Installation & Anwendung

Wiener Testsystem

Ab Version 8.26.00

SCHUHFRIED

passion for psychology

INHALTSVERZEICHNIS

Freigabe Revision L (Datum): 2024-01-27

1 VORWORT

Das Wiener Testsystem ist das Ergebnis von 25 Jahren Erfahrung in der computergestützten psychologischen Diagnostik. Es beinhaltet die gesamte Palette moderner Persönlichkeits- und Leistungsverfahren, die permanent gepflegt und weiterentwickelt werden. Das Spektrum der zu Verfügung stehenden Tests wird laufend erweitert – neben Testverfahren der „klassischen Testtheorie“ werden auf Basis innovativer Technologien und der „Modernen Testtheorie“ auch immer mehr adaptive und multimediale Verfahren entwickelt.

Die Bedienung des Wiener Testsystems ist einfach und verlangt keine computerspezifischen Kenntnisse. Mit Hilfe der übersichtlich aufgebauten Programmstruktur geben Sie Testverfahren vor, werten die Ergebnisse aus und verwalten die Daten. Die Testergebnisse können automatisch in Ihre Befunde, Gutachten, Berichte, etc. exportiert werden. Ein umfangreiches Hilfesystem unterstützt Sie bei Ihrer Arbeit.

Die durch das Qualitätsmanagement aufgestellten Richtlinien für Entwicklung und Produktion stellen lange Lebensdauer, hohe Ausfallsicherheit und Fehlerfreiheit unserer Produkte sicher. Qualifikation der Mitarbeiter und Qualität unserer Produkte werden laufend verbessert.

Gehen Sie bitte bei der Installation genau nach der vorliegenden Beschreibung vor. Sollten Sie Hilfe benötigen, stehen Ihnen die Mitarbeiter unseres Help Desk zur Verfügung:

E-Mail: support@schuhfried.com
Telefon: + 43 2236 42315–360
Fax: + 43 2236 46597

Wir wünschen Ihnen viel Freude und Erfolg bei der Arbeit mit dem Wiener Testsystem!

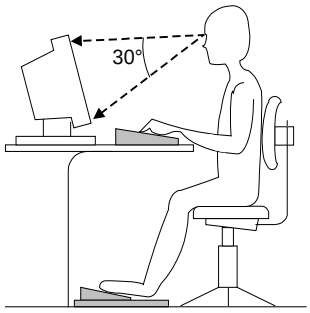
1.1 Zweckbestimmung

Das Wiener Testsystem ist die Softwarelösung der SCHUHFRIED GmbH zur computergestützten psychologischen Untersuchung. Das Einsatzgebiet reicht von individuellen Untersuchungen beziehungsweise Tests in der Personalpsychologie über die klinische Neuropsychologie, Verkehrspsychologie bis zur Sportpsychologie.
Die Tests im Wiener Testsystem sind breit gestreut und umfassen Intelligenztestbatterien, spezielle Intelligenztests, Leistungstests, Persönlichkeitstests sowie Einstellungs- und Interessentests. Die Tests basieren zum Teil auf "klassischer Testtheorie" oder auf "moderner Testtheorie". Es gibt adaptive und multimediale Verfahren. Die Tests sollen eine möglichst umfassende, möglichst objektive und möglichst valide psychologische Statusanalyse einer Person unterstützen. Auch für eine effektive Trainings- bzw. Interventionsplanung.

2 ERGONOMISCHE ANFORDERUNGEN AN DEN TESTPLATZ

Arbeitstisch und Sitzgelegenheit

Der Tisch und die Sitzhöhe der Sitzgelegenheit sollen so eingerichtet werden, dass in aufrechter Sitzposition gearbeitet werden kann. Der Blickwinkel auf den Bildschirm soll etwa 30 Grad betragen. Die Fußtasten müssen so aufgestellt sein, dass eine Betätigung in normaler Sitzposition möglich ist.



Optimale Höhe des Arbeitstisches

Beleuchtung

Arbeitsräume sollten durch Tageslicht belichtet sein. Sie müssen darüber hinaus mit einer ausreichend dimensionierten Beleuchtung versehen sein, die so anzuordnen ist, dass ein ausgewogener Kontrast zwischen Bildschirm und Arbeitsumgebung gewährleistet wird.
Der Bildschirm soll so aufgestellt werden, dass die Blickrichtung parallel zur Fensterfront erfolgt. Die Beleuchtung sollte sich nicht im Bildschirm spiegeln und nicht blenden. Ist aus räumlichen Gegebenheiten die „ideale“ Aufstellung des Bildschirmes nicht möglich, müssen durch andere geeignete Maßnahmen Blendwirkungen und Spiegelungen unterbunden werden.

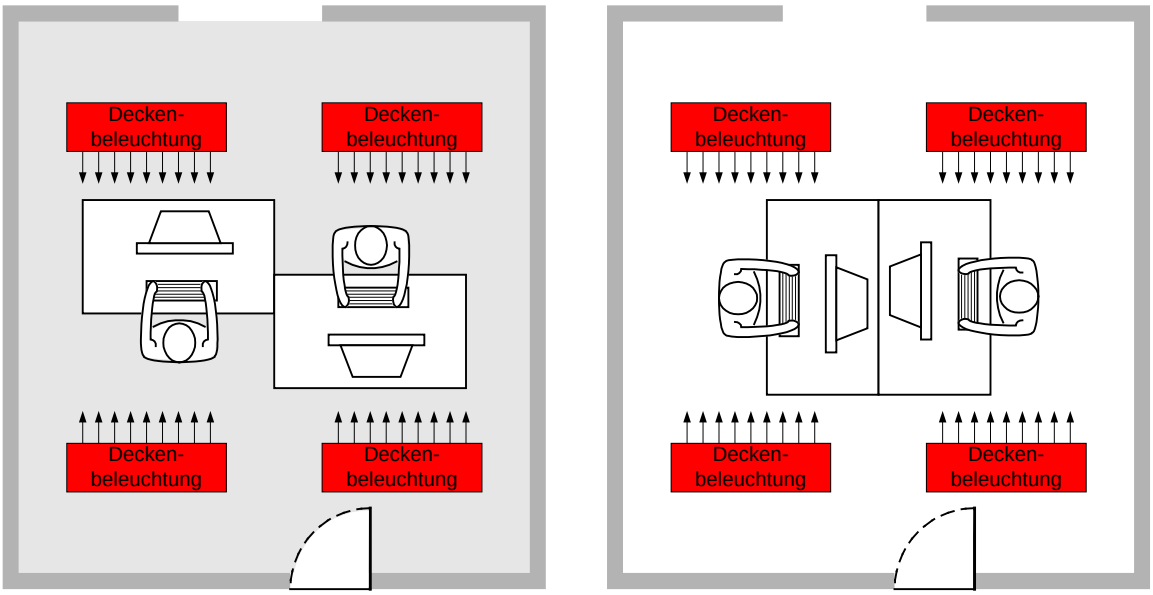


Abbildung 1: Falsche (links) und richtige (rechts) Positionierung des Arbeitsplatzes.

Lärm

Die Testung darf nicht durch Lärmeinwirkung gestört werden. Unter Berücksichtigung der von außen einwirkenden Geräuschen darf ein Lärmpegel von 50 dB(A) nicht überschritten werden.

Klima

Die Raumtemperatur an den Testplätzen muss zwischen 19 und 25 Grad Celsius liegen, die Luftgeschwindigkeit darf nicht mehr als 0,1 m/s betragen und die Luftfeuchtigkeit soll zwischen 30 und 70 Prozent bzw. bei Verwendung einer Klimaanlage zwischen 40 und 70 Prozent liegen.

Pausen

Die Einteilung der Pausen liegt unter Berücksichtigung der Belastbarkeit des Probanden in der Verantwortung des Psychologen. Bei Testbatterien können Pausen zwischen einzelnen Tests mit dem Programmmodul PAUSE eingefügt werden.

3 INSTALLATION DES WIENER TESTSYSTEMS

Die Eigenschaften von Windows erfordern, dass die folgenden Schritte genau eingehalten werden. **Installieren Sie zuerst das Wiener Testsystem, und schließen Sie die USB-Geräte erst nach der Installation an!**
Für Hilfe bei der Installation steht Ihnen unser HelpDesk (siehe Abschnitt 5.3) gerne telefonisch zur Verfügung.

3.1 Anschluss der Hardware

a. Packen Sie die Hardware des Wiener Testsystems aus und legen Sie sie bereit. Überprüfen Sie bitte, ob Ihr Computer genügend USB-Anschlüsse verfügbar hat; falls nicht, ist ein USB-Hub mit Netzteil nötig.
b. Schalten Sie den Computer ein und stecken Sie den USB-Stick mit der Installationssoftware, falls Sie diesen besitzen, an einem freien USB-Port an. Wenn Sie keinen USB-Stick besitzen, laden Sie das Setup über den Link in Ihrer E-Mail herunter. **Führen Sie zuerst die Installation des Wiener Testsystems** durch. Bei diesem Vorgang werden auch die Treiber installiert! **Falls Sie einen Lizenz-Dongle besitzen, stecken Sie diesen an einem weiteren freien USB-Port an.**
c. Der Testsystem-Dongle, die Probandentastaturen, die MLS-Arbeitsplatte und der Flimmer-Tubus sind USB-Geräte. Schließen Sie das **erste USB-Gerät** gemäß Abbildung 2 **nach der Installation** an den Computer an. In Kapitel 4 sind die einzelnen Peripherien und ihre Verkabelungen genau beschrieben.
d. Die **Periphere Wahrnehmung 2** wird mittels USB-Kabel an eine freie USB-Schnittstelle Ihres Computers angeschlossen. Der Zusammenbau der Peripheren Wahrnehmung 2 ist in Abschnitt 4.7 auf Seite 71 erläutert.
e. Freigegebene USB-Kopfhörer benötigen keine Treiberinstallation.

Hinweise:

- Falls Sie das USB-Gerät (Lizenz-Dongle) **vor der Installation** angeschlossen haben, kann es sein, dass Sie es abstecken und wieder anstecken müssen, damit es korrekt erkannt wird!
- Es ist notwendig, dass der **Port 1947** freigeschalten und nicht blockiert ist! Für die Kommunikation zwischen Server und Client (für Einzelplatzinstallation nicht relevant) müssen weitere Ports **am Server und am Client frei sein!** In der Regel sind das: 7001, 7011, 7012, 7013, 7014, 7015, 7016, 7017, 7018.
- Im Zuge der Installation wird Microsoft® SQL Server Express (genaue Version ist aus den Systemvoraussetzungen zu entnehmen) installiert. Bei Bedarf kann die Installation auf einem bereits installierten SQL Server durchgeführt werden.
- Mit der Tastenkombination **ESC + F5 bzw. ESC + E** kann eine Testdurchführung jederzeit unterbrochen werden. Bitte beachten Sie, dass es bei einigen Tests **nicht möglich** ist mit der Testung fortzufahren, da ein Neustart aufgrund von Lerneffekten die Testergebnisse beeinflussen kann.
- Das Wiener Testsystem kann ohne Abfrage von Benutzername und Passwort eingerichtet werden. In dem Fall kann nur ein Benutzer und ein Mandant angelegt werden! Bei Einrichtung weiterer Benutzer erscheint ein Anmeldedialog, in dem der gewünschte Benutzer ausgewählt werden kann.
- Sämtliche EXE-Dateien des Wiener Testsystems sind zertifiziert. Die Gültigkeit des zugrundeliegenden Zertifikats wird standardmäßig durch das Betriebssystem überprüft, wenn der Rechner in einem Netzwerk eingebunden ist. Falls der Rechner

keine Verbindung ins Internet hat, kann dies zu einer starken Verzögerung beim Starten der Administrationssoftware bzw. von Testverfahren führen. Dies kann vermieden werden, wenn die Zertifikatsüberprüfung im Internet über die Systemsteuerung von Windows abgeschaltet wird.

- Eine Remote-Installation mit einem HW-Dongle ist nicht möglich!

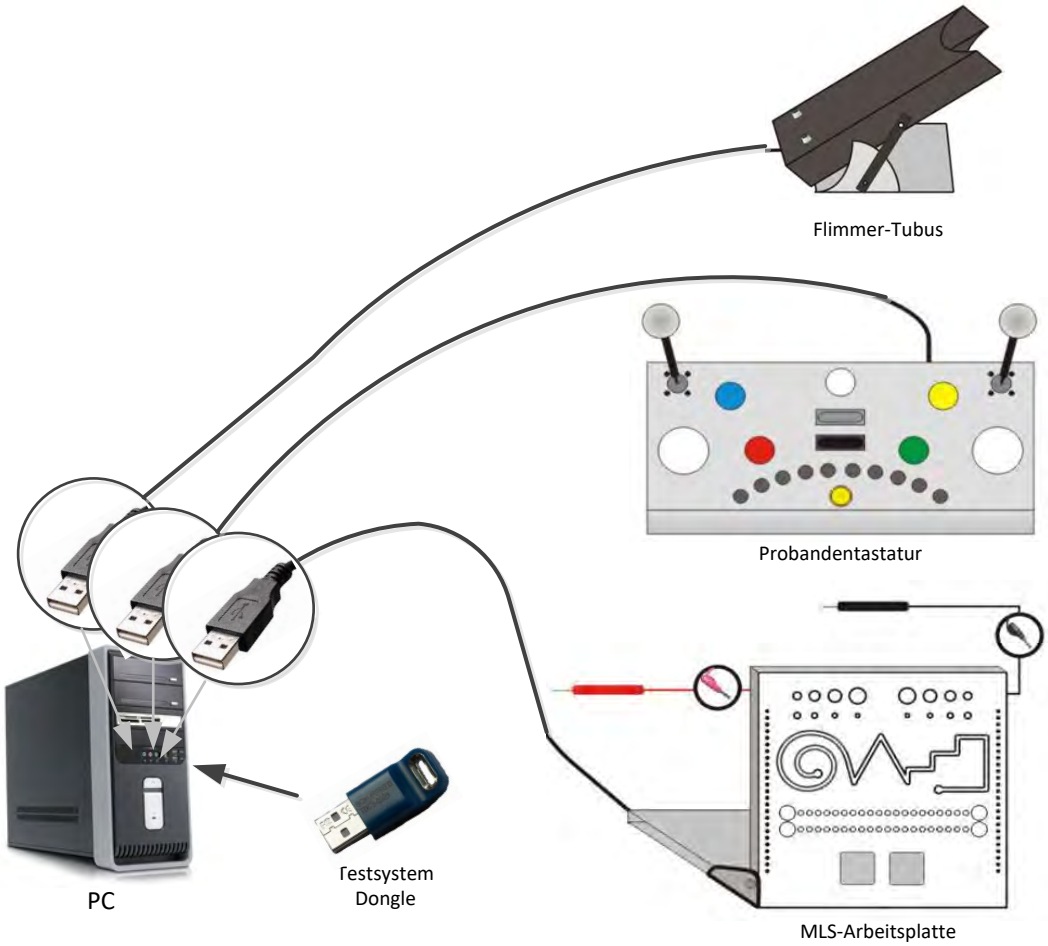


Abbildung 2: Anschluss der USB-Geräte an den PC

3.2 Software-Dongle – Erzeugung des Fingerprints

Bei Verwendung eines Software-Lizenz-Dongles muss **vor der Installation** des Wiener Testsystems ein Fingerprint des Computers, auf dem der Wiener Testsystem-Server installiert werden soll, erzeugt werden. Auf Basis dieses Fingerprints werden alle Lizenzen für das Wiener Testsystem, die in Zukunft benötigt und angefordert werden, bei SCHUHFRIED generiert. Diese neu erstellten Lizenzen werden Ihnen separat zugeschickt.

Zur Erzeugung des Fingerprints gehen Sie bitte wie folgt vor:

- Kopieren Sie aus dem Verzeichnis „**Tools**“ des Wiener Testsystems den Ordner „**GetFingerprint**“ in ein lokales Verzeichnis des Computers. Sie benötigen in diesem Verzeichnis Schreibrechte!
- Starten Sie das Programm „**GetFingerprint.exe**“.
- Es wird eine Datei mit der Endung „**c2v**“ im selben Verzeichnis erzeugt.
- Senden Sie diese Datei an info@schuhfried.com. Geben Sie in dieser E-Mail bitte die Lieferscheinnummer an, damit die Bearbeitung schneller erfolgen kann.
- Nach der Bearbeitung durch SCHUHFRIED erhalten Sie eine E-Mail mit einer Anleitung wie Sie die Lizenzen installieren können. Folgen Sie den Instruktionen. Dies ist auch im Abschnitt 3.6 dargestellt.

Beachten Sie bitte, dass der Fingerprint unbedingt auf dem Computer erzeugt werden muss, auf dem der „Wiener Testsystem-Server“ installiert wird.

Der Software-Dongle erfasst Hardware-abhängige Parameter des Rechners, auf dem er erzeugt worden ist. Dies gilt auch für spezifische Eigenschaften eines virtuellen Systems. Sollte das virtuelle System „verschoben“ werden, wird der Software-Dongle ungültig und Ihr Wiener Testsystem gesperrt. Für nähere Details wenden Sie sich bitte, **bevor der Server verändert wird**, an den SCHUHFRIED Support (siehe Abschnitt 5.3).
Die folgenden Eigenschaften des virtuellen Systems **müssen gleich bleiben**, damit der Software-Dongle gültig bleibt:

- Virtuelle MAC-Adresse
- CPU-Eigenschaften
- UUID (Universal Unique Identifier) des virtuellen Abbilds; die UUID wird durch die Virtualisierungssoftware generiert. Wenn ein Clone erzeugt wird, wird eine neue UUID erzeugt.

3.3 Installation des Wiener Testsystems

Achten Sie vor dem Start der Installation darauf, dass alle wichtigen Updates für Ihre Windows-Version installiert sind!
Führen Sie daher vor der Installation einen Neustart durch!

Falls Sie Ihr WTS von einer älteren Version updaten, achten Sie darauf, dass alle von Ihnen veränderten Konfigurationsdateien des WTS gesichert werden, da etwaige Änderungen in den Dateien überschrieben werden!

z. B.die Konfigurationsdatei WTSService.exe.config, zu finden unter C:\Program Files (x86)\SCHUHFRIED GmbH\Vienna Test System 8\Service oder die Konfigurationsdatei appsettings.json, zu finden unter C:\Program Files (x86)\SCHUHFRIED GmbH\TestPlayerWeb

Nach der Installation eines Updates sollten die Backup-Konfigruationsdateien wieder in diesen Pfaden gespeichert werden, damit die benutzerdefinierten Änderungen berücksichtigt werden.

Wenn Sie den WTS-Server installieren wollen, muss der WTS-Dongle am Server angesteckt werden und nicht auf einem Arbeitsplatz! Bei Verwendung eines Software-Dongles muss dieser vor der Installation des WTS-Servers installiert sein!

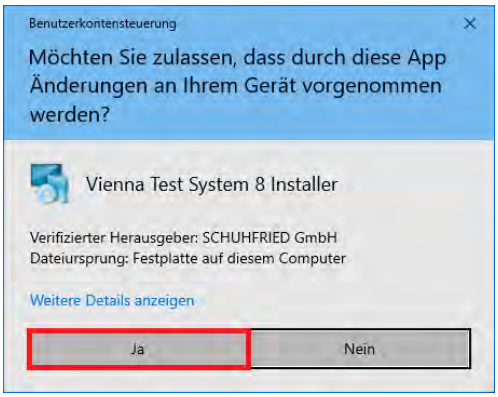
Bei diesem Setup werden der AdminClient und der Testplayer automatisch installiert. Wenn Sie das Clientsetup installieren wollen, lesen Sie bitte direkt das Kapitel
Installation des Wiener Testsystems – Clients

1. Starten Sie den für die Installation ausgewählten PC und melden Sie sich mit einem Benutzer an, der über lokale Administratorrechte verfügt!
2. Wenn Sie keinen USB-Stick mit dem Setup besitzen, laden Sie das Setup über den Link in Ihrer E-Mail herunter. Das Setup hat ca. 5 GB und wird in einer ZIP-Datei geliefert. Speichern Sie die Datei auf dem PC, auf dem Sie das Wiener Testsystem installieren möchten und entpacken Sie die Datei.

   Starten Sie die Installation mit einem Doppelklick auf die Datei **„Wts8Setup.exe“** und lesen Sie hier direkt ab Punkt 5 weiter.
3. Wenn Sie einen USB-Stick mit dem Setup besitzen, stecken Sie den USB-Stick in einen USB-Port Ihres Computers, um das Wiener Testsystem zu installieren.
4. Öffnen Sie den Arbeitsplatz (bei Windows 7 „Computer“). Doppelklicken Sie auf das Symbol für den USB-Stick. **Doppelklicken Sie auf die Datei „Wts8Setup.exe“**, um das Setup-Programm zu starten.

5. Anschließend öffnet sich eine Standardsicherheitsabfrage von Windows.

Bestätigen Sie die Sicherheitsabfrage mit „Ja“.



6. Bestätigen Sie nun die Lizenzvereinbarung

7. Nun startet die Installation des Wiener Testsystems (sowohl Server/Client als auch Einzelplatzinstallation).
Sie können nun zwischen der Standardinstallation und der benutzerdefinierten Installation wählen.
Wenn Sie die Standardinstallation wählen, lesen Sie bitte ab Punkt 10 weiter.

Bestätigen Sie mit „Weiter >“.

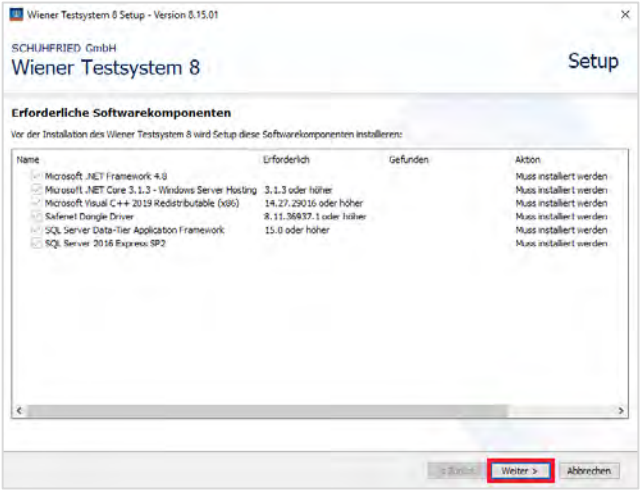
8. Im nächsten Schritt können Sie wählen, ob der Microsoft® SQL Server Express installiert werden soll (lesen Sie ab Punkt 10 weiter) oder ob ein bereits installierter SQL Server verwendet werden soll (siehe Punkt 9).

Nach Änderung oder Übernahme klicken Sie bitte auf „**Weiter >“**.

9. Falls die Wiener Testsystem SQL-Datenbank in einem vorhandenen SQL-Server verwendet werden soll, muss der „**Servername**“ und „**Katalogname**“ eingetragen werden.
Diese Informationen erfahren Sie von Ihrem SQL-Administrator.
Bestätigen Sie mit „Weiter >“.
Die Datenbank muss vor der Installation über Skripte installiert werden. Für mehr Informationen siehe Abschnitt 3.3.1. In diesem Fall muss die Option „Datenbank wurde bereits angelegt und aktualisiert“ ausgewählt werden.

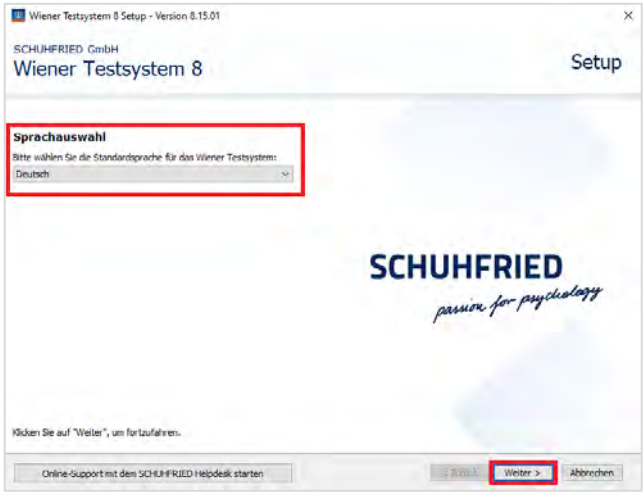
10. Das „Setup-Programm“ prüft nun, welche erforderlichen Programme installiert werden müssen. Nach der Prüfung wird eine Liste mit den erforderlichen Programmen dargestellt. (Bitte keine Änderungen in dieser Liste vornehmen!) Je nach Betriebssystem oder Installationen auf Ihrem PC können unterschiedliche Programme angewählt sein.

Bestätigen Sie mit „Weiter >“.



11. Wählen Sie nun die gewünschte Sprache aus.

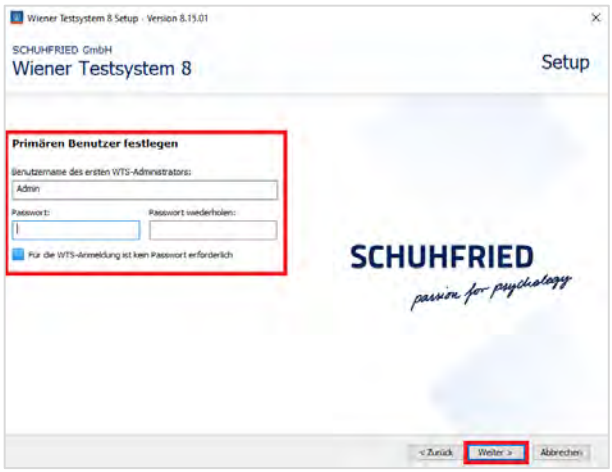
Bestätigen Sie mit „Weiter >“.



12. Im nächsten Schritt legen Sie den Benutzername und das Passwort für den Testsystemadministrator fest. Dieser Benutzer ist dann auf allen Clients verfügbar.
Das Wiener Testsystem Setup bietet hier als Vorauswahl den Benutzername „Admin“ an. Für die Vergabe des Benutzernamens gilt:

- Er darf nicht mit einem Leerzeichen beginnen oder enden.
- Er darf nur die Zeichen A-Z, a-z, 0-9 sowie die Sonderzeichen !"#$%'*+-=?^_|~ enthalten.

Vergeben Sie im Feld „Passwort“ ein Passwort Ihrer Wahl und bestätigen Sie das gewählte Passwort im Feld „Passwort wiederholen“.
Das gewählte Passwort muss mindestens acht Zeichen lang sein und darf nur folgende Zeichen enthalten: A-Z, a-z, 0-9 sowie die Sonderzeichen !"#$%'*+-=?^_|~.
Falls **kein Passwort** benötigt wird, kann die Option „Für die Anmeldung am Testsystem ist kein Passwort erforderlich“ angewählt werden. In diesem Fall startet das Wiener Testsystem ohne Benutzer-abfrage.
Wir weisen darauf hin, dass in diesem Fall andere geeignete technische und organisatorische Maßnahmen ergriffen werden müssen, um die Sicherheit der personenbezogenen Daten im Sinne der DSGVO zu gewährleisten.
Bestätigen Sie mit „Weiter >“.



Notieren Sie sich den Benutzernamen und das Passwort, des Testsystem-administrators!

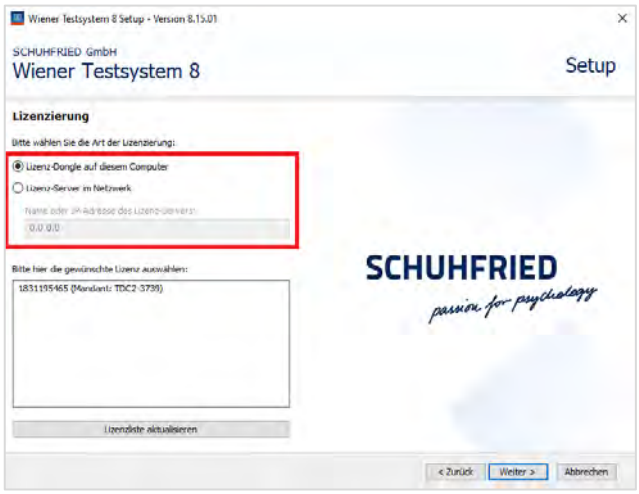
Ohne diese Zugangsdaten kann das Wiener Testsystem nicht gestartet werden!

13. Falls zu diesem Zeitpunkt noch kein WTS-Lizenz-Dongle angesteckt ist (oder mit einem Product Key installiert werden soll), können Sie die Dongle-Art im nächsten Schritt wählen.
Wählen Sie Ihre Dongle-Art und bestätigen Sie mit „**Weiter >**“. Falls der Lizenz-Dongle nicht angesteckt ist, werden Sie dazu aufgefordert.
Bitte beachten Sie, dass Sie im Falle eines Product Keys eine Internet-Verbindung während der Installation benötigen!

14. Wenn Sie einen Product Key besitzen, geben Sie diesen bitte im darunter erscheinenden Feld ein, bestätigen Sie mit „**Weiter >**“ und lesen Sie ab Punkt 15 weiter.

15. Nun muss angegeben werden, ob:

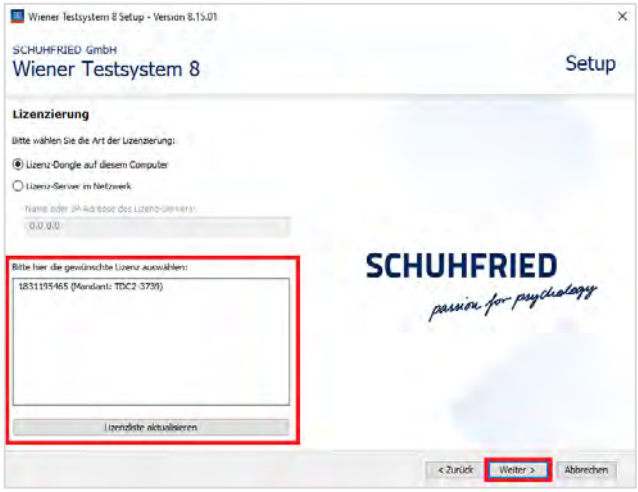
- der Wiener Testsystem Lizenz-Dongle (Software oder Hardware) auf dem Computer, auf dem der Wiener Testsystem Server installiert wird vorhanden ist (Option „**Lizenz-Dongle auf diesem Computer**“),
- oder ob er auf einem anderen Computer im Netzwerk ist (Option „**Lizenz-Server im Netzwerk**“).
  Ist der Lizenz-Server im Netzwerk verfügbar, muss der Name dieses Computers oder dessen IP-Adresse in das Eingabefeld unterhalb eingetragen werden. Klicken Sie auf „Lizenzliste aktualisieren“, nachdem die Adresse eingetragen ist und wählen Sie den Dongle.



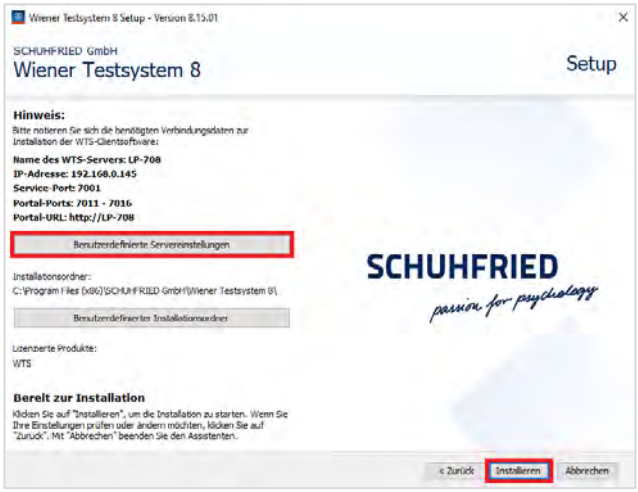
Sollten mehrere Mandaten verfügbar sein, können Sie wählen, welcher Mandant für

diese Wiener Testsystem Server Installation verwendet werden soll.

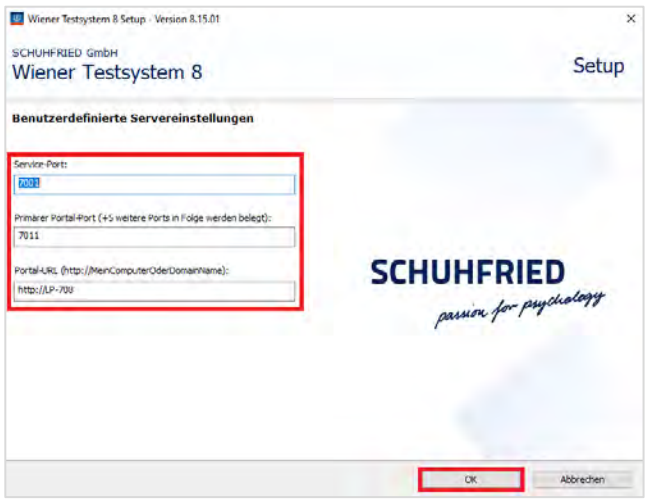
Bestätigen Sie mit „Weiter >“.



