E-Mail-Programm einrichten

Um dein E-Mail Programm für eine notraces.net Adresse einzurichten oder so zu verändern, dass es auch nach unserem Serverumzug E-Mails abholen kann musst du folgende Anleitung beachten.

Zuerst benötigst du folgende Informationen, die du in deinem E-Mail-Programm später eintragen musst:

- **Mailserver**: siehe Tabelle
- **Username**: Dieses ist in diesem Fall leider **nicht immer** identisch mit deiner bisherigen E-Mail-Adresse. Am einfachsten ist es, du meldest dich einmal mit deiner bisherigen E-Mail-Adresse als Benutzernamen und deinem Passwort an dem Webmailer an. Oben rechts wird deine sogenannte primäre E-Mail-Adresse angezeigt. Diese setzt sich etwa zusammen aus vorname.nachname@notraces.net und ist in Zukunft dein Benutzername für alle Dienste.
- **Paswort**: das kennst du (hoffentlich) noch.
- Als Absenderadresse kannst du entweder deine „neue“ E-Mail-Adresse eintragen - oder deine bisherige, bzw. jede E-Mail-Adresse, für die es bei deinem Konto ein sog. Alias gibt.

Einstellungen auf einen Blick:

(Entschuldigung - hier standen bisher z.T. falsche Ports. Wir erlauben nur ssl-Ports - also verschlüsselte Verbindungen)

Mailserver:

Protokoll	Server	Verschlüsselung	Port
Imap - secure (abholen)	imap.datenkollektiv.net	starttls	143
pop3 - secure (abholen)	pop.datenkollektiv.net	ssl	995
smtp - secure (verschicken)	smtp.datenkollektiv.net	starttls	587

Alternativ kann auch das ältere ssl-Protokoll für imap verwendet werden:

Imap - secure (abholen)	imap.datenkollektiv.net	ssl	993

Das sollte in Erwägung gezogen werden, wenn beim Mail-Programm für die Option „starttls“ nicht eingestellt werden kann, dass ausschließlich verschlüsselte Verbindungen akzeptiert werden sollen. Ansonsten wird erst probiert, eine verschlüsselte Verbindung aufzubauen, wenn das fehlschlägt wird einfach eine unverschlüsselte Verbindung aufgebaut. Zwar akzeptiert unser Mailserver gar keine unverschlüsselten Verbindungen, allerdings könnte die Verbindung manipuliert (siehe: man-in the middle sein und ein anderer Mailserver gibt sich als mail.datenkollektiv.net aus. Mehr dazu findet sich in diesem Artikel: http://www.heise.de/security/artikel/StartTLS-785453.html.

Alle Verschlüsselungsoptionen sollten auch automatisch erkannt werden.

