Promethean™

ActivConnect™ G-Series

ActivPanel™

Руководство по интеграции для ИТ-администраторов

TP-2046-RU-V01

Содержание

Введение и допущения

Панель ActivPanel поставляется вместе с мощным вычислительным устройством на базе Android™ 5.1 (Lollipop). Пользователь может расценивать ActivPanel как единое устройство, однако с точки зрения ИТ панель и ActivConnect G-Series представляют собой отдельные компоненты. Модульный подход обеспечивает гибкость при установке, обслуживании и модернизации устройства.

Настоящий документ призван помочь ИТ-администраторам настроить данное устройство для оптимального использования в вашей организации.

Руководство предполагает, что устройство было физически установлено и прикреплено к ActivPanel с помощью соответствующего кронштейна, подключено к источнику питания и подсоединено к правильным портам USB и HDMI®, как указано в руководстве по установке.

Настоящее руководство также предполагает, что изложенные технические условия являются понятными. Исходя из этого, данный документ не является руководством конечного пользователя и не описывает применения самого устройства.

Кроме того, предполагается, что панель ActivPanel включена, устройство загружено и отображает домашний экран.

Приложение Настройки

Обратите внимание, что настоящем руководстве вам будет неоднократно предложено открыть панель настройки. Поэтому с самого начала необходимо ознакомиться с процедурой доступа к ней.

В настоящем руководстве вы получите инструкции по работе в этом приложении. Это важный компонент для успешной конфигурации устройства. Для начала работы мы выделили основные настройки. Если вы хотите подробнее ознакомиться с процессом, мы рекомендуем вам воспользоваться статьями, посвященными настройкам Android Lollipop, которые представлены в Интернете.

Приложение Настройки позволяет изменять настройки устройства в соответствии с потребностями вашей организации.

Когда вы находитесь на главном экране устройства, вам необходимо открыть приложение для настройки.

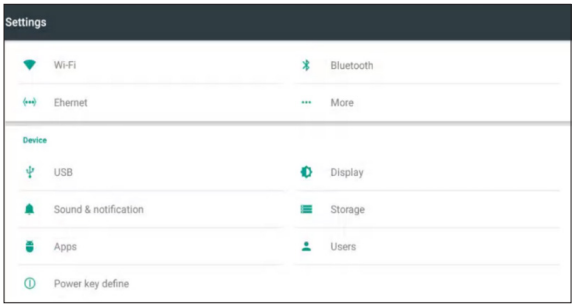
В правом нижнем углу главного экрана расположен значок категории приложения.

Нажмите его.

Теперь вам необходимо найти категорию Настройки. Значок этой категории выглядит как маленькая шестеренка.

Нажмите приложение настройки в этой категории.

Откроется экран с настройками.



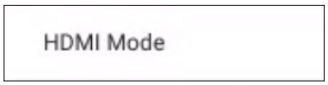
Настройка экрана

Как правило, нет необходимости устанавливать разрешение экрана, так как устройство определяет оптимальное разрешение в зависимости от того, к какому экрану оно подключено.

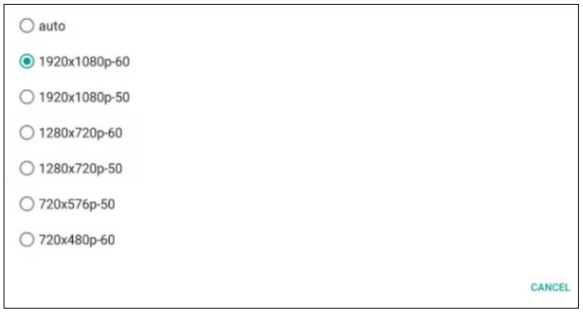
Однако если вы хотите проверить разрешение или изменить его, запустите приложение Настройки, как описано выше в данном документе, и перейдите к экрану Настройки.

Нажмите Экран.

Затем нажмите Режим HDMI



Выберите необходимое разрешение и частоту.



На устройстве установлено следующее аппаратное обеспечение: сетевая плата Gigabit Ethernet, двухполосный Wi-Fi® маршрутизатор с поддержкой стандарта 802.11 b/g/n/ac (AP6335) и устройство Bluetooth® 4.0.

В зависимости от того, как развернута инфраструктура сети, у вас есть возможность использовать Wi-Fi на устройстве или проводной Ethernet. Из соображений производительности мы настоятельно рекомендуем использовать проводное соединение.

Настройка Wi-Fi (рекомендуемые настройки безопасности представлены в разделе Приложение)

Запустите приложение Настройки, как описано выше в данном документе, и перейдите к экрану Настройки.

Нажмите Wi-Fi, чтобы открыть настройки.

Нажмите кнопку-переключатель Wi-Fi, чтобы включить соединение.

Устройство выполнит поиск доступных сетей Wi-Fi.

