

Promethean

ActivPanel™

ActivConnect™ OPS-G

Guide d'administration informatique

Table des matières

Table des matières	2
Introduction	3
Connexions réseau	4
Paramètres	6
Mise en miroir d'écran	9
Sécurité	13

Introduction

L'ActivConnect OPS-G est un puissant appareil Android fourni avec votre ActivPanel.

Ce guide indique aux administrateurs informatiques comment configurer l'ActivConnect OPS-G.

Ce guide suppose que les conditions suivantes sont remplies pour l'ActivConnect OPS-G :

- L'appareil est installé et monté sur l'ActivPanel à l'aide du support approprié.
- L'appareil est sous tension.

Connexions réseau

ActivConnect OPS-G est équipé des fonctionnalités suivantes : Gigabit Ethernet, Wi-Fi bi-bande 802.11 a/b/g/n/ac (RTL8822) et Bluetooth® 4.1 intégré.

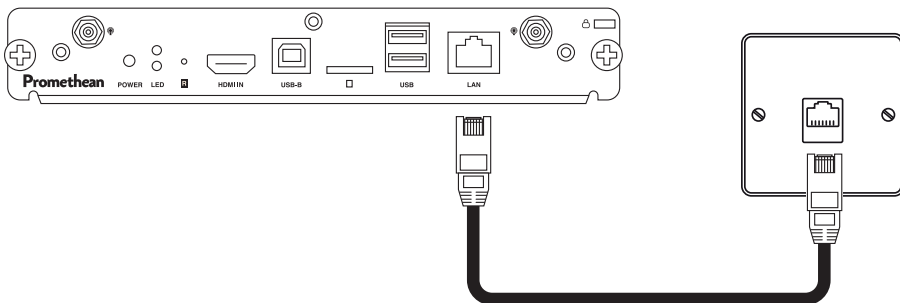
Vous pouvez connecter l'ActivConnect OPS-G à des réseaux câblés (Ethernet) et sans fil (Wi-Fi).



Pour de meilleures performances, établissez une connexion à un réseau câblé dès que possible.



Connexion à un réseau câblé

Utilisez un câble réseau pour connecter l'ActivConnect OPS-G à un port réseau.



Si votre entreprise utilise un serveur DHCP (Dynamic Host Configuration Protocol), la connexion est automatiquement configurée après que vous avez connecté le câble réseau. Si un serveur DHCP n'est pas en cours d'exécution, contactez votre service informatique.

Connexion à un réseau sans fil

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Wi-Fi**.
4. Activez le Wi-Fi.
La liste des réseaux sans fil disponibles s'affiche.
5. Sélectionnez le réseau auquel vous souhaitez vous connecter.

Modification des paramètres du proxy réseau

Pour modifier les paramètres du proxy réseau, vous devez connaître un nom d'hôte de proxy ou une adresse IP, ainsi qu'un numéro de port de proxy. Pour plus d'informations, contactez votre service informatique.



1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Configuration Ethernet > Proxy > Manuel**.
4. Saisissez les informations de proxy appropriées.
5. Sélectionnez **Connexion**.

Configuration du point d'accès Wi-Fi

ActivConnect OPS-G peut créer une petite zone de couverture Wi-Fi. Cette fonctionnalité permet d'établir une connexion Internet avec les appareils Wi-Fi à proximité. Elle permet également la mise en miroir d'écran sans fil pour un maximum de cinq appareils Wi-Fi.



Lorsque vous utilisez l'ActivConnect OPS-G comme point d'accès Wi-Fi, l'ActivConnect OPS-G doit être connecté à un réseau câblé pour fournir une connexion Internet à d'autres appareils.

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Plus > Point d'accès affilié et portable > Configurer un point d'accès sans fil**.
4. Le nom par défaut du point d'accès est ACON OPS.
Pour modifier le nom, revenez au menu précédent et sélectionnez **Plus > Définir le nom de l'appareil**.
5. Si nécessaire, modifiez les paramètres de **Sécurité**.
6. Saisissez un mot de passe et sélectionnez **Enregistrer**.
7. Sélectionnez le bouton à bascule **Point d'accès sans fil portable** pour activer le point d'accès.
8. Vous pouvez désormais connecter les appareils Wi-Fi à proximité au réseau ActivConnect OPS-G.

Paramètres

Les paramètres vous permettent de configurer l'ActivConnect OPS-G en fonction de vos besoins.

Pour plus d'informations, consultez l'aide d'Android.



Configuration Bluetooth

L'ActivConnect OPS-G est équipé du Bluetooth. Cette fonction permet de transférer des données à courte portée et de contrôler les appareils Bluetooth à proximité.

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Bluetooth**.
4. Sélectionnez le bouton à bascule **Bluetooth** pour l'activer.



