Promethean™

ActivConnect™ G-Series

ActivPanel™

Guide d'intégration pour les administrateurs informatiques

TP-2046-FR-V01

Table des matières

Introduction et avertissements

Votre ActivPanel est fourni avec un périphérique informatique Android ™ 5.1 (Lollipop) ultraperformant. Bien que l'ActivPanel puisse être considéré par l'utilisateur comme un dispositif complet tout-en-un, les administrateurs informatiques doivent, quant à eux, bien comprendre que le panneau et le système ActivConnect G-Series sont des éléments bien distincts. Cette approche modulaire présente de nombreux avantages en termes d'administration, de maintenance et de flexibilité pour les mises à niveau.

L'objectif de ce guide est d'assister les administrateurs informatiques dans la configuration du dispositif pour une utilisation optimale au sein de votre organisation.

Dans le présent guide, nous partons du principe que le dispositif est déjà installé et monté sur l'ActivPanel grâce au support approprié, alimenté et connecté aux ports USB et HDMI® conformément aux indications du guide d'installation.

Le sens des termes techniques utilisés est censé être maîtrisé. À ce titre, il ne s'agit pas d'un guide destiné à l'utilisateur final qui souhaiterait se servir du dispositif en question.

Il est entendu que l'ActivPanel doit être sous tension et que le dispositif est activé et affiche l'écran d'accueil.

Application des paramètres

Au fil de ce guide, vous serez invité à accéder au volet des paramètres à de nombreuses reprises. Par conséquent, nous vous recommandons de vous familiariser avec les modes d'accès à ce dernier.

Vous serez amené à lancer cette application tout au long du présent guide. Il s'agit d'une composante essentielle pour réussir la configuration de l'unité. Nous nous concentrons ici sur les paramètres principaux, mais si vous souhaitez approfondir le sujet, nous vous recommandons de rechercher les articles relatifs à Android Lollipop présents sur Internet.

L'application des paramètres ci-dessous vous permet de modifier les paramètres du dispositif afin de répondre aux exigences de votre organisation.

À partir de l'écran d'accueil du dispositif, vous devrez accéder à cette application.

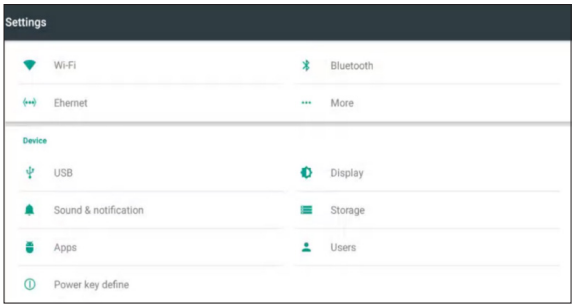
Dans le coin droit inférieur de l'écran d'accueil, vous retrouvez l'icône de catégorie d'application.

Appuyez sur cette icône.

Recherchez la catégorie des paramètres. L'icône relative à cette catégorie ressemble à un rouage.

Appuyez sur l'application des paramètres au sein de cette catégorie.

L'écran des paramètres s'affiche.



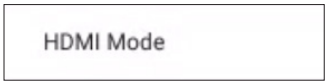
Configuration de l'écran

En principe, il n'est pas nécessaire de configurer la résolution de l'écran car le dispositif détecte la résolution optimale en fonction de l'écran auquel il est connecté.

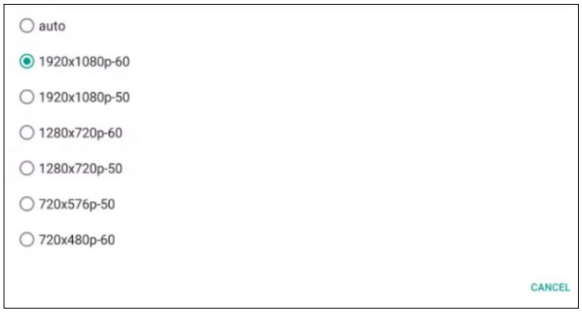
Toutefois, si vous souhaitez vérifier ou modifier la résolution, lancez l'application des paramètres, comme décrit ci-avant et accédez à l'écran des paramètres.

Appuyez sur Affichage.

Appuyez ensuite sur Mode HDMI



Sélectionnez la résolution et la fréquence souhaitées.



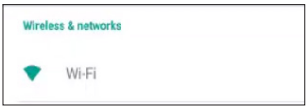
Le dispositif est équipé des fonctionnalités suivantes : Gigabit Ethernet, Wi-Fi® bi-bande 802.11 b/g/n/ac (AP6335) et Bluetooth® 4.0 intégré.

Selon la configuration de déploiement de votre infrastructure réseau, vous avez le choix entre le réseau Wi-Fi sur le dispositif ou l'Ethernet filaire. Pour des performances optimales, nous vous recommandons vivement de relier le dispositif à une connexion filaire.

