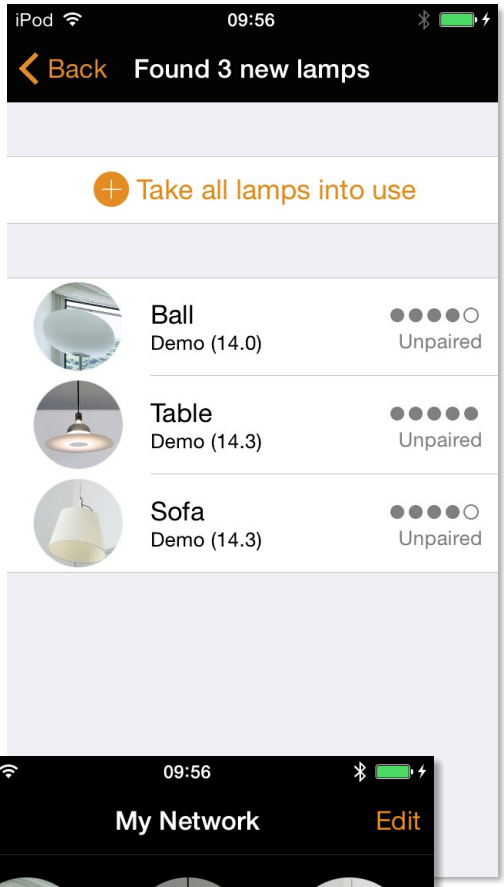
Casambi App
Kurzanleitung

Version 1.2.2 GER
26.2.2016

CASAMBI

www.casambi.com · support@casambi.com

Erstmalige Anwendung



Die Casambi App ist leicht in Betrieb zunehmen. Folgen Sie einfach diesen Schritten:

Casambi App aus Apple App Store oder Google Play downloaden

Casambi betriebene Leuchten einschalten.

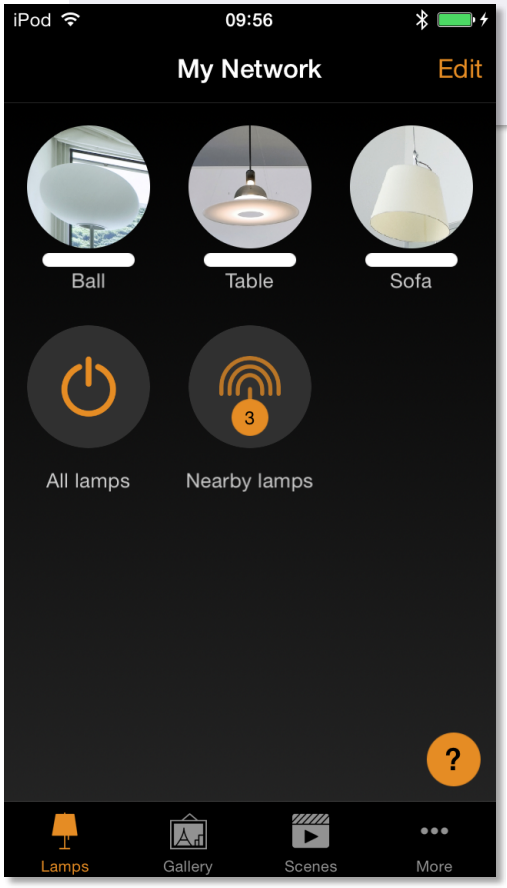
Die App öffnen.

Die Casambi App findet automatisch alle Casambi betriebenen Leuchten, die eingeschaltet sind.

Auf ‚Alle Leuchten in Benutzung nehmen' klicken.

Die Casambi App fügt automatisch alle Leuchten zu einem Netzwerk zusammen und öffnet ‚Leuchten'.

Standard Gesten zur Steuerung der App



Mit den folgenden Gesten können Sie Ihre Beleuchtung steuern

- Leuchten Symbol antippen, um die Leuchte an oder auszuschalten.
- Horizontal über das Leuchten Symbol streifen, um die Helligkeit der Leuchte anzupassen.
- Vertikal über das Leuchten Symbol streifen, um die Farbtemperatur der Leuchte anzupassen.
- Leuchten Symbol gedrückt halten, um die Lichtfarbe auszuwählen und auf der Farbenpalette zu speichern.

Linnoitustie 4 A,
02600 Espoo, Finland

www.casambi.com
support@casambi.com

Galerie

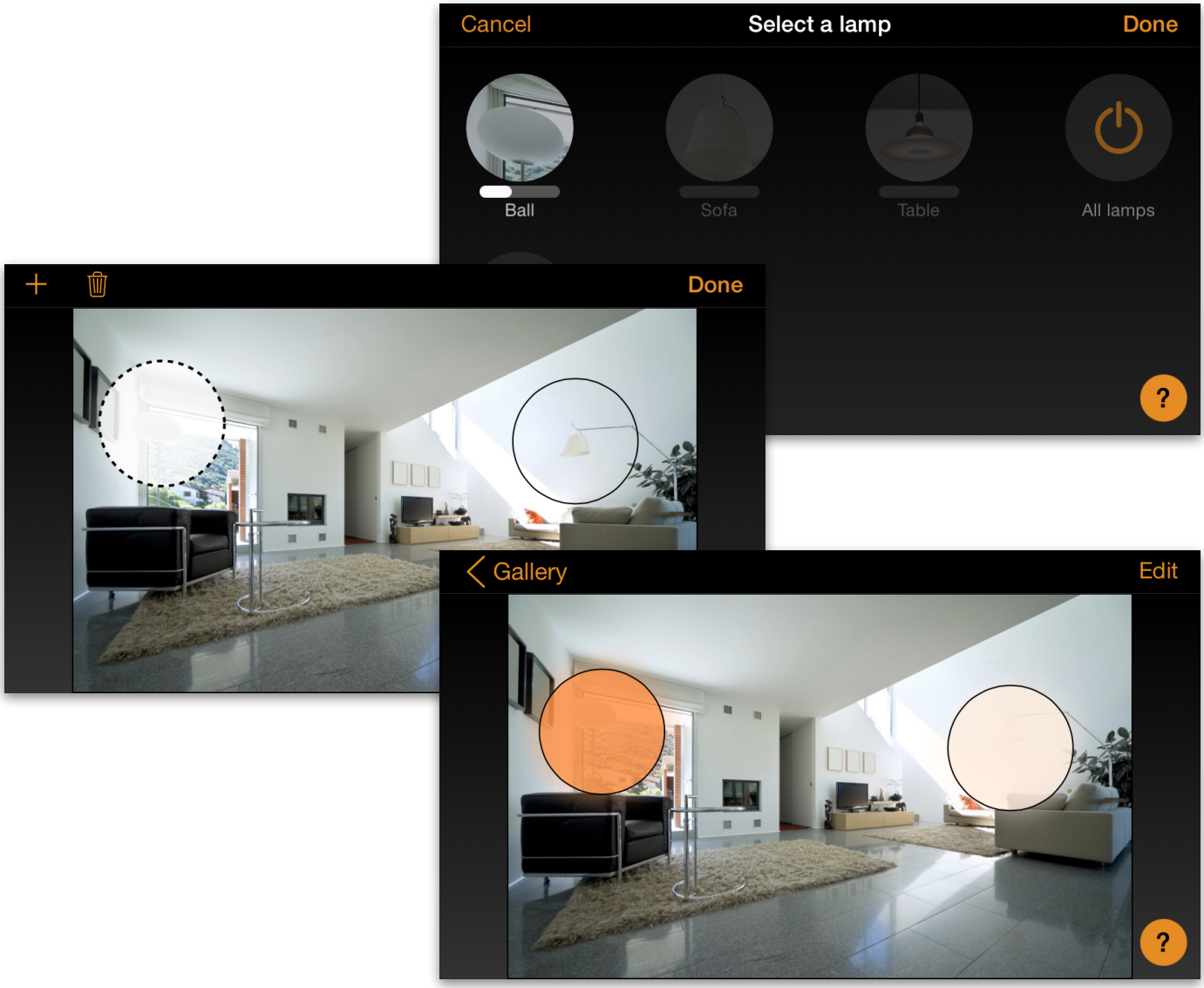
Die Galerie der Casambi App ist die intuitivste Weise Ihre Leuchten zu steuern. Machen Sie ein Foto Ihrer Wohnung, mit Ihren Leuchten im Bild, und platzieren Sie die Lichtsteuerung direkt auf den Leuchten im Bild.

