NAME

smtpd − Postfix SMTP server

SYNOPSIS

smtpd [generic Postfix daemon options]

sendmail −bs

DESCRIPTION

The SMTP server accepts network connection requests and performs zero or more SMTP transactions per connection. Each received message is piped through the **cleanup**(8) daemon, and is placed into the **incoming** queue as one single queue file. For this mode of operation, the program expects to be run from the **master**(8) process manager.

Alternatively, the SMTP server be can run in stand−alone mode; this is traditionally obtained with "**sendmail −bs**". When the SMTP server runs stand−alone with non $**mail_owner** privileges, it receives mail even while the mail system is not running, deposits messages directly into the **maildrop** queue, and disables the SMTP server's access policies. As of Postfix version 2.3, the SMTP server refuses to receive mail from the network when it runs with non $**mail_owner** privileges.

The SMTP server implements a variety of policies for connection requests, and for parameters given to **HELO, ETRN, MAIL FROM, VRFY** and **RCPT TO** commands. They are detailed below and in the **main.cf** configuration file.

SECURITY

The SMTP server is moderately security−sensitive. It talks to SMTP clients and to DNS servers on the network. The SMTP server can be run chrooted at fixed low privilege.

STANDARDS

RFC 821 (SMTP protocol)
RFC 1123 (Host requirements)
RFC 1652 (8bit−MIME transport)
RFC 1869 (SMTP service extensions)
RFC 1870 (Message size declaration)
RFC 1985 (ETRN command)
RFC 2034 (SMTP enhanced status codes)
RFC 2554 (AUTH command)
RFC 2821 (SMTP protocol)
RFC 2920 (SMTP pipelining)
RFC 3207 (STARTTLS command)
RFC 3461 (SMTP DSN extension)
RFC 3463 (Enhanced status codes)
RFC 3848 (ESMTP transmission types)
RFC 4409 (Message submission)
RFC 4954 (AUTH command)
RFC 5321 (SMTP protocol)
RFC 6531 (Internationalized SMTP)
RFC 6533 (Internationalized Delivery Status Notifications)

DIAGNOSTICS

Problems and transactions are logged to **syslogd**(8).

Depending on the setting of the **notify_classes** parameter, the postmaster is notified of bounces, protocol problems, policy violations, and of other trouble.

CONFIGURATION PARAMETERS

Changes to **main.cf** are picked up automatically, as **smtpd**(8) processes run for only a limited amount of time. Use the command "**postfix reload**" to speed up a change.

The text below provides only a parameter summary. See **postconf**(5) for more details including examples.

COMPATIBILITY CONTROLS

The following parameters work around implementation errors in other software, and/or allow you to override standards in order to prevent undesirable use.

broken_sasl_auth_clients (no)
Enable inter−operability with remote SMTP clients that implement an obsolete version of the AUTH command (RFC 4954).

disable_vrfy_command (no)
Disable the SMTP VRFY command.

smtpd_noop_commands (empty)
List of commands that the Postfix SMTP server replies to with "250 Ok", without doing any syntax checks and without changing state.

strict_rfc821_envelopes (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.

Available in Postfix version 2.1 and later:

smtpd_reject_unlisted_sender (no)
Request that the Postfix SMTP server rejects mail from unknown sender addresses, even when no explicit reject_unlisted_sender access restriction is specified.

smtpd_sasl_exceptions_networks (empty)
What remote SMTP clients the Postfix SMTP server will not offer AUTH support to.

Available in Postfix version 2.2 and later:

smtpd_discard_ehlo_keyword_address_maps (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.

smtpd_discard_ehlo_keywords (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.

smtpd_delay_open_until_valid_rcpt (yes)
Postpone the start of an SMTP mail transaction until a valid RCPT TO command is received.

Available in Postfix version 2.3 and later:

smtpd_tls_always_issue_session_ids (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).

Available in Postfix version 2.6 and later:

tcp_windowsize (0)
An optional workaround for routers that break TCP window scaling.

Available in Postfix version 2.7 and later:

smtpd_command_filter (empty)
A mechanism to transform commands from remote SMTP clients.

Available in Postfix version 2.9 and later:

smtpd_per_record_deadline (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).

