

Zu altes System/Mail-Client

Allgemeine Informationen

Um bei unseren E-Mail-Diensten jederzeit eine sichere Verschlüsselung gewährleisten zu können, passen wir diese regelmäßig an die jeweils aktuellen Empfehlungen für SSL/TLS-basierte Transport-Verschlüsselungen an. Wenn Ihr Betriebssystem, Ihr E-Mail-Programm bzw. die von Ihnen eingesetzte Software veraltet ist, kann das dazu führen, dass Sie per SMTP keine E-Mails mehr über unsere E-Mail-Server versenden können. Wir empfehlen daher immer den Einsatz eines noch in der Wartung des Herstellers befindlichen Betriebssystems bzw. einer solchen Software.

Sollten Sie aus einem speziellen Grund dennoch unbedingt ein veraltetes Betriebssystem oder eine veraltete Software benutzen müssen, so finden Sie in den nachfolgenden Abschnitten einen Workaround mit der Software „stunnel“. *Bitte bedenken Sie dennoch, dass Ihr veraltetes Betriebssystem bzw. Ihre veraltete Software weiterhin Sicherheitslücken haben und ein großes Sicherheitsrisiko für Sie darstellen kann! Die Nutzung eines aktuellen Betriebssystems bzw. einer aktuellen Software ist daher immer gegenüber der nachfolgend geschilderten Nutzung von „stunnel“ vorzuziehen!*

Derzeit unterstützen alle Versionen von Microsoft Windows ab Version 7 bzw. Server 2008 R2 (die beide bereits seit Januar 2020 seitens Microsoft eingestellt wurden und keine Sicherheitsupdates mehr erhalten) eine aktuelle Verschlüsselung, gegebenenfalls ist hierfür die manuelle Installation optionaler Updates erforderlich:

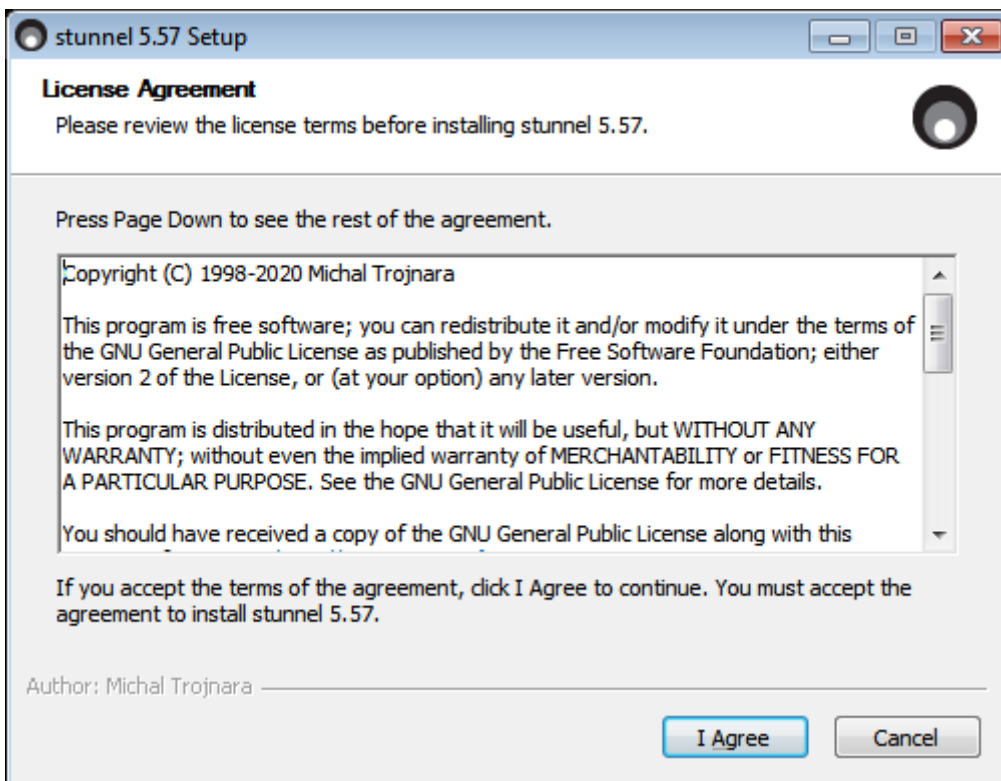
- [Cipher Suites in TLS/SSL \(Schannel SSP\)](#)
- [Update für Microsoft Windows 8.1 und Microsoft Windows Server 2012 R2](#)
- [Update für Microsoft Windows 8 und Microsoft Windows Server 2012](#)
- [Update für Microsoft Windows 7 und Microsoft Windows Server 2008 R2](#)

