NAME
`mixminiond.conf` – Mixminion server configuration file

SYNOPSIS
```
$HOME/mixminiond.conf
$HOME/etc/mixminiond.conf
/etc/mixminiond.conf
/etc/mixminion/mixminiond.conf
```

DESCRIPTION
`mixminiond` reads its configuration first from the command line, then from its configuration file, then from its built-in defaults. To find a configuration file, the software looks in the following locations:
1. the configuration file specified with the command-line **`–f`** | **`--config`** flag, if any.
2. `$HOME/mixminiond.conf`
3. `$HOME/etc/mixminiond.conf`
4. `/etc/mixminiond.conf`
5. `/etc/mixminion/mixminiond.conf`

The file itself is line-based, with lines grouped into sections. Blank line and lines beginning with '#' are treated as comments. All section headings and entries must appear in the first column.

Each non-comment line is either a section header, of the format "[SectionName]", or an entry of the format "Key: Value". Values may continue on to later lines by indenting the lines after the first, as in an RFC822-style message. All names are case-sensitive. Unless otherwise noted, sections and entries may appear in any order, but no section or entry may appear more than once.

We describe the recognized entry keys below, grouped by section.

The [Host] Section

`ShredCommand` A program (such as 'shred -u') used to securely delete files. [Default: use internal overwrite-and-delete functionality.]

`EntropySource` A character device to provide secure random data for generating keys and seeding the internal pseudorandom number generator. Not used on Windows. [Default: try `/dev/random`, `/dev/srandom`, and `/dev/random` in an appropriate order.]

`TrustedUser` The username of a user who should not trigger "file paranoia". For example, if `/home/` is owned by the user "system", setting "TrustedUser: system" would prevent warnings on startup. This option may appear more than once. [Default: none.]

`FileParanoia` Boolean: If true, check file permissions on private files and directories and their parents. [Default: yes]

The [Server] Section

`BaseDir` Location to store server files. This is the only file location that you need to specify; all others default to subdirectories of `${BaseDir}`. Defaults to `/var/spool/minion`.

`Homedir` An obsolete synonym for "BaseDir".

LogFile   A file to hold the server log. Defaults to ${BaseDir}/log.

StatsFile   A file to hold the server stats log. Defaults to ${BaseDir}/stats.

KeyDir   Directory to hold the server's keys and certificates. Defaults to ${BaseDir}/keys.

WorkDir   Directory to hold volatile or large data, such as messages, replay logs, and so on. Defaults to ${BaseDir}/work.

QueueDir   Directory to hold messages and packets. Defaults to ${WorkDir}/queues.

PidFile   File to hold the process identifier of the current server process. Defaults to ${BaseDir}/pid.

LogLevel   The minimum severity of messages to send to the server's log; log messages less severe than this will be ignored. Recognized severities are:

FATAL An unrecoverable error affecting the entire server and causing an immediate shutdown.

ERROR
    An unrecoverable error affecting a single packet or message.

WARN A warning message. This may reflect an error that has resulted in no lost data, or a worrisome situation that may not actually be an error.

INFO A non-error message describing server status. Logging these messages should not affect users' anonymity.

DEBUG
    A verbose debugging message. Logging these messages can fill up your disk space, and keeping the logs can endanger users' anonymity.

TRACE
    A hyper-verbose debugging message. Logging these messages can fill up your disk space rapidly, and keeping the logs will endanger users' anonymity.

LogLevel defaults to "WARN".

EchoMessages   Boolean: should the server send log messages to standard output as well as to the log file? Used for debugging. Defaults to "no".

Daemon   Boolean: should the server start in the background? (Not yet supported on Windows.) Defaults to "no".

LogStats   Boolean: should the server keep track of packet statistics such as number of packets received? Defaults to "yes".

StatsInterval   Interval: how often should the server flush packet statistics to disk? Defaults to "1 day".

IdentityKeyBits How large should the server's signing key be, in bits? Must be between 2048 and 4096. Defaults to "2048".

PublicKeyLifetime Interval: How often should the server rotate its public key? Must be at least one day. Defaults to "30 days".

PublicKeyOverlap Interval: How long after a server's public key stops getting used should the server continue to accept messages using that key? Defaults to "24 hours".

Mode   Should the server relay messages or not? Currently, only "relay" is supported.

Nickname   What nickname should the others call the server? These nicknames must be unique; must contain only letters, numbers, and hyphens; and must start with a letter. They should be easy to type, and not too long. Once your server has published its keys and been included in the directory, you can't change its nickname without becoming a different server.

