Promethean™

ActivConnect™ OPS-G
ActivPanel™

IT Administration Guide

TP-2094-EN-V01

Table of Contents

Introduction and assumptions

Your ActivPanel comes with a powerful Android™ 6.0 (Marshmallow) computing device. Whilst the ActivPanel can be considered by a user as complete seamless device it is essential to understand, from an IT perspective that the panel and the ActivConnect OPS-G are separate components. There are many benefits from an administration, maintenance and upgrade flexibility point of view from this modular approach.

The purpose of this publication is to assist IT administrators in setting up this device for optimal use within your organisation.

The guide assumes that the device has been physically installed and is mounted on the ActivPanel via the appropriate bracket, is powered up and has been connected to the correct USB and HDMI® ports as outlined in the installation guide.

This guide also assumes that the technical terms outlined are understood. To that end this is not an end user guide around usage of the actual device.

Additionally it also assumes that the ActivPanel is switched on and that the device is booted up and showing its home screen.

Note through this guide you will be asked to go into the settings panel numerous times so it's worth getting familiar with how to access it.

Throughout this guide you will be directed to execute this application. It is an essential component for successful configuration of the unit. We highlight the key settings to get you going but if you want to delve deeper we recommend that you research the Android Marshmallow settings articles that exist on the Internet.

The Settings App below allows you to modify the device settings to help meet your organisational needs.

Assuming you are on the home screen of the device you will need to access this settings app.

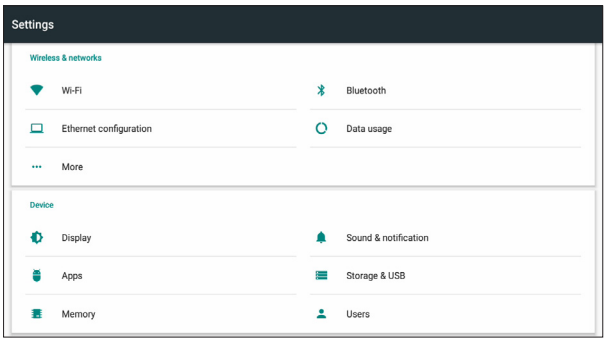
At the bottom right of the home screen you see the app category icon.

Tap this icon.

You will need to find the Settings category. The icon for this category looks like a small cog.

Now tap the settings app within this category.

This opens the settings screen.



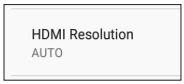
Setting the display

Normally it is not necessary to set the resolution of the display as the device detects the optimal resolution based on the display it is connected to.

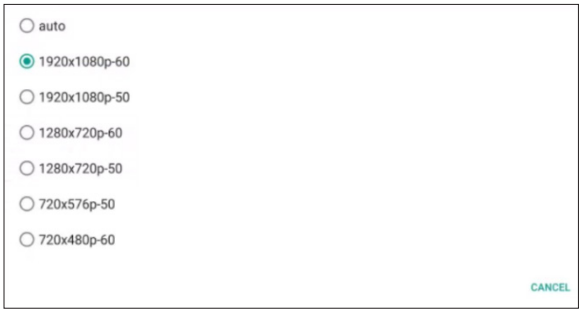
However if you wish to check this or modify then launch the Settings app as described previously in this document and navigate to the Settings screen.

Touch Display.

Then touch HDMI Resolution.



Select your desired resolution and frequency.



The device has Gigabit Ethernet, Dual Band 802.11 a/b/g/n/ac WIFI (RTL8822), and Bluetooth® 4.1 hardware built in.

Depending on how your network infrastructure is deployed you have the option of using Wi-Fi on the device or wired Ethernet. For performance reasons we strongly recommend that you connect the device to a wired connection.

Setting up Wi-Fi (See Appendix for recommended Security Settings)

Launch the Settings app as described previously in this document and navigate to the Settings screen.

