_cache_database, this parameter is implemented in the **tlsmgr(8)** daemon and therefore per-smtpd-instance master.cf overrides are not possible.

As of Postfix 2.11 this setting cannot exceed 100 days. If set <= 0, session caching is disabled, not just via the database, but also via RFC 5077 TLS session tickets, which don't require server-side storage. If set to a positive value less than 2 minutes, the minimum value of 2 minutes is used instead. TLS session tickets require an OpenSSL library (at least version 0.9.8h) that provides full support for this TLS extension.

This feature is available in Postfix 2.2 and later, and updated for TLS session ticket support in Postfix 2.11.

smtpd_tls_wrappermode (default: no)
Run the Postfix SMTP server in the non-standard "wrapper" mode, instead of using the STARTTLS command.

If you want to support this service, enable a special port in master.cf, and specify "-o smtpd_tls_wrappermode=yes" on the SMTP server's command line. Port 465 (smtps) was once chosen for this purpose.

This feature is available in Postfix 2.2 and later.

smtpd_upstream_proxy_protocol (default: empty)

The name of the proxy protocol used by an optional before-smtpd proxy agent. When a proxy agent is used, this protocol conveys local and remote address and port information. Specify "smtpd_upstream_proxy_protocol = haproxy" to enable the haproxy protocol.

NOTE: To use the nginx proxy with **smtpd(8)**, enable the XCLIENT protocol with smtpd_authorized_xclient_hosts. This supports SASL authentication in the proxy agent (Postfix 2.9 and later).

This feature is available in Postfix 2.10 and later.

smtpd_upstream_proxy_timeout (default: 5s)

The time limit for the proxy protocol specified with the smtpd_upstream_proxy_protocol parameter.

This feature is available in Postfix 2.10 and later.

smtpd_use_tls (default: no)

Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

Note: when invoked via "**sendmail -bs**", Postfix will never offer STARTTLS due to insufficient privileges to access the server private key. This is intended behavior.

This feature is available in Postfix 2.2 and later. With Postfix 2.3 and later use smtpd_tls_security_level instead.

smtputf8_autodetect_classes (default: sendmail, verify)

Detect that a message requires SMTPUTF8 support for the specified mail origin classes. This is a workaround to avoid chicken-and-egg problems during the initial SMTPUTF8 roll-out in environments with pre-existing mail flows that contain UTF8. Those mail flows should not break because Postfix suddenly refuses to deliver such mail to down-stream MTAs that don't announce SMTPUTF8 support.

The problem is that Postfix cannot rely solely on the sender's declaration that a message requires SMTPUTF8 support, because UTF8 may be introduced during local processing (for example, the client hostname in Postfix's Received: header, adding @$myorigin or .$mydomain to an incomplete address, address rewriting, alias expansion, automatic BCC recipients, local forwarding, and changes made by header checks or Milter applications).

For now, the default is to enable "SMTPUTF8 required" autodetection only for Postfix sendmail command-line submissions and address verification probes. This may change once SMTPUTF8 support achieves world domination. However, sites that add UTF8 content via local processing (see above) should autodetect the need for SMTPUTF8 support for all email.

Specify one or more of the following:

sendmail
: Submission with the Postfix **sendmail(1)** command.

smtpd Mail received with the **smtpd(8)** daemon.

qmqpd
: Mail received with the **qmqpd(8)** daemon.

forward
: Local forwarding or aliasing. When a message is received with "SMTPUTF8 required", then the forwarded (aliased) message always has "SMTPUTF8 required".

bounce
: Submission by the **bounce(8)** daemon. When a message is received with "SMTPUTF8 required", then the delivery status notification always has "SMTPUTF8 required".

notify Postmaster notification from the **smtp(8)** or **smtpd(8)** daemon.

verify Address verification probe from the **verify(8)** daemon.

all Enable SMTPUTF8 autodetection for all mail.

This feature is available in Postfix 3.0 and later.

smtputf8_enable (default: yes)
Enable preliminary SMTPUTF8 support for the protocols described in RFC 6531..6533. This requires that Postfix is built to support these protocols.

This feature is available in Postfix 3.0 and later.

soft_bounce (default: no)
Safety net to keep mail queued that would otherwise be returned to the sender. This parameter disables locally-generated bounces, changes the handling of negative responses from remote servers, content filters or plugins, and prevents the Postfix SMTP server from rejecting mail permanently by changing 5xx reply codes into 4xx. However, soft_bounce is no cure for address rewriting mistakes or mail routing mistakes.

Note: "soft_bounce = yes" is in some cases implemented by modifying server responses. Therefore, the response that Postfix logs may differ from the response that Postfix actually sends or receives.

Example:

```
soft_bounce = yes
```

stale_lock_time (default: 500s)
The time after which a stale exclusive mailbox lockfile is removed. This is used for delivery to file or mailbox.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

stress (default: empty)
This feature is documented in the STRESS_README document.

This feature is available in Postfix 2.5 and later.

strict_7bit_headers (default: no)
Reject mail with 8-bit text in message headers. This blocks mail from poorly written applications.

This feature should not be enabled on a general purpose mail server, because it is likely to reject legitimate email.

This feature is available in Postfix 2.0 and later.

strict_8bitmime (default: no)
Enable both strict_7bit_headers and strict_8bitmime_body.

This feature should not be enabled on a general purpose mail server, because it is likely to reject legitimate email.

This feature is available in Postfix 2.0 and later.

strict_8bitmime_body (default: no)
Reject 8-bit message body text without 8-bit MIME content encoding information. This blocks mail from poorly written applications.

Unfortunately, this also rejects majordomo approval requests when the included request contains valid 8-bit MIME mail, and it rejects bounces from mailers that do not MIME encapsulate 8-bit content (for example, bounces from qmail or from old versions of Postfix).

This feature should not be enabled on a general purpose mail server, because it is likely to reject legitimate email.

This feature is available in Postfix 2.0 and later.

strict_mailbox_ownership (default: yes)
Defer delivery when a mailbox file is not owned by its recipient. The default setting is not backwards compatible.

This feature is available in Postfix 2.5.3 and later.

strict_mime_encoding_domain (default: no)
Reject mail with invalid Content-Transfer-Encoding: information for the message/* or multipart/* MIME content types. This blocks mail from poorly written software.

This feature should not be enabled on a general purpose mail server, because it will reject mail after a single violation.

This feature is available in Postfix 2.0 and later.

strict_rfc821_envelopes (default: no)
Require that addresses received in SMTP MAIL FROM and RCPT TO commands are enclosed with <>, and that those addresses do not contain RFC 822 style comments or phrases. This stops mail from poorly written software.

By default, the Postfix SMTP server accepts RFC 822 syntax in MAIL FROM and RCPT TO addresses.

strict_smtputf8 (default: no)
Enable stricter enforcement of the SMTPUTF8 protocol. The Postfix SMTP server accepts UTF8 sender or recipient addresses only when the client requests an SMTPUTF8 mail transaction.

This feature is available in Postfix 3.0 and later.

sun_mailtool_compatibility (default: no)
Obsolete SUN mailtool compatibility feature. Instead, use "mailbox_delivery_lock = dotlock".

swap_bangpath (default: yes)
Enable the rewriting of "site!user" into "user@site". This is necessary if your machine is connected to UUCP networks. It is enabled by default.

