Network Deployment Guide

How to deploy ClickShare Conference (CX-), ClickShare Present (C-) and Clickshare Bar (CB) in your network

DATE 24/04/2024

Table of content

About this Network Deployment Whitepaper 4

Disclaimer 4

Limitations 4

General guidelines for the ClickShare Conference, Clickshare Bar and ClickShare Present system installation 5

General guidelines for Wireless Conferencing through the corporate network 7

ClickShare Conference, Clickshare Bar and ClickShare Present: secure and easy enterprise-wide deployment 8

Network deployment topology examples 9

Network connected setup 10

Dual network connected setup 13

Dedicated network setup 15

Standalone setup 17

Network deployment requirements 18

Base Units: first-time setup 18

Base Units: daily use 18

DNS 19

Base Units: auto-update and peripheral firmware update 19

NTP 19

SNMPv3 19

Buttons 20

ClickShare Desktop App 20

AirPlay 21

Google Cast 21

Miracast 21

Wireless Client mode 22

Dual Network Connection 23

Wired network authentication: 802.1X 24

REST API 24

XMS Cloud 24

XMS Edge 24

ClickShare Configurator 25

Overview of the required ports 25

Configuration 27

Wireless Client: configuration 27

Wired network authentication: 802.1X 30

Button network integration 31

Recommendations for Wi-Fi configuration 33

Buttons 33

Wi-Fi spectrum and channels organization 33

ClickShare Wi-Fi channel selection 36

Site survey 36

Generic configuration rules 36

Acronyms 40

About this Network Deployment Whitepaper

This guide helps you to get started with ClickShare Conference, ClickShare Bar and ClickShare Present product ranges and deploy the ClickShare Base Units or Bars within your Enterprise network.

Note: In this document, ClickShare Base Units and Bars will not always be mentioned separately. When referring to Base Units, one can always assume that this applies to Bars as well.

Note: This Network Integration Whitepaper only applies to the ClickShare Conference, ClickShare Bar and ClickShare Present models (C-5, C-10, CX-20, CX-30, CX-50 and CX-50 Gen2 and ClickShare Bar Core and Pro) and corresponding 'Gen 4' or 'Gen 4.1' Buttons. For the CS(E) product range, please refer to the corresponding Network Deployment Whitepaper, which you will find in the support pages of the respective products.

Disclaimer

Not all functionality described in this document may be available at this moment.

Please get in touch with your Barco contact if you have specific questions about availability and timeline.

More details on the unavailable features is given in the topologies section below.

The Network integration feature is provided "AS IS", without any liability or obligation on behalf of Barco. Barco cannot guarantee that the integration mode works in your Enterprise network. The reliability, quality and stability when sharing using the network integration modes depends on your specific network infrastructure.

Deciding on and deploying one or more ClickShare Base Units within the network requires the involvement of your IT department, especially of the persons responsible for the configuration of your network infrastructure and authentication protocols.

Limitations

Note that the **ClickShare Base Unit and ClickShare Button(s) cannot be used** to:

- Access the internet or as an access point to any wired network
- Bridge 2 or more networks into one network
- Provide network access (to guests or any other user) via the Button

Should you have any questions, please have a look at https://www.barco.com/support.

General guidelines for the ClickShare Conference, Clickshare Bar and ClickShare Present system installation

This document describes all details for the network installation of the ClickShare Conference, ClickShare Bar and ClickShare Present devices. This section will give you some recommendations which are true for all deployments and should be considered when choosing which deployment is best for your environment.

- **Keep your units up to date**. Barco provides free updates multiple times a year with security, stability, and functionality updates. For an optimal experience and to assure the security of the overall system, we recommend to always install the latest firmware.
- To ensure the best user experience for users, employees and guests, and administrators, **we strongly recommend connecting the Base Units to the network**, using either the wired ethernet connection or the ability to connect the Base Units to a wireless network. By doing so, both guests and employees can make use of BYOD services (e.g. AirPlay, Google Cast and Miracast) but also the ClickShare Apps without disconnecting from the wireless network or losing their internet connection. For management of the devices, including configuration, monitoring, updating and troubleshooting, networked devices enables the administrator to remotely access the installed base and to use the XMS management platform.
- **For optimal performance, we recommend using a direct connection between the Button and the Base Unit**. Integrating the Buttons into the corporate network may lead to increased latency, jitter and packet loss which in turn will lead to a decreased experience for the users. Take special care of optimizing and dimensioning your network when choosing to integrate the Buttons into your network for conferencing.
- **When integrating Buttons into the corporate network, or when choosing for Wireless Conferencing through the ClickShare Desktop App, please follow the guidelines** in the section below.
- **Place the Base Unit in an open emplacement** and avoid installing in a metallic shell. A metallic shell (or even shelf) could act as a Faraday cage and block the RF signal. When the ClickShare Base Unit is installed, control the signal strength at the potential ClickShare Button location. For correct performance, a signal strength of at least -70dBm is necessary. The most favorable setup is a direct line of sight between Base Unit and Buttons for high quality and low latency wireless conferencing. Any obstruction will cause the signal to follow a longer propagation path, possibly impacting performance.
- In normal operation mode, the IP address and SSID name are not displayed on the wallpaper by default. To access this information, simply connect to the Base Unit with the ClickShare Desktop App or the ClickShare Button and select the "about" menu in the application. This will open a window with all technical information of the Base Unit. More information on this can be found here: [KB11142].
- For optimal security, it is strongly advised to **change the default passwords**.
- For an optimal user experience, both ClickShare and BYOD services such as AirPlay, Google Cast or Miracast, have different implementations for presence and proximity detection. To take full advantage of these mechanisms, we strongly advise to **install the ClickShare Base Unit inside the meeting room, physically close to the display and not in a closed cabinet**. Next to this, we advise **not to turn off the Access Point of the Base Unit**. In case the Access Point of the ClickShare Base Units should not be visible to end-users or should not be accessible, the SSID of the Base Unit can be set to hidden and a custom password can be implemented. In this way, more reliable OTA (over the air) discovery mechanisms can be

used next to the network discovery mechanisms. For easy discovery, connect the Base Units to the same subnet as your mobile devices or provide a connection between the different network segments, as AirPlay, (and in lesser extent: Google Cast and Miracast over Infrastructure), make use of the mDNS protocol for device discovery. Note that for mDNS and SSDP to work on your network, ICMP / multicasting needs to be enabled. In some networks, especially when the network consists out of different VLANs, discovery protocols such as mDNS might not propagate between VLANs. This inconvenience can be addressed by installing mDNS repeaters, often built-in into routers (e.g. Cisco).

