Promethean™

ActivConnect™ G-Series

ActivPanel™

Guida integrativa per gli amministratori IT

TP-2046-IT-V01

Indice

Introduzione e presupposti

ActivPanel viene fornito con sistema Android™ 5.1 (Lollipop). Sebbene ActivPanel possa essere considerato dagli utenti come un dispositivo completo è importante comprendere, dal punto di vista informatico, che il pannello e ActivConnect G-Series sono componenti separati. Questo approccio modulare presenta numerosi vantaggi in termini di amministrazione, manutenzione e flessibilità di aggiornamento.

L'obiettivo di questa pubblicazione è di fornire assistenza agli amministratori IT nell'impostazione del dispositivo per l'uso ottimale all'interno dell'organizzazione.

In questa guida si presuppone che il dispositivo sia stato fisicamente installato e montato su ActivPanel tramite l'apposita staffa, sia acceso e sia stato connesso alle porte USB e HDMI® corrette, come illustrato nella guida di installazione.

Si presuppone inoltre che i termini tecnici contenuti nella presente guida siano noti, in quanto la presente pubblicazione non è rivolta all'utente finale per illustrare l'uso del dispositivo.

Inoltre, si presuppone che ActivPanel sia acceso e che il dispositivo sia stato avviato e mostri la schermata principale.

L'app Impostazioni

Nota: in questa guida verrà richiesto spesso di utilizzare il riquadro impostazioni pertanto è importante acquisire familiarità su come accedervi.

Nell'ambito della presente guida verrà richiesto di eseguire questa applicazione. Si tratta, infatti, di un componente fondamentale per la corretta configurazione dell'unità. Di seguito sono riportate le impostazioni principali per consentire di eseguire la prime operazioni, ma se si desidera approfondire la conoscenza di questo componente consigliamo di cercare articoli relativi alle impostazioni di Android Lollipop su Internet.

L'app Impostazioni illustrata di seguito consente di modificare le impostazioni del dispositivo per adattarle alle diverse esigenze organizzative.

Presupponendo che ci si trovi nella schermata principale del dispositivo, è necessario accedere a questa app.

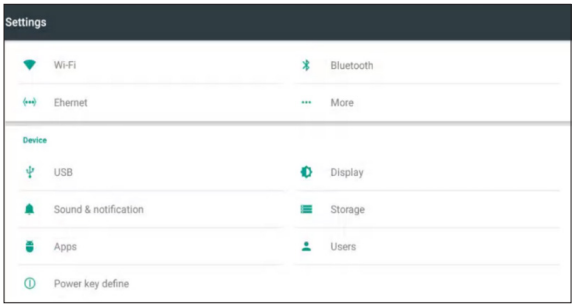
In basso a destra nella schermata principale è visualizzata l'icona della categoria dell'app.

Toccare questa icona.

A questo punto è necessario individuare la categoria Impostazioni. L'icona di questa categoria somiglia a un piccolo ingranaggio.

Toccare l'app delle impostazioni all'interno di questa categoria.

Si apre quindi la schermata delle impostazioni.



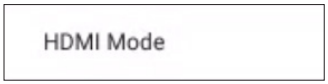
Impostazione del display

Generalmente non è necessario impostare la risoluzione del display, in quanto il dispositivo rileva la risoluzione ottimale in base al display al quale è collegato.

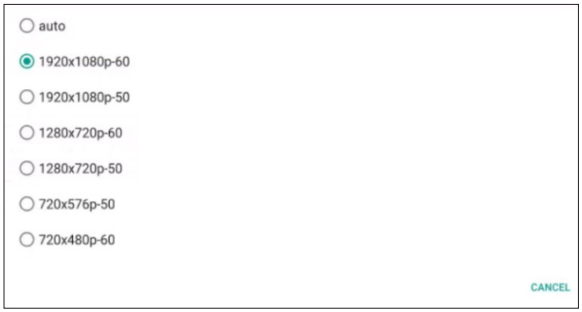
Tuttavia, se si desidera verificare questa impostazione o modificarla, avviare l'app Impostazioni come descritto in precedenza nel presente documento e accedere alla schermata Impostazioni.

Toccare Display.

Quindi toccare Modalità HDMI



Selezionare la risoluzione e la frequenza desiderate.



Il dispositivo dispone di connessione Gigabit Ethernet, Wi-Fi® Dual Band 802.11 b/g/n/ac (AP6335) e di un hardware Bluetooth® 4.0 integrato.

A seconda della distribuzione dell'infrastruttura di rete è possibile utilizzare il Wi-Fi sul dispositivo o la connessione Ethernet cablata. Ai fini delle prestazioni, si consiglia di collegare il dispositivo tramite connessione cablata.

Configurazione Wi-Fi (vedere l'Appendice per le Impostazioni di sicurezza consigliate)

Avviare l'app Impostazioni come descritto in precedenza nel presente documento e accedere alla schermata Impostazioni.

