

ClickShare C-5, C-10 Gen2

Modell C3010S



Installationshandbuch

Barco NV
Beneluxpark 21, 8500 Kortrijk, Belgium

Registered office: Barco NV
President Kennedypark 35, 8500 Kortrijk, Belgium

Urheberrecht ©

Alle Rechte vorbehalten. Ohne vorherige schriftliche Genehmigung von BARCO darf kein Teil dieser Publikation kopiert, vervielfältigt oder übersetzt werden. Ohne vorherige schriftliche Genehmigung von Barco darf das Dokument nicht aufgezeichnet, übertragen oder in einem Recherchiersystem gespeichert werden.

Änderungen

Diese Publikation wird „wie besehen“ zur Verfügung gestellt, ohne jegliche Garantien, weder ausdrücklich noch impliziert, einschließlich, aber nicht ausschließlich, implizierter Garantien der Handelsfähigkeit oder Eignung für einen gewissen Zweck. Barco kann jederzeit und ohne vorherige Ankündigung Verbesserungen bzw. Änderungen an den in der vorliegenden Dokumentation angeführten Produkten oder Programmen vornehmen.

Diese Publikation kann technische Ungenauigkeiten oder typografische Fehler enthalten. Die hierin enthaltenen Informationen werden regelmäßig aktualisiert; diese Änderungen werden in neue Ausgaben der Publikation eingefügt.

Die neueste Ausgabe der Barco-Handbücher kann von der Barco-Website www.barco.com heruntergeladen werden.

Reaktion auf Sicherheitsvorfälle des Produkts

Als globaler Marktführer im Technologiebereich engagiert sich Barco dafür, unseren Kunden sichere Lösungen und Dienstleistungen bereitzustellen und gleichzeitig Barcos geistiges Eigentum zu schützen. Wenn wir Bedenken im Hinblick auf die Sicherheit eines Produkts erhalten, wird unverzüglich der Prozess zur Reaktion auf Sicherheitsvorfälle des Produkts ausgelöst. Um bestimmte Sicherheitsbedenken anzusprechen oder Sicherheitsprobleme im Hinblick auf Barco-Produkte zu melden, informieren Sie uns bitte über die Kontaktinformationen, die Sie unter <https://www.barco.com/psirt> finden. Um unsere Kunden zu schützen, legt Barco Sicherheitsschwachstellen nicht öffentlich offen und bestätigt diese auch nicht, bis Barco eine Analyse des Produkts durchgeführt und eine Fehlerbehebung und/oder Maßnahmen zur Einschränkung veröffentlicht hat.

Patentschutz

Dieses Produkt ist durch Patente und/oder anhängige Patentanmeldungen abgedeckt. Für weitere Informationen: <https://www.barco.com/en/about-barco/legal/patents>.

Warenzeichen

Alle in dieser Betriebsanleitung verwendeten Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber. Alle genannten Marken- und Produktnamen sind nur als Beispiel gedacht und sind keine Werbung für die Produkte oder deren Hersteller.

Inhaltsverzeichnis

1	C-5, C-10 Gen2-Einführung	9
1.1	Informationen zu C-5, C-10 Gen2	10
1.2	Technische Daten – C-10	12
1.3	Technische Daten – C-5	14
1.4	Informationen zu Base Unit	16
1.5	Support für mobile Geräte	18
2	Erste Schritte	19
2.1	Installationsvoraussetzungen	20
2.2	Sicherheitsempfehlungen vor dem Start	21
2.3	Grundlegender Arbeitsablauf	22
3	C-5, C-10 Gen2-Installation	23
3.1	Installationsmethoden für die Base Unit	24
3.2	Tischgerät	25
3.3	Wand- oder Deckenmontage	26
3.4	Standardmäßige Verwendung der Base Unit	28
3.5	Anforderungen an die Netzwerkbereitstellung	29
3.6	Einrichtung mit Netzwerkverbindung	31
3.7	Einrichtung mit Dual-Netzwerkverbindung	32
3.8	Dedizierte Netzwerkkonfiguration	34
3.9	Verbinden eines Monitors mit der Base Unit	36
3.10	Touchscreen-Verbindungen mit der Base Unit	38
3.11	LAN-Verbindung	39
3.12	Stromversorgung	40
3.13	Erster Start der Base Unit	42
3.14	Starten ohne Konfiguration	43
3.15	Bevorzugte Startmethode	44
3.16	XMS Cloud-Registrierung	50
	3.16.1 Computer-Onboarding	50
	3.16.2 Mobiles Onboarding	51
3.17	Aktivieren der Kalenderintegration mit XMS Cloud	55
4	Vorbereiten der Buttons	61
4.1	Koppeln des Button	62
4.2	ClickShare Extension Pack	63

4.3	Installationsprogramm für das ClickShare Extension Pack	64
4.4	ClickShare Windows-zertifizierter Treiber	66
4.5	ClickShare-Desktop-App	67
4.6	MSI-Installationsprogramm der ClickShare-Desktop-App	68
5	C-5, C-10 Gen2 Configurator	69
5.1	Zugriff auf den Configurator	71
5.2	ClickShare-Konfigurationsassistent	75
5.3	Bildschirm-ID-Informationen	77
5.4	Personalisierung, Hintergrundbild	79
5.5	Personalisierung, personalisiertes Hintergrundbild	81
5.6	Verwalten der Konfigurationsdateien	83
5.7	Anzeige- und Audio-Einrichtung	85
5.8	Peripheriegeräte	86
5.9	Wi-Fi-Einstellungen	87
5.10	WLAN-Einstellungen, Zugriffspunkt-Einstellungen	88
5.11	Wi-Fi-Einstellungen, Drahtlosclient	91
5.12	Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS	92
5.13	Wi-Fi-Einstellungen, Drahtlosclient, EAP-TTLS	95
5.14	Wi-Fi-Einstellungen, Drahtlosclient, PEAP	96
5.15	Wi-Fi-Einstellungen, Drahtlosclient, WPA2-PSK	98
5.16	LAN-Einstellungen	99
5.17	LAN-Einstellungen, kabelgebundene Authentifizierung	102
5.18	LAN-Einstellungen, Sicherheitsmodus EAP-TLS	103
5.19	LAN-Einstellungen, Sicherheitsmodus EAP-TTLS	106
5.20	Services, mobile Geräte	108
5.21	Dienst, PresentSense	110
5.22	Dienst, ClickShare API, Fernbedienung über API	111
5.23	Dienste, SNMP	112
5.24	Sicherheit, Sicherheitsstufe	113
5.25	Sicherheit, Passwörter	115
5.26	Sicherheit, HTTP-Verschlüsselung	116
5.27	Statusinformationen Base Unit	118
5.28	Manuelles Festlegen von Datum und Uhrzeit	119
5.29	Festlegen von Datum und Uhrzeit, Zeit-Server	121
5.30	Energiesparen	122
5.31	Buttons	124
5.32	Buttons, externer Zugriffspunkt, EAP-TLS-Modus	125
5.33	Buttons, externer Zugriffspunkt, EAP-TTLS-Modus	127
5.34	Buttons, externer Zugriffspunkt, PEAP-Modus	128
5.35	Buttons, externer Zugriffspunkt, WPA2-PSK-Modus	129
5.36	Blackboard	130
5.37	XMS Cloud-Integration	131
5.38	Firmware-Aktualisierung	133
5.39	Support und Updates, Fehlersuche, Protokolleinstellungen	135
5.40	Fehlerbehebung, Alle Einstellungen löschen	136
5.41	Auf Werkseinstellungen zurücksetzen	137
5.42	Fehlersuche, Diagnose	138
6	Firmware-Aktualisierungen	139
6.1	Aktualisieren der C-5, C-10 Gen2-Firmware	140
7	Fehlerbehebung	141
7.1	Liste der Fehlerbehebungen	142

Index 147

C-5, C-10 Gen2- Einführung

1

1.1	Informationen zu C-5, C-10 Gen2	10
1.2	Technische Daten – C-10	12
1.3	Technische Daten – C-5	14
1.4	Informationen zu Base Unit	16
1.5	Support für mobile Geräte	18

Informationen zu diesem Dokument

Im Installationshandbuch wird die Installation von C-5, C-10 Gen2 in einem Besprechungsraum erläutert. Darüber hinaus werden die Schritte bis zur Betriebsbereitschaft des gesamten Systems erläutert. Es enthält genaue Informationen zur Konfiguration von C-5, C-10 Gen2.

Verfügbare Systemdokumentation

Neben dem Installationshandbuch sind ein Benutzerhandbuch und ein Sicherheitshandbuch auf Barcos Website www.barco.com/clickshare verfügbar.

Eine Druckausgabe der Sicherheitsanleitung ist im Lieferumfang des C-5, C-10 Gen2 enthalten.



Je nach C-5, C-10 Gen2-Version können einige Grafiken von den in diesem Handbuch verwendeten Grafiken abweichen. Dies hat jedoch keine Auswirkungen auf die Funktionalität.

1.1 Informationen zu C-5, C-10 Gen2

C-5, C-10 Gen2-Sets

ClickShare ist ein drahtloses Präsentationssystem und Ihre Eintrittskarte zu einer kollaborativen Besprechung.

Dieses Gerät hilft dem Referenten nicht nur, die Präsentation im Handumdrehen auf den Bildschirm zu bringen. Das Ergebnis ist eine deutlich verbesserte Effizienz solcher Konferenzen und eine bessere Entscheidungsfindung.

Das Set ist mit allen Laptop-, Desktop-, Tablet- und Smartphone-Betriebssystemen kompatibel.

Derzeit sind 3 verschiedene Sets auf dem Markt verfügbar. Jedes Set wird in einer bestimmten Region angeboten und kann aufgrund der Wi-Fi-Bestimmungen nur dort verwendet werden.

Komponenten

Ein Standardset besteht aus einer Base Unit und einem oder zwei Buttons. Abhängig davon, wo Sie das Produkt kaufen, variiert die Software der Base Unit.

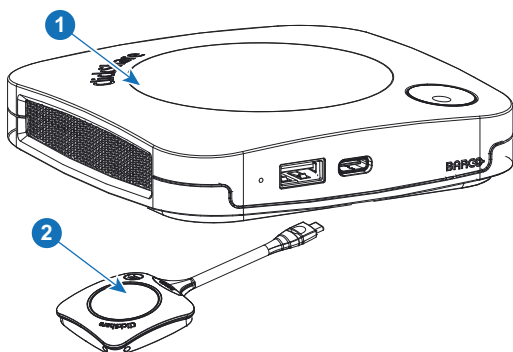


Abbildung 1-1

- 1 Base Unit
2 Button (ein oder zwei)

Mitgeliefertes Zubehör

Je nach Land, in dem Sie das Produkt kaufen, ist das folgende regionalisierte Zubehör ebenfalls im Lieferumfang enthalten.

Produkte ¹	Inhalt des Kartons
R9861611xxB1 ClickShare C-10	<ul style="list-style-type: none"> • R9861611, Base Unit • 1 x R9861600D1C² • Gleichstrom-Adapter mit Wechselstrom-Clips Typ A, C, G, I³ • Wandmontagesystem • Gedrucktes Sicherheitshandbuch
R9861611xxB2 ClickShare C-10	<ul style="list-style-type: none"> • R9861611, Base Unit • 2 x R9861600D1C², Button • Gleichstrom-Adapter mit Wechselstrom-Clips Typ A, C, G, I³ • Wandmontagesystem • Gedrucktes Sicherheitshandbuch

1. xx = EU, CN, NA, US, ZH, RW,
2. Für US, R9861600D1CUS, Button
3. Die mitgelieferten AC-Clips können abhängig von der Region variieren.

Produkte⁴**Inhalt des Kartons**

Produkte⁴	Inhalt des Kartons
R9861605xx ClickShare C-5	<ul style="list-style-type: none"> • R9861611, Base Unit • Gleichstrom-Adapter mit Wechselstrom-Clips Typ A, C, G, I³ • Wandmontagesystem • Gedrucktes Sicherheitshandbuch
R9861600D01C^{2, 5} Button	1 x R9861600D1C ^{2, 5} , , Button

Erfragen Sie bei Ihrem lokalen Händler, welche regionale Variante Sie für Ihr Land verwenden müssen.

4. xx = EU, CN, NA, US, ZH, RW,
5. Nicht für C-5

1.2 Technische Daten – C-10

Übersicht

Abmessungen (HxBxT)	34 mm x 135 mm x 135 mm
Netzteil	Standard-Wechselstromstecker mit 110/220 V oder USB-C
Leistungsaufnahme	Im Betrieb: 5-10 W, max. 24 W
Gewicht	900 g
Betriebssystem	Windows 10 und höher, macOS 11 (BigSur) und höher Android v9 und höher (ClickShare-App)* iOS 12 und höher (ClickShare-App)*
Videoausgänge	4K UHD (3.840*2.160) bei 30 Hz. HDMI 1.4b oder USB-C, DisplayPort 1.2
Audioausgang	HDMI
USB	1 X USB-A, 1 X USB-C
ClickShare Buttons	1
ClickShare-App	Desktop und Mobile
Native Protokolle	Airplay, Google Cast, Miracast*
Maximale Anzahl gleichzeitiger Verbindungen (mit Buttons und/oder App)	32
Geräuschpegel	Max. 25 dBA bei 0-30°C Max. 30 dBA bei 30-40°C
Authentifizierungsprotokoll	WPA2-PSK im Stand-Alone-Modus WPA2-PSK oder IEEE 802.1X mit ClickShare Button im Netzwerkintegrationsmodus
Protokoll für drahtlose Übertragung	IEEE 802.11 a/g/n/ac und IEEE 802.15.1
Reichweite	Mit Signalstärkemodulation einstellbar; max. 30 m (100 Fuß) zwischen ClickShare Button und ClickShare Base Unit Frequenzband 2,4 GHz und 5 GHz (DFS)
Frequenzband	2,4 GHz und 5 GHz (Unterstützung für DFS-Kanäle in ausgewählten Ländern)
Verbindungen	1 x Ethernet-LAN, 1 GBit 1x USB-Typ C 3.0 (Vorderseite); 1x USB-Typ A 3.0 (Vorderseite)
Temperaturbereich	Betrieb: 0°C bis +40°C (+32°F bis +104°F) Max: 35°C (95°F) auf 3.000 m Lagerung: -20°C bis +60°C (-4°F bis +140°F)
Luftfeuchtigkeit	Lagerung: 0 bis 90 % relative Luftfeuchtigkeit, nichtkondensierend Betrieb: 0 bis 85 % relative Luftfeuchtigkeit, nichtkondensierend
Diebstahlsicherung	Kensington-Schloss
Zertifizierungen	FCC/CE

Unterstützung für Touchscreen und Interaktivität	Ja
Raumdock (Peripherieunterstützung)	Nein
Lokale Anzeige	Ja
Netzwerkverbindung	LAN und WiFi*
Verwaltung und Berichterstellung	Ja
Gewährleistung	1 Jahr standardmäßig. 5 Jahre Abdeckung über SmartCare
*	* hängt von der Konfiguration ab, in künftigen Firmware-Aktualisierungen verfügbar

1.3 Technische Daten – C-5

Übersicht

Abmessungen (HxBxT)	34 mm x 135 mm x 135 mm
Netzteil	Standard-Wechselstromstecker mit 110/220 V oder USB-C
Leistungsaufnahme	Im Betrieb: 5-10 W, max. 24 W
Gewicht	900 g
Betriebssystem	Windows 10 und höher, macOS 11 (BigSur) und höher Android v9 und höher (ClickShare-App)* iOS 12 und höher (ClickShare-App)*
Videoausgänge	4K UHD (3.840*2.160) bei 30 Hz. HDMI 1.4b oder USB-C, DisplayPort 1.2
Audioausgang	HDMI
USB	1 X USB-A, 1 X USB-C
ClickShare Buttons	0
ClickShare-App	Desktop und Mobile
Native Protokolle	Airplay, Google Cast, Miracast
Maximale Anzahl gleichzeitiger Verbindungen (mit Buttons und/oder App)	32
Geräuschpegel	Max. 25 dBA bei 0-30°C Max. 30 dBA bei 30-40°C
Authentifizierungsprotokoll	WPA2-PSK im Stand-Alone-Modus WPA2-PSK oder IEEE 802.1X mit ClickShare Button im Netzwerkintegrationsmodus
Protokoll für drahtlose Übertragung	IEEE 802.11 a/g/n/ac und IEEE 802.15.1
Reichweite	Mit Signalstärkemodulation einstellbar; max. 30 m (100 Fuß) zwischen ClickShare Button und ClickShare Base Unit Frequenzband 2,4 GHz und 5 GHz (DFS)
Frequenzband	2,4 GHz und 5 GHz (Unterstützung für DFS-Kanäle in ausgewählten Ländern)
Verbindungen	1 x Ethernet-LAN, 1 GBit 1x USB-Typ C 3.0 (Vorderseite); 1x USB-Typ A 3.0 (Vorderseite)
Temperaturbereich	Betrieb: 0°C bis +40°C (+32°F bis +104°F) Max: 35°C (95°F) auf 3.000 m Lagerung: -20°C bis +60°C (-4°F bis +140°F)
Luftfeuchtigkeit	Lagerung: 0 bis 90 % relative Luftfeuchtigkeit, nichtkondensierend Betrieb: 0 bis 85 % relative Luftfeuchtigkeit, nichtkondensierend
Diebstahlsicherung	Kensington-Schloss
Zertifizierungen	FCC/CE

Unterstützung für Touchscreen und Interaktivität	/
Raumdock (Peripherieunterstützung)	Nein
Lokale Anzeige	Nur lokale Anzeige der Raumanzeige
Netzwerkverbindung	LAN und WiFi*
Verwaltung und Berichterstellung	Ja
Gewährleistung	1 Jahr standardmäßig. 5 Jahre Abdeckung über SmartCare
*	* hängt von der Konfiguration ab, in künftigen Firmware-Aktualisierungen verfügbar

1.4 Informationen zu Base Unit

Base Unit-Funktionalität

Die Base Unit empfängt die drahtlose Eingabe und steuert den Inhalt des Anzeigeräts im Besprechungsraum.

Die Base Unit kann im Besprechungsraum auf dem Tisch platziert oder an der Wand bzw. der Decke montiert werden. Die Anweisungen zur Installation der Base Unit finden Sie im Installationshandbuch.

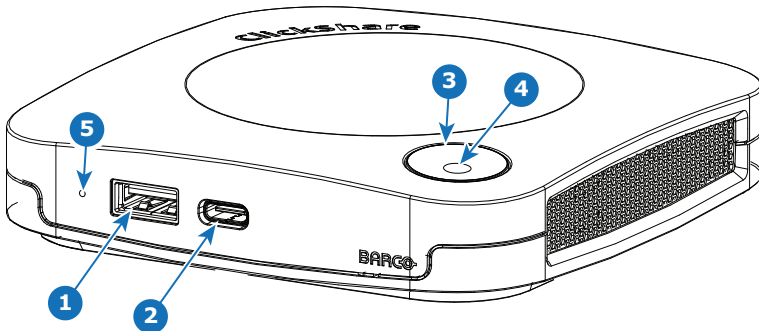


Abbildung 1–2

1	USB-Anschluss Typ A (USB 2.0)
2	USB-Anschluss Typ C (USB 2.0)
3	Status-LED-Ring
4	Standby-Taste
5	Taste zum Zurücksetzen der Hardware

USB-Anschlüsse

Der USB-C™-Anschluss wird verwendet, um die verfügbaren Buttons zu koppeln. Der USB-C™- und USB-A-Anschluss können zur Aktualisierung der Base Unit-Firmware verwendet werden, wenn dies nicht über XMS erfolgt.

Wenn Sie den Button an die Base Unit anschließen, wird der Button mit der Base Unit gekoppelt. Die Base Unit überprüft, ob Software und Firmware des Buttons aktuell sind. Falls nicht, aktualisiert die Base Unit die Software und/oder die Firmware.

Manchmal ist die Verwendung eines Adapters erforderlich, um die Verbindung zu einem dieser Anschlüsse herzustellen.

Status-LED-Ring

Die Farbe des LED-Rings um die Ein-/Ausschalttaste der Base Unit liefert Informationen zum Systemstatus.

LED-Verhalten	Erläuterung
Leuchtet rot	<ul style="list-style-type: none"> Empfängt Inhalte vom Button und sendet sie an den Monitor. während der ersten Phase des Startvorgangs der Base Unit.
Blinkt weiß	<ul style="list-style-type: none"> Das System wird gestartet (während der zweiten Phase) Der Button wird gekoppelt. Software der Base Unit
Blinkt langsam weiß	<ul style="list-style-type: none"> ECO-Standby-Modus
Leuchtet weiß	<ul style="list-style-type: none"> aktiv und einsatzbereit (z. B. wird die Willkommensnachricht auf dem Monitor angezeigt) Die Kopplung und Softwareaktualisierung des Buttons sind abgeschlossen. Sie können den Button jetzt von der Base Unit trennen.

LED-Verhalten	Erläuterung
Blinkt rot	<ul style="list-style-type: none"> Ein Fehler ist aufgetreten
Dunkel	<ul style="list-style-type: none"> Deep-Standby/Aus

Rückseitiges Layout der Base Unit

Auf der Rückseite der Base Unit befindet sich die Anschlussplatte.

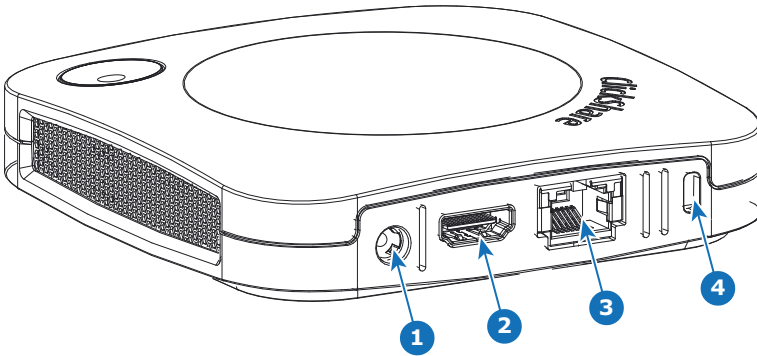


Abbildung 1–3

1	Stromversorgung
2	HDMI-Ausgang
3	LAN-Ethernet-Verbindung
4	Kensington-Schloss

Mechanische Vorrichtungen

Die mechanischen Vorrichtungen befinden sich an der Unterseite der Base Unit.

Antenne

Die Antenne ist in C-5, C-10 Gen2 integriert.

Layout der Base Unit-Unterseite

Das Seriennummernetikett mit der Barco-Teilenummer, Revisionsnummer, Produktionsdatum (Woche/Jahr) und der Seriennummer.

Das Produktetikett mit den entsprechenden Zertifizierungslogos.

Das Produktetikett enthält folgende Informationen:

- Das Barco-Logo
- Den Produktnamen
- Die Barco-Teilenummer
- Die Nennleistung
- Kennzeichnungen für entsprechende Standards (CE, CCC, UL, ...)
- Kennzeichnungen für die Entsorgungsverordnung
- „in....hergestellt“

1.5 Support für mobile Geräte

Übersicht

Die Apps in der folgenden Liste werden von ClickShare unterstützt und können auf Ihrem mobilen Gerät über Google Play oder den App Store von Apple installiert werden. Oder sie kann auf Ihrem Windows- oder Mac-PC installiert werden.

Bevor Sie ClickShare auf Ihrem mobilen Gerät verwenden können, müssen Sie die ClickShare Base Unit mit dem Wi-Fi des mobilen Geräts verbinden. Folgen Sie den Anweisungen im Benutzerhandbuch Ihres mobilen Geräts. Oder verbinden Sie die Base Unit mit dem Netzwerk. Dann müssen Sie das Wi-Fi nicht ausschalten.

App	Verwendet auf
ClickShare-App	iOS Android Windows Mac OS

Apps können von www.clickshare.app heruntergeladen werden.

Erste Schritte

2

2.1	Installationsvoraussetzungen	20
2.2	Sicherheitsempfehlungen vor dem Start	21
2.3	Grundlegender Arbeitsablauf	22

2.1 Installationsvoraussetzungen

Umgebungstemperaturen

Max. Umgebungstemperatur: 40 °C oder 104 °F

Min. Umgebungstemperatur: 0 °C oder 32 °F

Lagerungstemperatur: -10°C bis +60°C (14°F bis 140°F)

Relative Luftfeuchte

Lagerung: 0 bis 90 % relative Luftfeuchtigkeit, nichtkondensierend

Betrieb: 0 bis 85 % relative Luftfeuchtigkeit, nichtkondensierend

Prüfung der Umgebungsbedingungen

Bei Installation in Umgebungen, in denen das Gerät einer starken Staubentwicklung ausgesetzt ist, ist es äußerst ratsam und wünschenswert, dass dieser Staub ausgefiltert wird, bevor er am Gerät die Eingänge für saubere Luft erreicht. Vorrichtungen zum Extrahieren oder Abschirmen dieser starken Staubentwicklung vom Gerät sind unverzichtbar. Ist diese Lösung nicht praktikabel, müssen Maßnahmen erwogen werden, das Gerät an einen Standort mit reiner Luft zu verlegen.

Der Kunde hat jederzeit sicherzustellen, dass das Gerät vor dem Einfluss schädlicher Luftverschmutzung in seiner Nähe geschützt ist. Der Hersteller behält sich das Recht vor, die Reparatur eines Geräts zu verweigern, das nachlässig oder unsachgemäß benutzt wurde.

2.2 Sicherheitsempfehlungen vor dem Start

Sorgen Sie dafür, dass Ihre Base Units und Buttons aktuell sind

Barco verbessert seine Geräte fortlaufend, was bedeutet, dass bestehende Funktionen erweitert und neue ergänzt werden, aber auch, dass Sicherheits-Patches bereitgestellt werden. Daher wird dringend empfohlen, die Base Units mit der aktuell verfügbaren Firmware auf dem aktuellen Stand zu halten und sicherzustellen, dass die Buttons aktualisiert werden. Aktualisieren Sie Ihr Gerät immer auf die aktuelle Firmware. Daher wird dringend empfohlen, Ihr Gerät mit dem Internet zu verbinden, um automatisch Aktualisierungen zu erhalten.

Um sicherzustellen, dass alle Buttons aktualisiert werden, empfiehlt Barco dringend, alle Buttons unmittelbar nach der Aktualisierung der Base Unit mit der entsprechenden Base Unit zu koppeln.

XMS-Plattform

Verwalten Sie Base Units über die XMS (Cloud)-Verwaltungsplattform, um Aktualisierungen zu erhalten.

XMS ist Barcos sichere, cloudbasierte Lösung für die Konfiguration, Remoteverwaltung und Echtzeitstatus-Überwachung Ihrer Geräte, die über verschiedene Standorte verteilt ist. Genießen Sie einfache und automatisierte (Planung von) Softwareaktualisierungen, Base Unit-Konfiguration, das Erstellen von Vorlagen, die Hintergrundbild-Remoteinstallation, Benutzerverwaltung und Einblicke zur Förderung eines digitalen Arbeitsplatzes.

Schließen Sie die Base Unit weg

Falls Sie eine physische Manipulation der Hardware durch böswillige Personen befürchten, empfiehlt Barco, die Base Units wegzuschließen.

Ändern Sie das WLAN-Standardpasswort

Barco empfiehlt dringend, das WLAN-Standardpasswort zu ändern (gilt nur, wenn der Modus WPA2PSK verwendet wird). Damit wird es böswilligen Personen noch einmal schwieriger gemacht, den Verkehr zwischen Button und Base Unit ohne physischen Zugriff auf die Geräte abzufangen.

Ändern Sie das Configurator-Standardpasswort

Barco empfiehlt dringend, das Configurator-Standardpasswort zu ändern. Jede Person mit bösen Absichten, die lokal oder über benachbarte Netzwerke Zugriff auf die Base Unit hat, wird überprüfen, ob der Zugriff auf Configurator der Base Unit möglich ist, um wertvolle Informationen zu extrahieren, wie z. B. WLAN-Anmeldeinformationen.

2.3 Grundlegender Arbeitsablauf

Vor der Verwendung von C-5, C-10 Gen2

1. Packen Sie das Gerät und das mitgelieferte Zubehör aus.
Eine detaillierte Übersicht des Lieferumfangs von C-5, C-10 Gen2 finden Sie unter ["Informationen zu Base Unit"](#), Seite 16.
2. Installieren Sie die Base Unit im Besprechungsraum auf eine der möglichen Installationsarten.
Weitere Informationen zu den Installationsverfahren finden Sie unter ["Installationsmethoden für die Base Unit"](#), Seite 24.
3. Stellen Sie eine Videosignalverbindung mit der Base Unit und dem Monitor her. Informationen dazu finden Sie unter ["Anzeige- und Audio-Einrichtung"](#), Seite 85.
4. Schließen Sie die Base Unit an das Stromnetz an.
Ausführliche Informationen finden Sie unter ["Stromversorgung"](#), Seite 40.
5. Verbinden Sie die Base Unit über ein Netzkabel mit dem lokalen Netzwerk (stellen Sie sicher, dass die Base Unit mit dem Internet verbunden ist, damit sie den Aktualisierungsserver erreichen kann).
6. Konfigurieren Sie das Gerät (es kann ohne eine Konfiguration verwendet werden, diese wird aber empfohlen).
7. Registrieren Sie die Base Unit in XMS Cloud und fordern Sie das kostenlose SmartCare-Paket an.
Ausführliche Informationen finden Sie unter ["XMS Cloud-Registrierung"](#), Seite 50.
8. Koppeln Sie den/die Button(s). Weitere Informationen finden Sie unter ["Koppeln des Button"](#), Seite 62.

C-5, C-10 Gen2- Installation

3

3.1	Installationsmethoden für die Base Unit.....	24
3.2	Tischgerät.....	25
3.3	Wand- oder Deckenmontage	26
3.4	Standardmäßige Verwendung der Base Unit	28
3.5	Anforderungen an die Netzwerkbereitstellung	29
3.6	Einrichtung mit Netzwerkverbindung	31
3.7	Einrichtung mit Dual-Netzwerkverbindung	32
3.8	Dedizierte Netzwerkkonfiguration.....	34
3.9	Verbinden eines Monitors mit der Base Unit.....	36
3.10	Touchscreen-Verbindungen mit der Base Unit.....	38
3.11	LAN-Verbindung	39
3.12	Stromversorgung	40
3.13	Erster Start der Base Unit.....	42
3.14	Starten ohne Konfiguration	43
3.15	Bevorzugte Startmethode.....	44
3.16	XMS Cloud-Registrierung.....	50
3.17	Aktivieren der Kalenderintegration mit XMS Cloud	55

3.1 Installationsmethoden für die Base Unit



Um die optimale Leistung zu erzielen, installieren Sie die Base Unit nah an der Anzeige und vermeiden Sie Hindernisse zwischen der Base Unit und den Buttons.



Stellen Sie sicher, dass die Base Unit nicht in einem Metallgehäuse installiert wird.

Technische Installation

Die Base Unit kann auf verschiedene Arten in einem Besprechungsraum installiert werden.

- Auf dem Tisch
- An der Wand
- Deckenmontage

Eigenständig oder Netzwerkintegration

Die Base Unit kann eigenständig oder integriert in ein Unternehmensnetzwerk verwendet werden.

- Standardmäßige Verwendung
- Standardmäßige Verwendung mit Ethernet-Link
- Integration in das Unternehmensnetzwerk
- Duale Netzwerkintegration
- Integration in dediziertes Unternehmensnetzwerk

3.2 Tischgerät

Übersicht

Stellen Sie die Base Unit auf den Tisch im Besprechungsraum.

Die Base Unit wiegt insgesamt 530 g.

3.3 Wand- oder Deckenmontage

Informationen zur Wand- oder Deckenmontage

Um den C-5, C-10 Gen2 an der Wand oder Decke zu befestigen, wird eine Montagebasis verwendet. Diese Basis hat schlüsselförmige Bohrungen, damit Sie die Basis an der Wand oder Decke befestigen können. Sie können die Basis auch mit der selbstklebenden Folie montieren. Wenn Sie die Position des Geräts bestimmt haben, befolgen Sie die nächsten Schritte, um das Gerät zu montieren.

Montage mit Schrauben

1. Entnehmen Sie die Montagebasis aus der Verpackung.
2. Platzieren Sie die Montagebasis an der Wand oder Decke und markieren Sie die Bohrungen (1).

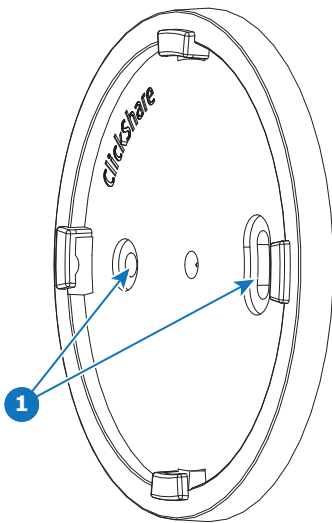


Abbildung 3-1

3. Wählen Sie einen Bohraufsatz, der etwas kleiner als die verwendeten Dübel ist, um einen guten Sitz sicherzustellen.
4. Bohren Sie die Löcher, wo Sie sie markiert haben.
5. Schlagen Sie mit einem Hammer Kunststoffdübel in die Bohrlöcher (bei Bedarf, abhängig vom Wand- oder Deckentyp).
6. Platzieren Sie die Montagebasis an der Decke oder Wand und drehen Sie die Schrauben ein.
7. Platzieren Sie das Gerät auf der Montagebasis und drehen Sie es gegen den Uhrzeigersinn, bis es einrastet.

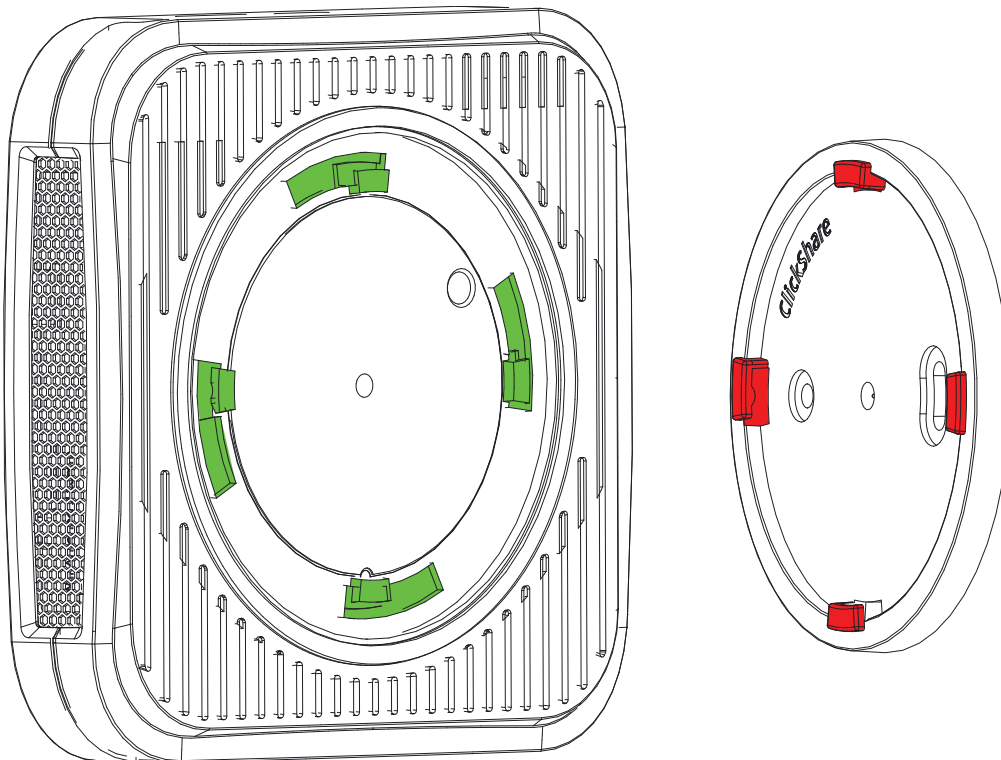


Abbildung 3-2

Montage mit der selbstklebenden Folie

1. Ziehen Sie die entfernbare Schutzfolie ab.

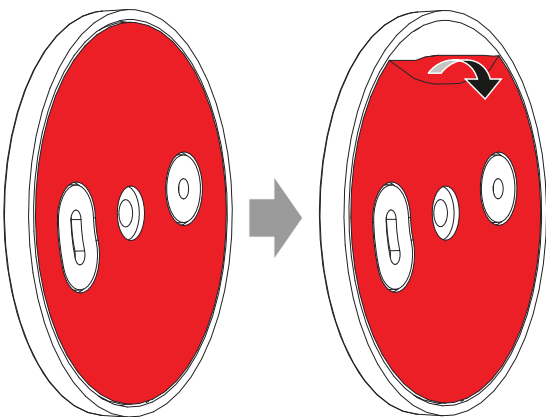


Abbildung 3-3

2. Kleben Sie die Basis an die gewählte Position.
3. Platzieren Sie das Gerät auf der Montagebasis und drehen Sie es gegen den Uhrzeigersinn, bis es einrastet ([Abbildung 3-2](#)).

3.4 Standardmäßige Verwendung der Base Unit

Übersicht

Diese Konfiguration ist im Hinblick auf die Installation die einfachste und kann für temporäre Konfigurationen und in Organisationen verwendet werden, in denen keine zentrale Verwaltung und Drittanbieter-Integration erforderlich sind.