Available in Postfix version 3.0 and later:

smtpd_dns_reply_filter (empty)
Optional filter for Postfix SMTP server DNS lookup results.

ADDRESS REWRITING CONTROLS

See the ADDRESS_REWRITING_README document for a detailed discussion of Postfix address rewriting.

receive_override_options (empty)
Enable or disable recipient validation, built−in content filtering, or address mapping.

Available in Postfix version 2.2 and later:

local_header_rewrite_clients (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.

BEFORE-SMTPD PROXY AGENT

Available in Postfix version 2.10 and later:

smtpd_upstream_proxy_protocol (empty)
The name of the proxy protocol used by an optional before−smtpd proxy agent.

smtpd_upstream_proxy_timeout (5s)
The time limit for the proxy protocol specified with the smtpd_upstream_proxy_protocol parameter.

AFTER QUEUE EXTERNAL CONTENT INSPECTION CONTROLS

As of version 1.0, Postfix can be configured to send new mail to an external content filter AFTER the mail is queued. This content filter is expected to inject mail back into a (Postfix or other) MTA for further delivery. See the FILTER_README document for details.

content_filter (empty)
After the message is queued, send the entire message to the specified *transport:destination*.

BEFORE QUEUE EXTERNAL CONTENT INSPECTION CONTROLS

As of version 2.1, the Postfix SMTP server can be configured to send incoming mail to a real−time SMTP−based content filter BEFORE mail is queued. This content filter is expected to inject mail back into Postfix. See the SMTPD_PROXY_README document for details on how to configure and operate this feature.

smtpd_proxy_filter (empty)
The hostname and TCP port of the mail filtering proxy server.

smtpd_proxy_ehlo ($myhostname)
How the Postfix SMTP server announces itself to the proxy filter.

smtpd_proxy_options (empty)
List of options that control how the Postfix SMTP server communicates with a before−queue content filter.

smtpd_proxy_timeout (100s)
The time limit for connecting to a proxy filter and for sending or receiving information.

BEFORE QUEUE MILTER CONTROLS

As of version 2.3, Postfix supports the Sendmail version 8 Milter (mail filter) protocol. These content filters run outside Postfix. They can inspect the SMTP command stream and the message content, and can request modifications before mail is queued. For details see the MILTER_README document.

smtpd_milters (empty)
A list of Milter (mail filter) applications for new mail that arrives via the Postfix **smtpd**(8) server.

milter_protocol (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.

milter_default_action (tempfail)
The default action when a Milter (mail filter) application is unavailable or mis−configured.

milter_macro_daemon_name ($myhostname)
The {daemon_name} macro value for Milter (mail filter) applications.

milter_macro_v ($mail_name $mail_version)
The {v} macro value for Milter (mail filter) applications.

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

milter_command_timeout (30s)
The time limit for sending an SMTP command to a Milter (mail filter) application, and for receiving the response.

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

milter_connect_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after completion of an SMTP connection.

milter_helo_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after the SMTP HELO or EHLO command.

milter_mail_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after the SMTP MAIL FROM command.

milter_rcpt_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after the SMTP RCPT TO command.

milter_data_macros (see 'postconf -d' output)
The macros that are sent to version 4 or higher Milter (mail filter) applications after the SMTP DATA command.

milter_unknown_command_macros (see 'postconf -d' output)
The macros that are sent to version 3 or higher Milter (mail filter) applications after an unknown SMTP command.

milter_end_of_header_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after the end of the message header.

milter_end_of_data_macros (see 'postconf -d' output)
The macros that are sent to Milter (mail filter) applications after the message end−of−data.

GENERAL CONTENT INSPECTION CONTROLS

The following parameters are applicable for both built−in and external content filters.

Available in Postfix version 2.1 and later:

receive_override_options (empty)
Enable or disable recipient validation, built−in content filtering, or address mapping.

EXTERNAL CONTENT INSPECTION CONTROLS

The following parameters are applicable for both before−queue and after−queue content filtering.

Available in Postfix version 2.1 and later:

smtpd_authorized_xforward_hosts (empty)
What remote SMTP clients are allowed to use the XFORWARD feature.