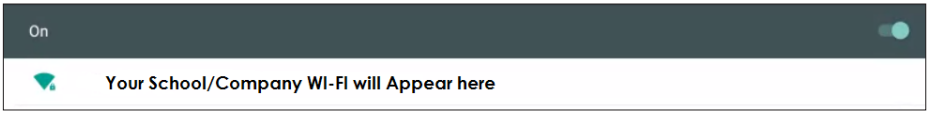
Toccare Wi-Fi per aprire le impostazioni.

Toccare il pulsante di attivazione/disattivazione Wi-Fi per attivare il Wi-Fi.

Il dispositivo avvierà quindi la ricerca delle connessioni Wi-Fi disponibili.

Le connessioni disponibili vengono visualizzate nella finestra sotto il pulsante di attivazione/disattivazione.

Toccare la rete Wi-Fi a cui si desidera connettersi.



Impostazioni proxy di rete

Seguire i passaggi riportati di seguito se l'organizzazione utilizza le impostazioni proxy di rete.

Saranno necessarie le seguenti informazioni:

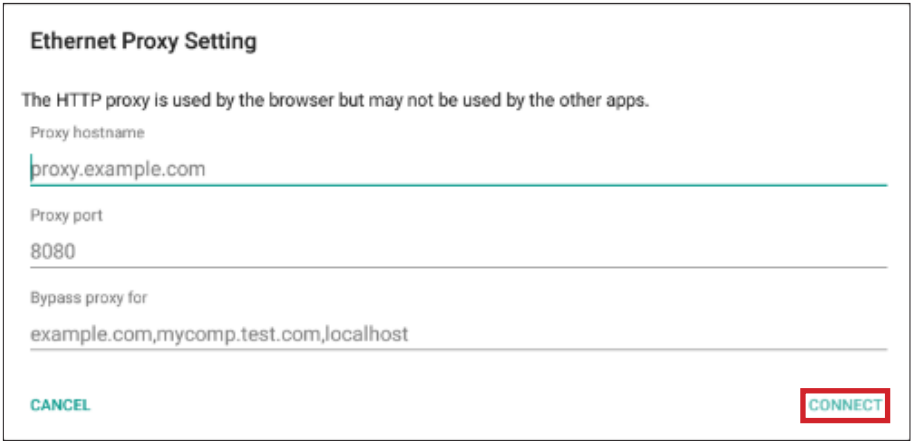
- Nome host proxy o indirizzo IP e numero porta proxy. Se non si è in possesso di questi dettagli, contattare il dipartimento IT
- Se l'organizzazione necessita di un'impostazione proxy wireless, fare clic sul nome wireless desiderato (SSID) per visualizzare la finestra seguente

Toccare la casella di selezione Opzioni avanzate, quindi toccare in corrispondenza di Proxy.

Toccare Manuale.

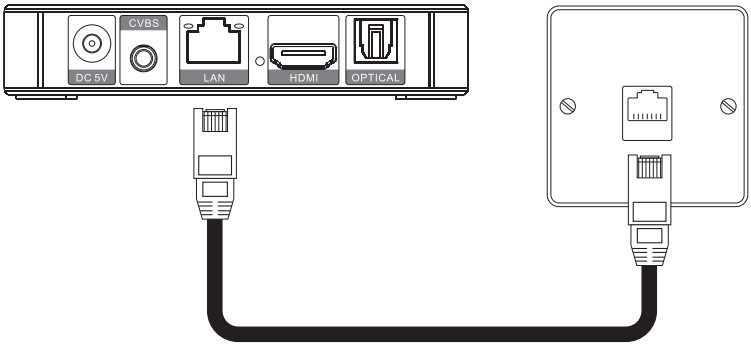
Inserire i dettagli delle impostazioni Proxy desiderate per la rete wireless.

Quindi inserire la password wireless e toccare Connetti.



Configurazione Ethernet (cablata) (vedere l'Appendice per le Impostazioni di sicurezza consigliate)

Per ottenere un segnale di rete più affidabile e uniforme si consiglia di collegare anche un cavo di rete dalla porta LAN del dispositivo a una porta di rete in classe/ufficio.



NOTA IMPORTANTE:

Se l'organizzazione utilizza un server DHCP (Dynamic Host Configuration Protocol), una volta collegato un cavo di rete, il server procederà a assegnare tutte le configurazioni. Se non è presente un server DHCP, rivolgersi al dipartimento IT per assistenza.

IMPOSTAZIONI PROXY DI RETE

Seguire i passaggi riportati di seguito se l'organizzazione utilizza le impostazioni proxy di rete.

Saranno necessarie le seguenti informazioni:

- Nome host proxy o indirizzo IP e numero porta proxy. Se non si è in possesso di questi dettagli, contattare il dipartimento IT.

Nella schermata Impostazioni toccare Ethernet.

Toccare Proxy.

Toccare Manuale.

Inserire i dettagli delle impostazioni Proxy della connessione Ethernet cablata (contattare il dipartimento IT se non si dispone di queste impostazioni). Al termine, toccare Connetti.