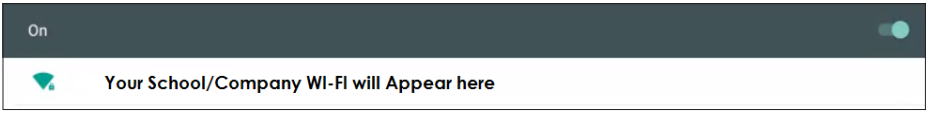
Touch Wi-Fi to open up the settings.

Touch the Wi-Fi toggle button to turn the WI-FI on.

The device will now search for available Wi-Fi Connections.

Available connections appear in the window below the toggle button.

Touch the Wi-Fi network you wish to connect to.



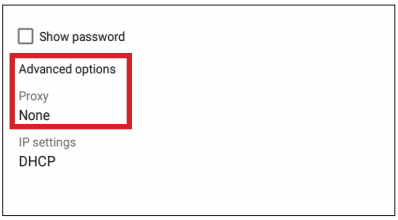
Network Proxy Settings

Continue with the following steps if your organisation uses Network Proxy Settings.

You will need the following information:

- A Proxy Host name or IP address and a Proxy Port Number. If you do not know this, contact your IT department
- If your organisation requires a wireless proxy setting, click on your relevant wireless name (SSID) and the window below appears

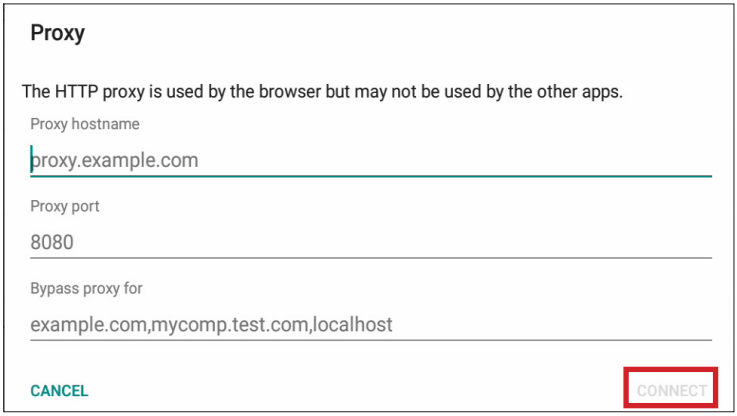
Touch the Advanced options drop-down menu, then touch where it says Proxy.



Touch Manual.

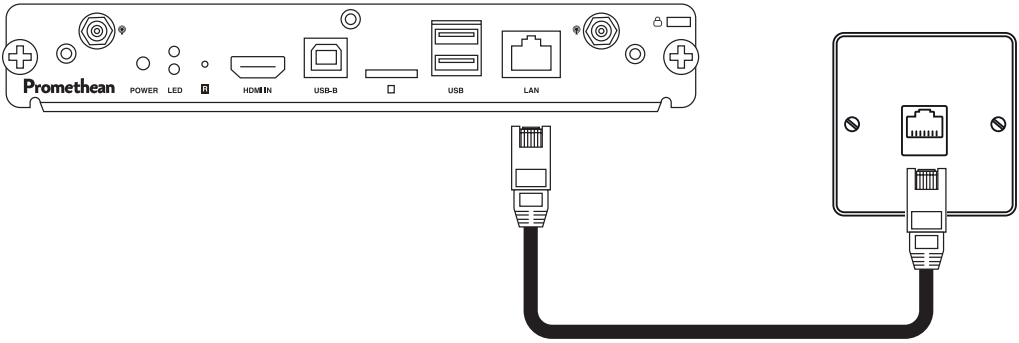
Enter the relevant Proxy settings details below for your wireless network.

Once complete enter your wireless password and touch CONNECT.



Setting up Ethernet (Wired)
(See Appendix for recommended Security Settings)

To create a more reliable and consistent network signal it is recommended that a network cable is also connected from the LAN port on the device to a network port in the classroom/Office.



IMPORTANT NOTE:

If your organisation is running a DHCP (Dynamic Host Configuration Protocol) Server, once a network cable is connected, it will auto assign all the configurations for you. If a DHCP server is not running. Please seek assistance from your IT Department.