Они появятся в окне, расположенном под кнопкой-переключателем.

Нажмите сеть Wi-Fi, к которой вы хотите подключиться.

Параметры прокси-сервера сети

Выполните следующие действия, если в вашей организации используются настраиваемые параметры прокси-сервера сети.

Вам потребуется следующая информация:

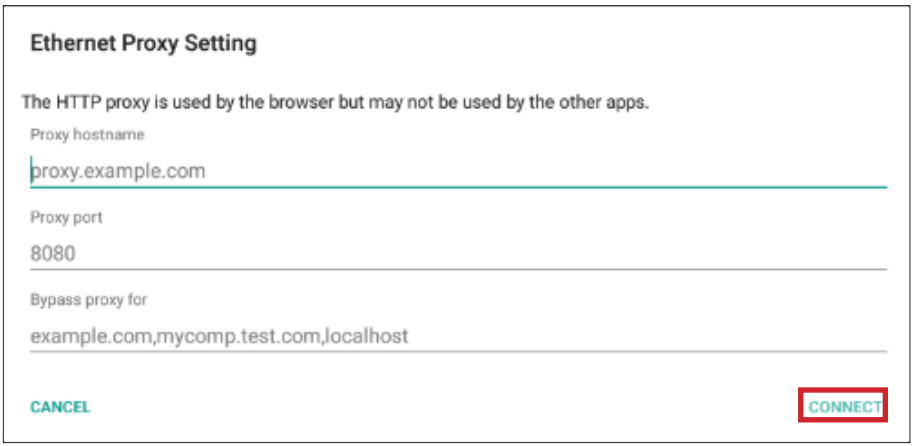
- Имя хоста прокси-сервера или IP-адрес и номер порта прокси-сервера. Если вы не располагаете такой информацией, обратитесь в ваш отдел ИТ
- Если в вашей организации используются настраиваемые параметры прокси-сервера беспроводной сети, нажмите соответствующую беспроводную сеть (SSID), появится такое окно

Нажмите пункт Дополнительные параметры, а затем выберите Прокси.

Нажмите Вручную.

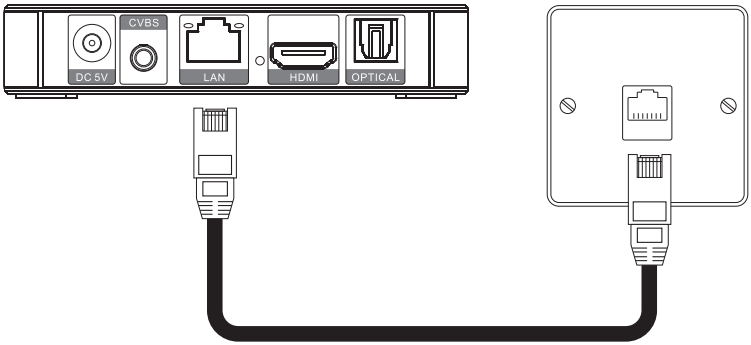
Введите соответствующие параметры прокси-сервера для вашей беспроводной сети.

После завершения введите пароль от беспроводной сети и нажмите Подключиться.



Настройка Ethernet (проводное подключение) (рекомендуемые настройки безопасности представлены в разделе Приложение)

Для того чтобы создать более надежный и непрерывный сигнал сети, рекомендуется соединить сетевым кабелем порт LAN на устройстве и сетевой порт в классе/кабинете.



ПРИМЕЧАНИЕ

Если в вашей организации запущен сервер DHCP (протокол динамической настройки узла), то при подключении сетевого кабеля он будет автоматически назначать все конфигурации. Если сервер DHCP не запущен, обратитесь в ваш отдел ИТ.

ПАРАМЕТРЫ ПРОКСИ-СЕРВЕРА СЕТИ

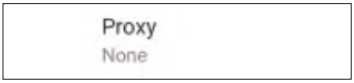
Выполните следующие действия, если в вашей организации используются настраиваемые параметры прокси-сервера сети.

Вам потребуется следующая информация:

- Имя хоста прокси-сервера или IP-адрес и номер порта прокси-сервера. Если вы не располагаете такой информацией, обратитесь в ваш отдел ИТ.

