Nur für Firmen:
Firewall-Einstellungen
gültig ab 16.11.2021

Damit die Tess – Relay-Dienste über den myMMXtc Windows Client, myMMXtc Web-Client, myMMXtc App und VPAD, ViTAB, rexfon genutzt werden können, müssen Sie folgende Einstellungen an Ihrer Firmen-Firewall vornehmen:

myMMXtc Windows Client: (Download von der Tess Homepage)

Lfd.-Nr.	SrcIP	SrcPort	Protokol	DestIP	DestPort
1	own	any	TCP	79.171.92.199	443
2	own	any	TCP	79.171.92.199	8080
3	own	any	UDP	79.171.92.199 79.171.92.200 79.171.92.201	3478-3479
4	own	25000-25999	UDP	79.171.92.199	33000-33999
5	own	25000-25999	UDP	any	25000-25999

myMMXtc Web-Client:

Lfd.-Nr.	SrcIP	SrcPort	Protokol	DestIP	DestPort
6	own	any	TCP	79.171.92.199	443
7	own	any	UDP	79.171.92.199 79.171.92.200 79.171.92.201	25000-25999

myMMXtc App: (Download aus iOS App Store und Google Play)

Lfd.-Nr.	SrcIP	SrcPort	Protokol	DestIP	DestPort
8	own	any	TCP	79.171.92.199	443
9	own	any	TCP UDP	79.171.92.199	5060
10	own	8000-8200	UDP	79.171.92.199 79.171.92.200 79.171.92.201	3478-3479
11	own	8000-8200	UDP	79.171.92.199	33000-33999
12	own	8000-8200	UDP	any	25000-25999

VPAD, ViTAB, rexfon: (Nur von Fremdanbietern)

Lfd.-Nr.	SrcIP	SrcPort	Protokol	DestIP	DestPort
13	own	5060	UDP	79.171.92.199	5060
14	own	5060-5061 32000-32001 33000-33001	UDP	79.171.92.199 79.171.92.200 79.171.92.201	3478-3479
15	own	32000-32001 33000-33001	UDP	79.171.92.199	33000-33999
16	own	32000-32001 33000-33001	UDP	any	25000-25999

Erläuterungen zu den laufenden Nummern.

Zu 1: **Port 443**, zwingend erforderlich: u.a. für die Authentifikation, Verbindungssteuerung, Textkommunikation

Zu 2: **Port 8080**, optional: für Bandbreitentest. Sofern eine garantierte Bandbreite für den myMMXtc Windows Client zur Verfügung gestellt wird, ist die Freigabe dieses Ports nicht notwendig

Zu 3: **Ports 3478-3479**, optional: für STUN Nutzung

Zu 4: **Ports 33000-33999**, erforderlich: für Warteschlangen Videos

Zu 5: **Ports 25000-25999**, zwingend erforderlich: für Audio und Videokommunikation mit dem Dolmetscher oder wenn der Service „Voice Carry Over – Selbst Sprechen“ im Rahmen von TeScript und TeSign genutzt werden soll

Zu 6: **Port 443**, zwingend erforderlich: u.a. für die Authentifikation, Verbindungssteuerung, Textkommunikation

Zu 7: **Ports 25000-25999**, zwingend erforderlich: für Audio und Videokommunikation mit dem Dolmetscher oder wenn der Service „Voice Carry Over – Selbst Sprechen“ im Rahmen von TeScript und TeSign genutzt werden soll

Zu 8: **Port 443**, zwingend erforderlich: u.a. für die Authentifikation

Zu 9: **Port 5060**, zwingend erforderlich bei Android: für SIP Kommunikation zum Auf- und Abbau von Verbindungen und der Textkommunikation

Zu 10: **Ports 3478-3479**, optional: für STUN Nutzung

Zu 11: **Ports 33000-33999**, erforderlich: für Warteschlangen Videos

Zu 12: **Ports 25000-25999**, zwingend erforderlich: für Audio- und Videokommunikation mit dem Dolmetscher oder wenn der Service „Voice Carry Over – Selbst Sprechen“ im Rahmen von TeScript und TeSign genutzt werden soll

Zu 13: **Port 5060**, zwingend erforderlich: für SIP Kommunikation zum Auf- und Abbau von Verbindungen

Zu 14: **Ports 3478-3479**, optional: für STUN Nutzung

Zu 15: **Ports 33000-33999**, erforderlich: für Warteschlangen Videos

Zu 16: **Ports 25000-25999**, zwingend erforderlich: für Audio und Videokommunikation mit dem Dolmetscher

Legende:

Optional: Muss nur eingerichtet werden, falls die beschriebene Funktionalität benötigt wird.

Erforderlich: Wird im Regelfall benötigt, kann aber unter bestimmten Bedingungen entfallen.

Zwingend erforderlich: Wird immer benötigt. Ohne diese Ports ist eine Kommunikation nicht gewährleistet.

Gelb = Änderung oder Neuerung

Hinweis:

Falls im Firmennetzwerk ein „stateful“ Firewall/ Paketfilter eingesetzt wird und das benutzte Endgerät verfügt über die Berechtigung des Internetzugriffs, müssen die oben aufgeführten Ports nicht explizit für Verkehr von außen freigegeben werden.

Stateful/dynamische Paketfilter
Aufbauend auf den Features eines einfachen Paketfilters, überwacht und speichert ein stateful Paketfilter den Status jeder Verbindung in einer State-Table genannten Tabelle. So merkt sich die Firewall, wenn beispielsweise aus dem internen Netzwerk eine Verbindung nach außen aufgebaut wird, die zu der Verbindung gehörenden IP-Adressen und Port-Nummern. Antwortpakete werden nur dann in das interne Netzwerk zugelassen, wenn sie genau zu den in der State-Table gespeicherten Verbindungsdaten passen, und innerhalb eines definierten Zeitfensters erscheinen.

Stand: 16.11.2021