

StandBy: Technische vereisten

Vereisten voor het gebruik van de StandBy applicatie(s) met betrekking tot hardware, systeemconfiguraties, koppelingsmogelijkheden, firewalls en connectiviteits vereisten.

Inhoudsopgave

SaaS / Cloud	2
Smartphone & apps	2
E-mails	3
Webapplicatie	3
Beveiligde verbindingen	4
Pushberichten	5
StandBy Android	6
Google Play Services.....	6
Android gebruikers & profielen.....	7
Profielen / Werkprofiel.....	7
Gebruikers ('Android accounts').....	7
Aanwezigheidsdetectie (pand, complex, terrein, etc.)	8
Binnenhuis positiebepaling (hal, zaal, kamer, sector, verdieping, etc.)	9
Aanwezigheids scherm	10
Integratie brandmeldcentrale/installatie	11
Integratie gebouw automatiseringssystemen of gebouwbeheersystemen	13
Portofoon functie	13
Netwerk instellingen.....	13
Browserondersteuning.....	14
Netwerkconfiguratie Voice (VoIP).....	15
Netwerkvereisten.....	16
QR code alarmeren	17
Koppeling met Flic buttons: Flic Hub vereisten	17
Netwerk vereisten.....	18
Vereisten.....	18
Koppeling met Microsoft Azure	19
Koppeling met Microsoft Entra ID (Single Sign On / SSO)	19

SaaS / Cloud

Het volledige StandBy systeem draait in de Cloud (Amazon): U hoeft geen (extra) server te plaatsen of services te installeren binnen uw huidige netwerk.

Alle data in het systeem is opvraagbaar, aanpasbaar en verwijderbaar via een JSON gebaseerde REST API.

Smartphone & apps

De mobiele applicatie van StandBy werkt op apparaten (smartphones en tablets) die draaien op het Android (Google) en iOS (Apple) besturingssysteem (OS):

- Voor Android is minimaal versie 7.0 (Nougat) vereist.
 - Geadviseerd: Minimaal Android 12
 - Zie ook het hoofdstuk '[StandBy Android & Google Play Services](#)' voor aanvullende voorwaarden
- Voor iOS is minimaal versie 13 vereist. Daarnaast dient de hardware een 64-bit processor te hebben: Dit is sinds (en inclusief) de iPhone 5S het geval (de iPhone 5 niet)
 - Geadviseerd: Minimaal versie 14.0
 - Geen ondersteuning voor:
 - iOS 15.0, 15.1 en 15.2 (update naar versie 15.3): Door een fout in het besturingssysteem van Apple werkt de automatische aanwezigheidsdetectie in deze 3 iOS versies niet betrouwbaar..

Smartphones veranderen continue, krijgen nieuwe functies alsook verbeterde beveiliging. Smartphones die binnen de bovenstaande OS versie vereisten vallen, dienen daarnaast te voldoen aan alle onderstaande vereisten. Indien dit niet voor alle smartphones van medewerkers binnen uw organisatie het geval is, kan de compatibiliteit met De BHV App het beste vooraf worden gecontroleerd bij StandBy Solutions:

- De telefoon is in de afgelopen 6 jaar voor het eerst op de markt gebracht in Nederland.
- De telefoon is in de afgelopen 4 jaar nog te koop geweest in een Nederlandse winkel
- De fabrikant van de telefoon ondersteunt de telefoon nog actief (security updates) of heeft dit tot maximaal 2 jaar geleden nog gedaan.

Voor de beste ervaring en werking van StandBy dienen de mobiele apparaten voorzien te zijn van een simkaart met mobiele data connectie ('mobiel internet'). Het is geen harde vereiste, maar wordt wel ten zeerste aanbevolen, zodat (bijvoorbeeld) aanwezigheid updates direct kunnen worden verzonden naar StandBy. Als er geen mobiele data (simkaart) in de telefoon zit, zorgt dit voor een veel slechtere ervaring bij het (automatisch) aan/afmelden van gebruikers. We adviseren dan ook ten zeerste alle telefoons uit te rusten met mobiele data simkaarten.

E-mails

StandBy verzend regelmatig berichten naar gebruikers om ze te informeren over gebeurtenissen in het systeem. Eén van de belangrijkste e-mails voor een vlotte start van het gebruik van StandBy is de account activatie e-mail, maar daarnaast kunnen gebruikers o.a. ook e-mails ontvangen over: vergeten wachtwoord opvragen/resetten, bevestiging (of herinnering) van uitloggen in de app, alarmeringen, interne berichten, beveiligingswaarschuwingen (account blokkade). Beheerders/teamleiders kunnen daarnaast aanvullende e-mails ontvangen, waaronder meldingen over bezettingstekorten.