SASL AUTHENTICATION CONTROLS

Postfix SASL support (RFC 4954) can be used to authenticate remote SMTP clients to the Postfix SMTP server, and to authenticate the Postfix SMTP client to a remote SMTP server. See the SASL_README document for details.

broken_sasl_auth_clients (no)
Enable inter−operability with remote SMTP clients that implement an obsolete version of the AUTH command (RFC 4954).

smtpd_sasl_auth_enable (no)
Enable SASL authentication in the Postfix SMTP server.

smtpd_sasl_local_domain (empty)
The name of the Postfix SMTP server's local SASL authentication realm.

smtpd_sasl_security_options (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**.

smtpd_sender_login_maps (empty)
Optional lookup table with the SASL login names that own sender (MAIL FROM) addresses.

Available in Postfix version 2.1 and later:

smtpd_sasl_exceptions_networks (empty)
What remote SMTP clients the Postfix SMTP server will not offer AUTH support to.

Available in Postfix version 2.1 and 2.2:

smtpd_sasl_application_name (smtpd)
The application name that the Postfix SMTP server uses for SASL server initialization.

Available in Postfix version 2.3 and later:

smtpd_sasl_authenticated_header (no)
Report the SASL authenticated user name in the **smtpd**(8) Received message header.

smtpd_sasl_path (smtpd)
Implementation−specific information that the Postfix SMTP server passes through to the SASL plug−in implementation that is selected with **smtpd_sasl_type**.

smtpd_sasl_type (cyrus)
The SASL plug−in type that the Postfix SMTP server should use for authentication.

Available in Postfix version 2.5 and later:

cyrus_sasl_config_path (empty)
Search path for Cyrus SASL application configuration files, currently used only to locate the $smtpd_sasl_path.conf file.

Available in Postfix version 2.11 and later:

smtpd_sasl_service (smtp)
The service name that is passed to the SASL plug−in that is selected with **smtpd_sasl_type** and **smtpd_sasl_path**.

STARTTLS SUPPORT CONTROLS

Detailed information about STARTTLS configuration may be found in the TLS_README document.

smtpd_tls_security_level (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.

smtpd_sasl_tls_security_options ($smtpd_sasl_security_options)
The SASL authentication security options that the Postfix SMTP server uses for TLS encrypted SMTP sessions.

smtpd_starttls_timeout (see 'postconf -d' output)
The time limit for Postfix SMTP server write and read operations during TLS startup and shutdown handshake procedures.

smtpd_tls_CAfile (empty)
A file containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates.

smtpd_tls_CApath (empty)
A directory containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates.

smtpd_tls_always_issue_session_ids (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).

smtpd_tls_ask_ccert (no)
Ask a remote SMTP client for a client certificate.

smtpd_tls_auth_only (no)
When TLS encryption is optional in the Postfix SMTP server, do not announce or accept SASL authentication over unencrypted connections.

smtpd_tls_ccert_verifydepth (9)
The verification depth for remote SMTP client certificates.

smtpd_tls_cert_file (empty)
File with the Postfix SMTP server RSA certificate in PEM format.

smtpd_tls_exclude_ciphers (empty)
List of ciphers or cipher types to exclude from the SMTP server cipher list at all TLS security levels.

smtpd_tls_dcert_file (empty)
File with the Postfix SMTP server DSA certificate in PEM format.

smtpd_tls_dh1024_param_file (empty)
File with DH parameters that the Postfix SMTP server should use with non−export EDH ciphers.

smtpd_tls_dh512_param_file (empty)
File with DH parameters that the Postfix SMTP server should use with export−grade EDH ciphers.

smtpd_tls_dkey_file ($smtpd_tls_dcert_file)
File with the Postfix SMTP server DSA private key in PEM format.

smtpd_tls_key_file ($smtpd_tls_cert_file)
File with the Postfix SMTP server RSA private key in PEM format.

smtpd_tls_loglevel (0)
Enable additional Postfix SMTP server logging of TLS activity.

smtpd_tls_mandatory_ciphers (medium)
The minimum TLS cipher grade that the Postfix SMTP server will use with mandatory TLS encryption.

smtpd_tls_mandatory_exclude_ciphers (empty)
Additional list of ciphers or cipher types to exclude from the Postfix SMTP server cipher list at mandatory TLS security levels.