If mDNS broadcast is not enabled or possible over different VLANs, following alternatives will be used or can be implemented:

- For AirPlay: next to mDNS, device discovery can also happen via Bluetooth beacons.
- For Miracast over infrastructure: Windows 10 will either use the IP information in the Wi-Fi beacon, or if this is not available, attempt to resolve the Base Unit's hostname via standard DNS. If not resolvable, Windows 10 will fall back to the standard Wi-Fi direct connection if available. Note that in a dual network setup, the IP address of the LAN interface will be advertised, not the IP address of the wireless connection.
- Google Cast mainly depends on SSDP for discovery.
- ClickShare Apps utilize **PresentSense™** technology to find and identify which Base Units are physically nearby. PresentSense™ utilizes different OTA discovery mechanisms such as Wi-Fi beacons and data over sound ("ultrasound") to find Base Units and sort them in order of physical distance to the end user. When the access point is disabled, proximity detection can also happen via ultrasound which is less reliable than the Wi-Fi beacons since the user can manually mute his device's microphone and it does requires a secondary device discovery mechanism such as mDNS or SSDP. If neither Wi-Fi beacons nor ultrasound are available, mDNS or SSDP will be used for device discovery over the network, yet these technologies cannot provide any information on proximity. **For an optimal user experience, we strongly advise to enable the Access Point of the Base Unit, even when the Buttons are connecting to the corporate network**. Disabling the access point will strongly reduce the PresentSense™ capabilities. In case you do not wish for the access points to be visible or accessible, or if you wish to limit interference on the Wireless network, you can choose to hide the SSID of the Base Unit, configure a strong password on the Wi-Fi so that no-one can access and use it, and set up the Base Unit's access point to operate on a 2.4GHz Wi-Fi channel. In this way, the unit will not interfere with your high quality 5GHz channels and by having the discovery mechanism work through Wi-Fi beacons instead of multicasting mDNS and SSDP over the Wi-Fi, your company wireless network is offloaded as much as possible.

- When connecting the **CX-50/CX-50 Gen2** onto the corporate network to enable BYOD protocols and the ClickShare Apps to share, we strongly advise to **change the standby mode to "eco standby"**. If not, BYOD protocols, the ClickShare apps and possibly the ClickShare Button will not be able to wake the CX-50/CX-50 Gen2 from standby.

General guidelines for Wireless Conferencing through the corporate network

As of the 2.8 firmware version, it is possible to integrate the ClickShare Buttons into the corporate network and to use corporate access points instead of the built-in access points of the ClickShare Base Units. Next to this, the 2.8 firmware version also introduces support for Wireless Conferencing through the ClickShare Desktop Apps.

For a good conferencing experience for your users and to minimize the impact of the additional network load on your network, please consider following guidelines:

- **For optimal performance, we recommend using a direct connection between the Conferencing Button and the Base Unit**. Integrating the Buttons into the corporate network may lead to increased latency, jitter and packet loss which in turn will lead to a decreased experience for the users. Take special care of optimizing and dimensioning your network when choosing to integrate the CX Buttons into your network.
- **Make sure the wireless conferencing streams flow through the wired LAN connection of the Base Unit.** We do not recommend routing the streams through a Base Unit's wireless client connection.
- When routing the ClickShare streams over the corporate network, take special care to **dimension your network** and provide enough bandwidth to the ClickShare application. Next to this, we advise to **ensure the shortest route through the network is used** by the ClickShare application to reduce latency to a minimum. Bandwidth requirements, network requirements and other details can be found here for Buttons and ClickShare Desktop app. **In general, we advise to ensure your network has a bandwidth of up to 30Mbit/s per host connection and has an end-to-end latency below 50ms.**

ClickShare Conference, Clickshare Bar and ClickShare Present: secure and easy enterprise-wide deployment

ClickShare Conference brings **wireless conferencing**, a revolutionary workplace experience. It combines powerful remote communication with easy-to-use wireless collaboration, in any meeting space.
Start a meeting from your device, **use your preferred conferencing platform**. Automatically you connect wirelessly to room cameras, speakerphones, sound bars for a more immersive meeting. In less than 7 seconds you **conference**, **collaborate** and **click** with our **secure**, **connected** and **cloud managed** solution. The ClickShare Conference range has a specific set of features to facilitate an enterprise-wide deployment, including full support for 'bring your own device' (BYOD)-users via the **ClickShare App**, **AirPlay**, **Miracast** and **Google Cast**, and **touch back** support for interactivity.

ClickShare Present brings **simple, easy wireless presentation** to any meeting room. It makes hybrid collaboration flow by sharing content from any device on the central room display in one click. It completes and empowers the existing set-up of Microsoft Teams, Zoom or Webex conference rooms. **Start a meeting within seconds**. Plug & Play with the ClickShare Button (Pc or Mac), go for **workflow integration with the ClickShare App** (laptop, mobile or tablet) or enable full BYOD (Airplay, Google Cast and Miracast). With one simple click you get content on screen. No cables, no software to download, no training needed. You and your guests present, meet, collaborate with our one-click meeting experience. Access interactivity features like annotation, blackboarding and touch back support to **make your meetings richer and more dynamic**.

ClickShare Bars are a premium, carbon-neutral, **all-in-one video bar** that enables engaging, effortless wireless conferencing in medium-sized meeting rooms with any videoconferencing platform. Thanks to its advanced AV capabilities (dual screen, 4K content sharing) and interactive features (touchback, annotation, blackboarding), it enables **crystal-clear audio, sharp views and enhanced interactivity** for meetings where all participants feel heard and seen. This solution offers unparalleled flexibility, allowing IT Managers to easily equip their meeting rooms. Paired with a 5-year warranty, **the bar overall reduces the Total Cost of Ownership** by consolidating all collaboration, audio and video functionalities into one powerful device.

The ClickShare devices come with **enhanced enterprise-strength security** that is configurable up to three levels. It can be controlled via the on-premise web configurator or via a **local or cloud-based central asset management system** eXperience Management Suite (XMS) and be fully integrated into your corporate network. The Base Units also offer a comprehensive API for integration with other applications as well as SNMP support for easy management with your preferred software package. When deploying the ClickShare Base Units, one can authenticate the devices using 802.1X wired network authentication. All ClickShare Base Units and Buttons can be identified with following MAC addresses:

The Base Units have MAC addresses starting with 00:04:A5 on the ethernet interface.

The ClickShare Conference Security whitepaper and more ClickShare support documentation can be found at https://www.barco.com/en/support

Network deployment topology examples

A ClickShare system has the flexibility to be integrated in a corporate network in different ways. Although ClickShare can be setup in a fully stand-alone, offline way, this is not recommended for both usability, security and ease of management reasons. The simplest setup, where the unit is connected to the enterprise network via a wired or wireless interface is described in the network connected setup. For meeting rooms which are frequently used by guests or for companies where the wireless and wired network are completely separated, we recommend the use of the CX-50 or CX-50Gen2, deployed as described in the dual network connected setup. Alternatively, the deployment of the ClickShare Base Units in a separated ClickShare (or AV) VLAN is described in the dedicated network setup. The fully non-connected example is described in the standalone section.