Om te zorgen dat uw medewerkers alle e-mails van StandBy ontvangen dient u te zorgen dat **alle (digitaal ondertekende) e-mails van @standbysolutions.nl en @standby-app.nl worden afgeleverd in de mailbox van uw medewerkers**. Standaard verzend StandBy berichten namens no-reply@standbysolutions.nl of support@standbysolutions.nl, maar andere adressen kunnen in de toekomst eveneens worden gebruikt. Alle e-mails zijn SPF en DKIM ondertekend en worden verzonden via Amazon SES (eu-west-1.amazonses.com)

E-mails dienen onaangepast en in originele staat aan de eindgebruiker te worden afgeleverd. E-mail berichten kunnen (externe) links, afbeeldingen en/of bijlagen bevatten. Als absoluut minimum dienen klikbare URL's in de e-mails naar *.standbysolutions.nl en *.standby-app.nl te worden toegestaan (hoofd- en subdomeinen).

Webapplicatie

De webapplicatie werkt op alle bekende besturingssysteem en browsers. (Windows, Apple, Ubuntu, Chrome, Firefox, Safari, Internet Explorer). Javascript dient ingeschakeld te zijn om gebruik te maken van de webapplicatie. Momenteel ondersteunen we de meest recente versies van de browsers Google Chrome, Microsoft Edge en Firefox (tot maximaal 6 maanden oud).

Voor het gebruik van de webapplicatie dienen in ieder geval de volgende hostnames/domeinen bereikbaar te zijn via het internet:

- *.standbysolutions.nl
- *.standby-app.nl
- fonts.googleapis.com
- fonts.gstatic.com

Let op: Het [aanwezigheidsscherm](#) is ook onderdeel van de webapplicatie. Voor het gebruik van het aanwezigheidsscherm (in bijvoorbeeld een narrowcasting systeem) gelden dezelfde vereisten.

Beveiligde verbindingen

Om beveiligde verbindingen op te kunnen zetten, zowel via de mobiele apparaten als de webapplicatie, dient poort 443 open te worden gezet voor uitgaande verbindingen in de firewall, wanneer de gebruikers verbonden zijn met een lokaal (bedrijfs)netwerk (ethernet, WiFi) van uw organisatie.

Pushberichten

Voor een juiste en snelle werking van pushberichten op Android en iOS apparaten (o.a. voor alarmeren), dient het bedrijfsnetwerk in de firewall toegang toe te staan voor uitgaand verkeer op de volgende poorten:

- *Android FCM (Firebase Cloud Messaging) ([source](#)):*
 - *For incoming messages (outside network -> in network): FCM typically uses port 5228, but it sometimes uses 5229 and 5230.*
 - *For outgoing connections (in network -> outside network), one of these (option #1 is preferred):*
 - i. *No IP restrictions on port 5228-5230*
 - ii. *All IP addresses contained in the IP blocks listed in Google's [ASN of 15169](#). Don't forget to update this at least once a month.*
 - *NAT: If your network implements Network Address Translation (NAT) or Stateful Packet Inspection (SPI), implement a 30 minute or larger timeout for our connections over ports 5228-5230. This enables us to provide reliable connectivity while reducing the battery consumption of your users' mobile device.*
- *Apple's iOS (Apple Push) ([source](#))*
 - *2195 TCP Apple Push Notification Service (APNS) - Push notifications*
 - *2196 TCP Apple Push Notification Service (APNS) - Feedback service*
- *Windows Phone (Windows Phone Push) ([source](#))*
 - *Port 80 en 443 (http en https):*

```
<CloudServiceDNS>
  <DNS FQDN="*.notify.windows.com" />
</CloudServiceDNS>
<ClientDNS>
  <DNS FQDN="*.wns.windows.com" />
  <DNS FQDN="*.notify.live.net" />
</ClientDNS>
```
 - *"If possible, we strongly suggest allow listing by FQDN as these will not change. If you whitelist by FQDN, you do not need to also whitelist the IP address ranges."*

De meeste (thuis)netwerken staan uitgaand verkeer standaard op alle poorten toe (verkeer van binnen

naar buiten). Corporate/Enterprise netwerken kunnen echter strikter zijn afgesteld, controleer daarom altijd of bovengenoemde poorten open staan (van binnen naar buiten). Voor betrouwbare en snelle aflevering van push berichten (o.a. alarmeringen) is het van belang dat deze configuratie wordt gerespecteerd.

StandBy Android

Google Play Services

De StandBy Android applicatie maakt gebruik van diensten (API's) die worden aangeboden via Google Play Services: een framework voor extra functionaliteiten op Android telefoons.