Configurazione della modalità hotspot

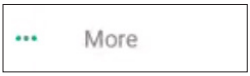
Il dispositivo può creare una piccola area di copertura Wi-Fi che consente ai dispositivi Wi-Fi che si trovano nelle vicinanze di stabilire la connessione a Internet tramite l'hotspot. Questa opzione è consigliata se il segnale Internet non è uniforme e può essere utilizzata per eseguire il mirroring wireless. L'hotspot non dispone di connettività a Internet ma se si collega anche un cavo Ethernet al dispositivo, che dispone di accesso a Internet, gli utenti possono accedere a Internet collegandosi all'hotspot. A seconda dei criteri di sicurezza in uso questa opzione potrebbe essere auspicabile o meno, pertanto questa funzione è disattivata per impostazione predefinita.

Inoltre, questa modalità può risultare molto utile per eseguire il mirroring dei dispositivi anche se la connessione a Internet non è presente/necessaria.

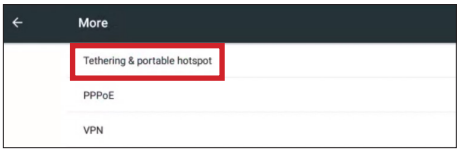
Tenere presente che il numero massimo di dispositivi che possono essere collegati a questo dispositivo è limitato a cinque per volta.

Accedere all'app Impostazioni per effettuare l'impostazione. Fare riferimento alle istruzioni su come avviare l'app Impostazioni.

Nella schermata Impostazioni toccare l'opzione "Altro".



Toccare Tethering e hotspot portatile



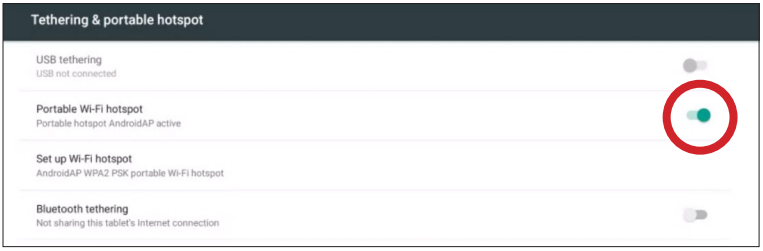
Toccare quindi Impostazione hotspot Wi-Fi.

Il nome predefinito dell'hotspot (SSID) è AndroidAP, ma è possibile modificarlo per adeguarlo alle proprie preferenze.

È inoltre possibile modificare il tipo di sicurezza in questa schermata.

Inserire una Password e toccare Salva.

Toccare il pulsante di attivazione Hotspot Wi-Fi portatile per attivarlo.

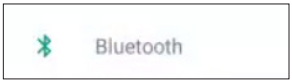


A questo punto verrà trasmesso il nome SSID configurato e sarà possibile effettuare la connessione tramite la normale procedura sui dispositivi connessi, selezionando l'SSID nella configurazione delle impostazioni wireless.

Configurazione del Bluetooth

Il dispositivo è dotato di Bluetooth 4.0, che può essere utilizzato per numerose applicazioni, dal trasferimento di file a breve distanza al controllo di robot e molti dispositivi. La condizione predefinita prevede che il Bluetooth sia disattivato. Se si necessita di questa funzionalità, è possibile attivarla/disattivarla dalla schermata Impostazioni.

Toccare Bluetooth.



Toccare il pulsante di attivazione Bluetooth per attivarlo.

Controllo dell'aggiornamento del software

Il dispositivo è dotato di un'applicazione OTA (Over the Air Update) integrata che ricerca periodicamente nuovi aggiornamenti e fornisce all'utente la possibilità di installare un aggiornamento, se presente.

L'app OTA tuttavia può essere anche eseguita manualmente.

È importante accettare questi aggiornamenti, in quanto spesso applicano patch di sicurezza e aggiornamenti a sistema operativo insieme a miglioramenti e ottimizzazioni delle funzionalità.

NOTA:

Affinché il dispositivo possa eseguire aggiornamenti regolari, è fondamentale inserire il seguente URL all'elenco degli elementi consentiti:
http://cdn-otaupdate.prometheanworld.com.
In questo modo tutti gli aggiornamenti importanti saranno scaricati e installati.

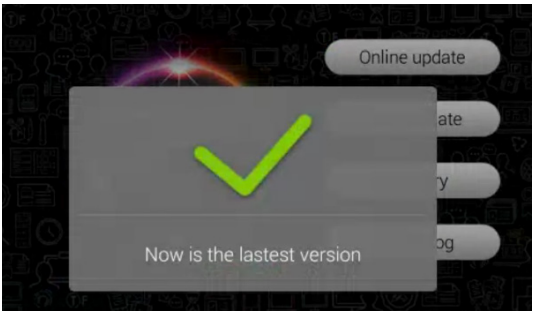
Toccare l'icona **App** nella schermata **Home**.

Toccare l'icona a forma di **ingranaggio** per aprire la schermata Impostazioni.

Toccare l'icona **Aggiorna**.

