

Installationsanleitung aBServer-Dienst

- [Konfiguration aBServer-Dienst](#)
 - [Allgemeine Informationen](#)
 - [Einstellungen](#)
 - [Zertifikatseinstellungen](#)
 - [Aktive Anmeldungen am Web-Service](#)
- [Server-Modul Anmeldedaten](#)
- [Konfigurationsbeispiel FRITZ!Box 7590](#)

Konfiguration aBServer-Dienst

Allgemeine Informationen

Mit diesem Modul kann der **aBServer-Dienst** konfiguriert werden. Dieses Modul kann nur lokal auf dem Rechner ausgeführt werden, auf dem das Programm installiert ist.

Konfiguration_Dienst_2.PNG

- **Windows-Dienst installieren bzw. deinstallieren**
- **Dienst starten/beenden**
Starten bzw. beenden des aBServer-Dienstes. Wenn Sie den Dienst beenden, ist kein Zugriff von außen mehr möglich
- **Einstellungen**
Aufrufen der [Einstellungen](#)
- **Aktive Anmeldungen abfragen**
Anzeige der momentan aktiven Anmeldungen am aBServer-Dienst

Voraussetzungen

Damit Ihre Mitarbeiter oder Filialen über das Internet auf Ihre Daten zugreifen können, müssen folgende Voraussetzungen erfüllt sein:

- Auf dem Server-Rechner muss als Betriebssystem Windows 10 / Server 2016 oder höher installiert sein.
- Auf dem Server, der die Daten extern zur Verfügung stellen soll, müssen eine Installation von aB-Agenta und der entsprechende Daten-Ordner vorhanden sein.
- Dieser Server muss über das Internet erreichbar sein. Das bedeutet, man muss eine statische öffentliche IP- oder www-Adresse besitzen, die auf diesen Server verweist. Sollten Sie keine statische IP-Adresse haben, kann man das künstlich über verschiedene Anbieter wie beispielsweise [TwoDNS](#) erreichen.
- Wenn Sie eine Firewall einsetzen, muss der entsprechende Port, an dem die Anfragen eingehen, an den Server weitergeleitet werden. Die korrekte Konfiguration der Firewall wird von uns vorausgesetzt. Wir stellen anhand der FRITZ!Box 7590 die [Konfiguration](#) einer Portweiterleitung vor.
- Damit der Zugriff über das Internet erfolgen kann, muss der **aBServer-Dienst** auf dem Server installiert und gestartet sein. Ebenso müssen die korrekten [Einstellungen](#) für den Zugriff getroffen worden sein.
- Für den Windows-Benutzer, der für den Remote-Zugriff eingesetzt wird, muss zwingend ein Kennwort definiert werden.

aBServer-Dienst in Betrieb nehmen

Um den aBServer-Dienst erstmalig in Betrieb zu nehmen führen Sie folgende Schritte aus:

- Prüfen und erfüllen Sie die oben genannten Voraussetzungen.

- Installieren Sie den Windows-Dienst, indem Sie auf die Schaltfläche Dienst installieren klicken.
- Klicken Sie auf Einstellungen und konfigurieren Sie den Dienst Ihren Gegebenheiten entsprechend. Siehe [aBServer-Dienst - Einstellungen](#)

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.

 Einstellungen

Remote-Zugriff

Dienst-Name

aBServerServiceFX



Modul-Kennwort

••••••••



Ordner-Freigabe

C:\aB-Agenta\Daten



SQL-Server-Freigabe

SERVER\ARTBASE2022

Anzahl Verbindungen

50

Port

50000

Kalender Synchronisation

Zeitintervall (in Min.)

Datenordner



API

Port

50001

Domain

abagenta-api.de

TLS/SSL

☒

 Zertifikatseinstellungen

Dokumentation API 2.1

https://localhost:50001/api2_1/swaggerui

Dokumentation API 2.0

<https://localhost:50001/api2/swaggerui>

CORS

☐

CORS Origins

Debug Log-Dateipfad



 Ports in der Windows-Firewall freigeben

 Hilfe

 Abbruch

 Ok

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 "IARTBASE2019"). 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.

