

# Dovecot Pro 2.2.x -> 2.3.1

Downgrading is possible to v2.2.27 and later.

## Settings changes

- director\_doveadm\_port setting removed. Name the inet\_listener doveadm { .. } instead.
- mbox\_purge\_preserve\_alt setting removed. It's always assumed to be "yes" now.
- director\_consistent\_hashing setting removed. It's always assumed to be "yes" now.
- recipient\_delimiters setting used to be treated as a separator string. Now it's instead treated as a list of alternative delimiter characters.
- Time interval based settings no longer default to "seconds". All numbers must explicitly be followed by the time unit (except 0). This is important, because some settings now support milliseconds as well.
- fs-posix: prefix=path parameter no longer automatically appends '/' to the path if it's not there. This allows using it properly as a prefix, instead of only a directory prefix. Make sure you have the '/' appended to the prefix, or the "dir/filename" will be accessed just as "dirname".
- ssl\_protocols setting was replaced by ssl\_min\_protocol. Now you only specify the minimum ssl protocol version Dovecot accepts, defaulting to TLSv1.
- ssl parameters were removed and replaced with ssl\_dh. See section 'Diffie-Hellman Parameters for SSL'

## Statistics redesign

The statistics code was redesigned. The old "stats" plugin was renamed to "old\_stats" and the "doveadm stats" was renamed to "doveadm oldstats". There's a new "doveadm stats" command that isn't compatible with the old one. Also the new stats code doesn't require a plugin, so make sure you remove stats from mail\_plugin setting. For more details see [Statistics](#).

So if you wish to keep using the old stats:

- mail\_plugins = stats -> mail\_plugins = old\_stats
- mail\_plugins = imap\_stats -> mail\_plugins = imap\_old\_stats
- service stats -> service old-stats
  - executable = stats -> executable = old-stats
  - fifo\_listener stats-mail -> fifo\_listener old-stats-mail
  - fifo\_listener stats-user -> fifo\_listener old-stats-user
  - unix\_listener stats -> unix\_listener old-stats
- plugin { stats\_refresh } -> plugin { old\_stats\_refresh }
- plugin { stats\_notify\_path } -> plugin { old\_stats\_notify\_path }
- plugin { stats\_track\_cmds } -> plugin { old\_stats\_track\_cmds }
- auth\_stats -> keep as auth\_stats
- stats\_\* settings -> old\_stats\_\*

## New submission service

Dovecot can now act as submission service. See <https://wiki.dovecot.org/Submission> for more information.

## Localhost auth penalty

Dovecot no longer disables auth penalty waits for clients connecting from localhost (or login\_trusted\_networks in general). The previous idea was that it would likely be a webmail that would have its own delays, but there are no guarantees about this.

If the old behavior is still wanted, it's possible to do nowadays even more generically with e.g.:

```
passdb {
  driver = passwd-file
  args = username_format=%{rip} /etc/dovecot/passdb
}
```

/etc/dovecot/passdb:

```
127.0.0.1:::nodelay=yes
192.168.10.124:::nodelay=yes
```

## Setting default changes

Setting	Old default value	New default value
mdbox_rotate_size	2M	10M
mailbox_list_index	no	yes
imap_logout_format	n=%i out=%o	in=%i out=%o deleted=%{deleted} expunged=%{expunged} trashed=% {trashed} hdr_count=%{fetch_hdr_count} hdr_bytes=%{fetch_hdr_bytes} body_count=%{fetch_body_count} body_bytes=%{fetch_body_bytes}
ssl_cipher_list	ALL:!LOW:!SSLv2:!EXP:!aNULL	ALL:!kRSA:!SRP:!kDHd:!DSS:!aNULL! eNULL:!EXPORT:!DES:!3DES:!MD5:!PSK! RC4:!ADH:!LOW@STRENGTH
mail_log_prefix	"%s(%u): "	"%s(%u)<%(pid)><%(session)>: "
mysql: ssl_verify_server_cert	no	yes
ssl_options		no_compression is now the default, and a new compression option is introduced for enabling compression

## Diffie-Hellman parameters for SSL

- ssl-parameters.dat file is now obsolete. You should use ssl\_dh setting instead: `ssl_dh=</etc/dovecot/dh.pem`
  - You can convert an existing ssl-parameters.dat to dh.pem:

```
dd if=/var/lib/dovecot/ssl-parameters.dat bs=1 skip=88 | openssl dhparam -inform der > /etc/dovecot/dh.pem
```
- ssl-params process has also been removed, as it is no longer used to generate these parameters.
- You are encouraged to create at least 2048 bit parameters. 4096 is industry recommendation.
- Please note that it will take LONG TIME to generate the parameters, and it should be done with a machine that has GOOD SOURCE OF ENTROPY. Running it on a virtual machine is not recommended, unless there is some entropy helper/driver installed. Running this on your production proxy can starve connections due to lack of entropy.

## Other changes

- Invalid postmaster\_address now causes a failure early on with sieve/imap\_sieve plugin enabled. It still defaults to postmaster@%d, which expands to invalid postmaster@ address if your usernames do not contain a domain, or are converted into domainless usernames by passdb/userdb. See [DomainLost](#).
- Linux: Dovecot no longer enables core dumping for "setuid processes", which most of them are.
  - To enable them with Linux kernel v3.6+: Make sure core dumps get written to a globally shared directory and enable them with: `sysctl -w fs.suid_dumpable=2`
    - With older Linux kernel versions you can set it to 1, but that's not good for security of your system.
  - You can also revert to old behavior with: `import_environment = $import_environment PR_SET_DUMPABLE`
    - However, this also may have some security implications depending on the setup. Mainly if you have system users and you've enabled chrooting or mail\_access\_groups, this could allow the system users to gain unintentional access.
- userdb nss was removed. Use userdb passwd instead.
- doveadm: table formatter prints the header now to stdout, not stderr
- doveadm: Removed mount commands
- OpenSSL version is required to be at least 1.0.1 for Dovecot to build
- subscriptions file is written in a new version 2 format. Dovecot v2.2.17 and newer can read this file.
- mail\_log plugin: Headers are logged as UTF-8 (instead of MIME-encoded)
- auth: When iterating users in userdb passwd, skip users that aren't in the first/last\_valid\_gid range
- auth protocol has changed some error fields:
  - temp -> code=temp\_fail
  - authz -> code=authz\_fail
  - user\_disabled -> code=user\_disabled

- pass\_expired -> code=pass\_expired
- auth now supports bcrypt algorithm by default.
- Some API changes have been made, if you have your own plugins please be aware that they might require change(s) to be compatible again.