Promethean™

ActivConnect™ G-Series

ActivPanel™

Guía de integración para administradores de TI

TP-2046-ES-V01

Índice

Introducción y supuestos

ActivPanel se suministra con un potente dispositivo Android™ 5.1 (Lollipop). Aunque el usuario considere el sistema ActivPanel como un dispositivo completo, desde una perspectiva de TI es esencial entender que el panel y ActivConnect G-Series son dos componentes distintos. Este carácter modular ofrece ventajas en lo que respecta a flexibilidad de administración, mantenimiento y actualización.

Esta publicación tiene la finalidad de asistir a los administradores de TI en las tareas de configuración de este dispositivo para su uso óptimo dentro de la organización.

La guía presupone que el dispositivo se ha instalado y está montado en ActivPanel con el soporte requerido; y está encendido y conectado a los puertos USB y HDMI® correctos, conforme a las indicaciones de la guía de instalación.

También presupone que el destinatario conoce y entiende la terminología técnica utilizada. No está pensada como guía de uso del dispositivo.

El sistema ActivPanel debe estar encendido y el dispositivo ya iniciado con la pantalla principal visible.

La aplicación de configuración

A lo largo de esta guía, se le pedirá repetidamente que utilice el panel de configuración, por lo que es aconsejable que se familiarice con el acceso al mismo.

La guía proporciona instrucciones para ejecutar la aplicación, que es un componente esencial para la correcta configuración de la unidad. Aunque aquí le explicamos los ajustes básicos, es aconsejable que lea los artículos sobre configuración de Android Lollipop disponibles en Internet.

En la aplicación de configuración podrá modificar los ajustes del dispositivo según corresponda a los requisitos de su organización.

El punto de acceso a la aplicación se encuentra en la pantalla de inicio.

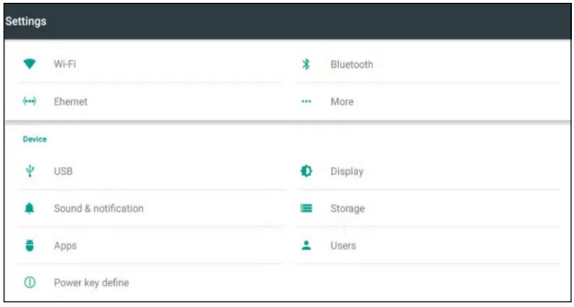
En la parte inferior derecha verá el icono de categorías de aplicación.

Pulse este icono.

Busque la categoría de configuración. El icono de esta categoría tiene forma de engranaje.

Pulse la aplicación de configuración dentro de esta categoría.

Se abrirá la pantalla de configuración.



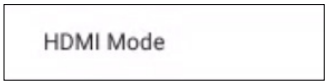
Ajustes de pantalla

Por lo general no hace falta definir la resolución de pantalla, puesto que el dispositivo detecta el valor óptimo según la conexión existente.

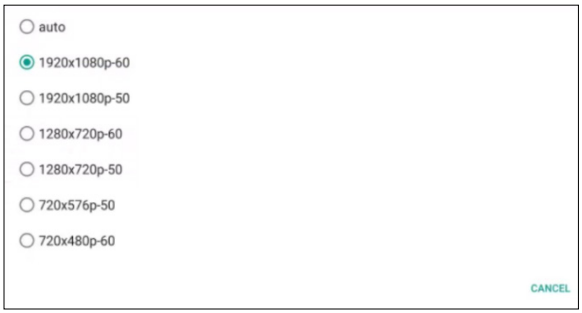
Pero si quiere comprobar el ajuste o modificarlo, abra la aplicación de configuración como se ha descrito arriba y vaya a la pantalla de configuración.

Pulse Display (Pantalla).

Pulse HDMI Mode (Modo HDMI).



Seleccione los valores de resolución y frecuencia deseados.



El dispositivo se suministra con Gigabit Ethernet, Dual Band 802.11 b/g/n/ac Wi-Fi® (AP6335) y Bluetooth® 4.0.

Dependiendo de la implementación de la infraestructura de red, puede optar por usar la conexión Wi-Fi del dispositivo o una conexión Ethernet con cable. Obtendrá un mejor rendimiento si utiliza una conexión con cable.

Configuración de Wi-Fi (el Apéndice contiene información sobre ajustes de seguridad)

Abra la aplicación de configuración como se ha descrito arriba y vaya a la pantalla de configuración.

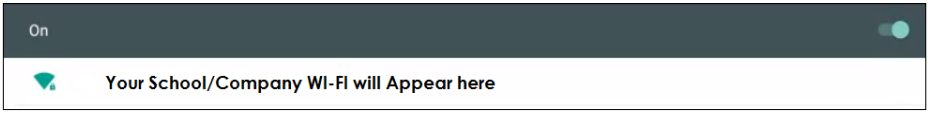
Pulse Wi-Fi para acceder a las opciones de configuración.