1. Fügen Sie ein Foto in die Galerie ein, in dem Sie auf ‚Bearbeiten' und dann das '+' Symbol anklicken.

2. Nachdem Sie das Foto eingefügt haben, können Sie die Steuerungen im Bild platzieren. Klicken Sie auf das '+' Symbol und wählen Sie die Leuchte aus, welche Sie dem Bild hinzufügen möchten. Bestätigen Sie mit ‚Fertig'.

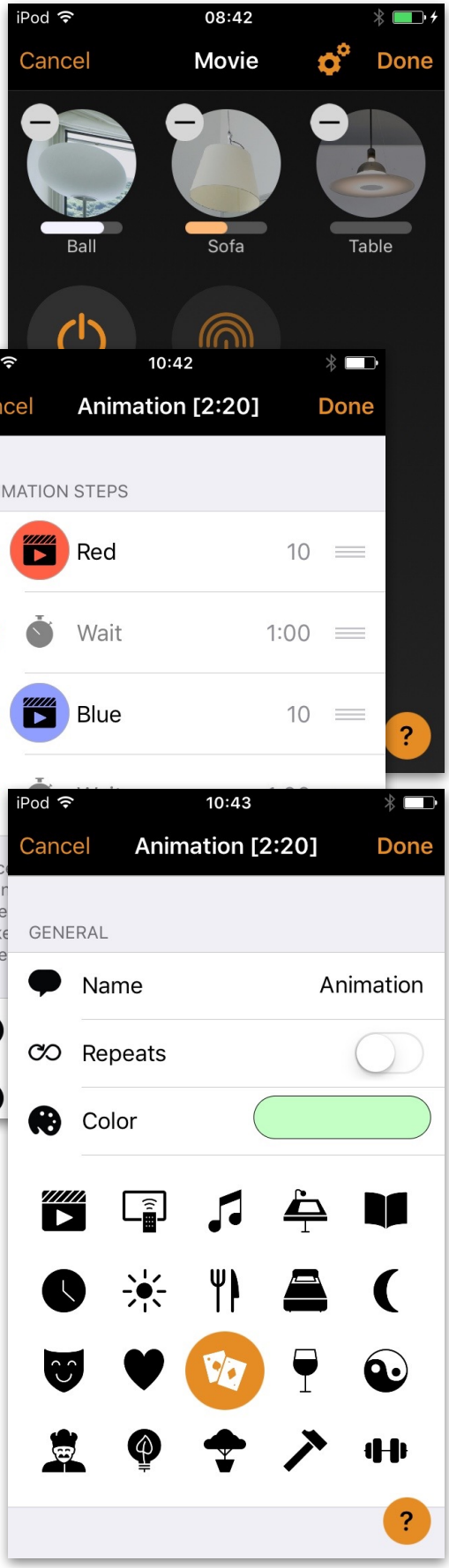
3. Wenn Sie alle Leuchten mit Steuerungen markiert haben, klicken Sie auf ‚Fertig'.

4. Sie können jetzt Ihre Leuchten direkt vom Foto steuern. Kein Verwechseln der Leuchten mehr möglich.



Linnoitustie 4 A,
02600 Espoo, Finland
www.casambi.com
support@casambi.com

Szenen und Animationen



Unter 'Szenen' können Sie Lichtszenen, passend für jeden Anlass erstellen. Es ist möglich mit einem Klick mehrere Leuchten zu steuern, um ein perfektes Ambiente zu schaffen. Eine Leicht kann in mehreren Szenen verwendet werden.

1. Auf ‚Szene hinzufügen' klicken und einen Namen für die Szene eingeben. Nun ‚Szene hinzufügen' wählen.

2. Eine oder mehrere Leuchten auswählen und für die Szene anpassen. Sie können jede Leuchte einzeln anpassen oder falls Sie für alle, die selbe Helligkeit, Farbtemperatur oder Farbe möchten, können Sie das ‚Leuchten der Szene' Symbol verwenden und alle Leuchten gemeinsam anpassen.

3. Wenn Sie die Szene fertig angepasst haben, klicken Sie auf ‚< Zurück' und bestätigen Sie mit ‚Fertig'.

4. Um weitere Szenen zu erstellen klicken Sie unter Szenen auf ‚Bearbeiten' und dann auf das '+' Symbol.

Unter ‚Szenen' ist es auch möglich Animationen zu erstellen. Animationen sind spezielle Szenen, welche von Szene zu Szene faden können. Sie können wie normale Szenen genutzt werden. Animationen können als Endlosschleife konfiguriert werden.