Note: with Postfix version 2.2, message header address rewriting happens only when one of the following conditions is true:

- The message is received with the Postfix **sendmail(1)** command,
- The message is received from a network client that matches $local_header_rewrite_clients,
- The message is received from the network, and the remote_header_rewrite_domain parameter specifies a non-empty value.

To get the behavior before Postfix version 2.2, specify "local_header_rewrite_clients = static:all".

Example:

```
swap_bangpath = no
```

syslog_facility (default: mail)
The syslog facility of Postfix logging. Specify a facility as defined in syslog.**conf**(5). The default facility is "mail".

Warning: a non-default syslog_facility setting takes effect only after a Postfix process has completed initialization. Errors during process initialization will be logged with the default facility. Examples are errors while parsing the command line arguments, and errors while accessing the Postfix main.cf configuration file.

syslog_name (default: see postconf −d output)
The mail system name that is prepended to the process name in syslog records, so that "smtpd" becomes, for example, "postfix/smtpd".

Warning: a non-default syslog_name setting takes effect only after a Postfix process has completed initialization. Errors during process initialization will be logged with the default name. Examples are errors while parsing the command line arguments, and errors while accessing the Postfix main.cf configuration file.

tcp_windowsize (default: 0)
An optional workaround for routers that break TCP window scaling. Specify a value > 0 and < 65536 to enable this feature. With Postfix TCP servers (**smtpd**(8), **qmqpd(8)**), this feature is implemented by the Postfix **master(8)** daemon.

To change this parameter without stopping Postfix, you need to first terminate all Postfix TCP servers:

```
# postconf -e master_service_disable=inet
# postfix reload
```

This immediately terminates all processes that accept network connections. Next, you enable Postfix TCP servers with the updated tcp_windowsize setting:

```
# postconf -e tcp_windowsize=65535 master_service_disable=
# postfix reload
```

If you skip these steps with a running Postfix system, then the tcp_windowsize change will work only for Postfix TCP clients (**smtp**(8), **lmtp(8)**).

This feature is available in Postfix 2.6 and later.

tls_append_default_CA (default: no)

Append the system-supplied default Certification Authority certificates to the ones specified with *_tls_CApath or *_tls_CAfile. The default is "no"; this prevents Postfix from trusting third-party certificates and giving them relay permission with permit_tls_all_clientcerts.

This feature is available in Postfix 2.4.15, 2.5.11, 2.6.8, 2.7.2 and later versions. Specify "tls_append_default_CA = yes" for backwards compatibility, to avoid breaking certificate verification with sites that don't use permit_tls_all_clientcerts.

tls_daemon_random_bytes (default: 32)

The number of pseudo-random bytes that an **smtp(8)** or **smtpd(8)** process requests from the **tlsmgr(8)** server in order to seed its internal pseudo random number generator (PRNG). The default of 32 bytes (equivalent to 256 bits) is sufficient to generate a 128bit (or 168bit) session key.

This feature is available in Postfix 2.2 and later.

tls_dane_digest_agility (default: on)

Configure DANE TLSA digest algorithm agility. When digest algorithm agility is enabled, and the server and client support a common strong digest algorithm, TLSA records with weaker digest algorithms are ignored.

Specify one of the following:

off DANE verification examines each well-formed record in the TLSA RRset whose matching type is either "0" (no hash used) or is one of the digest algorithms listed in $tls_dane_digests. This setting is not recommended.

on From each group of well-formed TLSA RRs a non-zero digest matching type with the same certificate usage and selector, DANE verification examines only those records whose matching type has the highest precedence (appear earliest in $tls_dane_digests).

maybe For compatibility with digest algorithm agility, each certificate or public key whose digest is included in a DANE TLSA RRset, SHOULD be published with the same set of digest matching type values as any other with the same usage and selector. Therefore, compatible TLSA RRsets will contain an identical count of well-formed RRs with each non-zero digest matching type for any fixed combination of usage and selector. When this constraint is violated, or any of the digest records are malformed, digest algorithm agility will disabled. Otherwise, digest algorithm agility is enabled.

Digest algorithm agility ensures that the strongest digest supported by both the Postfix SMTP client and the remote server is used, and weaker digests are ignored. This supports non-disruptive deprecation of outdated digest algorithms.

To ensure compatibility with digest algorithm agility during key rotation, when a certificate or public key is being replaced with another, and both are published during the transition, both the old and the new certificate MUST be specified with the same set of digests. One can change the list of digest algorithms later, once old keys are retired. At any given time, change either the list of digests without changing the list of certificates or public keys or the list of certificates or public keys without changing the list of digests. Full

value matching type "0" records are not subject to this constraint, but are discouraged due to the size of the resulting DNS records.

It is expected that this algorithm agility mechanism will be published in a standards track RFC for SMTP with DANE, and also in an eventual update to RFC 6698.

This feature is available in Postfix 2.11 and later.

tls_dane_digests (default: sha512 sha256)

RFC 6698 TLSA resource-record "matching type" digest algorithms in descending preference order. All the specified algorithms must be supported by the underlying OpenSSL library, otherwise the Postfix SMTP client will not support DANE TLSA security.

Specify a list of digest names separated by commas and/or whitespace. Each digest name may be followed by an optional "=<number>" suffix. For example, "sha512" may instead be specified as "sha512=2" and "sha256" may instead be specified as "sha256=1". The optional number must match the <a href="" -- https://www.iana.org/assignments/dane-parameters/dane-parameters.xhtml#matching-types -P >IANA assigned TLSA matching type number the algorithm in question. Postfix will check this constraint for the algorithms it knows about. Additional matching type algorithms registered with IANA can be added with explicit numbers provided they are supported by OpenSSL.

Invalid list elements are logged with a warning and disable DANE support. TLSA RRs that specify digests not included in the list are ignored with a warning.

Note: It is unwise to omit sha256 from the digest list. This digest algorithm is the only mandatory to implement digest algorithm in RFC 6698, and many servers are expected publish TLSA records with just sha256 digests. Unless one of the standard digests is seriously compromised and servers have had ample time to update their TLSA records you should not omit any standard digests, just arrange them in order from strongest to weakest.

When for a particular combination of "certificate usage" and "selector" the TLSA RRset contains records with more than one digest matching type, the tls_dane_digest_agility parameter determines whether all the RRs are used, or only those with the most preferred digest matching type.

The tls_dane_trust_anchor_digest_enable parameter controls whether any digest TLSA records are acceptable in usage "2" (trust anchor assertion) TLSA records.

This feature is available in Postfix 2.11 and later.

tls_dane_trust_anchor_digest_enable (default: yes)

RFC 6698 trust-anchor digest support in the Postfix TLS library. Enable support for RFC 6698 (DANE TLSA) DNS records that contain digests of trust-anchors with certificate usage "2". In this case the certificate usage logically requires the server administrator to configure the server to include the trust-anchor certificate in the server's SSL certificate chain. If enough domains mess this up, you can disable support for these TLSA records, but you'll no longer have secure connections that get it right and only publish trust anchor records.

At the dane security level, when a TLSA RRset includes only unusable associations, the Postfix SMTP client will automatically switch the connection to the encrypt security level. At the dane-only security level, the server in question is skipped and delivery is deferred if no secure servers are found.

The tls_dane_digests parameter controls the list of digest algorithms that are supported in TLSA records. The tls_dane_digest_agility parameter controls digest algorithm downgrade attack resistance.

This feature is available in Postfix 2.11 and later.

tls_disable_workarounds (default: see postconf −d output)

List or bit-mask of OpenSSL bug work-arounds to disable.

