

ELDAFTPS - Dokumentation für Software-Hersteller (SWH)

- 1. Serveradressen
- 2. Zertifikate
- 3. Anmeldedaten
 - 3.1. Seriennummer mit Kundenpasswort
 - 3.1.1. Beispiele von kodierte SHA512 Passwörtern
 - 3.2. Umgang mit anonymen Logins
- 4. Versionsausweis
- 5. Ablauf FTPs Transfer
 - 5.1. Allgemein
 - 5.2. Ablauf einer FTPs Übermittlung
 - 5.2.1. Abbildung des Ablaufs einer FTPs Übermittlung
 - 5.3. Implementierte FTP Kommandos
 - 5.4. Wichtige Hinweise
 - 5.4.1. Beispiel-Skript
 - 5.5. Beispiel-Code für eine Übertragung
- 6. Sonstiges
 - 6.1. Wichtige Status-Codes
 - 6.1.1. 425 - Can't open data connection.
 - 6.1.2. 425 - Data connection not encrypted, aborting.
 - 6.1.3. 452 - Storage limit reached
 - 6.1.4. 552 - Transfer stopped. File exceeded MAX_FILE_SIZE
 - 6.2. TLS Versionen
 - 6.3. Unverschlüsselte Verbindungen
 - 6.4. Maximale Dateigröße

1. Serveradressen

Die Adressen für die Produktiv- und Testsysteme sind aus Tabelle 1 zu entnehmen. Bitte beachten, dass die Umgebungen nur den passiven Transfermodus unterstützen! Für den passiven Transfer werden die Ports 10022 bis 10041 verwendet. Beim Servertyp des FTPs handelt es sich um FTPES (FTP über explizites TLS/SSL), der auf dem Apache FtpServer basiert.

| Bezeichnung | Adresse | Port | Transfermodus | FTPs |
|-----------------|-------------------|------|---------------|------|
| FTPs Produktion | ftps.elda.at | 21 | passiv | Ja |
| FTPs Test | ftps-test.elda.at | 21 | passiv | Ja |

Tabelle 1: FTPs Umgebungen

2. Zertifikate

Die bei den verschiedenen Server verwendeten Zertifikate können über die ELDA Homepage (<https://www.elda.at>) heruntergeladen werden.

3. Anmeldedaten

3.1. Seriennummer mit Kundenpasswort

Benutzerkennung: {Seriennummer}

Passwort: {Kundenpasswort}

Das Kundenpasswort muss kodiert an die Schnittstelle übergeben werden. Der Server erwartet ein mit dem SHA512-Algorithmus kodierte Kundenpasswort (HEX, lowercase). Die Eingabe der Seriennummer als Benutzerkennung erfolgt im Klartext. Der Einsatz des Kundenpassworts ist ab 1.4.2015 zwingend. Bis zu diesem Zeitpunkt wird erst gegen das Kundenpasswort geprüft, falls dieses beim Kunden gesetzt wurde. Nachdem das Kundenpasswort bei einem Kunden gesetzt wurde, kann man sich nicht mehr mit der Seriennummer authentifizieren! Wurde nur der Passwort-Token angefordert, kann weiterhin der Lizenzschlüssel verwendet werden.

3.1.1. Beispiele von kodierte SHA512 Passwörtern

| Klartext | Codiert |
|----------|--|
| 123456 | ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea10f35ee3cbc514797ed7ddd3145464e2a0bab413 |

| | |
|----------|--|
| passwort | 5630fa4e304e9dc0c18b47376dc77ef0a342895f44868ae20e85fcc6834df8d2186faad0bd985aaa171d58807b8e09e4743e5bb9d4d47dc6dc2b8c52e9b31cd4 |
|----------|--|

3.2. Umgang mit anonymen Logins

Anonyme Logins, etwas mit dem User "anonymous", werden vom ELDA-FTPs nicht unterstützt. Ein Login mit diesem Benutzernamen wird mit dem Statuscode 530 abgewiesen.

```
Status:      Auflösen der IP-Adresse für localhost
Status:      Verbinde mit 127.0.0.1:2121...
Status:      Verbindung hergestellt, warte auf Willkommensnachricht...
Status:      Initialisiere TLS...
Status:      Überprüfe Zertifikat...
Status:      TLS-Verbindung hergestellt.
Befehl:      USER anonymous
Antwort:     530 Anonymous connection is not allowed.
```

