



# SMTP-AUTH für Qmail (Client & Server)

Version 1.0  
01.09.2002

**Autor:** Alexander Konz, [a.konz@gmx.de](mailto:a.konz@gmx.de)

## Inhalt:

▪ Vorwort.....	3
▪ Was wollen wir erreichen? .....	3
▪ Voraussetzungen .....	3
▪ Herunterladen der notwendigen Dateien.....	4
▪ SMTP-AUTH-Patch (Server) installieren .....	5
▪ SMTP-AUTH-Patch (Client) installieren .....	8
▪ SMTP-AUTH-Patch (Server) testen .....	10
▪ SMTP-AUTH-Patch (Client) testen.....	12
▪ Nachwort .....	13

## Vorwort

---

Diese Howto setzt voraus, dass **Qmail und Utilities** gemäß dem Howto unter <http://www.treiber-forum.de/linux/berichte/qmail.php> installiert und konfiguriert wurden. Das Versenden und Empfangen von Mail muss problemlos funktionieren.

Sämtliche Pfadangaben in diesem Dokument orientieren sich an den Vorgaben des oben genannten Howto. Gegebenenfalls sind kleinere Änderungen notwendig.

Der Autor dieses Dokuments übernimmt **keinerlei Haftung** für Schäden jedwelcher Art, die direkt oder indirekt aus der Nutzung dieses Dokuments entstehen.

## Was wollen wir erreichen?

---

Das Ziel dieser Howto soll ein Qmail-System sein, dass ohne das prinzipbedingt unsichere POP/IMAP-before-SMTP Verfahren relaysicher gemacht wird. Wir nutzen dazu das standardisierte SMTP-AUTH Verfahren, dass zwischenzeitlich von nahezu allen modernen Email-Programmen unterstützt wird.

Wir werden das System so konfigurieren, dass beim Mailversand über Ihren Mailserver eine Authentifizierung durch Ihren Kunden durchgeführt werden muss, bevor der Mailversand (Relaying) möglich ist. Für diesen Zweck ist dieselbe Username / Passwortkombination zu verwenden wie für den Mailabruf per POP3 oder (falls von Ihnen installiert) IMAP.

## Voraussetzungen

---

Um SMTP-AUTH in Qmail zu aktivieren, sind je nach Wunsch ein oder zwei Patches nötig.

Wenn Qmail als Server fungieren soll, an dem sich Ihre Kunden per SMTP-AUTH authentifizieren müssen, ist der `qmail-smtpd-auth` Patch von **Elysium deeZine** notwendig.

Wenn Qmail sich selbst beim Versand von Mail per SMTP-AUTH authentifizieren soll (z.B. beim Mailserver Ihres Providers), ist der `qmail-remote-authenticated` Patch von **Jay Soffian** notwendig.

Es können beide Patches parallel benutzt werden, da sie sich nicht gegenseitig überschneiden.

Zum Herunterladen und Einspielen der Patches sind die Linux-Utilities **patch** und **wget** notwendig.

## Herunterladen der notwendigen Dateien

---

Wechseln Sie in das bereits aus dem Qmail-Howto bestehende Verzeichnis :

```
# cd ~/qmail
```

Laden Sie anschließend die nötigen Dateien herunter:

```
# wget http://members.elysium.pl/brush/qmail-smtpd-auth/dist/qmail-smtpd-auth-0.31.tar.gz  
# wget http://qmail.mirrors.space.net/qmail-remote\_authenticated\_smtp.patch
```

## SMTP-AUTH-Patch (Server) installieren

---

Wenn Sie möchten, dass sich Ihre Clients per SMTP-AUTH bei Ihrem Qmail authentifizieren müssen, lesen Sie bitte hier weiter. Wenn Sie SMTP-AUTH nur zur Authentifizierung beim Mailserver Ihres Providers benötigen, lesen Sie bitte beim nächsten Abschnitt weiter.

