Network Connection Overview

This document is intended as an overview of the operation, security model, and authentication process used by the Your Digital Directory (YDD) Computers and the YDD Digital Signage software application.

Overview

Your Digital Directory (YDD) utilizes a cloud based solution along with local/remote data to deliver media content to display screens. This content can be a combination of video web streaming, XML/javascript data, or media cached locally on a network or computer. If real-time media content is necessary, the YDD computer media player will be calling out when required to update the campaign with the requested information. Media content that is not real-time will be updated after hours to reduce bandwidth consumption.

Connecting to the Digital Signage Cloud Servers

The YDD Digital Signage network cloud is comprised of network servers and routers which are hosted at central data centers. The hosted servers provide all services to your Digital Signage network. The services include authentication, streaming of media files and database services. In order for the YDD Computer Media Player to join this cloud, the Computer Media Player must be registered. Next we insure that the YDD Computer Signage Player can transmit ingress and egress data from and to the digital signage cloud. The following sections will cover requirements for proper operation and transmission of the YDD Computer Signage Player.

Registering into the Digital Signage networks

When the YDD Computer Media Player boots up, the YDD Computer Media Player software is configured to automatically start. On the 1st boot, there will be a prompt to enter your login email and password. Once this information is provided, the Media Player will be associated with your account. After proper authentication is completed, the Media Player will be allowed to join your digital signage network.

Broadband

The YDD Computer Media Player relies on a broadband connection to download all of the campaign's data. This includes RSA authentication, XML configuration and media files. It also uses the broadband to access external data sources such as RSS, video podcasts and other data. It is vital to a successful integration of a digital signage solution that a fast and reliable internet connection is available. We recommend a connection upload minimum speed of 3 mbps and a download minimum speed of 10mbps. It should be noted that the YDD Computer Media Player will work with almost any type of connection however performance may be impacted with less than the minimums mentioned. Additionally, the YDD Computer Signage Player uses internal caching and retry mechanisms to insure smooth playback at all times.

The YDD Computer Media Player will not be affected when internet connection is down given that all resources had an opportunity to cache locally. The YDD Computer Media Player may also be rebooted when no connection exists; in such scenarios the YDD Computer Media Player will roll back to the last good known campaign. However, a fast broadband connection will allow for rapid download of content, smoother transitions into new content and more reliable remote control functionality.

Security

The YDD Computer Media Player uses an elaborate authentication scheme to validate against the Digital Signage servers. Once fully authenticated, the YDD Computer Media Player will be allowed to join the Digital Signage cloud. The YDD Computer Media Player uses 128 bit private and public keys. It is powered by RSA ciphering cryptography to insure maximum security. All tokens used are validated on the server side before they are allowed to pass through. The YDD Computer Media Player stores the authenticated password locally within the local file system as an encrypted key.

Firewall

The YDD Computer Media Player communicates with the hosted servers over TCP/IP. The protocol uses http and https (as well as RSA public / private keys over standard http) and raw sockets. In order to insure proper operation, the YDD Computer Media Player must be allowed to communicate with the hosted servers within the Digital Signage network.

The YDD Computer Media Player does not include an internal firewall and so no special configuration is required. However, if your local area or corporate network does have a firewall, you will need to insure proper rules exist within your firewall to allow traffic originating from the YDD Computer Media Player to pass through.

To allow access to our servers be sure to open type: SOCKET (port range 49152 to 65535), type: HTTP (port 80) and type: HTTPS (port 443) to the destination of: *.signage.me for both inbound and outbound traffic.
If you need explicit rules be sure to add:
54.213.139.226 signage.me
54.200.115.211 galaxy.signage.me
54.213.120.251 earth.signage.me
54.213.45.90 socket.earth.signage.me
54.213.141.167 eris.signage.me
54.213.3.30 socket.eris.signage.me
54.200.232.81 ida.signage.me
54.200.194.110 socket.ida.signage.me
54.200.159.110 ida2.signage.me
54.200.82.139 jupiter.signage.me
54.213.160.58 socket.jupiter.signage.me
54.213.145.191 moon.signage.me
54.213.120.28 socket.moon.signage.me
54.201.214.88 neptune.signage.me
54.200.235.59 socket.neptune.signage.me
54.213.160.52 pluto.signage.me
54.213.159.95 socket.pluto.signage.me

54.200.76.248 sun.signage.me
54.213.151.2 socket.sun.signage.me
54.213.159.84 repository.signage.me
54.213.159.84 repository2.signage.me
52.27.154.185 leda.signage.me
52.27.154.185 adnet.signage.me
54.200.230.159 leda2.signage.me
54.200.230.159 adnet2.signage.me
52.85.158.244
52.85.33.145
52.85.33.189
52.85.5.46
54.182.2.197
54.200.109.147
54.200.133.40
54.200.84.221
54.213.130.252
54.213.152.120
54.213.159.108
54.213.160.58
54.213.47.132
54.213.5.133
54.230.80.224
54.230.80.84
54.213.160.84 secure.digitalsignage.com

Note: If you have a firewall with an existing port 80 rule, this may NOT be enough. The reason is many firewalls will only allow HTTP traffic. However, the YDD Computer Media Player communicates using a persistent TCP/IP socket connection. You may need to add a rule in your gateway / router to specifically allow connection oriented traffic over port 80 (not just HTTP).
You should know opening port 80 on your firewall does not compromise in any way the security of your local area network. Allowing trusted traffic originating from within the LAN onto a specific destination is common practice. It does not induce any potential security breach. This is acceptable and standard procedure in internet security models.

Any questions related to the contents of this document should be sent to greg@yourdigitaldirectory.com

Updated 7/10/20