

Promethean

ActivPanel[™]
ActivConnect[™] OPS-G
IT-Administratorhandbuch

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Einführung	3
Netzwerkverbindungen	4
Einstellungen	6
Bildschirm spiegeln	9
Sicherheit	13

Einführung

ActivConnect OPS-G ist ein leistungsstarkes Android-Gerät, das mit Ihrem ActivPanel geliefert wird.

Dieser Leitfaden zeigt IT-Administratoren, wie das ActivConnect OPS-G einrichten wird.


In diesem Handbuch wird in Bezug auf das ActivConnect OPS-G Folgendes vorausgesetzt:

- Das Gerät wurde installiert und ist über die entsprechende Halterung am ActivPanel montiert.
- Das Gerät ist eingeschaltet.

Netzwerkverbindungen

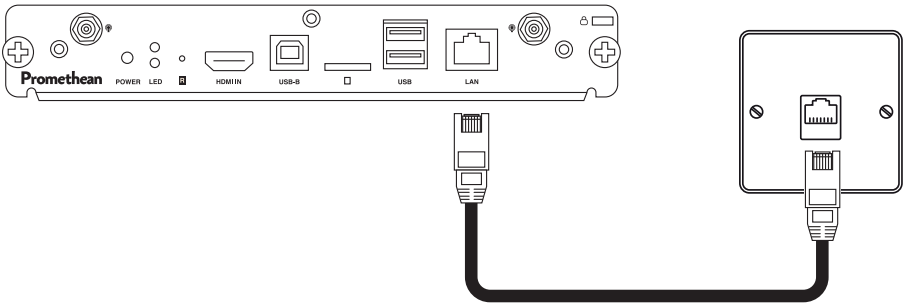
ActivConnect OPS-G bietet Gigabit Ethernet, Dual Band 802.11 b/g/n/ac WLAN (RTL8822)- und Bluetooth® 4.1-Hardware.

Sie können das ActivConnect OPS-G an kabelgebundene (Ethernet) und kabellose (WLAN) Netzwerke anschließen.

 Für eine bessere Leistung nutzen Sie nach Möglichkeit ein kabelgebundenes Netzwerk.



Verbinden mit einem kabelgebundenem Netzwerk

Verbinden Sie das ActivConnect OPS-G über ein Netzwerkkabel mit einem Netzwerkanschluss.




Wenn Ihre Organisation einen DHCP-Server (Dynamic Host Configuration Protocol) nutzt, wird die Verbindung nach dem Anschließen des Kabels automatisch konfiguriert. Wenden Sie sich an Ihre IT-Abteilung, falls kein DHCP-Server genutzt wird.

Verbinden mit einem kabellosen Netzwerk

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **WLAN**.
4. Schalten Sie die WLAN-Funktion ein.
Eine Liste verfügbarer kabelloser Netzwerke wird angezeigt.
5. Wählen Sie das Netzwerk aus, mit dem Sie eine Verbindung herstellen möchten.

Ändern der Netzwerk-Proxy-Einstellungen

Zum Ändern der Proxy-Einstellungen für das Netzwerk benötigen Sie den Hostnamen oder die IP-Adresse des Proxys und eine Proxy-Portnummer. Wenden Sie sich bezüglich Details an Ihre IT-Abteilung.



1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Ethernet-Konfiguration** > **Proxy** > **Manuell**.
4. Geben Sie die relevanten Proxy-Details ein.
5. Wählen Sie **Verbinden**.

Einrichten des WLAN-Hotspots

ActivConnect OPS-G kann ein WLAN mit geringer Reichweite erschaffen. Über diese Funktion lässt sich eine Internetverbindung für in der Nähe befindliche WLAN-Geräte bereitstellen. Es ermöglicht auch die drahtlose Spiegelung von bis zu fünf WLAN-Geräten.



Wenn Sie das ActivConnect OPS-G als WLAN-Hotspot verwenden, muss das ActivConnect OPS-G mit einem kabelgebundenen Netzwerk verbunden sein, um eine Internetverbindung für andere Geräte bereitstellen zu können.

