Systemvoraussetzungen

Client System

Ab Windows 7 (WebStart und Browser Oberfläche: x86/x64, Desktop Client: x64)

- Java 1.8 (x86/x64)
- Mozilla Firefox (aktuellste Version)
- Internet Explorer 11 (x86/x64)
- Chrome (aktuellste Version)

OSX (ab El Capitan 10.11)

- Apple Safari 11
- Mozilla Firefox (aktuellste Version)
- Chrome (aktuellste Version)

Linux

- Wird nicht offiziell unterstützt

Wir empfehlen immer die neueste Browser-Version zu installieren.

Welche Java-Version habe ich installiert?

Um sicher zu gehen, dass Sie die richtige Java Version installiert haben, können Sie hier überprüfen, welche Version auf ihrem System installiert ist:

http://www.java.com/de/download/installed.jsp

Server-System

Windows Server

- Java 1.8 (64bit) ab Version 161
- ab Window Server 2012
- ab MSSQL 2012Express oder MySQL5.7

Linux-Server (Debian)

- Java 1.8 (64bit) ab Version 161
- MySQL5.7

Minimale Systemvoraussetzungen

Bevor das FTAPI SecuTransfer System installiert wird, sollten Sie zunächst überprüfen, ob mindestens die nachfolgenden minimalen Systemvoraussetzungen erfüllt sind:

Software:

- Jedes Betriebssystem, auf dem eine Java VM lauffähig ist (z.B. Windows, Linux oder Unix)
- Installierte Sun Java-Version 1.8 (JRE ausreichend)
- Aktiviertes JavaScript in den verwendeten Internetbrowsern (an den Clients)

Hardware:

- Mindestens 2x2Ghz Prozessorleistung
- Mindestens 6GB **freier** Arbeitsspeicher
- Genügend große Festplatte für die Speicherung der Übertragungsdaten (dies ist generell abhängig davon, ob Ihre Use-cases große oder kleine Dateien versenden/nutzen)

Sonstiges:

- Bestehende, leistungsfähige Netzwerkverbindung
- Datenbank: wird zwischen 1-20 GB an Speicher benötigen, je nach Aktivität. Bei >100 aktiven internen Nutzern, empfehlen wir mind. 6 GB zusätzlich für die DB bereitzustellen.

Um einen optimalen Betrieb von FTAPI vor allem auch für höhere Anfragelasten zu gewährleisten, empfehlen wir die nachfolgenden Voraussetzungen auf dem Server-System:

- 4x2Ghz Prozessorleistung oder höher
- 12GB **freier** Arbeitsspeicher oder höher
- 250GB **freie** Festplatte oder mehr
- Gigabit Netzwerkverbindung

Java-Installation überprüfen

Um den FTAPI SecuTransfer Server betreiben zu können, benötigen Sie einen entsprechend leistungsfähigen Rechner.

Darüber hinaus müssen Sie sicherstellen, dass Sie auf dem Server die Java Version 1.8 oder höher (JRE ist ausreichend) installiert haben. Diese Information können Sie durch Eingabe des folgenden Befehls in Ihre Konsole/Terminal ermitteln:

```
java -version
```

Anschließend sollten Sie eine Ausgabe ähnlich der folgenden erhalten:

```
java version "1.8.0_77"
Java(TM) SE Runtime Environment (build 1.8.0_77-b03)
Java HotSpot(TM) 64-Bit Server VM (build 25.77-b03, mixed mode, sharing)
```

Sollten Sie eine Java-Version kleiner als 1.8 installiert haben oder der Befehl nicht gefunden werden, dann installieren Sie bitte eine aktuelle Java-Version auf ihrem System. Diese können Sie kostenlos unter folgender URL beziehen:
JRE unter http://www.java.com oder http://java.sun.com/j2se

Prüfen Sie zusätzlich, ob eine entsprechende JRE_HOME Umgebungsvariable gesetzt ist.

OpenJDK

Die Java-Variante OpenJDK wird derzeit für den Betrieb von FTAPI nicht offiziell unterstützt und kann daher bei der Verwendung zu Problemen führen! Aus diesem Grund wird dazu geraten Oracle Java zu verwenden.