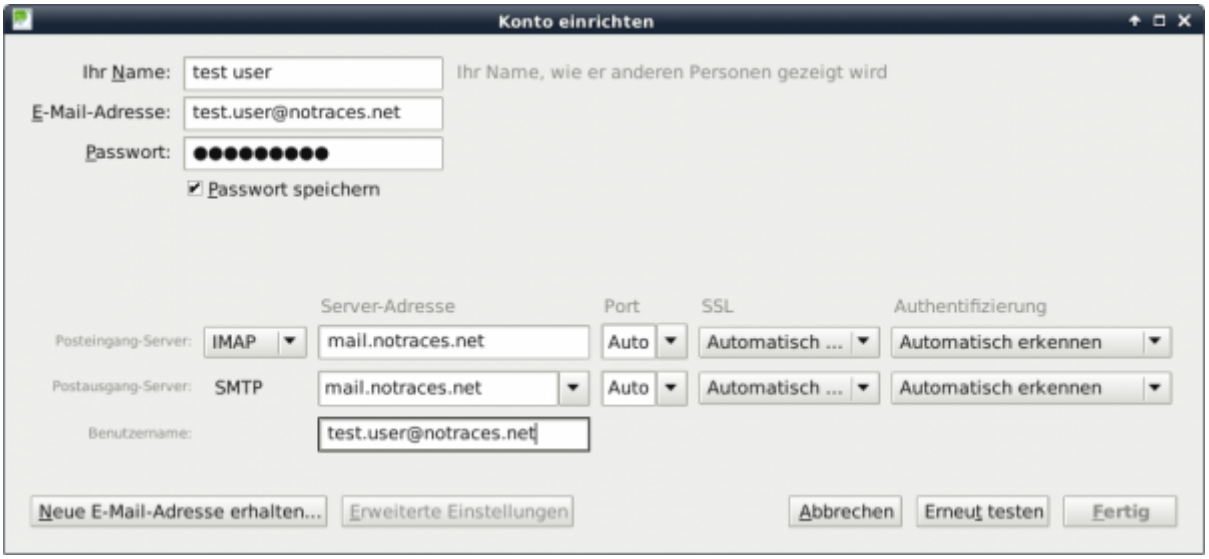
Thunderbird

Für Thunderbird gehst du in die → Einstellungen → Konten-Einstellungen und richtest dort ein neues Konto ein - bzw. veränderst ggf. dein vorhandenes.

Schritt 1:

(zum Vergrößern auf das Bild klicken)