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Mehr > Tethering und mobiler Hotspot > WLAN-Hotspot einrichten**.
4. Der Standardname des Hotspots lautet ACON OPS.
Um den Namen zu ändern, gehen Sie zum vorherigen Menü und wählen Sie **Mehr > Geräte name festlegen**.
5. Ändern Sie, falls erforderlich, die Einstellungen für **Sicherheit**.
6. Geben Sie ein Kennwort ein und wählen Sie **Speichern**.
7. Wählen Sie die **Mobiler WLAN-Hotspot**-Umschalttaste, um den Hotspot einzuschalten.
8. Sie können jetzt WLAN-Geräte in der Nähe mit dem ActivConnect OPS-G-Netzwerk verbinden.

Einstellungen

Sie können das ActivConnect OPS-G über die Einstellungen Ihren Anforderungen anpassen.

Weitere Informationen finden Sie in der Android-Hilfe.



Bluetooth einrichten

Das ActivConnect OPS-G ist mit Bluetooth ausgerüstet. Diese Funktion ermöglicht die Übertragung von Dateien über kurze Entfernungen und die Steuerung von Bluetooth-Geräten in der Nähe.

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Bluetooth**.
4. Wählen Sie die **Bluetooth-Umschaltfläche**, um die Funktion einzuschalten.



Ändern der Sprache

Sie können die Sprache und die Tastatureinstellungen ändern.

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Sprache und Eingabe**.
4. Ändern Sie die entsprechenden Einstellungen.

Ändern von Datum und Uhrzeit

Sie können das eingestellte Datum und die Uhrzeit ändern.



1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Datum und Uhrzeit**.
4. Wählen Sie eine Zeitzone oder deaktivieren Sie die Option **Automatische Zeitzone**, um Datum und Uhrzeit manuell einzustellen.

Ändern der Anzeigeeinstellungen



Das ActivConnect OPS-G erkennt automatisch die optimale Bildschirmauflösung für das ActivPanel.

Sie können die Bildschirmauflösung und -frequenz manuell ändern.

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Display**.
4. Wählen Sie **HDMI-Auflösung**.
5. Wählen Sie eine Auflösung und Bildwiederholfrequenz.

Ändern der Sicherheitseinstellungen

Sie können die Sicherheitseinstellungen wie z. B. die Bildschirmsperre ändern.



1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Sicherheit**.
4. Ändern Sie die entsprechenden Einstellungen.

Benutzer





Sie können, abhängig von den jeweiligen Anforderungen, zwei Arten von Benutzerkonten erstellen:

- **Benutzer**
Jeder Benutzer hat ohne Einschränkungen seine eigenen Apps und Inhalte. Dieser Benutzertyp ist für Mitarbeiter geeignet.
- **Eingeschränktes Profil**
Jeder Benutzer mit eingeschränktem Profil hat seine eigenen Apps und Inhalte. Sie können den Zugriff auf bestimmte Apps und Inhalte abhängig von den Benutzeranforderungen einschränken. Dieser Benutzertyp ist für Studenten geeignet.

Benutzer hinzufügen

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Benutzer**.
4. Wählen Sie **Benutzer oder Profil hinzufügen**.
5. Wählen Sie den Typ des Benutzers, den Sie erstellen möchten.
6. Um die Einstellungen für das neue Benutzerprofil zu bearbeiten, melden Sie sich als dieser Benutzer an.

Entfernen von Benutzern

1. Wählen Sie  > .
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Benutzer**.
4. Wählen Sie den Typ des zu entfernenden Benutzers.
 - Um einen eingeschränkten Benutzer zu entfernen, wählen Sie  und dann **Benutzer entfernen**.
 - Um einen Benutzer ohne Einschränkungen zu entfernen, wählen Sie  neben dessen Namen.

Aktualisieren der Software



Aktualisieren Sie die Software des ActivConnect OPS-G, um Sicherheitspatches und -funktionen auf dem neuesten Stand zu halten.

Promethean gibt die Verfügbarkeit neuer Updates bekannt. Wir empfehlen Ihnen außerdem, jeden Monat manuell nach Updates zu suchen.



Um sicherzustellen, dass Sie alle wichtigen Updates herunterladen und auf dem Gerät installieren, nehmen Sie die folgenden URLs in die Liste erlaubter Verbindungen (White List) auf:

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

1. Wählen Sie  > .
2. Wählen Sie **Aktualisierung**.
3. Wählen Sie **Online-Aktualisierung**.
Wenn ein neue Version verfügbar ist, wird sie vom System heruntergeladen.
4. Akzeptieren Sie nach Abschluss des Downloads das Update.
Das Gerät installiert das Update und startet anschließend neu.