smtpd_tls_mandatory_protocols (!SSLv2, !SSLv3)
The SSL/TLS protocols accepted by the Postfix SMTP server with mandatory TLS encryption.

smtpd_tls_received_header (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.

smtpd_tls_req_ccert (no)
With mandatory TLS encryption, require a trusted remote SMTP client certificate in order to allow TLS connections to proceed.

smtpd_tls_wrappermode (no)
Run the Postfix SMTP server in the non−standard "wrapper" mode, instead of using the STARTTLS command.

tls_daemon_random_bytes (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).

tls_high_cipherlist (ALL:!EXPORT:!LOW:!MEDIUM:+RC4:@STRENGTH)
The OpenSSL cipherlist for "HIGH" grade ciphers.

tls_medium_cipherlist (ALL:!EXPORT:!LOW:+RC4:@STRENGTH)
The OpenSSL cipherlist for "MEDIUM" or higher grade ciphers.

tls_low_cipherlist (ALL:!EXPORT:+RC4:@STRENGTH)
The OpenSSL cipherlist for "LOW" or higher grade ciphers.

tls_export_cipherlist (ALL:+RC4:@STRENGTH)
The OpenSSL cipherlist for "EXPORT" or higher grade ciphers.

tls_null_cipherlist (eNULL:!aNULL)
The OpenSSL cipherlist for "NULL" grade ciphers that provide authentication without encryption.

Available in Postfix version 2.5 and later:

smtpd_tls_fingerprint_digest (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**.

Available in Postfix version 2.6 and later:

smtpd_tls_protocols (!SSLv2, !SSLv3)
List of TLS protocols that the Postfix SMTP server will exclude or include with opportunistic TLS encryption.

smtpd_tls_ciphers (medium)
The minimum TLS cipher grade that the Postfix SMTP server will use with opportunistic TLS encryption.

smtpd_tls_eccert_file (empty)
File with the Postfix SMTP server ECDSA certificate in PEM format.

smtpd_tls_eckey_file ($smtpd_tls_eccert_file)
File with the Postfix SMTP server ECDSA private key in PEM format.

smtpd_tls_eecdh_grade (see 'postconf -d' output)
The Postfix SMTP server security grade for ephemeral elliptic−curve Diffie−Hellman (EECDH) key exchange.

tls_eecdh_strong_curve (prime256v1)
The elliptic curve used by the Postfix SMTP server for sensibly strong ephemeral ECDH key exchange.

tls_eecdh_ultra_curve (secp384r1)
The elliptic curve used by the Postfix SMTP server for maximally strong ephemeral ECDH key exchange.

Available in Postfix version 2.8 and later:

tls_preempt_cipherlist (no)
With SSLv3 and later, use the Postfix SMTP server's cipher preference order instead of the remote client's cipher preference order.

tls_disable_workarounds (see 'postconf -d' output)
List or bit−mask of OpenSSL bug work−arounds to disable.

Available in Postfix version 2.11 and later:

tlsmgr_service_name (tlsmgr)
The name of the **tlsmgr**(8) service entry in master.cf.

Available in Postfix version 3.0 and later:

tls_session_ticket_cipher (Postfix >= 3.0: aes−256−cbc, Postfix < 3.0: aes−128−cbc)
Algorithm used to encrypt RFC5077 TLS session tickets.

OBSOLETE STARTTLS CONTROLS

The following configuration parameters exist for compatibility with Postfix versions before 2.3. Support for these will be removed in a future release.

smtpd_use_tls (no)
Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

smtpd_enforce_tls (no)
Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption.

smtpd_tls_cipherlist (empty)
Obsolete Postfix < 2.3 control for the Postfix SMTP server TLS cipher list.

SMTPUTF8 CONTROLS

Preliminary SMTPUTF8 support is introduced with Postfix 3.0.

smtputf8_enable (yes)
Enable preliminary SMTPUTF8 support for the protocols described in RFC 6531..6533.

strict_smtputf8 (no)
Enable stricter enforcement of the SMTPUTF8 protocol.

smtputf8_autodetect_classes (sendmail, verify)
Detect that a message requires SMTPUTF8 support for the specified mail origin classes.

