Technical

July 2020

Security

embed signage use Rackspace Cloud servers which have assurances outlined here: http://www.rackspace.co.uk/about-us/security. Rackspace provides a 100% Network Uptime Guarantee and Datacenter SLA (100% HVAC/Power Uptime Guarantee). (http://www.rackspace.co.uk/managed-hosting/dedicated-servers/service-levels). Rackspace datacentres are accredited to PCI DSS, ISO27001, and ISAE 3402 Type II standards, ensuring embedsignage.com is secured by the best processes and technologies available.

From a database and server password change perspective, 60 day recurring tasks are in place that notify the development team to take action and change the relevant software management back end passwords (database, server admin dashboards, cloud storage etc). All software code is obfuscated to reduce risk of hacking. There are various processes running constantly on the servers to block any suspicious activity and notify the server administrators.

Automatically scheduled back ups for all embed signage infrastructure, servers, databases and files are run every 4 hours. Back ups are uploaded to our cloud storage which moves the backup files into 3 different storage locations within the UK Datacenter for redundancy.

Passwords are encrypted using industry standard hashing algorithms. Data is encrypted in transit and at rest. Two-Factor Authentication and Single Sign-On coming soon.

Networking

Users access their account via app.embedsignage.com on a compatible browser (Chrome, Firefox, Safari and IE9+). Here they can upload media files to their account and then publish content to registered devices. Devices connect via app.embedsignage.com and data is transmitted via Port 443 (HTTPS) between the account and the device. Media files for the account are hosted on Rackspace Cloud files with a unique CDN domain for every client account. Files are published via port 443 and a unique domain can be provided upon request for proxy clearance.

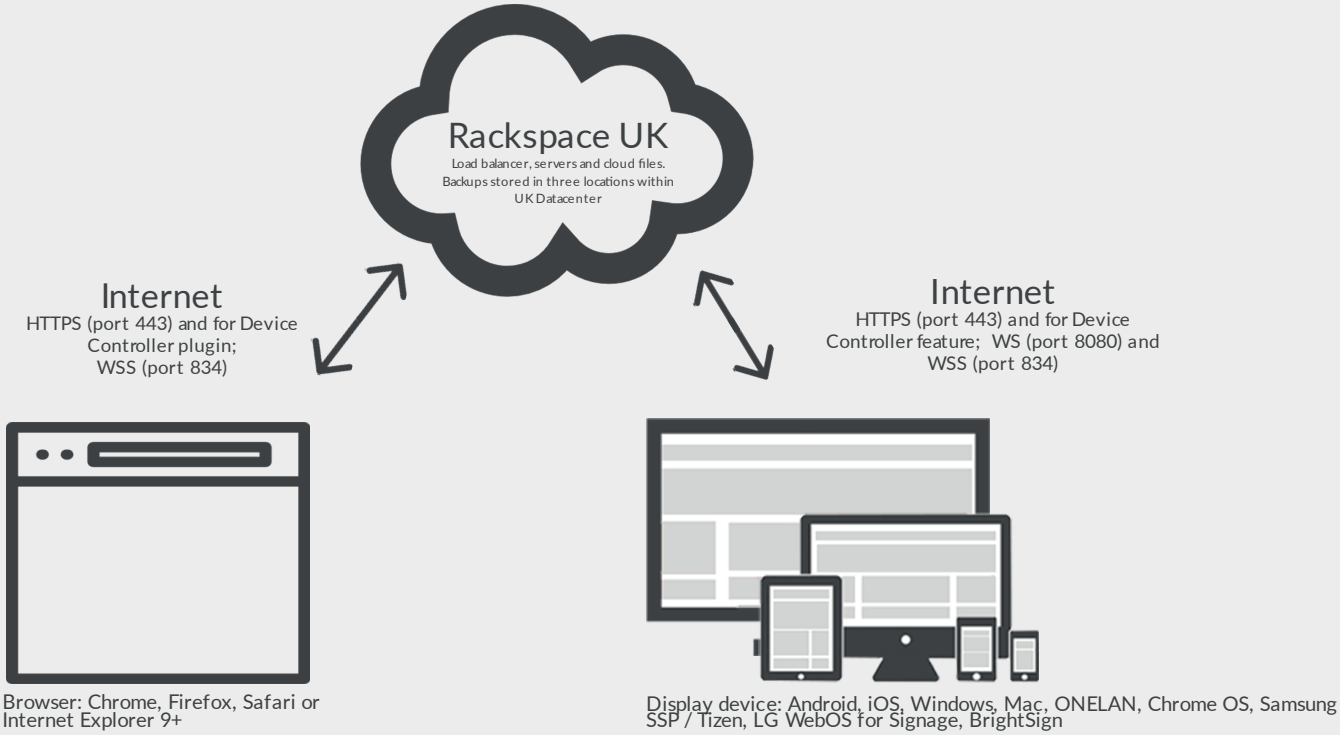
The remote screen management (Device Controller), Channel Sync and Device Interactions features through app.embedsignage.com use Websockets. To use these feature, the network must allow access from wss://websockets.embedsignage.com and ws://websockets.embedsignage.com (ports vary by device, refer to Firewall Approval table on page 3).

As embed signage is a cloud based digital signage platform, the registered devices need to use the internet to receive content. Once content has been downloaded to the devices it will be stored

locally for playback. If connection to app.embedsignage.com is interrupted, the locally stored content on the device will continue to playback avoiding any downtime.

If proxy servers are required to access the internet, hostname and port details must be entered on each device within the client network. For the most secure and reliable connection we recommend that devices avoid using 'public' and 'throttled' connections.

Topology



Any user that needs access to the UI will require availability of a network that permits outbound initiation of an Internet session using HTTPS port 443. All display devices / media players need to access embed signage to download content. Content downloads are initiated by outbound requests using HTTPS port 443.

For a user to use Device Controller feature they will require availability of a network that permits outbound initiation of an Internet session using WSS port 834 and WS port 8080.

Technical

July 2020

Firewall Approval

HOST	IP	PROTOCOL	PORT	DIRECTION
app.embedsignage.com	134.213.3.68	https	443	Outbound from User Interface & Device
embedsignage.com	162.13.162.147	https	443	Outbound from User Interface
storage101.lon3.clouddrive.com	94.236.56.96	https	443	Outbound from User Interface
ws://websockets.embedsignage.com*	162.13.157.199	ws	8080 & 80*	Outbound from User Interface & Device
wss://websockets.embedsignage.com*	162.13.157.199	wss	443* & 834	Outbound from User Interface & Device
rackcdn.com**	dynamic	https	443	Outbound from User Interface & Device
analytics.embedsignage.com	134.213.210.78	https	443	Outbound from User Interface & Device

***if the device cannot download content on the network (stuck on downloading files), rackcdn.com may be too generic. In this instance, please approve the account specific unique url for content which can be found in the Account Settings > Firewall Info section.*

**WEBSOCKET PORTS BY FEATURE & PLATFORM*			
Platform	Device Interactions	Channel Sync	Device Controller
iOS	834	834	8080
Android	8080	8080	8080
SSSP + Tizen	8080	8080	80
LG WebOS	80	80	80
macOS	834	834	80
ChromeOS	834	834	80
Windows	834	834	80
ONELAN	834	834	n/a (not available)
BrightSign	8080	834	443

User Responsibility

Users have a responsibility to keep their own passwords protected at all times and not shared with other users. We recommend that all users must be sufficiently trained and provided appropriate levels of access to carry out their allocated duties on the software. We also recommend that each user updates their own password every 60 days and does not leave their account logged in when their desktop / laptop is unattended.