Hinweis: Unterbrechen Sie das Softwareupdate nicht. Wenn das Softwareupdate unterbrochen wird, kann dies die Software beeinträchtigen.

Bildschirm spiegeln

Über die Bildschirmspiegelungsfunktion können Sie Inhalte von anderen Geräten auf dem ActivConnect OPS-G-Bildschirm anzeigen.

Das ActivConnect OPS-G ist mit Geräten mit folgenden Betriebssystemen kompatibel:

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



Weitere Informationen finden Sie unter: <https://support.prometheanworld.com/article/?kb=1532>.

Über die ActivCast-App



Um die Bildschirmspiegelung mit Windows-, Android- und Chrome OS-Geräten nutzen zu können, müssen Sie die ActivCast-App verwenden. Die ActivCast-App ist auf dem ActivConnect OPS-G vorinstalliert. iOS-Geräte können ihre Bildschirme ohne die ActivCast-App spiegeln, wir empfehlen jedoch, die App zu installieren.


Sie können die ActivCast-App über den folgenden Link herunterladen:

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

Umbenennen des Geräts

Um die Bildschirmspiegelung zu vereinfachen, können Sie Ihrem ActivConnect OPS-G einen Namen geben.

Wir empfehlen, für jedes Gerät einen anderen Namen zu verwenden, z. B. „ActivPanel 1“ oder „ActivPanel Klassenraum 1“.

1. Wählen Sie **ActivCast**.
2. Wählen Sie .
3. Wählen Sie **Einstellungen**.
4. Wählen Sie **Gerätename**.
5. Geben Sie den Gerätenamen ein.



Um die Sicherheit zu erhöhen, können Sie einen PIN-Code festlegen, der auf einem Gerät eingegeben werden muss, bevor die Bildschirmspiegelung verwendet werden kann.

Netzwerkanforderungen für die Bildschirmspiegelung

Der Bildschirm wird gespiegelt, indem ein H.264-codierter und AES 128-Bit-verschlüsselter Videostream über eine TCP-Verbindung übertragen wird. Dieser Stream wird mithilfe eines 128-Byte-Headers in Pakete unterteilt. AAC-ELD-Audio wird über das Airplay®-Protokoll gesendet. Die Hauptuhr wird mit NTP synchronisiert.

Die empfangenden und sendenden Geräte müssen mit demselben kabelgebundenen oder kabellosen Netzwerk verbunden sein.

Stellen Sie sicher, dass die Firewall Ihres Netzwerks ordnungsgemäß eingerichtet ist, um Bildschirm Spiegelung verwenden zu können. Die folgenden Anschlüsse müssen offen sein und zugelassen werden:

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

HTTP-Anforderungen

Die Bildschirm Spiegelung verwendet den hartcodierten Port 7100. Es handelt sich um einen HTTP-Server, der die folgenden Anforderungen unterstützt:

- POST / Stream
- Streampakete
- Codec-Daten
- Zeitsynchronisation
- Kennwortschutz

POST / Stream

Startet die Live-Videoübertragung. Der Client sendet eine binäre Eigenschaftsliste mit den Metadaten des Streams, dem direkt der eigentliche Stream folgt. Zu diesem Zeitpunkt ist die Verbindung keine gültige HTTP-Verbindung mehr.

Sobald der Server eine Stream-Anforderung erhält, sendet er die NTP-Anforderungen an den Client an Port 7010, der ebenfalls festcodiert ist. Der Client muss seine Masteruhrzeit exportieren. Die Masteruhrzeit wird für die Audio-/Videosynchronisation und Uhrwiederherstellung verwendet.

Streampakete

Der Videostream wird mithilfe von 128-Byte-Headern verpackt, gefolgt von einer optionalen Nutzlast.