16. Der nächste Installationsdialog zeigt die gesammelten Informationen die zum Verbinden der Clients notwendig sind. Diese Informationen werden im Setup der Wiener Testsystem Clients benötigt. **Notieren Sie sich diese Daten und verwahren Sie diese sicher. Sie benötigen diese Informationen für die Installation aller Wiener Testsystem Clients!**

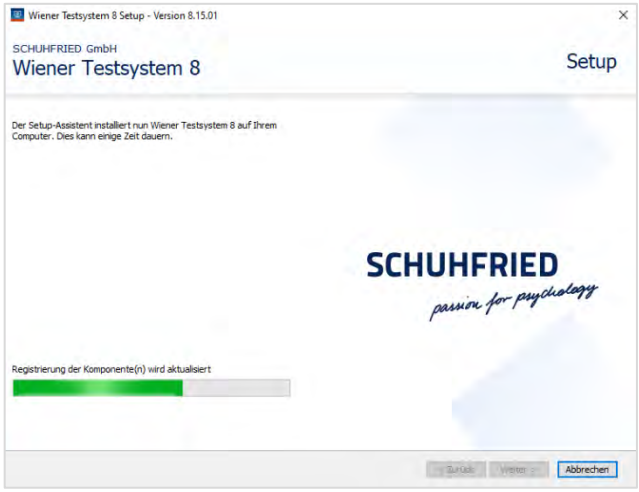


Über „Benutzerdefinierte Servereinstellungen“ kann außerdem festgelegt werden, über welche Ports der Wiener Testsystem Server und die Wiener Testsystem Clients miteinander kommunizieren. **Die hier angegebenen Ports müssen für Zugriffe der Clients geöffnet sein!**



Wenn Sie alle Einstellungen getroffen haben, klicken Sie bitte auf **„Installieren“**.

17. Die Installation des Wiener Testsystems wird nun durchgeführt. Dies kann einige Minuten in Anspruch nehmen.



18. Konnte die Installation erfolgreich abgeschlossen werden, erscheint die Bestätigung der Installation.

Beenden Sie nun die Installation mit einem Klick auf „OK“.

ACHTUNG:
Um zu überprüfen, ob die Installation erfolgreich war können Sie kontrollieren, ob der Dienst „WTS Service“ gestartet worden ist. In dem Fall können der AdminClient und der Testplayer mittels Shortcuts am Desktop gestartet werden.

Falls Sie Peripheriegeräte erworben haben, führen Sie bitte nun den **Hardwaretest** durch (siehe Kapitel 5.4, Abbildung 18), um sicher zu gehen, dass alle Geräte erfolgreich installiert wurden.

3.3.1 Installation des Servers mit Skripten

Dieser Punkt ist **ausschließlich bei einer Erstinstallation** durchzuführen, wenn das WTS mit **eigenem SQL-Server über Skripte installiert** werden soll. Wird die Installation komplett über das Setup durchgeführt, ist dieser Punkt nicht notwendig.

Um die Installation der WTS-Datenbank über Skripte durchführen zu können, muss folgendes vorhanden sein:

- SQL Server (genaue Version ist aus den Systemvoraussetzungen zu entnehmen)
- SQL Server Login mit ausreichenden Rechten, um einen weitere Login anzulegen

Bevor die Installation mit Skripten durchgeführt werden kann, muss ein Login „wtsnx“ in der vorgesehenen Datenbankinstanz angelegt werden. Dies ist für die Installation zwingend notwendig! Das Passwort für den Login erfahren Sie beim technischen Support.

Anlegen des Logins „wtsnx“ mit dem Microsoft SQL-Server Management Studio:

Verbinden Sie sich mit der entsprechenden SQL-Serverinstanz und fügen Sie einen neuen Login mit dem Namen „wtsnx“ unter „Security\Logins“ hinzu. Die folgenden Eigenschaften müssen dafür unter der Rubrik „General“ angepasst werden (siehe dazu auch Abbildung 3):

Login name:	wtsnx
Login type:	SQL Server authentication
Password:	Kontaktieren Sie den technischen Support
Enforce password policy:	Deaktivieren

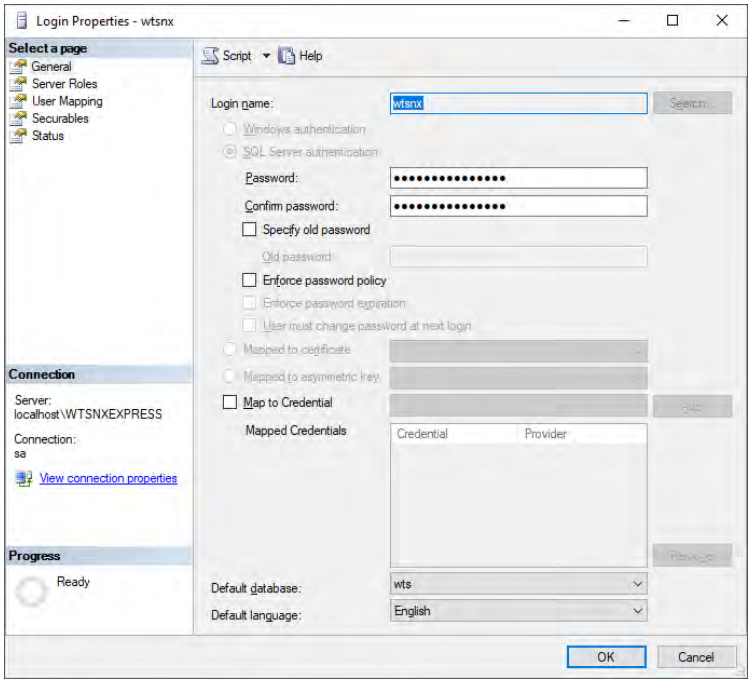


Abbildung 3: Einstellungen für den Login im Microsoft SQL-Server Management Studio

Bei der Installation werden diesem Login die Benutzerrollen “db_datareader” sowie “db_datawriter” in der Rubrik “User Mapping” zugewiesen. Ferner sollte dieser Benutzer die Berechtigungen für “Create Table”, “Create View” sowie “Create Procedure” besitzen.

Erzeugung der Datenbanken für die Installation des Wiener Testsystems:

Das Wiener Testsystem verwendet mehrere Datenbanken für verschiedene Arten von Daten. Die „WTS“ Datenbank beinhaltet Kandidaten- und Testdaten, die "DTC" Datenbank wird für die Web-Oberfläche und damit verbundenen Web-Funktionalitäten verwendet und die "WTSKatalog" Datenbank beinhaltet Metadaten über Tests und Test-Sets.

1. WTS Datenbank:

Die zur Verfügung stehenden Skripte müssen exakt in der folgenden Reihenfolge abgearbeitet werden:

- wts_1_create_database_v8.X.X.sql[1]
- wts_2_create_tables_v8.X.X.sql
- wts_3_insert_data_v8.X.X.sql
- wts_4_optimize_database_v8.X.X.sql

[1] „V8.X.X.sql“ steht für die Version. Bei der Version 8.15.01 heißen die Dateien daher zum Beispiel „wts_1_create_database_V8.15.1.sql“.

Die Skripte sind im Setup-Ordner im Verzeichnis „**Scripts\First Installation**“ abgelegt. Beachten Sie unbedingt die unten angeführten Hinweise!
Die Datenbank wird durch die Skripte mit der WTS Standard Collation “Latin1_General_CI_AI” erstellt.
Dabei wird standardmäßig eine Datenbank mit dem Namen “wts_deploy” erwartet. Datenbanknamen mit “-” im Namen sind unzulässig.

Ausführung der Skripte:

- Die Skripte 1, 2 und 4 können grundsätzlich aus dem MS SQL-Server Management Studio ausgeführt werden.
- Es wird **abgeraten das Skript 3** aus dem MS SQL-Server Management Studio heraus auszuführen, da das Skript sehr groß ist und zu einer „OutOfMemory“-Exception führen kann. Es wird daher empfohlen das Skript über „sqlcmd“ Commandline auszuführen. Dies muss mit den folgenden Parametern[2] geschehen:
    - sqlcmd -S <NameorIPofSQLServer>\<InstanceName> -U sa -P <password> -i <path to script & scriptname.sql>

Beispiel für die Instanz “wtsnxexpress” unter localhost mit dem User sa und dem Passwort 1234. Die Skripte sind unter „C:\temp\“ abgespeichert:

```
sqlcmd -S localhost\wtsnxexpress
       -U sa
       -P 1234
       -i C:\temp\wts_3_insert_data_v8.15.1.sql
```

2. DTC Datenbank:

Die zur Verfügung stehenden Skripte müssen exakt in der folgenden Reihenfolge abgearbeitet werden:

- dtc_1_create_database_v8.X.X.sql
- dtc_2_create_tables_v8.X.X.sql

Die Skripte sind im Setup-Ordner im Verzeichnis „**Scripts\First Installation**“ abgelegt.

Die Datenbank wird von den Skripten mit dem WTS-Standarddatenabgleich "SQL_Latin1_General_CP1_CI_AS" erstellt.

3. WTSKatalog Datenbank

Beachten Sie bei dieser Datenbank die folgende Reihenfolge:

- Im MS SQL-Server Management Studio rechtsklicken Sie auf Datenbanken und wählen Sie den Punkt „... anhängen“ aus.
- Klicken Sie auf die Schaltfläche „Hinzufügen“ und wählen Sie die Datei „WTSKatalog.mdf“ aus.
- **Achtung**: Tragen Sie, falls nötig, den Namen „WTSKatalog“ in das Spaltenfeld „Anhängen als “ ein.
- **Achtung:** Ändern Sie den Dateipfad im Spaltenfeld „Aktueller Dateipfad“ auf die .mdf- und .ldf-Datei im extrahierten Ordner.
- Führen Sie danach das Skript „productdb_1_update_schema_v8.X.X.sql“ auf der „WTSKatalog“ Datenbank aus.

Die Skripts und die .mdf-Datei sind im Setup-Ordner im Verzeichnis „**Scripts\First Installation**“ abgelegt.

[2] Die korrekte Installation kann nur mit dem User „sa“ garantiert werden!

Die Datenbank wird mit dem WTS-Standarddatenabgleich "SQL_Latin1_General_CP1_CI_AS" verknüpft.

Update der Datenbanken mit Skripten:
Dieser Schritt ist **nur dann notwendig,** wenn das **Update der Datenbanken des Wiener Testsystems nicht über das Setup, sondern über Skripte** ausgeführt werden soll.

Weiters muss das Passwort des SQL Logins „wtsnx“ auf die neueste Version aktualisiert werden, siehe Punkt 3.3.1.

1. WTS Datenbank

Die folgenden Skripte müssen exakt in der folgenden Reihenfolge abgearbeitet werden:

- wts_1_update_schema_v8.X.X.sql
- wts_2_update_data_v8.X.X.sql
- wts_3_optimize_database_v8.X.X.sql

Die Skripte sind im Setup-Ordner im Verzeichnis „**Scripts\Update Installation**“ abgelegt. Alle drei Skripte können aus dem MS SQL-Server Management Studio abgearbeitet werden.

2. DTC Datenbank

Das folgende Skript muss abgearbeitet werden:

- dtc_1_update_schema_v8.X.X.sql

Das Skript liegt im Verzeichnis „Scripts\Update Installation“.

Bitte beachten Sie: Wenn Sie ein Update einer früheren WTS-Version durchführen, die noch nicht mit einer DTC-Datenbank arbeitet (z. B. WTS 8.14.10), legen Sie bitte eine neue DTC-Datenbank an, wie unter Punkt „2. DTC Datenbank” in „Datenbanken für die Installation des Wiener Testsystems“ beschrieben.

3. WTSKatalog Datenbank

Die folgende Schritte müssen durchgeführt werden:

- Im MS SQL-Server Management Studio rechtsklicken Sie auf Datenbanken und wählen Sie den Punkt „... anhängen“ aus.
- Klicken Sie auf die Schaltfläche „Hinzufügen“ und wählen Sie die Datei „WTSKatalog.mdf“ aus.
- **Achtung**: Tragen Sie falls nötig den Namen „WTSKatalog“ in das Spaltenfeld „Anhängen als“ ein.
- **Achtung:** Ändern Sie den Dateipfad im Spaltenfeld „Aktueller Dateipfad“ auf die .mdf- und .ldf-Datei im extrahierten Ordner.
- Führen Sie danach das Skript „productdb_1_update_schema_v8.X.X.sql“ auf der „WTSKatalog“ Datenbank aus.
- Überprüfen Sie, ob die WTSKatalog-Datenbank dem wtsnx-Login zugeordnet ist und erstellen Sie eine entsprechende Zuordnung, wenn dies nicht der Fall ist.

Das Skript und die .mdf-Datei sind im Setup-Ordner im Verzeichnis „**Scripts\Update Installation**“ abgelegt.

Bitte beachten Sie: Wenn Sie ein Update einer früheren WTS-Version durchführen, die noch nicht mit einer WTSKatalog-Datenbank arbeitet (z. B. WTS 8.14.10), legen Sie bitte

stattdessen eine neue WTSKatalog-Datenbank an, wie unter Punkt „3. WTSKatalog-Datenbank“ in „Erstellen von Datenbanken für die Installation des Wiener Testsystems“ beschrieben.

3.3.2 Hinweise zur Installation

Mit den Daten in den Feldern „**Standard Benutzername“** und **„Kennwort“** ist der Einstieg in das Wiener Testsystem direkt nach der Installation möglich. Dieser Benutzer hat volle Rechte im Wiener Testsystem, er kann daher neue Benutzer anlegen und deren Berechtigungen einstellen.
Der während der Installation angelegte Benutzer ist automatisch in der höchsten Sicherheitsstufe (Sicherheitsstufe 0). Dieser Benutzer kann somit sämtliche Einstellungen im Wiener Testsystem ändern bzw. neue Benutzer anlegen.

Hinweis:

Es muss unbedingt einen Benutzer geben, der in der höchsten Sicherheitsstufe ist. Ansonsten kann das Wiener Testsystem nicht mehr verwalten werden.

Folgende Sicherheitsstufen gibt es:

Sicherheitsstufe	Berechtigung
0	In dieser Sicherheitsstufe sind alle Funktionen und Einstellungen des Wiener Testsystems zugänglich.
1	In dieser Sicherheitsstufe können keine Einstellungen geändert werden. Es können daher keine Testbatterien erstellt oder geändert werden, keine Grundeinstellungen (z.B. Ordner für Datenspeicherung) verändert werden und keine Tests installiert werden. Das Wiener Testsystem kann aber zur Testvorgabe benutzt werden und der Zugriff auf die Datenbanken ist uneingeschränkt möglich.
2	In dieser Sicherheitsstufe ist das Wiener Testsystem nur zur Testvorgabe und anschließenden Auswertung verwendbar. Die anderen Funktionen sind gesperrt. Die Testergebnisse sind insofern eingeschränkt zugänglich, dass lediglich die bei der Testvorgabe gespeicherten Datensätze im Anschluss an die Testvorgabe ausgewertet werden können. Andere Testergebnisse können nicht aufgerufen werden.
3	In dieser Sicherheitsstufe ist das Wiener Testsystem ausschließlich zur Testvorgabe verwendbar. Alle anderen Funktionen und der Zugriff auf die Datenbank sind komplett gesperrt.

Die Applikationen des Wiener Testsystems sind signiert. Die Signatur wird in der Standardeinstellung von Windows-Betriebssystemen über einen Server überprüft. Diese Prüfung findet statt, wenn Windows ein Netzwerk detektiert. Sollte die Kommunikation ins Internet durch Netzwerkeinstellungen blockiert werden, kann dies zu starken Verzögerungen beim Starten des Wiener Testsystems oder beim Starten von Testungen führen.
In diesem Fall empfiehlt es sich die Signaturprüfung abzuschalten.

3.3.3 Einzelplatz-Installation über Command-Line

Die Installation des Wiener Testsystems kann auch silent gesteuert über Parameter erfolgen. Der Aufruf ist folgendermaßen definiert:

```
WTS8setup.exe /qX DEFAULT_CULTURE=”de-DE” AC_USERNAME_PROP=”Admin”
AC_PASSWORD_PROP=”xxx” WTS_SERVICE_PORT=”7001”
WTS_PORTAL_PORT=”7011” WTS_PORTAL_URL=”xxx”
```

Weitere optionale Parameter:

```
PRODUCT_KEY=“XXXX“
LICENSE_FILE=“c:\TEMP\W12345_001_01_ID21_31001_Lizenz.v2c“
APPDIR=“C:\Program Files\Wiener Testsystem 8“
ICON_TP=“1“
/L*V „%temp%\WTS8Silent.log“
```

Erläuterungen:

Parameter	Wert	Beschreibung
/qx	qr	Keine Benutzereingabe mit Anzeige des Installationsfortschritts
	qb	Keine Benutzereingabe mit Anzeige des Installationsfortschritts als Fortschrittsbalken
	qn	Keine Benutzereingabe und keine Anzeige des Installationsfortschritts
DEFAULT_CULTURE	de-DE en-US …	**Pflichtparameter bei Erstinstallation** Bestimmt die Sprache der Admin Console und des Testplayers. Diese Angabe ist unbedingt erforderlich! Die Sprache der Oberfläche kann nachträglich umgestellt werden.
AC_USERNAME_PROP	Text	**Pflichtparameter bei Erstinstallation** Legt den ersten Login für das Wiener Testsystem fest.
AC_PASSWORD_PROP	Text	Definiert das Passwort für den oben festgelegten Login, falls NO_AC_PASSWORD nicht angegeben ist, muss dieser Parameter verwendet werden!
NO_AC_PASSWORD	1	Wenn der Parameter auf 1 ist, wird kein Passwort für den Login benötigt. Dies ist nicht empfohlen! Wenn ein Passwort vergeben wird, kann dieser Parameter entfallen.
PRODUCT_KEY	Text	Angabe des Product-Keys, falls mit einem solchen ein Software-Dongle installiert wird.
LICENSE_FILE	Text	Gibt den Pfad für eine v2c-Lizenzdatei an, falls diese im Zuge der Installation eingespielt werden soll. Dies ist bei einer Erstinstallation **nicht notwendig.**
APPDIR	Pfad	Dieser Eintrag bestimmt den Pfad, in dem das Wiener Testsystem installiert werden soll. Wenn dieser Parameter nicht angegeben wird, ist es das

		Installationsverzeichnis „C:\Programme (x86)\Schuhfried GmbH\Wiener Testsystem 8“.
ICON_TP	1	Wenn dieser Parameter gesetzt wird, erzeugt das Setup ein Icon für DirectTesting am Desktop und im Startmenü.
/L*V	Text	Wenn dieser Parameter angegeben ist, wird in der festgelegten Datei (vollständiger Pfad) eine Logdatei der Installation erzeugt.
/exelang	1031 1033	Startet das Setup in deutscher Sprache (optional). Startet das Setup in englischer Sprache (optional).
WTS_PORTAL_URL	Text	Bestimmt die Adresse, über welche das WTS-Portal erreichbar sein sollte. Dieser Wert sollte entweder der Domänenname oder der Maschinennamen sein (Default=Maschinenname).
WTS_SERVICE_PORT	7001	Bestimmt den Port für den WTS-Service. Hier muss ein freier Port im Bereich 7001 bis 7999 angegeben werden, über das die WTS-Clients mit dem WTS-Service am Server kommunizieren. Dieser Parameter **darf nicht** weggelassen werden.
WTS_PORTAL_PORT	7011	Bestimmt den Basis-Port für das WTS-Portal. Hier muss ein freies Port im Bereich 7001 bis 7999 angegeben werden. Zu beachten ist, dass auch 5 weitere Ports in Folge belegt werden. Die Angabe ist optional (Default=7011).
LICENSE_SERVER_ID	Text	Bestimmt die IP-Adresse oder den Namen des Dongle-Servers (nur anzugeben, wenn der Dongle an einem eigenen Lizenzserver angesteckt wird. Default="localhost")
DB_SERVER_INSTANCE	Text	Bestimmt den Server-Namen des SQL-Servers (nur anzugeben, wenn ein benutzerdefinierter SQL Server verwendet werden soll).
DB_CATALOG_NAME	Text	Bestimmt den Katalog-Namen des SQL-Servers (nur anzugeben, wenn ein benutzerdefinierter SQL Server verwendet werden soll).
SQL_SA_USER	Text	Bestimmt den Login-Namen des SQL-Server-Systemadministrators (nur, wenn ein benutzerdefinierter SQL Server verwendet wird und der sa-User angegeben werden kann).
SQL_SA_PASSWORD	Text	Bestimmt das Passwort des SQL-Server-Systemadministrators (nur, wenn ein benutzerdefinierter SQL Server verwendet wird und das sa-Passwort angegeben werden kann).
MANDANT_ID	Text	Über diesen Parameter kann der Mandant eingestellt werden, mit dem der Testplayer starten soll (z.B. W12345_001). Wenn „AUTO“ eingetragen ist, wird der erste Mandant gewählt, der am Server gefunden wird. Wenn der Mandant bei jedem Start eingegeben werden soll, muss **MANDANT_ID="-"** angegeben werden!

CERTIFICATE_FILEPATH	Text	Über diesen Parameter kann der Dateipfad zum eigenen Zertifikat angegeben werden, welches für die Kommunikation zwischen den Komponenten verwendet wird.
CERTIFICATE_PASSWORD	Text	Falls CERITIFICATE_FILEPATH gesetzt ist, kann mit diesem Parameter das Passwort vom eigenen Zertifikat angegeben werden.
CERTIFICATE_SUBJECT	Text	Falls CERITIFICATE_FILEPATH gesetzt ist, muss mit diesem Parameter das Subjekt (bzw. die Domäne) des eigenen Zertifikates angeben werden.
EXISTING_CERTIFICATE_ SUBJECT	Text	Optional. Wenn diese Variable übergeben wird, versucht das Installationsprogramm ein gültiges Zertifikat im Windows-Zertifikatspeicher (LocalComputer/Personal) zu finden, dessen CN (Common Name) der übergebenen Variable entspricht. Dieses Zertifikat muss einen privaten Schlüssel enthalten, der im Speicher zugänglich ist, und wird für alle TLS-Verbindungen sowie für andere Verschlüsselungs- und Signiervorgänge verwendet. Diese Variable kann nicht gleichzeitig mit EXISTING_CERTIFICATE_THUMBPRINT verwendet werden.
EXISTING_CERTIFICATE_ THUMBPRINT	Text	Optional. Wenn diese Variable übergeben wird, versucht das Installationsprogramm ein gültiges Zertifikat im Windows-Zertifikatspeicher (LocalComputer/Personal) zu finden, dessen Thumbprint der übergebenen Variable entspricht. Dieses Zertifikat muss einen privaten Schlüssel haben, der im Speicher zugänglich ist, und wird für alle TLS-Verbindungen und andere Verschlüsselungs- und Signiervorgänge verwendet. Diese Variable kann nicht gleichzeitig mit EXISTING_CERTIFICATE_SUBJECT verwendet werden.

Beispiele:
Installation in englischer Sprache mit Logfile:

```
WTS8setup.exe /qr DEFAULT_CULTURE=“en-US“ AC_USERNAME_PROP=“admin“
AC_PASSWORD_PROP=“admin“ /L*V „%temp%\WTS8Silent.log“
WTS_SERVICE_PORT=“7001“
                https://localhost"
```

Installation in deutscher Sprache mit DirectTesting Icon am Desktop ohne Password:

```
WTS8setup.exe /qr DEFAULT_CULTURE=“de-DE“ AC_USERNAME_PROP=“admin“
NO_AC_PASSWORD=“1“ ICON_TP=“1“ WTS_SERVICE_PORT=“7001“
                https://localhost"
```

Installation mit Product Key

```
WTS8setup.exe /qr DEFAULT_CULTURE=“de-DE“ AC_USERNAME_PROP=“admin“
AC_PASSWORD_PROP=“Admin123“ PRODUCT_KEY=“xxx-xxx-xxx-xxx-xxx“
WTS_SERVICE_PORT=“7001“
                https://localhost"
```

Installation mit eigenem Zertifikat

```
WTS8setup.exe /qn DEFAULT_CULTURE="en-US" AC_USERNAME_PROP="admin"
AC_PASSWORD_PROP="Admin123" WTS_SERVICE_PORT=“7001“
                https://localhost"
CERTIFICATE_FILEPATH="<path>\certificate.pfx"
CERTIFICATE_PASSWORD="MyCertPwd"
CERTIFICATE_SUBJECT=www.schuhfried.com
```

Hinweise:

- Die Parameter **AC_USERNAME_PROP**, **AC_PASSWORD_PROP** und **NO_AC_PASSWORD** werden nur bei einer Erstinstallation benötigt. Bei einem Update werden die allfälligen Angaben ignoriert.
- Die Parameter **DB_SERVER_INSTANCE** und **DB_CATALOG_NAME** sind nur dann anzugeben, wenn ein benutzerdefinierter SQL Server verwendet werden soll. Wenn sie nicht angegeben werden, wird automatisch der SQL-Server-Express installiert und als Datenbank verwendet. Wenn **DB_SERVER_INSTANCE** angegeben wird, wird die Installation des SQL-Server-Express als Pre-Requisite automatisch übersprungen.
- Die Parameter **SQL_SA_USER** und **SQL_SA_PASSWORD** sind nur dann anzugeben, wenn ein benutzerdefinierter SQL Server verwendet wird, sind aber optional. Werden sie nicht angegeben, muss die Datenbank vor Ausführung des Setups bereits erstellt bzw. aktualisiert worden sein, Setup kann die Datenbank ohne sa-User nicht erstellen bzw. aktualisieren.
- Wenn kein Dongle (Hardware- oder Software-Dongle) gefunden wird **und der Parameter PRODUCT_KEY** angegeben ist, wird versucht ein Software-Dongle zu erzeugen. Dazu ist eine **Internetverbindung** notwendig! Sollte ein Dongle vorhanden sein, wird ein allfällig angegebener Wert nach PRODUCT_KEY ignoriert.
- Doppelte Anführungszeichen (") um die Parameter-Werte sind nur dann notwendig, wenn der Wert Leerzeichen enthält (z.B. ein Pfad oder Dateiname)
- Wird ein Parameter angeführt, **muss dieser einen Wert** enthalten! Leere Werte (z.B. AC_PASSWORD_PROP=““ oder AC_PASSWORD_PROP=) sind nicht zulässig und führen zu einer fehlerhaften Verarbeitung.
- Der Parameter /exelang muss, wenn angegeben, an erster Stelle stehen. Es muss immer ein Leerzeichen vor der Sprach-ID (1031 oder 1033) stehen. /exelang=1031 funktioniert nicht.
- Der Parameter /exenoui wird vom aktuellen Installer nicht mehr unterstützt und ignoriert. Die Installation der Pre-Requisites erfolgt nun immer ohne Benutzerinterface.

Folgende Sprachen stehen in der Admin Console zu Verfügung:

Sprache	Sprachcode
Chinesisch – Simplified	zh-CN
Deutsch	de-DE
Englisch (USA)	en-US
Französisch	fr-FR
Italienisch	it-IT
Niederländisch	nl-NL
Polnisch	pl-PL
Portugiesisch	pt-PT

Sprache	Sprachcode
Rumänisch	ro-RO
Russisch	ru-RU
Schwedisch	sv-SE
Slowakisch	sk-SK
Slowenisch	sl-SI
Spanisch	es-ES
Tschechisch	cs-CZ
Türkisch	tr-TR

3.3.4 Problembehebung

Die Version 2012 des SQL Server wird nicht unterstützt

Wenn Ihre Installation noch auf der nicht mehr unterstützten Version 2012 des Microsoft SQL-Servers oder einer älteren Version basiert, zeigt das Installationsprogramm für das WTS eine entsprechende Meldung an. In diesem Fall ist keine Installation möglich.

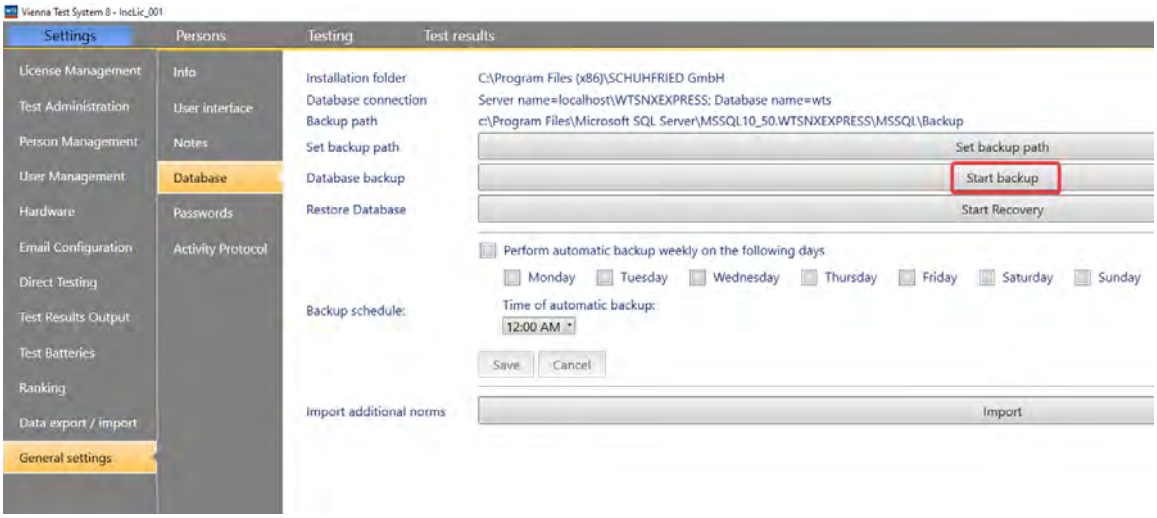
Installation mit einer benutzerdefinierten Datenbank

Bei einer benutzerdefinierten Installation Ihres WTS-Servers mit Skripts (3.3.1) müssen Sie erst Ihren SQL-Server upgraden, bevor Sie anhand der Anleitung im oben genannten Kapitel die WTS-Datenbank auf die neuste Version upgraden.

