Anleitung für die Installation und Konfiguration des Servers für die CASA24-App

Win-CASA 2022 ermöglicht es Ihnen, mittels iPhone oder Android-App auf Teile von Win-CASA zuzugreifen. Die folgenden Schritte dienen der Server-Einrichtung. Für die Installation und Benutzung der mobilen App verweisen wir auf die Anleitung „CASA24-App“ (s. Homepage).

Software24.com betreibt für den Zugriff einen zentralen Server, der den Datentransfer zwischen App und Ihrem Win-CASA Server (Einzelplatz- oder Netzwerkversion von Win-CASA) vermittelt. Dafür wird die öffentlich zugängliche IP-Adresse Ihres Win-CASA Servers auf dem zentralen Software24.com Server hinterlegt. Die Daten bleiben ausschließlich lokal bei Ihnen und werden direkt und standardmäßig SSL-verschlüsselt zwischen Ihrem Server und der App übertragen.

Um diesen mobilen Zugriff zu ermöglichen, sind folgende Vorarbeiten nötig:

- Der **lokale Win-CASA Server** muss entsprechend lizensiert und konfiguriert werden (Installation und Start des Dienstes für die App) – siehe **„A. Konfiguration des Win-CASA Servers“**
- Das **Netzwerk** muss so eingestellt werden, dass die von der App eingehenden Datenanfragen zum Win-CASA Server weitergeleitet werden. Die geschieht typischerweise mittels Einstellung des Routers oder mittels Lösung über einen Tunnel-Dienst wie ngrok – siehe **„B. Konfiguration des lokalen Netzwerkes**“ bzw**. „C. Alternative ohne Konfiguration des lokalen Netzwerkes: IP-Tunnel, z.B. mit ngrok“**
- Für den **Betrieb** müssen lokaler Win-CASA Server und weitere eventuelle Datenquellen wie Netzlaufwerke eingeschaltet und verfügbar sein.

Diese Anleitung soll erfahrenen Anwendern helfen, die Konfiguration rasch selbst durchzuführen. Bei Problemen wenden Sie sich gerne an unseren Support um festzustellen an welcher Stelle es hakt. Je nach Konfigurationsaufwand und lokaler Netzwerkarchitektur ist ggf. die Hilfe Ihres lokalen IT-Servicetechnikers für die Netzwerk-Konfiguration nach den vorliegenden Spezifikationen nötig. Bitte klären Sie vor Bestellung ab, ob Ihre IT diese Spezifikationen erfüllen kann. Nutzen Sie hierzu die aus der Win-CASA heraus verfügbare 30-tägige kostenlose Testphase (siehe A., p. 3).

A. Konfiguration des Win-CASA Servers

Lizensierung/ Aktivierung

Installation und Aktivierung

1. Webservice
2. Assistent
3. Lokaler Port
4. Windows-Dienst
5. Port für Kommunikation nach außen
6. Checkliste für Netzwerkkonfiguration
7. Verschlüsselungseinstellungen
8. Beenden des Assistenten
9. IP-Adresse und Port Nummer angeben
10. App-Kennwort für Benutzer vergeben

B. Konfiguration des lokalen Netzwerkes (ohne IP-Tunnel wie ngrok)

1. Web-Browser öffnen
2. IP-Adresse des Routers besuchen
3. Warnung
4. Zugangsdaten für Router
5. Port-Weiterleitung konfigurieren
6. IP-Adresse statisch vergeben

C. Alternative ohne Konfiguration des lokalen Netzwerkes: IP-Tunnel, z.B. mit ngrok

1. Installation
2. Entpacken der Zip-Datei
3. Eingabeaufforderung öffnen
4. Ngrok starten
5. URL kopieren
6. URL nach Win-CASA einfügen
7. Hinweise zur Verwendung

Bitte berücksichtigen Sie die Systemvoraussetzungen:

- Win-CASA: Standard-Systemvoraussetzungen (s. Homepage)
- Netzwerk: Konfiguration entsprechend B oder C muss möglich sein um Anfragen der App an den Win-CASA Server weiterzuleiten. Bitte klären Sie dies ggf. mit der lokalen IT-Servicetechnik ab und/ oder nützen Sie den 30-Tage Testzeitraum.
- Mobilgerät: S. Anleitung „CASA24-App“ (Homepage)

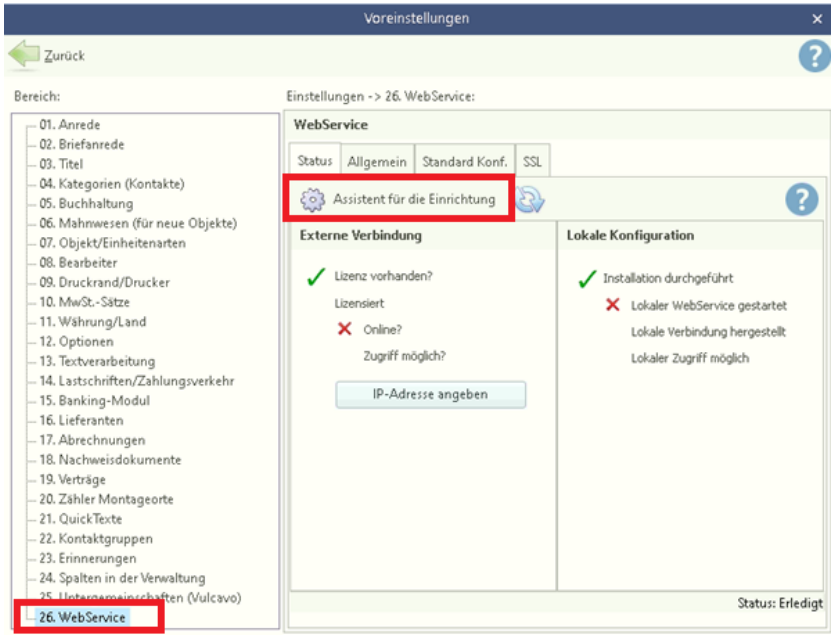
A. Konfiguration des Win-CASA Servers

Lizenzierung/ Aktivierung:

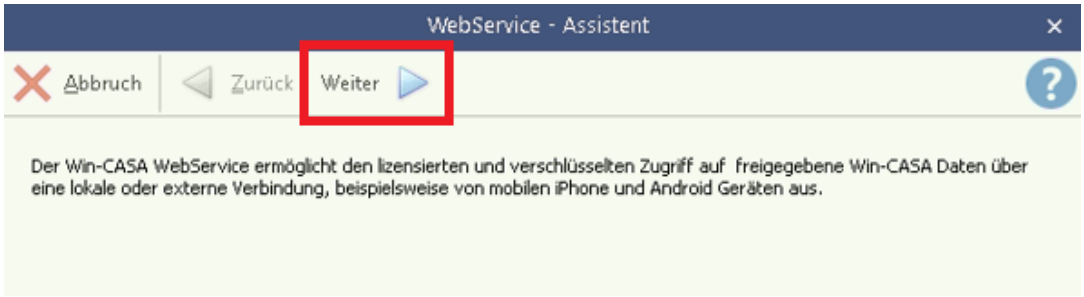
Klicken Sie auf Verwaltung -> Module auf „Casa24 Verwalter-App“. Im erscheinenden Fenster sehen Sie den Status des Win-CASA App-Servers und können die Konfiguration vornehmen. Links sehen Sie, ob eine Lizenz für den Zugriff verfügbar ist. Sie erhalten eine kostenfreie Testlizenz (30 Tage) durch Klick auf „Testlizenz freischalten“. Falls Sie über keine Lizenz verfügen, wenden Sie sich an unseren Support.

Installation und Aktivierung

1. Den Assistenten zur Einrichtung sowie alle Einstellungen und Konfigurationsmöglichkeiten rund um die App und den dazugehörigen WebService finden Sie unter **VERWALTUNG – Objekte & Wohnungen – Einstellungen unter Punkt 26, WebService.**
    a. Links finden Sie den Status der externen Verbindung (Lizenz vorhanden – Online – Zugriff möglich), rechts den Status der Lokalen Konfiguration (Installation des WebService durchgeführt, lokaler Webservice gestartet, lokale Verbindung hergestellt, lokaler Zugriff möglich).
    b. Bei erfolgreicher Konfiguration finden Sie hier grüne Haken
    c. Klicken Sie auf den Button um den Assistenten für die Einrichtung zu starten



2. Nun führt Sie der **Assistent** durch die Einrichtung. Klicken Sie nach Lektüre auf „Weiter“



3. Geben Sie nun einen **lokalen Port** an, auf dem der Win-CASA App-Server laufen soll. Port 9007 ist üblicherweise frei. Sie können mit dem Button „Port testen“ überprüfen ob der Port verfügbar ist. Klicken Sie danach auf weiter.

4. Installieren Sie nun den **Win-CASA App-Server als lokalen Windows-Dienst** mit Klick auf „Weiter“.
    a. Bestätigen Sie auf Anfrage Windows-Administratorrechte.
    b. Falls der lokale Dienst bereits installiert ist, können Sie ihn über diese Maske auch wieder entfernen.

5. Im nächsten Schritt können Sie auswählen über welchen **Port die Win-CASA Kommunikation** nach außen laufen soll. Dies hängt von Ihrer Netzwerk-Konfiguration ab:
    a. Wählen Sie „Standard“ um die Kommunikation über den gewählten Port (z.B. 9007) laufen zu lassen. Dieser muss dann für Zugriff von außen freigegeben sein/ werden. Wir empfehlen diese Option für:
        i. Normale Büro-Netzwerke in denen der Router konfiguriert werden kann. Ein Beispiel zur Konfiguration eines Büro-Netzwerkes mit Router finden Sie unten unter „B. Konfiguration des lokalen Netzwerkes“.
        ii. „Tunneln“ mittels ngrok oder ähnlichem Dienst. Ein Beispiel hierzu finden Sie unter „C. Alternative ohne Konfiguration des lokalen Netzwerkes: IP-Tunnel, z.B. mit ngrok“.
        iii. Alle anderen Netzwerke wo der gewählte Port (z.B. 9007) nach außen freigegeben werden kann

    b. Wählen Sie alternativ „NGINX“ um die Kommunikation über den http- bzw. https-Port (80 bzw. 443) laufen zu lassen. Diese Ports sind üblicherweise in allen Netzwerken geöffnet, da die Anbindung ans Internet über sie läuft.
        i. Diese Option empfiehlt sich bei restriktiven Einstellungen Ihrer Firewall bzw. Ihres Netzwerkes, bzw. wenn keine Möglichkeit besteht den lokalen Port (z.B. 9007) im Netzwerk freizugeben.

ii. Win-CASA installiert und konfiguriert entsprechend das Dienstprogramm „NGINX“ (https://www.nginx.com/) auf Ihrem Server. Dieses dient als „reverse proxy“ dazu, Anfragen an den Win-CASA Server auf den zuvor angegebenen lokalen Port umzuleiten (z.B. 9007).
iii. Die nachfolgende Netzwerkkonfiguration unterscheidet sich leicht von 5.a. (siehe „B. Konfiguration des lokalen Netzwerkes“ 5.c.iii).

6. Bestätigen Sie nun die **Checkliste zur Netzwerkkonfiguration** mit „Weiter“.

Ansicht bei Wahl „NGINX“:

7. Konfigurieren Sie zuletzt die **Verschlüsselungseinstellungen**. Wählen Sie eine der Optionen (empfohlen: Automatisch), klicken Sie auf „**Konfiguration anwenden**“, und dann auf „**Erledigt**“.