Die ClickShare Base Unit und der Button sind direkt und ohne Integration in das Unternehmensnetzwerk einsatzfähig. Die Base Unit sollte mindestens einmal mit dem Internet verbunden werden, um sie zu aktualisieren und zu registrieren. Benutzer können sich über die ClickShare Buttons, über die ClickShare-App oder Miracast oder über ihre Mobilgeräte und AirPlay oder Google Cast direkt mit der Base Unit verbinden.

Die Verwendung eines ClickShare Buttons ermöglicht die Aufrechterhaltung der Internetverbindung. Für die Verwendung der ClickShare-App, von AirPlay oder Google Cast ist eine Direktverbindung mit der Base Unit erforderlich. Ein Internetzugriff ist dann nur möglich, wenn das Gerät die gleichzeitige Verwendung von Daten (3G/4G) unterstützt. Beachten Sie, dass hierzu der Zugriffspunkt der Base Unit nicht ausgeschaltet sein darf, sichtbar und für die Verbindung für jeden verfügbar sein muss.

Die Freigabe über Miracast ist nur über Wi-Fi Direct möglich.

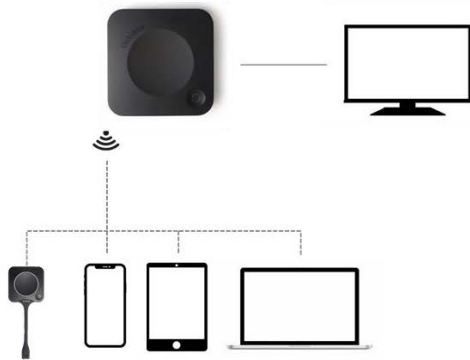


Abbildung 3–4

Da die ClickShare Base Unit und der Button direkt einsatzbereit sind, sind sie ideal für vorübergehende Konfigurationen, Besuchszentren und kleine bis mittelgroße Installationen ohne die Anforderungen oder Möglichkeiten einer Netzwerkintegration. Diese Konfiguration erfordert den geringsten Installationsaufwand und hält alle freigegebenen Daten vollständig von Ihrem Unternehmensnetzwerk getrennt. Die Aktualisierung und Konfiguration der Base Units muss manuell erfolgen.

3.5 Anforderungen an die Netzwerkbereitstellung

Allgemein

Dieses Thema enthält Empfehlungen für die Integration Ihrer Gerät in Ihr Unternehmensnetzwerk. Dort finden Sie eine detaillierte Übersicht in Bezug auf die Minimalanforderungen und erforderlichen Regeln für Ports und Firewall, die konfiguriert werden müssen, damit die spezifische Funktion funktioniert.

Base Unit: erstmalige Einrichtung

- **Aktivierung und Aktualisierung:** Für diesen Schritt ist, ähnlich wie bei der automatischen Aktualisierungsfunktionalität, die im Folgenden beschrieben wird, eine ausgehende TCP-Verbindung an Port 443 zu `update.cmp.barco.com` und `assets.cloud.barco.com` erforderlich.
- **Verbindung zu XMS Cloud** für die Aktivierung der SmartCare- und XMS-Cloud-Funktionen: Ausgehender TCP-Port 443 zu `*.azure-devices.net`, `*.core.windows.net` und `global.azure-devicesprovisioning.net`.

Für die erstmalige Einrichtung ist ein Laptop mit folgendem Zugriff erforderlich:

- XMS Cloud: ausgehender TCP-Port 443 zu `xms.cloud.barco.com`
- MyBarco-Portal: ausgehender TCP-Port 443 zu `*.barco.com` (`login/xms.cloud.barco.com`)
- (Optional) Web Configurator für das Gerät: TCP-Port 80 und 443 zur Base Unit oder die Möglichkeit zur Direktverbindung mit dem WLAN der Base Unit.

Übersicht der erforderlichen Ports

Öffnen Sie die folgenden Ports in Ihrem Netzwerk, um sicherzustellen, dass Sie Inhalt über ClickShare freigeben können:

Sender/Empfänger		Ports
ClickShare Button (Drahtlos-Präsentation)	TCP	2345, 6544
	UDP	
ClickShare-Desktop und -Mobil-Apps (Drahtlos-Präsentation)	TCP	6541-6545
	UDP	5353, 1900
Zusätzliche Ports für drahtlose Konferenzen (Button oder Desktop-App)	TCP	1235, 9999
	UDP	1234
AirPlay	TCP	4100-4200, 7000, 7100, 47000
	UDP	4100-4200, 5353
Google Cast	TCP	8008, 8009, 9080
	UDP	1900, 5353, 32768, 61000 ⁶
Miracast MS-MICE	TCP	7236, 7250
	UDP	7236
ClickShare Configurator	TCP	80, 443
	UDP	Nicht verfügbar
XMS Cloud	TCP	443
XMS Edge	TCP	4003
Automatische Aktualisierung	TCP	80, 443
	UDP	Nicht verfügbar

6. Google Cast wählt einen beliebigen UDP-Anschluss oberhalb von 32768 aus, um das Streaming von Videos zu vereinfachen.

Sender/Empfänger		Ports
SNMP	UDP	161 und 162
REST-API	TCP	4003

3.6 Einrichtung mit Netzwerkverbindung

Übersicht

Dies ist die einfachste Installation, die eine nahtlose Erfahrung für Mitarbeiter bietet. Es ist außerdem die empfohlene Konfiguration für vorübergehende Einrichtungen, Besucherzentren, kleine bis mittelgroße Installation ohne die Notwendigkeit einer Netzwerkintegration, für interne Konferenzräume, für Unternehmen mit einer flachen Netzwerktopologie oder wenn der ClickShare Button der Hauptzugriffspunkt für Personen auf das System sein wird.

In diesem Standardmodus sind der ClickShare Button und die Base Unit direkt einsatzfähig (der Button muss mit der Base Unit gekoppelt werden, bevor er verwendet werden kann) und Benutzer können über die ClickShare-Desktop-App, die ClickShare Mobile-App, AirPlay, Google Cast über das Netzwerk, mit dem die Base Unit verbunden ist, Inhalte über die Base Unit teilen, ohne die Internetkonnektivität zu verlieren. Die Freigabe über Miracast hängt von der Gerätekonfiguration ab.

Über einen ClickShare-Button können Gäste mit dem Gast-LAN verbunden bleiben und so ihre Internetkonnektivität beibehalten. Gast-Mobilgeräte müssen normalerweise direkt mit der Base Unit verbunden werden und können nur auf das Internet zugreifen, wenn das Gerät die gleichzeitige Verwendung von Daten (3G/4G) unterstützt.

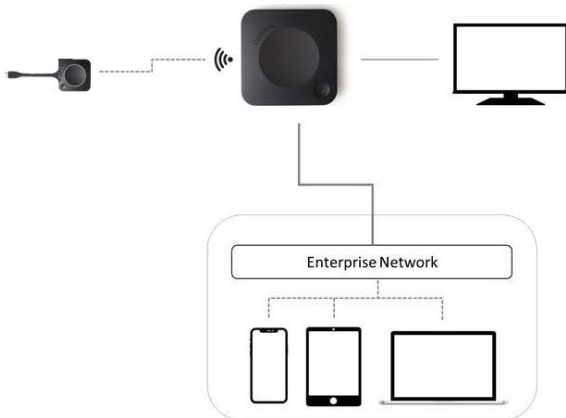


Abbildung 3–5

3.7 Einrichtung mit Dual-Netzwerkverbindung

Übersicht

Diese Installation bietet eine nahtlose Erfahrung für Mitarbeiter und Gäste und ist die empfohlene Konfiguration für jedes Unternehmen mit einer erweiterten Netzwerkkonfiguration, für Besprechungsräume, die häufig von Gästen, Besuchern und externen Personen verwendet werden, oder wenn die ClickShare-Apps und nativen BYOD-Protokolle, wie AirPlay, Google Cast und Miracast, häufig im Unternehmen genutzt werden.

Beim C-5, C-10 Gen2 deaktiviert die duale Netzwerkverbindungstopologie den Zugriffspunkt der Base Unit und die Buttons müssen über Unternehmenszugriffspunkte mit der Base Unit verbunden werden.

Beachten Sie, dass die Funktionen für drahtlose Konferenzen des ClickShare Button eingeschränkt sein können, wenn der Button in das Unternehmensnetzwerk integriert ist, und seine Leistung dann vom internen Netzwerk abhängt.

Die Benutzer können Inhalte über die ClickShare-Desktop-App, die ClickShare-Mobile-App, AirPlay, Miracast und Google Cast über eines der Netzwerke, mit denen die Base Unit verbunden ist, mit der Base Unit teilen.

Miracast MS-MICE ist nur über die LAN-Verbindung verfügbar, alle anderen Geräte verbinden sich direkt über Wi-Fi Direct mit der Base Unit.

ClickShare Base Units können in ein dediziertes Netzwerk oder VLAN integriert werden, es müssen aber dedizierte Firewall-Regeln übernommen werden, damit die Streams die verschiedenen Netzwerkabschnitte durchlaufen können.

Durch die Verbindung der Base Unit mit dem Unternehmensnetzwerk besteht die Möglichkeit die eXperience Management Suite (XMS) für die zentrale Verwaltung zu verwenden und/oder die Funktionalität für die automatische Aktualisierung zu verwenden, um die installierte Base Unit aktuell zu halten.

Eine Base Unit, die mit dem Netzwerk verbunden ist, kann über SNMP überwacht, über andere Drittanbietersysteme, wie Crestron, gesteuert und überwacht werden oder als Schnittstelle über die ClickShare Conference REST-API dienen.

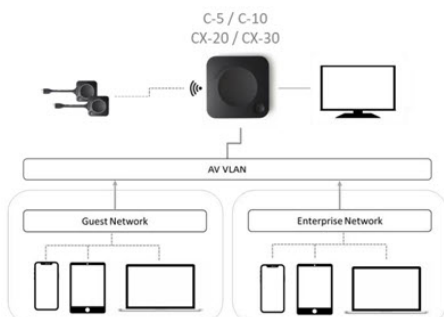


Abbildung 3–6

So erfolgt die Konfiguration über Configurator

1. Schließen Sie die Base Unit an, rufen Sie *ClickShare Configurator* auf und melden Sie sich an.
2. Wählen Sie *Button* im Menü *System* und klicken Sie auf **Einstellungen bearbeiten**.

Wählen Sie im Dropdown-Menü die Option *Externer Zugriffspunkt* aus, wählen Sie den bevorzugten Authentifizierungsmodus und füllen Sie die Details aus.

Klicken Sie auf **Änderungen speichern**. Ausführliche Informationen finden Sie unter ["Buttons"](#), Seite 124.

3. Koppeln Sie die Buttons erneut mit der Base Unit.
4. Optional kann das WiFi der Base Unit auf den Zugriffspunkt eingestellt oder deaktiviert werden. Weitere Informationen finden Sie unter ["Wi-Fi-Einstellungen, Drahtlosclient"](#), Seite 91.

Einrichtung über XMS

1. Melden Sie sich bei XMS an und rufen Sie die Registerkarte *Base Units* auf.
2. Wählen Sie in der Geräteliste die Unit(s) aus, um den Netzwerkintegration-Modus bereitzustellen.

3. Öffnen Sie die Dropdown-Liste *Konfigurieren* und wählen Sie *Netzwerkintegration*.
4. Wählen Sie einen der Authentifizierungsmodi für den Netzwerkintegration-Modus und füllen Sie die Details aus.
5. Koppeln Sie die ClickShare Buttons erneut mit der aktualisierten Base Unit, um die neue Konfiguration zu übernehmen.

Ausführliche Informationen zur Verwendung von XMS finden Sie im XMS-Benutzerhandbuch.

3.8 Dedizierte Netzwerkkonfiguration

Übersicht

Diese Installation bietet eine isolierte Netzwerkkonfiguration, bei der alle Verbindungen zu den und von den Base Units kontrolliert werden können. Dieses dedizierte AV-Netzwerk (oder ClickShare-Netzwerk) bzw. VLAN kann für eine detailliertere Zugriffssteuerung verwendet werden, um sicherzustellen, dass keine Verbindung zwischen den verbundenen physischen oder virtuellen LANs hergestellt wird oder zur Trennung des gesamten ClickShare-Verkehrs vom gesamten anderen IP-Verkehr, um Geschäftsanforderungen im Hinblick auf Bandbreite, Sicherheit und Latenz sicherzustellen.

In dieser Konfiguration können die Konfigurationen abhängig von der Netzwerktopologie und den Sicherheitsanforderungen des Unternehmens stark differieren. Hier beschreiben wir eine einfache Konfiguration, bei der die Base Unit in einem dedizierten AV-VLAN platziert wird, einem gängigen Verfahren in Unternehmen.

Bei dieser Konfiguration werden ClickShare Buttons und die Base Unit direkt einsatzbereit eingesetzt (Buttons müssen mit der Base Unit gekoppelt werden, bevor sie verwendet werden können). Da die Base Unit in einem dedizierten Netzwerk installiert wurde, ist eine Firewall-Konfiguration erforderlich, um die Verwendung der ClickShare-Desktop-App, der ClickShare Mobile-App, von AirPlay und Google Cast über das Netzwerk zu ermöglichen.

Wenn die Firewall nicht so konfiguriert ist, dass sie Verbindung vom Gast-Wi-Fi oder dem Mitarbeiter-Wi-Fi zulässt, können sich die Benutzer mit dem drahtlosen Zugriffspunkt der Base Unit verbinden, um Inhalte über die ClickShare-Desktop-App, die ClickShare-Mobile-App, AirPlay oder Chromecast zu teilen, und können sich nur mit dem Internet verbinden, wenn das Gerät die gleichzeitige Datennutzung (3G/4G/5G) unterstützt. Beachten Sie, dass hierzu der Zugriffspunkt der Base Unit nicht ausgeschaltet sein darf, sichtbar und für die Verbindung für jeden verfügbar sein muss. Mobilbenutzer sind auf die Erfahrung beschränkt, die in der eigenständigen Konfiguration beschrieben ist. Für Miracast muss die Base Unit für Miracast konfiguriert sein, sodass sie eine Wi-Fi Direct-Verbindung bietet.

Durch die Verbindung der Base Unit mit dem Unternehmensnetzwerk besteht die Möglichkeit die eXperience Management Suite (XMS) für die zentrale Verwaltung zu verwenden und/oder die Funktionalität für die automatische Aktualisierung zu verwenden, um die Installationsbasis aktuell zu halten.

Eine Base Unit, die mit dem Netzwerk verbunden ist, kann über SNMP überwacht, über andere Drittanbietersysteme, wie Overture oder Crestron, gesteuert und überwacht werden, oder als Schnittstelle über die ClickShare REST-API dienen.

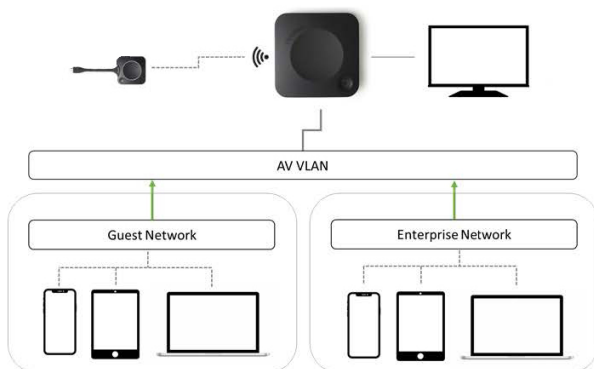


Abbildung 3–7

So erfolgt die Konfiguration über Configurator

1. Schließen Sie die Base Unit an, rufen Sie *ClickShare Configurator* auf und melden Sie sich an.
2. Wählen Sie *Button* im Menü *System* und klicken Sie auf **Einstellungen bearbeiten**.

Wählen Sie im Dropdown-Menü die Option *Externer Zugriffspunkt* aus, wählen Sie den bevorzugten Authentifizierungsmodus und füllen Sie die Details aus.

Klicken Sie auf **Änderungen speichern**. Ausführliche Informationen finden Sie unter ["Buttons"](#), Seite 124.

3. Koppeln Sie den Button erneut mit der Base Unit.

4. Optional kann das WLAN der Base Unit auf Zugriffspunkt eingestellt oder deaktiviert werden. Weitere Informationen finden Sie unter [“Wi-Fi-Einstellungen, Drahtlosclient”](#), Seite 91.

Einrichtung über XMS

1. Melden Sie sich bei XMS an und rufen Sie die Registerkarte *Base Units* auf.
2. Wählen Sie in der Geräteliste die Unit(s) aus, um den Netzwerkintegration-Modus bereitzustellen.
3. Öffnen Sie die Dropdown-Liste *Konfigurieren* und wählen Sie *Netzwerkintegration*.
4. Wählen Sie einen der Authentifizierungsmodi für den Netzwerkintegration-Modus und füllen Sie die Details aus.
5. Koppeln Sie den ClickShare Button erneut mit der aktualisierten Base Unit, um die neue Konfiguration zu übernehmen.

Ausführliche Informationen zur Verwendung von XMS finden Sie im XMS-Benutzerhandbuch.

3.9 Verbinden eines Monitors mit der Base Unit

Methoden für das Verbinden eines Monitors mit der Base Unit

Methode 1: Verbinden Sie Ihren Monitor über ein HDMI-Kabel mit der Base Unit.

Methode 2: Bei Monitoren, die Video über USB unterstützen, verbinden Sie den Monitor über ein USB-Kabel mit dem USB-C-Anschluss der Base Unit.

Anschluss über HDMI

1. Verbinden Sie die Base Unit über ein Monitorkabel mit dem Monitor.

 **Hinweis:** Im Lieferumfang von ClickShare sind keine Monitorkabel enthalten.

Verbinden Sie bei der Einrichtung einer Monitorkonfiguration das HDMI-Kabel mit dem Monitor. Falls erforderlich, verwenden Sie einen Adapter, um eine Verbindung zu einem DisplayPort oder DVI-Anschluss auf der Monitorseite herzustellen.

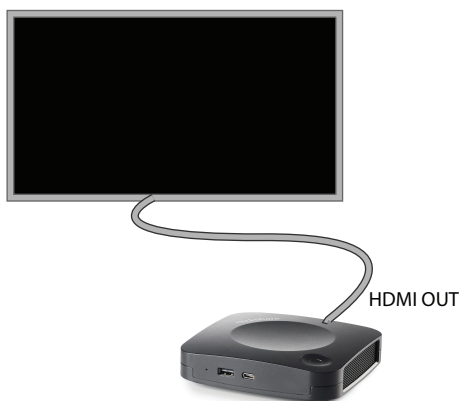


Abbildung 3-8 Monitorverbindung über HDMI

Video und Audio werden über das HDMI-Kabel übertragen.

Verbindung über den USB-C-Anschluss

1. Verbinden Sie den USB-C-Anschluss der Base Unit mit dem USB-Eingang des Monitors (nur für die Monitore, die Video über USB unterstützen).



Abbildung 3-9 Monitorverbindung über den USB-C-Anschluss

Video- und Audio werden über das USB-Kabel an den Monitor übertragen.



Wenn der Monitor über einen USB-C-Anschluss verbunden wird und dieser Monitor über zusätzliche USB-C-Anschlüsse verfügt, können eine Kamera und/oder eine Freisprecheinrichtung mit Echoausschaltung an diese Anschlüsse angeschlossen werden.
Wenn der Monitor des Weiteren 20 W über den USB-C-Anschluss ausgeben kann, kann die Base Unit auf diese Art mit Strom versorgt werden.



Wenn eine Verbindung über HDMI und über USB Typ C zwischen der Base Unit und dem Monitor hergestellt wird, hat die HDMI-Verbindung Priorität.



Ultrabreite Bildschirme können nur über eine DisplayPort-auf-USB-Verbindung angeschlossen werden.

3.10 Touchscreen-Verbindungen mit der Base Unit



Nur verfügbar beim C-10.

Informationen zur Verbindung

Ein einzelner Bildschirm kann mit der Base Unit verbunden werden.

Um eine Videoquelle anzuschließen, sollte eine HDMI-Verbindung zwischen der Base Unit und dem Monitor hergestellt werden. Um die Touch-Funktionalität zu verbinden, sollte ein USB-Kabel zwischen dem Touchscreen und der Base Unit angeschlossen werden. Eine Liste der unterstützten Touchscreens finden Sie auf der Website von Barco. Siehe <https://www.barco.com/en/support/docs/TDE9538>.

So stellen Sie eine Verbindung her

1. Verbinden Sie die Base Unit über ein HDMI-Kabel mit dem Touchscreen-Display. Falls erforderlich, verwenden Sie einen Adapter, um eine Verbindung zu einem DisplayPort oder DVI-Anschluss auf der Monitorseite herzustellen.
2. Verbinden Sie den USB-Ausgang des Touchscreen mit einem USB-Anschluss der Base Unit.

3.11 LAN-Verbindung

Informationen zur LAN-Verbindung

Die Base Unit kann mit einem lokalen Netzwerk oder direkt mit einem Laptop verbunden werden.

Maximal zulässige LAN-Geschwindigkeit: 1000 MBit

Wir empfehlen dringend die Verwendung der LAN-Verbindung und der XMS Cloud für die Konfiguration, Überwachung und zusätzliche Funktionalität. Die LAN-Verbindung verbessert auch das Benutzererlebnis erheblich, wenn die ClickShare-Apps und native Freigabeprotokolle, wie AirPlay und andere, verwendet werden.

So stellen Sie eine Verbindung her

1. Schließen Sie ein Netzkabel mit RJ-45-Anschluss am LAN-Anschluss an.
2. Verbinden Sie das andere Ende mit einem LAN.

3.12 Stromversorgung

Informationen zur Stromversorgung

Die Stromversorgung ist auf zwei Arten möglich:

- Über ein externes Netzteil (im Lieferumfang des Geräts enthalten)
- Über einen USB-C-Anschluss.



Wenn beide Verbindungen hergestellt wurden, hat das externe Netzteil Priorität.

So schließen Sie ein externes Netzteil an

1. Schließen Sie den Hohlstecker des Netzteils an den Stromeingang der Base Unit an.
2. Schieben Sie einen Steckeradapter (US, AU, IN, CH, EU oder UK) auf das Netzteil des ClickShare, bis er hörbar einrastet. Verwenden Sie die für Ihr Land zutreffende Variante.



Abbildung 3-10 Netzadapter

3. Verbinden Sie das Netzkabel mit der Wandsteckdose.

Über USB

1. Schließen Sie ein USB-C-Kabel an den USB-C-Anschluss an der Vorderseite des Geräts an.



Abbildung 3–11 Laden über USB-Strom

2. Schließen Sie das andere Ende an eine USB-Steckdose oder ein Netzteil an.

3.13 Erster Start der Base Unit

Ablauf

1. Starten Sie die Base Unit zum ersten Mal.

Der folgende Bildschirm wird auf dem verbundenen Monitor angezeigt.

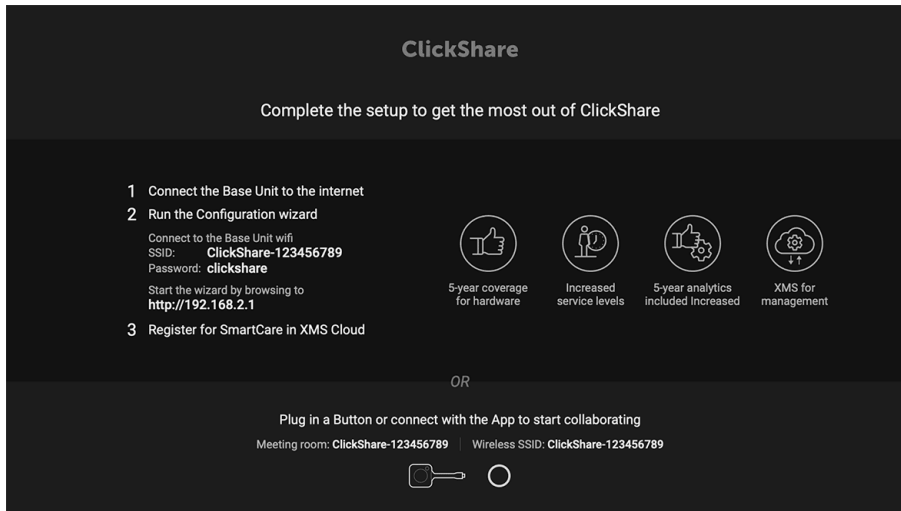


Abbildung 3–12 Onboarding-Bildschirm

Es gibt zwei Möglichkeiten, um fortzufahren:

1. Führen Sie eine Prüfung auf Aktualisierungen durch (optional), konfigurieren Sie die Base Unit und registrieren Sie sie bei XMS Cloud. Siehe ["Bevorzugte Startmethode"](#), Seite 44
2. Schließen Sie einen Button an und starten Sie die Bildschirmfreigabe. Siehe ["Starten ohne Konfiguration"](#), Seite 43

3.14 Starten ohne Konfiguration

Erste Schritte

1. Schließen Sie einen Button an und starten Sie die Bildschirmfreigabe.

Sobald sich ein Benutzer mit der Base Unit verbindet, wird auf der Anzeige des Besprechungsraums das Standardhintergrundbild angezeigt und das Gerät kann mit seiner Standardkonfiguration verwendet werden. Solange der Konfigurationsassistent aber nicht abgeschlossen wurde, wird der Bildschirm für die erste Einrichtung erneut bei jedem Neustart des Geräts angezeigt.

Die Registrierung des Geräts ist nur im Konfigurationsassistenten oder über ClickShare Configurator möglich und wenn die Base Unit mit dem Internet verbunden ist.

3.15 Bevorzugte Startmethode

Welche Schritte werden ausgeführt?

Nach der optionalen Überprüfung der Firmware-Aktualisierung sollte der Konfigurationsassistent gestartet werden, um die Base Unit zu konfigurieren.

So starten Sie den Auffüllmodus

1. Verbinden Sie das WLAN des Geräts anhand der Anweisungen.
Die Standard-SSID lautet ClickShare-[serial number].
Passwort: clickshare
2. Wenn die WiFi-Verbindung hergestellt wurde, fahren Sie mit den Netzwerkeinstellungen des Geräts fort.
Navigieren Sie zu <http://192.168.2.1>
Der ClickShare Configurator-Assistent wird gestartet.

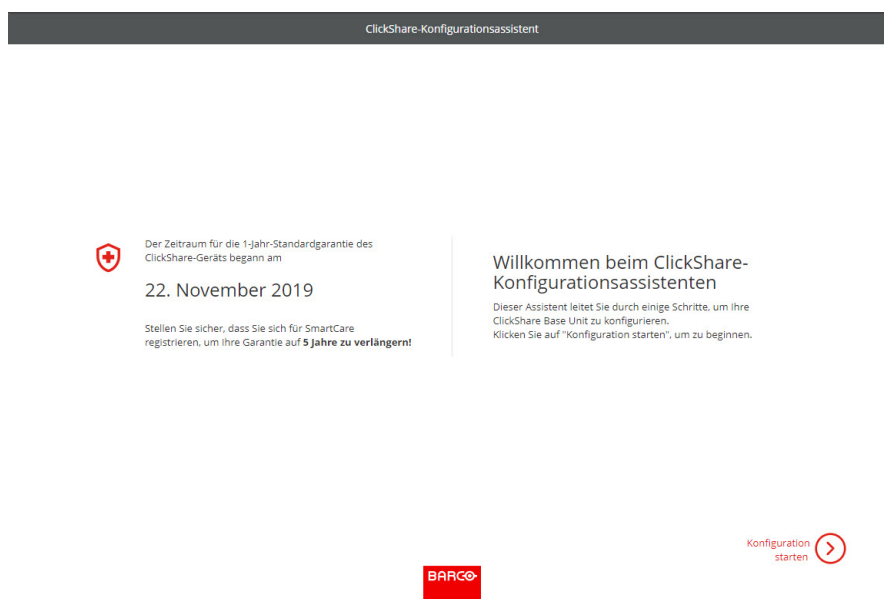


Abbildung 3–13

3. Klicken Sie auf **Konfiguration starten**.
Das Fenster für die *Firmware-Aktualisierung* wird angezeigt.

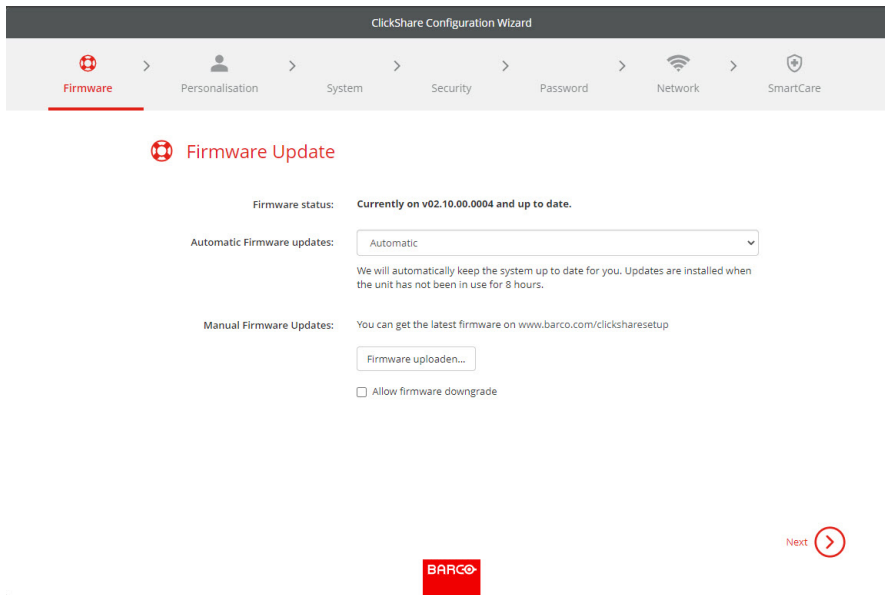


Abbildung 3–14

Wenn eine Internetverbindung besteht, können Sie *Automatisch* für die Firmware-Aktualisierung auswählen (empfohlen). Wenn Sie *Nein* auswählen, können Sie die Aktualisierung noch immer manuell durchführen, indem Sie die Software auf einen USB-Stick herunterladen.

Wenn eine Internetverbindung besteht und die Einstellung auf *Automatisch* eingestellt ist, wird die Softwareprüfung durchgeführt und die aktuelle Version wird heruntergeladen, aber die Aktualisierung der Firmware wird nur durchgeführt, wenn der Konfigurationsassistent abgeschlossen wurde.

Ausführliche Informationen zur automatischen Firmware-Aktualisierung finden Sie unter [“Firmware-Aktualisierung”](#), Seite 133.

Klicken Sie auf **Weiter**, um zur nächsten Seite zu wechseln, und auf **Zurück**, um zur vorherigen Seite zurückzukehren.

4. Schritt zur Personalisierung

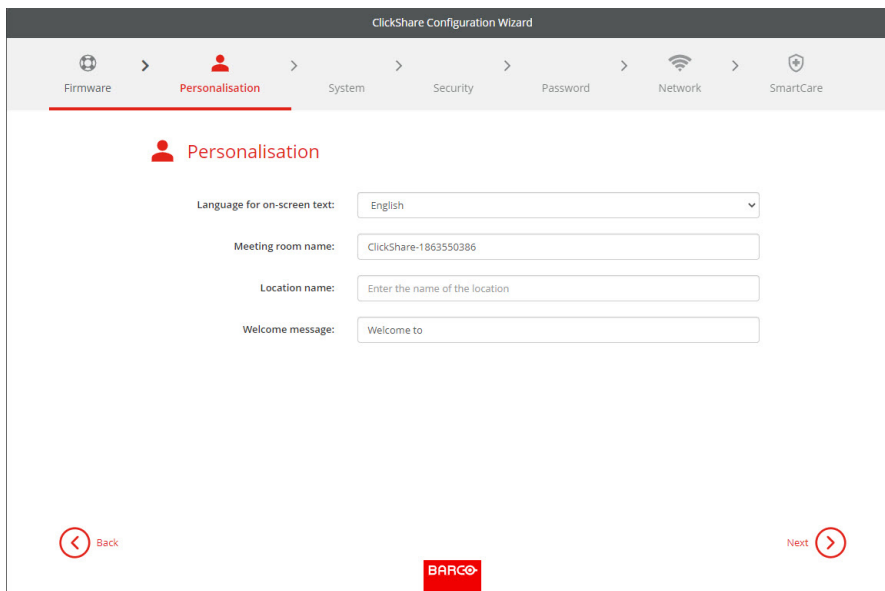


Abbildung 3–15

Geben Sie die zu verwendende Sprache für die Bildschirmanzeige ein. Weitere Informationen finden Sie unter [“Bildschirm-ID-Informationen”](#), Seite 77.

Geben Sie den Namen des Besprechungsraums, den Standort des Besprechungsraums und die Begrüßungsnachricht ein. Weitere Informationen finden Sie unter [“Bildschirm-ID-Informationen”](#), Seite 77.

5. Systemeinstellungen

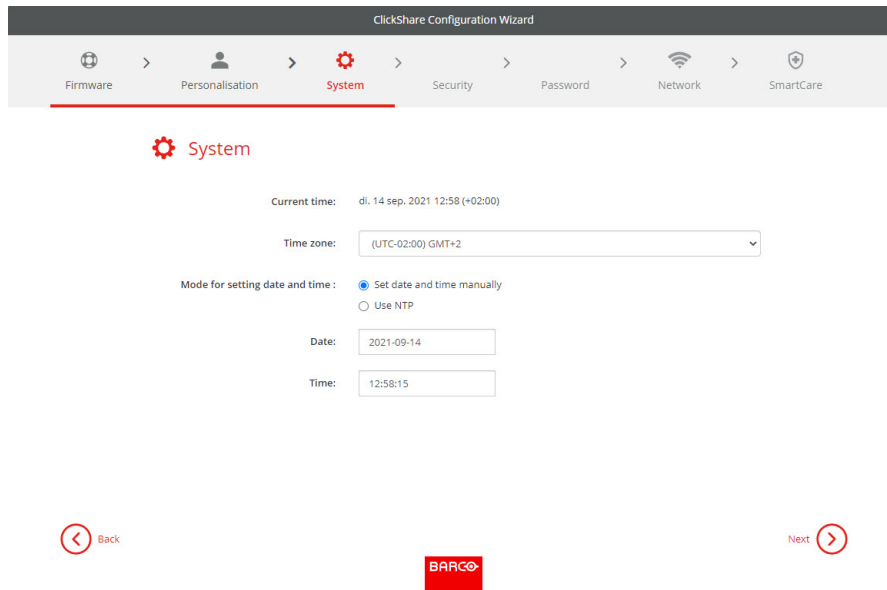


Abbildung 3–16

Geben Sie eine Zeitzone ein und treffen Sie eine Auswahl zwischen der manuellen Zeitkonfiguration und der Verwendung von NTP.

Weitere Informationen zur manuellen Zeitkonfiguration finden Sie unter [“Manuelles Festlegen von Datum und Uhrzeit”](#), Seite 119.

Weitere Informationen zur Verwendung eines NTP-Servers finden Sie unter [“Festlegen von Datum und Uhrzeit, Zeit-Server”](#), Seite 121.

6. Sicherheitseinstellungen

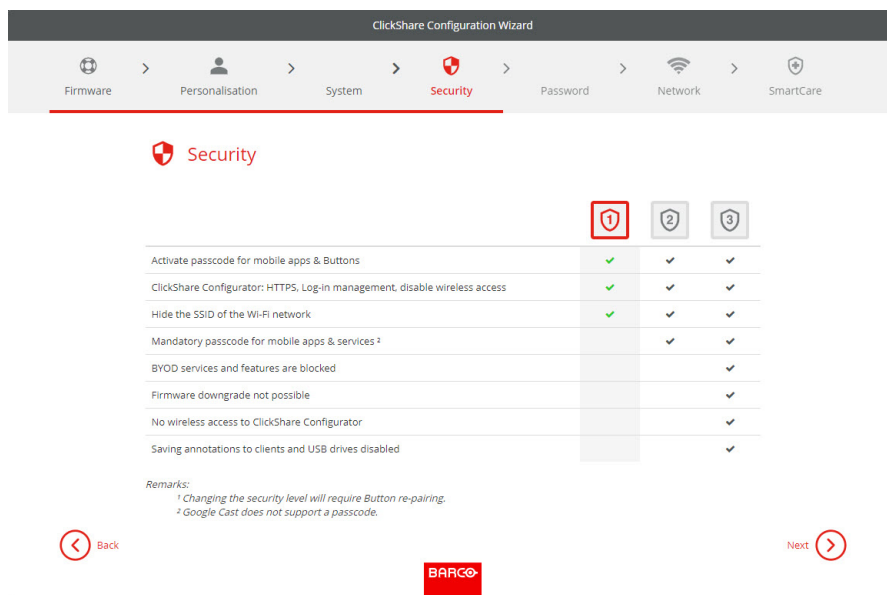


Abbildung 3–17

Legen Sie die gewünschte Sicherheitsstufe fest. Weitere Informationen finden Sie unter [“Sicherheit, Sicherheitsstufe”](#), Seite 113.

7. Passwortänderung

The screenshot shows the 'ClickShare Configuration Wizard' interface. The navigation bar at the top includes 'Firmware', 'Personalisation', 'System', 'Security', 'Password', 'Network', and 'SmartCare'. The 'Password' step is currently active. Below the navigation bar, the title 'Password' is displayed with a lock icon. The main content area contains three input fields: 'ClickShare Configurator Password', 'Current password:', 'New password:', and 'Confirm password:'. Each field is currently empty and masked with dots. At the bottom of the screen, there are 'Back' and 'Next' navigation buttons, and the BARCO logo is centered.