Configuration Wi-Fi (voir l'annexe pour les paramètres de sécurité recommandés)

Lancez l'application des paramètres comme décrit ci-avant et accédez à l'écran des paramètres.

Pour ouvrir les paramètres, appuyez sur Wi-Fi.



Appuyez sur le bouton bascule pour activer la Wi-Fi.

Le dispositif recherche alors les connexions Wi-Fi disponibles.

Les connexions disponibles s'affichent dans la fenêtre en dessous du bouton bascule.

Appuyez sur le réseau Wi-Fi auquel vous souhaitez vous connecter.

Paramètres proxy réseau

Continuez avec les étapes suivantes si votre organisation utilise les paramètres proxy réseau.

Vous aurez besoin des informations suivantes :

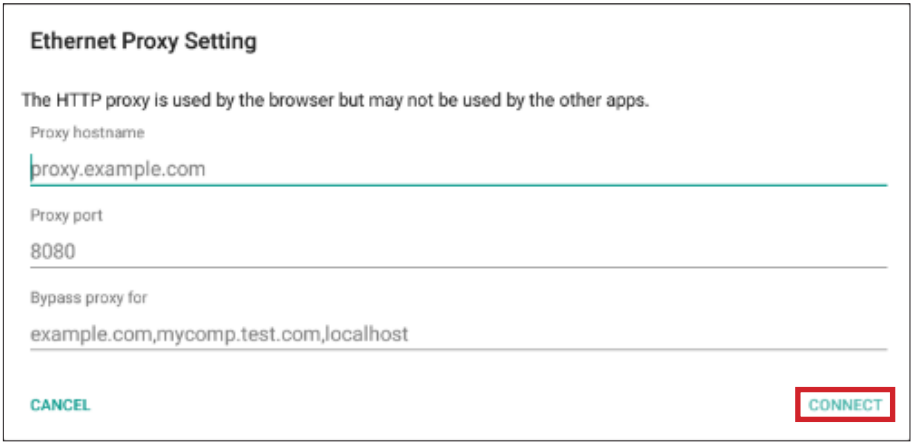
- Nom d'hôte du proxy ou adresse IP et numéro de port du proxy. Si vous ne disposez pas de ces informations, contactez votre service informatique.
- Si votre organisation requiert un paramètre proxy sans fil, cliquez sur le nom du réseau sans fil (SSID) approprié. La fenêtre ci-dessous s'affichera.

Sélectionnez Options avancées, puis appuyez sur Proxy.

Appuyez sur Manuel.

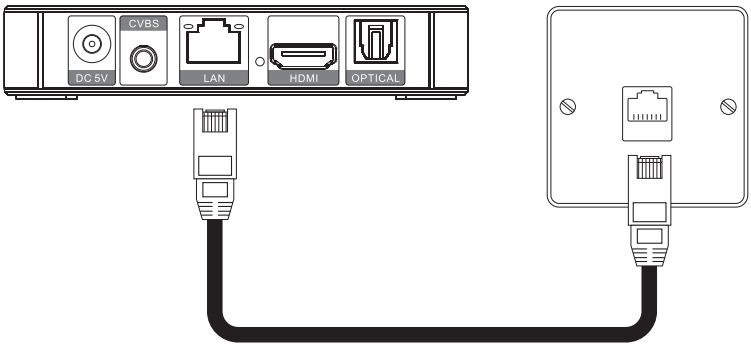
Saisissez les informations de paramètres proxy appropriées ci-dessous concernant votre réseau sans fil.

Une fois la saisie terminée, saisissez votre mot de passe de réseau sans fil et appuyez sur Se connecter.



Configuration d'Ethernet (filaire)
(voir l'annexe pour les paramètres de sécurité recommandés)

Pour que le signal réseau soit plus fiable et durable, nous vous recommandons de connecter un câble réseau entre le port LAN du dispositif et le port réseau de la classe ou du bureau.



REMARQUE IMPORTANTE :

Si votre organisation exécute un serveur de protocole DHCP (Dynamic Host Configuration Protocol), une fois le câble réseau connecté, toutes les configurations seront automatiquement assignées. Si le serveur de protocole DHCP ne s'exécute pas : veuillez faire appel à votre service informatique.

PARAMÈTRES PROXY RÉSEAU

Continuez avec les étapes suivantes si votre organisation utilise les paramètres proxy réseau.

Vous aurez besoin des informations suivantes :

- Nom d'hôte du proxy ou adresse IP et numéro de port du proxy. Si vous ne disposez pas de ces informations, contactez votre service informatique.

À partir de l'écran des paramètres, appuyez sur Ethernet.

Appuyez sur Proxy.

Appuyez sur Manuel.

Saisissez les paramètres proxy appropriés concernant votre connexion Ethernet filaire (contactez votre service informatique si vous ne disposez pas de ces informations). Une fois les informations saisies, appuyez sur Se connecter.

