

AGFEO

AGFEO OS

Wiki: Netzwerk- und Firewall- Nutzung, Port-/Host-Übersicht



AGFEO ES- und HyperVoice Kommunikationssysteme

Übersicht der von den AGFEO Produkten benutzten Netzwerkports

Alle Angaben ohne Gewähr!

Stand 24.10.2023LB

Inhalt:

Vorwort.....	3
Relevante Sicherheitsbetrachtungen	3
Besondere Hinweise	3
Informationen für einen Betrieb hinter Firewall-Systemen	3
Unterstützung für Quality of Service (QoS)	4
Besondere Hinweise	4
Netzwerkports der AGFEO PBX Systeme	5
Allgemeine Dienste.....	5
SIP Ports für VoIP Verbindungen.....	5
Integrierter ASIP-Server.....	5
Integrierter SIP Server (Registrar)	6
Extern SIP zur Anmeldung (Client) am SIP Provider (UDP)	6
Extern SIP zur Anmeldung am SIP Provider (TCP)	6
RTP Ports für VoIP Verbindungen.....	7
Ältere ES-Systeme (<i>ohne</i> ES PURE IP X IT, ES 7xx IT plus)	7
Neuere ES-Systeme (ES PURE IP X IT, ES 7xx IT plus) und AGFEO HyperVoice	7
Systemzugriff auf externe Serveradressen	7
Netzwerkports der AGFEO SIP und ASIP Endgeräte	9
AGFEO SIP Geräte (SIP/RTP)	9
Systemzugriff auf externe Serveradressen	10
AGFEO ASIP Geräte (IP-Systemtelefone)	10

Netzwerkports sonstiger AGFEO Produkte	11
Netzwerkports sonstiger Softwareprodukte.....	11

Vorwort

Relevante Sicherheitsbetrachtungen

Es ist zu beachten, dass Kommunikationsprodukte wie Telefonanlage und Endgeräte und/oder Software mitunter im besonderen Fokus unberechtigter Zugriffsversuche stehen. Aus Sicherheitsgründen empfehlen wir neben ausreichend starken / sicheren Passwörtern ausschließlich entsprechend *abgesicherte Verbindungen* zu nutzen. Insbesondere bei Zugriffswünschen über öffentliche Netze wie z.B. dem Internet etc. sind z.B. *VPN-Verbindungen* zu bevorzugen.

AGFEO übernimmt keinen Support oder Haftung, wenn Kommunikationsprodukte auf Grund z.B. mangelnder Absicherung oder Maßnahmen, die nicht dem jeweiligen Stand der Technik darstellen von unberechtigtem Zugriff und/oder Manipulation Dritter betroffen sind.

Somit sind z.B. bei Einsatz der Produkte aus fremden Netzen heraus (z.B. HomeOffice, Filialstandort etc.) keine Portfreigaben anzulegen, sondern für den Zugriff auf/mit/über Kommunikationsprodukte ausschließlich geeignete, gesicherte Verbindungen (z.B. VPN) zu verwenden!

Bitte beachten:

- Unsere technische Hotline supportet ausschließlich VPN-Verbindungen!
- Die Einstellungs-Option „Nicht-private-IP-Adressen“ zuzulassen sollte aus Sicherheitsüberlegungen heraus sinnvollerweise nicht aktiviert werden und kann als Nebeneffekt z.B. die Anmeldung und Nutzung von SIP-Geräten unterbinden.

Informationen für einen Betrieb hinter Firewall-Systemen

Gängige Netzstrukturen führen zu einem einer Firewall nachgelagerten Betrieb unserer Produkte. Dies bedeutet, dass das AGFEO Kommunikationssystem und entsprechend daran angeschlossene Produkte vom öffentlichen Datenverkehr und Zugriffsversuchen aus dem Internet abgeblockt (gesichert) sind.

Zur externen Kommunikation mit z.B. Providern unterstützen unsere Produkte vielfältige technische Verfahren, um trotz vorgeschalteter Firewall-Systeme eine sichere, stabile Verbindung zu ermöglichen. So senden AGFEO Kommunikationssysteme z.B. kleine *KeepAlive* Pakete, um den SIP-Transfer über Firewall-Systeme hinaus zu ermöglichen.