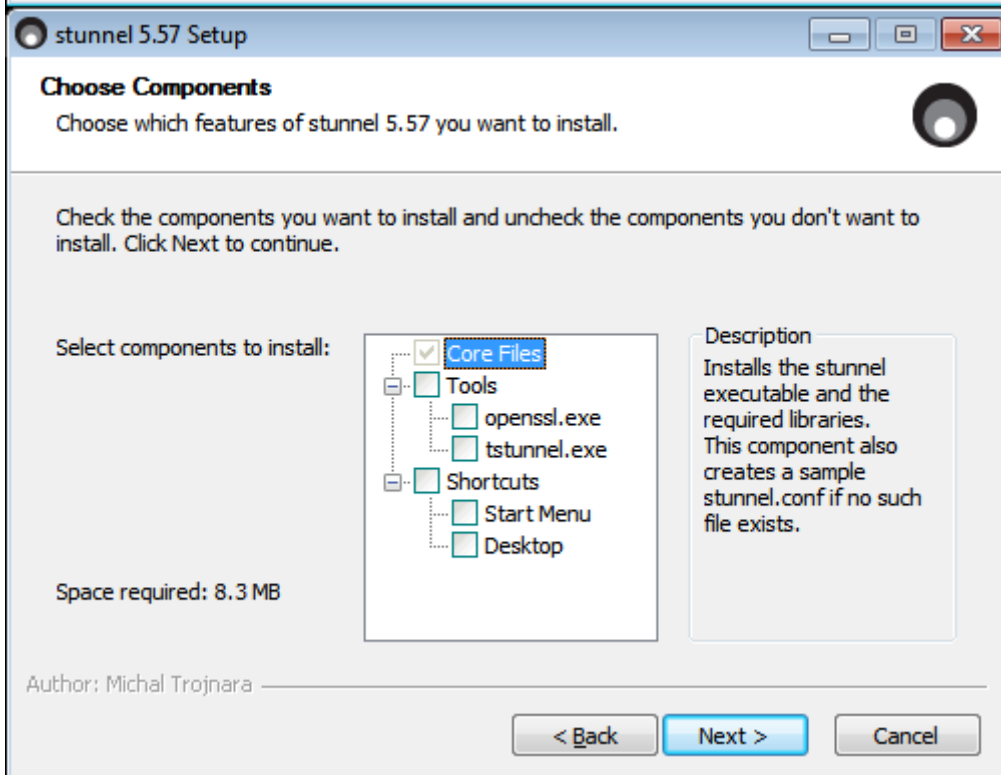
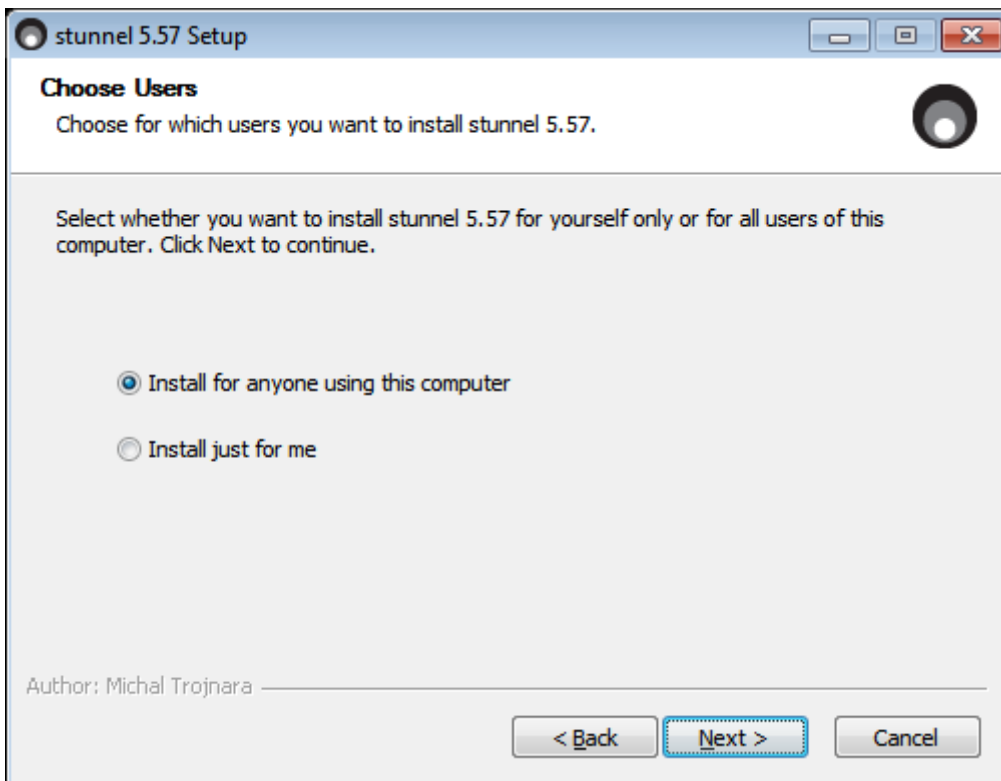
Bei [stunnel](#) handelt es sich um eine Software zum Aufbau eines SSL/TLS-Tunnels, dieser wird zwischen unseren E-Mail-Servern und Ihrem System aufgebaut. Auf Ihrem System stellt „stunnel“ anschließend den SMTP-Dienst auf dem TCP-Port 587 bereit, so dass Sie den SMTP-Versand in Ihrer Software auf den Server „127.0.0.1“ mit Port 587 - ohne Verschlüsselung - umstellen müssen. Sollten Sie eine Anti-Viren-Software einsetzen, müssen Sie gegebenenfalls entsprechende Ausnahmen hinzufügen.