Reverse-Proxy-Server

Der Betrieb mit Hilfe eine Reverse-Proxys ist grundsätzlich möglich. Da hierbei jedoch zahlreiche individuelle Faktoren bestehen, werden diese nicht im Handbuch beschrieben. Sollte es weiterführende Fragen geben, wenden Sie sich bitte an den Support.

Interne Infrastruktur (FTAPI Server)

Hier wird kurz zusammengefasst, welche Infrastruktur innerhalb des Netzes zur Verfügung stehen muss, damit ein fehlerfreier Betrieb des FTAPI Systems gewährleistet werden kann.

Portfreigaben in der Firewall

Damit der FTAPI Server von außerhalb erreichbar ist, sollten die folgenden Ports in der Firewall auf den FTAPI Server weitergeleitet werden:
Natürlich können Sie Ihr FTAPI System auch komplett intern betreiben, allerdings können externe User dann nicht auf die Daten zugreifen.

FTAPI Ports

443: Dieser Port wird für die https Verbindung verwendet. Jegliche Kommunikation über diesen Port ist mit einem SSL-Zertifikat verschlüsselt (siehe unten)

80: Dieser Port wird nicht zwangsläufig für den fehlerfreien Betrieb von FTAPI benötigt. Hier wird legiglich eine Weiterleitung auf den Port 443 vorgenommen, was zu einer bessern User-experience führt. (Um das gleiche Verhalten zu haben kann auch die Firewall diese Weiterleitung durchführen)

IIS (Microsoft Internet Information Services)

Da FTAPI SecuTransfer mit dem Tomcat Server von Apache läuft, sollte **kein IIS auf dem Server installiert werden**.

Dieser kann nicht für den FTAPI Server verwendet werden und reserviert nur die Ports, die der FTAPI benötigt.

URL und Zertifikat

URL

Um den FTAPI Server ansprechen zu können, ist eine eindeutige URL notwendig.

Nur eine URL

Da die URL im FTAPI eingetragen wird und z.B. für die E-Mail Benachrichtigungen verwendet wird, kann es immer nur eine URL geben.

Sowohl interne als auch externe Zugriffe auf das System müssen über diese URL erfolgen.

Es spielt allerdings keine Rolle, ob der Zugriff von intern auch über die externe Firewall läuft oder nicht. Es ist also durchaus möglich, über den internen DNS ein anderes Routing zum FTAPI Server zu konfigurieren. (Außnahme: SSL-Offloading. Siehe unten)

Für die gewählte URL müssen die entsprechenden DNS Einträge gesetzt werden, damit diese über das Internet erreichbar ist.
Auch hier ist es prinzipiell möglich, den FTAPI Server nur intern zu betreiben, in dem Fall muss natürlich nur der interne DNS konfiguiert werden und kein externer.

Zertifikat

Für die gewählte URL muss ein offiziell signiertes SSL Zertifikat zur Verfügung stehen.
Achtung: Da Java nur Verbindungen von offiziell signierten Zertifikaten zulässt, sollte ein solches verwendet werden, da sonst weder der Desktop Client, noch das Outlook Add-In, noch die mobilen Apps verwendet werden können.

Wenn ein selbst signiertes Zertifikat verwendet wird, dann kann für die Desktop App der Java Keystore angepasst werden, um die Verbindung zu ermöglichen.
Da dies sowohl einen hohen Aufwand bedeutet, als auch keine Lösung für das Outlook Add-In oder die mobilen Apps darstellt, empfehlen wird Ihnen in jedem Fall ein offizielles Zertifikat zu verwenden.

Hierbei spielt es keine Rolle, ob ein Wildcard- oder ein Domänen-Zertifikat verwendet wird, beide können im FTAPI eingebunden werden.

Zusammenfassung

Für einen reibungslosen Betrieb muss ein offiziell signiertes Zertifikat verwendet werden.

Zur Installation müssen dann die folgenden Daten zur Verfügung stehen:

1. Das signierte Zeritifikat (meist in einem dieser Formate: .pem, .cer)
2. Der private key des Zertifikats (meist in diesem Format: .key)

Genauere Infos zu Zertifikaten

Weitere Informationen, wie das Erstellen eines Zertifikats, finden Sie in unserem Handbuch auf dieser Seite: SSL Zertifikat und HTTPS

SSL-Offloading

Es ist möglich, den FTAPI Server mit einem sogenannten SSL-Offloading zu betreiben.