Pulse el botón de activación/desactivación de Wi-Fi para activarla.

El dispositivo iniciará una búsqueda de conexiones Wi-Fi disponibles.

Aparecerán en la ventana debajo del botón de activación/desactivación.

Pulse la red Wi-Fi a la que quiera conectarse.



Configuración de proxy de red

Realice el siguiente procedimiento si su organización utiliza configuración proxy de red.

Necesitará estos datos:

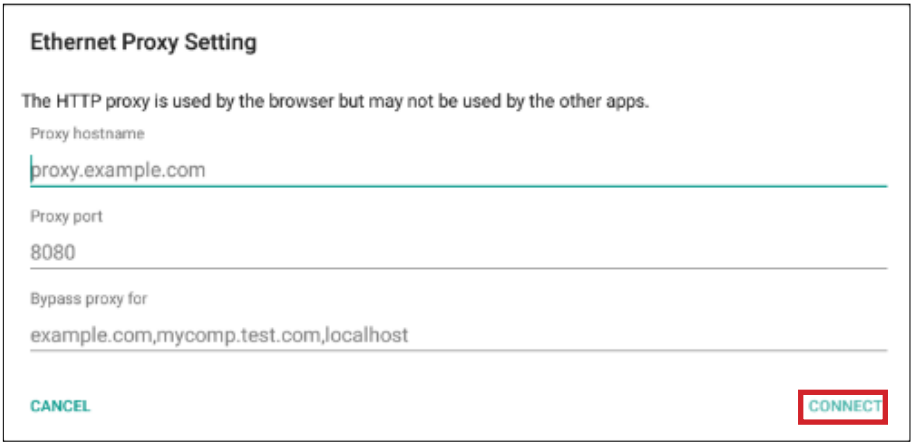
- Un nombre de host proxy o una dirección IP y un número de puerto proxy. Si no tiene esos datos, consulte con su departamento de TI.
- Si su organización requiere un valor de proxy inalámbrico, haga clic en la opción relevante (SSID). Se abrirá la ventana mostrada a continuación.

Seleccione la casilla Advanced Options (Opciones avanzadas) y pulse Proxy.

Pulse Manual.

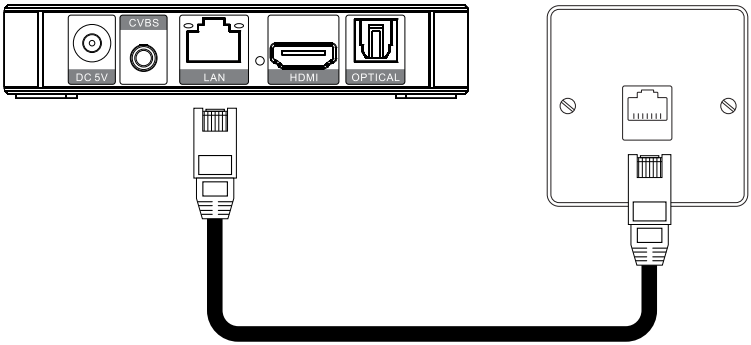
Introduzca los datos proxy requeridos para su red inalámbrica.

Introduzca su contraseña inalámbrica y pulse Connect (Conectar).



Configuración de Ethernet (con cable)
(el Apéndice contiene información sobre ajustes de seguridad)

Para obtener una señal de red más fiable y estable, también se debería conectar un cable de red entre el puerto LAN del dispositivo y un puerto de red en la ubicación de uso (aula/sala/oficina).



NOTA IMPORTANTE:

Si su organización usa un servidor DHCP (Dynamic Host Configuration Protocol), al conectar un cable de red se realizará la asignación automática de todas las configuraciones. Si no hay un servidor DHCP. Solicite asistencia a su departamento de TI.

CONFIGURACIÓN DE PROXY DE RED

Realice el siguiente procedimiento si su organización utiliza configuración proxy de red.

Necesitará estos datos:

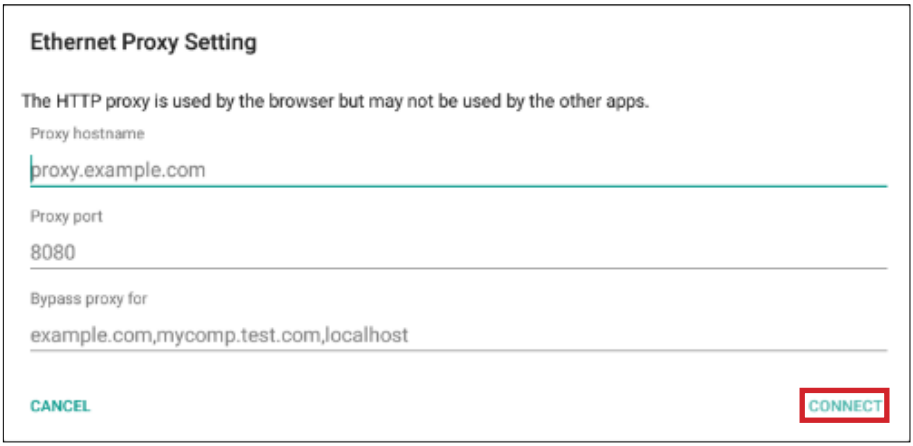
- Un nombre de host proxy o una dirección IP y un número de puerto proxy. Si no tiene esos datos, consulte con su departamento de TI.

En la pantalla de configuración, pulse Ethernet.

Pulse Proxy.

Pulse Manual.

Introduzca los datos de proxy para su conexión Ethernet con cable (consulte con su departamento de TI si es necesario). Después de introducirlos pulse Connect (Conectar).



Configuración de un modo de hotspot o zona Wi-Fi

El dispositivo puede crear un área de cobertura Wi-Fi en la que otros dispositivos Wi-Fi podrán conectarse a la red o a Internet. Esto puede ser conveniente si la señal de Internet es inestable. También se puede usar para crear duplicaciones inalámbricas. La zona Wi-Fi propiamente dicha no tiene conectividad a Internet, pero si además se conecta un cable Ethernet al dispositivo y este tiene conexión a Internet, los usuarios pueden acceder a Internet conectándose a la zona Wi-Fi. La elección dependerá de las políticas de seguridad vigentes, por lo que esta función está desactivada de modo predeterminado.

Además, este modo puede ser útil para duplicar dispositivos aunque no haya o no se requiera Internet.

El máximo de dispositivos que pueden conectarse simultáneamente a este dispositivo es 5.

Abra la aplicación de configuración para configurar el valor. Consulte las instrucciones para abrir la aplicación.

En la pantalla de configuración, pulse la opción "More" (Más).

Pulse Tethering and Portable Hotspot (Anclaje a red y zona portátil).

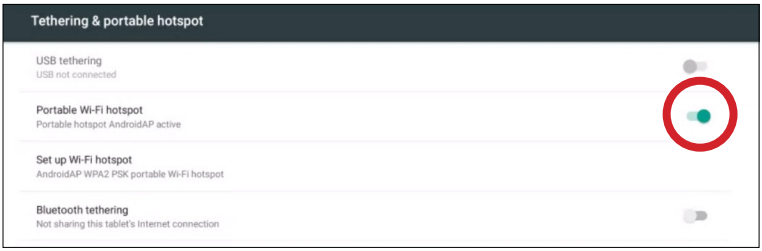
Pulse Setup Wi-Fi Hotspot (Configurar la zona Wi-Fi).

El nombre predeterminado de la zona (SSID) es AndroidAP. Puede elegir otro nombre.

También puede cambiar el tipo de seguridad de esta pantalla.

Introduzca una contraseña y pulse Save (Guardar).

Pulse el botón de activación/desactivación de Portable Wi-Fi Hotspot (Zona Wi-Fi portátil).

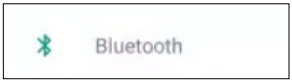


El nombre SSID que configure se difundirá y podrá conectarse usando el procedimiento habitual, eligiendo el SSID en su configuración inalámbrica.

Configuración de Bluetooth

Este dispositivo está dotado de Bluetooth 4.0. Entre sus muchas aplicaciones están la transferencia de archivos en un radio de acción cercano y el control de robots y diversos dispositivos. De modo predeterminado, la función Bluetooth está desactivada. Si la necesita, puede activarla desde la pantalla de configuración.

Pulse Bluetooth.



Pulse el botón de activación/desactivación de Bluetooth para activar la función.

Comprobación de vigencia del software

El dispositivo tiene integrada una aplicación OTA (Over the Air Update) que realiza exámenes periódicos para comprobar si existen actualizaciones y ofrecer al usuario la oportunidad de aceptarlas.

Esta aplicación también se puede usar manualmente.

Es importante aceptar las actualizaciones ya que, además de mejoras de funciones, solemos incluir frecuentemente parches de seguridad y actualizaciones de sistema operativo.

NOTA:

Para que el dispositivo implemente actualizaciones periódicamente, es esencial incluir esta URL en la lista de direcciones autorizadas: http://cdn-otaupdate.prometheanworld.com.
De esta forma se asegura la descarga e instalación de todas las actualizaciones importantes.