Telefoons met de Google Play Store ('app winkel') kunnen in bijna alle gevallen ook het Google Play Services framework downloaden en installeren. Vrijwel alle consumenten telefoons (en tablets) in Nederland hebben deze software al voorgeïnstalleerd (Google Play Store en Google Play Services).

Indien Google Play Services niet is geïnstalleerd kan bepaalde functionaliteit niet beschikbaar zijn in de StandBy applicatie. Een concreet voorbeeld hiervan is de aanwezigheidsdetectie op basis van geofencing. Deze 'geofencing' dienst wordt aangeboden op de telefoon door middel van het Google Play Services framework, zonder het framework werkt deze functie dus niet. Als alternatief kan er gebruik worden gemaakt van aanwezigheidsdetectie op basis van WiFi detectie.

Installatie van de StandBy Android applicatie zonder Google Play (Services) kan niet worden gegarandeerd.

LET OP: Sinds 16 mei 2019 zijn de vereiste Google Play Services **niet meer beschikbaar op nieuw uitgebrachte Huawei telefoons**. Dit is het gevolg van Amerikaanse sancties tegen Huawei. Lees [hier de volledige uitleg van Google](#) over deze sancties en de gevolgen voor de diensten van Google op deze telefoons.

Sommige Huawei telefoons zullen in de praktijk nog steeds kunnen werken met de StandBy app, maar er is geen mogelijkheid om officiële ondersteuning te bieden. Per type/model telefoon zijn er verschillen in (on)mogelijkheden en door de maatregelen is niet op voorhand te zeggen welk apparaat wel of niet zal werken. Zo kan het voorkomen dat op de éne Huawei telefoon alle modules werken, terwijl op een ander model Huawei telefoon de aanwezigheidsdetectie (geofencing) of het ontvangen van alarmeringen (push berichten) niet werkt.

Android gebruikers & profielen

Profielen / Werkprofiel

Het is mogelijk om de StandBy app (in één user account) in een (werk)profiel te installeren en gebruiken. Houdt er rekening mee dat gebruikers hiermee een grote(re) verantwoordelijkheid krijgen om werk-apps niet te pauzeren of op tijd weer in te schakelen. Als de werk-app in pauze modus blijft staan, kan er niet worden gegarandeerd dat alarmeringen aankomen en aanwezigheidsdetectie correct blijft werken.

We adviseren sterk om de pauze modus niet te gebruiken als de StandBy app binnen het werkprofiel wordt geïnstalleerd.

De permissie 'Voorkomen dat toestemmingen automatisch worden ingetrokken' is normaliter vereist voor het gebruik van de StandBy app. Bij het gebruik van een werkprofiel komt deze vereiste te vervallen omdat het werkprofiel wordt beheerd door uw IT-beheerder en permissies niet automatisch na enige tijd inactiviteit (kunnen) worden ingetrokken. (Let op: Deze vereiste is vervallen vanaf StandBy app versie 2.34.5 en nieuwer)

Gebruikers ('Android accounts')

De StandBy app op Android werkt uitsluitend als deze binnen één gebruikersaccount ("[user](#)") wordt geïnstalleerd en gebruikt. Het is niet mogelijk om een tweede gebruiker ("[secondary user](#)") toe te voegen en de StandBy app daar te installeren.

Hoewel de StandBy app kan worden geïnstalleerd en de gebruiker kan inloggen, werkt de functionaliteit niet (betrouwbaar). Als de gebruiker wisselt naar een andere 'user' op de Android telefoon, stoppen de belangrijkste modules van de StandBy app met functioneren: De locatie van de gebruiker wordt niet meer gemonitord (geen aanwezigheidsdetectie) en de gebruiker ontvangt geen alarmeringen meer, ook geen hoge prioriteit alarmering. Alarmeringen komen pas weer aan als de gebruiker naar de Android 'user' wisselt waar de StandBy app in is geïnstalleerd. Dit gebeurt zowel als het eerste ('system user') en/of een tweede 'user' account wordt gebruikt. Beide gevallen worden niet ondersteund, er dient altijd maar één 'user' in het Android OS te worden gebruikt. Standaard worden telefoons geïnstalleerd met maar één Android 'user' account.

Om bovenstaande redenen kan de StandBy app het gebruik van meerdere Android 'users' niet ondersteunen en raden we ten eerste af de app op deze manier te gebruiken.

Aanwezigheidsdetectie (pand, complex, terrein, etc.)