4. Versionsausweis

Die aktuell installierte Version des ELDA-FTPs Servers ist aus einer Willkommensnachricht nach erfolgreichem Login ersichtlich.

```
Antwort:     331 User name okay, need password for .
Befehl:      PASS *****
Antwort:     230-User 103265 logged in at 2021-06-29T14:08:55, proceed.
Antwort:     230 Running ELDA FTPS Version 1.3.8.2
```

5. Ablauf FTPs Transfer

5.1. Allgemein

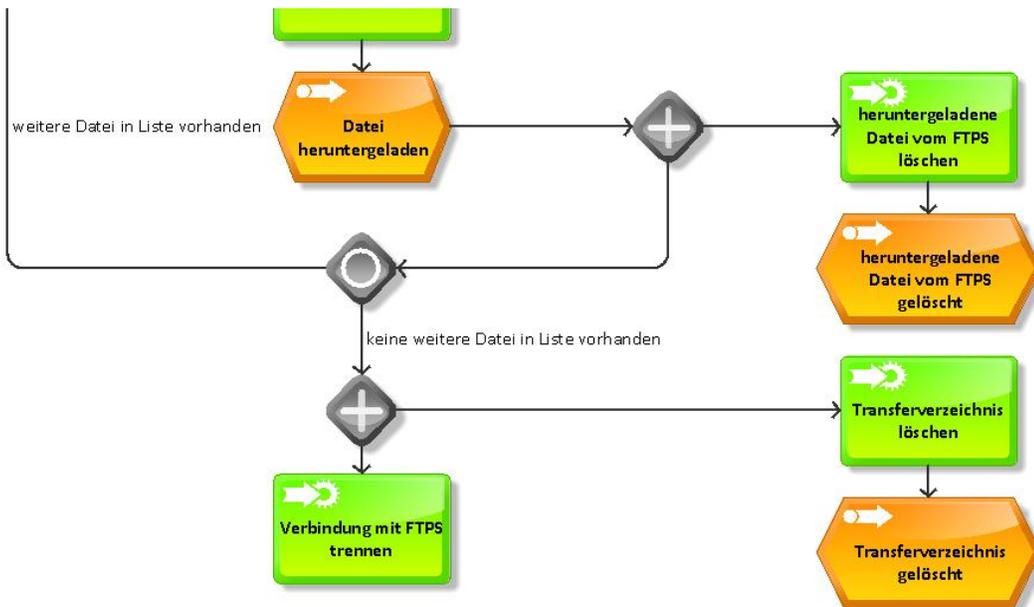
Bei dieser Übertragungsmethode werden die hochgeladenen Dateien nicht gesammelt (ausgelöst durch die Datei "elda.eot") an das ELDA-Backend gesendet, sondern jede hochgeladene Datei wird einzeln und unmittelbar nach dem Upload an das ELDA-Backend übertragen.

Die Datei "elda.ret" muss zwingend vom Client angefordert werden; das Anfordern bewirkt, dass die Datei "elda.ret" generiert wird und die darin aufgelisteten Dateien auf dem FTPs-Server bereitgestellt werden. Sind keine Dateien zum Download verfügbar, befindet sich in der Datei "elda.ret" ein einzelnes Leerzeichen. Bitte beachten Sie, dass die Verarbeitung der hochgeladenen Dateien eine gewisse Zeit dauert und es sich daher empfiehlt die Datei "elda.ret" erst nach einer gewissen zeitlichen Verzögerung anzufordern.

5.2. Ablauf einer FTPs Übermittlung

1. Eine FTPs-Verbindung zum ELDA-Server auf Port 21 herstellen
2. Die Leitung mit dem Befehl "**AUTH**" verschlüsseln
3. User über den Befehl "**USER**" und Passwort mit dem Befehl "**PASS**" senden
 - a. Sollte Punkt 2 übersprungen worden sein, wird hier der Fehlercode 425 zurück gegeben
4. Mit dem Befehl "**PUT**" die gewünschte Anzahl an Dateien hochladen
5. Die Datei "elda.ret" mit dem Befehl "**GET**" abholen
 - a. Darin ist pro Zeile ein Dateiname angegeben, der zum Download zur Verfügung steht
 - b. Sind keine verfügbaren Dateien vorhanden, steht darin ein einzelnes Leerzeichen
6. Mit "**GET**" die verfügbaren Dateien herunterladen
7. Mit "**QUIT**" die Session beenden

5.2.1. Abbildung des Ablaufs einer FTPs Übermittlung



5.3. Implementierte FTP Kommandos

Der ELDA FTPs-Server unterstützt die folgende Liste an Kommandos. Für weitere Information zu diesen, siehe [die Liste der FTP-Kommandos auf Wikipedia](#).