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.

- **Datenordner**

An dieser Stelle können Sie den Datenordner einstellen, dessen Kalender automatisch synchronisiert werden soll.

Optionen API

- **Port**

Hier stellen Sie das Intervall ein, in dem der Online-Kalender synchronisiert werden soll. Das System startet dann automatisch eine Synchronisation der hinterlegten Kalender.

- **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, das 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**

In diesem Ordner werden gegebenenfalls Log-Dateien gespeichert.

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 'ARTBASE2019'. 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.

Zertifikatseinstellungen

Um den Zugriff auf die API von außen abzusichern, benötigt man eine Internet-Domain und ein Zertifikat zur Verschlüsselung.

Die Domain muss auf Ihren Internet-Anschluss verweisen, damit Anfragen aus z.B. einem Webbrowser auch an den aBServer-Dienst weitergeleitet werden können.

Haben Sie bereits ein gekauftes Zertifikat für die entsprechende Domain, können Sie dieses hier importieren. Haben sie kein Zertifikat für die Domain, kann der aBServer-Dienst automatisch ein LetsEncrypt-Zertifikat erzeugen und aktualisieren.

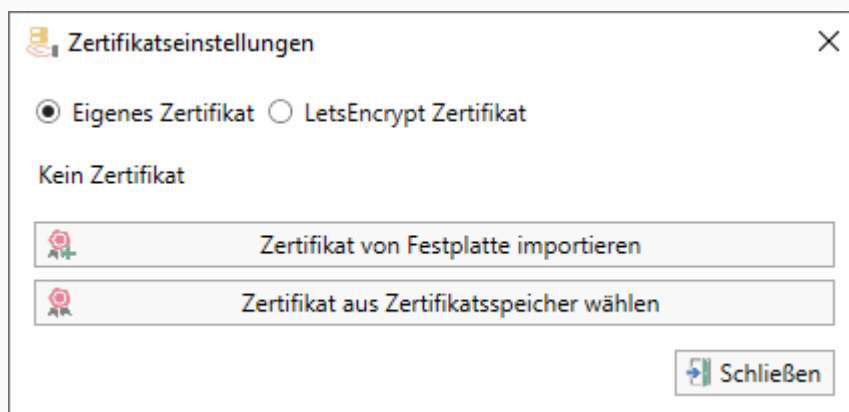
LetsEncrypt-Zertifikate sind kostenlos, haben dafür aber nur eine Gültigkeit von 3 Monaten. Der aBServer-Dienst versucht ab 30 Tage vor Ablauf der Gültigkeit das LetsEncrypt-Zertifikat zu erneuern. Damit der Abruf eines LetsEncrypt-Zertifikats funktioniert, muss der externe Port 80 an den internen hier eingestellten Port weitergeleitet werden.

Zusätzlich schaut der Dienst jeden Tag im Windows-Zertifikatsspeicher nach, ob dort ein aktuelles Zertifikat für die in den Einstellungen hinterlegte Domain gibt. Wenn dem so ist, wird dieses für die Verschlüsselung der API-Zugriffe genommen. So können Sie die Erzeugung eines LetsEncrypt-Zertifikats auch außerhalb unseres Dienstes realisieren bzw. ein gültiges gekauftes Zertifikat im Zertifikatsspeicher importieren.

Im Dialog für die Zertifikatseinstellungen kann man zwischen zwei Optionen wählen:

Eigenes Zertifikat

Hier kann man beispielsweise ein gekauftes Zertifikat in den Zertifikatsspeicher importieren und für den Service nutzen oder ein bereits im Zertifikatsspeicher vorhandenes Zertifikat auswählen.



- **Zertifikat von Festplatte importieren**

Durch einen Klick auf diesen Knopf können Sie ein Zertifikat auf der Festplatte auswählen. Dieses Zertifikat wird in den Windows-Zertifikatsspeicher importiert und an den API-Port gebunden, damit ein verschlüsselter Zugriff stattfinden kann.