1. Auf ‚Bearbeiten' in der oberen rechten Ecke klicken und dann das '+' Symbol wählen.

2. Auf ‚Animation hinzufügen' klicken.

3. Ablauf der Animation erstellen. Es können Szenen und Wartezeiten zur Animation hinzugefügt werden. Zum Beispiel: Szene Rot, Wartezeit, Szene Blau und nochmals Wartezeit hinzufügen. Stellen Sie die Fadezeit der Szenen auf 10 Sekunden und die Wartezeit auf 1 Minute. Diese Animation wird in 10 Sekunden in die Szene Rot faden und diese wird 1 Minute aktiv sein. Dann wird die Szene Rot in 10 Sekunden in die Szene Blau faden, welche für 1 Minute aktive bleibt.

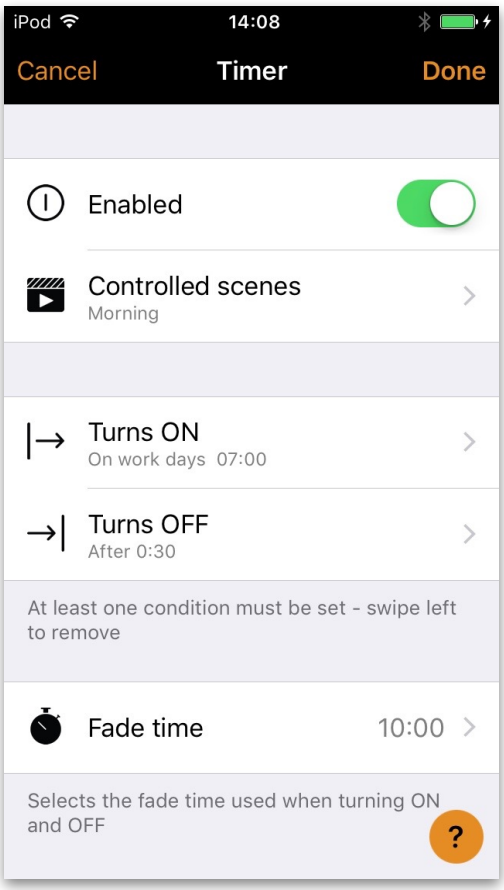
4. In den allgemeinen Einstellungen kann die Animation als Endlosschleife konfiguriert werden.

5. Mit ‚Fertig' die Einstellungen bestätigen

Linnoitustie 4 A,
02600 Espoo, Finland

www.casambi.com
support@casambi.com

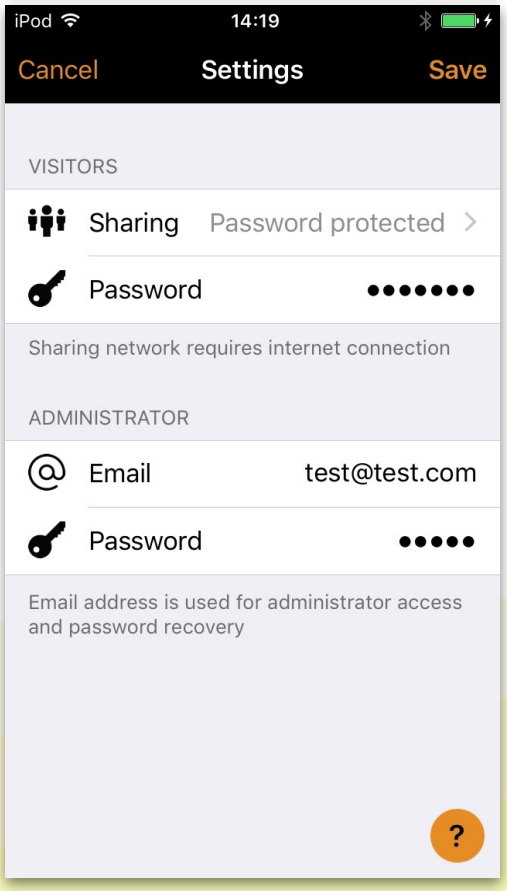
Timer



Mit dem Timerfunktion können Sie eine Liste an Timern erstellen, welche zeitbasiert Szenen und Animationen an und ausschalten können.

1. Unter Mehr Timer auswählen. Auf ‚Timer hinzufügen' klicken, um einen neuen Timer zu erstellen.'
2. Auf ‚Ausgewählte Szene' klicken und eine Szene auswählen, welche vom Timer gesteuert werden soll.
3. Auf ‚Schaltet EIN' klicken um die Zeit anzugeben, wann die Szenen eingeschaltet werden soll. Auf ‚Schaltet AUS' klicken un die Zeit anzugeben, wann die Szene ausgeschaltet werden soll.
4. Für den Timer kann eine Fadezeit bestimmt werden, sodass die Szene weicher startet.
5. Mit ‚Fertig' die Einstellungen bestätigen.

Netzwerke und Freigabe



Wenn Sie Ihre Leuchten von mehreren Smartphones und Tablets aus bedienen möchten, können Sie unter Netzwerk-konfigurierung die Freigabeoption ändern. Die Standard-einstellung eines Netzwerks ist nicht teilen ‚somit ist das Netzwerk nur auf dem einrichtenden Gerät gespeichert.

1. Unter ‚Mehr' ‚Netzwerkkonfigurierung' wählen und auf ‚Freigabeoptionen' klicken.
2. Durch klicken auf Freigabe öffnet sich die Freigabeoptionen.
3. Es gibt vier verschiedene Freigabeoptionen: Nicht teilen, Nur Administrator, Passwort geschützt und Offen. Wenn die Option Nur Administrator, Passwort geschützt oder Offen gewählt werden, wird das Netzwerk in die Cloud hochgeladen, um weiteren mobilen Geräten zugriff zu gewähren.
4. Emailadresse und Passwort für das Netzwerk einfügen
5. Einstellungen mit ‚Sichern' bestätigen.