Voor aanwezigheidsdetectie van zogeheten 'hoofdlocaties', zoals bijv. een gebouw, complex of terrein, wordt er gebruik gemaakt van gebiedsbewaking (ook wel 'geofencing' genaamd):

Bij geofencing wordt er (automatisch en gecombineerd) gebruik gemaakt van WiFi, GSM en GPS signalen van de smartphone om op energiezuinige en zo accuraat mogelijke wijze de locatie van de gebruiker te bepalen. De applicatie bepaalt vervolgens of de gebruiker binnen de 'geofence' is of niet. Een geofence is een virtuele cirkel op de kaart rond de werkplek(ken). Als een gebruiker hier binnen komt met de telefoon, wordt diegene als aanwezig gedetecteerd, als je er buiten bent, is de gebruiker afwezig.

Specificaties en vereisten voor het gebruik van geofences:

- Rond iedere hoofdlocatie ligt een geofence cirkel met een minimale radius van 120 meter. Er is geen beperking op hoe groot de geofence mag worden.
- Er dient minimaal 300 meter tussen de middelpunten van 2 hoofdlocaties te zitten (ze mogen dus niet té dicht bij elkaar liggen).
 - Voorbeeld: Beide cirkels zijn 120 meter groot, dat maakt al een totale afstand van 240 meter, dan moet er dus nog minimaal 60 meter tussen de randen van deze 2 cirkels zitten.
- Indien de locaties 'net niet' naast elkaar passen is het altijd mogelijk om hiervoor een controle aan te vragen bij StandBy Solutions. Afhankelijk van de tussenliggende afstanden, de werklocatie en succesvolle resultaten uit een test kunnen de locaties mogelijk dichterbij elkaar.
 - Waarom moet dit gecontroleerd worden? Bepaalde gebouwen en locaties kunnen een probleem zijn voor de nauwkeurigheid van het vaststellen van de huidige locatie door smartphones. Denk hierbij aan een hoge toren, een grote hal, een gebouw met veel staal of heel goede isolatie, een gebouw in dichtbevolkt gebied, etc. Als na een test blijkt dat er geen sprake is van negatieve effecten, kunnen locaties nog iets dichterbij elkaar worden geplaatst.
 - De geofence cirkel kan na bovenstaande controle worden teruggebracht tot een minimum van 100 meter radius per cirkel (in plaats van 120).
 - Indien er meerdere geofence cirkels dichtbij elkaar liggen, dient er -na de controle- nog steeds 50 meter tussen de 2 randen van de cirkels te zitten (middelpunten 250 meter van elkaar).
- Locaties die te dicht bij elkaar liggen worden binnen StandBy als één grote (gecombineerde) locatie geregistreerd.

Binnenhuis positiebepaling (hal, zaal, kamer, sector, verdieping, etc.)

Voor binnenshuis positiebepaling (indoor localization) kan gebruik worden gemaakt van...

1. ... netwerk identificatie nummers: BSSID's (de unieke nummers van WiFi access points).
Om deze functie te gebruiken is het vereist dat de BSSID's kunnen worden geëxporteerd uit uw netwerksysteem. Indien dit niet mogelijk is kunt u zelf (of als dienstverlening door StandBy) uw bedrijfslocatie(s) laten scannen en voorzien van locatielabels. BSSID's worden openbaar uitgezonden en kunnen daardoor ook zonder centraal netwerkmanagementsysteem worden verzameld.
2. ... beacons: os verkrijgbare hardware die verspreid door het gebouw wordt geplaatst. Beacons werken op basis van Bluetooth Low Energy onafhankelijk van het (bedrijfs)netwerk en kunnen direct in het stopcontact worden geprikt, achter het stopcontact worden ingebouwd of ergens los worden geplaatst met een batterij.

Detectie obv beacons (#2) werkt op Android vanaf OS versie 4.3 en op iOS vanaf versie 9.0. Zowel Android als iOS apparaten dienen tevens over Bluetooth Low Energy hardware te beschikken. Bij Apple's iPhone's is dit het geval vanaf de iPhone 4S, voor Android verschilt dit per device.

Aanwezigheids scherm

Voor het plaatsen van een aanwezigheidsscherm met hierop informatie over welke personen momenteel op een locatie aanwezig zijn kan gebruik worden gemaakt van de 'Aanwezigheidsscherm' module.

