K-SOFT
iT-Center

Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath

Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de

Erkrath im November 2025

Sehr geehrte Anwender: innen,

dieses Dokument unterstützt Sie bei der Umstellung und Einrichtung des Flottenmanagers auf die Version 10.9.x

Wesentliche Hinweise und umzusetzende Schritte

- Hinweise
  - Hohe Passwortverschlüsselung wurde umgesetzt (Erklärung letzte Seite)
  - Deutliche Erweiterung der Flottenmanager Web-Version
  - Download der Updates nur noch über das FmWeb

- Schritte
  - Deaktivierung des alten TaskCentre (sofern noch im Einsatz)
  - Installation und Einrichtung des neuen FmWeb.Blazor Service

Voraussetzung für das Update auf dem Server

- Windows Server 2016 bis 2025
- Microsoft SQL-Server 2016 bis 2022 (auch Express)
- Microsoft .NET Framewort 9.x

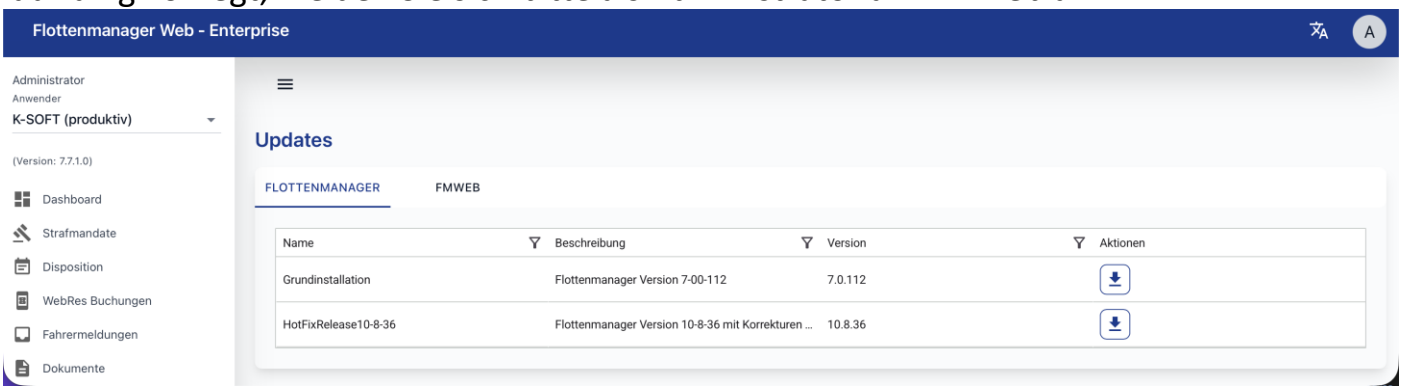
Bevor Sie starten, sollten Sie sicherstellen

- Das Sie den Flottenmanager in der Version 10.8.36 lauffähig installiert haben
- Das FmWeb in Version 7.6.7 muss installiert und lauffähig sein

Sollten Sie das FmWeb noch nicht installiert haben und noch mit dem TaskCentre-Dienst arbeiten, benötigen Sie einen Umstellungstermin. Über die Flottenmanager.net-Seite können Sie diesen hier buchen. Der Aufwand liegt i.d.R. bei 30 bis 45 Minuten.
Wir weisen darauf hin, dass kurzfristig nur bedingt Termine für eine Unterstützung zur Verfügung stehen und Sie benötigte Hilfe rechtzeitig buchen.

Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath
Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de

So fern wie oben beschrieben der Flottenmanager 10.8.36 und FmWeb.Blazor 7.6.7 lauffähig vorliegt, melden Sie sich bitte als Administrator am FmWeb an:



Unter Systemadministration/Updates im Menü finden Sie den aktuellen Hotfix sowie die aktuelle FmWeb7.7.6

Das Hotfix kann **nach** der Installation und Einrichtung von FmWeb wie gewohnt installiert werden!

Bei laufendem <u>Taskcenter-Service</u>
muss dieser nicht nur beendet, sondern auch künftig **deaktiviert** werden! Anschließend kann die zu Verfügung gestellte FmWeb7.6.7 auf dem C: \ Laufwerk unter C: \FmWeb entpackt werden. In der appsettings.json müssen entsprechende Einträge mit einem Editor von der Administration konfiguriert werden! Details dazu weiter unten im Dokument.

Bei laufendem <u>FmWeb.Blazor-Service</u>
muss vor dem Update diese in der Windows-Server-Aufgabenplanung gestoppt werden! Anschließend sollte das bestehende FmWeb-Verzeichnis umbenannt werden z.B. FmWeb7.6.7. Danach kann das ZipFile der FmWeb7.7.6 zu C: \FmWeb entpackt werden.

