Systemvorrausetzungen für ein DICOM-Mail Gateway
(Die Systemvoraussetzungen gelten gleichermaßen für ein virtuelles- oder physisches System)

Server:
Auf dem System sollte eines der folgenden Betriebssysteme mit aktuellen Patches installiert sein:

- Microsoft Windows 8.1 oder Server 2012 R2
- Microsoft Windows 10 oder Server 2016/19

Einzelplatzlösung (Minimalvoraussetzung):

- 2 CPU Kerne
- 6 GB RAM
- Min. 200 GB Speicherplatz aufgeteilt in D: 50GB und E: 150GB

Mehrplatzlösung (Minimalvoraussetzung):

- 4 CPU Kerne
- 8 GB RAM
- Min. 200 GB Speicherplatz aufgeteilt in D: 50GB und E: 150GB

Firewall-Regeln:
Das Mail Gateway muss für den Betrieb die VISUS Mailserver im Internet erreichen. Dies sind folgende Server:

- mail2.dicommail.com (88.198.20.208)
- mail3.dicommail.com (212.227.159.62)
- mail4.dicommail.com (85.214.139.129)
- mail5.dicommail.com (84.16.252.81)

Diese Verbindungen zu den Servern müssen Proxyfrei über Port 25 (SMTP/TLS) und Port 995 (POP3S) erfolgen.

Wir empfehlen außerdem, dass auf dem System eine Anti-Viren-Software als Präventivschutz installiert ist. Erfahrungsgemäß läuft unsere Software JiveX mit den gängigen Produkten einwandfrei.

Clients:
Dem Anwender stehen zwei verschiedene Clients zur Verfügung, ein Desktopclient, JiveX Review Client, und der Webclient JiveX Review Web. Der Review Client läuft auf allen gängigen Windows Betriebssystemen ab Windows 7, der Review Web Client lässt sich sowohl auf Windows als auch auf MacOS Systemen nutzen.

JiveX Status Monitoring:
JiveX Status Monitoring überwacht den Betriebszustand des Systems und der JiveX-Dienste und gibt diese Informationen an den Service des Teleradiologie Verbundes weiter. Hierdurch kann ein dauerhafter Betrieb des Systems unterstützt werden.

Für die Umsetzung benötigen wir eine weitere Firewall-Freischaltung für die ausgehende Kommunikation zu unserem zentralen Server.

- atlas79.mydhp.de (195.62.121.79 Port 8140 [TCP])

VPN-Verbindung zu Installation und Service-Zwecken:
Der Service-Bereich der VISUS Health IT GmbH bevorzugt für Wartungs- und Supportfälle einen End-to-Site VPN Zugang (IPsec oder SSL VPN), sollte dies Aufgrund von Vorgaben nicht machbar sein, kann man auf Fernwartungs-Clients wie Teamviewer oder Anydesk ausweichen.