

**Promethean**

# ActivPanel™

## ActivConnect™ OPS-G

Guida all'amministrazione IT

# Indice

Indice	2
Introduzione	3
Connessioni di rete	4
Impostazioni	6
Mirroring dello schermo	9
Sicurezza	13

# Introduzione

ActivConnect OPS-G è un potente dispositivo Android fornito con ActivPanel.

Questa guida mostra agli amministratori IT come configurare ActivConnect OPS-G.

Questa guida presuppone quanto segue per ActivConnect OPS-G:

- Il dispositivo è stato installato e montato su ActivPanel tramite la staffa appropriata.
- Il dispositivo è acceso.

# Connessioni di rete

ActivConnect OPS-G dispone di Gigabit Ethernet, Wi-Fi Dual Band 802.11 a/b/g/n/ac (RTL8822) e hardware Bluetooth® 4.1 integrati.

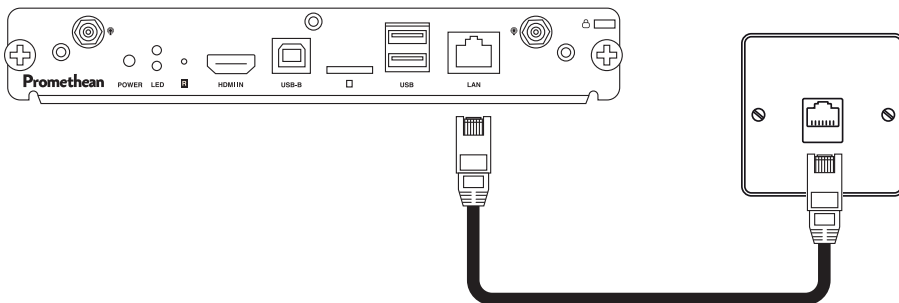
È possibile collegare ActivConnect OPS-G a reti cablate (Ethernet) e wireless (Wi-Fi).



Per prestazioni migliori, connettersi a una rete cablata quando possibile.



## Connessione a una rete cablata

Utilizzare un cavo di rete per collegare ActivConnect OPS-G a una porta di rete.





Se la propria organizzazione utilizza un server DHCP (Dynamic Host Configuration Protocol), la connessione viene configurata automaticamente dopo aver collegato il cavo di rete. Se non è presente un server DHCP, contattare il dipartimento IT.

## Connessione a una rete wireless

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Wi-Fi**.
4. Attivare il Wi-Fi.  
Viene visualizzato un elenco di reti wireless disponibili.
5. Selezionare la rete a cui si desidera connettersi.

## Modifica delle impostazioni del proxy di rete

Per modificare le impostazioni del proxy di rete, è necessario conoscere un nome host o un indirizzo IP proxy, nonché un numero di porta proxy. Per i dettagli, contattare il proprio reparto IT.



1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Configurazione Ethernet > Proxy > Manuale**.
4. Inserire i dettagli proxy rilevanti.
5. Selezionare **Connetti**.

## Impostazione dell'hotspot Wi-Fi

ActivConnect OPS-G può creare una piccola area di copertura Wi-Fi. Questa funzionalità può fornire una connessione Internet ai dispositivi Wi-Fi nelle vicinanze. Consente inoltre il mirroring dello schermo wireless per un massimo di cinque dispositivi Wi-Fi.



Quando si utilizza ActivConnect OPS-G come hotspot Wi-Fi, ActivConnect OPS-G deve essere connesso a una rete cablata per fornire una connessione Internet ad altri dispositivi.

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Più > Tethering e hotspot portatile > Imposta hotspot Wi-Fi**.
4. Il nome predefinito dell'hotspot è ACON OPS.  
Per modificare il nome, accedere al menu precedente e selezionare **Più > Imposta nome dispositivo**.
5. Se necessario, modificare le impostazioni di **Sicurezza**.
6. Inserire una password e selezionare **Salva**.
7. Selezionare il pulsante di attivazione/disattivazione **Hotspot Wi-Fi portatile** per attivare l'hotspot.
8. Ora è possibile collegare i dispositivi Wi-Fi nelle vicinanze alla rete ActivConnect OPS-G.

# Impostazioni

Le impostazioni consentono di impostare ActivConnect OPS-G in base alle proprie esigenze.

Per ulteriori informazioni, consultare l'assistenza Android.



