

# Wiki / Postfix

## Dieser Artikel wurde für die folgenden Ubuntu-Versionen getestet:

Dieser Artikel ist größtenteils für alle Ubuntu-Versionen gültig.

## Artikel für fortgeschrittene Anwender

Dieser Artikel erfordert mehr Erfahrung im Umgang mit Linux und ist daher nur für fortgeschrittene Benutzer gedacht.

## Achtung!

Falls Postfix im Internet agieren soll und nicht nur in der eigenen LAN-Spielwiese, so müssen Postfix und abhängige Programme (zum Beispiel **Dovecot**) sehr sorgfältig konfiguriert werden, damit kein **offenes Relay** entsteht!

Ein gutes Tutorial findet man unter **Authentifizierung Postfix via Dovecot** .

## Zum Verständnis dieses Artikels sind folgende Seiten hilfreich:

1. **Installation von Programmen**
2. **Ein Terminal öffnen**
3. **Einen Editor öffnen**

## Inhaltsverzeichnis

1. Installation
2. Grundkonfiguration
3. Postfix Server steuern
4. Besondere Konfigurationen
5. Funktionstest
6. Anhang: Smarthost-Provider
7. Fehlerbehandlung
8. Links



Damit ein Linux-Rechner direkt E-Mails verschicken kann, muss ein MTA ( **Mail Transfer Agent** [[https://de.wikipedia.org/wiki/Mail\\_Transfer\\_Agent](https://de.wikipedia.org/wiki/Mail_Transfer_Agent)]) installiert und konfiguriert sein. Der Klassiker unter den MTA ist sendmail, dieser ist jedoch sehr umständlich zu konfigurieren, deshalb hat sich Postfix

zum Standard entwickelt.

Im Prinzip könnte man den Postfix-Server aufsetzen und gleich E-Mails verschicken. Doch leider ist das im Zeitalter von Spam nicht mehr so einfach. Ein SMTP-Server ohne eine feste IP-Adresse und ohne ordentliche Zertifikate wäre eine ideale Spam-Schleuder. Deshalb akzeptiert eigentlich kein E-Mail-Server E-Mails von solchen Servern. Man muss daher die eigenen E-Mails über einen "ordentlichen" SMTP-Server ( **Smarthost** [https://de.wikipedia.org/wiki/SMTP-Relay-Server]), wie z.B. den von web.de und Co., leiten. Für ortsgebundene Rechner bietet sich der Server des eigenen Internet-Dienstansbieters an, da dieser meistens keine zusätzliche Authentifizierung erfordert.

Ein MTA ist aber auch dann erforderlich, wenn lokale Benutzer auf dem System untereinander E-Mails verschicken wollen. In diesem Fall findet kein Datenaustausch zu einem externen SMTP-Server statt. Lautet der Name des Rechners beispielsweise "ubuntu", so ist "root@ubuntu" eine gültige E-Mail-Adresse. Das Versenden von lokalen E-Mails wird unter anderem von Diensten wie **Cron** [https://wiki.ubuntuusers.de/Cron/] verwendet, um den Administrator über mögliche Probleme zu informieren. Die im Folgenden beschriebene Konfiguration ermöglicht sowohl das Versenden von E-Mails an externe als auch an interne Empfänger.

## Installation

Folgende Pakete müssen installiert <sup>[1]</sup> werden:

- **postfix**
- **libsasl2-modules** (wenn der Smarthost eine Authentifizierung benötigt)
- **bsd-mailx** (optional, um über die Konsole mit dem Befehl mail Mails verschicken zu können)



**Jetzt installieren**

[apt://postfix,libsasl2-modules,bsd-mailx] mit **apturl** [https://wiki.ubuntuusers.de

/apturl/]

```
sudo apt-get install postfix libsasl2-modules bsd-mailx
```

### Hinweis:

Beim Einsatz von Monitoring-Programmen, die via E-Mail informieren sollen, wird **mailx** oft zwingend benötigt.

Alternativ kann in diesem Fall auch **ssmtp**  eingesetzt werden, wodurch sich die Installation von **postfix** und **mailx** erübrigt.