VERP SUPPORT CONTROLS

With VERP style delivery, each recipient of a message receives a customized copy of the message with his/her own recipient address encoded in the envelope sender address. The VERP_README file describes configuration and operation details of Postfix support for variable envelope return path addresses. VERP style delivery is requested with the SMTP XVERP command or with the "sendmail −V" command−line option and is available in Postfix version 1.1 and later.

default_verp_delimiters (+=)
The two default VERP delimiter characters.

verp_delimiter_filter (−=+)
The characters Postfix accepts as VERP delimiter characters on the Postfix **sendmail**(1) command line and in SMTP commands.

Available in Postfix version 1.1 and 2.0:

authorized_verp_clients ($mynetworks)
What remote SMTP clients are allowed to specify the XVERP command.

Available in Postfix version 2.1 and later:

smtpd_authorized_verp_clients ($authorized_verp_clients)
What remote SMTP clients are allowed to specify the XVERP command.

TROUBLE SHOOTING CONTROLS

The DEBUG_README document describes how to debug parts of the Postfix mail system. The methods vary from making the software log a lot of detail, to running some daemon processes under control of a call tracer or debugger.

debug_peer_level (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 (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.

error_notice_recipient (postmaster)
The recipient of postmaster notifications about mail delivery problems that are caused by policy, resource, software or protocol errors.

internal_mail_filter_classes (empty)
What categories of Postfix−generated mail are subject to before−queue content inspection by non_smtpd_milters, header_checks and body_checks.

notify_classes (resource, software)
The list of error classes that are reported to the postmaster.

smtpd_reject_footer (empty)
Optional information that is appended after each Postfix SMTP server 4XX or 5XX response.

soft_bounce (no)
Safety net to keep mail queued that would otherwise be returned to the sender.

Available in Postfix version 2.1 and later:

smtpd_authorized_xclient_hosts (empty)
What remote SMTP clients are allowed to use the XCLIENT feature.

Available in Postfix version 2.10 and later:

smtpd_log_access_permit_actions (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).

KNOWN VERSUS UNKNOWN RECIPIENT CONTROLS

As of Postfix version 2.0, the SMTP server rejects mail for unknown recipients. This prevents the mail queue from clogging up with undeliverable MAILER−DAEMON messages. Additional information on this topic is in the LOCAL_RECIPIENT_README and ADDRESS_CLASS_README documents.

show_user_unknown_table_name (yes)
Display the name of the recipient table in the "User unknown" responses.

canonical_maps (empty)
Optional address mapping lookup tables for message headers and envelopes.

recipient_canonical_maps (empty)
Optional address mapping lookup tables for envelope and header recipient addresses.

Parameters concerning known/unknown local recipients:

mydestination ($myhostname, localhost.$mydomain, localhost)
The list of domains that are delivered via the $local_transport mail delivery transport.

inet_interfaces (all)
The network interface addresses that this mail system receives mail on.

proxy_interfaces (empty)
The network interface addresses that this mail system receives mail on by way of a proxy or network address translation unit.

inet_protocols (all)
The Internet protocols Postfix will attempt to use when making or accepting connections.

local_recipient_maps (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.

unknown_local_recipient_reject_code (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.

Parameters concerning known/unknown recipients of relay destinations:

relay_domains (Postfix >= 3.0: empty, Postfix < 3.0: $mydestination)
What destination domains (and subdomains thereof) this system will relay mail to.

relay_recipient_maps (empty)
Optional lookup tables with all valid addresses in the domains that match $relay_domains.

unknown_relay_recipient_reject_code (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.

Parameters concerning known/unknown recipients in virtual alias domains:

virtual_alias_domains ($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.

virtual_alias_maps ($virtual_maps)
Optional lookup tables that alias specific mail addresses or domains to other local or remote address.

unknown_virtual_alias_reject_code (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.

Parameters concerning known/unknown recipients in virtual mailbox domains:

virtual_mailbox_domains ($virtual_mailbox_maps)
Postfix is final destination for the specified list of domains; mail is delivered via the $virtual_transport mail delivery transport.

virtual_mailbox_maps (empty)
Optional lookup tables with all valid addresses in the domains that match $virtual_mailbox_domains.

unknown_virtual_mailbox_reject_code (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.

RESOURCE AND RATE CONTROLS

The following parameters limit resource usage by the SMTP server and/or control client request rates.