Configuration d'un mode de point d'accès

Le dispositif peut créer un réseau Wi-Fi de portée restreinte, permettant aux dispositifs Wi-Fi à proximité de se connecter (ou d'améliorer la connectivité) à Internet via le point d'accès. Vous pouvez envisager cette option si votre signal Internet est de faible qualité ou en cas de mise en miroir sans fil. Le point d'accès en lui-même n'offre pas de connectivité Internet mais si vous connectez un câble Ethernet au dispositif connecté à Internet, les utilisateurs pourront se connecter au Web grâce à une connexion au point d'accès. Selon vos politiques de sécurité, vous pouvez ou non choisir cette option. Elle est désactivée par défaut.

Ce mode est particulièrement intéressant pour les dispositifs de mise en miroir, même si Internet n'est pas présent/souhaité.

Veuillez noter qu'à l'heure actuelle, cinq appareils maximum peuvent être reliés au dispositif.

Accédez à l'application des paramètres pour procéder à la configuration. Veuillez vous référer aux instructions sur les modalités de lancement de l'application des paramètres.

Sur l'écran des paramètres, sélectionnez l'option Plus.

Sélectionnez Partage de connexion et point d'accès mobile.

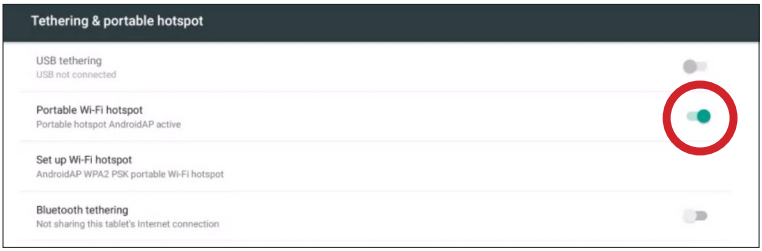
Appuyez ensuite sur l'option de configuration du point d'accès Wi-Fi.

Le nom par défaut du point d'accès (SSID) est AndroidAP. Vous pouvez lui réattribuer le nom de votre choix.

Vous pouvez également changer le type de sécurité sur cet écran.

Saisissez un mot de passe et appuyez sur Enregistrer.

Appuyez sur le bouton bascule du point d'accès Wi-Fi mobile pour activer ce dernier.



Ce paramètre diffuse le nom SSID du réseau que vous avez configuré ; vous pouvez alors y connecter vos dispositifs via le processus standard, en sélectionnant le SSID dans la configuration des paramètres sans fil.

Configuration Bluetooth

Le dispositif est équipé de la fonctionnalité Bluetooth 4.0. Plusieurs applications sont possibles : transfert de fichiers à courte portée mais aussi commande de robots et de divers dispositifs. Par défaut, la fonctionnalité Bluetooth est désactivée. Vous pouvez l'activer ou la désactiver à partir de l'écran des paramètres.

Appuyez sur Bluetooth.

Appuyez sur le bouton bascule Bluetooth pour activer cette fonctionnalité.

Vérification de la mise à jour du logiciel

Le dispositif inclut une application OTA (Over The Air) qui recherche régulièrement de nouvelles mises à jour et donne à l'utilisateur la possibilité de les accepter le cas échéant.

L'application OTA peut être également lancée manuellement.

Ces mises à jour sont importantes car nous appliquons souvent des correctifs de sécurité ainsi que des mises à jour de système d'exploitation conjointement à des améliorations et optimisations de fonctionnalités.

REMARQUE :

Afin que le dispositif effectue des mises à jour régulières, il est capital que l'URL suivante soit enregistrée sur liste blanche : http://cdn-otaupdate.prometheanworld.com.
Son enregistrement sur liste blanche garantit le téléchargement et l'installation de toutes les mises à jour importantes.

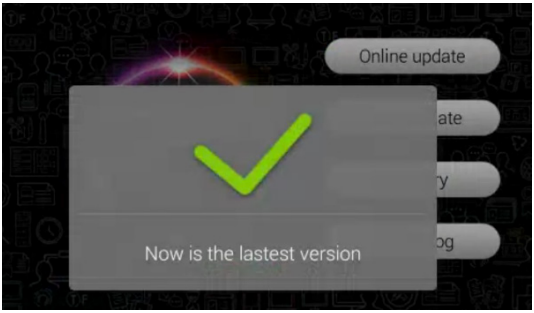
Appuyez sur l'icône **Application** dans l'écran d'**accueil**.

Pour ouvrir l'écran des paramètres, appuyez sur l'icône représentant un **rouage**.

Appuyez sur l'icône **Mettre à jour**.

Appuyez sur l'icône **Mise à jour en ligne**.

Remarque : Si la dernière mise à jour est déjà installée sur le dispositif, un message s'affiche vous informant que la toute dernière version est en cours d'utilisation.



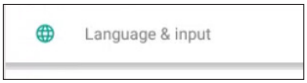
Si une nouvelle mise à jour est disponible, le système la télécharge. Vous pouvez ensuite appuyer sur le bouton de mise à jour pour accepter cette dernière.