Linnoitustie 4 A,
02600 Espoo, Finland

www.casambi.com
support@casambi.com

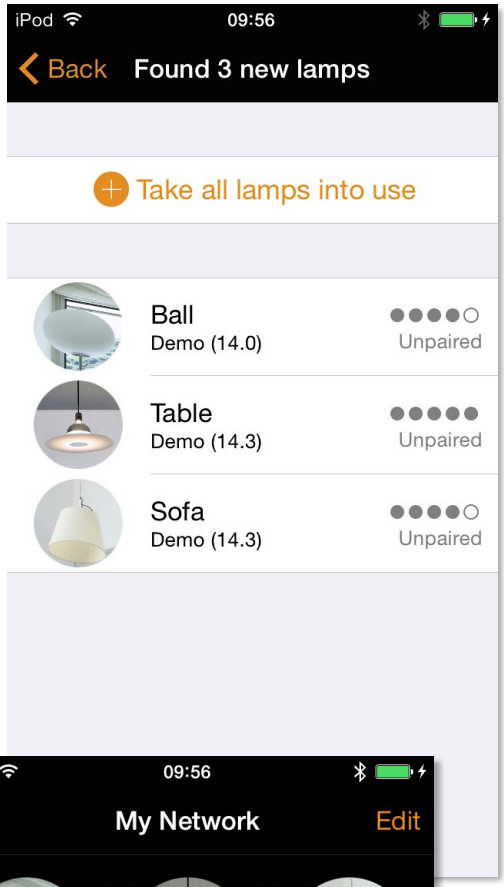
Casambi App
Short User Guide

Version 1.2.2
29.12.2015

CASAMBI

www.casambi.com · support@casambi.com

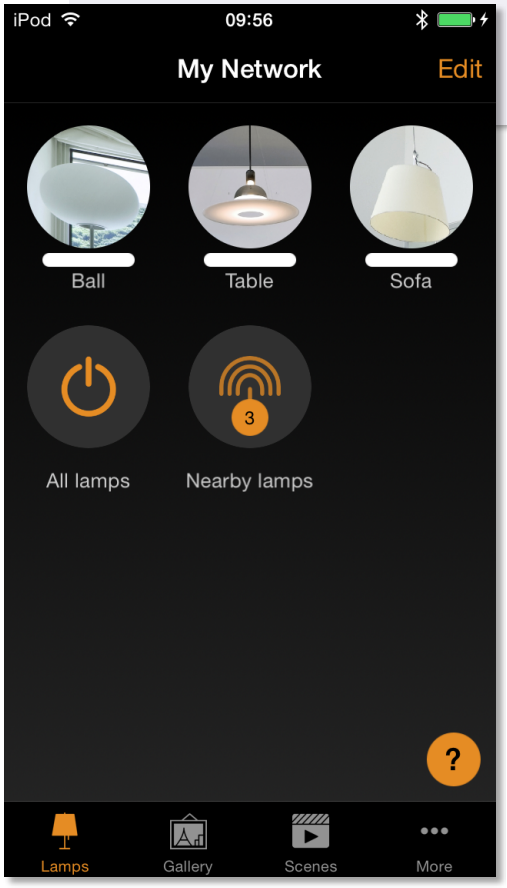
First time use



Casambi app is easy to use. Follow these simple steps.

1. Download the app from Apple App Store or Google Play Store.
2. Turn on your Casambi enabled luminaires.
3. Open the app.
4. Casambi app will automatically find all Casambi enabled luminaires that are switched on.
5. Tap on the 'Take all lamps into use'
6. Casambi app will automatically add all luminaires to one network and open the 'Lamps' tab

Basic gestures



Here are the basic gestures how to control your lights.

- To turn off or on your luminaire just tap on the lamp control.
- Pan lamp control left or right to adjust light level of the luminaire.
- Pan lamp control up or down to adjust the colour temperature of the luminaire.
- Hold on top of the lamp control to change the colour and save colours to palette.

Linnoitustie 4 A,
02600 Espoo, Finland
www.casambi.com
support@casambi.com

Gallery

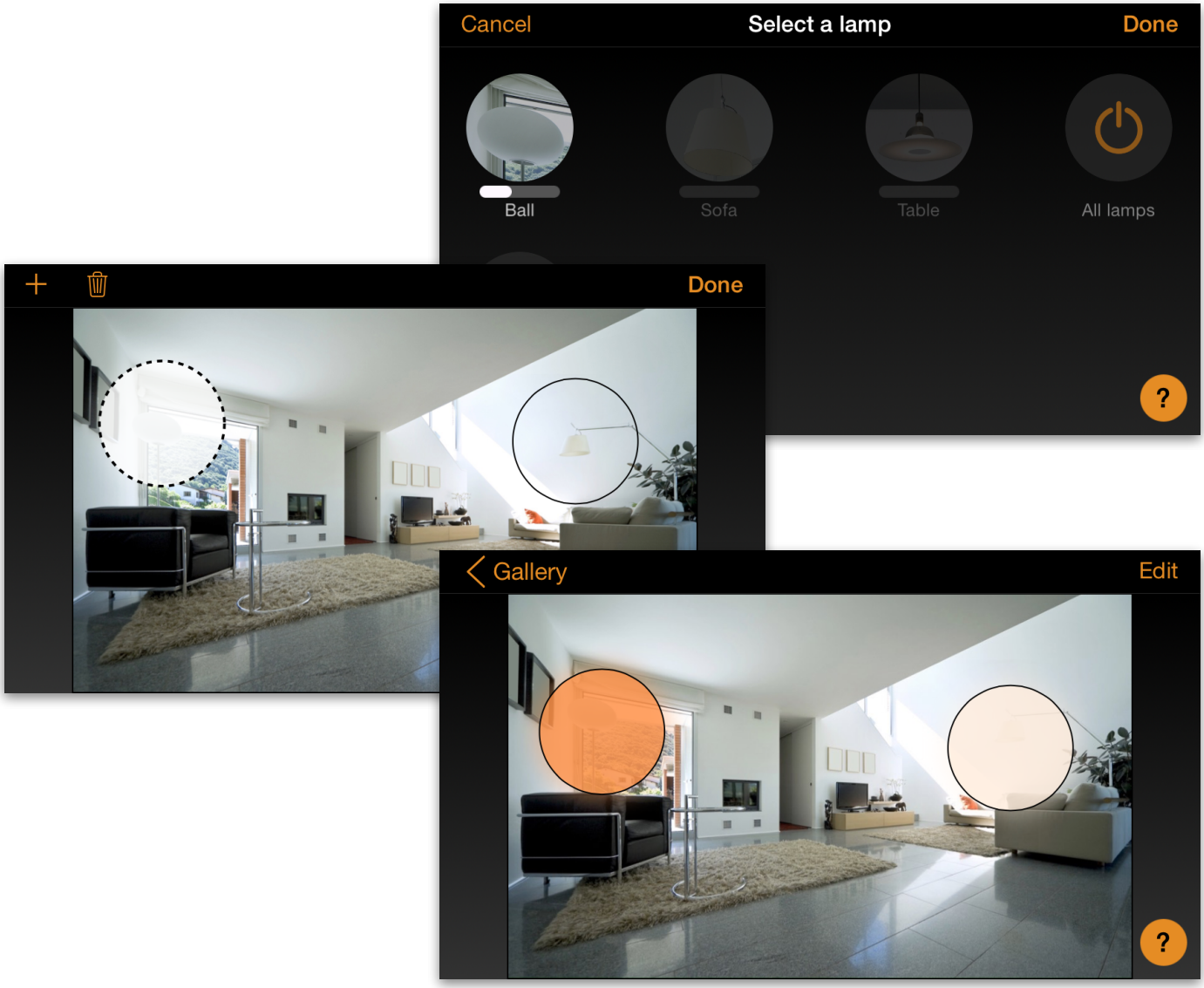
The Gallery in Casambi app is the most natural way of controlling your luminaires. Take a picture of the room where your luminaires are, and place lamp controls over them in the picture. You can also take a panorama picture to have more luminaires in one photo.