   Die Optionen im Einzelnen:

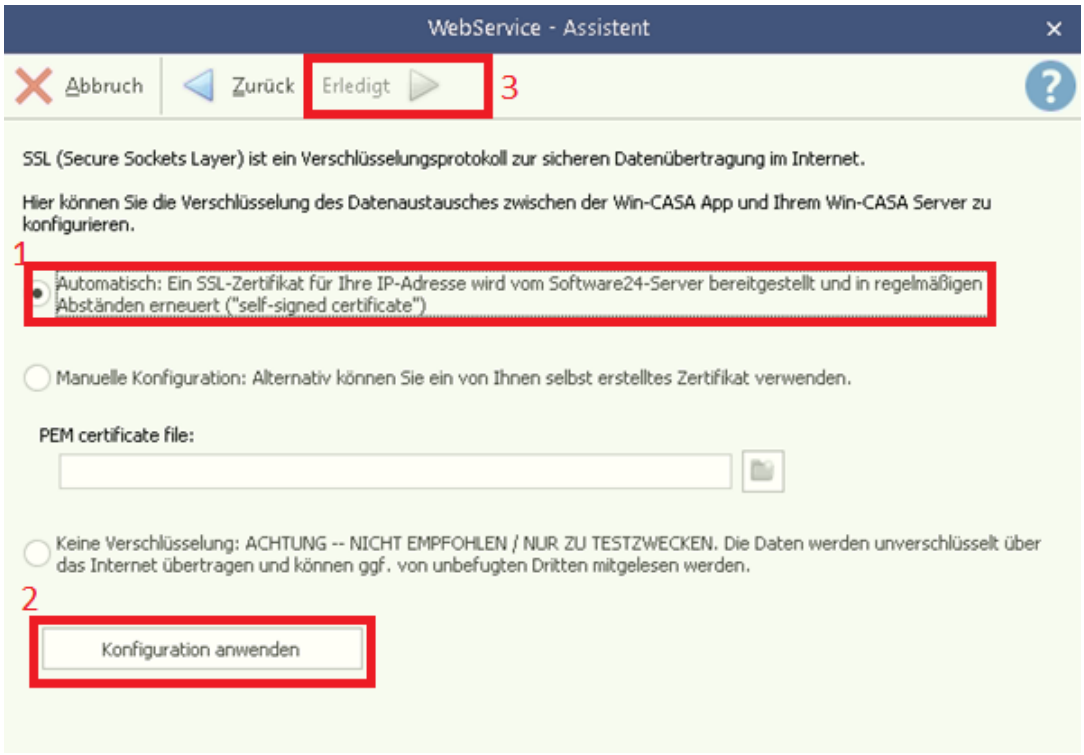
   a. Für viele Kunden empfehlen wir die Datenübertragung mittels automatisch konfiguriertem SSL (secure sockets layer), der Standard-Verschlüsselung zur Datenübertragung im Internet die z.B. auch beim Internet-Banking zum Einsatz kommt. Für Ihr Win-CASA erzeugt der zentrale Software24-Server ein Verschlüsselungszertifikat, das verschlüsselt auf Ihren Server übertragen und in regelmäßigen Abständen automatisch erneuert wird („self-signed certificate“). Wir empfehlen diese Option, wenn Sie:

      i. Auf dem Win-CASA Server kein von einer Zertifizierungsbehörde erzeugtes Zertifikat haben

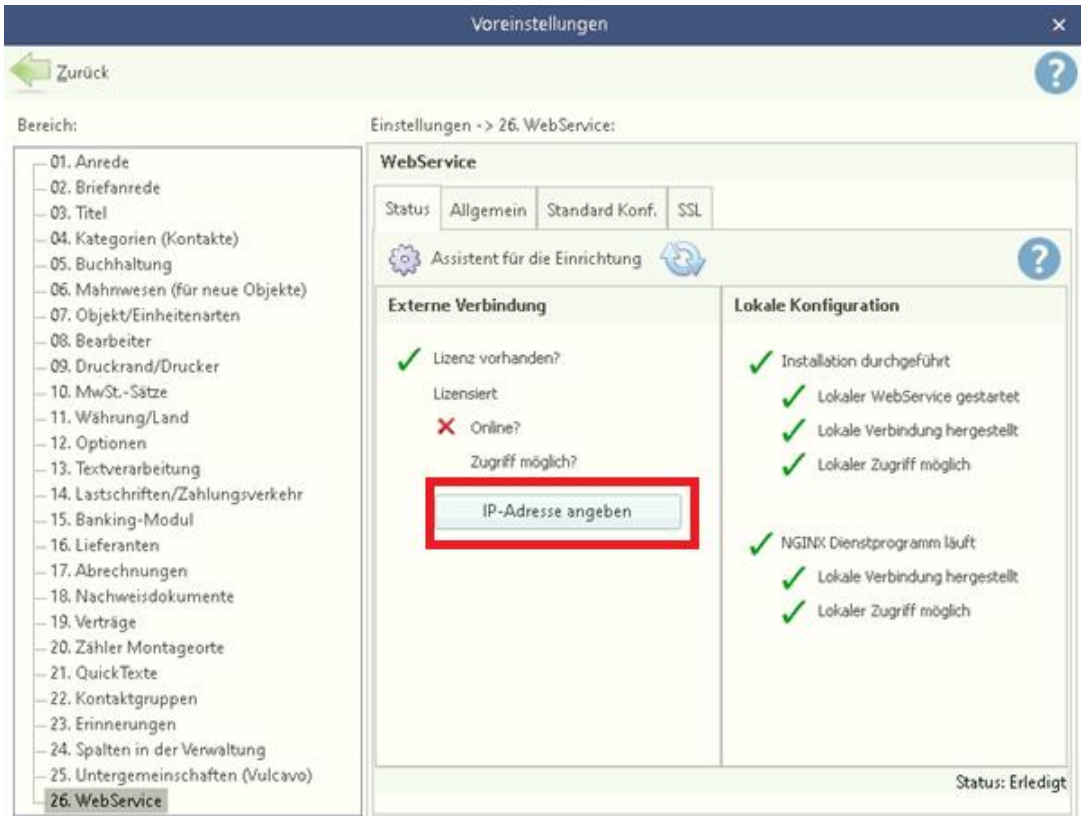
ii. Insbesondere für den Fall dass Ihr Win-CASA Server nicht über eine Domain-URL im Internet erreichbar ist und/ oder nicht über eine statische öffentliche IP-Adresse verfügt

b. Alternativ wählen Sie die Manuelle Konfiguration um ein von Ihnen selbst ausgewähltes Zertifikat (PEM-Datei) zu verwenden. Nutzen Sie dies wenn:
   i. Sie bereits über eine Domain verfügen (www.IheSeite.de) *und*
   ii. Diese Domain bzw. Webseite bereits über ein SSL-Zertifikat (üblicherweise von einer Zertifizierungsbehörde) verfügt *und*
   iii. Ihr Win-CASA Server über diese Domain oder eine Sub-Domain erreichbar ist (hierzu müssen Sie ggf. die entsprechende Konfiguration in Ihren DNS-Einstellungen vornehmen)