The OpenSSL toolkit includes a set of work-arounds for buggy SSL/TLS implementations. Applications, such as Postfix, that want to maximize interoperability ask the OpenSSL library to enable the full set of recommended work-arounds.

From time to time, it is discovered that a work-around creates a security issue, and should no longer be

used. If upgrading OpenSSL to a fixed version is not an option or an upgrade is not available in a timely manner, or in closed environments where no buggy clients or servers exist, it may be appropriate to disable some or all of the OpenSSL interoperability work-arounds. This parameter specifies which bug work-arounds to disable.

If the value of the parameter is a hexadecimal long integer starting with "0x", the bug work-arounds corresponding to the bits specified in its value are removed from the **SSL_OP_ALL** work-around bit-mask (see openssl/ssl.h and SSL_CTX_**set_options**(3)). You can specify more bits than are present in SSL_OP_ALL, excess bits are ignored. Specifying 0xFFFFFFFF disables all bug-workarounds on a 32-bit system. This should also be sufficient on 64-bit systems, until OpenSSL abandons support for 32-bit systems and starts using the high 32 bits of a 64-bit bug-workaround mask.

Otherwise, the parameter is a white-space or comma separated list of specific named bug work-arounds chosen from the list below. It is possible that your OpenSSL version includes new bug work-arounds added after your Postfix source code was last updated, in that case you can only disable one of these via the hexadecimal syntax above.

CRYPTOPRO_TLSEXT_BUG
New with GOST support in OpenSSL 1.0.0.

DONT_INSERT_EMPTY_FRAGMENTS
See SSL_CTX_**set_options**(3)

LEGACY_SERVER_CONNECT
See SSL_CTX_**set_options**(3)

MICROSOFT_BIG_SSLV3_BUFFER
See SSL_CTX_**set_options**(3)

MICROSOFT_SESS_ID_BUG
See SSL_CTX_**set_options**(3)

MSIE_SSLV2_RSA_PADDING
also aliased as **CVE-2005-2969**. Postfix 2.8 disables this work-around by default with OpenSSL versions that may predate the fix. Fixed in OpenSSL 0.9.7h and OpenSSL 0.9.8a.

NETSCAPE_CHALLENGE_BUG
See SSL_CTX_**set_options**(3)

NETSCAPE_REUSE_CIPHER_CHANGE_BUG
also aliased as **CVE-2010-4180**. Postfix 2.8 disables this work-around by default with OpenSSL versions that may predate the fix. Fixed in OpenSSL 0.9.8q and OpenSSL 1.0.0c.

SSLEAY_080_CLIENT_DH_BUG
See SSL_CTX_**set_options**(3)

SSLREF2_REUSE_CERT_TYPE_BUG
See SSL_CTX_**set_options**(3)

TLS_BLOCK_PADDING_BUG
See SSL_CTX_**set_options**(3)

TLS_D5_BUG
See SSL_CTX_**set_options**(3)

TLS_ROLLBACK_BUG
See SSL_CTX_**set_options**(3). This is disabled in OpenSSL 0.9.7 and later. Nobody should still be using 0.9.6!

TLSEXT_PADDING
Postfix >= 3.4. See SSL_CTX_**set_options**(3).

This feature is available in Postfix 2.8 and later.

tls_eecdh_strong_curve (default: prime256v1)

The elliptic curve used by the Postfix SMTP server for sensibly strong ephemeral ECDH key exchange. This curve is used by the Postfix SMTP server when "smtpd_tls_eecdh_grade = strong". The phrase "sensibly strong" means approximately 128-bit security based on best known attacks. The selected curve must be implemented by OpenSSL (as reported by **ecparam(1)** with the "-list_curves" option) and be one of the curves listed in Section 5.1.1 of RFC 4492. You should not generally change this setting. Remote SMTP client implementations must support this curve for EECDH key exchange to take place. It is unwise to choose an "exotic" curve supported by only a small subset of clients.

The default "strong" curve is rated in NSA Suite B for information classified up to SECRET.

Note: elliptic curve names are poorly standardized; different standards groups are assigning different names to the same underlying curves. The curve with the X9.62 name "prime256v1" is also known under the SECG name "secp256r1", but OpenSSL does not recognize the latter name.

If you want to take maximal advantage of ciphers that offer forward secrecy see the Getting started section of FORWARD_SECRECY_README. The full document conveniently presents all information about Postfix "perfect" forward secrecy support in one place: what forward secrecy is, how to tweak settings, and what you can expect to see when Postfix uses ciphers with forward secrecy.

This feature is available in Postfix 2.6 and later, when it is compiled and linked with OpenSSL 1.0.0 or later on platforms where EC algorithms have not been disabled by the vendor.

tls_eecdh_ultra_curve (default: secp384r1)

The elliptic curve used by the Postfix SMTP server for maximally strong ephemeral ECDH key exchange. This curve is used by the Postfix SMTP server when "smtpd_tls_eecdh_grade = ultra". The phrase "maximally strong" means approximately 192-bit security based on best known attacks. This additional strength comes at a significant computational cost, most users should instead set "smtpd_tls_eecdh_grade = strong". The selected curve must be implemented by OpenSSL (as reported by **ecparam(1)** with the "-list_curves" option) and be one of the curves listed in Section 5.1.1 of RFC 4492. You should not generally change this setting.

This default "ultra" curve is rated in NSA Suite B for information classified up to TOP SECRET.

If you want to take maximal advantage of ciphers that offer forward secrecy see the Getting started section of FORWARD_SECRECY_README. The full document conveniently presents all information about Postfix "perfect" forward secrecy support in one place: what forward secrecy is, how to tweak settings, and what you can expect to see when Postfix uses ciphers with forward secrecy.

This feature is available in Postfix 2.6 and later, when it is compiled and linked with OpenSSL 1.0.0 or later on platforms where EC algorithms have not been disabled by the vendor.

tls_export_cipherlist (default: see postconf −d output)

The OpenSSL cipherlist for "export" or higher grade ciphers. This defines the meaning of the "export" setting in smtpd_tls_ciphers, smtpd_tls_mandatory_ciphers, smtp_tls_ciphers, smtp_tls_mandatory_ciphers, lmtp_tls_ciphers, and lmtp_tls_mandatory_ciphers. With Postfix releases before the middle of 2015 this is the default cipherlist for the opportunistic ("may") TLS client security level and also the default cipherlist for the SMTP server. You are strongly encouraged to not change this setting.

This feature is available in Postfix 2.3 and later.

tls_high_cipherlist (default: see postconf −d output)

The OpenSSL cipherlist for "high" grade ciphers. This defines the meaning of the "high" setting in smtpd_tls_ciphers, smtpd_tls_mandatory_ciphers, smtp_tls_ciphers, smtp_tls_mandatory_ciphers, lmtp_tls_ciphers, and lmtp_tls_mandatory_ciphers. You are strongly encouraged to not change this setting.

This feature is available in Postfix 2.3 and later.

tls_legacy_public_key_fingerprints (default: no)

A temporary migration aid for sites that use certificate *public-key* fingerprints with Postfix 2.9.0..2.9.5, which use an incorrect algorithm. This parameter has no effect on the certificate fingerprint support that is available since Postfix 2.2.

Specify "tls_legacy_public_key_fingerprints = yes" temporarily, pending a migration from configuration files with incorrect Postfix 2.9.0..2.9.5 certificate public-key finger prints, to the correct fingerprints used by Postfix 2.9.6 and later. To compute the correct certificate public-key fingerprints, see TLS_README.

