

Terminalmanagementsystem (TMS)

Installationsanleitung für Windows

Version 1.0.0

Historie

Version	Datum	Beschreibung
0.9.0	11.06.2026	Initiale Version
1.0.0	17.06.2026	Erste Version nach QS

Inhaltsverzeichnis

1	Einleitung	3
2	Vorbereitung	4
2.1	Installation von IIS (Internet Information Server)	4
2.1.1	Import/Erstellung des SSL-Browserzertifikats	4
2.2	Installation von Hosting Bundle für .Net9	4
2.3	Installation von SQL Server 2025 Express	4
2.4	Ersteinrichtung der Datenbank	4
2.4.1	Erstellung der Anwendungsdatenbank	5
2.4.2	Erstellung der Anmeldung	5
2.5	Installation von WireGuard	6
3	Konfiguration der TMS-Website	7
3.1	Einrichtung des Website-Verzeichnisses	7
3.2	Vorbereitung der „appsettings.json“-Datei	7
3.2.1	ConnectionString	7
3.2.2	Systemlog	7
3.2.3	Lizenzinformation	7
3.2.4	Datenbankmigration	8
3.2.5	E-Mail-Dienst	8
4.1	Erstellung des Anwendungspools	11
4.2	Einstellung der HTTPS-Bindung	11
4.3	Einbindung der Anwendung	11
4.4	Einrichtung der Anwendungsberechtigungen	12
4.5	Start der Anwendung	12

1 Einleitung

Das Terminalmanagementsystem (TMS) von CHERRY dient zur zentralen Verwaltung und Administration von Kartenterminals wie das CHERRY eHealth Terminal ST-1506. Über eine intuitive Frontend-Schnittstelle wird die Konfiguration von Kartenterminals sowohl im Staging-Prozess als auch im Feld ermöglicht.

Die Anbindung der Kartenterminals an das TMS funktioniert unabhängig von dem Verbindungsstatus des Kartenterminals zum Konnektor. Die Anbindung ist auch möglich, wenn das Kartenterminal nicht mit dem Konnektor verbunden ist.

Ebenfalls bietet das TMS die notwendigen Konnektorfunktionen, um einen täglichen Betrieb mit und um das Kartenterminal zu ermöglichen, wie z.B. Pairing der Kartenterminals, Zuordnung zu Arbeitsplätzen usw.

Für den Anwender stellt sich das TMS als Browseranwendung dar und wird über eine IP-Adresse oder URL aufgerufen.

Auf der Plattform, auf der das TMS betrieben wird, erfolgt die Einbindung eines Verzeichnisses mit der kompilierten .NET-Applikation in den entsprechenden Applikationsserver IIS (Internet Information Services). Die .NET-Applikation läuft nur mit der .NET-Runtime-Version, die als Bundle installiert wird.

Das TMS kann nur unter den Betriebssystemen Windows und Linux installiert werden. Für eine Installation unter Linux wird auf die entsprechende Docker-Installationsanleitung verwiesen (https://ehealth.cherry.de/TMS/TMS_Docker_Installationsanleitung_V1.0.pdf).

Diese Installationsanleitung beschreibt die überwiegend manuelle Installation unter Windows 2022 oder höher und erläutert die notwendigen Konfigurationen sowohl für den E-Mail-Server als auch für WireGuard. Als Datenbanksystem wird Microsoft SQL Server lokal installiert. Falls eine externe Datenbank genutzt wird, entfällt die lokale Datenbankinstallation.

2 Vorbereitung

Folgende Installationen müssen zunächst durchgeführt werden.