Nachdem Sie den Patch heruntergeladen haben, entpacken Sie diesen bitte:

```
# tar xzf qmail-smtpd-auth-0.31.tar.gz
```

Im neu angelegten Verzeichnis `qmail-smtpd-auth-0.31` finden Sie nun 4 Dateien vor. Kopieren Sie die beiden Dateien `base64.c` und `base64.h` ins Qmail-Source Verzeichnis:

```
# cd qmail-smtp-auth-0.31
# cp base64.c base64.h ~/qmail/qmail-1.03
```

Um im Fall des Falls den Patch rückgängig machen zu können, sollten Sie noch einige Dateien im Qmail-Source Verzeichnis sichern:

```
# cd ~/qmail/qmail-1.03
# cp Makefile Makefile.old
# cp TARGETS TARGETS.old
# cp qmail-smtpd.8 qmail-smtpd.8.old
# cp qmail-smtpd.c qmail-smtpd.c.old
```

Spielen Sie anschließend den Patch ein:

```
# cd ~/qmail/qmail-smtpd-auth.0.31
# patch -d ~/qmail/qmail-1.03 < auth.patch
```

Nach dem Einspielen sollte „patch“ vier gepatchte Dateien melden und es sollten keine Fehler auftreten.

Nun müssen Sie den geänderten Quelltext neu übersetzen. Wechseln Sie dazu ins Qmail-Source Verzeichnis und geben Sie „make“ ein:

```
# cd ~/qmail/qmail-1.03
# make
```

Da Sie nur `qmail-smtpd.c` geändert haben, wurde beim make-Lauf nur `qmail-smtpd` neu erstellt, was Sie anhand des Dateidatums kontrollieren können und sollten.

Als nächstes müssen Sie Ihr laufendes Qmail beenden ...

```
# /etc/rc.d/qmail stop
```

... damit das betroffene Programm gesichert und gegen die neue Version ausgetauscht werden kann:

```
# make setup check
```

Nachdem das Programm und die ebenfalls geänderte man-Page zu `qmail-smtpd` ausgetauscht wurde, müssen Sie abschließend noch einige Kleinigkeiten in der Konfiguration ändern, um SMTP-AUTH nutzen zu können.

Öffnen Sie mit einem Texteditor die Datei `/var/qmail/supervise/qmail-smtpd/run` und entfernen Sie in der letzten Zeile den Verweis auf `relay-ctrl-check` (`/usr/local/bin/relay-ctrl-check`). Löschen Sie anschließend die gesamte sechste Zeile der Datei (`/usr/local/bin/envdir /etc/relay-ctrl \`).

In dieser „run“-Datei wird die von Ihnen gepatchte Version von `qmail-smtpd` aufgerufen, der Sie noch drei Parameter übergeben müssen, die durch den Patch notwendig geworden sind. Als ersten Parameter geben Sie den Hostnamen Ihres Systems an (Inhalt von `/var/qmail/control/me`), gefolgt von `/home/vpopmail/bin/vchkpw`. Abschließend fügen Sie dahinter noch `/bin/true` ein, so dass Sie folgende „run“-Datei erhalten:

```
#!/bin/sh
QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 8000000 \
/usr/local/bin/tcpserver -v -p -c "$MAXSMTPD" \
-d "$QMAILDUID" -g "$NOFILESGID" 0 smtp /var/qmail/bin/qmail-smtpd \
host.domain.de /home/vpopmail/bin/vchkpw /bin/true 2>&1
```

Würden Sie Qmail mit dieser „run“-Datei starten, hätten Sie das Problem, dass sämtliche Username / Passwort-Kombinationen nicht als gültig erkannt werden und die Authentifizierung fehlschlägt.

Um diesen Fehler zu beheben, müssen Sie in der zweiten und dritten Zeile der „run“-Datei jeweils `qmaild` durch `vpopmail` ersetzen. Dies führt dazu, dass `qmail-smtpd` nicht mehr unter dem Benutzer `qmaild` sondern als `vpopmail` läuft und damit auch Zugriff auf die `vpopmail`-Benutzerdatenbank erhält.

Nachdem Sie diesen Teil der Konfiguration durchgeführt haben, müssen Sie noch beim POP3- und beim ggf. zusätzlich installierten IMAP-Service den `relay-ctrl-check` entfernen, damit dieser nicht mehr in Kraft tritt.