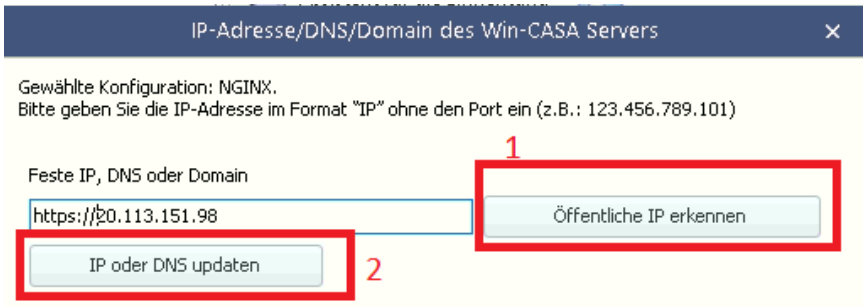
c. **NUR ZU TESTZWECKEN: Keine Verschlüsselung**. Sie haben auch die Möglichkeit, keine Verschlüsselung zu benutzen und die Daten unverschlüsselt über das http-Protokoll zu übertragen. Diese Option kann zur Fehlersuche oder zu Testzwecken hilfreich sein, wir empfehlen sie aber ausdrücklich nicht für den produktiven Betrieb: ***ACHTUNG – Wenn Sie diese Option wählen, könnten die übertragenen Daten ggf. von unbefugten Personen mitgelesen werden!***



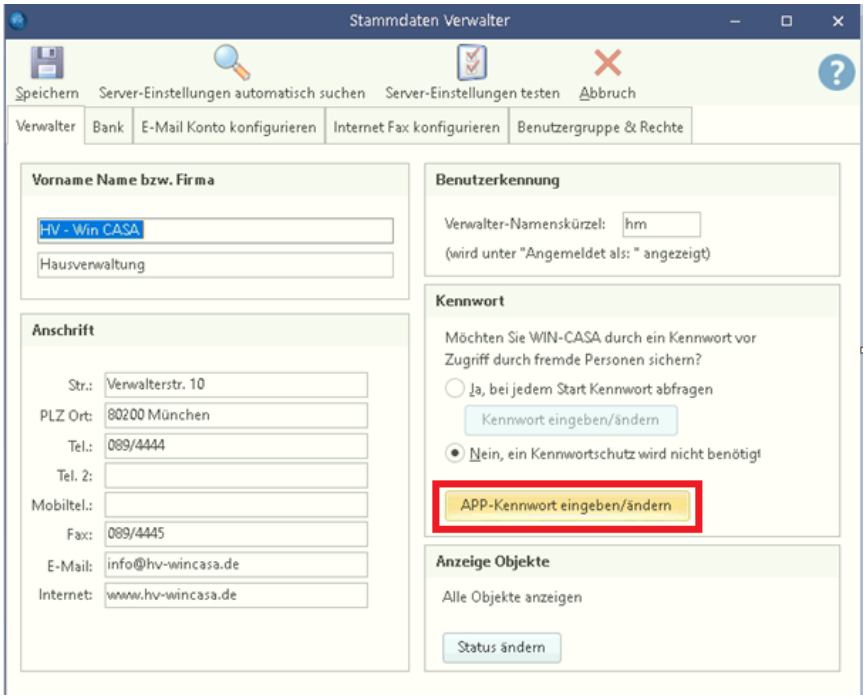
8. Nachdem der Assistent abgeschlossen ist und die Netzwerkkonfiguration durchgeführt wurde, geben Sie bitte die IP-Adresse ein unter der der Win-CASA Server von außen erreicht werden kann. Klicken Sie dazu unter den Einstellungen 26 WebService auf **„IP-Adresse angeben“**



9. Geben Sie nun im erscheinenden Fenster die **IP-Adresse** ein.
    a. Sie können die von außen sichtbare IP-Adresse Ihres Win-CASA Servers mittels Klick auf „Öffentliche IP erkennen“ eintragen lassen
    b. Geben Sie die IP-Adresse im entsprechenden Format ein (wird automatisch vervollständigt):
        i. Wenn Sie NGINX gewählt haben: https://123.456.789.123 bzw. https://www.meinedomain.de
        ii. Wenn Sie die Standard-Konfiguration gewählt haben, fügen Sie bitte entsprechend einen Doppelpunkt und die Port-Nummer hinzu: https://123.456.789.123:9007 bzw. https://www.meinedomain.de:9007
        iii. Falls Sie keine SSL-Verschlüsselung benutzen, ersetzen Sie bitte „https“ durch „http“. **ACHTUNG**: Nur zu Testzwecken, siehe Kommentar in 7c
        iv. Wenn Sie einen Dienst wie ngrok verwenden, geben Sie die entsprechende URL ein (z.B. https://aaab-5-61-129-135.ngrok.io – siehe „C. Alternative ohne Konfiguration des lokalen Netzwerkes: IP-Tunnel, z.B. mit ngrok“)



10. Um die App zu verwenden, müssen Sie für jeden Benutzer ein **APP-Kennwort** zur Identifizierung vergeben haben. Sie können dies in den Stammdaten Verwalter tun (VERWALTUNG – Objekte & Wohnungen – Verwalter – Bearbeiten – Mitarbeiter auswählen und „Mitarbeiter Daten“ klicken – Kennwort: APP-Kennwort eingeben/ändern)



B. Konfiguration des lokalen Netzwerkes (ohne IP-Tunnel wie ngrok)

Die folgende Anleitung gibt einen Eindruck davon, wie die lokale Netzwerkkonfiguration in einem kleinen Büronetzwerk funktionieren kann. Die Details hängen aber vom lokalen Setup und Hersteller des Routers ab.