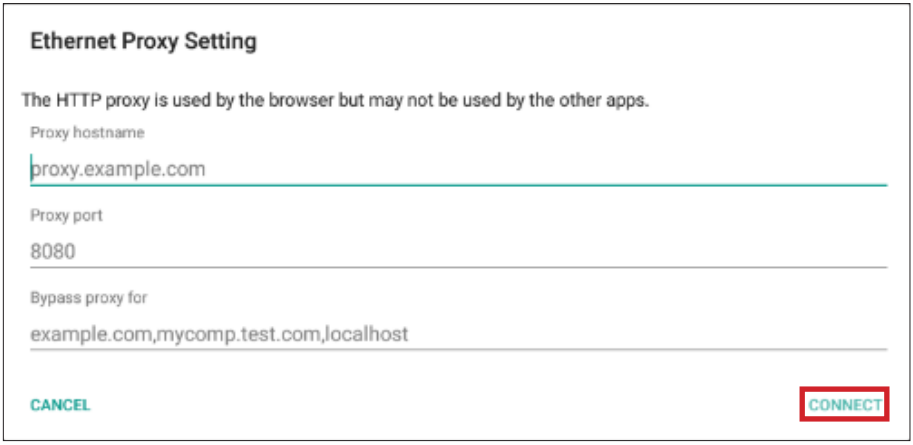
На экране Настройки нажмите Ethernet.

Выберите Прокси.



Нажмите Вручную.

Введите соответствующие параметры прокси-сервера для подключения к проводной сети Ethernet (обратитесь в ваш отдел ИТ, если вы не располагаете такой информацией). По завершении нажмите Подключиться.



Настройка режима точки доступа

Данное устройство может создавать небольшую зону покрытия Wi-Fi, позволяющую находящимся поблизости устройствам с возможностью подключения по Wi-Fi устанавливать соединение с Интернетом или самим устройством через точку доступа. Этот вариант подходит в ситуациях, когда интернет-сигнал нестабилен. Кроме того, он может использоваться для зеркалирования по беспроводной сети. Сама точка доступа не имеет подключения к Интернету. Однако если вы подключите устройство к Интернету через кабель Ethernet, то пользователи смогут получить доступ в сеть, подключившись к точке доступа. Использование этой функции зависит от принятой в вашей организации политики безопасности, поэтому она отключена по умолчанию.

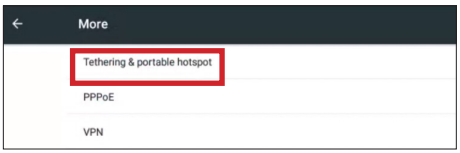
Кроме того, этот режим может быть очень полезен для зеркалирования устройств, даже если подключение к Интернету отсутствует или нежелательно.

Обратите внимание, что в настоящее время к устройству можно подключить не более пяти устройств.

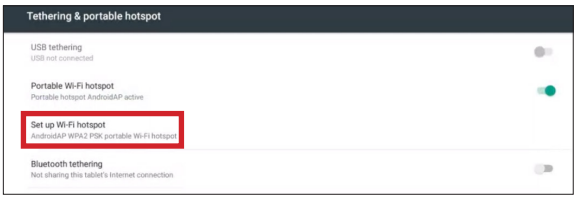
Откройте приложение Настройки. Инструкция по запуску данного приложения представлена выше.

На экране Настройки нажмите пункт «Дополнительно».

Выберите Режим модема и точка доступа



Затем нажмите Настройка точки доступа к Wi-Fi.

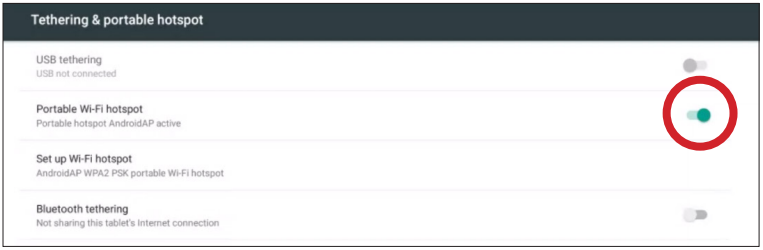


По умолчанию точка доступа (SSID) названа AndroidAP. Вы можете изменить это имя по своему усмотрению.

Также на этом экране можно изменить тип безопасности.

Введите пароль и нажмите Сохранить.

Нажмите кпопку-переключатель напротив пункта Точка доступа к Wi-Fi, чтобы включить ее.

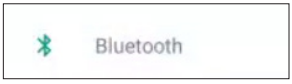


Устройство начнет передавать настроенное вами имя SSID. Теперь с других устройств можно подключиться к сети стандартным способом – необходимо выбрать SSID в конфигурации настроек беспроводной сети.

Настройка Bluetooth

Данное устройство поддерживает возможность связи по Bluetooth версии 4.0. Ее можно применять по-разному: передавать файлы на небольшом расстоянии, управлять роботами и различными устройствами. По умолчанию устройство Bluetooth отключено. При необходимости его можно включить и выключить на экране Настройки.

Выберите Bluetooth.



Нажмите кпопку-переключатель напротив пункта Bluetooth, чтобы включить связь.

Проверка актуального состояния программного обеспечения

Устройство имеет встроенное приложение OTA (Беспроводное обновление), которое периодически проверяет наличие обновлений и позволяет пользователю выполнить обновление, если обнаруживает его.

