

# BigBlueButton

BigBlueButton (kurz auch BBB) ist ein Open-Source-Webkonferenzsystem.

## Vorteile

- Viele Moderationstools für Vorträge, Konferenzen und Unterricht
- Breakout-Rooms (kleinere Unterräume)
- Passwort für Räume und Lobby möglich
- Relativ Simpel zu benutzen, auch spontan
- Räume sind relativ schnell erstellt
- gemeinsam Youtube-Videos anschauen
- Telefoneinwahl (per Telefonnummer)
- gut für viele Teilnehmende geeignet (200+)
- Multi-User-Whiteboard

## Nachteile

- Nicht besonders barrierefrei, v.a. für die Benutzung mit dem Handy
- Nicht so leicht selbst zu hosten
- Nicht Ende-zu-Ende-verschlüsselt (Server-Admins und Angreifende können theoretisch mithören und aufzeichnen)
- Videoübertragung mit vielen Leuten funktioniert eher schlecht (wie bei anderen Tools auch)

## Empfehlung

Ich empfehle BigBlueButton für Vorträge, Workshops und allgemein größere Meetings zu denen bspw. öffentlich eingeladen wird. Es ist auch für Plena geeignet, allerdings ist es vom Handy aus nur sehr nervig zu benutzen, weshalb ich hier eher Jitsi oder Mumble wählen würde. Ein eigener Server ist in der Regel nicht nötig und bietet wenig Vorteile.

## Anleitungen

- <https://www.senfcall.de/help#videotutorials>

## Serverliste

- <https://www.senfcall.de/>

- <https://bbb.random-redirect.de/>

# BigBlueButton mit Torbrowser, Tails oder whonix

(gilt auch für andere WebRTC basierenden Anwendungen)

BigBlueButton nutzt das WebRTC-Protokoll. Der torbrowser unterstützt dieses Protokoll nicht (--disable-webrtc Flag bei der Kompilierung), um zu verhindern, dass Nutzer durch IP Leaks deanonymisiert werden.

Die Installation eines andern Browsers, wie firefox-esr, umgeht einen Großteil der Anonymisierungstechniken von Tails. Für den Betreiber einer BigBlueButton-Instanz, sind Nutzer dann eindeutig zuordenbar. Dieser Workaround sollte daher nur in Erwägung gezogen werden, wenn keine besseren Alternativen vorhanden sind.

## 1. Installieren von firefox-esr (oder via GUI z.B. Synaptic)

```
sudo apt-get update && sudo apt-get install firefox-esr
```

## 2. Konfigurieren von firefox-esr

Bei Tails und Whonix ist standardmäßig der Internetzugriff für zusätzliche Software deaktiviert. Um dies zu beheben, muss manuell ein SOCKS-Proxy in den Firefox-ESR-Einstellungen konfiguriert werden (unter "Network Settings" ganz unten in about:preferences#general) mit folgenden Angaben: SOCKS-Host: 127.0.0.1 und Port: 9050.

Eine weitere Option ist die Verwendung von BigBlueButton mit firefox in Whonix, die möglicherweise robuster gegen IP-Leaks, aber dennoch nicht vollständig anonym ist. Die beste Lösung für den Erhalt der Anonymität ist die Nutzung von Nicht-WebRTC-Protokollen oder der Verzicht auf Echtzeitkommunikation.

---

Version #6

Erstellt: 4 Dezember 2024 12:47:05 von technikdoku

Zuletzt aktualisiert: 29 Dezember 2024 20:31:53 von Admin S