Vous devez impérativement autoriser la procédure de mise à jour. Après quoi, le système redémarre automatiquement et effectue la mise à jour. Veillez à ne pas interrompre la procédure, au risque de provoquer des défaillances au niveau du dispositif.

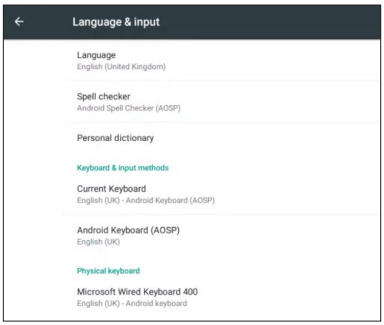
Langue et saisie

Appuyez sur l'application des **Paramètres**.

Appuyez sur **Langue et saisie**.



Dans cette section, vous pouvez définir les paramètres de langue et de saisie spécifiques à votre zone/pays.



Sécurité

Appuyez sur l'application des **Paramètres**.

Appuyez sur **Sécurité**.

Sélectionnez les paramètres de sécurité que vous souhaitez modifier.

REMARQUE :

Consultez l'annexe pour connaître les meilleures pratiques en matière de politique de sécurité.

Date et heure

Appuyez sur l'application des **Paramètres**.

Appuyez sur **Date et heure**.

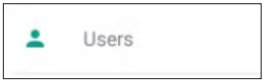
Sélectionnez la date et l'heure correspondant à votre région.

Remarque : pour définir votre fuseau horaire, vous devez d'abord désactiver le paramètre Fuseau horaire automatique.

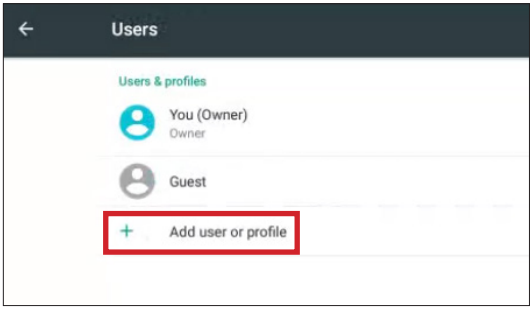
Création de profils d'utilisateur

Appuyez sur l'application des **paramètres**.

Appuyez sur **Utilisateurs**.

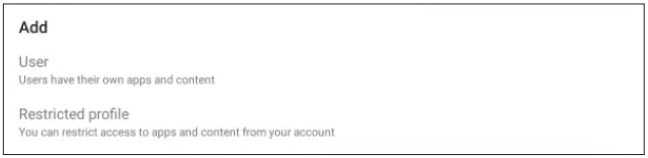


Appuyez sur **Ajouter un utilisateur ou un profil**.



Faites votre choix parmi les deux options proposées. Par exemple :

- **Utilisateur** : peut s'appliquer à un membre du personnel, par exemple
- **Profil limité** : peut s'appliquer aux élèves, par exemple



Application ActivCast™ (mise en miroir)

La suite d'applications permet la projection des écrans Activcast Windows®, Mac OS X®, iOS™, Android™ et Chrome OS™ sur le récepteur ActivCast en mode sans fil. L'application du récepteur ActivCast est préinstallée sur votre dispositif et peut être exécutée à partir de l'écran d'accueil dudit dispositif.

Une application dédiée devra être installée sur les dispositifs dont les écrans doivent être projetés sur le récepteur Activcast ; à l'exception des dispositifs iOS et Mac OS X® qui disposent d'émetteurs de mise en miroir intégrés compatibles avec ActivCast. Toutefois, l'utilisation de l'application de l'émetteur ActivCast présente de nombreux avantages. Actuellement, il n'existe pas d'émetteur ActivCast pour Mac OS X car ce système inclut un émetteur intégré. Si vous souhaitez bénéficier de fonctionnalités supplémentaires concernant l'émetteur ActivCast, vous pouvez utiliser le navigateur Chrome sous OS X et installer le plug-in émetteur ActivCast.

Pour acquérir les émetteurs ActivCast, veuillez accéder à l'URL suivante et faites défiler la page jusqu'à la section des téléchargements logiciels.

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

Pour savoir comment projeter l'écran de votre dispositif, consultez l'article suivant :

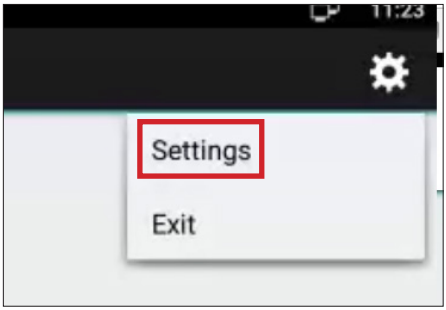
https://support.prometheanworld.com/article/?kb=1532

Dénomination des dispositifs

Lorsque vous lancez l'application Activcast à partir de l'écran d'accueil de vos dispositifs, vous avez la possibilité de renommer l'identification du récepteur. Nous vous recommandons d'utiliser un nom différent pour chaque dispositif/ActivPanel : par exemple, ActivPanel classe 1, Salle de conférence... ou tout autre nom en conformité avec les usages en cours au sein de votre école/entreprise. Vous pourrez ainsi identifier l'emplacement des différents dispositifs dans l'établissement.