This feature is available in Postfix 2.9.6 and later.

tls_low_cipherlist (default: see postconf −d output)

The OpenSSL cipherlist for "low" or higher grade ciphers. This defines the meaning of the "low" setting in smtpd_tls_ciphers, smtpd_tls_mandatory_ciphers, smtp_tls_ciphers, smtp_tls_mandatory_ciphers, lmtp_tls_ciphers, and lmtp_tls_mandatory_ciphers. You are strongly encouraged to not change this setting.

This feature is available in Postfix 2.3 and later.

tls_medium_cipherlist (default: see postconf −d output)

The OpenSSL cipherlist for "medium" or higher grade ciphers. This defines the meaning of the "medium" setting in smtpd_tls_ciphers, smtpd_tls_mandatory_ciphers, smtp_tls_ciphers, smtp_tls_mandatory_ciphers, lmtp_tls_ciphers, and lmtp_tls_mandatory_ciphers. This is the default cipherlist for mandatory TLS encryption in the TLS client (with anonymous ciphers disabled when verifying server certificates). This is the default cipherlist for opportunistic TLS with Postfix releases after the middle of 2015. You are strongly encouraged to not change this setting.

This feature is available in Postfix 2.3 and later.

tls_null_cipherlist (default: eNULL:!aNULL)

The OpenSSL cipherlist for "NULL" grade ciphers that provide authentication without encryption. This defines the meaning of the "null" setting in smtpd_mandatory_tls_ciphers, smtp_tls_mandatory_ciphers and lmtp_tls_mandatory_ciphers. You are strongly encouraged to not change this setting.

This feature is available in Postfix 2.3 and later.

tls_preempt_cipherlist (default: no)

With SSLv3 and later, use the Postfix SMTP server's cipher preference order instead of the remote client's cipher preference order.

By default, the OpenSSL server selects the client's most preferred cipher that the server supports. With SSLv3 and later, the server may choose its own most preferred cipher that is supported (offered) by the client. Setting "tls_preempt_cipherlist = yes" enables server cipher preferences.

While server cipher selection may in some cases lead to a more secure or performant cipher choice, there is some risk of interoperability issues. In the past, some SSL clients have listed lower priority ciphers that they did not implement correctly. If the server chooses a cipher that the client prefers less, it may select a cipher whose client implementation is flawed. Most notably Windows 2003 Microsoft Exchange servers have flawed implementations of DES-CBC3-SHA, which OpenSSL considers stronger than RC4-SHA. Enabling server cipher-suite selection may create interoperability issues with Windows 2003 Microsoft Exchange clients.

This feature is available in Postfix 2.8 and later, in combination with OpenSSL 0.9.7 and later.

tls_random_bytes (default: 32)

The number of bytes that **tlsmgr(8)** reads from $tls_random_source when (re)seeding the in-memory pseudo random number generator (PRNG) pool. The default of 32 bytes (256 bits) is good enough for 128bit symmetric keys. If using EGD or a device file, a maximum of 255 bytes is read.

This feature is available in Postfix 2.2 and later.

tls_random_exchange_name (default: see postconf −d output)

Name of the pseudo random number generator (PRNG) state file that is maintained by **tlsmgr(8)**. The file is created when it does not exist, and its length is fixed at 1024 bytes.

As of version 2.5, Postfix no longer uses root privileges when opening this file, and the default file location was changed from ${config_directory}/prng_exch to ${data_directory}/prng_exch. As a migration aid, an attempt to open the file under a non-Postfix directory is redirected to the Postfix-owned data_directory, and a warning is logged.

This feature is available in Postfix 2.2 and later.

tls_random_prng_update_period (default: 3600s)
The time between attempts by **tlsmgr(8)** to save the state of the pseudo random number generator (PRNG) to the file specified with $tls_random_exchange_name.

This feature is available in Postfix 2.2 and later.

tls_random_reseed_period (default: 3600s)
The maximal time between attempts by **tlsmgr(8)** to re-seed the in-memory pseudo random number generator (PRNG) pool from external sources. The actual time between re-seeding attempts is calculated using the PRNG, and is between 0 and the time specified.

This feature is available in Postfix 2.2 and later.

tls_random_source (default: see postconf −d output)
The external entropy source for the in-memory **tlsmgr(8)** pseudo random number generator (PRNG) pool. Be sure to specify a non-blocking source. If this source is not a regular file, the entropy source type must be prepended: egd:/path/to/egd_socket for a source with EGD compatible socket interface, or dev:/path/to/device for a device file.

Note: on OpenBSD systems specify /dev/arandom when /dev/urandom gives timeout errors.

This feature is available in Postfix 2.2 and later.

tls_session_ticket_cipher (default: Postfix >= 3.0: aes−256−cbc, Postfix < 3.0: aes−128−cbc)
Algorithm used to encrypt RFC5077 TLS session tickets. This algorithm must use CBC mode, have a 128-bit block size, and must have a key length between 128 and 256 bits. The default is aes-256-cbc. Overriding the default to choose a different algorithm is discouraged.

Setting this parameter empty disables session ticket support in the Postfix SMTP server. Another way to disable session ticket support is via the tls_ssl_options parameter.

This feature is available in Postfix 3.0 and later.

tls_ssl_options (default: empty)
List or bit-mask of OpenSSL options to enable.

The OpenSSL toolkit provides a set of options that applications can enable to tune the OpenSSL behavior. Some of these work around bugs in other implementations and are on by default. You can use the tls_disable_workarounds parameter to selectively disable some or all of the bug work-arounds, making OpenSSL more strict at the cost of non-interoperability with SSL clients or servers that exhibit the bugs.

Other options are off by default, and typically enable or disable features rather than bug work-arounds. These may be turned on (with care) via the tls_ssl_options parameter. The value is a white-space or comma separated list of named options chosen from the list below. The names are not case-sensitive, you can use lower-case if you prefer. The upper case values below match the corresponding macro name in the ssl.h header file with the SSL_OP_ prefix removed. It is possible that your OpenSSL version includes new options added after your Postfix source code was last updated, in that case you can only enable one of these via the hexadecimal syntax below.

You should only enable features via the hexadecimal mask when the need to control the feature is critical (to deal with a new vulnerability or a serious interoperability problem). Postfix DOES NOT promise backwards compatible behavior with respect to the mask bits. A feature enabled via the mask in one release may be enabled by other means in a later release, and the mask bit will then be ignored. Therefore, use of the hexadecimal mask is only a temporary measure until a new Postfix or OpenSSL release provides a better solution.

If the value of the parameter is a hexadecimal long integer starting with "0x", the options corresponding to the bits specified in its value are enabled (see openssl/ssl.h and SSL_CTX_**set_options**(3)). You can only enable options not already controlled by other Postfix settings. For example, you cannot disable protocols or enable server cipher preference. Do not attempt to turn all features by specifying 0xFFFFFFFF, this is unlikely to be a good idea. Some bug work-arounds are also valid here, allowing them to be re-enabled

if/when they’re no longer enabled by default. The supported values include:

ENABLE_MIDDLEBOX_COMPAT
Postfix >= 3.4. See SSL_CTX_**set_options**(3).

LEGACY_SERVER_CONNECT
See SSL_CTX_**set_options**(3).