Toccare **Aggiornamento online.**

Nota: se sul dispositivo è già installato l'aggiornamento più recente, viene visualizzato un messaggio che informa che è in uso la versione più aggiornata.



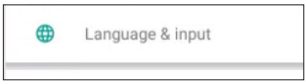
Se è disponibile un nuovo aggiornamento, il sistema provvede a scaricarlo ed è possibile procedere e accettare l'aggiornamento toccando il pulsante relativo all'aggiornamento.

È importante consentire l'elaborazione dell'aggiornamento. Al termine, il sistema viene riavviato automaticamente per applicare l'aggiornamento. Consentire al sistema di completare questo processo, in quanto la relativa interruzione potrebbe causare instabilità del dispositivo in termini di utilizzo.

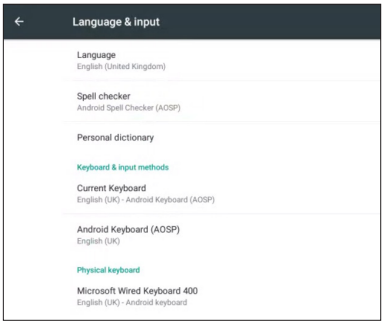
Lingua e inserimenti

Toccare l'app **Impostazioni**.

Toccare **Lingua e inserimenti**.



In questa sezione è possibile configurare le impostazioni di Lingua e tastiera specifiche per la propria regione/paese.



Sicurezza

Toccare l'app **Impostazioni**.

Toccare **Sicurezza**.

Selezionare i parametri di sicurezza che si desiderano modificare.

NOTA:

consultare l'Appendice per scoprire le migliori procedure relative alla politica di sicurezza.

Data e ora

Toccare l'app **Impostazioni**.

Toccare **Data e ora.**

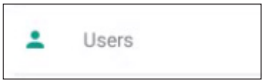
Selezionare la data e l'ora specifici per la propria regione.

Nota: per impostare il proprio fuso orario, è necessario disattivare l'impostazione Fuso orario automatico.

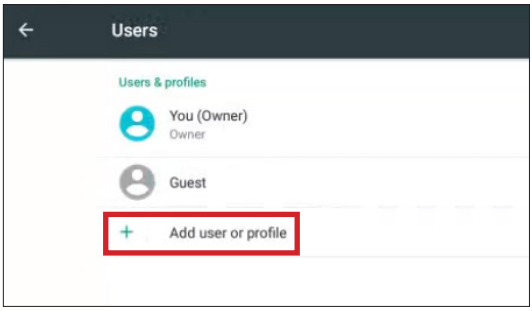
Creazione di utenti

Toccare l'app **Impostazioni**.

Toccare **Utenti.**



Toccare **Aggiungi utente o profilo**.



Sono disponibili due opzioni, pertanto è possibile selezionare quale opzione creare. Ad esempio:

- **Utente** - Può essere selezionato per un membro dello staff
- **Profilo limitato** - Può essere adatto agli studenti

App ActivCast™ (mirroring)

La suite di applicazioni Activcast consente ai dispositivi Windows®, Mac OS X®, iOS™, Android™ e Chrome OS™ d eseguire il mirroring dei propri schermi al ricevitore ActivCast tramite wireless. L'applicazione ricevitore ActivCast è pre-installata sul dispositivo e può essere eseguita dalla schermata principale del dispositivo.

Per i dispositivi per i quali si desidera trasmettere lo schermo al ricevitore ActivCast, il dispositivo di invio necessita dell'installazione di un'applicazione. Questa affermazione non è necessariamente applicabile ai prodotti iOS e Mac OS X, in quanto i dispositivi Apple® dispongono di dispositivi integrati che inviano segnali per il mirroring con i quali ActivCast è compatibile. Tuttavia sono numerosi i vantaggi derivanti dall'uso dell'app ActivCast. Attualmente, non si dispone di un dispositivo di invio ActivCast per Mac OS X, in quanto quest'ultimo dispone di un simile dispositivo integrato. Se si desidera sfruttare tutte le funzioni extra del dispositivo di invio ActivCast, è possibile utilizzare il browser Chrome su OS X e installare il plug-in del dispositivo di invio ActivCast.

Per acquisire i dispositivi di invio ActivCast, accedere alla seguente URL e scorrere fino alla sezione di download Software.

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

Per istruzioni su come effettuare il mirroring dello schermo del dispositivo consultare questo articolo.

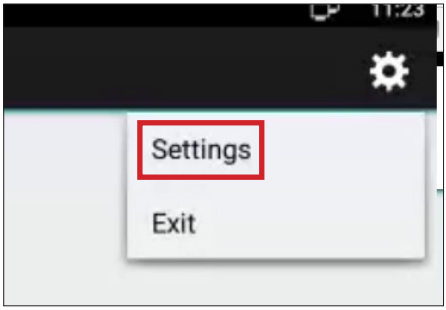
https://support.prometheanworld.com/article/?kb=1532

Denominazione dispositivi

Quando si avvia l'applicazione Activcast dalla schermata principale dei dispositivi, è possibile rinominare l'identificazione del ricevitore. Si consiglia di assegnare un nome univoco a ciascun dispositivo/ActivPanel. Ad esempio "ActivPanel 1 per la classe" o "per la sala riunioni", o qualsiasi altra denominazione sia ritenuta corretta nell'ambiente scolastico/aziendale. In questo modo è possibile identificare dove si trovano i dispositivi all'interno della scuola.