Abbildung 3–18

Wir empfehlen die Änderung des Standardpassworts für den Configurator-Aufruf. Weitere Informationen finden Sie unter [“Sicherheit, Passwörter”](#), Seite 115.

8. Netzwerkeinstellungen

The screenshot shows the 'ClickShare Configuration Wizard' interface. The navigation bar at the top includes 'Firmware', 'Personalisation', 'System', 'Security', 'Password', 'Network', and 'SmartCare'. The 'Network' step is currently active. Below the navigation bar, the title 'Network' is displayed with a Wi-Fi icon. The main content area contains several configuration options: 'Frequency band:' (set to 5 GHz), 'Channel:' (set to 36), 'SSID:' (set to ClickShare-1863550386), a checked 'Broadcast SSID' checkbox, 'New Wi-Fi passphrase:' (with a placeholder 'Enter a new passphrase'), and 'Confirm Wi-Fi passphrase:' (with a placeholder 'Confirm the passphrase'). At the bottom of the screen, there are 'Back' and 'Next' navigation buttons, and the BARCO logo is centered.

Abbildung 3–19

Wählen Sie das Frequenzband, den Kanal und geben Sie nach Bedarf eine WLAN-Passphrase ein. Weitere Informationen finden Sie unter [“WLAN-Einstellungen, Zugriffspunkt-Einstellungen”](#), Seite 88.

9. SmartCare-Registrierung

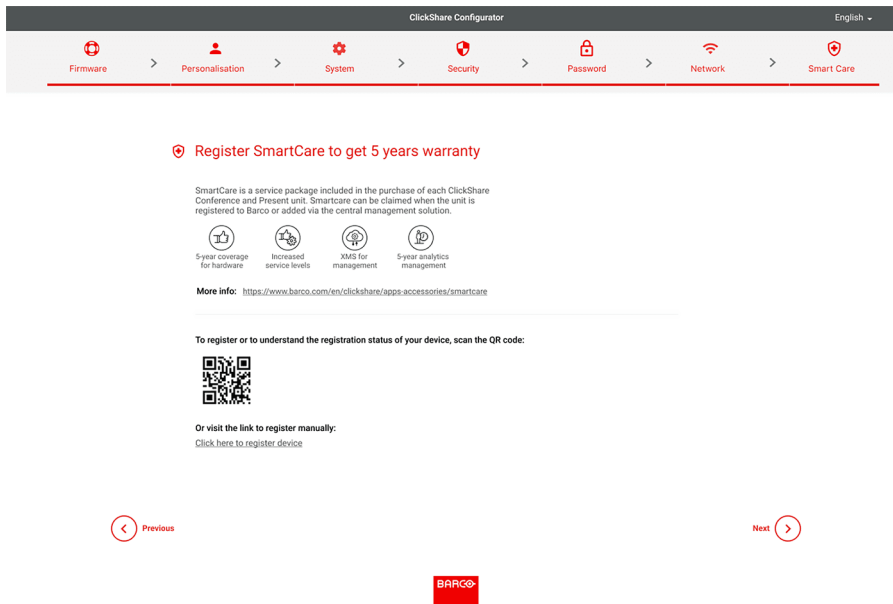


Abbildung 3–20 SmartCare-Seite

Zur Aktivierung von SmartCare ist die Registrierung der Base Unit in XMS Cloud erforderlich. Es gibt zwei Möglichkeiten für die Registrierung in XMS Cloud.

- **Computerregistrierung:** Klicken Sie auf den Link unterhalb des QR-Codes, um den Registrierungsprozess zu starten. Ausführliche Informationen finden Sie unter [“Computer-Onboarding”](#), Seite 50.
- **Mobile Registrierung:** Scannen Sie den QR-Code auf dem Bildschirm oder auf der Karte, die in der Verpackung enthalten ist. Ausführliche Informationen finden Sie unter [“Mobiles Onboarding”](#), Seite 51.

10. Übersichtsseite

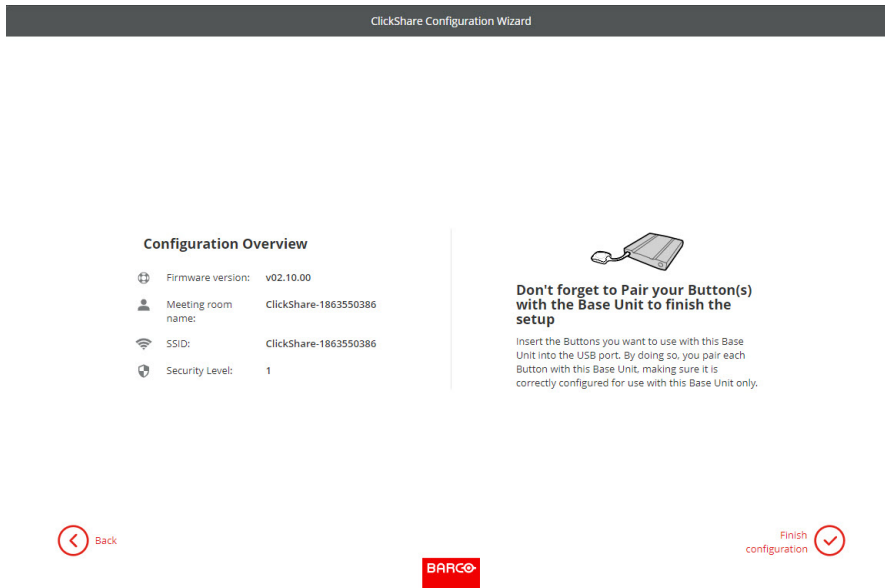


Abbildung 3–21

Bietet eine Übersicht über die aktuelle Konfiguration.

Klicken Sie auf **Konfiguration abschließen (Finish configuration)**. Wenn Ihr Gerät mit dem Internet verbunden ist und die automatische Firmware-Aktualisierung festgelegt wurde, werden eine Software-Prüfung und eine Aktualisierung durchgeführt. Der Configurator startet automatisch mit einer Meldung, dass das Gerät konfiguriert ist.

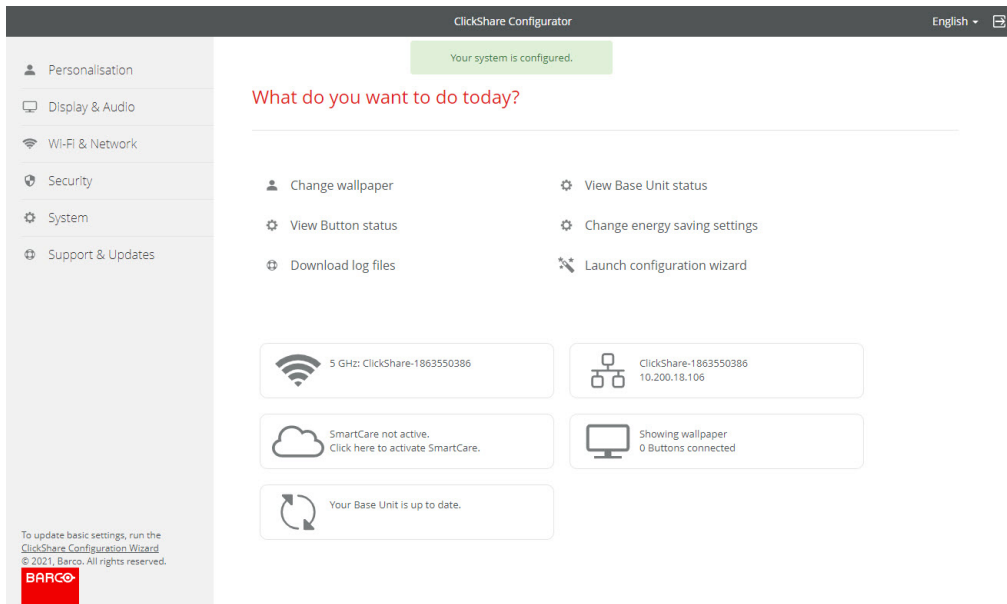


Abbildung 3–22

3.16 XMS Cloud-Registrierung

Infos zur Registrierung

Die Registrierung der Base Unit ermöglicht mehr Kontrolle, mehr verfügbare Funktionen und bietet ein **5-Jahres-SmartCare-Paket**.

Ein SmartCare-Paket enthält:

- 5 Jahre Abdeckung für Hardware
- Erweiterte Service-Ebenen
- XMS für die Verwaltung
- 5 Jahre Analyseverwaltung

Weitere Informationen finden Sie unter <https://www.barco.com/en/clickshare/apps-accessories/smartcare>.

3.16.1 Computer-Onboarding


So führen Sie die Registrierung am Computer durch

1. Klicken Sie auf den Link unterhalb des QR-Codes auf der SmartCare-Seite des Konfigurators.

Abbildung 3–23 Beispiel der Anmeldeseite für die Registrierung auf dem Computer.

Wenn eine Anmeldeseite angezeigt wird, geben Sie die Kontodaten ein und melden Sie sich an, um fortzufahren.

2. Werden die Geräte für einen Kunden installiert?
 - ▶ **Wenn ja**, wählen Sie *Verkäufer/Integrator* aus und erstellen Sie den Kunden, der in XMS Organisation genannt wird, in den unten stehenden Feldern oder wählen Sie ihn aus.
 - ▶ **Wenn nicht**, wählen Sie *Eigentümer/Administrator* aus und erstellen oder wählen Sie einen Namen für die Organisation, in der das Gerät installiert ist.

-  **Tip:** Eine Base Unit kann immer nur für eine Organisation registriert werden. Wenn eine Base Unit auf eine andere Organisation umgestellt werden muss, dann muss die Verknüpfung der Base Unit zuerst aufgehoben werden!

Verfügbare Base Unit(s) werden automatisch gescannt und für die Registrierung vorbereitet.

- Überprüfen Sie die Informationen, um sicherzustellen, dass die richtigen Base Units der richtigen Organisation hinzugefügt werden. Wenn die Informationen korrekt sind, klicken Sie auf **Weiter**.

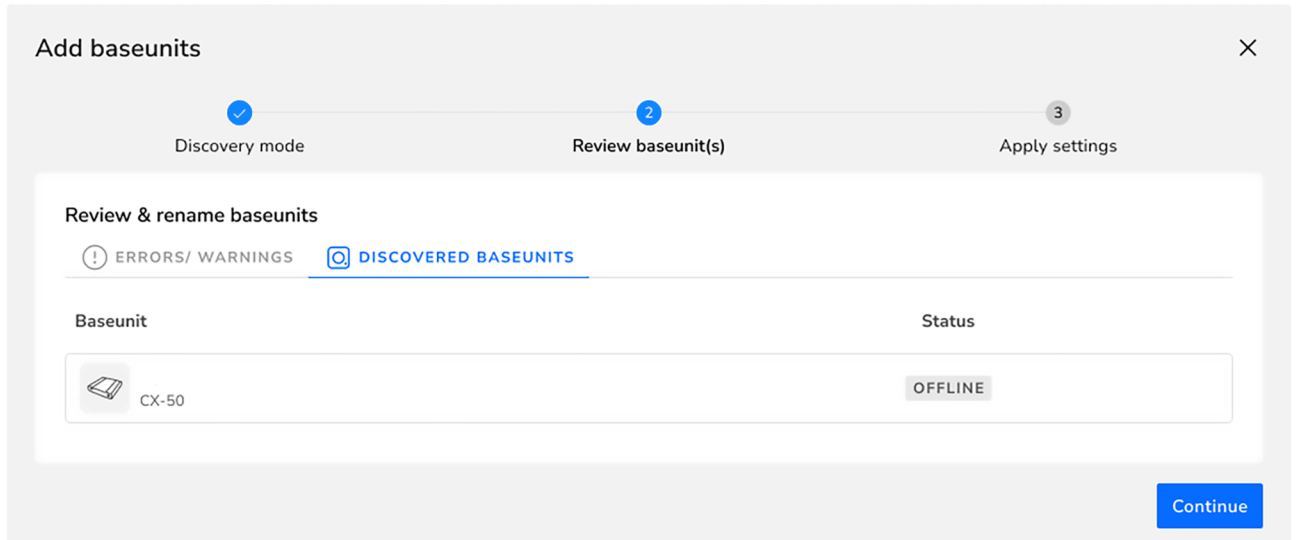


Abbildung 3–24 Beispiel für verknüpfte Base Units

Verbinden Sie die Base Unit mit dem Netzwerk, um das Onboarding abzuschließen.

- Weitere Informationen zur Verwaltung der hinzugefügten Base Unit(s) oder zur Verwendung von XMS Cloud finden Sie im XMS Cloud-Benutzerhandbuch.

3.16.2 Mobiles Onboarding

So registrieren Sie sich auf einem Mobilgerät

- Scannen Sie den QR-Code auf der SmartCare-Seite des Konfigurators oder auf der Karte in der Schachtel.



Abbildung 3–25 Beispiel für die Startseite nach dem Scannen des QR-Codes.

- Werden die Geräte für einen Kunden installiert?
 - ▶ **Wenn ja**, klicken Sie auf *Verkäufer/Integrator*.
 - ▶ **Wenn nicht**, klicken Sie auf *C-5, C-10 Gen2-Eigentümer/Administrator*.



Tip: Eine Base Unit kann immer nur für eine Organisation registriert werden. Wenn eine Base Unit auf eine andere Organisation umgestellt werden muss, dann muss die Verknüpfung der Base Unit zuerst aufgehoben werden!

Die Registrierungsseite wird angezeigt.

3. Klicken Sie auf den Pfeil > oder suchen Sie die gewünschte Organisation in der Liste und klicken Sie auf den Pfeil >.

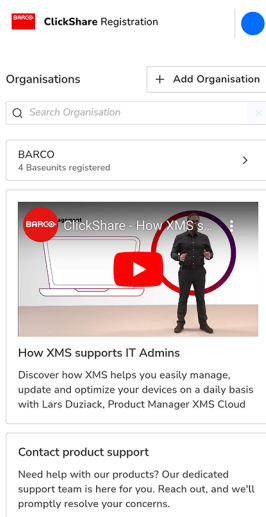


Abbildung 3–26 Beispiel für die Registrierungsseite.

Wenn die gewünschte Organisation nicht in der Liste enthalten ist, gehen Sie wie folgt vor, um eine neue Organisation in XMS zu erstellen.

- a) Klicken Sie auf **+ Organisation hinzufügen**, um eine neue Organisation zu erstellen.
- b) Geben Sie den Namen ein und wählen Sie das entsprechende Land aus.

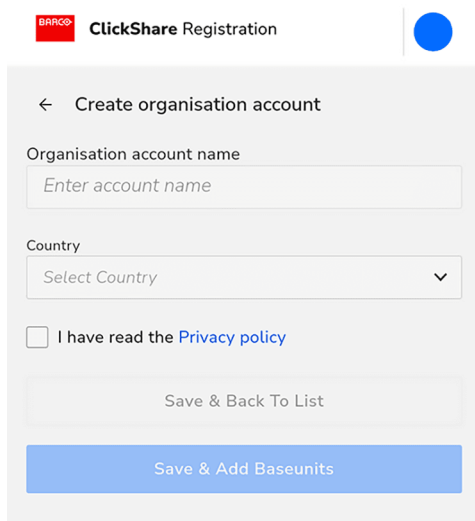


Abbildung 3–27 Beispiel für die Erstellung einer Organisation.

- c) Lesen Sie die **Datenschutzerklärung** und aktivieren Sie das Kontrollkästchen.
- d) Klicken Sie auf **Base Units speichern und hinzufügen**, um die Base Unit mit der neu erstellten Organisation zu verknüpfen, oder klicken Sie auf **Speichern und zurück zur Liste**, um eine weitere Organisation zu erstellen oder eine bestehende auszuwählen.

Es wird ein Überblick über die ausgewählte Organisation angezeigt. Zeigen Sie die derzeit registrierten Base Units an oder verschaffen Sie sich einen schnellen Überblick über die Base Units, die noch auf den Abschluss der Registrierung warten.

4. Klicken Sie auf **Base Unit hinzufügen**, um mit der Registrierung von Geräten zu beginnen.

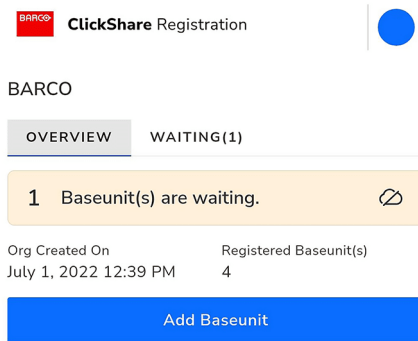


Abbildung 3–28 Beispiel für die Organisationsübersicht.

5. Scannen Sie den QR-Code auf der Unterseite der Base Unit, um sie in XMS Cloud zu registrieren.



Tip: Der Browser muss Zugriff auf die Kamera haben, um die Codes scannen zu können!

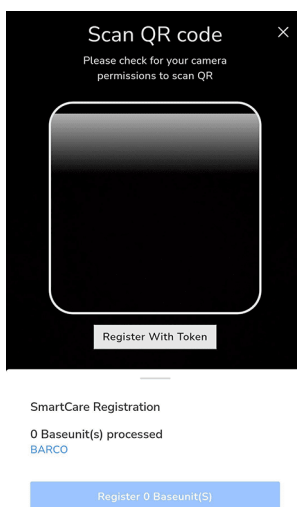


Abbildung 3–29 Beispiel einer Seite zum Scannen von QR-Codes.

Richten Sie die Kamera so aus, dass der gesamte QR-Code in das weiße abgerundete Rechteck passt. Bei Erfolg wird die Base Unit verarbeitet und registriert.

Wenn der QR-Code fehlt oder Schwierigkeiten beim Scannen auftreten, folgen Sie den nachstehenden Schritten, um die Base Unit manuell hinzuzufügen.

- a) Klicken Sie auf die Schaltfläche „Mit Token registrieren“, um die Base Unit manuell hinzuzufügen.

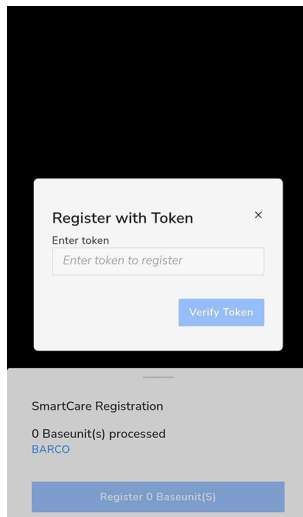


Abbildung 3–30 Beispiel einer manuellen Registrierung mit einem Token.

- b) Geben Sie die Seriennummer der Base Unit ein.
- c) Klicken Sie auf *Token verifizieren*, um die Base Unit zu verarbeiten und zu registrieren.



Tip: Wenn die Kamera- und Token-Registrierung nicht gefunden werden kann, klicken Sie auf + *Weitere hinzufügen*, um sie erneut zu öffnen.

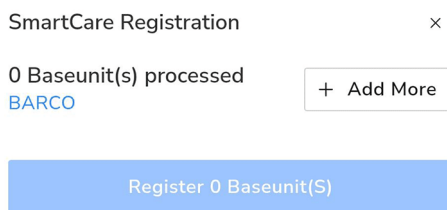


Abbildung 3–31

Wiederholen Sie diese (Teil-)Schritte, bis alle gewünschten Base Units hinzugefügt wurden.

- 6. Überprüfen Sie die Liste der hinzugefügten Base Unit(s) und klicken Sie auf *Base Unit(s) registrieren*.
Es wird ein Pop-up-Fenster angezeigt, in dem darauf hingewiesen wird, dass die Base Unit mit dem Netzwerk verbunden sein muss, um das Onboarding abzuschließen.
- 7. Weitere Informationen zur Verwaltung der hinzugefügten Base Unit(s) oder zur Verwendung von XMS Cloud finden Sie im XMS Cloud-Benutzerhandbuch.

3.17 Aktivieren der Kalenderintegration mit XMS Cloud

Informationen zum Kalender

Durch die Kalenderfunktion können Sie Ihren Raumkalender auf dem Monitor anzeigen, der mit dem ClickShare-Gerät verbunden ist.

Integration von Secure Azure AD

Mit XMS Cloud können Sie die Verfügbarkeit des Besprechungsraums mit ClickShare auf dem Bildschirm anzeigen (optionale Funktion). Dies erfolgt sicher über Azure Enterprise-Anwendungen, die mit Azure AD integriert werden. Um die Sicherheitsrisiken zu mindern, die sich durch die Integration von Azure Enterprise-Anwendungen in Azure AD ergeben, nutzt diese Funktion zwei separate Azure Enterprise-Anwendungen, ClickShare Meeting Room Discovery und ClickShare Calendar Sync. ClickShare Meeting Room Discovery ist eine Anwendung für mehrere Organisationen, während ClickShare Calendar Sync eine Einzelorganisation-Anwendung ist, die nur im Azure AD des Kunden gehostet wird. Die ClickShare Base Units greifen nur über die Einzelorganisation-Anwendung ClickShare Calendar Sync und einen für jeden Kunden eindeutigen und zufälligen Client-Schlüssel auf die Kalender zu. Der Client-Schlüssel wird von Microsoft erstellt und weist folgende Eigenschaften auf: zufällige Generierung, automatischer Ablauf nach 24 Monaten.

Ausführliche Informationen finden Sie im Sicherheits-Whitepaper „XMS Cloud and (Virtual) Edge Security Whitepaper“ von Barco, das Sie auf der Barco-Website herunterladen können.



Überprüfen Sie den Herausgeber (Barco) der Enterprise-Anwendung, bevor Sie diese zu Ihrer Organisation hinzufügen.



Beschränken Sie den Zugriff auf die Enterprise-Anwendung ClickShare Calendar Sync mit einer Anwendungszugriffsrichtlinie in Microsoft Exchange Online auf die erforderlichen Besprechungsräume (und keine anderen Kalender).

Die Rolle des IT-Administrators in diesem Prozess

Um den Abruf des Kalenders auf dem Gerät zu aktivieren, muss XMS Cloud mit Ihrem Microsoft Azure-Konto „verbunden“ sein. Diese „Verbindung“ ermöglicht die Erkennung der Räume und die Freigabe ihrer Anmeldeinformationen für die Geräte. Die Genehmigung der O365-Administratoren Ihres Unternehmens ist erforderlich.

1. Wenden Sie sich vor dem Start der Integration an einen IT-Administrator mit der **globalen Administratorrolle in Azure Active Directory**. Nur diese Art von Konto kann die Integration aktivieren.
2. Fügen Sie die Anmeldeinformationen des IT-Administrators zu der XMS-Organisation hinzu, der Sie den Kalender hinzufügen möchten.
3. Bitten Sie den IT-Administrator, sich bei XMS Cloud anzumelden, die Kalender-Seite aufzurufen und die Schritte im Abschnitt *So erfolgt die Konfiguration* durchzuführen.
4. Nach den Schritten unter „So erfolgt die Konfiguration“ kann der Kunde oder der Integrator mit den Schritten unter *Einem Kalender einen Besprechungsraum zuweisen* fortfahren.

Vor dem Start

Standardmäßig wird das Microsoft Kalender-Plug-in in Ihrer aktuellen Organisation installiert. Ist dies nicht der Fall (oder wurde es manuell entfernt), gehen Sie wie folgt vor, um es wiederherzustellen:

1. Navigieren Sie in XMS Cloud zu *Marktplatz* >> *Kalender* und klicken Sie auf **Details anzeigen**.
2. Klicken Sie im Detailfenster auf **Zu XMS hinzufügen**.

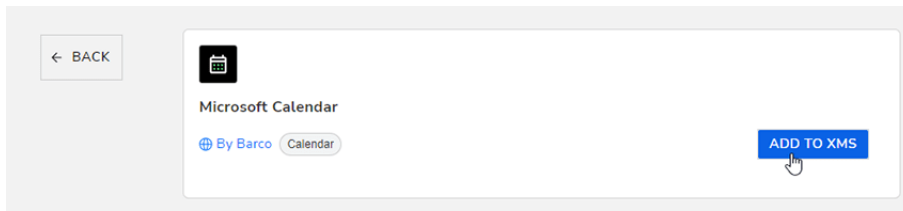


Abbildung 3–32

So richten Sie den Kalender ein (als IT-Administrator)

Die folgenden Aktionen müssen vom IT-Administrator mit einer globalen Administratorrolle in Azure Active Directory durchgeführt werden.

1. Rufen Sie in XMS Cloud die Seite *Marktplatz >> Microsoft Kalender* auf.

Die Kalender-Standardseite wird angezeigt.

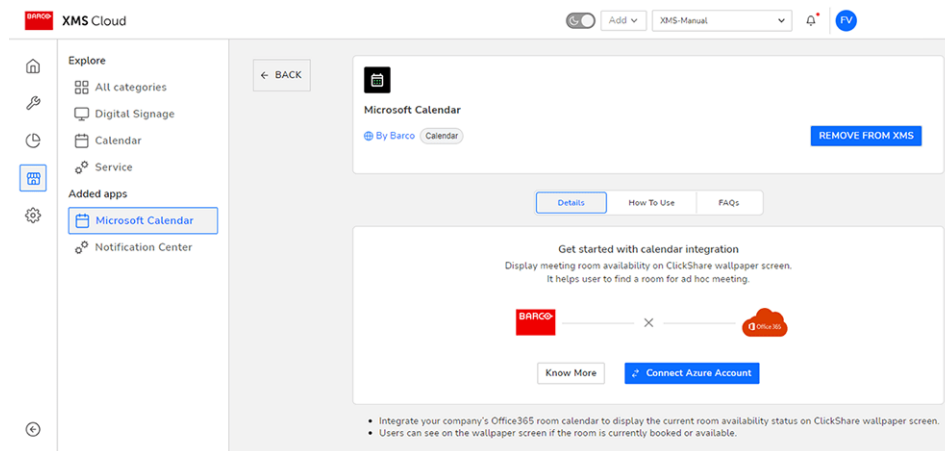


Abbildung 3–33

2. Klicken Sie auf **Azure-Konto verbinden**.

Sie werden zu Ihrem Microsoft Azure-Konto weitergeleitet. Das Microsoft-Anmeldefenster wird angezeigt.

3. Melden Sie sich mit den richtigen Administrator-Anmeldedaten an.

Sobald Sie angemeldet sind, wird der Genehmigungsbildschirm für ClickShare Meeting Room Discovery angezeigt.

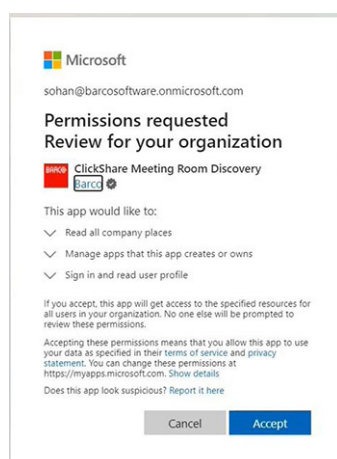


Abbildung 3–34

4. Lesen Sie die Meldung auf dem Bildschirm und klicken Sie auf **Akzeptieren**.

Wenn Sie zugestimmt haben, werden Sie zu XMS Cloud zurückgeleitet und eine Seite, die der folgenden ähnelt, wird angezeigt:

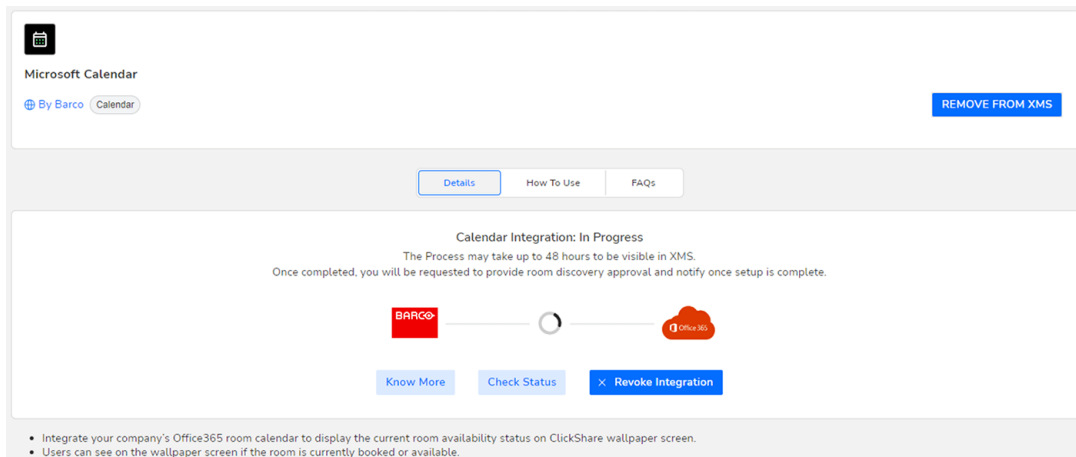


Abbildung 3–35

Dieser Vorgang sollte in 10 bis 30 Minuten abgeschlossen sein. Nur in Ausnahmefällen kann dies länger dauern.

5. Sobald der Prozess abgeschlossen ist, wird der Bildschirm aktualisiert und zeigt die Schaltfläche **Integration fortsetzen an**.

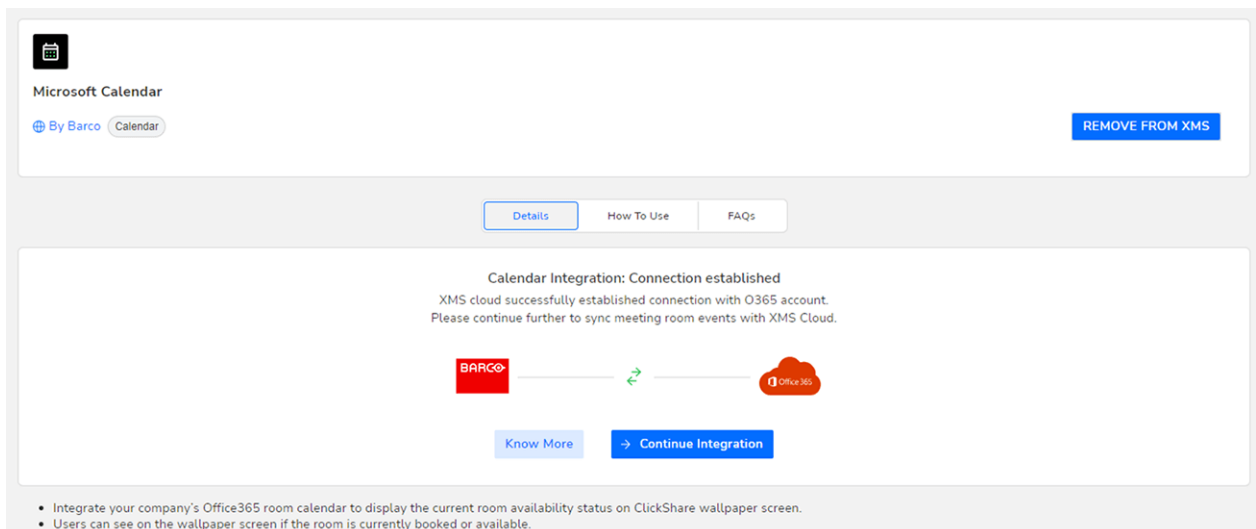


Abbildung 3–36

6. Klicken Sie auf **Integration fortsetzen**, um die endgültige Genehmigung des O365-Administrators zum Lesen der Kalenderinformationen für jedes Raumkonto anzufordern und Anmeldedaten für Geräte zu generieren, um dies zu erreichen.

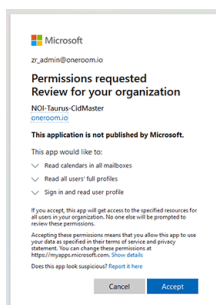


Abbildung 3–37

7. Klicken Sie auf **Akzeptieren**.

Ihre Verbindung mit Microsoft Kalender ist nun aktiv. Der Menüpunkt *Kalender* ist nun auch im Menü *Verwalten* sichtbar.

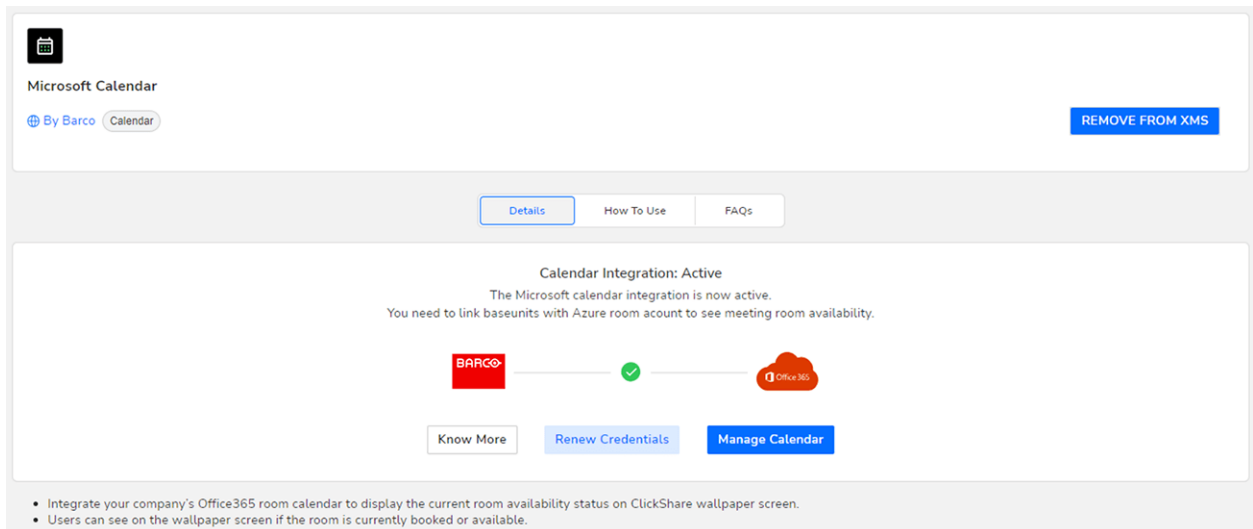


Abbildung 3–38

Um Ihren Kalender-Besprechungsräumen Base Unit-Geräte zuzuweisen, klicken Sie auf **Kalender verwalten**.

Alternativ können Sie auch in XMS Cloud zu *„Verwalten“ >> Kalender* wechseln.

Einem Kalender einen Besprechungsraum zuweisen

1. Wählen Sie auf der Seite „Kalender verwalten“ den gewünschten Besprechungsraum aus und klicken Sie auf **+ Base Unit verknüpfen**.

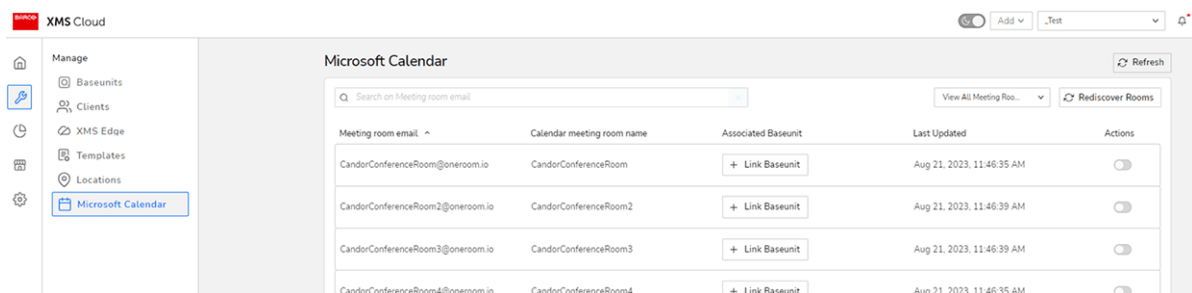


Abbildung 3–39 Beispiel für das Fenster „Kalender verwalten“.

Das Base Unit-Auswahlfenster wird angezeigt.

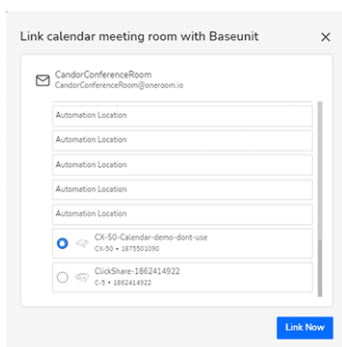


Abbildung 3–40 Beispiel für das Base Unit-Auswahlfenster.

2. Wählen Sie das gewünschte Base Unit-Gerät aus, das mit dem gewählten Besprechungsraum verknüpft werden soll.
3. Klicken Sie auf **Jetzt verknüpfen**.

Das Base Unit-Gerät ist nun mit dem ausgewählten Besprechungsraum verknüpft.

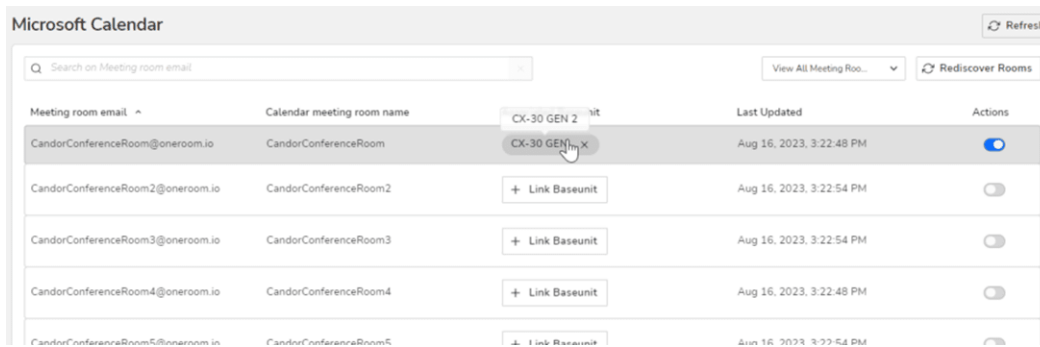


Abbildung 3–41 Beispiel für einen Besprechungsraum, der mit einem Base Unit-Gerät verknüpft ist

4. Wiederholen Sie diesen Vorgang für jeden Besprechungsraum, der über ein ClickShare-Base Unit-Gerät verfügt.

Informationen zu Anmeldeinformationen

Standardmäßig muss der Benutzer nichts gegen ablaufende Anmeldeinformationen tun, da XMS Cloud die Anmeldeinformationen bei einer regelmäßigen Überprüfung der Anmeldeinformationen automatisch erneuert. Wenn sie erneut wurden, gelten die aktualisierten Anmeldeinformationen für die nächsten sechs Monate.