Das lokale Netzwerk muss so konfiguriert werden, dass:

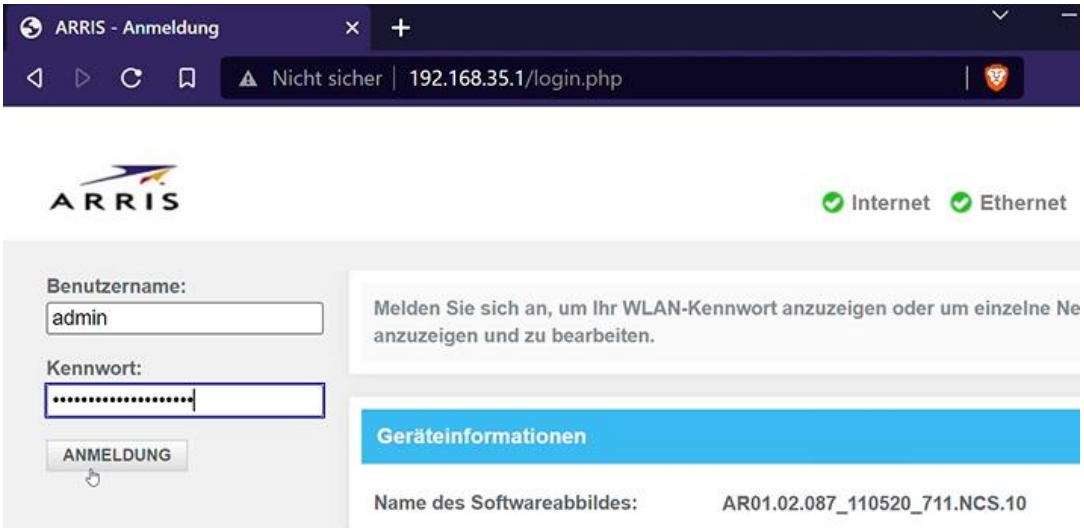
- Der gewählte **Kommunikationsport** (s. Schritt 3, z.B. 9007) **freigeschalten** ist (Firewall-Einstellungen) – dies ist in einem kleinen Büronetzwerk ohne Hardware-Firewall üblicherweise gegeben
- Daten, die an die angegebene **IP-Adresse** geschickt werden (s. Schritt 9) an den Win-CASA Server **weitergeleitet** werden („**Port Forwarding**“) – der Rest der Anleitung bezieht sich hierauf.

1. **Öffnen Sie einen Web-Browser**, beispielsweise Chrome, Firefox, oder Safari

2. Geben Sie die **lokale IP-Adresse Ihres Routers** ein (z.b. 192.168.35.1)
    a. Um die IP-Adresse herauszufinden, öffnen Sie die Eingabeaufforderung (z.B. drücken Sie „Windows-Taste + R“ und geben Sie „cmd“ ein sowie klicken Sie auf „OK“). Geben Sie „ipconfig“ ein und bestätigen Sie mit Enter. Sie finden die IP-Adresse Ihres Routers bei Ihrem W-LAN oder Ethernet-Adapter unter „Standard-Gateway“ / „Default Gateway“.
    b. Alternativ können Sie die häufigsten IP-Adressen ausprobieren: 192.168.1.1 ; 192.168.0.1 ; 192.168.2.1 (z.B. Telekom) ; 192.168.100.1 ; 192.168.1.254 ; 192.168.8.1 ; 192.168.10.1 ; 10.0.0.1 ; „fritz.box“ ; 192.168.160.1
    c. Alternativ können Sie auch der ausführlichen Anleitung hier folgen: https://nordvpn.com/de/blog/router-ip-adresse/

3. Es kann sein, dass Sie eine **Warnung** erhalten dass es unsicher sei, die IP-Adresse Ihres Routers zu besuchen („Ihre Verbindung ist nicht privat“, „Ihre Verbindung ist nicht sicher“, „Diese Webseite ist nicht sicher“, o.ä.). Dies liegt daran, dass für den Zugriff innerhalb Ihres Netzwerkes keine SSL-Verschlüsselung eingerichtet ist. Sie können dies ignorieren indem Sie links unten auf „Erweitert“ klicken und auf „Webseite besuchen“.

4. Geben Sie nun Ihren **Usernamen und Ihr Passwort für den Router** ein.

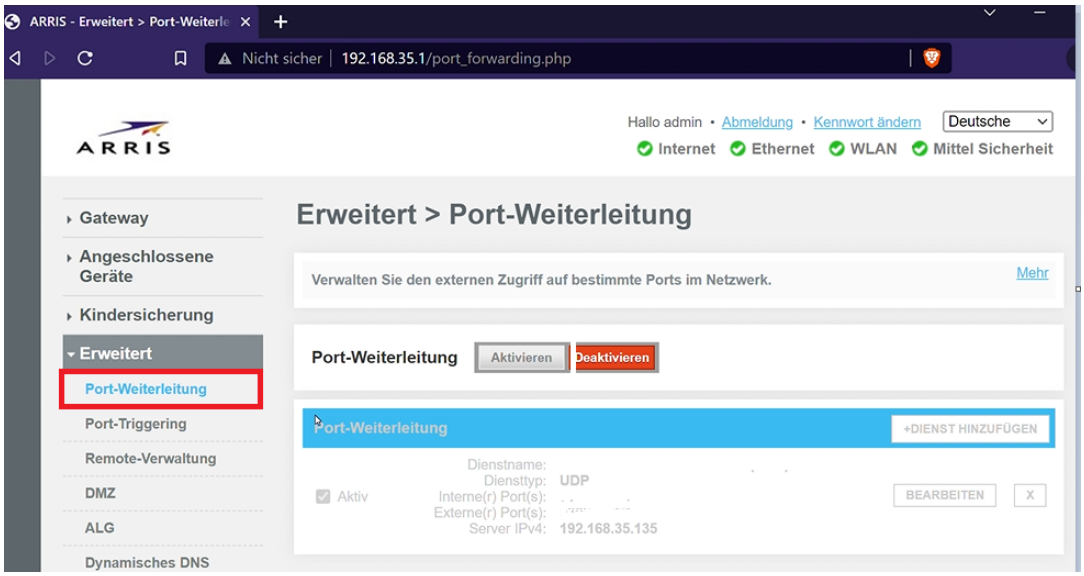


   a. Diese wurden normalerweise bei der Installation Ihres Routers vergeben und notiert
   b. Falls Sie diese nicht (mehr) kennen, versuchen Sie:
      i. Die Informationen auf dem Router zu finden (z.B. auf einem Aufkleber auf der Rückseite oder dem Boden, Beschriftung „Router login“, „Gerätepasswort“, oder ähnlich)
      ii. Falls Sie keine login-Informationen finden, können Sie die folgenden Standard-User und Passwörter probieren:

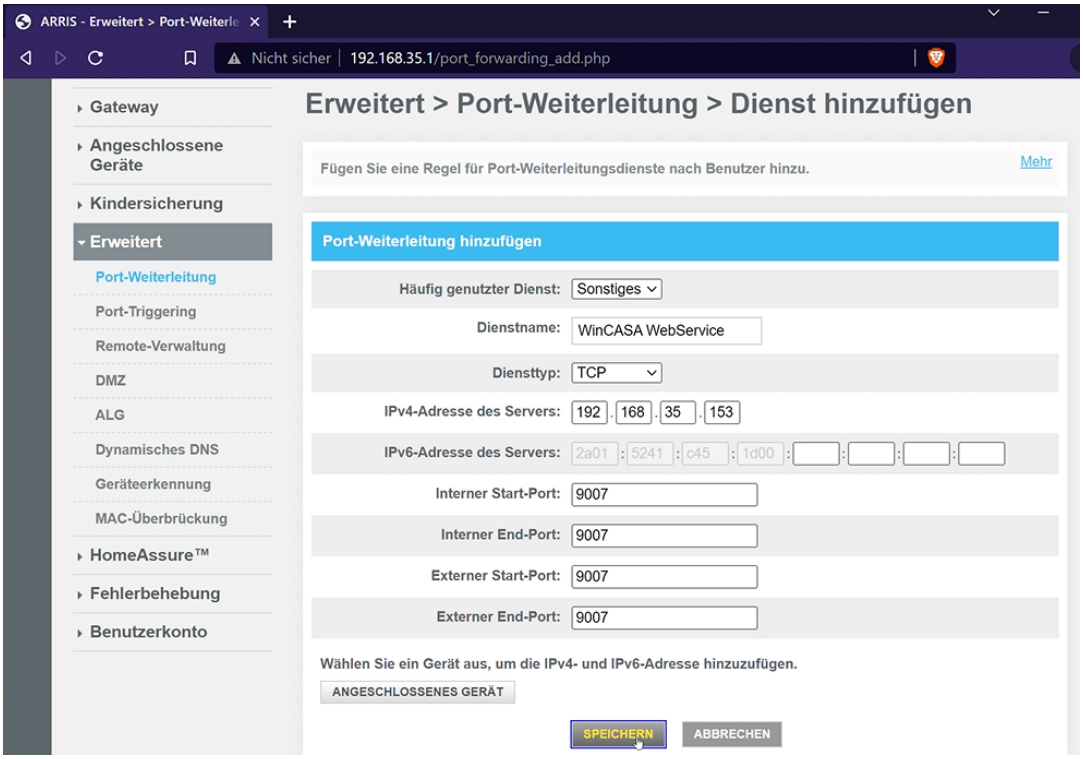
Router-Hersteller	*User*	*Passwort*
- 3Com	admin	admin
- Asus	admin	admin
- Belkin	admin	admin
- Cisco	admin	admin
- Linksys	admin	admin
- Netgear	admin	Password
- TP Link	admin	admin
- D-Link	admin	(leer lassen)

      iii. Wenn Sie die Modellnummer des Routers kennen, können Sie sie via Google suchen oder auf dieser Seite: https://192-168-1-1ip.mobi/default-router-passwords-list/
      iv. Wenn dies alles nicht hilft, findet sich auf den meisten Routern eine Reset-Taste. Wenn Sie diese mehr als 30 Sekunden lang drücken, wird der Router in den Auslieferungszustand zurückgesetzt. Sie können das Passwort verwenden, mit dem der Router ausgeliefert wurde und ihn neu konfigurieren. **ACHTUNG:** die bestehende Konfiguration des Routers wird dadurch gelöscht!

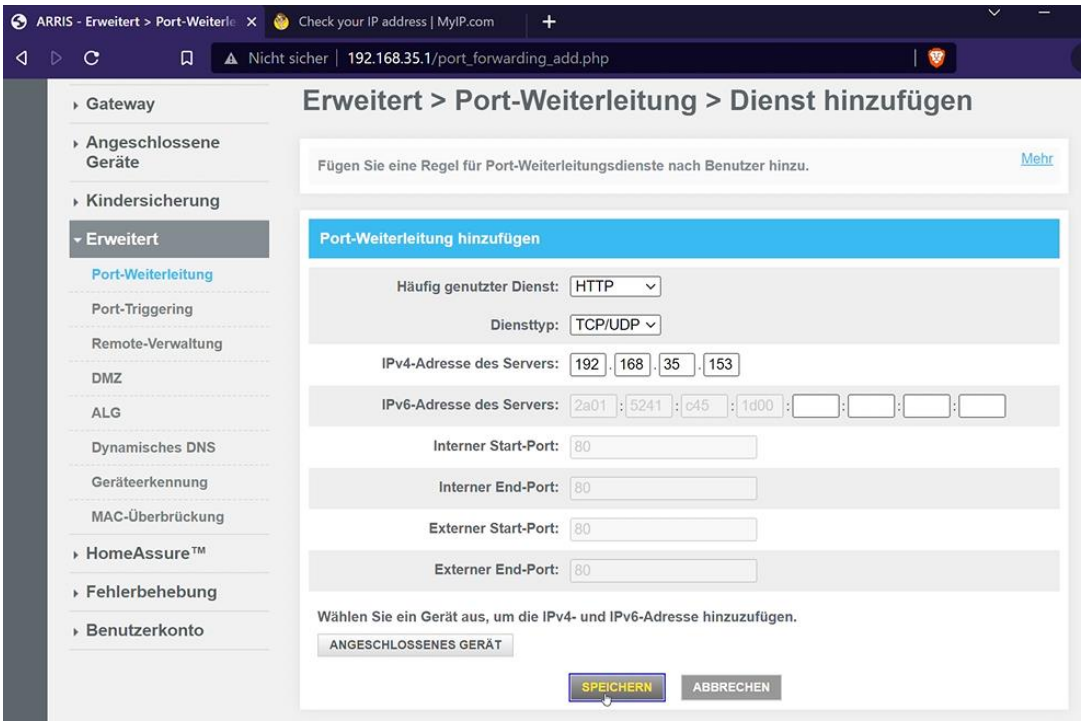
5. Konfigurieren Sie nun die **Port-Weiterleitung**:
    a. Suchen Sie hierzu die ein Menü „Port-Weiterleitung“/ „Port forwarding“. Oft befindet sich dies unter „Erweitert“/ „Advanced“.
    b. Falls die Port-Weiterleitung deaktiviert ist, aktivieren Sie sie