Above examples maintain a direct connection between the Buttons and the Base Unit where possible. ClickShare also provides the possibility to use the corporate wireless access points and enterprise network to provide connectivity between Button and Base Units. This can be useful when you want to limit the amount of access points in your environment or place the Base Unit in a confined space, in or outside the meeting room (not recommended), but introduces an unknown and hard to control variability in terms of latency and quality.

Note that in the different examples, you can limit the amount of visible access points in your environment by configuring the network access points to be hidden. If the access point is not hidden, we recommend using the same name for the SSID as used for the meeting room name.

Network connected setup

This is the simplest installation which offers a seamless experience for employees and is the recommended setup for internal meeting rooms, for companies with a flat network topology or when the ClickShare Button will be the main way for people to use the system.

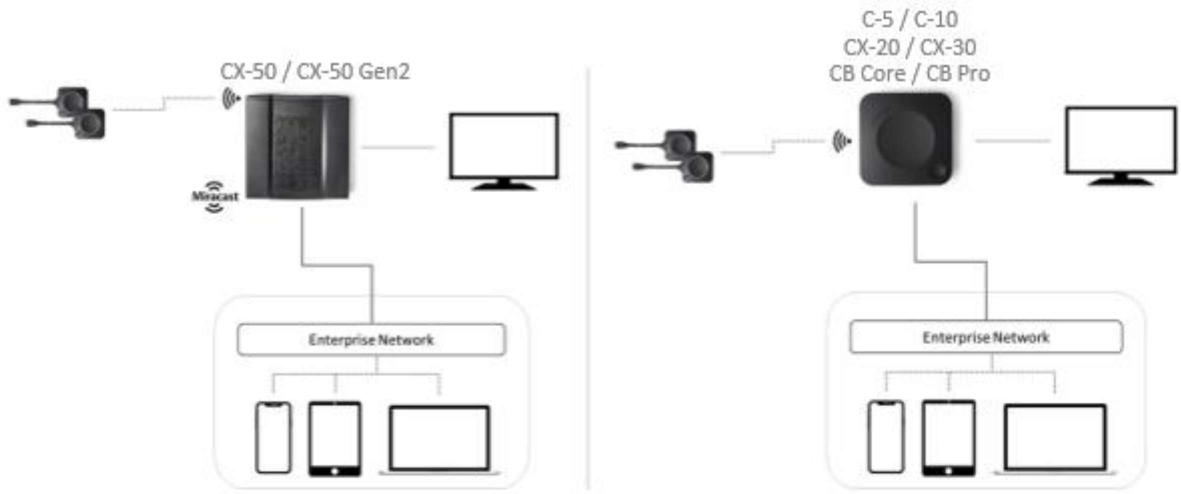


Figure: 'network connected' network topology diagram – wired connection

In this default mode, ClickShare Buttons and Base Units operate directly out of the box and users can share to the Base Unit with the ClickShare Desktop App, the ClickShare Mobile App, AirPlay, Google Cast via the network to which the Base Unit is connected without losing the internet connectivity. Sharing via Miracast depends on the model and the configuration of the device as is shown in the table below.

When the **employee Wi-Fi network is separated from the Corporate network**, dedicated firewall rules will need to be configured to allow sharing from employee mobile devices to the Base Units (an overview is given in the overview of the required ports). If **the Guest Wi-Fi network is on a different VLAN or network**, similar configuration will be required for them to share over the network. Note that some network discovery protocols such as mDNS might not propagate between VLANs. This inconvenience can be addressed by installing mDNS repeaters, often built-in into routers (e.g. Cisco) or by following the recommendations for presence detection described in the general guidelines or in the network deployment requirements.

If the above configurations are not possible or desired, we recommend to either isolate the Base Units in a dedicated network, as described in the dedicated network section, or to setup your Base Unit in a dual network configuration, as described in the dual network connected setup.

In case the above network configuration cannot be set up to enable access from the guest or BYOD Wi-Fi network, guests and mobile users can still connect to the wireless access point of the Base Unit to share with the ClickShare Desktop App, ClickShare Mobile Apps, AirPlay or Chromecast and will only be able to access the internet if the device supports to use data (3G/4G/5G) at the same time. Note that this requires the Base Unit's access point is not turned off, is visible and can be connected to by anyone. For Miracast, the Base Unit will have to be configured for Miracast to offer a Peer-to-Peer, Wi-Fi direct connection as Miracast Over Infrastructure will not be available in this case.

Connecting the Base Unit to the Enterprise network opens the possibility for using the **eXperience Management Suite (XMS)** for central management and/or using the auto-update functionality to keep your installed base up to date. Connecting to XMS Cloud can be done directly or via XMS Edge. One can also use an offline XMS Edge to configure the Base Units in case a cloud connection is not allowed. Last, a ClickShare Conference Base Unit which is connected to the network, can be monitored through **SNMP**, can be controlled and monitored by **other 3rd party systems** such as QSC or Crestron or can be interfaced through the **ClickShare REST API.**

Note that the connection to the network can be done with a wired connection (as is shown in "Figure: 'network connected' network topology diagram – wired connection") or with a wireless connection. This is shown in the figure below:

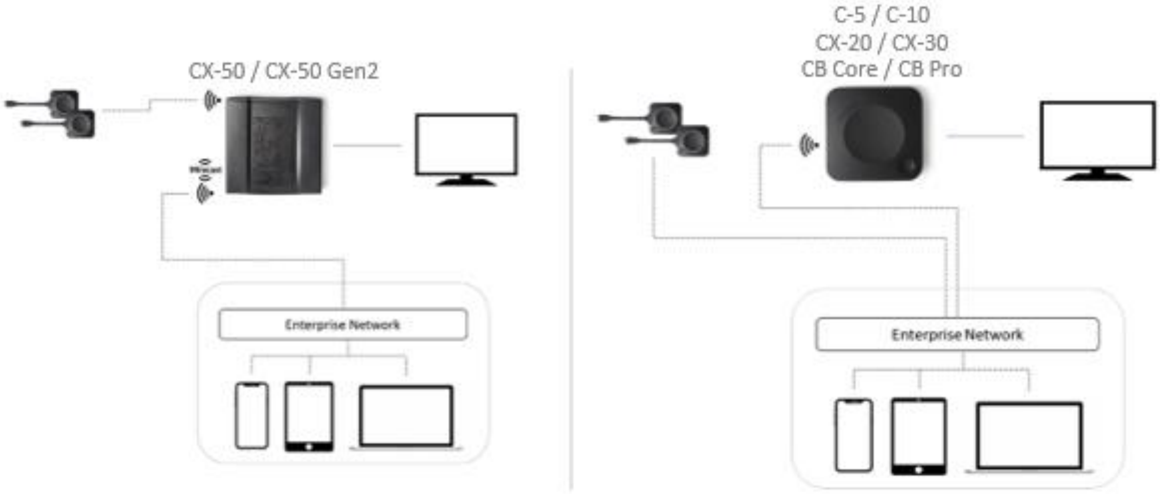


Figure: 'network connected' network topology diagram – wireless connection

For the C-5, C-10, CX-20 and CX-30 as well as the ClickShare Bar Core and Pro, this configuration has several disadvantages as the access point of the Base Unit is disabled and Buttons must connect to the Base Unit via corporate access points.

