MOOD HARMONY
NETWORK REQUIREMENTS

v1.10

TABLE OF CONTENTS

Intended Audience

This document is designed for IT professionals interested in learning about the network requirements of Mood's Harmony platform.

Introduction

Mood Media's Harmony platform is a proprietary content management system (CMS) that enables businesses to deliver engaging music and digital signage experiences to their customers. Harmony media players are a key component of this platform—they are a range of purpose-built, solid-state devices that securely connect to the Harmony CMS in the cloud. This document will explore the benefits and advanced security features of the Harmony media player lineup.

Benefits of Harmony Media Players

1. Purpose-Built Hardware

Harmony media players are designed specifically for the task of delivering high-quality audio and video content in commercial environments. Unlike general-purpose computers, these devices are optimized for reliability, performance, and ease of deployment. Key benefits of the purpose-built hardware include:

- Fanless, solid-state design for silent operation and increased durability
- No moving parts, reducing the risk of hardware failure
- Compact form factor for discreet installation in various environments
- Low power consumption, reducing energy costs for businesses
- Hardened security profile to protect against physical and digital threats

2. Scalable Performance

The Harmony media player lineup offers a range of devices with varying levels of performance, ensuring that businesses can select the optimal solution for their specific needs. From expertly optimized players for basic audio playback to high-performance models capable of delivering interactive 4K visual experiences, the Harmony platform can scale to meet the requirements of any business.

3. Flexible Content Management

Harmony media players seamlessly integrate with the Harmony CMS, allowing businesses to manage and update their content remotely. The cloud-based CMS provides a user-friendly interface for scheduling content, creating playlists, and monitoring player status. This flexibility enables businesses to adapt quickly to changing customer preferences and market trends.

4. Local Content Storage and Advanced Network Management

While streaming content is an option, most clients elect to configure their Harmony media players to download content to local storage and play it from there. This approach offers two significant benefits:

1. Reduced network traffic: By downloading content to local storage, the media players do not need to continuously stream content, which minimizes the impact on the client's network.
2. Increased resilience to network outages: With content stored locally, the media players can continue to operate even in the event of a network outage, ensuring uninterrupted in-store experiences.

In addition to local content storage, the Harmony platform allows clients to configure advanced network management features for their media players. These features include:

- Download and maintenance windows: Clients can specify designated time periods during which the media players are authorized to download content, minimizing network impact during peak business hours.
- Bandwidth throttling: Clients can set limits on the amount of bandwidth the media players are allowed to use, ensuring that content downloads do not interfere with other critical network operations.

5. Reliable Connectivity

All Harmony media players connect to the CMS using secure outbound HTTPS (TCP443) calls to https://harmony.moodmedia.com. This ensures that the players can maintain a reliable connection to the CMS without requiring complex network configurations or the need to open inbound ports on firewalls. The outbound-only communication model also reduces the risk of unauthorized access to the players.

Advanced Security Features

1. Secure Boot

Select models of the Harmony media player lineup feature a secure boot process that ensures the integrity of the device's firmware and operating system. This process verifies that the software running on the player has not been tampered with or modified by unauthorized parties. Secure boot helps protect against malware, rootkits, and other threats that could compromise the security of the device.

2. Encrypted Communication

All communication between Harmony media players and the Harmony CMS is encrypted using industry-standard TLS (Transport Layer Security) protocols. This encryption protects sensitive data, such as content and device management information, from interception or tampering by third parties. The use of HTTPS (TCP:443) for all communication ensures that the players can securely connect to the CMS even in networks with strict firewall policies.
Note: other network traffic to 3rd party data sources may be required based on the experience.

3. Hardened Hardware & Operating System

Harmony media players run on a variety of operating systems that have all been specifically configured to minimize the attack surface and reduce the risk of security vulnerabilities.

- Regular patching (see next section)
- Non-essential components, packages, services and programs have been disabled or removed
- All networks ports are closed to inbound traffic (unless otherwise required by the project)
- Content is encrypted in transit and at rest on the device, unless required otherwise by the project
- All models are regularly scanned for known vulnerabilities by Mood's cyber security team using 3rd party software

Beyond those best practices, additional hardening is implemented based on the device's hardware and operating system:

- Manufacturer default passwords have been changed - all passwords for privileged accounts exceeding minimum strength guidelines
- Auto-login and program executions occur on least-privilege accounts/basis
- 3rd party executables must be cryptologically signed in order to be executed with elevated privileges
- OS-level firewalls and security agents are enabled to prevent/detect/protect from unauthorized activity
- Optional: Ability to disable IO on a firmware/hardware level
- Optional: Ability to install 3rd party EDR (Endpoint Threat Detection and Response) agents

4. Regular Software & Security Updates

Mood Media is committed to the continuous development and improvement of the Harmony platform. Its dedicated engineering team works diligently to enhance the features, performance, and security of the system. As part of this commitment, Mood Media's security team continuously monitors for emerging threats and vulnerabilities that could impact the Harmony platform. Security updates and patches are regularly deployed to the media players via the Harmony CMS. While each media player model has its own security life cycle and patching mechanism, Mood Media will regularly upgrade the device's security for as long as the manufacturer provides security updates. In addition, Mood will continue to provide regular software upgrades to the Harmony software running on the media players for the duration of the life of the media player. These software upgrades include new features, bug fixes, performance improvements, and security-related upgrades. To ensure a safe and smooth rollout of these updates, Mood follows a canary deployment process. This approach involves gradually releasing updates to a small subset of players, monitoring their performance, and then progressively deploying the updates to larger groups of players once stability and performance have been verified. This proactive approach to security and software updates, combined with the canary deployment process, ensures that the players remain protected against the latest threats and continue to deliver optimal performance and functionality while minimizing potential disruptions.

Network Requirements

- All mandatory network traffic initiates from the Harmony media player. In other words, the traffic is always outbound from the media player making it safe and easy to operate on a client network.
- Outbound traffic includes: content updates (downloaded and stored locally to the device), optional 3rd party data feeds (e.g. weather, news, POS data, social media feeds, etc), software & security updates, health reporting, device settings and proof of play reporting.
- The following ports must be open for outbound initiated traffic to the following URLs:
    - HTTP/HTTPS TCP80 & TCP443
        - Common to all Harmony models:
            - harmony.moodmedia.com (dynamic IP – CDN)
            - harmony.moodmedia.com/feeds
            - mvision-us.moodmedia.com
        - For Harmony MAVP-B2 & BrightSign units only
            - *.bsn.cloud
            - *.brightsignnetwork.com
    - NTP/UDP123
        - time.nist.gov
        - time.brightsignnetwork.com
        - OR to a Custom NTP Address (i.e. self-hosted NTP server or Google NTP Server)
- Notes:
    - harmony.moodmedia.com is powered by AWS Cloudfront and public IP addresses will vary over time and region. Harmony is hosted in AWS US East (Northern Virginia) Region.
    - bsn.cloud & brightsignnetwork.com domains are required for the Harmony MAVP-B2 and BrightSign media players
- OPTIONAL: **For clients utilizing Mood's Advertising option: the media players must be able to contact the Vibenomics servers 24x7. The Vibenomics app will perform the following functions on the network:
    - Request ads from the Vibenomics platform
    - Download ads from the Vibenomics platform
    - Respond with ad status (proof of play)
    - Diagnostic logging
    - App updates (Download new app versions)
- Outbound HTTPS (TCP443) to:
    - Vibenomics media: media.vibenomics.com

- Vibenomics API: api-prod.vibenomics.com
- Bug reporting service: notify.bugsnag.com