Häufig gestellte Fragen (FAQ)

Account Sperrung

Problembeschreibung / Symptome

Aus Sicherheitsgründen bekommen Sie keinen Hinweis auf einen gesperrten E-Mail Account. Je nach dem, welchen Mailclient Sie verwenden, erkennen Sie dies jedoch an folgenden Symptomen.

Webclient

Verwenden Sie den Webclient über https://mail.etes.de kann ein gesperrter Account folgende Symptome aufweisen:

- Eine vermeintlich falsche Eingabe des Nutzernamen oder Passworts:

- Fehler im Netzwerkdienst:

Problembehebung

Um einen E-Mail Account zu entsperren, schreiben Sie uns eine E-Mail mit Informationen zu dem betroffenen Account an support@etes.de oder rufen uns an unter 0711 / 48 90 83– 0.

In Zukunft werden Sie auch über Ihren Kundenzugang auf https://my.etes.de in der Lage sein, E-Mail Accounts zu entsperren. Aktuell ist dies jedoch nicht möglich.

Ursachen

Einer Sperrung des E-Mail Accounts liegen drei Ursachen zu Grunde:

1. **Gewollter Sperrung**
   Eventuell wurde der Account aufgrund eines ausgeschiedenen Mitarbeiters o.Ä. absichtlich gesperrt.
2. **Sperrung durch den Nutzer**
   Sie haben zu oft ein falsches Passwort verwendet. Am naheliegendsten ist natürlich eine falsche Eingabe. Ein Mailclient, der ein veraltetes Passwort hinterlegt hat kann z.B. auch der Grund sein.
3. **Sperrung durch Dritte**
   Unbefugte, die sich Zugang zu Ihrem E-Mail Account verschaffen wollen, verwenden oft eine *Brute Force Attacke*. Dabei werden so lange verschiedene Passwörter ausprobiert, bis das richtige Passwort gefunden wird.
   Um solchen Angriffen entgegen zu wirken, wird Ihr E-Mail Account nach einer bestimmten Anzahl von Fehlerversuchen für eine gewisse Zeit gesperrt.

Was tun bei Spam?

Bei ETES Groupware gibt es einen von uns kontinuierlich gepflegten und stetig erweiterten Spam- und Viren-Filter. Trotz aller Bemühungen und Mechanismen kommt es dennoch manchmal vor, dass Spam- E-Mails in Ihr Postfach zugestellt werden. In solchen Situationen sind wir auf Ihre Unterstützung angewiesen, indem Sie uns diese Spam-E-Mails melden und zur Verfügung stellen.

Spam richtig melden

Falls Sie Spam erhalten, leiten Sie uns bitte die Mails **als Anhang** per Mail an **report-spam@etes.de** weiter.

Folgend verschiedene Anleitungen für das Weiterleiten der Mail als Anhang für die jeweiligen Clients:

Zimbra-Webclient

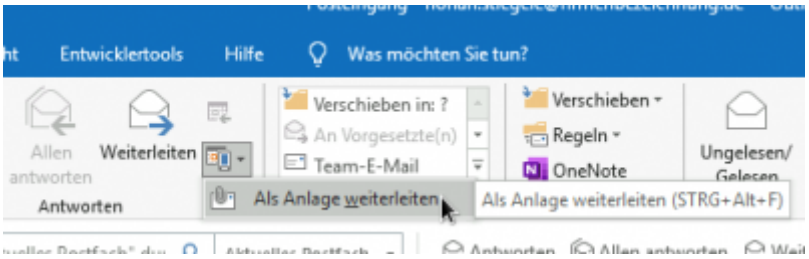
- Um im Zimbra-Webclient eine Mail als Anhang weiterzuleiten, verfassen Sie eine neue Mail und gehen Sie dann auf Anhang und dort auf Mail.

- Nun können Sie in Ihrem Postfach alle Mails auswählen, die Sie uns in Bezug auf Spam melden wollen.

Outlook

In Outlook gibt es mehrere Möglichkeiten die betroffenen Mails als Anhang zu versenden.

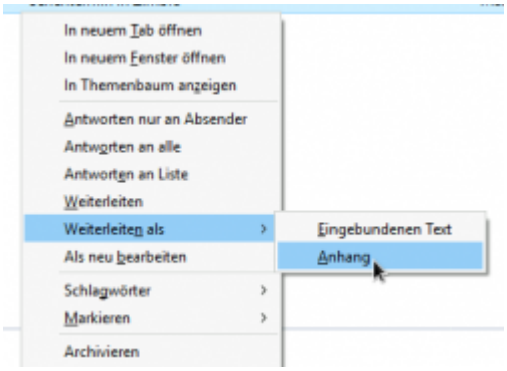
1. Zum einen können Sie alle Mails markieren und dann findet sich im Reiter „Start“ neben „Weiterleiten“ unter dem Aufklapp-Pfeil die Funktion „Als Anlage weiterleiten“



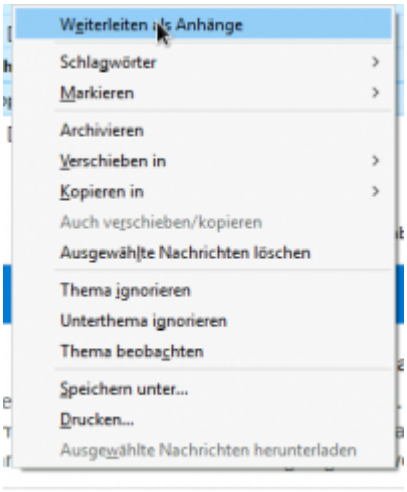
2. Zum anderen ist es auch möglich, eine neue Mail zu verfassen, die betroffenen Mails zu markieren und sie per „Drag-and-drop“ in die Mail zu ziehen.

Thunderbird

1. Für das Weiterleiten einer einzelnen Mail können Sie mit durch Rechtsklick auf die Mail, dann „Weiterleiten als“ und dann „Anhang“ eine neue Mail erstellen die diese Mail als Anhang anhängen.



2. Bei mehreren Mails sieht das ein wenig anders aus. Falls Sie uns mehrere Mails haben, markieren Sie diese und dann können sie per Rechtsklick direkt die Option „Weiterleiten als Anhänge“ auswählen.



3. Ebenfalls kann man auch einfach eine neue Mail erstellen und per „Drag-and-drop“ die Mails als Anhang hinzufügen.

TLSv1.2 (oder neuer) erforderlich

Situation

Zum 1. März 2020 haben wir die für **HTTPS, POP3 und IMAP** verwendeten veralteten SSL/TLS-Verschlüsselungsprotokolle **TLSv1.0 und TLSv1.1 deaktiviert**. Zum 15. Februar 2021 haben wir die gleiche Abschaltung für **SMTP** (für den Versand von E-Mails über die TCP-Ports 465 bzw. 587) vorgenommen. Somit kann auf unsere authentifizierten E-Mail-Dienste seit dem 15. Februar 2021 ausschließlich über das SSL/TLS-Verschlüsselungsprotokoll TLSv1.2 (oder neuer) zugegriffen werden.

Technisch begründet wird die Mindestanforderung von TLSv1.2 z.B. durch RFC 7525 bzw. PCI DSS. Darüber hinaus haben wir die bei TLSv1.2 möglichen Cipher-Suites auf die nachfolgenden beschränkt; diese bieten alle Perfect Forward Secrecy und Authenticated Encryption und erfüllen damit die von TLSv1.3 verpflichtend geforderten Eigenschaften.

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256

Probleme

Allerdings haben Microsoft **Windows 7 SP1 und 8** als auch Microsoft **Windows Server 2008 R2 und 2012** standardmäßig **TLSv1.2 nicht aktiviert** ist und somit schlägt unter Umständen der **Zugriff** auf die Groupware-Cloud **mittels Microsoft Outlook fehl**. Bei Microsoft Windows 8.1 und 10 bzw. Microsoft Windows Server 2016 und 2019 ist TLSv1.2 bereits standardmäßig aktiviert, so dass hierbei kein Handlungsbedarf erforderlich ist.

Ähnlich verhält es sich bei macOS (auch: Mac OS X bzw. OS X): TLSv1.2 wird **erst seit macOS Sierra (10.12.6) bzw. High Sierra (10.13)** unterstützt, insbesondere wenn Sie die vom

Betriebssystem mitgelieferte E-Mail-Software „Mail“ verwenden.

