

# LAN-TSE Software

## Inhaltsverzeichnis

|  |          |
|--|----------|
| <b>Extrahieren der Dateien und erste Schritte</b> .....        | <b>1</b> |
| <b>Konfiguration und Installation in der Konsole</b> .....     | <b>2</b> |
| <i>Wichtige Einstellungen der Config</i> .....                 | 2        |
| <b>Weboberfläche nach erfolgreich gestarteten Dienst</b> ..... | <b>3</b> |
| <b>Hyper-V oder VMware etc.</b> .....                          | <b>3</b> |
| <b>Energieverwaltung bei USB ausschalten</b> .....             | <b>6</b> |
| <b>Einstellungen der Firewall</b> .....                        | <b>6</b> |

Mit unserer Middleware steuern Sie einheitlich verschiedene TSE Geräte einfach an. Der Aufruf innerhalb des Netzwerkes erlaubt den einfachen Zugriff auf die TSE. Somit kann diese insbesondere auch aus Sicherheitsgründen (Diebstahl) z.B. im Server Rack installiert werden und muss nicht an der Kasse selbst installiert sein.

Download Link der Software:

<https://www.dbfakt.de/downloads/get/54/dbfakt-lan-tse-software>

## Extrahieren der Dateien und erste Schritte

Bitte erstellen Sie einen neuen Ordner z.B.: c:\DBFAKT\_TSE und kopieren danach die Dateien aus dem ZIP in den neuen Ordner.

Installation von

**vc\_redist.x64.exe**

„Windows Powershell“ als **Administrator** aufrufen.

In den Ordner wechseln, wo die Dateien liegen:

**cd c:\DBFAKT\_TSE**

**.\lantse.ps1**

Sollte nun eine Fehlermeldung kommen bzgl. etwaiger Berechtigungen, dann:

**powershell-server-defaults.cmd**

ausführen und Powershell neu starten.

Wenn immer noch Fehlermeldungen kommen wegen fehlender Benutzerrechte, dann:

**Set-ExecutionPolicy RemoteSigned**

und Powershell neu starten.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\Administrator> cd C:\dbFakt_TSE
PS C:\dbFakt_TSE> .\lantse.ps1
Parameter:
install      Dienst installieren
uninstall    Dienst entfernen
start        Dienst starten
stop         Dienst beenden
restart      Dienst neu starten
add-eventlog Ereignislog anlegen
del-eventlog Ereignislog löschen
get-eventlog Ereignislog anzeigen
run          Start als Anwendung
config       Erzeugen/Ändern der Konfigurationsdatei
PS C:\dbFakt_TSE>
  
```

## Konfiguration und Installation in der Konsole

Bei erster Installation bitte in nachfolgenden Reihenfolge starten:

Benutzte Ports: **netstat -a -n | findstr ABH**

```

.\lantse.ps1 config
.\lantse.ps1 install
.\lantse.ps1 add-eventlog
.\lantse.ps1 run           (Evtl. die Firewall zulassen)
  
```

Testen auf <http://localhost:2020> ob erreichbar