Также работу в приложении OTA можно выполнить вручную.

Необходимо выполнять обновления, так как в них часто включаются исправления системы безопасности, обновления операционной системы, а также усовершенствования функций.

ПРИМЕЧАНИЕ

Для выполнения регулярных обновлений устройства необходимо добавить следующий URL-адрес в белый список:
http://cdn-otaupdate.prometheanworld.com.
Таким образом можно гарантировать, что все важные обновления будут загружены и установлены.

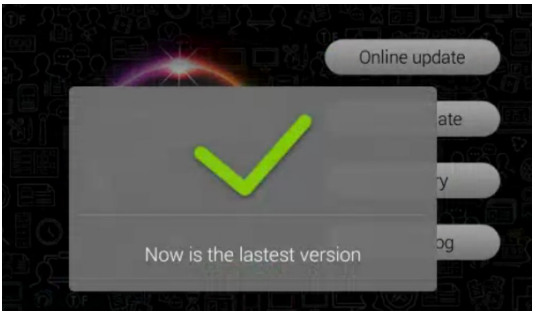
Нажмите значок **Приложение** на экране **Главный**.

Выберите значок **Шестеренка**, чтобы открыть экран Настройки.

Нажмите значок **Обновление**.

Выберите пункт **Обновление через Интернет**.

Примечание. Если на устройстве уже установлено последнее обновление, появится соответствующее сообщение.



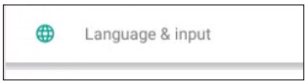
При наличии обновления система загружает его, после чего вы можете установить его, нажав соответствующую кнопку.

Важно дождаться окончания процесса обновления. После этого система автоматически перезагрузится и применит обновление. Дождитесь завершения процесса, так как его прерывание может привести в дальнейшем к нестабильной работе устройства.

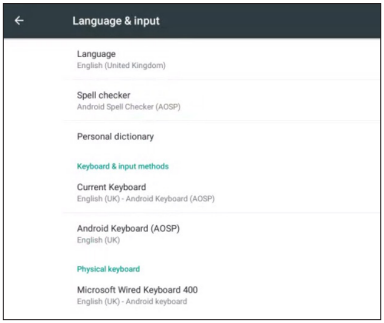
Язык и ввод

Нажмите значок приложения **Настройки**.

Выберите **Язык и ввод**.



В этом разделе вы можете установить язык и задать настройки клавиатуры для вашего региона/страны.



Безопасность

Нажмите значок приложения **Настройки**.

Выберите **Безопасность**.

Выберите параметр безопасности, который необходимо изменить.

ПРИМЕЧАНИЕ

Рекомендации по настройке безопасности представлены в разделе Приложение.

Дата и время

Нажмите значок приложения **Настройки**.

Выберите **Дата и время**.

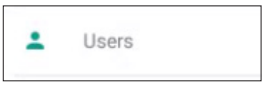
Выберите дату и время вашего региона.

Примечание. Чтобы установить часовой пояс, необходимо сперва отключить параметр Автоматически определять часовой пояс.

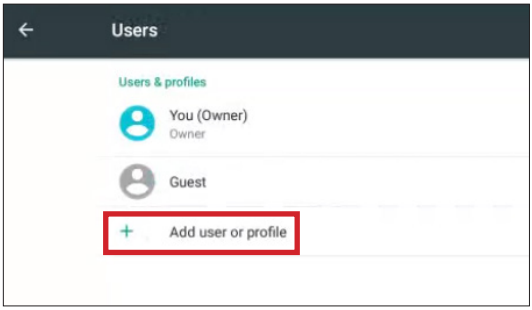
Создание пользователей

Нажмите значок приложения **Настройки**.

Выберите **Пользователи**.

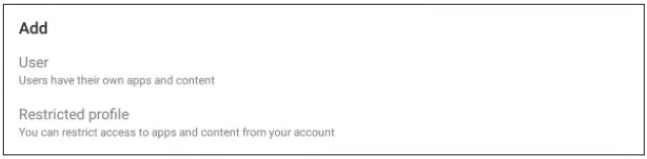


Нажмите **Добавить пользователя или профиль**.



Выберите из двух предлагаемых вариантов. Например:

- **Пользователь** – может являться сотрудником
- **Профиль с ограничениями** – может являться учеником



Приложение ActivCast™ (зеркалирование)

Пакет приложений Activcast позволяет устройствам с Windows®, Mac OS X®, iOS™, Android™ и Chrome OS™ дублировать их экраны на приемник ActivCast по беспроводной сети. Приложение для приемника ActivCast предустановлено на устройстве и может быть запущено с главного экрана.