Note that Wireless Conferencing capabilities of the ClickShare Button might be limited when the Button is integrated into the corporate network, and its performance will depend on the internal network. More details on setting up a high performing Wireless Conferencing setup when integrating the Buttons into the corporate network can be found in the guidelines section. Next to this, PresentSense™ for the ClickShare Apps will be limited to network discovery protocols and ultrasound as is described in the PresentSense™ section. The CX-50/CX-50 Gen2 will remain fully functional in this mode of operation and is the recommended device for this type of setups.

Sharing with Miracast depends on ClickShare model and installation mode:

	Base Unit is connected to the network via the LAN cable	**Base Unit is connected to a wireless network via client mode**
C-5, C-10, CX-20 and CX-30, CB Core and Pro	Miracast via Wi-Fi Direct and Over Infrastructure (MS-MICE), but only available when the Base Unit's access point is turned OFF (*,**)	Over Infrastructure (MS-MICE) (***)
CX-50 and CX-50 Gen2	Via Wi-Fi Direct and Over Infrastructure (MS-MICE)	Over Infrastructure (MS-MICE) (***)

Table: Miracast operation for different models and installation modes

* Concurrent connectivity is only supported on the CX-50/CX-50 Gen2.

** In this configuration, the access point of the Base Unit is disabled and Buttons must connect to the Base Unit via corporate access points. Note that Wireless Conferencing capabilities of the ClickShare Button might be limited when the Button is integrated into the corporate network, and its performance will depend on the internal network. More details on setting up a high performing Wireless Conferencing setup when integrating the Buttons into the corporate network can be found in the guidelines section. Next to this, PresentSense™ for the ClickShare Apps will be limited to network discovery protocols and ultrasound as is described in the PresentSense™ section. The CX-50 will remain fully functional in this mode of operation and is the recommended device for this type of setups.

*** If the Base Unit is set up in a dual network configuration, MS-MICE will only be available on the LAN connection. When not connected to that network, the user's device will connect to the Base Unit through Wi-Fi direct.

Dual network connected setup

This installation offers a seamless experience for employees and guests and is the recommended setup for any organization with an advanced network configuration, for meeting rooms which will be frequently used by guests, visitors and externals or when the ClickShare Apps and native BYOD protocols, such as AirPlay, Google Cast and Miracast, will be frequently used in the organization.

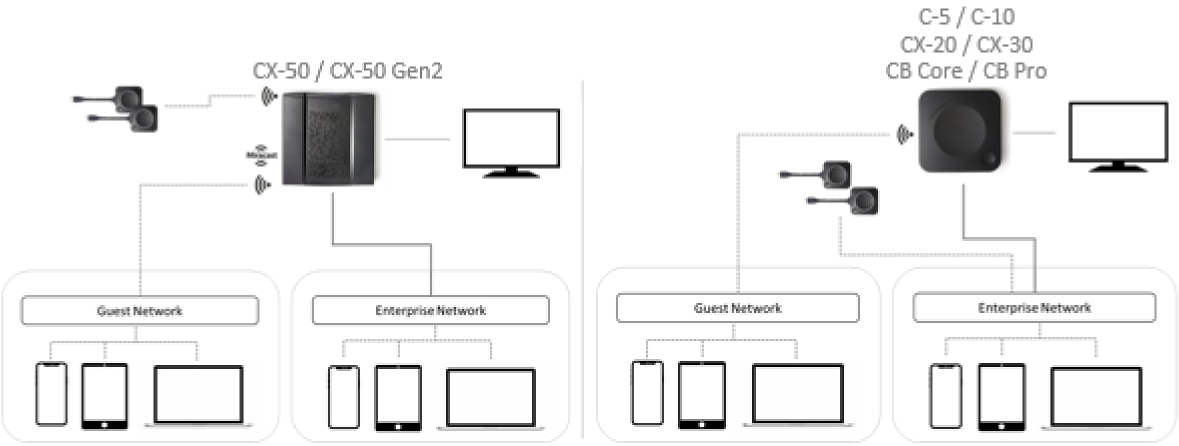


Figure: 'dual network setup' network topology diagram

In this setup, ClickShare Buttons connect directly to the Base Units access point with the CX-50/CX-50 Gen2. For the C-5, C-10, CX-20 and CX-30, as well as the ClickShare Bar Core and Pro, the dual network connection topology will disable the access point of the Base Unit and Buttons must connect to the Base Unit via Corporate access points. Note that Wireless Conferencing capabilities of the ClickShare Button might be limited when the Button is integrated into the corporate network, and its performance will depend on the internal network. More details on setting up a high performing Wireless Conferencing setup when integrating the Buttons into the corporate network can be found in the guidelines section. Next to this, PresentSense™ for the ClickShare Apps will be limited to network discovery protocols and ultrasound as is described in the PresentSense™ section. The CX-50/CX-50 Gen2 will remain fully functional in this mode of operation and is the recommended device for this type of setups.

Users can share to the Base Unit with the ClickShare Desktop App, the ClickShare Mobile App, AirPlay, Miracast and Google Cast via either network to which the Base Unit is connected. Miracast MS-MICE will only be available through the LAN connection, all other devices will connect to the Base Unit directly over Wi-Fi direct.

The ClickShare Base Units can still be integrated in a dedicated network or VLAN, as described in the dedicated network section. If this is the case, dedicated firewall rules will be required to allow the streams to go through the different network sections. Note that some network discovery protocols such as mDNS might not propagate between VLANs. This inconvenience can be addressed by installing mDNS repeaters, often built-in into routers (e.g. Cisco) or by following the recommendations for presence detection described in the general guidelines or in the network deployment requirements.

Connecting the Base Unit to the Enterprise network opens the possibility for using the **eXperience Management Suite (XMS)** for central management and/or using the auto-update functionality to keep your installed base up to date. Connecting to XMS Cloud can be done directly or via XMS Edge or one can use an offline XMS Edge to configure the Base Units. Last, a ClickShare Conference Base Unit which is connected to the network, can be monitored through **SNMP**, can be controlled and monitored by **other 3rd party systems** such as QSC or Crestron or can be interfaced through the **ClickShare REST API.**

Dedicated network setup

This installation offers an isolated network setup where all connections from and to the Base Units can be controlled. This dedicated AV (or ClickShare) network or VLAN can be used for more fine-grained access control, to ensure no connection can happen between any of the connected physical or virtual LANs or to separate all ClickShare traffic from all other IP traffic to ensure business requirements in terms of bandwidth, security and latency.