Toccare l'icona ActivCast nella schermata principale.

Nell'angolo superiore destro della schermata, toccare **Impostazioni**.



Toccare il **Nome dispositivo** e modificare il nome per adeguarlo alle convenzioni stabilite dalla propria organizzazione. Consigliamo inoltre di impostare un codice pin in questa schermata per incrementare il livello di sicurezza. Una volta configurata questa impostazione, il dispositivo di invio riceverà istruzione di inserire questo codice.

Affinché il mirroring funzioni correttamente, il ricevitore e il dispositivo di invio ActivCast devono essere collegati a una rete raggiungibile da entrambi i dispositivi. La rete può essere sia cablata che wireless. La connessione a una rete è stabilita dal sistema operativo sul dispositivo di invio e il ricevitore tramite gli strumenti integrati standard propri del sistema operativo.

Dal punto di vista della sicurezza, ActivCast funziona sul computer di un utente come qualsiasi altra applicazione, pertanto è soggetta a tutte le politiche di sicurezza dell'organizzazione.

Per consentire il corretto funzionamento di Airplay® è necessario attenersi a quanto segue:

- Se la rete in uso utilizza un firewall, è necessario impostare l'applicazione ActivCast come attendibile e la rete viene applicata a profili pubblici, privati e domini.
- Le porte seguenti devono essere aperte e consentite:

  TCP da 6000 a 7000, 7100, 47000, 47010

  UDP 5353, da 6000 a 7000, 7011

Mirroring dello schermo

Airplay non richiede una configurazione in grado di rilevare i dispositivi compatibili sulla rete, grazie al *rilevamento del servizio basato su DNS*, basato su *DNS multicast*, vale a dire **Bonjour**®. Tuttavia, sono presenti istanze in cui Bonjour o Multicast non possono essere supportati su una rete o in cui esistono più VLAN e sottoreti. Promethean ha sviluppato una tecnologia che agevola queste situazioni e sarà illustrata in seguito nel presente documento.

Il mirroring dello schermo si ottiene trasmettendo un codice **H.264** e una trasmissione video AES 128bit cifrata attraverso la connessione TCP.

Questa trasmissione è inserita in un pacchetto con header 128 byte. L'audio **AAC-ELD** viene inviato tramite il protocollo Airplay. Per quanto riguarda l'orologio principale, viene sincronizzato tramite **NTP**.

Inoltre, non appena un client inizia a riprodurre video, viene effettuata una connessione Airplay standard per inviare l'URL video e il mirroring viene interrotto. In questo modo si evita di dover decodificare o ricodificare il video, causando perdite in termini di qualità.

Richieste HTTP

Il mirroring dello schermo si collega a una porta 7100 hardcoded. Si tratta di un server HTTP che supporta le seguenti richieste:

POST /riproduzione

Avviare la trasmissione video in tempo reale. Il client invia un elenco proprietario binario contenente informazioni sulla riproduzione, immediatamente seguite dalla riproduzione stessa. A questo punto, la connessione non è più una connessione HTTP valida.

Non appena il server riceve una richiesta **/stream**, invierà le richieste NTP al client sulla porta 7010, anch'essa hardcoded. Il client deve eseguire l'esportazione dell'orologio principale in questa posizione e questo verrà utilizzato per la sincronizzazione audio/video e il ripristino dell'orologio.

Pacchetti di riproduzione

La riproduzione video è inserita in un pacchetto che utilizza header da 128 byte, seguita da un payload opzionale.

Dati Codec

Questo pacchetto contiene i dati extra H.264 in formato **avcC** *(ISO/IEC 14496:15)* e viene inviato all'inizio della riproduzione, ogni volta che le proprietà video potrebbero subire modifiche, quando si modifica l'orientamento dello schermo e quando lo schermo viene acceso o spento.

Sincronizzazione oraria

Le richieste vengono inviate al client Airplay a intervalli di 3 secondi. La data di riferimento per data e ora corrisponde all'inizio della sessione di mirroring.

Protezione tramite password

Un server Airplay può necessitare di una password per la visualizzazione dei contenuti di una rete. Questa password viene implementata tramite lo standard **HTTP Digest Authentication** *(RFC 2617)*, tramite HTTP per qualsiasi occasione.

Questa protezione tramite password viene implementata automaticamente da ActivCast.

Rilevamento

I dispositivi di invio ActivCast che funzionano con ricevitori ActivCast devono stabilire su quale ricevitore ActivCast eseguire il mirroring.

