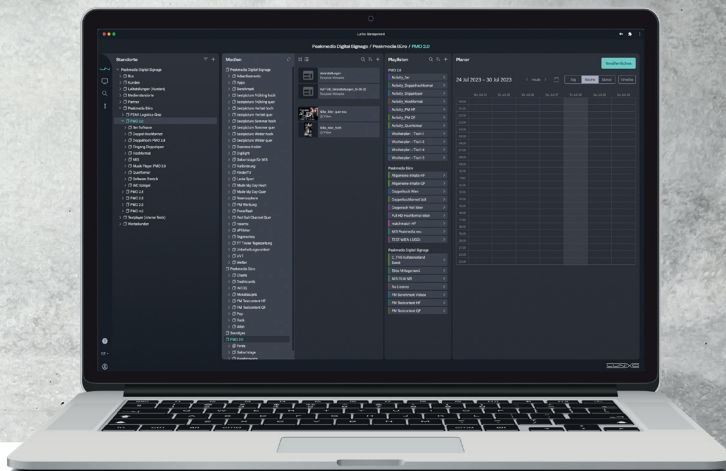




CMS INFOSHEET



UNTERSTÜTZTE DATEIFORMATE

.jpg, .png, .pdf, .mp3, .mp4, .mov, .webm, m4a

MÖGLICHE AUFLÖSUNGEN

HD Ready (720p) = 1280x720

Full HD (1080p) = 1920x1080

4K (2160p) = 3840x2160

NETZWERK- ANFORDERUNGEN

Port: 443 TCP (ausgehend)
lunixo.com

Grundsätzlich ist nur diese Freischaltung notwendig um über lunixo.com/management den Player zu steuern

Port: 443 TCP (ausgehend)
lunixossh.westeurope.cloudapp.azure.com

Um erweiterten Support zu bekommen ist diese Freischaltung notwendig (SSH)

Port: 80 TCP (ausgehend)
at.archive.ubuntu.com

Der Player kann mit der ausgelieferten Version betrieben werden. Sollten jedoch Updates erwünscht sein (security, neue Funktionen,...), muss dieser Port freigeschalten sein

Port: 123 UDP (ausgehend)
ntp.ubuntu.com

Der NTP Server, der sicherstellt, dass der Player immer die korrekte Uhrzeit hat



WEITERE INFOS

- Eine zeitliche Sperre bei Fehlversuchen beim Login ist eine Sicherheitsmaßnahme, die verhindern soll, dass unbefugte Benutzer durch wiederholte Versuche, ein Passwort zu erraten, Zugriff auf ein Konto erhalten. Wenn ein Benutzer eine bestimmte Anzahl von fehlerhaften Anmeldeversuchen durchführt, wird das Konto für einen bestimmten Zeitraum gesperrt. Dies gibt dem legitimen Benutzer Zeit, sich zu melden und das Konto wiederherzustellen, und verhindert, dass unbefugte Benutzer durch wiederholte Anmeldeversuche Zugriff erhalten. Es ist wichtig, dass die Sperrdauer und die Anzahl der erlaubten Fehlversuche sorgfältig ausgewählt werden, um sicherzustellen, dass sie effektiv sind, ohne dass legitimen Benutzern Unannehmlichkeiten entstehen.
- **Login:** Es besteht die Möglichkeit einer 2FA welche empfohlen wird. 2-Faktor-Authentifizierung, auch als Zwei-Faktor-Authentifizierung oder 2FA bezeichnet, ist eine zusätzliche Sicherheitsmaßnahme, die verwendet wird, um die Sicherheit von Lunixo zu erhöhen. 2FA erfordert, dass Benutzer nicht nur ihren Benutzernamen und ihr Passwort eingeben, sondern auch einen weiteren Faktor, einen Sicherheitstoken, die nur für einen begrenzten Zeitraum gültig ist. Auf diese Weise kann sichergestellt werden, dass nur autorisierte Benutzer auf ein Konto zugreifen können.
- SSL (Secure Sockets Layer)
- **Hosting:** Lunixo wird auf Microsoft Azure gehostet Azure ist eine cloudbasierte Plattform, die Unternehmen bei der Entwicklung, Bereitstellung und Verwaltung von Anwendungen und Diensten unterstützt. Azure bietet umfangreiche Sicherheitsfunktionen, um sicherzustellen, dass die Daten und Anwendungen, die auf der Plattform gehostet werden, geschützt sind. Dazu gehören verschlüsselte Datenübertragung, Datensicherung und Wiederherstellung, Firewall-Regeln und Zugriffskontrollen, um nur einige zu nennen. Azure bietet auch regelmäßige Sicherheitsüberprüfungen und -aktualisierungen, um sicherzustellen, dass die Plattform immer auf dem neuesten Stand der Technik bleibt.

Auf Benutzerseite wird folgendes Empfohlen:

- Verwenden Sie starke Passwörter und aktualisieren Sie sie regelmäßig.
- Verwenden Sie 2-Faktor-Authentifizierung, um den Zugriff auf Lunixo zu schützen.
- Verwenden Sie Firewalls und andere Netzwerksicherheitsmaßnahmen, um unbefugten Zugriff auf Ihr Netzwerk zu verhindern.
- Führen Sie regelmäßige Sicherheitsüberprüfungen durch, um Schwachstellen in Ihren Systemen und Prozessen zu identifizieren und zu beheben.
- Es ist wichtig, dass diese Maßnahmen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie wirksam bleiben und dem Bedarf des Unternehmens entsprechen.

Die Nutzung von LUNIXO untersteht der Datenschutz-Grundverordnung (EU) 2016/679.
Weitere Infos erhalten Sie bei Peakmedia digital signage GmbH.