ProMAX MediaHub IT & Security Whitepaper

Contents

MediaHub Overview

The ProMAX MediaHub is a desktop server appliance. MediaHubs are designed to be used in groups of 2 or more, to create a peer-to-peer network where datasets are replicated. This approach is generally used for users requiring large datasets and/or using large files such as Video, Photo, Audio and Design teams. These types of users gain benefits from having a local copy of data, however, that data needs to exist in 1 or more other location for various reasons including collaboration, backup and archive.

MediaHub OS

The ProMAX MediaHub runs a Windows 10 Professional operating system. ProMAX Platform software is installed by default and in most cases, users only access the MediaHub through the ProMAX Platform software. The ProMAX Platform software runs as several local services with an interface run in an locally hosted IIS website. The GUI is accessed through a Chrome or Microsoft Edge (chromium edition) browser. Although, it is a Windows 10 based OS, it is generally handled by users and administrators as an appliance.

Software Installation

The ProMAX MediaHub requires installation of a the ProMAX Listener application on any client device that it will interact with. This software is provided for Windows and Mac clients and runs in the background on each client system that will access data on the MediaHub.

MediaHub Security

All MediaHub have a unique identification key, these keys are used to link MediaHub devices into a unique and private cluster. ProMAX uses publicly available discovery servers to establish an initial connection. If a connection cannot be made to one or more of the paired devices, the software will announce itself and its location on the discovery servers, and begin to search for the missing paired devices via their own announcements. Once paired devices are located, a connection is attempted over TCP or UDP protocols depending on the communication paths available to the devices. Once the cluster is has established direct connections, data will only be passed directly between MediaHub devices and does not flow through any secondary servers. MediaHubs not joined to a specific cluster cannot gain access to data within that cluster.

All data sent between MediaHubs (and Platform servers when used) is encrypted using AES-128 bit TLS 1.3.

Internal storage on a ProMAX MediaHub also supports BitLocker drive encryption. This is optional and can be enabled. BitLocker is disabled by default.

Firewalls and Port Requirements

By default ProMAX MediaHub uses Universal Plug and Play features found in most commercial routers for general NAT translation to enable easy connectivity and will communicate through most firewalls if UPnP is active. If UPnP is unavailable/not activated (almost always the case in an enterprise environment), users will need to forward TCP/UDP 22000 to your mediahub or Platform device. If you have multiple Mediahub devices behind the same firewall, contact ProMAX Support for recommendations.

Antivirus

ProMAX MediaHub ships with Microsoft Defender installed and active. Because the system is running on Windows 10 Pro, most 3rd party antivirus programs can be run on the unit. Note that ProMAX does not test specific 3rd Party Antivirus programs and some programs may adversely affect the sync system. ProMAX recommends that you test appropriately before deploying 3rd Party antivirus to your mediahub clusters.

Active Directory / LDAP

Because ProMAX MediaHub runs on a Windows 10 Pro operating system and can be joined to a domain. By default however, Mediahubs are designed to run as standalone mini-servers in the users homes running local accounts. If you require joining a domain as part of your installation process ProMAX can be engaged for Professional services to assist that process.

VPN Support

MediaHub can utilize existing VPN based network connections to facilitate connectivity to internal networks from outside locations. We do not generally recommend this configuration due to most VPN configurations dramatically reducing available bandwidth. In some cases if security requires, this approach can be used to allow one or more MediaHubs to access other units behind significantly locked down networks. If performance is placed above extreme security, then making direct connections can via port forwarding is the recommended deployment configuration.

Discovery Servers

The ProMAX MediaHub uses a set of publicly available discover servers to establish initial connections and find paired devices while online. Data is not passed through these discover servers at any point.

For organizations wishing to set up a private discovery server, ProMAX offers managed services to help your team configure and deploy a custom discover server. For more information on this please contact your ProMAX representative.

MediaHub Setup

For information on setting up a MediaHub please go to www.promax.com/setup

Additional Requirements?

If your IT requirements go beyond what is outlined in this document, please book time with us at https://www.promax.com/mediahub_security_discussion

IT and Security requirements beyond what is outlined above may be possible, but may require professional services agreements.