# KeyScan ScanApp - Dienst

Dieses Dokument dient der Anleitung zur Einrichtung des Dienstes zur Kommunikation mit der KeyScan ScanApp. Für die Verwendung des Dienstes wird keine zusätzliche Lizenz benötigt. Des Weiteren entfällt die Notwendigkeit, dass gleichzeitig eine KeyScan Programminstanz geöffnet sein muss. Der Dienst funktioniert vollkommen autark und übernimmt die Kommunikation sowie den Datenaustausch mit der KeyScan ScanApp.

## 1. Einrichtung

Die Einrichtung des Dienstes sollte durch einen erfahrenen Systemadministrator durchgeführt werden. Gerne sind wir Ihnen hierbei auch behilflich.

Der Dienst kann je nach Anwendungsfall auf einem lokalen PC oder einem gemeinsam genutzten Server installiert werden.

**Wichtige Voraussetzung!**

Sowohl die zum Dienst dazugehörigen Programme, als auch weitere notwendige Dateien müssen zwingenden in das Verzeichnis **C:\KeyScanService** kopiert werden.

Bitte legen Sie dieses Verzeichnis als Administrator an.

### 1.1. Dateien kopieren und entpacken

Im Installationsverzeichnis von KeyScan befindet sich der Unterordner „bin“. Dort findet sich die ZIP-Datei **KeyScanService.zip**, in der alle notwendigen Programme gepackt enthalten sind.

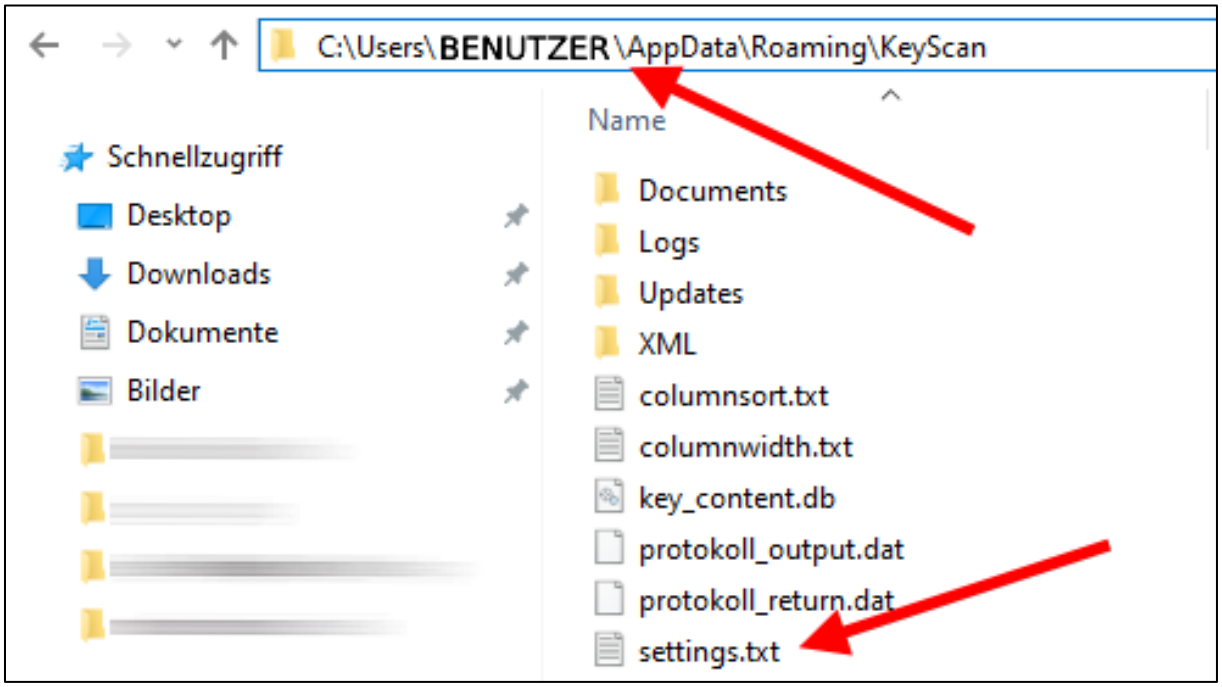
Entpacken Sie diese ZIP-Datei auf dem Server in das Verzeichnis C:\KeyScanService

Bitte starten Sie an diesem Punkt noch keines der Programme!