--> **I.d.R. sind daher keine Portfreigaben in der Firewall vorzunehmen!**

Achten Sie allerdings in der Firewall auf korrekte TimeOut- bzw. UDP/TCP-Aging bzw. Verfalls-Werte und stellen Sie bei hochwertigen Firewall-Systemen sicher, vorhandene SIP ALG (application layer gateway) bzw. andere SIP NAT Helper Verfahren **ABZUSCHALTEN!**

Geben Sie auf keinen Fall den Port 5060 (oder gar 80 bzw. 443) in der Firewall frei!

Unterstützung für Quality of Service (QoS)

Alle AGFEO IP-Telefonendgeräte unterstützen zur optimierten Sprachübertragung der RTP-Sprachpakete einen QoS-Mechanismus gemäß folgendem Codepoint Wert:

DSCP: expedited forwarding (EF)

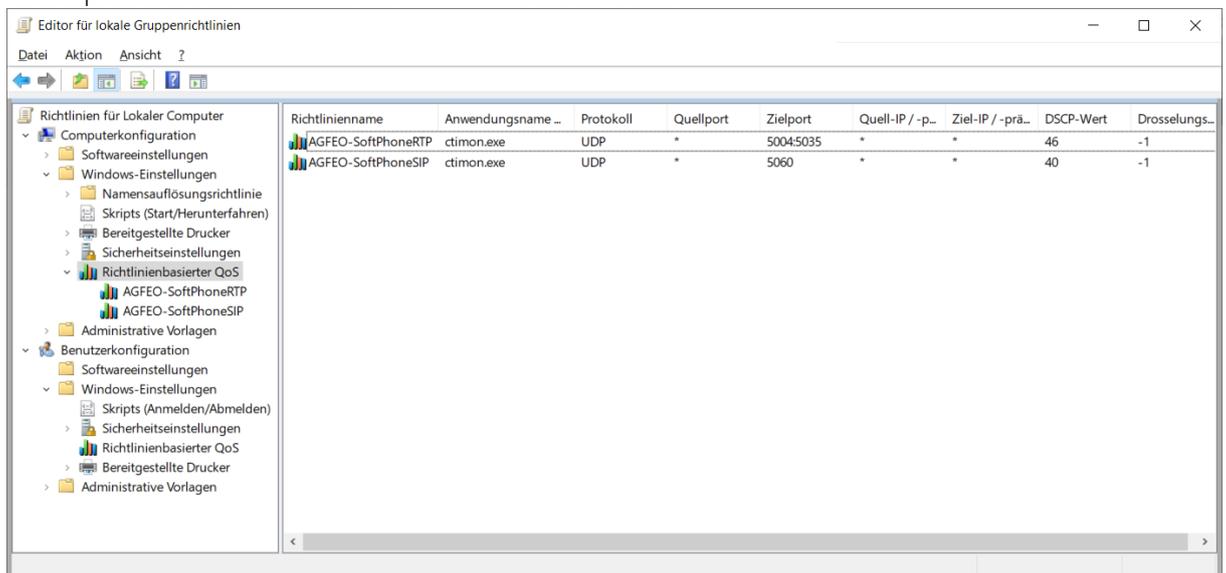
Bits: 101110

Dez: 46

Die entsprechende Kennzeichnung ist automatisch aktiv und kann nicht abgeschaltet werden.

Bitte beachten:

- die verwendeten aktiven Netzwerkkomponenten des Kundennetzwerks (LAN) müssen QoS aktiv unterstützen
- bei öffentlichen Netzen (Internet/VPN/WAN) wird eine QoS-Kennzeichnung i.d.R nicht berücksichtigt und ist daher wirkungslos
- Bei Nutzung der SoftPhone Funktion des AGFEO VISOfon unter MS Windows kann QoS ausschließlich über gesondert einzurichtende Gruppenrichtlinien Funktionen des Betriebssystems aktiviert werden. Nachstehender Screenshot zeigt die Einrichtung einer *richtlinienbasierten QoS Unterstützung* unter MS Windows durch eine Gruppenrichtlinie auf globaler Computerkonfigurations-Ebene und hinsichtlich getrennter Codepoint-Werte für die RTP/Sprechwege- und SIP/Signalisierungs-Datenpakete der SoftPhone Funktion des AGFEO VISOfon.