На устройствах, с которых необходимо передавать изображение экранов на приемник ActivCast, должно быть установлено соответствующее приложение. Это не относится к устройствам с iOS и Mac OS X, так как устройства Apple® имеют встроенные средства для зеркалирования, совместимые с ActivCast. Однако у приложения для передатчика ActivCast есть свои преимущества. В настоящее время не существует передатчика ActivCast для Mac OS X, так как в этой операционной системе имеется встроенный передатчик. Если вы хотите использовать дополнительные функции передатчика ActivCast, рекомендуем воспользоваться браузером Chrome в OS X с установленным модулем передатчика ActivCast.

Чтобы загрузить передатчики ActivCast, перейдите по указанной ссылке и прокрутите страницу вниз до раздела Загрузка ПО.

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

Инструкции по зеркалированию экрана устройства представлены в следующей статье.

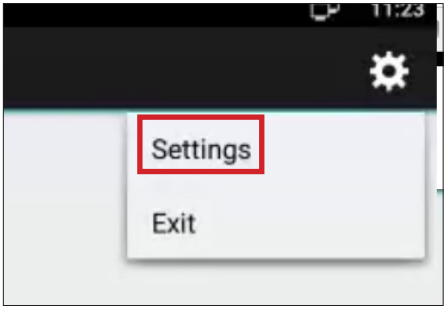
https://support.prometheanworld.com/article/?kb=1532

Присвоение имен устройствам

При запуске приложения ActivCast с главного экрана устройства у вас есть возможность переименовать идентификатор приемника. Для каждого устройства/ActivPanel рекомендуется задать отдельное имя. Например, Classroom ActivPanel 1, Boardroom или любое другое название, рекомендованное к использованию в вашем учебном заведении или компании. Это поможет определить, где именно находятся устройства.

Нажмите значок ActivCast на главном экране.

Нажмите значок в виде шестеренки и выберите **Настройки** в правом верхнем углу экрана.



Нажмите **Имя устройства** и измените его в соответствии с принятым в школе/компании порядком наименования. Также в целях обеспечения безопасности мы рекомендуем вам установить пин-код в этом же разделе. При его наличии на передающем устройстве нужно будет указать пин-код перед работой.

Требования к сети для зеркалирования

Для зеркалирования приемник ActivCast и передатчик ActivCast должны быть подключены к сети, доступной для обоих устройств. Данная сеть может быть проводной и беспроводной. Подключение к сети устанавливается через операционную систему передатчика и приемника с помощью стандартных встроенных средств операционной системы.

С точки зрения безопасности ActivCast работает так же, как и любое другое приложение на компьютере пользователя. Поэтому на его работу распространяются требования политики безопасности, принятой в организации.

Для корректной работы Airplay® требуется следующее:

- Если в вашей сети используется брандмауэр, необходимо внести приложение ActivCast в список доверенных. Это применимо к домену, частным и общим профилям.
- Необходимо открыть следующие порты и разрешить соединение с ними.

  TCP 6000-7000, 7100, 47000, 47010

  UDP 5353, 6000-7000, 7011

Зеркалирование экрана

Airplay не требует отдельной настройки для того, чтобы находить совместимые устройства в сети благодаря *технологии обнаружения сервисов на основе DNS*, основанной на *многоадресной DNS*, известной также, как **Bonjour®**. Однако бывают случаи, когда Bonjour или Multicast не поддерживаются в сети или когда имеется несколько сетей VLAN и подсетей. В Promethean разработали технологию, учитывающую такие ситуации. Она будет описана далее в этом документе.

Зеркалирование экрана достигается путем передачи видеопотока с кодировкой **H.264** и 128-разрядным шифрованием AES через соединение TCP.

Данный поток пакетирован с помощью 128-байтного заголовка. Аудио в формате **AAC-ELD** отправляется через протокол Airplay. Тактовый генератор синхронизируется с помощью **NTP**.

Кроме того, когда клиент начинает проигрывать видеозапись, создается стандартное подключение Airplay для отправки URL-адреса видео, а процесс зеркалирования прекращается. Это позволяет избежать декодирования и повторного кодирования видео, которое приводит к потери качества.

Запросы HTTP

Зеркалирование экрана подключается к жестко запрограммированному порту 7100. Это сервер HTTP, который поддерживает следующие запросы:

POST /поток

Начните прямую передачу видео. Клиент отправляет список бинарных свойств с информацией о потоке, за которым сразу же следует сам поток. С этого момента соединение более не является допустимым соединением HTTP.

Как только сервер получает запрос **/stream**, он начинает посылать клиенту запросы NTP на порт 7010, который также жестко запрограммирован. Клиент должен экспортировать туда тактовый генератор, который будет использоваться для синхронизации аудио и видео и восстановления тактовой частоты.

Пакеты потоков

Видеопоток пакетирован с помощью 128-байтных заголовков. За ним следует необязательная полезная нагрузка.