Umgehung

Sollten Sie auf unsere **Groupware-Cloud mittels Microsoft Outlook in Verbindung mit einer älteren Windows-Version zugreifen**, bitten wir Sie den **Microsoft Easy Fix 51044 (MSI-Datei) sowie die Registry-Anpassung (REG-Datei) einzuspielen**. Starten Sie bitte nach dem Einspielen beider Anpassungen Ihr Microsoft Outlook neu; anschließend sollte der Zugriff wieder funktionieren.

Lösung

Da Microsoft Windows 7 SP1 und Microsoft Windows 2008 R2 seitens Microsoft bereits zum 14. Januar 2020 eingestellt wurden, sollte ein Wechsel auf eine neuere Windows-Version unbedingt erfolgen sollte, da Sie bereits seit zuvor genanntem Datum keine Sicherheitsupdates mehr erhalten.

Bei macOS (auch: Mac OS X bzw. OS X) wurde macOS Sierra (10.12) bereits im Oktober 2019 eingestellt und macOS High Sierra (10.13) ist im Dezember 2020 eingestellt worden. Noch ältere Betriebssystem-Versionen wie OS X El Capitan (10.11), Yosemite (10.10), Mavericks (10.9), Mountain Lion (10.8) oder Lion (10.7) unterstützen gar keine moderne Verschlüsselung. Auch hier sollte ein Wechsel auf eine aktuelle Version unbedingt erfolgen, da Sie bei diesen Betriebssystem-Versionen, teilweise bereits seit vielen Jahren, keine Sicherheitsupdates mehr erhalten.

Siehe auch

- Zu altes System/Mail-Client (für SMTP)
- Microsoft-Update bei Groupware-Cloud-Benutzern erforderlich

Mailversand per Starface

Die VoIP-Telefonanlage Starface nutzt in Version 6.7 das Linux-Betriebssystem CentOS 6.10 (als Nachbau von Red Hat Enterprise Linux 6.10, welches von Red Hat als Hersteller zum 30.11.2020 eingestellt wurde). Der dabei standardmäßig mitgelieferte Postfix unterstützt in der Standardkonfiguration kein TLSv1.2 für ausgehende SMTP-Verbindungen, so dass der Mailversand per SMTP über unsere E-Mail-Server nicht funktioniert.

Wichtig: Diese manuelle Anpassung ist nicht updatesicher, d.h. nach einem Update von Starface muss diese wiederholt werden - so lange, bis Starface eine neue Version veröffentlicht, die nicht mehr auf CentOS 6 basiert.

Mittels einer SSH-Verbindung mit `root`-Rechten können Sie mit wenigen Schritten die Postfix-Konfiguration zumindest manuell so anpassen, dass beim SMTP-Versand zumindest TLSv1.2 verwendet wird:

- `postconf -e 'smtp_tls_mandatory_protocols = !SSLv2'`
- `/etc/init.d/postfix restart`
- Test des Mailversands per Starface durchführen

Die generelle Problematik wurde auch vor der Einstellung von Red Hat Enterprise Linux 6 an Red Hat gemeldet, allerdings wurde aufgrund der Einstellung des Produkts und der oben geschilderten alternativen Konfigurationsmöglichkeit kein Update mehr hierfür veröffentlicht.

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

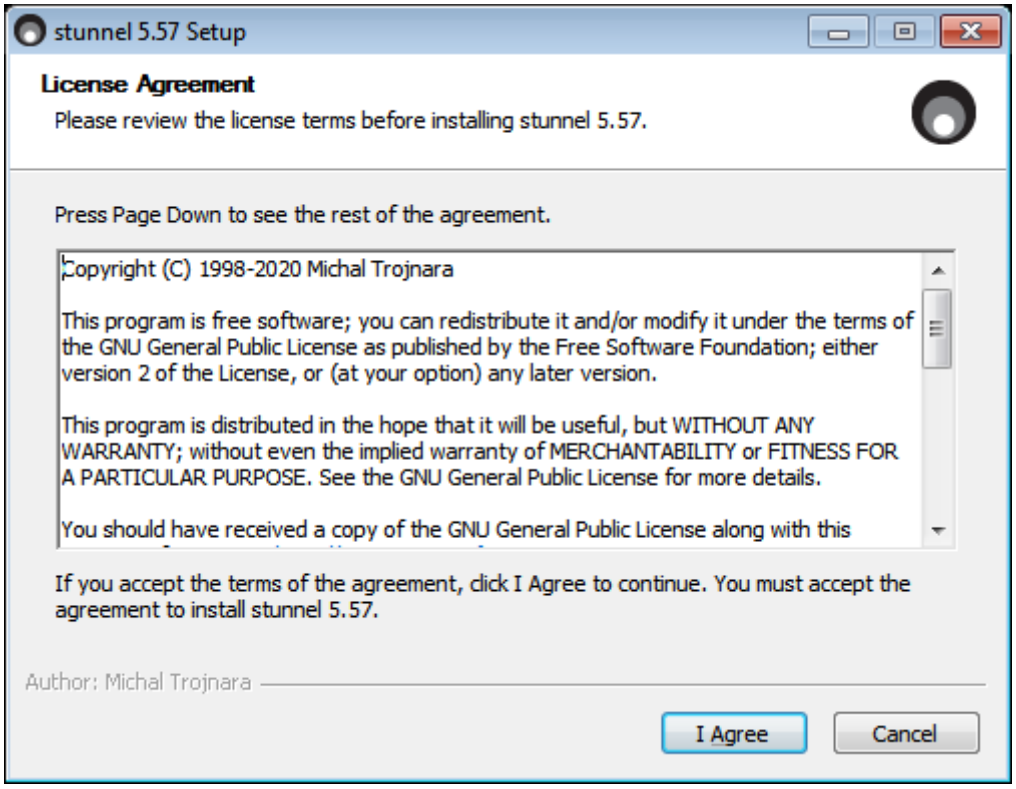
Bei stunnel handelt es sich um eine Software zum Aufbau eines SSL/TLS-Tunnels, dieser wird zwischen unseren E-Mail-Servern und Ihrem System aufgebaut. Auf Ihrem System stellt „stunnel“ anschließend den SMTP-Dienst auf dem TCP-Port 587 bereit, so dass Sie den SMTP-Versand in Ihrer Software auf den Server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

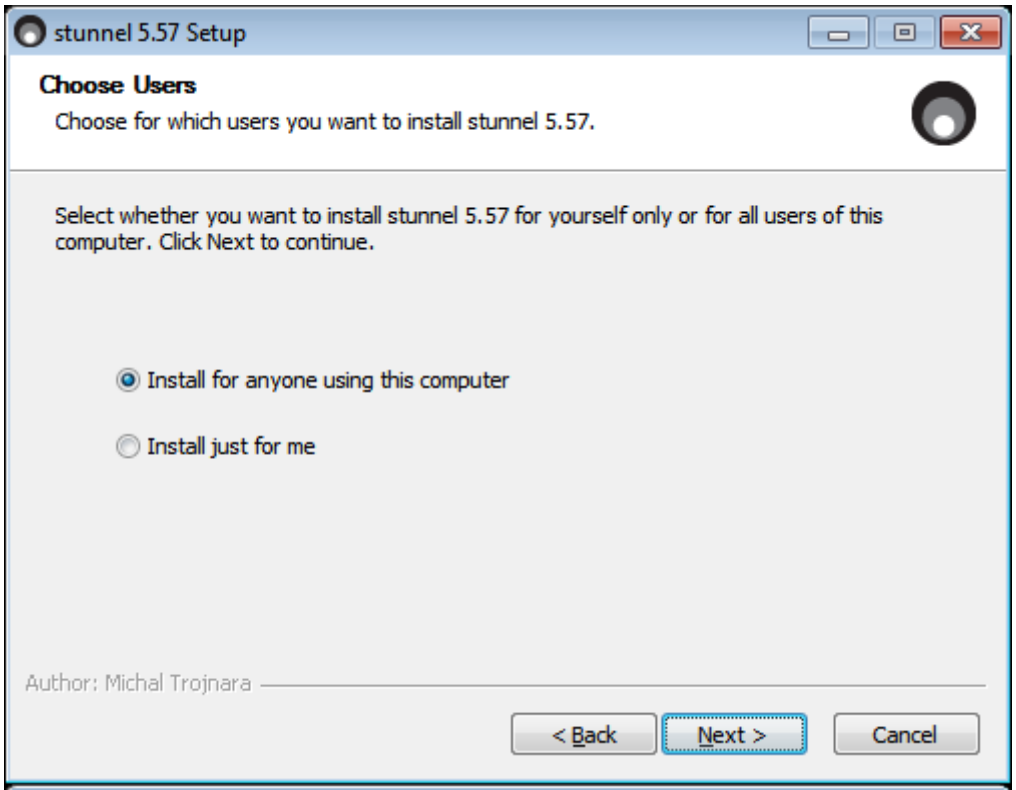
Wichtig: Auch „stunnel“ muss gelegentlich aktualisiert werden, da auch diese Software mit der Zeit Sicherheitslücken aufweisen oder veraltet sein kann. Beziehen Sie damit auch „stunnel“ in Ihre