### 1.2. Einstellungen kopieren

Damit der Service die grundlegenden Einstellungen hat, muss die Datei **settings.txt** aus einem beliebigen, aber konfigurierten Benutzerprofil in das Zielverzeichnis C:\KeyScanService kopiert werden!

Die Einstellungsdatei befindet sich immer in den Benutzerprofilen unter C:\Users\JEWEILIGE BENUTZERKENNUNG\AppData\Roaming\KeyScan.




## 1.3. Voraussetzungen prüfen und ggf. weitere Dateien kopieren

Damit der Dienst problemlos funktioniert, ist es wichtig, die Voraussetzungen zu prüfen. Es ist darauf zu achten, dass die folgenden Punkte vom Computer, auf dem der Dienst laufen soll, erreichbar sind:

- Datenbankdatei: Wird die von uns mitgelieferte Datenbankdatei genutzt, muss diese in einem gemeinsam genutzten Verzeichnis abgelegt und erreichbar sein.
  *Eintrag in der settings.txt:* DBFile = Pfad zur Datenbankdatei
  *Ist dieser Eintrag leer, wird ein Microsoft SQL Server als Datenbank genutzt*

- MS SQL Server als Datenbank: Nutzen Sie einen eigenen Microsoft SQL Server als Datenbank, achten Sie bitte auf folgendes:
  - Die 32-Bit ODBC Verbindung zur Datenbank muss als System-DNS eingetragen sein und dieselbe Bezeichnung haben, wie bereits eingerichtet
  - Die Datei MSSQL.xml aus dem Benutzerprofil \XML muss in das Zielverzeichnis kopiert werden

  *Eintrag in der settings.txt:* MSSQLUSE = 1

- Dokumentenverzeichnis: Damit die von KeyScan automatisch generierten PDF-Protokolle richtig abgelegt werden können, muss auch hier ein gemeinsam genutztes Verzeichnis für die Dokumente erreichbar sein.
  *Eintrag in der settings.txt:* DocDir = Pfad zu den KeyScan Dokumenten

- Bestandsdaten aus Fremdsoftware (DOMUS, …): Bezieht KeyScan die Liegenschaften und Adressen aus einer fremden Datenbank, so muss auf folgendes geachtet werden:
  - Die 32-Bit ODBC Verbindung zur Datenbank muss als System-DNS eingetragen sein und dieselbe Bezeichnung haben, wie bereits eingerichtet

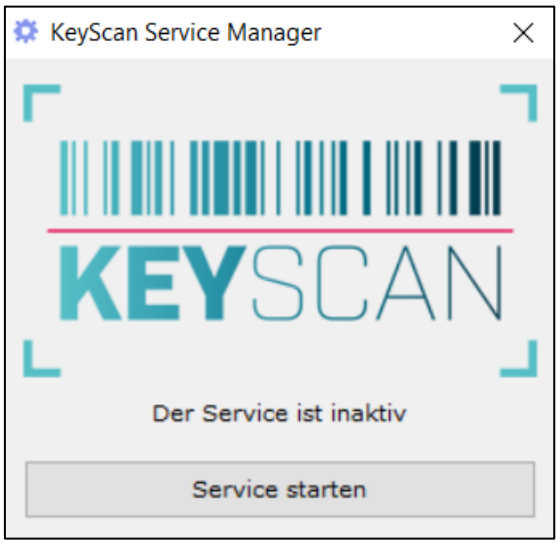
- Die Datei ODBCData.xml aus dem Benutzerprofil \XML muss in das Zielverzeichnis kopiert werden.