Sie können die Anmeldeinformationen manuell erneuern, indem Sie auf der Seite des Kalender-Plug-ins auf „Anmeldeinformationen erneuern“ klicken.

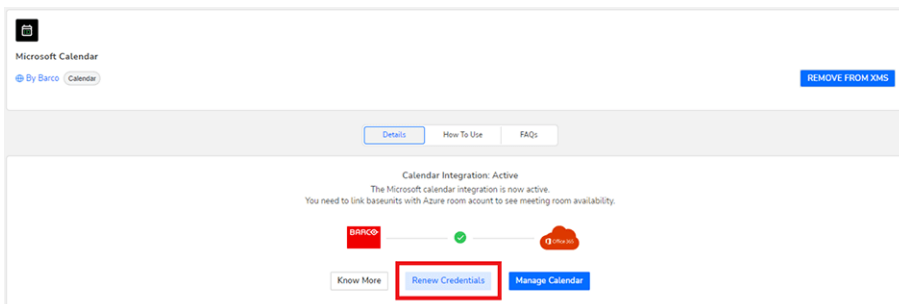


Abbildung 3–42

Vorbereiten der Buttons

4

4.1	Koppeln des Button	62
4.2	ClickShare Extension Pack	63
4.3	Installationsprogramm für das ClickShare Extension Pack	64
4.4	ClickShare Windows-zertifizierter Treiber	66
4.5	ClickShare-Desktop-App	67
4.6	MSI-Installationsprogramm der ClickShare-Desktop-App	68

4.1 Koppeln des Button

Koppeln des Button mit der Base Unit

Um einen Button verwenden zu können, muss dieser der verwendeten Base Unit zugewiesen sein. Dieser Vorgang wird als Koppeln bezeichnet. Jeder Button muss vor der Verwendung aktualisiert und gekoppelt werden.

Wenn Sie zusätzliche Buttons erwerben oder wenn ein Button einer anderen Base Unit zugewiesen werden soll, muss dieser Button (erneut) gekoppelt werden. Die Software der Buttons wird im Hintergrund aktualisiert und hat keine Auswirkungen auf die Benutzer, während sie das System nutzen. Wird die Software der Base Unit auf eine ältere Version herabgestuft oder aktualisiert, müssen die Buttons für eine Softwareaktualisierung manuell gekoppelt werden.



Ein Button kann immer nur mit einer Base Unit gekoppelt werden.
Der Button verbindet sich immer mit der Base Unit, mit der er zuletzt gekoppelt wurde.

So koppeln Sie einen Button mit der Base Unit, indem Sie ihn anschließen

1. Schließen Sie den Button an den USB-C™-Anschluss an, der an der verwendeten Base Unit verfügbar ist.

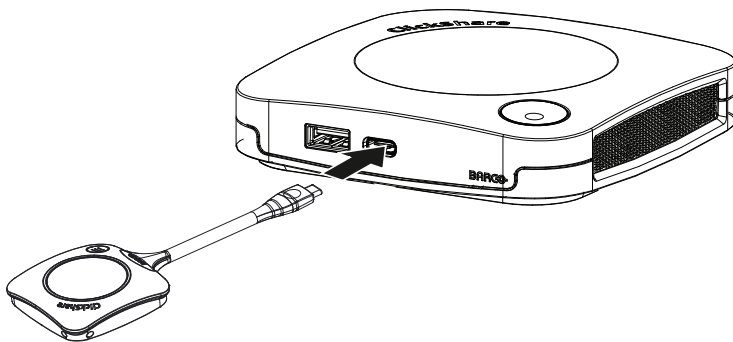


Abbildung 4–1

Die LED der Base Unit blinkt, während sich die kreisförmige LED am Button füllt. Das bedeutet, dass das Koppeln durchgeführt wird.

Die Base Unit überprüft automatisch, ob die Software des Buttons aktuell ist. Falls nicht, aktualisiert die Base Unit die Software des Buttons. Dieser Vorgang kann einige Zeit dauern.

Während des Koppelns und des Aktualisierungsvorgangs wird ein kleiner Verlaufs Balken angezeigt.

Das Koppeln kann zu folgenden Ergebnissen führen:

- Wenn die LEDs am Button grün und an der Base Unit weiß leuchten, ist der Button mit der Base Unit gekoppelt. Sie können den Button von der Base Unit trennen.

2. Trennen Sie den Button von der Base Unit.

Der Button ist jetzt einsatzbereit. Schließen Sie für die Präsentation einen Button an.

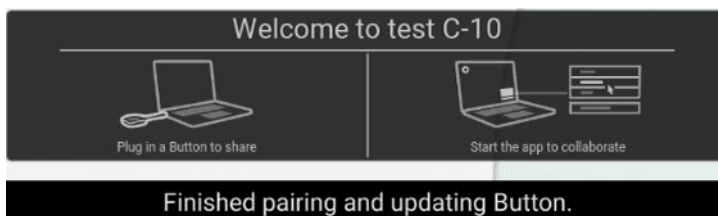


Abbildung 4–2

4.2 ClickShare Extension Pack

Informationen

Das ClickShare Extension Pack ist eine Sammlung von Tools, um Ihr ClickShare-Benutzererlebnis zu erweitern. Dieses Extension Pack enthält den ClickShare-Startprogrammdienst und einen Treiber, um die Erweiterter-Desktop-Funktionalität zu aktivieren (nur für Windows). Beide Tools werden standardmäßig installiert. Um das Standardverhalten des Installationsprogramms zu ändern, muss das Installationsprogramm mit Befehlszeilenparametern ausgeführt werden.

Das ClickShare Extension Pack kann manuell vom Endbenutzer installiert, auf dem Laptop-Abbild Ihres Unternehmens vorinstalliert oder über SCCM oder andere Tools unternehmensübergreifend bereitgestellt werden.

Das ClickShare Extension Pack kann in Kombination mit einem Button und/oder der ClickShare-Desktop-App verwendet werden.

Das aktuelle Extension Pack können Sie unter <http://www.barco.com/en/product/clickshare-extension-pack> herunterladen.

4.3 Installationsprogramm für das ClickShare Extension Pack

Interaktive Konfiguration

Bei dieser Konfiguration führt der Benutzer das Installationsprogramm aus, das das ClickShare Extension Pack auf dem Computer installiert, nachdem der Benutzer der EULA zugestimmt hat.

Nach Fertigstellung der Konfiguration startet das ClickShare-Startprogramm automatisch. Der Erweiterer-Desktop-Treiber kann erst verwendet werden, nachdem der Benutzer den Computer neu gestartet hat.

Starten der Konfiguration

1. Laden Sie das ClickShare Extension Pack herunter (Download über <http://www.barco.com/en/product/clickshare-extension-pack>).
2. Extrahieren Sie die heruntergeladene Datei.
3. Klicken Sie auf *ClickShare-Extension-Pack.msi*, um die Installation zu starten.

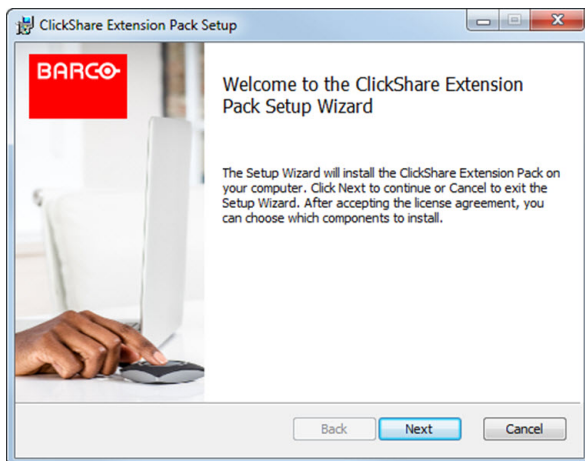


Abbildung 4–3

4. Klicken Sie auf **Weiter**, akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**, um fortzufahren.

Befolgen Sie bei Bedarf die Anweisungen auf dem Bildschirm.

Automatische Installation

Bei dieser Konfiguration kann ein Benutzer oder ein IT-Admin das ClickShare Extension Pack über die Windows-Eingabeaufforderung installieren. Die folgende Beschreibung dient als Beispiel für eine automatische Installation (Versionsnummern werden hier lediglich zu Beispielszwecken benutzt. Die aktuellste Version ist grundsätzlich auf der Website von Barco verfügbar):

Installation nur mit Startprogramm:

```
msiexec. exe /i ClickShare-Extension-Pack-01.00.02.0003. msi ACCEPT_EULA=YES
INSTALLFOLDER=C:\ LAUNCH_APP=YES /qn
```

Installation nur mit erweitertem Desktop:

```
msiexec. exe /i ClickShare-Extension-Pack-01.00.02.0003. msi ACCEPT_EULA=YES
ADDLOCAL=ExtendedDesktopDriverFeature INSTALLFOLDER=C:\ LAUNCH_APP=YES /qn
```

Vollständige Installation (Startprogramm und erweiterter Desktop):

```
msiexec. exe /i ClickShare-Extension-Pack-01.00.02.0003. msi ACCEPT_EULA=YES
ADDLOCAL=ALL INSTALLFOLDER=C:\ LAUNCH_APP=YES /qn
```



Der Computer startet neu. Dies kann mit /norestart unterdrückt werden. Damit die Erweiterter-Desktop-Funktion einsatzbereit ist, ist nach der Installation ein Neustart erforderlich. Falls der Endbenutzer entscheiden soll, ob er einen Neustart durchführen möchte, kann /promptrestart /QB!+ verwendet werden (grundlegende Benutzerschnittstelle, keine Abbrechen-Option sondern eine Eingabeaufforderung zum Neustart).

Parameterbeschreibung

ACCEPT_EULA	Dieser Parameter gibt an, dass das Installationsprogramm den Text der Endbenutzerlizenzvereinbarung unverändert akzeptiert. Dieser Parameter muss auf JA festgelegt werden, um mit der Installation fortfahren zu können.
INSTALLFOLDER	Diese Parameter legen das Installationsverzeichnis für das ClickShare-Startprogramm fest. Falls kein Ordner festgelegt wird, ist der Ordner „Programmdateien“ der Standardordner.
LAUNCH_APP	Ist dieser Parameter auf JA eingestellt, wird das ClickShare-Startprogramm sofort nach Fertigstellung der Installation gestartet. Falls nicht, wird die Startprogramm-Anwendung nicht gestartet.
/qn	Dieser Parameter gibt an, dass die Installation im automatischen Modus durchgeführt wird, d. h. während des Installationsvorgangs werden keine sichtbaren Fenster angezeigt.
ADDLOCAL	Dieser Parameter gibt die Art der Installation an. Wenn kein Parameter ergänzt wird, wird nur das Startprogramm installiert.

Windows-Umgebungsvariable

Die zu verwendende Variable ist CLICKSHARE_LAUNCHER_CLIENT_PATH. Der Wert sollte der Pfad zur Client-Software sein.

4.4 ClickShare Windows-zertifizierter Treiber

Info

Der ClickShare Windows-zertifizierte Treiber wird automatisch installiert, wenn Sie einen Button an einen Windows-Computer anschließen.

Dieser Windows-Treiber startet automatisch die ausführbare Datei auf dem Button.

Beachten Sie, dass für die Unterstützung von Buttons mit Firmware-Version 4.10 oder höher mindestens Version **1.20.0** erforderlich ist. Wenn eine ältere Version auf dem Computer installiert ist, starten Sie Windows-Update und *prüfen Sie auf Updates*, während der Button mit dem Computer verbunden ist. Unter Windows 7, 8 und 8.1 muss der Treiber manuell heruntergeladen und installiert werden.

4.5 ClickShare-Desktop-App

Info

Wenn die ClickShare-Desktop-App auf Ihrem Computer installiert ist, können Sie einen Konferenzraum betreten und innerhalb von wenigen Sekunden Bilder auf dem Bildschirm anzeigen, ohne dass Sie einen Button anschließen müssen. Die ClickShare-Desktop-App kann in Kombination mit einem Button verwendet werden.

Die ClickShare-Desktop-App verbindet sich mit dem Konferenzraum-Bildschirm, um Ihre Inhalte zu teilen. Dafür wird Präsenzerkennungstechnologie verwendet. Die ClickShare-Desktop-App verwenden Präsenzerkennungstechnologien, um zu bestimmen, welcher Konferenzraum der nächstgelegene für den Benutzer ist. Klicken Sie einfach auf den Namen des Konferenzraums. Das bedeutet, dass Sie niemals eine IP-Adresse eingeben oder durch lange Listen mit Konferenzräumen scrollen müssen, bevor Sie sich mit Ihrem Konferenzraum verbinden können. Dies ist noch einfacher, wenn die PresentSense-Funktionalität verwendet wird. Betreten Sie einfach einen Besprechungsraum und klicken Sie auf **Verbinden**.

Wenn Sie Outlook für die Tagesordnung verwenden, erhalten Sie auch eine sofortige Übersicht über Ihre nächsten Besprechungen. Sie müssen nicht in Outlook nach dem Termin oder der Einladung suchen. Klicken Sie einfach auf **Beitreten**, um Ihrer Konferenz beizutreten.

Montage

Wenn die ClickShare-Desktop-App in Ihrer IT-Umgebung nicht bereits bereitgestellt wurde, können Sie sie von www.clickshare.app herunterladen und ohne Administratorrechte installieren. Für die Installation der ClickShare-Desktop-App mit der Funktion Kalenderintegration sind Administratorrechte erforderlich. Weitere Informationen zum MSI-Installationsprogramm finden Sie unter "[MSI-Installationsprogramm der ClickShare-Desktop-App](#)", Seite 68.

4.6 MSI-Installationsprogramm der ClickShare-Desktop-App



ACHTUNG: Die Installation kann nur mit Administratorrechten durchgeführt werden.



Bevor Sie das Installationsprogramm für die ClickShare-Desktop-App ausführen, müssen Sie alle vorherigen Installationen der ClickShare-App auf dem Computer deinstallieren.

Vorgehen bei der Installation

1. Laden Sie das MSI-Installationsprogramm von www.clickshare.app herunter.
2. Führen Sie das MSI-Installationsprogramm aus, indem Sie auf die heruntergeladene Datei doppelklicken.

Der Installationsassistent wird gestartet. Befolgen Sie die in den verschiedenen Fenstern angezeigten Anweisungen.

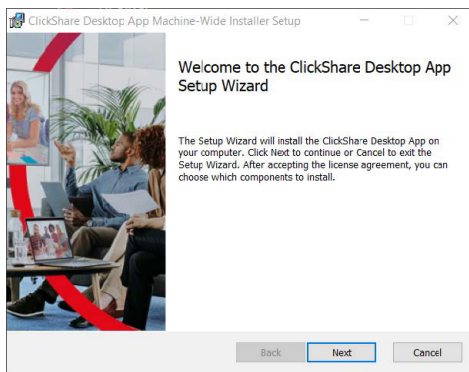


Abbildung 4-4

3. Lesen die Lizenzvereinbarung und aktivieren Sie das Kontrollkästchen „Ich akzeptiere die Lizenzvereinbarung“, um fortzufahren.

Tippen Sie auf **Weiter**.

4. Aktivieren Sie die notwendigen Komponenten und klicken Sie auf **Installieren**.

Die ClickShare-Desktop-App und die ausgewählten Funktionen sind jetzt für alle Benutzer des Computers verfügbar.

C-5, C-10 Gen2 Configurator

5

5.1	Zugriff auf den Configurator	71
5.2	ClickShare-Konfigurationsassistent	75
5.3	Bildschirm-ID-Informationen	77
5.4	Personalisierung, Hintergrundbild	79
5.5	Personalisierung, personalisiertes Hintergrundbild	81
5.6	Verwalten der Konfigurationsdateien	83
5.7	Anzeige- und Audio-Einrichtung	85
5.8	Peripheriegeräte	86
5.9	Wi-Fi-Einstellungen	87
5.10	WLAN-Einstellungen, Zugriffspunkt-Einstellungen	88
5.11	Wi-Fi-Einstellungen, Drahtlosclient	91
5.12	Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS	92
5.13	Wi-Fi-Einstellungen, Drahtlosclient, EAP-TTLS	95
5.14	Wi-Fi-Einstellungen, Drahtlosclient, PEAP	96
5.15	Wi-Fi-Einstellungen, Drahtlosclient, WPA2-PSK	98
5.16	LAN-Einstellungen	99
5.17	LAN-Einstellungen, kabelgebundene Authentifizierung	102
5.18	LAN-Einstellungen, Sicherheitsmodus EAP-TLS	103
5.19	LAN-Einstellungen, Sicherheitsmodus EAP-TTLS	106
5.20	Services, mobile Geräte	108
5.21	Dienst, PresentSense	110
5.22	Dienst, ClickShare API, Fernbedienung über API	111
5.23	Dienste, SNMP	112
5.24	Sicherheit, Sicherheitsstufe	113
5.25	Sicherheit, Passwörter	115
5.26	Sicherheit, HTTP-Verschlüsselung	116
5.27	Statusinformationen Base Unit	118
5.28	Manuelles Festlegen von Datum und Uhrzeit	119
5.29	Festlegen von Datum und Uhrzeit, Zeit-Server	121
5.30	Energiesparen	122
5.31	Buttons	124
5.32	Buttons, externer Zugriffspunkt, EAP-TLS-Modus	125
5.33	Buttons, externer Zugriffspunkt, EAP-TTLS-Modus	127
5.34	Buttons, externer Zugriffspunkt, PEAP-Modus	128
5.35	Buttons, externer Zugriffspunkt, WPA2-PSK-Modus	129
5.36	Blackboard	130
5.37	XMS Cloud-Integration	131
5.38	Firmware-Aktualisierung	133
5.39	Support und Updates, Fehlersuche, Protokolleinstellungen	135
5.40	Fehlerbehebung, Alle Einstellungen löschen	136
5.41	Auf Werkseinstellungen zurücksetzen	137
5.42	Fehlersuche, Diagnose	138

Informationen zur Konfiguration

Die Konfiguration des Geräts ist auf folgende Arten möglich:

- XMS Cloud
- den lokalen Configurator

Der Configurator in XMS Cloud wird (auf lange Sicht) ausgefeilter sein als der lokale Configurator. Daher sollten Sie Ihre Geräte vorzugsweise über XMS Cloud konfigurieren. Weitere Informationen finden Sie in der XMS-Dokumentation.

Die nächsten Themen beschreiben den lokalen Configurator.



In einigen Menüs wird der *Configurator* als *WebUI* angezeigt. Zum Beispiel ist WebUI-Passwort das Passwort, um den Configurator aufzurufen.

5.1 Zugriff auf den Configurator

Zugriff auf den Configurator

Es gibt drei Möglichkeiten, um auf den Configurator zuzugreifen:

- Über das LAN
- Direkte Ethernet-Verbindung zwischen Computer und Base Unit.
- Über das drahtlose Netzwerk der Base Unit

Beim ersten Zugriff auf den Configurator wird der ClickShare-Konfigurationsassistent automatisch gestartet.


Der Konfigurationsassistent kann jederzeit zum Ändern der Konfiguration gestartet werden, wodurch die Verwendung der Menüs vermieden wird.

So greifen Sie über das LAN auf den Configurator zu

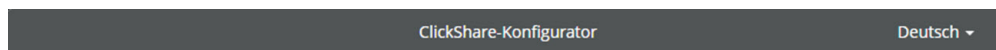
1. Öffnen Sie einen Browser.

 *Hinweis:* Die Browser Microsoft Edge, Firefox, Google Chrome und Safari werden unterstützt.

2. Rufen Sie die IP-Adresse des Geräts auf.

 *Hinweis:* Wenn Sie die IP-Adresse nicht kennen, da *Info zu Netzwerk anzeigen* deaktiviert ist, stellen Sie die Verbindung über eine Direktverbindung oder über eine Drahtlosverbindung zu dem Gerät her, um die verkabelte IP-Adresse zu ermitteln.

Ein Anmeldebildschirm wird angezeigt.



Am ClickShare-Konfigurator anmelden

Benutzername:

Passwort:

Daten merken

Ich habe die [EULA](#) und [Datenschutzerklärung](#) gelesen und akzeptiere sie

© 2019, Barco. All rights reserved.



Abbildung 5–1 Anmeldebildschirm

3. Klicken Sie zum Ändern der Sprache auf das Dropdown-Listenfeld neben der aktuellen Sprache, und wählen Sie die gewünschte Sprache für den Configurator aus.

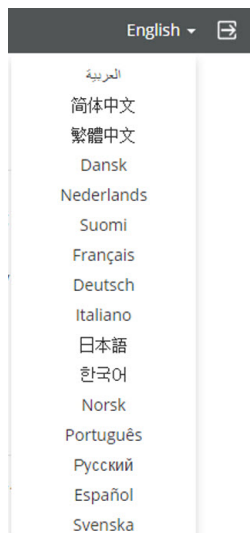


Abbildung 5–2 Configurator-Sprachen

Folgende Sprachen stehen zur Auswahl:

- Arabisch
- Vereinfachtes Chinesisch
- Traditionelles Chinesisch
- Dänisch
- Niederländisch
- Englisch
- Finnisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Koreanisch
- Norwegisch
- Portugiesisch
- Russisch
- Spanisch
- Schwedisch

Die Configurator-Sprache wird in die gewählte Sprache geändert.

4. Geben Sie den Benutzernamen „admin“ und das Kennwort ein, lesen und akzeptieren Sie die Endbenutzerlizenzvereinbarung (EULA) und die Datenschutzrichtlinie und klicken Sie auf **OK**.

Standardmäßig ist „admin“ als Kennwort eingestellt.

Warnung: Es wird dringend empfohlen, das Standardkennwort bei der ersten Verwendung in ein starkes Kennwort zu ändern, um zu verhindern, dass andere Personen, die auf den Configurator zugreifen, die Einstellungen der ClickShare-Base Unit ändern können. Siehe Abschnitt „Sicherheit, Passwörter“.

Der Configurator wird geöffnet.



Abbildung 5–3 Startbildschirm

Die Sprache des Configurator kann auf jeder Seite der Benutzeroberfläche geändert werden.

Der Bildschirm ist in zwei Fenster geteilt. Das linke Fenster mit den Auswahltasten und das rechte Fenster zur Konfiguration der ausgewählten Funktion.

Im Startbildschirm wird Folgendes angezeigt:

- die verdrahtete IP-Adresse
- die drahtlose SSID
- die Anzahl der verbundenen Buttons
- der Systemstatus
- der SmartCare-Status

Jedes dieser Felder bietet auch eine direkte Verknüpfung mit der beschriebenen Funktion.



Wenn Sie die IP-Adresse nicht finden können (z. B. wenn kein Monitor verfügbar ist), sollten Sie Ihren Laptop über ein gekreuztes Ethernet-Kabel direkt mit der Base Unit verbinden und über die feste IP-Adresse 192.168.1.23 auf die Webschnittstelle zugreifen. Stellen Sie sicher, dass Ihr eigener LAN-Adapter auf den Bereich 192.168.1.x festgelegt ist.

So greifen Sie über eine direkte Verbindung auf den Configurator zu.

1. Verbinden Sie Ihren Laptop über ein Ethernet-Kabel mit der Base Unit.
2. Öffnen Sie einen Browser auf Ihrem Laptop.



Hinweis: Die Browser Microsoft Edge, Firefox und Safari werden unterstützt.

3. Rufen Sie <http://192.168.1.23> auf.


Ein Anmeldebildschirm wird angezeigt.

4. Geben Sie den Benutzernamen „admin“ und das Kennwort ein, lesen und akzeptieren Sie die Endbenutzerlizenzvereinbarung und klicken Sie auf **OK**.

Standardmäßig ist „admin“ als Kennwort festgelegt.

Der Configurator wird geöffnet. Die verkabelte IP-Adresse wird auf der Startseite angezeigt.

So greifen Sie über das drahtlose Netzwerk der Base Unit auf den Configurator zu

1. Verbinden Sie Ihren Laptop mit dem drahtlosen Netzwerk der Base Unit.
Die Standard-SSID für das Verbinden mit der Base Unit lautet „ClickShare-<Basis-Seriennummer>“ und das Kennwort „clickshare“.
2. Öffnen Sie einen Browser auf Ihrem Laptop.
 *Hinweis:* Die Browser Microsoft Edge, Firefox und Safari werden unterstützt.
3. Rufen Sie <http://192.168.2.1> auf.
Ein Anmeldebildschirm wird angezeigt.
4. Geben Sie den Benutzernamen „admin“ und das Kennwort ein, lesen und akzeptieren Sie die Endbenutzerlizenzvereinbarung und klicken Sie auf **OK**.
Standardmäßig ist „admin“ als Kennwort festgelegt.
Der Configurator wird geöffnet. Die verkabelte IP-Adresse wird auf der Startseite angezeigt.



Das 5-GHz-Frequenzband wird möglicherweise von älteren Laptopmodellen nicht unterstützt. Falls Ihre Base Unit auf diesen Frequenzbereich eingestellt ist, können sich diese Geräte nicht über das drahtlose Netzwerk mit der Base Unit verbinden.

Funktionsübersicht

Gruppe	Funktion
Personalisierung	Bildschirm-ID
	Hintergrundbild
	Konfigurationsdateien
Anzeige und Audio	Anzeige und Audio
	Peripheriegeräte
Wi-Fi und Netzwerk	Wi-Fi-Einstellungen
	LAN-Einstellungen
	Dienstleistungen
Sicherheit	Sicherheitsstufen
	Passwörter
System	Base Unit-Status
	Datum und Uhrzeit
	Energiesparen
	Buttons
	Blackboard
Support und Updates	XMS
	Firmware
	Fehlersuche

5.2 ClickShare-Konfigurationsassistent



Dieses Verfahren entspricht dem Onboarding-Vorgang.

Informationen zum Konfigurationsassistenten

Während des ersten Starts der Base Unit wird der Konfigurationsassistent automatisch gestartet.

Sie können den Konfigurationsassistenten auch starten, indem Sie unten links auf **Konfigurationsassistent** klicken oder auf der Dashboard-Seite auf „Konfigurationsassistent starten“.



Abbildung 5–4 Konfigurationsassistent, Start

Alle für die Konfiguration der Base Unit notwendigen Grundeinstellungen werden über diesen Konfigurationsassistenten eingerichtet. Sobald der Konfigurationsassistent abgeschlossen ist, ist die Base Unit einsatzbereit.

Die Begrüßungsseite gibt auch an, an welchem Datum die Garantie beginnt. Standardmäßig liegt dieser Zeitraum bei einem Jahr und kann durch die Registrierung des Geräts verlängert werden.

 Der Zeitraum für die 1-Jahr-Standardgarantie des ClickShare-Geräts begann am
22. November 2019
Stellen Sie sicher, dass Sie sich für SmartCare registrieren, um Ihre Garantie auf **5 Jahre zu verlängern!**

Willkommen beim ClickShare-Konfigurationsassistenten

Dieser Assistent leitet Sie durch einige Schritte, um Ihre ClickShare Base Unit zu konfigurieren.
Klicken Sie auf "Konfiguration starten", um zu beginnen.


Konfiguration
starten 



Abbildung 5–5 Konfiguration-Begrüßungsseite

Klicken Sie auf **Konfiguration starten**.

Füllen Sie die erforderlichen Elemente aus und klicken Sie auf **Weiter**, um fortzufahren.

Um zum vorherigen Schritt zurückzukehren, klicken Sie auf **Zurück**.

Weitere Informationen zu speziellen Themen finden Sie in den jeweiligen Kapiteln.

Der ClickShare-Konfigurationsassistent kann jederzeit gestartet werden, um die aktuelle Konfiguration zu ändern. Dies erfolgt durch einen Klick auf **ClickShare-Konfigurationsassistent** am linken unteren Rand eines jeden Bildschirms oder auf *Konfigurationsassistent starten* auf der Startseite.

Firmware	Firmware-Aktualisierung – automatisch	Siehe "Firmware-Aktualisierung" , Seite 133
	Firmware-Aktualisierung – manuell	
Personalisierung	Sprache von On-Screen-Texten	Siehe "Bildschirm-ID-Informationen" , Seite 77.
	Name des Besprechungsraums, Standort des Besprechungsraums und Willkommensnachricht	Siehe "Bildschirm-ID-Informationen" , Seite 77.
System	Zeitzone, manuelle Zeiteinstellung	Siehe "Manuelles Festlegen von Datum und Uhrzeit" , Seite 119.
	NTP verwenden	Siehe "Festlegen von Datum und Uhrzeit, Zeit-Server" , Seite 121.
Sicherheit	Stufeneinstellungen	Siehe "Sicherheit, Sicherheitsstufe" , Seite 113.
Kennwort	ClickShare Configurator-Passwort	Siehe "Sicherheit, Passwörter" , Seite 115.
Netzwerk	Frequenzband, Kanal, WiFi-Passphrase	Siehe "WLAN-Einstellungen, Zugriffspunkt-Einstellungen" , Seite 88.
SmartCare für ClickShare	Registrieren des Geräts zum Erhalten des SmartCare-Pakets	Siehe "XMS Cloud-Registrierung" , Seite 50.

5.3 Bildschirm-ID-Informationen

Informationen zur Geräteidentifizierung

Die folgenden Elemente können gesendet werden:

- Bildschirmsprache Unabhängig von der Configurator-Sprache.
- Besprechungsraumname
- Standort des Besprechungsraums
- Willkommensnachricht, die im Konferenzraum angezeigt wird
- Anzeige der Netzwerkinformationen
 - Aktiviert: LAN-Informationen wie z. B. die kabelgebundene IP-Adresse werden angezeigt. Die Wi-Fi-IP-Adresse und SSID werden ebenfalls angezeigt.
 - Nicht aktiviert: Es werden keine LAN- oder Wi-Fi-Informationen angezeigt (Standardkonfiguration).
- Kinomodus aktivieren
 - Aktiviert: Der gesamte Bildschirm wird für die Inhaltsfreigabe verwendet. Es wird keine Statusleiste mehr angezeigt. Die Statusleiste wird angezeigt, um Statusänderungen, Benachrichtigungen, den Pin-Code usw. anzuzeigen, und wird dann wieder ausgeblendet. Ohne Touchscreens können Sie die Statusleiste über ein „Tag“ aufrufen, um die Notation- und Wandtafel-Funktion zu starten.
 - Deaktiviert: Die Statusleiste verbleibt auf dem Bildschirm.

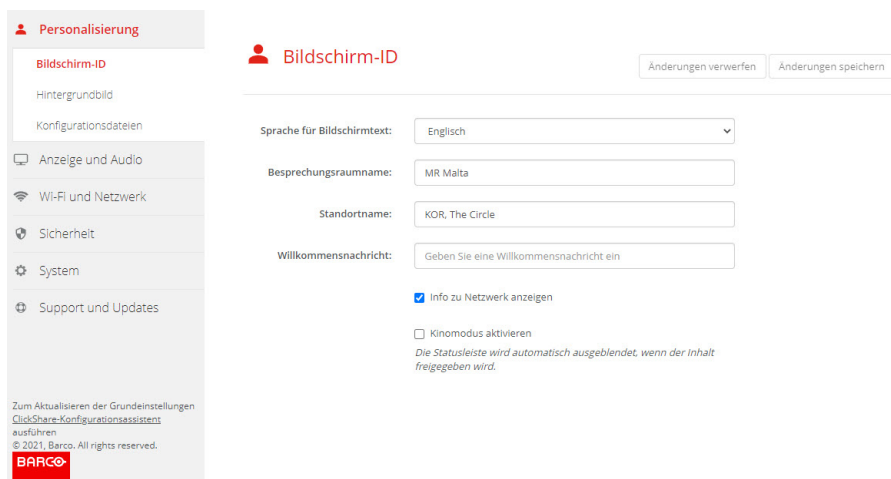


Abbildung 5–6 Bildschirm-ID

Bildschirm-Sprachauswahl

1. Melden Sie sich bei Configurator an.
2. Klicken Sie auf *Personalisierung* → *Bildschirm-ID*.
3. Wahl der gewünschten Sprache des On-Screen-Textes. Klicken Sie auf das Dropdown-Listenfeld neben *Sprache für Bildschirmtext* und wählen Sie die gewünschte Sprache aus.

Folgende Sprachen stehen zur Auswahl:

- Arabisch
- Vereinfachtes Chinesisch
- Traditionelles Chinesisch
- Dänisch
- Niederländisch
- Englisch
- Finnisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Koreanisch
- Norwegisch

- Portugiesisch
- Russisch
- Spanisch
- Schwedisch

Name des Besprechungsraums, Standort und Willkommensnachricht

1. Melden Sie sich bei Configurator an.
2. Klicken Sie auf *Personalisierung* → *Bildschirm-ID*.
3. Klicken Sie auf das Eingabefeld neben *Besprechungsraumname* und geben Sie einen Namen für den Besprechungsraum ein.

Dieser Text wird auf dem Gerät angezeigt, wenn der Button freigegeben werden kann („Bereit zur Anzeige auf...“), auf dem zentralen, mit der Base Unit verbundenen Bildschirm und in der Liste der AirPlay-Empfänger auf dem iOS-Gerät des Benutzers.

4. Klicken Sie auf das Eingabefeld neben *Standortname* und geben Sie einen Standort ein.
5. Klicken Sie auf das Eingabefeld neben *Willkommensnachricht* und geben Sie die gewünschte Nachricht ein.

5.4 Personalisierung, Hintergrundbild

Informationen zum Hintergrundbild

Beim Start von C-5, C-10 Gen2 wird ein Hintergrundbild angezeigt. Die Anzeige des Hintergrundbilds kann deaktiviert werden.

Standardmäßig sind zwei allgemeine ClickShare-Hintergrundbilder verfügbar. Es können auch persönliche Hintergrundbilder hochgeladen werden. Die Standardhintergrundbilder können aus dem System gelöscht werden.

Auswahl des Hintergrundbildes

1. Bei Configurator anmelden
2. Klicken Sie auf *Personalisierung* → *Hintergrundbild*.

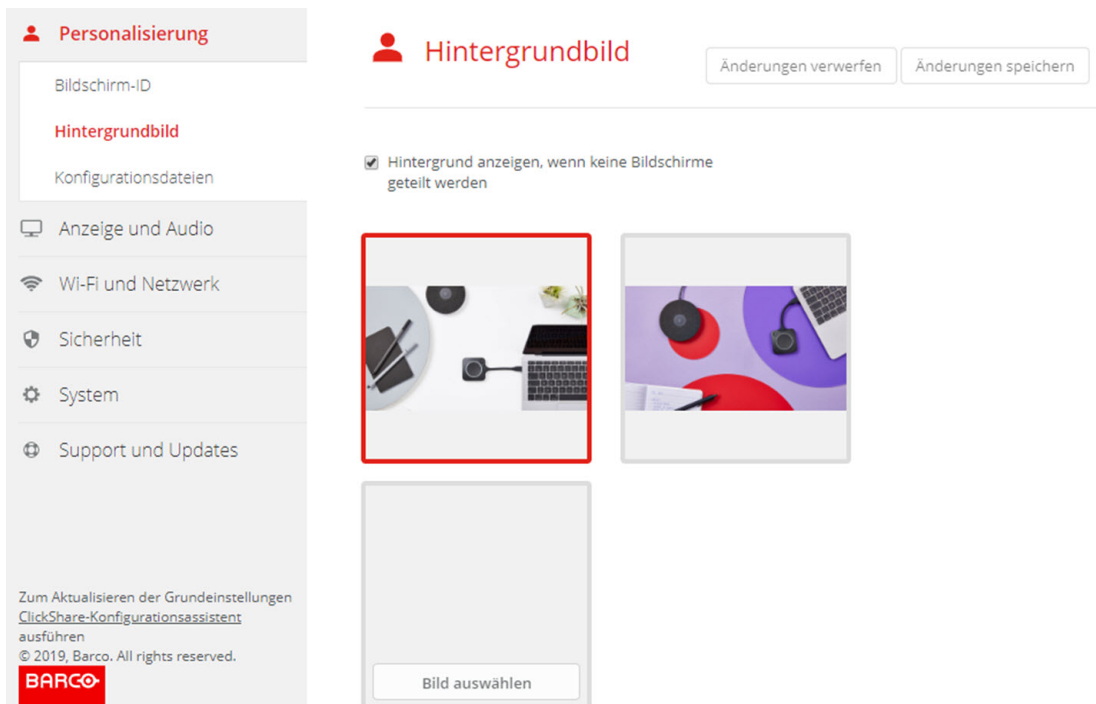


Abbildung 5–7 Auswahl des Hintergrundbildes

Das Auswahlfenster *Hintergrundbild* wird angezeigt. Das aktuell ausgewählte Hintergrundbild wird mit einer roten Umrandung angezeigt.

3. Wählen Sie eines der verfügbaren Hintergrundbilder aus und klicken Sie auf **Änderungen speichern**.

Hinweis: Standardmäßig sind zwei allgemeine Barco-Hintergrundbilder verfügbar. Diese werden automatisch entsprechend dem Seitenverhältnis des Bildschirms skaliert.

