
TeamDrive Personal Server Benutzerhandbuch

TDPS 1.0

Linux

1. TEAMDRIVE PERSONAL SERVER	3
1.1. STRUKTUR DES PERSONAL SERVER	3
1.1.1. VERZEICHNISSTRUKTUR	3
1.1.1.1. data\	3
1.1.1.2. tdpsd	4
1.1.1.3. stop-tdps	4
1.1.1.4. watch-tdps	4
1.1.1.5. tdpsd-md5pwd	4
1.1.1.6. tdps.config	4
1.2. TEAMDRIVE PERSONAL SERVER INSTALLIEREN	5
1.3. TEAMDRIVE PERSONAL SERVER UPDATEN	6
1.4. TEAMDRIVE PERSONAL SERVER KONFIGURIEREN	6
1.4.1. KONFIGURATIONSPARAMETER	6
1.4.1.1. Gültiger Lizenzschlüssel	6
1.4.1.2. Server Passwort	6
1.4.1.3. Hostname /-adresse	7
1.4.1.4. Portnummer	7
1.4.1.5. Pfad des Repositories	7
1.4.1.6. Maximale Größe für das Repository in MB, GB oder TB	8
1.5. TEAMDRIVE PERSONAL SERVER VERWENDEN	8
1.5.1. STARTEN DES SERVERS	8
1.5.2. STOPPEN DES SERVERS	8
1.5.3. ÜBERPRÜFEN DES SERVER-STATUS	8
1.6. BACKUP DES PERSONAL SERVERS	9
2. TEAMDRIVE CLIENT	9
3. SICHERHEIT	14
3.1. ANTIVIREN-SOFTWARE	14
3.2. HINWEISE ZUM DATENSCHUTZ UND HINWEISE FÜR ADMINISTRATOREN	15

1. TeamDrive Personal Server

1.1. Struktur des Personal Server

1.1.1. Verzeichnisstruktur

...\TeamDrive Personal Server\

data

tdpsd

stop-tdps

watch-tdps

tdps-md5pwd

tdps.config

1.1.1.1. data\

In diesem Verzeichnis wird standardmäßig das Repository Ihres Servers angelegt. Alle Daten aus den SharedSpaces der Nutzer, die an diesem Server angemeldet sind liegen in diesem Verzeichnis. Sie können den Speicherort der Daten über das Attribut „repository-data“ in der tdps.config ändern.

HINWEIS: Das Repository Ihres Servers sollte auf einem lokalen Volume liegen. Netzlaufwerke werden nicht unterstützt. Der Server arbeitet mit File-Locking.

ACHTUNG: Machen Sie unbedingt regelmäßig ein Backup dieses Verzeichnisses, insbesondere vor einem Update. Alle Daten der Nutzer des TD Personal Servers sind hier gespeichert.

Sollten Sie den Standardpfad nutzen, könnte dieser bei einer Neuinstallation oder einem Update auf die überschrieben werden.

1.1.1.2. tdpsd

Datei zum Starten des TeamDrive Personal Servers.

1.1.1.3. stop-tdps

Datei zum Stoppen des Personal Servers.

1.1.1.4. watch-tdps

Datei startet den Personal Server und zeigt den Status im Konsolenfenster an.

1.1.1.5. tdpsd-md5pwd

Verschlüsselt ihr Passwort per MD5

1.1.1.6. tdps.config

Hier sind sämtliche Einstellungen Ihres TeamDrive Personal Servers gespeichert. Sie müssen diese noch manuell mit einem Texteditor editieren.

HINWEIS: Wir empfehlen regelmäßig ein Backup dieser Datei zu machen.