NETWORK PROXY SETTINGS

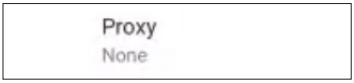
Continue with the following steps if your organisation uses Network Proxy Settings.

You will need the following information:

- A Proxy Host name or IP address and a Proxy Port Number. If you do not know this, contact your IT department.

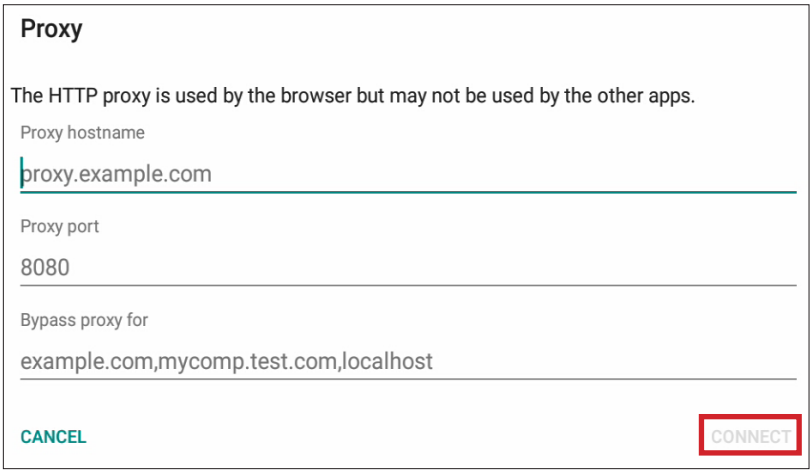
From the Settings screen touch Ethernet configuration.

Touch Proxy.



Touch Manual.

Enter the relevant Proxy settings details for your wired Ethernet Connection (Contact your IT department if you do not know these settings). Once complete, touch CONNECT.



Setting up a hotspot mode

The device can create a small area of Wi-Fi coverage allowing nearby Wi-Fi devices to connect to the Internet/ gain connectivity to it through the hotspot. This may be an option if your internet signal is inconsistent. In addition, this can be used for wireless mirroring. The hotspot itself does not have internet connectivity but if you also connect an Ethernet cable to the device and that has Internet then users can gain access to the Internet by connecting to the hotspot. Depending on your security policies you may or may not want this, so this feature is turned off by default.

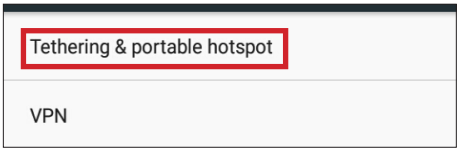
Additionally, this mode can be very useful for mirroring devices even if the internet is not present/desired.

Note the maximum number of devices that can be attached to the device is limited to five at this time.

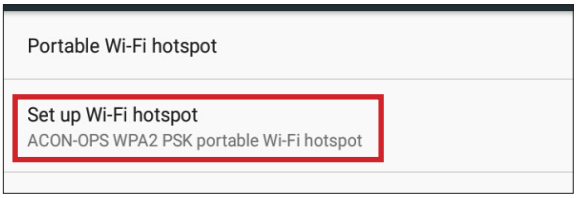
Access the Settings app to set this up. Please refer to the instructions on how to launch the Settings app.

On the Settings screen touch the "More" option.

Touch Tethering & portable hotspot.



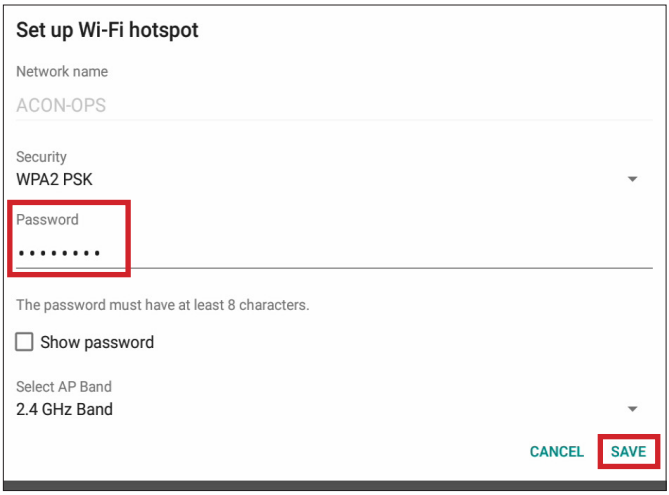
Then touch Set up Wi-Fi hotspot.