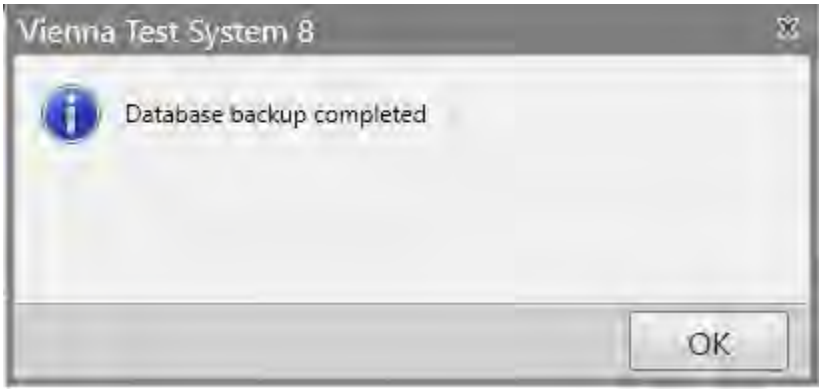
Standard-Installation

Bei einer Standard-Installation führen Sie bitte die folgenden Schritte durch, bevor Sie mit dem Einrichten beginnen:

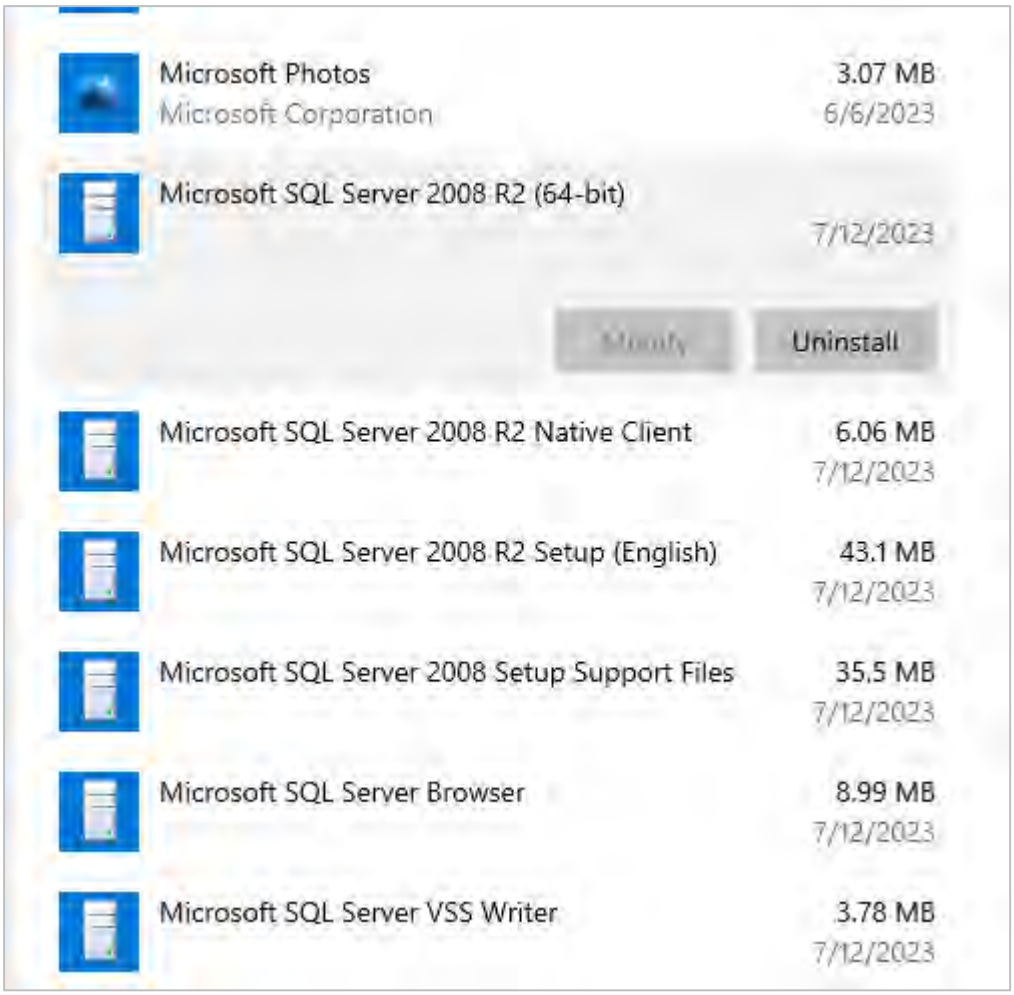
1. Öffnen Sie den Wiener Testsystem Client



Gehen Sie auf „Einstellungen“– „Allgemeine Einstellungen“ – „Datenbank“ und klicken Sie im Menüband „Backup der Datenbank“ auf die Schaltfläche „Backup starten“. Es empfiehlt sich, die Datenbank vorher über die Schaltfläche „Backup-Pfad einstellen“ unter einem von Ihnen festgelegten Pfad auf der Festplatte zu speichern. Das Backup der Datenbank kann einige Zeit in Anspruch nehmen (je nach Größe Ihrer Datenbank und Ihrer Hardware einige Minuten oder Stunden). Nach Abschluss des Backups wird der folgende Dialog angezeigt:

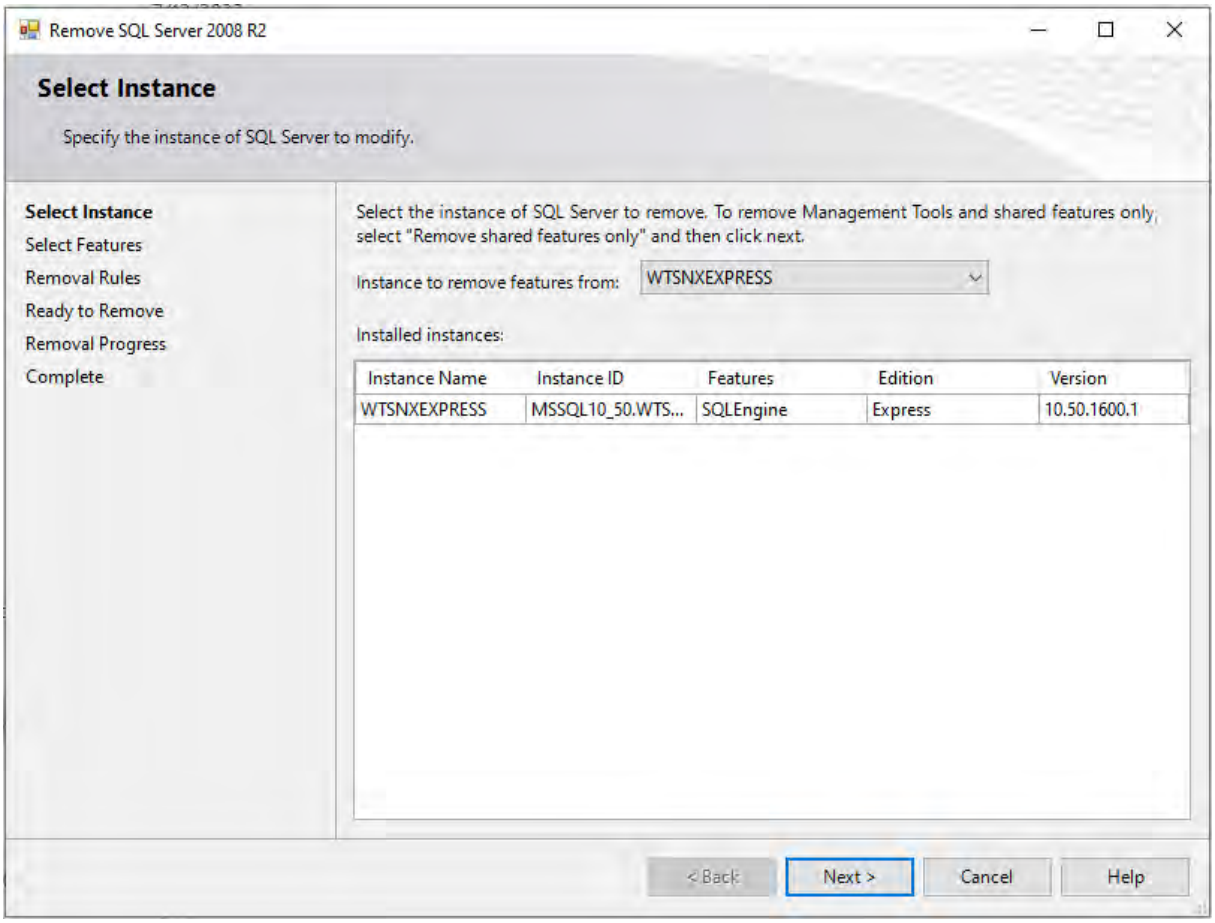


2. Schließen Sie den Wiener Testsystem Client
3. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie im Kontextmenü „Task-Manager“.
4. Wenn der Task-Manager angezeigt wird, gehen Sie auf „WTS Service“ im Menüreiter „Dienste“.
5. Klicken Sie mit der rechten Maustaste auf „WTS Service“ und im Kontextmenü auf „Anhalten“. Warten Sie, bis der Dienst angehalten ist.
6. Klicken Sie mit der rechten Maustaste auf die Schaltfläche „Starten“ in Windows OS. Es wird ein Pop-up-Fenster angezeigt.
7. Klicken Sie im Kontext-Menü auf „Apps und Features“.
8. Es wird ein Windows-Dialog mit allen Ihren installierten Apps angezeigt.
9. Scrollen Sie zu „Microsoft SQL Server“. Es können mehrere Apps installiert sein, die mit dieser Bezeichnung anfangen. Hier ein Beispiel:

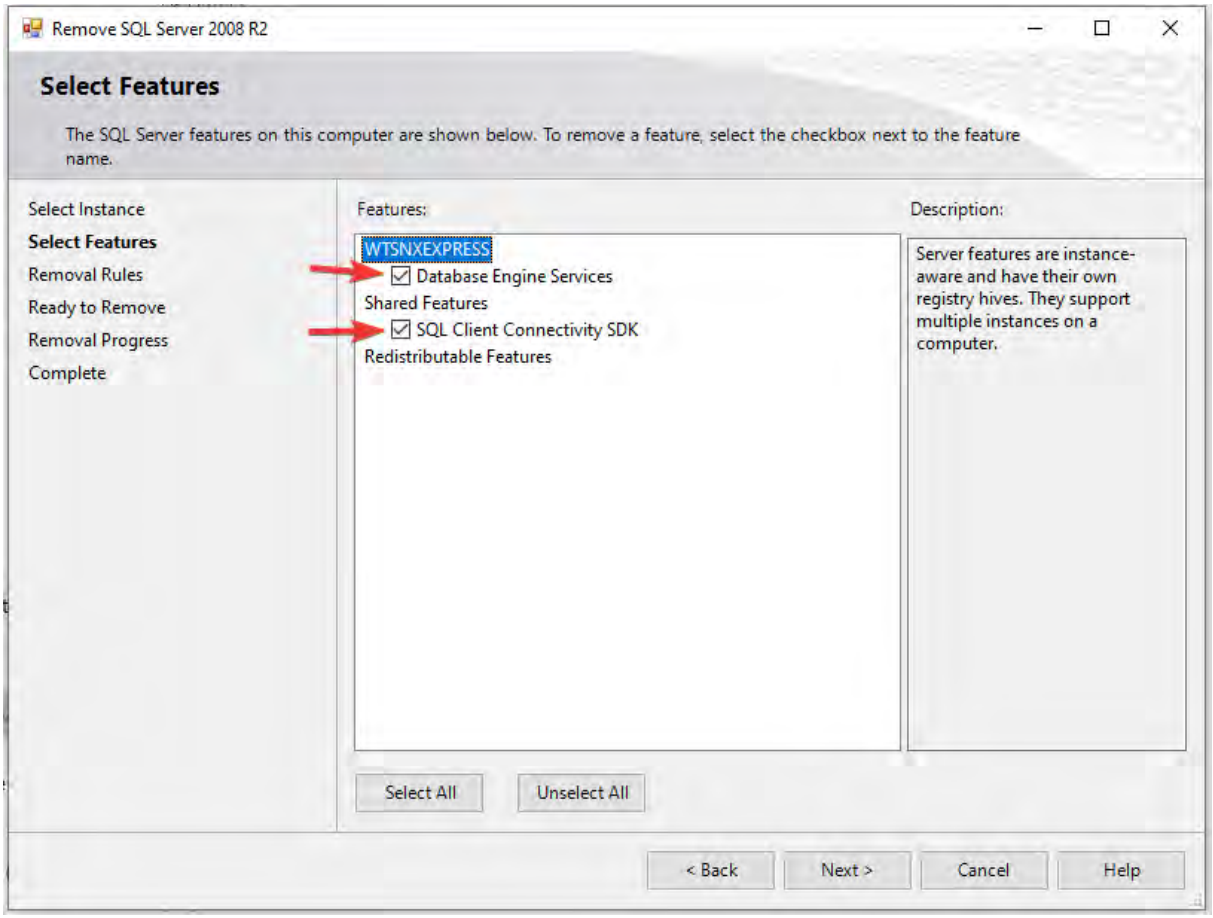


10. Deinstallieren Sie die Version, die nach dem Jahr, der Version und der Bitmap-Beschreibung keine weiteren Wörter enthält (die auf dem Bildschirm ausgewählte Version kann je nach der von Ihnen verwendeten Version des SQL-Servers unterschiedlich sein).
11. Klicken Sie auf die Schaltfläche „Deinstallieren“, um den SQL-Server zu deinstallieren.
12. Der folgende (oder ein sehr ähnlicher) Dialog wird angezeigt:

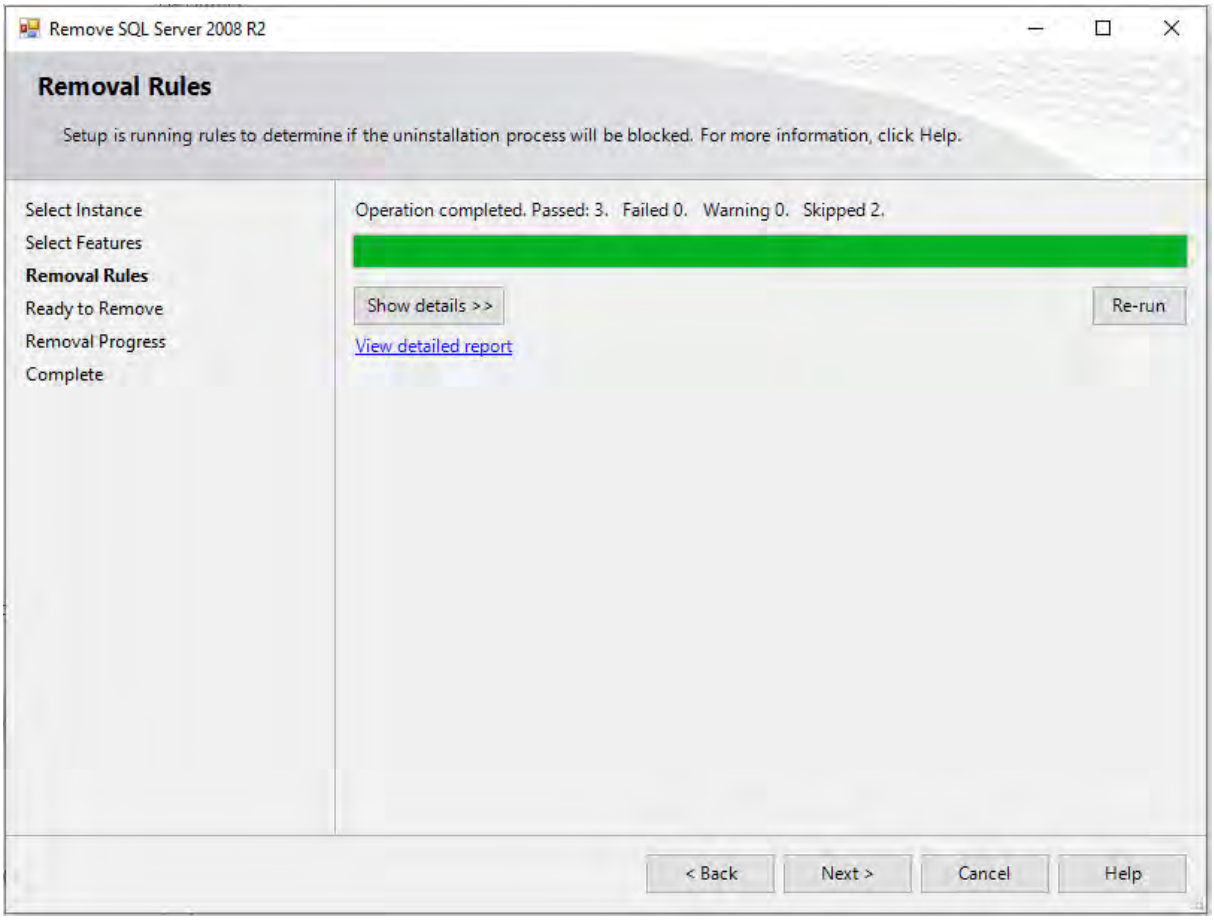
13. Klicken Sie auf den Link „Entfernen“. (Es kann eine Aufforderung von OS Windows angezeigt werden, die Sie dazu auffordert, zusätzliche Funktionen wie „.NET Framework 3.5“ zu installieren, klicken Sie einfach auf „Diese Funktion downloaden und installieren“.
14. Abhängig von Ihrer SQL-Server-Version zeigt das Deinstallationsprogramm des SQL-Server den folgenden (oder einen sehr ähnlichen) Dialog an:



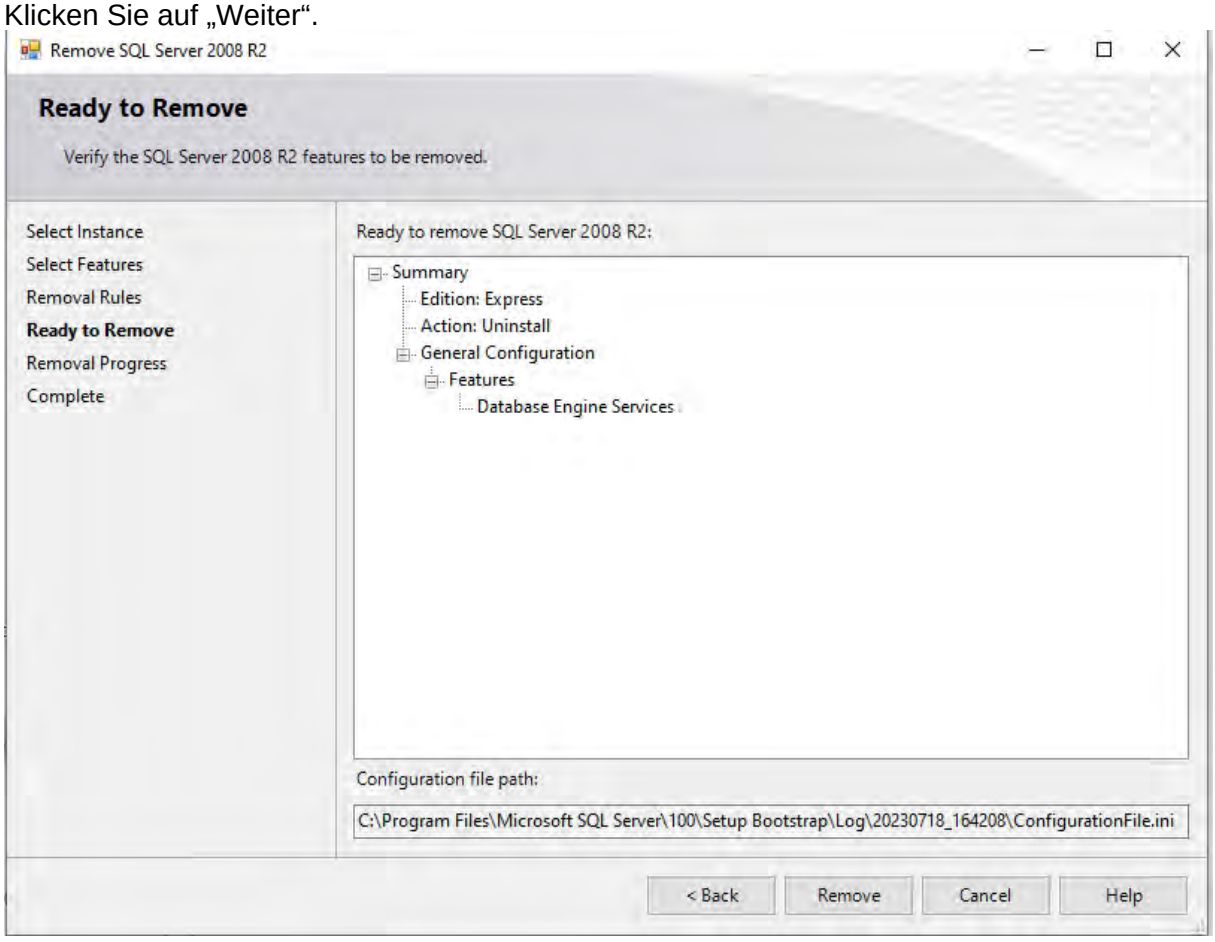
15. Klicken Sie auf „Weiter“.



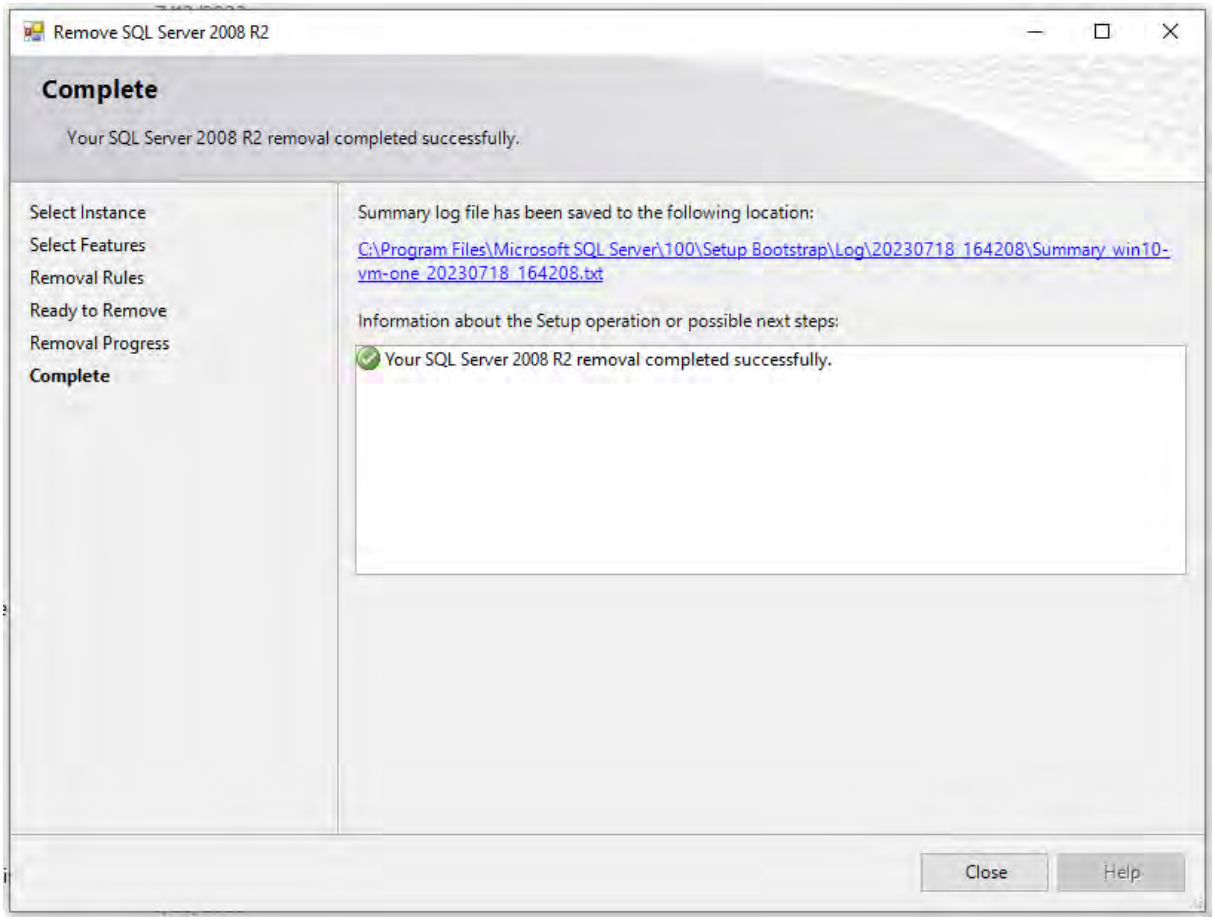
16. Aktivieren Sie alle Kontrollkästchen und klicken Sie auf „Weiter“.



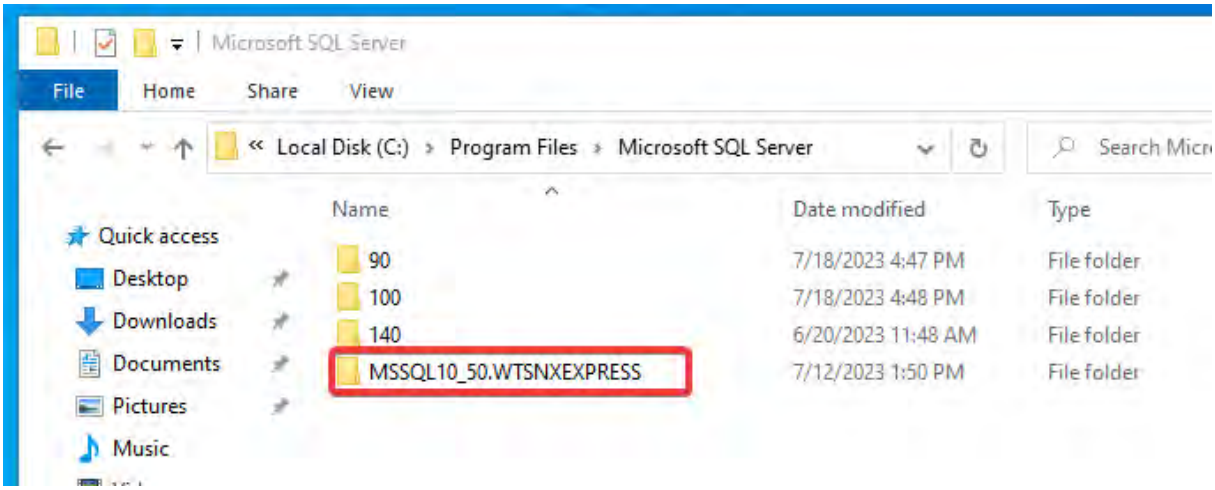
17. Klicken Sie auf „Weiter“.



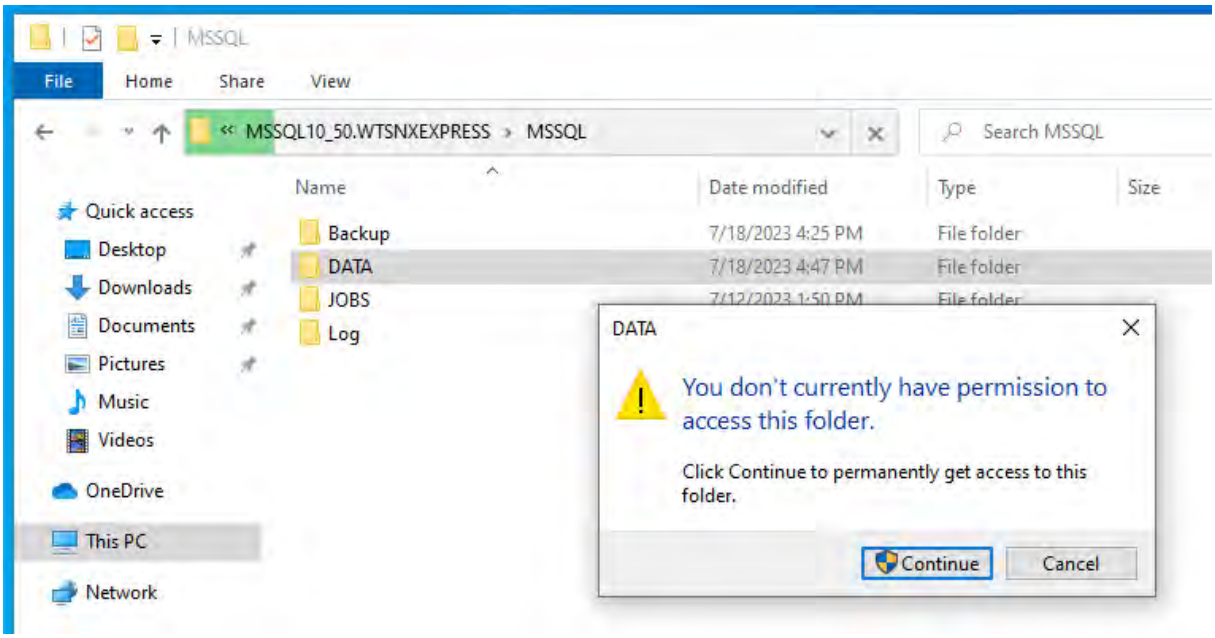
18. Klicken Sie auf „Entfernen“ und warten Sie, bis die Deinstallation abgeschlossen ist.



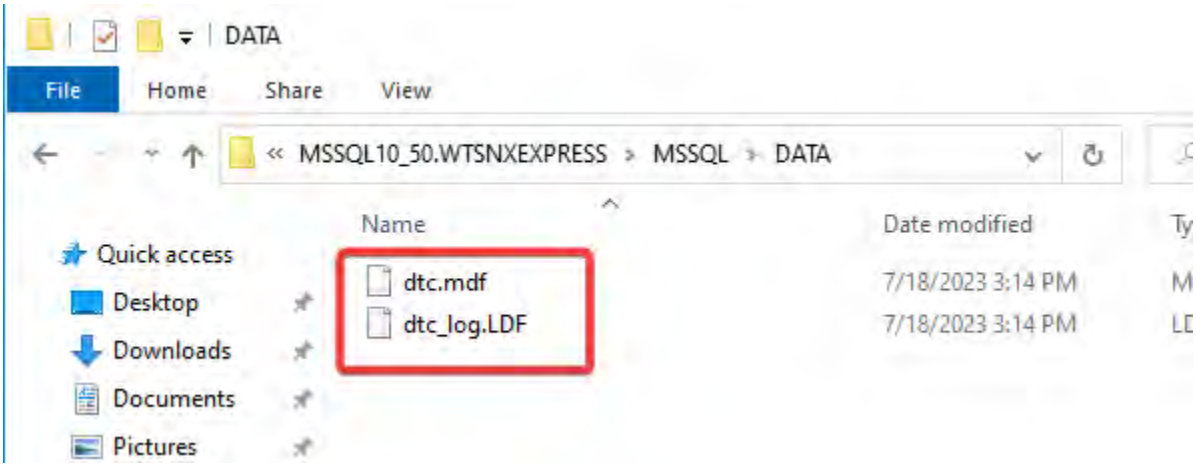
19. Klicken Sie auf „Beenden“.
20. Sehr wichtiger Schritt: Führen Sie einen Neustart Ihres Computers durch.
21. Öffnen Sie den Explorer und gehen Sie auf dem Laufwerk C: zum Pfad C:\Programme\Microsoft SQL Server.
22. Der Name eines der Unterordner endet mit der Zeichenfolge „WTSNXEXPRESS“, z. B.:



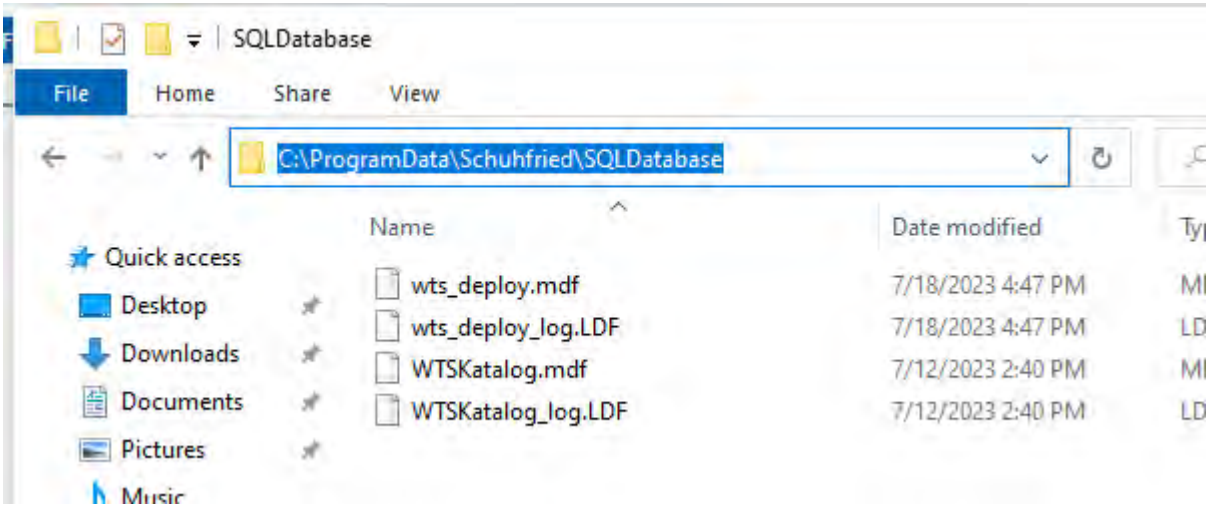
23. Gehen Sie auf diesen Ordner und dann auf den Pfad des Unterordners MSSQL\Data.
24. Windows fragt die Administratorberechtigung ab.



25. Erteilen Sie die Adminstratorberechtigung, indem Sie auf die Schaltfläche „Weiter“ klicken.
26. Nun sollten 2 Dateien mit der Bezeichnung „dtc.mdf“ und „dtc_log.LDF“ angezeigt werden:



27. Öffnen Sie ein weiteres Fenster des Explorers und geben Sie in der Adressleiste den folgenden Pfad ein: c:\programdata\schuhfried\sqldatabase. Bestätigen Sie mit der Eingabetaste.



28. Schneiden Sie die Dateien „dtc.mdf“ und „dtc_log.LDF“ aus dem Ordner „MSSQL\Data“ aus und fügen Sie sie in den Ordner „c:\programdata\schuhfried\sqldatabase“ ein.

29. Gehen Sie auf den Ordner mit der neusten Version des WTS-Installationsprogramms und starten Sie es erneut. Es sollte die neuere Version des Microsoft-SQL-Servers installieren und Ihre Datenbankdateien sollten erhalten bleiben. Falls das Installationsprogramm nicht ordnungsgemäß läuft, wenden Sie sich an den Kunden-Support.

3.4 Installation des Wiener Testsystems – Clients

Achten Sie vor dem Start der Installation darauf,
dass alle wichtigen Updates für Ihre Windows Version installiert sind!
Führen Sie daher vor der Installation einen Neustart durch!

Falls Sie Ihr WTS von einer älteren Version updaten, achten Sie darauf, dass alle von Ihnen veränderten Konfigurationsdateien des WTS gesichert werden, da etwaige Änderungen in den Dateien überschrieben werden.

In diesem Abschnitt wird die Installation des Wiener Testsystems Clients beschrieben. Es werden Ihnen im Setup drei „Programme“ zur Installation angeboten, die auf den Wiener Testsystem Server zugreifen können:

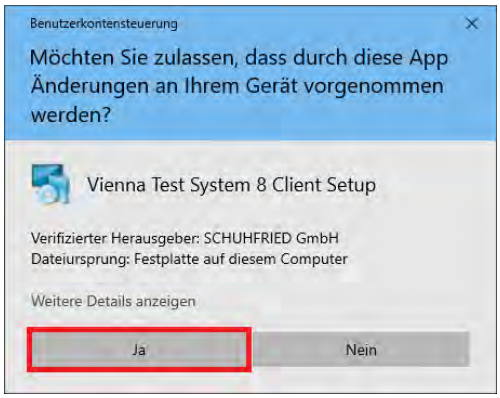
- **WTS-Testplayer:** Über dieses Programm können Personen, die zuvor über die Administrator-Konsole angelegt wurden, Tests und Testbatterien durchführen.
- **Administrator-Konsole:** Über dieses Programm können Sie das Wiener Testsystem konfigurieren, neue Lizenzen installieren, Datenbank Backups erzeugen, Benutzer und Personen anlegen, Benutzer- und Personendaten verwalten, Testbatterien erstellen sowie Testergebnisse auswerten, ausdrucken, exportieren und auch WORD Reports erzeugen.
- **Kontrollmonitor:** Dieses Programm dient dazu die Aktivitäten der Testplayer zu überwachen. Sie können sehen an welchem Testplayer von welcher Person welcher Test durchgeführt wird.

1. Starten Sie den für die Installation ausgewählten PC und melden Sie sich mit einem Benutzer an, der über lokale Administratorrechte verfügt!
2. Wenn Sie eine Online-Lizenz erworben haben, laden Sie das Setup über den Link in Ihrer E-Mail herunter. Das Setup hat ca. 5 GB und wird in einer ZIP-Datei geliefert. Speichern Sie die Datei auf dem PC, auf dem Sie das Wiener Testsystem installieren möchten und entpacken Sie die Datei.