1.2. TeamDrive Personal Server installieren

- a) Entpacken Sie die Datei „TeamDrivePersonalServerLinux_XXXX.tar.zip“.
„tar -xzf TeamDrivePersonalServerLinux_XXXX.tar.gz“
- b) Öffnen Sie ein Terminal und wechseln in das Verzeichnis in dem der entpackte Ordner liegt.
- c) Ändern Sie ggf. die Rechte, die Sie zum Editieren und ausführen der Dateien benötigen: **„chmod -R 755 tdps“**
- d) Falls Sie ein 64Bit Betriebssystem installiert haben, ist es unter Umständen möglich, dass die von uns verwendeten 32Bit Bibliotheken nicht standardmäßig nicht installiert sind. Wir werden wahrscheinlich zeitnah auch eine 64Bit-Version anbieten. Auf Debain-basierenden Distributionen, wie Ubuntu oder Collax können Sie diese Bibliotheken mit folgendem Befehl nachladen:
„apt-get install libc6-i386 lib32gcc1 lib32z1 lib32stdc++6 ia32-libs“
- e) Wechseln Sie ins Verzeichnis tdps : **„cd tdps“**
- f) Verschlüsseln Sie Ihr Passwort: **„./tdps-md5pwd meinPasswort“**



```
vmplanet@ubuntu-vm: ~/tdpsd
Datei Bearbeiten Ansicht Terminal Hilfe
vmplanet@ubuntu-vm:~$ tar -xzf ./TeamDrivePersonalServerLinux_1008.tar.gz
tdpsd/
tdpsd/data/
tdpsd/mime.types
tdpsd/stop-tdps
tdpsd/tdps-md5pwd
tdpsd/tdps.config
tdpsd/tdpsd
tdpsd/TeamDrivePersonalServerLinux_1008_de.pdf
tdpsd/TeamDrivePersonalServerLinux_1008_en.pdf
tdpsd/watch-tdps
tdpsd/data/space-db
vmplanet@ubuntu-vm:~$ chmod -R 755 ./tdpsd/
vmplanet@ubuntu-vm:~$ cd tdpsd/
vmplanet@ubuntu-vm:~/tdpsd$ ./tdps-md5pwd meinPasswort
F14A298BC87FFF2CD757F71054FDD94D
vmplanet@ubuntu-vm:~/tdpsd$
```

1.3. TeamDrive Personal Server updaten

ACHTUNG: Sichern Sie zunächst die Konfigurationsdatei `tdps.config` und Ihr Repository. Beim Update können ältere Dateien leicht überschrieben werden.

1. Stoppen Sie den TeamDrive Personal Server.
2. Installieren Sie die neue Version in ein **anderes** Verzeichnis, als das Vorige.
3. Kopieren Sie den data-Ordner aus der alten Version über den data-Ordner der neuen Installation.

HINWEIS: Es ist möglich, dass sich das Format der Konfigurationsdatei beim Versionswechsel ändert. Deshalb ist es nicht ratsam die Datei einfach zu überschreiben.

HINWEIS: Überprüfen Sie auch ob eine aktuellere Version dieser Dokumentation existiert und beachten Sie dann diese.

1.4. TeamDrive Personal Server konfigurieren

Editieren Sie die Datei „`tdps.config`“. Sie befindet sich im Hauptverzeichnis des TeamDrive Personal Servers.

1.4.1. Konfigurationsparameter

Die meisten der Werte können bleiben, wie sie sind. Die für den Aufbau eines Testservers nötigen Werte sind die folgenden.

1.4.1.1. Gültiger Lizenzschlüssel

license-key=TMDR-0610-BD2A-190C-0000-0001

Hier wird Ihr Lizenzschlüssel eingetragen. Sie bekommen diesen, wenn Sie einen Personal Server erworben haben, von uns mitgeteilt. Defaultwert ist ein Demoschlüssel, der bis zum 01.06.2010 gültig ist.

1.4.1.2. Server Passwort

server-password=F14A298BC87FFF2CD757F71054FDD94D

Ihr Passwort wird MD5-verschlüsselt in die Datei eingetragen. Sie können dazu den mit gelieferten MD5-Generator benutzen „`./tdps-md5pwd`“ **meinPasswort**“

Hier als Default „meinPasswort“

1.4.1.3. Hostname /-adresse

server-host=192.168.30.157

Die Adresse (Hostname oder IP-Adresse) unter der der Server von außen zu erreichen ist.

HINWEIS: Für eine lokale Installation (Server und Client auf dem gleichen System) kann das „127.0.0.1“ bzw. „localhost“ sein. Soll der Client auf einem anderen Rechner laufen, tragen Sie hier bitte die IP-Adresse des Servers ein. Sie können diese finden, indem Sie in der Eingabeaufforderung folgenden Befehl ausführen: „ipconfig /all“

Ist bei einer globalen Betriebsweise ein Router vor den Server geschaltet, muss hier die nach außen sichtbare Adresse des Routers eingetragen werden und im Router eine entsprechende Weiterleitung des Ports eingerichtet werden. Bedenken Sie außerdem, dass Ihr Internet Service Provider (ISP) Ihnen unter Umständen bei jeder Verbindung eine andere IP-Adresse zuweist.

Um unter diesen Umständen eine für den Client feste Adresse zu erzeugen, können Sie einen Dienst wie zum Beispiel DynDNS (www.dyndns.com) nutzen. In diesem Fall muss hier der bei DynDNS registrierte Hostname eingetragen werden (teamdriveServer.dyndns.net o.ä.)