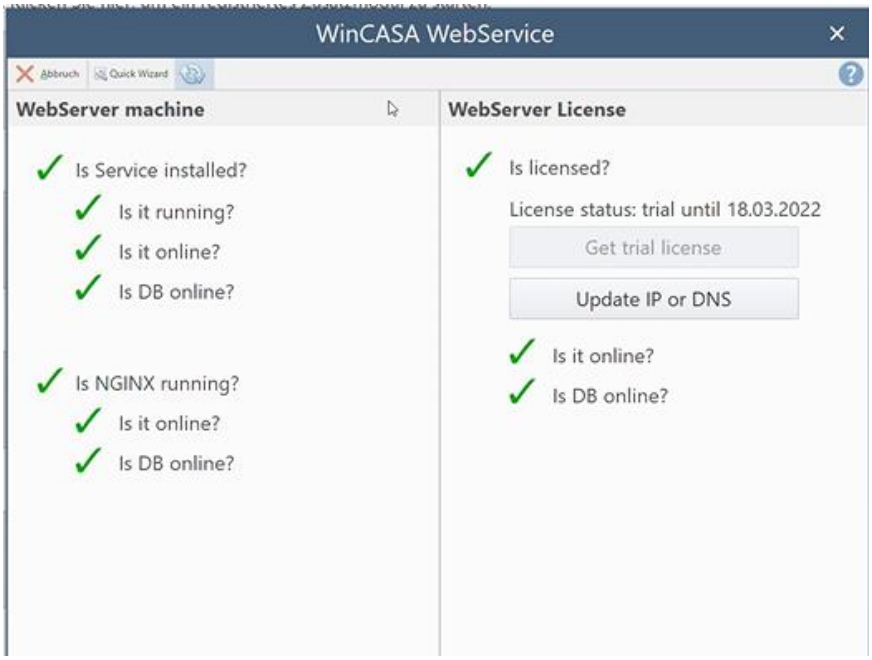
    c. Fügen Sie eine Port-Weiterleitung für Win-CASA hinzu („Dienst hinzufügen“ oder ähnlich).
        i. Finden Sie zunächst die lokale IP-Adresse des Win-CASA Servers heraus. Sie können dies wieder über die Eingabeaufforderung mit „ipconfig“ tun (Eintrag „IPv4-Adresse“). Eine ausführliche Anleitung finden Sie hier: https://www.heise.de/tipps-tricks/IP-Adresse-herausfinden-so-klappt-s-3823461.html
        ii. Wenn Sie die „Standard-“ Konfiguration gewählt haben (unter A.5), wählen Sie einen „sonstigen“ Dienst (kein Standard-Port) über TCP. Geben Sie als „Server“ die statische lokale IP-Adresse des Win-CASA Servers ein (s. voriger Schritt). Geben Sie als Port jeweils den ausgewählten Kommunikationsport (z.B. 9007) ein.



iii. Wenn Sie NGINX gewählt haben (A.5.b), wählen Sie Port 443 bzw. den HTTPS-Dienst. Geben Sie die statisch lokale IP-Adresse des Win-CASA Servers ein.



d. Wenn alles funktioniert hat, sollten Sie nun grüne Haken bei „Online“ vorfinden:



(Falls Sie die Standardkonfiguration A.5.a verwenden, d.h. keine lokale Portweiterleitung mit NGINX benutzen, erscheinen die drei unteren grünen Haken auf der linken Seite nicht.)

6. In vielen WLAN-Netzwerken werden IP-Adressen dynamisch vergeben, d.h., die gerade eingegebene IP-Adresse des Win-CASA Servers kann sich nach Neustart oder Neuanmeldung des Win-CASA Servers im WLAN ändern. In diesem Fall müsste man die obige Konfiguration mit der neuen IP-Adresse wiederholen. Wir empfehlen daher, für den Win-CASA Server eine **feste IP-Adresse zu vergeben**.

    a. Kurzanleitung:
        i. Öffnen Sie ein Explorerfenster.
        ii. Suchen Sie links das lokale Netzwerk (ganz unten).
        iii. Klicken Sie rechts auf „Netzwerk“, dann auf „Eigenschaften“.
        iv. Im erscheinenden Fenster klicken Sie links auf „Adaptereinstellungen ändern“.
        v. Wählen Sie die Netzwerk-Verbindung aus, für die Sie die Einstellungen ändern möchten (also z.B., wenn der Win-CASA-Server via WLAN mit dem Netzwerk verbunden ist, den WLAN Adapter).
        vi. Klicken Sie im erscheinenden Fenster auf „Eigenschaften“, und anschließend auf „Internetprotokoll Version 4 (TCP/IPv4)“.
        vii. Im erscheinenden Fenster ändern Sie „IP Adresse automatisch beziehen“ auf „Folgende IP-Adresse verwenden“. Geben Sie die IP-Adresse des Win-CASA Servers ein (s. Schritt 5.c.i). Subnetzmaske und Standardgateway können Sie auch dem Befehl „ipconfig“ entnehmen (üblicherweise geben Sie bei „Subnetzmaske“ 255.255.255.0 ein, sowie bei „Standardgateway“ die lokale IP-Adresse Ihres Routers (z.B. 168.168.0.1, s. Schritt 2).

    b. Detailliertere Anleitungen finden Sie beispielsweise unter
        i. https://www.giga.de/ratgeber/specials/feste-ip-adresse-vergeben/
        ii. https://www.giga.de/hardware/avm-fritz-box-fon-wlan-7390/tipps/fritzbox-feste-ip-vergeben-so-geht-s/