- **Zertifikat aus Zertifikatsspeicher auswählen**

Durch einen Klick auf diesen Knopf können Sie ein Zertifikat aus dem Windows Zertifikatsspeicher auswählen. Dieses Zertifikat wird an den API-Port gebunden, damit ein verschlüsselter Zugriff stattfinden kann.

LetsEncrypt Zertifikat

Wählt man diese Option, kann man die für LetsEncrypt benötigten Informationen hinterlegen, damit der Service selbständig ein Zertifikat anfordern und aktualisieren kann.

Zertifikateinstellungen [X]

☐ Eigenes Zertifikat ☒ LetsEncrypt Zertifikat

Kein Zertifikat

E-Mail:

Zertifikatspasswort:

Account-Key:

Account-Key Staging:

Domains: [Add] [Remove]

Port HTTP-Listener: [Firewall]

LetsEncrypt Zertifikat abrufen

Schließen

■ E-Mail

Diese Mailadresse ist benötigt, um bei LetsEncrypt einen Account für die Zertifikatserstellung anzulegen. An diese Mailadresse werden hin und wieder Benachrichtigungen von LetsEncrypt versandt.

■ Zertifikatspasswort

Dieses Passwort wird später für die Verbindung von privatem und öffentlichem Schlüssel des Zertifikats benötigt. Wählen Sie hier ein sicheres Kennwort.

■ Account-Key

Dieser Key wird von LetsEncrypt automatisch vergeben und dient später zur Wiedererkennung des LetsEncrypt Accounts in deren Produktivumgebung.

■ Account-Key Staging

Dieser Key wird von LetsEncrypt automatisch vergeben und dient später zur Wiedererkennung des LetsEncrypt Accounts in deren Testumgebung.

■ Domains

Für die hier eingetragenen Domains gilt das später ausgestellte Zertifikat. Sie können ein LetsEncrypt-Zertifikat für mehrere Domains erstellen, die API läuft aber immer nur für eine dieser Domains.

Rechts neben der Auflistung sind zwei Knöpfe zum Einfügen bzw. Löschen von Domains. Die Domain der API wird schon aus dem Einstellungsfenster übernommen und sollte nicht gelöscht werden, da das später erzeugte Zertifikat sonst nicht für diese Domain gilt.

■ Port HTTP-Listener

An diesem Port horcht unser Service bei der Neuerstellung bzw. Aktualisierung des LetsEncrypt Zertifikats. Von außen muss der Port 80 am Router/der Firewall auf diesen Port weitergeleitet werden.

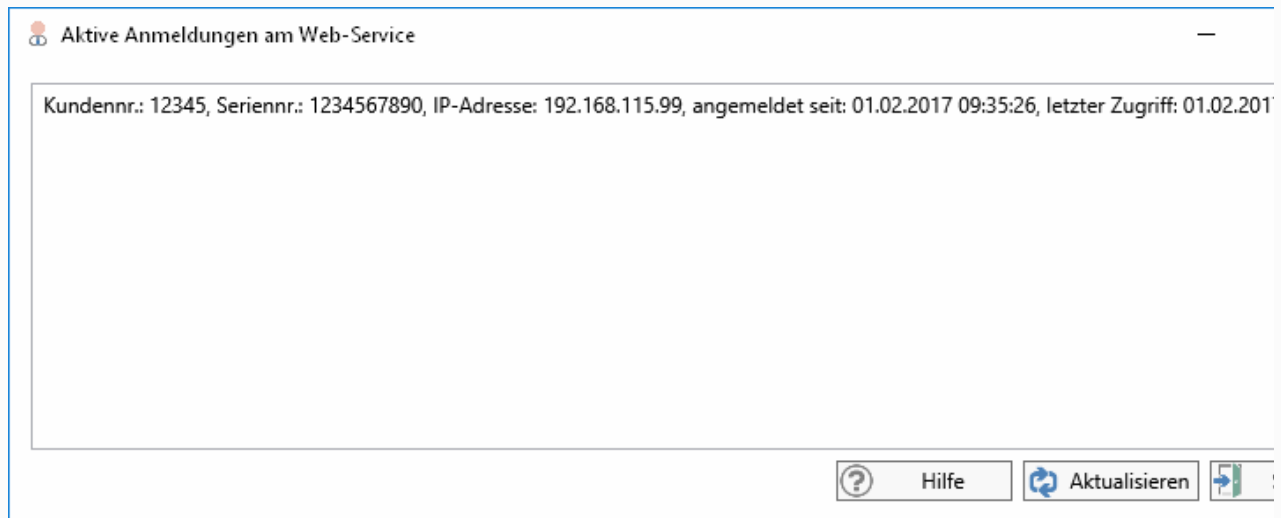
Der kleine Knopf neben der Einstellung sorgt für eine Freigabe des Ports in der lokalen Windows-Firewall. Sollten Sie eine andere Software als Firewall nutzen, müssen Sie dort diesen Port manuell freigeben für eingehende TCP-Verbindungen.