## Configurazione del Bluetooth

Il dispositivo ActivConnect OPS-G è dotato di Bluetooth. Questa funzione consente il trasferimento di file a corto raggio e il controllo di dispositivi Bluetooth situati nelle vicinanze.

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Bluetooth**.
4. Selezionare il pulsante di attivazione/disattivazione **Bluetooth** per attivarlo.



## Modifica della lingua

È possibile modificare la lingua e le impostazioni della tastiera.

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Lingua e inserimenti**.
4. Modificare le impostazioni richieste.

## Modifica di data e ora

È possibile modificare le impostazioni di data e ora.

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Data e ora**.
4. Selezionare un fuso orario o deselezionare l'opzione **Fuso orario automatico** per impostare manualmente la data e l'ora.

## Modifica delle impostazioni dello schermo





ActivConnect OPS-G rileva automaticamente la risoluzione di visualizzazione ottimale per ActivPanel.

È possibile modificare manualmente la risoluzione dello schermo e la frequenza di aggiornamento.

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Display**.
4. Selezionare **Risoluzione HDMI**.
5. Seleziona una risoluzione e una frequenza di aggiornamento.

## Modifica delle impostazioni di sicurezza

È possibile modificare le impostazioni di sicurezza, come il blocco dello schermo.



1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Sicurezza**.
4. Modificare le impostazioni richieste.

## Utenti





È possibile creare due tipi di account utente, in base alle relative esigenze:

- **Utente**  
Ogni utente ha le proprie app e i propri contenuti, senza restrizioni. Questo tipo di utente è adatto per i membri dello staff.
- **Profilo con limitazioni**  
Ogni utente con profilo con limitazioni ha le proprie app e i propri contenuti. È possibile limitare l'accesso a determinate app e contenuti, a seconda delle esigenze dell'utente. Questo tipo di utente è adatto per gli studenti.

## Aggiunta di utenti

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Utenti**.
4. Selezionare **Aggiungi utente o profilo**.
5. Selezionare il tipo di utente che si desidera creare.
6. Per modificare le impostazioni per il nuovo profilo utente, accedere come tale utente.

## Rimozione di utenti

1. Selezionare  > .
2. Selezionare **Impostazioni**.
3. Selezionare **Utenti**.
4. Scegliere il tipo di utente da rimuovere.
  - Per rimuovere un utente con restrizioni, selezionare , quindi **Rimuovi utente**.
  - Per rimuovere un utente senza restrizioni, selezionare  accanto al relativo nome.

## Aggiornamento del software



Aggiornare il software su ActivConnect OPS-G per assicurarsi che disponga sempre delle ultime patch e funzionalità di sicurezza.

Promethean comunicherà quando saranno disponibili nuovi aggiornamenti. Consigliamo inoltre di controllare manualmente gli aggiornamenti ogni mese.



Per garantire che tutti gli aggiornamenti importanti vengano scaricati e installati sul dispositivo, autorizzare i seguenti URL:

- <http://cdn-otaupdate.prometheanworld.com>
- <https://otaupdate.prometheanworld.com>

1. Selezionare  > .
2. Selezionare **Aggiorna**.
3. Selezionare **Aggiornamento online**.  
Se è disponibile un nuovo aggiornamento, il sistema lo scarica.
4. Al termine del download, accettare l'aggiornamento.  
Il dispositivo installa l'aggiornamento e si riavvia.

**Nota:** Non interrompere l'aggiornamento del software. Se l'aggiornamento del software viene interrotto, può influire sul software.



# Mirroring dello schermo

La funzione di mirroring dello schermo consente di trasmettere contenuti da altri dispositivi sulla schermata di ActivConnect OPS-G.

ActivConnect OPS-G è compatibile con i dispositivi che eseguono i seguenti sistemi operativi:

- Windows®
- iOS™
- Android
- Chrome OS™



Per ulteriori informazioni, vedere: <https://support.prometheanworld.com/article/?kb=1532>.

## Informazioni sull'app ActivCast



Per utilizzare il mirroring dello schermo con dispositivi Windows, Android e Chrome OS, è necessario utilizzare l'app ActivCast. L'app ActivCast è preinstallata su ActivConnect OPS-G. I dispositivi iOS possono eseguire il mirroring dei propri schermi senza l'app ActivCast, ma si consiglia di installarla.


È possibile scaricare l'app ActivCast tramite il link sottostante:

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

## Ridenominazione del dispositivo

Per semplificare il mirroring dello schermo, è possibile assegnare un nome a ActivConnect OPS-G.