1. Add a photo of your room to Casambi Gallery by tapping 'Edit' and after that the '+' sign.

2. After you have added a photo you can add lamp controls to the picture. Tap on the '+' sign, select a lamp control that you want to add to the picture and tap 'Done'.

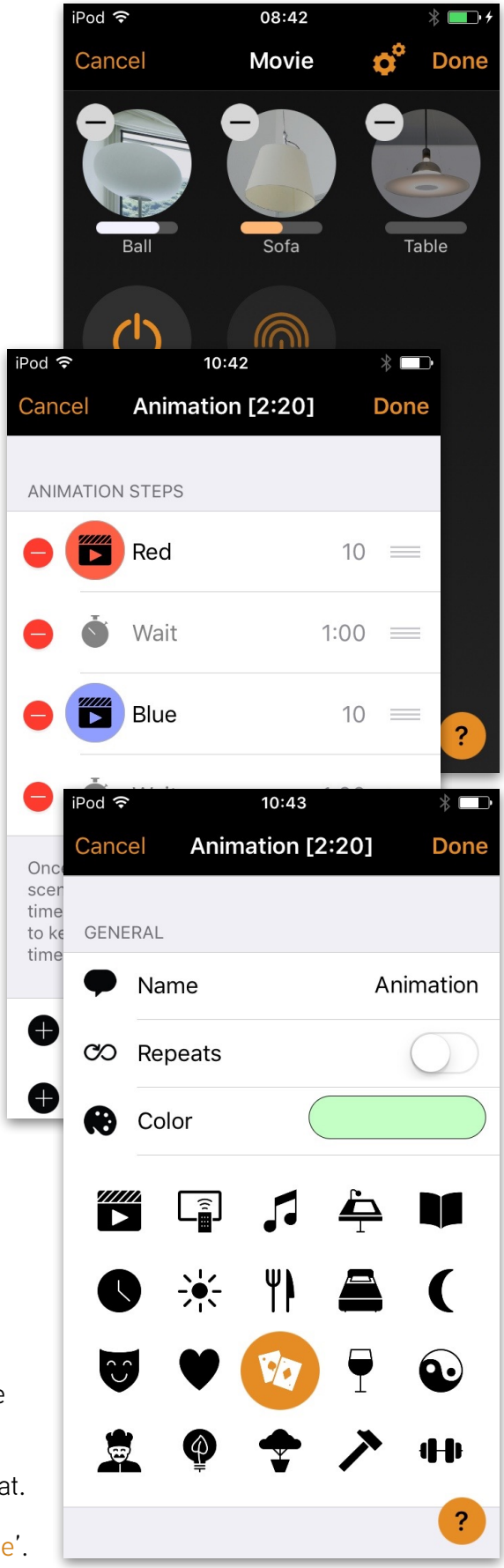
3. After you have added controls over all the luminaires in the picture tap 'Done'.

4. Now you can control your luminaires visually from the picture. No need to guess which luminaire is which.



Linnoitustie 4 A,
02600 Espoo, Finland
www.casambi.com
support@casambi.com

Scenes and animations



In the 'Scenes' tab you can create different lightings for different occasions. It is possible to control multiple luminaires with one tap to create perfect ambience. One luminaire can be used in several scenes.

1. Tap on 'Add a scene' and enter a name for the scene. Select the 'Add a scene' option
2. Select one or multiple lamp controls and adjust the luminaires for the scene. You can adjust the luminaires separately or if you want to have same dim level or colour for all you can use the 'Lamps in scene' control to adjust all luminaires in the scene.
3. When you are done editing the scene tap on 'Done'.
4. If you would like to create more scenes tap on the 'Edit' on top right corner and then tap on the '+' sign.

In the 'Scenes' tab it is also possible to create animations. Animations or dynamic scenes are special scene type that fade from scene to scene. They can be used like ordinary scenes. Animations can also repeat.

1. Tap on the 'Edit' on top right corner and then tap on the '+' sign.
2. Tap on the 'Add an animation' option
3. Add animation steps. You can add scenes and wait times to animation. Example:

   - Add Scene Red, fade time 10 sec
   - Add wait 1 min
   - Add Scene Blue, fade time 10 sec

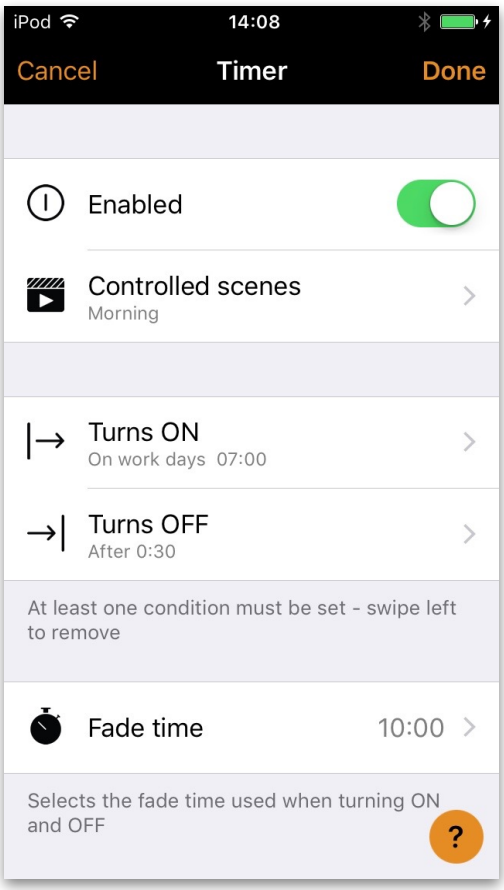
   This animation setting will fade in to scene Red in 10 seconds and Red will be active for 1 minute. Then the scene Red will fade into scene Blue in 10 seconds.
4. In General settings you can set the animation to repeat.
5. When you are done editing the animation tap on 'Done'.