The default name of the hotspot (SSID) is ACON-OPS. You may change this to a name of your choosing.

You can also change the security type on this screen.

Enter a Password and touch SAVE.



Touch the Portable Wi-Fi Hotspot toggle button to turn it on.

This will now broadcast the SSID name you configured, and you can now connect to it through the normal process on your connecting devices by choosing the SSID in your wireless settings configuration.

Setting up Bluetooth

The device is equipped with Bluetooth 4.1. It has many applications ranging from short range file transfer to controlling robots and a variety of devices. The default condition is that Bluetooth is disabled. If you need this facility then you can turn it on/off from the Settings screen.

Touch Bluetooth.

Touch the Bluetooth toggle button to turn it on.

Checking the software is up to date

The device has a built in OTA (Over the Air Update) application that periodically scans for new updates and gives the user a choice to accept the update if one exists.

The OTA app however can be executed manually as well.

It is important to accept these updates as we frequently apply security patches and operating system updates alongside feature improvements and enhancements.

NOTE:

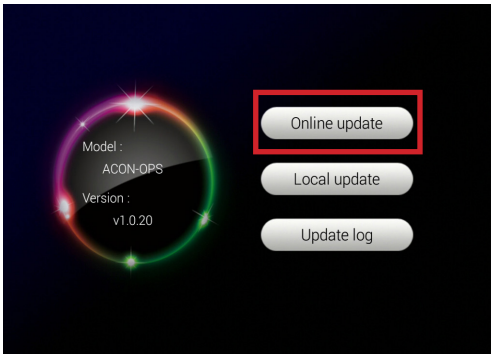
In order for the device to perform regular updates, it is vital that the following URL is whitelisted:
http://cdn-otaupdate.prometheanworld.com.
Whitelisting this URL will ensure that all important updates are downloaded and installed.

Touch the **App** icon on the **Home** screen.

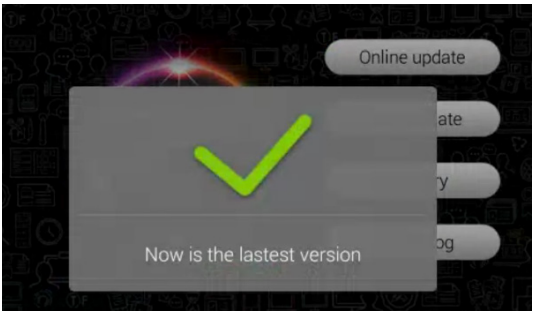
Touch the **Cog** icon to open the Setting screen.

Touch the **Update** icon.

Touch **Online Update.**



Note: If the device already has the latest update installed, a message appears advising you that you are running the most current version.



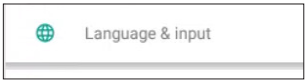
If a new update is available, the system downloads it and you can then proceed to accept the update by tapping the button labelled update.

It is important that you allow the update to be processed. Once this has happened the system automatically reboots and applies the update. Please let the system finish this process, as interrupting it could cause instability of the device in terms of usage.

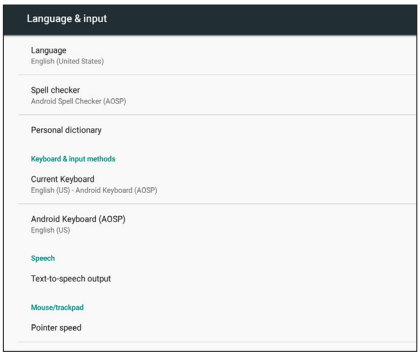
Language and Input

Touch the **Settings** app.