Modification de la langue

Vous pouvez modifier les paramètres de langue et de saisie.

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Langue et saisie**.
4. Modifiez les paramètres nécessaires.

Modification de la date et de l'heure

Vous pouvez modifier les paramètres de date et d'heure.

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Date et heure**.
4. Choisissez un fuseau horaire ou désactivez l'option **Fuseau horaire automatique** pour définir manuellement la date et l'heure.

Modification des paramètres d'affichage





L'ActivConnect OPS-G détecte automatiquement la résolution d'affichage optimale pour l'ActivPanel.

Vous pouvez modifier manuellement la résolution d'affichage et le taux de rafraîchissement.

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Écran**.
4. Sélectionnez **Résolution HDMI**.
5. Sélectionnez une résolution et un taux de rafraîchissement.

Modification des paramètres de sécurité

Vous pouvez modifier les paramètres de sécurité tels que le verrouillage d'écran.



1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Sécurité**.
4. Modifiez les paramètres nécessaires.

Utilisateurs





Vous pouvez créer deux types de compte utilisateur, en fonction de vos besoins :

- **Utilisateur**
Chaque utilisateur dispose de ses propres applications et contenus, sans restrictions. Ce type d'utilisateur convient pour les membres du personnel.
- **Profil restreint**
Chaque utilisateur à profil restreint dispose de ses propres applications et contenus. Vous pouvez limiter l'accès à certaines applications et certains contenus selon les besoins de l'utilisateur. Ce type d'utilisateur convient pour les étudiants.

Ajout d'utilisateurs

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Utilisateurs**.
4. Sélectionnez **Ajouter un utilisateur ou un profil**.
5. Sélectionnez le type d'utilisateur que vous souhaitez créer.
6. Pour modifier les paramètres du profil du nouvel utilisateur connectez-vous avec le compte de cet utilisateur.

Suppression d'utilisateurs

1. Sélectionnez  > .
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Utilisateurs**.
4. Choisissez le type d'utilisateur à supprimer.
 - Pour supprimer un utilisateur limité, sélectionnez  puis **Supprimer l'utilisateur**.
 - Pour supprimer un utilisateur sans restrictions, sélectionnez  en regard de son nom.

Mise à jour du logiciel



Mettez à jour le logiciel de l'ActivConnect OPS-G afin de veiller à ce qu'il dispose toujours des dernières fonctionnalités et des derniers correctifs de sécurité.

Promethean vous informera lorsque de nouvelles mises à jour seront disponibles. Nous vous recommandons également de vérifier manuellement l'existence de mises à jour tous les mois.



Afin de veiller à ce que toutes les mises à jour importantes soient téléchargées et installées sur votre appareil, mettez les adresses URL sur liste blanche :

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

1. Sélectionnez  > .
2. Sélectionnez **Mettre à jour**.
3. Sélectionnez **Mise à jour en ligne**.
Si une nouvelle mise à jour est disponible, le système la télécharge.
4. Une fois le téléchargement terminé, acceptez la mise à jour.
L'appareil installe la mise à jour puis redémarre.

Remarque : N'interrompez pas la mise à jour de l'appareil. En cas d'interruption de la mise à jour, le logiciel peut s'en trouver affecté.

Mise en miroir d'écran

La fonction de mise en miroir d'écran vous permet de projeter du contenu d'autres appareils sur l'écran de l'ActivConnect OPS-G.

L'ActivConnect OPS-G est compatible avec les appareils exécutant les systèmes d'exploitation suivants :

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

 Pour plus d'informations, voir : <https://support.prometheanworld.com/article/?kb=1532>.

À propos de l'application ActivCast



Pour utiliser la mise en miroir d'écran sur des appareils Windows, Android et Chrome OS, vous devez utiliser l'application ActivCast. L'application ActivCast est préinstallée sur l'ActivConnect OPS-G. Les appareils iOS peuvent mettre en miroir leur écran sans l'application ActivCast, mais nous vous recommandons d'installer cette dernière.


Vous pouvez télécharger l'application ActivCast en suivant le lien ci-dessous :


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

Changement de nom de l'appareil

Afin de faciliter la mise en miroir, vous pouvez donner un nom à votre ActivConnect OPS-G.

Nous vous recommandons d'utiliser un nom différent pour chaque appareil, par exemple « ActivPanel 1 » ou « ActivPanel Salle 1 ».

1. Sélectionnez **ActivCast**.
2. Sélectionnez .
3. Sélectionnez **Paramètres**.
4. Sélectionnez **Nom de l'appareil**.
5. Saisissez le nom de l'appareil.

 Afin d'améliorer la sécurité, vous pouvez définir un code PIN qui doit être saisi sur un appareil avant de permettre l'utilisation de la mise en miroir d'écran.