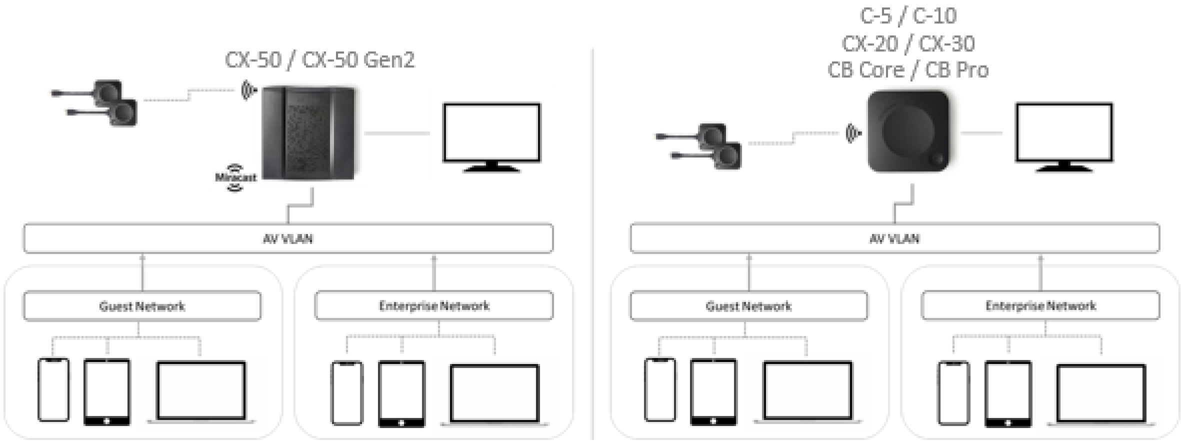


Figure: Network integration in dedicated network with routed Enterprise network topology diagram

In this setup, the configurations can widely differ depending on network topology and security requirements in the organization. Here, we will describe a simple setup where the Base Units is placed in a dedicated AV VLAN, a commonly used practice within organizations. Variations where the VLAN has its own access points for the Buttons to connect to or where Base Units run in a dual network configuration to separate Guest Wi-Fi and the corporate network even further are for the readers' own exploration.

In this setup, ClickShare Buttons and Base Units operate directly out of the box. Since the Base Units have been installed in a dedicated network, firewall configuration will be required to enable the use of the ClickShare Desktop App, the ClickShare Mobile App, AirPlay and Google Cast over the network (an overview is given in the overview of the required ports). Note that some network discovery protocols such as mDNS might not propagate between VLANs. This inconvenience can be addressed by installing mDNS repeaters, often built-in into routers (e.g. Cisco) or by following the recommendations for presence detection described in the general guidelines or in the network deployment requirements. Sharing via Miracast depends on the model and the configuration of the device, as is shown in the table in the network connected section, as well as the firewall configuration in case Miracast Over Infrastructure is used.

If the firewall is not configured to allow connections from either the guest Wi-Fi or the employee Wi-Fi, users can connect to the wireless access point of the Base Unit to share with the ClickShare Desktop App, ClickShare Mobile App, AirPlay and Chromecast and will only be able to access the internet if the device supports to use data (3G/4G/5G) at the same time. Note that this requires that the Base Unit's access point is not turned off, is visible and can be connected to by anyone. Mobile users are limited to the experience described in the standalone setup. For Miracast, the Base Unit will have to be configured for Miracast to offer a Wi-Fi direct connection.

Connecting the Base Unit to the Enterprise network opens the possibility for using the **eXperience Management Suite (XMS)** for central management and/or using the auto-update functionality to keep your installed base up to date. Connecting to XMS Cloud can be done directly or via XMS Edge or one can use an offline XMS Edge to configure the Base Units. Last, a ClickShare Conference Base Unit which is connected to the network, can be monitored through **SNMP**, can be controlled and monitored by **other 3rd party systems** such as QSC or Crestron or can be interfaced through the **ClickShare REST API.**

Standalone setup

This setup is the simplest in terms of installation and can be used for temporary setups and in organizations where central management and 3rd party integration are not required and where the system will be used exclusively with the ClickShare Button. Note that this setup requires manual interaction with each of the Base Units for updating and configuration, that all functionalities offered in XMS Cloud are not accessible to the customer and not all functionalities of the device can be used in a user-friendly way or at all.

Users who wish to share with the ClickShare Desktop App, ClickShare Mobile App, AirPlay and Chromecast will have to connect to the Base Unit's access point and will only be able to access the internet if the device supports to use data (3G/4G) at the same time. Note that this requires the Base Unit's access point is not turned off, is visible and can be connected to by anyone. Sharing via Miracast will only be possible via Wi-Fi direct when using the CX-50 or CX-50Gen2.

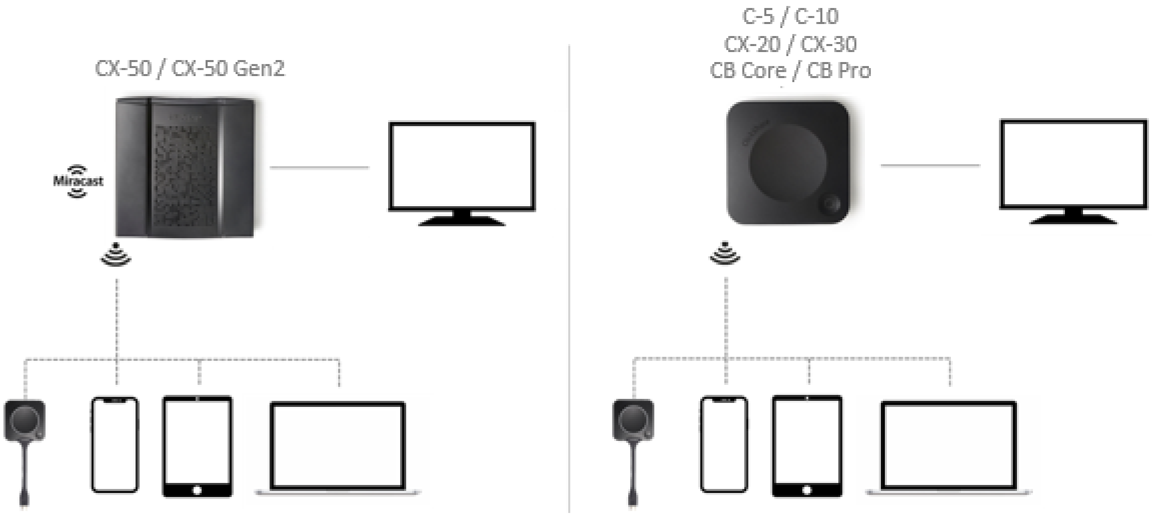


Figure: Standalone topology diagram

Network deployment requirements

This chapter contains all recommendations for integrating ClickShare into your enterprise network. For each function, a detailed overview is given in terms of minimal requirements and required ports and firewall rules needed to be configured to make the specific function work. An overview is given in the overview of the required ports

Base Units: first-time setup

- Activation and update: for this action, similar to the auto-update functionality described below, an outbound TCP connection on port 443 is required towards update.cmp.barco.com and assets.cloud.barco.com[1] and port 80 is required towards www.barco.com (location of the JSON file containing the firmware file list)
- Connection to XMS Cloud for activating SmartCare and XMS Cloud functionality: TCP Port 443 outbound to *.azure-devices.net and global.azure-devices-provisioning.net
- XMS Edge is currently not supported for the first-time setup of the ClickShare Conference devices.