Esistono quattro modalità principali per identificare il ricevitore ActivCast:

- Tramite il nome
- Tramite un codice QR
- Tramite un ID di connessione
- Tramite l'indirizzo IP

Tutti questi elementi sono presenti nella schermata principale dell'app del ricevitore ActivCast.

Il motivo per cui esistono diversi modi con cui il dispositivo può stabilire la connessione ad ActivConnect è legato alla modalità di configurazione delle reti.

Tramite il nome del ricevitore

Supponiamo che ActivConnect sia denominato "Classe".

Questo nome viene trasmesso tramite le reti alle quali è connessa l'app di ricezione ActivCast.

L'applicazione di invio ActivCast installata sul dispositivo è "in attesa" di questi nomi.

Quando viene ricevuto, un nome viene inserito in elenco. È sufficiente selezionarlo per stabilire la connessione.

Tuttavia, alcune reti bloccano questa trasmissione, chiamata Bonjour. Questo nome non viene mai visualizzato.

Tramite un codice QR

Se si dispone di un tablet/telefono e si avvia l'app di invio ActivCast è possibile eseguire la scansione del codice visualizzato sullo schermo AC.

Questo codice contiene tutte le informazioni necessarie per stabilire una connessione.

Il dispositivo deve trovarsi su una rete a cui sia collegato anche il ricevitore ActivCast, ma in questo modo non ci si deve preoccupare della trasmissione bonjour.

Tramite l'ID di connessione

Questo metodo elimina l'esigenza di disporre di Bonjour sulla rete. È molto simile alla disponibilità del codice QR su un dispositivo mobile in quanto anche questo metodo crea una voce di database per il dispositivo ActivCast e un ID di connessione che viene utilizzato per cercare le informazioni.

Di seguito viene riportato un flusso di lavoro di livello elevato...

L'applicazione ActivCast contatta un server cloud all'indirizzo promethean.api.splashtop.com e trasmette il suo nome e indirizzo IP alle reti a cui è collegata. Il server cloud quindi crea un ID di connessione e il ricevitore ActivCast lo visualizza.

Ora sul dispositivo di invio è possibile utilizzare l'applicazione ActivCast e toccare l'icona che consente di inserire l'ID di connessione.

Quando l'utente digita questo ID, l'ID di connessione viene nuovamente inviato al servizio cloud citato sopra dal dispositivo dell'utente. Il servizio quindi cerca l'ID nel database e reinvia il suo nome e indirizzo IP al dispositivo di invio, che a sua volta stabilisce la connessione.

I dispositivi devono trovarsi sulla stessa rete a cui è collegata l'unità del ricevitore ActivCast.

Questo metodo non funziona se il ricevitore ActivCast o il dispositivo di invio non dispongono di una connessione a Internet per poter raggiungere il servizio cloud. Inoltre, se un firewall o proxy sono configurati sulla rete, questi potrebbero bloccare l'URL splashtop prometheanapi. In tal caso, gli esperti IT dovrebbero riuscire ad aggiungere l'URL all'elenco degli elementi consentiti.

Tramite l'indirizzo IP

Questa modalità consente di stabilire una connessione diretta senza dover accedere a un server cloud o utilizzare bonjour.

Il dispositivo di invio deve poter raggiungere l'indirizzo IP visualizzato. Ci si deve trovare su una delle reti alle quali è collegato il ricevitore ActivCast.

Regolazione delle prestazioni per il mirroring

Se si esaminano le prestazioni di invio wireless di dati sullo schermo del dispositivo tramite una rete a un dispositivo ricevente è necessario prendere in considerazione numerosi fattori.

Spesso gli utenti riportano che quando si utilizzano questi protocolli di mirroring wireless a casa, tutto funziona correttamente, vale a dire essi riescono a inviare il proprio schermo alla TV senza alcun problema. Quando poi gli utenti cercano di effettuare questa operazione al lavoro/a scuola le condizioni potrebbero essere molto diverse.

Uno dei principali problemi si riscontra in quanto i requisiti di un organizzazione in termini di collegamento in rete devono approcciarsi a sicurezza, larghezza di banda e segmentazione delle reti in modo molto serio. Esistono innumerevoli motivi per i quali una demo su una rete dedicata spesso presenta prestazioni eccellenti mentre quando viene distribuita in un ambiente reale il risultato sperato non viene quasi mai raggiunto.

Lo stato attuale delle soluzioni di presentazioni wireless disponibili sul mercato le vede tutte vulnerabili a queste condizioni.

A questo scopo, desideriamo accertarci che gli utenti siano consapevoli degli ostacoli che possono presentarsi durante l'uso di un'applicazione di mirroring, in modo da poter regolare di conseguenza le proprie aspettative.

La sezione all'interno di questo documento che illustra i requisiti di rete è da prendere in considerazione solamente per la fase di rilevamento, in quanto esamina dettagliatamente questo aspetto. Se si presuppone che la fase di rilevamento di un dispositivo di invio e un ricevitore abbia stabilito una connessione, possiamo concentrarci sulla effettiva trasmissione dei dati dello schermo del dispositivo di invio al ricevitore.