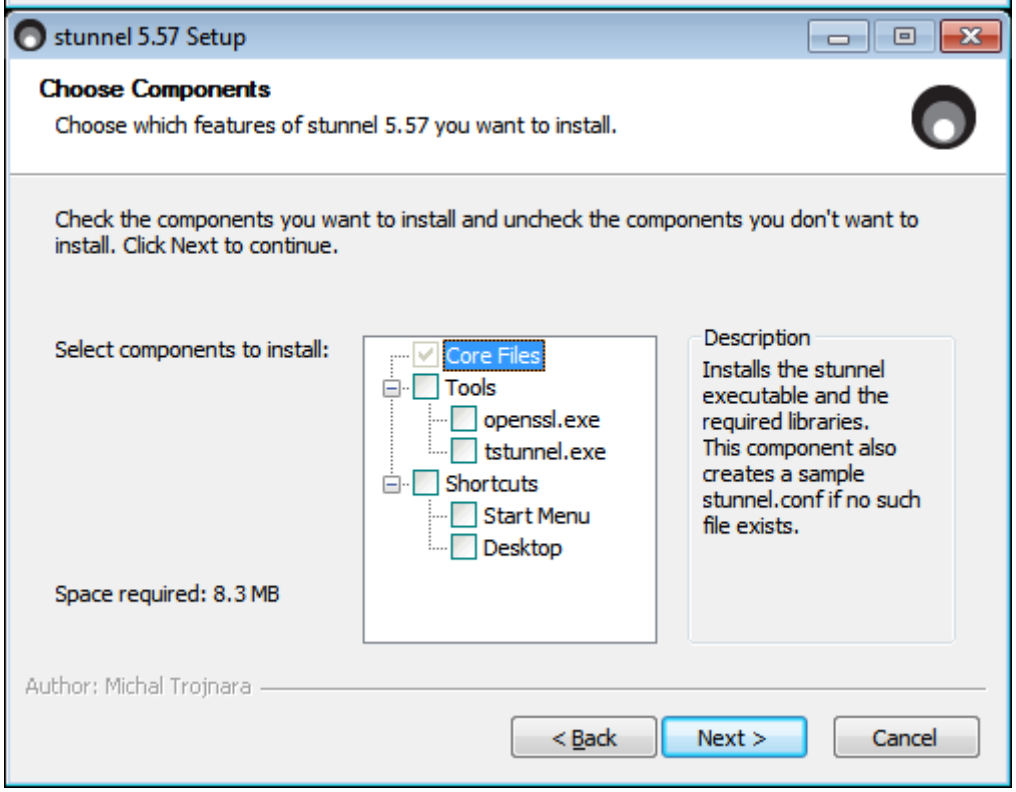
regelmäßigen Sicherheitsupdates mit ein!

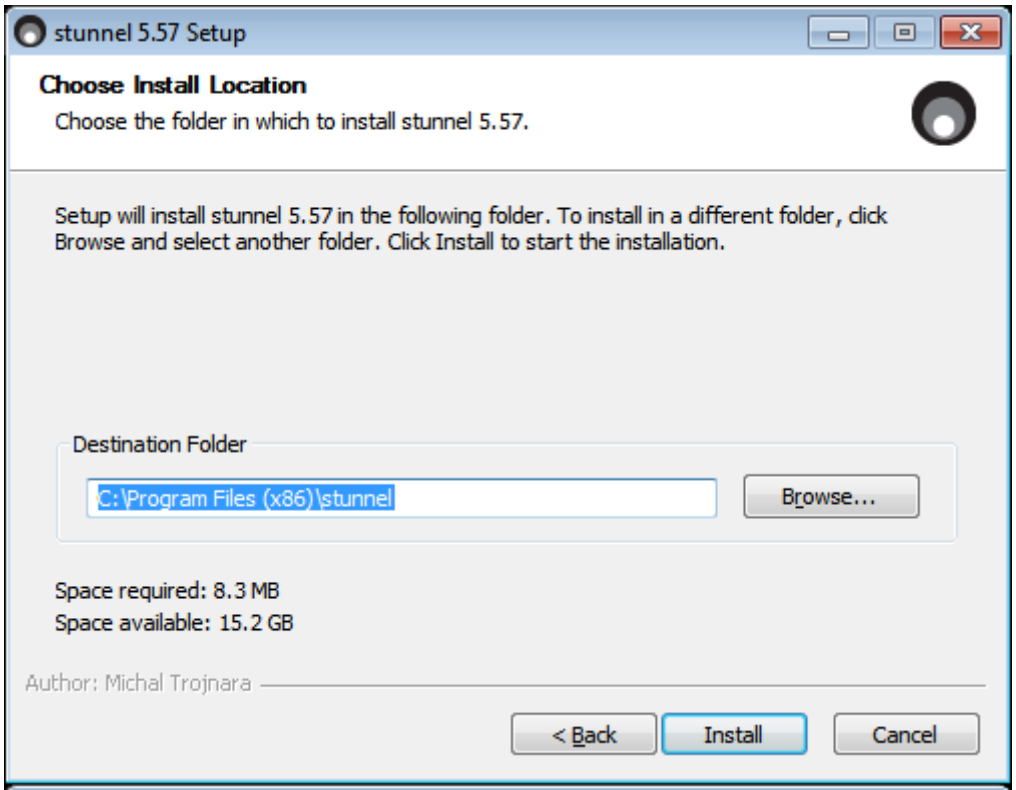
Installation von stunnel

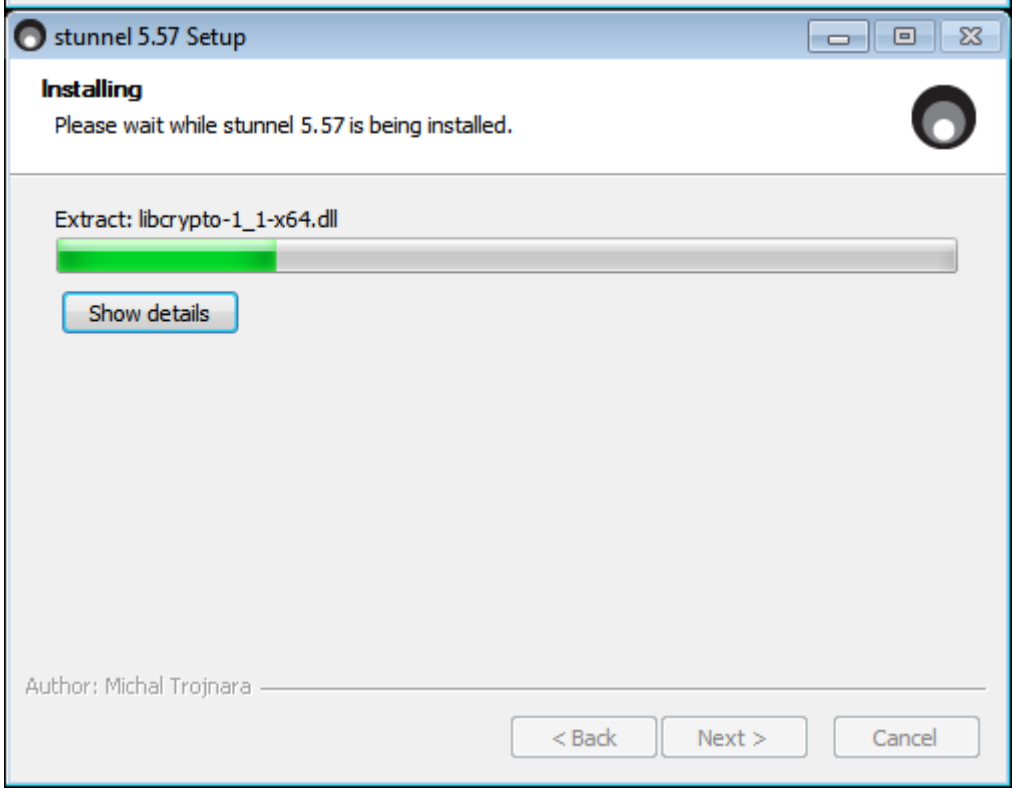
Bitte laden Sie als erstes den MSI-Installer der Software „stunnel“ unter https://www.stunnel.org/downloads.html herunter und installieren Sie diese genau wie auf den nachfolgenden Screenshots geschildert.

