

Systemanforderungen ATT 3D Lernwelt

Unterstützte Betriebssysteme

- **Windows 8.1**
- **Windows 10** (keine N Versionen wie z.B. Windows 10 Home N)
- **Mac OS X ab Version 10.13**

Hardwareanforderung

- **Standard Rechner bzw. Laptop: kein Thin (bzw. Slim) Client**
- **Festplattenspeicher:** 1,5 GB verfügbarer Festplattenspeicher
- **Arbeitsspeicher:** mind. 2 GB Arbeitsspeicher, empfohlen: 4 GB oder mehr
- **Prozessorleistung:** 2 Ghz Dual-Core CPU
- **Grafikkarte:** mind. DirectX9 Grafikkarte, Intel HD Graphics 2500/3000, empfohlen: Intel HD Graphics 4600 oder dedizierte Grafikkarte z.B. nVidia Geforce GT 430, AMD Radeon HD 5570 oder neuer
- **Soundkarte**
- **Computermaus**
- **Headset**



Bitte beachten Sie, dass Sie ausschließlich mit einem (handelsüblichen) Headset mit integrierter Sprachfunktion (Mikrofon) an einer virtuellen Veranstaltung teilnehmen können. Andere Konfigurationen können störende Echos erzeugen.

Stellen Sie sicher, dass Ihr Mikrofon bzw. Ihre Kamera bezüglich der neuen Datenschutzverordnung bei Windows 10 offen ist (Windows 10: Start > Einstellungen > Datenschutz > Mikrofon > (> Kamera) Zulassen, dass Apps auf Ihr Mikrofon (Kamera) zugreifen > Ein)

Internet Bandbreite

Minimum: DSL 3000

Empfohlen: DSL 6000 und höher

Drahtlose Netzwerke: Stellen Sie sicher, dass Ihre Verbindung stabil ist, da es ansonsten zu Verbindungsabbrüchen während Ihrer Sitzung kommen kann.

Firewalls

Die Windows-Firewall darf die Anwendung nicht blockieren. Klicken Sie bitte auf **Zugriff zulassen**. Falls Sie keine Standard Windows-Firewall verwenden, klicken Sie bitte auf **nicht blockieren**.

Information zur Einrichtung in restriktiv gesicherten Netzwerken:

Ports

Entweder muss Port 80 oder vorzugsweise Port 443 für das Protokoll TCP freigeschaltet sein. Proxy-Server können in der Anwendung konfiguriert werden.

SSL Zertifikatsabfrage

Der Client für die ATT 3D Welt stellt HTTPS Anfragen zu verschiedenen Domains und überprüft dabei das SSL Zertifikat strikt auf Gültigkeit. Für den Betrieb der Anwendung muss daher die SSL Inspection in der Firewall oder dem Proxy-Server für Anfragen an folgende Domains deaktiviert werden:

*.tricat-spaces.net
*.tricat.net
*.tricat-dns.net

Folgende Aktivitäten müssen zusätzlich für die genannten Domains erlaubt sein:

Update der Anwendung

- erfordert den Download von passwortgeschützten Archiven und ausführbaren Dateien

Die Authentifizierung des Clients beim Server

- erfordert die erlaubte Nutzung eines MS Edge User-Agent Request Headers
- erfordert die erlaubte Nutzung selbstausgestellter Zertifikate
- erfordert das Durch- bzw. Weiterreichen des Zertifikats via Proxy etc. zwischen Client und Server