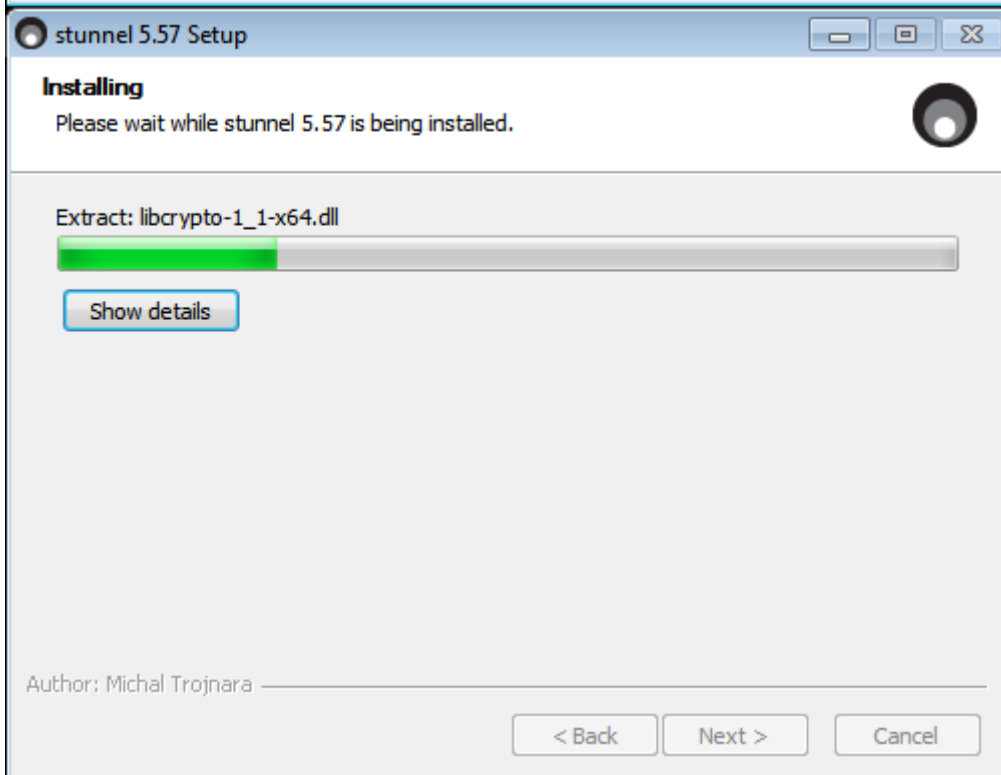
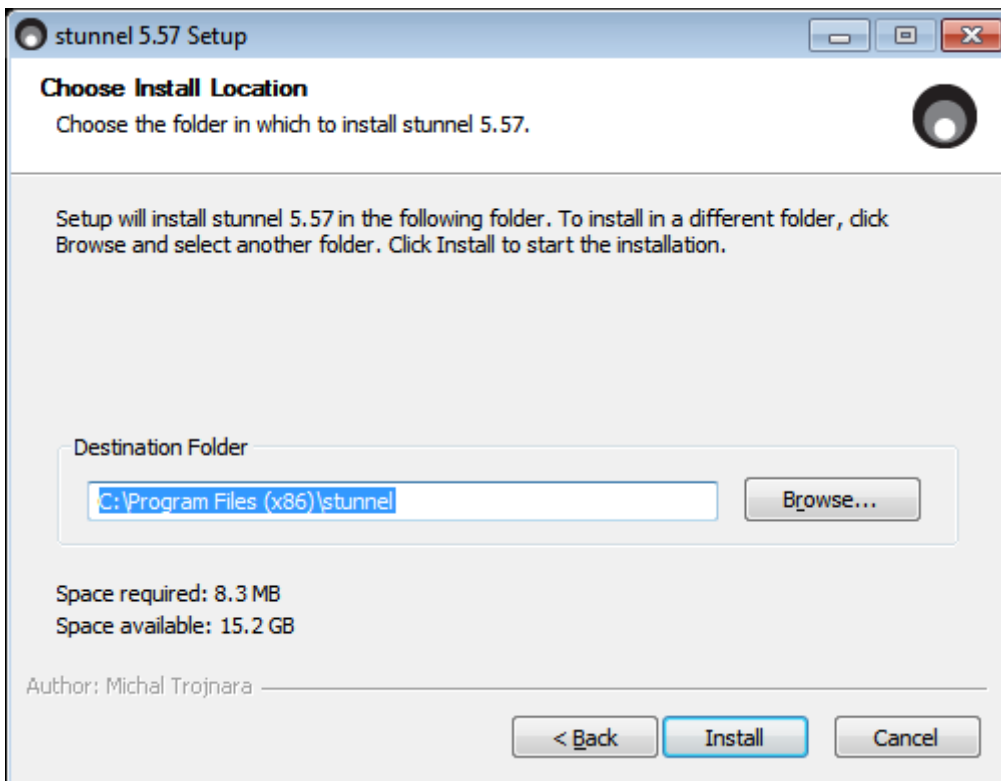
Wichtig: Auch „stunnel“ muss gelegentlich aktualisiert werden, da auch diese Software mit der Zeit Sicherheitslücken aufweisen oder veraltet sein kann. Beziehen Sie damit auch „stunnel“ in Ihre regelmäßigen Sicherheitsupdates mit ein!