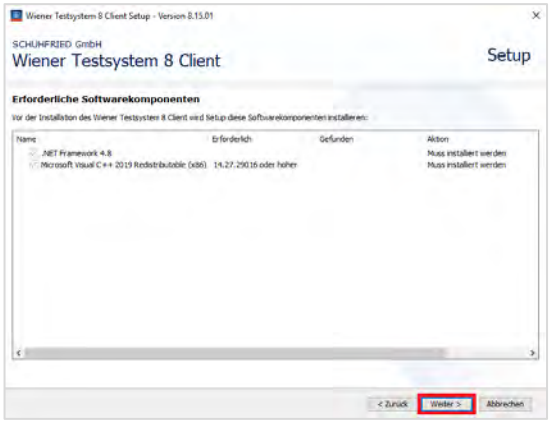
   Starten Sie die Installation mit einem Doppelklick auf die Datei **„Wts8Setup.exe“** und lesen Sie hier direkt ab Punkt 5 weiter.
3. Wenn Sie einen USB-Stick mit dem Setup besitzen, stecken Sie diesen in einen USB-Port Ihres Computers, um die Wiener Testsystem Installation zu ermöglichen.
4. Öffnen Sie den Arbeitsplatz (bei Windows 7 „Computer“) und doppelklicken Sie auf das Symbol für den USB-Stick. Im Unterordner „content“ **doppelklicken Sie auf die Datei „ClientSetup.exe“** um das Setup-Programm zu starten.

5. Anschließend öffnet sich eine Standardsicherheitsabfrage von Windows.

   Bestätigen Sie die Sicherheitsabfrage mit „Ja“.



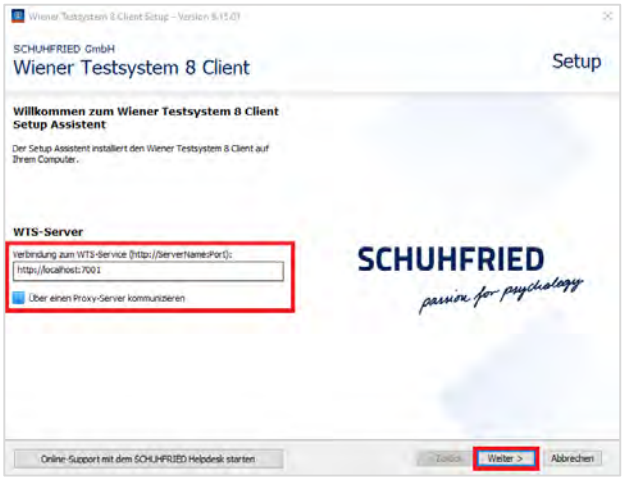
6. Falls das .NET Framework 4.8 noch nicht installiert ist, müssen Sie der Endbenutzer-Lizenzvereinbarung zustimmen.
   Im Anschluss werden die notwendigen Programme aufgelistet. (Bitte keine Änderungen in der Programmliste vornehmen!)
   Bestätigen Sie mit „Weiter >“.
   Diese beiden Schritte entfallen, falls das Framework auf dem Client-PC bereits installiert ist!



7. Im nächsten Schritt müssen die Verbindungsdaten zum „WTS-Server“ angegeben werden. Tragen Sie den **Namen** (oder die IP-Adresse) des Servers sowie den **Port des Dienstes** ein.

Das Format für die Serveradresse ist: http://SERVERNAME:PORT, z.B.: http://WTSSERV:7001.

Falls ein Proxy-Server verwendet wird, klicken Sie die Checkbox „Über einen Proxy-Server kommunizieren“ und tragen Sie Ihre Konfiguration ein.



Auch bei den Clients müssen die verwendeten Ports für die Kommunikation offen sein!

In den nächsten Schritten legen Sie fest, welche Komponenten auf dem Computer installiert werden sollen:

8. In diesem Schritt können Sie den **WTS-Testplayer** (zum Testen mit Direct Testing) **installieren.**

Es können anschließend die folgenden Optionen eingetragen werden:

- Standardsprache: Diese Sprache ist unabhängig von der Testsprache.
- Mandant: Hier kann eingestellt werden, ob ein fixer Mandant verwendet werden soll, oder bei jedem Start des Testplayers nach dem Mandanten gefragt werden soll.
- Test-Info am WTS-Kontrollmonitor anzeigen: Ist notwendig, wenn ein Kontrollmonitor verwendet wird. Dafür muss die Verbindung (IP-Adresse oder Name **und** Port) zu dem Rechner, auf dem der Kontrollmonitor installiert ist, angegeben werden.
- Symbole auf dem Desktop:
  - Testplayer für Direct Testing
  - Hardwaretest um am Client die angeschlossen Hardware von SCHUHFRIED zu überprüfen.

9. In diesem Schritt können Sie die **WTS-Administrationssoftware installieren.**
Sie können die Standardsprache einstellen und entscheiden, ob ein Icon am Desktop erzeugt werden soll.
Die Sprache der Administrations-software kann nachträglich noch umgestellt werden.
Im Zuge der Installation wird auch der Testplayer installiert. Es können somit Testungen aus der Administrationssoftware gestartet werden, ohne extra den Testplayer zu installieren.
Über die Checkbox kann eingestellt werden, ob ein Icon am Desktop erstellt werden soll.

10. In diesem Schritt können Sie den **WTS-Kontrollmonitor installieren.**
Sie können die Standardsprache einstellen und entscheiden, ob ein Icon am Desktop erzeugt werden soll.

Installieren Sie den Kontrollmonitor auf dem Computer, von dem aus die Testplätze überwacht werden sollen.
Zur Konfiguration des Kontrollmonitors sehen Sie auch in Abschnitt 3.8.

11. Sie erhalten nun eine Zusammenfassung Ihrer Einstellungen. Um die Installation zu beginnen, betätigen Sie **„Installieren“**.

Dabei bedeutet:

- TP: Testplayer
- AC: Administrationssoftware (samt den Sparten)
- CM: Kontrollmonitor

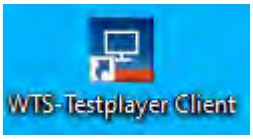
12. Nun wird die Installation durchgeführt.

13. Konnte die Installation erfolgreich abgeschlossen werden, erscheint die Bestätigung der Installation. **Bestätigen Sie mit „Fertigstellen“**.

Die Installation ist nun abgeschlossen. Sie finden am Desktop und im Startmenü Einträge zum Starten der jeweiligen Programme.

Icon zum Aufruf der
Administrations-Software des Wiener Testsystems

Je nach lizenzierter Version kann das Icon den Zusatznamen (HR, Neuro, Verkehr oder Sport) tragen.



Icon zum Aufruf des
Testplayers für Direct Testing mit dem Wiener Testsystem

Icon zum Aufruf des
Kontrollmonitors für das Wiener Testsystem

3.4.1 Hinweise zur Client-Installation

Wenn Sie **nur** die Administrationssoftware installieren, können Sie keine Tests starten; auch nicht direkt aus der Administrationssoftware. Dafür benötigen Sie **auch** die Installation des Testplayers.
Falls Sie einen Proxy-Server verwenden, werden diese von den globalen Proxyeinstellungen von Windows übernommen.[3]
Für die Konfiguration des Features „**Picture 2 Proof**“ muss der Testplayer mit dem Parameter „-c“ gestartet werden, z.B.: „C:\Program Files (x86)\SCHUHFRIED GmbH\Wiener Testsystem 8 Client\TestPlayer\WTSTestplayer.exe -c“. Die ausgewählte Kamera wird dann in der Konfigurationsdatei von WTSTestplayer.exe gespeichert. Es muss sichergestellt sein, dass der Benutzer, der die Kamera konfiguriert, Schreibrechte für den Ordner hat, in dem sich die oben genannte Konfigurationsdatei befindet.

3.4.2 Hinweise zur Installation

Mit den Daten, die in den Feldern **„Standard Benutzername“** und **„Kennwort“** bei der Wiener Testsystem Server Installation eingegeben wurden, ist der Start des Wiener Testsystems nach der Installation möglich. Dieser Benutzer hat volle Administrations-Rechte im Wiener Testsystem. Damit können daher neue Benutzer anlegt und deren Berechtigungen gesetzt werden.

Es muss unbedingt einen Benutzer geben dem die Sicherheitsstufe (0=Null) zugewiesen ist. Ohne einen Benutzer in dieser Sicherheitsstufe können keine administrativen Aufgaben im Wiener Testsystem durchgeführt werden.
Folgende Sicherheitsstufen gibt es:

Sicherheitsstufe	Berechtigung
0	In dieser Sicherheitsstufe sind alle Funktionen und Einstellungen des Wiener Testsystems zugänglich.
1	In dieser Sicherheitsstufe können keine Einstellungen geändert werden. Es können daher keine Testbatterien erstellt oder geändert werden, keine Grundeinstellungen (z.B. Ordner für Datenspeicherung) verändert werden und keine Tests installiert werden. Das Wiener Testsystem kann aber zur Testvorgabe benutzt werden und der Zugriff auf die Datenbanken ist uneingeschränkt möglich.
2	In dieser Sicherheitsstufe ist das Wiener Testsystem nur zur Testvorgabe und anschließenden Auswertung verwendbar. Die anderen Funktionen sind gesperrt. Die Testergebnisse sind insofern eingeschränkt zugänglich, dass lediglich die bei der Testvorgabe gespeicherten Datensätze im Anschluss an die Testvorgabe ausgewertet werden können. Andere Testergebnisse können nicht aufgerufen werden.
3	In dieser Sicherheitsstufe ist das Wiener Testsystem ausschließlich zur Testvorgabe verwendbar. Alle anderen Funktionen und der Zugriff auf die Datenbank sind komplett gesperrt.

[3] Gilt nur, wenn sich der Proxy-Server zwischen dem Rechner, auf dem die Client-Installation ausgeführt wird, und dem Rechner, auf dem der Server installiert ist, befindet.

Die Applikationen des Wiener Testsystems sind signiert. Die Signatur wird in der Standardeinstellung von Windows-Betriebssystemen über einen Server überprüft. Diese Prüfung findet statt, wenn Windows ein Netzwerk detektiert. Sollte die Kommunikation ins Internet durch Netzwerkeinstellungen blockiert werden, kann dies zu starken Verzögerungen beim Starten des Wiener Testsystems oder beim Starten von Testungen führen.
In diesem Fall empfiehlt es sich die Signaturprüfung abzuschalten.

3.4.3 Installation der Clients über Command-Line

Die Installation der Clients (Administrations-Software (ADSW) und Testplayer(TP)) kann auch silent gesteuert über Parameter erfolgen. Folgendermaßen ist der Aufruf definiert:

```
ClientSetup.exe     /qx
          INSTALL_AC=1 LANGUAGE_AC=de-DE
          INSTALL_TP=1 LANGUAGE_TP=de-DE MANDANT_ID=AUTO
          WTS_SERVICE_BASE_ADDRESS=https://XX.XX:7xxx
```

Die Parameter für das Client-Setup werden immer automatisch festgelegt und können nicht in der Commandline des One-Setup vorgegeben werden:
INSTALL_TP=1
INSTALL_AC=1
INSTALL_CM=0
ICON_TP=1
ICON_AC=1
ICON_HWT=1
ICON_CM=0
WTS_SERVICE_BASE_ADDRESS=http:|//localhost:[WTS_SERVICE_PORT]
LANGUAGE_AC=[DEFAULT_CULTURE] LANGUAGE_TP=[DEFAULT_CULTURE]
MANDANT=”mandantname”
MANDANT_ID=AUTO
Wenn die automatisch gewählten Parameter nicht passend sind, dann sollte RUN_CLIENT_SETUP=0 verwendet werden und das Client-Setup mit den gewünschten Parametern extra aufgerufen werden.

Erläuterungen:

Parameter	Wert	Beschreibung
/qx	qr	Keine Benutzereingabe mit Anzeige des Installationsfortschritts
	qb	Keine Benutzereingabe mit Anzeige des Installationsfortschritts als Fortschrittsbalken
	qn	Keine Benutzereingabe und keine Anzeige des Installationsfortschritts
INSTALL_AC **INSTALL_TP** **INSTALL_CM**	1/0	Wenn einer dieser Parameter auf „1“ gesetzt ist, wird die Administrationssoftware (AC), der Testplayer (TP) oder der Server des Kontrollmonitors (CM) installiert. Wenn ein Parameter auf „0“ gesetzt ist, wird das entsprechende Paket nicht installiert. Wird die AC oder der TP installiert, **muss** die **„WTS_SERVICE_BASE_ADDRESS“** angegeben werden. Für die zu installierende Komponente muss weiters die Default-Sprache eingestellt werden (siehe unten).

WTS_SERVICE_BASE_ADDRESS		**Adresse des WTS-Services und Port** über den die Clients mit dem Server kommunizieren. Diese Parameter sind unbedingt erforderlich, wenn TP oder AC installiert werden, z.B. WTS_SERVICE_BASE_ADDRESS=WTSSERV:7001
LANGUAGE_AC **LANGUAGE_TP** **LANGUAGE_CM**		Die Sprache, in der die Administrations-Software, der Testplayer oder der Kontrollmonitor installiert werden. Folgende Sprachen sind verfügbar: • cs-CZ: Tschechisch • de-DE: Deutsch • en-US: Englisch • es-ES: Spanisch • fr-FR: Französisch • it-IT: Italienisch • nl-NL: Niederländisch • pl-PL: Polnisch • pt-PT: Portugiesisch • ro-RO: Rumänisch • ru-RU: Russisch • sk-SK: Slowakisch • sl-SL: Slowenisch • sv-SE: Schwedisch • tr-TR: Türkisch • zh-CN: Chinesisch
MANDANT		Optionaler Parameter – Client-Name: Wenn diese Option angegeben wird, versucht das Client-Setup nicht, den Client über die Serverinstallation aufzulösen, so dass das Client-Setup unabhängig vom Server-Setup installiert werden kann. Wenn dieser Parameter angegeben wird, ist es nicht nötig, dass der Server erreichbar ist. Der Parameter akzeptiert ebenfalls keinen leeren String (“”)
MANDANT_ID		Über diesen Parameter kann der Mandant eingestellt werden, mit dem der Testplayer starten soll (z.B. W12345_001). Wenn „AUTO“ eingetragen ist, wird der erste Mandant gewählt, der am Server gefunden wird. Wenn der Mandant bei jedem Start eingegeben werden soll, muss **MANDANT_ID="-"** angegeben werden!
ACTIVATE_CM	0/1	Einstellung für den **Testplayer**, um den Kontrollmonitor zu verwenden (bei „1“). Durch diese Einstellung schickt der TP die notwendigen Informationen an den Kontrollmonitor.
RUN_CLIENT_SETUP	0	Die Ausführung des Client-Setups wird unterdrückt.
ICON_AC **ICON_TP** **ICON_HWT** **ICON_CM**	0/1	Bestimmt, ob die entsprechenden Desktop-Icons installiert werden. Bei der Testplayerinstallation kann angegeben werden, ob zusätzlich zum Icon des Testplayers auch ein Icon für den Hardware-Test angelegt werden soll.
CACHE_DIRECTORY	String	Angabe des Pfads, in dem der Cache der Administrationssoftware und des Testplayers aufgebaut werden soll. Beispiel: CACHE_DIRECTORY=“d:\temp\schuhfried“
/exelang	1031 1033	Setup in deutscher Sprache starten (optional) Setup in englischer Sprache starten (optional)

Beispiele:

Installation der Administrationssoftware mit Icon in englischer Sprache:

```
ClientSetup.exe /qr INSTALL_AC=1 ICON_AC=1 LANGUAGE_AC=en-US
    WTS_SERVICE_BASE_ADDRESS=https://192.168.0.113:7001
```

Installation des Testplayers in Deutsch mit Verwendung des Kontrollmonitors und Icons für Testplayer und Hardware-Test:

```
ClientSetup.exe /qr INSTALL_TP=1 ICON_TP=1 ICON_HWT=1
    LANGUAGE_TP=de-DE MANDANT_ID=AUTO
    WTS_SERVICE_BASE_ADDRESS=https://WTS_SERVER:7001
    ACTIVATE_CM=1 CM_SERVICE_BASE_ADDRESS=https://WTS_CM_SERV:8888
```

Installation des Kontrollmonitor-Servers in Italienisch:

```
ClientSetup.exe /qr INSTALL_CM=1 ICON_CM=1 LANGUAGE_CM=it-IT
```

Installation des Testplayers in Deutsch ohne Verwendung des Kontrollmonitors, mit Icon für den Testplayer, mit einem bestimmten Mandanten:

```
ClientSetup.exe /qr INSTALL_TP=1 ICON_TP=1 LANGUAGE_TP=de-DE
    MANDANT_ID=W12345_003
    WTS_SERVICE_BASE_ADDRESS=https://WTS_SERVER:7001
    CACHE_DIRECTORY=”D:\Temp\Schuhfried”
```

Installation des Testplayers in Englisch ohne Verwendung des Kontrollmonitors, mit Icon für den Testplayer, ohne bestimmten Mandanten:

```
ClientSetup.exe /qr INSTALL_TP=1 ICON_TP=1 LANGUAGE_TP=en-US
    WTS_SERVICE_BASE_ADDRESS=https://WTS_SERVER:7001
    MANDANT_ID=
```

Hinweise:

- Die Adressen des WTS-Servers und des Kontrollmonitors können entweder mit IP-Adressen angegeben werden oder mit den Domänennamen.
- Wenn **jedes Mal beim** Starten des Testplayers der Mandant ausgewählt werden soll, muss der Wert bei „`MANDANT_ID`“ weggelassen werden.
- Doppelte Anführungszeichen um die Werte eines Properties sind nicht notwendig, aber zulässig (z.B. `DEFAULT_CULTURE=“en-US“`). Es ist aber nicht möglich, einem Property (außer bei `MANDANT_ID`) einen Leerwert zuzuweisen. Z.Bsp. ist `TP_PROP=““` oder `LANGUAGE_TP=` nicht zulässig und führt zu einer fehlerhaften Verarbeitung.
- Wichtig ist, dass der WTS-Server und das Port korrekt angegeben werden und der Dienst am Server während der Installation erreichbar ist. Die Installation läuft auch ohne erreichbaren Server durch, ist dann aber nicht erfolgreich!
- Bei den Parametern `INSTALL_xx, ICON_xx` und `ACTIVATE_CM` kann auch der Defaultwert 0 explizit angegeben werden. Dieser führt dazu, dass die jeweilige Komponente bzw. das jeweilige Icon NICHT installiert wird (z.B. `INSTALL_TP=0`).
- Da ein Doppelslash (//) in der Commandline eine reservierte Zeichenfolge ist, muss davor unbedingt noch das | Zeichen gesetzt werden. Davon sind insbesondere URL-Angaben betroffen, die mit https://.... beginnen. Daher muss https://meine-domäne:7001 geschrieben werden, statt https:|//meine-domäne:7001 geschrieben werden!
- Der Parameter /exelang muss, wenn angegeben, an erster Stelle stehen.

Die Clients können auch silent deinstalliert werden. Dafür kann, je nach Betriebssystem, der folgende Befehl verwendet werden:

```
msiexec /uninstall wts8clientsetup.msi /quiet
msiexec /uninstall wts8clientsetup.x64.msi /quiet
```

3.5 Update des Wiener Testsystems

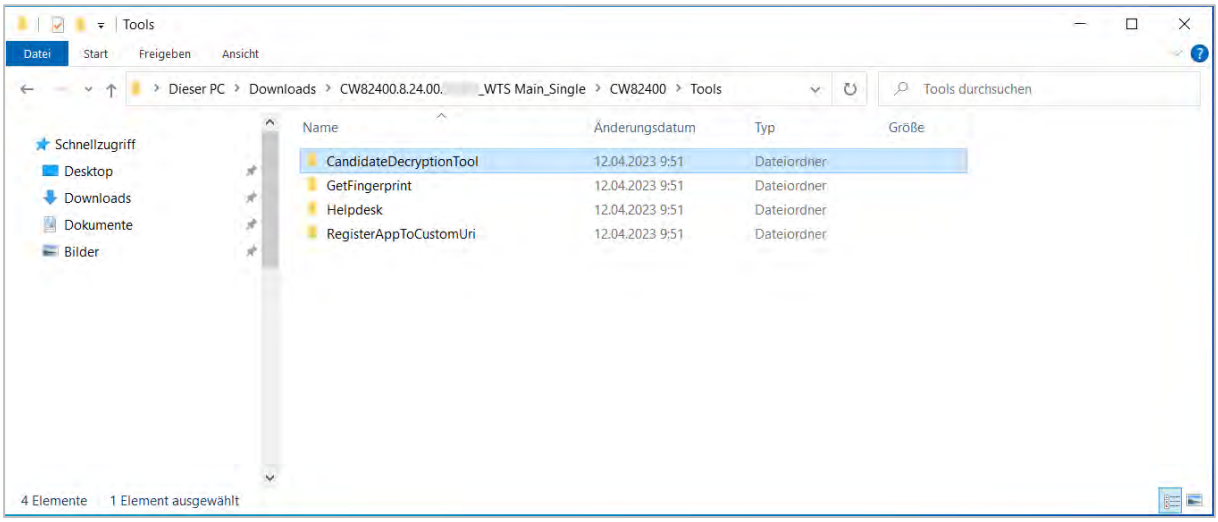
Für das Updaten des Wiener Testsystems folgen Sie einfach der Installationsanleitung, die Ihrem System entspricht. Bitte beachten Sie, dass Sie im Zuge des Updates **als erstes den Server** updaten und **anschließend die Clients!**
Ab Version 8.24.00 werden die Kandidatendaten in der Datenbank nicht verschlüsselt und alle Daten werden während der Installation des WTS entschlüsselt. In diesem Fall kann die Einrichtung erst fortgeführt werden, wenn ein Lizenz-Dongle für einen Client/eine Umgebung vorhanden ist. Jedoch gibt ist für den Fall, dass die Daten innerhalb der Datenbank gesichert werden müssen, unter folgenden Link eine Liste möglicher Lösungen aufgeführt: https://schuhfried.com/increase-security/ oder in Abschnitt 7.5 des Handbuchs „IT-Sicherheitskonzept“.
Nach dem Update des ersten Clients sollte das WTS System auf ordnungsgemäße Funktion überprüft werden. Danach können die restlichen (Client) Systeme entsprechend aktualisiert werden.
Beim Start eines Clients wird geprüft, ob die Version des Clients mit der Version des Servers übereinstimmt. Der Client wird nicht gestartet, falls die Versionen nicht übereinstimmen.
Bitte halten Sie für das Update der Clients die **IP-Adresse (oder den Namen) des Servers** bereit, da Sie diese im Zuge des Updates neu eingeben müssen.

Bitte beachten Sie, dass bei einem Update ein allfällig vorhandener SW-Dongle erhalten bleibt. Es gilt daher weiterhin, dass sich die spezifischen Eigenschaften eines virtuellen Systems nicht ändern dürfen. Sollte das virtuelle System „verschoben“ werden, wird der Software-Dongle ungültig und Ihr Wiener Testsystem gesperrt. Für nähere Details wenden Sie sich bitte, **bevor der Server verändert wird**, an den SCHUHFRIED Support (siehe Abschnitt 5.3).
Die folgenden Eigenschaften des virtuellen Systems **müssen gleichbleiben**, damit der Software-Dongle gültig bleibt:

- Virtuelle MAC-Adresse
- CPU-Eigenschaften
- UUID (Universal Unique Identifier) des virtuellen Abbilds; die UUID wird durch die Virtualisierungssoftware generiert. Wenn ein Clone erzeugt wird, wird eine neue UUID erzeugt.

3.5.1 Manuelles Entschlüsseln von Kandidatendaten

Bei Aktualisierung des WTS entschlüsselt der WTS Setup Installer automatisch die Daten des Kandidaten, wenn diese in der Datenbank verschlüsselt sind. Vor dem Starten des WTS Setup Installers können Sie das „CandidateDecryptionTool“ jedoch auch manuell über die Befehlszeile starten. Achtung: WTS Service muss vorher gestoppt werden. Natürlich muss der Lizenz-Dongle für einen Client/eine Umgebung auf dem Computer eingesteckt oder über den lokalen Sentinel-Server verfügbar sein. Nach Entschlüsselung der Daten durch das Entschlüsselungs-Tool darf WTS Service nicht erneut gestartet werden, da es ansonsten die Daten wieder verschlüsselt. Das Entschlüsselungs-Tool ist im Lieferumfang unter dem folgenden Pfad verfügbar:
“~\CW82400\Tools\CandidateDecryptionTool\CandidateDecryptionTool.exe” (siehe folgende Tabelle).



Um das Entschlüsselungstool zu starten, die Befehlszeile (cmd) öffnen und in den Ordner wechseln, in dem sich das Tool befindet. Dann den Namen des Tools „CandidateDecryptionTool.exe“ eingeben. Eine Übersicht der Eingabeparameter für das Tool:

Parameter	Wert	Beschreibung
- [connectionstring | c]	string	Datenverbindungszeichenfolgen im Format MS SQL z. B.: “Server=<hostname>\WTSNXEXPRESS;Initial Catalog=wts;Persist Security Info=False;User ID=wtsnx;Password=<password>; MultipleActiveResultSets=False;Encrypt=False;TrustServer Certificate=False;Connection Timeout=30;"

Beispiel:

```
CandidateDecryptionTool.exe -c "Server=TestSetupEnv-ms
    \WTSNXEXPRESS;Initial Catalog=wts;Persist Security
    Info=False;User
    ID=wtsnx;Password=<password>;MultipleActiveResultSets=False;Encr
    ypt=False;TrustServerCertificate=False;Connection Timeout=30;"
```

CandidateDecryptionTool verfügt über keine Fortschrittsanzeige. Der Fortschritt und das Ergebnis des Entschlüsselungsvorgangs können über die Log-Datei unter dem folgenden Pfad eingesehen werden: “C:\Users\<username>\AppData\Local\Temp\CandidateDecryptionTool\ CandidateDecryptionTool.log”

3.5.2 Aktualisierung des WTS mit einem Lazy-Update der Datenbank

Ab Version 8.26 unterstützt unser Installationsprogramm den neuen Kommandozeilenparameter „UPDATE_DB=false“, der es ermöglicht, nur die Installationsdateien auf die neueste Version zu aktualisieren, ohne die Datenbank zu aktualisieren. Dies ist hilfreich, wenn Sie mehrere WTS-Server haben, auf denen Sie das Installationsprogramm parallel laufen lassen und dann eine zentrale Datenbank aktualisieren wollen, da es verhindert, dass unsere Installationsprogramme einen Konflikt der Datenbank-Updates verursachen. Für eine spätere Datenbankaktualisierung stellen wir jetzt mehrere

weitere Werkzeuge im Unterordner „Tools“ des dekomprimierten Archivs des Installationsprogramms zur Verfügung.
Wenn Sie eine Aktualisierung der Datenbank vorbereiten, nachdem Sie Ihre Serverdateien aktualisiert haben, kopieren Sie immer den gesamten Ordner „Tools“ auf den Server, auf dem das Update erfolgen soll. Das wichtigste dieser Tools befindet sich im Unterordner „DbUpdaterCli“ des Ordners „Tools“. Dieses Tool aktiviert auch andere Tools aus dem Ordner „Tools“, daher ist es wichtig, den gesamten Ordner zu kopieren.
Wenn das Installationsprogramm mit dem Parameter „UPDATE_DB=false“ (für eine Standard-Installation) oder „UPDATE_DB=false SQL_SA_USER_DECLARED=true“ (für eine benutzerdefinierte Datenbank-Installation) ausgeführt wird, sollte eine JSON-Konfigurationsdatei erzeugt werden, die für die Ausführung von „DbUpdater.exe“ verwendet wird. Bei der Verwendung von „UPDATE_DB=false“ im benutzerdefinierten Datenbank-Modus können Sie einen SQL-Benutzer mit Leseberechtigung angeben, da bei der Einrichtung nichts in die Datenbank geschrieben wird.
Diese JSON-Konfigurationsdatei sollte im Verzeichnis „Tools/DbUpdaterCli/db-full-update-params.json“ erstellt werden.

WICHTIG: Für diesen Installationsmodus ist es notwendig, die Datei Wts8Setup.exe von einem kurzen Dateipfad aus zu starten, z. B. c:\tmp\CW82600\Wts8Setup.exe, da sonst die Datenbankaktualisierung nach Abschluss der Installation fehlschlagen kann.

Durchführung eines kompletten Datenbank-Updates nach Installation mit „UPDATE_DB=false“:

1. Gehen Sie auf den Ordner „Tools“ und anschließend auf den Ordner „DbUpdaterCli“ Ihres entpackten Installationsarchivs.
2. Öffnen Sie als Administrator die PowerShell dieses Ordners.
3. Öffnen Sie „Tools/DbUpdaterCli/db-full-update-params.json“ in einem Texteditor Ihrer Wahl.
4. Überprüfen Sie anhand des Abschnitts *Parameters inside full-update-config.json* , dass alle Werte für die Installation korrekt sind.
5. Führen Sie den Befehl „.\DbUpdater.exe -x -y db-full-update-params.json“ aus.
6. Wenn der Befehl fehlerhaft ausgeführt wird, starten Sie nicht den Dienst WTS Service, sondern wenden Sie sich an den Kunden-Support.

Parameter in db-full-update-params.json

- *DbServerInstanceName* – SQL-Server zur Verbindung bei einem Update der Datenbank, standardmäßig „localhost\\WTSNXEXPRESS“.
- *WtsnxUserName* – Name eines SQL-Benutzers mit Vollzugriff auf alle WTS-Datenbanken, standardmäßig „wtsnx“.
- *WtsnxPassword* – aktuelles Passwort des SQL-Benutzers mit Vollzugriff auf alle WTS-Datenbanken, standardmäßig „wtsnx“-Benutzer.
- *NewWtsnxPassword* – neues Passwort, dass für den SQL-Benutzer mit Vollzugriff auf alle WTS-Datenbanken eingerichtet wird (standardmäßig „wtsnx“-Benutzer) – entspricht meistens dem Parameter „WtsnxPassword“ (keine Änderung des Passworts).
- *SaUserName* – Name des SQL-Benutzers mit Servereigentümerrechten (z. B. zur Änderung der Datenbank, standardmäßig „sa“.
- *SaPassword* – aktuelles SQL-Passwort des Benutzers mit Servereigentümerrechten.

- *NewSaPassword* – neu festzulegendes SQL-Passwort für den Benutzer mit Servereigentümerrechten. Entspricht in den meisten Fällen dem Parameter „SaPassword“ (keine Änderung des Passworts).
- *DbLegacyPasswords* – dieser Parameter wird intern zur Konfiguration des Datenbankbenutzers benötigt. In den meisten Fällen ist ein JSON-Array ausreichend ([]).
- *DbName* – Bezeichnung der WTS-Datenbank, standardmäßig „wts“
- *ProductDbName* – Bezeichnung der WTS-Produktdatenbank, standardmäßig „WTSKatalog“.
- *WtsDbMdfFilePath* – Dies ist der Pfad zur Datei der WTS-Datenbank. Dieser Parameter wird vom Installationsprogramm in der Struktur der Konfigurationsdatei „JSON“ erstellt, standardmäßig „c:\\programdata\\schuhfried\\sqldatabase\\wts_deploy.m“.
- *SqlDbDir* – Pfad für den Ordner, in dem das WTS die Datenbanken speichert, standardmäßig „c:\\programdata\\schuhfried\\sqldatabase“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *ProductDbDir* – Pfad des Ordners, in dem sich die Quelldateien „.mdf“ und „.ldf“ für die Datenbank „WTSKatalog“ befinden, standardmäßig „.\\“. Das Installationsprogramm erstellt diesen Parameter in der Struktur der JSON-Konfigurationsdatei.
- *DoWriteEncryptionActivityLogEntry* – Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“. Beispiel: „wahr“.
- *ContentUpdateFolderPath* – „C:\\update“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“. Erfordert einen absoluten Pfad.
- *MediaFolderPath* – Pfad für den Ordner mit den Mediendateien der aktuellen Version des WTS, standardmäßig „c:\\programdata\\schuhfried\\media“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“. Erfordert einen absoluten Pfad.
- *MandantName* – Name des Mandanten. Beispiel: „IncLic_001“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *MandantCulture* – Sprachcode für die Sprache des Mandanten. Beispiel: „en-US“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *AcUserName* – Name des Benutzers mit Administratorrechten. Beispiel: „Admin“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *AcPassword* – Passwort des Benutzers mit Administratorrechten oder leer. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *HardwareKeyId* – HASP-Lizenzschlüssel-ID für den Mandanten. Beispiel: „213567016854890580“. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.
- *ProductLanguage –* MS-Windows-Sprachcode der Produktsprache des WTS (1031 – Deutsch de-DE, 1033 – Englisch en-US) – wird auf die für den Mandanten festgelegte Sprache gesetzt. Beispiel: 1033. Das Installationsprogramm erstellt diesen Parameter in der Struktur für den Konfigurationsordner „JSON“.

3.6 Lizenzinstallation

3.6.1 Installation von Lizenzen

Software-Freischaltecodes können ausschließlich über „Lizenzdateien“ nachinstalliert werden! Lizenzdateien haben die Endung „V2C“ oder „SFLIC“.
Gehen Sie folgendermaßen vor, um eine Lizenzdatei in Ihr System einzuspielen:

1. Speichern Sie die Lizenzdatei (Endung „V2C“ oder „SFLIC“) auf dem Rechner ab, auf dem das Wiener Testsystem installiert ist.
2. Öffnen Sie das Wiener Testsystem und gehen Sie zu "**Einstellungen -> Lizenzverwaltung -> Lizenzen**".
3. Klicken Sie die Schaltfläche **„…“** (siehe unten) und wählen Sie die zuvor abgespeicherte Lizenzdatei aus. Damit wird die Datei in das leere Feld links von der Schaltfläche geschrieben.
4. Klicken Sie nun auf „**Update einspielen**“. Sie erhalten eine Bestätigung, dass die neuen Lizenzen eingespielt worden sind.