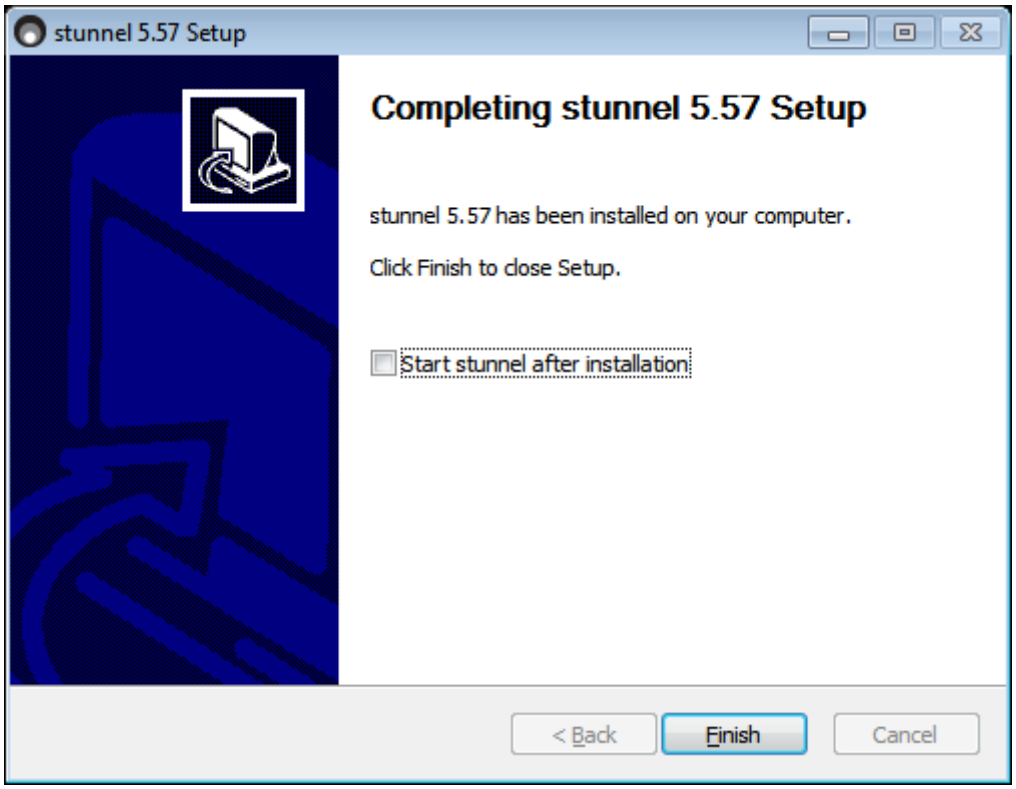
- 


stunnel 5.57 Setup
Choose Users
Choose for which users you want to install stunnel 5.57.
Select whether you want to install stunnel 5.57 for yourself only or for all users of this computer. Click Next to continue.
Install for anyone using this computer
Install just for me
Author: Michal Trojnara
< Back
Next >
Cancel

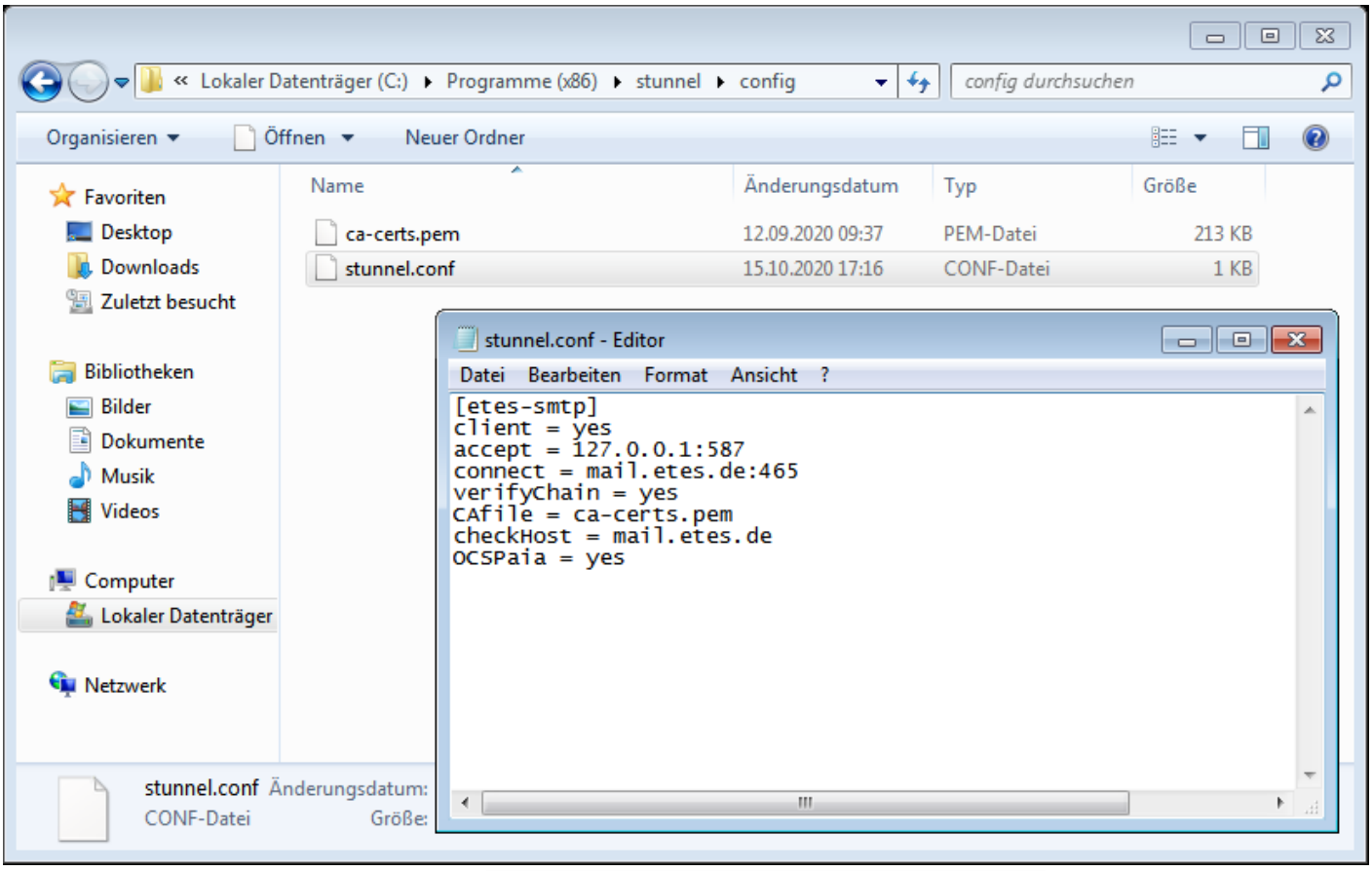

stunnel 5.57 Setup
Choose Components
Choose which features of stunnel 5.57 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Core Files
Tools
openssl.exe
tstunnel.exe
Shortcuts
Start Menu
Desktop
Description
Installs the stunnel executable and the required libraries. This component also creates a sample stunnel.conf if no such file exists.
Space required: 8.3 MB
Author: Michal Trojnara
< Back
Next >
Cancel


stunnel 5.57 Setup
Choose Install Location
Choose the folder in which to install stunnel 5.57.
Setup will install stunnel 5.57 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\stunnel
Browse...
Space required: 8.3 MB
Space available: 15.2 GB
Author: Michal Trojnara
< Back
Install
Cancel


stunnel 5.57 Setup
Installing
Please wait while stunnel 5.57 is being installed.
Extract: libcrypto-1_1-x64.dll
Show details
Author: Michal Trojnara
< Back
Next >
Cancel