```
.\lantse.ps1 start
```

### Wichtige Einstellungen der Config

```
.\lantse.ps1 config
```

|                             |   |
|-----------------------------|---|
| Host                        | Entweder localhost / IP Adresse / oder * für beides |
| Port                        | z.B. 2020   |
| PUK* <sup>2</sup>           | 123456  |
| Admin Pin* <sup>2</sup>     | 12345   |
| TimeAdmin-PIN* <sup>2</sup> | 12345   |
| Client-ID* <sup>2</sup>     | dbFakt (dbFakt Nutzer zwingend „dbFakt“)            |
| Laufwerk                    | Laufwerk der TSE z.B. „x“                           |

(Wenn über einen Share dann erstmal ein physische Laufwerk nehmen und danach in der appsettings.Production.json den UNC Pfad angeben)

AuthData (Lizenzkey von dbFakt zum Aktivieren der Anwendung)

\*<sup>2</sup> wird auf der TSE gespeichert

Install Dienst installieren

|              |   |
|--------------|---|
| Uninstall    | Dienst entfernen                                  |
| Start        | Dienst starten                                    |
| Stop         | Dienst stoppen                                    |
| Restart      | Dienst neu starten                                |
| Add-Eventlog | Ereignisanzeige (bitte unbedingt aktivieren)      |
| Del-Eventlog | Ereignisanzeige löschen                           |
| Get-Eventlog | Zeigt die 100 letzten Einträge in der Konsole an. |