Codec-Daten

Dieses Paket enthält die zusätzlichen H.264-Daten im AVCC-Format (ISO/IEC 14496:15). Es wird gesendet:

- Am Anfang des Streams
- Bei jeder möglichen Änderung der Videoeigenschaften
- Bei Änderung der Bildschirmausrichtung
- Bei Ein- oder Ausschalten des Bildschirms

Zeitsynchronisation

Anforderungen werden an den Airplay-Client in 3-Sekunden-Intervallen gesendet. Das Referenzdatum für die Zeitstempel ist der Beginn der Spiegelungssitzung.

Kennwortschutz

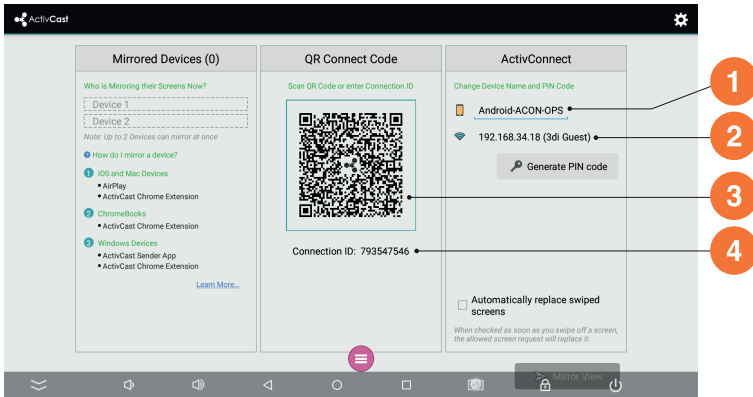
Ein Airplay-Server kann ein Passwort zum Anzeigen von Inhalten im Netzwerk anfordern. Dieses wird mithilfe der standardmäßigen HTTP Digest Authentication (RFC 2617) implementiert. Der Passwortschutz wird durch ActivCast automatisch implementiert.

Identifizieren des ActivCast-Empfängers

Bevor Sie die Bildschirmspiegelung starten können, muss das sendende Gerät das empfangende Gerät identifizieren.

Optionen zum Identifizieren des ActivCast-Empfängers

Es gibt vier Möglichkeiten, den ActivCast-Empfänger zu identifizieren. Diese Informationen werden auf dem Hauptbildschirm der ActivCast-App auf dem empfangenden Gerät angezeigt.



- 1 Name**
Der Name des Empfängers wird gesendet. Sie können dann mit der ActivCast-App eine Verbindung zum Empfänger herstellen.
- 2 IP-Adresse**
Erstellt eine direkte Verbindung ohne einen Cloud-Server.
- 3 QR-Code**
Wenn Sie die ActivCast-App mit einem Mobilgerät nutzen, können Sie den auf dem ActiveCast-Bildschirm zum Spiegelungsstatus angezeigten QR-Code scannen.
- 4 Verbindungs-ID**
Der Empfänger hat eine eindeutige ID. Erstellt eine direkte Verbindung ohne einen Cloud-Server.

Tipps für die Bildschirmspiegelung

Die Bildschirmspiegelung kann durch externe Bedingungen wie Bandbreite, Netzwerkabdeckung und Sicherheitseinstellungen beeinflusst werden. Lesen Sie die folgenden Tipps, um die besten Ergebnisse bei der Bildschirmfreigabe zu erzielen.

Funktion	Tipps
Ethernet	Verbinden Sie Ihr Empfangsgerät über ein Netzkabel mit dem Netzwerk. Ethernet ist der zuverlässigste Verbindungstyp.
WLAN	Prüfen Sie auf kabellose Netzwerkstörungen. Stellen Sie sicher, dass das sendende Gerät den schnellsten 802.11-Modus verwendet, den es bewältigen kann. Wechseln Sie in den 5-GHz-Modus. Konfigurieren Sie den Router für optimale Airplay-Nutzung.
Bildschirmauflösung des sendenden Geräts	Das Spiegeln von Bildschirmen mit hoher Auflösung verringert die Leistung. Verringern Sie die Auflösung des sendenden Geräts, bis Sie eine akzeptable Leistung erreichen.
Bluetooth	Deaktivieren Sie Bluetooth während der Bildschirmspiegelung. Bluetooth und WLAN 802.11 können sich gegenseitig stören.

Um unbefugten Zugriff oder die Ausnutzung der Ressourcen Ihrer Organisation zu verhindern, sollten alle Benutzer von ActivConnect OPS-G die in den Sicherheitsrichtlinien beschriebenen Schritte ausführen.