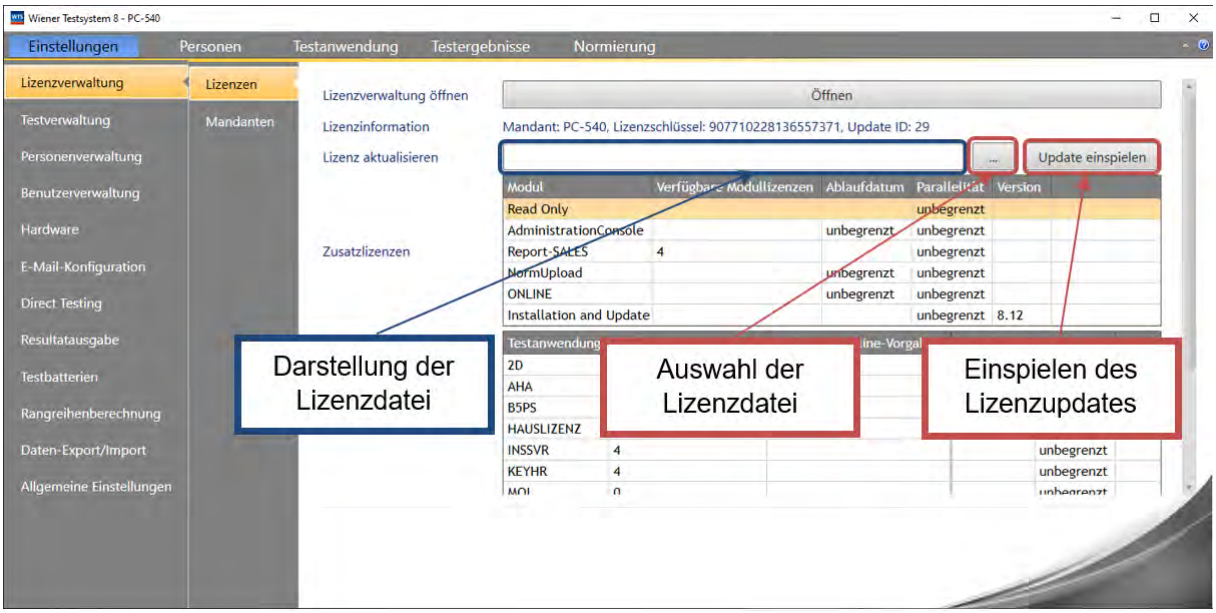


Abbildung 4: Einspielen von zusätzlichen Lizenzen

Hinweis:

- Um eine Lizenzdatei installieren zu können, müssen sämtliche bisherigen Lizenzdateien bereits installiert sein.
- Die erste Lizenzdatei eines Systems ist bereits installiert. Bei einer Installation des Wiener Testsystems muss diese daher nicht gesondert installiert werden.
- Die Lizenzdatei mit der Endung „SFLIC“ beinhaltet sämtliche bisherigen Lizenzdateien. Sämtliche „fehlenden“ Lizenzdateien werden automatisch installiert.

3.6.2 Lizenzinstallation ohne Administrationssoftware

Wenn ein Software Dongle verwendet wird, muss die Lizenz installiert werden, bevor das Wiener Testsystem installiert wird. Daher kann man in diesem Fall nicht dem Ablauf aus Abschnitt 3.6.1 folgen. Über das „Sentinel Admin Control Center“ können **nur Dateien mit der Endung „v2c“** installiert werden. Um die Lizenzen zu installieren, muss daher folgendermaßen vorgegangen werden:

1. Öffnen Sie Ihren Internet Browser und geben Sie http://localhost:1947 in der Adressleiste ein.
2. Es öffnet sich das „Sentinel Admin Control Center“.
3. Wählen Sie „Update/Attach“ in der linken Navigationsleiste.
4. Öffnen Sie mit „Durchsuchen …“ die erhaltenen Lizenzdatei.
5. Klicken Sie auf „Apply File“ um die Lizenzen zu installieren.
6. Es wird eine Bestätigung ausgegeben, dass die Lizenzen installiert worden sind.

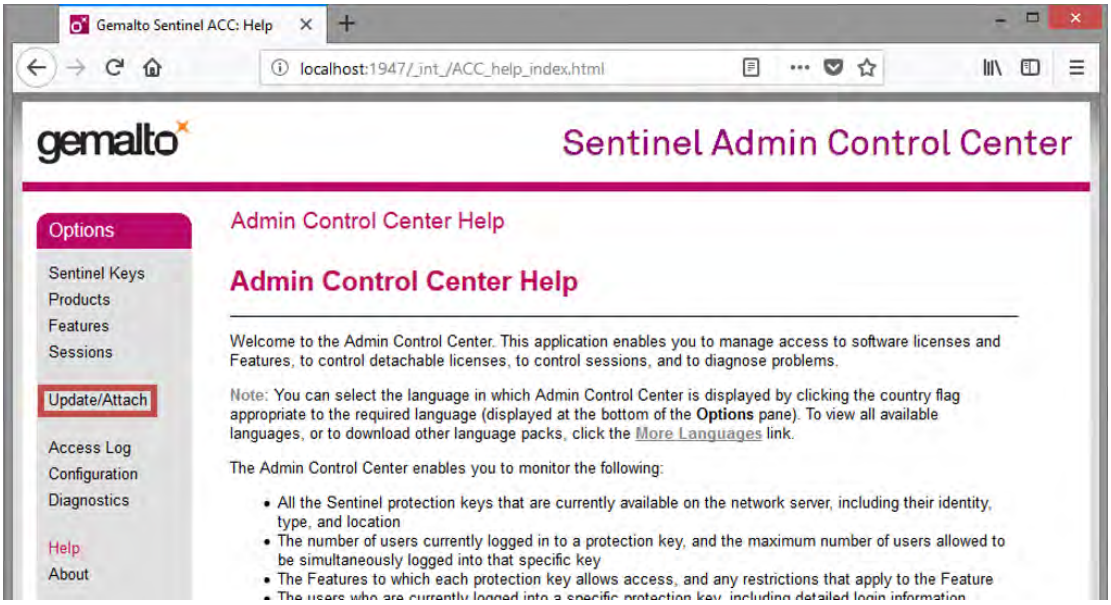


Abbildung 5: Sentinel Admin Control Center

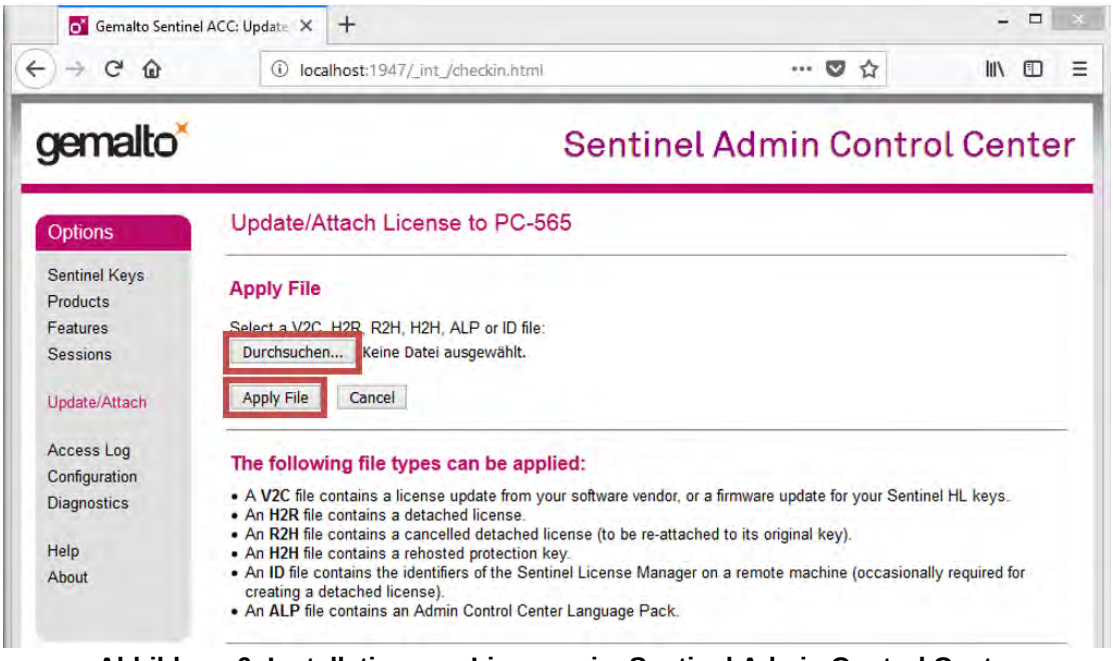


Abbildung 6: Installation von Lizenzen im Sentinel Admin Control Center

3.7 Deinstallation

So können Sie das Wiener Testsystem von der Festplatte Ihres Computers wieder entfernen:

1. Öffnen Sie die Windows-Systemsteuerung über das Windows-Startmenü. Wählen Sie dazu **„Start“ → „Systemsteuerung“**.
2. Doppelklicken Sie auf „**Programme und Funktionen“**.
3. Wählen Sie **„Wiener Testsystem“**.
4. Klicken Sie die Schaltfläche **„Deinstallieren/ändern“**.
5. Wählen Sie in der Programmliste **„Wiener Testsystem“** und klicken Sie auf **„Ändern/Entfernen“**.
6. Folgen Sie den Anweisungen und wählen Sie **„Entfernen“**.

Die Datenbanken, und damit sämtliche Personen und Ergebnisse, **bleiben** auf Ihrem System erhalten, auch wenn das System deinstalliert wurde!
Für nähere Informationen wenden Sie sich bitte an den Help Desk (siehe Abschnitt 5.3).

3.8 Der Kontrollmonitor

Das Wiener Testsystem bietet mit dem **Kontrollmonitor** ein Programm, das zur Überwachung und Steuerung von Testplätzen in einer Client-Server Anlage dient. Dieses Programm kann auf einem „beliebigen“ Rechner nach der Installation des Clients für den Kontrollmonitor gestartet werden, zu dem sich die Testplätze verbinden können, und zeigt pro Testplatz die folgenden Informationen an:

- Name des Computers
- Personendaten (Name und Geburtsdatum)
- Test und Testform, der auf diesem Testplatz gerade bearbeitet wird
- Verschiedene Hinweise, wenn eine Person Hilfe durch den Testleiter benötigt. In diesem Fall blinkt das Feld „Status“ rot-grün und beim entsprechenden Testplayer steht unter „Statusnachricht“ der Warnhinweis.

Weiters kann der Kontrollmonitor zur zentralen Beendigung einer Pause verwendet werden, falls eine Pause[4] in der Testbatterie vorgegeben wird. Kommt eine Person zur Pause, so wird die Testdurchführung so lange angehalten, bis der Testleiter die Pause zentral (Schaltfläche „PAUSE auf allen Testplätzen beenden“ in der Abbildung 7) im Kontrollmonitor beendet.

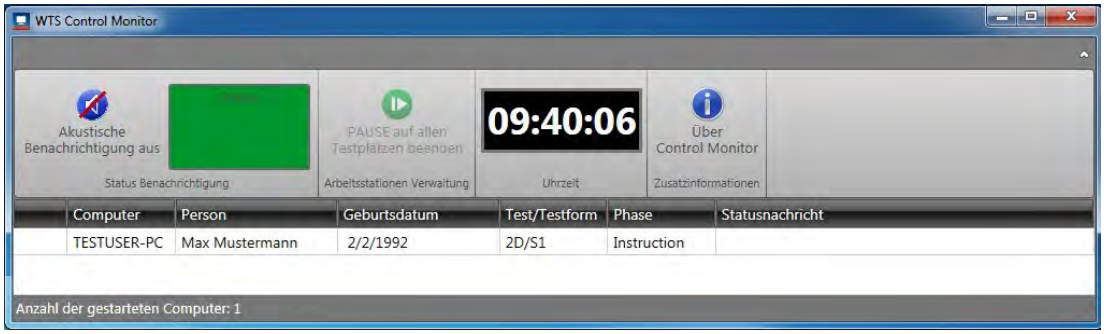


Abbildung 7: Kontrollmonitor

Wenn es bei einem Testplatz zu einem Problem kommt (Hinweis, dass der Testleiter benötigt wird), so wird am Kontrollmonitor neben der optischen Signalisierung auch eine akustische Benachrichtigung ausgegeben. Dies kann über die Schaltfläche „Akustische Benachrichtigung aus“ ausgeschalten werden.

3.8.1 Installation des Kontrollmonitors

Der Kontrollmonitor kann auf einem beliebigen Rechner im Netzwerk installiert werden, es muss sich dabei nicht um den Server handeln, auf dem die Dienste des Wiener Testsystems laufen.
Da die Clients Informationen an den Kontrollmonitor schicken, muss gewährleistet sein, dass die Verbindung zwischen dem Dienst des Kontrollmonitors und den Testplayern möglich ist.
Zur Installation des Kontrollmonitors bestätigen Sie die Komponente „**Kontrollmonitor**“ (siehe Abschnitt 3.4).

[4] Dies setzt die Verwendung der Pause „S1: Pause mit Testleitersteuerung“ voraus

3.9 Verschlüsselte Kommunikation in WTS (HTTPS)

Die Kommunikation zwischen Clients und Server wird im WTS 8 mit einer standardisierten Microsoft-Technologie implementiert mit dem Namen „Windows Communication Foundation“ (kurz WCF). WCF bietet mehrere Möglichkeiten die Kommunikation abzusichern. Die Variante, die im WTS standardmäßig benutzt wird, bietet die Sicherstellung von Vertraulichkeit, Integrität und Authentifizierung auf dem ganzen Weg (end-to-end) zwischen den Clients und dem Server („Message“-Security). Diese Variante ist auf der Applikationsebene implementiert und dabei wird AES-256 für die Verschlüsselung verwendet (https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/wcf/message-of-wshttpbinding).
Zusätzliche Information zur „WCF Security“ finden Sie hier: https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/security-overview
Die anderen APIs werden standardmäßig unter HTTPS gehostet, wobei ein selbstsigniertes, vertrauenswürdiges SSL-Zertifikat benutzt wird.

Im Allgemeinen verwendet WTS immer verschlüsselte Kommunikation. Die Notwendigen Zertifikate werden automatisch generiert.

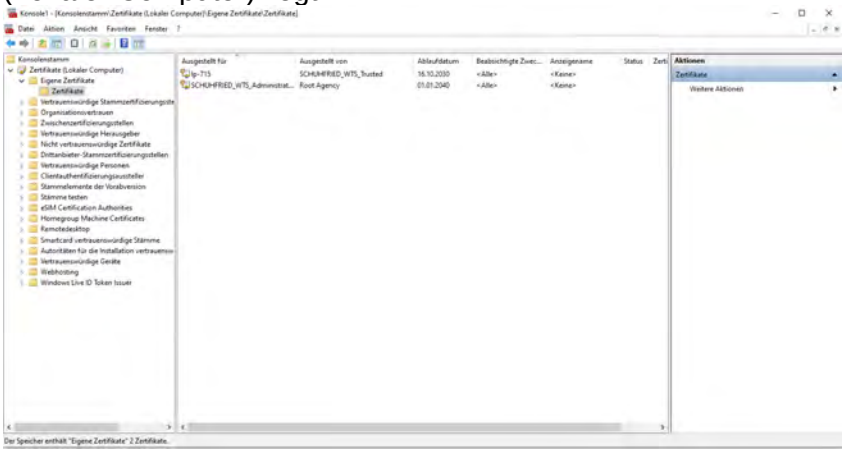
3.9.1 Eigenes HTTPS Zertifikat

Um ein eigenes HTTPS Zertifikat zu verwenden kann die Installation via Command Line durchgeführt werden (Beispiel unter Kapitel 3.3.3). Eine nachträgliche Konfiguration ist manuell möglich jedoch nicht empfohlen. Derzeit können nur gültige RSA-Zertifikate (2048 Bit) verwendet werden.

3.9.2 Eigenes HTTPS Zertifikat - Manuelle Installation

Neben dem WTS Service, beinhaltet das WTS weitere APIs, die mittels HTTPS kommunizieren. Standardmäßig verschlüsseln der WTS Service und diese APIs ihre Kommunikation mit einem vertrauenswürdigen selbstsignierten SSL-Zertifikat, jedoch besteht die Möglichkeit ein eigenes, für die gehostete Domäne ausgestelltes SSL-Zertifikat zu verwenden.
Dafür sind folgende Schritte notwendig:

- Vergewissern Sie sich, dass ihr Zertifikat unter Eigene Zertifikate > Zertifikate (Lokaler Computer) liegt



- Geben Sie den Namen („Subject“) des Zertifikates in den folgenden Config-Dateien an:

- “Installationspfad“\Wiener Testsystem 8\Service\WTSService.exe.config (unter „findValue“ von „serviceCertificate“)

Auch in den Bereichen „QueueStorageSection“ und „ReportSection“ mit den Attributen „CertificateSearchValue="FindBySubjectName" CertificateSearchKind="your-certificate-CN"

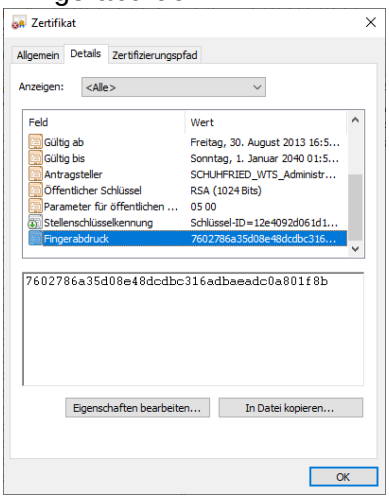
- “Installationspfad“\Wiener Testsystem 8\Api\appsettings.json“ und
- “Installationspfad“\Wiener Testsystem 8\Portal\appsettings.json“ und
- “Installationspfad“\Wiener Testsystem 8\Testplayer.web\appsettings.json“ und
- “Installationspfad“\Wiener Testsystem 8\Identity\appsettings.json” im AppSettings Bereich

```
,,
"AppSettings": {
  "EnableSwagger": false,
  "SwaggerVirtualDir": "",

  "EnableLicenseApi": true,
  "EnableLegacyApi": true,
  "EnableProductApi": true,
  "EnableCommonApi": true,
  "EnableStaticApi": true,
  "EnableSettingApi": true,
  "EnableCandidateApi": true,
  "EnableReportApi": true,
  "EnableResultApi": true,
  "EnablePermissionsApi": true,
  "EnableTestApi": true,
  "EnableUserApi": true,

  "PortalApiAddress": "https://localhost:7013",
  "QueueNames": "1_reporting,2_general,3_import,3_export",
  "CertificateSearchKind": "FindBySubjectName",
  "CertificateSearchValue": "localhost"
},
```

- Binden des Zertifikats an https.sys
  - Fingerabdruck des zuvor importierten Zertifikats finden:
    i. Navigieren Sie zu dem importierten Zertifikat und doppelklicken Sie darauf
    ii. Gehen Sie zum Tab “Details” und suchen in der Spalte “Feld” nach “Fingerabdruck”



    iii. Kopieren Sie den Wert des Fingerabdrucks (entfernen Sie Leerzeichen, sofern vorhanden)
    7ffd45b2302b3c17fc47e74cfed80288fb25569c

    iv. Öffnen Sie die Windows-Eingabeaufforderung (cmd.exe) mit Administrator-Rechten

    v. Befehl für Bindung vorbereiten (ändern Sie **SERVICEPORT** and **THUMBPRINT**)
    netsh http add sslcert ipport=0.0.0.0:**SERVICEPORT** certhash=**THUMBPRINT** appid={76ac1965-2c8f-4f47-9251-9d8f357a7a3d}

    vi. Der Befehl sollte wie folgt aussehen, in der Windows-Eingabeaufforderung ausführen
    netsh http add sslcert ipport=0.0.0.0:7001 certhash=7ffd45b2302b3c17fc47e74cfed80288fb25569c appid={76ac1965-2c8f-4f47-9251-9d8f357a7a3d}

    vii. Wenn die Bindung erfolgreich war bekommen Sie folgende Meldung zu sehen
    “SSL Zertifikat erfolgreich installiert”

    viii. Um zu verifizieren, ob das Zertifikat installiert wurde führen Sie folgenden Befehl aus
    “netsh http show sslcert”

    ix. Dann bekommen Sie folgende Ausgabe

- Wenn sich durch die Änderung des Antragsstellers des Zertifikats (subject) auch die URL geändert hat, unter der das WTS den Dienst und die APIs bereitstellt, müssen in der WTS-Datenbank die Werte in der Tabelle „Client“ anhand der korrekten URL aktualisiert werden (das mitgelieferte SQL-Skript "update_identityserverconfiguration.sql" kann für diese Aufgabe verwendet werden, nachdem die korrekte URL hinzugefügt wurde; das Skript ist im Ordner "Scripts\Help" gespeichert).
- Starten Sie das WTS Service neu

3.9.3 Verwendung eines eigenen HTTPS-Zertifikats – automatische Installation

Ab Version 8.26 unterstützt das Installationsprogramm auch die Installation mit eigenen Zertifikaten der Benutzer, die über Kommandozeilenoptionen übergeben werden:

- EXISTING_CERTIFICATE_SUBJECT – Übertrag des Common Name (CN) des Zertifikatsubjekts eines unter „LocalComputer/Personal windows certificate store“ gespeicherten Zertifikats.
- EXISTING_CERTIFICATE_THUMBPRINT – Übertrag des Thumbprint des Zertifikatsubjekts eines unter „LocalComputer/Personal windows certificate store“ gespeicherten Zertifikats.

In beiden Fällen (das Installationsprogramm findet keine ungültigen Zertifikate) muss das Zertifikat einen privaten Schlüssel mit einer Länge von mindestens 2048 Bit enthalten.

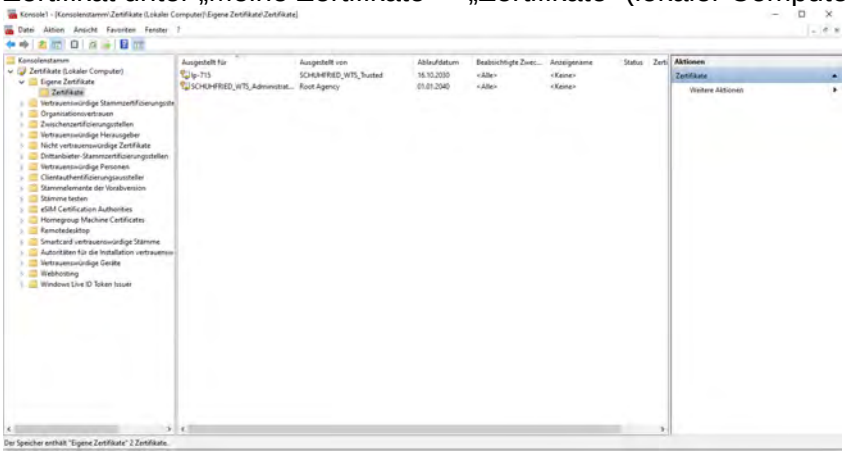
Das Installationsprogramm konfiguriert alle Konfigurationen und koppelt das Zertifikat an die benötigten Ports.

3.9.4 Konfiguration von VIS Universal Plugin via verschlüsselte Verbindung über HTTPS

Die folgenden Schritte beschreiben, wie Sie das Universal-Plugin über HTTPS konfigurieren, indem Sie das beim Setup zur Verfügung gestellte selbstsignierte Zertifikat oder Ihr eigenes SSL-Zertifikat verwenden.

Die folgenden Schritte müssen durchgeführt werden:

- (Optional, wenn Sie Ihr eigenes Zertifikat nutzen) Versichern Sie sich, dass Ihr Zertifikat unter „Meine Zertifikate“ > „Zertifikate“ (lokaler Computer) verfügbar ist

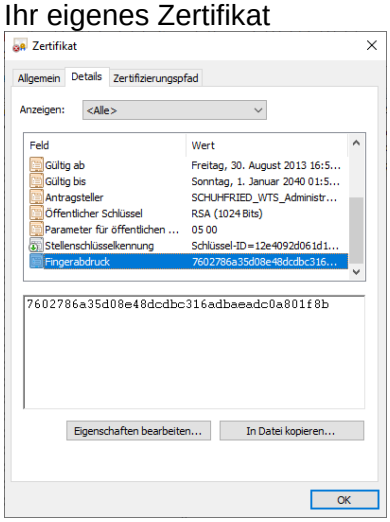


- (Optional, wenn Sie Ihr eigenes Zertifikat nutzen) Geben Sie den Namen („Thema“) des Zertifikats unter „Installation path“\Vienna Test System 8\Service\Plugin\WTS.Integration.Plugins.Universal.UniversalPlugin.dll.config (unter „findValue“ von „serviceCertificate“) ein.

```
<behaviors>
  <serviceBehaviors>
    <behavior name="serviceConfigHttps">
      <serviceMetadata httpsGetEnabled="true"/>
      <!-- To receive exception details in faults for debugging purposes, set the value below to true.  Set to false before deployment to avoid disclosing ex
      <serviceDebug includeExceptionDetailInFaults="false"/>
      <dataContractSerializer maxItemsInObjectGraph="6553600"/>
      <serviceCredentials>
        <userNameAuthentication userNamePasswordValidationMode="Custom" customUserNamePasswordValidatorType="WTS.Business.Common.CommonCore.Configuration.Cus
        <!--SchuhfriedSelfSignedCertificate - trusted root certificate that needs to be installed on the machine out of Schuhfried Root Authority-->
          <serviceCertificate findValue="SchuhfriedSelfSignedCertificate" storeLocation="LocalMachine" storeName="My" x509FindType="FindBySubjectName" />
        <clientCertificate>
          <authentication certificateValidationMode="None"/>
        </clientCertificate>
      </serviceCredentials>
    </behavior>
  </serviceBehaviors>
  <endpointBehaviors>
    <behavior name="TimeSyncFreeEndpointBehavior">
      <timeSyncFreeEndpointBehavior />
    </behavior>
  </endpointBehaviors>
</behaviors>
<serviceHostingEnvironment multipleSiteBindingsEnabled="true"/>
<extensions>
  <behaviorExtensions>
    <add name="timeSyncFreeEndpointBehavior" type="WTS.Business.Common.CommonCore.Configuration.TimeSyncFreeEndpointBehavior, WTS.Business.Common.CommonCore,
  </behaviorExtensions>
```

- Binden des Zertifikats an https.sys
  - Fingerabdruck des zuvor importierten Zertifikats finden:

    I. Öffnen Sie „Zertifikate verwalten“ und gehen Sie auf „Eigene“ > „Zertifikate“
    II. Suchen Sie den „Fingerabdruck“ des SchuhfriedSelfSignedCertificate oder Ihr eigenes Zertifikat



III. Kopieren Sie den Wert des Fingerabdrucks (entfernen Sie Leerzeichen, sofern vorhanden)
7ffd45b2302b3c17fc47e74cfed80288fb25569c

IV. Öffnen Sie die Windows-Eingabeaufforderung (cmd.exe) mit Administrator-Rechten

V. Befehl für Bindung vorbereiten (ändern Sie **SERVICEPORT** und **THUMBPRINT**)
netsh http add sslcert ipport=0.0.0.0:SERVICEPORT certhash=THUMBPRINT appid={f1a6cd02-6d60-4bea-822b-5f55cfac45a9}

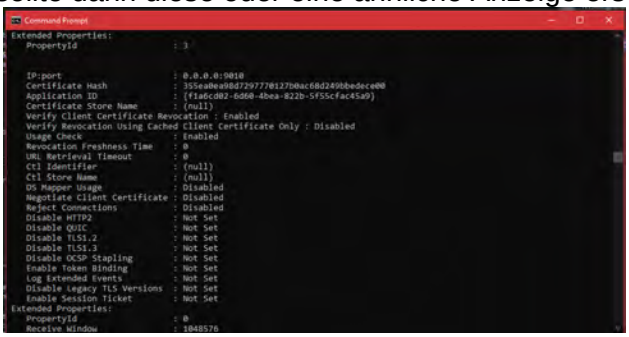
VI. Der Befehl sollte wie unten aussehen – führen Sie ihn in der Windows-Eingabeaufforderung aus
netsh http add sslcert ipport=0.0.0.0:9010 certhash=7ffd45b2302b3c17fc47e74cfed80288fb25569c appid={f1a6cd02-6d60-4bea-822b-5f55cfac45a9}
Hinweis: Wenn Sie VIS aus einer Version aktualisieren, die bereits HTTPS verwendet, müssen Sie die SSL-Zertifikatzuordnung durch entfernen, indem Sie den folgenden Befehl ausführen:
netsh http delete sslcert ipport=0.0.0.0:9010

VII. Wenn die Bindung erfolgreich war, sollte „SSL-Zertifikat erfolgreich installiert“ oder ähnliches angezeigt werden.

VIII. Führen Sie diesen Befehl aus, um das zu verifizierende Zertifikat zu installieren.

IX. “netsh http show sslcert”

X. Es sollte dann diese oder eine ähnliche Anzeige erscheinen:



o Starten Sie das WTS Integration Service neu

3.9.5 Konfiguration des VIS Universal Plugin über eine verschlüsselte Verbindung (HTTP)

Standardmäßig wird das VIS über das Setup für HTTPS installiert. Das vorige Kapitel enthält Anweisungen zur richtigen Verknüpfung des vom VIS verwendeten Ports mit dem entsprechenden HTTPS-Zertifikat. Wenn aus irgendeinem Grund HTTP verwendet werden muss (z. B. aufgrund der Migration von einer früheren WTS-Version), müssen die folgenden Schritte durchgeführt werden, um sicherzustellen, dass das VIS nach der Aktualisierung weiterhin ordnungsgemäß über HTTP kommuniziert:

- Anhalten des WTS Integration Service (nur wenn dieser läuft)
- In "Installationspfad"\Vienna Test System 8\Service\Plugin\WTS.Integration.Plugins.Universal.UniversalPlugin.dll.config den Knoten "service" mit dem Kommentar "HTTPS configuration, primary use" auskommentieren und den Knoten "service" mit dem Kommentar "HTTP configuration, legacy use" auskommentieren

```
<services>
    <!--HTTPS configuration, primary use-->
    <!--<service behaviorConfiguration="HttpsBehaviour"
             name="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.UniversalPluginService">-->
        <!--MEX Endpoint for enabling client creation-->
        <!--<endpoint address="mex" binding="mexHttpsBinding" bindingConfiguration=""
          name="MetadataEndpoint" contract="IMetadataExchange" />-->

        <!--<endpoint address="Universal" binding="basicHttpsBinding"
                  bindingConfiguration="basicHttpsBindingConfig" name="Standard"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginService" />
        <endpoint address="UniversalSpecialCase" binding="basicHttpsBinding"
                  bindingConfiguration="basicHttpsBindingConfig" name="Special"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginSpecialCaseService" />

        <endpoint address="UniversalServiceStreamed" binding="basicHttpsBinding"
                  bindingConfiguration="basicHttpsBindingConfigStreamed"
                  name="Streamed"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginServiceStreamed" />

        <host>
            <baseAddresses>-->
                <!--<add baseAddress="https://{some_domain}:9010" />-->
            <!--</baseAddresses>
        </host>
    </service>-->

    <!--HTTP configuration, legacy use-->
    <service behaviorConfiguration="HttpBehaviour"
             name="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.UniversalPluginService">

        <!--MEX Endpoint for enabling client creation-->
        <endpoint address="mex" binding="mexHttpBinding" bindingConfiguration=""
                  name="MetadataEndpoint" contract="IMetadataExchange" />

        <endpoint address="UniversalService" binding="wsHttpBinding"
                  bindingConfiguration="WSHttpBinding" name="Standard"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginService" />
        <endpoint address="UniversalServiceSpecialCase" binding="wsHttpBinding"
                  bindingConfiguration="WSHttpBinding" name="Special"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginSpecialCaseService" />

        <endpoint address="UniversalServiceStreamed" binding="basicHttpBinding"
                  bindingConfiguration="basicHttpBindingConfigStreamed"
                  name="Streamed"
                  contract="WTS.Integration.Plugins.Universal.UniversalPlugin.Service.IUniversalPluginServiceStreamed" />

        <host>
            <baseAddresses>
                <add baseAddress="http://localhost:9010" />
            </baseAddresses>
        </host>
    </service>
```

- Starten Sie den WTS Integration Service

3.10 Manuelle Anpassungen am System nach der Installation

3.10.1 Änderung des Maschinennamens nach der Installation

Falls kein vollwertiges SSL-Zertifikat verwendet wird, sollte die Änderung des Maschinennamen bei schon einem bereits installiertem Wiener Testsystem unbedingt vermieden werden, da das selbstsignierte, mitgelieferte SSL-Zertifikat auf den Maschinennamen gebunden ist und, nach der Änderung, daher die Kommunikation der jeweiligen Komponenten nicht mehr richtig konfiguriert ist.
Falls es doch noch dazu kommt, sollten folgende Schritte ausgeführt werden:

1. Wiener Testsystem deinstallieren (die Datenbank wird dabei nicht gelöscht)
2. Sicher gehen, dass das Zertifikat „SchuhfriedSelfSignedCertificate“ gelöscht ist:
    a. Öffnen Sie das „Zertifikat Management“ (Führen Sie „certlm.msc“ am lokalen Rechner aus)
    b. Gehen Sie zu “Eigene Zertifikate”->”Zertifikate”
    c. Rechtsklick auf „SchuhfriedSelfSignedCertificate“ und Löschen auswählen
3. Wiener Testsystem erneut installieren (dabei wird die vorhandene Datenbank erkannt und verwendet)
4. Anpassungen in der WTS Datenbank mittel SQL Skript um die neuen Rechnernamen zu übernehmen (update_identityserverconfiguration.sql; gespeichert im Ordner "Scripts\Help").