Öffnen Sie mit einem Texteditor die Datei `/var/qmail/supervise/qmail-pop3d/run` und entfernen Sie die gesamte dritte Zeile (`/usr/local/bin/envdir /etc/relay-ctrl \`). Anschließend entfernen Sie in der letzten Zeile den Verweis auf `relay-ctrl-allow`, so dass Sie folgende „run“-Datei erhalten:

```
#!/bin/sh
exec env - PATH="/var/qmail/bin:/usr/local/bin" \
tcpserver -H -R 0 pop3 \
/var/qmail/bin/qmail-popup host.domain.de \
/home/vpopmail/bin/vchkpw /var/qmail/bin/qmail-pop3d Maildir 2>&1
```

Falls Sie auch den Courier IMAP-Server installiert haben, müssen Sie zum Abschluß noch den **relay-ctrl-check** beim IMAP-Zugriff deaktivieren. Dazu beenden Sie zuerst den laufenden IMAP-Server:

```
# /etc/rc.d/courier-imap stop
```

Dann öffnen Sie mit einem Texteditor die Datei `/usr/lib/courier-imap/etc/imapd`. Dort finden Sie folgende Zeile ...

```
AUTHMODULES="authdaemon relay-ctrl-allow"
```

... die Sie gegen folgende Zeile austauschen:

```
AUTHMODULES="authdaemon"
```

Damit hat der **relay-ctrl-check** bei POP3, SMTP und ggf. IMAP keinerlei Relevanz mehr. Sie können nun noch den Cronjob löschen, den Sie während der Qmail-Installation eingerichtet hatten. Ausserdem können Sie die Verzeichnisse `/etc/relay-ctrl` und `/var/spool/relay-ctrl` inklusive Inhalt entfernen.

Starten Sie jetzt wieder Qmail und ggf. den IMAP-Server und achten Sie in den Logfiles auf evtl. auftauchende Fehlermeldungen:

```
# /etc/rc.c/qmail start
# /etc/rc.d/courier-imap start      (ggf.)
```

Sie haben nun einen Qmail-Server, der nur noch lokale E-Mail annimmt. Für ausgehende Post Ihrer Clients ist es ab sofort nötig, sich per SMTP-AUTH zu authentifizieren.

Wie Sie die korrekte Funktion Ihres SMTP-AUTH-Servers testen, können Sie im übernächsten Abschnitt lesen. Der nächste Abschnitt beschäftigt sich mit SMTP-AUTH als Client (z.B. um sich beim Mailserver Ihres Providers zu authentifizieren).

## SMTP-AUTH-Patch (Client) installieren

---

Wenn Sie möchten, dass sich Ihr Qmail-Server bei anderen Mailservern per SMTP-AUTH authentifizieren soll, lesen Sie hier bitte weiter.

Den dazu notwendigen Patch haben Sie bereits in einem der vorherigen Abschnitte heruntergeladen. Da dieser nicht gepackt ist, können Sie ihn direkt einspielen. Vorher sollten Sie aber erst die zu patchende Datei sichern, um sie im Notfall wiederherstellen zu können:

```
# cd ~/qmail/qmail-1.03
# cp qmail-remote.c qmail-remote.c.old
```

Dann spielen Sie den Patch ein:

```
# cd ~/qmail
# patch -d qmail-1.03/ < qmail-remote_authenticated_smtp.patch
```

Das „patch“-Utility sollte Ihnen eine gepatchte Datei melden und sich ohne Fehlermeldungen beenden. Nun müssen Sie die gepatchte Datei neu übersetzen. Dazu wechseln Sie ins Qmail-Source Verzeichnis und geben „make“ ein:

```
# cd ~/qmail/qmail-1.03
# make
```

Anhand des Dateidatums von **qmail-remote** können Sie überprüfen, ob die Datei neu übersetzt wurde.