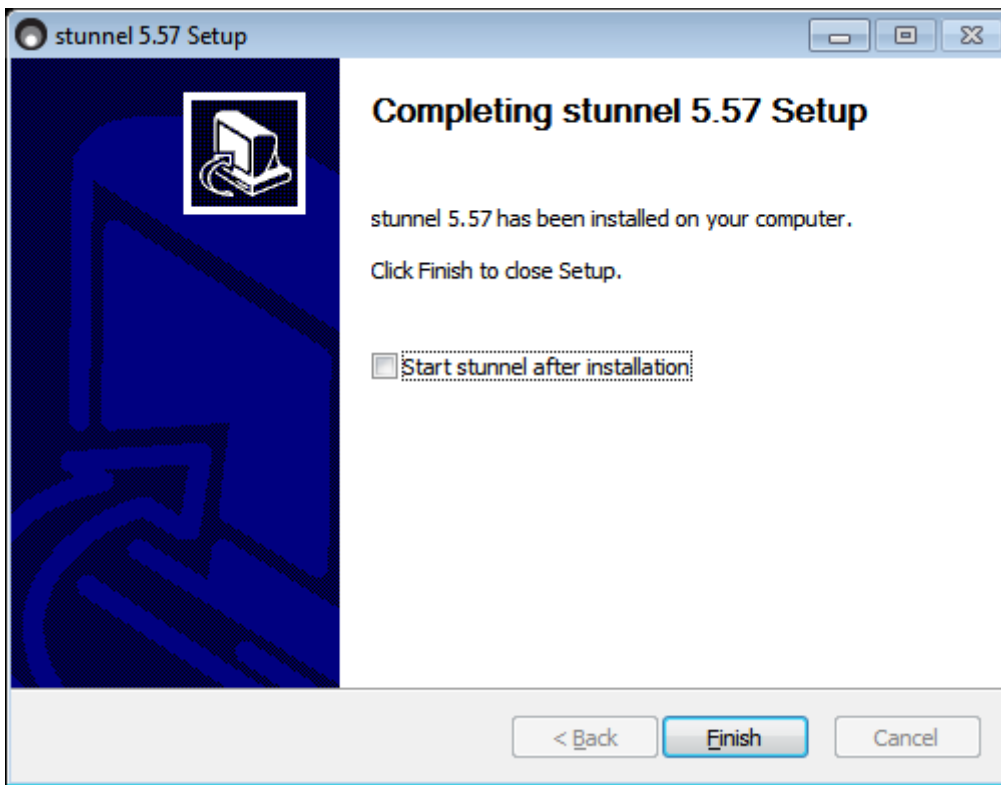
Installation von stunnel

Bitte laden Sie als erstes den MSI-Installer der Software „stunnel“ unter <https://www.stunnel.org/downloads.html> herunter und installieren Sie diese genau wie auf den nachfolgenden Screenshots geschildert.