2.1 Installation von IIS (Internet Information Server)

Geben Sie über Powershell als Administrator folgenden Befehl ein:

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

2.1.1 Import/Erstellung des SSL-Browserzertifikats

1. Öffnen Sie die IIS-Console.
2. Klicken Sie links unter „Verbindungen“ in der Verzeichnisstruktur auf den ersten Knotenpunkt, der mit dem Server-Namen gekennzeichnet ist.
3. Suchen Sie auf der mittleren Startseite nach „Serverzertifikate“ und öffnen diese Anwendung. Sofern Sie ein eigenes SSL-Zertifikat besitzen, können Sie dieses importieren.
4. Sie haben auch die Möglichkeit, ein Self-Signed-Zertifikat zu erzeugen. Dazu klicken Sie auf „Selbstsigniertes Zertifikat erstellen...“ und vergeben auf der rechten Leiste einen Namen. Als Zertifikatsspeicher wählen Sie „Webhosting“ aus.

2.2 Installation von Hosting Bundle für .Net9

Wichtig: Bei der Installation des Hosting Bundles muss IIS bereits installiert sein!

1. Suchen Sie unter [Download .NET 9.0 \(Linux, macOS, and Windows\) | .NET](#) nach dem Eintrag „Hosting Bundle“ unter „ASP.NET Core Runtime 9.X.X“.
2. Klicken Sie auf den entsprechenden Link, um das Hosting Bundle der .net9-Runtime zu installieren. Diese Installation liefert die notwendige Runtime-Umgebung für die TMS-Applikation.

2.3 Installation von SQL Server 2025 Express

1. Laden Sie auf der Microsoft-Seite die Installationsdatei von SQL Server 2025 Express und installieren Sie diese.
2. Nach der Installation erhalten Sie das Angebot, die Anwendung „SQL Server Management Studio 21“ zu installieren. Nehmen Sie dieses Angebot wahr. Über das SSMS wird die Datenbank eingerichtet.

2.4 Ersteinrichtung der Datenbank

Die Ersteinrichtung der Datenbank erfolgt in folgenden Schritten:

1. Öffnen Sie das SSMS.

Das Fenster „Verbinden“ erscheint.

2. Ihnen wird als Servername die Verbindung „ServerName/SQLEXPRESS“ vorgeschlagen. Übernehmen Sie diesen Vorschlag.
3. Wählen Sie als Authentication „Windows-Authentifizierung“ aus.
4. Setzen Sie das Flag „Trust Server Certificate“.
5. Klicken Sie auf „Verbinden“.

Es öffnet sich der Datenbankknoten mit u. a. den Unterpunkten „Datenbanken“ und „Sicherheit“.

6. Klicken Sie mit der rechten Maustaste auf den obersten Knotenpunkt und rufen Sie den Menüpunkt „Eigenschaften“ auf.
7. Navigieren Sie im aktiven Fenster zum Reiter „Sicherheit“.
8. Aktivieren Sie unter „Serverauthentifizierung“ die Option „SQL-Server und Windows-Authentifizierungsmodus“ und bestätigen Sie dies mit „OK“.

2.4.1 Erstellung der Anwendungsdatenbank

1. Klicken Sie mit der rechten Maustaste auf den Knotenpunkt „Datenbanken“ und wählen Sie den Punkt „Neue Datenbank“ aus.
2. Tragen Sie im geöffneten Fenster den Datenbanknamen „TMS.Konnektor“ ein und klicken Sie auf „OK“.

Die Datenbank wird erstellt.

2.4.2 Erstellung der Anmeldung

Die Anwendung wird über eine Benutzeranmeldung auf die Datenbank zugreifen. Die Anmeldung wird wie folgt erstellt:

1. Klicken Sie in der SSMS-Konsole unter dem Knotenpunkt „Sicherheit“ mit der rechten Maustaste auf „Anmeldungen“.
2. Wählen Sie „Neue Anmeldung...“ aus.
3. Geben Sie im aktiven Fenster unter der Seite „Allgemein“ zunächst einen Anmeldenamen ein (z.B. „TMS“).
4. Wählen Sie als Authentifizierungsoption „SQL-Authentifizierung“ aus.
5. Tragen Sie hier ein Kennwort ein und bestätigen Sie die Eingabe.
6. Wählen Sie den Punkt „Kennwortrichtlinie erzwingen“ ab, um das automatische Ablaufen des Kennwortes zu vermeiden.
7. Wählen Sie auf der Seite „Benutzerzuordnung“ in der oberen Darstellung die Datenbank „TMS.Konnektor“ aus und klicken Sie dann die Rollen „db_owner“ und „db_securityadmin“ an.
8. Klicken Sie zur Übernahme „OK“.