Das ausgewählte Hintergrundbild wird mit einer roten Umrandung angezeigt.

Die Nachricht **Erfolgreich angewandte Änderungen** wird im Fenster der Hintergrundbild-Auswahl oben angezeigt.



Sie können auch ein persönliches Hintergrundbild hinzufügen, z. B. Ihr Firmenlogo. Weitere Informationen zum Hinzufügen eines neuen Hintergrundbildes zu der Liste finden Sie unter ["Personalisierung, personalisiertes Hintergrundbild"](#), Seite 81.

Herunterladen des Hintergrundbildes

1. Bewegen Sie den Mauszeiger über das Hintergrundbild, das heruntergeladen werden soll, und klicken rechts oben Sie auf das Symbol zum Herunterladen.



Abbildung 5–8 Herunterladen des Hintergrundbilds

Das Hintergrundbild wird auf den PC heruntergeladen.

Aktivieren und Deaktivieren des Hintergrundbilds

1. Aktivieren Sie im Fenster für das Hintergrundbild das Kontrollkästchen *Hintergrundbild anzeigen, wenn keine Bildschirme geteilt werden*.

Aktiviert: Hintergrundbild wird angezeigt, wenn keine Inhalte geteilt werden.

Nicht aktiviert: Hintergrundbild wird nicht angezeigt, wenn keine Inhalte geteilt werden. Die Videoausgabe der Base Unit wird deaktiviert, wenn keine Inhalte geteilt werden. Diese Funktion ist besonders dann praktisch, wenn die Base Unit in ein Raumsystem integriert ist, wie zum Beispiel in ein Cisco-Videokonferenzsystem, Microsoft Teams-Raumsystem oder ein Zoom-Raumsystem.

5.5 Personalisierung, personalisiertes Hintergrundbild

Vorgehensweise beim Hochladen

1. Bei Configurator anmelden
2. Klicken Sie auf *Personalisierung* → *Hintergrundbild*.

Das Auswahlfenster *Hintergrundbild* wird angezeigt. Das aktuell ausgewählte Hintergrundbild wird mit einer roten Umrandung angezeigt.

3. Bewegen Sie den Mauszeiger über die freie Stelle und klicken Sie **Bild auswählen**.

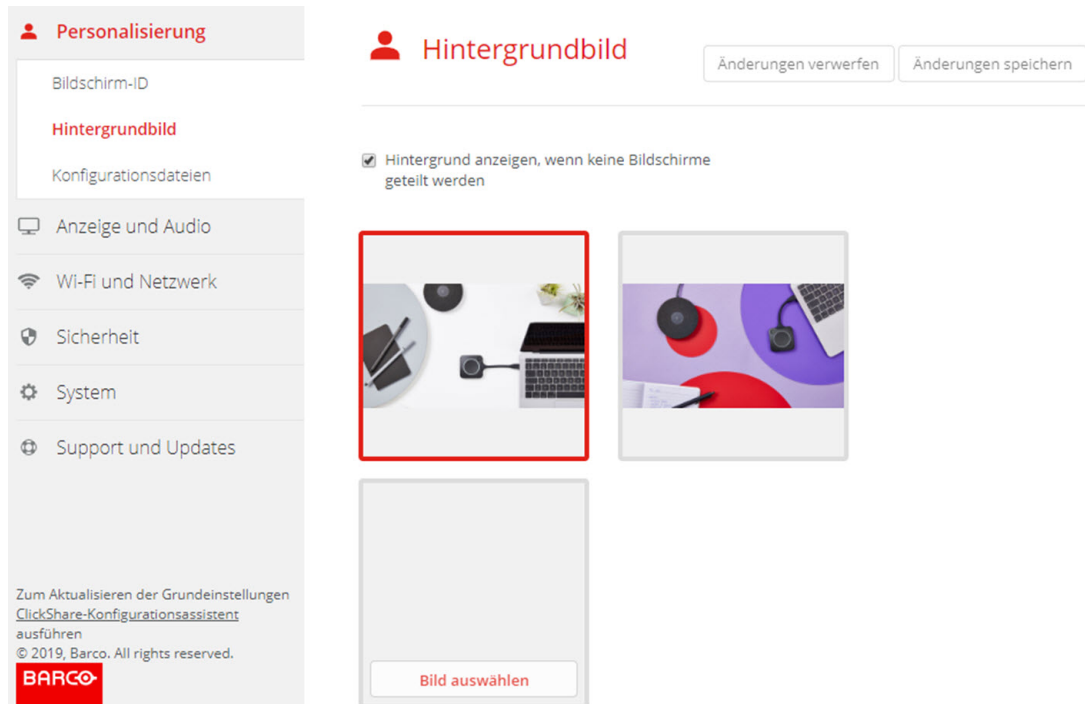


Abbildung 5–9 Auswahl des personalisierten Hintergrundbilds

Ein Browserfenster wird angezeigt.

4. Suchen Sie nach dem gewünschten Bild, und klicken Sie auf „Öffnen“, um das Bild zu laden.
Der Inhalt der Datei wird überprüft und bei gültigem Format und gültiger Größe wird die Datei hochgeladen. Das neue Hintergrundbild wird rot umrandet.
5. Klicken Sie auf **Änderungen speichern**, um das personalisierte Hintergrundbild zu übernehmen.
Die Nachricht **Erfolgreich angewandte Änderungen** wird oben auf der Seite angezeigt.

Ändern des personalisierten Bilds

1. Klicken Sie auf *Personalisierung* → *Hintergrundbild*.
2. Bewegen Sie den Mauszeiger über die freie Stelle und klicken Sie **Bild ändern**.

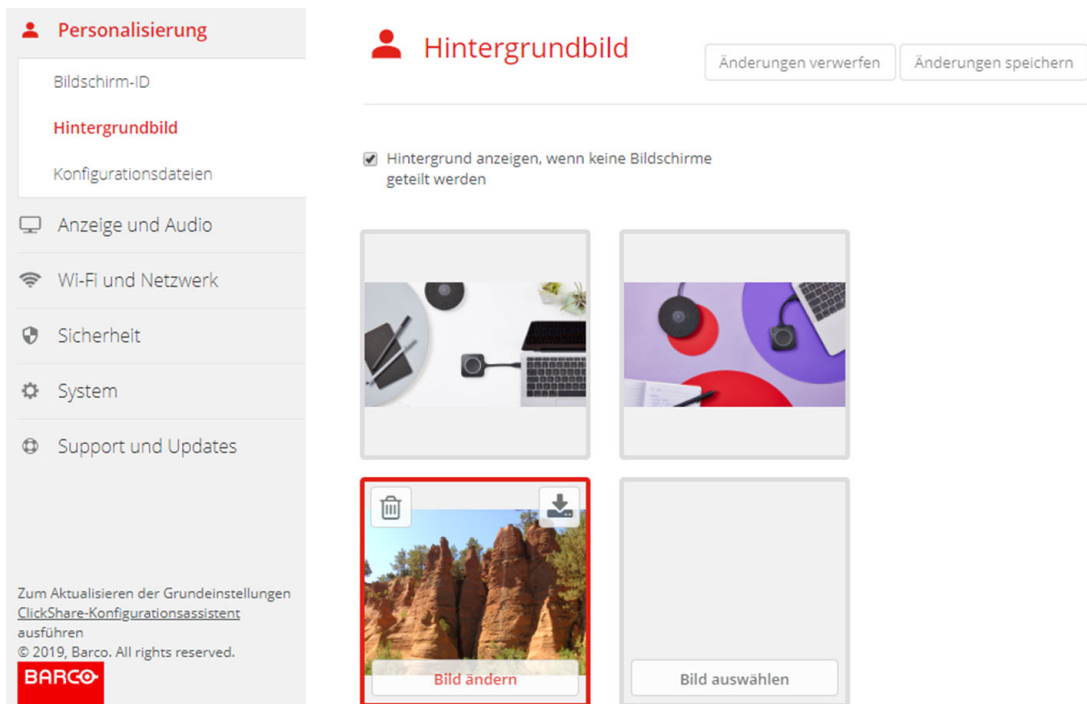


Abbildung 5–10 Bild ändern

3. Suchen Sie nach dem gewünschten Bild, und klicken Sie auf „Öffnen“, um das Bild zu laden. Der Inhalt der Datei wird überprüft und bei gültigem Format und gültiger Größe wird die Datei hochgeladen. Das neue Hintergrundbild wird rot umrandet.
4. Klicken Sie auf **Änderungen speichern**, um das personalisierte Hintergrundbild zu übernehmen und die vorherige Datei zu ersetzen.
Die Nachricht **Erfolgreich angewandte Änderungen** wird oben auf der Seite angezeigt.

Löschen des personalisierten Hintergrundbilds

1. Bewegen Sie den Mauszeiger über das aktuelle Bild und klicken Sie auf den Papierkorb, um das Bild zu löschen.

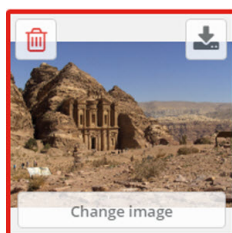


Abbildung 5–11 Löschen des Hintergrundbilds

Das personalisierte Hintergrundbild wird gelöscht und das Standardhintergrundbild wird aktiviert.

5.6 Verwalten der Konfigurationsdateien

Informationen zum Verwalten der Konfigurationsdateien

Eine vollständige Sicherung kann heruntergeladen, aber nicht für die Duplizierung der Konfigurationseinstellungen auf anderen Base Units verwendet werden. Daher kann eine übertragbare Version heruntergeladen werden. Diese übertragbare Version kann über die Schaltfläche „Konfiguration hochladen“ auf die anderen Base Units (selber Typ) geladen werden. Über dieselbe Schaltfläche kann auch die vollständige Sicherung auf die Original-Base Unit hochgeladen werden.

Eine übertragbare Sicherung umfasst Folgendes:

- Hintergrundbilder
- Hintergrundbildeinstellungen
- Anmelde-Einstellungen
- Alle Anzeige-Einstellungen
- Sprache Bildschirmmenü
- Standort
- Willkommensnachricht
- Wi-Fi-Kanal
- Wi-Fi-Frequenz

So verwalten Sie die Konfigurationsdateien

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Personalisierung* → *Konfigurationsdateien*.

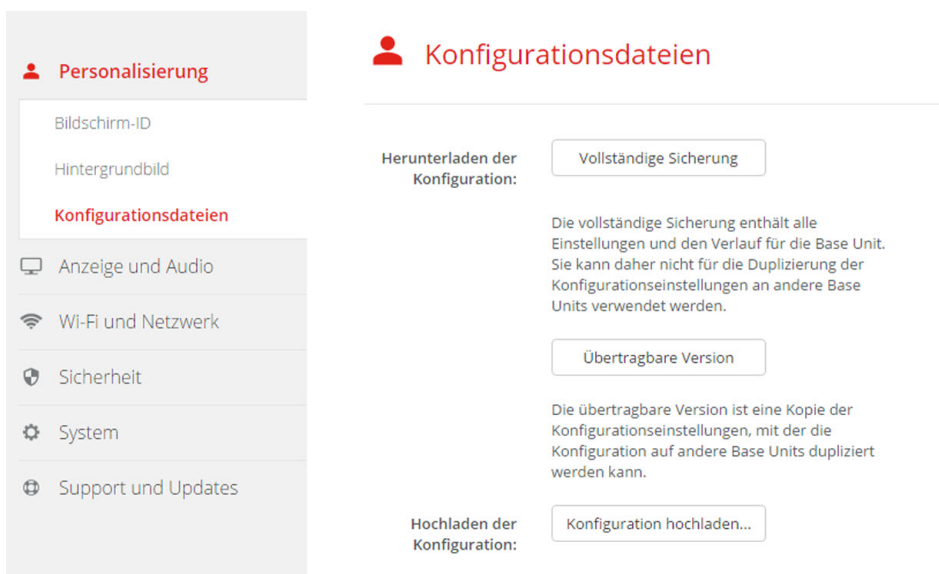


Abbildung 5–12 Konfigurationsdateien

3. Klicken Sie auf **Vollständige Sicherung**, um eine vollständige Sicherung herunterzuladen.
Es wird eine xml-Datei mit allen Informationen und dem Verlauf heruntergeladen. Diese Datei kann nur auf derselben Base Unit wiederverwendet werden.
4. Klicken Sie auf **Übertragbare Version**, um eine übertragbare Version herunterzuladen.
Eine xml-Datei, die übertragbare Informationen enthält, mit denen Einstellungen auf eine weitere Base Unit dupliziert werden können.
5. Klicken Sie auf **Konfiguration hochladen**, um eine Konfiguration hochzuladen.
Ein Browserfenster wird angezeigt. Navigieren Sie zu der hochzuladenden Datei (xml-Datei) und klicken Sie auf **Öffnen**, um sie hochzuladen.
Eine vollständige Sicherung kann auf die Base Unit hochgeladen werden, auf der die Sicherung erstellt wurde. Eine übertragbare Version kann auf eine beliebige Base Unit (selbes Modell) hochgeladen werden.



Beim Hochladen einer Konfigurationsdatei geht der Verlauf der Softwareaktualisierungen und der gekoppelten Buttons verloren. Gekoppelte Buttons bleiben weiterhin funktionsfähig, wenn die SSID oder das Wireless-Kennwort der Base Unit nicht geändert wurden.

5.7 Anzeige- und Audio-Einrichtung

Auflösung

Die Ausgabeauflösung des Monitors ist auf „Automatisch“ eingestellt. Das bedeutet, dass die C-5, C-10 Gen2-Ausgabeauflösung automatisch an die Auflösung des Monitors angepasst wird. Für HDMI-Monitore ist eine Hot Plug-Erkennung verfügbar.

Wenn ein Monitor an den Ausgang angeschlossen ist, werden Modell und Anbieter angezeigt.

Wenn kein Monitor angeschlossen ist, wird die Anzeige *Nicht verbunden* neben *Anzeige-Ausgang* angezeigt.

CEC

Consumer Electronics Control (CEC) ist eine Funktion von HDMI, die es Benutzern ermöglichen soll, Geräte, die über HDMI angeschlossen sind, über nur eine Fernbedienung zu steuern und zu kontrollieren.

Aktivieren Sie das Kontrollkästchen neben *CEC aktivieren*, um CEC zu aktivieren.

Wenn *Anzeige-Ausgang DisplayPort* ist, wird diese CEC nicht unterstützt. Die folgende Meldung wird angezeigt: *Die aktuelle Verbindung (DisplayPort) unterstützt kein CEC.*

Audio

Aktivieren oder deaktivieren Sie den Audioausgang.

Aktivieren Sie das Kontrollkästchen vor „Audio aktivieren“, um die Audioausgabe zu aktivieren.

Einrichtung des Bildschirmschoners

1. Melden Sie sich bei *Configurator* an.

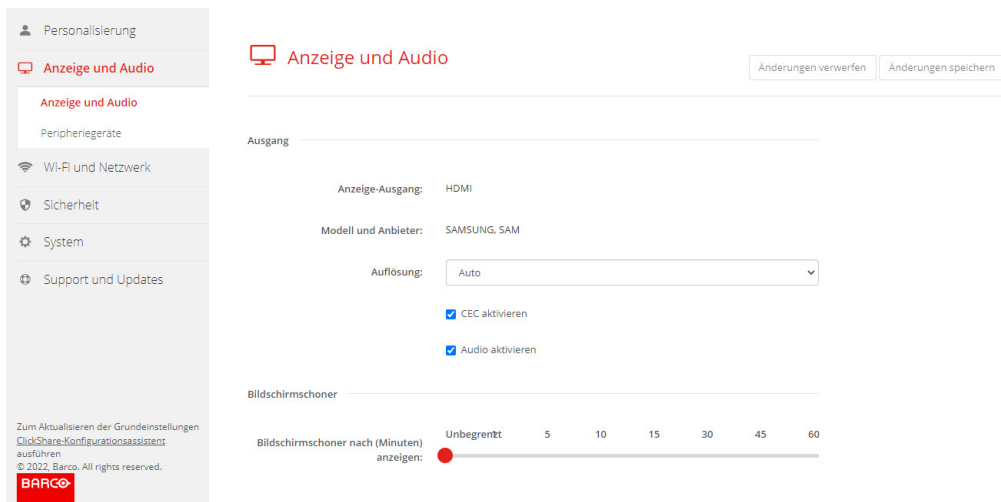


Abbildung 5–13

2. Klicken Sie auf *Anzeige und Audio* → *Anzeige und Audio*.
3. Für die Aktivierung des Bildschirmschoners müssen Sie den Schieberegler nach links oder rechts auf der Leiste verschieben, bis die gewünschte Verzögerungszeit erreicht ist.

Wenn der Schieberegler vollständig nach links geschoben ist, wird der Bildschirmschoner nie aktiviert.

4. Tippen Sie auf **Änderungen speichern**.

5.8 Peripheriegeräte

Übersicht

Im Peripheriegeräte-Bereich finden Sie Informationen zum Lautsprecher.

So rufen Sie die Seite auf

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Anzeige und Audio* → *Peripheriegeräte*.

Die Informationen zum Lautsprecher werden angezeigt.

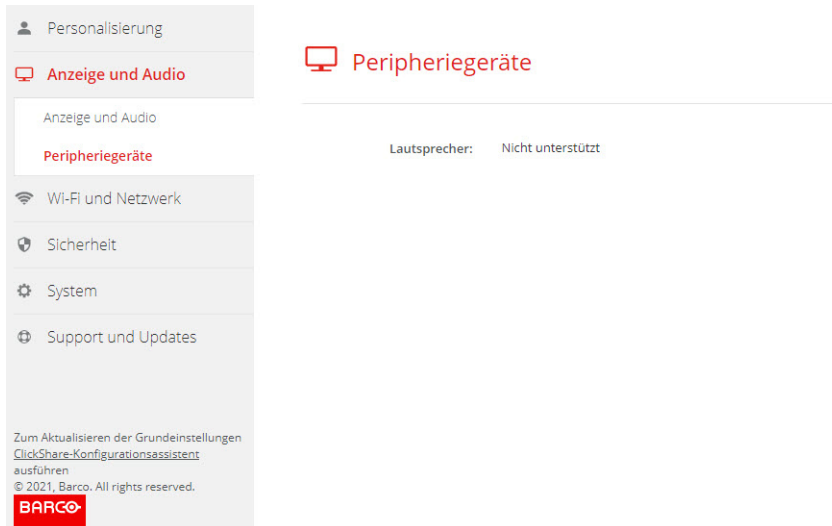


Abbildung 5–14

5.9 Wi-Fi-Einstellungen



WARNUNG: Es ist nicht gestattet, die Base Unit außerhalb der für sie vorgesehenen geografischen Region zu verwenden.

Info

Der Betriebsmodus der Wi-Fi-Einstellung kann auf drei verschiedene Modi eingestellt werden:

- Zugriffspunkt
- Drahtlos-Client
- Aus

Ändern des Betriebsmodus

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Wi-Fi und Netzwerk* → *Wi-Fi-Einstellungen*.

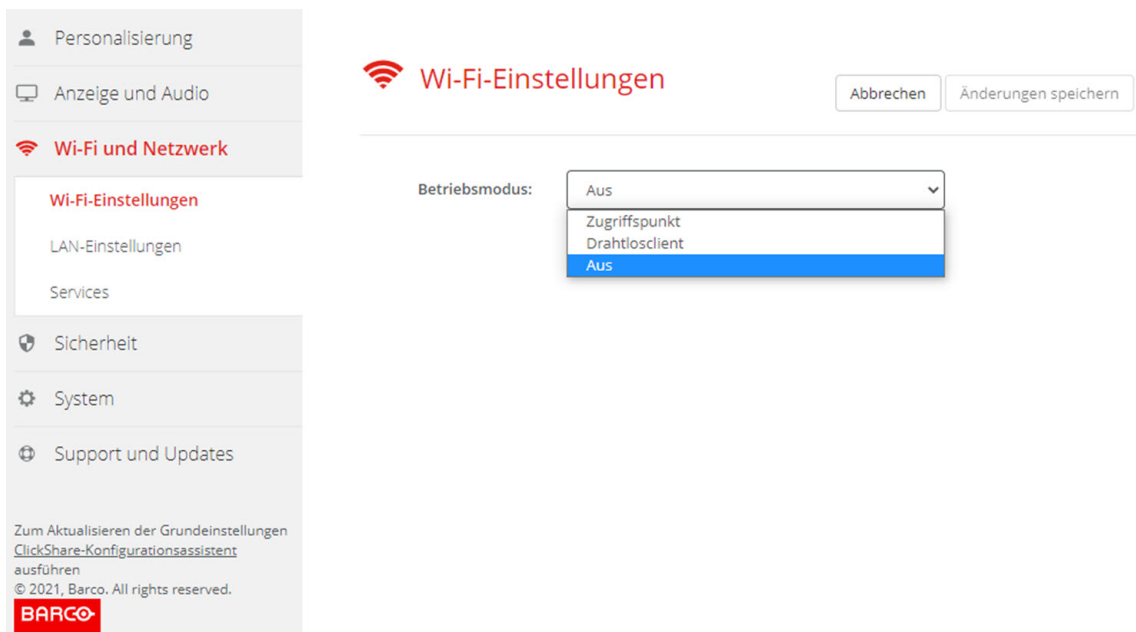


Abbildung 5–15 Wi-Fi-Einstellungen

3. Wählen Sie den Betriebsmodus, indem Sie auf das Dropdown-Listenfeld klicken und die gewünschte Option auswählen.

Folgende Optionen sind möglich:

- Zugriffspunkt
- Drahtlos-Client
- Aus

4. Um die Zugriffspunkt-Einstellungen zu ändern, wählen Sie „Zugriffspunkt“ aus.
Ausführliche Informationen finden Sie unter [“WLAN-Einstellungen, Zugriffspunkt-Einstellungen”](#), Seite 88.
5. Um die Drahtlosclient-Einstellungen zu ändern, wählen Sie „Drahtlosclient“.
Ausführliche Informationen finden Sie unter [“Wi-Fi-Einstellungen, Drahtlosclient”](#), Seite 91.

5.10 WLAN-Einstellungen, Zugriffspunkt-Einstellungen

So nehmen Sie eine Änderung vor

1. Aktivieren Sie das Kontrollkästchen neben der Option *Aktivieren*.

Aktiviert: Die Zugriffspunkt-Einstellungen sind aktiviert. Alle aktuellen Einstellungen können geändert werden.

Deaktiviert: Die Zugriffspunkt-Einstellungen sind deaktiviert.

2. Geben Sie bei Bedarf eine neue Wi-Fi-Passphrase ein und bestätigen Sie diese.

Abbildung 5–16 WLAN-Einstellungen, Zugriffspunkt-Einstellungen

3. Geben Sie einen öffentlichen Namen (SSID) für das drahtlose Netzwerk ein.
Die Standard-SSID lautet *ClickShare-<Seriennummer der Base Unit>*.
4. Wenn Sie diese SSID übertragen möchten, aktivieren Sie das Kontrollkästchen vor *SSID-Übertragung aktivieren*.

Informationen zur Auswahl des Frequenzbandes und des Kanals

In einer idealen Konfiguration sollten für zwei ClickShare Base Units, die sich innerhalb der Reichweite der anderen befinden, keine sich überschneidenden Kanäle verwendet werden. Da sich die Kanäle im 2,4-GHz-Band überschneiden, ist ein bewährtes Verfahren, die Kanäle 1, 6 und 11 auf einer Etage zu verwenden. Auf den Etagen darüber und darunter wird das Kanalmuster verschoben, um eine Überschneidung zwischen den Etagen zu vermeiden, indem zum Beispiel Kanal 6 in der Mitte des dargestellten Musters platziert wird.

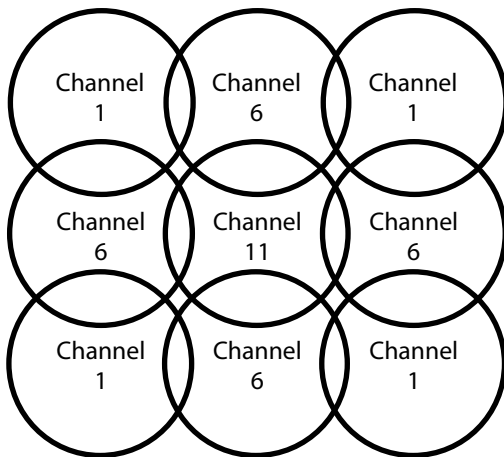


Abbildung 5–17

Die 5-GHz-Kanäle überschneiden sich nicht und werden von Nicht-WiFi-Geräten seltener als die 2,4-GHz-Kanäle verwendet. Des Weiteren werden 5-GHz-Signale stärker gedämpft als 2,4-GHz-Signale. Daher wird die Verwendung eines 5-GHz-Kanals empfohlen. Damit verringert sich die Auswirkung des ClickShare-Systems auf andere installierte ClickShare-Einheiten und andere WLAN-Benutzer.

Frequenzband- und Kanalauswahl

1. Wählen Sie den Kanal für die Drahtlosverbindung, indem Sie auf das Dropdown-Listenfeld klicken und den gewünschten Kanal auswählen.

Die verfügbaren Kanäle in der Liste variieren entsprechend der regionalen Version Ihrer Base Unit. Bei einem Wechsel des Frequenzbands oder der Drahtlosverbindung ist kein erneutes Koppeln der Buttons erforderlich.

Im Idealfall wird der ClickShare-Kanal nach der Durchführung einer Drahtlos-Standortaufnahme ausgewählt. Eine Standortaufnahme verzeichnet die Quellen von Interferenzen und der aktiven HF-Systeme. Auf dem Markt sind verschiedene Tools für eine WiFi-Standortaufnahme verfügbar. Auf Grundlage der Ergebnisse der Standortaufnahme kann der am wenigsten belegte Kanal gefunden und für den jeweiligen Konferenzraum ausgewählt werden.

2. Wählen Sie das Frequenzband für die Drahtlosverbindung aus, 2,4 GHz oder 5 GHz, indem Sie auf das Dropdown-Listenfeld klicken und das korrekte Band auswählen.

Unter dem Kanalauswahlfenster wird eine Anzeige der verfügbaren Bandbreiten des aktuellen Kanals angezeigt. Um zu sehen, ob über einen anderen Kanal eine ausreichende Bandbreite verfügbar ist, wählen Sie den Kanal in der Dropdown-Liste aus und speichern Sie die Änderungen. Die Seite wird mit den neuen Einstellungen neu geladen und eine Anzeige des Kanals wird nach ungefähr 1 Minute angezeigt. Es ist nicht erforderlich, die Seite neu zu laden, um das Ergebnis zu sehen.

Die verfügbaren Kanäle in der Liste variieren entsprechend der regionalen Version Ihrer Base Unit. Bei einem Wechsel des Frequenzbands oder der Drahtlosverbindung ist kein erneutes Koppeln der Buttons erforderlich.

Wechseln Sie zu einem anderen Kanal, wenn „Intensive Verwendung, wechseln Sie zu einem anderen WiFi-Kanal“ angezeigt wird. Die Seite wird nach ungefähr einer Minute neu geladen.

ClickShare Configurator-Zugriff über Wi-Fi

1. Um den Zugriff auf den Configurator über Wi-Fi zu erlauben, aktivieren Sie das Kontrollkästchen vor *WebUI über Wi-Fi verfügbar*.

Aktiviert: Configurator über Wi-Fi verfügbar.

Nicht aktiviert: Zugriff auf Configurator über Wi-Fi blockiert.

IP-Adresse und Subnetzmaske

1. Um die IP-Adresse oder die Subnetzmaske zu ändern, klicken Sie auf das Eingabefeld und geben Sie die vier Oktette der neuen IP-Adresse oder Subnetzmaske ein.



Hinweis: Für die statische IP-Adresszuweisung darf NICHT 0.0.0.0 verwendet werden.

Drahtlosclient-Einstellungen

Weitere Informationen finden Sie unter [“Wi-Fi-Einstellungen, Drahtlosclient”](#), Seite 91.

5.11 Wi-Fi-Einstellungen, Drahtlosclient

Einführung

Der Modus Drahtlosclient ermöglicht die Verbindung der Base Unit mit einem Netzwerk über Wi-Fi statt über die Ethernet-Schnittstelle. Er bietet eine identische Funktionalität wie bei einer kabelgebundenen Netzwerkverbindung: vollständige Netzwerkintegration, Funktionalität für die automatische Aktualisierung und zentrale Verwaltung in XMS. Er bietet eine stärkere Flexibilität bei der Platzierung der Base Unit, da an der Aufstellungsposition kein Netzkabel mehr erforderlich ist.

Beachten Sie, dass das Base Unit-Wi-Fi belegt ist und nicht mehr für Direktverbindungen verwendet werden kann, weder vom ClickShare-Button noch über die ClickShare-Apps oder AirPlay, Google Cast oder Miracast, wenn der Modus Drahtlosclient aktiviert ist. Das bedeutet, dass diese Verbindungen über das Unternehmensnetzwerk erfolgen müssen. Als Konsequenz werden die Buttons bei der Einrichtung des Modus Drahtlosclient automatisch so konfiguriert, dass sie sich mit dem gleichen Netzwerk wie die Base Unit verbinden. Diese Einstellung kann aber manuell auf der Buttons-Registerkarte im System-Menü geändert werden.



Für drahtlose Konferenzen wird eine Direktverbindung zwischen dem Button und der Base Unit empfohlen.

So aktivieren Sie den Drahtlos-Client

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Wi-Fi und Netzwerk* → *Wi-Fi-Einstellungen*.
3. Klicken Sie auf **Einstellungen bearbeiten (Edit settings)**.
4. Klicken Sie auf das Dropdown-Feld neben *Betriebsmodus* und wählen Sie *Drahtlos-Client* aus.

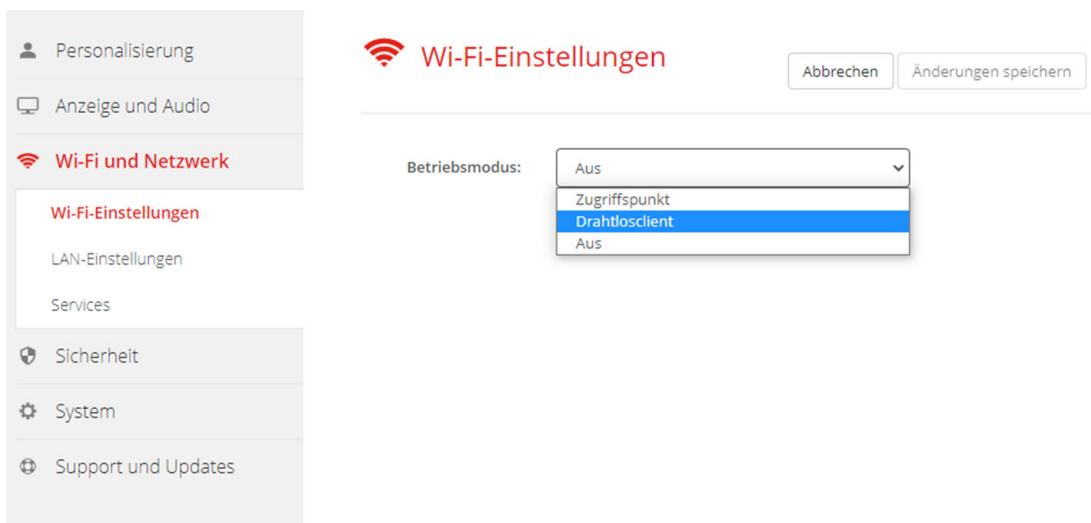


Abbildung 5–18 Wi-Fi-Einstellungen, Drahtlosclient

5.12 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS

Informationen zu EAP-TLS

EAP-TLS (Transport Layer Security) ist eine EAP-Methode, die auf Zertifikaten basiert, wodurch eine gegenseitige Authentifizierung zwischen Client und Server möglich ist. Diese Methode erfordert eine PKI (Public Key Infrastruktur) für die Verteilung von Server- und Clientzertifikaten. Für einige Organisationen stellt dies möglicherweise ein zu großes Hindernis dar. In diesen Fällen bieten sich mit EAP-TTLS und PEAP gute Alternativen. Auch wenn ein X.509-Clientzertifikat nicht unbedingt vom Standard erfordert wird, ist es in den meisten Implementierungen, einschließlich ClickShare, zwingend erforderlich. Wenn EAP-TLS über Clientzertifikate implementiert wird, gilt es als eine der sichersten EAP-Methoden. Der einzige kleine Nachteil im Vergleich zu PEAP und EAP-TTLS ergibt sich aus der unverschlüsselten Übertragung der Benutzeridentität, bevor der TLS-Quittungsbetrieb ausgeführt wurde. EAP-TLS wird über SCEP, INDES oder das manuelle Hochladen eines Zertifikats unterstützt.

So starten Sie die Verwendung von EAP-TLS

1. Wählen Sie in der Dropdown-Liste neben *Authentifizierungsmodus* die Option *EAP-TLS*.

The screenshot displays the configuration interface for EAP-TLS authentication. The 'Authentifizierungsmodus' dropdown is set to 'EAP-TLS'. The 'Zertifikat angeben' dropdown is set to 'Clientzertifikat und Zertifizierungsstellenzertifikat'. The 'Clientzertifikat hochladen' section includes a 'Bestand kiezen' button and instructions: 'Zulässige Dateiformate: .pfx (PKCS#12), .p12 (Base64 codiertes DER). Die Datei sollte mindestens das Clientzertifikat und den entsprechenden privaten Schlüssel enthalten.' The 'Zertifizierungsstellenzertifikat hochladen' section also includes a 'Bestand kiezen' button and instructions: 'Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER). Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.' The 'Verfahren' dropdown is set to 'Automatisch (DHCP)'. Other fields like 'Unternehmens-SSID', 'Domäne', 'Identität', 'IP-Adresse', 'Subnetzmaske', 'Standard-Gateway', and 'DNS-Server' are currently empty.

Abbildung 5–19 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS

2. Füllen Sie die *Unternehmens-SSID* aus.
Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.
3. Füllen Sie *Domäne* und *Identität* aus.
4. Wählen Sie das Zertifizierungsverfahren aus. Klicken Sie auf das Dropdown-Feld und wählen Sie das gewünschte Verfahren aus.
 - Manually provide Client & CA certificates
 - Automatische Registrierung über SCEP

Manuelle Bereitstellung von Zertifikaten

1. Laden Sie ein Client-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Zulässige Dateiformate:

- .pfx (PKCS#12)
- .pb12 (Base64-codiertes DER)

Die Datei sollte mindestens das Client-Zertifikat und den entsprechenden privaten Schlüssel enthalten.

2. Geben Sie das Kennwort für das Client-Zertifikat ein.
3. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem
- .cer
- .crt
- .pb7 (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

4. Speichern Sie die Änderungen.

Verwenden der automatischen Registrierung

Das Simple Certificate Enrolment Protocol (SCEP) ist ein Protokoll, das die Ausgabe und das Widerrufen von Zertifikaten in skalierbarer Weise ermöglicht. Die Unterstützung für SCEP ist integriert, um eine schnellere und reibungslosere Integration der ClickShare Base Unit und der Buttons in das Unternehmensnetzwerk zu ermöglichen.

Bis zur Base Unit-Firmware-Version 02.11.01 war die SCEP-Implementierung speziell auf den Network Device Enrollment Service (NDES) ausgerichtet, der Teil von Windows Server ist. Ab der Base Unit-Firmware-Version 02.12.00 unterstützen wir sowohl NDES als auch Standard-SCEP.

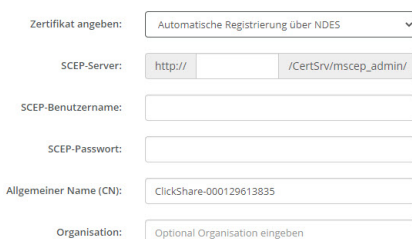
NDES erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Windows-Servers in Ihrem Netzwerk, der den NDES-Dienst ausführt. Nur http ist zulässig. Zum Beispiel: `http://meinServer` oder `http://10.192.5.1`.

SCEP-Benutzername: Dies ist ein Benutzer in Ihrem Active Directory, der die erforderliche Erlaubnis besitzt, auf den NDES-Dienst zuzugreifen und das abzufragende Kennwort anzufordern. Zur Absicherung sollte der Benutzer Mitglied der CA-Administratorengruppe sein (im Falle eines Einzel-CAs) oder Anmeldebefugnisse für die konfigurierten Zertifikatvorlagen besitzen.

SCEP-Kennwort: Das entsprechende Passwort für den SCEP-Benutzernamen, den Sie für die Authentifizierung beim Dienst verwenden.

Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.



Zertifikat angeben:

SCEP-Server:

SCEP-Benutzername:

SCEP-Passwort:

Allgemeiner Name (CN):

Organisation:

Abbildung 5–20 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS, NDES

SCEP erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Servers, auf dem der SCEP-Dienst ausgeführt wird, mit angehängtem Port und Suffix. Nur http ist zulässig. Zum Beispiel: `http://meinServer:8080/scep` oder `http://10.192.5.1/test`

SCEP-Challenge: Das entsprechende abzufragende SCEP-Kennwort.

Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.