StandBy biedt de mogelijkheid om op apparaten [met een webbrowser en internetverbinding](#) het 'aanwezigheids scherm' te tonen. Dit werkt op basis van een URL die kan worden gegenereerd in de beheerders webapplicatie. De URL kan worden gebruikt op een laptop, die bijv. is gekoppeld aan een externe monitor - of de URL kan worden ingeladen binnen een narrowcasting systeem

Om te controleren of de betreffende (ingebouwde) browser/het narrowcasting systeem voldoet aan de technische vereisten kan als test de volgende URL worden ingeladen:

- <https://misc.standbysolutions.nl/~jordi/standby-browser-engine-test/>
- Of: <https://standbysolutions.nl/testaanwezigheidsscherm> (het ~ teken kan problemen geven bij toetsenborden op TV schermen)
- De drie bovenste items moeten alle 3 groen worden om het aanwezigheidsscherm te kunnen inladen. Als deze niet groen worden, is de browser technisch gezien niet geschikt voor het tonen van het aanwezigheidsscherm.
- Iedere functie in de lijst eronder moet een 'CHECK!' bevatten. Indien dit niet het geval is, kan het resultaat worden gedeeld met StandBy support om te controleren wat het probleem is en of er nog mogelijkheden zijn om het aanwezigheidsscherm op dat systeem te tonen.

Op het gebruik van de URL in een eigen (narrowcasting) systeem is een 'fair use policy' van toepassing: **De URL is bedoeld op maximaal één keer per dag ingeladen te worden (zodra het scherm aan gaat)**, daarna dient de URL niet meer te worden ververs. De webapplicatie zorgt er zelf voor dat de gegevens op het scherm actueel blijven (automatische verversing).

Een eventueel extern (narrowcasting) systeem mag dus **niet** voor iedere keer dat het aanwezigheidsscherm op een fysiek scherm wordt vertoond, de pagina volledig opnieuw inladen. Deze moet op de achtergrond actief blijven (gedurende het vertonen van andere 'slides' op het narrowcasting systeem) zonder dat de aangeleverde URL opnieuw wordt ingeladen.

Indien een narrowcasting systeem onjuist is geconfigureerd (zoals het constant verversen van het volledige StandBy aanwezigheidsscherm) heeft StandBy het recht om de verbinding (tijdelijk) te verbreken totdat de configuratie is aangepast.

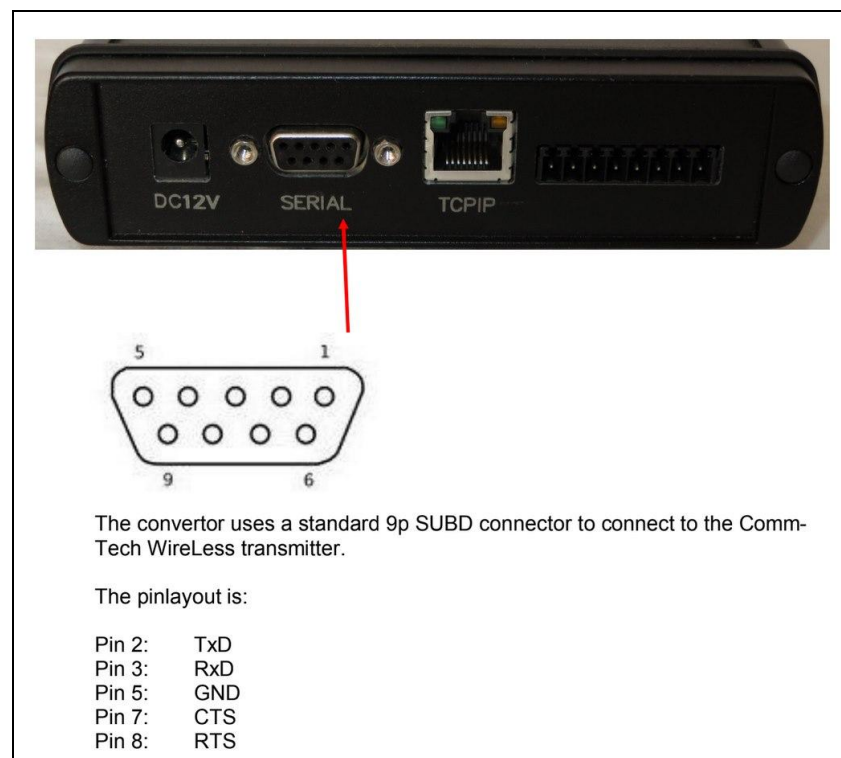
Integratie brandmeldcentrale/installatie

Integratie met BMC/BMI is mogelijk wanneer deze beschikt over een vrije ESPA kaart voor ESPA 4.4.4 (standaard)

Daarnaast moet er de mogelijkheid zijn om binnen max. 5 meter van de centrale een ESPA-IP converter (ESPA IP converter wordt geleverd door StandBy) te plaatsen. De IP converter dient tevens bekabeld verbinding te kunnen maken met het internet (ethernet kabel) en een stroompunt (standaard stopcontact). Deze moeten dus allemaal bij elkaar in de buurt beschikbaar zijn, op de plek waar de ESPA-IP converter zal worden geplaatst. Meestal is dit de ruimte waarin de BMC installatie staat (technische/server ruimte).