2.5 Installation von WireGuard

Falls Sie die WireGuard-Funktionen des TMS nutzen wollen, installieren Sie WireGuard für Windows (<https://www.wireguard.com/install/>).

3 Konfiguration der TMS-Website

3.1 Einrichtung des Website-Verzeichnisses

1. Erstellen Sie ein Verzeichnis möglichst auf der obersten Verzeichnisstruktur, z.B. „C:/Website“.
2. Erstellen Sie zwei weitere Verzeichnisse „C:/Website/logs“ und „C:/Website/TMS.Konnektor“.
3. Kopieren Sie die gesamten Website-Anwendungsdateien des TMS, die Sie von CHERRY erhalten haben, in das Verzeichnis „C:/Website/TMS.Konnektor“.

3.2 Vorbereitung der „appsettings.json“-Datei

1. Suchen Sie unter den Website-Anwendungsdateien die Datei „appsettings.json“ oder alternativ die Datei „appsettings.Production.json“.
2. Öffnen Sie diese in einem Texteditor (z.B. Notepad++). Beachten Sie, dass Sie die json-Struktur der Datei nicht verändern, ansonsten startet die Anwendung nicht.

3.2.1 ConnectionString

1. Geben Sie unter „ConnectionStrings:TMSContext“ folgenden Text ein:

```
Server=localhost\\SQLEXPRESS;Database=TMS.Konnektor;User  
Id=TMS;Password=XXXX;TrustServerCertificate=true;
```

2. Für XXXX geben Sie das Passwort ein, das Sie für die Anmeldung in der Datenbank eingegeben haben. Alternativ geben Sie für „localhost“ den Namen der Plattform ein.

3.2.2 Systemlog

Geben Sie unter „Serilog:WriteTo:Args:path“ das Verzeichnis und den Namen der Log-Datei für das Systemlog unter der Beachtung der doppelten Trennungszeichen „\\“ ein:

```
C:\\Website\\logs\\TMSService.log
```

3.2.3 Lizenzinformation

Die Lizenzinformationen müssen vor dem ersten Start der Anwendung in die appsettings eingetragen werden. Sie erhalten von CHERRY die folgenden Informationen zur Lizenz:

- Installation
- Kundenkennung
- Kundenschlüssel

Diese Information tragen Sie in die entsprechenden Felder der json-Datei ein.

3.2.4 Datenbankmigration

Sofern Sie die TMS-Anwendung noch nicht gestartet haben, geben Sie unter „Migration:Aktiv“ ein „Ja“ ein. Das bedeutet, dass beim ersten Start in der Datenbank die notwendigen Tabellen und Stammdaten erzeugt werden. Die entsprechenden Importdateien werden unter „Migration:Dateien“ gelistet und mit der Anwendung ausgeliefert.

Hinweis: Die Migrationsdateien befinden sich im Verzeichnis „/wwwroot/database/mssql“ der Installation der Anwendungsdateien.

3.2.5 E-Mail-Dienst

Zur Einrichtung des E-Mail-Dienstes stehen verschiedene Optionen zur Verfügung. Über den E-Mail-Dienst versendet das TMS für verschiedene Zwecke E-Mails, z.B. für die Einrichtung eines Benutzers oder die Versendung eines Berichtes im Monitoring.

Es werden sowohl Zugriffe über SMTP mit Basic Authentication als auch über OAuth2 (Open Authorization) unterstützt. Bei Verwendung eines Microsoft-Dienstkontos kann zusätzlich der Zugriff über Microsoft Graph aktiviert werden.