1.4.1.4. Portnummer

server-port=37655

Der Port auf dem der Server arbeitet.

HINWEIS: Der Port muss ggf. in der Firewall freigeschaltet werden.

1.4.1.5. Pfad des Repositories

repository-data=./data

Hier wird das Repository des Servers abgelegt.

Standardmäßig wird dieses im TeamDrivePersonalServer-Programmverzeichnis abgelegt.

HINWEIS: Achten Sie darauf, dass das Repository auf einem NTFS Volume liegt. Z.Z. werden keine Netzlaufwerke unterstützt. Wir empfehlen ein lokales Laufwerk zu verwenden.

ACHTUNG: Dieses Verzeichnis sollte regelmäßig gesichert werden!!!

1.4.1.6. Maximale Größe für das Repository in MB, GB oder TB

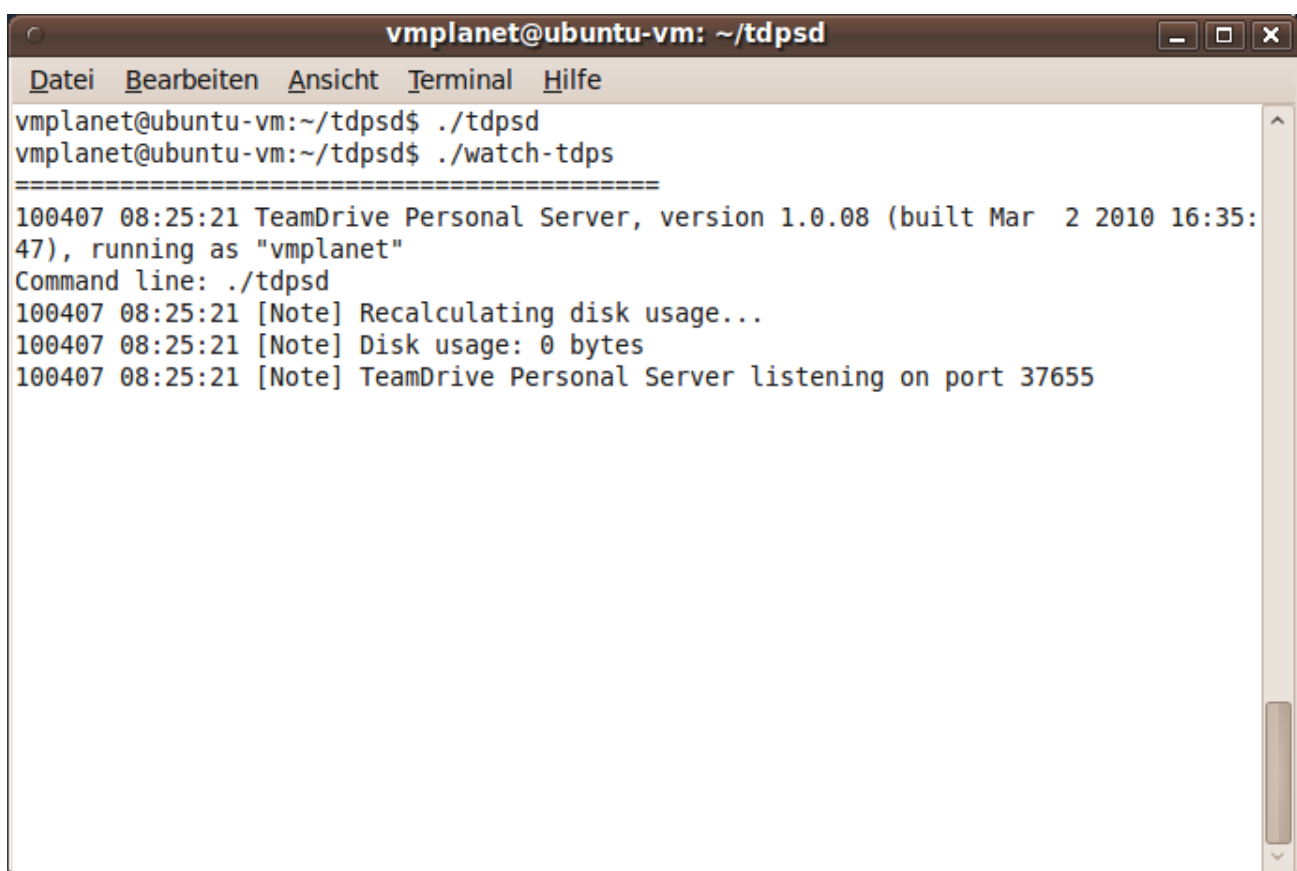
repository-size=5GB

Die minimale Größe für ein Repository ist 10MB. Sollten Sie eine Storage-limitierte Lizenz besitzen, darf der repository-size-Wert die maximale Storagegröße nicht überschreiten, da sonst der Server nicht startet.

