



DISPONIC[®]
PROFESSIONELLE DIENSTPLANUNG

DISPONIC ab Vers. 7 / DISPONIC to go
Vorbedingungen für Selbsthoster

Stand: 16.04.2026



INHALTSVERZEICHNIS

1	EINLEITUNG	2
1.1	Installationsszenario „Intern/Extern“	2
1.2	Installationsszenario „Full“	3
2	WINDOWS-BENUTZER	3
3	ZERTIFIKATE	4
4	CHECKLISTE VORBEDINGUNGEN	5
5	NACH DER INSTALLATION	6

1 EINLEITUNG

Mit der Auslieferung von DISPONIC to go erfolgt die Installation des gesamten Produktes über einen sog. Serverinstaller. Dieser hält Datenbank, Webservice und API auf einem synchronen Stand. Die Installation der Clients erfolgt anschließend wie gewohnt.

Die Installation mit dem Serverinstaller bringt schon einige Vorbereitungen auf neue Sicherheitsfeatures mit, die ab Version 7 zwingend erforderlich sind. So werden wir, z. B. neue Datenbankbenutzer mit spezifischen Rollen erstellen.

Folgende Checklisten dienen zur Prüfung, ob für die Installation von DISPONIC to go (bzw. DISPONIC ab Version 7) alle Vorbedingungen erfüllt sind. Wir stellen hierzu auch die Anwendung DisponicServerSetupAuditor.exe zur Verfügung, die einige (nicht alle) der Punkte prüft.

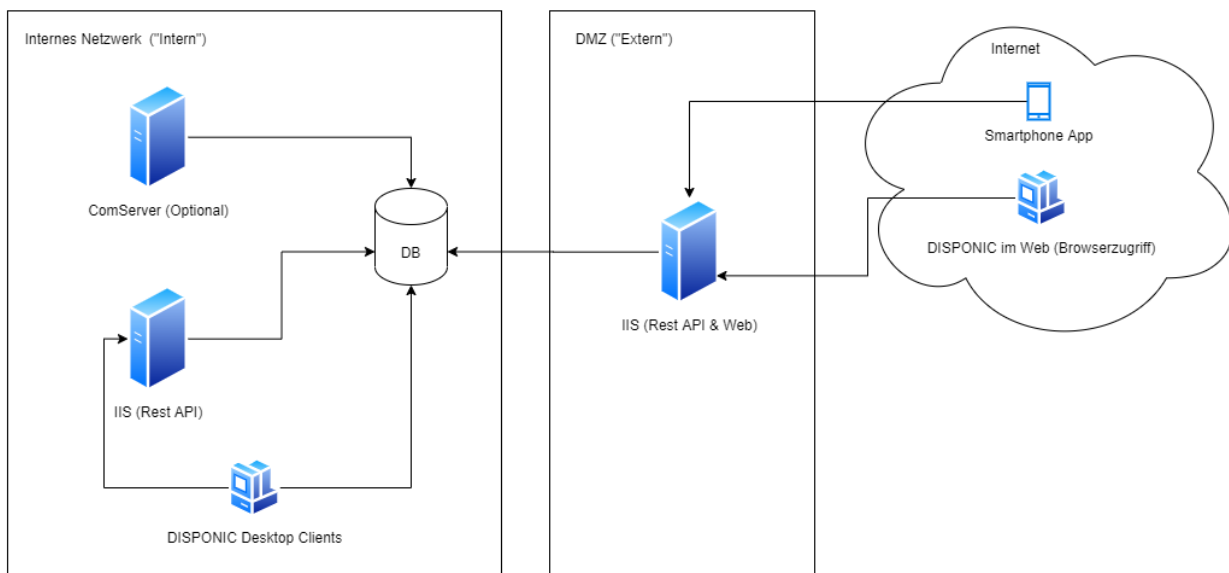
Mögliche serverseitige Installationsszenarien DISPONIC unterstützt zwei verschiedene Installationsszenarien.

1.1 Installationsszenario „Intern/Extern“

Dies ist das Standard-Szenario und bietet die beste Sicherheit.

Dabei werden Module mit Internetzugang (Web / Rest API) auf einem separaten Server installiert.