Note that the first-time setup requires a laptop with access to:

- XMS Cloud: outbound TCP Port 443 to xms.cloud.barco.com
- MyBarco portal: outbound TCP Port 443 to *.barco.com (login/xms.cloud.barco.com).
- (Optional) Web Configurator of the device: TCP ports 80 and 443 to the Base Unit or ability to connect directly to the Base Unit's Wi-Fi.

Details on how to configure network settings during first-time setup can be found in the Configuration section.

Base Units: daily use

- By preference, connect the Base Unit to the network via the ethernet cable. In a dual network setup, it is advised to use the wired connection to connect to the network that will be most used or requires the highest quality.
- In case the Base Units require wired network authentication: 802.1X is available as of the 02.05 firmware release. The MAC addresses of the Base Units start with 00:04:A5
- The assigned IP-address of the Base Unit is not shown on the wallpaper by default. Use the ClickShare Desktop App or the application on the ClickShare Button to find out the IP address of the Base Unit by clicking the "about" menu in the application. To display the IP addresses and the SSID of the Base Unit on the wallpaper, check the "Show network info" checkbox in the Configuration page, under "Personalization > On-screen ID". More information can be found here: [KB11142].
- The internal Wi-Fi access points on the ClickShare Base Units can be disabled once Buttons are integrated into the corporate network to reduce wireless clutter. Note that this disables direct connections to the Base Units, as well as presence detection in the ClickShare Desktop App. For an optimal user experience, we advise following the recommendations for presence detection described in the in the general guidelines or in the specific sections below.
- Provide enough bandwidth to prevent bottlenecks in your network, which could potentially degrade the ClickShare experience.

[1] These are redirects generated by Amazon Web Services that can change and are managed by Amazon.

- Check whether the corporate wireless access points support the IEEE 802.11d standard.

DNS

For the Buttons to be able to share their content with the Base Unit, they must be able to resolve the Base Unit's hostname within the network or link to a fixed IP.

It is strongly recommended to **reserve IP addresses in your DHCP server for each Base Unit**. This will prevent issues when the hostname is not resolvable. The DHCP entry binds the IP address to the MAC address. Another option is to set a fixed IP address within the ClickShare Configurator.

If no DNS is available, the Buttons will fall back to the IP address of the Base Unit at the moment of USB pairing. The Buttons need to be assigned an IP address on the network to which they are connected via a DHCP server.

Base Units: auto-update and peripheral firmware update

To use the auto-update function for ClickShare or to be able to update your peripherals through the ClickShare Base Units, ensure that an outbound connection over TCP port 443 can be set up towards update.cmp.barco.com, assets.cloud.barco.com[1], globa.azure-devices-provisioning.net, eeprom.cmp.barco.com and port 80 towards www.barco.com (location of the JSON file containing the firmware file list)

NTP

When using the EAP-TLS protocol, it is recommended to also **configure NTP on the Base Unit** via the ClickShare Configurator. The Base Unit must have the correct time to handle the certificates required for EAP-TLS. It is recommended to use **an NTP server with high availability on the local corporate network**.

When using an NTP server on the internet, the Base Unit cannot connect through a proxy server.

SNMPv3

ClickShare Conference has built-in support for the **Simple Network Management Protocol (SNMP)** on the Base Unit. SNMP is an internet standard protocol for collecting and organizing information about managed devices on IP networks. In general, an SNMP management suite (running on a server) communicates with an SNMP agent (running on the device). The SNMP agent (the ClickShare Base Unit) collects and exposes device information, the SNMP management suites will be able to approach the ClickShare devices via the SNMP protocol. Writing via SNMP in order to configure the ClickShare device is not supported by ClickShare. More information can be found here: [KB8471]. Note that we only work with TRAPS.

SNMPv3 is supported on the entire ClickShare Conference and ClickShare Present product ranges and can be configured via the ClickShare Configurator. The functionality is enabled in all security levels. Make sure to open UDP ports 161 and 162 on the firewalls for proper functioning.

[1] These are redirects generated by Amazon Web Services that can change and are managed by Amazon.

Buttons

For an **optimal user experience** and to stream the captured content smoothly to the Base Unit, each Button needs at least:

- 2 Mbps bandwidth to present static content
- between 5 and 15 Mbps for optimal video performance
- between 10 and 15 Mbps upstream (from Button to Base Unit) and between 15 and 30 Mbps downstream (from Base Unit to Button) for optimal Wireless Conferencing performance

For more details on optimizing your Wi-Fi environment and Wi-Fi settings on your ClickShare deployment, please refer to section Buttons.

When integrating the Buttons into the corporate network, the ClickShare Button will require following ports to be opened:

- For screen sharing: TCP port 2345, 6544
- For wireless conferencing (CX Base Units only): UDP port 1234 and TCP ports 1235, 9999

To ensure a good Wireless Conferencing experience, the end-to-end latency of the network should be below 50ms.

Details on how to configure the Button network integration can be found in the Configuration section.

ClickShare Desktop App

- The ClickShare Desktop App uses SSDP and mDNS for advertisement and discovery within the network, requiring opening UDP port 1900 (SSDP) and UDP port 5353 (mDNS) in the network. Only one of both is needed for successful discovery and we mainly advise the use of SSDP for network discovery as this protocol is easier to route in complex network setups.
- For presence detection, which will sort the Base Units according to the measured signal strength, we strongly advise to leave the Base Unit Wi-Fi access point enabled. To be used for presence detection, it is not required for the SSID to be visible or for the end-user to know the Wi-Fi password. When disabled, presence detection can also happen via 'data over sound' which is less reliable than the Wi-Fi beacons since the user can manually mute his device's microphone and still requires a secondary presence detection mechanism such as mDNS or SSDP. In case you do not wish for the access points to be visible or accessible, or if you wish to limit interference on the Wireless network, you can choose to hide the SSID of the Base Unit, configure a strong password on the Wi-Fi so that no-one can access and use it, and set up the Base Unit's access point to operate on a 2.4GHz Wi-Fi channel. In this way, the unit will not interfere with your high quality 5GHz channels and by having the discovery mechanism work through Wi-Fi beacons instead of multicasting mDNS and SSDP over the Wi-Fi, your company wireless network is offloaded as much as possible.
- The required bandwidth for sharing via the ClickShare Desktop App is estimated around 2Mbps for static content and between 5 Mbps and 15 Mbps for video content per ClickShare App connection. When the local view of the meeting room is used, an additional estimated downstream bandwidth between 5 Mbps and 7 Mbps per ClickShare App is required. The

ClickShare Desktop App will connect to the Base Unit via TCP and will use a port in the range of 6541-6545.