Konfiguration von stunnel



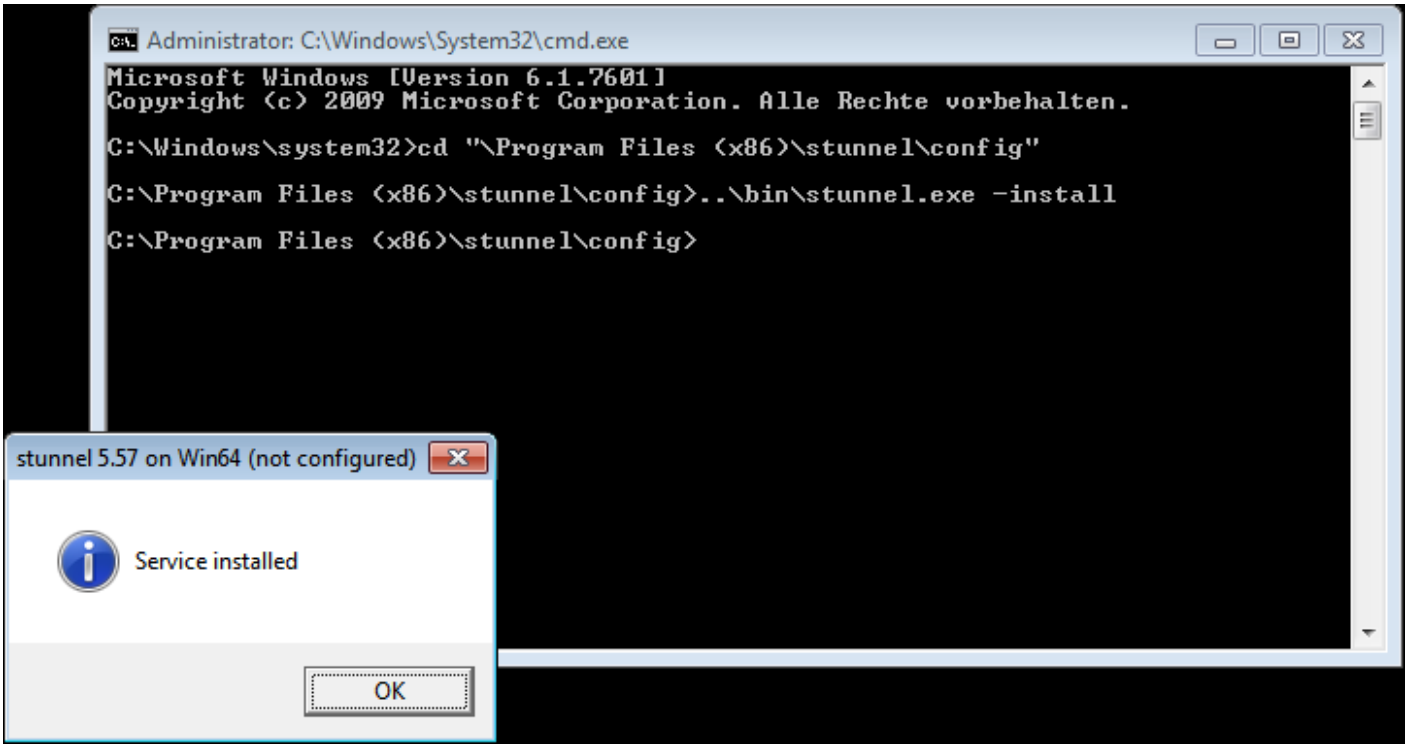
Öffnen Sie die Konfigurationsdatei `C:\Programme (x86)\stunnel\config\stunnel.conf` (32 Bit-System) bzw. `C:\Programme\stunnel\config\stunnel.conf`

(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.