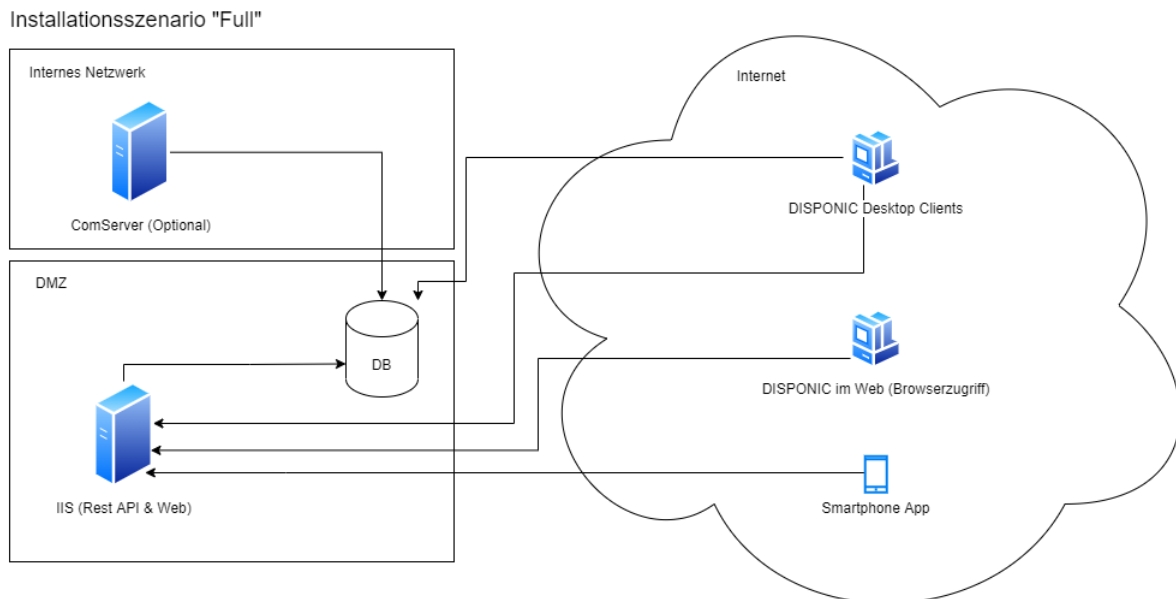
Installationsszenario "Intern / Extern"



Bitte beachten Sie, dass sich die DISPONIC Desktop-Clients in diesem Szenario im selben Netzwerk wie die Datenbank befinden müssen. Soll ein Zugriff von außerhalb dieses Netzwerks erfolgen, empfehlen wir die Nutzung einer VPN-Verbindung.

1.2 Installationsszenario „Full“

Das Installationsszenario „Full“ wird ausdrücklich nicht empfohlen und wird nur aus Kompatibilitätsgründen unterstützt, da dadurch zwingend der SQL Datenbankserver eine direkte Verbindung zum Internet haben muss. Wird dieses Szenario gewählt, ist der Einsatz eines IPS (Intrusion Prevention Systems) obligatorisch, falls die Desktop Clients direkten Zugriff aus dem Internet auf die Datenbank haben.



2 WINDOWS-BENUTZER

Nur notwendig, wenn sich IIS und Datenbank auf getrennten Servern befinden.

Alternativ kann für dieses Szenario auch ein SQL-Benutzer verwendet werden.

MIT ACTIVE DIRECTORY

Je nach Installationsszenario (siehe 0 Mögliche serverseitige Installationsszenarien) können IIS und Datenbank-Server entweder auf demselben Host oder auf getrennten Hosts betrieben werden:

- **IIS & Datenbank auf demselben Server**
Kein zusätzliches Windows-Benutzerkonto erforderlich.
- **IIS und Datenbank auf unterschiedlichen Servern**
Für jede IIS-Instanz muss ein eigenes Windows-Benutzerkonto angelegt werden.
Diese Konten erhalten im Installationsprozess nur die minimal notwendigen Berechtigungen in der Datenbank.
Wird im intern/extern Szenario die Datenbank auf einem komplett separaten Server betrieben, müssen entsprechend zwei separate Konten eingerichtet werden (einmal für den IIS intern und einmal für den IIS extern)

OHNE ACTIVE DIRECTORY

Haben die Server keine Anbindung an einen AD, so sind alternativ SQL Benutzer anzulegen, welche dann nach der Installation durch den Serverinstaller der entsprechenden Rolle „disponic_dmz“ zugeordnet werden müssen.

3 ZERTIFIKATE

Je nach Installationsszenario werden unterschiedliche Zertifikate benötigt.

Für den SQL Server

Datenabfragen zum SQL Server erfolgen von allen DISPONIC-Anwendungen ausschließlich SSL/TLS-verschlüsselt.