De IP converter wordt geleverd met stroomadapter (voor in het stopcontact) en een seriële Sub D 9 pins adapter. De ethernetkabel en de seriële kabel zelf (tussen de ESPA kaart en StandBy IP converter) dienen al aanwezig te zijn en deze worden niet door StandBy meegeleverd. Op de seriële poort van de IP converter dient een mannelijke SUB D9 aansluiting te worden aangesloten. (zie afbeelding hieronder)

In onderstaande linker afbeelding kan de 9-pins configuratie van de seriële poort obv RS232 op de BMC IP Converter worden afgelezen. Deze pin indeling moet in de kabel tussen de BMC en de IP converter kloppend worden gemaakt. Indien de ESPA kaart op de BMC (nog) niet deze pin indeling gebruikt, zorg dan dat de aansluitingen volgens de specificatie worden aangesloten.



- E: support@standbysolutions.nl - W:

De beschikbare ethernetkabel (met RJ45 aansluiting voor op de IP converter) moet verbinding kunnen maken met het internet (DHCP enabled). De StandBy IP converter maakt verbinding met de StandBy Alarmserver over poort 7450 (let op: Dit is dus niet de veelgebruikte internet poort 80 [HTTP] of 443 [HTTPS]). De netwerkbeheerder dient te zorgen dat de StandBy IP converter niet voor andere gebruikers binnen het netwerk te benaderen is (black/whitelisting en/of op een eigen vlan).

De IP converter maakt verbinding met de StandBy BHV App cloud op het IP:

- IP: 54.72.66.167
- Poort: 7450

Standaard maakt de IP converter gebruik van DHCP. Een static IP is ook mogelijk: Dit dient vóór de levering van de BMC IP Converter kenbaar te worden gemaakt bij StandBy Solutions zodat dit kan worden geconfigureerd vóór de installatiedatum op locatie. Stuur in dit geval het gewenste statische IP adres mee.

Voor de IP converter is een stabiele verbinding belangrijker dan een snelle verbinding. Er is in de praktijk weinig data nodig om de koppeling mogelijk te maken. Zorg dat de gebruikte internetlijn minimaal 5Mb/s bandbreedte voor up- en download heeft.

De IP converter wordt standaard opgeleverd met onderstaande configuratie. Aanpassingen hieraan zijn mogelijk (indien de brandmeldcentrale een andere configuratie heeft) en dienen vooraf te worden gecommuniceerd:

- Port: ESPA 4.4.4
- Serial speed: 9600 baud
- Bits: 8 bits
- Parity: None
- Stopbits: 1 bit
- Handshake: None

Integratie gebouw automatiseringssystemen of gebouwbeheersystemen

Integratie met gebouwbeheersystemen is mogelijk door middel van een software koppeling. Hiervoor biedt StandBy Solutions een API.

Portofoon functie

Netwerk instellingen

Voor het gebruik van de portofoon functie dient het (WiFi en/of mobiele data) netwerk te worden gecontroleerd op diverse configuraties:

Netwerk configuratie: Het netwerk dient websocket verbindingen toe te staan. De firewall mag langdurige websocket verbindingen niet sluiten/blokkeren.

Spraak communicatie:

Netwerk test van Twilio: <https://networktest.twilio.com/?edge=dublin>

Deze online tool, die moet worden uitgevoerd vanaf het te gebruiken (bedrijfs / WiFi)netwerk, heeft ongeveer 2-5 minuten nodig om een volledige netwerktest uit te voeren. Eventuele foutmeldingen dienen te worden verholpen om te zorgen dat portofoon gesprekken in StandBy probleemloos kunnen plaatsvinden. (Let op: Error meldingen over fouten mbt Video functionaliteit worden genegeerd)

Indien de portofoon functie wordt gebruikt in de mobiele app, dient de test ook te worden uitgevoerd in de browser van de mobiele telefoon (smartphone). Indien er ook gebruik wordt gemaakt van de portofoon functie via de Alarmcentrale webapplicatie, dient de test ook te worden uitgevoerd op de betreffende computers/laptops (in dezelfde browser als waarin de Alarmcentrale webapplicatie wordt gebruikt).

Voorbeeld testresultaat Twilio netwerktest (okt, 2024):

Alle drie de items die beginnen met "Voice" moeten slagen (Pass) voor een juiste werking van de portofoonfunctie. De (bovenste drie) items die beginnen met "NTS" en de (onderste vier)

items die beginnen met “Video” mogen mislukken (Fail) en zijn niet vereist voor de portofoonfunctie.