1.5. TeamDrive Personal Server verwenden

1.5.1. Starten des Servers

Starten Sie den Server mit dem Befehl „./tdpsd“



```
vmplanet@ubuntu-vm: ~/tdpsd
Datei Bearbeiten Ansicht Terminal Hilfe
vmplanet@ubuntu-vm:~/tdpsd$ ./tdpsd
vmplanet@ubuntu-vm:~/tdpsd$ ./watch-tdps
=====
100407 08:25:21 TeamDrive Personal Server, version 1.0.08 (built Mar  2 2010 16:35:
47), running as "vmplanet"
Command line: ./tdpsd
100407 08:25:21 [Note] Recalculating disk usage...
100407 08:25:21 [Note] Disk usage: 0 bytes
100407 08:25:21 [Note] TeamDrive Personal Server listening on port 37655
```

1.5.2. Stoppen des Servers

Starten Sie den Server mit dem Befehl „./stop-tdps“.

1.5.3. Überprüfen des Server-Status

Starten Sie den Server mit dem Befehl „watch-tdps“, dann wird der Status in der Konsole angezeigt.

Außerdem wird der Serverstatus jederzeit in der Log-Datei protokolliert.

1.6. Backup des Personal Servers

Alles, was Sie brauchen um Ihren Server zu rekonstruieren, sind das Repository und die Konfigurationsdatei. Darum ist es wichtig diese beiden Komponenten zu sichern.

Wir empfehlen auch Ihre Daten zu sichern, bevor Sie ein Update des Servers durchführen.

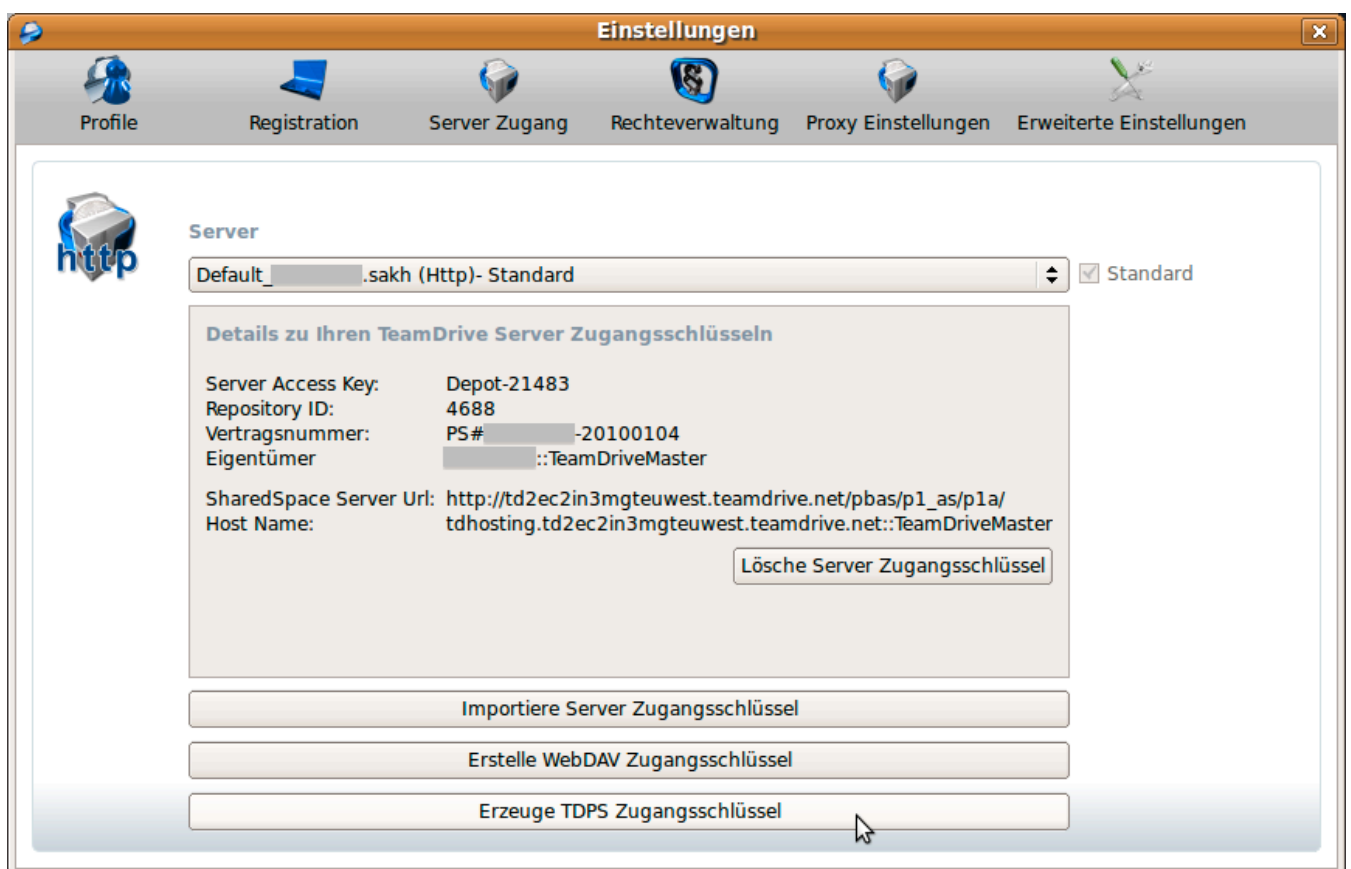
Standardmäßig liegt das Repository im TeamDrive Personal Server-Ordner. Wenn Sie einen anderen Speicherort angegeben haben, befindet sich das Repository an dem von Ihnen angegebenen Ort.