- The ClickShare Desktop App for MacOS and Windows will check for updates and download the latest version from "assets.cloud.barco.com[1]" on Port 443. When this domain is blocked in the firewall of the employee's computer, both the request to install the App when launching the executable from the Button and the request to update to the latest version in the installed App will not show.
- To optimize the user experience, ClickShare will collect usage data in compliance with GDPR and privacy requirements. [ClickShare Security Whitepaper] For this it will open a connection on Port 443 toward api.amplitude.com.
- For a good user experience when using the Wireless Conferencing capabilities of the ClickShare Desktop App, the App require up to 30Mbit/s per host connection and requires the network to have an end-to-end latency below 50ms. Next to this, UDP port 1234 and TCP port 9999 are used for audio and video transfer. More details on setting up a high performing setup when integrating the Buttons into the corporate network can be found in the guidelines section.

AirPlay

- AirPlay requires the use of the Bonjour® protocol for network discovery. This protocol is based on multicast DNS to make the ClickShare Base Unit discoverable within your network and requires opening UDP port 5353.
- AirPlay can also use presence detection based on Bluetooth. When Base Units are discovered through Bluetooth, the AirPlay enabled device will check if it can connect to the Base Unit. If Bluetooth is not used, there will be no way to filter or sort of the Base Units list. For more than 10 Base Units in your Enterprise network, it is recommend using a structured meeting room name, e.g. "Building A – Floor 2 – Meeting Room Rome". This will allow users to quickly find the correct meeting room in a long list. Not that the Bluetooth beacon will only contain the wired IP, if connected.
- Connection to the Base Unit will happen through TCP ports 4100-4200; 7000; 7100; 47000 and UDP ports 4100-4200.

Google Cast

- Google Cast requires multicast to make the ClickShare Base Unit discoverable within your network, this requires UDP port 1900 (SSDP) and UDP port 5353 (mDNS) to be opened
- Google Cast is a proprietary protocol, which does not allow filtering or sorting of the Base Units list. For more than 10 Base Units in your Enterprise network, it is recommend using a structured meeting room name, e.g. "Building A – Floor 2 – Meeting Room Rome". This will allow users to quickly find the correct meeting room in a long list.
- For streaming, Google Cast requires TCP ports 808;809;9080 to be opened and UDP ports 32768-61000 for optimal streaming quality.

Miracast

Miracast P2P (Wi-Fi direct) and Miracast MS-MICE (Over Infrastructure) are available on all ClickShare models, but availability of the feature depends on the configuration of the device. The

[1] These are redirects generated by Amazon Web Services that can change and are managed by Amazon.

main target for Miracast on ClickShare Conference is Windows 10 laptops.

A dedicated Wi-Fi chip in the Base Unit allows direct discovery & connection by Miracast compatible devices (typically Windows 10 computers & certain Android smartphones). This dedicated chip allows for every type of user (employee or guest) to easily detect & connect to the ClickShare Base Unit to start sharing using Miracast.

- Miracast P2P is compatible with all four different network deployment options.
- Miracast P2P discovery happens over the air (ota), using Wi-Fi beaconing.
- Miracast P2P requires the Base Unit SSID not to be set to hidden on the C-5, C-10, CX-20 and CX-30, as well as the ClickShare Bar Core and Pro

Note that the availability of Miracast P2P (Wi-Fi direct) and Miracast Over Infrastructure (MS-MICE) depends on both model and configuration, as can be seen in the overview table in the network connected deployment section

Wireless Client mode

Wireless Client mode allows to connect the Base Unit to a network over Wi-Fi instead of via the Ethernet interface. It brings identical functionality as a wired network connection; complete network integration, auto-update functionality and central management in XMS. It offers increased flexibility in the placement of the ClickShare Base Unit as a network cable drop is no longer required on the installation location.

Wireless Client mode can be configured in the ClickShare Configurator; navigate to the **Wi-Fi Settings** tab in the **Wi-Fi & Settings** menu. On the C-5, C-10, CX-20 and CX-30, as well as the ClickShare Bar Core and Pro, click **Edit settings** and select 'Client mode' in the drop-down menu. Choose the authentication method, fill in the details and click 'Save changes'. On the CX-50/CX-50 Gen2, enable the wireless client mode, fill in the details and click 'Save changes'

For wireless client mode the supported authentication methods are:

- WPA2-Personal
- WPA2-Enterprise (802.1x EAP)
    - PEAP
    - EAP-TTLS
    - EAP-TLS*

(*) Certificates for EAP-TLS can be provided via the web or rest interface. Alternatively, the baseunit can be instructed to query an NDES or SCEP server and enroll to acquire a certificate.

Note that although all units support client mode, this will introduce some limitations on the CX-20 and CX-30, as well as the ClickShare Bar Core and Pro, as is noted in the table on Miracast in the network connected deployment section

As is shown in the table, when Wireless Client mode is enabled on the C-5, C-10, CX-20 or CX-30, as well as the ClickShare Bar Core and Pro, the functionality will be limited in the sense that the Base Unit Wi-Fi is occupied and can no longer be used for direct connections, either from the ClickShare Button, the ClickShare Apps or from AirPlay or Google Cast. For the CX-20 and the CX-30, as well as the ClickShare Bar Core and Pro, this means that these connections need to happen over the corporate network, which will limit the Wireless Conferencing capabilities of the ClickShare Conference Button and its performance will depend on the company network. More details on setting up a high performing Wireless Conferencing setup when integrating the Buttons into the corporate network can be found in the guidelines section. Next to this, presence detection based on Wi-Fi beacons will not be available for the ClickShare Apps, reducing the PresentSense™ capabilities as is described in the PresentSense™ section. The CX-50/CX-50 Gen2 will remain fully functional in this mode of operation and is the recommended device for this type of setups. Integrating Buttons into the corporate network can be configured in the **Buttons** tab in the **System** menu in the Configurator or in XMS.

For the CX-50/CX-50 Gen2, configuring the unit to connect to a Wireless network will not disable the access point of the Base Unit, which means the Buttons can still connect directly to the Base Unit and presence detection based on Wi-Fi beacons remains available.

Details on how to set up the Wireless Client mode can be found in the Configuration section.

Dual Network Connection

When combining the Wireless Client with the wired ethernet connection on the Base Unit, the Base Unit can be connected to two different (virtual or physical) networks at the same time.

Dual network functionality allows for instance to connect simultaneously to the corporate and guest LAN, allowing both employees and guests to share content via the ClickShare Apps, AirPlay or Google Cast to the ClickShare Base Unit without the need to change their network connection and lose their internet connection. This also eliminates the need for the IT administrator to route traffic between the two networks. The built-in firewall in the Base Unit prevents any traffic bridging between the two connected networks.

Remark that the dual network capability cannot be used for failover / load balancing purposes on one network. Neither can it be used for link bundling for increased capacity. Both interfaces need to be connected to different subnets.

Limitations do apply on the C-5, C-10, CX-20 and CX-30, as well as the ClickShare Bar Core and Pro when set up in a dual network mode as the access point will no longer be available for these devices. This is described in the Wireless Client Mode section.