| Run          | Starten der Anwendung auf der Konsole             |

## Weboberfläche nach erfolgreich gestarteten Dienst

Rufen Sie bitte nach erfolgreicher Installation die Oberfläche über die in der Konfig eingegebene IP-Adresse und Port auf:

<http://192.168.111.40:2020>

The screenshot shows a web browser window with the URL <http://192.168.111.40:2020>. The page title is "LAN-TSE" with a serial number "ZaAZ0h25SmbjGKS8Oyo1sbv65zcomuuRqedHrVbVNEg=". The main heading is "Status". Below it, there are several status indicators:

- Clients: 1 von 100
- Speicherbelegung: 259 kiB von 6.5 GiB
- Signaturen: 254 von 20000000 garantiert
- Laufende Transaktionen: 0 von 512

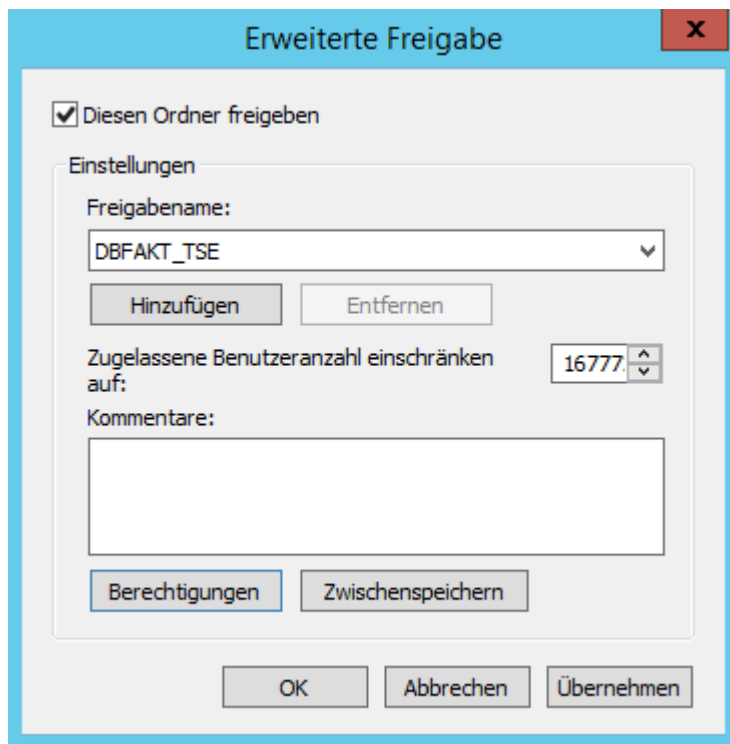
There are several colored status boxes:

- Selbsttest** (green)
- Zeit** (green)
- Datenintegrität 0 ECC-Fehler** (green)
- Speicherlebensdauer 100%** (green)
- Reservespeicher 100%** (green)
- Retention 98%** (black)
- Muss nicht ersetzt werden** (yellow)
- tseHealth** (yellow)
- Zertifikat gültig bis 2026-01-20T23:59:59+01:00** (green)

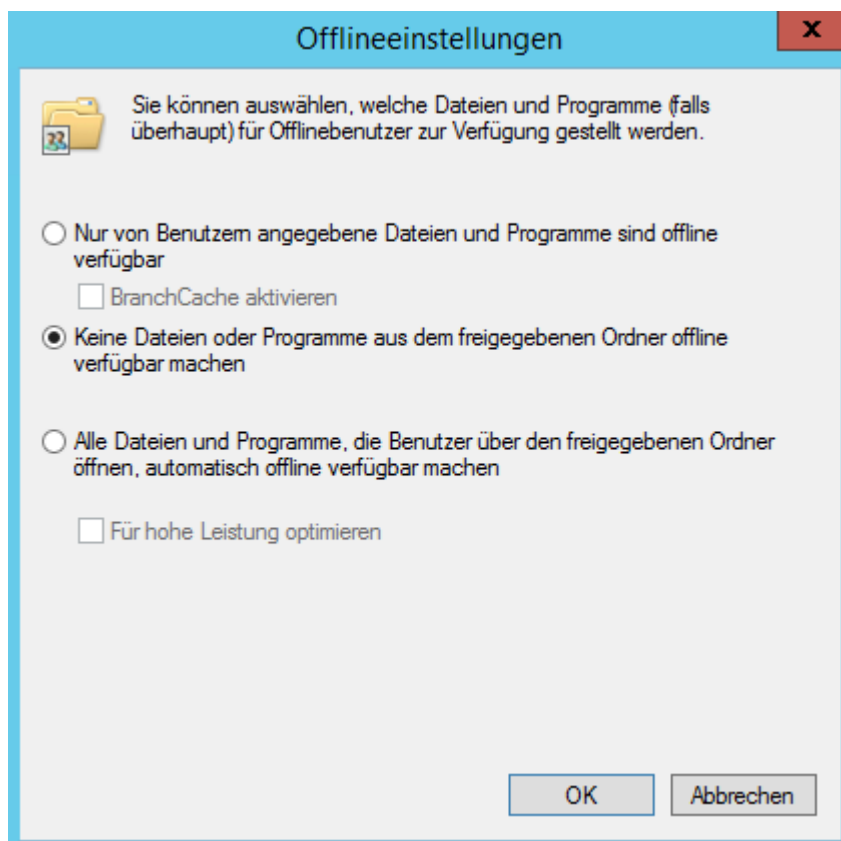
Probieren Sie das bitte von jedem Rechner aus, welcher auf die TSE zugreifen muss.

## Hyper-V oder VMware etc.

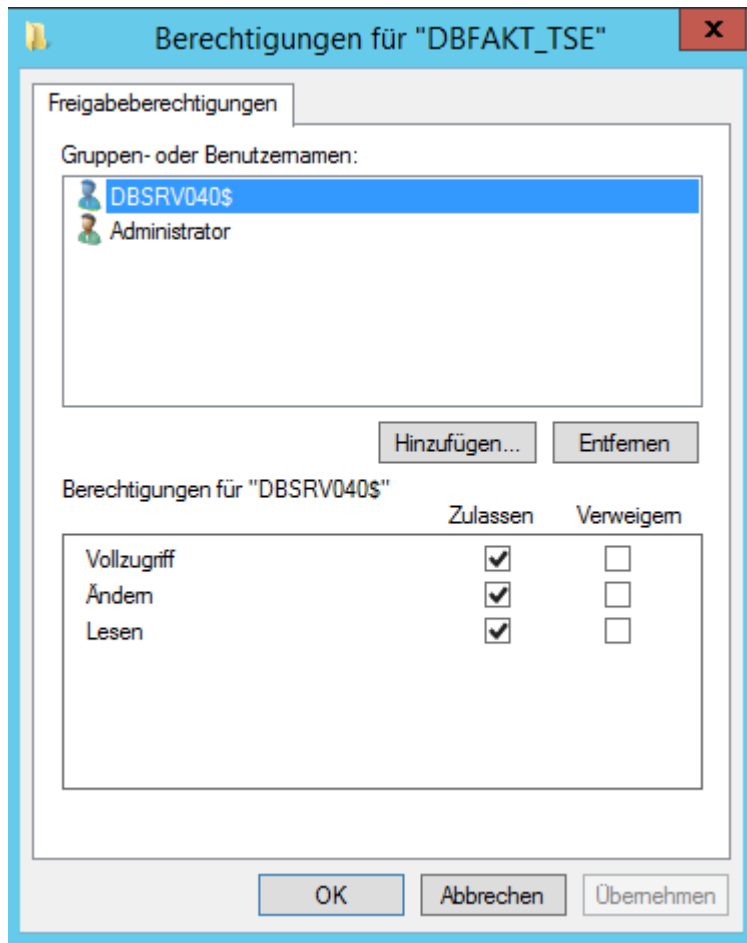
Bei Serverumgebungen mit Hyper-V bitte die TSE als Laufwerk freigeben:



Bitte bei „Zwischenspeichern“ die Auswahl „Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen“ bei der nachfolgenden Einstellung setzen.

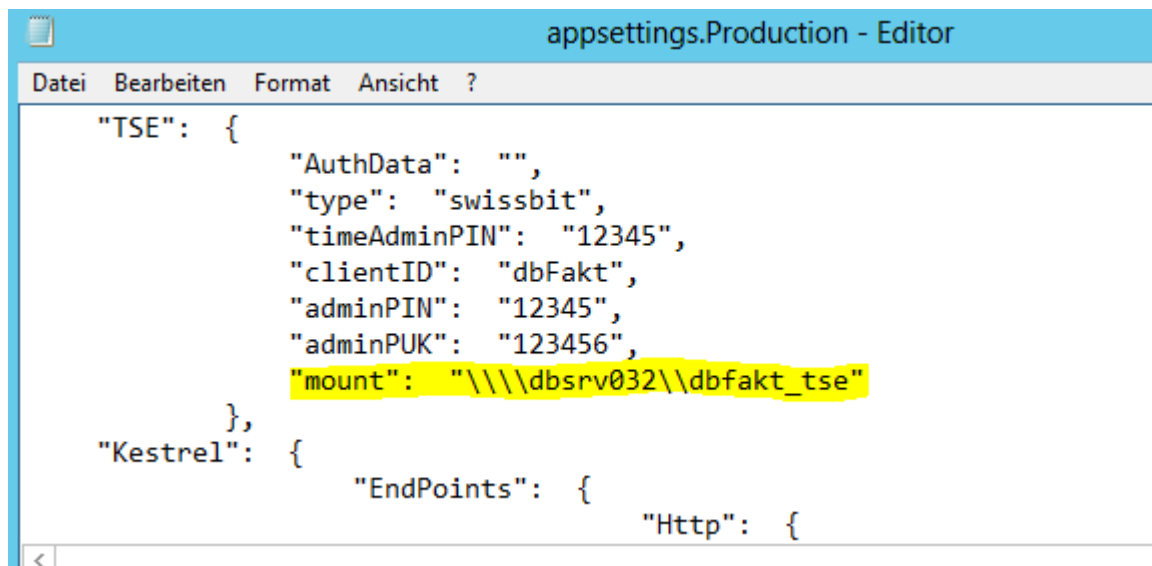


Bitte bei den Berechtigungen das Gerätekonto der virtuellen Maschine mit Vollzugriff erlauben:

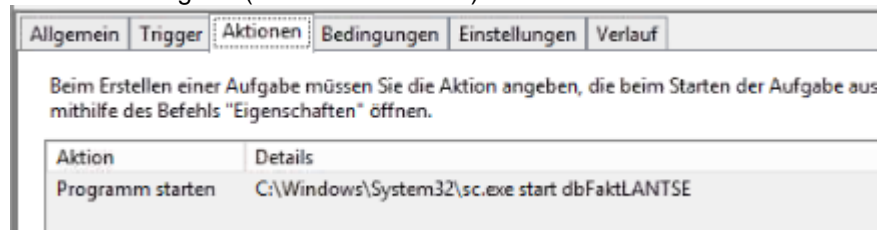


Wenn der Host nicht mit in der Domäne ist muss ein Benutzer manuell auf dem Host sowie auf dem virtuellen Server angelegt werden.

Es kann dann noch hilfreich sein in der „appsettings.Production.json“ nach der Config den Eintrag des Laufwerks „mount“ auf einen UNC Pfad abzuändern:



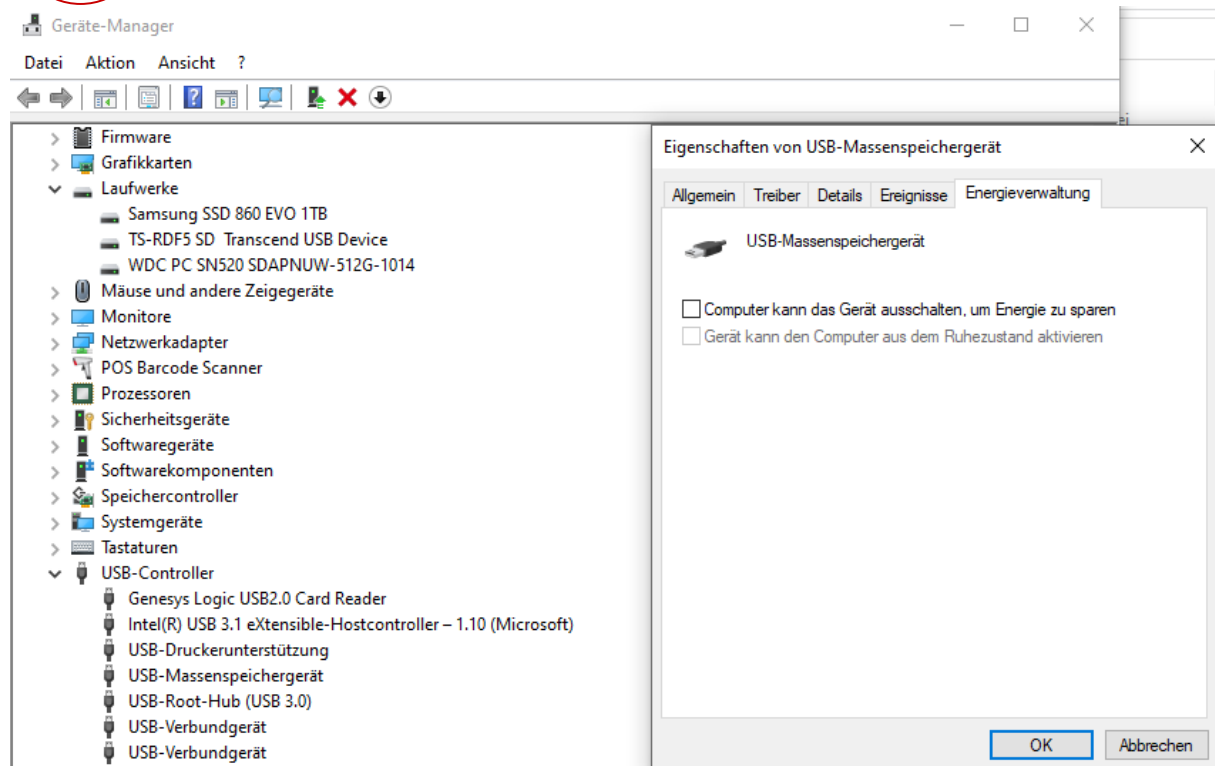
Sollte es immer wieder vorkommen das nach einem Reboot der Dienst nicht gestartet ist dann bitte ein solche Aufgabe (Intervall 5 Minuten) einrichten:



## Energieverwaltung bei USB ausschalten



Bitte deaktivieren Sie die Einstellung für die Energiesparoption bei dem USB Port.



## Einstellungen der Firewall

Wenn Sie von Clients nicht auf die TSE via Browser zugreifen können, dann sollten Sie auf dem Host noch eine Portfreigabe der Firewall konfigurieren:

### Assistent für neue eingehende Regel

#### Regeltyp

Wählen Sie den Typ der zu erstellenden Firewallregel aus.

**Schritte:**

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Welchen Regeltyp möchten Sie erstellen?

**Programm**  
Regel, die die Verbindungen für ein Programm steuert.