Screenshot zeigt Betrieb an einem ES-System!

Bei Betrieb an einer AGFEO HyperVoice oder ES-Pure IP X IT bitte beachten, dass diese Systeme andere RTP Ports verwenden! Die Zielportrange ist dann entsprechend anzupassen (s.u.)!

Netzwerk-Nutzung AGFEO PBX

Kommunikationssysteme der ES und HV Serie

1. Übersicht der Netzwerkports des AGFEO Kommunikationssystems

AGFEO ES- und HyperVoice System nutzen Netzwerkverbindungen für unterschiedliche Dienste. I.d.R. werden die Port-Verbindungen der Systemdienste nur abgehend aufgebaut.

Angegeben sind immer die per Default verwendeten Quellports, sofern diese nicht individuell verändert wurden.

1.1 Allgemeine Dienste

Übersicht der allgemein relevanten IP-Dienste der AGFEO Kommunikationssysteme.

Port	Protokoll	Beschreibung	Richtung
53	UDP	DNS (Namensauflösung)	Abgehend
53	TCP	DNS (Namensauflösung)	Abgehend
80	TCP	http Web-Konfiguration AGFEO Dashboard	Eingehend
123	UDP	NTP	Beidseitig
123	TCP	NTP	Beidseitig
389	TCP	Zugriff auf zentrale Anlagenkontakte durch AGFEO SIP Endgeräte (wie z.B. T14SIP oder DECT IP Handteile)	Eingehend
443	TCP	https Web-Konfiguration AGFEO Dashboard Zugriff auf AGFEO Cloud-Dienste	Beidseitig
1883	TCP	MQTT Broker Nur wenn MQTT Broker Funktion aktiviert	eingehend
3232	TCP	TAPI-/CSTA-Server	eingehend
Dyn.	TCP	MQTT Client (dynamische Portbelegung)	abgehend

1.2 VoIP Signalisierungsdaten (SIP/ASIP)

AGFEO Kommunikationssysteme verfügen gleichzeitig über VoIP *Server* und *-Client* Funktionalität. Diese nutzen je nach Verwendung und Ziel unterschiedliche Ports.

Integrierter *ASIP*-Server zur Anmeldung interner AGFEO System IP Geräte

Port	Protokoll	Beschreibung	Richtung
5904	TCP	Interner ASIP Registrar Anmeldung von internen AGFEO ASIP Telefonen	Initial nur eingehend

Integrierter SIP-Server (Registrar) zur Anmeldung interner SIP Geräte

Port	Protokoll	Beschreibung	Richtung
5060	UDP	Interner SIP Registrar Anmeldung von internen SIP Endgeräten	initial nur eingehend

Extern SIP zur Anmeldung (als Client) am SIP-Provider mittels SIP over UDP
(Normal-Fall)

Port	Protokoll	Beschreibung	Richtung
5064 – 5127	UDP	<p>Quellport für SIP Client (max 32 Accounts)</p> <p>Je externem SIP Account werden 2 Ports benötigt! Die benötigte Portrange reduziert sich dementsprechend in Abhängigkeit der aktivierten externen SIP Accounts.</p> <p>Sollten NAT-Regeln in einer vorgelagerten Firewall notwendig sein (s.a. Angaben auf Seite 3), so sollte die Erreichbarkeit der Anlage aus dem Internet mittels z.B. IP-Adress-Whitelisting auf die VoIP-Server des Providers beschränkt werden!</p>	Abgehend

Extern SIP zur Anmeldung (als Client) am SIP-Provider mittels SIP over TCP
(Sonderfall. Z.B. bei aktivierter Verschlüsselung und einigen Providern)