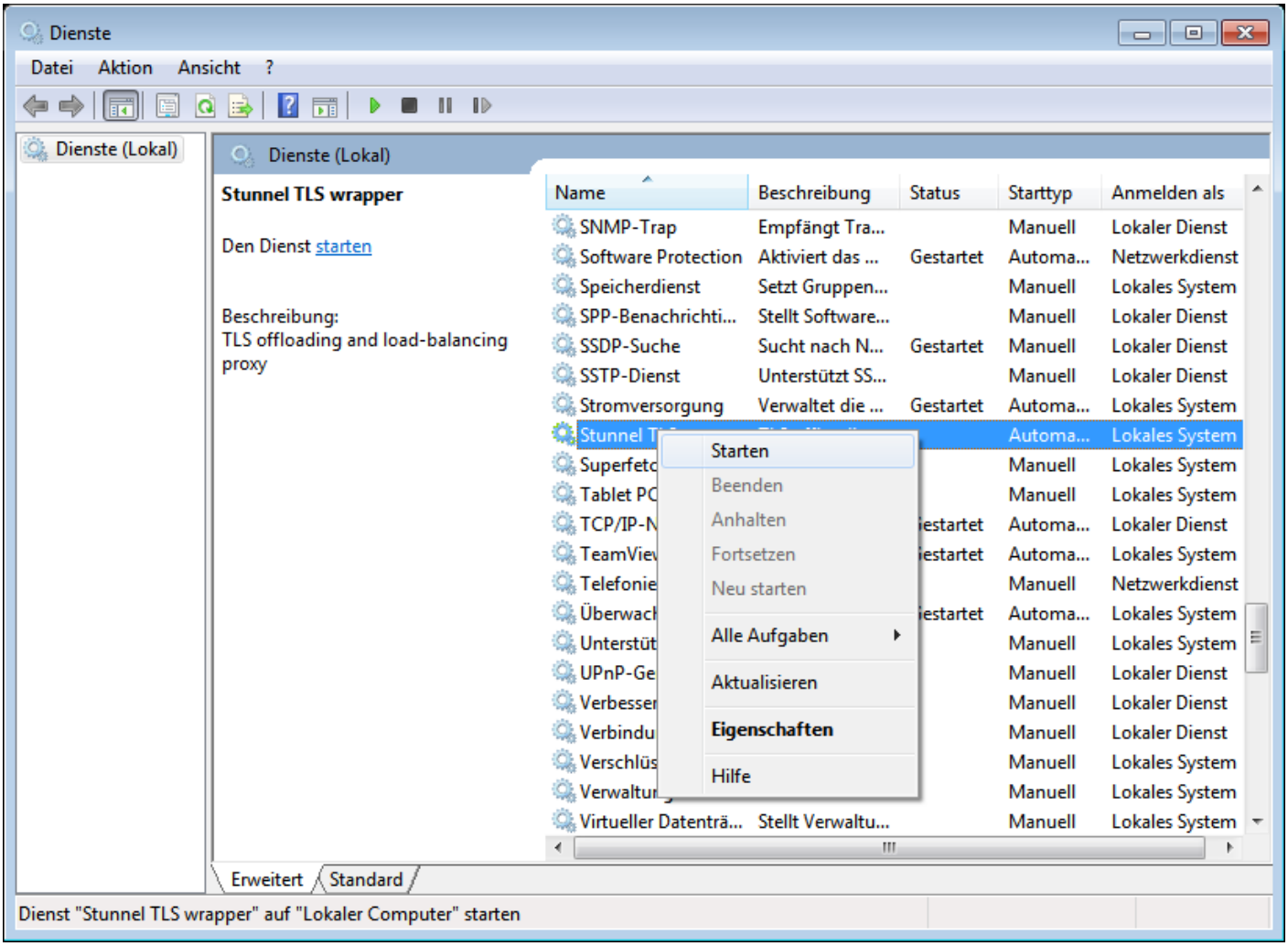
Führen Sie anschließend eine Eingabeaufforderung (`cmd.exe`) mit Administrator-Rechten aus und geben Sie die folgenden Befehle ein:

```
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“ wegklicken können.



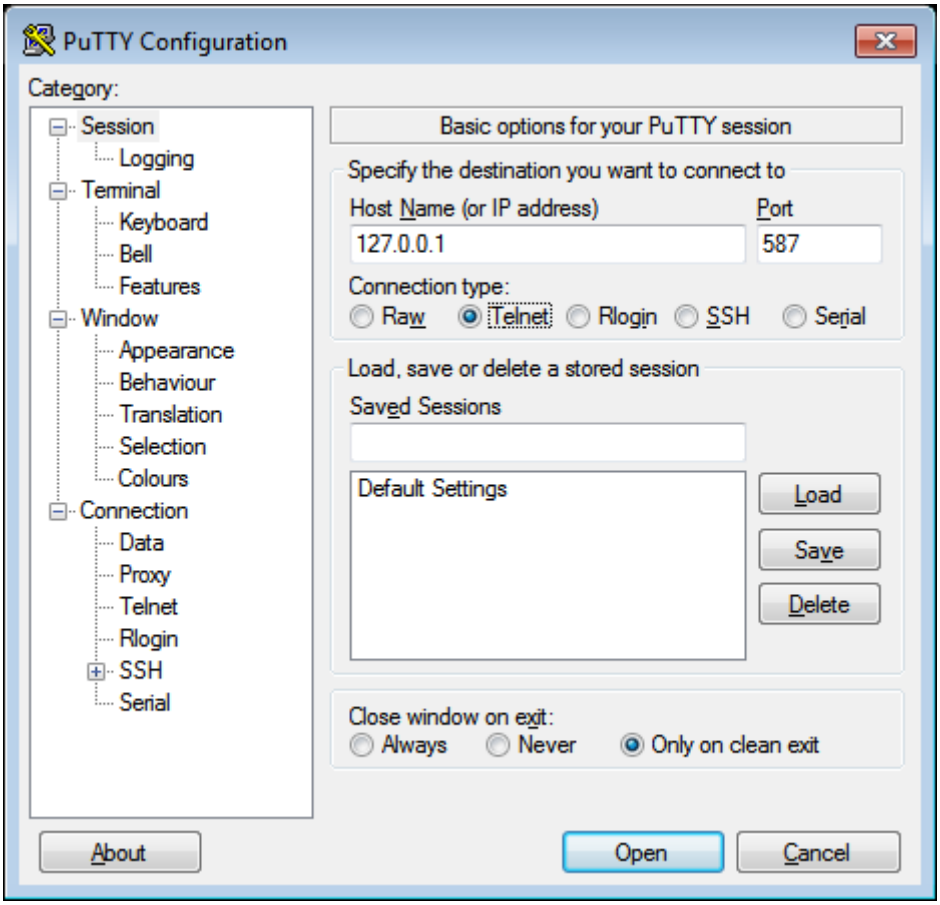
Im letzten Schritt öffnen Sie bitte die Verwaltung der Dienste (`services.msc`) und starten Sie den Dienst „Stunnel TLS wrapper“ mit einem Rechtsklick und im erscheinenden Kontextmenü mit „Starten“.

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-

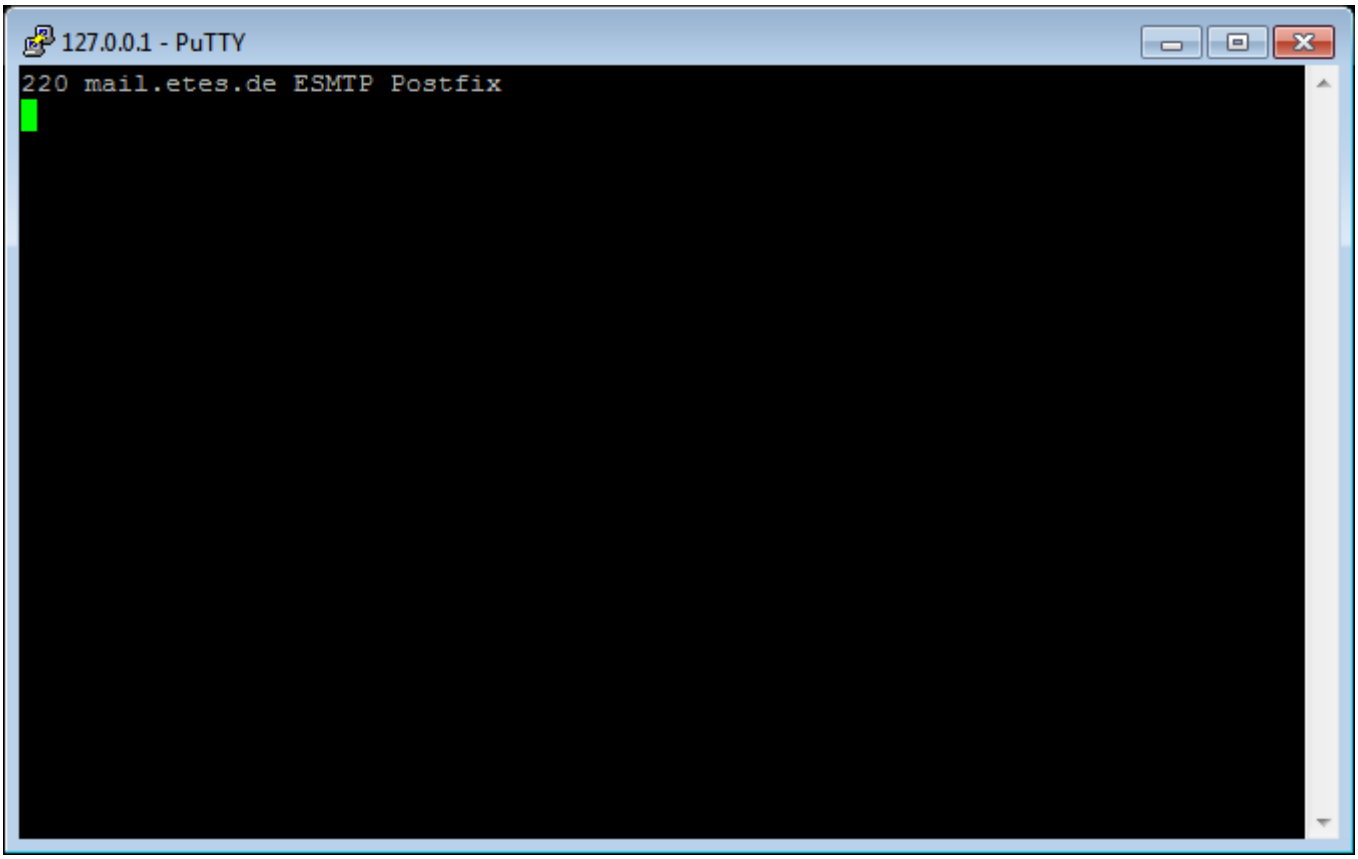


Mittels PuTTY oder

```
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.

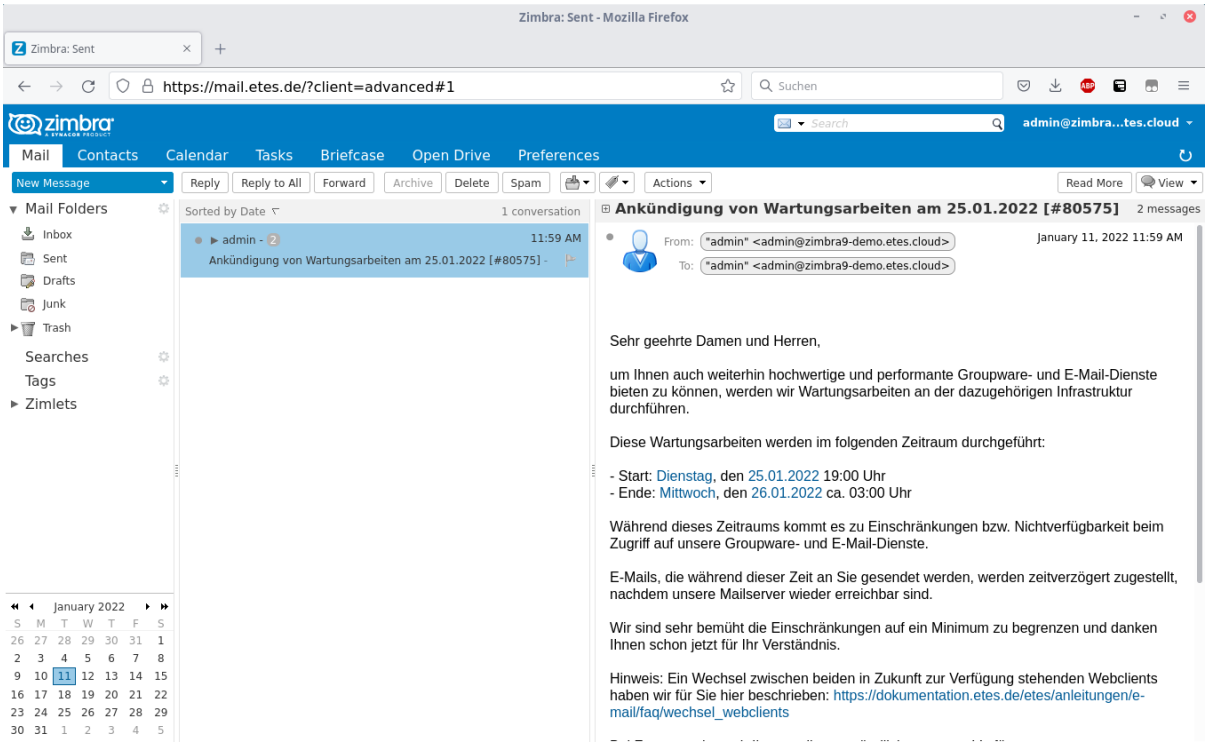
Wechsel zwischen den verschiedenen Webclients