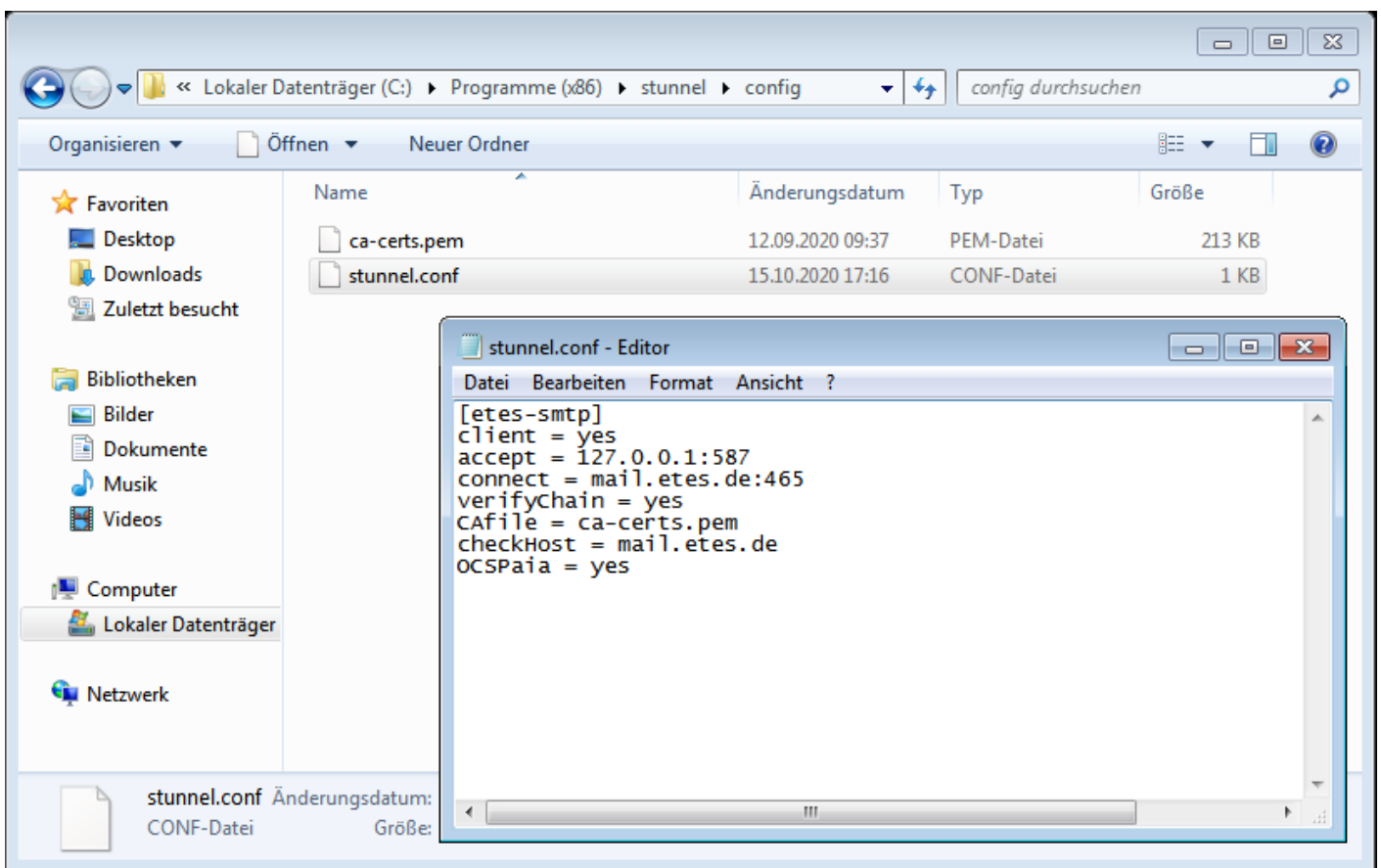








Konfiguration von stunnel



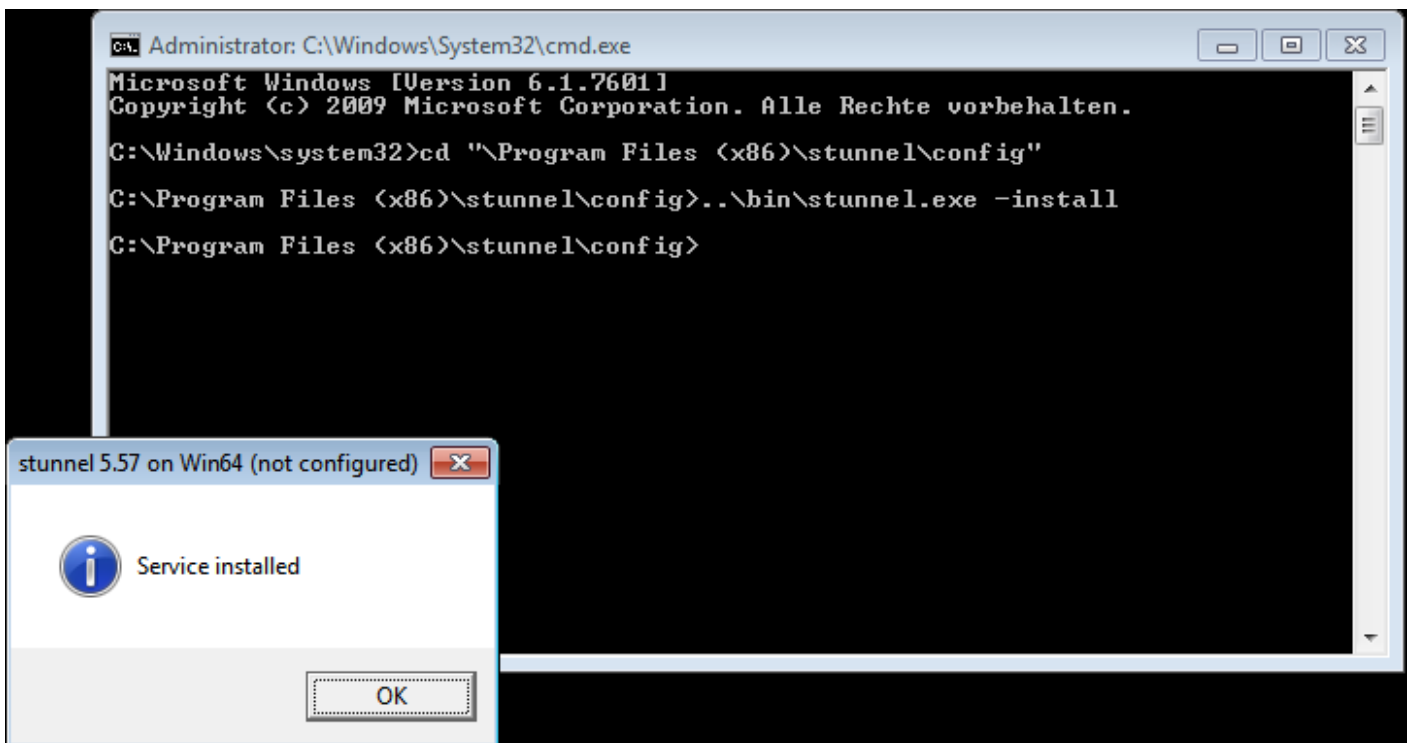
Öffnen Sie die Konfigurationsdatei `C:\Programme (x86)\stunnel\config\stunnel.conf` (32 Bit-System) bzw. `C:\Programme\stunnel\config\stunnel.conf`