NO_TICKET
Enabled by default when needed in fully-patched Postfix >= 2.7. Not needed at all for Postfix >= 2.11, unless for some reason you do not want to support TLS session resumption. Best not set explicitly. See SSL_CTX_**set_options**(3).

NO_COMPRESSION
Disable SSL compression even if supported by the OpenSSL library. Compression is CPU-intensive, and compression before encryption does not always improve security.

NO_RENEGOTIATION
Postfix >= 3.4. This can reduce opportunities for a potential CPU exhaustion attack. See SSL_CTX_**set_options**(3).

NO_SESSION_RESUMPTION_ON_RENEGOTIATION
Postfix >= 3.4. See SSL_CTX_**set_options**(3).

PRIORITIZE_CHACHA
Postfix >= 3.4. See SSL_CTX_**set_options**(3).

TLSEXT_PADDING
Postfix >= 3.4. See SSL_CTX_**set_options**(3).

This feature is available in Postfix 2.11 and later.

tls_wildcard_matches_multiple_labels (default: yes)
Match multiple DNS labels with "*" in wildcard certificates.

Some mail service providers prepend the customer domain name to a base domain for which they have a wildcard TLS certificate. For example, the MX records for example.com hosted by example.net may be:

```
example.com. IN MX 0 example.com.mx1.example.net.
example.com. IN MX 0 example.com.mx2.example.net.
```

and the TLS certificate may be for "*.example.net". The "*" then corresponds with multiple labels in the mail server domain name. While multi-label wildcards are not widely supported, and are not blessed by any standard, there is little to be gained by disallowing their use in this context.

Notes:

- In a certificate name, the "*" is special only when it is used as the first label.
- While Postfix (2.11 or later) can match "*" with multiple domain name labels, other implementations likely will not.
- Earlier Postfix implementations behave as if "tls_wildcard_matches_multiple_labels = no".

This feature is available in Postfix 2.11 and later.

tlsmgr_service_name (default: tlsmgr)
The name of the **tlsmgr(8)** service entry in master.cf. This service maintains TLS session caches and other information in support of TLS.

This feature is available in Postfix 2.11 and later.

tlsproxy_enforce_tls (default: $smtpd_enforce_tls)
Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption. See smtpd_enforce_tls for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_service_name (default: tlsproxy)
The name of the **tlsproxy(8)** service entry in master.cf. This service performs plaintext <=> TLS ciphertext conversion.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_CAfile (default: $smtpd_tls_CAfile)
A file containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates. See smtpd_tls_CAfile for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_CApath (default: $smtpd_tls_CApath)
A directory containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates. See smtpd_tls_CApath for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_always_issue_session_ids (default: $smtpd_tls_always_issue_session_ids)
Force the Postfix **tlsproxy(8)** server to issue a TLS session id, even when TLS session caching is turned off. See smtpd_tls_always_issue_session_ids for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_ask_ccert (default: $smtpd_tls_ask_ccert)
Ask a remote SMTP client for a client certificate. See smtpd_tls_ask_ccert for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_ccert_verifydepth (default: $smtpd_tls_ccert_verifydepth)
The verification depth for remote SMTP client certificates. A depth of 1 is sufficient if the issuing CA is listed in a local CA file. See smtpd_tls_ccert_verifydepth for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_cert_file (default: $smtpd_tls_cert_file)
File with the Postfix **tlsproxy(8)** server RSA certificate in PEM format. This file may also contain the Postfix **tlsproxy(8)** server private RSA key. See smtpd_tls_cert_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_ciphers (default: $smtpd_tls_ciphers)
The minimum TLS cipher grade that the Postfix **tlsproxy(8)** server will use with opportunistic TLS encryption. See smtpd_tls_ciphers for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_dcert_file (default: $smtpd_tls_dcert_file)
File with the Postfix **tlsproxy(8)** server DSA certificate in PEM format. This file may also contain the Postfix **tlsproxy(8)** server private DSA key. See smtpd_tls_dcert_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_dh1024_param_file (default: $smtpd_tls_dh1024_param_file)
File with DH parameters that the Postfix **tlsproxy(8)** server should use with non-export EDH ciphers. See smtpd_tls_dh1024_param_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_dh512_param_file (default: $smtpd_tls_dh512_param_file)
File with DH parameters that the Postfix **tlsproxy(8)** server should use with export-grade EDH ciphers. See smtpd_tls_dh512_param_file for further details. The default SMTP server cipher grade is "medium" with Postfix releases after the middle of 2015, and as a result export-grade cipher suites are by default not used.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_dkey_file (default: $smtpd_tls_dkey_file)
File with the Postfix **tlsproxy(8)** server DSA private key in PEM format. This file may be combined with the Postfix **tlsproxy(8)** server DSA certificate file specified with $smtpd_tls_dcert_file. See smtpd_tls_dkey_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_eccert_file (default: $smtpd_tls_eccert_file)
File with the Postfix **tlsproxy(8)** server ECDSA certificate in PEM format. This file may also contain the Postfix **tlsproxy(8)** server private ECDSA key. See smtpd_tls_eccert_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_eckey_file (default: $smtpd_tls_eckey_file)
File with the Postfix **tlsproxy(8)** server ECDSA private key in PEM format. This file may be combined with the Postfix **tlsproxy(8)** server ECDSA certificate file specified with $smtpd_tls_eccert_file. See smtpd_tls_eckey_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_eecdh_grade (default: $smtpd_tls_eecdh_grade)
The Postfix **tlsproxy(8)** server security grade for ephemeral elliptic-curve Diffie-Hellman (EECDH) key exchange. See smtpd_tls_eecdh_grade for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_exclude_ciphers (default: $smtpd_tls_exclude_ciphers)
List of ciphers or cipher types to exclude from the **tlsproxy(8)** server cipher list at all TLS security levels. See smtpd_tls_exclude_ciphers for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_fingerprint_digest (default: $smtpd_tls_fingerprint_digest)
The message digest algorithm to construct remote SMTP client-certificate fingerprints. See smtpd_tls_fingerprint_digest for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_key_file (default: $smtpd_tls_key_file)
File with the Postfix **tlsproxy(8)** server RSA private key in PEM format. This file may be combined with the Postfix **tlsproxy(8)** server RSA certificate file specified with $smtpd_tls_cert_file. See smtpd_tls_key_file for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_loglevel (default: $smtpd_tls_loglevel)
Enable additional Postfix **tlsproxy(8)** server logging of TLS activity. Each logging level also includes the information that is logged at a lower logging level. See smtpd_tls_loglevel for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_mandatory_ciphers (default: $smtpd_tls_mandatory_ciphers)
The minimum TLS cipher grade that the Postfix **tlsproxy(8)** server will use with mandatory TLS encryption. See smtpd_tls_mandatory_ciphers for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_mandatory_exclude_ciphers (default: $smtpd_tls_mandatory_exclude_ciphers)
Additional list of ciphers or cipher types to exclude from the **tlsproxy(8)** server cipher list at mandatory TLS security levels. See smtpd_tls_mandatory_exclude_ciphers for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_mandatory_protocols (default: $smtpd_tls_mandatory_protocols)
The SSL/TLS protocols accepted by the Postfix **tlsproxy(8)** server with mandatory TLS encryption. If the list is empty, the server supports all available SSL/TLS protocol versions. See

smtpd_tls_mandatory_protocols for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_protocols (default: $smtpd_tls_protocols)
List of TLS protocols that the Postfix **tlsproxy(8)** server will exclude or include with opportunistic TLS encryption. See smtpd_tls_protocols for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_req_ccert (default: $smtpd_tls_req_ccert)
With mandatory TLS encryption, require a trusted remote SMTP client certificate in order to allow TLS connections to proceed. See smtpd_tls_req_ccert for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_security_level (default: $smtpd_tls_security_level)
The SMTP TLS security level for the Postfix **tlsproxy(8)** server; when a non-empty value is specified, this overrides the obsolete parameters smtpd_use_tls and smtpd_enforce_tls. See smtpd_tls_security_level for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_tls_session_cache_timeout (default: $smtpd_tls_session_cache_timeout)
Obsolete expiration time of Postfix **tlsproxy(8)** server TLS session cache information. Since the cache is shared with **smtpd(8)** and managed by **tlsmgr(8)**, there is only one expiration time for the SMTP server cache shared by all three services, namely smtpd_tls_session_cache_timeout.