Die Konfigurationsdatei finden Sie im TeamDrive Personal Server-Ordner.

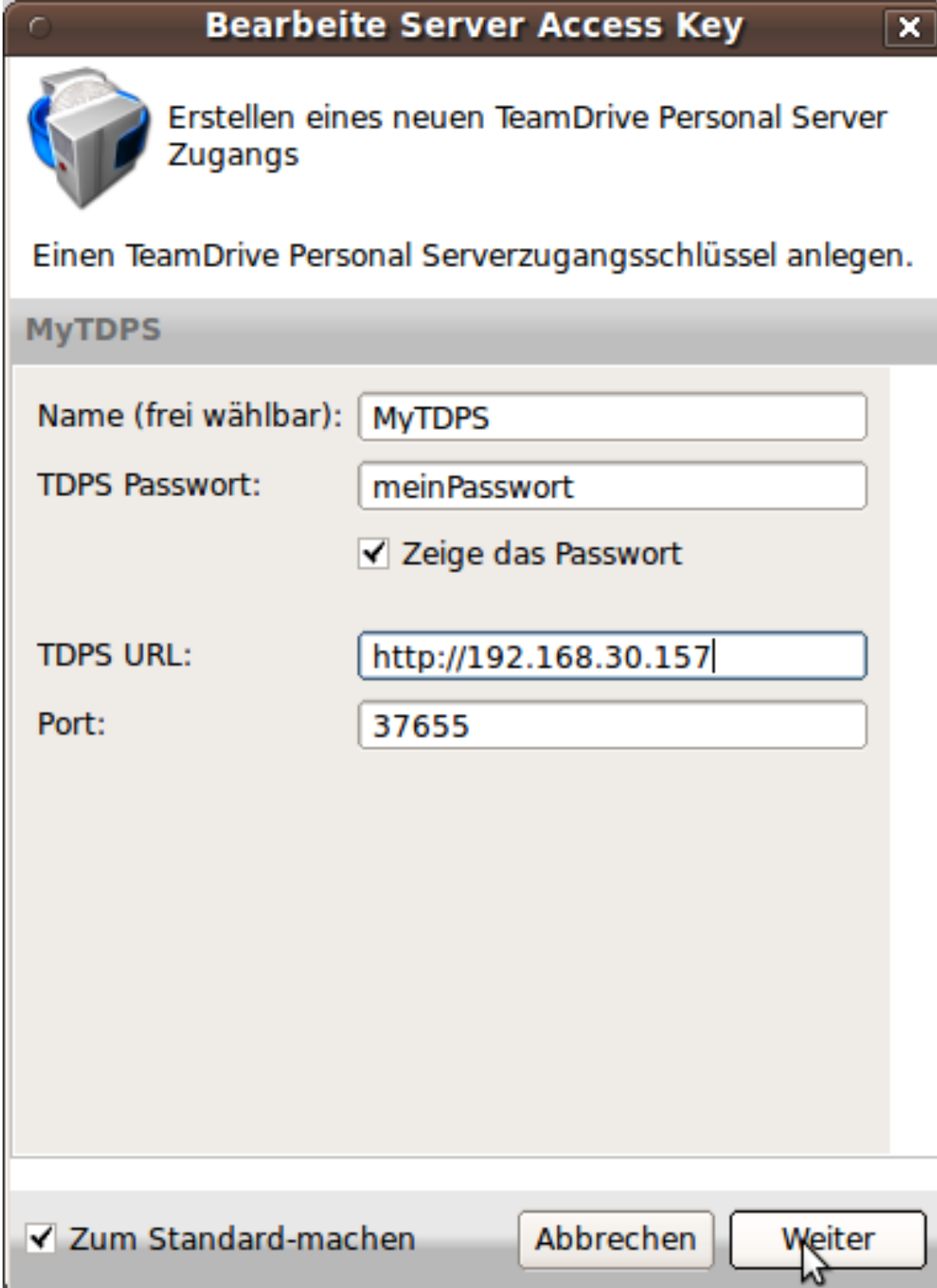
2. TeamDrive Client

Um Ihren TeamDrive Client so einzurichten, dass er mit Ihrem TeamDrive Personal Server zusammen arbeitet, benötigen Sie eine TeamDriveinstallation, mindestens eine Personal-Lizenz und den laufenden TeamDrive Personal Server. Gehen Sie wie folgt vor.


- a) Starten Sie TeamDrive
- b) Öffnen Sie die „Einstellungen“ und wechseln Sie zu „Server Zugang“



c) Wählen Sie „TDPS Zugangsschlüssel erstellen“



Bearbeite Server Access Key

 Erstellen eines neuen TeamDrive Personal Server Zugangs