Port	Protokoll	Beschreibung	Richtung
dyn.	TCP	<p>Bei SIP over TCP-Verbindungen werden die Quellport des jeweiligen SIP Accounts rein <i>dynamisch</i> über die Portrange 1024-65535 ausgehandelt.</p> <p>Sollten NAT-Regeln in einer vorgelagerten Firewall notwendig sein (s.a. Angaben auf Seite 3), so sollte die Erreichbarkeit der Anlage aus dem Internet mittels z.B. IP-Adress-Whitelisting auf die VoIP-Server des Providers beschränkt werden!</p> <p>TCP nur bei Nutzung einer im SIP Account aktivierten TCP-Funktion und in Abhängigkeit des SIP Providers!</p>	Abgehend

1.3 VoIP Verbindungen - Sprechwege (RTP)

AGFEO ES und HyperVoice Systeme nutzen für die RTP Sprachdaten unterschiedliche Ports. Je Gespräch werden 2 Ports benötigt.

Ältere ES-Systeme (ohne ES PURE IP X IT, ES 7xx IT plus)

Portrange	Protokoll	Beschreibung	Richtung
Startport =5004	UDP		Beidseitig
5004 - 5035		Maximal verwendete Portrange für SIP Extern, SIP Intern und ASIP Intern Die tatsächliche Portrange ist abhängig von der Anzahl vorhandener Sprachkanäle des ES-Systems.	
Konkret: 5004 - 5011 5004 - 5015 5004 - 5027 5004 - 5035		ES mit 4 IP-Kanälen (zB ES 5xx) ES mit 6 IP-Kanälen (zB ES 54x) ES mit 12 IP-Kanälen (zB ES 628/ES730IT) ohne Lizenz ES mit 16 oder mehr IP-Kanälen (zB ES 770 IT)	
		Hinweis: Bei Einsatz von IP-Modulen in alten ES 7xx IT Systemen (ohne „plus“-Upgrade Kit) nutzen alle ETH Interfaces dieselben Ports für die RTP Sprachdaten.	

Neuere ES-Systeme und AGFEO HyperVoice (ES-PURE IP X IT bzw. ES 7xx IT plus)

Portrange	Protokoll	Beschreibung	Richtung
Startport =5204	UDP		Beidseitig
5204 - 5263		Nur ES PURE IP X IT (mit max. 30 IP Kanälen)	
5204 - 5331		Nur ES 7xx IT plus (mit max. 64 IP Kanälen)	
5204 - 5523		Nur HyperVoice-Systeme	
		Maximal verwendete Portrange für SIP Extern, SIP Intern und ASIP Intern Sprechwege. Die tatsächliche Portrange ist abhängig von der Anzahl vorhandener IP-Kanal- (ES PURE IP X IT, ES 7xx IT plus) bzw. CALLS- (HyperVoice) Lizenzen im System!	

1.4 Zugriff auf externe Serveradressen (AGFEO Cloudzugriff)

AGFEO Kommunikationssysteme greifen mitunter auf externe Cloud-Ressourcen von AGFEO zu. Die Kommunikation erfolgt ausschließlich verschlüsselt über Port 443 und rein abgehend.

Adresse	Protokoll	Beschreibung	Richtung
remote.agfeo.de	TCP / https	AGFEO Fernwartungsplattform	Abgehend
remote2.agfeo.de	TCP / https	AGFEO RemoteAPP Server für Fernzugriff der AGFEO APPs	Abgehend

pbx.agfeo.de	TCP / https	AGFEO Lizenz-Server	Abgehend
aws.agfeo.de	TCP / https	AGFEO Heartbeat-Server für HyperVoice Systeme	Abgehend

Netzwerk-Nutzung AGFEO Endgeräte

AGFEO Endgeräte mit SIP und ASIP Technik

Nachfolgend die Portübersichten für AGFEO VoIP-Geräte

Angegeben sind immer die per Default verwendeten, VoIP relevanten *Quellports*, sofern nicht z.B. über die Webkonfiguration individuell verändert. Alle IP Endgeräte können darüber hinaus weitere, hier nicht spezifizierte Ports für besondere Dienste (zB Webkonfiguration, Updatevorgang, DHCP, DNS, NTP etc.) verwenden.