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

queue_minfree (0)
The minimal amount of free space in bytes in the queue file system that is needed to receive mail.

message_size_limit (10240000)
The maximal size in bytes of a message, including envelope information.

smtpd_recipient_limit (1000)
The maximal number of recipients that the Postfix SMTP server accepts per message delivery request.

smtpd_timeout (normal: 300s, overload: 10s)
The time limit for sending a Postfix SMTP server response and for receiving a remote SMTP client request.

smtpd_history_flush_threshold (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.

Available in Postfix version 2.3 and later:

smtpd_peername_lookup (yes)
Attempt to look up the remote SMTP client hostname, and verify that the name matches the client IP address.

The per SMTP client connection count and request rate limits are implemented in co−operation with the **anvil**(8) service, and are available in Postfix version 2.2 and later.

smtpd_client_connection_count_limit (50)
How many simultaneous connections any client is allowed to make to this service.

smtpd_client_connection_rate_limit (0)
The maximal number of connection attempts any client is allowed to make to this service per time unit.

smtpd_client_message_rate_limit (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.

smtpd_client_recipient_rate_limit (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.

smtpd_client_event_limit_exceptions ($mynetworks)
Clients that are excluded from smtpd_client_*_count/rate_limit restrictions.

Available in Postfix version 2.3 and later:

smtpd_client_new_tls_session_rate_limit (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.

Available in Postfix version 2.9 and later:

smtpd_per_record_deadline (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).

TARPIT CONTROLS

When a remote SMTP client makes errors, the Postfix SMTP server can insert delays before responding. This can help to slow down run−away software. The behavior is controlled by an error counter that counts the number of errors within an SMTP session that a client makes without delivering mail.

smtpd_error_sleep_time (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.

smtpd_soft_error_limit (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.

smtpd_hard_error_limit (normal: 20, overload: 1)
The maximal number of errors a remote SMTP client is allowed to make without delivering mail.

smtpd_junk_command_limit (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.

Available in Postfix version 2.1 and later:

smtpd_recipient_overshoot_limit (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.

ACCESS POLICY DELEGATION CONTROLS

As of version 2.1, Postfix can be configured to delegate access policy decisions to an external server that runs outside Postfix. See the file SMTPD_POLICY_README for more information.

smtpd_policy_service_max_idle (300s)
The time after which an idle SMTPD policy service connection is closed.

smtpd_policy_service_max_ttl (1000s)
The time after which an active SMTPD policy service connection is closed.

smtpd_policy_service_timeout (100s)
The time limit for connecting to, writing to, or receiving from a delegated SMTPD policy server.

Available in Postfix version 3.0 and later:

smtpd_policy_service_default_action (451 4.3.5 Server configuration problem)
The default action when an SMTPD policy service request fails.

smtpd_policy_service_request_limit (0)
The maximal number of requests per SMTPD policy service connection, or zero (no limit).

smtpd_policy_service_try_limit (2)
The maximal number of attempts to send an SMTPD policy service request before giving up.

smtpd_policy_service_retry_delay (1s)
The delay between attempts to resend a failed SMTPD policy service request.

ACCESS CONTROLS

The SMTPD_ACCESS_README document gives an introduction to all the SMTP server access control features.

smtpd_delay_reject (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.

parent_domain_matches_subdomains (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.

smtpd_client_restrictions (empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client connection request.

smtpd_helo_required (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.

smtpd_helo_restrictions (empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client HELO command.

smtpd_sender_restrictions (empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client MAIL FROM command.

smtpd_recipient_restrictions (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.

smtpd_etrn_restrictions (empty)
Optional restrictions that the Postfix SMTP server applies in the context of a client ETRN command.

allow_untrusted_routing (no)
Forward mail with sender−specified routing (user[@%!]remote[@%!]site) from untrusted clients to destinations matching $relay_domains.

smtpd_restriction_classes (empty)
User−defined aliases for groups of access restrictions.

smtpd_null_access_lookup_key (<>)
The lookup key to be used in SMTP **access**(5) tables instead of the null sender address.

permit_mx_backup_networks (empty)
Restrict the use of the permit_mx_backup SMTP access feature to only domains whose primary MX hosts match the listed networks.