## Grundkonfiguration

Anschließend wird man gleich zur Grundkonfiguration von Postfix geleitet, die aus einer Serie von Fragen besteht. Bei Fragen, auf die hier nicht besonders eingegangen wird, sollte einfach der Standardwert bestätigt werden. Je nachdem, wie man die erste Frage beantwortet, tauchen bestimmte

Fragen später vielleicht gar nicht auf.

## General type of configuration?

Als erstes wird nach dem allgemeinen Einsatzzweck des Servers gefragt. Zur Auswahl stehen folgende Möglichkeiten:

Typ	Beschreibung	Einsatzszenarien
" <i>Internet Site</i> "	Standard. Mail wird empfangen und verschickt.	Echter Mailserver mit fester IP-Adresse, z.B. Root-Server
" <i>Internet mit Smarthost</i> "	Wie Internet Site, aber Mail wird nicht direkt an den entfernten Server zugestellt, sondern über einen anderen Server (etwa beim ISP) geleitet.	Mailserver mit dynamischer IP-Adresse, die sonst sehr oft als potentielle Spam- oder Virenversender blockiert werden.
" <i>Satellite System</i> "	Keine Mail wird empfangen, alle ausgehende Mail über einen Smarthost (s.o.) verschickt.	Mail durch Admin-Skripte oder Webapplikationen verschicken lassen.
" <i>Local only</i> "	Mail wird lokal auf dem Rechner zugestellt, es wird keine Mail von außen empfangen bzw. nach außen geschickt.	Wie " <i>Satellite System</i> ", aber die Mail soll direkt auf demselben System gelesen werden.

## Where should mail for root go?

Hier sollte man entweder den Benutzernamen des Admins eintragen oder seine gültige E-Mail-Adresse.

## Mailname

Dies ist der Name des Rechners, der jeder ausgehenden Mail als Absender-Domain hinzugefügt wird. In den meisten Fällen sollte man einfach den Hostnamen als Mailnamen akzeptieren, außer man ist im Besitz eines geeigneteren Domain-Namens.

## SMTP relay host?

Hier sollte man den Mailserver des Anbieters eintragen, über den man die Mail verschicken will, z.B. *smtp.mailanbieter.de*.

## Für welche weiteren Rechner möchten Sie Mails akzeptieren?

Wenn man den Mailserver für bestimmte Domains betreibt, die hier noch nicht aufgelistet werden, muss man diese ergänzen.

## Local Networks

Hier trägt man ein, welche Maschinen Mail über diesen Server verschicken dürfen. Es ist wichtig, dass man seinen Server hier nicht Unbekannten zur Verfügung stellt, die darüber dann Spam oder Viren verschicken können (*Open Relay*). Als Vorgabe steht dort *127.0.0.0/8*, was bedeutet, dass man nur vom lokalen Rechner aus Mails versenden darf. Wer seinen Mailserver aus dem ganzen LAN zum Versand nutzen will, sollte hier zusätzlich sein eigenes Netz eintragen:

```
127.0.0.0/8, 192.168.1.0/24
```

Wer seinen Server, bspw. einen Root-Server, über das Internet nutzen will, sollte hier auf keinen Fall weite Adressbereiche erlauben, sondern für den Versand stattdessen eine **Authentifizierung** [[https://wiki.ubuntuusers.de/Postfix/Erweiterte\\_Konfiguration/](https://wiki.ubuntuusers.de/Postfix/Erweiterte_Konfiguration/)] verlangen.

### Hinweis:

Je nach Ubuntu-Version sehen diese Fragen etwas anders aus. Der wichtigste Punkt ist immer der SMTP-Server, wenn man *Smarthost* oder *Satellite* gewählt hat. Hat man sich in der Konfiguration vertan, kann man diese im Terminal <sup>[2]</sup> mit

```
sudo dpkg-reconfigure postfix
```

wiederholen, in welchem Fall noch viel mehr Fragen gestellt werden. Ebenso kann man diesen Befehl ausführen, wenn eine wichtige Einstellung, die man verändern wollte (z.B. "*Local Networks*"), bei der Installation übergangen wurde.

Danach ist die erste Konfiguration von Postfix abgeschlossen. Diese wird in der Datei **/etc/postfix/main.cf** hinterlegt.