Linnoitustie 4 A,
02600 Espoo, Finland
www.casambi.com
support@casambi.com

Timer

With schedule/timer function you can create a list of timers that will turn scenes or animations on and off based on time.

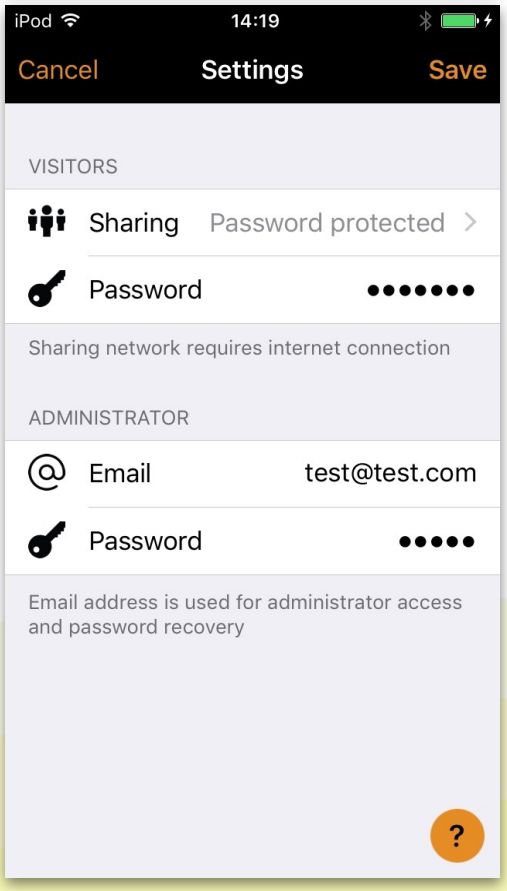
1. Go to More tab and select Schedule. Create a new timer by tapping the 'Add a timer'
2. Tap on the 'Controlled scenes' and select a scene or animation that this timer will control
3. Tap on the 'Turns ON' button to set the time when the scene should turn on and tap on the 'Turns OFF' button to set the time when the scene should turn off.
4. It is also possible to set a fade time for the timer so that the scene will come on smoothly.
5. When you are done editing the timer tap on 'Done'.



Networks and Sharing

If you want to control your luminaires from more than one mobile device you need to change the network sharing settings. As a default the created network is not shared and only stored in the device that created it.

1. Go to 'More' tab and select 'Network setup' and 'Sharing settings'.
2. Tap on the Sharing and the 'Sharing mode' screen will open.
3. There are four different sharing modes: Not Shared, Administrator only, Password protected and Open. When you select Administrator only, Password protected or Open mode the network will be uploaded to cloud server and then it can be accessed also from other mobile devices.
4. Add also email address and password for the network.
5. Confirm your settings with 'Save'.



Linnoitustie 4 A,
02600 Espoo, Finland
www.casambi.com
support@casambi.com

10 Punkte zur Sicherheit von Casambi

1. WiFi ist ein Problem
Wenn für den Standardbetrieb einer Lichtsteuerlösung WiFi benötigt wird, ist die Architektur der Lichtsteuerlösung grundsätzlich falsch ausgelegt.
Neben Problemen bei Leistung, Kosten, Stromverbrauch und Bedienerfreundlichkeit macht WiFi äußerst verwundbar für Cyber-Attacken und setzt so die Sicherheit des Systems aufs Spiel.
Casambi nutzt eine verbrauchsarme Bluetooth-Verbindung und ein maßgeschneiderteres „Mesh-Netzwerk“ für den Standardbetrieb – eine WiFi-Verbindung ist nicht nötig.

2. Das Casambi-Netzwerk
Das Casambi-Netzwerk (Kommunikation zwischen mobilen Endgeräten und Casambi-Einheiten sowie Casambi-Einheiten und der Cloud und dem Server) ist ein eigenständiges geschlossenes Netzwerk. Es besteht kein Zugang zu lokalen Gebäudenetzwerken.

3. Die Casambi-Cloud
Log-In und Passwort sind erforderlich für einen Zugriffstoken zum lokalen Bluetooth-Netzwerk.
Die Passwörter werden mit klassischer symmetrischer Verschlüsselung gespeichert. Mit einem Zugriffstoken hat man nur Zugang zu einem lokalen Netzwerk.

4. Server
Casambi nutzt Linux-Server, die mit bewährter Branchenpraxis geschützt sind. Sämtliche Kommunikation läuft über HTTPS*.
Die Server verfügen über eine Firewall und werden rund um die Uhr überwacht. Aktualisiert werden sie mit Sicherheits-Updates, der Zugang ist auf gewisse Mitarbeiter begrenzt und die gespeicherte Information ist verschlüsselt.

5. Kommunikation zwischen mobilen Endgeräten und einer Casambi-Einheit
Jede Anfrage wird mit einer eindeutigen Authentifizierung quittiert, um sicherzustellen, dass der Nutzer auch zur Durchführung der Operation berechtigt ist, d.h. hier zur Änderung der Konfiguration oder Steuerung der Leuchten. Firmware-Aktualisierungen werden mit Authentifizierung quittiert, die Einheiten akzeptieren nur Firmware, die original von Casambi stammt.

6. Kommunikation zwischen zwei Casambi-Einheiten
Sämtliche Kommunikation zwischen zwei Casambi-Einheiten wird mit 128-bit AES verschlüsselt und quittiert. Jede Einheit führt eine Authentifizierung mit allen Nachbar-Einheiten durch. Jedes Paket enthält einen Rollencode, der gegen Replay-Angriffe schützt (hören und erneut senden).

7. Gateway-Kommunikation
Der Gateway-Zugang erfolgt über die Casambi-Cloud. Sämtliche Kommunikation über HTTPS*.

8. Geteilte Einstellungen
Vergessen Sie nicht, Ihre Einstellungen zum Teilen des Netzwerkes auf ein geeignetes Level zu setzen. Behandeln Sie bitte das Administratorengerät und die Passwörter als vertraulich.

