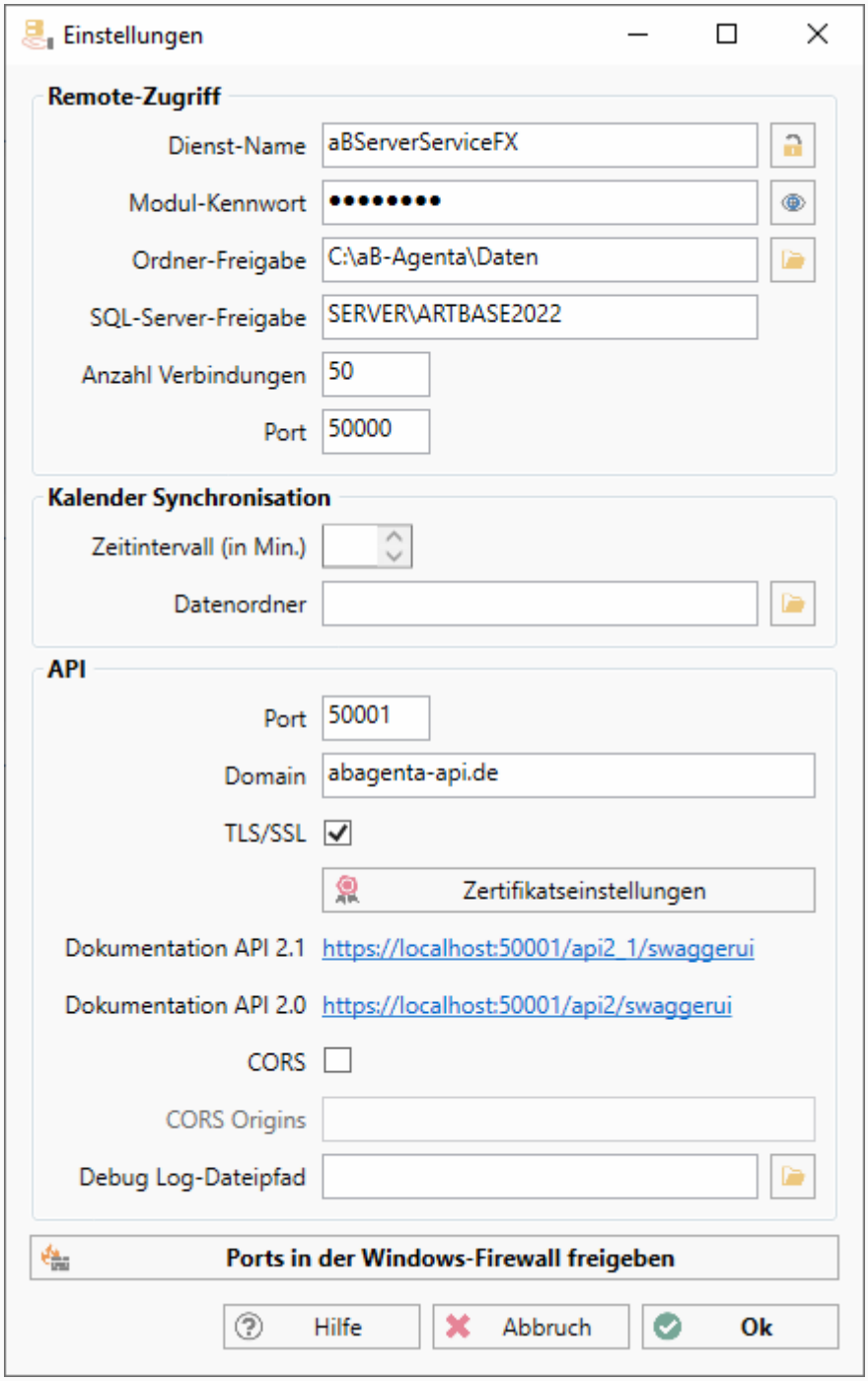
Einstellungen

In diesem Dialog können Sie die Einstellungen für den Remote-Zugriff und den Zugriff über unsere API konfigurieren.

Sie erreichen diesen Dialog über Konfiguration aBServer-Dienst.



Optionen Remote-Zugriff

- ### Dienst-Name
  Der Name des Windows-Dienstes. Dieser ist vorgegeben und kann nicht geändert werden.
- ### Modul-Kennwort
  Das Modul-Kennwort muss bei Verbindungen von außen angegeben werden und stellt eine zusätzliche Sicherheitsmaßnahme dar. Durch einen Klick auf den Knopf  können Sie sich das Modul-Kennwort anzeigen lassen.
- ### Ordner-Freigabe
  Tragen Sie hier Ihren Datenordner ein. Dadurch geben Sie externen Nutzern die Erlaubnis, auf diesen Datenordner zuzugreifen. Falls Sie mehrere Pfade angeben möchten, tragen Sie diese hintereinander ein und trennen sie mit einem Semikolon ";".
- ### SQL-Server-Freigabe
  Tragen Sie hier die SQL-Server-Instanz Ihres Datenordners ein (standardmäßig "*\ARTBASE2025*"). Dadurch geben Sie externen Nutzern die Erlaubnis, auf diesen SQL-Server zuzugreifen. Falls Sie mehrere Instanzen angeben möchten, tragen Sie diese hintereinander ein und trennen sie mit einem Semikolon ";".
- ### Anzahl Verbindungen
  Die maximale Anzahl gleichzeitig verbundener Clients.
- ### Port
  Der TCP-Port, der für Remote-Sitzungen verwendet wird. Der Standardwert ist 50000. Mit 0 wird der Remote-Zugriff deaktiviert.

