Security Features

Security Features we have incorporated in the Mediascreen Players:

Exclusively Outbound Traffic

- Mediascreen uses only outbound traffic. No inbound listening port (TCP or UDP) is required.
- Mediascreen does not use port forwarding, DMZ, or UPnP in the network.

Digital Signature Verification for Schedule Files and Configuration Files

- Schedule and Configuration files are digitally signed using RSA encryption keys.
- It is not possible for an attacker to force the Player to play a different schedule file than one generated by the system for this specific device.

HTTPS Certificate checks

- Schedule Files, Configuration Files, and Media Files are downloaded using HTTPS.
- SSL certificate check is enforced throughout the system.

Software Upgrading Verification Checks

- On each software upgrade, software packages downloaded are verified using GPG RSA-based encryption keys.
- Upgrading will fail if verification fails.

Device Firewall

- Devices have a standard firewall policy enabled by default, that only allows inbound SSH access.
- SSH can also be a firewall for the LAN interface, leaving nothing accessible from the LAN, without any service disruption.

HTTP Proxy Authentication Support

- Mediascreen Players support using an HTTP Proxy. The Proxy is required to support the ”CONNECT” method for HTTPS connections.
- Mediascreen supports using authentication credentials for HTTP Proxies.

Customization Scripts

- Device support customization scripts for altering default behavior.
- These are issued remotely as part of the Configuration file which is digitally signed and secured.

VPN for Advanced Remote Support

- For providing advanced remote support, Mediascreen establishes a VPN connection to our online server.
- Only direct communication between the device and the server is allowed, no traffic forwarding or between devices traffic is allowed.
- The VPN service can be permanently disabled without any service disruption, but in cases of severe error, it will degrade our Support Team’s ability for aggressive remote support.

Secure Software Initialization

- The whole SD card that holds the Player software can be re-written through USB on boot. You place a zip file on a USB flash drive, attach it on the Player, and boot it. Upon boot, the Player will self-rewrite the whole SD card.
- Prior to starting this process, the software verifies the integrity and authenticity of the zip file. All images are signed.

Here are a few overall network security precautions that you can take to secure your internal network:

Network segmentation

- The network on which Mediascreen Players are connected to can be segmented and be totally separate from the rest of the local network.
- Mediascreen Player only needs Internet access. No direct local network access is required for any reason.

VLAN

- You can use a separate port-based VLAN on your network to connect Mediascreen Player to the Internet.
- This VLAN will only have access to your router/gateway and no connectivity with the rest of your network will be possible.
- Mediascreen Players do not yet support VLAN tagging, but this can be implemented through a custom script. Port-based VLAN tagging is recommended though.

Inbound Firewalling

- You can configure your firewall to only accept outbound traffic initiated by Mediascreen Players. No Internet-initiated traffic is required.

WiFi Security

- If you use a WiFi network for your Mediascreen Players, many WiFi Access Points and Routers provide features that can help you have a secure setup:
- You can have separate SSIDs, one for the Mediascreen Players, and another for the rest of your network. Different SSIDs can be secured using different WiFi keys/passwords.
- You can set up an SSID to disallow inter-device communications. So, you can have an SSID where all devices connected to it cannot connect to each other, only to the wired network. If you connect the WiFi AP/Router directly to the Gateway, it will only allow Internet access and no access to the rest of the LAN.
- You can use a MAC-based access-list policy so that only specific devices can connect to the WiFi network.
- You should always secure your WiFi networks using WPA. WEP encryption can be easily bypassed, so it is strongly recommended to use WPA/WPA2. (Mediascreen Players support WPA-PSK and WPA2-PSK using passphrases or hex keys. WEP encryption is also supported, but better avoid it.)
- You can always use a completely different WiFi network for Mediascreen Players. Ether landline/cable-based, or even through a 3G router.

MAC filtering

- You can set up your (wired or wireless) network to allow only specific devices to access the network or access the Internet.

Firewall Exceptions Required for restricted networks:

Hostname	Ports	Usage & Comments
hub.dsbackend.com	443/TCP	IoT hub used for communication with Players from the Mediascreen Platform
repo.dsbackend.com	80/TCP	Software Updates repository – no HTTPS required since packages are digitally signed
https://dsbackend.s3.amazonaws.com/	443/TCP	Scheduling Information and Media Downloads (new location)
remote.dsbackend.com	1194/TCP	[optional] Used by our Support Team for advanced remote troubleshooting
widgets.dsbackend.com	443/TCP	[optional] Used by some of our Widgets requiring online info (currently: Weather, Twitter)

IMPORTANT NOTES:

Keep in mind that the repo.dsbackend.com and AWS domains will resolve to multiple IP addresses. You can find those IP addresses using this guide: https://aws.amazon.com/premiumsupport/knowledge-center/s3-find-ip-address-ranges/

In case you are using IP-based firewalls, then, besides the above, you will also need to add the following IP to your firewall exceptions: **108.128.247.33 and 52.210.76.69.**