Die folgenden Konfigurationsbeispiele zeigen die verschiedenen Möglichkeiten auf:

Beispiel 1: SMTP von Microsoft ohne OAuth2

```
"EmailSender": {
  "FromName": "CHERRY Terminalmanagementsystem (no-reply)",
  "FromEmail": "tms@cherry.de",
  "Host": "smtp-mail.outlook.com",
  "Port": 587,
  "EnableSSL": 3, //0 = none, 1=Auto, 2=TLS, 3=StartTLS
  "UserName": "tms@cherry.de",
  "Password": "xyz1234",
  "SecretIsEncrypted": "encrypt"
}
```

Dieses Beispiel zeigt die Konfiguration für den Zugriff auf ein Microsoft-Konto über SMTP.

Für `SecretIsEncrypted` stehen 3 Optionen zur Verfügung:

1. `false` → Das Passwort ist nicht verschlüsselt angegeben.
2. `true` → Das Passwort ist verschlüsselt angegeben.
3. `encrypt` → Das Passwort wird beim Start der TMS-Anwendung zunächst verschlüsselt und in der `appsettings` mit `SecretIsEncrypted = „true“` eingetragen.

Wenn Sie lokale ungesicherte SMTP-Server ohne Authentifikation nutzen, werden die Felder `UserName` und `Password` nicht angegeben.

Beispiel 2: Google-Privatkonto mit OAuth2

```
"EmailSender": {
  "FromName": "Max Mustermann",
  "FromEmail": "max.mustermann@gmail.com",
  "Host": "smtp.gmail.com",
  "EnableSSL": 3, //0 = none, 1=Auto, 2=TLS, 3=StartTLS
  "SecretIsEncrypted": "false",
  "AccountType": "Google",
  "OAuth2": {
    "ClientId": "XXXXYYYYZZZZ",
    "ClientSecret": "AAABBBBCCCC",
    "RefreshToken": "1//03q5... "
  }
}
```

`SecretIsEncrypted` bezieht sich in diesem Beispiel auf die beiden Einträge `ClientSecret` und `RefreshToken`.

Die Informationen zu `ClientId` und `ClientSecret` erhalten Sie in der Google Cloud Console (<https://console.cloud.google.com>), nachdem Sie sich dort angemeldet haben und ein Projekt erstellen.

Ein `RefreshToken` wird hier gesetzt, da der `Access-Token` nur eine Stunde gültig ist. Wie ein `RefreshToken` für ein Google-Konto erzeugt wird, erfahren Sie über die Google-Hilfe im Internet.

Beispiel 3: Microsoft-Konto über Graph

```
"EmailSender": {
  "FromEmail": "tms@cherry.de",
  "Host": "graph.microsoft.com",
  "SecretIsEncrypted": "false",
  "AccountType": "Microsoft",
  "OAuth2": {
    "TenantId": "5e0e1b52-21b5-4e7b-83bb-612ec460677e",
    "ClientId": "c60a5637-cffe-4602-85b2-cc62a4f2552e",
    "ClientSecret": "YwFRf..."
  }
}
```

`SecretIsEncrypted` bezieht sich in diesem Beispiel auf den Eintrag `ClientSecret`.

Die Parameter `TenantId`, `ClientId` und `ClientSecret` erhalten Sie über das Microsoft Entra Admin Center (<https://entra.microsoft.com>) unter dem entsprechenden Konto.

Durch die Eingabe des Hosts durch „graph.microsoft.com“ wird der Zugriff via Graph aktiviert. In diesem Fall wird die Berechtigung „Mail.Send“ als Berechtigung im Entra Admin Center konfiguriert, damit das TMS E-Mails versenden kann.