■ LetsEncrypt Zertifikat abrufen

Durch einen Klick auf diesen Knopf wird der Zertifikatsabruf direkt gestartet und man kann sehen, ob der Abruf mit den getätigten Einstellungen erfolgreich durchläuft.

Aktive Anmeldungen am Web-Service

In diesem Dialog können Sie sehen, welche Rechner aktuell am aBServer-Dienst angemeldet sind.



- **Aktualisieren**

Hier können Sie die Prüfung nach aktiven Anmeldungen erneut anstoßen und danach erhalten Sie die aktualisierte Liste der aktiven Anmeldungen.

Server-Modul Anmeldedaten

Um mit aB-Agents eine Remote-Sitzung zu einem aBServer-Dienst aufzubauen (also von einem externen Arbeitsplatz aus), klicken Sie im Applikationsmenü auf **Remote Daten-Ordner öffnen**. Sie gelangen daraufhin zum Dialog **Server-Modul Anmeldedaten**.

In diesem Dialog können Sie die Anmeldedaten für den aBServer-Dienst eingeben. So können Sie sich an diesem Modul anmelden, um die Daten von der Zentrale über eine Internet-Verbindung abzurufen. Voraussetzung hierfür ist die Einrichtung des Server Moduls auf dem Server in der Zentrale und die Freigabe des Datenverkehrs. Die Informationen, mit welchen Daten sie sich am Server Modul anmelden können, müssen Ihnen bekannt sein oder als verschlüsselte Datei vorliegen.

Server-Modul Anmeldedaten

Bezeichnung: Daten Zentrale

Zugangsdaten Voll-Version | Zugangsdaten Demo-Version

IP-Adresse: mustermann.twodns.de

Port: 50000

Windows-Domäne:

Windows-Benutzer: Bernd Gansen

Windows-Kennwort:

Modul-Kennwort:

Daten-Ordner: C:\aB-Agents\Daten

☒ Kennwörter speichern

Buttons: [Up/Down Icons] [Hilfe] [Abbruch] [Ok]

- **Bezeichnung**
Eine Bezeichnung für die Verbindung. Diese Angabe dient der besseren Übersicht und muss nicht ausgefüllt werden.
- **IP-Adresse**
IP-Adresse oder DNS-Name des Servers, auf dem der aBServer-Dienst ausgeführt wird.
- **Port**
Port, auf dem die Anfragen an das Server Modul gestellt werden können. Der Standardwert ist 50000.
- **Windows-Domäne**
Windows-Domäne des Servers. In den meisten Fällen muss diese nicht angegeben werden.
- **Windows-Benutzer**
Windows-Benutzer, mit dem Sie sich am Server anmelden möchten. Dieser Benutzer muss

auf dem Server vorhanden und aktiviert sein.

- **Windows-Kennwort**

Kennwort für den Windows-Benutzer.

- **Modul-Kennwort**

Das Modul-Kennwort des aBServer-Dienstes. Dieses Kennwort wurde bei der [Konfiguration des aBServer-Dienstes](#) eingetragen (Siehe Konfiguration aBServer-Dienst).