Entsprechend wird ein Zertifikat benötigt, welches die Verbindung der Anwendungen zur Datenbank absichert. Dieses wird i. d. R. über *SQL Server Configuration Manager* → *SQL Server-Netzwerkconfiguration* → *Zertifikat hinterlegt*. – Oft handelt es sich hierbei um ein *selbstsigniertes Zertifikat*.

Das Zertifikat zur Absicherung des SQL Server muss im Zertifikatsspeicher in unter den Vertrauenswürdigen Zertifikaten, als auch unter Webhosting abgelegt sein.

Für den / die Webserver (IIS):

Der Webserver (bzw. die Webserver, abhängig vom Installationsszenario) benötigen ein gültiges Zertifikat.

Dies kann, je nach Zugriffsweg, ein Domain-Zertifikat oder ein internes Zertifikat sein.

Entscheidend ist, dass die Zertifikatskette im jeweiligen Szenario vollständig und vertrauenswürdig ist.

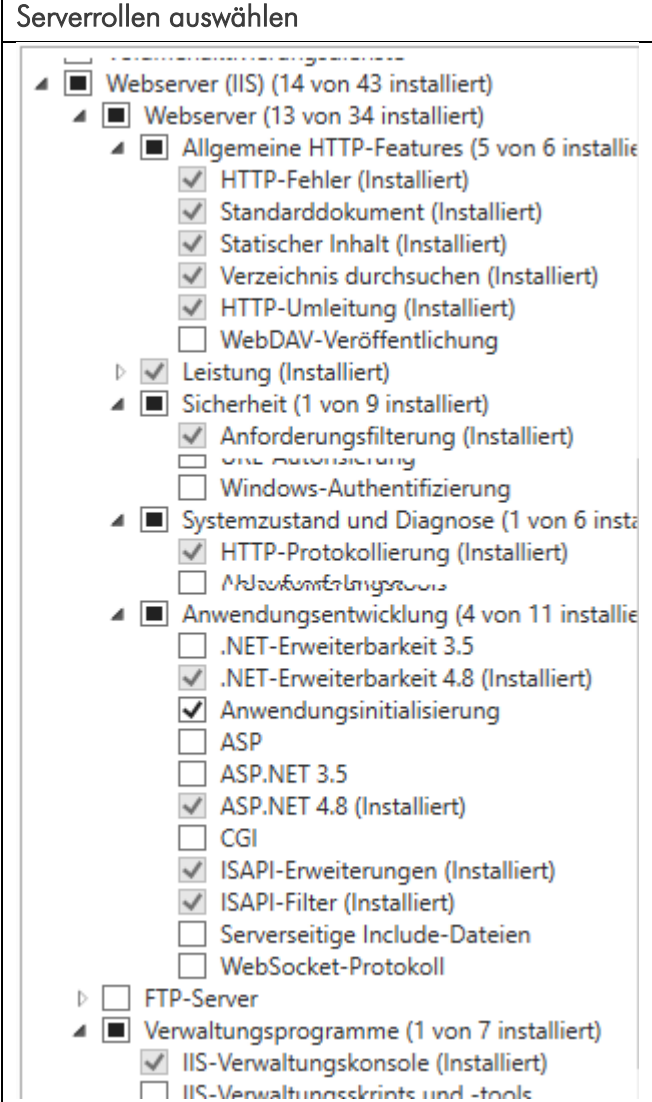
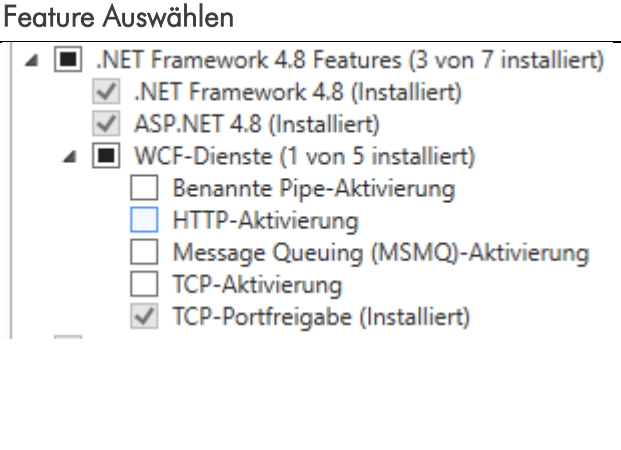
Wird ein Zugriff über das Internet realisiert (z. B. Web-Client oder DISPONIC to go App), muss z.B. der externe IIS entsprechend mit einem passenden Zertifikat ausgestattet sein.