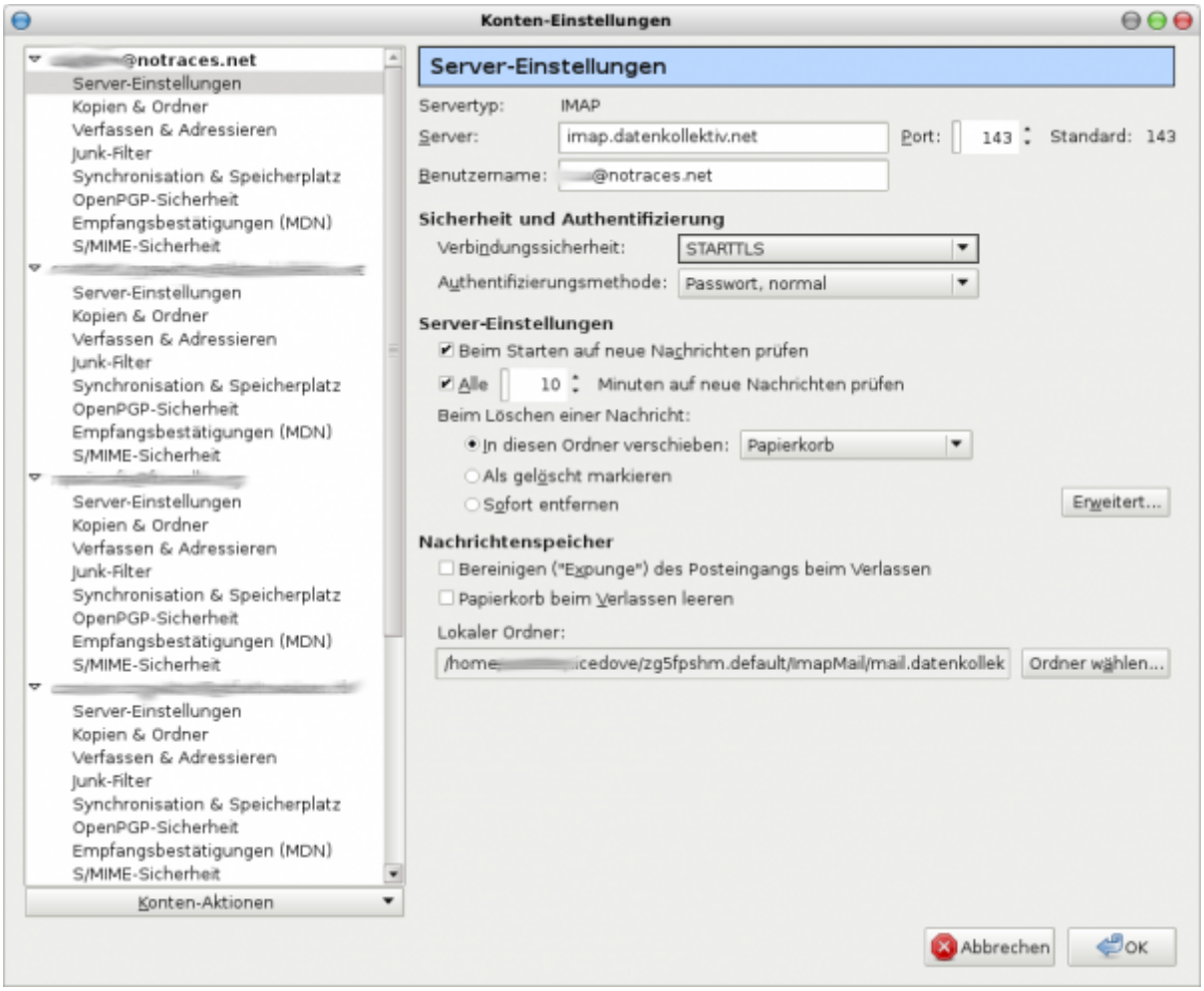
Schritt 2



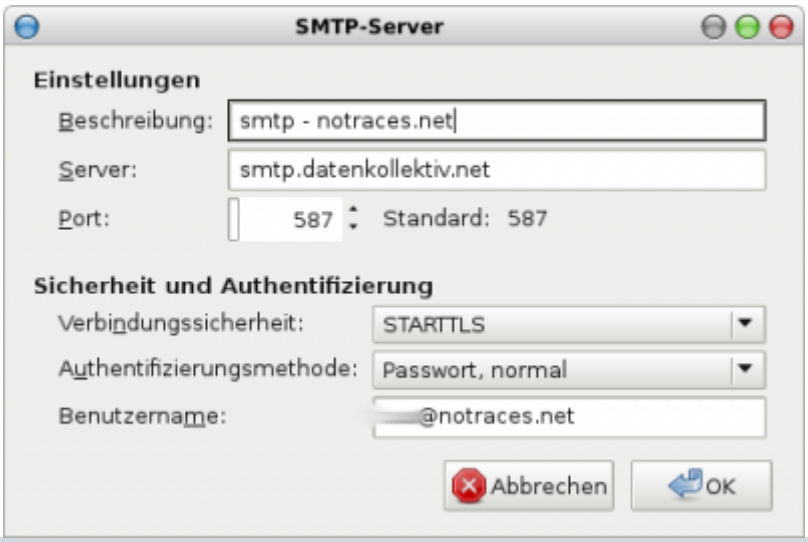
(zum Vergrößern auf das Bild klicken)

Die eingerichteten Konten sollten dann so aussehen:

Imap - Empfangen



SMTP - Postausgang



Imap oder Pop?

Sowohl Imap als auch pop3 sind sog. „Protokolle“ um E-Mails vom Server abzuholen. Der Unterschied dabei: Während Imap die Emails immer auf dem Server beläßt und somit eher eine Art „Ansicht“ der Daten auf dem Server bietet (mit allen Unterordnern, ist pop3 ein Protokoll, das die Emails vom Server auf deinen Computer herunterlädt. Dein E-Mail-

Programm arbeitet dann mit den lokalen Emails.

Imap hat den Vorteil, dass von unterschiedlichen Email-Programmen aus immer die gleichen Daten verfügbar sind. Sogar wenn mehrere Personen in den gleichen Ordnern arbeiten. Allerdings brauchst du dazu immer eine Netzwerkverbindung (obwohl viele Programme anbieten, die Imap-Daten auch lokal zwischen zu speichern).

Wenn du die Daten allerdings vom Server löschen willst (z.B. aus Datenschutzgründen) dann ist pop3 zu empfehlen. Dann muss allerdings ausgewählt werden, dass die E-Mails auch wirklich vom Server gelöscht werden. Dann kannst du allerdings auch keinen Webmailer mehr benutzen.

Zertifikate einrichten

Um eine vertrauenswürdige verschlüsselte Verbindung mit dem Mailserver aufzubauen, empfehlen wir das Wurzelzertifikat unserer CA zu installieren.

- In diesem Link wird das beschrieben: Zertifikate in Thunderbird importieren

So lange das nicht installiert ist, wird Thunderbird eine Zertifikatswarnung ausgeben:

Anstatt hier den Fingerprint zu überprüfen und eine Ausnahmeregel hinzuzufügen, sollte das Wurzelzertifikat installiert werden, damit allen von uns für unsere Server ausgestellten Zertifikate vertraut wird.

In Thunderbird kann es zu Problemen kommen, wenn neben dem installierten Wurzelzertifikat

zusätzliche „Sicherheits-Ausnahmeregeln“ für den gleichen Server eingerichtet sind. Manche Thunderbird-Versionen verweigern ohne aussagekräftige Fehlermeldung die Verbindung.

Also bitte nur ein Zertifikat für den Server installieren. Sollte das Zertifikat verändert werden, muss die „alte Version“ unter → Einstellungen → Erweitert → Zertifikate. Dann unter → Zertifizierungsstellen die, die sich auf datenkollektiv.net oder notraces.net beziehen, löschen.