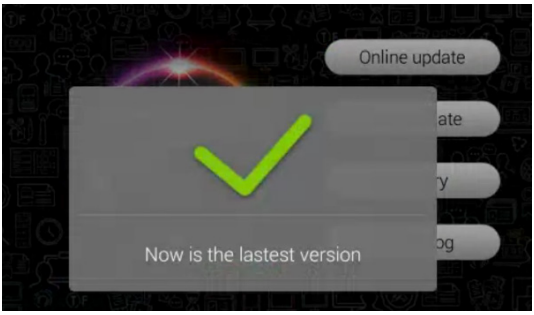
Pulse el icono de aplicación en la pantalla de inicio.

Pulse el icono de engranaje en la pantalla de configuración.

Pulse el icono de actualización.

Pulse **Online update** (Actualización en línea).

Nota: Si el dispositivo ya tiene instalada la actualización más reciente, un mensaje indicará que se está ejecutando la última versión.



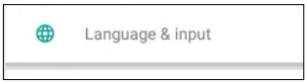
Si hay una nueva actualización disponible, el sistema la descargará y podrá aceptarla pulsando el botón de actualización.

Debe esperar a que se procese la actualización. Una vez completada la operación, el sistema se reiniciará automáticamente y la actualización entrará en vigor. Evite interrumpir el proceso de actualización, ya que las interrupciones pueden crear inestabilidad en el funcionamiento del dispositivo.

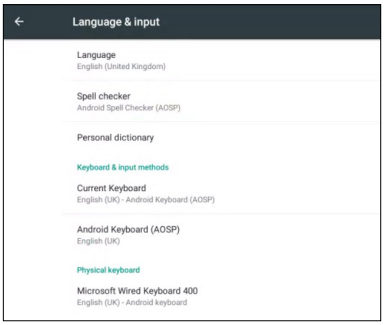
Teclado e idioma

Pulse la aplicación de configuración.

Pulse **Language & Input** (Teclado e idioma).



En esta sección puede configurar los ajustes de teclado e idioma específicos de su región/país.



Seguridad

Pulse la aplicación de configuración.

Pulse **Security** (Seguridad).

Seleccione los parámetros de seguridad que quiera modificar.

NOTA:

Consulte lo relativo a prácticas recomendadas de políticas de seguridad, en el Apéndice de este documento.

Fecha y hora

Pulse la aplicación de configuración.

Pulse **Date & Time** (Fecha y hora).

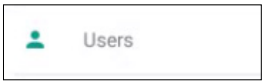
Seleccione la fecha y hora específicas de su región.

Nota: Antes de configurar su zona horaria debe desactivar el ajuste Automatic Time Zone (Zona horaria automática).

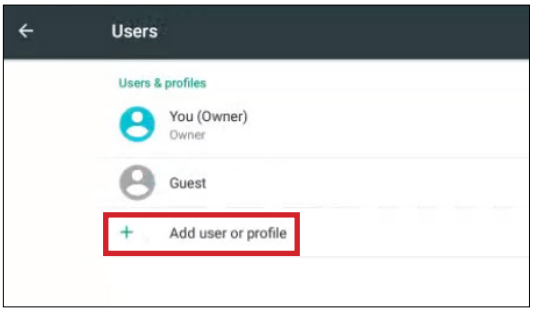
Creación de usuarios

Pulse la aplicación de configuración.

Pulse **Users** (Usuarios).



Pulse **Add User or Profile** (Agregar usuario o perfil).



Puede elegir una de estas dos opciones:

- **User** (Usuario) - Por ejemplo, para un miembro de la plantilla de la organización
- **Restricted Profile** (Perfil restringido) - Por ejemplo, para estudiantes

ActivCast™ (duplicación)

La suite de aplicaciones Activcast permite la duplicación inalámbrica de pantallas de dispositivos con Windows®, Mac OS X®, iOS™, Android™ y Chrome OS™ en el receptor de ActivCast. La aplicación del receptor ActivCast está preinstalada en el dispositivo y se puede ejecutar desde su pantalla de inicio.

Para dispositivos que quieran transmitir su pantalla al receptor ActivCast, es preciso instalar una aplicación en el dispositivo emisor. Esto no es estrictamente aplicable a dispositivos con iOS y Mac OS X, ya que los dispositivos Apple® tienen emisores de duplicación compatibles con ActivCast. No obstante, el uso de la aplicación emisora ActivCast tiene sus ventajas. De momento no tenemos un emisor ActivCast para Mac OS X, ya que dicho sistema tiene uno incorporado. Si quiere usar las funciones extra del emisor ActivCast, puede usar el navegador Chrome de OS X e instalar el complemento emisor ActivCast.

Para adquirir los emisores ActivCast, visite esta URL y vaya a la sección de descargas de software.