Sollten Sie Ihr Qmail im vorangegangenen Abschnitt bereits wieder gestartet haben, müssen Sie es jetzt erneut beenden, um die betroffene Datei austauschen zu können:

```
# /etc/rc.d/qmail stop
```

Sichern Sie für den Notfall die alte Datei und tauschen Sie sie gegen die neu übersetzte aus:

```
# cp /var/qmail/bin/qmail-remote /var/qmail/bin/qmail-remote.old
# cp qmail-remote /var/qmail/bin
```

Sie haben jetzt ein Qmail-System, das sich beim Ausliefern von Mail beim entfernten Mailserver per SMTP-AUTH authentifizieren kann.

Um dieses Feature zu nutzen, muss es in **/var/qmail/control/smtproutes** konfiguriert werden.

Durch den Patch ändert sich die Syntax dieser Datei im Gegensatz zur Qmail-Dokumentation geringfügig. Qmail erwartet jetzt zwei weitere Parameter, nämlich einen Usernamen und ein Passwort, beide jeweils Base64-kodiert. Utilities, um beliebige Zeichenketten in Base64 zu kodieren, finden Sie im Internet.

Wenn Sie Ihre gesamte ausgehende Mail über ein und denselben Mailserver verschicken möchten (z.B. Mailserver Ihres Providers), ist die Konfiguration sehr einfach.

Folgende Zeile in `/var/qmail/control/smtproutes` sorgt z.B. dafür, dass alle ausgehende Mail über den Mailserver `mail.provider.de` verschickt wird, bei dem sich Qmail mit dem Usernamen `trottell` (Base64: `dHJvdHRlbA==`) und dem Passwort `ich` (Base64: `aWNo`) anmeldet:

```
:mail.provider.de dHJvdHRlbA== aWNo
```

Wenn Sie Ihre ausgehende Mail stattdessen lieber direkt bei den jeweils zuständigen Mailservern einwerfen möchten mit Ausnahme der Domain `testdomain.de`, sähe eine entsprechende Zeile so aus:

```
testdomain.de:mail.provider.de dHJvdHRlbA== aWNo  
.testdomain.de:mail.provider.de dHJvdHRlbA== aWNo
```

Jetzt würde nur noch Mail an `testdomain.de` und an alle **Subdomains von `testdomain.de`** über den Mailserver Ihres Providers verschickt. Die restliche Mail würde direkt an den jeweils zuständigen Mailserver geschickt (aber: **ohne SMTP-AUTH!**).

Für weitere Einstellungsmöglichkeiten dieser Datei konsultieren Sie bitte die Qmail-Dokumentation und die man-Page, insbesondere bei bereits bestehenden komplexeren Routing-Tabellen.

Für den Standard-Benutzer empfiehlt sich allerdings die erstgenannte Möglichkeit, sämtliche ausgehende Mail über den Mailserver Ihres Providers abzuwickeln. Auch aus netztopologischer Sicht ist das in den meisten Fällen die beste Wahl.

## SMTP-AUTH (Server) testen

---

In diesem Abschnitt können Sie lesen, wie Sie Ihr Qmail-System testen können, ob sich Clients erfolgreich am Server authentifizieren können.

Um diesen Test durchzuführen, sind Grundkenntnisse im Bedienen eines telnet-Clients sowie ein Base64-Encoder notwendig, um die Zugangsdaten umzuwandeln.

Wir gehen im Folgenden davon aus, dass in Ihrem vpopmail eine Emailadresse `test@domain.de` mit dem Passwort `testing` existiert. Bitte prüfen Sie vor der Durchführung dieses Tests, ob sich dieser User erfolgreich per POP3 oder IMAP am Mailserver anmelden kann.

Da wir beim Testen die Base64-Varianten der Zugangsdaten benötigen, erhalten wir mit einem Base64-Encoder für die oben genannten Daten als Username die Zeichenkette `dGVzdEBkb21haW4uZGU=` und für das Passwort `dGVzdGluZw==`.

Für die folgenden Zeilen gilt: Texte, die der Server zu Ihnen schickt, sind **grün** geschrieben, Texte die Sie eingeben müssen, sind **rot** geschrieben. Bitte beachten Sie, dass die Ausgabe je nach telnet-Client etwas variieren kann.