<u>Wichtig</u>
Bitte nicht nur die Datei appsettings.json aus dem alten Verzeichnis in das neu kopieren und überschreiben. Damit fehlen Ihnen die neuen benötigten Konfigurations-möglichkeiten!

Es sollten alle Kundensystemspezifischen Einstellungen einzeln in die neue Datei kopiert werden. Weiteres folgt in einer Beschreibung zur appsettings.json Datei weiter unten.

Blau	SQL-SERVER connect
Ocker	Server-URL für den nativen Client
Braun	Publizierte Web-Adresse im Intranet mit Ports (https:// auskommentiert – Zertifikat wird dafür benötigt!)
Grün	Wird (optional) für die Fahrer-Rückmeldung aus dem Fahrzeug benötigt

Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath

Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de

appsettings.json Datei-Inhalt

```
{
 "AllowedHosts": "*",
 "ConnectionStrings": {
  "FpSystemContext": "Server=SERVERNAME\\SQL2022;Database=FPSystem;User
Id=Flottenmanager;Password=Flottenmanager;MultipleActiveResultSets=true;TrustServerCertificate=True",
  "TenantContextTemplate": "Server= SERVERNAME\\SQL2022;Database=Flottenmanager{0};User
Id=Flottenmanager;Password=xxxxxxxxxx;MultipleActiveResultSets=true;TrustServerCertificate=True"
 },

 //ServerURL - setzt FmWebUrl - kritisch für nativen und Webclient
 "ServerUrl": "http://SERVERNAME:9998",

 "Kestrel": {
  "Endpoints": {
   //"Https": {
   //  "Url": "https://localhost:445"
   //},
   "Http": {
    "Url": "http://*:9998"
   }
  }
 },

// Einrichtung für Fahrer-Rückmeldungen (optional)
 "UpdateUrl": "https://api-fmweb-prod.cloudkasten.net/",
 "Tunnel": {
  "Token":
"eyJhIjoiOWJkMGRlY2NmNzUxNxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxQ4MS00YTE2LTllYzAtNzg1MDFmNThmxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxbFl6SmlOR0kxT1RVNCJ9"
 },
 "feature_management": {
  "feature_flags": [
   {
    "id": "UseTextInputForDriversLogin",
    "enabled": false
   },
   {
    "id": "Beta",
    "enabled": false
   }
  ]
 },
 "OpenIdConnect": {
  "Enabled": false,
  "Authority": "",
  "ClientId": "",
  "ClientSecret": "",
  "Scope": "openid profile email",
  "ResponseType": "code",
  "SaveTokens": true,
  "UsePkce": true
 }
}
```

Speichern sie die Datei appsettings.json und starten den Dienst FmBlazor.exe zunächst im Direktfenster!
Sollten beim Start Fehler auftreten, werden diese im Fenster aufgelistet.
Wenn der Start ohne Fehler erfolgte und auf dem Server mit localhost:Port die Anmeldeseite erscheint, können Sie wie auf den kommenden Seiten beschrieben die App in die Aufgabenplanung eintragen.
Ein Fehler beim Start, könnte das Fehlende .NET Framework 9.x sein.

Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath
Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de

Der Service FmWeb.Blazor muss laufen, sonst ist ein Anmelden über den Fuhrpark-Client nicht möglich.