This feature is available in Postfix 2.8 and later.

tlsproxy_use_tls (default: $smtpd_use_tls)
Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption. See smtpd_use_tls for further details.

This feature is available in Postfix 2.8 and later.

tlsproxy_watchdog_timeout (default: 10s)
How much time a **tlsproxy(8)** process may take to process local or remote I/O before it is terminated by a built-in watchdog timer. This is a safety mechanism that prevents **tlsproxy(8)** from becoming non-responsive due to a bug in Postfix itself or in system software. To avoid false alarms and unnecessary cache corruption this limit cannot be set under 10s.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

This feature is available in Postfix 2.8.

trace_service_name (default: trace)
The name of the trace service. This service is implemented by the **bounce(8)** daemon and maintains a record of mail deliveries and produces a mail delivery report when verbose delivery is requested with "**sendmail -v**".

This feature is available in Postfix 2.1 and later.

transport_delivery_slot_cost (default: $default_delivery_slot_cost)
A transport-specific override for the default_delivery_slot_cost parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_delivery_slot_cost parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_delivery_slot_cost").

transport_delivery_slot_discount (default: $default_delivery_slot_discount)
A transport-specific override for the default_delivery_slot_discount parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_delivery_slot_discount parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_delivery_slot_discount").

transport_delivery_slot_loan (default: $default_delivery_slot_loan)
A transport-specific override for the default_delivery_slot_loan parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_delivery_slot_loan parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_delivery_slot_loan").

transport_destination_concurrency_failed_cohort_limit (default: $default_destination_concurrency_failed_cohort_limit)
A transport-specific override for the default_destination_concurrency_failed_cohort_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_concurrency_failed_cohort_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_concurrency_failed_cohort_limit").

This feature is available in Postfix 2.5 and later.

transport_destination_concurrency_limit (default: $default_destination_concurrency_limit)
A transport-specific override for the default_destination_concurrency_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_concurrency_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_concurrency_limit").

transport_destination_concurrency_negative_feedback (default: $default_destination_concurrency_negative_feedback)
A transport-specific override for the default_destination_concurrency_negative_feedback parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_concurrency_negative_feedback parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_concurrency_negative_feedback").

This feature is available in Postfix 2.5 and later.

transport_destination_concurrency_positive_feedback (default: $default_destination_concurrency_positive_feedback)
A transport-specific override for the default_destination_concurrency_positive_feedback parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_concurrency_positive_feedback parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_concurrency_positive_feedback").

This feature is available in Postfix 2.5 and later.

transport_destination_rate_delay (default: $default_destination_rate_delay)
A transport-specific override for the default_destination_rate_delay parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_rate_delay parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_rate_delay").

This feature is available in Postfix 2.5 and later.

transport_destination_recipient_limit (default: $default_destination_recipient_limit)
A transport-specific override for the default_destination_recipient_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_destination_recipient_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_destination_recipient_limit").

transport_extra_recipient_limit (default: $default_extra_recipient_limit)
A transport-specific override for the default_extra_recipient_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_extra_recipient_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_extra_recipient_limit").

transport_initial_destination_concurrency (default: $initial_destination_concurrency)
A transport-specific override for the initial_destination_concurrency parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_initial_destination_concurrency parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_initial_destination_concurrency").

This feature is available in Postfix 2.5 and later.

transport_maps (default: empty)
Optional lookup tables with mappings from recipient address to (message delivery transport, next-hop destination). See **transport(5)** for details.

Specify zero or more "type:table" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found. If you use this feature with local files, run "**postmap /etc/postfix/transport**" after making a change.

Pattern matching of domain names is controlled by the presence or absence of "transport_maps" in the parent_domain_matches_subdomains parameter value.

For safety reasons, as of Postfix 2.3 this feature does not allow $number substitutions in regular expression maps.

Examples:

```
transport_maps = dbm:/etc/postfix/transport
transport_maps = hash:/etc/postfix/transport
```

transport_minimum_delivery_slots (default: $default_minimum_delivery_slots)
A transport-specific override for the default_minimum_delivery_slots parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_minimum_delivery_slots parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_minimum_delivery_slots").

transport_recipient_limit (default: $default_recipient_limit)
A transport-specific override for the default_recipient_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: some *transport*_recipient_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_recipient_limit").

transport_recipient_refill_delay (default: $default_recipient_refill_delay)
A transport-specific override for the default_recipient_refill_delay parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_recipient_refill_delay parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_recipient_refill_delay").

This feature is available in Postfix 2.4 and later.

transport_recipient_refill_limit (default: $default_recipient_refill_limit)
A transport-specific override for the default_recipient_refill_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_recipient_refill_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_recipient_refill_limit").

This feature is available in Postfix 2.4 and later.

transport_retry_time (default: 60s)
The time between attempts by the Postfix queue manager to contact a malfunctioning message delivery transport.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

transport_time_limit (default: $command_time_limit)
A transport-specific override for the command_time_limit parameter value, where *transport* is the master.cf name of the message delivery transport.

Note: *transport*_time_limit parameters will not show up in "postconf" command output before Postfix version 2.9. This limitation applies to many parameters whose name is a combination of a master.cf service name and a built-in suffix (in this case: "_time_limit").

transport_transport_rate_delay (default: $default_transport_rate_delay)
A transport-specific override for the default_transport_rate_delay parameter value, where the initial *transport* in the parameter name is the master.cf name of the message delivery transport.

trigger_timeout (default: 10s)
The time limit for sending a trigger to a Postfix daemon (for example, the **pickup(8)** or **qmgr(8)** daemon). This time limit prevents programs from getting stuck when the mail system is under heavy load.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks). The default time unit is s (seconds).

undisclosed_recipients_header (default: see postconf −d output)
Message header that the Postfix **cleanup(8)** server inserts when a message contains no To: or Cc: message header. With Postfix 2.8 and later, the default value is empty. With Postfix 2.4-2.7, specify an empty value to disable this feature.

Example:

```
# Default value before Postfix 2.8.
# Note: the ":" and ";" are both required.
undisclosed_recipients_header = To: undisclosed-recipients:;
```

unknown_address_reject_code (default: 450)
The numerical response code when the Postfix SMTP server rejects a sender or recipient address because its domain is unknown. This is one of the possible replies from the restrictions reject_unknown_sender_domain and reject_unknown_recipient_domain.

Do not change this unless you have a complete understanding of RFC 5321.

unknown_address_tempfail_action (default: $reject_tempfail_action)
The Postfix SMTP server's action when reject_unknown_sender_domain or reject_unknown_recipient_domain fail due to a temporary error condition. Specify "defer" to defer the remote SMTP client

request immediately. With the default "defer_if_permit" action, the Postfix SMTP server continues to look for opportunities to reject mail, and defers the client request only if it would otherwise be accepted.