Twilio WebRTC Diagnostics

Checks your browser and network environment to ensure you can use Twilio's WebRTC products.

Pass	NTS: TURN UDP Connectivity
Verifies UDP connectivity from your browser to Twilio's TURN servers.	
Pass	NTS: TURN TCP Connectivity
Verifies TCP connectivity from your browser to Twilio's TURN servers. Note: TCP connectivity is not currently supported in Twilio Voice.	
Pass	NTS: TURN TLS Connectivity
Verifies TLS connectivity from your browser to Twilio's TURN servers. Note: TLS connectivity is not currently supported in Twilio Voice.	
Pass	Voice: Bandwidth
Determine how many simultaneous Twilio Voice calls your network can support.	
Pass	Voice: Test call using PCMU
Test the browser's ability to make calls with Twilio Voice.	
An edge location can be specified by adding it as a query param: https://networktest.twilio.com/?edge=ashburn	
Pass	Voice: Test call using Opus
Test the browser's ability to make calls with Twilio Voice.	
An edge location can be specified by adding it as a query param: https://networktest.twilio.com/?edge=ashburn	
Pass	Video: Insights Connectivity
Verifies connectivity from your browser to Twilio Insights endpoint	
Pass	Video: Signaling Connectivity
Verifies connectivity from your browser to Twilio signaling endpoint.	
Fail	Video: Test Group Room with TURN
Test browser's ability to connect to a Group Room through TURN relay with Twilio Video.	
Fail	Video: Test Group Room without TURN
Test browser's ability to connect to a Group Room through Media Server with Twilio Video.	

Browserondersteuning

De portofoonfunctie in de Alarmcentrale webapplicatie is alleen geschikt voor moderne browsers. Momenteel ondersteunen we de meest recente versies van browsers Google Chrome, Microsoft Edge en Firefox (tot maximaal 6 maanden oud). Voor Microsoft Edge dient minimaal Versie 130.0.2849.52 te worden gebruikt (versie van okt, 2024)

De portofoonfunctie werkt NIET in de legacy versie van 'Microsoft Edge', dit komt door technische beperkingen in deze reeds uitgefaseerde browser.

Voor het gebruik van de portofoon functie in de Alarmcentrale webapplicatie is het daarnaast vereist dat er werkende speakers/koptelefoon/oortjes zijn aangesloten op de computer, dat er een werkende microfoon is aangesloten op de computer én dat de gebruiker van de Alarmcentrale toestemming kan en mag geven in de browser voor het gebruik van de microfoon:



Netwerkconfiguratie Voice (VoIP)

StandBy maakt gebruik van de Dublin ("Ireland (ie1)") regio van Twilio. De netwerkconfiguratie specificaties voor het gebruik van de portofonie functie zijn als volgt:

Er is één globale IP range die moet worden toegestaan (region onafhankelijk) in de netwerkconfiguratie:

- Protocol: UDP
- Source IP (in your network): ANY
- Source port (in your network): ANY
- Destination IP ranges: 168.86.128.0/18
- Destination port ranges: 10000-60000

Poort 443 dient ook bereikbaar te zijn voor uitgaande verzoeken. Dit is echter in vrijwel alle netwerken al het geval (HTTPS communicatie)

Op onderstaande pagina kan **de actuele range van IP adressen en poorten worden gecontroleerd:**

<https://www.twilio.com/docs/voice/client/javascript/voice-client-js-and-mobile-sdks-network-connectivity-requirements> (items: "Voice Media Server connectivity requirements" en onder "Signalling connectivity requirements" -> "Mobile Voice SDKs")

Netwerkvereisten

Iedere client/device op het netwerk die wil deelnemen aan een portofoon gesprek dient minimaal een 100kbps down/upload snelheid te hebben om de in en uitgaande audiokwaliteit te kunnen garanderen.

Indien er per verbonden client een limiet is ingesteld adviseren we als absoluut minimum 15Mb/s toe te staan zodat we zeer ruim aan de veilige kant te zitten en eventuele andere apps -die potentieel veel data verbruiken- niet direct impact hebben op de kwaliteit van het portofoon gesprek.

Bandwidth (Uplink/Downlink) - Per codec, platform dependent	Opus*: 40kbps / 40kbps PCMU: 100kbps / 100kbps
Latency (RTT)	< 200ms
Jitter	< 30ms
Packet Loss	< 3%

Bron: Twilio, april 2023

QR code alarmeren

Voor klanten met de module 'QR code alarmeren' is het voor gebruikers vereist om een internetverbinding te hebben. Ook moet de telefoon een camera bevatten die QR codes kan scannen.