Available in Postfix version 2.0 and later:

smtpd_data_restrictions (empty)
Optional access restrictions that the Postfix SMTP server applies in the context of the SMTP DATA command.

smtpd_expansion_filter (see 'postconf -d' output)
What characters are allowed in $name expansions of RBL reply templates.

Available in Postfix version 2.1 and later:

smtpd_reject_unlisted_sender (no)
Request that the Postfix SMTP server rejects mail from unknown sender addresses, even when no explicit reject_unlisted_sender access restriction is specified.

smtpd_reject_unlisted_recipient (yes)
Request that the Postfix SMTP server rejects mail for unknown recipient addresses, even when no explicit reject_unlisted_recipient access restriction is specified.

Available in Postfix version 2.2 and later:

smtpd_end_of_data_restrictions (empty)
Optional access restrictions that the Postfix SMTP server applies in the context of the SMTP END−OF−DATA command.

Available in Postfix version 2.10 and later:

smtpd_relay_restrictions (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.

SENDER AND RECIPIENT ADDRESS VERIFICATION CONTROLS

Postfix version 2.1 introduces sender and recipient address verification. This feature is implemented by sending probe email messages that are not actually delivered. This feature is requested via the reject_unverified_sender and reject_unverified_recipient access restrictions. The status of verification probes is maintained by the **verify**(8) server. See the file ADDRESS_VERIFICATION_README for information about how to configure and operate the Postfix sender/recipient address verification service.

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

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

address_verify_sender ($double_bounce_sender)
The sender address to use in address verification probes; prior to Postfix 2.5 the default was "postmaster".

unverified_sender_reject_code (450)
The numerical Postfix SMTP server response code when a recipient address is rejected by the reject_unverified_sender restriction.

unverified_recipient_reject_code (450)
The numerical Postfix SMTP server response when a recipient address is rejected by the reject_unverified_recipient restriction.

Available in Postfix version 2.6 and later:

unverified_sender_defer_code (450)
The numerical Postfix SMTP server response code when a sender address probe fails due to a temporary error condition.

unverified_recipient_defer_code (450)
The numerical Postfix SMTP server response when a recipient address probe fails due to a temporary error condition.

unverified_sender_reject_reason (empty)
The Postfix SMTP server's reply when rejecting mail with reject_unverified_sender.

unverified_recipient_reject_reason (empty)
The Postfix SMTP server's reply when rejecting mail with reject_unverified_recipient.

unverified_sender_tempfail_action ($reject_tempfail_action)
The Postfix SMTP server's action when reject_unverified_sender fails due to a temporary error condition.

unverified_recipient_tempfail_action ($reject_tempfail_action)
The Postfix SMTP server's action when reject_unverified_recipient fails due to a temporary error condition.

Available with Postfix 2.9 and later:

address_verify_sender_ttl (0s)
The time between changes in the time−dependent portion of address verifi cation probe sender addresses.

ACCESS CONTROL RESPONSES

The following parameters control numerical SMTP reply codes and/or text responses.

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

defer_code (450)
The numerical Postfi x SMTP server response code when a remote SMTP client request is rejected by the "defer" restriction.

invalid_hostname_reject_code (501)
The numerical Postfi x SMTP server response code when the client HELO or EHLO command parameter is rejected by the reject_invalid_helo_hostname restriction.

maps_rbl_reject_code (554)
The numerical Postfi x 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.

non_fqdn_reject_code (504)
The numerical Postfi x 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.

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

reject_code (554)
The numerical Postfi x SMTP server response code when a remote SMTP client request is rejected by the "reject" restriction.

relay_domains_reject_code (554)
The numerical Postfi x SMTP server response code when a client request is rejected by the reject_unauth_destination recipient restriction.

unknown_address_reject_code (450)
The numerical response code when the Postfi x SMTP server rejects a sender or recipient address because its domain is unknown.

unknown_client_reject_code (450)
The numerical Postfi x SMTP server response code when a client without valid address <=> name mapping is rejected by the reject_unknown_client_hostname restriction.

unknown_hostname_reject_code (450)
The numerical Postfi x SMTP server response code when the hostname specifi ed with the HELO or EHLO command is rejected by the reject_unknown_helo_hostname restriction.