Das bedeutet, dass das SSL Zertifikat am Proxy installiert wird, der dann die Verschlüsselte Verbindung mit dem Client aufbaut.

Dieser Proxy kommuniziert dann im plain text (keine Verschlüsselung) mit dem FTAPI Server, was bedeutet, dass dieser kein Zertifikat mehr benötigt.

Diese Einstellung bedeutet allerdings, dass auch interne Nutzer über die Firewall geleitet werden müssen, da sie sonst keine SSL-Verbindung bekommen.

SMTP

Damit der FTAPI Server E-Mail-Benachrichtigungen versenden kann, muss ein Mail Server (SMTP-Server, z.B. Exchange) zur Verfügung stehen.

Über diesen muss der FTAPI Server in der Lage sein, E-Mails zu **relayen.** Das bedeutet, dass hier kein Postfach eingerichtet werden muss.

Best-practices sind:

1. Einen eigenen Connector bei dem SMTP Server erstellen, über den "anonym" E-Mails versandt werden können.
   Dieser Connector wird dann auf die IP Adresse des FTAPI Servers beschränkt.
2. Es wird ein Connector verwendet, bei dem man sich mit Username und Passwort authentifizieren muss.
   Diese Login Daten werden für die Installation vorbereitet, sodass sie dann entsprechend eingetragen werden können.

Wichtig

Damit der FTAPI Server Emails korrekt versenden kann muss der verbundene Connector in der Lage sein, Emails "anonym" zu relayen.

Für mehr Informationen melden Sie sich gerne bei uns: https://www.ftapi.com/service/Support-Anfrage

Datenbank

Damit der FTAPI Server erfolgreich laufen kann, muss eine Datenbank angebunden werden.

Diese kann entweder lokal installiert werden, oder auch im Netzwerk zur Verfügung stehen (für unterstützte Versionen siehe oben).

Sollte eine Datenbank auf einem anderen Server verwendet werden, ist es wichtig, dass dieser TCP/IP Verbindungen zulässt (dies ist bei MySQL per default aktiviert, bei MSSQL muss es erst konfiguriert werden).

Um bei der Installation Zeit zu sparen ist es empfehlenswert, die Datenbank schon vorab zu installieren.

Nur eine MSSQL Version

Sollten Sie eine MSSQL verwenden wollen beachten Sie bitte, dass immer **nur eine** MSSQL Version installiert sein darf!

LDAP / Active Directory (Optional)

Diese Einstellungen sind nur relevant, wenn Sie Ihr AD an FTAPI anbinden wollen.
Sollte das nicht gewünscht sein, oder sollten Sie kein AD einsetzen, kann dieser Punkt übersprungen werden.

Um das FTAPI System mit einem AD zu verbinden, wird eine interne Verbindung zum entsprechenden Server benötigt.
Das bedeutet, falls Ihr FTAPI in einer DMZ stehen soll und das AD im internen Netz ist, muss es eine entsprechende Verbindung geben, da das AD ansonsten nicht angesprochen werden kann.

Außerdem wird ein User benötigt, der Zugriff auf das AD hat.
Dieser User muss mindestens lesende Zugriffe auf das gesamte AD haben.

Da das FTAPI System in jedem Fall nur lesend auf das AD zugreift, kann hier auch der Admin User des AD verwendet werden.
Das hat den Vorteil, dass Sie keinen zusätzlichen User verwalten müssen, dessen Passwort gegebenenfalls ablaufen kann.

Genauere Informationen zur Konfiguration des ADs finden Sie in unserem Handbuch auf dieser Seite: LDAP und Active Directory

Checkliste

Diese Checkliste können Sie sich ausdrucken, um dann die entsprechenden Punkte abhaken zu können.

- [ ] Portfreigaben in der Firewall (443 und 80)
- [ ] DNS Einträge (eine URL)
- [ ] Signiertes Zertifikat für die eine URL
- [ ] SMTP Konnektor
- [ ] Datenbank Zugriff aktiviert oder lokale Instanz installiert
- [ ] AD Zugriff (Optional)