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

En este artículo encontrará instrucciones sobre la duplicación de la pantalla de su dispositivo:

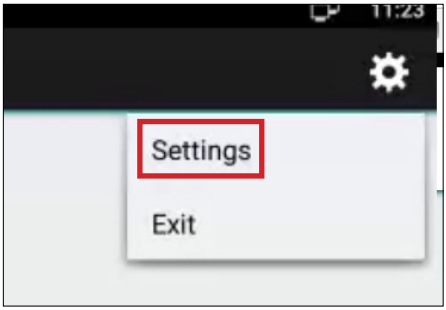
https://support.prometheanworld.com/article/?kb=1532

Asignación de nombres a dispositivos

Al iniciar la aplicación Activcast desde la pantalla de inicio de su dispositivo, puede optar por cambiar el nombre de identificación del receptor. Es aconsejable que cada dispositivo/ActivPanel tenga su propio nombre. Por ejemplo, Aula ActivPanel 1 o Sala de reuniones, o cualquier otra convención de uso habitual en su entorno de trabajo. Esto ayuda a identificar la ubicación de los dispositivos.

Pulse el icono de ActivCast en la pantalla de inicio.

Pulse el icono de engranaje y luego **Settings** (Configuración) en la esquina superior derecha de la pantalla.



Pulse el nombre del dispositivo y cámbielo de acuerdo con las convenciones aceptadas en su entorno. También es aconsejable configurar un código PIN en esta pantalla, como medida de seguridad. Con un PIN configurado, se pedirá al dispositivo emisor que lo introduzca.

Para que funcione la duplicación, tanto el receptor como el emisor ActivCast deben estar conectados a una red accesible y enrutable para ambos (puede ser inalámbrica o con cable). La conexión a una red la establece el sistema operativo del emisor y el receptor, mediante las herramientas habitualmente integradas en el sistema.

Desde el punto de vista de la seguridad, ActivCast funciona como cualquier otra aplicación en el equipo del usuario. Por lo tanto, está sujeta a las políticas de seguridad de una organización.

Para que Airplay® funcione correctamente se requiere lo siguiente:

- Si la red utiliza un servidor de seguridad, es necesario configurar la aplicación ActivCast para que sea "de confianza" y aplicable a perfiles públicos, privados y de dominio.
- Los siguientes puertos deben estar abiertos y permitidos:

  TCP 6000-7000, 7100, 47000, 47010

  UDP 5353, 6000-7000, 7011

Duplicación de pantalla

Airplay no requiere ninguna configuración para poder encontrar dispositivos compatibles en la red, gracias a la *detección de servicios DNS*, basada en *DNS de multidifusión*, también conocido como **Bonjour®**. Pero en algunos casos ni Bonjour ni Multicast pueden usarse en una red, o hay varias redes VLAN y subredes. Para afrontar estas situaciones, Promethean ha desarrollado una tecnología que se explica más adelante en este documento.

La duplicación de pantalla se consigue mediante la transmisión de secuencias de vídeo con codificación **H.264** y cifrado AES de 128 bits, a través de una conexión TCP.

Las secuencias se empaquetan con un encabezado de 128 bytes. El audio **AAC-ELD** se envía mediante el protocolo Airplay. El reloj maestro se sincroniza mediante **NTP**.

Además, en cuanto un cliente empieza a reproducir vídeo, se establece una conexión Airplay estándar para enviar la URL de vídeo y la duplicación se detiene. Así se evita la descodificación y la recodificación del vídeo, con la consiguiente pérdida de calidad.

Solicitudes HTTP

La duplicación de pantalla establece conexión con un puerto 7100 codificado de forma rígida. Se trata de un servidor HTTP que admite estas solicitudes:

POST /stream

Se inicia la transmisión de vídeo en directo. El cliente envía una lista binaria de propiedades con información sobre la secuencia, y acto seguido se envía la secuencia propiamente dicha. En este punto, la conexión deja de ser una conexión HTTP válida.

En cuanto el servidor recibe una solicitud **/stream**, envía solicitudes NTP al cliente en el puerto 7010, también codificado de forma rígida. El cliente debe exportar ahí su reloj maestro, que se usará para sincronización de audio/vídeo y recuperación de reloj.

Paquetes de secuencias

La secuencia de vídeo se empaqueta con encabezados de 128 bytes, seguidos de una carga opcional.

Datos de códec

Este paquete contiene los datos H.264 extra en formato **avcC** *(ISO/IEC 14496:15)*. Esos datos se envían al principio de la secuencia, cada vez que cambian las propiedades de vídeo, cuando cambia la orientación de la pantalla y cuando esta se enciende o apaga.

Sincronización de tiempo

Se envían solicitudes al cliente de Airplay cada 3 segundos. La fecha de referencia de las marcas de tiempo es el comienzo de la sesión de duplicación.