Einen TeamDrive Personal Serverzugangsschlüssel anlegen.

MyTDPS

Name (frei wählbar):

TDPS Passwort:

☒ Zeige das Passwort


TDPS URL:

Port:

☒ Zum Standard-machen

- d) Tragen Sie die Informationen entsprechend Ihren Einstellungen Ihres Servers ein. Und bestätigen Sie mit „Weiter“

Bearbeite Server Access Key ✕

**Erstellen eines neuen TeamDrive Personal Server Zugangs**

Einen TeamDrive Personal Serverzugangsschlüssel anlegen.

MyTDPS


Name (frei wählbar):

TDPS Passwort:

☒ Zeige das Passwort

TDPS URL:

Port:

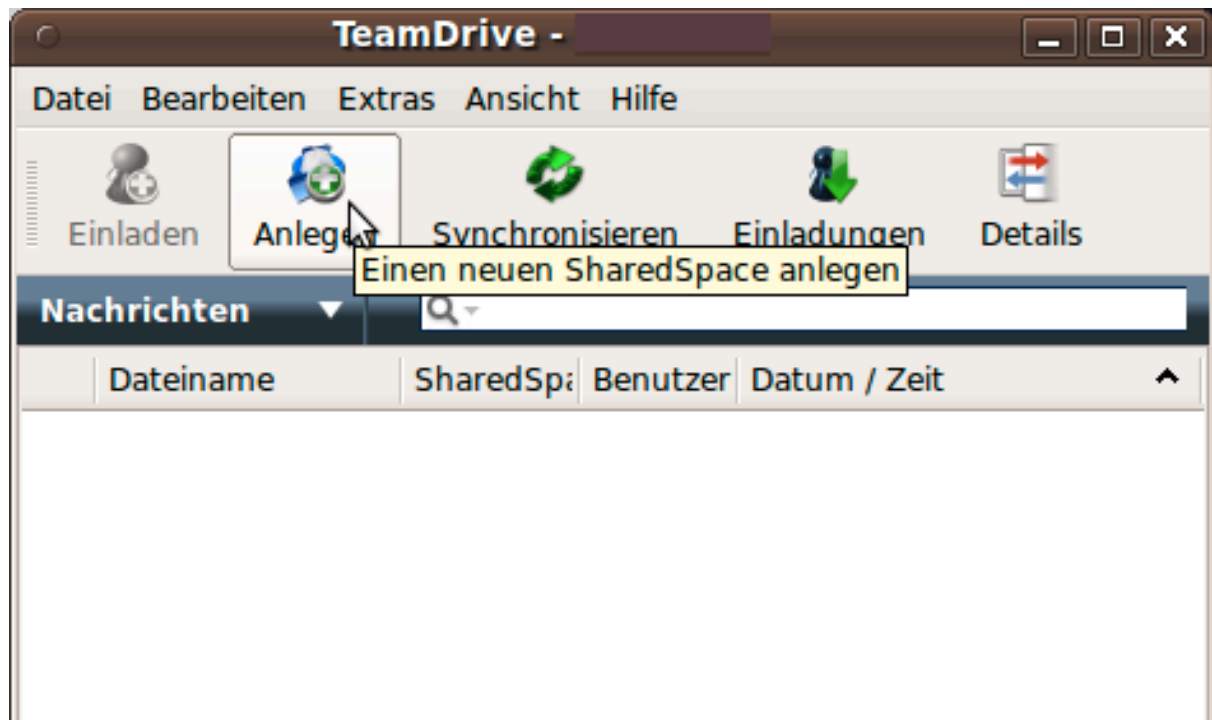
 **Server Access Key wurde erfolgreich erstellt.**