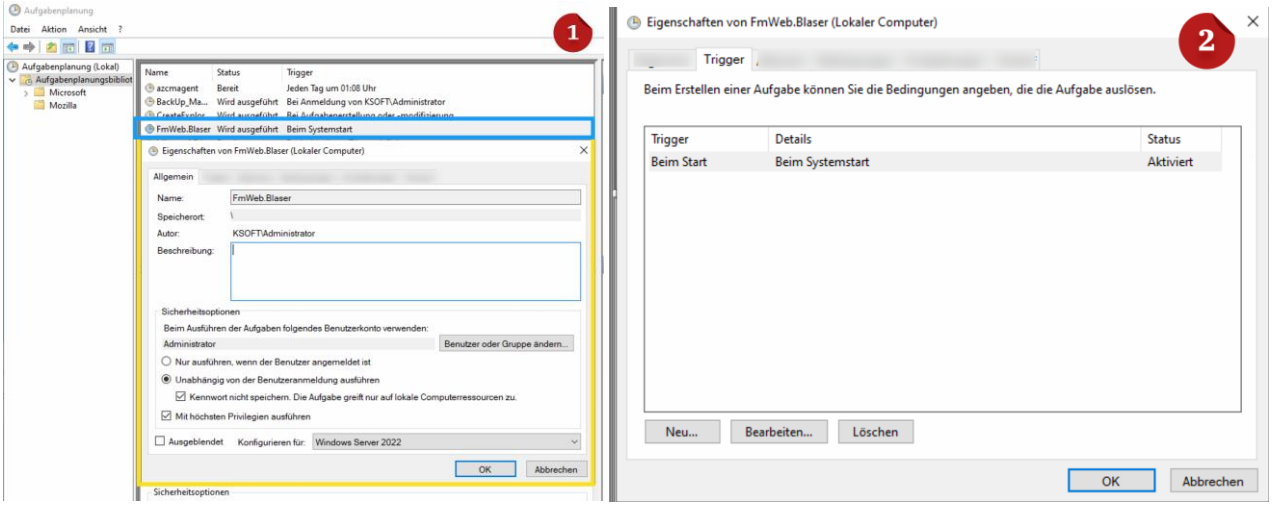
Um dies sicherzustellen, z.B. bei einem Serverneustart (nach Systemupdates), sollte über die Aufgabenverwaltung der Start der Anwendung zeitverzögert mit Parameter automatisiert werden. Auch eine Überwachung des Dienstes mit bestehenden Tools, ob der Dienst läuft, ist ratsam.

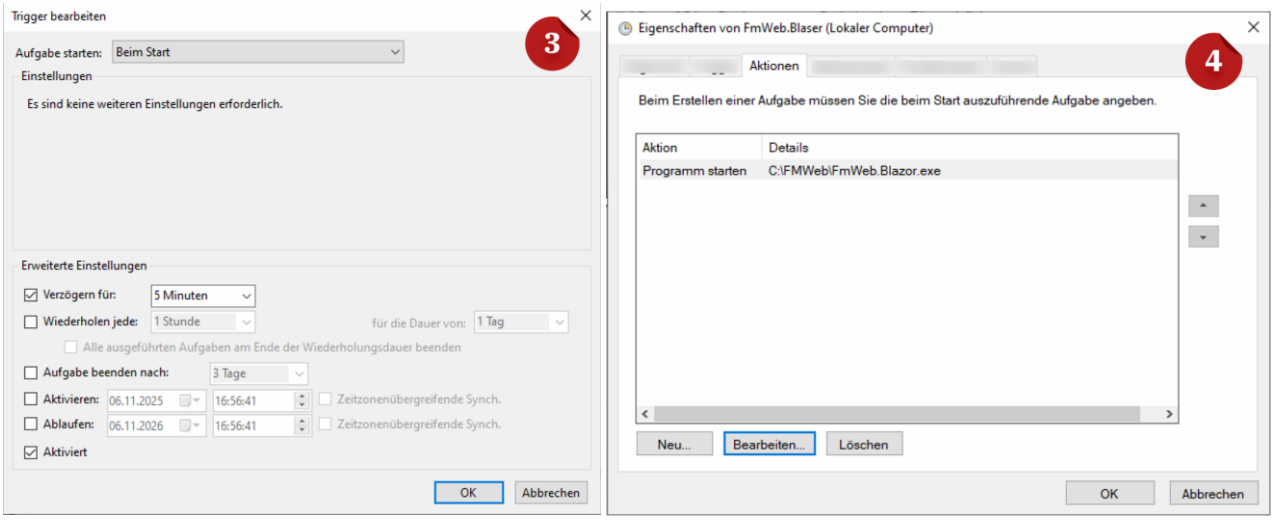
Bei nicht ausgeführtem FmWeb.Blazor ist

- Ein Anmelden mit dem nativen Client nicht möglich
- Steht das Portal für die Fahreranmeldung nicht mehr zur Verfügung
    - Keine Fahrzeugbuchungen und Rückmeldungen mehr möglich
- Werden keine E-Mails (z.B. zur Führerscheinkontrolle) versendet
- Keine Rückmeldungen vom FleetSync- und YellowFox-Task abgeholt