Zertifikat angeben:

SCEP-Server:

SCEP-Challenge:

Allgemeiner Name (CN):

Abbildung 5–21 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TLS, SCEP

5.13 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TTLS

Informationen zu EAP-TTLS

EAP TTLS (Tunneled Transport Layer Security) ist eine EAP-Implementierung von Juniper Networks. Es wurde für die Bereitstellung einer Authentifizierung entwickelt, die so stark ist wie EAP-TLS, aber nicht für jeden Benutzer die Ausgabe eines Zertifikats erfordert. Stattdessen werden Zertifikate nur an die Authentifizierungsserver ausgeteilt. Die Authentifizierung der Benutzer erfolgt über ein Kennwort, wobei die Kennwörter über einen sicher verschlüsselten Tunnel transportiert werden, der auf den Serverzertifikaten basiert.

Die Authentifizierung der Benutzer wird in derselben Sicherheitsdatenbank ausgeführt, die bereits vom Unternehmens-LAN verwendet wird, z. B. SQL- oder LDAP-Datenbanken oder Tokensysteme. Da EAP-TTLS in der Regel ohne Clientzertifikat in Unternehmensumgebungen implementiert wird, wurde dafür keine Unterstützung integriert. Wenn Sie für jeden Benutzer Clientzertifikate verwenden möchten, schlagen wir die Verwendung von EAP-TLS vor.

So starten Sie die Verwendung von EAP-TTLS

1. Wählen Sie in der Dropdown-Liste neben *Authentifizierungsmodus* die Option *EAP-TTLS*.

The screenshot displays the configuration page for a wireless client. On the left is a navigation sidebar with categories: Personalisierung, Anzeige und Audio, Wi-Fi und Netzwerk (highlighted), LAN-Einstellungen, Services, Sicherheit, System, and Support und Updates. The main content area is titled 'Wi-Fi-Einstellungen' and contains the following fields:

- Authentifizierungsmodus:** A dropdown menu set to 'EAP-TTLS'.
- Unternehmens-SSID:** An empty text input field.
- Domäne:** An empty text input field.
- Identität:** An empty text input field.
- Anonyme Identität:** An empty text input field.

Below these fields is a note: *Lassen Sie dieses Feld leer, um während des Authentifizierungsprozesses nicht die anonyme Identität zu verwenden.*

- Passwort:** An empty text input field.
- Zertifizierungsstellenzertifikat hochladen (optional):** A section with a 'Bestand kiezen' button and the text: 'Geen bestand gekozen'. Below it, it lists 'Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER). Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.'
- Verfahren:** A dropdown menu set to 'Automatisch (DHCP)'.
- IP-Adresse:** A disabled text input field.
- Subnetzmaske:** A disabled text input field.
- Standard-Gateway:** A disabled text input field.
- DNS-Server:** A disabled text input field.

At the bottom left of the sidebar, there is a note: 'Zum Aktualisieren der Grundeinstellungen [ClickShare-Konfigurationsassistent](#) ausführen' and a copyright notice: '© 2021, Barco. All rights reserved.' The Barco logo is also present.

Abbildung 5–22 Wi-Fi-Einstellungen, Drahtlosclient, EAP-TTLS

5.14 Wi-Fi-Einstellungen, Drahtlosclient, PEAP

Informationen zu PEAP

PEAP (Protected Extensible Authentication Protocol) ist eine EAP-Implementierung, die in Zusammenarbeit zwischen Cisco Systems, Microsoft und RSA Security entwickelt wurde. Sie baut unter Verwendung des CA-Zertifikats des Servers einen sicheren TLS-Tunnel auf, in dem dann die jeweilige Benutzerauthentifizierung durchgeführt wird. Auf diese Weise kann sie während der Benutzerauthentifizierung die Sicherheit von TLS nutzen, benötigt aber keine PKI.

Die Standardversion schreibt nicht vor, welche Methode für die Authentifizierung im Tunnel verwendet werden soll. In den vorliegenden Anwendungshinweisen zu PEAP beziehen wir uns jedoch auf PEAPv0 mit EAP-MSCHAPv2 als interne Authentifizierungsmethode. Dies ist eine der beiden zertifizierten PEAP-Implementierungen in den WPA- und WPA2-Standards und die mit Abstand geläufigste und am weitesten verbreitete PEAP-Implementierung.

So starten Sie die Verwendung von PEAP

1. Wählen Sie in der Dropdown-Liste neben *Authentifizierungsmodus* die Option *PEAP*.

The screenshot shows the configuration page for a wireless client. On the left is a navigation menu with categories like Personalisierung, Anzeige und Audio, Wi-Fi und Netzwerk (selected), Sicherheit, System, and Support und Updates. The main content area is titled 'Wi-Fi-Einstellungen'. The 'Authentifizierungsmodus' dropdown is set to 'PEAP'. Below it are input fields for 'Unternehmens-SSID', 'Domäne', 'Identität', and 'Anonyme Identität'. A note below the 'Anonyme Identität' field reads: 'Lassen Sie dieses Feld leer, um während des Authentifizierungsprozesses nicht die anonyme Identität zu verwenden.' There is a 'Passwort' field. Below that is a section for 'Zertifizierungsstellenzertifikat hochladen (optional)' with a 'Bestand kiezen' button and a note: 'Geen bestand gekozen. Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER). Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.' Below this are dropdowns for 'Verfahren' (set to 'Automatisch (DHCP)'), and input fields for 'IP-Adresse', 'Subnetzmaske', 'Standard-Gateway', and 'DNS-Server'. At the bottom left of the page is the BARCO logo and copyright information: '© 2021, Barco. All rights reserved.'

Abbildung 5–23 Wi-Fi-Einstellungen, Drahtlosclient, PEAP

2. Füllen Sie die *Unternehmens-SSID* aus.
Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.
3. Füllen Sie *Domäne* und *Identität* aus.
4. Geben Sie ein *Kennwort* ein.
5. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem

- .cer
- .crt
- .pb7 (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

6. Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu speichern.

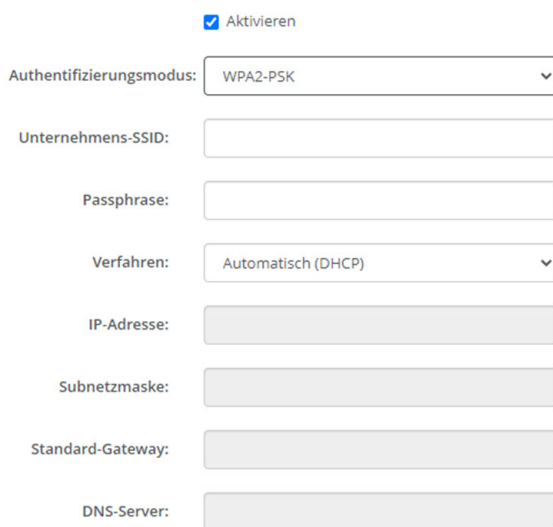
5.15 Wi-Fi-Einstellungen, Drahtlosclient, WPA2-PSK

Informationen zu WPA2-PSK

WPA2-PSK unterscheidet nicht zwischen einzelnen Benutzern. Es gibt ein Kennwort (Pre-Shared Key, PSK) für alle Clients, die sich mit der drahtlosen Infrastruktur verbinden. Dadurch wird die Einrichtung erheblich vereinfacht. Nach der Verbindung werden alle Daten, die zwischen dem Client und dem AP (Access Point) übertragen werden, über einen 256-Bit-Schlüssel verschlüsselt.

So starten Sie die Verwendung von WPA2-PSK

1. Wählen Sie in der Dropdown-Liste neben *Authentifizierungsmodus* die Option *WPA2-PSK*.



Aktivieren

Authentifizierungsmodus: WPA2-PSK

Unternehmens-SSID:

Passphrase:

Verfahren: Automatisch (DHCP)

IP-Adresse:

Subnetzmaske:

Standard-Gateway:

DNS-Server:

Abbildung 5–24 Wi-Fi-Einstellungen, Drahtlosclient, WPA-PSK

2. Füllen Sie die *Unternehmens-SSID* aus.
Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.
3. Füllen Sie die Passphrase aus.
Der in WPA2-PSK für die Authentifizierung in der drahtlosen Infrastruktur verwendete Schlüssel. Dies kann eine 64-stellige hexadezimale Zeichenkette oder ein Kennwort mit 8 bis 63 druckbaren ASCII-Zeichen sein.
4. Tippen Sie auf **Änderungen speichern**.

5.16 LAN-Einstellungen

Informationen zu den LAN-Netzwerkeinstellungen

Eine Netzwerkverbindung kann über DHCP oder durch die manuelle Eingabe einer festen IP-Adresse konfiguriert werden.



DHCP

Dynamisches Hostkonfigurationsprotokoll. DHCP ist ein Kommunikationsprotokoll, mit dem Netzwerkadministratoren die Zuweisung der IP-Adressen im Netzwerk einer Organisation zentral verwalten und automatisieren können. Bei Verwendung des Internetprotokolls benötigt jede Maschine, die sich mit dem Internet verbinden kann, eine eindeutige IP-Adresse. Richtet eine Organisation ihre Computerbenutzer mit einer Verbindung zum Internet ein, muss jeder Maschine eine IP-Adresse zugewiesen werden. Ohne DHCP muss die IP-Adresse manuell an jedem Computer eingegeben werden und, bei Verlegung von Computern an eine andere Position in einem anderen Teil des Netzwerks, eine neue IP-Adresse eingegeben werden. Mit DHCP kann ein Netzwerkadministrator IP-Adressen zentral überwachen und verteilen sowie automatisch eine neue IP-Adresse senden, wenn ein Computer an anderer Stelle im Netzwerk angeschlossen wird.

Hostname und Verfahren

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Wi-Fi und Netzwerk* → *LAN-Einstellungen*.

The screenshot displays the 'LAN-Einstellungen' (LAN Settings) page. On the left is a navigation sidebar with options like 'Personalisierung', 'Anzeige und Audio', 'Wi-Fi und Netzwerk' (selected), 'Services', 'Sicherheit', 'System', and 'Support und Updates'. The main content area is titled 'LAN-Einstellungen' and includes buttons for 'Änderungen verwerfen' and 'Änderungen speichern'. Below the title, there are sections for 'LAN-Hostname-Einstellungen' (with a 'Hostname' field containing 'ClickShare-1863550238'), 'Primärschnittstelle' (with a 'Verfahren' dropdown set to 'Automatisch (DHCP)'), 'IP-Adresse' (10.200.20.205), 'Subnetzmaske' (255.255.254.0), 'Standard-Gateway' (10.200.20.1), 'MAC-Adresse' (00:04:A5:01:03:EE), and 'DNS-Server' (10.197.192.11, 10.193.251.11). A 'Status' section shows 'Status Deaktiviert' and a button for 'Kabelgebundene Authentifizierung einrichten ...'. At the bottom, there is a 'LAN-Proxy-Einstellungen' section with a checkbox for 'Proxy-Server verwenden'.

Abbildung 5–25 LAN-Einstellungen

3. Klicken Sie auf das Eingabefeld neben *Hostname* und geben Sie einen Hostnamen für die Base Unit ein. Der Standard-Hostname lautet *ClickShare-<Seriennummer der Base Unit>*.

- Um das Verfahren auszuwählen, klicken Sie auf das Dropdown-Listefeld neben Methode und wählen Sie *Automatisch (DHCP)* oder *Manuell*.

Wenn Sie Automatisch (DHCP) auswählen, werden die Felder für IP-Adresse, Subnetzmaske und Standard-Gateway abgeblendet. Die aktuell verwendeten Einstellungen sind ausgefüllt.

- Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu übernehmen.

Manuelle (feste) IP-Adresse

- Klicken Sie auf das Dropdown-Listefeld neben der Menüoption *Verfahren*, und wählen Sie *Manuell* aus. Die Eingabefelder „IP-Adresse“, „Subnetz“ und „Gateway“ sind aktiviert.

- Klicken Sie auf das Eingabefeld der *IP-Adresse*, und füllen Sie die vier Oktette aus.



Hinweis: Die Adresse enthält vier Oktette mit einem Maximalwert von 255. Für die statische IP-Adresszuweisung darf NICHT 0.0.0.0 verwendet werden.

- Klicken Sie auf das Eingabefeld der *Subnetzmaske*, und füllen Sie die vier Oktette gemäß des lokalen Subnetzes aus.

- Klicken Sie auf die Eingabefelder für das *Standard-Gateway* und tragen Sie die notwendigen Daten in die vier Oktette ein. Legen Sie das Standard-Gateway auf die IP-Adresse des Routers fest (dieser MUSS sich im lokalen Subnetz befinden!).



Hinweis: 0.0.0.0 ist NICHT zulässig. Ist kein Router im lokalen Subnetz vorhanden, geben Sie in dieses Feld eine beliebige IP-Adresse im Subnetz ein.

- Klicken Sie in das Eingabefeld DNS-Server und füllen Sie die bevorzugten DNS-Server (maximal 5) in einer durch Kommata getrennten Liste aus.

- Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu übernehmen.



Verwenden Sie nicht die IP-Adresse 192.168.2.x für eine Subnetzmaske 255.255.255.0 und nicht die IP-Adresse 192.168.x.x für eine Subnetzmaske 255.255.0.0

Verwenden eines Proxy-Servers

Diese Einstellung ist wichtig für die automatische Aktualisierungsfunktion der Base Unit, für die Internetzugriff erforderlich ist.

- Aktivieren Sie das Kontrollkästchen neben „Proxy-Sever verwenden“.

Proxy-Server verwenden

Serveradresse:

Server-Anschluss (optional):

Benutzername (optional):

Passwort (optional):

Abbildung 5–26 Proxy-Einstellungen

Die Proxy-Einstellungen sind verfügbar.

- Geben Sie die Adresse des Proxy-Servers ein. Geben Sie die IP-Adresse oder Hostnamen ein.

Für einige Proxy-Server ist eine Portnummer, ein Benutzername und ein Passwort erforderlich. Bei manchen Proxy-Servern ist dies optional.

- Geben Sie optional den verwendeten Serverport ein.
- Geben Sie optional den Benutzernamen ein.

5. Geben Sie optional das Passwort ein.
6. Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu übernehmen.

5.17 LAN-Einstellungen, kabelgebundene Authentifizierung

Einrichtung

1. Klicken Sie auf **Einrichtung der kabelgebundenen Authentifizierung (Setup wired authentication...)**.

The screenshot displays the 'LAN-Einstellungen' (LAN Settings) page. On the left is a navigation sidebar with categories like Personalisierung, Anzeige und Audio, Wi-Fi und Netzwerk (selected), Sicherheit, System, and Support und Updates. The main content area is titled 'LAN-Einstellungen' and includes buttons for 'Änderungen verwerfen' and 'Änderungen speichern'. Below the title are sections for 'LAN-Hostname-Einstellungen' (Hostname: ClickShare-1863550238), 'Primärschnittstelle' (Method: Automatisch (DHCP)), 'IP-Adresse' (10.200.20.205), 'Subnetzmaske' (255.255.254.0), 'Standard-Gateway' (10.200.20.1), 'MAC-Adresse' (00:04:A5:01:03:EE), and 'DNS-Server' (10.197.192.11, 10.193.251.11). At the bottom, there is a 'Status kabelgebundene Authentifizierung' section with a 'Status Deaktiviert' indicator and a button 'Kabelgebundene Authentifizierung einrichten ...'. A 'LAN-Proxy-Einstellungen' section at the very bottom has a checkbox for 'Proxy-Server verwenden' which is currently unchecked.

Abbildung 5–27 Kabelgebundene Authentifizierung

Der Konfigurationsassistent wird gestartet.

2. Wählen Sie das Authentifizierungsverfahren aus. Klicken Sie auf das Dropdown-Feld und wählen Sie das gewünschte Verfahren aus.

Die folgenden Methoden stehen zur Auswahl:

- Keine Authentifizierung: Es wird kein Authentifizierungsmechanismus auf die kabelgebundene Schnittstelle angewendet.
- EAP-TLS
- EAP-TTLS
- PEAP

5.18 LAN-Einstellungen, Sicherheitsmodus EAP-TLS

Informationen zu EAP-TLS

EAP-TLS (Transport Layer Security) ist eine EAP-Methode, die auf Zertifikaten basiert, wodurch eine gegenseitige Authentifizierung zwischen Client und Server möglich ist. Diese Methode erfordert eine PKI (Public Key Infrastruktur) für die Verteilung von Server- und Clientzertifikaten. Für einige Organisationen stellt dies möglicherweise ein zu großes Hindernis dar. In diesen Fällen bieten sich mit EAP-TTLS und PEAP gute Alternativen. Auch wenn ein X.509-Clientzertifikat nicht unbedingt vom Standard erfordert wird, ist es in den meisten Implementierungen, einschließlich ClickShare, zwingend erforderlich. Wenn EAP-TLS über Clientzertifikate implementiert wird, gilt es als eine der sichersten EAP-Methoden. Der einzige kleine Nachteil im Vergleich zu PEAP und EAP-TTLS ergibt sich aus der unverschlüsselten Übertragung der Benutzeridentität, bevor der TLS-Quittungsbetrieb ausgeführt wurde. EAP-TLS wird über SCEP oder das manuelle Hochladen eines Zertifikats unterstützt.

So richten Sie EAP-TLS ein

1. Wählen Sie den Authentifizierungsmodus *EAP-TLS*.

ClickShare-Assistent für kabelgebundene Authentifizierung

Authentifizierungsmodus:

Domäne:

Identität:

Bescheinigung vorlegen:

Client-Zertifikat hochladen: Geen bestand gekozen
Zulässige Dateiformate: .pfx (PKCS#12), .p12 (Base64 codiertes DER). Die Datei sollte mindestens das Clientzertifikat und den entsprechenden privaten Schlüssel enthalten.

Kennwort Clientzertifikat:

Zertifikat Zertifizierungsstelle hochladen: Geen bestand gekozen
Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER). Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.

Konfiguration speichern

BARCO

Abbildung 5–28 EAP-TLS

2. Füllen Sie *Domäne* und *Identität* aus.
3. Wählen Sie das Zertifizierungsverfahren aus. Klicken Sie auf das Dropdown-Feld und wählen Sie das gewünschte Verfahren aus.
 - Manually provide Client & CA certificates
 - Automatische Registrierung über SCEP

Manuelle Bereitstellung von Zertifikaten

1. Laden Sie ein Client-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Zulässige Dateiformate:

- .pfx (PKCS#12)
- .p12 (Base64-codiertes DER)

Die Datei sollte mindestens das Client-Zertifikat und den entsprechenden privaten Schlüssel enthalten.

2. Geben Sie das Kennwort für das Client-Zertifikat ein.
3. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem
- .cer
- .crt
- .pb7 (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

4. Speichern Sie die Konfiguration.

Verwenden der automatischen Registrierung

Das Simple Certificate Enrolment Protocol (SCEP) ist ein Protokoll, das die Ausgabe und das Widerrufen von Zertifikaten in skalierbarer Weise ermöglicht. Die Unterstützung für SCEP ist integriert, um eine schnellere und reibungslosere Integration der ClickShare Base Unit und der Buttons in das Unternehmensnetzwerk zu ermöglichen.

Bis zur Base Unit-Firmware-Version 02.11.01 war die SCEP-Implementierung speziell auf den Network Device Enrollment Service (NDES) ausgerichtet, der Teil von Windows Server ist. Ab der Base Unit-Firmware-Version 02.12.00 unterstützen wir sowohl NDES als auch Standard-SCEP.

NDES erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Windows-Servers in Ihrem Netzwerk, der den NDES-Dienst ausführt. Nur http ist zulässig. Zum Beispiel: `http://meinServer` oder `http://10.192.5.1`.

SCEP-Benutzername: Dies ist ein Benutzer in Ihrem Active Directory, der die erforderliche Erlaubnis besitzt, auf den NDES-Dienst zuzugreifen und das abzufragende Kennwort anzufordern. Zur Absicherung sollte der Benutzer Mitglied der CA-Administratorengruppe sein (im Falle eines Einzel-CAs) oder Anmeldebefugnisse für die konfigurierten Zertifikatvorlagen besitzen.

SCEP-Kennwort: Das entsprechende Passwort für den SCEP-Benutzernamen, den Sie für die Authentifizierung beim Dienst verwenden.

Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.

The screenshot shows a configuration form with the following fields:

- Zertifikat angeben:** A dropdown menu set to "Automatische Registrierung über NDES".
- SCEP-Server:** A text input field containing "http://" followed by a small button labeled "/CertSrv/mscep_admin/".
- SCEP-Benutzername:** An empty text input field.
- SCEP-Passwort:** An empty text input field.
- Allgemeiner Name (CN):** A text input field containing "ClickShare-000129613835".
- Organisation:** A text input field containing "Optional Organisation eingeben".

Abbildung 5–29 LAN-Einstellungen, Drahtlosclient, EAP-TLS, NDES

SCEP erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Servers, auf dem der SCEP-Dienst ausgeführt wird, mit angehängtem Port und Suffix. Nur http ist zulässig. Zum Beispiel: `http://meinServer:8080/scep` oder `http://10.192.5.1/test`

SCEP-Challenge: Das entsprechende abzufragende SCEP-Kennwort.

Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.

The screenshot shows a configuration form with the following fields:

- Zertifikat angeben:** A dropdown menu set to "Automatische Registrierung über SCEP".
- SCEP-Server:** A text input field containing "http://" followed by an empty text input field.
- SCEP-Challenge:** An empty text input field.
- Allgemeiner Name (CN):** A text input field containing "ClickShare-000129613835".

Abbildung 5–30 LAN-Einstellungen, Drahtlosclient, EAP-TLS, SCEP

5.19 LAN-Einstellungen, Sicherheitsmodus EAP-TTLS

Informationen zu EAP-TTLS

EAP TTLS (Tunneled Transport Layer Security) ist eine EAP-Implementierung von Juniper Networks. Es wurde für die Bereitstellung einer Authentifizierung entwickelt, die so stark ist wie EAP-TLS, aber nicht für jeden Benutzer die Ausgabe eines Zertifikats erfordert. Stattdessen werden Zertifikate nur an die Authentifizierungsserver ausgeteilt. Die Authentifizierung der Benutzer erfolgt über ein Kennwort, wobei die Kennwörter über einen sicher verschlüsselten Tunnel transportiert werden, der auf den Serverzertifikaten basiert.

Die Authentifizierung der Benutzer wird in derselben Sicherheitsdatenbank ausgeführt, die bereits vom Unternehmens-LAN verwendet wird, z. B. SQL- oder LDAP-Datenbanken oder Tokensysteme. Da EAP-TTLS in der Regel ohne Clientzertifikat in Unternehmensumgebungen implementiert wird, wurde dafür keine Unterstützung integriert. Wenn Sie für jeden Benutzer Clientzertifikate verwenden möchten, schlagen wir die Verwendung von EAP-TLS vor.

So richten Sie EAP-TTLS ein

1. Wählen Sie den Authentifizierungsmodus *EAP-TTLS*.

Abbildung 5–31 EAP-TTLS

2. Füllen Sie *Domäne* und *Identität* aus.

Domäne	Die Unternehmensdomäne, für die Sie sich registrieren, sollte mit derjenigen übereinstimmen, die in Ihrem Active Directory definiert ist.
Identity	Die Identität des Benutzerkontos in Active Directory, die von den ClickShare Buttons für die Verbindung zum Unternehmensnetzwerk verwendet wird.

3. Geben Sie das *Kennwort* ein.

Das entsprechende Kennwort für die Identität, die Sie für die Authentifizierung im LAN-Netzwerk verwenden. Pro Base Unit verwendet jeder Button dieselbe Identität und dasselbe Kennwort, um sich mit dem Unternehmensnetzwerk zu verbinden.

4. Laden Sie optional das CA-Zertifikat hoch.

Die folgenden Formate sind zulässig:

- .pem
- .cer
- .crt
- .pb7 (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

5. Klicken Sie auf **Konfiguration speichern (Save configuration)**.

5.20 Services, mobile Geräte

ClickShare-App

Die ClickShare-App ist standardmäßig aktiviert und macht es möglich, ein Mobilgerät mit der Base Unit zu verbinden.

Streaming von Informationen über AirPlay

Bevor Sie Informationen streamen und über ClickShare anzeigen können, muss Ihr Gerät mit dem drahtlosen Netzwerk der Base Unit verbunden werden. Anschließend muss AirPlay auf Ihrem Gerät aktiviert werden. Weitere Informationen zur Aktivierung von AirPlay erhalten Sie im Benutzerhandbuch Ihres Geräts.

Die unterstützten Versionen von AirPlay sind auf der Barco-Website www.barco.com/clickshare aufgeführt. Die Unterstützung für eine noch nicht veröffentlichte Version dieser Protokolle kann durch Barco nicht garantiert werden.

Streaming über Google Cast

Bevor Sie Informationen spiegeln und über ClickShare anzeigen können, muss Ihr Gerät mit dem drahtlosen Netzwerk der Base Unit verbunden werden. Bei der Aktivierung von Google Cast auf Ihrem Gerät wird eine Übersicht über die Zugriffspunkte bereitgestellt. Weitere Informationen zur Verwendung von Google Cast erhalten Sie im Benutzerhandbuch Ihres Geräts.

Die unterstützten Versionen von Google Cast sind auf der Barco-Website www.barco.com/clickshare aufgeführt. Die Unterstützung für eine noch nicht veröffentlichte Version dieser Protokolle kann durch Barco nicht garantiert werden.

Google Cast unterstützt nicht die Verwendung eines Passworts.



Google Cast kann nur verwendet werden, wenn die Uhr der Base Unit korrekt eingestellt ist. Ist dies nicht der Fall, kann Google Cast keine Verbindung zur Base Unit herstellen.

Informationen zum Streaming über Miracast™

Mit Miracast™ ist eine nahtlose Anzeige von Multimediainhalten zwischen Miracast®-Geräten möglich. Miracast ermöglicht den Benutzern die drahtlose Multimedia-Freigabe, einschließlich hochauflösenden Bildern und High-Definition (HD)-Videoinhalten, zwischen WLAN-Geräten, auch wenn kein WLAN-Gerät verfügbar ist.

Miracast richtet ein eigenes Netzwerk ein, um Informationen zu streamen und diese über ClickShare anzuzeigen, sodass keine Notwendigkeit für eine Direktverbindung mit der Base Unit besteht. Miracast muss auf dem Gerät aktiviert werden. Weitere Informationen zur Aktivierung von Miracast finden Sie im Benutzerhandbuch Ihres Geräts.

Die unterstützten Versionen von Miracast sind auf der Barco-Website www.barco.com/clickshare aufgeführt. Die Unterstützung für eine noch nicht veröffentlichte Version dieser Protokolle kann durch Barco nicht garantiert werden.



Um Miracast verwenden zu können, müssen Sie den Zugriffspunkt deaktivieren und die Buttons in das Unternehmensnetzwerk integrieren.

Auswahl Codetyp

1. Melden Sie sich bei *Configurator* an.
2. Klicken auf *Wi-Fi und Netzwerk* → *Services*.

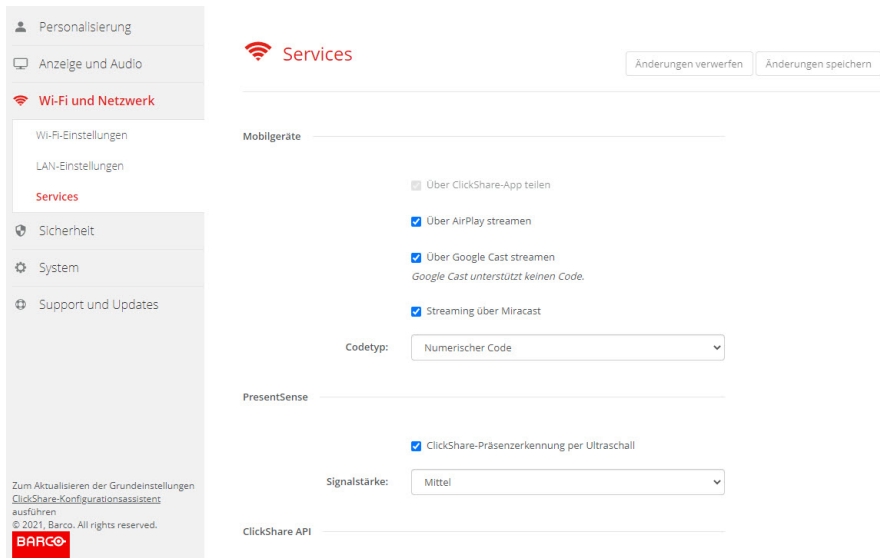


Abbildung 5–32 Dienste, mobile Geräte

3. Um die Freigabe von Inhalten über die ClickShare-App zuzulassen, wird *Über ClickShare-App teilen* standardmäßig aktiviert und kann nicht geändert werden.

Um das Streamen über AirPlay zu ermöglichen, aktivieren Sie das Kontrollkästchen neben *Über AirPlay streamen*.

Um das Streamen (Mirroring) über Google Cast zu ermöglichen, aktivieren Sie das Kontrollkästchen neben *Über Google Cast streamen*. Google Cast unterstützt nicht die Verwendung eines Passworts.

Um das Streamen über Miracast zu ermöglichen, aktivieren Sie das Kontrollkästchen neben *Streaming über Miracast*.

Hinweis: Ab Firmware-Version 2.12 werden AirPlay, Google Cast und Miracast beim Zurücksetzen auf die Werkseinstellungen deaktiviert.

4. Klicken Sie auf das Dropdown-Listefeld, und wählen Sie den gewünschten Codetyp aus.
- Kein Passwort
 - Numerisches Passwort

Die Kennung gilt für alle BYOD-Bildschirmfreigaben mit Ausnahme von Google Cast.

5.21 Dienst, PresentSense

Informationen zu PresentSense

Die PresentSense-Funktion macht die Verbindung mit einer Base Unit einfach, wenn Sie einen Besprechungsraum betreten. Wenn diese Funktion aktiviert und die ClickShare-Desktop-App auf dem Computer des Benutzers installiert ist, erkennt die Base Unit beim Betreten eines Besprechungsraums über ein Ultraschallsignal, das die Geräte-ID und den Pincode enthält, Ihre Anwesenheit und stellt die Verbindung über den enthaltenen Pincode her, nachdem der Benutzer in einem Popup-Fenster auf seinem Computer auf **Verbinden** geklickt hat.

Die App stellt automatisch eine Verbindung her bzw. trennt sie, wenn Sie den Besprechungsraum betreten bzw. ihn verlassen. Weder die Auswahl des Besprechungsraums noch die Eingabe eines Pincodes ist erforderlich. Nur wer im Raum ist, kann sehen und hören, was Sie tun.

So nehmen Sie eine Aktivierung vor

1. Melden Sie sich bei *Configurator* an.
2. Klicken auf *Wi-Fi und Netzwerk* → *Services*.

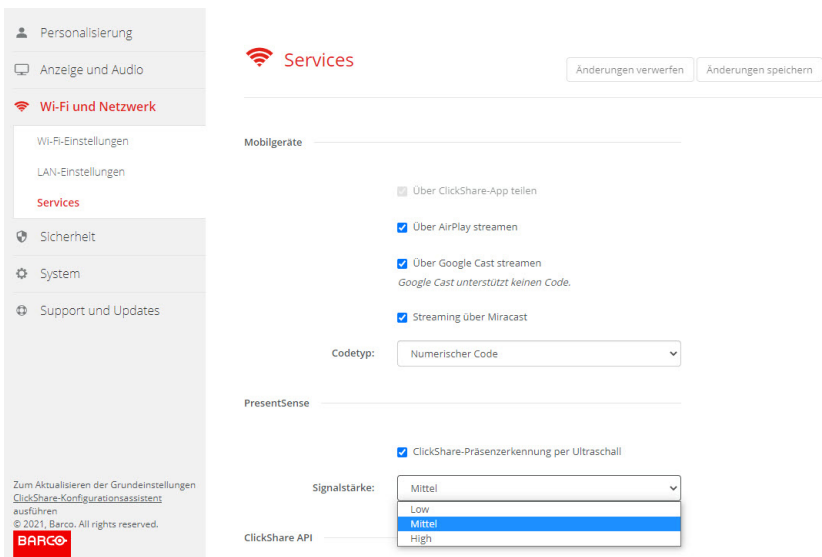


Abbildung 5–33 PresentSense

3. Aktivieren Sie im Bereich *PresentSense* das Kontrollkästchen neben der Option *ClickShare-Präsenzerkennung über Ultraschall*.

Aktiviert: Die PresentSense-Erkennung ist aktiviert.

Deaktiviert: Die PresentSense-Erkennung nicht aktiviert.

4. Wählen Sie die Signalstärke, indem Sie auf das Dropdown-Feld neben *Signalstärke* klicken.

Folgende Optionen sind möglich:

- Niedrig
- Mittel
- Hoch

5.22 Dienst, ClickShare API, Fernbedienung über API

Informationen zu den API-Einstellungen

Die API kann aktiviert oder deaktiviert werden, d. h. dass der Zugriff auf die Einheit von einem externen Gerät aus zugelassen oder blockiert werden kann.

Diese Funktionen sind standardmäßig aktiviert.

API-Dokumentation

Die API-Dokumentation ist in der Base Unit enthalten. Klicken Sie einfach auf *API-Dokumentation anzeigen*, um auf die Dokumentation zuzugreifen. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um auf die auf der Base Unit gespeicherte Dokumentation zuzugreifen.



Der Standardbenutzername und das Standardkennwort sind mit denen von Configurator identisch (admin/admin). Diese können unter *Sicherheit* → *Passwörter* geändert werden.

ClickShare API

Fernbedienung über API

[API-Dokumentation anzeigen](#)

Abbildung 5–34 ClickShare API-Dokumentation

So aktivieren Sie die Fernbedienung über API

1. Melden Sie sich bei *Configurator* an.
2. Klicken auf *Wi-Fi und Netzwerk* → *Services*.
3. Aktivieren Sie das Kontrollkästchen für *Fernbedienung über API*, um diese Funktion zu aktivieren.

Dieses Kontrollkästchen ist standardmäßig aktiviert.

Aktiviertes Kontrollkästchen: Fernbedienung über API ist zulässig. Ein Passwort kann verwendet werden, um den Zugriff zu schützen.

Nicht aktiviertes Kontrollkästchen: Fernbedienung über API ist nicht zulässig.

Informationen zur API-Dokumentation

Die vollständige API-Dokumentation für die Integration mit Drittanbietern ist auf der Base Unit gespeichert und mit dem Benutzernamen und Kennwort geschützt.

So zeigen Sie die API-Dokumentation an

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *API-Dokumentation anzeigen*.
3. Geben Sie Ihren Benutzernamen und das Kennwort ein und klicken Sie auf **OK**.

Die Dokumentation wird als anklickbare HTML-Seite angezeigt.

5.23 Dienste, SNMP

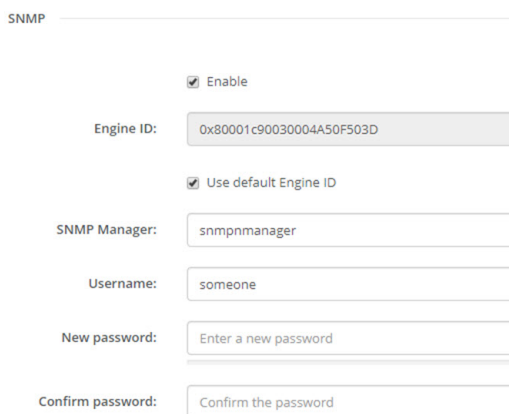
Informationen zu SNMP

Das Simple Network Management Protocol (SNMP) ist ein Internet-Standardprotokoll für die Zusammenstellung und Organisation von Informationen zu verwalteten Geräten in IP-Netzwerken und für die Änderung dieser Informationen zur Änderung des Geräteverhaltens. Im Allgemeinen kommuniziert eine SNMP-Verwaltungssuite (die auf einem Server läuft) mit einem SNMP-Agenten (der auf dem Gerät läuft). Der SNMP-Agent sammelt und legt Geräteinformationen in der Form von Variablen offen, die einer MIB (Management Information Base) entsprechen. SNMP-Managementsuites können mit ClickShare-Geräten über das SNMP-Protokoll kommunizieren, um Geräteinformationen anzufordern.

SNMPv3 wird unterstützt.

So führen Sie die Aktivierung durch

1. Melden Sie sich bei *Configurator* an.
2. Klicken auf *Wi-Fi und Netzwerk* → *Services*.
3. Scrollen Sie zu *SNMP*.



SNMP

Enable

Engine ID:

Use default Engine ID

SNMP Manager:

Username:

New password:

Confirm password:

Abbildung 5–35 Dienst, SNMP

4. Aktivieren Sie das Kontrollkästchen vor *Aktivieren*.

Die Konfigurationsfelder sind verfügbar.

So konfigurieren Sie

1. Wenn Sie die Standard-*Modul-ID* verwenden, stellen Sie sicher, dass das Kontrollkästchen *Standard-Modul-ID verwenden* aktiviert ist.

Die Standard-Modul-ID ist eine Kombination aus der Barco Enterprise Number und der MAC-Adresse (eth0).

2. Füllen Sie die Adresse *SNMP-Manager* aus.

Dies ist die Hostadresse, welche die TRAP-Ereignisse/Meldungen empfängt.

Mögliche Traps sind:

- Der Trap „Alarm CPU-Temperatur“, der zeigt, dass die CPU-Temperatur den Grenzwert übersteigt.
- Der Trap „Alarm Gehäuselüftergeschwindigkeit“, der zeigt, dass der Gehäuselüfter sich zu langsam dreht.
- Der Trap „Alarm Prozess wird nicht ausgeführt“, der zeigt, dass einer der überwachten Prozesse nicht läuft.