IT-Administratoren sind zudem für die Aufrechterhaltung der Gerätesicherheit und die Einhaltung der Sicherheitsvorschriften der Organisation verantwortlich.

Sicherheitsrichtlinie

1. Alle Benutzer- und Administrator-Passcodes müssen den Richtlinien Ihrer Organisation entsprechen. Passcodes sollten relativ lang sein und eine Kombination aus Großbuchstaben, Kleinbuchstaben, numerischen Zeichen und Interpunktionszeichen enthalten.
2. Ändern Sie die Administrator-Passcodes alle 3 Monate oder gemäß den Richtlinien Ihrer Organisation.
3. Ändern Sie die Benutzer-Passcodes alle 30 Tage oder gemäß den Richtlinien Ihrer Organisation.
4. Wir empfehlen, die Funktion zur Sichtbarkeit des Kennworts auszuschalten.
5. Verwenden Sie nicht denselben Passcode mehr als einmal.
6. Teilen Sie Ihren Passcode nicht mit anderen Personen, einschließlich Ihrem Vorgesetzten oder Familienmitgliedern.
7. Senden Sie keine Passcodes per E-Mail.
8. Geben Sie in Fragebögen und Sicherheitsformularen keine Passcodes preis.
9. Geben Sie keinen Hinweis auf das Format eines Passcodes (zum Beispiel „mein Familienname“).
10. Notieren Sie die Passcodes nicht.
11. Speichern Sie keine Passcodes auf unverschlüsselten Geräten.
12. Jeder Benutzer, der den Verdacht hat, dass sein Passcode kompromittiert wurde, muss dies dem IT-Administrator melden und sofort alle Kennwörter ändern.
13. Schützen Sie das Gerät mit Antivirensoftware.
14. Um vertrauliche Daten zu schützen, die auf dem Gerät gespeichert sind, empfehlen wir die Nutzung der Geräteverschlüsselung.
15. Installieren Sie keine Apps aus unbekanntem Quellen.
16. Wir empfehlen, Benachrichtigungen zu deaktivieren, wenn das Gerät gesperrt ist.
17. Wenn das Gerät kompromittiert ist, ist der IT-Administrator dafür verantwortlich, alle erforderlichen Maßnahmen zu ergreifen.

Benutzeranforderungen

1. Benutzer dürfen nur Daten laden, die relevant und für Ihre Rolle entscheidend sind.
2. Benutzer müssen alle Hardware- und Softwarefehler dem IT-Administrator melden.
3. Wenn ein Benutzer vermutet, dass über das Gerät ein unbefugter Zugriff auf Daten erfolgt ist, muss er dies gemäß den Richtlinien der Organisation melden.
4. Installieren Sie keine Software, die nicht für Benutzer bestimmt ist.
5. Benutzer dürfen keine raubkopierte Software oder illegale Inhalte auf das Gerät herunterladen.
6. Anwendungen dürfen nur aus Quellen installiert werden, die von Android zugelassen wurden.
7. Das Gerät muss über Softwareaktualisierungen des Herstellers auf dem neuesten Stand gehalten werden. Überprüfen Sie monatlich, ob Software-Updates verfügbar sind.

8. Das Gerät darf nicht mit Geräten verbunden werden, die nicht über einen aktuellen und aktivierten Virenschutz verfügen. Das verbundene Gerät muss ebenfalls den Richtlinien der Organisation entsprechen.
9. Externe Geräte müssen entsprechend den Richtlinien der Organisation verschlüsselt sein.
10. Benutzer müssen bei der Nutzung persönlicher E-Mail-Konten auf dem Gerät vorsichtig sein. Insbesondere müssen Sie darauf achten, dass Daten der Organisation ausschließlich über das organisationseigene E-Mail-System versendet werden. Wenn ein Benutzer vermutet, dass Unternehmensdaten über ein privates E-Mail-Konto gesendet wurden, sei es im Textkörper oder als Anhang, muss er umgehend den IT-Administrator benachrichtigen.

TP-2094-DE-V02 ©2018 Promethean Limited. Alle Rechte vorbehalten. Die Verfügbarkeit der Produkte kann je nach Land abweichen. Technische Daten können jederzeit ohne Vorankündigung geändert werden.