Protección mediante contraseña

Un servidor de Airplay podría requerir una contraseña para mostrar contenido de la red. Para implementar esto se usa el estándar de **autenticación implícita de HTTP** *(RFC 2617)*, mediante el protocolo HTTP para todo.

ActivCast implementa automáticamente esta protección mediante contraseña.

Descubrimiento

Los emisores ActivCast que funcionan con receptores ActivCast deben definir el receptor ActivCast objeto de la duplicación.

Hay cuatro formas principales para identificar el receptor ActivCast:

- Por su nombre
- Por un código QR
- Por un ID de conexión
- Por su dirección IP

Todos estos elementos se pueden encontrar en la pantalla principal de la aplicación del receptor ActivCast.

Las distintas posibilidades de conexión entre el dispositivo y ActivConnect se deben a las formas de configurar las redes.

Nombre del receptor

Supongamos que su ActivConnect se llama "Aula".

Este nombre se difunde en las redes a las que está conectada la aplicación ActivCast receptora.

La aplicación ActivCast emisora instalada en su dispositivo está a la espera de estos nombres.

Al llegar uno de ellos, se incluye en una lista. Solo hace falta un clic en el nombre para establecer la conexión.

Pero hay redes que bloquean esta difusión, denominada Bonjour. Por eso el nombre nunca es visible.

Por código QR

Si tiene una tablet o un teléfono e inicia la aplicación ActivCast emisora, puede escanear el código mostrado en la pantalla AC.

Este código contiene toda la información necesaria para establecer una conexión.

El dispositivo debe estar en la misma red a la que esté conectado el receptor ActivCast, pero se elimina la incertidumbre de la difusión Bonjour.

Por ID de conexión

Este método también elimina la necesidad de usar Bonjour en la red. Es muy similar al código QR disponible en dispositivos móviles, ya que crea una entrada de base de datos para el dispositivo ActivCast y un ID de conexión que se usa para buscar información.

Aquí se detalla un flujo de trabajo de alto nivel...

La aplicación ActivCast contacta con un servidor en la nube en promethean.api.splashtop.com y pasa su nombre y direcciones IP para las redes a las que está conectado. A continuación el servidor en la nube crea un ID de conexión y el receptor ActivCast lo muestra.

Ahora puede usar la aplicación ActivCast en su dispositivo y pulsar el icono que permite introducir el ID de conexión.

Cuando el usuario lo introduce, el ID de conexión se vuelve a enviar desde el dispositivo del usuario al servicio en la nube mencionado anteriormente. Busca este ID en su base de datos y envía el nombre y la dirección IP al emisor, que crea la conexión.

Los dispositivos tienen que estar en la misma red que la unidad receptora ActivCast a la que están conectados.

Este método no funcionará si el receptor ActivCast o el dispositivo emisor no tienen una conexión a Internet par acceder al servicio en la nube. Además, si hay un servidor de seguridad o proxy configurado en alguna de sus redes, podría bloquear la URL promethean.api. splashtop. De ser así, el departamento de TI debería poder incluir esta URL entre las autorizadas.

Por dirección IP

Se establece una conexión directa sin tener que visitar un servidor en la nube ni usar Bonjour.

El dispositivo emisor debe poder acceder a la dirección IP mostrada. Debe estar en una de las redes a las que está conectado el receptor ActivCast.

Ajustes para optimizar la duplicación

Hay varios factores que intervienen en el rendimiento de los envíos de datos inalámbricos a través de una red a un dispositivo receptor.

Los usuarios suelen afirmar que al usar protocolos inalámbricos de duplicación desde un entorno doméstico todo funciona bien al enviar su pantalla al televisor. Pero las cosas cambian al intentar lo mismo en un entorno profesional (una oficina o una escuela, por ejemplo).

Una de las cuestiones fundamentales es que las organizaciones deben tomar muy en serio los requisitos de seguridad, ancho de banda y segmentación de las redes. Hay múltiples razones por las que una demostración impecable en una red dedicada no produce el mismo resultado al realizarla en un entorno real de mayor envergadura.

Las soluciones de presentación inalámbricas disponibles actualmente presentan vulnerabilidades en ese sentido.

Por eso queremos asegurarnos de que usted y los usuarios de su entorno tengan conciencia de los obstáculos que podrían encontrar al utilizar una aplicación de duplicación, y de que ajusten sus expectativas en consecuencia.

La sección de este documento que explica los requisitos de red se centra únicamente en la fase de descubrimiento. Si presuponemos que en la fase de descubrimiento un emisor y un receptor han establecido una conexión, debemos concentrarnos en la transmisión real de los datos de pantalla del dispositivo emisor al receptor.

Requisitos de ancho de banda

Suponiendo que un dispositivo envía la pantalla a través de una red a 1080p, la red debería ser capaz de gestionar 8 Mbps para transmitir esos datos y para que el receptor los muestre.