Данные кодеков

Этот пакет содержит дополнительные данные H.264 в формате **avcC** *(ISO/IEC 14496:15)*. Он отправляется в начале потока каждый раз при изменении свойств видео, при изменении ориентации экрана и при включении и выключении экрана.

Синхронизация времени

Запросы отправляются клиенту Airplay с интервалом в 3 секунды. Исходной датой для временных меток является начало сессии зеркалирования.

Защита паролем

Сервер Airplay может потребовать пароль для отображения любого содержимого из сети. Это реализовано с помощью стандартной дайджест-аутентификации **HTTP Digest Authentication** *(RFC 2617)* через HTTP для всех операций.

Защита паролем осуществляется автоматически с помощью ActivCast.

Технология обнаружения

Передатчикам ActivCast, работающим с приемниками ActivCast, необходимо установить, через какой приемник ActivCast требуется осуществить зеркалирование.

Существуют четыре основных способа идентификации приемника ActivCast:

- По имени
- По QR-коду
- По идентификатору соединения
- По IP-адресу

Все эти пункты можно найти на главном экране приложения для приемника ActivCast.

Наличие разных способов подключения устройства к ActivConnect обусловлено настройкой сетей.

Имя приемника

Предположим, что устройство ActivConnect называется «Classroom».

Это имя транслируется в сети или сетях, к которым подключено приложение приемника ActivCast.

Приложение передатчика ActivCast, установленное на устройстве, находится в режиме «ожидания» этих имен.

Как только имя появляется, оно заносится в список. Для соединения достаточно просто нажать на имя.

Однако некоторые сети блокируют эту передачу, которая называется Bonjour. Это имя никогда не отображается.

По QR-коду

При запуске приложения передатчика ActivCast на планшете/телефоне можно просканировать отображаемый на экране AC код.

Этот код содержит всю информацию, необходимую для установления соединения.

Устройство по-прежнему должно находиться в сети, к которой также подключен приемник ActivCast. В этом случае не нужно беспокоиться о передаче Bonjour.

Идентификатор соединения

Для этого способа также не нужно наличие Bonjour в сети. Он очень схож с соединением с помощью QR-кода, доступным на мобильных устройствах. В базе данных для вашего устройства ActivCast создается запись и идентификатор соединения, который используется для поиска информации.

Схема работы выглядит следующим образом.

Приложение ActivCast устанавливает связь с облачным сервером на веб-сайте promethean.api.splashtop.com и передает свое имя и IP-адрес(а) для сетей, к которым оно подключено. Затем облачный сервер создает идентификатор соединения, и приемник ActivCast отображает его.

Теперь на передающем устройстве можно использовать приложение ActivCast и нажимать значок, позволяющий ввести идентификатор соединения.

После ввода пользователем идентификатора соединения он снова отправляется с устройства пользователя в облачный сервис, упомянутый выше. Сервис ищет этот идентификатор в своей базе данных и отправляет имя и IP-адрес передатчику, который, в свою очередь, создает соединение.

Устройства должны находиться в той же сети, что и блок приемника ActivCast.

Данный способ не работает, если приемник ActivCast или передающее устройство не подключены к Интернету и не могут установить соединение с облачным сервисом. Кроме того, при наличии в сети брандмауэра или прокси-сервера URL-адрес promethean.api.splashtop может блокироваться. В такой ситуации у отдела ИТ должна быть возможность добавить данный URL-адрес в белый список.

По IP-адресу

Соединение устанавливается напрямую, и не нужно использовать облачный сервер или Bonjour.

Передающее устройство должно иметь возможность подключения к отображаемому IP-адресу. Необходимо находиться в одной из сетей, к которой подключен приемник ActivCast.

Настройка производительности для зеркалирования

Существует множество факторов производительности в случае отправки данных экрана устройства на принимающее устройство по беспроводной сети.

По словам пользователей, при использовании в домашних условиях беспроводных протоколов для зеркалирования все работало должным образом. То есть, передача экрана устройства на экран телевизора осуществлялась беспрепятственно. В стенах офиса или учебного заведения результат может значительно отличаться.

Необходимо принимать во внимание требования организации в отношении сетей: их безопасности, пропускной способности и сегментации. Существует множество причин, по которым блестящая презентация через выделенную сеть часто показывает потрясающие результаты, а при развертывании в реальной среде не отвечает ожиданиям.

Все беспроводные решения для проведения презентаций, имеющиеся на рынке в настоящее время, так или иначе уязвимы.

Поэтому мы хотим проинформировать вас и ваших пользователей о возможных трудностях при использовании приложения для зеркалирования.

Раздел данного документа, разъясняющий требования к сети, касается в основном фазы обнаружения и подробно рассматривает ее. Если предположить, что соединение было установлено в ходе фазы обнаружения передатчика и приемника, нам необходимо сосредоточиться на фактической передаче данных с экрана передающего устройства на приемник.