## Postfix Server steuern

Wie alle anderen Dienste bringt auch Postfix Start/Stop-Skripte mit. Diese Skripte lassen sich natürlich auch zum Kontrollieren des Servers verwenden.

```
# Allgemein
sudo /etc/init.d/postfix
{start|stop|restart|reload|flush|check|abort|force-reload}
# Beispiel
sudo /etc/init.d/postfix restart
```

- "*start*" - Startet den Dienst
- "*stop*" - Stoppt den Dienst
- "*restart*" - Startet den Server neu, bestehende Verbindungen auf den Server werden gekappt
- "*reload*" - Lädt die Konfigurationsdateien neu, ohne dass Verbindungen getrennt werden
- "*flush*" - Es wird versucht, alle Mails, die in der Warteschlange liegen, zu senden

- "*abort*" - Stoppt Postfix sofort, alle laufenden Postfix Prozesse werden angehalten

Mehr dazu im Wiki unter **Dienste** [<https://wiki.ubuntuusers.de/Dienste/>].

## Besondere Konfigurationen

### Authentifizierung am Smarthost

Wenn der SMTP-Server auf dem Smarthost zum Versenden der Mail ein Passwort verlangt, muss die eben erstellte Konfiguration `/etc/postfix/main.cf` allerdings noch einmal editiert <sup>[3]</sup> und diese Zeilen eingefügt werden:

```
smtp_sasl_auth_enable = yes
# noplaintext weglassen, wenn Passwörter im Klartext übertragen werden
müssen:
# (nicht empfohlen, nur wenn's anders nicht funktioniert)
smtp_sasl_security_options = noplaintext noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
```

Wie in der Konfigurationsdatei ersichtlich, holt Postfix die Zugangsdaten aus der Datei `/etc/postfix/sasl_password` bzw. aus einer Datenbank, die aus der `sasl_password` generiert wird. Die Datei sollte man vorzugsweise mit folgendem Befehl erstellen, da sonst ein Umwandeln in eine Datenbank nicht immer möglich ist. Dazu muss man ein Terminalfenster öffnen <sup>[2]</sup> und den folgenden Befehl eingeben:

```
sudo touch /etc/postfix/sasl_password
```

Nun schreibt man seine Daten nach folgendem Muster in die Datei

```
smtp.mailanbieter.de username:ganzgeheimesspasswort
```

Damit nicht gleich jeder das Passwort lesen kann, sollte man noch die Berechtigungen der Datei einschränken (eventuell ist das für Sicherungskopien oder die nachfolgend erzeugte Datenbank zu wiederholen):

```
sudo chmod 600 /etc/postfix/sasl_password
```

Jetzt muss noch die Datenbank erzeugt werden:

```
sudo postmap hash:/etc/postfix/sasl_password
```

Danach muss man postfix neu starten:

```
sudo /etc/init.d/postfix restart
```

### Korrekten Absender setzen

Viele E-Mail-Anbieter erwarten inzwischen, dass man seine Post mit "richtigen" Absenderadressen verschickt - also nicht *ich@localhost* oder *user@meinrechner*. Einige, wie GMX, gehen sogar so weit, nur die eigene, korrekte Adresse zu akzeptieren. Deshalb muss man Postfix beibringen, die lokalen Adressen durch die gewünschte offizielle zu ersetzen.

Folgende Zeile muss man dafür in die Datei **/etc/postfix/main.cf** einfügen:

```
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

Dann erstellt man in einem Editor mit Root-Rechten <sup>[3]</sup> die Datei **/etc/postfix/sender\_canonical** mit beliebig vielen Zuordnungen, z.B.:

```
benutzer email.adresse@gmx.net
www-data beispiel@example.com
root email.adresse@gmx.net
```

Zu guter Letzt erstellt man auch aus dieser Datei eine Postfix-Datenbank und lädt die Postfix-Konfiguration im Terminal <sup>[2]</sup> neu:

```
sudo postmap /etc/postfix/sender_canonical
sudo /etc/init.d/postfix restart
```

## Verschlüsselung aktivieren

Standardmäßig werden die Mails unverschlüsselt an den nächsten Server verschickt. Inzwischen wird dies aus Sicherheitsgründen von immer mehr Anbietern nicht mehr unterstützt (Web.de, GMX, T-Online, etc).

Durch Setzen des `smtp_tls_security_level` auf `encrypt` werden nur noch verschlüsselte Verbindungen aufgebaut. Man sollte den Wert zumindest aber auf `may` setzen. In diesem Fall wird versucht, eine verschlüsselte Verbindung aufzubauen, wenn dies möglich ist.

In die **/etc/postfix/main.cf** hierzu folgendes hinzufügen:

```
smtp_tls_security_level = may
```

Ob die Mail verschlüsselt wurde, sieht man daran, dass in den Kopfzeilen ("header") der Mail bei der entsprechenden Verbindung **ESMTPS(A)** steht:

```
Received: from Meinserver (meine-reverse-dns [Meine IP])
        by Derserver (Postfix) with ESMTPSA id 0E523340030E
        for <me@example.com>; Tue,  8 Apr 2014 10:21:11 +0200 (CEST)
```

## Mehr Konfigurationsmöglichkeiten

Weitere Konfigurationsmöglichkeiten beschreibt der Artikel **Postfix/Erweiterte Konfiguration** [[https://wiki.ubuntuusers.de/Postfix/Erweiterte\\_Konfiguration/](https://wiki.ubuntuusers.de/Postfix/Erweiterte_Konfiguration/)]:

- **Aliase** [https://wiki.ubuntuusers.de/Postfix/Erweiterte\_Konfiguration/] - E-Mail-Umleitungen, z.B. für *root* oder *postmaster*
- **TLS-Verschlüsselung** [https://wiki.ubuntuusers.de/Postfix/Erweiterte\_Konfiguration/] - Clients Verschlüsselung anbieten
- **SASL-Authentifizierung** [https://wiki.ubuntuusers.de/Postfix/Erweiterte\_Konfiguration/] - Authentifizierung von Clients verlangen
- **Sender-abhängige Authentifizierung** [https://wiki.ubuntuusers.de/Postfix/Erweiterte\_Konfiguration/#Sender-abhaengige-Authentifizierung] - Statt einem Smarthost E-Mails individuell über verschiedene SMTP-Server versenden
- **Greylisting-Server** [https://wiki.ubuntuusers.de/Postfix/Erweiterte\_Konfiguration/] - Postgrey als Greylisting-Server einsetzen

## Funktionstest

Jetzt kann man z.B. mit mail aus dem Paket **mailx** eine E-Mail verschicken. Der Befehl dazu sieht im Prinzip so aus:

```
mail -s "testbetreff" email@adresse.de < testmailtext.txt
```

Danach sollte man die Datei **/var/log/mail.log** durchlesen und überprüfen ob alles geklappt hat. Hoffentlich steht nun am Ende der Datei etwas ähnliches wie das hier:

```
...from=<email@gmx.net>...  
...to=<xyz@example.com>,... status=sent... Message accepted
```

## Anhang: Smarthost-Provider

Die Anti-Spam-Maßnahmen mancher Mail-Anbieter können einem als Betreiber eines Heim- oder SOHO-Servers schon ein bisschen das Leben schwer machen. Hier werden ein paar davon beschrieben, und wie man über sie korrekt Mail verschicken kann.

### AOL

AOL erschwert die Konfiguration zusätzlich, weil unumgängliche Filterungsmaßnahmen durchgeführt werden. Nicht nur wird Mail mit anderen Absendern als der angemeldeten AOL-Kennung aggressiv gefiltert, sie leiten auch alle ausgehende Post auf dem regulären SMTP-Port 25 über einen Zwangs-Proxy weiter, der wiederum die gleiche Filterung durchführt. Der Einsatz der AOL-eigenen Mailserver als Smarthost ist deswegen nicht zu empfehlen. Um aber einen externen Anbieter als Smarthost benutzen zu können, muss man statt dem Standardport 25 den *Mail submission*-Port 587 verwenden, z.B. so:

```
relayhost = [mail.gmx.net:587]
```


## Arcor

Arcor-Internet-Kunden können über ihren eigenen Internetzugang ohne weitere Authentifizierung E-Mails mit beliebigem Absender versenden, sofern dieser eine gültige E-Mail-Adresse darstellt:

- **Korrekten Absender setzen**

Auch von unterwegs bzw. über Internet-Anbieter, die es versäumen, ihren Kunden einen eigenen Smarhost bereitzustellen (etwa im Kabelmodem-Bereich) kann man die Arcor-SMTP-Server auf diese Art nutzen, wenn man sich authentifiziert:

- **Authentifizierung am Smarhost**

Es funktioniert auch als Freemail-Kunde des sogenannten **PIA** [[http://www.arcor.de/register/reg\\_01.jsp](http://www.arcor.de/register/reg_01.jsp)] -Systems, daher ist Arcor eine gute Wahl für einen Smarhost. Man braucht das entsprechende Postfach noch nicht einmal als Kontaktadresse zu nutzen, sondern benutzt es nur für den SMTP-Auth und verschickt darüber seine reguläre Mail mit beliebigen Absender-Domains, die allerdings auf Internet-weite Gültigkeit geprüft werden (nicht also von *user@localhost* o.ä. - weshalb der o.g. Schnelltest per **mail**-Befehl scheitern könnte). Zu beachten ist, dass Arcor die Adresse, mit der man sich authentifiziert hat, in einem Zusatz-Header in die Mail einträgt, den der Empfänger lesen kann. Darüber hinaus ist eine Freemail-Registrierung nur aus Deutschland möglich. Es sind folgende Einträge in **/etc/postfix/main.cf** erforderlich (wodurch die Anmelde-Informationen leider unverschlüsselt übertragen werden):

```
relayhost = mail.arcor.de
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
smtp_sasl_security_options = noanonymous
```

Der noch in zahlreichen Beispielen aufgeführte Server *postman.arcor-online.net* ist seit November 2005 außer Betrieb.

## GMX

Um mit Postfix auch über GMX E-Mails versenden zu können, muss man folgende, weiter oben beschriebene Schritte ausführen:

- **Authentifizierung am Smarhost**
- **Korrekten Absender setzen**

Außerdem gilt es folgende Besonderheiten zu beachten:

- GMX akzeptiert nur Mail mit demselben Absender, als der man sich authentifiziert hat. Dieser Anbieter ist deswegen nur als Smarhost geeignet, wenn alle ausgehenden Mails denselben Absender tragen dürfen. Will man dies bei GMX umgehen, kann man sich auch mit der Kundennummer authentifizieren in der `sasl_password`, man trägt dann dort etwa `mail.gmx.net`



12345678:meinZugangspasswort ein.

- Die Benutzerkennung in der `/etc/postfix/sasl_password` besteht aus der vollständigen E-Mail-Adresse und nicht nur aus dem Benutzernamen, z.B.:

```
mail.gmx.net beispiel@gmx.de:geheim
```

Eine minimale `main.cf` sieht dann so aus:

```
alias_database = hash:/etc/aliases
inet_interfaces = loopback-only
mailbox_size_limit = 0
relayhost = mail.gmx.net:587
sender_canonical_maps = hash:/etc/postfix/sender_canonical
smtp_generic_maps = hash:/etc/postfix/generic
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = encrypt
```

## OVH

Wer den SMTP-Server des Webhosters **OVH** [<http://www.ovh.de>] als Smarthost verwendet, muss ähnliche Änderungen vornehmen wie bei GMX. In der Datei `/etc/postfix/main.cf` muss folgender Eintrag geändert werden:

```
smtp_sasl_security_options = noanonymous
```

## WEB.DE

- Der Versand und Empfang über externe Programme muss unter "*Einstellungen -> POP3/IMAP Abruf*" aktiviert werden.
- Von einer WEB.DE-Absenderadresse lässt sich keine Mail an WEB.DE-Empfänger senden. In `/var/log/mail.log` wird in diesem Fall folgende Meldung ausgegeben: "*Authentication failed, or POP3 logon too old. (in reply to MAIL FROM command)*"

Seit der Sicherheitsaktualisierung vom 10.03.2009 muss die SMTP-Authentifizierung über TLS im Klartext erfolgen. Dazu wird in der Datei `/etc/postfix/main.cf` folgender Eintrag geändert <sup>[3]</sup>:

```
smtp_sasl_security_options = noanonymous
```

## Gmail

- Wenn man unter gmail (`[smtp.googlemail.com]:587`) diese Fehler erhält:

```
"530 5.7.0 Must issue a STARTTLS command first."
```

, hilft folgende Option:

```
smtp_tls_security_level = may
```

, natürlich in Zusammenhang mit:

```
smtp_sasl_security_options = noanonymous
```

## 1und1.de

Bei 1&1 ist zu beachten, dass der Parameter *noplaintext* entfernt werden muss, also:

```
relayhost = smtp.1und1.de
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
smtp_sasl_security_options = noanonymous
```

## Posteo

Bei Posteo gelten prinzipiell dieselben Vorgaben wie bei 1&1. Die Verbindung muss via STARTTLS (Port 587) erfolgen, Verbindungen über SSL (Port 465) werden zurückgewiesen. Zusätzlich muss man jedoch **MX** [[https://de.wikipedia.org/wiki/MX\\_Resource\\_Record](https://de.wikipedia.org/wiki/MX_Resource_Record)]-Lookups deaktivieren. Das geschieht über die FQDN-Schreibweise in eckigen Klammern (ggfs. auch in der Datei **/etc/postfix/tls\_policy** verwenden!):

```
relayhost = [posteo.de]:587
```

Versäumt man diese spezielle Notation, kommentiert Postfix das mit einer Fehlermeldung, die der folgenden ähnlich ist:

```
connect to mx02.posteo.de[89.146.194.165]:587: Connection refused
```

Im Kanal <http://www.youtube.com/user/ctaasDE>  ist ein Video zur Installation von Postfix unter Ubuntu 10.04.1 LTS veröffentlicht. Auch wird hier noch auf den HylaFAX-Server eingegangen.

## Fehlerbehandlung

### **fatal: open database /etc/aliases.db: No such file or directory"**

Nach dem Versenden einer Mail wurde in der Log-Datei folgender Fehler festgehalten:

```
| "fatal: open database /etc/aliases.db: No such file or directory".
```

Der Befehl

```
sudo newaliases
```

schafft Abhilfe.

## GMX SASL authentication

```
"SASL authentication failed; cannot authenticate to server mail.gmx.net[213.165.64.21]: no mechanism available"
```


Mit einer Sicherheitsaktualisierung vom 10.03.2009 hat GMX die SMTP-Authentifizierung geändert: diese muss jetzt TLS-verschlüsselt und im Klartext erfolgen. Die Konfiguration wird in **GMX** beschrieben.

## Problem mit Smarthost

Trotz Einrichtens der Benutzerauthentifizierung am Smarthost und der Umwandlung der Absenderadresse kann postfix keine E-Mails über den Smarthost versenden. Manchmal kommt es hier zu Problemen mit der Namensauflösung des Smarthosts. Hier hilft es, wenn man nicht seinen eigenen Router als Nameserver, sondern die Nameserver des Internet-Anbieters direkt angibt. Die notwendigen Schritte sind unter **interfaces** [<https://wiki.ubuntuusers.de/interfaces/#DNS-Server-angeben>] und **DNS Problembehebung** [[https://wiki.ubuntuusers.de/DNS\\_Problembehebung/](https://wiki.ubuntuusers.de/DNS_Problembehebung/)] erklärt.

Nochmals unterstrichen werden sollte auch, dass die Datei **sasl\_password** unbedingt mit 'sudo touch sasl\_password' angelegt werden sollte UND NICHT mit einem Editor wie nano etc., ansonsten wird kein richtiger Zeitstempel erzeugt, und die smtp-Authentifizierung arbeitet nicht. Außerdem müssen der smtp-smarthost, z.B. smtp.gmx.net, in der main.conf bei 'relayname=' unbedingt mit dem in der Datei **sasl\_password** übereinstimmen. Die Verwendung verschiedener Namen, die aber evtl. zur gleichen IP-Adresse zeigen (z.B. mail.gmx.net), führt ebenfalls zu Problemen.

## Network unreachable – Postfix fatal error

In diesem **Blogbeitrag** [<http://disfunctions.de/tutorials/network-unreachable-postfix-fatal-error/>]  (05/2011) wird genauer auf den Fehler **42947** [<https://launchpad.net/bugs/42947>] eingegangen und eine Lösung beschrieben.

## Anhänge mit mehr als 10 MB

Die Postfix-Voreinstellung für die maximale Größe einer E-Mail ist 10 MB. Der Versuch, größere E-Mails (E-Mail Body plus Attachments) zu Verschicken endet mit einer Fehlermeldung im E-Mail-Client. Die aktuelle Einstellung kann mit