Wichtig ist, dass dafür die gleiche Version vom Wiener Testsystem für die De-Installation und erneute Installation verwendet wird.

3.10.2 Änderung der Bit.ly Konfiguration

Für den Versand der Testlinks verwendet das WTS System das externe Tool „Bitly“. Folgende Änderungen können an der Konfiguration vorgenommen werden:

1. **IsBitlyEnabled**
   Durch diesen Schlüssel kann die Verwendung des Bitly Dienstes Ein/Aus geschalten werden. Gültige Werte sind „true“ und „false“.
   Hier ein Beispiel:

   ```
   <add key="IsBitlyEnabled" value="false"></add>
   ```

2. **BitlyAccessToken**
   Durch diesen Schlüssel kann das Default Token des Systems überschrieben werden. Es kann beispielsweise ein eigener Bitly Account verwendet werden.
   Hier ein Beispiel:

   ```
   <add key="BitlyAccessToken" value="123456789abcdefghijk"></add>
   ```

3.11 Hinweise zur Datenbanksicherung und Wiederherstellung

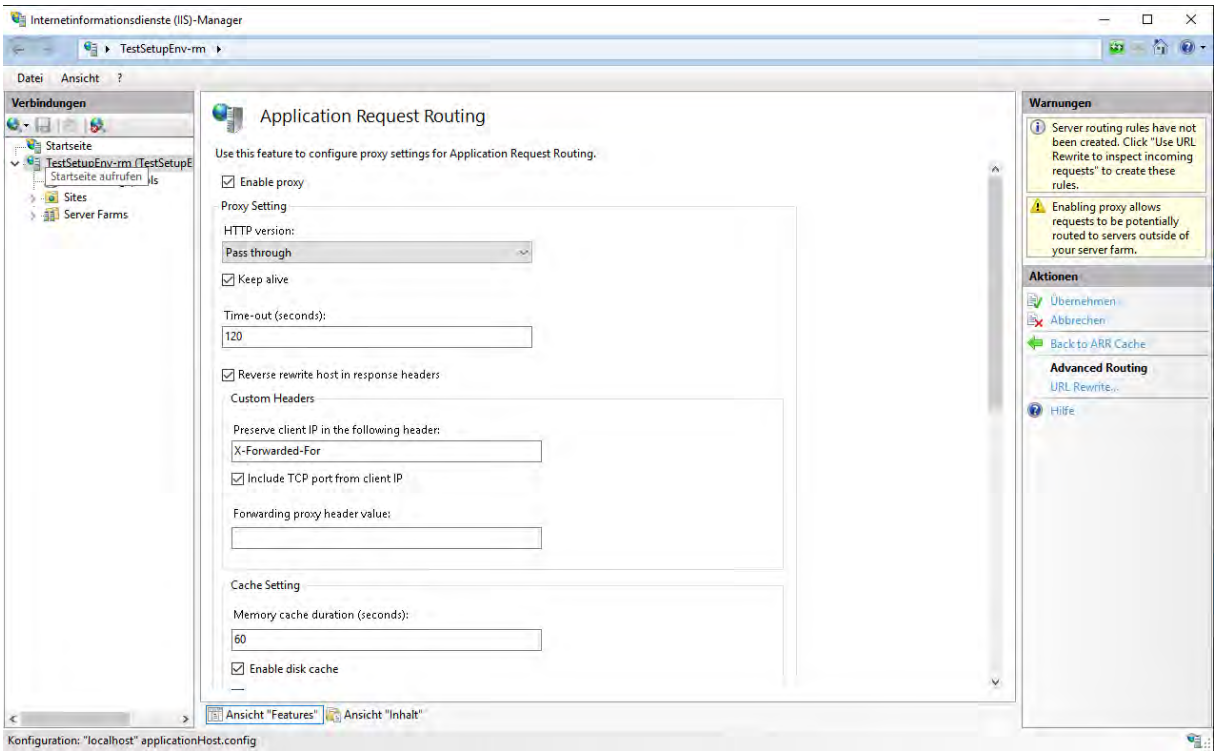
Sollten das WTS System auf einem anderen Rechner wiederhergestellt werden ist es notwendig, die Datenbank mithilfe eines SQL Skripts (update_identityserverconfiguration.sql) zu konfigurieren.

3.12 Einrichten von TestPlayer Web mit einem Reverse-Proxy über IIS

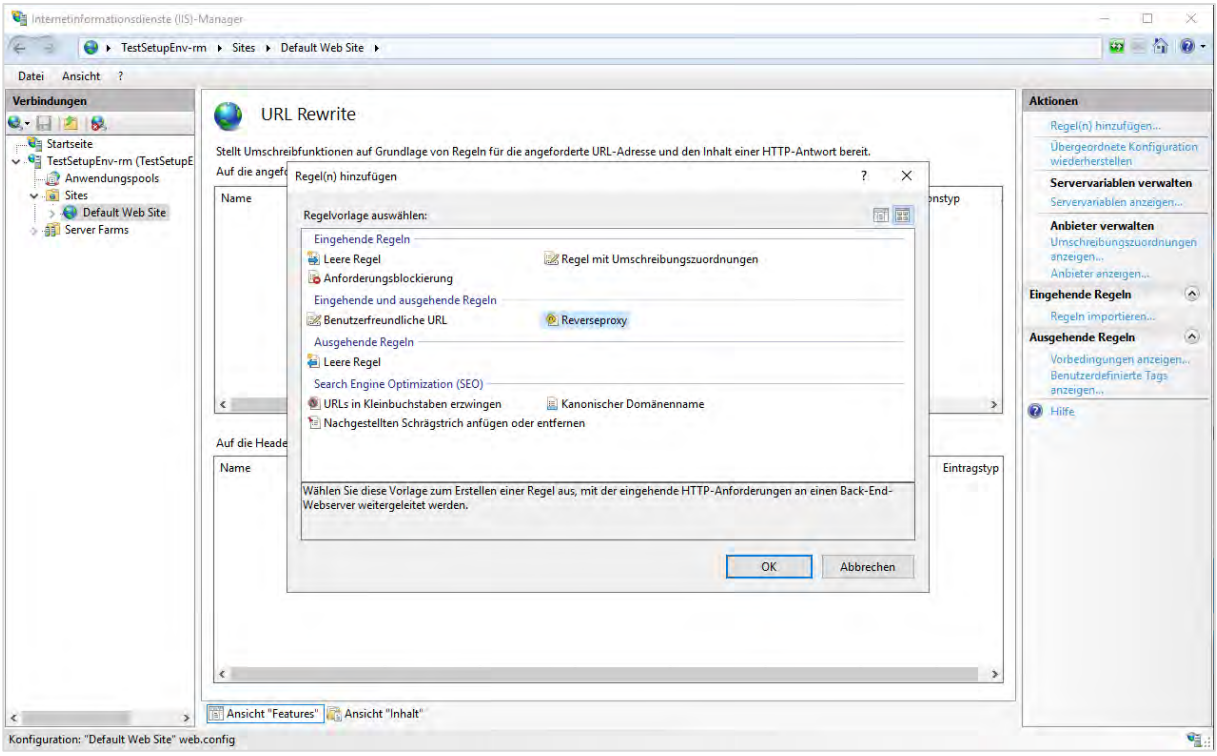
Testplayer Web wird in Kestrel gehostet. Es werden jedoch manchmal zusätzliche Konfigurationsoptionen benötigt, die Kestrel nicht bietet (z. B. Port Sharing). In diesem Fall kann über Internet Information Services (IIS) ein Reverse Proxy konfiguriert werden.

Dazu sind die folgenden Schritte erforderlich:

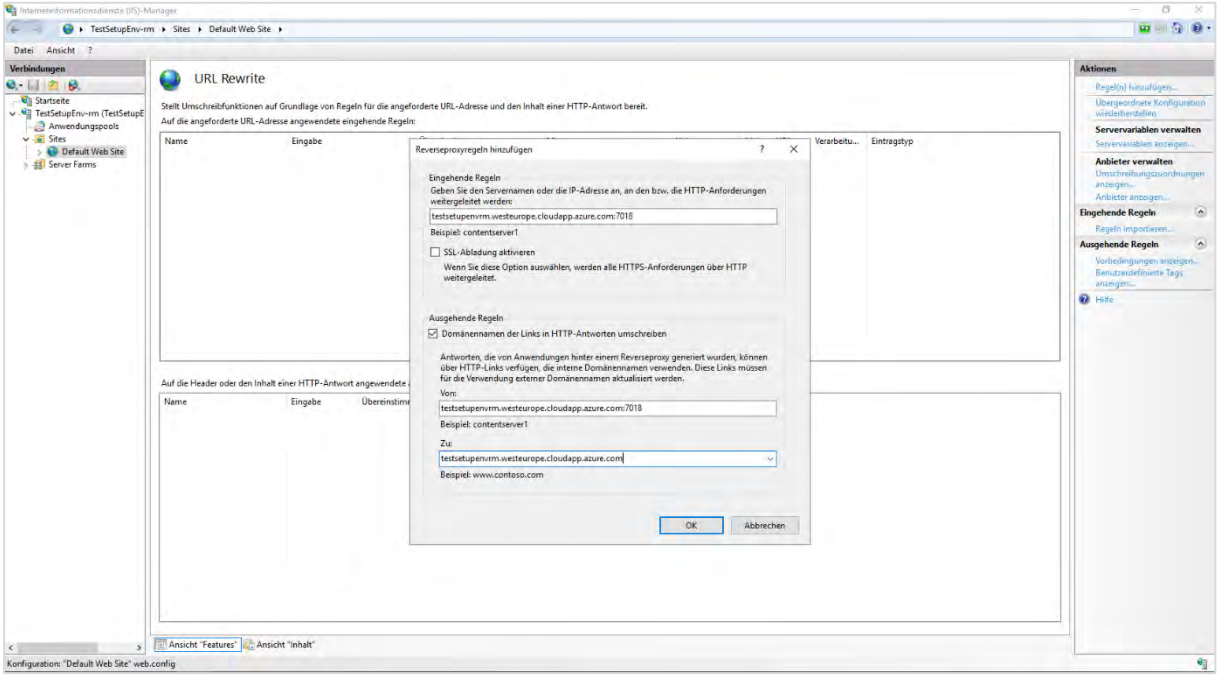
1. Laden Sie IIS Module URL Rewrite herunter and installieren Sie es mit den Standardeinstellungen (https://iis-umbraco.azurewebsites.net/downloads/microsoft/url-rewrite)
2. Laden Sie IIS Module Application Request Routing (ARR) herunter and installieren Sie es mit den Standardeinstellungen (https://iis-umbraco.azurewebsites.net/downloads/microsoft/application-request-routing)
3. Starten Sie IIS und gehen Sie auf „Application Request Routing“, aktivieren Sie dann „Enable proxy“ und klicken Sie auf „Übernehmen“



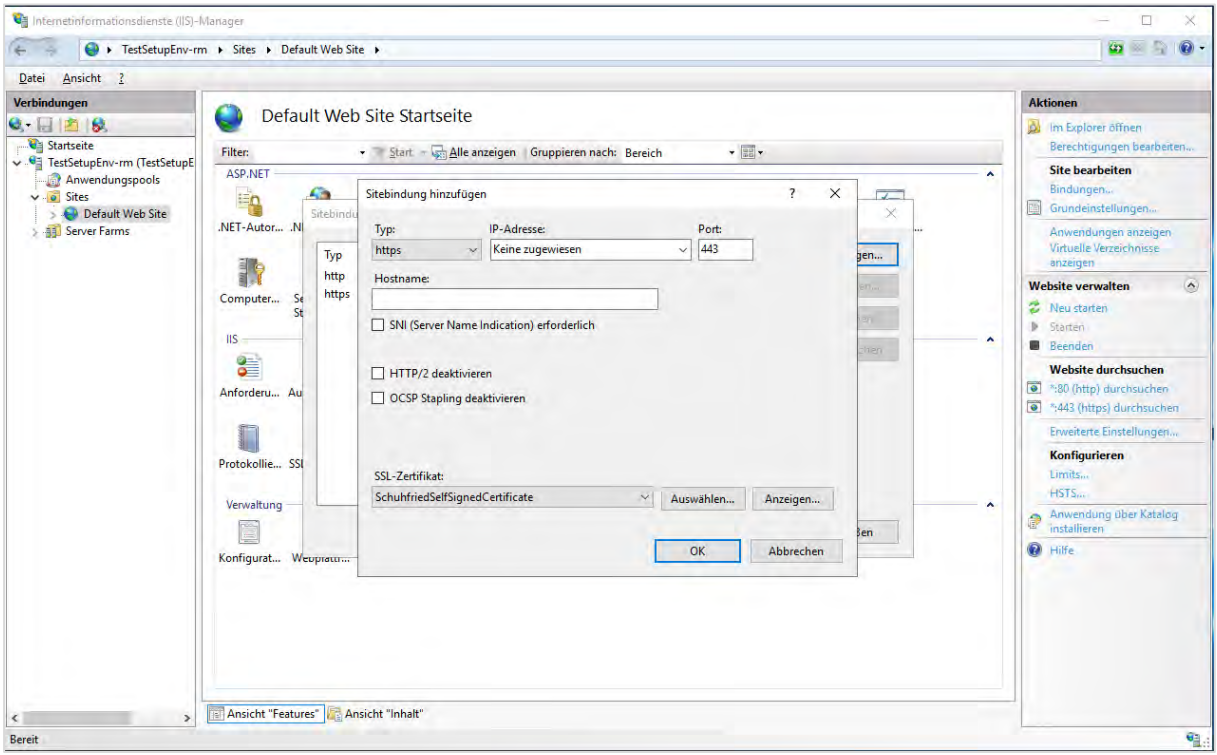
4. Gehen Sie auf eine Website (entweder eine Standard-Website oder erstellen Sie eine neue) und klicken Sie auf „URL Rewrite“
5. Konfigurieren Sie eine neue Reverse-Proxy-Regel
    a. „Regel(n) hinzufügen“...
    b. Wählen Sie „Reverseproxy“ aus



    c. Geben Sie unter „Eingehende Regeln“ „{domain}:7018“ ein, wobei „domain“ für die Domäne steht, unter der TestPlayer Web in Kestrel gehostet wird
    d. Deaktivieren Sie „SSL-Abladung aktivieren“
    e. Aktivieren Sie „Domänennamen der Links in HTTP-Antworten umschreiben“ und legen Sie unter „Zu“ die Domäne fest. Klicken Sie auf „OK“.

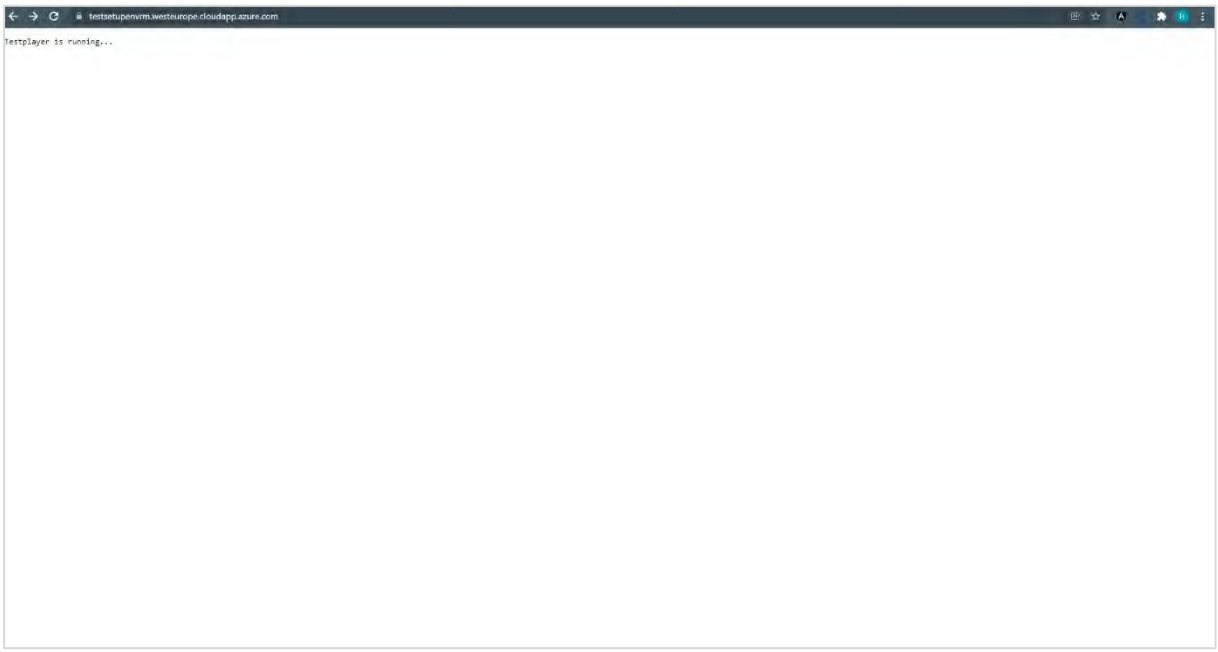


6. Klicken Sie mit der rechten Maustaste auf die Website, wählen Sie „Sitebindungen bearbeiten“ und fügen Sie, falls noch nicht vorhanden, eine Bindung für HTTPS hinzu. Bei „SSL-Zertifikat“ können Sie das vom Setup installierte Zertifikat auswählen Ihr eigenes für die konfigurierte Domäne ausgestelltes Zertifikat verwenden. Klicken Sie auf „OK“.



7. Wenn der TestPlayer Web nicht auf demselben Rechner installiert ist, auf dem der IIS-Reverse-Proxy konfiguriert ist, muss der „Grenzwert für den Antwortpuffer (KB)“ (Application Request Routing Cache -> Server Proxy Settings) möglicherweise erhöht werden. Sie erkennen dies, wenn bei der Testdurchführung eine weiße Seite angezeigt wird. Wir empfehlen, diesen Wert auf 2048 zu erhöhen. Je nach verwendetem Test kann dieser Wert jedoch höher sein.

Wenn alles richtig konfiguriert wurde, sollten Sie folgenden Inhalt sehen, wenn Sie zu der konfigurierten Domäne navigieren:



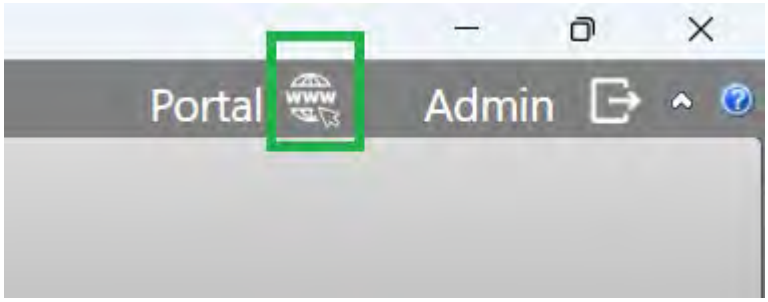
Hinweis: Damit der Reverse Proxy richtig konfiguriert werden kann, darf die hinzugefügte Website kein virtuelles Verzeichnis enthalten.

3.13 Web-Portal

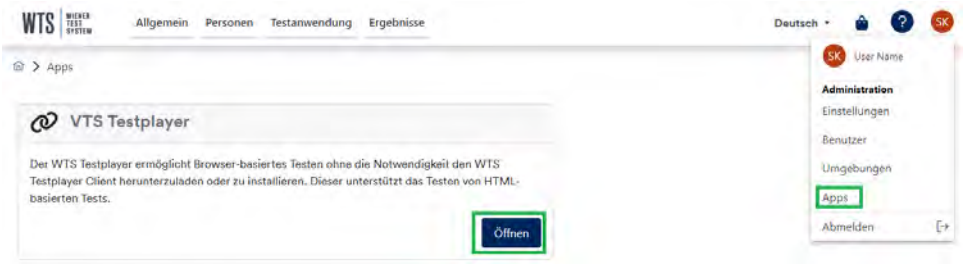
Das Portal ist eine neue, in das WTS integrierte webbasierte Benutzeroberfläche, die über Webbrowser zugänglich ist. Dabei ist es wichtig zu wissen, dass das Portal keine Verbindung zum Internet herstellt oder Daten nach außen überträgt. Es ist jedoch mit Ihrem installierten WTS verknüpft, so dass eine nahtlose Interaktion und Funktionalität zwischen beiden gewährleistet ist.

Gehen Sie bitte wie folgt vor, um auf das Portal zuzugreifen:

1. Öffnen Sie den Wiener Testsystem Client.
2. In der oberen linken Ecke befindet sich neben dem Wort „Portal“ ein Weltkugel-Icon.
3. Wenn Sie auf das Icon klicken, werden Sie automatisch zu einem Internetbrowser mit der Portal-URL weitergeleitet.
4. Sie werden aufgefordert, sich mit Ihrem Benutzernamen und Passwort anzumelden.



Darüber hinaus kann der browserbasierte Testplayer aufgerufen werden, indem Sie im Portal zum Bereich „Apps“ navigieren und den Bereich „WTS Testplayer“ von dort öffnen.



4 BESCHREIBUNG DER PERIPHERIEGERÄTE

4.1 Testsystem Dongle

4.1.1 Lieferumfang

- 1 Stk. Testsystem Dongle
- 1 Set Aufkleber in den Farben rot, grün, gelb und schwarz
  (in Verbindung mit einer Probandentastatur nicht im Lieferumfang enthalten)

ACHTUNG !
Ihr Testsystem Dongle beinhaltet die Lizenzen für Ihre gesamte Wiener Testsystem Software.

Wenn Sie über keine Probandentastatur verfügen, die rote, grüne, gelbe und schwarze Taste jedoch bei Tests benötigt wird, kann diese durch die Computertastatur ersetzt werden:

Rote Taste:	Linke Strg Strg - oder Alt Alt - oder Umschalt ⇧ - Taste
Grüne Taste:	Rechte Strg Strg - oder Alt Alt - oder Umschalt ⇧ - Taste
Gelbe Taste:	Backspace- (Zurück-) Taste ←
Schwarze Taste:	Leertaste Space

Da manche Tastaturen, besonders bei Laptop-Computern, eine ungünstige Tastenanordnung haben, stehen die oben genannten Alternativen zur Verfügung. Wählen Sie jeweils jene Tasten aus, die am günstigsten platziert sind, und markieren Sie diese mit den mitgelieferten farbigen Aufklebern.

4.1.2 Spezifikationen

Spannungsversorgung	5V über das USB-Kabel
Stromverbrauch	max. 30mA
max. Abmessungen (B/H/T)	15 x 8 x 75mm
Gewicht (ohne Zubehör)	9,5g
Lagertemperatur	-20 to 60°C
Betriebstemperatur	10 to 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.2 Die Probandentastaturen

4.2.1 Lieferumfang

1 Stk. Probandentastatur, advanced (Ag) oder universal (Ug)
2 Stk. Joystick-Knüppel (nur bei Probandentastatur Ug)
2 Stk. Joystickschablonen (nur bei Probandentastatur Ug)

Probandentastatur Advanced

- 7 Farbtasten, 10 Zifferntasten, 1 Sensortaste
- 2 Drehregler
- Anschlussmöglichkeiten für Fußtasten
- Anschlussmöglichkeiten für Fußpedale - analog
- Tongenerator (Lautsprecher)
- Anschlussmöglichkeit für Kopfhörer und Mikrofon (Klinkenstecker)

Probandentastatur Universal

- 7 Farbtasten, 10 Zifferntasten, 1 Sensortaste
- 2 Drehregler
- 2 analoge Joysticks
- 2 Joystickschablonen
- Anschlussmöglichkeiten für Fußtasten
- Anschlussmöglichkeiten für Fußpedale - analog
- Tongenerator (Lautsprecher)
- Anschlussmöglichkeit für Kopfhörer und Mikrofon (Klinkenstecker)

4.2.2 Inbetriebnahme

Schließen Sie die Probandentastur über das mitgelieferte USB-Kabel an dem Computer an, auf dem das Wiener Testsystem installiert ist und verwendet werden soll. Verbinden Sie das USB-Kabel mit der USB-B Buchse an der Rückseite der Probandentastatur und das andere Ende mit einem freien Steckplatz (USB-A Buchse) an Ihrem Computer.

In Abbildung 8 sind die Anschlussmöglichkeiten der Probandentastatur zu sehen.

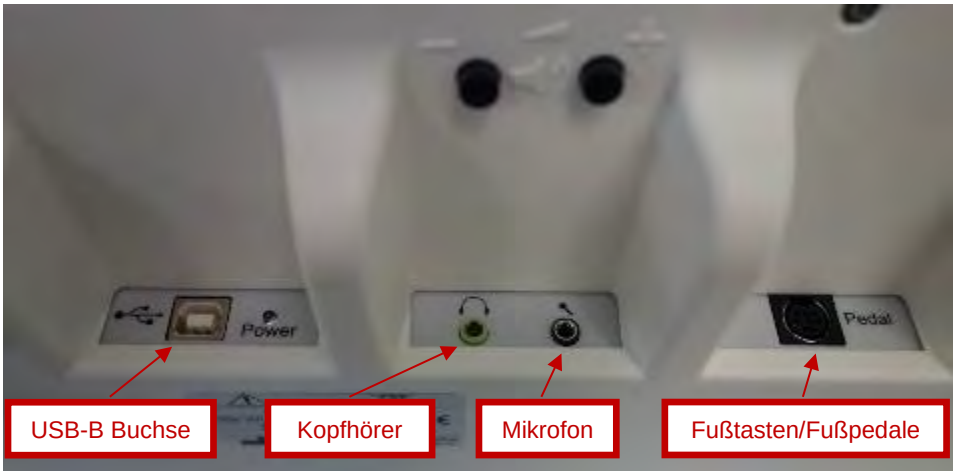


Abbildung 8: Anschlussmöglichkeiten Probandentastatur

4.2.3 Joystickschablonen

Die Joystickschablone wird wie dargestellt (siehe Abbildung 9) auf die Probandentastatur Ug gesteckt. Zur einfacheren Montage kann der Joystick-Knüppel abgezogen werden.

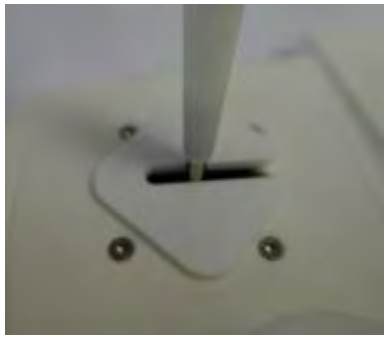


Abbildung 9: Auf Probandentastatur angebrachte Joystickschablone

Joystickschablonen werden bei einigen Tests zur Begrenzung der Joystick-Freiheitsgrade auf eine Richtung verwendet. In den Instruktionen dieser Tests werden folgende Symbole verwendet (siehe Abbildung 10).

Abbildung 10: Joystickschablone Symbole

4.2.4 Ton Ein- und Ausgabe

Die Tonausgabe im Wiener Testsystem erfolgt wahlweise durch den internen Lautsprecher oder über ein Headset (als Zubehör erhältlich). Das Headset kann über je einen 3,5mm Klinkenstecker für Kopfhörer und Mikrofon an der Probandentastatur angeschlossen werden. Die Buchsen für den Anschluss des Headsets sind mit einem Kopfhörer und einem Mikrofon –Symbol markiert. Falls ein USB-Head-Set verwendet werden soll, so schließen Sie dieses an einem freien USB-Steckplatz am Computer an. Bei angestecktem Headset ist der interne Lautsprecher der Probandentastatur abgeschaltet.
Die Lautstärke kann mit dem Tasten (+) und (-) auf der Rückseite der Probandentastatur eingestellt, aber nicht auf null abgeregelt werden.

4.2.5 Fußtasten und Fußpedale

Der Anschluss von Fußtasten oder Fußpedalen (als Zubehör erhältlich) erfolgt über eine einzige Anschlussbuchse. Die Buchse ist mit der Aufschrift „Pedal“ gekennzeichnet. Schließen Sie je nach Bedarf die Fußtasten oder die Fußpedale an.

4.2.6 Spezifikationen

Spannungsversorgung	+5V DC über das USB-Kabel
Stromverbrauch	max. 500mA
Schutzklasse	
Gerätetyp	B
max. USB-Kabellänge	3m
max. Headset-Kabellänge	3m
max. Abmessungen (B/H/T)	495 x 50 x 230mm
Gewicht (ohne Zubehör)	1,495kg
Lagertemperatur	-20 bis 60°C
Betriebstemperatur	10 bis 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.3 Fußtasten

Die Fußtasten werden an der Rückseite einer Probandentastatur angeschlossen.
(siehe Abbildung 8).

4.3.1 Lieferumfang

- 1 Paar-Fußtasten (links & rechts)

4.3.2 Spezifikationen

max. Abmessungen (B/H/T)	je 160 x 55 x 310mm
Gewicht (ohne Zubehör)	1,55kg
Lagertemperatur	-20 bis 60°C
Betriebstemperatur	10 bis 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.4 Fußpedale – Analog

Die Fußpedale – Analog werden an die Probandentastatur Universal angeschlossen (siehe Abbildung 8).

4.4.1 Lieferumfang

- 1 Paar-Fußpedale – Analog (links & rechts)

4.4.2 Spezifikationen

max. Abmessungen (B/H/T)	je 80 x 60 x 200mm
Gewicht (ohne Zubehör)	0,85kg
Lagertemperatur	-20 bis 60°C
Betriebstemperatur	10 bis 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.5 MLS-Arbeitsplatte

4.5.1 Lieferumfang

Pos.	Stk.	Bezeichnung
1	1	MLS-Arbeitsplatte
2	2	Griffel (rot = links, schwarz = rechts)
3	2	Griffelhalterung
4	2	Stifthalter mit je 25 Stiften kurz
5	2	Stifthalter mit je 25 Stiften lang

Die MLS-Arbeitsplatte verfügt über

- Bohrungen unterschiedlichen Durchmessers.
- Eine mehrfach gekrümmte, ausgefräste Linie.
- Zweimal 20 Kontaktpunkte.
- Links und rechts jeweils 25 kleine Bohrungen.
- 2 Tapping Zielflächen.

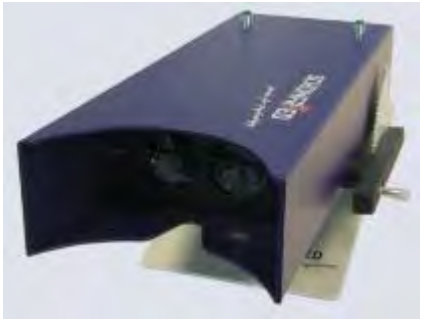
4.5.2 Spezifikationen

Spannungsversorgung	5V über das USB-Kabel
Stromverbrauch	max. 500mA
Schutzklasse	⧈
Gerätetyp	B
max. Abmessungen (B/H/T)	310 x 50 x 300mm
Gewicht (ohne Zubehör)	5,4kg
Lagertemperatur	-20 bis 60°C
Betriebstemperatur	10 bis 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.6 Flimmer-Tubus

4.6.1 Lieferumfang

- 1 Stk. Flimmer-Tubus



Reizlichtquelle:
Rote, diffuse Leuchtdiode mit einer Wellenlänge von 655 nm und einer Lichtintensität von 5,4 mcd.
Die abgegebenen Lichtimpulse sind Rechteckimpulse, die in Schritten von 0.1 Hertz in einem Bereich von 10.0 bis 100.0 Hertz mit einem Tastverhältnis von 50% einstellbar sind.

Umfeld (Hintergrundbeleuchtung):
Das Umfeld mit einer Lichtintensität von 600mcd hat einen Durchmesser von 30mm.