2.0 VoIP-Netzwerkports der AGFEO Endgeräte

2.1 Ports der AGFEO SIP Geräte

AGFEO SIP Geräte nutzen für VoIP Funktionen je Typ unterschiedliche Ports.

Gerät	Quellport SIP	Quellports RTP	Anmerkungen
T14 SIP	5060 UDP	Portrange 10000-10200 UDP	Portrange mit 200 Ports per Default
DECT IP Basis DECT IP Handteile	5060 UDP	Portrange 50004 – 50043 UDP	Je verwendeter DECT IP Basis
AGFEO VISOfon mit aktivem SIP- SoftPhone	Portrange 1024-65535 UDP	Portrange 1024 – 65535 UDP	Ohne aktive Vorgabe durch das Kommunikationssystem verwendet das AGFEO Dashboard für die SIP SoftPhone Funktion die Portrange 1024 bis 65535 mit einer dynamischen Portbelegung (Default-Einstellung!).
	60104 UDP	65100 – 65120	Nur bei aktivierter Vorgabe durch AGFEO TK-System und unverstellter Default-Einstellung!
	individuell UDP	individuell UDP	Durch Anpassung einer speziellen INI Datei (s.a. OnlineHilfe)
AGFEO IP Video TFE	5060 UDP	Portrange	

Neben den angegebenen Ports können in Abhängigkeit des jeweils eingesetzten Endgerätes, weitere Standard-Dienste (NTP, DNS, DHCP, Multicast, TFTP etc.) verwendet werden.

2.2 Zugriff auf externe Serveradressen (AGFEO Cloud)

Einige AGFEO SIP Geräte benötigen mitunter Zugriff auf externe Serveradressen.

Adresse	Protokoll	Beschreibung	Richtung
dect.agfeo.de	TCP / http	AGFEO DECT IP Updateserver für Firmware-Updates der DECT IP Basen	Abgehend

2.3 Ports für AGFEO System IP Geräte (ASIP)

AGFEO ASIP Geräte nutzen technisch ein komplett anderes Verfahren als einfache SIP Geräte und nutzen somit auch abweichende Ports.

Port	Verfahren	Anmerkungen	Richtung
80	TCP	Web-Konfiguration Firmware-Update	beidseitig
2153	TCP	Für ASIP Signalisierungsdaten	abgehend
5896	UDP	Für ASIP RTP Sprachdaten	beidseitig
12179	UDP	AGFEO Werkzeugsuche	eingehend

Netzwerk-Nutzung sonstige AGFEO Produkte

Sonstige AGFEO Produkte

Nachfolgend die Portübersichten sonstiger AGFEO Produkte

3.0 Sonstige AGFEO Produkte (wie z.B. weitere Softwareprodukte etc.)

Produkt	Dienst	Port	Anmerkung
AGFEO Dashboard APP	Datenkommunikation und FMC / OneNumber Rufaufbau	443	Abgehend Erstzugriff lokal, danach Zugriff über sicheren AGFEO RemoteServer Dienst (Cloud)
AGFEO Dashboard PC	CTI-Kommunikation	80 443	Initial abgehend Unverschlüsselt Verschlüsselt, sofern aktiviert
AGFEO TSP TAPI Treiber	Anlagenverbindung	3232	abgehend
AGFEO Werkzeug	Gerätesuchdienst	12172 12176 12178 12179 12181 12185 12186 12187 12188 12189 12190 12191 12192	TK-HomeServer LM 510 LM 508 ST xx IP LM 509 ES 51x, ES 52x ES 5xx UP, ES 54x, ES 6XX DECT IP Basis ES 7xx IT (inkl. "plus") ES Pure IP x IT IP-Video TFE 1/2 Smart Connect Box (SCB) IP700 Modul
	Firmware Update	12174	Nur LM/TKHS
	Status-Übermittlung	12175	nur ältere AS Geräte/Module
	TFTP Server	69	nur bei aktivem DECT IP Update
	Wireshark Trace	39321	nur bei aktivem Mitschnitt
	Syslog Server	514	„aus“ per Default

Irrtümer und Änderungen vorbehalten

© AGFEO 2023LB