(64 Bit-System) mit Administrator-Rechten mit einem Texteditor (z.B. `notepad.exe`), löschen Sie die bisherige Beispielkonfiguration und fügen Sie nur nachfolgenden Inhalt ein:

```
[etes-smtp]
client = yes
accept = 127.0.0.1:587
connect = mail.etes.de:465
verifyChain = yes
CAfile = ca-certs.pem
checkHost = mail.etes.de
OCSPaia = yes
```

Sollten Sie als E-Mail-Server statt „mail.etes.de“ derzeit „mailout.etes.de“ verwenden, verwenden Sie an dieser Stelle an beiden Stellen bitte ebenfalls „mailout.etes.de“.

Speichern Sie die Änderungen an der Konfigurationsdatei anschließend.



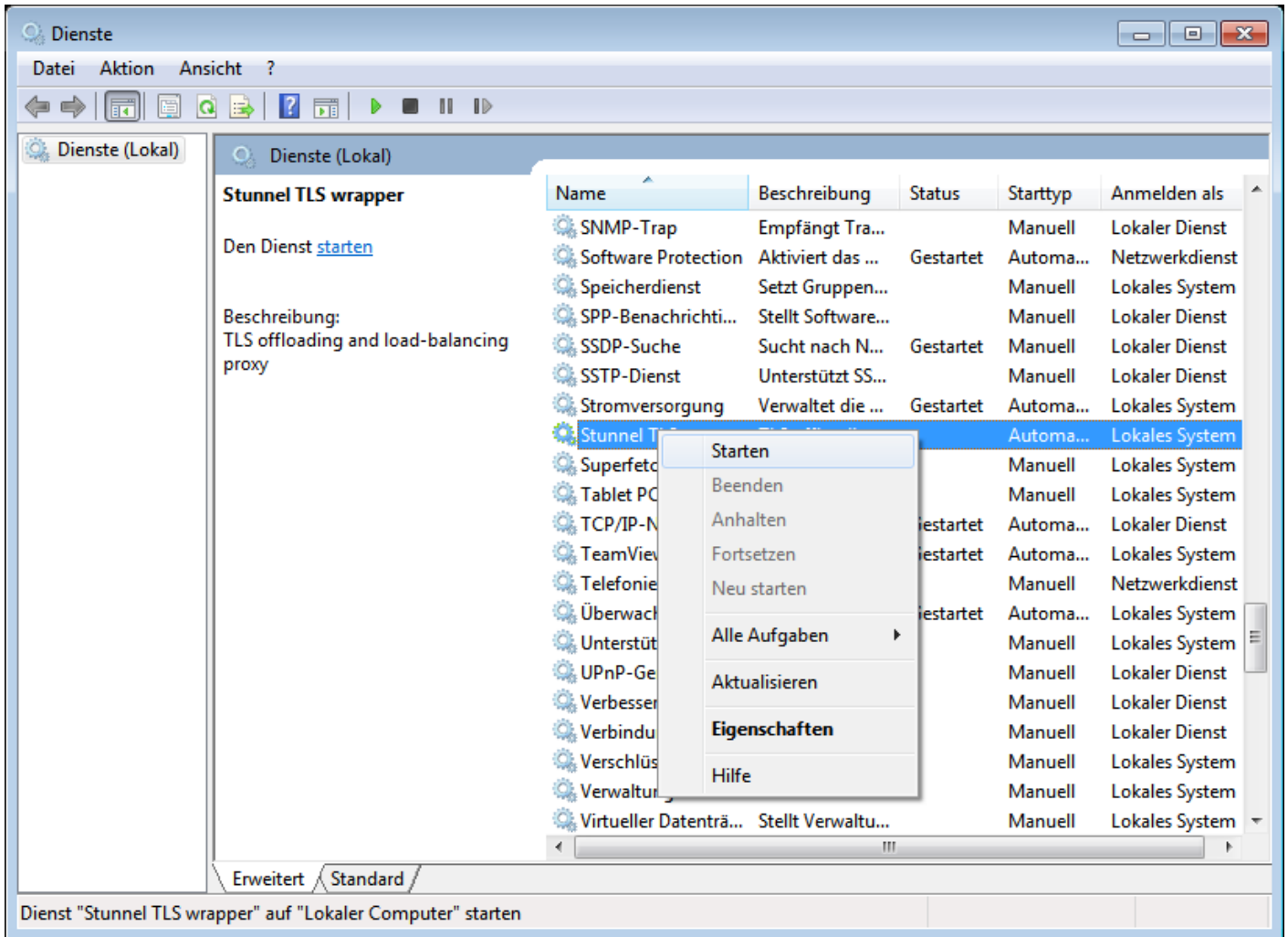
Führen Sie anschließend eine Eingabeaufforderung (`cmd.exe`) mit Administrator-Rechten aus und geben Sie die folgenden Befehle ein:

```
cd "%Program Files (x86)\stunnel\config"
```