Requisiti di larghezza di banda

Affinché il dispositivo possa inviare il proprio schermo tramite la rete a 1080p, la rete deve poter essere in grado di gestire 8 Mbps per trasmettere questi dati e perché il ricevitore li possa visualizzare.

Se un utente desidera riprodurre un video 1080p a 25 fotogrammi al secondo si può affermare che 20 Mbps sono sufficienti.

Ciò presume che diversi utenti stiano eseguendo queste azioni, che l'infrastruttura wireless non sia affollata da altre attività e che si disponga di una buona copertura e di un'ottima larghezza di banda.

Questo argomento in particolare non può essere trattato in modo approfondito all'interno del presente documento né tantomeno Promethean dichiara che l'app ActivCast o qualsiasi altra tecnologia di mirroring commerciale equiparabile, diffusa tramite reti normali, possa garantire prestazioni perfette in qualsiasi condizione.

Per ricapitolare, quindi, il dispositivo di invio ActivCast/dispositivo di invio nativo Airplay comprime i dati su schermo e li trasmette in un ambiente sconosciuto.

Il ricevitore quindi codifica quei dati e li invia allo schermo.

Riteniamo di aver ottimizzato le procedure di compressione e codifica, ma non abbiamo alcun poter sulla rete.

Considerando quanto sopra affermato e illustrato, esistono alcuni suggerimenti e indicazioni su come migliorare le prestazioni, se necessario.

Utilizzare collegamenti Ethernet

L'Ethernet è ancora il tipo di connessione più affidabile. Sebbene possa sembrare strano suggerire una connessione cablata per un sistema wireless, consigliamo caldamente che il dispositivo di ricezione ActivCast venga collegato tramite cavo.

Connessione Wi-Fi

Verificare la presenza di interferenze nella rete wireless. Accertarsi che il dispositivo di invio stia utilizzando la modalità 802.11 più rapida che possa gestire. Passare alla modalità a 5 GHz e verificare che il router sia configurato per l'uso ottimale di Airplay.

Questo elenco non è completo, in quanto sono presenti altre variabili ambientali da tenere in considerazione.

Risoluzione del display del dispositivo di invio

Il dispositivo di invio potrebbe impiegare una risoluzione troppo elevata, che la rete non riesce ad elaborare. Se si cerca di inviare al ricevitore uno schermo con risoluzione 4k, è molto probabile che la rete non sia in grado di gestire un tale quantitativo di dati. Cercare di ridurre la risoluzione del dispositivo di invio per poter raggiungere prestazioni accettabili.

Bluetooth

Poiché Bluetooth e wireless 802.11 sono controllati dalla stessa interfaccia e dispongono di antenne adiacenti, è possibile che interferiscano tra loro quando sono entrambi in uso. Si consiglia di spegnere il Bluetooth su entrambi i dispositivi durante il mirroring.

APPENDICE: Passcode e politica di sicurezza

"Passcode o passphrase non sono la stessa cosa delle password. Una passcode/passphrase è una versione più lunga della password e, pertanto, più sicura. Generalmente una passcode/passphrase è composta da più parole e, pe questo motivo, le passcode/passphrase sono più sicure in caso di attacchi e rientrano a tutti gli effetti nel sistema di sicurezza di un dispositivo"

Panoramica

Le passcode costituiscono un aspetto importante della sicurezza di un computer. Una passcode scarsa può causare accessi non autorizzati e/o sfruttamento delle risorse dell'organizzazione. Tutti gli utenti, compresi soggetti terzi e fornitori con accesso ai sistemi dell'organizzazione, sono tenuti a seguire i passaggi indicati di seguito per selezionare e rendere sicure le proprie password.

I professionisti IT sono inoltre responsabili di garantire che la sicurezza del dispositivo sulla rete sia affidabile e sottoposta a continui backup, per soddisfare i requisiti dell'organizzazione.

Scopo

Lo scopo della presente politica è stabilire uno standard per la creazione di passcode affidabili in ActivPanel/ ActivConnect G-Series, nonché proteggere le passcode e stabilirne la frequenza di modifica.

Questa politica riporta inoltre le migliori procedure relative alla sicurezza del dispositivo da applicare per ActivPanels/ ActivConnect G-Series.

Ambito

L'ambito di questa politica include tutto il personale (utenti finali/amministratori IT) che dispone o è responsabile d un account su ActivPanels/ActivConnect G-Series con accesso alla struttura e alla relativa rete.

1.0 Politica

1.1. Creazione della passcode/Sicurezza dello schermo:
(Blocco schermo: impostato come predefinito dopo 5 secondi dalla pressione del pulsante di sospensione)

Tutte le passcode di livello utente e sistema devono risultare conformi al regolamento dell'organizzazione. A esempio, semplici, numeriche, alfanumeriche, alfanumeriche complesse e speciali schemi di caratteri. La lunghezza minima deve essere compresa tra 1 e 16 caratteri. Una buona passcode è relativamente lunga e contiene una combinazione di lettere maiuscole e minuscole e di caratteri numerici e punteggiatura.