- **Nicht geteilt:** Das Netzwerk ist nur auf dem Gerät gespeichert, auf dem es auch eingerichtet wurde. Andere Geräte haben keinen Zugang zum Netzwerk.
- **Nur Administrator:** Das Netzwerk wird nur mit einem Administrator-E-mail und Passwort lokalisiert und erreicht (das bei Einrichtung des Netzwerks gewählt wird).
- **Passwort-geschützt:** Andere Geräte haben über ein Besucher-Passwort Zugang zum Netzwerk. Änderungen erfordern ein Administratoren-Passwort.
- **Offen:** Andere Geräte haben ohne Passwort Zugang zum Netzwerk. Änderungen erfordern ein Administratoren-Passwort.

9. „Worst-Case” Szenario mit Casambi
Sollte ein Casambi-Netzwerk wider Erwarten gehackt werden, kann ein Hacker nach dem Eindringen lediglich das Licht steuern.

10. Intelligent und vernetzt
Die ideale Netzwerk-Architektur umfasst intelligente Geräte, die eigene Intelligenz besitzen und deshalb nur wenn nötig angeschlossen werden – und nicht erst durch die Verbindung intelligent werden. **Casambi ist nämlich tatsächlich intelligent & vernetzt.**

*HTTPS steht für Hyper Text Transport Protocol Secure und ist ein bewährtes End-to-End Kommunikationsverfahren. HTTPS halt Hacker vom Ausspähen der Passwörter und Hacken der Nutzerkonten ab.
Z.B. wird HTTPS gewöhnlich von Banken und anderen Webseiten mit Geldverkehr eingesetzt.

CASAMBI

10 Points on Casambi Security

1. WiFi is a Problem
If WiFi is needed for the normal operation of a lighting control solution, there is something fundamentally wrong with that lighting control solution's architecture. Besides bringing problems in performance, cost, power consumption and user experience, WiFi adds a high vulnerability for cyber attacks and puts the system's security at risk. Casambi uses Bluetooth Low Energy and a tailored mesh network for normal operation, no WiFi connection is needed.

2. The Casambi Network
The Casambi network (communication from mobile devices to Casambi units and Casambi units to the cloud and server) is an own, closed network. Local building networks cannot be accessed.

3. The Casambi Cloud
Log In and Password are needed that allows an access token to a local "Bluetooth network". Passwords are stored using one-way hash algorithms. With an access token only a local network can be accessed.

4. Servers
Casambi uses Linux servers protected with industry best practices. All communication is done via HTTPS*. Servers are firewalled and monitored 24/7. They are kept up to date with security updates, access only by limited personnel and the stored information is encrypted.

5. Communication between a mobile device and a Casambi unit
Each request is signed with a unique authentication to verify that user has privileges to perform operation, i.e. changing configuration or controlling fixtures.

Firmware updates are signed with authentication, units only accepts firmware that originates from Casambi.

6. Communication between two Casambi units
All communication between two Casambi units are encrypted with 128-bit AES and signed. Each unit performs authentication with all nearby units. Each packet contains rolling code that protects against replay attacks (listen and resend).

7. Gateway Communication
The gateway access is through the Casambi cloud.
All communication is HTTPS*.

8. Sharing Settings
Please remember to set your network sharing settings on a suitable level. Please keep the administrator device and the passwords as your personal knowledge.

- **Not Shared:** The Network is only stored on the device the network has been created with. Other devices cannot access the network.
- **Administrator Only:** The Network is discovered and accessed only with an administrator e-mail and password (chosen at the stage of creating the network).
- **Password Protected:** Other devices can access the network with a visitor password. Modifications require an administrator password.
- **Open:** Other devices can access the network without any password. Modifications require an administrator password.

9. Worse case scenario with Casambi
In case, against all odds, a Casambi network would be hacked, the only thing a hacker can do after such an intrusion- is to control the lighting.

10. Smart and connected
The ideal network architecture includes smart devices, that are smart on their own and are connected only when needed- instead of needing a connection to be smart.
Casambi is truly Smart & Connected.

*HTTPS stands for Hyper Text Transport Protocol Secure and is a trusted end-to-end communication process. HTTPS prevents hackers from sniffing out passwords and hijack user accounts.
Example: HTTPS commonly used by banks and other websites handling money.

CASAMBI

10 arguments pour la sécurité de Casambi

1. Le Wi-Fi est un problème
Si une solution de gestion de la lumière nécessite le Wi-Fi pour son fonctionnement normal, alors l'architecture de la solution de gestion de la lumière est foncièrement mal conçue.
En plus de problèmes de performance, de coût, de consommation électrique et de convivialité, le Wi-Fi rend extrêmement vulnérable aux cyberattaques et met ainsi en péril la sécurité du système.
Casambi utilise pour son fonctionnement normal une liaison Bluetooth à faible consommation et un réseau Mesh taillé sur mesure – aucune liaison Wi-Fi n'est nécessaire.

2. Le réseau Casambi
Le réseau Casambi (communication entre des terminaux mobiles et des unités Casambi, ainsi qu'entre des unités Casambi et la cloud et le serveur) est un réseau autonome fermé. Il n'y a pas d'accès aux réseaux locaux de bâtiment.

3. La cloud Casambi
Un identifiant et un mot de passe sont requis afin d'obtenir un jeton d'accès au réseau local Bluetooth.
Les mots de passe sont stockés avec un chiffrement symétrique classique. Un jeton permet d'accéder uniquement à un réseau local.

4. Serveur
Casambi utilise des serveurs Linux protégés selon les usages de la branche qui ont fait leurs preuves. Toute communication se fait par HTTPS*.
Les serveurs disposent d'un firewall et sont surveillés 24 heures sur 24. Ils sont actualisés par des mises à jour de sécurité, l'accès est restreint à un nombre limité de collaborateurs et à l'information stockée.

5. Communication entre des terminaux mobiles et une unité Casambi
Chaque interrogation est confirmée par une authentification univoque, afin de vérifier que l'utilisateur est autorisé à l'opération, c'est-à-dire en l'occurrence à modifier la configuration ou la gestion des luminaires.
Les mises à jour de firmware sont confirmées par une authentification, les unités acceptent uniquement des firmwares originaux provenant de Casambi.