This feature is available in Postfix 2.6 and later.

unknown_client_reject_code (default: 450)
The numerical Postfix SMTP server response code when a client without valid address <=> name mapping is rejected by the reject_unknown_client_hostname restriction. The SMTP server always replies with 450 when the mapping failed due to a temporary error condition.

Do not change this unless you have a complete understanding of RFC 5321.

unknown_helo_hostname_tempfail_action (default: $reject_tempfail_action)
The Postfix SMTP server's action when reject_unknown_helo_hostname fails due to an temporary error condition. Specify "defer" to defer the remote SMTP client request immediately. With the default "defer_if_permit" action, the Postfix SMTP server continues to look for opportunities to reject mail, and defers the client request only if it would otherwise be accepted.

This feature is available in Postfix 2.6 and later.

unknown_hostname_reject_code (default: 450)
The numerical Postfix SMTP server response code when the hostname specified with the HELO or EHLO command is rejected by the reject_unknown_helo_hostname restriction.

Do not change this unless you have a complete understanding of RFC 5321.

unknown_local_recipient_reject_code (default: 550)
The numerical Postfix SMTP server response code when a recipient address is local, and $local_recipient_maps specifies a list of lookup tables that does not match the recipient. A recipient address is local when its domain matches $mydestination, $proxy_interfaces or $inet_interfaces.

The default setting is 550 (reject mail) but it is safer to initially use 450 (try again later) so you have time to find out if your local_recipient_maps settings are OK.

Example:

```
unknown_local_recipient_reject_code = 450
```

This feature is available in Postfix 2.0 and later.

unknown_relay_recipient_reject_code (default: 550)
The numerical Postfix SMTP server reply code when a recipient address matches $relay_domains, and relay_recipient_maps specifies a list of lookup tables that does not match the recipient address.

This feature is available in Postfix 2.0 and later.

unknown_virtual_alias_reject_code (default: 550)
The Postfix SMTP server reply code when a recipient address matches $virtual_alias_domains, and $virtual_alias_maps specifies a list of lookup tables that does not match the recipient address.

This feature is available in Postfix 2.0 and later.

unknown_virtual_mailbox_reject_code (default: 550)
The Postfix SMTP server reply code when a recipient address matches $virtual_mailbox_domains, and $virtual_mailbox_maps specifies a list of lookup tables that does not match the recipient address.

This feature is available in Postfix 2.0 and later.

unverified_recipient_defer_code (default: 450)
The numerical Postfix SMTP server response when a recipient address probe fails due to a temporary error condition.

Unlike elsewhere in Postfix, you can specify 250 in order to accept the address anyway.

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.6 and later.

unverified_recipient_reject_code (default: 450)
The numerical Postfix SMTP server response when a recipient address is rejected by the reject_unverified_recipient restriction.

Unlike elsewhere in Postfix, you can specify 250 in order to accept the address anyway.

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.1 and later.

unverified_recipient_reject_reason (default: empty)
The Postfix SMTP server's reply when rejecting mail with reject_unverified_recipient. Do not include the numeric SMTP reply code or the enhanced status code. By default, the response includes actual address verification details.

Example:

```
unverified_recipient_reject_reason = Recipient address lookup failed
```

This feature is available in Postfix 2.6 and later.

unverified_recipient_tempfail_action (default: $reject_tempfail_action)
The Postfix SMTP server's action when reject_unverified_recipient fails due to a temporary error condition. Specify "defer" to defer the remote SMTP client request immediately. With the default "defer_if_permit" action, the Postfix SMTP server continues to look for opportunities to reject mail, and defers the client request only if it would otherwise be accepted.

This feature is available in Postfix 2.6 and later.

unverified_sender_defer_code (default: 450)
The numerical Postfix SMTP server response code when a sender address probe fails due to a temporary error condition.

Unlike elsewhere in Postfix, you can specify 250 in order to accept the address anyway.

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.6 and later.

unverified_sender_reject_code (default: 450)
The numerical Postfix SMTP server response code when a recipient address is rejected by the reject_unverified_sender restriction.

Unlike elsewhere in Postfix, you can specify 250 in order to accept the address anyway.

Do not change this unless you have a complete understanding of RFC 5321.

This feature is available in Postfix 2.1 and later.

unverified_sender_reject_reason (default: empty)
The Postfix SMTP server's reply when rejecting mail with reject_unverified_sender. Do not include the numeric SMTP reply code or the enhanced status code. By default, the response includes actual address verification details.

Example:

```
unverified_sender_reject_reason = Sender address lookup failed
```

This feature is available in Postfix 2.6 and later.

unverified_sender_tempfail_action (default: $reject_tempfail_action)
The Postfix SMTP server's action when reject_unverified_sender fails due to a temporary error condition. Specify "defer" to defer the remote SMTP client request immediately. With the default "defer_if_permit" action, the Postfix SMTP server continues to look for opportunities to reject mail, and defers the client request only if it would otherwise be accepted.

This feature is available in Postfix 2.6 and later.

verp_delimiter_filter (default: −=+)

The characters Postfix accepts as VERP delimiter characters on the Postfix **sendmail(1)** command line and in SMTP commands.

This feature is available in Postfix 1.1 and later.

virtual_alias_address_length_limit (default: 1000)

The maximal length of an email address after virtual alias expansion. This stops virtual aliasing loops that increase the address length exponentially.

This feature is available in Postfix 3.0 and later.

virtual_alias_domains (default: $virtual_alias_maps)

Postfix is final destination for the specified list of virtual alias domains, that is, domains for which all addresses are aliased to addresses in other local or remote domains. The SMTP server validates recipient addresses with $virtual_alias_maps and rejects non-existent recipients. See also the virtual alias domain class in the ADDRESS_CLASS_README file

This feature is available in Postfix 2.0 and later. The default value is backwards compatible with Postfix version 1.1.

The default value is $virtual_alias_maps so that you can keep all information about virtual alias domains in one place. If you have many users, it is better to separate information that changes more frequently (virtual address -> local or remote address mapping) from information that changes less frequently (the list of virtual domain names).

Specify a list of host or domain names, "/file/name" or "type:table" patterns, separated by commas and/or whitespace. A "/file/name" pattern is replaced by its contents; a "type:table" lookup table is matched when a table entry matches a lookup string (the lookup result is ignored). Continue long lines by starting the next line with whitespace. Specify "!pattern" to exclude a host or domain name from the list. The form "!/file/name" is supported only in Postfix version 2.4 and later.

See also the VIRTUAL_README and ADDRESS_CLASS_README documents for further information.

Example:

```
virtual_alias_domains = virtual1.tld virtual2.tld
```

virtual_alias_expansion_limit (default: 1000)

The maximal number of addresses that virtual alias expansion produces from each original recipient.

This feature is available in Postfix 2.1 and later.

virtual_alias_maps (default: $virtual_maps)

Optional lookup tables that alias specific mail addresses or domains to other local or remote address. The table format and lookups are documented in **virtual(5)**. For an overview of Postfix address manipulations see the ADDRESS_REWRITING_README document.

This feature is available in Postfix 2.0 and later. The default value is backwards compatible with Postfix version 1.1.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found. Note: these lookups are recursive.