Appuyez sur l'icône ActivCast dans l'écran d'accueil.

Appuyez sur l'icône en forme de rouage, puis sur celle des **Paramètres** dans le coin droit supérieur de l'écran.



Appuyez sur le **nom de l'appareil** et modifiez le nom conformément aux usages en cours dans votre école/entreprise. Pour plus de sécurité, nous vous recommandons de définir un code PIN à partir de cet écran des paramètres. Une fois le code enregistré, l'appareil émetteur vous invitera à le saisir.

Prérequis réseau pour la mise en miroir

Pour que la mise en miroir fonctionne correctement, le récepteur et l'émetteur ActivCast doivent être connectés à un réseau accessible par l'émetteur et le récepteur, lesquels doivent pouvoir prendre en charge le routage. La connexion peut être filaire ou sans fil. La connexion à un réseau est établie par un système d'exploitation sur l'émetteur et le récepteur grâce aux outils standard intégrés dudit système.

En matière de sécurité, la solution ActivCast fonctionne comme n'importe quelle autre application sur la machine de l'utilisateur. Elle est soumise à l'ensemble des politiques de sécurité de l'organisation.

Pour permettre le bon fonctionnement d'Airplay®, les conditions suivantes doivent être remplies :

- Si votre réseau utilise un pare-feu, vous devez définir l'application ActivCast comme approuvée. Cette procédure s'applique aux profils Domaine, Privé et Public.
- Les ports suivants doivent être ouverts et autorisés :

  TCP 6000-7000, 7100, 47000, 47010

  UDP 5353, 6000-7000, 7011

Mise en miroir d'écran

Airplay ne requiert pas de configuration pour la détection de dispositifs compatibles sur le réseau, grâce à la fonctionnalité de *découverte des services DNS* basée sur la *multidiffusion DNS*, à savoir **Bonjour®**. Cependant, dans certains cas, Bonjour ou la multidiffusion ne peuvent pas être pris en charge sur un réseau, notamment lorsque plusieurs réseaux VLAN ou sous-réseaux existent. Promethean a développé une technologie permettant de gérer ce type de situation. Ce point sera abordé ci-après.

La mise en miroir d'écran est effectuée via la transmission d'un flux vidéo (codage **H.264** et chiffrage 128 bit AES) via une connexion TCP.

Ce flux est mis en paquets avec un en-tête de 128 bits. Le flux audio **AAC-ELD** est envoyé via le protocole Airplay. L'horloge principale est synchronisée via **NTP**.

De plus, dès qu'un client lance une lecture de vidéos, une connexion Airplay standard est établie pour envoyer l'URL de la vidéo, et la mise en miroir est interrompue. Cette procédure permet d'éviter le décodage et le ré-encodage de la vidéo, synonymes de perte de qualité.

Requêtes HTTP

La mise en miroir d'écran se connecte à un port 7100 codé de manière irréversible. Il s'agit d'un serveur HTTP prenant en charge les requêtes suivantes :

POST /stream

La transmission vidéo en direct est lancée. Le client envoie une liste de propriétés binaires contenant des informations relatives au 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 **/stream**, 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

Le paquet contient les données H.264 complémentaires au format **avcC** *(ISO/IEC 14496:15)*. Il est envoyé au démarrage du flux, à chaque fois que les propriétés de la vidéo sont susceptibles de changer, lorsque l'écran change d'orientation et lorsque ce dernier est mis sous/hors tension.

Synchronisation date/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 projection.

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)*, via HTTP dans tous les cas.

Cette protection par mot de passe est automatiquement mise en œuvre par ActivCast.

Découverte

Les émetteurs ActivCast fonctionnant avec les récepteurs ActivCast doivent identifier le récepteur ActivCast prévu pour la projection.

Il existe quatre moyens d'identifier le récepteur ActivCast :

- À partir de son nom
- À partir d'un code QR
- À partir d'un ID de connexion
- À partir de son adresse IP

Tous ces éléments se trouvent dans l'écran principal de l'application du récepteur ActivCast.

L'existence de plusieurs modalités de connexion entre votre dispositif et ActivConnect est liée à la configuration des réseaux.

Nom du récepteur

Admettons que votre ActivConnect est dénommé Salle de classe.

Ce nom est diffusé parmi le ou les réseaux auxquels l'application réceptrice ActivCast est connectée.

L'application de l'émetteur ActivCast installée sur votre dispositif est en attente de ces noms.

À chaque fois qu'un nom est saisi, il est aussitôt répertorié. En cliquant simplement dessus, vous serez connecté.