3. Geben Sie *Benutzername* ein.
4. Geben Sie ein neues Kennwort ein und bestätigen Sie dieses.

5.24 Sicherheit, Sicherheitsstufe

Informationen zu Sicherheitsstufen

Für die Nutzung des ClickShare-Systems kann eine Sicherheitsstufe festgelegt werden. Standardmäßig ist Stufe 1 aktiviert. Eine Sicherheitsstufe sind vordefinierte Einstellungen, die automatisch festgelegt werden, wenn eine Stufe ausgewählt wird.

Stufe 1: Bietet Unterstützung für reguläre, tägliche Abläufe einer beliebigen Organisation.

Stufe 1 beinhaltet standardmäßige Sicherheitsoptionen und Verschlüsselung für Audio- und Videodaten.

Die standardmäßigen Sicherheitsoptionen sind:

- PIN-Codeaktivierung für mobile Anwendungen und Buttons,
- ClickShare Configurator (WebUI)-Zugriff über HTTPS mit Anmeldeverwaltung,
- kein drahtloser ClickShare Configurator (WebUI)-Zugriff und keine Fernbedienung über API,
- SSID des Wi-Fi-Netzwerks wird nicht angezeigt.

Stufe 2: Diese Stufe bietet ein höheres Maß an Sicherheit, passend für Organisationen mit höheren Sicherheitsanforderungen.

Stufe 2 enthält die Sicherheitsmaßnahmen von Stufe 1 sowie einen obligatorischen PIN-Code für mobile Geräte. Alphanumerische PIN-Codes für mobile Anwendungen und Buttons. Die Buttons benötigen eine Zertifizierung für die Kopplung.

Stufe 3: Diese Stufe wird für Organisationen mit sehr strengen Sicherheitsanforderungen verwendet.

Stufe 3 enthält die Sicherheitsmaßnahmen von Stufe 2; zusätzlich werden mobile Anwendungen blockiert, eine Herabstufung der Firmware ist nicht möglich und drahtloser Zugriff auf den Configurator (WebUI) ist nicht zulässig.

Wurde eine Sicherheitsstufe festgelegt, können die einzelnen Elemente dieser Sicherheitsstufe im Configurator geändert werden. Bei Änderung eines einzelnen Elements wird die Anzeige der Sicherheitsstufe entsprechend angepasst. Die anderen Einstellungen werden jedoch nicht automatisch geändert.

Wenn z. B. Stufe 3 festgelegt wurde und Sie die Nutzung mobiler Anwendungen erlauben, wird die Anzeige der Sicherheitsstufe auf Stufe 2 geändert. Alle anderen Elemente, die ursprünglich in Stufe 3 festgelegt wurden, verbleiben in dieser Stufe.



Um die einzelnen Änderungen zurückzusetzen, wählen Sie die gewünschte Sicherheitsstufe und klicken Sie auf **Änderungen speichern**.



Das Ändern der Sicherheitsstufe erfordert ein erneutes Koppeln der Buttons. Das Ändern der Sicherheitsstufe von Stufe 1 auf eine höhere Stufe verändert die Kompatibilitätseinstellung für Buttons mit Zertifikat (R9861006D01). So lange die Sicherheitseinstellung höher als Stufe 1 ist, können diese nicht gekoppelt werden.

So legen Sie die Sicherheitsstufe fest

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Sicherheit* → *Sicherheitsstufe*.



Abbildung 5–36 Sicherheitsstufen

3. Wählen Sie das Symbol mit der gewünschten Sicherheitsstufe.
4. Klicken Sie auf **Änderungen speichern**, um die Einstellung zu übernehmen.

5.25 Sicherheit, Passwörter

Informationen zu Passwörtern

Für den Zugriff auf den ClickShare Configurator werden ein Benutzername und ein Passwort benötigt. Das Kennwort kann jeder Zeit geändert werden, um die Einstellungen der *ClickShare-Konfiguration* zu schützen.

Ändern des Passworts für ClickShare Configurator und API

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Sicherheit* → *Passwörter*.

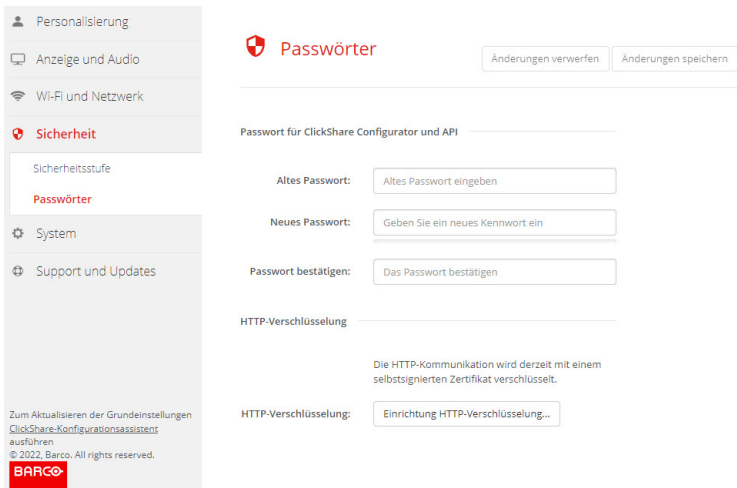


Abbildung 5–37 Passwörter

3. Klicken Sie im Fenster *Passwort* auf das Eingabefeld neben *Altes Passwort* und geben Sie das alte Passwort ein.
4. Klicken Sie in das Eingabefeld neben *Neues Passwort* und geben Sie ein neues Passwort ein.
5. Klicken Sie in das Eingabefeld neben *Passwort bestätigen* und geben Sie das neue Passwort erneut ein.
6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu übernehmen.

5.26 Sicherheit, HTTP-Verschlüsselung

Informationen zur HTTP-Verschlüsselung

Die HTTP-Verschlüsselung kann mit einem selbstsignierten Zertifikat oder einem benutzerdefinierten Zertifikat eingerichtet werden. Standardmäßig wird ein selbstsigniertes Zertifikat verwendet.

Einrichtung

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Sicherheit* → *Passwörter*.

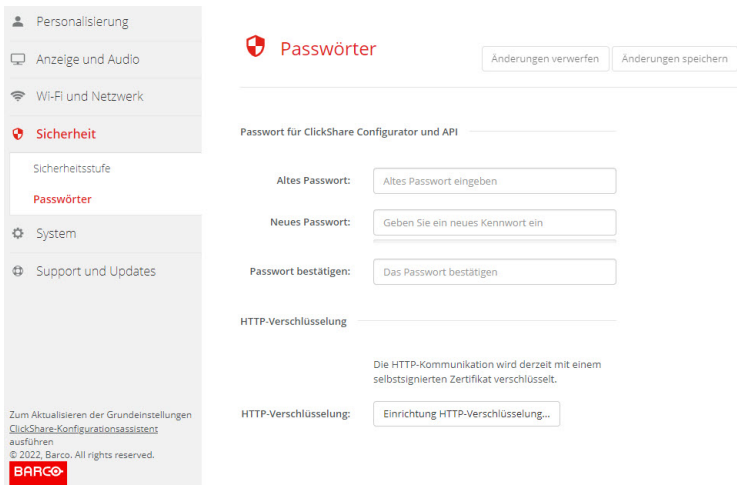


Abbildung 5–38 HTTP-Verschlüsselung

3. Klicken Sie auf **HTTP-Verschlüsselung...**
4. Wählen Sie das Zertifikat aus.

Folgende Optionen sind möglich:

- Verwenden eines selbstsignierten Zertifikats
- Verwenden Sie ein benutzerdefiniertes Zertifikat.

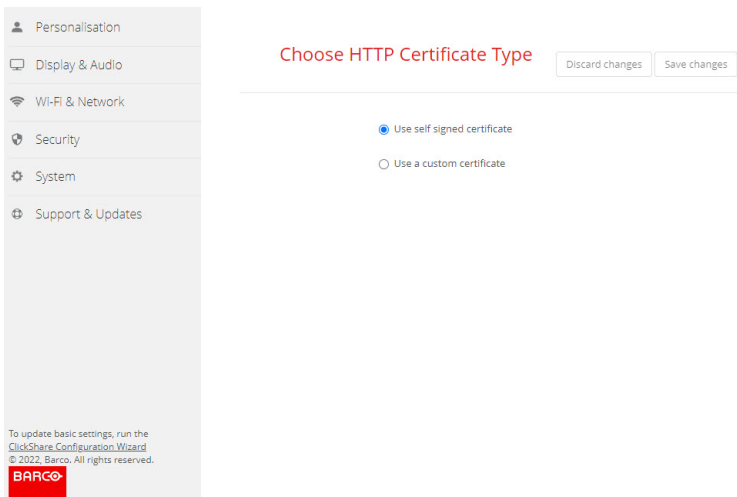


Abbildung 5–39 HTTP-Verschlüsselung

Upload des benutzerdefinierten Zertifikats

1. Geben Sie Ihre Passphrase ein.

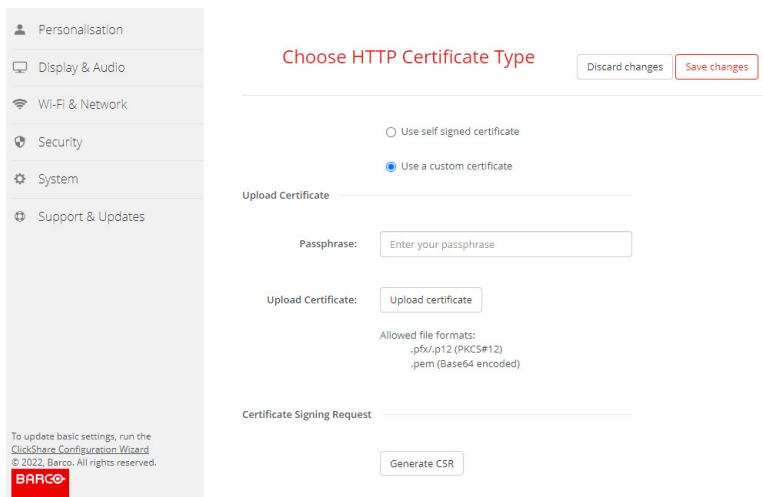


Abbildung 5–40 Upload des benutzerdefinierten Zertifikats

2. Klicken Sie auf **Zertifikat hochladen.**

Ein Browserfenster wird angezeigt.

3. Wählen Sie die gewünschte benutzerdefiniertes Zertifikatdatei aus und tippen Sie auf „Öffnen“.

Die zulässigen Dateiformate sind:

- .pfx/.p12 (PKCS#12)
- .pem (Base64-codiert)

4. Klicken Sie auf **CSR generieren.**

Die Seite *Zertifikatsignierungsanforderung herunterladen* wird angezeigt.

5. Füllen Sie die Seite aus und klicken Sie auf **Herunterladen.**

Eine CSR-Datei wird erstellt und auf Ihren Computer heruntergeladen.

5.27 Statusinformationen Base Unit

Statusinformationen

Folgende Informationen sind verfügbar:

- Modellinformationen, Name und Teilenummer
- Seriennummer
- Firmware-Version
- Zuerst verwendet
- Zuletzt verwendet
- Aktuelle Betriebszeit: Zeit seit dem letzten Start
- Gesamte Betriebszeit: Zeit seit dem ersten Start
- Gesamtstatus

Base Unit neu starten

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Support* → *Base Unit Status*.

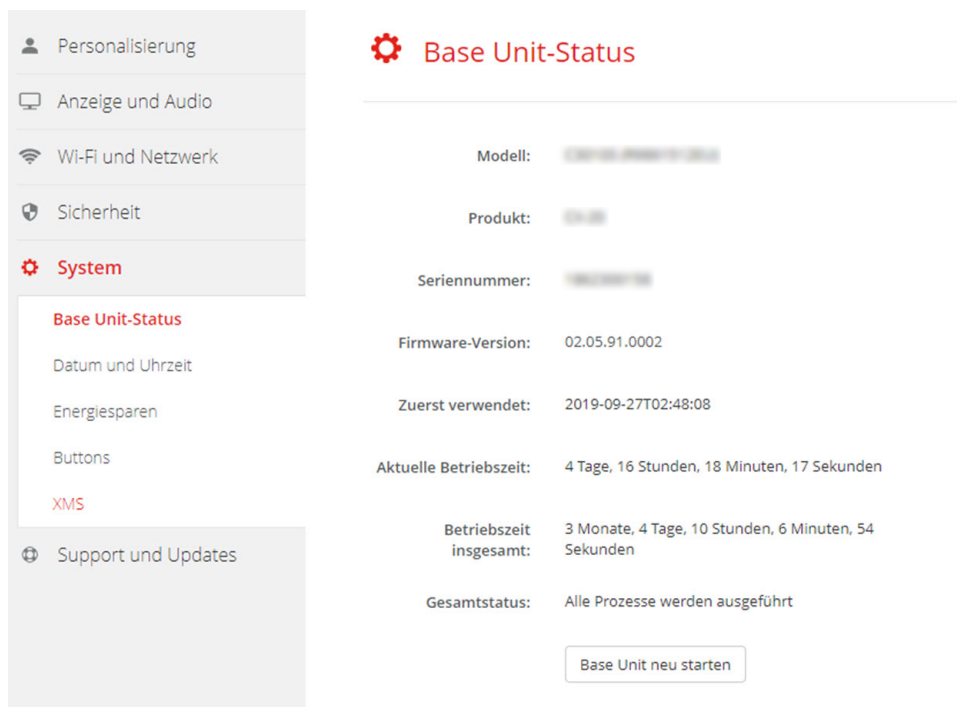


Abbildung 5–41

3. Um die Base Unit neu zu starten, klicken Sie auf **Base Unit neu starten**.

Während des Neustarts wird eine Mitteilung zum Neustart des ClickShare-Systems einschließlich Fortschrittsbalken angezeigt.

Nach dem Neustart müssen Sie sich erneut anmelden.

5.28 Manuelles Festlegen von Datum und Uhrzeit

Informationen zur Einrichtung von Datum und Uhrzeit

Das Datum und die Uhrzeit können manuell festgelegt werden. Hierzu wird die Zeitzoneanzeige oder mindestens ein NTP-Server verwendet.

Einrichtung

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *System* → *Datum und Uhrzeit*.

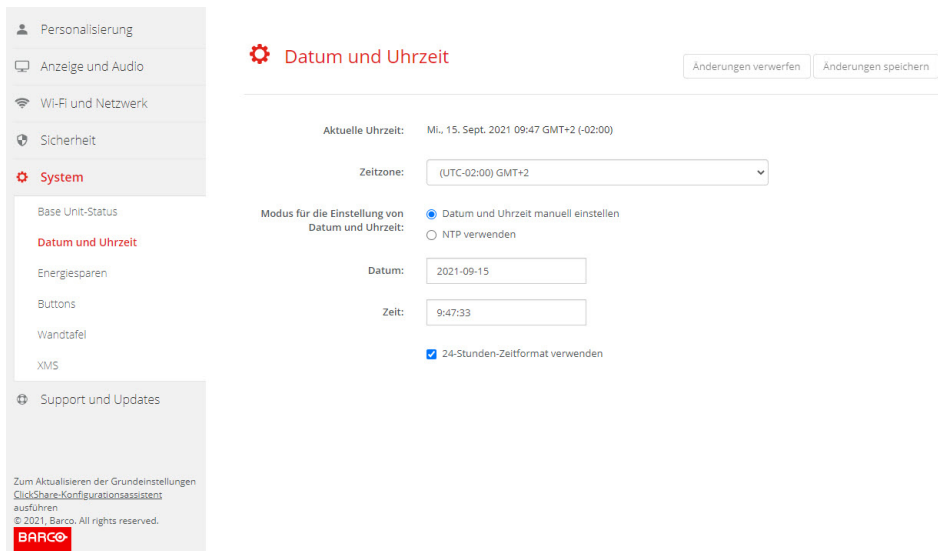


Abbildung 5–42 Manuelles Aktualisieren der Uhrzeit und des Datums

Die aktuelle Zeit wird neben *Aktuelle Zeit* angezeigt.

3. Wählen Sie Ihre Zeitzone. Klicken Sie auf das Dropdown-Listefeld neben *Zeitzone* und wählen Sie die entsprechende Zeitzone aus.
4. Aktivieren Sie das Optionsfeld vor *Datum und Uhrzeit manuell einstellen*.
5. Klicken Sie auf das Eingabefeld neben *Datum*, um das Datum zu ändern.

Ein Kalenderfenster wird geöffnet. Das aktuelle Datum wird mit rotem Hintergrund angezeigt.

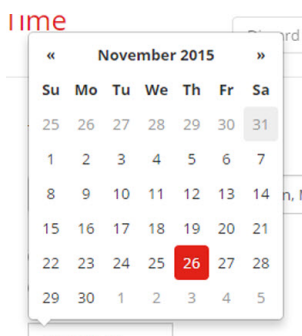


Abbildung 5–43 Auswahl des Datums

6. Um den Monat zu ändern, klicken Sie auf den Links- oder Rechtspfeil neben dem Monatsnamen, bis Sie den gewünschten Monat und das gewünschte Jahr erreicht haben.
Klicken Sie auf eine Nummer im Nummernfeld, um den Tag festzulegen.
7. Klicken Sie auf das Zeitfeld neben *Zeit*, um die Zeit zu ändern.
Ein Fenster mit drei Zählern wird geöffnet.



Abbildung 5–44 Festlegen der Uhrzeit

8. Klicken Sie auf den Aufwärts-/Abwärtspfeil für jeden Zähler, bis Sie die gewünschten Angaben für Stunde, Minuten und Sekunden erreicht haben.
9. Wählen Sie das Zeitformat aus.
Aktiviert: Das 24-Stunden-Zeitformat wird verwendet.
Nicht aktiviert: Das 12-Stunden-Zeitformat wird verwendet.
10. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu übernehmen.

5.29 Festlegen von Datum und Uhrzeit, Zeit-Server

Informationen zur Nutzung des NTP-Servers

Die Uhr wird kontinuierlich mit einem externen Zeit-Server synchronisiert, wodurch sich die Abweichung auf Millisekunden beschränkt. Weitere Zeit-Server können hinzugefügt werden.

Solange keine Synchronisierung mit einem Zeit-Server erfolgt, wird der Status als „Deaktiviert“ angezeigt.

Einrichtung

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *System* → *Datum und Uhrzeit*.

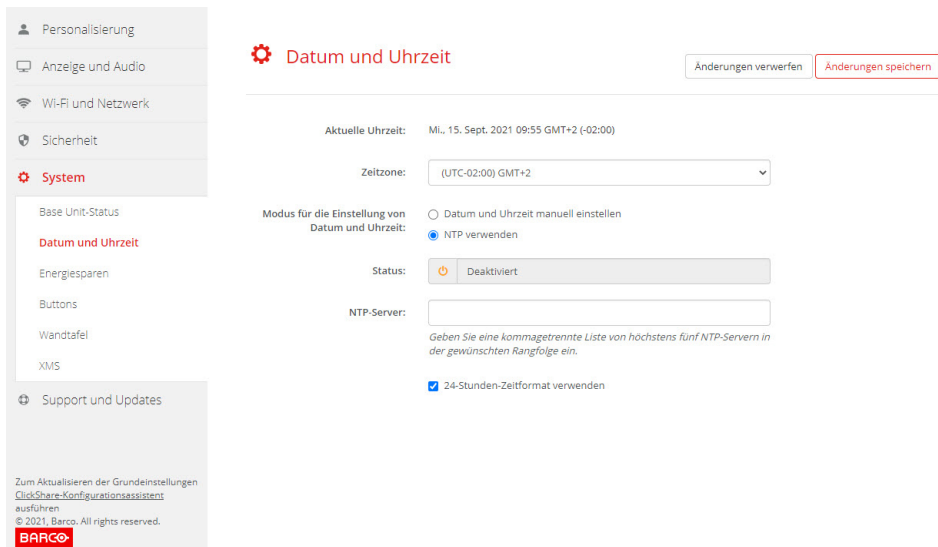



Abbildung 5–45 Festlegen des Zeit-Servers

Die aktuelle Zeit wird neben *Aktuelle Zeit* angezeigt.

3. Klicken Sie auf die Optionsschaltfläche neben *NTP verwenden*.
4. Geben Sie eine NTP-Server-Adresse neben *NTP-Server* ein. Geben Sie die IP-Adresse oder den Servernamen ein.

 **Hinweis:** Es können mehrere Server (maximal 5) hinzugefügt werden, die durch ein Komma voneinander getrennt sind.

5. Wählen Sie das Zeitformat aus.

Aktiviert: Das 24-Stunden-Zeitformat wird verwendet.

Nicht aktiviert: Das 12-Stunden-Zeitformat wird verwendet.

6. Klicken Sie auf **Änderungen speichern**, um die Änderungen zu übernehmen.

Es erfolgt eine Synchronisierung mit dem NTP-Server. Das Statusfeld zeigt den Fortschritt an.

5.30 Energiesparen

Informationen zu Standby

Standby nach (Minuten): Wird während des Zeitlimits für Standby keine Verbindung zum Client erkannt, wird die Base Unit in den ausgewählten Standby-Modus versetzt.

Standardeinstellung: Zeit bis Standby: 10 Minuten, die Base Unit wird in den Eco-Standby-Modus versetzt.

ECO-Modus

Wenn die Base Unit in den ECO-Standby-Modus versetzt wird, wird das HDMI-Ausgabesignal deaktiviert. Die LEDs der Base Unit blinken langsam weiß, um den ECO-Standby-Modus anzuzeigen.

Leistungsaufnahme im Eco-Standby: 2,6 W

Die Base Unit wird durch eine der folgenden Aktionen reaktiviert:

- Button oder App verbinden sich mit der Base Unit
- Drücken der Standby-Taste auf der Base Unit
- Kopplung eines Button über den USB-Anschluss der Base Unit
- Anschließen einer HDMI-Anzeige
- Wenn ein CEC-Ereignis eingeht

Standby-Modus

Wenn die Base Unit in den Deep-Standby-Modus wechselt, werden alle Prozesse heruntergefahren, einschließlich des Wi-Fi-Zugriffspunkts und der LAN-Verbindung. Die LEDs der Base Unit leuchten nicht, um diesen Standby-Modus anzuzeigen.

Die Base Unit wird nur reaktiviert, wenn die Standby-Taste an der Base Unit gedrückt wird.

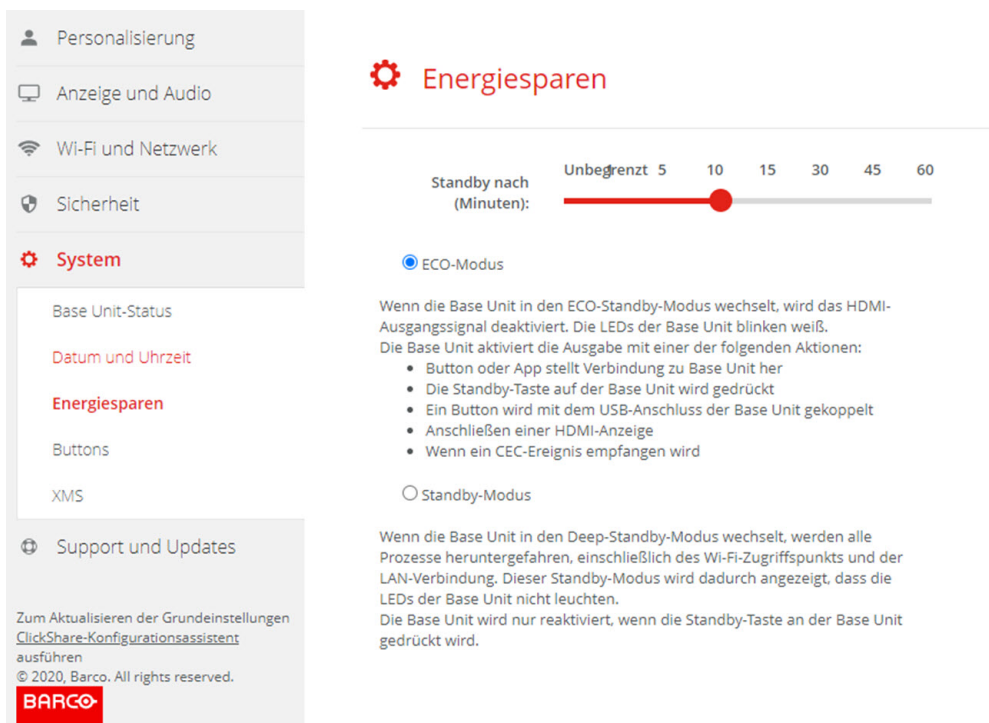


Abbildung 5–46 Energiesparen

So ändern Sie das Anzeigzeitlimit

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *System* → *Energiesparen*.
3. Bewegen Sie den Schieberegler nach links oder rechts, bis die gewünschte Standby-Zeit erreicht ist, um eine Verzögerungszeit festzulegen.

5.31 Buttons

Informationen zum Handbuch des Button

Die Button-Seite zeigt an, mit welcher Base Unit bzw. mit welchem Netzwerk die Buttons verbunden sind. Sie zeigt auch ihren aktuellen Status an.

Wenn eine Netzwerkverbindung besteht, zeigt sie die Domäne, die Identität und das bereitgestellte Zertifikat.

Die Buttons können mit der Base Unit oder mit einem externen Zugriffspunkt verbunden werden.

Alle Buttons, die mit der Base Unit verwendet werden, sind in der Liste der Buttons aufgeführt. Diese enthält:

- Seriennummer
- MAC-Adresse
- Artikelcode
- Firmware-Version
Sie können die Software der Buttons über Wi-Fi aktualisieren.
- Modell-Infos
- Anzahl der Verbindungen
- Letzte Verbindung

So bearbeiten Sie die Einstellungen

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *System* → *Buttons*.

The screenshot shows the 'Buttons' configuration page in the ClickShare Configurator. The left sidebar contains a navigation menu with categories like 'Personalisierung', 'Anzeige und Audio', 'Wi-Fi und Netzwerk', 'Sicherheit', 'System', 'Wandtafel', 'XMS', and 'Support und Updates'. The 'System' category is expanded, showing options like 'Base Unit-Status', 'Datum und Uhrzeit', 'Energiesparen', 'Buttons', 'Wandtafel', and 'XMS'. The 'Buttons' section is active, displaying a table of connected buttons. The table has columns for 'Auswählen', 'Seriennummer', 'MAC-Adresse', 'Artikelcode', 'Firmware', 'Modellinformationen', 'Verbindungen', and 'Letzte Verbindung'. Two buttons are listed: one with serial number 1200463655 and another with 1860086321. A 'Buttons bearbeiten' button is located in the top right corner of the main content area.

Auswählen	Seriennummer	MAC-Adresse	Artikelcode	Firmware	Modellinformationen	Verbindungen	Letzte Verbindung
<input type="checkbox"/>	1200463655	EC:5C:84:04:D4:21	R9861600D01C	04.18.00.0001	GEN4.1	6	2023-09-19T08:04:58
<input type="checkbox"/>	1860086321	08:3A:88:1F:19:6E	R9861600D01C	04.18.00.0001	GEN4.0	13	2023-09-19T08:04:43

Abbildung 5–47 Übersicht Buttons

Die aktuelle Liste der verbundenen Buttons mit ihren jeweiligen Details wird angezeigt.

3. Klicken Sie auf **Einstellungen bearbeiten (Edit settings)**.
4. Wählen Sie aus, ob Buttons eine Verbindung zu einem externen Zugangspunkt oder zu Ihrem ClickShare-Gerät herstellen sollen.



Hinweis: Für den externen Zugangspunkt müssen zusätzliche Einstellungen vorgenommen werden.

5.32 Buttons, externer Zugriffspunkt, EAP-TLS-Modus

So füllen Sie die Einstellungen aus

1. Füllen Sie die *Unternehmens-SSID* aus.

Buttons

Abbrechen Änderungen speichern

Buttons verbunden mit: Externer Zugriffspunkt

Einstellungen externer Zugriffspunkt

Authentifizierungsmodus: EAP-TLS

Unternehmens-SSID: Home Sweet Home

Domäne:

Identität:

Bescheinigung vorlegen: Clientzertifikat und Zertifikat der Zertifizierungsstelle

Client-Zertifikat hochladen: Bestand kiezen Geen bestand gekozen
Zulässige Dateiformate: .pfx (PKCS#12), .p12 (Base64 codiertes DER).
Die Datei sollte mindestens das Clientzertifikat und den entsprechenden privaten Schlüssel enthalten.

Kennwort Clientzertifikat:

Zertifikat Zertifizierungsstelle hochladen: Bestand kiezen Geen bestand gekozen
Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER).
Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.

Abbildung 5–48 Buttons, externer Zugriffspunkt, EAP-TLS-Modus

Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.

2. Füllen Sie *Domäne* und *Identität* aus.
3. Wählen Sie das Zertifizierungsverfahren aus. Klicken Sie auf das Dropdown-Feld und wählen Sie das gewünschte Verfahren aus.
 - Manually provide Client & CA certificates
 - Automatische Registrierung über SCEP

Manuelle Bereitstellung von Zertifikaten

1. Laden Sie ein Client-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Zulässige Dateiformate:

- .pfx (PKCS#12)
- .p12 (Base64-codiertes DER)

Die Datei sollte mindestens das Client-Zertifikat und den entsprechenden privaten Schlüssel enthalten.

2. Geben Sie das Kennwort für das Client-Zertifikat ein.
3. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem

- .cer
- .crt
- .pb7 (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

4. Speichern Sie die Änderungen.

Verwenden der automatischen Registrierung

Das Simple Certificate Enrolment Protocol (SCEP) ist ein Protokoll, das die Ausgabe und das Widerrufen von Zertifikaten in skalierbarer Weise ermöglicht. Die Unterstützung für SCEP ist integriert, um eine schnellere und reibungslosere Integration der ClickShare Base Unit und der Buttons in das Unternehmensnetzwerk zu ermöglichen.

Bis zur Base Unit-Firmware-Version 02.11.01 war die SCEP-Implementierung speziell auf den Network Device Enrollment Service (NDES) ausgerichtet, der Teil von Windows Server ist. Ab der Base Unit-Firmware-Version 02.12.00 unterstützen wir sowohl NDES als auch Standard-SCEP.

NDES erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Windows-Servers in Ihrem Netzwerk, der den NDES-Dienst ausführt. Nur http ist zulässig. Zum Beispiel: http://meinServer oder http://10.192.5.1.

SCEP-Benutzername: Dies ist ein Benutzer in Ihrem Active Directory, der die erforderliche Erlaubnis besitzt, auf den NDES-Dienst zuzugreifen und das abzufragende Kennwort anzufordern. Zur Absicherung sollte der Benutzer Mitglied der CA-Administratorengruppe sein (im Falle eines Einzel-CAs) oder Anmeldebefugnisse für die konfigurierten Zertifikatvorlagen besitzen.

SCEP-Kennwort: Das entsprechende Passwort für den SCEP-Benutzernamen, den Sie für die Authentifizierung beim Dienst verwenden.

Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.

Abbildung 5–49 Button-Einstellungen, Drahtlosclient, EAP-TLS, NDES

SCEP erfordert die folgenden Parameter:

SCEP-Server: Dies ist die IP-Adresse oder der Hostname des Servers, auf dem der SCEP-Dienst ausgeführt wird, mit angehängtem Port und Suffix. Nur http ist zulässig. Zum Beispiel: http://meinServer:8080/scep oder http://10.192.5.1/test

SCEP-Challenge: Das entsprechende abzufragende SCEP-Kennwort.

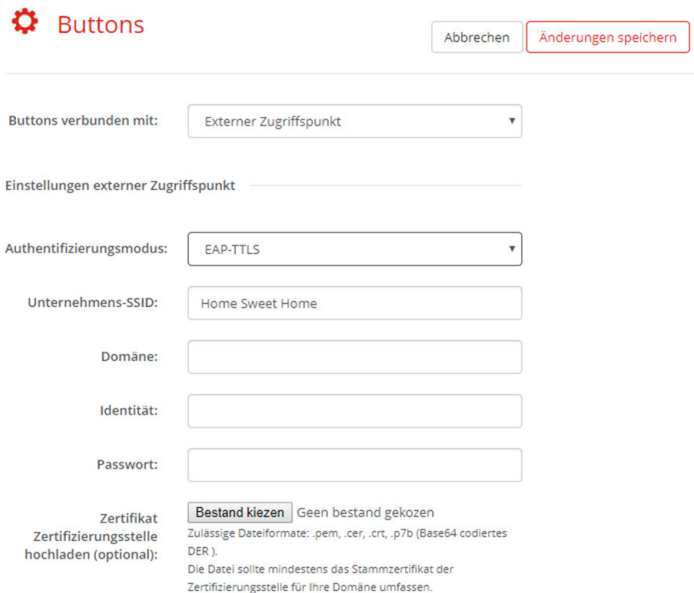
Allgemeiner Name (CN): Die Identität, die Sie mit dem Zertifikat verknüpfen möchten.

Abbildung 5–50 Button-Einstellungen, Drahtlosclient, EAP-TLS, SCEP

5.33 Buttons, externer Zugriffspunkt, EAP-TTLS-Modus

So füllen Sie die Einstellungen aus

1. Füllen Sie die *Unternehmens-SSID* aus.



Buttons Abbrechen Änderungen speichern

Buttons verbunden mit:

Einstellungen externer Zugriffspunkt

Authentifizierungsmodus:

Unternehmens-SSID:

Domäne:

Identität:

Passwort:

Zertifikat hochladen (optional): Geen bestand gekozen
 Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER).
 Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.

Abbildung 5–51 Buttons, externer Zugriffspunkt, EAP-TTLS-Modus

Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.

2. Füllen Sie *Domäne* und *Identität* aus.
3. Geben Sie ein *Kennwort* ein.
4. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem
- .cer
- .crt
- .p7b (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

5. Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu speichern.

5.34 Buttons, externer Zugriffspunkt, PEAP-Modus

So füllen Sie die Einstellungen aus

1. Füllen Sie die *Unternehmens-SSID* aus.

Buttons Abbrechen Anderungen speichern

Buttons verbunden mit:

Einstellungen externer Zugriffspunkt

Authentifizierungsmodus:

Unternehmens-SSID:

Domäne:

Identität:

Passwort:

Zertifikat Geen bestand gekozen
 Zertifizierungsstelle hochladen (optional):
 Zulässige Dateiformate: .pem, .cer, .crt, .p7b (Base64 codiertes DER).
 Die Datei sollte mindestens das Stammzertifikat der Zertifizierungsstelle für Ihre Domäne umfassen.

Abbildung 5–52 Buttons, externer Zugriffspunkt, PEAP-Modus

Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.

2. Füllen Sie *Domäne* und *Identität* aus.
3. Geben Sie ein *Kennwort* ein.
4. Laden Sie das CA-Zertifikat hoch. Klicken Sie auf „Datei auswählen“ und suchen Sie die gewünschte Datei.

Die folgenden Formate sind zulässig:

- .pem
- .cer
- .crt
- .p7b (Base64-codiertes DER)

Die Datei sollte mindestens das Stamm-CA-Zertifikat für Ihre Domäne enthalten.

5. Klicken Sie auf **Änderungen speichern**, um die Einstellungen zu speichern.

5.35 Buttons, externer Zugriffspunkt, WPA2-PSK-Modus

So füllen Sie die Einstellungen aus

1. Füllen Sie die *Unternehmens-SSID* aus.

Buttons

Abbrechen Änderungen speichern

Buttons verbunden mit: Externer Zugriffspunkt

Einstellungen externer Zugriffspunkt

Authentifizierungsmodus: WPA2-PSK

Unternehmens-SSID: Home Sweet Home

Passphrase:

Abbildung 5–53 Buttons, externer Zugriffspunkt, WPA2-PSK-Modus

Die SSID der drahtlosen Infrastruktur Ihres Unternehmens, mit der sich die ClickShare Buttons verbinden.

2. Füllen Sie die Passphrase aus.

Der in WPA2-PSK für die Authentifizierung in der drahtlosen Infrastruktur verwendete Schlüssel. Dies kann eine 64-stellige hexadezimale Zeichenkette oder ein Kennwort mit 8 bis 63 druckbaren ASCII-Zeichen sein.

3. Klicken Sie auf **Änderungen speichern (Save changes)**, um die Einstellungen zu speichern.

5.36 Blackboard



Nur verfügbar beim C-10.

Informationen zur Wandtafel

Das Speichern der Informationen von einer Wandtafel kann aktiviert oder deaktiviert werden. Wenn es aktiviert ist, werden die Informationen auf der Festplatte aller verbundenen Buttons, den verbundenen ClickShare-Apps und auf den mit der Base Unit verbundenen USB-Sticks gespeichert.

So ändern Sie die Wandtafel-Einstellung

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *System* → *Tafel*.

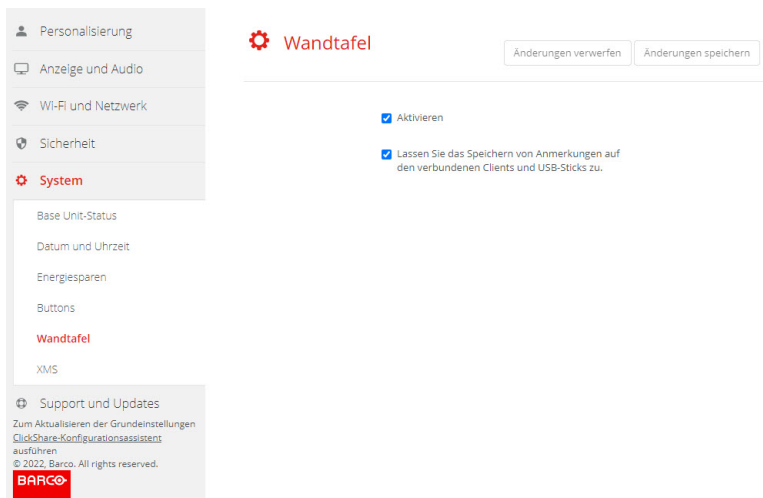


Abbildung 5–54 Anmerkungen speichern

3. Aktivieren oder deaktivieren Sie das Kontrollkästchen vor Aktivieren oder Deaktivieren, um die Wandtafel-Funktion zu aktivieren oder zu deaktivieren.