- **Daten-Ordner**

Der Daten-Ordner auf dem Server, den Sie öffnen möchten. Dieser Pfad wird aus der Sicht des Servers angegeben. Das heißt, der Pfad muss vom Server aus erreichbar sein.

- **Kennwörter speichern**

Wenn Sie diese Option aktivieren, werden die Kennwörter gespeichert und müssen beim nächsten Mal nicht wieder angegeben werden.

- **Export**

Exportieren der eingetragenen Anmeldedaten in eine verschlüsselte Datei, um diese an Außenstellen weiterzugeben.

- **Import**

Importieren einer verschlüsselten Datei mit den Anmeldedaten. Diese werden dann in die Eingabefelder des Dialogs übernommen.

Konfigurationsbeispiel

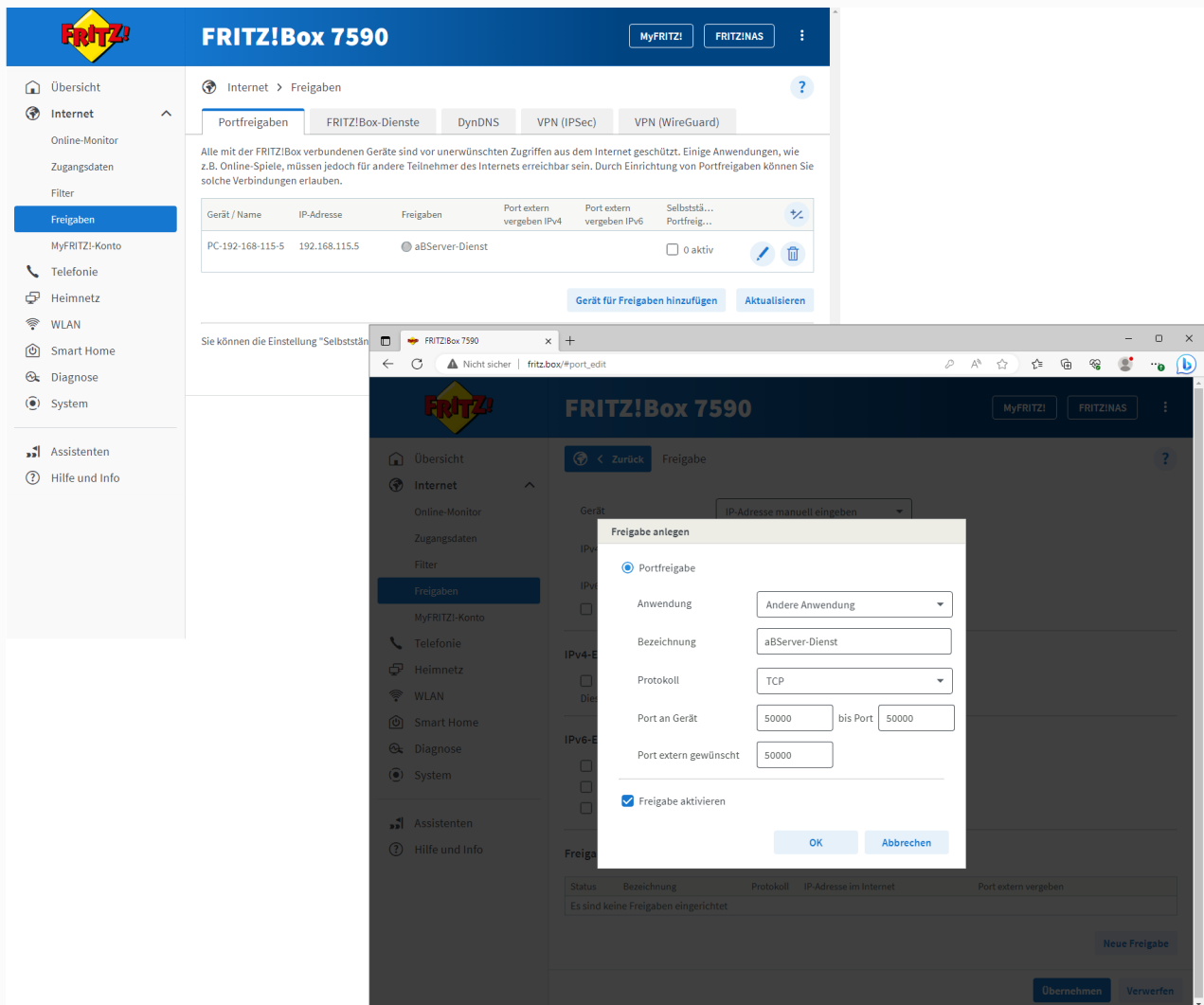
FRITZ!Box 7590

Bei der Konfigurationsoberfläche aktueller Geräte handelt es sich meist um ein sogenanntes Web-Interface, dass über einen Webbrowser aufgerufen wird. Um dieses Interface aufzurufen muss man typischerweise die dem jeweiligen Gerät intern zugewiesene IP-Adresse aufrufen. Die Standard IP-Adresse des Gerätes finden Sie in der Bedienungsanleitung.

Um Ihre Firewall zu konfigurieren, wenden Sie sich bitte an Ihren EDV-Betreuer. Sie können ihm das folgende Beispiele zu Unterstützung vorzeigen.

In diesem Abschnitt wird die Konfiguration der **FRITZ!Box 7590** zur Freigabe des aBServer-Dienstes erläutert. Die Konfigurations-Oberfläche lässt sich über die Adresse <http://fritz.box> im Browser aufrufen.

Die FRITZ!Box 7590 enthält keine Firewall im eigentlichen Sinne. Will man aber Datenverkehr von außen an einen Rechner im Netzwerk weiterleiten, muss man dazu eine Weiterleitung definieren.



Zur Einrichtung der Weiterleitung klicken Sie in der Navigationsleiste links auf

Internet

und wählen dort den Unterpunkt