- ABOR
- AUTH
- CWD
- DELE
- FEAT
- HELP
- LANG
- LIST
- MLSD
- MODE
- PASS
- PASV
- PBSZ
- PROT
- PWD
- QUIT
- REST
- RETR
- SITE
- STAT
- STOR
- STOU
- TYPE
- USER

5.4. Wichtige Hinweise

Beim Hoch- bzw. Herunterladen keine Pfadangaben verwenden, der Server weist dem Client automatisch das richtige Arbeitsverzeichnis zu.

Richtig

```
PUT x:\tmp\test.txt test.txt
GET elda.ret
GET xyz
```

Falsch

```
PUT x:\tmp\test.txt \test.txt
GET /elda.ret
```

Die in der Datei "elda.ret" aufgelisteten Dateien können Empfangsbestätigungen, Fehler- oder Warnhinweise sein. Eine Fehler- bzw. Warnungsdatei enthält entsprechende Codes, welche in der Dokumentation zu den Fehlercodes auf der ELDA-Homepage (<https://www.elda.at>) aufgelistet sind.

5.4.1. Beispiel-Skript

```
open ftps-test.elda.at 21
prot p
user XXXXXX Pppppppp
binary
put c:\gkkdfu\test1.txt test.txt
get elda.ret c:\gkkdfu\elda.ret
bye
```

5.5. Beispiel-Code für eine Übertragung

```
FTPSCClient client = new FTPSCClient("TLSv1.2");
client.connect("ftps-test.elda.at", 2121);
client.enterLocalPassiveMode();
client.execPBSZ(0);
client.execPROT("P");
client.login("username", "password");

File file = new File("dateiname");
FileInputStream fis = new FileInputStream(file);

client.storeFile("remotename", fis);

if(client.getReplyCode() != 226){
    throw new Exception("hochladen nicht erfolgreich!");
}
File localDirectory = new File("directoryname");
localDirectory.mkdir();
File eldaRet = new File("directoryname"+File.separator+"elda.ret");
client.retrieveFile("elda.ret", new FileOutputStream(eldaRet));
List<String> filesToDownload = readEldaRet(eldaRet); // Filenamen aus eldaRet auslesen
for(String file : filesToDownload){
    if(StringUtils.isNotBlank(file)){
        client.retrieveFile(file, new FileOutputStream(new File("directoryname"+File.separator+file)));
    }
}

client.quit();
```

6. Sonstiges

6.1. Wichtige Status-Codes

6.1.1. 425 - Can't open data connection.

Dieser Fehler kann beim Herunterladen der Datei "elda.ret" auftreten, wenn der Server unter starker Last steht. In diesem Fall sollte der Client so programmiert sein, dass der Fehler abgefangen und nach einem kurzen Intervall das erneute Abholen dieser Datei versucht wird.

6.1.2. 425 - Data connection not encrypted, aborting.

Dieser Fehler kommt, wenn vom Server eine verschlüsselte Datenverbindung vorausgesetzt wird, diese aber clientseitig nicht aktiviert bzw. eingeleitet ist. Eine sehr wahrscheinliche Ursache für diesen Fehler ist, dass der Befehl "PROT P" nicht abgesetzt wurde.

6.1.3. 452 - Storage limit reached

Dieser Fehler kommt, wenn auf dem Server vor der Übertragung nicht mehr genügend temporärer Speicher frei ist, oder während der Übertragung dieser ausgeht.

6.1.4. 552 - Transfer stopped. File exceeded MAX_FILE_SIZE

Wird eine Datei übermittelt, die über dem Dateilimit liegt, wird die Übertragung abgebrochen und dieser Fehler zurückgegeben. Siehe Punkt 6.3 für das aktuelle Limit.

6.2. TLS Versionen

Seit November 2021 werden die TLS Versionen 1.0 und 1.1 nicht mehr unterstützt.

6.3. Unverschlüsselte Verbindungen

Unverschlüsselte Verbindungen werden vom FTPs **nicht** unterstützt. Eine Verschlüsselung ist zwingend erforderlich.

6.4. Maximale Dateigröße

Die maximale Dateigröße für komprimierte und unkomprimierte Dateien gleichermaßen beträgt aktuell 220 MB.

Version 21 (07-Okt-2022 01:52:59)