Firewall-Freigaben für Digital Signage Display mit dem CMS DC-Engine Cloud (AllSignage Offline Viewer) und der Remote-Software „Splashtop“

Der stabile Betrieb eines Digital Signage Systems hängt maßgeblich von der vorhandenen Netzwerk- und Routerkonfiguration ab. In der Praxis stellt nicht die Hardware oder Software den häufigsten Fehlerfaktor dar, sondern eingeschränkte oder falsch konfigurierte Netzwerkumgebungen.

Damit Inhalte zuverlässig geladen, Geräte korrekt gesteuert und Statusmeldungen übertragen werden können, müssen bestimmte ausgehende Verbindungen im Netzwerk erlaubt sein.

Dieses Dokument beschreibt die notwendigen technischen Voraussetzungen und dient als verbindliche Grundlage für die Vorbereitung der IT-Infrastruktur vor der Installation.

Für den Betrieb eines Signage-Displays oder Mediaplayers über das CMS (DC-Engine Cloud. / AllSignage Offline Viewer) werden ausschließlich ausgehende Verbindungen benötigt. Es sind keine eingehenden Ports erforderlich.

Zieldomain: signage.allnet.de bzw. signage.display-concepts.de

Benötigte Firewall-Freigaben:

Zweck	Zieldomain	Port	Protokoll	Beschreibung
CMS-Verbindung & Content-Download	signage.allnet.de bzw.: signage.display-concepts.de	443	TCP (HTTPS / WebSocket)	Allgemeine Kommunikation mit dem Server, Statusmeldungen, Screenshot-Uploads, Content-Download, dauerhafte WebSocket-Verbindung bei Streaming
Steuerbefehle / Gerätekommandos	signage.allnet.de bzw.: signage.display-concepts.de	1883	TCP (MQTT)	Empfang von Steuerbefehlen aus dem Backend (z. B. neue Playlist, Screenshot anfordern, Download-Trigger)

Allgemein gilt:

Die Router- und Netzwerkeinstellungen sind unter Berücksichtigung der individuellen Datenschutz- und Sicherheitsanforderungen des Kunden so zu konfigurieren, dass die für einen stabilen und reibungslosen Betrieb erforderlichen Netzwerk- und Kommunikationsdienste nicht unnötig eingeschränkt oder unterbrochen werden. Hierzu zählen beispielsweise auch sinnvoll abgestimmte Timeout-, Verbindungs-, Filter- und Energiespareinstellungen innerhalb der Netzwerk- und Sicherheitsinfrastruktur.

Remote-Zugriff über die Managed-Software Splashtop

(Zusätzlich (optional), falls Remote-Support über **Splashtop** genutzt wird)

Für einen stabilen und reibungslosen Betrieb von Splashtop bzw. des Splashtop Streamers sollten Router-, Firewall- und Netzwerkeinstellungen auf Kundenseite so konfiguriert sein, dass notwendige Internet- und Kommunikationsverbindungen nicht durch Sicherheits- oder Energiesparmechanismen eingeschränkt werden.

Hierzu zählen insbesondere:

- Zulassung ausgehender Internetverbindungen für Splashtop-Dienste
- Freigabe erforderlicher TCP-/UDP-Ports
- Keine restriktiven Timeout- oder Session-Limits im Router bzw. in Firewalls
- Stabile DNS-Auflösung und Freigabe relevanter Splashtop-Domains
- Vermeidung automatischer Netzwerkisolierungen oder Sicherheitsfilter, die dauerhafte Verbindungen unterbrechen können
- Unterstützung lokaler Direktverbindungen im internen Netzwerk (Peer-to-Peer)
- Optional: Unterstützung von Wake-on-LAN (WOL) für Fernstart-Funktionen

Relevante technische Freigaben sind:

- **Ausgehende Verbindungen / Internetzugriff**
  - TCP 80
  - TCP 443
  - TCP/UDP 8200
  - TCP/UDP 3817

- **Lokale Direktverbindungen (optional)**
  - TCP 6783–6785

- **Wake-on-LAN (optional)**
  - UDP 7 oder UDP 9

- **DNS-/Firewall-Whitelist**
  - *.splashtop.com
  - *.splashtop.eu
  - *.api.splashtop.com
  - *.relay.splashtop.com
  - update.splashtop.com
  - update-g3.splashtop.com

Splashtop benötigt im Standardbetrieb in der Regel keine manuellen Portweiterleitungen oder komplexen Routeranpassungen, sofern die oben genannten Kommunikationswege nicht durch Sicherheitsrichtlinien oder Netzwerkrestriktionen blockiert werden.

Hinweis: Diese Freigaben und Einstellungen sind nur erforderlich, wenn Remote-Zugriff per Splashtop gewünscht bzw. eingesetzt wird.