*Eintrag in der settings.txt:* UseODBC = 1

## 2. Service starten

Sobald alle Voraussetzungen getroffen sind, kann nun der Dienst-Manager gestartet werden. Dafür haben wir ein kleines Programm geschrieben, welches einen einfachen Überblick über den Status des Dienstes gibt und mit dessen Hilfe der Dienst jederzeit gestartet und auch beendet werden kann.

Starten Sie dazu das Programm **KeyScanServiceManager.exe**.




Hier können Sie sehen, ob der Dienst bereits aktiv ist oder nicht. Die Schaltfläche ermöglicht es Ihnen dann, den Dienst entsprechend zu starten. Der KeyScanServiceManager registriert den Dienst im System und startet diesen danach automatisch.

## 3. Status und Fehler

Der Service schreibt alle wichtigen Schritte in die Datei C:\KeyScanService**servicelog.txt**. Hier können Sie einsehen, ob alle notwendigen Module geladen und gestartet wurden. Sollte es zu Fehlern kommen, kann anhand der Fehlermeldung weitere gehandelt werden.

## 4. Netzwerk und Firewall Einstellungen

Befindet sich das Smartphone oder Tablet, auf dem die KeyScan ScanApp genutzt wird, per WLAN im gleichen Netzwerk wie der PC oder Server, auf dem der KeyScan Dienst läuft, sollte es grundsätzlich keine Probleme mit der Kommunikation geben.

Zur Problemfindung oder für andere Anwendungsfälle, bei denen das Smartphone oder Tablet evtl. nicht im gleichen Netzwerk ist, können die folgenden Schritte probiert werden. Wir weisen ausdrücklich darauf hin, dass dies durch einen erfahrenen Netzwerkadministrator erfolgen sollte!

Unter Windows können Dienste so konfiguriert werden, dass diese als sogenannte Netzwerkdienste ausgeführt werden und von außerhalb erreichbar sind. Hier die grundlegenden Schritte:

**1. Dienst als Netzwerkdienst konfigurieren:**

- Öffnen Sie den Dienst-Manager: Drücken Sie **Windows-Taste + R**, geben Sie **services.msc**
- Suchen Sie nach dem KeyScanApp Dienst, um diesen zu konfigurieren.
- Rechtsklicke auf den Dienst und **Eigenschaften** auswählen.
- Zum Tab **Anmelden** (oder ähnlich benannt) wechseln.
- Hier den **Netzwerkdienst** als Anmeldekonto auswählen.

**2. Portfreigabe in der Firewall:**

- Öffnen Sie die Windows-Firewall mit erweiterter Sicherheit: **Windows-Taste + R**, und **wf.msc** eingeben.
- Wählen Sie **Eingehende Regeln** und dann **Neue Regel**....
- Wählen Sie **Port** und klicken Sie auf **Weiter**.
- Wählen Sie **TCP** und geben Sie den Port ein, den der Dienst verwendet.
- Wählen Sie **Zulassen die Verbindung** und klicken Sie auf **Weiter**.
- Geben sie abschließend einen Namen und eine Beschreibung für die Regel ein und klicken Sie auf **Fertigstellen**.

**3. Externe Netzwerkkonfiguration:**

- Stellen Sie sicher, dass die Netzwerkhardware (Router, Firewall) so konfiguriert ist, dass eingehende Verbindungen zum entsprechenden Port an den betreffenden Computer weitergeleitet werden.

**4. Teste die Konfiguration:**

- Starte Sie den Dienst neu.
- Versuchen Sie nun, mit der KeyScan ScanApp einen beliebigen Schlüssel zu scannen.

Beachten Sie, dass das Öffnen von Ports und das Zulassen externer Verbindungen Sicherheitsrisiken mit sich bringt. Stellen Sie sicher, dass die notwendigen Sicherheitsvorkehrungen getroffen werden, um unautorisierten Zugriff zu verhindern.