Touch **Language & Input**.



In this section you can set your Language and Keyboard settings specific to your region/country.



Security

Touch the **Settings** app.

Touch **Security**.

Select the Security parameter's that you wish to change.

NOTE:

See the Appendix for Security policy best practices.

Date and Time

Touch the **Settings** app.

Touch **Date & Time.**

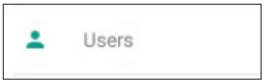
Select the Date and Time specific to your region.

Note: To set your time zone, you must disable The Automatic Time Zone setting first.

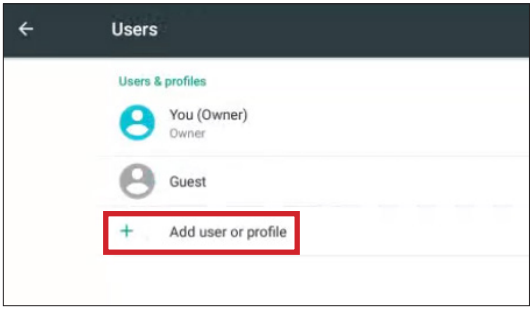
Creating Users

Touch the Settings app.

Touch **Users.**

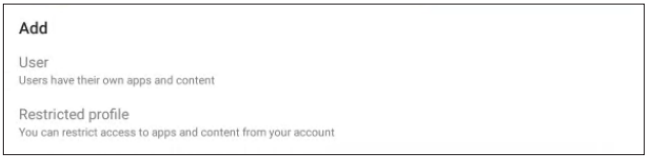


Touch **Add User or Profile**.



You have two options here so choose which option you want to create. For Example:

- **User** - Could be for a member of staff
- **Restricted Profile** - Could be for students



ActivCast™ App (Mirroring)

The Activcast suite of applications allows Windows®, iOS™, Android™ and Chrome OS™ devices to mirror their screens to the ActivCast receiver wirelessly. The ActivCast receiver application is pre-installed on your device and can be executed from the home screen of the device.

For devices that want to transmit their screen to the ActivCast receiver then the sending device needs an application installed to do so. This statement is not strictly true for iOS as Apple® devices have built-in mirroring senders that ActivCast is compatible with. However there are advantages to using the ActivCast sender app. To acquire the ActivCast Senders, please visit this URL and scroll down to the Software downloads section.

https://support.prometheanworld.com/product/activconnect-ops-g

To get instructions on how to mirror your device screen then please visit this article.

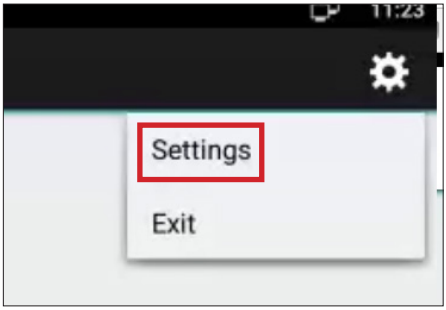
https://support.prometheanworld.com/article/?kb=1532

Device Naming

When you launch the Activcast application from the devices home screen you have the option to rename the receiver identification. We recommend that each device/ActivPanel has its own name. For example, Classroom ActivPanel 1 or Boardroom etc., or whatever naming convention is deemed best practice in your school/company environment. This helps to identify where the devices are located within your school.

Touch the ActivCast icon on the home screen.

Touch the cog icon and then **Settings** in the top right-hand corner of the screen.



Touch the **Device Name** and change the name to the naming convention your school/company has decided on. We also recommend that you set a pin code from this settings screen to provide security. When this is set the sending device will be challenged to enter this code.

For mirroring to work, both the ActivCast receiver and the ActivCast sender have to be connected to a network that can be reached and routable by both the sender and the receiver. This can be wired or wireless. Connecting to a network is established by the operating system on the sender and the receiver using the normal built-in tools of the operating system.

From a security standpoint ActivCast works like any other application on a user's machine. Therefore it is subject to all the security polices of an organisation.