6. Communication entre deux unités Casambi
Toute communication entre deux unités Casambi est chiffrée et confirmée par AES 128-bit. Chaque unité effectue une authentification avec les toutes les unités voisines. Chaque paquet reçoit un code de roulement qui protège contre des attaques de réinsertion (écouter et envoyer de nouveau).

7. Communication avec la passerelle
L'accès à la passerelle se fait à travers la cloud Casambi. Toute communication utilise HTTPS*.

8. Paramètres partagés
N'oubliez pas de définir un niveau approprié pour vos paramètres de partage du réseau. Traitez de façon confidentielle l'appareil d'administration et les mots de passe, s'il vous plaît.

- **Non partagé :** Le réseau n'est enregistré que sur l'appareil où il a été configuré. D'autres appareils n'ont pas accès au réseau.
- **Uniquement l'administrateur :** Le réseau est localisé et atteint uniquement par un e-mail et mot de passe d'administrateur (choisi lors du paramétrage du réseau).
- **Protégé par mot de passe :** D'autres appareils ont accès au réseau par mot de passe de visiteur. Tout changement requiert un mot de passe d'administrateur.
- **Ouvert :** D'autres appareils ont accès au réseau sans mot de passe. Tout changement requiert un mot de passe d'administrateur.

9. Scénario « worst-case » avec Casambi
Au cas où, contre toute attente, un réseau Casambi serait piraté, le pirate ne peut que piloter la lumière après son intrusion.

10. Intelligent et connecté
L'architecture de réseau idéale comprend des appareils intelligents qui possèdent leur propre intelligence et pour cela ne sont connectés qu'en cas de nécessité – et ne deviennent pas intelligents seulement au moment de la connexion. **Car Casambi est réellement intelligent & connecté.**

*HTTPS signifie Hyper Text Transport Protocol Secure, un procédé de communication de bout en bout qui a fait ses preuves. HTTPS empêche le pirates d'espionner les mots de passe et de pirater les comptes des utilisateurs.
HTTPS est p.ex. utilisé couramment par des banques et d'autres sites Web de transactions financières.

CASAMBI

10 argumenten voor de veiligheid van Casambi

1. WiFi is een probleem
Indien voor de standaard werking van een lichtbesturingsoplossing WiFi benodigd wordt, is de architectuur van de lichtbesturingsoplossing in principe verkeerd geconfigureerd.
Naast problemen bij vermogen, kosten, stroomverbruik en gebruiksvriendelijkheid is WiFi uiterst kwetsbaar voor cyberaanvallen en wordt zodoende de veiligheid van het systeem op het spel gezet.
Casambi maakt gebruik van een verbruiksarme Bluetooth-verbinding en een op maat geknipt “Mesh”-netwerk voor de standaard werking – een WiFi-verbinding is niet nodig.

2. Het Casambi-netwerk
Het Casambi-netwerk (communicatie tussen mobiele eindapparaten en Casambi-eenheden enerzijds en tussen Casambi-eenheden en de Cloud en server anderzijds) is een autonoom, gesloten netwerk. Er bestaat geen toegang tot lokale gebouwnetwerken.

3. De Casambi-Cloud
Login en wachtwoord zijn noodzakelijk voor een toegangstoken tot het lokale Bluetoothnetwerk.
De wachtwoorden worden met klassieke symmetrische codering opgeslagen. Met een toegangstoken heeft men alleen toegang tot een lokaal netwerk.

4. Server
Casambi maakt gebruik van Linux-servers die beschermd zijn doordat ze in de branche hun deugdelijkheid reeds bewezen hebben. Al de communicatie verloopt via HTTPS*.
De servers beschikken over een firewall en worden dag en nacht gemonitord. Geactualiseerd worden ze met veiligheidsupdates, de toegang is beperkt tot een begrensd aantal medewerkers en de opgeslagen informatie. Is gecodeerd.

5. Communicatie tussen mobiele eindapparaten en een Casambieenheid
Elke aanvraag wordt met een duidelijke authentificatie beantwoord om na te gaan, of de gebruiker ook gerechtigd is om de verrichting uit te voeren, waarbij het hier specifiek om een wijziging van de configuratie of besturing van de armaturen gaat.
Firmware-updates worden met authentificatie beantwoord, de eenheden accepteren uitsluitend Firmware die oorspronkelijk van Casambi afkomstig is.

6. Communicatie tussen twee Casambi-eenheden
Al de communicatie tussen twee Casambi-eenheden wordt met 128-bit AES Gecodeerd en beantwoord. Iedere eenheid voert een authentificatie met alle nabijgelegen eenheden uit. Elk pakket bevat een rollencode die tegen Replay-aanvallen beschermt (horen en opnieuw zenden).

7. Gateway-communicatie
De Gateway-toegang volgt door middel van de Casambi-Cloud. Al de communicatie verloopt via HTTPS*.

8. Gedeelde instellingen
Vergeet niet, uw instellingen voor het delen van het netwerk op een geschikt niveau te zetten. Gelieve het administratorapparaat en de wachtwoorden vertrouwelijk te behandelen.

- **Niet gedeeld:** het netwerk is alleen opgeslagen op het apparaat, waarop het ook ingesteld werd. Andere apparaten hebben geen toegang tot het netwerk.
- **Alleen administrator:** het netwerk wordt alleen met een administrator-e-mail en (bij de inrichting van het netwerk gekozen) wachtwoord gelokaliseerd en bereikt.
- **Door een wachtwoord beschermd:** andere apparaten hebben door middel van een bezoekerswachtwoord toegang tot het netwerk. Wijzigingen vereisen een administratorwachtwoord.
- **Open:** andere apparaten hebben zonder wachtwoord toegang tot het netwerk. Wijzigingen vereisen een administratorwachtwoord.

9. “Worst-Case” scenario met Casambi
Indien een Casambi-netwerk, tegen de verwachting in, gehackt wordt, kan een hacker na het binnendringen enkel en alleen het licht besturen.

10. Intelligent en verbonden
De ideale netwerkarchitectuur omvat intelligente apparaten die eigen intelligentie bezitten en daarom alleen wanneer nodig aangesloten worden – en niet pas door de verbinding intelligent worden. **Casambi is namelijk werkelijk intelligent & verbonden.**

*HTTPS staat voor Hyper Text Transport Protocol Secure en is een beproefde End-to-End communicatiemethode. HTTPS weerhoudt hackers van het bespioneren van de wachtwoorden en het hacken van gebruikersaccounts. Zo wordt HTTPS bijvoorbeeld gewoonlijk door banken en andere websites met geldverkeer toegepast.

CASAMBI