Available in Postfi x version 2.0 and later:

default_rbl_reply (see 'postconf -d' output)
The default Postfi x SMTP server response template for a request that is rejected by an RBL−based restriction.

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

rbl_reply_maps (empty)
Optional lookup tables with RBL response templates.

Available in Postfix version 2.6 and later:

access_map_defer_code (450)
The numerical Postfix SMTP server response code for an **access**(5) map "defer" action, including "defer_if_permit" or "defer_if_reject".

reject_tempfail_action (defer_if_permit)
The Postfix SMTP server's action when a reject−type restriction fails due to a temporary error condition.

unknown_helo_hostname_tempfail_action ($reject_tempfail_action)
The Postfix SMTP server's action when reject_unknown_helo_hostname fails due to an temporary error condition.

unknown_address_tempfail_action ($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.

MISCELLANEOUS CONTROLS

config_directory (see 'postconf -d' output)
The default location of the Postfix main.cf and master.cf configuration files.

daemon_timeout (18000s)
How much time a Postfix daemon process may take to handle a request before it is terminated by a built−in watchdog timer.

command_directory (see 'postconf -d' output)
The location of all postfix administrative commands.

double_bounce_sender (double−bounce)
The sender address of postmaster notifications that are generated by the mail system.

ipc_timeout (3600s)
The time limit for sending or receiving information over an internal communication channel.

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

mail_owner (postfix)
The UNIX system account that owns the Postfix queue and most Postfix daemon processes.

max_idle (100s)
The maximum amount of time that an idle Postfix daemon process waits for an incoming connection before terminating voluntarily.

max_use (100)
The maximal number of incoming connections that a Postfix daemon process will service before terminating voluntarily.

myhostname (see 'postconf -d' output)
The internet hostname of this mail system.

mynetworks (see 'postconf -d' output)
The list of "trusted" remote SMTP clients that have more privileges than "strangers".

myorigin ($myhostname)
The domain name that locally−posted mail appears to come from, and that locally posted mail is delivered to.

process_id (read−only)
The process ID of a Postfix command or daemon process.

process_name (read−only)
The process name of a Postfix command or daemon process.

queue_directory (see 'postconf -d' output)
The location of the Postfix top−level queue directory.

recipient_delimiter (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).

smtpd_banner ($myhostname ESMTP $mail_name)
The text that follows the 220 status code in the SMTP greeting banner.

syslog_facility (mail)
The syslog facility of Postfix logging.

syslog_name (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".

Available in Postfix version 2.2 and later:

smtpd_forbidden_commands (CONNECT, GET, POST)
List of commands that cause the Postfix SMTP server to immediately terminate the session with a 221 code.

Available in Postfix version 2.5 and later:

smtpd_client_port_logging (no)
Enable logging of the remote SMTP client port in addition to the hostname and IP address.

SEE ALSO

anvil(8), connection/rate limiting
cleanup(8), message canonicalization
tlsmgr(8), TLS session and PRNG management
trivial−rewrite(8), address resolver
verify(8), address verification service
postconf(5), configuration parameters
master(5), generic daemon options
master(8), process manager
syslogd(8), system logging

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
ADDRESS_CLASS_README, blocking unknown hosted or relay recipients
ADDRESS_REWRITING_README Postfix address manipulation
FILTER_README, external after−queue content filter
LOCAL_RECIPIENT_README, blocking unknown local recipients
MILTER_README, before−queue mail filter applications
SMTPD_ACCESS_README, built−in access policies
SMTPD_POLICY_README, external policy server
SMTPD_PROXY_README, external before−queue content filter
SASL_README, Postfix SASL howto
TLS_README, Postfix STARTTLS howto
VERP_README, Postfix XVERP extension
XCLIENT_README, Postfix XCLIENT extension
XFORWARD_README, Postfix XFORWARD extension

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

SASL support originally by:
Till Franke
SuSE Rhein/Main AG
65760 Eschborn, Germany

TLS support originally by:
Lutz Jaenicke
BTU Cottbus
Allgemeine Elektrotechnik
Universitaetsplatz 3−4
D−03044 Cottbus, Germany

Revised TLS support by:
Victor Duchovni
Morgan Stanley