To allow Airplay® to work correctly the following are required:

- If your network employs a firewall it is necessary to set the ActivCast application to be trusted and applies to Domain, Private and public profiles.
- The following ports need to be open and allowed.

  TCP 6000-7000, 7100, 47000, 47010

  UDP 5353, 6000-7000, 7011

Screen Mirroring

Airplay does not require any configuration to be able to find compatible devices on the network, thanks to *DNS-based service discovery*, based on *multicast DNS*, aka **Bonjour**®. However, there are instances when Bonjour or Multicast cannot be supported on a network or when multiple VLAN's and subnets exist. Promethean have developed a technology to allow for these situations and this will be explained later on this document.

Screen mirroring is achieved by transmitting an **H.264** encoded and AES 128bit encrypted video stream over a TCP connection.

This stream is packetized with a 128-byte header. **AAC-ELD** audio is sent using the Airplay protocol. As for the master clock, it is synchronized using **NTP**.

Moreover, as soon as a client starts a video playback, a standard Airplay connection is made to send the video URL, and mirroring is stopped. This avoids decoding and re-encoding the video, which would incur a quality loss.

HTTP requests

Screen mirroring connects to a hard-coded port 7100. This is a HTTP server which supports the following requests:

POST /stream

Start the live video transmission. The client sends a binary property list with information about the stream, immediately followed by the stream itself. At this point, the connection is no longer a valid HTTP connection.

As soon as the server receives a **/stream** request, it will send NTP requests to the client on port 7010, which is hard-coded as well. The client needs to export its master clock there, which will be used for audio/video synchronization and clock recovery.

Stream Packets
The video stream is packetized using 128-byte headers, followed by an optional payload.

Codec Data
This packet contains the H.264 extra data in **avcC** format *(ISO/IEC 14496:15)*. It is sent at the beginning of the stream, each time the video properties might change, when screen orientation changes, and when the screen is turned on or off.

Time Synchronization
Requests are sent to the Airplay client at 3 second intervals. The reference date for the timestamps is the beginning of the mirroring session.

Password Protection
An Airplay server can require a password for displaying any content from the network. This is implemented using standard **HTTP Digest Authentication** *(RFC 2617)*, over HTTP for everything.

This password protection is implemented automatically by ActivCast.

Discovery
The ActivCast senders that work with ActivCast receivers need to establish which ActivCast receiver they want to mirror to.

There are four main ways to identify the ActivCast receiver:

- By its name
- By a QR code
- By a connection id
- By its IP address

All of these items can be found on the ActivCast receiver app main screen.

The reason why there are different ways for your device to make a connection to the ActivConnect is down to the way networks are configured.

Name of Receiver
Let us say that your ActivConnect is called “Classroom” .

This name is broadcasted over the network(s) that the ActivCast receiving app is connected to.

Your ActivCast sender application installed on your device is “waiting” for these names.

Once a name comes in it is listed. You can simply click it and then you will be connected.

However, some networks block this broadcast which is called Bonjour. You never see this name.

By QR code
If you have a tablet/phone and launch the ActivCast sender app you can scan the code displayed on the AC screen.

This code contains all the information needed to make a connection.

Your device still needs to be on a network that the ActivCast receiver is also connected to, but this eliminates the need to worry about the bonjour broadcast.

A Connection ID

This method also eliminates the need to have Bonjour working on your network. It is very similar to the QR code available on mobile in so much that it creates a database entry for your ActivCast device and a connection ID that is used to lookup the information.

Here is a high level workflow...

The ActivCast application contacts a cloud server at promethean.api.splashtop.com and passes its name and IP address(s) for the networks that it is connected to. The cloud server then creates a connection ID and ActivCast receiver displays this.

Now on your sending device you can use the ActivCast application and tap the icon that allows you to enter the connection ID.

Once the user types this in that connection ID is again sent to the cloud service mentioned above from the user's device. It looks up this ID in its database and sends the name and IP address back the sender which in turn creates the connection.