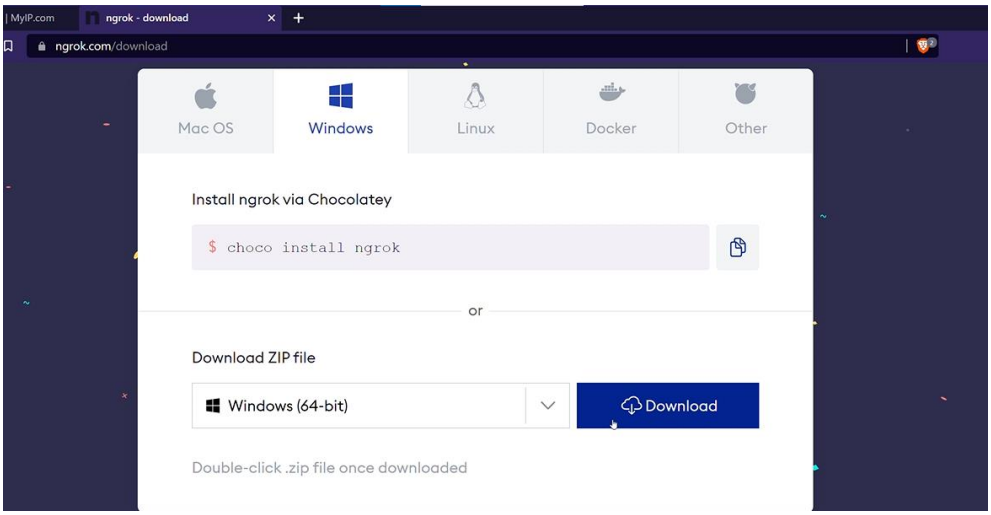
C. Alternative ohne Konfiguration des lokalen Netzwerkes: IP-Tunnel, z.B. mit ngrok

In manchen Fällen kann die obige Netzwerk-Konfiguration für Testzwecke zu umständlich sein, oder kein Zugriff auf das lokale Netzwerk bestehen (z.B. Win-CASA läuft lokal auf einem Laptop im Coworking-Space).

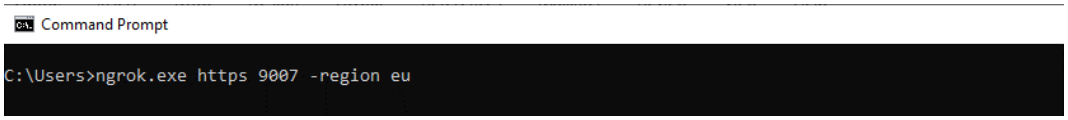
Dann besteht die Möglichkeit einen Dienst zu verwenden, der Anfragen an eine öffentliche IP-Adresse über einen Tunnel auf den Win-CASA Server umleitet („**reverse tunneling**“). Die folgende Anleitung benutzt ngrok (https://ngrok.com/), weitere ähnliche Dienste sind beispielsweise https://expose.dev/ , https://pagekite.net, https://boringproxy.io/, https://loophole.cloud/ (ausführliche Liste hier).

Die Verwendung eines solchen Dienstes führt dazu, dass die Win-CASA Daten zwischen Win-CASA Server und Win-CASA App über den Dienst übertragen werden. Die folgende Anleitung beschränkt sich auf die technische Umsetzung; klären Sie am besten mit Ihrem Datenschutzbeauftragten etwaige weitere Implikationen (z.B. ob ein AV-Vertrag mit dem Anbieter abzuschließen ist oder ob der Anbieter in Ihre Datenschutzerklärung aufzunehmen ist). Stellen Sie auch hier sicher, dass Ihre Daten verschlüsselt über SSL übertragen werden.

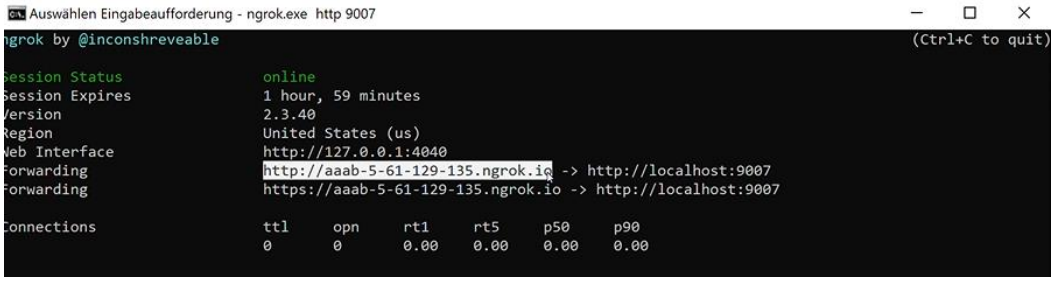
1. Installieren Sie ngrok von https://ngrok.com/download



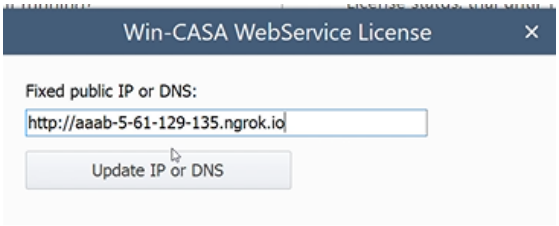
2. Speichern Sie die .zip Datei und entpacken Sie sie (Rechtsklick -> entpacken).
3. Öffnen Sie die Eingabeaufforderung und wechseln Sie in den Ordern der die entpackte ngrok.exe Datei enthält (z.B. „cd C:\Users\JulianeMoller\Downloads\ngrok-stable-windows-amd64“).
4. Starten Sie den entsprechenden ngrok Dienst z.B. über „ngrok.exe https 9007 –region eu“. Hierbei nehmen wir an, dass NGINX nicht verwendet wird (5.a) und dass der gewählte Port für den Win-CASA Server 9007 ist.



5. Markieren und kopieren Sie die angezeigte URL (stellen Sie sicher, keine Leerzeichen am Anfang oder am Ende mit zu kopieren).



6. Kopieren Sie die angezeigte URL in die entsprechende Win-CASA Einstellung. Stellen Sie sicher, dass sie mit https:// beginnt um die SSL Verschlüsselung zu aktivieren.



7. Mit der gratis-Version von ngrok (ohne Anmeldung) bleibt die URL für 2 Stunden gültig und ist auf etwa 20 „Verbindungen“ pro Minute beschränkt. Ein „Klick“ in der App benötigt zwischen 1 und 4 Verbindungen. Entsprechend ist eine testweise Nutzung möglich, eine produktive Nutzung aber ggf. nur eingeschränkt möglich.