Néanmoins, certains réseaux bloquent cette diffusion, dénommée Bonjour. Ce nom ne s'affiche jamais.

À partir d'un code QR

Si vous disposez d'une tablette ou d'un téléphone et que vous lancez l'application de l'émetteur ActivScan, vous pouvez scanner le code affiché sur l'écran de l'AC.

Ce code contient toutes les informations nécessaires à la mise en connexion.

Votre dispositif doit se trouver sur un réseau auquel le récepteur ActivCast est également connecté, mais ceci élimine tous les problèmes liés à la diffusion via Bonjour.

ID de connexion

Cette méthode ne nécessite pas le fonctionnement de Bonjour sur votre réseau. Le principe est similaire à celui du code QR disponible sur mobile dans le sens où une entrée de base de données est créée pour votre dispositif ActivCast ; un ID de connexion servant à la consultation d'informations est également créé.

Il s'agit d'un workflow de niveau élevé.

L'application ActivCast contacte un serveur cloud sur promethean.api.splashtop.com et communique son nom ainsi que son ou ses adresses IP aux réseaux auxquels il est connecté. Le serveur cloud crée ensuite un ID de connexion que le récepteur ActivCast affiche.

Vous pouvez utiliser l'application ActivCast sur votre dispositif émetteur et appuyer sur l'icône vous permettant de saisir l'ID de connexion.

Une fois la saisie effectuée, l'ID de connexion est à nouveau envoyé au service cloud mentionné ci-dessus, à partir du dispositif de l'utilisateur. L'ID est recherché dans la base de données et le nom ainsi que l'adresse IP sont renvoyés à l'émetteur qui, à son tour, établit la connexion.

Les dispositifs doivent être sur le même réseau que celui auquel l'unité du récepteur ActivCast est connectée.

Cette méthode ne fonctionne pas si le récepteur ActivCast ou le dispositif émetteur ne dispose pas de connexion Internet pour atteindre le service cloud. De plus, si un pare-feu ou un proxy est configuré sur votre ou vos réseaux, l'URL du splashtop promethean.api. risque d'être bloquée. Auquel cas, les services informatiques devront mettre cette URL sur liste blanche.

Par adresse IP

Une connexion directe est établie sans qu'un accès au serveur cloud ni l'utilisation de Bonjour ne soient nécessaires.

Votre dispositif émetteur doit être en mesure d'accéder à l'adresse IP affichée. Vous devez être sur l'un des réseaux auxquels le récepteur ActivCast est relié.

Réglage des performances pour la mise en miroir

Plusieurs facteurs doivent être pris en compte lorsqu'il s'agit d'évaluer les performances d'envoi en mode sans fil de données d'écran d'un dispositif via un réseau vers un dispositif récepteur.

Les utilisateurs observent souvent que lorsqu'ils utilisent de tels protocoles de mise en miroir sans fil à domicile, aucun problème ne survient en ce qui concerne l'envoi de données pour la projection de leur écran sur le téléviseur. Il en est tout autrement lorsque les utilisateurs font la même expérience au travail ou à l'école.

L'un des principaux enjeux pour les organisations en matière de mise en réseau consiste à prendre en compte les questions de sécurité, de bande passante et de segmentation des réseaux. Si votre démonstration se passe dans les meilleures conditions sur un réseau dédié, cela ne sera pas forcément le cas si elle est déployée à grande échelle dans un environnement élargi. Bien des facteurs peuvent expliquer cette réalité.

Les solutions de présentation sans fil actuellement proposées sur le marché présentent toutes des vulnérabilités à cet égard.

C'est pourquoi nous souhaitons vous sensibiliser (ainsi que vos utilisateurs) aux obstacles susceptibles de surgir lorsque vous utilisez une application de mise en miroir, de façon à ce que vous vous prépariez en conséquence.

La section du présent document décrivant les prérequis réseau ne concerne que la phase de découverte, étudiée sous tous ses aspects. Considérons une phase de découverte au cours de laquelle un émetteur et un récepteur établissent une connexion. Il s'agit de se pencher sur la transmission réelle des données d'écran du dispositif émetteur vers le récepteur.

Prérequis concernant la bande passante

Supposons qu'un dispositif transmet le contenu de son écran via un réseau 1080p. D'après des calculs, ce réseau devrait pouvoir prendre en charge un débit de 8 Mbits/s pour la transmission des données et l'affichage par le récepteur.

Si l'utilisateur souhaite diffuser une vidéo 1080p à raison de 25 images par seconde, un débit de 20 Mbits/s sera probablement suffisant. En supposant qu'un certain nombre d'utilisateurs effectuent ces actions, que l'infrastructure sans fil ne soit pas mobilisée par d'autres activités et que vous disposiez d'une bonne couverture et d'une excellente bande passante.