Mit dem Update auf Zimbra 9, welches wir in der Nacht vom 25.01. auf den 26.01.2022 installiert haben, stehen Ihnen zwei Webclients zur Verfügung.

Classic: Unter Zimbra8 als Modern bekannter Webclient, der bisherige HTML-Client entfällt
Modern: Neuer Webclient, wird auch für mobile Endgeräte verwendet. Bietet aktuell noch nicht den vollständigen Funktionsumfang des Classic-Clients

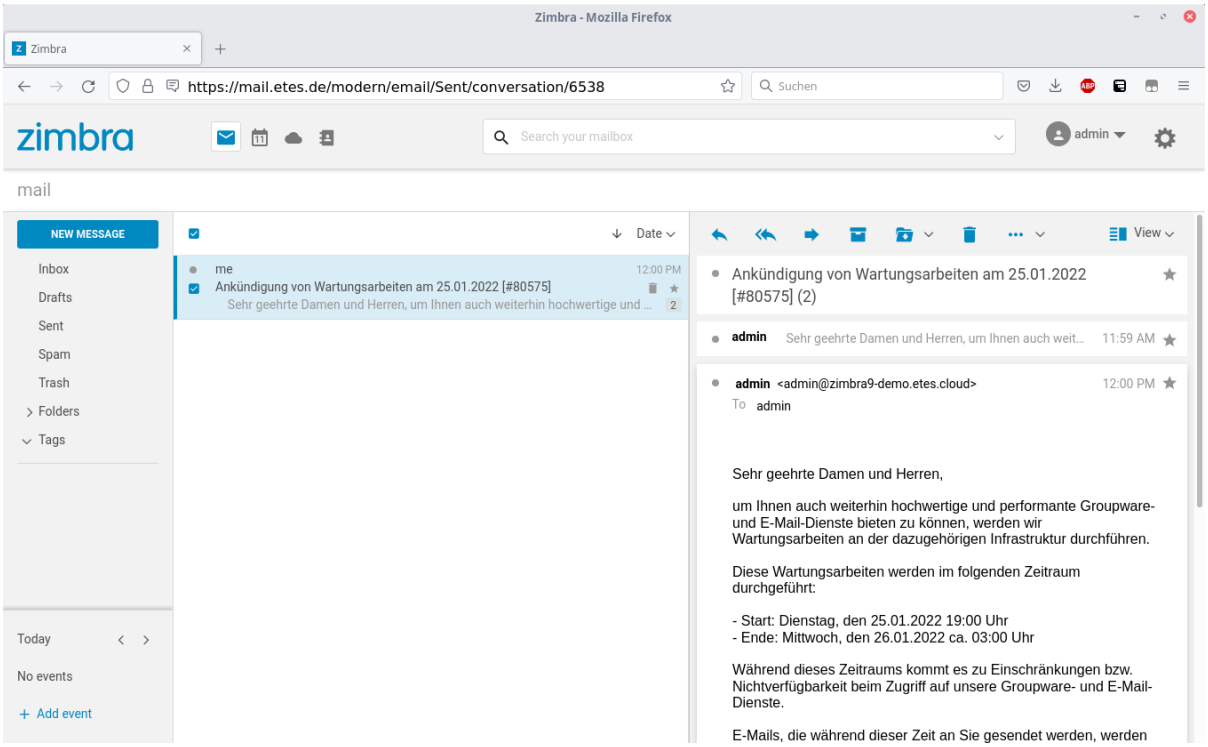
Classic Client

Der Classic Client sieht wie folgt aus:



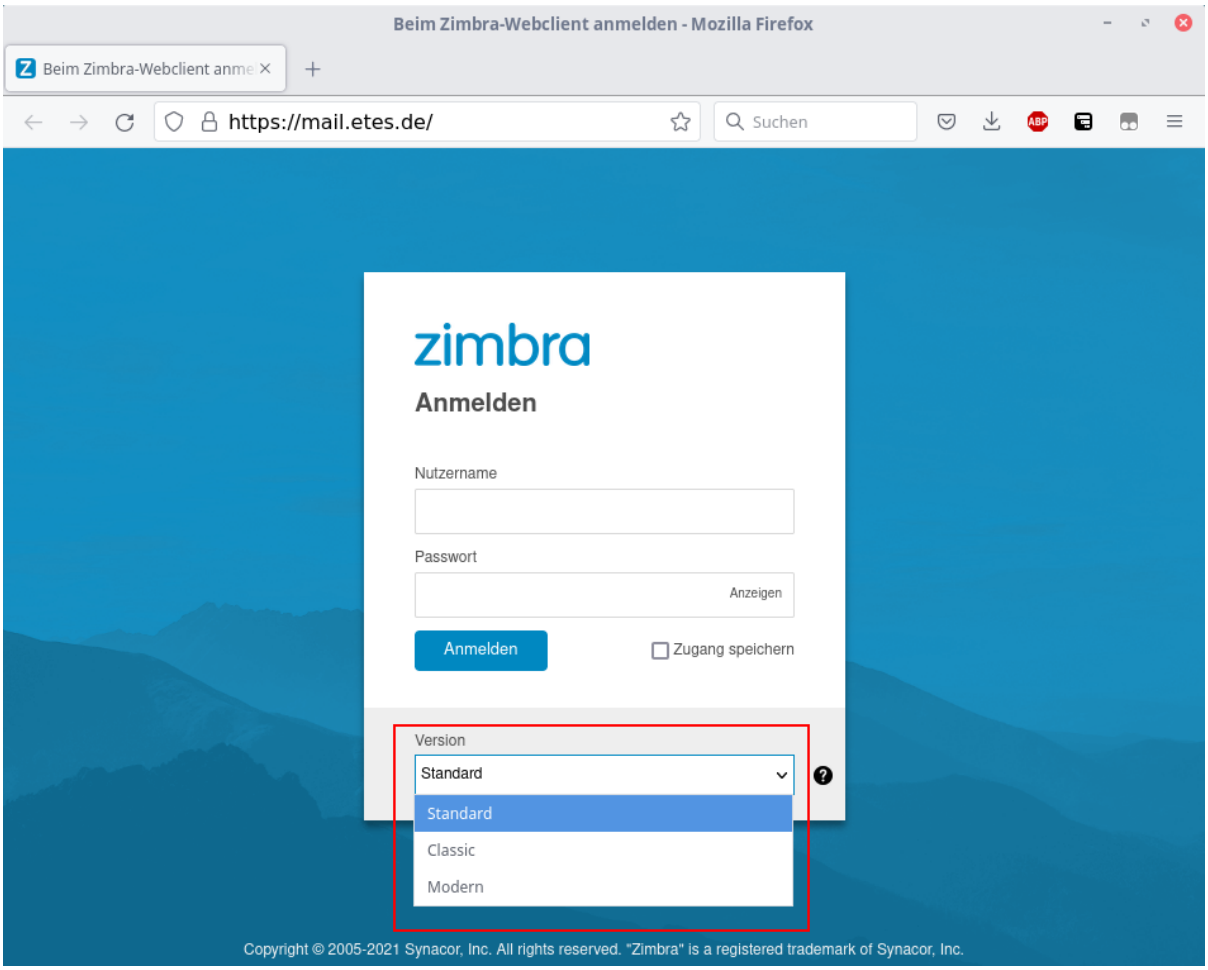
Modern Client

Der Modern Client sieht wie folgt aus:



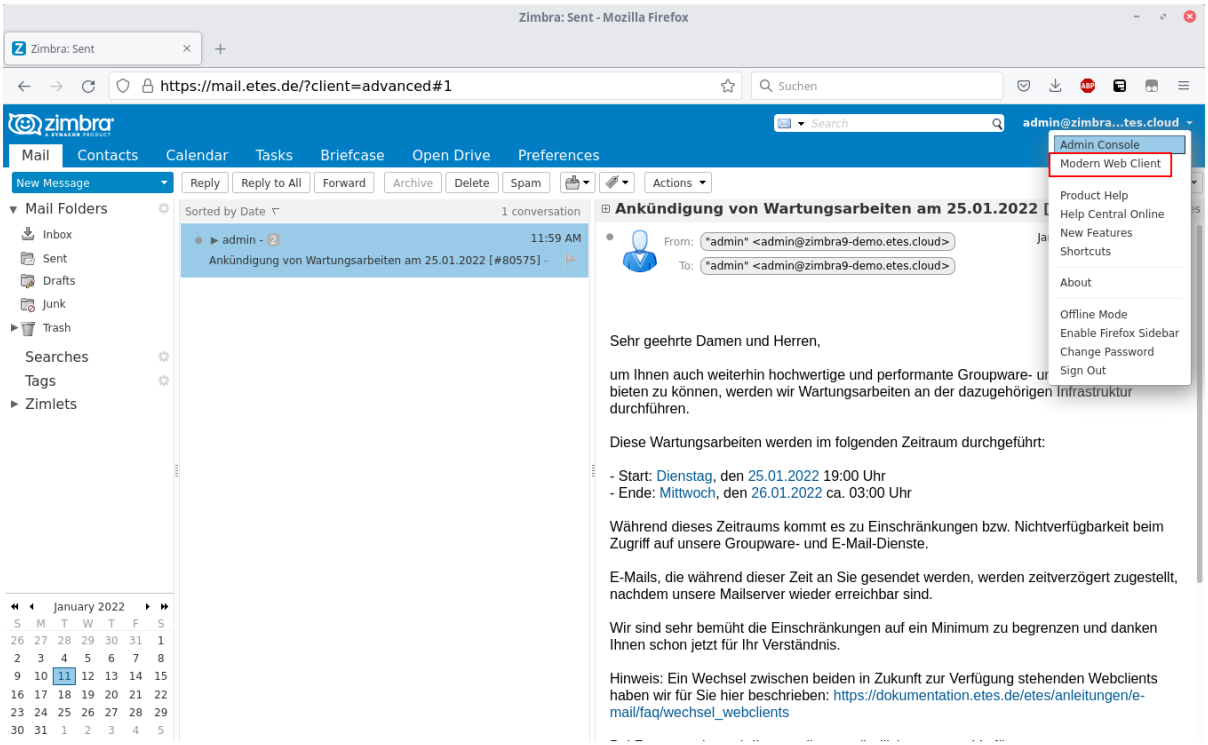
Auswahl des Clients beim Login

Sie können zwischen den beiden Clients direkt beim Login auswählen:



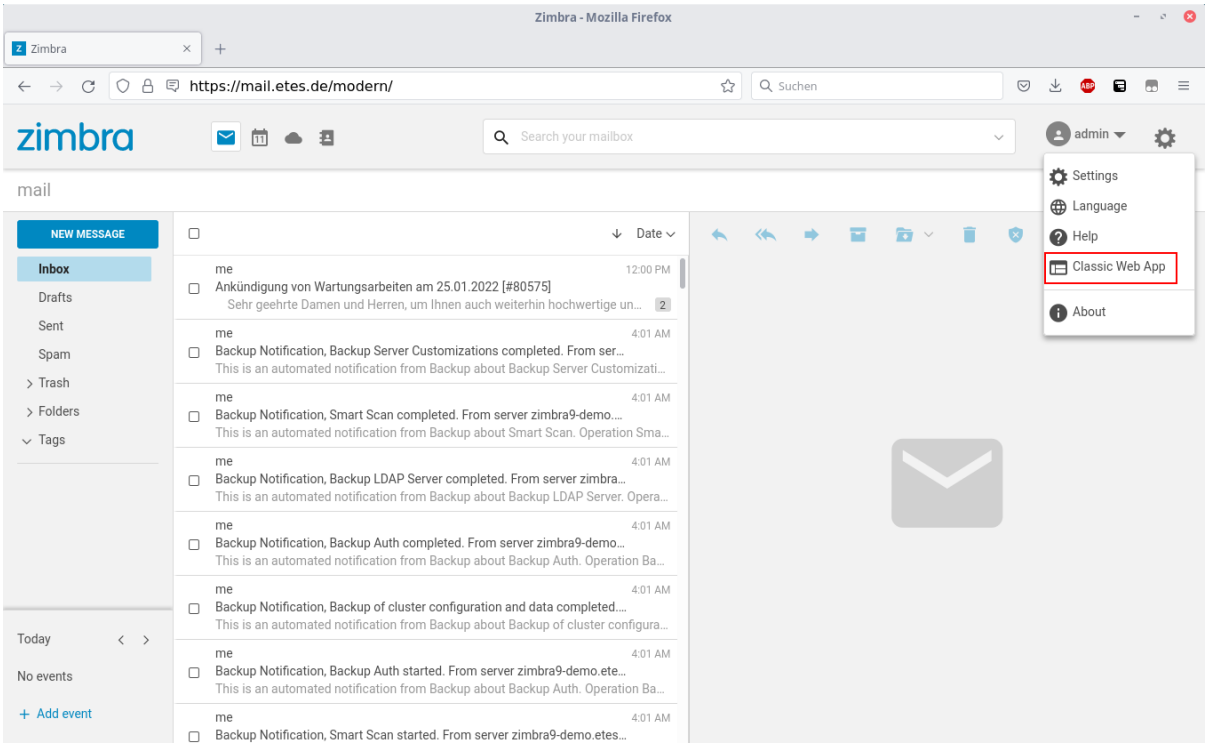
Wechsel vom Classic zum Modern Webclient

Um von Classic zum Modern Webclient zu wechseln klicken Sie rechts oben bitte auf den Pfeil hinter Ihrer E-Mail-Adresse und wählen dann bitte "Modern Web Client" aus:



Wechsel vom Modern zum Classic Webclient

Um vom Modern zum Classic Webclient zu wechseln klicken Sie bitte rechts oben auf das Zahnrad und wählen dann bitte "Classic Web App" aus:


Zimbra - Mozilla Firefox
Zimbra
https://mail.etes.de/modern/
Suchen
zimbra
Search your mailbox
admin
Settings
Language
Help
Classic Web App
About
mail
NEW MESSAGE
Inbox
Drafts
Sent
Spam
Trash
Folders
Tags
Date
me 12:00 PM
Ankündigung von Wartungsarbeiten am 25.01.2022 [#80575]
Sehr geehrte Damen und Herren, um Ihnen auch weiterhin hochwertige un... 2
me 4:01 AM
Backup Notification, Backup Server Customizations completed. From ser...
This is an automated notification from Backup about Backup Server Customizati...
me 4:01 AM
Backup Notification, Smart Scan completed. From server zimbra9-demo....
This is an automated notification from Backup about Smart Scan. Operation Sma...
me 4:01 AM
Backup Notification, Backup LDAP Server completed. From server zimbra...
This is an automated notification from Backup about Backup LDAP Server. Opera...
me 4:01 AM
Backup Notification, Backup Auth completed. From server zimbra9-demo...
This is an automated notification from Backup about Backup Auth. Operation Ba...
me 4:01 AM
Backup Notification, Backup of cluster configuration and data completed....
This is an automated notification from Backup about Backup of cluster configura...
me 4:01 AM
Backup Notification, Backup Auth started. From server zimbra9-demo.ete...
This is an automated notification from Backup about Backup Auth. Operation Ba...
me 4:01 AM
Backup Notification, Smart Scan started. From server zimbra9-demo.etes...
Today
No events
Add event