**Port**  
Regel, die die Verbindungen für einen TCP- oder UDP-Port steuert.

**Vordefiniert:**  
  
Regel, die die Verbindungen für einen Windows-Vorgang steuert.

**Benutzerdefiniert**  
Benutzerdefinierte Regel

< Zurück   Weiter >   Abbrechen

### Assistent für neue eingehende Regel

#### Protokolle und Ports

Geben Sie die Protokolle und Ports an, für die diese Regel gilt.

**Schritte:**

- Regeltyp
- Protokolle und Ports**
- Aktion
- Profil
- Name

Betrifft diese Regel TCP oder UDP?

**TCP**

**UDP**

Gilt diese Regel für alle lokalen Ports oder für bestimmte lokale Ports?

**Alle lokalen Ports**

**Bestimmte lokale Ports:**

Beispiel: 80, 443, 5000-5010

< Zurück   Weiter >   Abbrechen





**Assistent für neue eingehende Regel** ✕

**Name**

Geben Sie den Namen und die Beschreibung dieser Regel an.

**Schritte:**

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- **Name**

Name:

Beschreibung (optional):

**Assistent für neue eingehende Regel**

**Aktion**

Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.

**Schritte:**

- Regeltyp
- Protokolle und Ports
- Aktion**
- Profil
- Name

Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?

**Verbindung zulassen**  
Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.

**Verbindung zulassen, wenn sie sicher ist**  
Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

**Verbindung blockieren**