Ce sujet à proprement parler ne peut pas être abordé en détail au sein de ce document. En aucun cas Promethean ne peut garantir que l'application ActivCast (de même que toute autre technologie de mise en miroir commercialisée comparable utilisant des réseaux standard) fonctionnera sans accroc dans toutes les situations.

Pour récapituler, l'émetteur Airplay natif/ActivCast compresse les données écran et les transmet dans un environnement inconnu.

Le récepteur décode ensuite ces données et les restitue à l'écran.

Nous nous sommes efforcés d'optimiser la compression ainsi que le décodage, mais nous ne sommes pas en mesure d'influencer le réseau.

Il existe malgré tout des astuces pour améliorer les performances, le cas échéant.

Utiliser une connexion Ethernet

La connexion Ethernet reste la plus fiable. Bien qu'une connexion filaire puisse vous sembler illogique pour un système sans fil, nous vous recommandons vivement de câbler votre installation pour le dispositif récepteur ActivCast.

Connexion Wi-Fi

Vérifiez l'état des interférences sur le réseau sans fil. Assurez-vous que le dispositif émetteur utilise bien le mode 802.11 le plus rapide possible. Passez en mode 5 GHz et assurez-vous que le routeur est configuré pour un usage Airplay optimal.

Il ne s'agit pas là d'une liste exhaustive : il existe d'autres considérations liées à l'environnement à prendre en compte.

Résolution de l'affichage du dispositif émetteur

Votre dispositif émetteur affiche peut-être une résolution trop élevée pour être prise en charge par votre réseau. Si vous essayez d'envoyer les données d'un écran 4K vers le récepteur, il est fort probable que votre réseau ne pourra pas prendre en charge cette quantité de données. Pensez à réduire la résolution du dispositif émetteur jusqu'à ce que les performances soient correctes.

Bluetooth

Étant donné que les connexions Bluetooth et sans fil 802.11 sont contrôlées à partir de la même interface et disposent d'antennes adjacentes, il y a un risque d'interférences entre ces deux types de connexions lorsqu'elles sont activées au même moment. Nous vous recommandons de **désactiver** le mode Bluetooth pour les **deux** dispositifs lors de la mise en miroir.

ANNEXE : Codes d'accès et politique de sécurité

« Les codes d'accès et les phrases secrètes diffèrent des mots de passe. Un code d'accès/une phrase secrète est une version développée d'un mot de passe et présente donc un plus haut degré de sécurité. Un code d'accès/une phrase secrète est en principe composé(e) de plusieurs mots. À ce titre, il/elle offre davantage de sécurité contre les éventuelles attaques et constitue ainsi un élément central du système de sécurité d'un dispositif. »

Vue d'ensemble

Le code d'accès représente un des piliers de la sécurité des ordinateurs. Un code d'accès mal choisi peut entraîner des intrusions non autorisées et/ou une exploitation des ressources de votre organisation. Tous les utilisateurs, y compris les sous-traitants et les fournisseurs, disposant d'un accès à vos systèmes sont tenus de prendre les mesures adéquates (telles que décrites ci-dessous) lors du choix et de la sécurisation de leur mot de passe.

Quand aux responsables informatiques, ils doivent veiller à ce que la sécurisation du dispositif sur le réseau soit fiable et à ce qu'un système de récupération d'urgence soit disponible. Les politiques de l'organisation en la matière doivent être également respectées.

Objectif

L'objectif de la présente politique est d'établir une norme pour la création de codes d'accès fiables sur les systèmes ActivPanel/ActivConnect G-Series, tout en protégeant lesdits codes d'accès, en déterminant la fréquence à laquelle ils doivent être modifiés.

La politique présente également les meilleures pratiques à adopter en matière de sécurité des dispositifs pour les systèmes ActivPanel/ActivConnect G-Series.

Portée

La présente politique s'adresse à tous les effectifs (utilisateurs finaux ou administrateurs informatiques) qui disposent ou sont responsables d'un compte sur les systèmes ActivPanel/ActivConnect G-Series, et qui sont en droit d'accéder à votre site et aux réseaux associés.

1.0 Politique

1.1. Création du code d'accès/Sécurité des données de l'écran (verrouillage de l'écran : défini par défaut sur 5 secondes après une pression sur le bouton de veille) :

Tous les codes d'accès, aux niveaux utilisateur et système, doivent être conformes à vos politiques. saisie simple, numérique, alphanumérique, alphanumérique complexe, caractères spéciaux, etc. ; nom d'utilisateur comprenant entre 1 et 16 caractères. Un mot de passe fiable doit être relativement long et comprendre une combinaison de lettres majuscules et minuscules, de chiffres et de caractères de ponctuation.

1.2. Changement de code d'accès : Il est recommandé de modifier les codes des comptes racine, d'activation, d'administration et d'administration des applications tous les trimestres, ou conformément aux politiques de votre organisation.

1.3. Visibilité du code d'accès : Nous vous recommandons de désactiver cette fonction.

1.4. Codes d'accès au niveau utilisateur : Il est recommandé de changer les codes tous les 30 jours. Le cas échéant, reportez-vous aux politiques de votre organisation.