Contact-Email   An email address that people can use to contact the server's administrator. Generally, this email address should not depend on the same computer or network hosting the server it describes--otherwise, people will have no way to tell the administrator if the network problems.

Comments   A string to include in your server descriptor's "Comments" section. You may want to describe the server's stability, policies, and so forth.

MixAlgorithm   What approach should the server use to delay messages in its Mix pool and prevent blending attacks? The recognized algorithms are:

                    Timed   Store messages as they arrive, and try to deliver all messages every time *MixInterval* elapses. Not secure, but useful for debugging.

                    DynamicPool Store messages as they arrive. Every time MixInterval elapses, sends messages chosen at random, such that it always keeps MixPoolMinSize messages in the pool, never sends unless it has over MixPoolMinSize messages, and never sends more than MixPoolRate of the messages in the pool. This algorithm is also called "Cottrell" or "Mixmaster".

                    BinomialDynamicPool
                             Store messages as they arrive. Every time MixInterval elapses, send a *randomly chosen* number of messages based on the number that DynamicPool would send. This algorithm is also called "Binomial" or "BinomialCottrell".

                    Defaults to "Timed".

MixInterval   How often should the server consider flushing messages from the mix pool? See MixAlgorithm for more informatino. Defaults to "30 min".

MixPoolRate   Fraction: When running with the DynamicPool or BinomialDynamicPool algorithm, how much of the pool do we flush at once? See MixAlgorithm for more information. Setting this value too high can enable some blending attacks. Defaults to "60%".

MixPoolMinSize   Fraction: When running with the DynamicPool or BinomialDynamicPool algorithm, how many messages do we try to keep in the pool? Setting this value too low can enable some blending attacks. See MixAlgorithm for more information. Defaults to "5".

Timeout   Interval: In general, how long do we wait for another computer to respond on the network before assuming that it is down? Defaults to "5 min".

MaxBandwidth   Size: If specified, we try not to use more than this amount of network bandwidth for MMTP per second, on average.

MaxBandwidthSpike Size: If specified, we try not to use more than this amount of network bandwidth for MMTP per second, ever.

The [DirectoryServers] Section

Publish　　　　　　　Boolean: should the server advertise itself to the directory servers? Don't turn this on until you want users to start using your server. Defaults to "no".

Do *not* set this option to "yes" before you are reasonable confident that you like your server's configuration, and that it will stay up for a while. In particular, please do not delete your server's keys after you have published it, or else the directory will not accept your new keys.

The [Incoming/MMTP] Section

Enabled　　　　　　　Boolean: should the server accept incoming packets? Must be "yes".

Hostname　　　　　　A public hostname that other servers can reach your host by resolving. This hostname *must* be reachable by others, or else they won't be able to find your server. Defaults to the result of gethostname(3).

IP　　　　　　　　　　The IP address your server will tell others to connect to. Older versions of Mixminion use this instead of *Hostname*. If you don't provide this, Mixminion will try to guess your IP, but may guess wrong.

Port　　　　　　　　The port your server will tell others to connect to. Defaults to "48099".

ListenIP　　　　　　The IP address your server will *actually* listen on. Use this option if you are behind a firewall that forwards MMTP connections to your server. Defaults to the value of *IP*.

ListenPort　　　　The Port your server will *actually* listen on. Use this option if you are behind a firewall that forwards MMTP connections to your server. Defaults to the value of *Port*.

The [Outgoing/MMTP] Section

This section configures the outgoing connections your server uses to transmit Type III packets.

Enabled　　　　　　　Should this server deliver packets via MMTP? Must be "yes".

Retry　　　　　　　　RetrySchedule: how often, and for how long, should the server attempt to deliver failing messages? Defaults to "Every 1 hour for 1 day, every 7 hours for 5 days".

MaxConnections　　Integer: How many outgoing connections, at most, will the server try to open at once? Defaults to "16".

The [Delivery/Fragmented] Section

This section configures server-side reassembly of fragmented messages.

Enabled　　　　　　　Boolean: Should the server reassemble fragmented messages at all? Default: "no".

MaximumSize　　　　Size: What is the largest message size, after compression, that we will try to reassemble?

MaximumInterval　Interval: How long will the server hold fragments for a message before giving up on the message? Defaults to "2 days".

The [Delivery/SMTP] Section

This section configures outgoing email delivery.

Enabled   Boolean: Does the server support outgoing email? Don't enable this unless you have your ISP's permission to run a remailer. Defaults to "no".

Retry   RetrySchedule: How often, and for how long, should the server attempt to send failed SMTP messages? Defaults to "every 7 hours for 6 days".