Freigaben

Sollten für das Gerät bereits Freigaben existieren, klicken Sie rechts daneben auf den Stift zur Bearbeitung der Freigaben. Ansonsten klicken Sie dann unterhalb der Liste der Freigaben auf

Gerät für Freigaben hinzufügen

Sollten Sie ein neues Gerät hinzugefügt haben, geben Sie für das Gerät die entsprechenden Informationen ein:

- **Gerät**

In dieser Liste können Sie den Computer auswählen, auf dem der aBServer-Dienst ausgeführt wird. Sollte der Rechner hier nicht eingetragen sein, können Sie den Punkt manuelle Eingabe der IP-Adresse wählen und geben dann im Feld "IPv4-Adresse" die interne IP-Adresse des Rechners ein

- **IPv4-Adresse**

Hier sieht man die IPv4-Adresse des gewählten Gerätes.

Klicken Sie dann unter der Liste der Freigaben auf **Neue Freigabe**.

- **Anwendung**

"Andere Anwendung"

- **Bezeichnung**

Benutzerdefinierter Name für die Regel. In unserem Beispiel ist der Name aBServer-Dienst.

- **Protokoll**

"TCP"

Die Anfragen für das Server Modul benutzen immer das TCP Protokoll, damit die Anfragen auch auf Transport-Ebene verschlüsselt werden können.

- **Port an Gerät**

"Benutzerdefinierter Port"

Tragen Sie hier den Port ein, den sie bei der Konfiguration des aBServer-Dienstes eingetragen haben. In der Standardkonfiguration ist dies Port 50000. Sie können diesen jedoch auch in der aBServer-Dienst Konfiguration anpassen.

- **bis Port**

gleicher Port wie Port an Gerät

- **Port extern gewünscht**

"Benutzerdefinierter Port"

Tragen Sie hier den Port ein, an dem die Anfragen von außen an der FRITZBox ankommen. Typischerweise ist das der gleiche Port wie intern, in unserem Beispiel also 50000.

Dieser Port ist frei definierbar.