```
postconf -n | egrep message_size_limit
```

angezeigt werden, wobei die Größe in Byte ausgegeben wird. Mit folgenden Befehlen kann die maximale Größe einer E-Mail auf 100 MB erhöht werden:

```
sudo postconf -e "message_size_limit = 104857600"
```

```
sudo service postfix restart
```

Falls Postfix zusammen mit einem Smarthost eingesetzt wird, sollte `message_size_limit` natürlich an das Smarthost-System angeglichen werden und dessen Begrenzungseinstellung nicht überschreiten.

## Links

- Homepage: **Postfix** [<http://www.postfix.org/>]  und **Postfix** [<http://de.postfix.org/>] 
  - **Postfix/Erweiterte Konfiguration** [[https://wiki.ubuntuusers.de/Postfix/Erweiterte\\_Konfiguration/](https://wiki.ubuntuusers.de/Postfix/Erweiterte_Konfiguration/)]
- **Postfix** [[https://de.wikipedia.org/wiki/Postfix\\_\(Mail\\_Transfer\\_Agent\)](https://de.wikipedia.org/wiki/Postfix_(Mail_Transfer_Agent))]
- **Postfix-TLS-Optionen** [<https://kofler.info/postfix-tls-optionen/>]  - Blogbeitrag, 11/2016
- **Postfix 1.x bei Wikibooks** [<https://de.wikibooks.org/wiki/Postfix>] 
- **Postfix mit Gmail als Smarthost** [<http://www.my-it-brain.de/wordpress/postfix-mit-gmail-als-smarthost/>]  - Blogbeitrag, 11/2013
- **Umleitung von Mails an root zum eigenen Postfach (Evolution)** [<https://forum.ubuntuusers.de/post/2582672/>] - Beispiel im Forum
- **Lokale Mails in Thunderbird lesen** [<https://wiki.ubuntuusers.de/Thunderbird/Einrichtung/#Lokaler-Mailspool-var-mail>]
- **Automatische E-Mail-Weiterleitung und -Beantwortung bei Abwesenheit mit Postfix** [<https://bitbucket.org/wolfmanx/ws-vacation/>] 
- **Postfix als Satellitensystem** [[https://ctaas.de/software-raid.htm#mdadm\\_postfix\\_E-Mail\\_config](https://ctaas.de/software-raid.htm#mdadm_postfix_E-Mail_config)]  - Weiterleitung von beliebigen System-E-Mails an eine externe E-Mailadresse. Mit SoftwareRAID-Beispiel: Laufwerksprobleme werden autom. per E-Mail gemeldet. Auch für durch crontab, rsync u. ä. generierte Mails geeignet.

---

**Diese Revision** [<https://wiki.ubuntuusers.de/Postfix/a/revision/944263/>] wurde am 16. Oktober 2017 16:26 von **BillMaier** erstellt.

Die folgenden Schlagworte wurden dem Artikel zugewiesen: **Netzwerk** [<https://wiki.ubuntuusers.de/wiki/tags/Netzwerk/>], **Server** [<https://wiki.ubuntuusers.de/wiki/tags/Server/>], **Internet** [<https://wiki.ubuntuusers.de/wiki/tags/Internet/>], **Email** [<https://wiki.ubuntuusers.de/wiki/tags/Email/>], **SMTP** [<https://wiki.ubuntuusers.de/wiki/tags/SMTP/>]

Inhalte von ubuntuusers.de lizenziert unter Creative Commons, siehe <https://ubuntuusers.de/lizenz/>.