Einrichtung der Aufgabenplanung

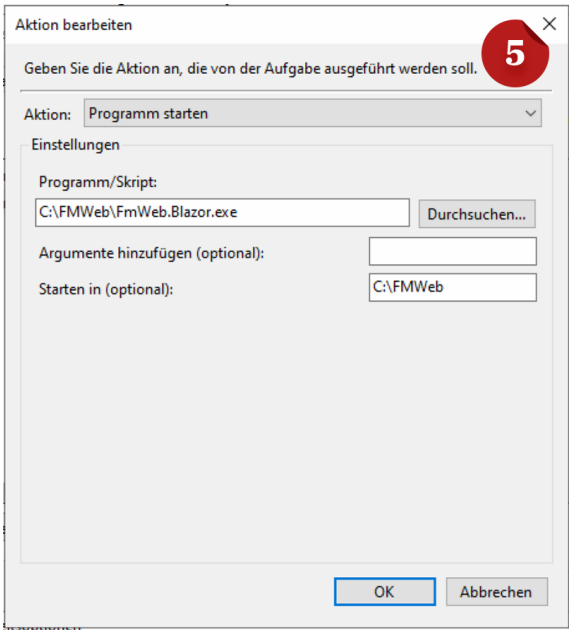
Achten Sie bitte auf exakt gleiche Einstellungen:

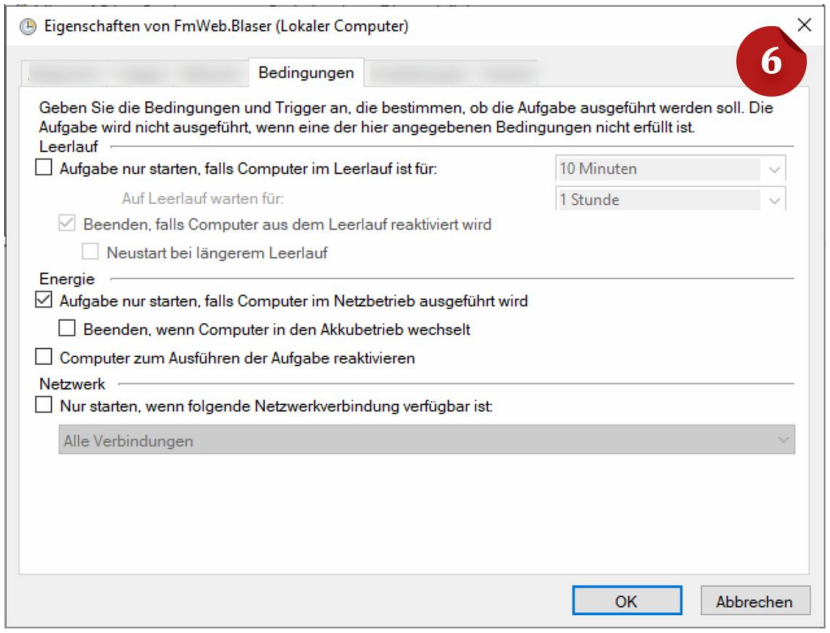


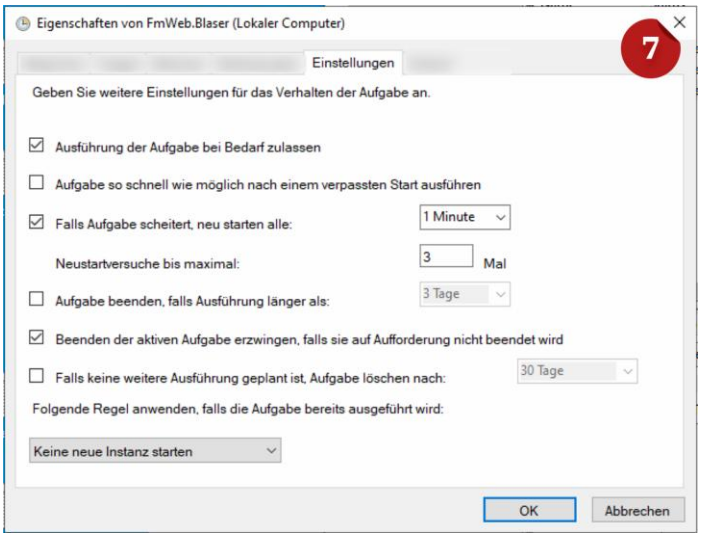


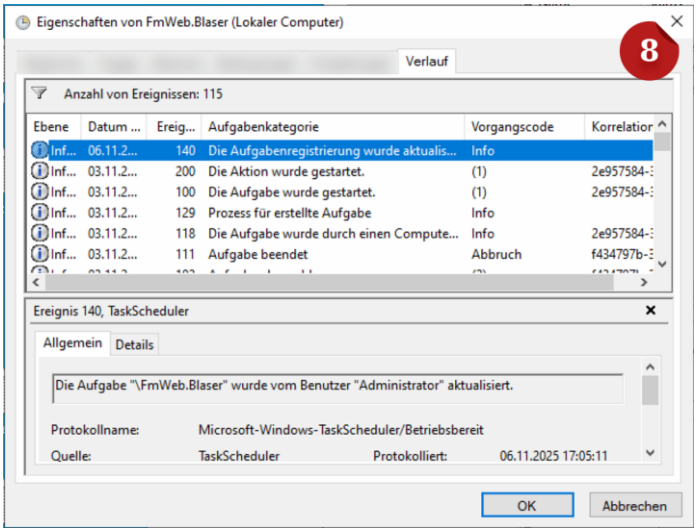
Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath

Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de









Zertifikate

Um die Applikation als https://SERVERNAME:PORT laufen zu lassen, müssen Sie selbst ein Zertifikat einrichten. Es ist zu empfehlen, wenn möglich, den Ortner „Cert“ nicht in den FmWeb-Ortner zu legen, da dieser sonst bei jedem Update auch in den neuen Versions-Ordner kopiert werden muss. Dies wird leider oft vergessen!

Michael Kombüchen
Niermannsweg 11-15
D – 40699 Erkrath
Tel +49 2104 – 233 880
Sup +49 2104 – 233 8822
Mail info@k-soft.de

Passwörter

Alle Passwörter werden nun ausschließlich gehasht und gesalzen gespeichert. Das bedeutet:

- Keine Klartext-Speicherung: Passwörter liegen nie im System lesbar vor.
- Individuelles Salt pro Passwort: Jedes Passwort erhält einen eigenen, kryptographisch starken Zufallswert. Damit werden auch gleiche Passwörter stets unterschiedlich gespeichert.
- Verwendung eines etablierten Standards (PBKDF2 mit SHA-256, 100.000 Iterationen): Dieses Verfahren gilt als sicherer Branchenstandard, vergleichbar mit bcrypt oder Argon2, und macht ein Ausprobieren von Passwörtern für Angreifer äußerst aufwendig.
- Zukunftssichere Struktur: Durch unser Speicherformat können wir die Sicherheitsparameter (z. B. Iterationen) jederzeit an neue Best Practices anpassen.

Damit erfüllen wir den geforderten Punkt vollständig und stellen sicher, dass selbst im unwahrscheinlichen Fall eines Datenbanklecks Ihre Benutzerpasswörter geschützt bleiben.

Warum dieses Passwort-Hashing-Verfahren sicher ist

Kurz gesagt: Wir speichern **niemals** Ihr Klartext-Passwort. Stattdessen nutzen wir ein bewährtes, mehrstufiges Verfahren, das Angriffe teuer und unattraktiv macht.

Kernelemente der Sicherheit

- **Einweg-Ableitung statt simples Hashing**
  Wir verwenden **PBKDF2 mit SHA-256** (ein industrieller Standard). Dieser Algorithmus leitet aus dem Passwort einen Schlüssel ab – zurückrechnen ist praktisch unmöglich.
- **Individuelles, kryptografisch starkes Salt**
  Für **jedes** Passwort erzeugen wir mit einem kryptografischen Zufallszahlengenerator ein eigenes 16-Byte-Salt. Das verhindert Rainbow-Table-Angriffe und sorgt dafür, dass gleiche Passwörter **verschiedene** Ergebnisse liefern.
- **Absichtlich "langsam" (Work-Factor)**
  Durch **100.000 Iterationen** wird jede Prüfrechnung absichtlich verlangsamt. Das kostet legitime Nutzer*innen kaum Zeit, zwingt Angreifer aber zu massivem Rechenaufwand pro Versuch. (Den Work-Factor können wir bei Bedarf erhöhen, um mit der Hardware-Entwicklung Schritt zu halten.)
- **Konstante Vergleichszeit**
  Beim Prüfen verwenden wir einen **zeitkonstanten Vergleich**. So lassen sich aus Messungen der Antwortzeit keine Rückschlüsse auf Teiltreffer ziehen (Schutz vor Timing-Angriffen).
- **Update-fähiges Speicherformat**
  Wir speichern `Iterationen.Salt.Hash` (jeweils Base64). Dadurch können wir später die Iterationszahl erhöhen oder auf modernere Verfahren migrieren, ohne Passwörter neu anfordern zu müssen.

Was bedeutet das für Sie im Ernstfall?

Sollte jemand unbefugt eine Datenbankkopie erlangen, findet er dort **nur** zufällige Salts und aus PBKDF2 abgeleitete Werte. Ein Durchprobieren ("Brute Force") wird durch Salt **und** Iterationen aufwendig und teuer – insbesondere bei ausreichend langen, einzigartigen Passwörtern.