If you use this feature with indexed files, run "**postmap /etc/postfix/virtual**" after changing the file.

Examples:

```
virtual_alias_maps = dbm:/etc/postfix/virtual
virtual_alias_maps = hash:/etc/postfix/virtual
```

virtual_alias_recursion_limit (default: 1000)

The maximal nesting depth of virtual alias expansion. Currently the recursion limit is applied only to the left branch of the expansion graph, so the depth of the tree can in the worst case reach the sum of the expansion and recursion limits. This may change in the future.

This feature is available in Postfix 2.1 and later.

virtual_delivery_status_filter (default: $default_delivery_status_filter)
Optional filter for the **virtual(8)** delivery agent to change the delivery status code or explanatory text of successful or unsuccessful deliveries. See default_delivery_status_filter for details.

This feature is available in Postfix 3.0 and later.

virtual_destination_concurrency_limit (default: $default_destination_concurrency_limit)
The maximal number of parallel deliveries to the same destination via the virtual message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

virtual_destination_recipient_limit (default: $default_destination_recipient_limit)
The maximal number of recipients per message for the virtual message delivery transport. This limit is enforced by the queue manager. The message delivery transport name is the first field in the entry in the master.cf file.

Setting this parameter to a value of 1 changes the meaning of virtual_destination_concurrency_limit from concurrency per domain into concurrency per recipient.

virtual_gid_maps (default: empty)
Lookup tables with the per-recipient group ID for **virtual(8)** mailbox delivery.

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

In a lookup table, specify a left-hand side of "@domain.tld" to match any user in the specified domain that does not have a specific "user@domain.tld" entry.

When a recipient address has an optional address extension (user+foo@domain.tld), the **virtual(8)** delivery agent looks up the full address first, and when the lookup fails, it looks up the unextended address (user@domain.tld).

Note 1: for security reasons, the **virtual(8)** delivery agent disallows regular expression substitution of $1 etc. in regular expression lookup tables, because that would open a security hole.

Note 2: for security reasons, the **virtual(8)** delivery agent will silently ignore requests to use the **proxymap(8)** server. Instead it will open the table directly. Before Postfix version 2.2, the **virtual(8)** delivery agent will terminate with a fatal error.

virtual_mailbox_base (default: empty)
A prefix that the **virtual(8)** delivery agent prepends to all pathname results from $virtual_mailbox_maps table lookups. This is a safety measure to ensure that an out of control map doesn't litter the file system with mailboxes. While virtual_mailbox_base could be set to "/", this setting isn't recommended.

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

Example:

```
virtual_mailbox_base = /var/mail
```

virtual_mailbox_domains (default: $virtual_mailbox_maps)
Postfix is final destination for the specified list of domains; mail is delivered via the $virtual_transport mail delivery transport. By default this is the Postfix **virtual(8)** delivery agent. The SMTP server validates recipient addresses with $virtual_mailbox_maps and rejects mail for non-existent recipients. See also the virtual mailbox domain class in the ADDRESS_CLASS_README file.

This parameter expects the same syntax as the mydestination configuration parameter.

This feature is available in Postfix 2.0 and later. The default value is backwards compatible with Postfix version 1.1.

virtual_mailbox_limit (default: 51200000)

The maximal size in bytes of an individual **virtual(8)** mailbox or maildir file, or zero (no limit).

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

virtual_mailbox_lock (default: see postconf −d output)

How to lock a UNIX-style **virtual(8)** mailbox before attempting delivery. For a list of available file locking methods, use the "**postconf -l**" command.

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

This setting is ignored with **maildir** style delivery, because such deliveries are safe without application-level locks.

Note 1: the **dotlock** method requires that the recipient UID or GID has write access to the parent directory of the recipient's mailbox file.

Note 2: the default setting of this parameter is system dependent.

virtual_mailbox_maps (default: empty)

Optional lookup tables with all valid addresses in the domains that match $virtual_mailbox_domains.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

In a lookup table, specify a left-hand side of "@domain.tld" to match any user in the specified domain that does not have a specific "user@domain.tld" entry.

The remainder of this text is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

The **virtual(8)** delivery agent uses this table to look up the per-recipient mailbox or maildir pathname. If the lookup result ends in a slash ("/"), maildir-style delivery is carried out, otherwise the path is assumed to specify a UNIX-style mailbox file. Note that $virtual_mailbox_base is unconditionally prepended to this path.

When a recipient address has an optional address extension (user+foo@domain.tld), the **virtual(8)** delivery agent looks up the full address first, and when the lookup fails, it looks up the unextended address (user@domain.tld).

Note 1: for security reasons, the **virtual(8)** delivery agent disallows regular expression substitution of $1 etc. in regular expression lookup tables, because that would open a security hole.

Note 2: for security reasons, the **virtual(8)** delivery agent will silently ignore requests to use the **proxymap(8)** server. Instead it will open the table directly. Before Postfix version 2.2, the **virtual(8)** delivery agent will terminate with a fatal error.

virtual_maps (default: empty)

Optional lookup tables with a) names of domains for which all addresses are aliased to addresses in other local or remote domains, and b) addresses that are aliased to addresses in other local or remote domains. Available before Postfix version 2.0. With Postfix version 2.0 and later, this is replaced by separate controls: virtual_alias_domains and virtual_alias_maps.

virtual_minimum_uid (default: 100)

The minimum user ID value that the **virtual(8)** delivery agent accepts as a result from $virtual_uid_maps table lookup. Returned values less than this will be rejected, and the message will be deferred.

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

virtual_transport (default: virtual)

The default mail delivery transport and next-hop destination for final delivery to domains listed with $virtual_mailbox_domains. This information can be overruled with the **transport(5)** table.

Specify a string of the form *transport:nexthop*, where *transport* is the name of a mail delivery transport defined in master.cf. The*:ne xthop* destination is optional; its syntax is documented in the manual page of the corresponding delivery agent.

This feature is available in Postfix 2.0 and later.

virtual_uid_maps (default: empty)

Lookup tables with the per-recipient user ID that the **virtual(8)** delivery agent uses while writing to the recipient's mailbox.

This parameter is specific to the **virtual(8)** delivery agent. It does not apply when mail is delivered with a different mail delivery program.

Specify zero or more "type:name" lookup tables, separated by whitespace or comma. Tables will be searched in the specified order until a match is found.

In a lookup table, specify a left-hand side of "@domain.tld" to match any user in the specified domain that does not have a specific "user@domain.tld" entry.

When a recipient address has an optional address extension (user+foo@domain.tld), the **virtual(8)** delivery agent looks up the full address first, and when the lookup fails, it looks up the unextended address (user@domain.tld).

Note 1: for security reasons, the **virtual(8)** delivery agent disallows regular expression substitution of $1 etc. in regular expression lookup tables, because that would open a security hole.

Note 2: for security reasons, the **virtual(8)** delivery agent will silently ignore requests to use the **proxymap(8)** server. Instead it will open the table directly. Before Postfix version 2.2, the **virtual(8)** delivery agent will terminate with a fatal error.

SEE ALSO

postconf(1),
Postfix configuration parameter maintenance
master(5),
Postfix daemon configuration maintenance

LICENSE

The Secure Mailer license must be distributed with this software.

AUTHOR(S)

Wietse Venema
IBM T.J. Watson Research
P.O. Box 704
Yorktown Heights, NY 10598, USA

Wietse Venema
Google, Inc.
111 8th Avenue
New York, NY 10011, USA

Viktor Dukhovni