Si consiglia di utilizzare un nome diverso per ciascun dispositivo, ad esempio "ActivPanel 1" o "ActivPanel Classroom 1".

1. Selezionare **ActivCast**.
2. Selezionare .
3. Selezionare **Impostazioni**.
4. Selezionare **Nome dispositivo**.
5. Inserire il nome del dispositivo.



Per migliorare la sicurezza, è possibile impostare un codice PIN che deve essere inserito su un dispositivo affinché questo possa utilizzare il mirroring dello schermo.

## Requisiti di rete per il mirroring dello schermo

Il mirroring dello schermo si ottiene trasmettendo un codice H.264 e una trasmissione video AES a 128 bit cifrata attraverso la connessione TCP. Questa trasmissione video è inserita in un pacchetto con header 128 byte. L'audio AAC-ELD viene inviato tramite il protocollo Airplay®. L'orologio principale è sincronizzato con NTP.

I dispositivi di ricezione e invio devono essere connessi alla stessa rete cablata o wireless.

Per utilizzare il mirroring dello schermo, assicurarsi che il firewall della rete sia impostato correttamente. Le porte seguenti devono essere aperte e consentite:

- TCP da 6000 a 7000, 7100, 47000 e 47010
- UDP 5353, da 6000 a 7000 e 7011

## Richieste HTTP

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

- POST/riproduzione
- Pacchetti di riproduzione
- Dati Codec
- Sincronizzazione oraria
- Protezione tramite password

### POST/riproduzione

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

Non appena il server riceve una richiesta di riproduzione, invierà le richieste NTP al client sulla porta 7010, anch'essa hardcoded. Il client deve eseguire l'esportazione dell'orologio principale 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). Viene inviato:

- All'inizio della riproduzione
- Ogni volta che le proprietà video potrebbero cambiare
- Quando l'orientamento dello schermo cambia
- 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

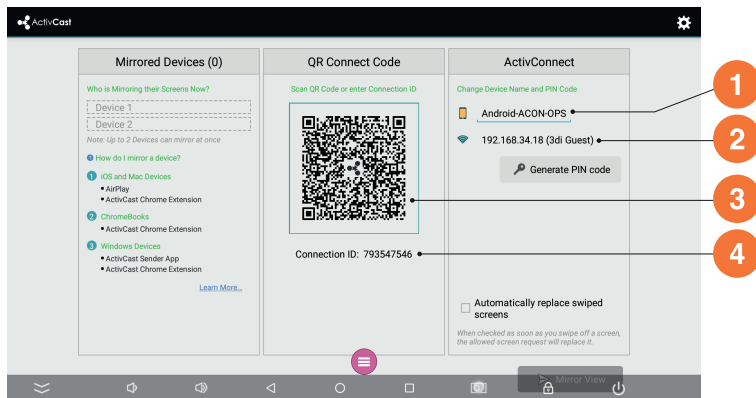
Un server Airplay può necessitare di una password per la visualizzazione dei contenuti di una rete. Questa password viene implementata tramite lo standard HTTP Digest Authentication (RFC 2617). La protezione tramite password viene implementata automaticamente da ActivCast.

# Identificazione del ricevitore ActivCast

Prima di poter avviare il mirroring dello schermo, il dispositivo di invio deve identificare il dispositivo ricevente.

## Opzioni per l'identificazione del ricevitore ActivCast

Esistono quattro modalità per identificare il ricevitore ActivCast. Questa informazione si trova nella schermata principale dell'app ActivCast sul dispositivo ricevente.



1

### Nome

Il nome del destinatario viene trasmesso ed è possibile collegarsi al ricevitore usando l'app ActivCast.

2

### Indirizzo IP

Crea una connessione diretta senza un server cloud.

3

### Codice QR

Se si dispone di un dispositivo mobile e si avvia l'app ActivCast, è possibile eseguire la scansione del codice QR visualizzato nella schermata di stato del mirroring ActivCast.

4

### ID di connessione

Il ricevitore ha un ID univoco. Crea una connessione diretta senza un server cloud.

## Suggerimenti per il mirroring dello schermo

Il mirroring dello schermo può essere influenzato da condizioni esterne come larghezza di banda, copertura di rete e impostazioni di sicurezza. Per ottenere la migliore esperienza durante la condivisione dello schermo, consultare i suggerimenti di seguito.