Configuration réseau requise pour la mise en miroir d'écran

La mise en miroir d'écran s'effectue par transmission d'un flux vidéo (codage H.264 et chiffrement AES 128 bits) via une connexion TCP. Ce flux vidéo est mis en paquets avec un en-tête de 128 octets. Le flux audio AAC-ELD est envoyé via le protocole Airplay®. L'horloge principale est synchronisée avec NTP.

Les appareils émetteurs et destinataires doivent être connectés au même réseau câblé ou sans fil.

Pour utiliser la mise en miroir d'écran, veillez à ce que le pare-feu de votre réseau soit correctement configuré. Les ports suivants doivent être ouverts et autorisés :

- TCP 6000-7000, 7100, 47000, 47010
- UDP 5353, 6000-7000, 7011

Requêtes HTTP

La mise en miroir d'écran nécessite un port 7100 codé de manière irréversible. Il s'agit d'un serveur HTTP qui prend en charge les requêtes suivantes :

- POST/stream
- Paquets de flux
- Données codec
- Synchronisation heure
- Protection par mot de passe

POST/stream

La transmission vidéo en direct est lancée. Le client envoie une liste de propriétés binaires contenant les métadonnées de flux, immédiatement suivies du flux proprement dit. À ce stade, il ne s'agit plus d'une connexion HTTP valide.

Dès que le serveur reçoit une requête de flux, il envoie les requêtes NTP au client sur le port 7010, lui aussi codé de manière irréversible. Le client doit y exporter son horloge principale, laquelle sera utilisée pour la synchronisation audio-vidéo et la récupération d'horloge.

Paquets de flux

Ce flux est mis en paquets avec un en-tête de 128 bits, suivi d'une charge utile optionnelle.

Données codec

Ce paquet contient les données H.264 complémentaires au format AVCC (ISO/CEI 14496:15). Il est envoyé :

- au début du flux ;
- chaque fois que les propriétés vidéo sont susceptibles de changer ;
- lorsque l'orientation de l'écran change ;
- lorsque l'écran est allumé ou éteint ;

Synchronisation heure

Les requêtes sont envoyées au client Airplay avec 3 secondes d'intervalle. La date de référence pour l'horodateur correspond au début de la séance de mise en miroir.

Protection par mot de passe

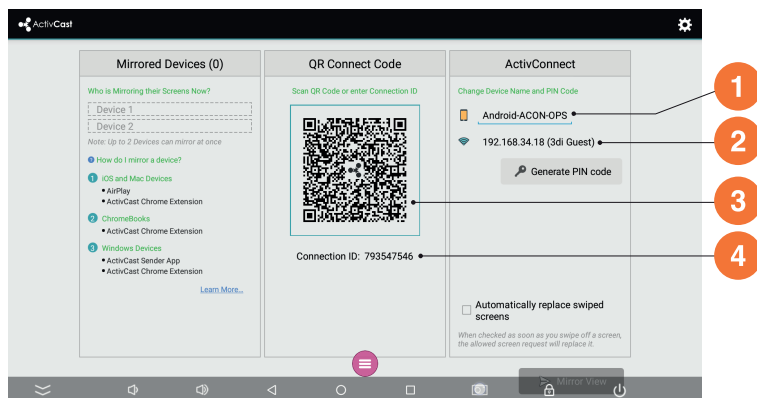
Un serveur Airplay peut nécessiter la saisie d'un mot de passe pour l'affichage de tout contenu à partir du réseau. Cette intégration s'effectue via une authentification HTTP Digest standard (RFC 2617). La protection par mot de passe est automatiquement mise en œuvre par ActivCast.

Identification du récepteur ActivCast

Avant que vous puissiez démarrer la mise en miroir d'écran, l'appareil émetteur doit identifier l'appareil destinataire.

Options d'identification du récepteur ActivCast

Il existe quatre moyens d'identifier le récepteur ActivCast. Ces informations s'affichent à l'écran principal de l'application ActivCast sur l'appareil destinataire.



1 Nom
Le nom du récepteur est diffusé et vous pouvez vous connecter au récepteur à l'aide de l'application ActivCast.

2 Adresse IP
Crée une connexion directe sans serveur cloud.

3 Code QR
Si vous possédez un appareil mobile et si vous démarrez l'application ActivCast, vous pouvez scanner le code QR affiché à l'écran de statut de la mise en miroir de l'application ActivCast.

4 ID de connexion
Le récepteur dispose d'un ID unique. Crée une connexion directe sans serveur cloud.

Astuce pour la mise en miroir d'écran

La mise en miroir d'écran peut être affectée par des facteurs externes tels que la bande passante, la couverture réseau et les paramètres réseau. Afin de bénéficier de la meilleure expérience possible lors de la mise en miroir de l'écran, suivez les conseils ci-dessous.