Optionen Kalender-Synchronisation

- ### Zeitintervall (in Min.)
  Hier stellen Sie das Intervall ein, in dem der Online-Kalender synchronisiert werden soll. Das System startet dann automatisch eine Synchronisation der hinterlegten Kalender. Mit 0 ist die automatische Synchronisation deaktiviert.
- ### Datenordner
  An dieser Stelle können Sie den Datenordner einstellen, dessen Kalender automatisch synchronisiert werden soll. Mehrere Datenordner trennen Sie mit einem Semikolon ";".

Optionen API

- ### Port
  Der TCP-Port, über den die API erreichbar ist. Lassen Sie das Feld leer, um die API zu deaktivieren.
- ### Standard Datenordner
  Optional: API-Anfragen werden auf diesen Datenordner angewandt, sofern nicht ausdrücklich ein anderer angegeben ist. Bleibt das Feld leer, muss jede API-Anfrage einen

Datenordner angeben.

- ### Domain
  Das ist die Domain, mit der auf die API zugegriffen wird. Diese Domain wird nur benötigt, wenn TLS/SSL eingeschaltet wird. Das System sucht dann täglich anhand dieser Domain nach einem Zertifikat im Zertifikatsspeicher, dass an den entsprechenden Port gebunden wird.
  Die Angabe ist notwendig, falls die Verschlüsselung per TLS/SSL eingeschaltet wird.
- ### TLS/SSL
  Hier können Sie festlegen, ob der API-Zugriff verschlüsselt stattfinden soll.
  Wenn Sie den Zugriff von außen über das Internet freigeben, sollten Sie diese Option zwingend setzen, weil ansonsten Daten und Kennwörter unverschlüsselt übertragen werden.
  Findet der Zugriff z.B. immer über eine VPN-Verbindung statt, ist eine Verschlüsselung nicht zwingend notwendig.
- ### Zertifikatseinstellungen
  Die Zertifikatseinstellungen sind notwendig, wenn der Zugriff auf die API über TLS/SSL verschlüsselt stattfinden soll. Öffnen des Dialogs für die Zertifikatseinstellungen.
- ### Dokumentation API 2.1
  Link zum Aufruf der API 2.1 Dokumentation von diesem Dienst. So können Sie eine API-Implementierung mit Ihren eigenen Daten testen.
- ### Dokumentation API 2.0
  Link zum Aufruf der API 2.0 Dokumentation von diesem Dienst. So können Sie eine API-Implementierung mit Ihren eigenen Daten testen.
- ### CORS
  Einschalten der CORS-Funktion für die API. Dadurch können auch an anderer Stelle gehostete Webseiten auf unsere API zugreifen.
- ### CORS Origins
  Wenn CORS eingeschaltet ist, kann man hier einschränken, von welchen Webseiten der Zugriff erlaubt ist. Ist das Feld leer, gilt CORS für alle, ansonsten kann man IP-Adressen oder Domain-Namen eintragen, für die CORS erlaubt sein soll. Einzelne Einträge werden dabei durch eine Pipe "|" getrennt. Die Angabe ist optional.
- ### Debug Log-Dateipfad
  Hier geben Sie eine Textdatei an, in der alle eingehenden API-Anfragen (Header und Inhalt) protokolliert werden. **Achtung:** Diese Option kostet Performance und Speicherplatz und speichert unter Umständen sensible Daten (auch Kennwörter) im Klartext. Nur für Testzwecke verwenden!

Vorgehensweise für die Inbetriebnahme des Dienstes

Definieren Sie als erstes ein **Modul-Kennwort** für den externen Zugriff. Dieses Kennwort muss keine besonderen Richtlinien erfüllen. Da es sich aber um eine zusätzliche Sicherheit für den Zugriff von außen darstellt, sollte dieses Kennwort eine ausreichende Komplexität erfüllen.

Legen Sie nun unter **Ordner-Freigabe** das Verzeichnis fest, das für den Zugriff von außen freigegeben werden soll. Typischerweise ist das der **aB-Agenta Datenordner**. Auf diesen und untergeordnete Ordner können die externen Versionen zugreifen. Alle Ordner in den Ebenen darüber

werden durch den **aBServer-Dienst** gesperrt.

Bei der **SQL-Server-Freigabe** wird der SQL-Server-Name eingetragen, an dem die aB-Agenta-Datenbank angebunden ist. Hierbei handelt es sich standardmäßig um '\ARTBASE2025'. Sollten Sie nicht genau wissen, wie der SQL-Server-Name lautet, können Sie diesen auch in der **SQL-Datenbank-Verwaltung** von aB-Agenta nachschauen. Rufen Sie diese über die **Zusatzmodule** innerhalb von aB-Agenta auf.

Zuletzt wählen Sie noch einen **Port**, an dem der **aBServer-Dienst** auf Anfragen wartet. Der Port-Bereich bei einem Windows-Betriebssystem reicht von 1 bis 65535. Dabei sind zwischen 1 und 49151 einige Ports durch Standards belegt, wie beispielsweise Port 80 für Internet-Verkehr über das http-Protokoll. Die benutzerdefinierten Ports beginnen ab 49152. Wir geben standardmäßig den Port 50000 vor. Sollte dieser bereits durch eine andere Anwendung benutzt werden, definieren Sie einfach einen anderen. Der gewählte Port muss noch an der externen Firewall freigeschaltet und weitergeleitet werden. Wir haben die Portweiterleitung am Beispiel einer FritzBox beschrieben. Die Freigabe der Ports (Remote-Zugriff und API) in der Windows Firewall kann durch einen Klick auf den Knopf Ports in der Windows-Firewall freigeben automatisch gemacht werden.

Erstellt: 2026-08-13 07:07:49 CEST von API
Zuletzt aktualisiert: 2026-10-28 13:34:37 CET von API