4 Konfiguration von IIS

4.1 Erstellung des Anwendungspools

1. Öffnen Sie die IIS-Console.
2. Klicken Sie in der Verzeichnisstruktur links unter „Verbindungen“ auf den ersten Knotenpunkt, der mit dem Server-Namen gekennzeichnet ist.
3. Aktivieren Sie mit der rechten Maustaste den Knotenpunkt „Anwendungspool“ und wählen den Punkt „Anwendungspool hinzufügen...“ aus.
4. Geben Sie im geöffneten Fenster den Namen „TMS.Konnektor“ ein und wählen unter „.NET CLR Version:“ den Punkt „Kein verwalteter Code“ aus.
5. Bestätigen Sie mit „OK“.
6. Klicken Sie mit der rechten Maustaste im mittleren Fenster auf den erzeugten Anwendungspool-Datensatz und wählen Sie den Punkt „Erweiterte Einstellungen“ aus.
7. Setzen Sie folgende Parameter:
 - Identität (Gruppe Prozessmodell) => LocalSystem
 - Leerlauftimeout (Gruppe Prozessmodell) => 0
 - Regelmäßiges Zeitintervall (Gruppe Wiederverwendung) => 0
8. Bestätigen Sie mit „OK“.

4.2 Einstellung der HTTPS-Bindung

1. Klicken Sie in der Verzeichnisstruktur links unter „Verbindungen“ mit der rechten Maustaste auf „Default Web Site“.
2. Wählen Sie „Bindungen bearbeiten“.

Wird kein Datensatz des Typs „https“ im geöffneten Fenster dargestellt, erstellen Sie diesen wie folgt:

1. Klicken Sie auf „Hinzufügen“.
2. Geben Sie als Typ „https“ an.
3. Wählen Sie als SSL-Zertifikat das bereits vorbereitete Zertifikat (Import/Erstellung des SSL-Browserzertifikats) aus.
4. Bestätigen Sie mit „OK“.

4.3 Einbindung der Anwendung

1. Klicken Sie in der Verzeichnisstruktur links unter „Verbindungen“ mit der rechten Maustaste auf „Default Web Site“.
2. Wählen Sie „Anwendung hinzufügen...“.
3. Geben Sie als „Alias“ den Text „TMS.Konnektor“ ein.

4. Wählen Sie Anwendungspool „TMS.Konnektor“ aus.
5. Tragen Sie unter „Physischer Pfad“ das Verzeichnis „C:/Website/TMS.Konnektor“ ein, unter dem Sie die Anwendungsdateien gespeichert haben.
6. Bestätigen Sie mit „OK“.

4.4 Einrichtung der Anwendungsberechtigungen

1. Klicken Sie mit der rechten Maustaste auf die erstellte Anwendung „TMS.Konnektor“.
2. Wählen Sie den Punkt „Berechtigungen bearbeiten...“ aus.
3. Gehen Sie im geöffneten Fenster auf den Reiter „Sicherheit“.

Wenn im Fenster unter „Gruppen- und Benutzernamen“ der Eintrag „IIS_IUSERS“ fehlt, müssen Sie diesen nachtragen. Dazu gehen Sie wie folgt vor:

1. Klicken Sie auf „Bearbeiten“ → „Hinzufügen“ → „Erweitert“.
2. Klicken Sie auf „Jetzt suchen“, um im geöffneten Fenster nach den Benutzergruppen zu suchen.
3. Klicken Sie auf den Eintrag „IIS_IUSERS“ in den Suchergebnissen.
4. Bestätigen Sie mit „OK“.
5. Wiederholen Sie die Bestätigung für jedes geöffnete Fenster.

4.5 Start der Anwendung

1. Klicken Sie in der IIS-Konsole mit der rechten Maustaste auf den ersten Knoten in der linken Leiste „Verbindungen“.
2. Wählen Sie den Punkt „Starten“.
3. Zum Stoppen der Anwendung wählen Sie den Punkt „Beenden“.

Nach dem Start öffnen Sie den lokalen Browser und geben die URL <https://localhost/TMS.Konnektor> ein, um auf das TMS zuzugreifen.

Wenn Sie die Anwendung außerhalb der Plattform von einem anderen Computer aus starten wollen, geben Sie die IP-Adresse der Installationsplattform statt „localhost“ ein.

Nach dem Erststart startet die Login-Maske des TMS.