Aktiviert: Wandtafel-Funktion aktiviert

Deaktiviert: Wandtafel-Funktion deaktiviert

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen vor *Speichern der Anmerkungen auf verbundenen Clients und USB-Sticks zulassen*.

Aktiviert: Anmerkungen auf der Wandtafel können gespeichert werden.

Deaktiviert: Es können keine Anmerkungen auf der Wandtafel gespeichert werden.

5.37 XMS Cloud-Integration

Übersicht

Wenn Ihr Gerät nicht registriert und mit dem Cloud-Dienst verbunden ist, wird die folgende Meldung angezeigt: Das Gerät wurde nicht zu XMS Cloud hinzugefügt. Um Ihr Gerät zur XMS Cloud hinzuzufügen, klicken Sie hier: <https://xms.barco.com/add>.

Das Geräte-Token wird vergeben und kann kopiert werden.

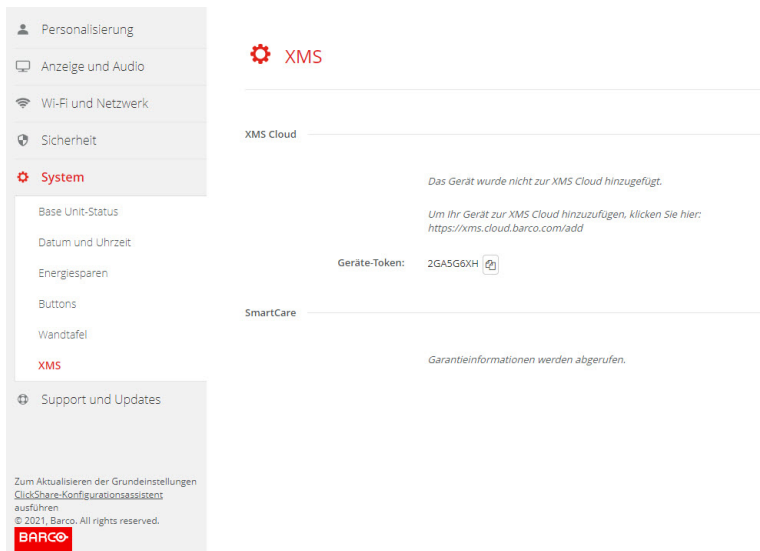


Abbildung 5–55 XMS Cloud, keine Registrierung

Wenn Ihr Gerät korrekt registriert ist, wird die folgende Meldung angezeigt: *Das ClickShare-Gerät wurde erfolgreich registriert.*

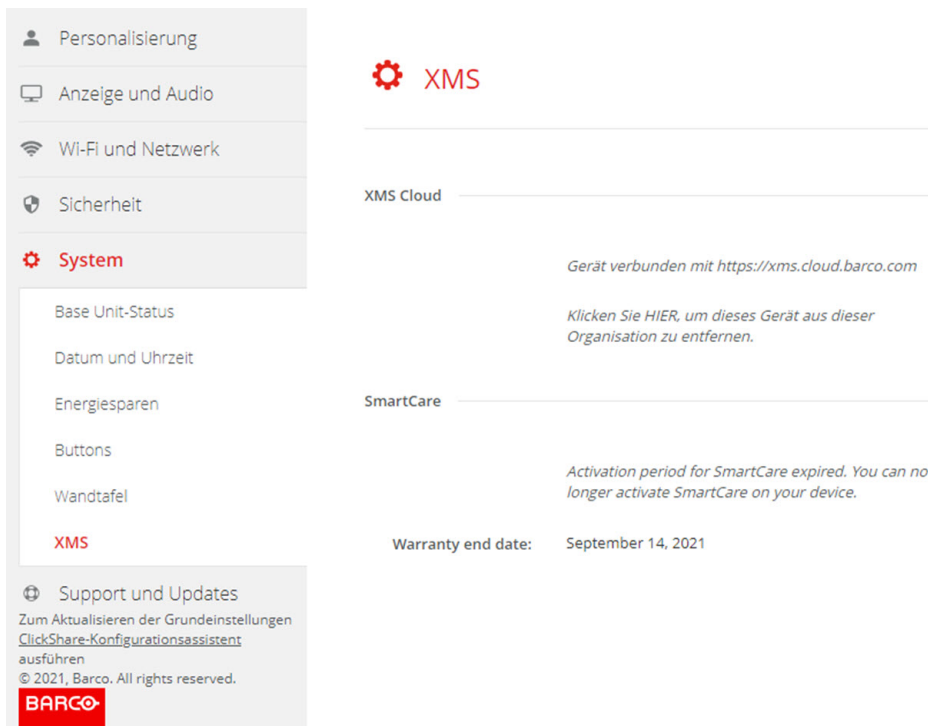


Abbildung 5–56 XMS Cloud

Möglichkeiten

1. Überprüfen Sie die Netzwerkeinstellungen oder registrieren Sie Ihr Gerät bei XMS Cloud.

Befolgen Sie die Schritte unter [“XMS Cloud-Registrierung”, Seite 50](#).

SmartCare

Das SmartCare-Paket ist im Kauf jeder ClickShare-Einheit enthalten.

Für die seltenen Fällen, in denen es zu Problemen mit den ClickShare-Einheiten kommt, haben wir SmartCare eingeführt, ein Servicepaket, das Ihrem Unternehmen Budgetplanbarkeit, einen schnellen Hardwareaustausch und Support von Experten sowohl von Barco als auch von unseren Partnern für bis zu fünf Jahre bietet.

Wenn SmartCare aktiviert wurde, wird im SmartCare-Bereich die Meldung *SmartCare aktiv, gültig bis ...* angezeigt.

Wenn es noch nicht aktiviert wurde, haben Sie nach der ersten Einrichtung sechs Monate lang Zeit, um SmartCare zu aktivieren und fünf Jahre Hardware-Abdeckung zu genießen.

Wenn der Aktivierungszeitraum abgelaufen ist, wird das Garantie-Enddatum angezeigt.

5.38 Firmware-Aktualisierung

Informationen zur Firmware-Aktualisierung

Die Firmware der Base Unit kann über die Web-Schnittstelle aktualisiert werden. Die aktuelle Version der Firmware ist auf der Barco-Website verfügbar.

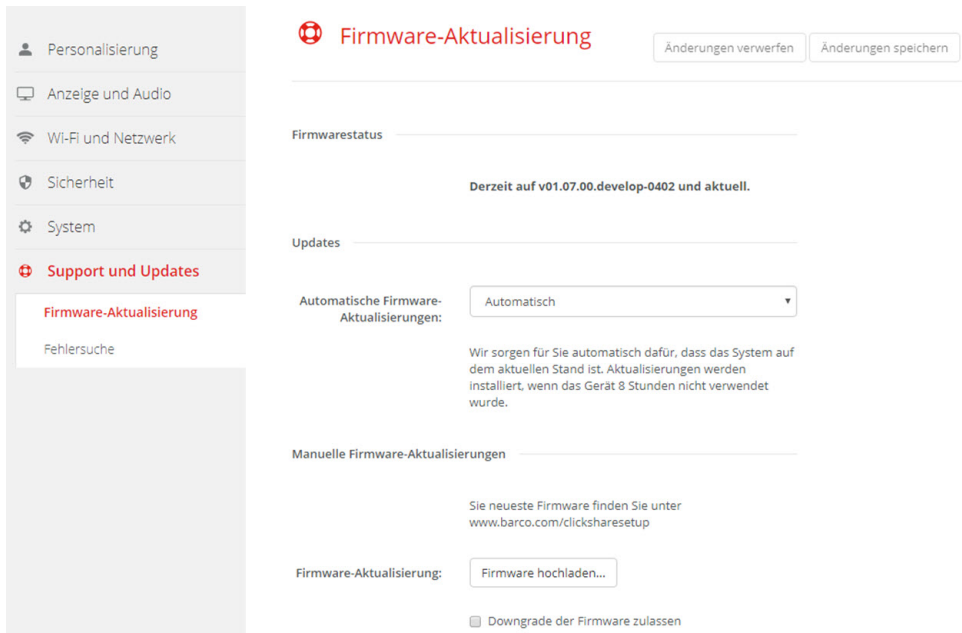


Abbildung 5–57 Firmware-Aktualisierung


Über automatische Firmware-Aktualisierungen


Es gibt drei Möglichkeiten, automatische Aktualisierungen zu konfigurieren:

- **Automatisch:** Das System erkennt Firmware-Aktualisierungen automatisch und installiert sie, wenn es nicht verwendet wird.
- **Benachrichtigen:** Das System erkennt Firmware-Aktualisierungen automatisch und benachrichtigt Sie über das Webschnittstellen-Dashboard und die Firmware-Seite. Die Aktualisierung kann dann über die Seite *Support und Updates* → *Firmware* gestartet werden.
- **Aus:** Das System erkennt keine Firmware-Aktualisierungen und benachrichtigt Sie nicht.

Manuelle Firmware-Aktualisierung

1. Laden Sie die aktuelle Version der Firmware von der Barco-Website herunter.
2. Melden Sie sich bei *Configurator* an.
3. Klicken Sie auf *Support und Updates* → *Firmware*.
4. Um eine Firmware-Version hochzuladen, klicken Sie auf **Firmware hochladen...**
Ein Browserfenster wird angezeigt.
5. Navigieren Sie zu der Datei mit der neuen Firmware und klicken Sie auf **Öffnen**, um das Hochladen zu starten.

 **Hinweis:** Die Datei sollte eine .enc-Datei sein. Möglicherweise müssen Sie die von der Barco-Website geladene Datei extrahieren.

 **Hinweis:** Das Aktualisieren der Base Unit-Software kann einige Minuten dauern. Der Fortschritt kann auf dem Monitor im Besprechungsraum verfolgt werden.

Die Software der Base Unit wird aktualisiert.



Falls ein Downgrade der Firmware auf der Base Unit erforderlich ist, aktivieren Sie das Kontrollkästchen neben *Downgrade der Firmware zulassen*.

Firmware-Aktualisierung ohne den Configurator

Neben der Verwendung des Configurator zur Aktualisierung der Firmware sind folgende Methoden möglich:

- Wenn Ihr Gerät mit einem Netzwerk verbunden und über die XMS (Cloud)-Verwaltungsplattform verwaltet wird, kann die Firmware über diese Verwaltungslösung aktualisiert werden. Ausführliche Informationen zur Aktualisierung der Firmware auf diese Art finden Sie auf den Barco-Webseiten zu XMS (<https://www.barco.com/en/page/xms-cloud-management-platform>).
- Laden Sie die Firmware auf einen USB-Stick herunter und schließen Sie ihn an Ihr Gerät an. Ausführliche Informationen finden Sie unter "Aktualisieren der C-5, C-10 Gen2-Firmware", Seite 140.

5.39 Support und Updates, Fehlersuche, Protokolleinstellungen

Informationen zur Protokollierung

Die Protokolldaten des Button und der Base Unit sind in Protokolldateien auf der Base Unit gespeichert. Diese Protokolldateien können Informationen zur Fehlerbeseitigung enthalten. Sie können auf einen lokalen Computer heruntergeladen und auf der Base Unit gelöscht werden. Die Fehlerprotokollierung deckt nur ein paar Stunden ab, bevor sie überschrieben wird. Daher ist es wichtig, die Protokollierung sofort herunterzuladen, sobald Sie ein Problem mit Ihrem System entdecken.

Hinweise zum Gebrauch

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Support und Updates* → *Fehlersuche*.

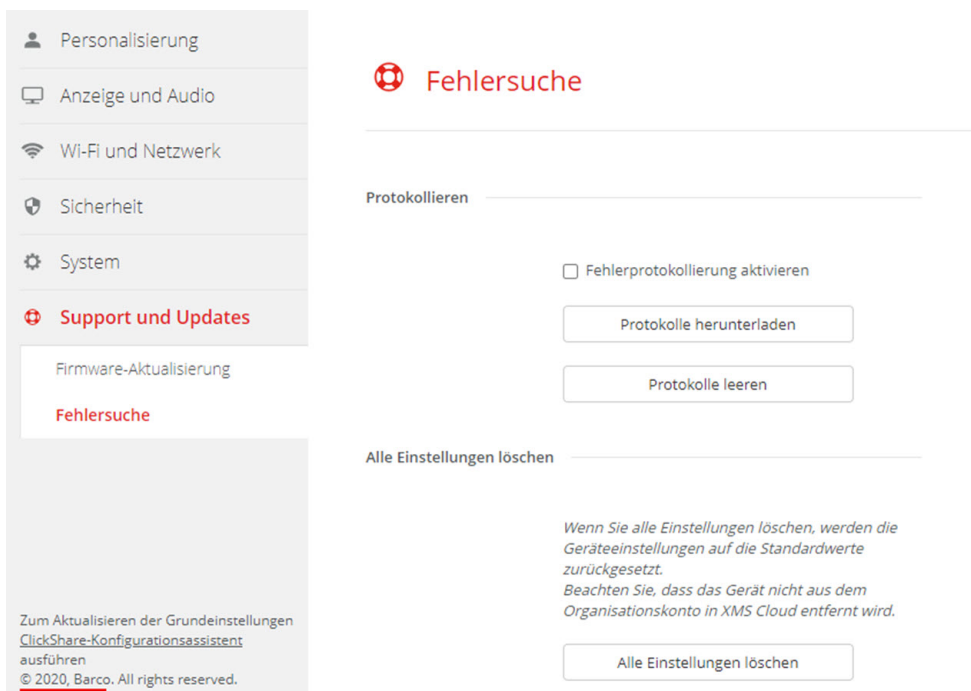


Abbildung 5–58 Fehlersuche, Protokollierung

3. Aktivieren Sie das Kontrollkästchen neben *Fehlerprotokollierung aktivieren*, um ein Fehlerprotokoll zu erstellen.
4. Reproduzieren Sie das Problem, das Sie melden möchten.
5. Klicken Sie auf **Protokolle herunterladen**, um die aktuelle Protokolldatei herunterzuladen.
6. Klicken Sie auf **Protokolle leeren**, um die aktuelle Protokolldatei zu löschen.

5.40 Fehlerbehebung, Alle Einstellungen löschen

Informationen zum Löschen aller Einstellungen

Wenn Sie alle Einstellungen löschen, werden die Geräteeinstellungen auf die Standardeinstellungen zurückgesetzt. Es ist nicht erforderlich, die Schritte zur Verfahren zum Onboarding zu durchlaufen.



Das Gerät wird nicht aus dem Unternehmenskonto in XMS Cloud entfernt.

So gehen Sie zum Löschen vor

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Support und Updates* → *Fehlersuche*.
3. Um alle Einstellungen zu löschen und auf die Standardeinstellungen zurückzusetzen, klicken Sie auf **Alle Einstellungen löschen**.

The screenshot displays the 'Fehlersuche' (Troubleshooting) interface. On the left, a sidebar lists various settings categories, with 'Support und Updates' and 'Fehlersuche' highlighted. The main area shows the 'Fehlersuche' title and a 'Protokollieren' (Logging) section. This section includes a checkbox for 'Fehlerprotokollierung aktivieren' (Enable error logging), which is currently unchecked. Below this are two buttons: 'Protokolle herunterladen' (Download logs) and 'Protokolle leeren' (Clear logs). Further down, there is an 'Alle Einstellungen löschen' (Delete all settings) section with a button labeled 'Alle Einstellungen löschen'. A warning message is displayed below this button, stating that deleting all settings will reset device settings to default values and that the device will not be removed from the organization's account in XMS Cloud.

Abbildung 5–59 Fehlersuche, Protokollierung

5.41 Auf Werkseinstellungen zurücksetzen

Informationen zum Zurücksetzen

Wenn Sie ein Zurücksetzen auf die Werkseinstellungen durchführen, werden die Geräteeinstellungen auf die werkseitigen Standardeinstellungen zurückgesetzt. Des Weiteren wird die Base Unit aus dem Unternehmenskonto in XMS Cloud entfernt und die Schritte für die erstmalige Konfiguration werden gestartet, als ob das Gerät gerade erst ausgepackt worden wäre.



Das Gerät muss mit dem Internet verbunden sein, um die erstmalige Konfiguration abzuschließen.

So nehmen Sie die Zurücksetzung vor

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Support und Updates* → *Fehlersuche*.

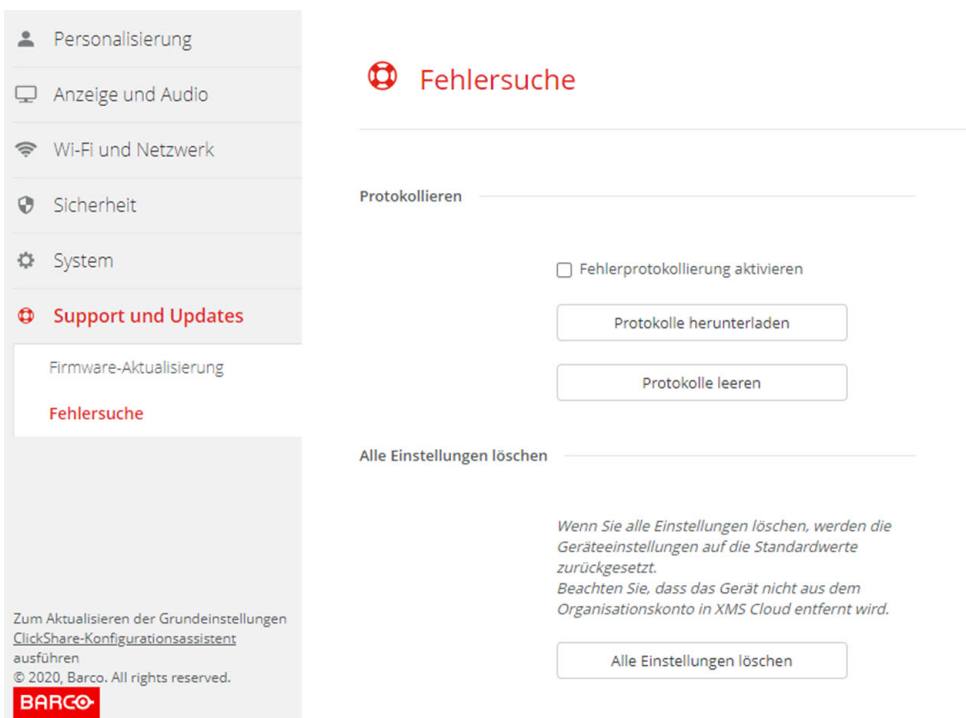


Abbildung 5–60 Zurücksetzen auf Werkseinstellungen

3. Klicken Sie auf **Auf Werkseinstellungen zurücksetzen**.

Die folgende Meldung wird angezeigt: „Mit diesem Vorgang werden alle Einstellungen der Base Unit gelöscht und durch die Standardeinstellungen ersetzt. Möchten Sie wirklich fortfahren?“

4. Wenn Sie fortfahren möchten, klicken Sie auf **Yes, remove all settings (Ja, alle Einstellungen löschen)**. Wenn nicht, klicken Sie auf **No, I changed my mind (Nein, ich habe meine Meinung geändert)**.

Sobald Sie auf „Ja“ geklickt haben, startet das System neu.

5.42 Fehlersuche, Diagnose

Informationen zur Diagnose

Ein TCP-Auslesetest erfasst zwei Minuten lang die Netzwerkdaten. Das Ergebnis wird in eine separate Datei im Protokollarchiv geschrieben. Diese Datei kann nur mit einem Tool für die Netzwerküberwachung geöffnet werden.

Erste Schritte

1. Melden Sie sich bei *Configurator* an.
2. Klicken Sie auf *Support und Updates* → *Fehlersuche*.
3. Klicken Sie im Diagnose-Bereich auf **TCP-Auslesetest ausführen**.

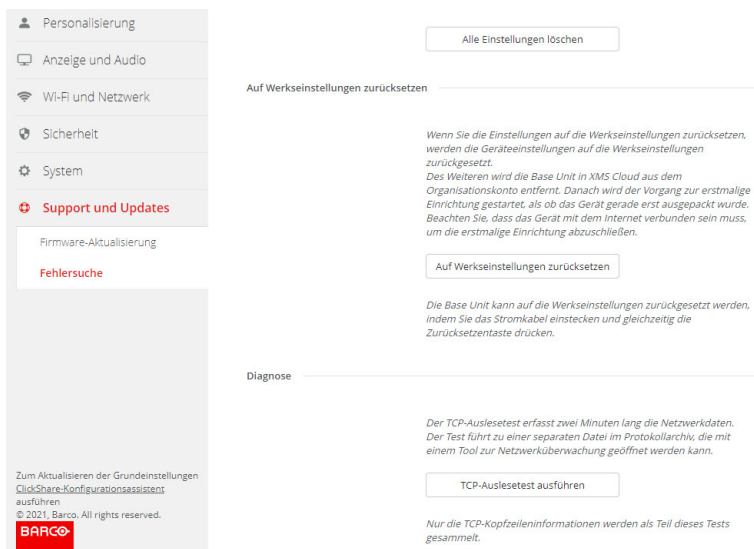


Abbildung 5–61 Fehlersuche, Diagnose

Eine separate Datei wird in das Protokollarchiv geschrieben.

Nur die TCP-Header-Informationen werden als Teil dieses Tests zusammengestellt.

Firmware- Aktualisierungen

6

6.1	Aktualisieren der C-5, C-10 Gen2-Firmware	140
-----	---	-----

6.1 Aktualisieren der C-5, C-10 Gen2-Firmware



Wenn Sie das Gerät zum ersten Mal starten, ist eine Softwareaktualisierung erforderlich. Diese Aktualisierung kann nur über das Netzwerk erfolgen.

Informationen zu Firmware-Aktualisierungen

Es gibt verschiedene Möglichkeiten, um die Software der Base Unit zu aktualisieren:

- automatische Aktualisierungen, wenn eine Verbindung zum Netzwerk besteht oder wenn das Gerät in XMS Cloud konfiguriert ist.
- über den Configurator, weitere Informationen, siehe [“Firmware-Aktualisierung”](#), Seite 133
- durch das Kopieren der Software auf einen USB-Stick

So aktualisieren Sie die Software der Base Unit durch das Kopieren der Software auf einen USB-Stick

1. Laden Sie die aktuelle Version der Firmware von der Barco-Website www.barco.com/clickshare herunter. Klicken Sie auf **Support** und wählen die Schaltfläche für die Firmware-Aktualisierung Ihres Gerätetyps.
2. Extrahieren Sie die ZIP-Datei.
3. Kopieren Sie die ENC-Datei auf einen USB-Stick.
Sie können mehrere Firmwares für mehrere Gerätearten auf dem gleichen Stick speichern.
4. Schließen Sie den USB-Stick am USB-Anschluss an der Vorderseite der Base Unit an.
5. Folgen Sie den Anweisungen auf dem Bildschirm im Besprechungsraum.
6. Wenn die Bildschirmmeldung angibt, dass der Vorgang abgeschlossen ist, können Sie den USB-Stick entfernen.

Die Base Unit wird neu gestartet.

Fehlerbehebung

7

7.1	Liste der Fehlerbehebungen	142
-----	----------------------------------	-----

7.1 Liste der Fehlerbehebungen

Barco-Knowledge Base und YouTube-Videos

Besuchen Sie die Produktseite von Barcos Website und wählen Sie in der rechten Spalte die Option **Support**. Sie erhalten Zugriff auf Barcos *Knowledge Base* (<https://www.barco.com/en/support/knowledge-base>) und die *aktuellsten Tutorialvideos*. Weitere YouTube-Videos finden Sie unter <https://www.youtube.com/user/barcoTV>. Wählen Sie dort ClickShare aus.

Problemlösung

Problem	Ursache	Lösung
Die Bildqualität auf dem Monitor im Besprechungsraum ist nicht zufriedenstellend	Die Qualität oder Länge des Kabels zwischen Base Unit und dem Monitor oder die Verbindung zwischen diesen beiden. Schlechte Auflösung auf dem Monitor Das System kann die durchschnittliche Laptop-Auflösung von 3 Megapixel verarbeiten. Beim Hoch- oder Runterskalieren auf dem Monitor im Besprechungsraum können jedoch sichtbare Artefakte auftreten.	<ul style="list-style-type: none"> Tauschen Sie das Kabel aus. Verwenden Sie ein anderes Kabel. <ul style="list-style-type: none"> Ändern Sie die Auflösung auf der Webschnittstelle und passen sie diese der nativen Auflösung des Monitors im Besprechungsraum an.
Die Drahtlosverbindung der Benutzer ist schlecht. Die Verbindung vom Button zur Base Unit wird immer wieder unterbrochen.	Überlastung der Drahtlosverbindung Geringe Signalstärke	<ul style="list-style-type: none"> Verwenden Sie einen WiFi-Scanner, um einen freien Drahtloskanal zu finden, und wählen Sie diesen über die Webschnittstelle aus. Sie können hierzu sowohl kommerzielle, als auch kostenlose Online-Tools, wie inSSIDer oder Xirrus verwenden. Lesen Sie „WiFi-Einstellungen“. Stellen Sie die Base Unit näher an den Tisch im Besprechungsraum. Entfernen Sie so viele Hindernisse wie möglich zwischen den Buttons und der Base Unit.
Die Webschnittstelle ist nicht verfügbar	Browser Keine Verbindung	<ul style="list-style-type: none"> Verwenden Sie einen anderen Browser (Version). Überprüfen Sie die Browser-Einstellungen. Es gibt drei Möglichkeiten, um auf die Webschnittstelle zuzugreifen. Lesen Sie das entsprechende Kapitel in der Dokumentation. Überprüfen Sie die Proxy-Einstellungen
Den Benutzern wird kein ClickShare-Laufwerk angezeigt,	<ul style="list-style-type: none"> Die Laufwerke werden nicht automatisch aktualisiert 	<ul style="list-style-type: none"> Aktualisieren Sie die Ansicht auf Ihrem Laptop.

Problem	Ursache	Lösung
wenn sie den Button an ihren Laptop anschließen.	<ul style="list-style-type: none"> Windows versucht das ClickShare-Laufwerk einem bereits reservierten Laufwerksbuchstaben zuzuweisen <p>Eine schlechte Verbindung zum USB-Anschluss am Laptop</p> <ul style="list-style-type: none"> Einige USB-Geräte sind möglicherweise aufgrund einer Unternehmensrichtlinie blockiert. Die USB-Anschlusseinstellungen auf dem Laptop schränken möglicherweise die Verwendung von Hochleistungs-USB-Geräten ein, wenn der Laptop über den Akku versorgt wird. 	<ul style="list-style-type: none"> Verwenden Sie Microsoft Windows Disk Management, um das Laufwerk einem freien Laufwerksbuchstaben zuzuweisen. Erneut am USB-Anschluss anschließen. Verwenden Sie einen anderen USB-Anschluss. Starten Sie den Laptop neu. <p>Wenn möglich, ändern Sie die Richtlinie für den USB-Anschluss am Laptop.</p>
Geringe Videoleistung	Laptopleistung	<ul style="list-style-type: none"> Senken Sie die Bildschirmauflösung auf dem Laptop. Deaktivieren Sie die Hardware-Beschleunigung für Video. Verwenden Sie nur einen Teil des Monitors, um das Video zu zeigen. Klicken Sie mit der rechten Maustaste auf das ClickShare-Symbol in der Systemleiste und klicken Sie dann auf „Erfassungsmodus“, um die aktuelle Einstellung umzuschalten.
	Drahtlose Konnektivität	Siehe „Die Konnektivität der Benutzer ist schlecht“
Das Video wird nicht auf dem Bildschirm angezeigt	Der Player verwendet Überdeckungen	<ul style="list-style-type: none"> Deaktivieren Sie die Verwendung von Überdeckungen in den Einstellungen des Videoplayers. Das Video ist durch HDCP geschützt und kann nicht mit dem ClickShare wiedergegeben werden.
Einige Windows-Programme werden nicht auf dem Monitor angezeigt	Die Verwendung von Überdeckungen, 3D oder Hardware-Beschleunigung im GPU	<ul style="list-style-type: none"> Deaktivieren Sie Überdeckungen oder Hardware-Beschleunigung im GPU. Deaktivieren Sie AeroGlass unter Windows 7

Problem	Ursache	Lösung
<p>Unter Windows 7 erscheint die folgende Nachricht über das Windows Aero-Farbschema: „Windows hat festgestellt, dass die Verbindung Ihres Computers langsam ist. Dies könnte durch zu wenige Ressourcen für die Ausführung des Windows Aero-Farbschemas verursacht werden. Für eine Verbesserung...“.</p>	<p>ClickShare verwendet Ressourcen vom GPU. In Kombination mit anderen Programmen, die diese Ressourcen verwenden, zeigt Windows 7 manchmal diese Nachricht an und schlägt vor, Aero zu deaktivieren, um die Leistung Ihres Laptops zu verbessern.</p>	<ul style="list-style-type: none"> • Aktualisieren Sie die Base Unit auf die aktuelle Softwareversion. <p>Diese Nachricht können Sie ruhigen Gewissens ignorieren und „Aktuelles Farbschema beibehalten“ wählen.</p>
<p>Ihr Bildschirm wird nicht durch Druck auf den Button auf dem Monitor angezeigt</p>	<p>Die Anzahl der geteilten Videos auf dem Bildschirm wurde überschritten. Wenn der Raumdock verwendet wird, kann nur ein Teilnehmer seinen Bildschirm teilen.</p> <p>Die ClickShare-Software wird nicht ausgeführt.</p>	<p>Verwenden Sie die Vollbildanzeigefunktion, indem Sie den Button zwei Sekunden lang gedrückt halten.</p> <p>Gehen Sie zum ClickShare-Laufwerk und führen Sie die Software aus.</p>
<p>Ihr Inhalt wird vom Monitor entfernt und die LEDs auf dem Button blinken weiß</p>	<p>Die Verbindung zur Base Unit wurde unterbrochen.</p>	<p>ClickShare versucht die Verbindung automatisch wiederherzustellen. Falls dies nicht funktioniert, blinken die LEDs auf dem Button rot.</p> <p>Trennen Sie den Button von Ihrem Laptop und versuchen Sie es mit einem anderen Button.</p>
<p>Auf dem Monitor wird überhaupt nichts angezeigt.</p>	<p>Die Monitore sind ausgeschaltet.</p> <p>Das Monitorkabel ist nicht richtig angeschlossen</p> <p>Der Monitor erkennt die Base Unit nicht oder kann ihre Ausgangsauflösung nicht anzeigen.</p> <p>Die Base Unit ist im Standby-Modus</p>	<p>Schalten Sie die Monitore ein.</p> <p>Schließen Sie das Monitorkabel an den Monitor und an die Base Unit an.</p> <p>Ändern Sie die entsprechende Einstellung über die Webschnittstelle.</p> <p>Drücken Sie kurz auf die Standby-Taste auf der Base Unit oder schließen Sie einen Button an und führen Sie die ClickShare-Software aus.</p>
<p>Schlechte WiFi-Konnektivität</p>	<p>Überlastung des Funkkanals</p> <p>Metallgehäuse, Wände, Bauelemente ... können Reflexionen erzeugen, die das Drahtlossignal verschlechtern.</p> <p>Hindernisse zwischen den Buttons und der Base Unit verursachen</p>	<p>Verwenden Sie Scan-Tools für Drahtlosnetzwerke, um nach freien oder am geringsten überlasteten Kanälen zu suchen.</p> <p>Stellen Sie die Base Unit an einen anderen Platz im Raum.</p>

Problem	Ursache	Lösung
	eine Verringerung der Funksignalstärke und -qualität.	Vermeiden Sie eine Platzierung in Gehäusen, Zwischendecken, unter dem Tisch, hinter der Wand, in einem anderen Raum... Lesen Sie das ClickShare-Whitepaper zu WLAN, siehe www.barco.com/clickshare .
Die Webschnittstelle zeigt einen Fehler in den Vorgängen „WiFi-Zugangspunkt-Daemon“ und/oder „DHCP-Server“	Die Konfigurationsdatei ist beschädigt	Navigieren Sie zu der Registerkarte „Konfiguration“ auf der Webschnittstelle und klicken Sie auf „Standardeinstellungen laden“.
ClickShare-Base Unit startet nicht korrekt	Die Konfigurationsdatei ist beschädigt	Navigieren Sie zu der Registerkarte „Konfiguration“ auf der Webschnittstelle und klicken Sie auf „Standardeinstellungen laden“.
Keine LAN-Verbindung zur Base Unit	Falsche IP-Adresse	Die IP-Adresse liegt nicht in Ihrer LAN-Reichweite DHCP ist nicht aktiviert.
Keine WLAN-Verbindung zur Base Unit	Die SSID ist nicht korrekt	Geben Sie die korrekte SSID ein

Finden Sie das aufgetretene Problem in der folgenden Tabelle und wenden Sie die Lösung an.

Index

A

API-Dokumentation 111
API-Einstellungen 111
API-Passwort 115
Audio-Setup 85

B

Base Unit
 Display
 Verbindung 36
 Ein-/Ausschalten
 Verbindung 40
 Erste Einrichtung 42
 Bevorzugte Methode 44
 Keine Konfiguration 43
 Ethernet
 Verbindung 39
 Info 16
 LAN
 Verbindung 39
 Montage
 Verfahren 24
 Neu starten 118
 Tischgerät 25
 Touch-Screen
 Verbindung 38
Bedingung 20
Besprechungsraumname 77
Bewährte Situation 28
Blackboard 130
Button
 Koppeln 62
 Vorbereiten 61
Buttons 124
 Externer Zugriffspunkt
 EAP-TLS 125
 EAP-TTLS 127
 PEAP 128
 WPA2-PSK 129

C

C-5, C-10 Gen2
 Info 10
ClickShare API 111
 Kennwort 115
Computer-Onboarding
 XMS Cloud 50
Configurator 69
 Zugang 71
Configurator-Passwort 115

D

Datum – Uhrzeit
 Manuell 119
 NTP-Server 121
 Zeit-Server 121
Desktop-App 67
 MSI-Installationsprogramm 68
Dienstleistungen
 Mobile Geräte 108
 PresentSense 110

E

Energiesparen 122
Erste Einrichtung
 Base Unit 42
 Bevorzugte Methode 44
 Keine Konfiguration 43
Erste Schritte 19
Extension Pack 63
 Installationsprogramm 64

F

Fehlerbehebung 141
 Protokollierung 136
Fehlersuche
 Diagnose 138

Protokolleinstellungen 135
 Firmware
 Update 139–140
 Base Unit 133
 Button 133

G

Grundlegender Arbeitsablauf 22

H

Hintergrundbild 79
 personalisiert 81
 HTTP-Verschlüsselung 116

K

Kalenderintegration 55
 Konfiguration
 Assistent 75
 Konfiguration hochladen 83
 Konfigurationsdateien 83
 Koppeln
 Button 62

L

LAN-Einstellungen 99
 Kabelgebundene Authentifizierung 102
 EAP-TLS 103
 EAP-TTLS 106
 Liste der Fehlerbehebungen 142

M

Mobile Geräte 108
 Mobiles Gerät
 Support 18
 Mobiles Onboarding
 XMS Cloud 51
 Monitoreinrichtung 85
 Montage 23
 Base Unit
 Verfahren 24
 Bereitstellung im Netzwerk
 Anforderungen 29
 Bewährte Situation 28
 Deckenmontage
 Base Unit 26
 Einrichtung mit Netzwerkverbindung 31
 Dediziert 34
 Dual-Netzwerk 32
 Tischgerät
 Base Unit 25
 Wandmontage
 Base Unit 26

P

Passwörter 115
 Peripheriegeräte 86
 Personalisierung
 Hintergrundbild 79
 personalisiert 81
 Personalisiertes Hintergrundbild 81
 Ports 29
 PresentSense 110
 Protokolleinstellungen 135

S

Sicherheit 20
 Empfehlungen 21
 HTTP-Verschlüsselung 116
 Sicherheitsstufe 113
 SNMP 112
 Sprache 77
 Standortname 77
 Statusinformationen 118
 System
 XMS 131

T

Technische Daten 12, 14
 Button 9
 C-10 9
 C-5 9
 Tischgerät
 Base Unit 25

U

Übertragbare Version 83
 Umgebung 20
 Update
 Firmware
 Base Unit 133
 Button 133

V

Verbindung wird hergestellt
 Base Unit
 Display 36
 Ein-/Ausschalten 40
 Ethernet 39
 LAN 39
 Touch-Screen 38
 Vollständige Sicherung 83
 Vorbereiten
 Button 61

W

WebUI-Passwort 115
 Werkseinstellungen 137
 Wi-Fi-Einstellungen 87–88

- Drahtlos-Client 91
 - EAP-TLS 92
 - EAP-TTLS 95
 - PEAP 96
 - WPA-PSK 98
- Willkommenstext 77
- Windows
 - Zertifizierter Treiber 66

X

- XMS Cloud 131
 - Computer-Onboarding 50
 - Mobiles Onboarding 51
- XMS Cloud registrieren 50
- XMS Cloud-Kalender 55
- XMS Cloud-Onboarding 50
- XMS Cloud-Registrierung 50



R5900117DE /04 | 2023-12-11

www.barco.com