Funzionalità	Suggerimenti
Ethernet	Collegare il dispositivo ricevente alla rete con un cavo di rete. L'Ethernet è il tipo di connessione più affidabile.
Wi-Fi	Verificare la presenza di interferenze nella rete wireless. Accertarsi che il dispositivo di invio stia utilizzando la modalità 802.11 più rapida possibile. Passare alla modalità a 5 GHz. Configurare il router per l'utilizzo ottimale di Airplay.
Risoluzione del display sul dispositivo di invio	Il mirroring degli schermi ad alta risoluzione riduce le prestazioni. Ridurre la risoluzione del dispositivo di invio per poter raggiungere prestazioni accettabili.
Bluetooth	Disattivare il Bluetooth durante il mirroring dello schermo. Bluetooth e wireless 802.11 possono interferire tra loro.

Per impedire l'accesso non autorizzato o lo sfruttamento delle risorse della propria organizzazione, tutti gli utenti di ActivConnect OPS-G devono adottare le misure appropriate descritte nella politica di sicurezza.

Gli amministratori IT sono inoltre responsabili della gestione della sicurezza della rete del dispositivo e del rispetto delle norme di sicurezza dell'organizzazione.

## Politica di sicurezza

1. Tutti i passcode degli utenti e degli amministratori devono essere conformi alle politiche dell'organizzazione. I passcode devono essere relativamente lunghi e contenere una combinazione di lettere maiuscole, lettere minuscole, caratteri numerici e caratteri di punteggiatura.
2. Si consiglia di modificare i passcode degli amministratori ogni 3 mesi o secondo quanto richiesto dalle politiche dell'organizzazione.
3. Si consiglia di modificare i passcode degli utenti ogni 30 giorni o secondo quanto richiesto dalle politiche dell'organizzazione.
4. Si consiglia di disattivare la funzione di visibilità della password.
5. Non utilizzare lo stesso passcode più di una volta.
6. Non condividere il passcode con nessun altro, incluso il proprio manager o familiari.
7. Non inviare i passcode via e-mail.
8. Non rivelare i passcode su questionari o moduli di sicurezza.
9. Non fornire suggerimenti in merito al formato di un passcode (ad esempio, "il mio cognome").
10. Non scrivere i passcode.
11. Non memorizzare i passcode su dispositivi non crittografati.
12. Qualsiasi utente che sospetti che la compromissione del proprio passcode deve segnalarlo all'amministratore IT e cambiare immediatamente tutte le password.
13. Proteggere il dispositivo con un software antivirus.
14. Per proteggere i dati riservati memorizzati sul dispositivo, si consiglia di utilizzare la crittografia del dispositivo.
15. Non installare app provenienti da fonti sconosciute.
16. Si consiglia di disabilitare le notifiche quando il dispositivo è bloccato.
17. Se il dispositivo è compromesso, l'amministratore IT è responsabile dell'adozione delle azioni necessarie.

## Requisiti utente

1. Gli utenti devono utilizzare il dispositivo solo con dati rilevanti ed essenziali per il proprio ruolo.
2. Gli utenti devono segnalare tutti gli errori hardware e software all'amministratore IT.
3. Se un utente sospetta che si sia verificato un accesso non autorizzato ai dati tramite il dispositivo, deve segnalarlo come previsto dalla politica dell'organizzazione.
4. Non installare alcun software non destinato agli utenti.
5. Gli utenti non devono caricare software piratati o contenuti illegali sul dispositivo.
6. Le applicazioni devono essere installate solo da fonti approvate da Android.
7. Il dispositivo deve essere aggiornato con gli aggiornamenti software forniti dal produttore. Verificare la presenza di aggiornamenti software ogni mese.
8. Il dispositivo non deve essere collegato a dispositivi che non dispongono di protezione antivirus aggiornata e abilitata. Il dispositivo connesso deve inoltre rispettare la politica dell'organizzazione.

9. I dispositivi esterni devono essere crittografati in linea con la politica dell'organizzazione.
10. Gli utenti devono prestare attenzione all'utilizzo di account e-mail personali sul dispositivo. 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 l'amministratore IT.

---

IP-2094-IT-V02 ©2018 Promethean Limited. Tutti i diritti riservati. La disponibilità dei prodotti può variare a seconda del paese. Le specifiche del prodotto sono soggette a modifiche senza preavviso.