Wir verbinden uns mit dem Mailserver auf Port 25:

```
# telnet mail.domain.de 25
Trying 123.123.123.123...
Connected to mail.domain.de.
Escape character is '^]'
220 mail.domain.de SMTP
```

Die Verbindung zum Mailserver ist also geglückt. Wir begrüßen den Mailserver mit unserem Hostnamen:

```
ehlo hostname
```

und sollten erhalten:

```
250-mail.domain.de
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-PIPELINING
250 8BITMIME
```

Hier sehen wir, dass uns der Mailserver drei Authentifizierungsverfahren zur Auswahl stellt (LOGIN, CRAM-MD5 und PLAIN). Wir werden hier nur die LOGIN-Variante testen, da sie in den meisten Programmen genutzt wird. Das teilen wir dem Mailserver auch mit:

```
auth login
```

Der Server sollte nun mit

```
334 VXNlcm5hbWU6
```

antworten. Wenn wir diese Zeichenkette per Base64 dekodieren, erhalten wir **Username:**. Er möchte unseren Benutzernamen haben, den wir ihm Base64-kodiert übermitteln:

```
dGVzdEBkb2lhaW4uZGU=
```

Der Server antwortet mit

```
334 UGFzc3dvcmQ6
```

Wenn wir auch diese Zeichenkette einmal per Base64 dekodieren, erhalten wir **Password:**, welches wir ebenfalls Base64-kodiert übermitteln:

```
dGVzdGluZw==
```

Wenn die von uns gesendete Kombination aus Benutzername und Passwort korrekt war, meldet sich der Server mit

```
235 ok, go ahead (#2.0.0)
```

Andernfalls erhalten wir (nach kurzer Wartezeit):

```
535 authorization failed (#5.7.0)
```

Falls die Authentifizierung geklappt hat, kann jetzt (bis zum Abmelden am Server mittels quit) problemlos sowohl lokale als auch ausgehende Mail verschickt werden.

Schlägt die Authentifizierung dagegen fehl oder wird sie überhaupt nicht durchgeführt, ist es nicht mehr möglich, Mail an Adressen zu versenden, deren Domains nicht auf Ihrem Mailserver verwaltet werden.

Zu beachten ist, dass nach dem Einspielen des SMTP-AUTH-Patches (Server) der Received:-Header Ihres Qmail-Systems anders aufgebaut wird als ohne Patch.

Zur Verdeutlichung hier ein Beispiel **ohne** Patch:

```
Received: from host.domain.de (HELO hostname) (192.168.10.10)  
by mail.domain.de with SMTP; 2 Aug 2002 15:12:58 -0000
```

und ein Beispiel **mit** Patch:

```
Received: from host.domain.de (HELO hostname) (test@domain.de@192.168.10.10)  
by mail.domain.de with SMTP; 2 Aug 2002 15:16:26 -0000
```

Im Gegensatz zum patchlosen Qmail fügt der Patch noch zusätzlich zur IP-Adresse den Usernamen mit ein, mit dem sich der Mailversender an Ihrem Mailserver angemeldet hatte. Damit steht eindeutig fest, wer diese Email verschickt hat. Diese Zusatzinformation ist sehr hilfreich für ein evtl. vorhandenes Abuse-Management.

## SMTP-AUTH (Client) testen

---

In diesem Abschnitt können Sie lesen, wie Sie die SMTP-AUTH Client-Authentifizierung Ihres Qmail-Systems testen können.

Wenn man sich überlegt, welchen Sinn die Authentifizierung hat, stellt man schnell fest, dass ohne oder mit ungültiger Authentifizierung kein Mailversand an Domains möglich ist, die nicht direkt auf dem angesprochenen Mailserver verwaltet werden.

Daher kann dieser Test auch recht einfach durchgeführt werden, indem man über seinen eigenen Mailserver einfach eine Email z.B. an einen GMX-Account schickt und sich danach die Headerzeilen der bei GMX aufgelaufenen Email anschaut.

Wir gehen im Folgenden davon aus, dass Ihr Qmail-System so konfiguriert wurde, dass sämtliche ausgehende Mail über den Mailserver Ihres Providers [mail.provider.de](mailto:mail.provider.de) abgewickelt wird; Anmeldeinformationen dort seien [kunde0815@domain.de](mailto:kunde0815@domain.de) mit Passwort [4711](#).