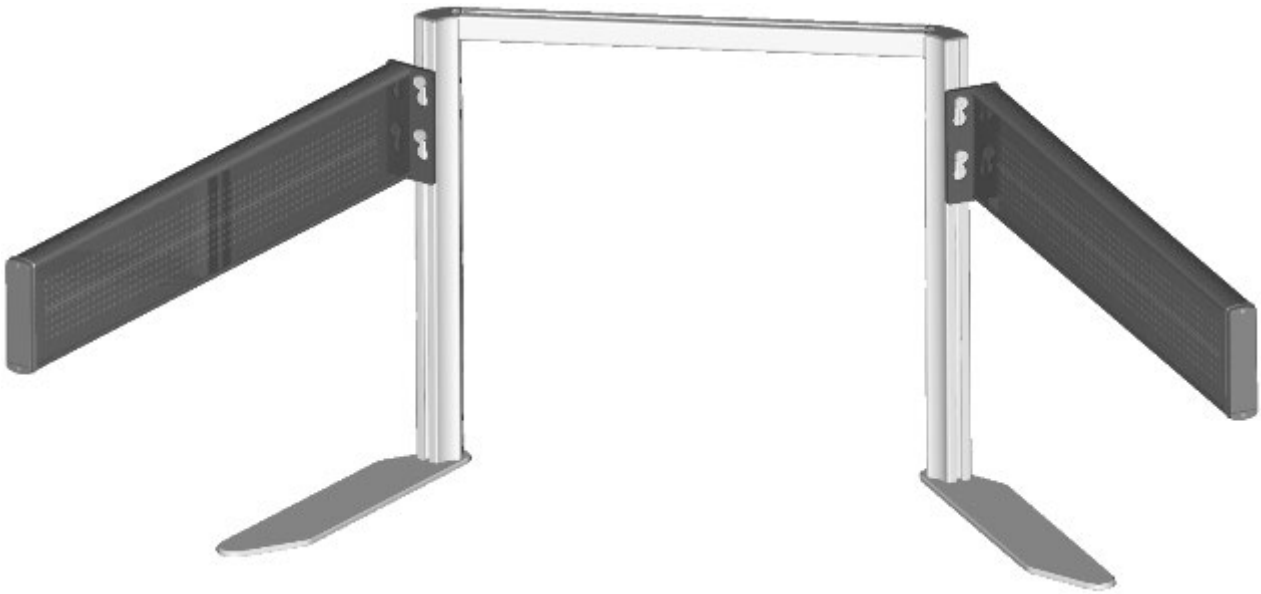
Tubus – das optische System:
2 Sammellinsen (konkavkonvex) mit 250mm Brennweite erzeugen ein virtuelles Bild der Lichtquelle in einer Entfernung von 12m.
Sehwinkel für Lichtquelle: 1,2°
Sehwinkel für Umfeld: 10°

4.6.2 SPEZIFIKATION

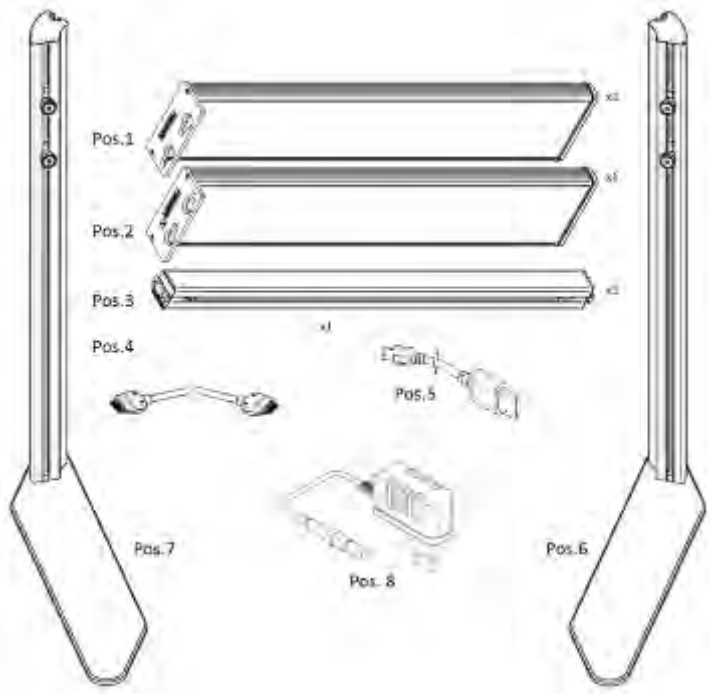
Spannungsversorgung	5V über das USB-Kabel
Stromverbrauch	max. 500mA
Schutzklasse	⧈
Gerätetyp	B
Max. Abmessungen (B/H/T)	160 x 100 x 400mm
Gewicht (ohne Zubehör)	1,8kg
Lagertemperatur	-20 to 60°C
Betriebstemperatur	10 to 30°C
Relative Luftfeuchtigkeit	max. 70%, nicht kondensierend

4.7 Periphere Wahrnehmung 2 (PP-HW2)

4.7.1 Lieferumfang

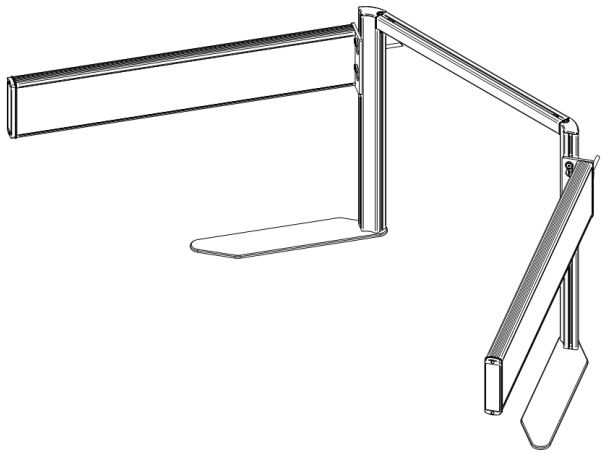


Pos.	Stk.	Bezeichnung
1	1	Linkes Anzeigeelement
2	1	Rechtes Anzeigeelement
3	1	Querbalken
4	1	Verbindungskabel 20pol./1m
5	1	Verbindungskabel USB/3m
6	1	Rechter Standfuß
7	1	Linker Standfuß
8	1	Schaltnetzteil 5V/4A

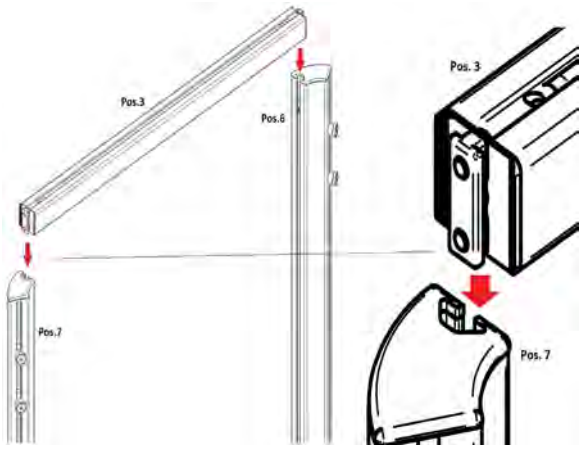


4.7.2 Mechanischer Zusammenbau

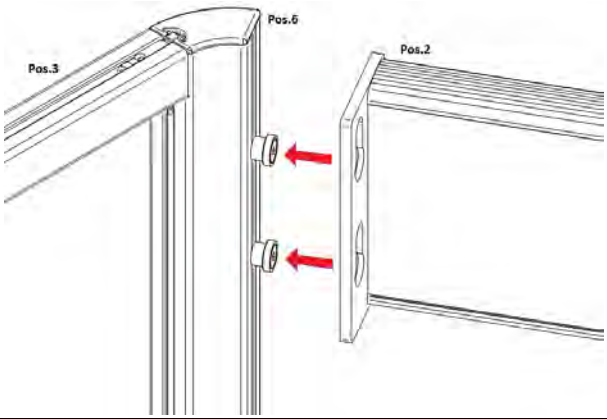
Ziel



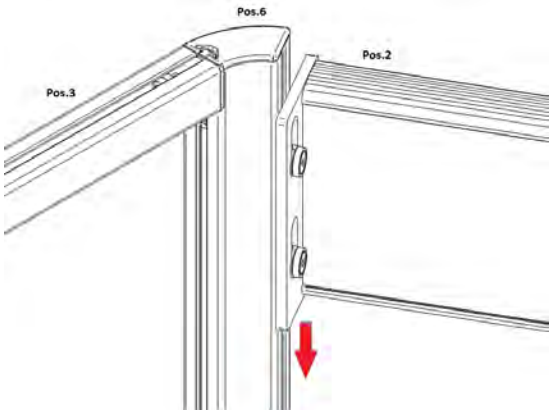
1. Querbalken mit Standfüßen verbinden



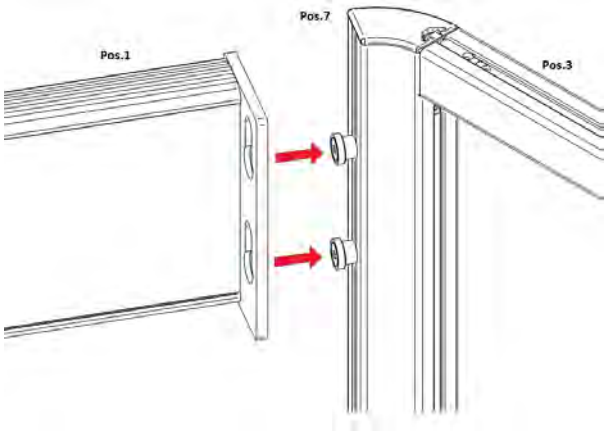
2. Anzeigeelement rechts einhängen



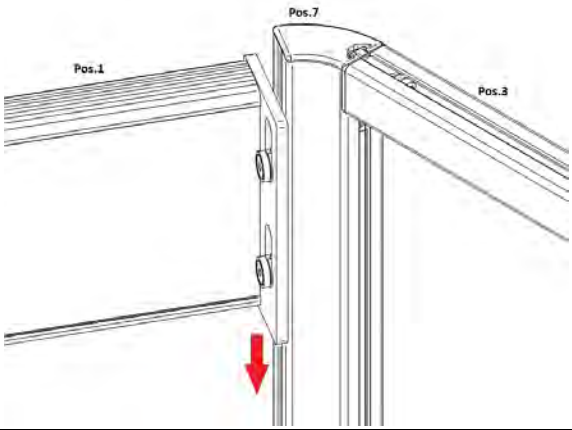
3. Anzeigeelement rechts einrasten



4. Anzeigeelement links einhängen

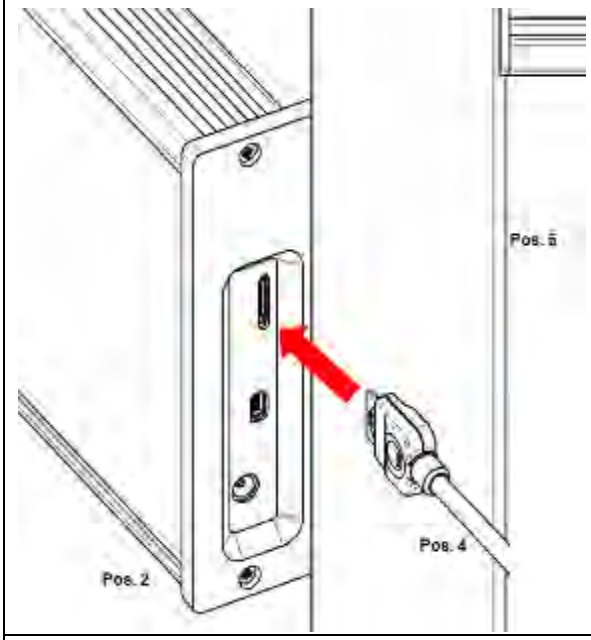


5. Anzeigeelement links einrasten

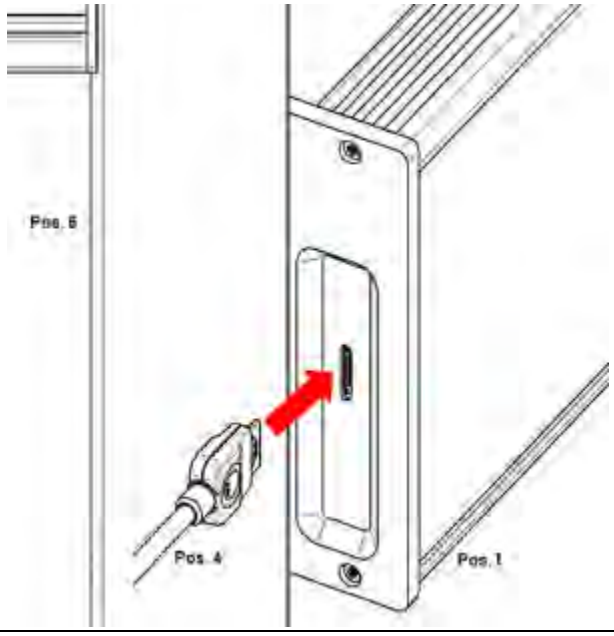


4.7.3 Verkabelung

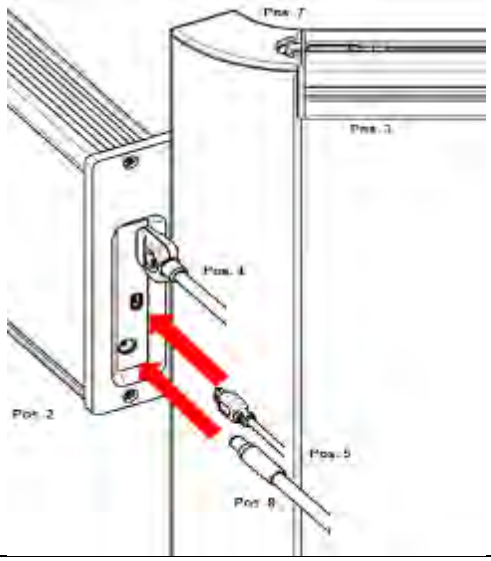
1. Anzeigeelement rechts verkabeln



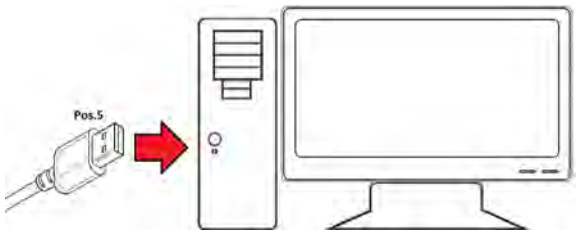
2. Anzeigeelement links verkabeln



3. USB- und Netz- Kabelverbindung



4. Anschluss an Computer über USB-Kabel



ACHTUNG:

- Das Gerät darf nur mit den im Lieferumfang enthaltenen Teilen verwendet werden!
- Es darf nur das beigelegte Schaltnetzteil von *CINCON ELECTRONICS CO. , LTD.* mit der Typenbezeichnung *TR30RAM050* verwendet werden!

Um das Gerät in Betrieb zu nehmen, ist die Verkabelung der einzelnen Komponenten notwendig. Verbinden Sie zunächst die beiden Anzeigeelemente (Pos.1 und Pos.2) mit dem dafür vorgesehenen Verbindungskabel (Pos.4). Das Verbindungskabel kann mit einem der beiden Stecker-Enden wahlweise auf dem linken, oder rechten Anzeigeelement angesteckt werden. Siehe hierfür Schritt 1 und Schritt 2.
Verbinden Sie anschließend das USB-Verbindungskabel (Pos.5) mit dem rechten Anzeigeelement (Pos.2) und dem Computer (Schritt 3 und Schritt 4).

Die Stromversorgung erfolgt über das mitgelieferte Schaltnetzteil (Pos.8), welches ebenfalls mit dem rechten Anzeigeelement (Pos.2) verbunden wird (Schritt 3). Das Schaltnetzteil (Pos.8) muss zudem an eine Netzsteckdose angeschlossen werden.

Um den Betrieb des Geräts zu beenden, folgen Sie bitte den Schritten der Verkabelung in umgekehrter Reihenfolge.

Platzieren Sie den für den Probanden vorgesehenen Monitor im Freiraum zwischen den Anzeigeelementen der Peripheren Wahrnehmung so, dass die Vorderseite mit dem Rahmen, an dem die Anzeigeelemente montiert sind, abschließt.

4.7.4 Spezifikationen

Betriebsspannung	5V / 4A
Leistung	20W
	Schutzklasse I; Gerätetype B
max. Abmessungen (BxHxT)	1450 x 560 x 800 mm
Gewicht (ohne Zubehör)	9,6kg
Lagertemperatur	-20 bis 60°C
Betriebstemperatur	10 bis 30°C
Relative Luftfeuchte	max. 70%, nicht kondensierend
Schaltnetzteil	Hersteller: CINCON Electronics Co., LTD. Modell: TR30RAM050 Output: 5V DC 4.0A

4.7.5 Anforderungen an die Testumgebung

Die Testumgebung sollte eine ungestörte Bearbeitung des Tests durch die Testperson bzw. den Probanden ermöglichen. Dies betrifft unter anderem die Störung durch optische und akustische Reize.
Die Umgebungshelligkeit darf höchstens 2500 Lux betragen, da ansonsten der Kontrast zwischen den präsentierten Reizen und der Umgebungshelligkeit zu gering ist. In diesem Fall sollte die Umgebungshelligkeit reduziert werden.
Die Umgebungshelligkeit wird dabei von der PP-R-Hardware durch einen speziellen Helligkeitssensor gemessen. Ist sie zu hoch, wird eine Testung verhindert.

4.7.6 Positionierung des Probanden

Der Proband sollte eine Sitzposition wie in Abschnitt 2 einnehmen. Dabei ist es wichtig, dass sich der Kopf des Probanden zwischen den zwei Anzeigeelementen befindet. Der Kopf sollte sich auf Höhe der weißen Markierungen in der Mitte der Sensorlatten befinden. Dies ermöglicht die Bestimmung der Kopfposition durch das Gerät.
Der **Abstand** zwischen dem Metallrahmen und dem Gesicht **muss zwischen 20 und 45** cm betragen. Dieser Abstand wird durch die PP-R-Hardware gemessen. Wird diese Bedingung nicht eingehalten, erfolgt ein Feedback durch das Wiener Testsystem.
Der seitliche Abstand zwischen Kopf und der Bildschirmmitte sollte maximal 10 cm betragen. Dieser Abstand wird ebenfalls durch die PP-R-Hardware gemessen. Wird diese Bedingung nicht eingehalten, erfolgt ein Feedback durch das Wiener Testsystem.
Die richtige (und Beispiele für falsche) Sitzposition ist in Abbildung 11 schematisch dargestellt. Um die vertikale Position der Anzeigeelemente besser anpassen zu können, gibt es zwei Positionen, an denen diese eingehängt werden können. Für größere Personen ist die obere Aufhängemöglichkeit zu verwenden, bei kleineren Positionen (oder Kindern) ist die Untere zu bevorzugen.

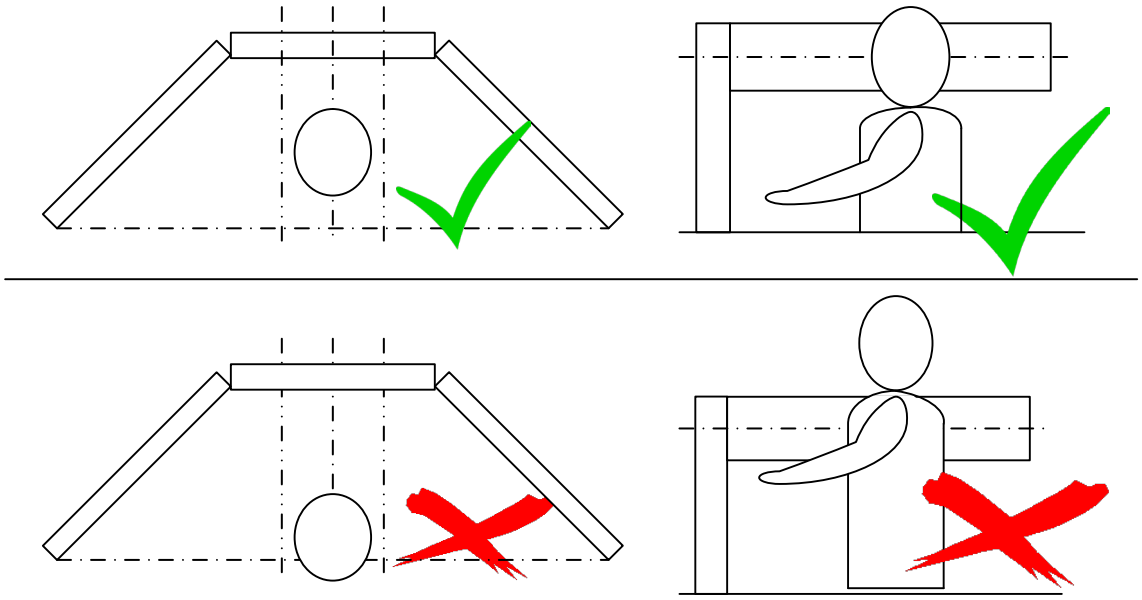


Abbildung 11: Richtige (oben) und falsche (unten) Sitzposition bei der PP-R

4.7.7 Warn- und Sicherheitshinweise

ACHTUNG: Um das RISIKO eines elektrischen Schlages zu vermeiden, darf dieses Gerät nur an ein VERSORGUNGSNETZ mit Schutzleiter angeschlossen werden.

5 HILFESTELLUNG

5.1 Hilfefunktion des Wiener Testsystems

Das Wiener Testsystem beinhaltet eine umfangreiche und kontextsensitive Hilfe. Von der Installation und Nutzung des WTS über Tipps und Tricks bis hin zu Literaturverweisen können Sie dort alle Informationen finden.

Sie können die Hilfe jederzeit im Wiener Testsystem durch anwählen der Schaltfläche aufrufen.

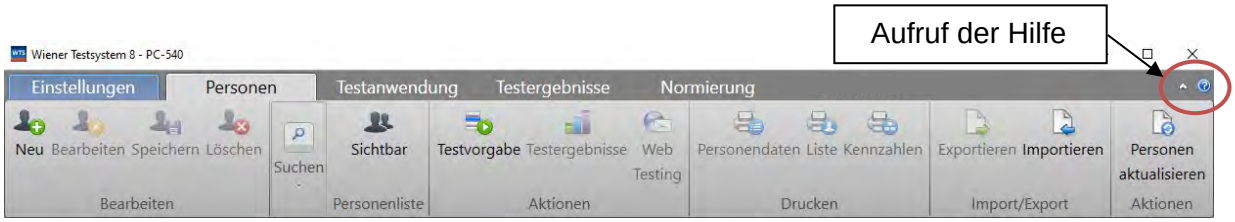


Abbildung 12 Aufruf der Hilfe

Abbildung 13 zeigt die Hilfe des Wiener Testsystems. Hier kann man nach Stichworten suchen (Lupensymbol) sowie zu den entsprechenden Abschnitten navigieren.

Abbildung 13: Hilfefenster des Wiener Testsystems

Die digitalen Testmanuale können Sie in der Lasche „Testanwendung“, mit der Schaltfläche „Manual“ für einen angewählten Test in der Sprache der Verwaltungsoberfläche öffnen (siehe Abbildung 14).

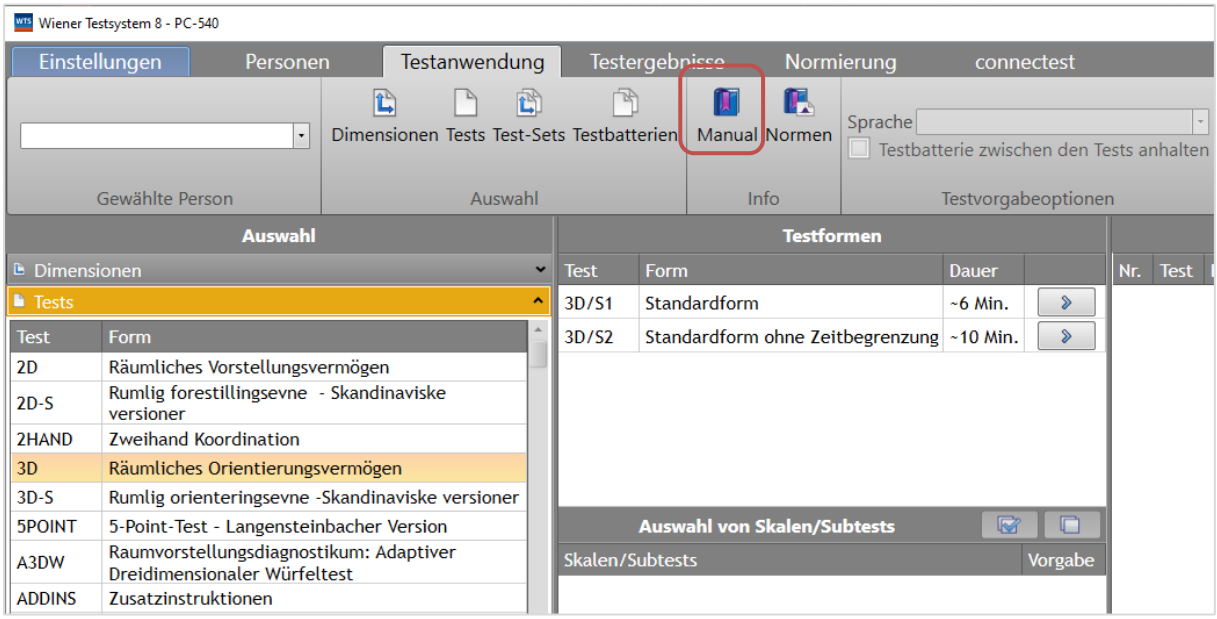


Abbildung 14: Auswahl der digitalen Testmanuale

5.2 Manuale

Manuale können auch in anderen Sprachen als der der Verwaltungsoberfläche geöffnet werden. Dazu gehen Sie zu „Einstellungen → Testverwaltung -> Durchführung“ und klicken die Schaltfläche neben „Testmanual öffnen“ (siehe Abbildung 15). Über die Drop-Down Liste bei jedem Test und der Schaltfläche „Anzeigen“ im Ribbon wird das Manual in der angewählten Sprache geöffnet werden.

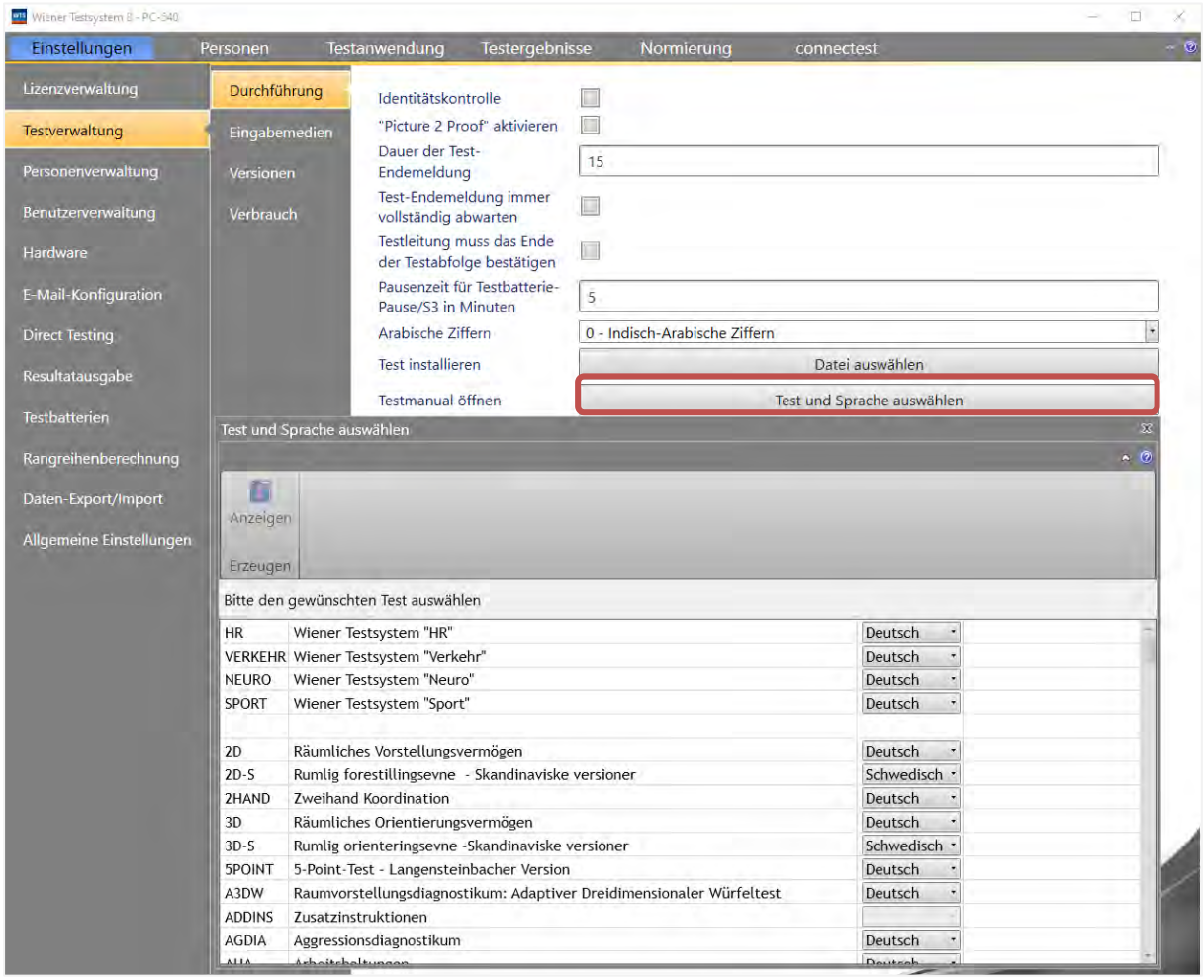


Abbildung 15: Aufruf von Testmanualen in unterschiedlichen Sprachen

Das Manual für die einzelnen Sparten (HR, Sport, Verkehr und Neuro) können in demselben Fenster aufgerufen werden.

5.3 Kundendienst

Den Begriff Kundendienst nehmen wir wörtlich. Darum bieten wir bestmöglichen Support auf allen Gebieten:

- **Support**

  Bei technischen Fragen oder Schwierigkeiten wenden Sie sich bitte an unseren HelpDesk.

- **Psychologische Fachberatung**

  Ein Team erfahrener Psychologinnen und Psychologen steht Ihnen jederzeit gern für fachliche Fragen zur Verfügung.

- **Produktinformation**

  Unsere Berater informieren Sie gern über alle unsere Produkte.

Österreich: +43 2236 42315-0
info@schuhfried.com
www.schuhfried.com/de

5.3.1 Problembehebung

Falls ein Gerät nicht funktioniert, können Sie die nachfolgenden Prozeduren zur Eingrenzung und Behebung des Fehlers durchführen:

- Gerät abstecken und wieder anstecken
- Windows neu starten
- Gerät an einem anderen USB-Anschluss anstecken (es kann sein, dass der Gerätetreiber neu zu installieren ist)
- Andere USB-Geräte abstecken
- Gerät ohne USB-HUB direkt am Computer anstecken

So können Sie die Funktion Ihrer Geräte mit dem Wiener Testsystem überprüfen:

Starten Sie Hardwaretest indem Sie unter „Einstellungen → Hardware → Hardwaretest“ die Schaltfläche klicken. Im ersten Fenster (siehe Abbildung 16) sehen Sie eine Liste aller verfügbaren Geräte.

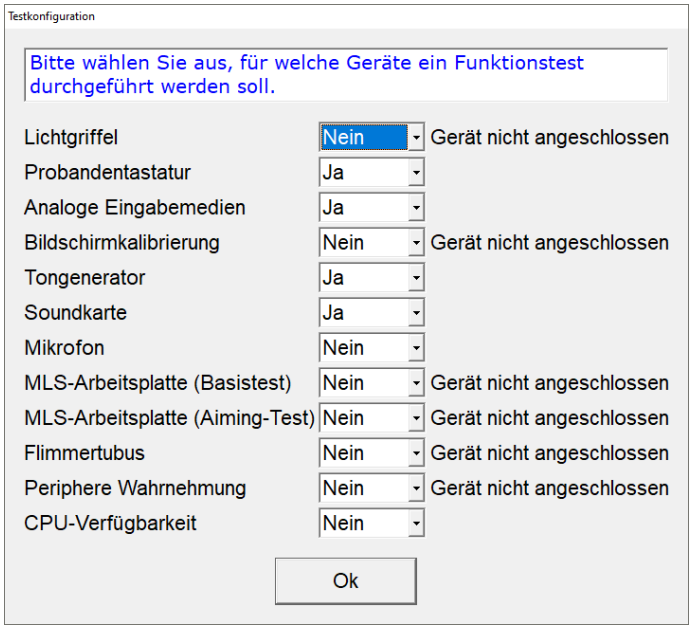


Abbildung 16: Angeschlossene Geräte im Wiener Testsystem

Ist ein Problem nicht lösbar, kontaktieren Sie bitte den Produktsupport der Firma SCHUHFRIED GmbH.

E-Mail: support@schuhfried.com
Telefon: + 43 2236 42315-360
Fax: + 43 2236 46597

5.4 Hardwaretest

Unter **Einstellungen → Hardware** können Sie die Hardwaretests beziehungsweise die Kalibrierung des Bildschirms starten:

- Für die Überprüfung eines der folgenden Geräte klicken sie auf Schaltfläche „Starten“ neben „**Hardwaretest“**:
  - Probandentastatur
  - Fußtasten
  - Fußpedale
  - MLS-Arbeitsplatte
  - Flimmer-Tubus
  - Periphere Wahrnehmung (PP-HW – mit serieller Schnittstelle und massiver Aluminium-Grundplatte)

- Für die Überprüfung der **Peripheren Wahrnehmung PP-HW2** (USB-Schnittstelle) wählen Sie „Starten“ neben „PP-R Hardwaretest“ aus

- Zur Kalibrierung der Touch-Eingabe wählen Sie die Schaltfläche „Starten“ neben „**Kalibrierung der Touch-Eingabe**“.