Hinweis: Für den IIS muss das Zertifikat im Zertifikatsspeicher „WebHosting“ abgelegt sein.

Wenn Sie das Szenario „Full“ einsetzen, können Sie das Domain-Zertifikat auch für den SQL-Server verwenden.

4 CHECKLISTE VORBEDINGUNGEN

- Die Hardwarevoraussetzungen für den Server lt. [DISPONIC-Systemvoraussetzungen](#) sind gegeben.
- Hosting Bundle von ASP.NET Core Runtime 8.0.x muss installiert sein. ([.NET 8.0 Download Seite](#))
- .NET Desktop Runtime 8.0.x (x64) muss installiert sein ([.NET 8.0 Download Seite](#))
- Microsoft Internet Information Services (IIS) muss mit folgenden Einstellungen installiert sein

Serverrollen auswählen	Feature Auswählen
	

Beachten Sie bitte, dass „WWW-Dienste – Sicherheit - Windows-Authentifizierung“ auch mit installiert sein muss, wenn Sie diese verwenden möchten.

Verwenden Sie das IIS Feature 'Application Request Routing (ARR)', so kontaktieren Sie vor der Installation unseren Support, da noch weitere individuelle Voraussetzungen gelten könnten.

- Die folgenden URL-Domains müssen von den IIS-Webservern erreichbar sein:
 - o activationserver.disponic.de: 443
 - o activationserverfallback.disponic.de: 443
 - o disponic.de:443
- Ein SQL-Server in der Mindestversion, wie den [DISPONIC-Systemvoraussetzungen](#) angegeben, ist installiert.

- Benutzer sind wie unter „2 Windows-Benutzer “ beschrieben angelegt.
- Der Authentifizierungsmodus des SQL Server ist auf „Mixed Mode“ eingestellt.
- Die Datenzugriffe sind wie unter „3 Zertifikate“ beschrieben abgesichert.
- Die frei Festplattenkapazität des Laufwerks C: und des Laufwerks, auf dem die Datenbanken liegen, entspricht mindestens der Gesamtgröße aller Datenbanken.

Um zu prüfen, ob die Vorbedingungen erfüllt sind, nutzen Sie bitte unser Tool. Dieses können Sie unter folgendem Link herunterladen: [DisponicServerSetupAuditor.zip](#)

5 NACH DER INSTALLATION

- **UMSTELLUNG AUF AKTIVIERUNGSCODE**

Bis jetzt melden sich die Anwender an der Datenbank an, in dem beim Start des DISPONIC-Clients im Anmeldefenster die Datenbankinstanz und der Datenbankname angegeben werden.

Ab jetzt muss anstatt dessen eine Aktivierungskode angegeben werden. Dieser kann im Anmeldedialog über den Knopf mit dem Diskettensymbol gespeichert werden, so dass jeder Anwender die Angabe nur einmal tätigen muss.

Um den Aktivierungskode eingeben zu können, müssen zunächst Datenbankinstanz und Datenbankname gelöscht werden.

Wenn DISPONIC über eine Verknüpfung mit Startparametern erfolgt, dann kann dieser einfach ausgetauscht werden, siehe Beispiel:

```
ALT: -instance:MYCOMPUTER\DISPONIC -database:DISPONIC  
NEU: -activationcode: iFDc4E$Rs#Wi
```

Den für Sie gültigen Aktivierungskode erhalten Sie beim Installationstermin. Gerne auch im Vorfeld, bitte fragen Sie bei uns an.

- **VERWENDEN DER FUNKTION PASSWORT ZURÜCKSETZEN**

Neu kommt u. a. die Funktion, dass Anwender ihr Passwort für Web und DISPONIC to go selbst zurücksetzen können. Dafür muss ein SMTP-Server zur Verfügung stehen. Zur Einrichtung siehe hierzu im Dokument [DISPONIC Serverinstaller Handbuch](#).

- **NUTZEN VON PUSH-BENACHRITIGUNGEN**

Wenn Sie DISPONIC to go nutzen, können die Mitarbeiter zu Dienstplanänderungen Push-Benachrichtigungen auf Ihr Smartphone erhalten. Hierfür müssen Sie ein Firebase Projekt einrichten. Siehe hierzu im Dokument [DISPONIC Serverinstaller Handbuch](#).

- **WEITERE INFORMATIONEN PER E-MAIL**

Sie erhalten eine E-Mail mit den Aktivierungscodes für DISPONIC und DISPONIC to go.