Si un usuario quiere enviar un vídeo de 1080p a 25 fotogramas por segundo, puede que 20 Mbps sean suficientes.

Esto será así siempre y cuando haya solo unos cuantos usuarios realizando estas acciones, no haya ninguna otra actividad acaparando la infraestructura de la red y la cobertura y el ancho de banda sean buenos.

Pero este es un tema que no podemos tratar en profundidad en este documento. Y Promethean no puede garantizar el funcionamiento perfecto en cualquier tipo de condiciones de la aplicación ActivCast o cualquier otra tecnología de duplicación comercial similar que use redes normales.

En resumen, el emisor ActivCast o Airplay nativo comprimen los datos de pantalla y luego los transmiten a través de un entorno desconocido.

El receptor descodifica esos datos y los muestra en pantalla.

Creemos que hemos optimizado la compresión y la descodificación, pero no podemos influir en el funcionamiento de la red.

No obstante, estas son algunas sugerencias para mejorar el rendimiento.

Usar conexiones Ethernet

Ethernet sigue siendo el tipo de conexión más fiable. Aunque pueda parecer extraño, tratándose de un sistema inalámbrico, es muy aconsejable usar una dispositivo receptor ActivCast con cable.

Conexión Wi-Fi

Compruebe si hay interferencias de red inalámbrica. Asegúrese de que el dispositivo emisor usa el modo 802.11 más rápido posible. Use el modo de 5 GHz y asegúrese de que el enrutador está configurado para un uso óptimo de Airplay.

Esta lista de sugerencias no es exhaustiva, ya que hay otras consideraciones medioambientales a tener en cuenta.

Resolución de pantalla del dispositivo emisor

Puede que el dispositivo emisor tenga configurada una resolución demasiado alta para la red. Si intenta enviar una pantalla de 4k al receptor, es probable que la red no sea capaz de gestionar tal cantidad de datos. Puede ser conveniente reducir la resolución del dispositivo emisor para ver si mejora el rendimiento.

Bluetooth

Dado que las conexiones Bluetooth y 802.11 inalámbricas se controlan mediante la misma interfaz y tienen antenas contiguas, podrían interferir mutuamente cuando ambas se están usando. Es aconsejable **desactivar** Bluetooth en **ambos** dispositivos al duplicar.

APÉNDICE: Códigos de acceso y política de seguridad

“Los códigos de acceso no son lo mismo que las contraseñas. Un código de acceso es una versión más larga de una contraseña, y por lo tanto más segura. Un código de acceso suele estar compuesto por varias palabras, y por ello ofrece más seguridad frente a ataques y constituye una parte integral del sistema de seguridad de un dispositivo.”

Presentación

Los códigos de acceso son una parte importante de la seguridad informática. Un código de acceso mal elegido puede permitir el acceso no autorizado y/o el uso indebido de los recursos de su organización. Todos los usuarios, incluidos contratistas y proveedores con acceso a los sistemas de su organización son responsables de tomar las medidas apropiadas, detalladas más adelante, para seleccionar y proteger sus contraseñas.

Los profesionales de TI también son responsables de asegurar que la protección de los dispositivos de una red es robusta y capaz de recuperarse después de desastres, y de que cumple con las normas de la organización.

Propósito

El propósito de esta política es establecer un estándar para la creación de códigos de acceso seguros en ActivPanel/ActivConnect G-Series, así como el modo de proteger esos códigos y entender la frecuencia con que se deben cambiar.

La política también detalla las prácticas recomendadas para la seguridad de los dispositivos aplicables a ActivPanel/ActivConnect G-Series.

Ámbito

Esta política es aplicable a todo el personal (usuarios finales/administradores de TI) responsable de cuentas de ActivPanels/ActivConnect G-Series con acceso a sus instalaciones y a su red.

1.0 Política

1.1. Creación de códigos de acceso/Pantalla de seguridad:
(Bloqueo de pantalla: El valor predeterminado es 5 segundos después de pulsar el botón de suspensión.)

Todos los códigos de acceso de nivel de usuario y de sistema deben ser conformes a las normativas de la organización (empresa/escuela). Por ejemplo, usarán un patrón simple, numérico, alfanumérico, alfanumérico complejo o de caracteres especiales. Longitud de entre 1 y 16 caracteres. Un código de acceso es relativamente largo y contiene una combinación de mayúsculas y minúsculas, así como caracteres numéricos y signos de puntuación.

1.2. Cambio de código de acceso: Por ejemplo, para cuentas raíz, de activación, administración y de administración de aplicaciones, es aconsejable cambiarlos cada trimestre o según las normativas de la organización.