SMTPServer   Hostname of the SMTP server that should be used to deliver outgoing messages. Defaults to "localhost".

MaximumSize   Size: Largest message size (before compression) that we are willing to deliver. Defaults to "100K".

AllowFromAddress   Boolean: Do we allow user-configurable return addresses? (Note that this allows the user to set only the "Username" portion of the 'From: "[Anon] Username" <returnaddress>' header. Defaults to "yes".

X-Abuse   What should the X-Abuse header of outgoing messages contain?

Comments   What should the Comments header of outgoing messages contain?

Message   If provided, a message to put before the content of any outgoing messages.

FromTag   What should the 'tag' portion of outgoing return addresses contain? Defaults to "[Anon]".

ReturnAddress   Must contain an email address to put in the "From" header of outgoing mail.

BlacklistFile   The name of a file describing which outgoing addresses to support. The file format is line-based. Lines starting with # and empty lines are ignored. Whitespace is ignored. All other lines take the format 'deny type value', type is one of the following:

    address   Match an email address, exactly. "Deny address fred@fred" matches "fred@fred" and 'FRED@FRED'.

    user   Match the part of an email address before the @, exactly. "Deny user fred" matches "fred@fred" and "fred@alice", but not "bob@fred" or "mr-fred@alice".

    onehost   Match the part of an email address after the @, exactly. "Deny onehost fred" matches "bob@fred" but not "bob@fred.com" or "bob@host.fred".

    allhosts   Match the part of an email address after the @, or any parent domain thereof. "Deny allhosts fred.com" matches "bob@fred.com" and "bob@host.fred.com", but not "bob@com".

    pattern   match the email address if the provided regex appears anywhere in it. "Deny pattern /./" matches everything; "Deny pattern /(..)*/" matches all addresses with an even number of characters. See `perlre`(1) for a description of the regular expression syntax.

The [Delivery/MBOX] Section

This section configures outgoing delivery to locally configured users via the

Enabled   Should the 'MBOX' module be enabled? Defaults to "no".

AddressFile   The name of file contain mapping mbox names to email addresses. The file format is line-based. Blank lines and lines starting with '#' are ignored. All other lines must be of the format "mboxname: emailaddress@example.com".

RemoveContact   A contact address that users can email to be removed from the address file.

Retry,   SMTPServer,   MaximumSize,   AllowFromAddress,   X-Abuse,   Comments, Message, FromTag, ReturnAddress
See the corresponding entries in the [Delivery/SMTP] section.

The [Delivery/SMTP-Via-Mixmaster] Section

This section is deprecated; it allows you to use Mixmaster to deliver anonymous messages via the Type I/II remailer network. This feature was useful when there were no Type III remailers that supported outgoing SMTP delivery, but that time has long since passed.

Argument Formats

Boolean values   Boolean values are case-insensitive. "Yes", "y", "1", "true", and "on" are considered true; "No", "n", "0", "false" and "off" are considered false.

Intervals of time   Time intervals are given as a floating-point value, and a unit. The units may be single or plural. Recognized units are "second", "sec", "minute", "min", "hour", "day", "week", "month" (30 days), "mon", and "year" (365 days). "1.5 hour", "90 min", "90 minutes", and "5400 sec" are all the same value.

Sizes   Data sizes are given as a numeric value and a unit. The units are case-insensitive, and may be single or plural. Recognized units are "b", "byte", "octet", "K", "KB", "M", "MB", "G", and "GB". If no units are given, we default to "bytes". "524288 bytes", "524288", "512K", "512 KB", and ".5 MB" are all the same size.

Retry Schedules   Delivery retry schedules are given as a comma-separated series of elements. An element may be either an Interval, which indicates a single retry attempt after that interval has passed; or a string of the format "every <Interval1> for <Interval2>", which retries with a period of Interval1 until Interval2 has passed.

For example, "5 minutes, every 10 min for 1 hour, 1 day", makes one attempt after 5 minutes, and 6 more attempts at ten-minute intervals thereafter, then one final attempt 1 day after that.

Note: New deliveries are only attempted when MixInterval has passed; if the intervals in a RetrySchedule are smaller than the value of MixInterval, they are interpreted to mean, "Retry at the earliest opportunity."

Fractions   A fraction may be given as a floating point value between 0.0 and 1.0, or a percentage (followed by a single percent sign).

EXAMPLE

See the mixminiond.conf file in the standard Mixminion distribution for an example.

AUTHORS

See the AUTHORS section in mixminion(1). mixminion(1)

SEE ALSO

mixminion(1) mixminiond(8)