☒ Zum Standard-machen

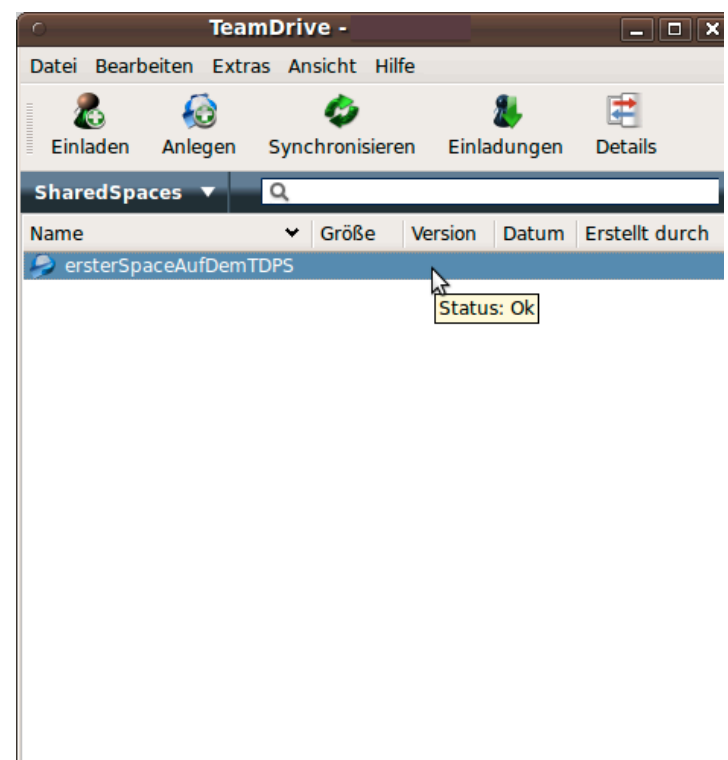
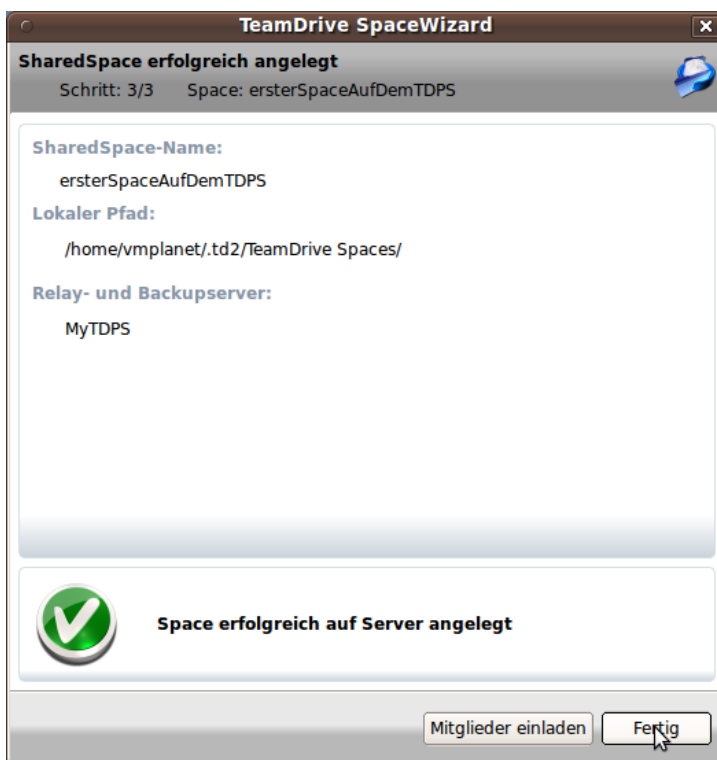
e) Schließen Sie die Einstellungen



f) Sie können TeamDrive jetzt in Verbindung mit Ihrem TeamDrive Personal Server nutzen.



g) Legen Sie einen Space an



3. Sicherheit

Der jeweilige Client-PC und Server sollte hinreichend vor dem unberechtigten Zugriff Dritter geschützt werden.