Требования к пропускной способности соединения

Предположим, что изображение экрана устройства с разрешением 1080 пикселей передается по сети, тогда можно подсчитать, что сеть должна быть в состоянии обрабатывать до 8 Мбит/с для передачи этой информации и ее отображения на приемнике.

Если пользователь хочет демонстрировать видео с разрешением 1080 пикселей и скоростью 25 кадров в секунду, можно сказать, что скорость 20 Мбит/с будет достаточной.

Это при условии, что несколько пользователей выполняют эти действия, беспроводная инфраструктура не перегружена, а сеть имеет хороший охват и высокую пропускную способность.

В данном документе невозможно полностью рассмотреть указанную тему. Promethean не может гарантировать, что приложение ActivCast или любая другая подобная коммерческая технология зеркалирования при использовании в обычных сетях будет обеспечивать превосходную производительность в любых условиях.

Следует повторить, что передатчик ActivCast или встроенный передатчик Airplay сжимает данные экрана, а затем передает их через неизвестную среду.

Затем приемник декодирует эти данные и выводит их на экран.

Мы считаем, что оптимизировали процессы сжатия и декодирования, но у нас нет возможности повлиять на сеть.

Учитывая все вышеизложенное, предлагаем вам несколько рекомендаций по улучшению производительности в случае необходимости.

Использование подключений Ethernet

Ethernet по-прежнему остается самым надежным типом соединения. Рекомендация использовать проводное соединение для беспроводной системы может показаться странной. Однако мы советуем подключать устройство приема ActivCast с помощью проводов.

Подключение по Wi-Fi

Проверьте наличие помех в беспроводной сети. Убедитесь, что передающее устройство использует самый быстрый режим – 802.11. Переключитесь в режим 5 ГГц и убедитесь, что маршрутизатор настроен для оптимального использования Airplay.

Данный перечень не является исчерпывающим, поскольку также необходимо учитывать другие обстоятельства.

Передача разрешения экрана устройства

Ваше передающее устройство может работать при таком высоком разрешении, которое вашей сети не удастся обработать. При попытке отправить на приемник экран с разрешением 4k велика вероятность того, что ваша сеть не сможет справиться с таким объемом данных. Уменьшайте разрешение экрана передающего устройства до тех пор, пока не будет достигнут приемлемый уровень производительности.

Bluetooth

Поскольку устройства Bluetooth и беспроводной сети 802.11 управляются одним и тем же интерфейсом и имеют примыкающие антенны, возможны помехи при одновременном использовании этих двух видов связи. При зеркалировании рекомендуется **ВЫКЛЮЧАТЬ** Bluetooth на **обоих** устройствах.

ПРИЛОЖЕНИЕ. Парольные фразы и политика безопасности

«Парольные фразы – не то же самое, что и пароли. Парольная фраза представляет собой более длинную версию пароля, и поэтому она более надежна. Парольная фраза обычно состоит из нескольких слов, поэтому она более устойчива ко взломам и является неотъемлемой частью системы безопасности устройства»

Обзор

Парольные фразы являются важным аспектом компьютерной безопасности. Простая парольная раза может привести к несанкционированному доступу к ресурсам компании и их недобросовестному использованию. Все пользователи, включая подрядчиков и поставщиков, имеющие доступ к системам компании, несут ответственность за принятие соответствующих действий по выбору и защите парольных фраз.

ИТ-специалисты также ответственны за обеспечение надежной безопасности устройства в сети, за его аварийное восстановление и соответствие требованиям организации.

Цель

Целью данной политики является установка стандарта для создания надежных парольных фраз на устройствах ActivPanel/ActivConnect G-Series, защита парольных фраз и периодичность их изменения.

Политика также предлагает рекомендации по обеспечению безопасности устройств ActivPanel/ ActivConnect G-Series.

Область применения

Данная политика распространяется на всех сотрудников (конечные пользователи/ИТ-администраторы), несущих ответственность за использование устройств ActivPanel/ActivConnect G-Series и имеющих доступ к сети и на территорию компании.

1.0. Политика

1.1. Создание парольных фраз/безопасность экрана. (Блокировка экрана: по умолчанию установлен период в 5 секунд после нажатия кнопки сна)

Все парольные фразы на пользовательских и системных уровнях должны удовлетворять требованиям компании. Например, следующим шаблонам: простой, цифровой, буквенно-цифровой, сложный буквенно-цифровой и использующий специальные символы. Минимальная длина: от 1 до 16 символов. Надежная парольная фраза является достаточно длинной и содержит комбинацию букв верхнего и нижнего регистра, цифр и пунктуационных символов.

1.2. Изменение парольной фразы. Например, пароли root, enable, admin, учетные записи администраторов приложения рекомендуется менять раз в квартал или в зависимости от правил, установленных в организации.