Die `/var/qmail/control/smtproutes` sähe daher folgendermassen aus:

```
:mail.provider.de a3VuZGUwODElQGRvbWFPbi5kZQ== NDcxMQ==
```

Erstellen Sie mit einem beliebigen Email-Client eine neue Email mit etwas Text. Beachten Sie bitte, dass Sie eine Empfängeradresse angeben, die garantiert nicht von Ihrem Mailserver verwaltet wird, z.B. GMX, Web.de, etc.

Schicken Sie nun diese Email über Ihren Mailserver ab. Nach kurzer Zeit sollte sich dieser mit dem Mailserver Ihres Providers in Verbindung setzen und die Email dort absetzen.

Kontrollieren Sie, ob die Email beim Empfänger angekommen ist. Falls das der Fall ist, können Sie davon ausgehen, dass das SMTP-AUTH-Verfahren Ihres Qmail-Systems einwandfrei funktioniert, denn wenn Ihr Provider-Mailserver es nicht akzeptiert hätte, wäre die Email dort auf jeden Fall zurückgewiesen worden.

Sollte die Email allerdings nicht beim Empfänger ankommen, sollten Sie in den Logfiles von Qmail nachschauen, ob irgendwelche Fehler protokolliert wurden. Der am öftesten auftretende Fehler ist ein Tippfehler bei den Base64-kodierten Zugangsdaten. Weiterhin ist natürlich zu überprüfen, ob der von Ihnen genutzte Provider-Mailserver überhaupt die SMTP-AUTH-Authentifizierung unterstützt.

## Nachwort

---

Wie bereits im Vorwort erwähnt wurde, übernimmt der Autor dieses Dokuments **keinerlei Haftung** für Schäden, die direkt oder indirekt aus der Verwendung dieser Howto resultieren.

Bedanken möchte ich mich an dieser Stelle bei Rene Schleicher, Autor der Qmail-Howto. Er stand als Korrekturleser zur Verfügung und sorgte für die eine oder andere Verbesserung der Textabschnitte. Desweiteren wäre ohne seine Howto natürlich auch diese Anleitung nicht möglich gewesen.

Diese Howto wurde bereits auf mehreren Systemen getestet und für funktionsfähig erklärt. Leider kann es aber durch ungünstige Softwarekonstellationen oder andere Softwareversionen zu Problemen kommen, die hier evtl. nicht beachtet wurden. In diesem Fall empfiehlt der Autor, einen erneuten Versuch mit den hier angesprochenen Versionen zu testen.

Der Autor versucht, diese Howto stets auf dem aktuellen Stand zu halten. Da sie jedoch primär auf die Qmail-Howto aufsetzt, verzichtet der Autor nötigenfalls auf ein Update, falls die Qmail-Howto nicht ebenfalls mit neuen Versionen aktualisiert wird, um eine eventuell auftretende Fehlfunktion des ganzen Systems zu verhindern (Versionskompatibilität, etc.).

Falls Probleme beim Installieren auftauchen, ist der Autor selbstverständlich daran interessiert, davon zu erfahren, um sie in einer aktualisierten Version gezielt anzusprechen und um bisher nicht gefundene Schwachstellen zu eliminieren.

Um dem Autor ein Problem der Installation mitzuteilen, sollten Sie ihm so viel Daten als möglich zur Verfügung stellen, um das Problem nachstellen zu können. Dazu zählen auf jeden Fall:

- verwendetes Betriebssystem (Kernelversion und Distribution)
- Version des Compilers (falls Kompilierungsfehler auftreten)
- eingesetzte Softwareversionen (Qmail, vpopmail, etc.)

Ferner sind zur Analyse folgende Daten und Dateien notwendig:

- Inhalt von `/var/qmail/control`, `/var/qmail/alias`, `/var/qmail/supervise`
- Logfileauszüge (das Problem beschreibend)

Der Autor wünscht viel Vergnügen!

Alexander König