Fonctionnalité	Conseil
Ethernet	Connectez votre appareil destinataire au réseau à l'aide d'un câble réseau. Ethernet est le type de connexion le plus fiable.
Wi-Fi	Vérifiez l'état des interférences sur le réseau sans fil. Vérifiez que l'appareil émetteur utilise le mode 802.11 le plus rapide possible. Passez en mode 5 GHz. Configurez le routeur pour un usage Airplay optimal.
Résolution d'affichage sur l'appareil émetteur	La mise en miroir d'écrans haute résolution réduit les performances. Diminuez la résolution de l'appareil émetteur jusqu'à atteindre des performances acceptables.
Bluetooth	Désactivez le Bluetooth pendant la mise en miroir d'écran. Les fonctions Bluetooth et sans fil 802.11 peuvent créer des interférences entre elles.

Afin d'empêcher tout accès non autorisé ou toute exploitation des ressources de votre entreprise, il est recommandé à tous les utilisateurs de l'ActivConnect OPS-G de suivre les étapes appropriées décrites dans la politique de sécurité.

Les administrateurs informatiques sont également tenus d'assurer la sécurité réseau de l'appareil et de se conformer aux réglementations de sécurité de l'entreprise.

Politique de sécurité

1. Tous les codes d'accès utilisateur et administrateur doivent être conformes aux politiques de votre entreprise. Les codes d'accès doivent être relativement longs et contenir une combinaison de majuscules, de minuscules, de chiffres et de signes de ponctuation.
2. Modifiez les codes d'accès administrateur tous les 3 mois ou à la fréquence établie par les politiques de votre entreprise.
3. Modifiez les codes d'accès utilisateur tous les 30 jours ou à la fréquence établie par les politiques de votre entreprise.
4. Nous vous recommandons de désactiver la fonction d'affichage du mot de passe.
5. N'utilisez pas plusieurs fois le même mot de passe.
6. Ne partagez vos codes d'accès avec personne, y compris votre responsable ou les membres de votre famille.
7. N'envoyez pas vos codes d'accès par e-mail.
8. N'affichez pas vos codes d'accès dans les questionnaires ou les formulaires de sécurité.
9. Ne donnez pas d'indice concernant vos codes d'accès (par exemple, « mon nom de famille »).
10. Ne notez pas vos codes d'accès par écrit.
11. N'enregistrez pas vos codes d'accès sur des appareils non chiffrés.
12. Tout utilisateur suspectant une compromission de ses codes d'accès doit le signaler à son administrateur informatique et modifier immédiatement tous ses mots de passe.
13. Protégez l'appareil avec un logiciel antivirus.
14. Afin de protéger les données confidentielles enregistrées sur l'appareil, nous vous recommandons d'utiliser le chiffrement d'appareil.
15. N'installez pas d'applications de sources inconnues.
16. Nous vous recommandons de désactiver les notifications lorsque l'appareil est verrouillé.
17. Si l'appareil est compromis, l'administrateur informatique est tenu de prendre les mesures éventuelles qui s'imposent.

Configuration utilisateur requise

1. Les utilisateurs doivent utiliser l'appareil uniquement avec des données pertinentes et essentielles à leur travail.
2. Les utilisateurs doivent signaler toute défaillance matérielle et logicielle à l'administrateur informatique.
3. Si un utilisateur pense qu'un accès non autorisé aux données a eu lieu via l'appareil, il doit le signaler conformément aux politiques de l'entreprise.
4. N'installez aucun logiciel non destiné aux utilisateurs.
5. Les utilisateurs ne doivent pas charger de logiciels piratés ou de contenu illégal sur l'appareil.
6. Les applications installées doivent obligatoirement provenir de sources approuvées par Android.
7. L'appareil doit être maintenu à jour avec les mises à jour logicielles fournies par le fabricant. Vérifiez l'existence de mises à jour tous les mois.

8. L'appareil ne doit pas être connecté à des appareils ne disposant d'aucune protection antivirus à jour activée. L'appareil connecté doit également être conforme aux politiques de l'entreprise.
9. Les appareils externes doivent être chiffrés conformément aux politiques de l'entreprise.
10. Les utilisateurs doivent faire preuve de prudence lorsqu'ils utilisent des comptes de messagerie personnels sur l'appareil. Ils doivent veiller à ce que les données de l'entreprise soient uniquement envoyées via le système de messagerie de l'entreprise. Si un utilisateur soupçonne que des données de l'entreprise ont été envoyées à partir d'un compte de messagerie électronique personnel, que ce soit dans le corps du texte ou en pièce jointe, il doit en informer l'administrateur informatique.

TP-2094-FR-V02 ©2018 Promethean Limited. Tous droits réservés. La disponibilité des produits dépend du pays. Les spécifications produit sont sujettes à modification sans préavis.