1.2. Modifica della passcode: le passcode per account di gestione applicazione, amministrazione, abilitazione e root, ad esempio, devono essere cambiate ogni tre mesi o sulla base delle regole dell'organizzazione di appartenenza.

1.3. Visibilità della passcode: si consiglia di disattivare questa funzione.

1.4. Passcode di livello utente: l'intervallo di modifica consigliato ammonta a 30 giorni o sulla base delle regole dell'organizzazione.

1.5. Protezione tramite passcode/riutilizzo di una passcode: impedire l'uso delle passcode due o tre volte

1.6. Passcode: non condividere la propria passcode con nessuno. Tutte le passcode devono essere considerate come informazioni riservate e confidenziali.

1.7. Passcode: non inserire le proprie passcode in messaggi e-mail o altri tipi di comunicazioni elettroniche.

1.8. Non riportare una passcode su questionari o moduli di sicurezza.

1.9. Non fornire suggerimenti in merito al formato di una passcode (ad esempio, "il mio cognome").

1.10. Non condividere la propria passcode con nessuno, compresi assistenti amministrativi, segretari, manager, colleghi mentre si è in vacanza e membri della propria famiglia.

1.11. Non scrivere le passcode da nessuna parte né tantomeno custodirle da qualche parte in ufficio. Non memorizzare le passcode su un file sul computer o sui dispositivi mobile (telefono, tablet) senza che siano state crittografate.

1.12. Chiunque sospetti che la propria passcode possa essere stata compromessa deve riportare l'accaduto al dipartimento IT e modificare tutte le password.

1.13. Blocco automatico: ActivPanel/ActivConnect G-Series. Dopo 15 minuti di inattività, si consiglia di impostare ActivPanel per il blocco automatico, per evitare a terzi parti di accedere a dati riservati.

1.14. Antivirus: tutti i dispositivi ActivPanel/ActivConnect G-Series devono essere protetti da un software antivirus per evitare le minacce derivanti da apparecchiature USB mobili e siti Web/app esterni. L'antivirus è impostato per eseguire la scansione delle applicazioni o dei supporti alla prima installazione.

1.15. Crittografia del dispositivo: si consiglia di eseguirla su ActivPanel/ActivConnect G-Series per proteggere i dati digitali riservati archiviati sul dispositivo.

1.16. Installazione da fonti sconosciute: l'impostazione predefinita blocca l'installazione di app sconosciute. Si consiglia di mantenere questa impostazione per evitare potenziali minacce.

1.17. Notifiche: si consiglia di non visualizzare notifiche quando ActivPanel/ActivConnect G-Series sono bloccati (ad es. informazioni/e-mail riservate).

1.18. Backup e ripristino: se ActivConnect G-Series risulta compromesso, si consiglia che gli account di amministrazione dell'applicazione eseguano le azioni necessarie.

2.0 Requisiti utente

2.1. Gli utenti devono caricare solo i dati importanti e fondamentali per i propri ruoli in ActivPanel/ ActivConnect G-Series.

2.2. Gli utenti devono riportare immediatamente tutti i casi di rotture/malfunzionamenti al dipartimento IT.

2.3. Se un utente sospetta che si sia verificato un accesso non autorizzato ai dati scolastici/aziendali tramite ActivPanel/ActivConnect G-Series l'utente deve riportare tale eventualità conformemente alla procedura di gestione dei problemi della propria organizzazione.

2.4. ActivPanel/ActivConnect G-Series non devono disporre di software/firmware, progettati per poter accedere a funzionalità che non possono essere divulgate agli utenti.

2.5. Gli utenti non devono caricare software piratati o contenuti illegali su ActivPanel/ActivConnect G-Series.

2.6. Le applicazioni devono essere installate solamente da fonti approvate di piattaforme proprietarie ufficiali. L'installazione di codice da fonti non considerate affidabili è vietata. Se non si è certi se un'applicazione provenga o meno da una fonte approvata, contattare il proprio dipartimento IT.

2.7. Gli ActivPanel/ActivConnect G-Series devono essere mantenuti aggiornati con le più recenti patch del produttore o di rete. Come requisito minimo, è necessario controllare la presenza di patch settimanalmente e applicarle almeno una volta al mese.

2.8. Gli ActivPanel/ActivConnect G-Series non devono essere collegati a un PC che non dispone di una protezione antivirus e malware aggiornata e attiva e che non risulta conforme alle politiche dell'azienda/ scuola.

2.9. I dispositivi devono essere crittografati secondo gli standard di conformità della propria organizzazione.

2.10. Gli utenti devono fare attenzione se decidono di unire account di posta personali e lavorativi su ActivPanel/ ActivConnect G-Series. In particolare, devono prestare particolare attenzione a inviare i dati aziendali solamente tramite il sistema di posta aziendale. Se un utente sospetta l'invio di dati aziendali da un account di posta personale, contenuti sia nel corpo dell'e-mail sia come allegati, deve immediatamente informare il dipartimento IT di <Azienda X>.