De gescande QR code leidt gebruikers door naar een website waar het alarm telefoonnummer staat, daarom is een browser en werkende internetverbinding vereist op de telefoon (smartphone) van de gebruiker.

Vanzelfsprekend dient de gebruiker die de code scant en wil bellen ook een werkende telefoonverbinding te hebben.

Koppeling met Flic buttons: Flic Hub vereisten

Aan één Flic Hub kunnen maximaal 64 Flic buttons worden gekoppeld. Alle buttons moeten wel binnen het Bluetooth bereik van een hub blijven. Het bereik van het Bluetooth signaal is zeer sterk afhankelijk van de omgeving waarin deze wordt gebruikt. De fabrikant stelt dat de connectie in een vrije ruimte (buiten) tot maximaal 50 meter mogelijk is. In de praktijk zien we dat een verbinding met de Flic hub mogelijk is met een bereik van 10 tot 25 meter. Dit is sterk afhankelijk van de ruimte, het aantal muren, personen in de ruimte, kasten en ander meubilair in de ruimte.

In de regel wil je, ongeacht van de afstand, voor iedere aparte (ommuurde) ruimte een eigen Flic hub. Oftewel: iedere kamer waarin minimaal één Flic button wordt geplaatst, dient ook een eigen Flic hub te krijgen.

Een schematisch overzicht van de (draadloze en bekabelde) componenten is op aanvraag beschikbaar bij StandBy Solutions.

Netwerk vereisten

Het apparaat moet vrije toegang hebben op (remote) servers over poort 443 zodat het alarmsignaal over een beveiligde/encrypted HTTPS verbinding naar de StandBy server kan worden verzonden.

Voor het functioneren van de verbindingshub dienen de volgende firewall regels/uitzonderingen te worden toegepast:

```
api.flic.io (tcp port 443)
flichub.s3.eu-west-2.amazonaws.com (tcp port 80, 443)
flic-firmware-flic-io.s3.amazonaws.com (tcp port 443)
connectivitycheck.gstatic.com (tcp port 80)
pool.ntp.org port 123
flic-device-manager.s3.amazonaws.com (tcp port 443)
dm-api.flic.io (tcp port 443)
dm.flic.io (tcp port 443)
```

Vereisten

Flichub technical requirements (official, up to date requirements:

https://static1.shortcutlabs.com/wp-content/uploads/2020/10/Flic_Hub_Manual.pdf / Zie ook: <https://flic.io/start>):

Vereisten (in het Engels), zoals vastgesteld in september, 2018:

- At least 1A(mp) power supply to ensure stable behaviour
- Internet via WiFi or Ethernet. StandBy strongly advises (and only supports) the use of ethernet cable usage. This is to prevent potential issues with the wireless connection
- The Flichub will connect to the network like any other internet enabled device. It should at least have access to the outside world (firewall) on port 80 (HTTP) and 443 (HTTPS) [Normally, this is already possible, unless the network is configured in a more restrictive way]
- Flichub can be used in temperatures between -20 C and 54 C (below or above it should not be used)
- Do not use chemicals to clean the Flichub; Do not put the Flichub in/under water. (splash proof IP44 only)

Specifications of the Flichub hardware:

- CONNECTIVITY: WiFi, Bluetooth 4.2, Flic Bluetooth Low Energy Protocol, Ethernet, 3,5mm Audio in/out, 2,5mm IR output.
- COMPATIBILITY: Flic buttons and PbF buttons, iOS 10.3+ and Android 4.4+.
- RANGE: **Up to 50m (150ft)**
- SIZE: 86mm x 66mm x 12.8mm
- MATERIALS: Polycarbonate PC
- WEIGHT: 48.6g
- CARE & CLEANING: Dust or clean with a damp cloth
- INGRESS PROTECTION: IP40
- POWER: 900mA max & 250mA standby

Koppeling met Microsoft Azure

De StandBy BHV app kan gebruikersdata synchroniseren vanuit Microsoft Azure.

Voor de mogelijkheden en configuratie stappen, zie ook (apart opvraagbaar):

Documentatie: StandBy BHV App gebruikers synchronisatie met Microsoft Azure (Microsoft Graph API)

Koppeling met Microsoft Entra ID (Single Sign On / SSO)

De StandBy BHV app kan gebruik maken van identity platform Microsoft Entry ID. Via dit platform kunnen gebruikers via een (interactieve) Single Sign On flow inloggen op de BHV App. Gebruikers hebben hierdoor geen wachtwoord nodig om in te loggen.

Voor de mogelijkheden en configuratie stappen, zie ook onze SSO specifieke documentatie (apart opvraagbaar):

Documentatie: Single Sign On (SSO) in de BHV App via Microsoft Entra ID