Sollten Sie „stunnel“ auf einem abweichenden Pfad installiert haben, geben Sie natürlich hier bitte den abweichenden Pfad an.

```
..\bin\stunnel.exe -install
```

Danach erscheint, wie auf dem Screenshot angezeigt, eine Bestätigungsmeldung, welche Sie mit „OK“ wegeklicken können.



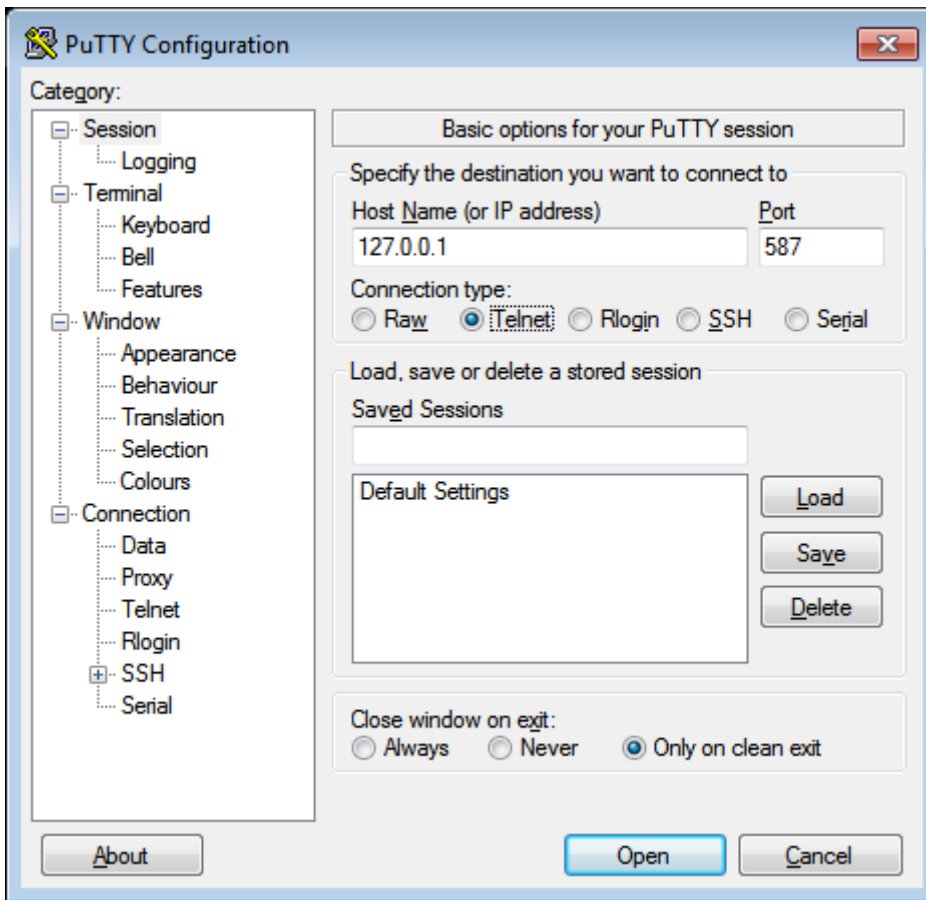
Im letzten Schritt öffnen Sie bitte die Verwaltung der Dienste (`services.msc`) und starten Sie den Dienst „Stunnel TLS wrapper“ mit einem Rechtsklick und im erscheinenden Kontextmenü mit „Starten“.

Hat alles geklappt, stellt „stunnel“ jetzt den SMTP-Dienst auf dem TCP-Port 587 bereit, so dass Sie den SMTP-Versand in Ihrer Software auf den Server „127.0.0.1“ mit Port 587 - ohne Verschlüsselung - umstellen müssen. Sollten Sie eine Anti-Viren-Software einsetzen, müssen Sie gegebenenfalls entsprechende Ausnahmen hinzufügen.

Wichtig: Auch „stunnel“ muss gelegentlich aktualisiert werden, da auch diese Software mit der Zeit Sicherheitslücken aufweisen oder veraltet sein kann. Beziehen Sie damit auch „stunnel“ in Ihre regelmäßigen Sicherheitsupdates mit ein!