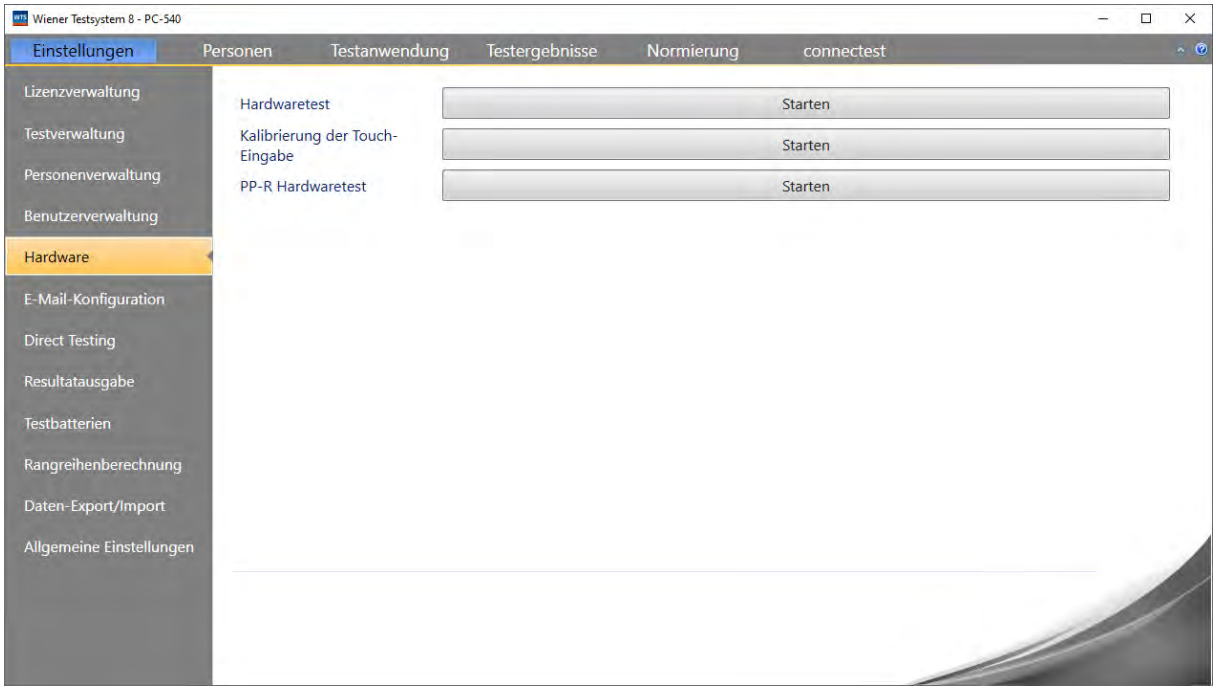


Abbildung 17: Hardwaretests

5.4.1 Hardwaretest

Verwenden Sie nach der kompletten Installation den Hardwaretest, um die Funktionstauglichkeit der Peripherie des Wiener Testsystems zu überprüfen.
In Abhängigkeit von Ihrem Qualitätsmanagementsystem wird empfohlen, den Hardwaretest Viertel- bis Halbjährlich durchzuführen, auf alle Fälle nach jeder Änderung Ihres Systems. Abschließend können Sie sich einen Bericht als Bestätigung der Durchführung ausdrucken.

Zu Beginn wird Ihnen ein Fenster angezeigt, in dem ersichtlich ist, welche Geräte angeschlossen sind. Überprüfen Sie, ob bei sämtlichen Ihrer Geräte ein „Ja“ eingetragen ist.
Nachdem Sie „Ok“ geklickt startet der Hardware-Test mit dem ersten eingetragenen Gerät. Bitte beachten Sie, dass die **Fußtasten** im Rahmen der Überprüfung der **Probandentastatur** überprüft werden, und die **Fußpedale** ein Teil der Prüfung unter **Analoge Eingabemedien** sind.

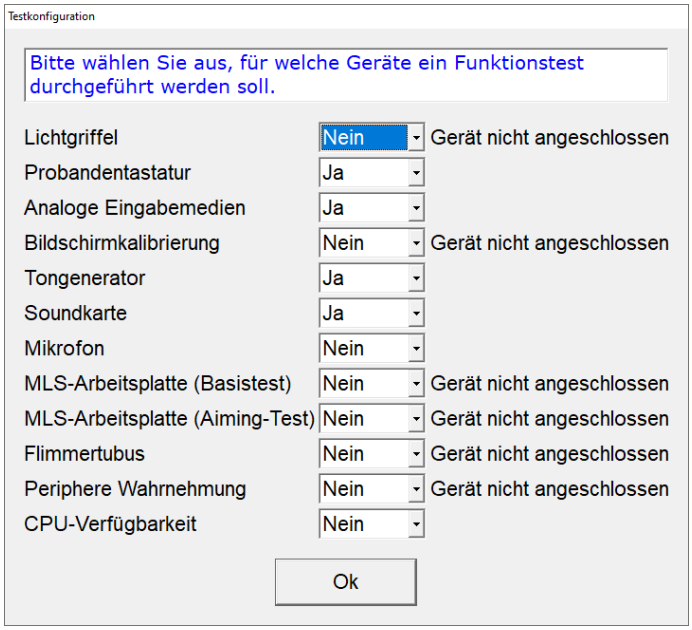
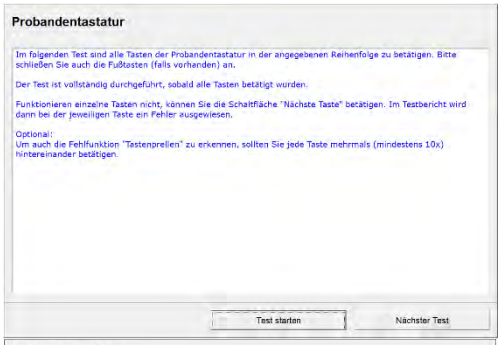


Abbildung 18: Angeschlossene Geräte im Wiener Testsystem

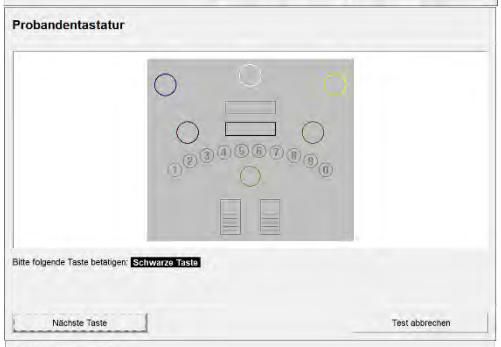
Das Programm leitet Sie bei jedem Gerät durch die Prüfung. Führen Sie sämtliche angegebenen Schritte durch.

Hardwaretest am Beispiel der Probandentastatur

1. Bei jedem Test erhalten Sie eine Einleitung, der Erläuterungen zur Testdurchführung gegeben wird.
   Klicken Sie auf „Test starten“ um die Überprüfung durchzuführen. Falls Sie den Test überspringen wollen, klicken Sie auf „Nächster Test“.



2. Sie werden aufgefordert die jeweilige Taste zu drücken. Wenn sie dies durchgeführt haben, müssen sie die nächste Taste drücken.
   Falls eine Taste nicht funktioniert, klicken Sie auf „Nächste Taste“, um den Test abzuschließen. Nicht betätigte Tasten werden im Bericht vermerkt.



3. Wenn der Test komplett durchgeführt worden ist, können Sie ihn mit „Test abschließen“ beenden.
   Der Test für die nächste Hardware-komponente (siehe Abbildung 18) wird automatisch aufgerufen.

CPU-Verfügbarkeit

Der Test der „CPU-Verfügbarkeit“ dient der Kontrolle, ob Hintergrundprozesse das Wiener Testsystem beeinflussen.
Lassen Sie die Überprüfung mindestens **5 Minuten** laufen und brechen dann mit ESC ab.
Verlängern Sie die Überprüfung, falls Unterbrechungen auftreten.

5.4.2 Kalibrierung der Touch-Eingabe

Für die Kalibrierung benötigen Sie ein Kalibrierungsmodul der Firma SCHUHFRIED. Schließen sie dieses an einen freien USB-Platz an ihrem PC oder Laptop an.
Die Kalibrierung der Touch-Eingabe ist sowohl für die Verwendung bei visuellen Reizen bei zeitkritischen Tests notwendig als auch wenn mit einem PC-Lautsprecher[5] bei auditiven Reizen gearbeitet werden soll. Im ersten Schritt müssen sie auswählen, ob die visuelle Touch-Eingabe, oder ob die Touch-Eingabe auf auditive Reize kalibriert werden soll (siehe Abbildung 19).

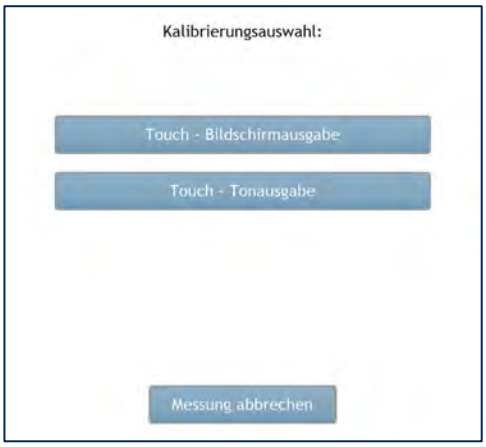


Abbildung 19: Auswahl der Kalibrierungsart

Nach der Auswahl wird, nach einer Startseite, eine Anleitung bezüglich des Anschlusses der Kalibrierungstools (siehe Abbildung 20). Der Abschluss der Kalibrierung wird Ihnen am Bildschirm dargestellt, siehe Abbildung 21.

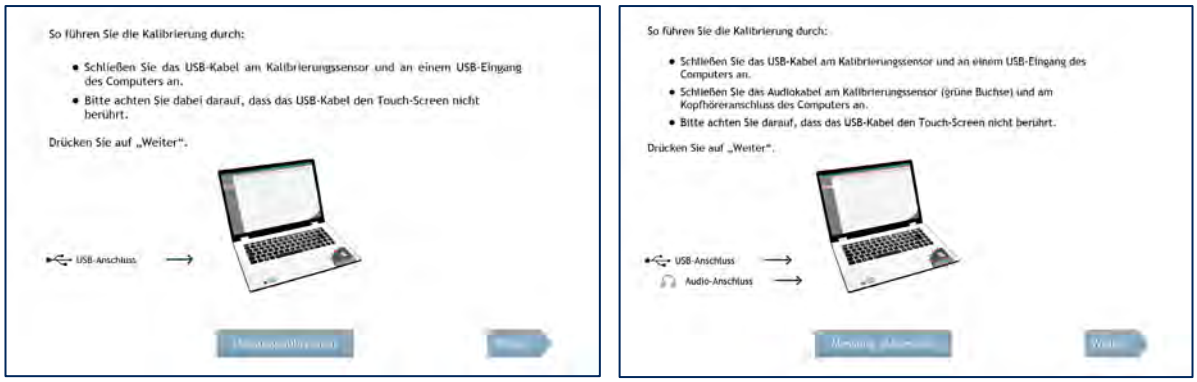


Abbildung 20: Vorbereitungsseite für die visuelle Touch-Kalibrierung (links) und die auditive Touch-Kalibrierung (rechts)

[5] Dies ist bei Verwendung von USB-Audiogeräten **nicht notwendig**!

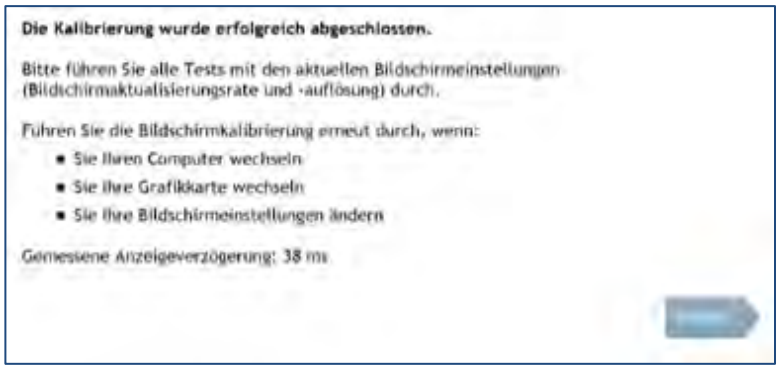


Abbildung 21: Bestätigung der Kalibrierung

5.4.3 PP-HW2 Hardwaretest

Nach dem Start des PP-HW2 Hardwaretest werden Sie aufgefordert die HW-Seriennummer[6] einzutragen, sowie die Person, welche die Prüfung durchführt (siehe Abbildung 22). Führen Sie die Prüfung Schritt für Schritt durch (siehe Abbildung 23) und bestätigen Sie mit „OK“ (die Schaltfläche wird Blau hinterlegt).

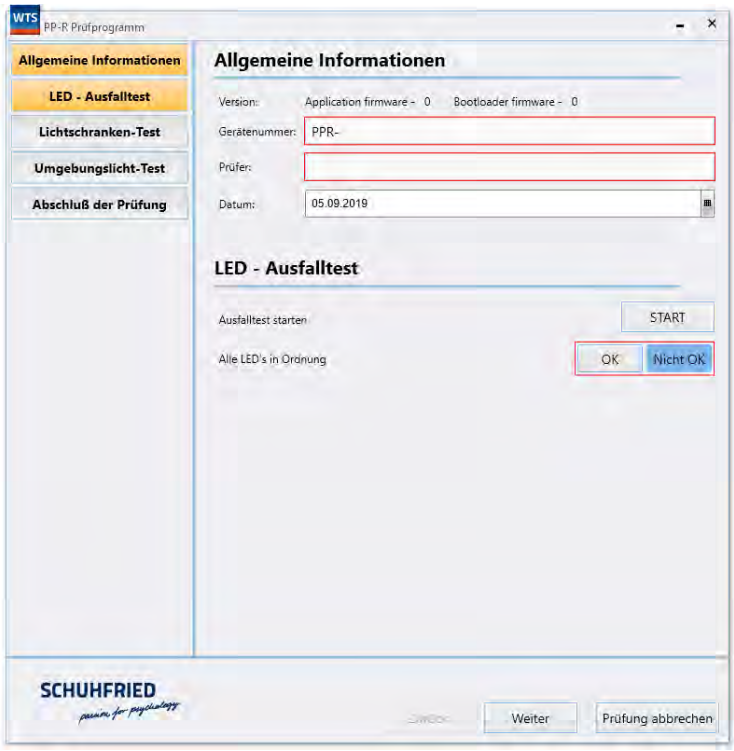


Abbildung 22: Schritt Eins des Hardwaretests der PP-HW2

[6] Die Seriennummer finden Sie am Geräteschild auf der Rückseite eines Flügels.

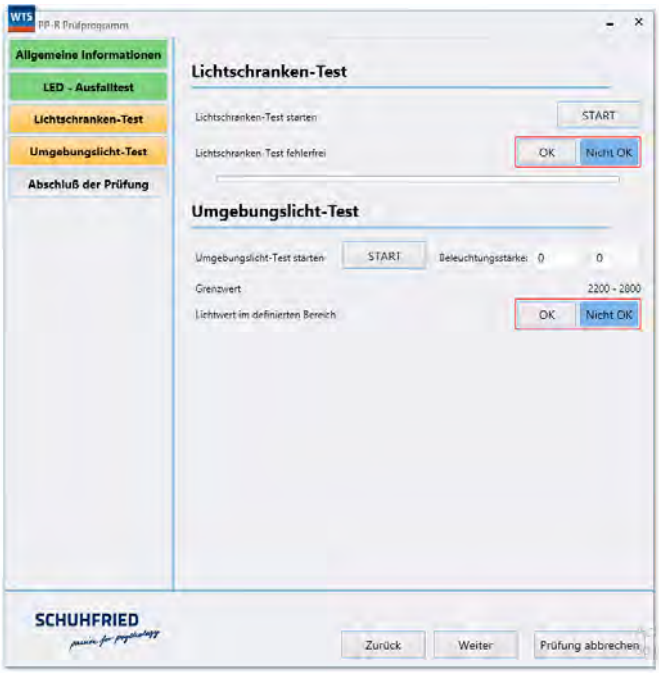


Abbildung 23: Schritt Zwei und Drei der Überprüfung

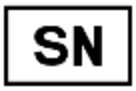
Zum Abschluss kann ein Protokoll bezüglich der Prüfung ausgedruckt werden.

6 ZUSÄTZLICHE HINWEISE

6.1 Warnhinweise

Dieses Zeichen weist auf die Begleitpapiere hin. Es ist ein genaues Studium der Betriebsanleitung vor der Inbetriebnahme notwendig.

Symbol für das Herstellungsdatum: Neben diesem Symbol ist das Herstellungsdatum angegeben.



Symbol für die Seriennummer: Neben diesem Symbol ist die Seriennummer des Gerätes angegeben.

Dieses Symbol gibt an, dass dieses Gerät einer getrennten Sammlung von Elektro- und Elektronikgeräten zugeführt werden muss, beziehungsweise vom Hersteller zurückgenommen wird.

Symbol für den Hersteller. Neben diesem Symbol ist der Hersteller angegeben.

Symbol für Geräte der Schutzklasse 2 nach der IEC 60417-5172

Symbol für die Typenbezeichnung: Neben diesem Symbol ist die Typenbezeichnung des Gerätes angegeben

Dieses Symbol gibt die Umgebungstemperaturgrenzen für Lagerung und Transport an.

Dieses Symbol gibt die relative Luftfeuchtigkeitsgrenzen für Lagerung und Transport an.

Dieses Symbol gibt die relativen Luftdrucksgrenzen für Lagerung und Transport an.

6.2 Wartung der Geräte

Grundsätzlich sind alle Geräte des Wiener Testsystems wartungsfrei. Es wird jedoch empfohlen, die einwandfreie Funktion der Geräte mit dem Wiener Testsystem-Hardwaretest halbjährlich zu überprüfen.
Instandhaltung, Instandsetzung und Änderungen müssen entsprechend den Bestimmungen des Elektrotechnikgesetzes ausgeführt werden.
Der Hersteller macht darauf aufmerksam, dass bei Veränderungen an den Geräten und bei Instandsetzungsarbeiten durch nicht autorisierte Personen oder Firmen die Garantieverpflichtung und Produkthaftung erlischt.
Die Reinigung der Geräte muss grundsätzlich im abgeschalteten Zustand erfolgen.
Verwenden Sie zur Reinigung der Geräte ausschließlich Desinfektionsmittel, oder mildes Reinigungsmittel, das Sie auf einem weichen Reinigungstuch auftragen. Vermeiden Sie das Auftragen von Reinigungs- oder Desinfektionsmitteln direkt auf das Gerät und deren Einzelteile, um zu verhindern, dass Flüssigkeit in das Gehäuse dringt.
Als Reinigungs- bzw. Desinfektionsmittel eignen sich grundsätzlich Flächendesinfektionsmittel. Falls die Geräte in Gesundheitseinrichtungen eingesetzt werden, dann sind Flächendesinfektionsmittel zu verwenden, die für Medizinprodukte gem. MPG und RL 93/42/EWG zugelassen sind. Zulässig sind Flüssigkeiten auf Basis von Alkohol (Ethanol) oder auf Wirkstoffbasis aktiven Sauerstoffs, die keine Lösungsmittel enthalten und nicht scheuern (z.B. Schülke mikrozid AF liquid oder ANTISEPTICA Descogen Liquid r.f.u.).
Warten Sie nach Reinigung der Geräte einige Minuten, bevor Sie diese wiederverwenden. Dadurch ist es möglich, dass eventuelle Reste von Reinigungs- oder Desinfektionsmitteln noch verdampfen.
Die vom Hersteller vorgesehene Produktlebensdauer beträgt 10 Jahre gerechnet ab dem Fertigungsdatum. Dieses Datum finden Sie auf dem Typenschild.

6.3 Sicherheitshinweise

Obwohl die Geräte keine Medizinprodukte sind, wurden sie gemäß den Anforderungen der ÖVE-Norm EN 60601 entwickelt, erfüllen diese Vorschriften aber nur, wenn sie an eine EDV-Anlage angeschlossen werden, die diese Vorschriften ebenfalls erfüllt.
Verlegen Sie die angeschlossenen Kabel so, dass ein unbeabsichtigtes Hängenbleiben oder Hinunterwerfen der Geräte verhindert wird. Die Kabel sollten sich nicht im Bereich des Probanden befinden, aber so viel Spielraum haben, dass sich jeder Proband die zu bedienenden Geräte zurechtstellen kann.
Beachten Sie bei der Verwendung von Kopfhörern darauf, dass die Lautstärke nicht maximal ist, wenn der Proband die Kopfhörer aufsetzt, um eine Schädigung des Gehörs zu vermeiden.
Verwenden Sie kein Peripheriegerät, wenn Teile beschädigt oder abgebrochen sind.
Die Wiener Testsystem USB-Peripheriegeräte dürfen nicht in Feuchträumen oder in explosionsgefährdeten Bereichen verwendet werden.
Der Hersteller bzw. Lieferant betrachtet sich nur dann für Sicherheit und Funktion der Geräte verantwortlich, wenn

- Montage, Erweiterungen, Neueinstellungen, Änderungen oder Reparaturen durch von ihm ermächtigte Personen ausgeführt werden und
- die elektrische Installation des betreffenden Raumes den Anforderungen der IEC-Festlegungen bzw. der ÖVE-EN 7 entspricht und
- die Geräte in Übereinstimmung mit der Gebrauchsanleitung verwendet werden, und die Geräte nicht gleichzeitig mit USB-Peripheriegeräten anderer Hersteller betrieben werden.

6.3.1 EMV-Hinweise

Falls die Eingabe- und Ausgabemedien des Wiener Testsystems im klinischen Umfeld eingesetzt werden, sind hinsichtlich der EMV besondere Vorsichtsmaßnahmen zu treffen. Auch im Nicht-Medizinischen Umfeld ist bezüglich EMV besondere Vorsicht geboten. Um einen sicheren Betrieb zu gewährleisten, ist das Verwenden von tragbaren und mobilen HF-Kommunikationseinrichtungen untersagt, da es zu starken Beeinträchtigungen der Funktion kommen kann.

6.3.2 ESD-Hinweise

In jedem Eingabemedium sind alle notwendigen Vorkehrungen von elektrostatischen Entladungen getroffen worden, um Bauteilschäden zu vermeiden. Die überschüssige Energie wird mittels Schutzdioden an die Erde abgeleitet. Sollte es zu einem Absturz des Eingabegerätes kommen, sind die Punkte aus Abschnitt 5.3.1 sequentiell durchzuführen. Wenn das Gerät während eines Tests ausgefallen ist, dann muss dieser wiederholt werden. Ursachen für ESD-Entladungen können durch Reibungen von Gummisohlen auf Kunststoff- oder Teppichböden entstehen. Besondere Vorsicht ist bei Berührung mit elektrisch leitenden Elementen geboten.
Im Kapitel 6.6 wird die EMV-gerechte Instandsetzung und die zutreffenden Leitlinien näher erörtert.

6.4 Haftungsausschluss

Der Hersteller bzw. Lieferant betrachtet sich nur dann für Sicherheit und Funktion der Geräte verantwortlich, wenn

- Montage, Erweiterungen, Neueinstellungen, Änderungen oder Reparaturen durch von ihm ermächtigte Personen ausgeführt werden und
- die elektrische Installation des betreffenden Raumes den Anforderungen der IEC-Festlegungen bzw. der ÖVE-EN 7 entspricht und
- die Geräte in Übereinstimmung mit der Gebrauchsanleitung verwendet werden und die Geräte nicht gleichzeitig mit USB-Peripheriegeräten anderer Hersteller betrieben werden.

6.5 Verpackung und Transport

Die Verpackung ist wiederverwendbar und sollte für einen eventuellen Transport aufbewahrt werden. Wir empfehlen für den Transport dieselben Bedingungen wie bei der Lagerung.
Der in der Verpackung enthaltene Schaumstoff besteht aus reinem PE und wird FCKW-frei geschäumt.
Entsorgung: Recycling durch einen PE-Verarbeiter

- In Verbrennungsanlagen rückstandsfrei
- Auf Deponien grundwasserneutral

6.6 Leitlinien und Herstellererklärung für EMV gerechte Errichtung in Gesundheitseinrichtungen

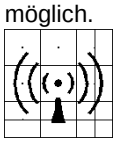
Tabelle 1: Elektromagnetische Aussendung

Das PANEL Ag/Ug ist für den Betrieb in einer wie unten angegebenen Umgebung bestimmt. Der Kunde oder der Anwender des PANEL Ag/Ug sollte sicherstellen, dass es in einer derartigen Umgebung betrieben wird.		
Störaussendungsmessungen	**Übereinstimmung**	**Elektromagnetische Umgebung - Leitfaden**
HF-Aussendungen nach CISPR 11	Gruppe 1	Das PANEL Ag/Ug verwendet HF-Energie ausschließlich zu seiner internen Funktion. Daher ist seine HF-Aussendung sehr gering, und es ist unwahrscheinlich, dass benachbarte elektronische Geräte gestört werden.
HF-Aussendungen nach CISPR 11	Klasse B	Das PANEL Ag/Ug ist für den Gebrauch in allen Einrichtungen einschließlich Wohnbereichen und solchen bestimmt, die unmittelbar an ein öffentliches Versorgungsnetz angeschlossen sind, das auch Gebäude versorgt, die für Wohnzwecke genutzt werden.
Aussendungen von Oberschwingungen nach IEC 61000-3-2	Nicht anwendbar	
Spannungsänderungen und Flicker nach IEC 61000-3-3	Nicht anwendbar	

Tabelle 2: Elektromagnetische Störfestigkeit

Das PANEL Ag/Ug ist für den Betrieb in der unten angegebenen elektromagnetischen Umgebung bestimmt. Der Kunde oder der Anwender des PANEL Ag/Ug sollte sicherstellen, dass es in einer solchen Umgebung benutzt wird.			
Störfestigkeitsprüfung	**IEC 60601-Prüfpegel**	**Übereinstimmungs-pegel**	**Elektromagentische Umgebung - Leitlinie**
Entladung statischer Elektrizität (ESD) nach IEC 61000-4-2	± 6 kV Kontaktentladung ± 8 kV Luftentladung	± 6 kV Kontaktentladung ± 8 kV Luftentladung	Fußböden sollten aus Holz oder Beton bestehen oder mit Keramikfliesen versehen sein. Wenn der Fußboden mit synthetischem Material versehen ist, muss die relative Luftfeuchtigkeit mindestens 30 % betragen.
schnelle transiente elektrische Störgrößen/Bursts nach IEC 61000-4-4-	± 2 kV für Netzleitungen ± 1 kV für Eingangs- und Ausgangsleitungen	Nicht anwendbar	Die Qualität der Versorgungsspannung sollte der einer typischen Geschäfts- oder Krankenhausumgebung entsprechen.
Stoßspannungen (Surges) nach IEC 61000-4-5	± 1 kV Gegentaktspannung ± 2 kV Gleichtaktspannung	Nicht anwendbar	Die Qualität der Versorgungsspannung sollte der einer typischen Geschäfts- oder Krankenhausumgebung entsprechen.
Spannungseinbrüche, Kurzzeitunterbrechungen und Schwankungen der Versorgungsspannung nach IEC 61000-4-11	< 5 % U_T (> 95 % Einbruch der U_T) für ½ Periode 40 % U_T (60 % Einbruch der U_T) für 5 Perioden 70 % U_T (30 % Einbruch der U_T) für 25 Perioden < 5 % U_T (> 95 % Einbruch der U_T) für 5 s	Nicht anwendbar	Die Qualität der Versorgungsspannung sollte der einer typischen Geschäfts- oder Krankenhausumgebung entsprechen. Wenn der Anwender des PANEL Ag/Ug fortgesetzte Funktion auch beim Auftreten von Unterbrechungen der Energieversorgung fordert, wird empfohlen, das PANEL Ag/Ug aus einer unterbrechungsfreien Stromversorgung oder einer Batterie zu speisen.
Magnetfeld bei der Versorgungsfrequenz (50 Hz/60 Hz) nach IEC 61000-4-8	3 A/m	3 A/m	Magnetfelder bei der Netzfrequenz sollten den typischen Werten, wie sie in der Geschäfts- und Krankenhausumgebung vorzufinden sind, entsprechen.
Anmerkung	U_T ist die Netzwechselspannung vor der Anwendung der Prüfpegel.		

Tabelle 3: Elektromagnetische Störfestigkeit

<table>
<tr><td colspan="4">Das PANEL Ag/Ug ist für den Betrieb in der unten angegebenen elektromagnetischen Umgebung bestimmt. Der Kunde oder der Anwender des PANEL Ag/Ug sollte sicherstellen, dass es in einer solchen Umgebung benutzt wird.</td></tr>
<tr><td>Störfestigkeitsprüfungen</td><td>IEC 60601-Prüfpegel</td><td>Übereinstim-mungspegel</td><td>Elektromagnetische Umgebung - Leitlinien</td></tr>
<tr><td></td><td></td><td></td><td>Tragbare und mobile Funkgeräte werden in keinem geringeren Abstand zum PANEL Ag/Ug einschließlich der Leitungen als dem empfohlenen Schutzabstand verwendet, der nach der für die Sendefrequenz geeigneten Gleichung berechnet wird.
Empfohlener Schutzabstand:</td></tr>
<tr><td>Geleitete HF-Störgrößen nach IEC 61000-4-6</td><td>3 V_{eff}
150 kHz bis 80 MHz</td><td>3 → $V1$ in V</td><td>$d = \left(\frac{3{,}5}{V1}\right) * \sqrt{P}$</td></tr>
<tr><td>Gestrahlte HF-Störgrößen nach IEC 61000-4-3</td><td>3 V/m
80 MHz bis 2,5 GHz</td><td>3 → $E1$ in V/m</td><td>$d = \left(\frac{3{,}5}{E1}\right) * \sqrt{P}$
für 80 MHz bis 800 MHz</td></tr>
<tr><td></td><td></td><td></td><td>$d = \left(\frac{7}{E1}\right) * \sqrt{P}$
für 800 MHz bis 2,5 GHz</td></tr>
<tr><td></td><td></td><td></td><td rowspan="3">mit P als der maximalen Nennleistung des Senders in Watt (W) gemäß Angaben des Senderherstellers und d als empfohlenem Schutzabstand in Metern (m).
Die Feldstärke stationärer Funksender sollte bei allen Frequenzen gemäß einer Untersuchung vor Ort[a] geringer als der Übereinstimmungspegel sein.[b]
In der Umgebung von Geräten, die das folgende Bildzeichen tragen, sind Störungen möglich.
  </td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="4">Anmerkung 1 Bei 80 MHz und 800 MHz gilt der höhere Frequenzbereich
Anmerkung 2 Diese Leitlinien mögen nicht in allen Fällen anwendbar sein. Die Ausbreitung elektromagnetischer Größen wird durch Absorption und Reflexion der Gebäude, Gegenstände und Menschen beeinflusst.</td></tr>
<tr><td colspan="4">a Die Feldstärke stationärer Sender, wie z.B. Basisstationen von Funktelefonen und mobilen Landfunkdiensten, Amateurstationen, AM- und FM-Rundfunk- und Fernsehsendern können theoretisch nicht genau vorherbestimmt werden. Um die elektromagnetische Umgebung in Folge von stationären HF-Sender zu ermitteln, ist eine Untersuchung des Standortes zu empfehlen. Wenn die ermittelte Feldstärke am Standort des PANEL Ag/Ug den oben angegebenen Übereinstimmungspegel überschreitet, muss das PANEL Ag/Ug hinsichtlich seines normalen Betriebs an jedem Anwendungsort beobachtet werden. Wenn ungewöhnliche Leistungsmerkmale beobachtet werden, kann es notwendig sein, zusätzliche Maßnahmen zu ergreifen, wie z.B. eine veränderte Ausrichtung oder ein anderer Standort des PANEL Ag/Ug.

b Über den Frequenzbereich von 150 kHz bis 80 MHz sollte die Feldstärke geringer als [V1] V/m sein.</td></tr>
</table>

Tabelle 4: Empfohlene Schutzabstände

Empfohlene Schutzabstände zwischen tragbaren und mobilen HF-Telekommunikationsgeräten und dem PANEL Ag/Ug			
Das PANEL Ag/Ug ist für den Betrieb in einer elektromagnetischen Umgebung bestimmt, in der die HF-Störgrößen kontrolliert sind. Der Kunde oder der Anwender des PANEL Ag/Ug kann dadurch helfen, elektromagnetische Störungen zu vermeiden, indem er den Mindestabstand zwischen tragbaren und mobilen HF-Telekommunikationsgeräten (Sendern) und dem PANEL Ag/Ug - abhängig von der Ausgangsleistung des Kommunikationsgerätes, wie unten angegeben – einhält.			
Nennleistung des Senders W	**Schutzabstand abhängig von der Sendefrequenz m**		
	150 kHz bis 80 MHz $d = \left(\frac{3,5}{V1}\right) * \sqrt{P}$	**80 MHz bis 800 MHz** $d = \left(\frac{3,5}{E1}\right) * \sqrt{P}$	**800 MHz bis 2,5 GHz** $d = \left(\frac{7}{E1}\right) * \sqrt{P}$
0,01	0,12	0,12	0,23
0,1	0,37	0,37	0,74
1	1,17	1,17	2,33
10	3,69	3,69	7,38
100	11,67	11,67	23,33
Für Sender, deren maximale Nennleistung nicht in obiger Tabelle angegeben ist, kann der Abstand unter Verwendung der Gleichung bestimmt werden, die zur jeweiligen Spalte gehört, wobei P die maximale Nennleistung des Senders in Watt (W) gemäß Angabe des Senderherstellers ist.			
Anmerkung 1	Bei 80 MHz und 800 MHz gilt der höhere Frequenzbereich.		
Anmerkung 2	Diese Leitlinien mögen nicht in allen Fällen anwendbar sein. Die Ausbreitung elektromagnetischer Größen wird durch Absorption und Reflexion der Gebäude, Gegenstände und Menschen beeinflusst.		