Hinweis: Hierzu empfehlen wir die entsprechende Literatur des Bundesamtes für Sicherheit und Informationstechnologie (BSI) (www.bsi.bund.de), insbesondere verweisen wir auf das Grundschriftbuch des BSI (www.bsi.bund.de/gshb/deutsch/m/m04151.html)

Verschlüsselter Datenaustausch während des gesamten Datenflusses ist das grundlegende Merkmal von TeamDrive.

Der verschlüsselte Datenaustausch unterteilt sich in drei Schritte:

Schritt 1: Wird ein Mitglied (Benutzer eines Client-PC's) in einen SharedSpace eingeladen, ruft die TeamDrive-Software den Public Key (öffentlichen Schlüssel) vom Registrierungsserver ab.

Schritt 2: Für den Zugriff auf einen (gemeinsamen) SharedSpace wird ein „Datenschlüssel“ (256 Bit-AES-Schlüssel) lokal erzeugt, der mit dem Public Key des eingeladenen Mitglieds verschlüsselt und über einen eigenen Kommunikationsweg dem TeamDrive-Anwender übermittelt wird. Zu keinem Zeitpunkt gelangt ein Datenschlüssel auf einen Server.

Schritt 3: Mit dem Datenschlüssel werden die Daten des SharedSpaces verschlüsselt, sobald sie den Client-PC verlassen. In verschlüsselter Form werden die Daten auf einem Server zwischengespeichert. Die Verschlüsselung gewährleistet, dass die Daten des SharedSpaces nur von dessen Mitgliedern abgerufen werden können. Auf dem Server liegen nur verschlüsselte Daten. Indem jedes Mitglied einen Datenschlüssel zugeteilt bekommen hat, ist es gleichzeitig autorisiert und wird Daten aus den SharedSpace erhalten. Diese Daten werden durch den Daten-Schlüssel automatisch entschlüsselt und können eingesehen bzw. bearbeitet werden

3.1. Antiviren-Software

Die TeamDrive-Daten werden von der lokalen Antiviren-Software überwacht, u.a., indem der Virens Scanner die entsprechende Datei beim Zugriff prüft. Alle SharedSpaces im lokalen Dateisystem sollten standardmäßig von Ihrer aktuellen Antivirensoftware überwacht werden.

Hinweis: Wir empfehlen grundsätzlich die Nutzung einer lokalen Antiviren-Software auf jedem Client, weil jeder TeamDrive-Nutzer sehr schnell eine Vielzahl von SharedSpaces mit unterschiedlichen Teams nutzen kann. Selbstschutz ist die sicherste Methode!

3.2. Hinweise zum Datenschutz und Hinweise für Administratoren

Mit TeamDrive ist die Einhaltung der Datenschutzvorschriften von Unternehmen und Behörden gewährleistet. Um eine optimale Einhaltung der datenschutzrechtlichen Vorschriften zu ermöglichen, sollten die nachfolgenden Hinweise bei der Installation und Verwendung des Produktes beachtet werden.

Der jeweilige Client-PC und Server sollte hinreichend vor dem unberechtigten Zugriff Dritter geschützt werden.

Die sonstigen betrieblichen Datenschutzvorschriften finden auch beim Einsatz der TeamDrive-Anwendung. Hinsichtlich der Erstellung von Verfahrensverzeichnissen und der ggf. erforderlichen Vorabkontrolle bestehen keine Besonderheiten beim Einsatz des Produktes.

Für den Fall, dass das Produkt nicht unter Verwendung eines eigenen internen Data-SpaceDepot-Servers zum Einsatz kommt, sind im Verhältnis zum Provider des SpaceDepots die Voraussetzungen der Auftragsdatenverarbeitung zu beachten. Auch hier gelten keine Besonderheiten im Vergleich zu anderen IT-Produkten, die einen externen Datenspeicher nutzen. Der Auftraggeber muss den Auftragnehmer sorgfältig auswählen und schriftliche Weisungen erteilen. In der Regel ist ein gesonderter Auftragsdatenverarbeitungsvertrag zu schließen. Weitere Informationen zur Auftragsdatenverarbeitung mit entsprechenden Mustern finden Sie z.B. beim Virtuellen Datenschutzbüro (www.datenschutz.de) ggf. sind auch wir bei weiteren Fragen behilflich und können Kontakte vermitteln.

Version dieses Dokumentes: 1.2

Dieses Produkt enthält Programmbibliotheken des OpenSSL Projektes, zur Verwendung des OpenSSL Toolkits (www.openssl.org)