Sollten Sie Probleme haben oder die Konfiguration manuell prüfen wollen, so finden Sie im nachfolgenden Abschnitt dazu weiterführende Informationen.

Test der stunnel-

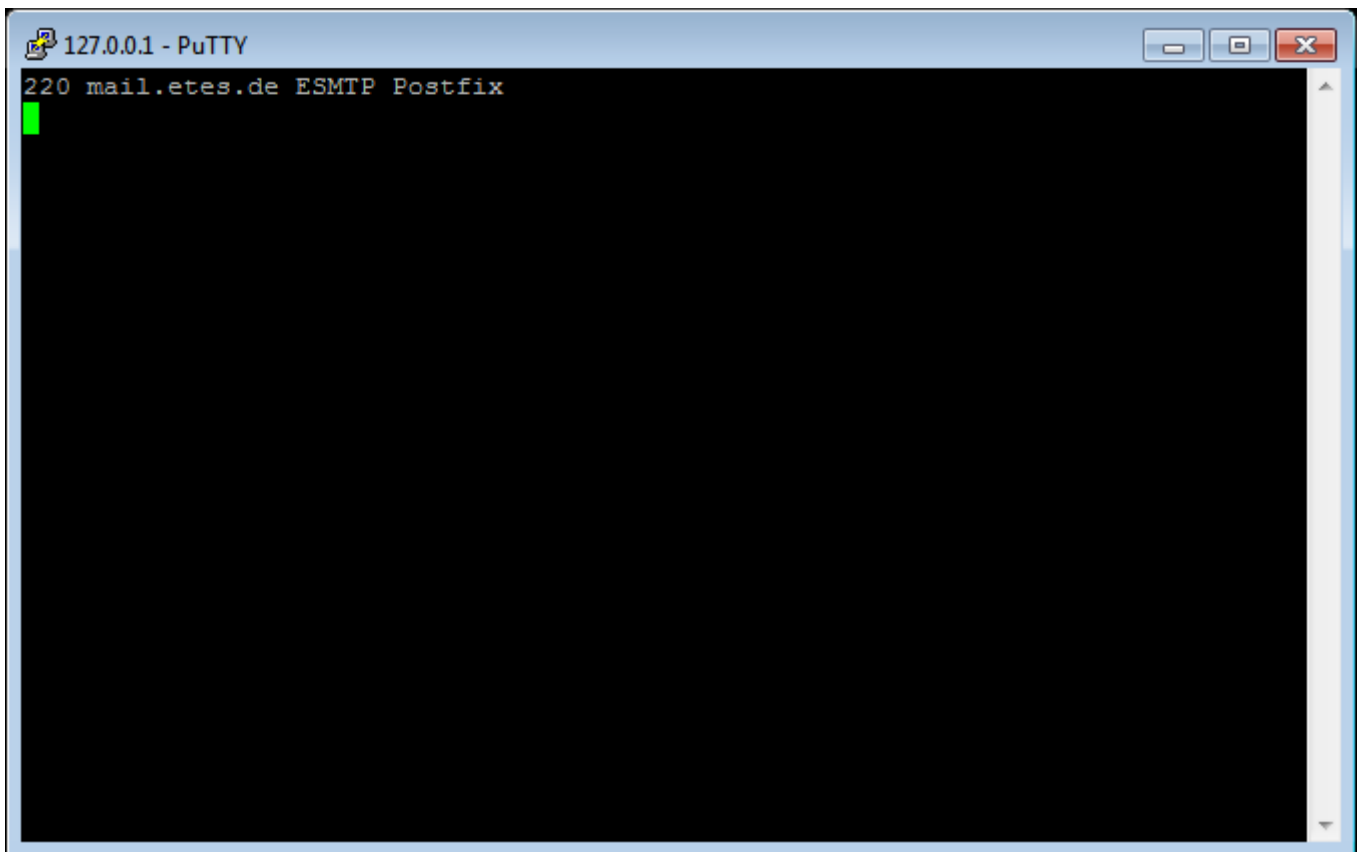


Mittels PuTTY oder

```
telnet 127.0.0.1 587
```

können Sie überprüfen, ob der SSL/TLS-Tunnel von Ihrem System zu unseren E-Mail-Servern korrekt aufgebaut wird.

Bei der Verwendung von PuTTY geben Sie als „Host Name (or IP address)“ die „127.0.0.1“ an, tragen als Port „587“ ein und stellen den „Connection type“ auf „Telnet“. Anschließend klicken Sie auf „Open“.



Unabhängig ob `telnet.exe` oder PuTTY verwendet wurden, wird Ihnen im Erfolgsfall

```
220 <server>.etes.de ESMTP Postfix
```

angezeigt, wobei der genaue Name des angezeigten E-Mail-Servers je Versuch variieren kann.

Revision #3

Created 14 February 2023 12:34:04 by Paul Vaßen

Updated 14 February 2023 12:36:05 by Paul Vaßen