1.3. Видимость парольной фразы. Рекомендуется отключать эту функцию.

1.4. Парольные фразы пользовательского уровня. Их рекомендуется менять каждый месяц или в зависимости от правил, установленных в организации.

1.5. Защита парольной фразы/повторное использование парольной фразы. Не рекомендуется повторно использовать парольные фразы

1.6. Парольные фразы. Не сообщайте их никому. Все парольные фразы являются конфиденциальной информацией.

1.7. Парольные фразы. Не вставляйте парольные фразы в сообщения электронной почты и другие формы электронной коммуникации.

1.8. Не указывайте парольные фразы в анкетах или документации по безопасности.

1.9. Не оставляйте подсказки к парольным фразам (например, «моя фамилия»).

1.10. Не сообщайте никому парольные фразы, установленные в компании, в том числе административным помощникам, секретарям, менеджерам, коллегам, находящимся в отпуске, и членам семьи.

1.11. Не записывайте парольные фразы и не храните их на своем рабочем месте. Не храните парольные фразы в незашифрованном виде в каком-либо файле на компьютере или мобильных устройствах (телефонах, планшетах).

1.12. Если у пользователя имеется подозрение, что его парольная фраза попала в чужие руки, ему необходимо сообщить об этом в отдел ИТ и изменить все пароли.

1.13. Автоматическая блокировка. ActivPanel/ActivConnect G-Series. Во избежание несанкционированного доступа к конфиденциальным данным третьих лиц рекомендуется установить автоматическую блокировку ActivPanel, включающуюся через 15 минут простоя устройств.

1.14. Антивирусная программа. Все устройства ActivPanel/ActivConnect G-Series должны быть защищены антивирусным программным обеспечением во избежание угроз со стороны мобильного USB-оборудования и внешних веб-сайтов/приложений. В антивирусной программе необходимо задать настройки сканирования приложений или носителей при их первой установке.

1.15. Шифрование устройства. Рекомендуется обеспечить защиту конфиденциальных данных, хранящихся на устройствах ActivPanel/ActivConnect G-Series.

1.16. Установка программ из неизвестных источников. По умолчанию включена блокировка установки неизвестных приложений. Не рекомендуется выключать данную блокировку во избежание потенциальных угроз.

1.17. Уведомления. Рекомендуется отключить отображение уведомлений (конфиденциальная информация/электронные письма), когда устройства ActivPanel/ActivConnect G-Series находятся в заблокированном режиме.

1.18. Резервное копирование и сброс данных. Если кто-либо посторонний получил доступ к ActivConnect G-Series, необходимо принять соответствующие меры через учетные записи администраторов приложения.

2.0. Требования к пользователям

2.1. Пользователи должны загружать только актуальные и необходимые данные в соответствии со своей ролью на устройствах ActivPanel/ActivConnect G-Series.

2.2. О любых поломках/сбоях в работе пользователи должны немедленно сообщать в отдел ИТ.

2.3. Если у пользователя имеется подозрение, что кто-либо получил несанкционированный доступ через устройства ActivPanel/ActivConnect G-Series к данным компании/учебного заведения, ему необходимо сообщить об инциденте в соответствии с принятой в учреждении процедурой.

2.4. Запрещено устанавливать на устройства ActivPanel/ActivConnect G-Series любое программное обеспечение для доступа к функциям, не предназначенным для пользователя.

2.5. Пользователям запрещено загружать на устройства ActivPanel/ActivConnect G-Series пиратское программное обеспечение или незаконное содержимое.

2.6. Разрешено устанавливать приложения только из официальных и проверенных источников. Запрещается устанавливать программы из ненадежных источников. В случае возникновения сомнений относительно надежности ресурса необходимо обратиться в отдел ИТ.

2.7. Необходимо поддерживать устройства ActivPanel/ActivConnect G-Series в актуальном состоянии с помощью исправлений, выпущенных производителем или сетью. Наличие исправлений необходимо проверять каждую неделю и применять их как минимум раз в месяц.

2.8. Запрещено подключать устройства ActivPanel/ActivConnect G-Series к компьютеру, на котором не установлена и не включена актуальная антивирусная программа и который не удовлетворяет требованиям политики компании/учебного заведения.

2.9. Данные устройств должны быть зашифрованы в соответствии с требованиями компании.

2.10. Необходимо с осторожностью объединять личные и рабочие учетные записи электронной почты на устройствах ActivPanel/ActivConnect G-Series. Для передачи данных учреждения пользователям необходимо использовать только корпоративную систему электронной почты. Если у пользователя имеется подозрение, что данные учреждения были отправлены с личной учетной записи электронной почты в теле письма или в качестве приложения к нему, ему следует незамедлительно сообщить об этом в отдел ИТ организации.