The devices have to be on the same network that the ActivCast receiver unit is connected to.

This method does not work if either the ActivCast receiver or the sending device do not have an internet connection to reach the cloud service. Additionally, if there is a firewall or proxy set up on your network(s) then it might block the promethean.api. splashtop URL. In this case IT should be able to "whitelist" this URL.

By IP address

This makes a direct connection without the need to visit a cloud server or use bonjour.

Your sending device has to be able to reach the IP address displayed. You have to be on one of the networks that the ActivCast receiver is attached to.

Performance Tuning for Mirroring

There are many factors involved when considering the performance of wirelessly sending device screen data over a network to a receiving device.

It is often cited by user that when using such wireless mirroring protocols at home that everything works well in terms of being able to send their screen to the TV without a hitch. When users try and obtain the same experience at work/school things can be very different!

One of the fundamental issues is that organisational requirements in terms of networking have to take security, bandwidth, and segmentation of networks as a serious concern. There are a myriad of reasons why a slick demo on a dedicated network often shows stunning performance only to fall short of the desired result when rolled out at scale in a real environment.

The current state of wireless presentation solutions within the market are all vulnerable to these conditions.

To that end, we want to ensure that you and your users are aware of the stumbling blocks that can occur when using a mirroring application so that you can set expectations accordingly.

The section within this document that explains the network requirements is really only concerned with the discovery phase and goes into great detail around this aspect. If we assume that the discovery phase of a sender and a receiver have made a connection, we have to now concentrate on the actual transmission of the sending device screen data to the receiver.

Bandwidth requirements

To make a simple assumption that a device is sending its screen over the network at 1080p then we could calculate that the network should be able to handle 8 Mbps to transmit this data and the receiver to display it.

If a user wants to stream a 1080p video at 25 frames per second you could declare that 20 Mbps would be sufficient.

This is assuming a handful of users are performing these actions, the wireless infrastructure is not being swamped by other activity, and you have good coverage and great bandwidth.

This particular topic cannot be covered in depth within this document and neither do Promethean declare that the ActivCast app, or any other comparable commercial mirroring technology out in the wild using normal networks, can guarantee pristine performance in every condition.

To reiterate, the ActivCast sender / native Airplay sender compresses the screen data and then transmits that data over an unknown environment.

The receiver then decodes that data and renders it to the screen.

We believe we have optimised the compression and the decoding but have no ability to influence the network.

With all that said and done there are some hints and tips on how to improve performance if needed.

Use Ethernet connections

Ethernet is still the most reliable connection type. Whilst this may seem odd to suggest a wired connection for a wireless system, it is highly recommended that your ActivCast receiving device is hard wired.

Wi-Fi Connection

Check for wireless network interference. Make sure the sending device is using the fastest 802.11 mode it can handle. Switch to 5 GHz mode and ensure that the router is configured for optimal Airplay usage.

This is not an exhaustive list as there are other environmental considerations to take into account.

Sending device display resolution

Your sending device could well be operating at such a high resolution that your network can't handle it. If you are trying to send a 4k screen over to the receiver then it's highly likely that your network cannot handle this amount of data. Consider reducing the resolution of the sending device until you achieve acceptable performance.

Bluetooth

Because the Bluetooth and 802.11 wireless are controlled by the same interface and have adjoining antennas, the two have the potential to interfere with each other when they are both in use. It is recommended that Bluetooth is switched **OFF** on **both** devices whilst mirroring.

APPENDIX: Passcodes and Security Policy

"Passcodes or Passphrases are not the same as passwords. A passcode/Passphrase is a longer version of a password and is therefore, more secure. A passcode/Passphrase is typically composed of multiple words, because of this, a Passcode/Passphrase is more secure against attacks and forms an integral part of the security system of a device"

Overview

Passcodes are an important aspect of computer security. A poorly chosen passcode may result in unauthorized access and/or exploitation of <Company/School Name>'s resources. All users, including contractors and vendors with access to <Company/School Name> systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

IT professionals are also responsible to ensure device security on the network is robust and disaster recoverable, and meets the organization's regulations.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passcodes on the ActivPanel / ActivConnect OPS-G, as well as how to protect those passcodes, and understand the frequency of changing the passcodes.