1.3. Visibilidad de código de acceso: Es aconsejable desactivar esta función.

1.4. Códigos de acceso de nivel de usuario: El intervalo de cambio recomendado es de 30 días o según las normativas de la organización.

1.5. Protección mediante código de acceso/Reutilización de código de acceso: Se debe evitar el uso repetido de códigos de acceso previos.

1.6. Códigos de acceso: No comparta su código de acceso con nadie. Todos los códigos de acceso deben tratarse como información confidencial.

1.7. Código de acceso: No inserte código de acceso en mensajes de correo electrónico ni otras formas de comunicación electrónica.

1.8. No divulgue ningún código de acceso en cuestionarios ni formularios de seguridad.

1.9. No proporcione ninguna descripción de un código de acceso (por ejemplo, "mi apellido").

1.10. No comparta sus códigos de acceso con nadie, ni siquiera con personal administrativo, responsables, colegas ni miembros de su familia.

1.11. No guarde en la oficina ningún código de acceso escrito. No guarde códigos de acceso en un archivo de un sistema informático ni en dispositivos móviles (teléfono, tablet) sin cifrarlos.

1.12. Si algún usuario sospechara que su código de acceso ha sido interceptado, deberá notificar el incidente al departamento de TI y cambiar todas sus contraseñas.

1.13. Bloqueo automático: ActivPanels/ActivConnect G-Series. El bloqueo automático se debería configurar para todos los sistemas ActivPanel al cabo de 15 minutos de inactividad, para impedir que personas ajenas a los sistemas accedan a datos confidenciales.

1.14. Antivirus: Todos los sistemas ActivPanel/ActivConnect G-Series deben tener instalado software antivirus que los proteja de amenazas procedentes de equipos USB móviles y aplicaciones o sitios web externos. Los programas antivirus examinan aplicaciones y medios en el momento de su instalación.

1.15. Cifrado de dispositivos: Es aconsejable utilizar el cifrado para proteger los datos digitales confidenciales guardados en sistemas ActivPanel/ActivConnect G-Series.

1.16. Instalación de fuentes desconocidas: De modo predeterminado se bloquea la instalación de aplicaciones desconocidas. Es aconsejable mantener el bloqueo para mitigar posibles amenazas.

1.17. Notificaciones: Es aconsejable no mostrar notificaciones (por ejemplo, correo electrónico o información confidencial) cuando los sistemas ActivPanel/ActivConnect G-Series están bloqueados.

1.18. Copia de seguridad y restablecimiento: Si el sistema ActivConnect G-Series se viera comprometido, se deberían tomar las medidas pertinentes en las cuentas de administración de las aplicaciones.

2.0 Requisitos de usuario

2.1. Los usuarios solo deberían cargar en ActivPanel/ActivConnect G-Series datos que sean relevantes y esenciales para su función.

2.2. Los usuarios deberían notificar inmediatamente averías o defectos de funcionamiento al departamento de TI.

2.3. Si un usuario sospecha que se ha producido el acceso no autorizado a los datos de la escuela/empresa a través de ActivPanel/ActivConnect G-Series, deberá notificar el incidente siguiendo las directrices existentes para tales casos.

2.4. No se debe instalar en ActivPanel/ActivConnect G-Series software/firmware cuya finalidad sea obtener acceso a funciones no destinadas al usuario.

2.5. Los usuarios no deben cargar software pirateado ni contenido ilegal en ActivPanel/ActivConnect G-Series.

2.6. Solo se deben instalar aplicaciones procedentes de fuentes oficiales autorizadas. Se prohíbe el uso de código de instalación de fuentes que no sean de confianza. Si tiene dudas sobre la procedencia aprobada de una aplicación, póngase en contacto con el departamento de TI.

2.7. Los sistemas ActivPanel/ActivConnect G-Series deben mantenerse actualizados con parches de red o proporcionados por fabricantes. Se deberían hacer búsquedas semanales como mínimo para averiguar si hay parches nuevos, aplicables al menos una vez al mes.

2.8. Los sistemas ActivPanel/ActivConnect G-Series no se deben conectar a equipos PC que no estén debidamente protegidos con programas antivirus y antimalware o que no cumplan con las políticas de la organización.

2.9. Los dispositivos se deben cifrar de acuerdo con las normas de cumplimiento de su organización.

2.10. Los usuarios deben obrar con precaución en lo concerniente al uso combinado de cuentas de correo personales y profesionales en ActivPanel/ActivConnect G-Series. Los datos empresariales solo se deben enviar a través del sistema de correo electrónico corporativo. Si un usuario sospecha que se han enviado datos empresariales desde una cuenta de correo personal, ya sea como parte del cuerpo del mensaje o como datos adjuntos, deberá notificarlo inmediatamente al departamento de TI de la empresa.