1.5. Protection par code d'accès/réutilisation du code d'accès : empêchez que les codes d'accès soient utilisés deux ou trois fois.

1.6. Codes d'accès : ne communiquez votre code d'accès à personne. Tous les codes d'accès doivent être traités comme des informations sensibles et confidentielles.

1.7. Codes d'accès : veillez à ne pas insérer de codes d'accès dans vos messages électroniques et autres formes de communication électronique.

1.8. Ne communiquez pas vos codes d'accès dans les questionnaires ou formulaires de sécurité.

1.9. Ne donnez pas d'indications facilement identifiables pour vos codes d'accès (exemple : nom de famille).

1.10. Ne communiquez vos codes d'accès à personne, y compris des assistants, secrétaires, directeurs, collègues en vacances ou encore membres de votre famille.

1.11. N'écrivez pas vos codes d'accès et ne les laissez pas à la vue des autres sur votre lieu de travail. Ne conservez pas vos codes d'accès dans un fichier informatique ou dans vos dispositifs mobiles (téléphone, tablette), à moins de les chiffrer.

1.12. Tout utilisateur soupçonnant que son code d'accès a été compromis doit reporter l'incident aux services informatiques et changer tous ses mots de passe.

1.13. Verrouillage automatique : systèmes ActivPanel/ActivConnect G-Series. Il est recommandé d'activer la fonctionnalité de verrouillage automatique après 15 minutes d'inactivité, afin d'éviter tout accès aux données potentiellement sensibles des systèmes ActivPanel par des tiers.

1.14. Antivirus : tous les systèmes ActivPanel/ActivConnect G-Series doivent être protégés par un logiciel antivirus afin d'éviter toute menace provenant d'équipements USB mobiles et de sites/d'applications Web externes. Les antivirus sont configurés de façon à analyser les applications et/ou les médias lors de la première installation.

1.15. Chiffrement du dispositif : le chiffrement est recommandé pour les systèmes ActivPanel/ActivConnect G-Series de façon à protéger les données numériques confidentielles stockées sur votre dispositif.

1.16. Installation de sources inconnues : le blocage d'installations d'applications inconnues est défini par défaut. Il est recommandé de conserver ce paramètre afin de minimiser tout risque potentiel.

1.17. Notifications : nous vous recommandons de ne pas afficher les notifications (pouvant contenir des informations/e-mails sensibles) lorsque les systèmes ActivPanel/ActivConnect G-Series sont verrouillés.

1.18. Sauvegarde et réinitialisation : si le système ActivConnect G-Series est compromis, les comptes d'administration liés à l'application doivent prendre les mesures nécessaires pour y remédier.

2.0 Configuration utilisateur requise

2.1. Les utilisateurs envoient des données vers les systèmes ActivPanel/ActivConnect G-Series à condition qu'elles soient utiles/essentielles dans le cadre de leur fonction.

2.2. Les utilisateurs doivent reporter les défaillances et dysfonctionnements au département informatique sans délai.

2.3. Si un utilisateur soupçonne l'intrusion non autorisée dans des données de l'école/l'entreprise via les systèmes ActivPanel/ActivConnect G-Series, il devra reporter l'incident conformément aux procédures en vigueur.

2.4. Les systèmes ActivPanel/ActivConnect G-Series ne doivent pas être équipés de logiciels/micrologiciels conçus pour accéder à des fonctionnalités non destinées à l'utilisateur.

2.5. Les utilisateurs ne doivent pas charger de logiciels piratés ou aux contenus illicites sur les systèmes ActivPanel/ActivConnect G-Series.

2.6. Les applications doivent être installées uniquement à partir de sources approuvées sur les plateformes propriétaires officielles. L'installation d'un code issu de sources non approuvées est interdite. Si vous ne savez pas si une application provient d'une source approuvée, contactez votre département informatique.

2.7. Les systèmes ActivPanel/ActivConnect G-Series doivent être mis à jour avec les correctifs fournis (fabricant ou réseau). Les correctifs doivent être vérifiés au moins une fois par semaine et appliqués au moins une fois par mois.

2.8. Les systèmes ActivPanel/ActivConnect G-Series ne doivent pas être connectés à un ordinateur qui ne disposerait pas d'une protection antivirus/antimalware activée et qui ne respecterait pas la politique de l'entreprise/l'école.

2.9. Les dispositifs doivent être chiffrés en répondant aux normes de votre organisation.

2.10. Les utilisateurs doivent être particulièrement vigilants lorsqu'ils utilisent conjointement des comptes de messagerie électronique personnels et professionnels sur les systèmes ActivPanel/ActivConnect G-Series. Ils doivent notamment s'assurer que les données de l'entreprise sont envoyées uniquement via le système de messagerie professionnel. 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 immédiatement en informer les services informatiques de <l'entreprise X>.