The policy also outlines device security best practices to adopt on the ActivPanels/ActivConnect OPS-G.

Scope

The scope of this policy includes all personnel (end-users/IT administrators) who have or are responsible for an account on ActivPanels/ActivConnect OPS-G that has access to <Company/School Name> facility, and has access to the <Company/School Name> network.

1.0 Policy

1.1. Passcode Creation/Screen Security: (Screen Lock: default set to 5 seconds after sleep button pressed)

All user-level and system-level passcodes must conform to the (Company/School Name) Regulations. For example, Simple, Numeric, Alphanumeric, Complex alphanumeric and Special Character Pattern. Minimum length between 1 and 16 characters' long. A good passcode is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

1.2. Passcode Change: For example, root, enable, admin, application administration accounts, recommended be changed every quarter or based on your organization's regulations.

1.3. Passcode visibility: It is recommended that this function is disabled.

1.4. User-level passcodes: The recommended change interval is every 30 days or based on your organization's regulations.

1.5. Passcode Protection/Passcode-Re-use: Prevent passcodes from being used two or three times

1.6. Passcodes: Please do not share your passcode with anyone. All passcodes are to be treated as sensitive, Confidential <Company/School Name> information.

1.7. Passcodes: Please do not insert passcodes into email messages, Alliance cases or other forms of electronic communication.

1.8. Do not reveal a passcode on questionnaires or security forms.

1.9. Do not hint at the format of a passcode (for example, "my family name").

1.10. Do not share <Company/School Name> passcodes with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

1.12. Do not write passcodes down and store them anywhere in your office. Do not store passcodes in a file on a computer system or mobile devices (phone, tablet) without encryption.

1.13. Any user suspecting that his/her passcode may have been compromised must report the incident to IT and change all passwords.

1.14. Auto Lock: ActivPanels/ActivConnect OPS-G. After 15 minutes of inactivity the ActivPanels are recommended to be set to auto lock, avoiding access to potentially sensitive data from third parties.

1.15. Antivirus: All ActivPanels/ActivConnect OPS-G must be protected by Antivirus Software to avoid threats from Mobile USB equipment and external web sites/apps. Antivirus is set to scan applications and or media on first install.

1.16. Device Encryption: It is recommended on ActivPanels/ActivConnect OPS-G to protect confidential digital data stored on device.

1.17. Installation of unknown sources: Default set to block installation of unknown Apps. Recommended to keep this setting to mitigate against potential threats.

1.18. Notifications: It is recommended to not show any notifications when the ActivPanels/ActivConnect OPS-G is locked (i.e. sensitive information/emails).

1.19. Backup and Reset: If the ActivConnect OPS-G is compromised, it is recommended that the application administration accounts perform the needed actions.

2.0 User Requirements

2.1. Users must only load data that is relevant and essential to their role onto the ActivPanels/ActivConnect OPS-G.

2.2. Users must report all breakages/malfunctions to the IT department immediately.

2.3. If a user suspects that unauthorized access to school/company data has taken place via the ActivPanels/ActivConnect OPS-G, the user must report the incident in alignment with <School/ Company >'s incident handling process.

2.4. ActivPanels/ActivConnect OPS-G must not have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

2.5. Users must not load pirated software or illegal content onto the ActivPanels/ActivConnect OPS-G.

2.6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact your IT department.

2.7. ActivPanels/ActivConnect OPS-G must be kept up-to-date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.

2.8. ActivPanels/ActivConnect OPS-G must not be connected to a PC which does not have up-to-date and enabled Anti-Virus malware protection and which does not comply with corporate/school policy.

2.9. Devices must be encrypted in line with <schools/Company X>'s compliance standards.

2.10. Users must be cautious about the merging of personal and work email accounts on the ActivPanels/ ActivConnect OPS-G. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify <Company X> IT immediately.