When in a dual network setup, Mircast connections will only go over the Infrastructure (using MS-MICE) when the user's device can connect to the wired interface (LAN) of the Base Unit. In all other cases, the user's device will connect to the Base Unit directly, using Wi-Fi direct.

Important: when the Buttons are configured to connect to the Base Unit over corporate access points, it is important to know that the Button will attempt to reach the Base Unit via the primary interface, which is the Wired connection. If the desired connection path is through the wireless interface of the Base Unit, pair the Button with the Base Unit with no network cable connected to the Base Unit and connect the Base Unit to the wired network after that, otherwise the Button will be configured to connect to the primary interface, being the LAN.

Wired network authentication: 802.1X

IEEE 802.1x, an IEEE Standard for Port-Based Network Access Control (PNAC), provides protected authentication for secure network access on the wired interface. ClickShare allows to configure the network authentication details through the web configurator once the Base Unit is set up for the first time. Log into the web configurator and navigate to 'Wi-Fi & Network', "LAN Settings" and click the 'Setup wired authentication' button in the 'Primary Interface' section, which will guide you through the wizard to setup the authentication. In terms of authentication protocols, ClickShare Base Units support PEAP, EAP-TLS and EAP-TTLS.

Details on how to set up the wired network authentication can be found in the Configuration section.

REST API

ClickShare Base Units can be integrated in 3rd party systems through a RESTful API. For the C and CX range of Base Units, the ClickShare API has been redesigned to meet modern interface standards and the API defined for the CS(E) products cannot be used to interface with a C, CB or CX device. The REST API is on by default and uses the same credentials as the web Configurator (default: admin/admin, although we strongly recommend to change this password on your devices). The REST API can be disabled via the web Configurator of the ClickShare device under 'Wi-Fi & Network' > 'Services' in the 'ClickShare API' section. In this section you will also find the API reference when selecting 'View API documentation'. To access the swagger interface, you will be prompted to enter the credentials of the REST API.

To enable the use of the REST API, TCP Port 4003 (HTTPS) needs to be opened.

When setting the firmware file source URL, depending if HTTP(S) or FTP is used, the appropriate ports will need to be open for the firmware download to be successful.

XMS Cloud

ClickShare Base Units will connect to XMS Cloud through following outbound ports:

- Port 443 TCP to following domains
  - sil-xms-prd01-iothub.azure-devices.net [1]
  - *.cloudapp.azure.com [1]
  - silxmsprd01sa.blob.core.windows.net
  - *.azure-devices.net – IOT XMS for device control
  - barcoprdwebsitefs.azureedge.net
  - xms.cloud.barco.com
  - *.core.windows.net – for device logs
  - Azure.microsoft.com – for connection test
- Port 80 TCP to *barco.com for firmware download

XMS Edge

XMS Edge (XMS-110 and XMS virtual Edge) uses the following outbound ports for communication to XMS Cloud:

- Port 53 TCP/UDP to access DNS server
- Port 123 TCP/UDP to access NTP server for time synchronization (if set)
- Port 443 (HTTPS) to following domains
  - *.azure-devices.net – for device control
  - *.core.windows.net – for device logs
  - azure.microsoft.com – for connection test
  - barcoprdwebsitefs.azureedge.net – for firmware download
  - sil-xms-prd01-iothub.azure-devices.net – for firmware download
  - update-xms.cloud.barco.com – for XMS Edge devices its own firmware
  - *.cloudfront.net - for XMS Edge devices its own firmware [1]
- Port 80 to update.barco.com to download the firmware package [2]

For setup and communication on the local network

- Port 4001 (HTTPS) and port 4000 (HTTP) to accomplish device management for CS and CSE Base Unit, XMS edge communicates with the Base Units over the REST API within the local network.
- Port 4003 (HTTPS) to accomplish device management for C and CX Base Unit, XMS edge communicates with the Base Units over the REST API within the local network.
- Port 25/465/587 TCP for setting SMTP server for sending e-mails/alerts. The ports can be changed inside XMS.

ClickShare Configurator

Inbound TCP connection to port 443 to the IP of the Base Unit. The ClickShare Configurator can also be accessed by connecting directly to the Base Unit's Wi-Fi as is described in KB11142. Note that the access to the configurator through the access point of the Base Unit can be disabled in the settings of the Configurator.

Overview of the required ports

Open the following ports on your network to ensure that you can share content via ClickShare:

[1] These are redirects generated by Amazon Web Services that can change and are managed by Amazon.

[2] These are redirects generated by Azure Cloud Services that can change in the future and are managed by Azure.

Sender/Receiver		**CX range**
ClickShare Button (wireless presentation)	TCP	2345, 6544
	UDP	
ClickShare Desktop and Mobile Apps (wireless presentation)	TCP	6541-6545
	UDP	5353; 1900
Additional ports for Wireless Conferencing (Button or 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	n/a
XMS Cloud	TCP	80; 443
XMS Edge	TCP	4003
Auto-update	TCP	80; 443
	UDP	n/a
SNMP	UDP	161 and 162
REST API	TCP	4003

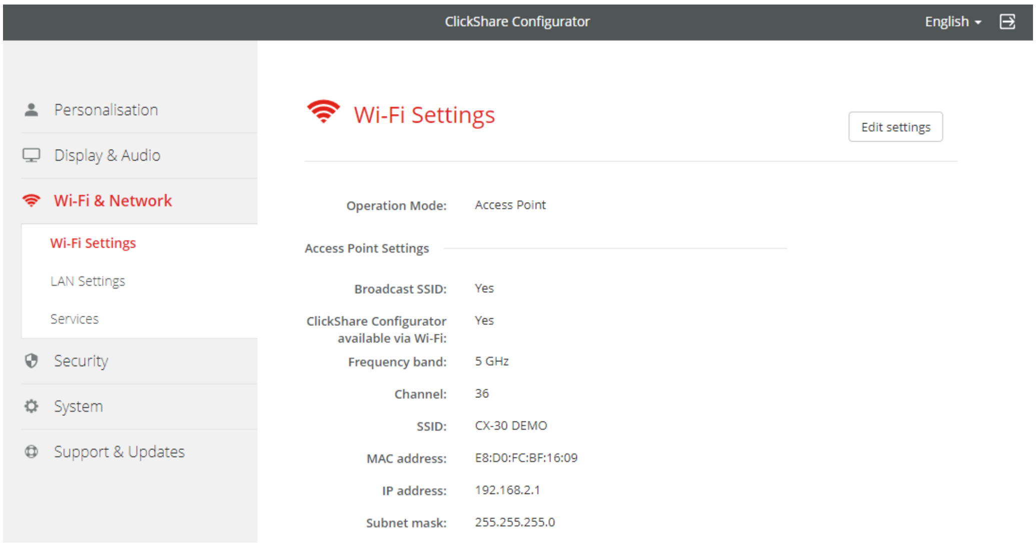
Table: Firewall recommendations

[6] Google Cast will pick a random UDP port above 32768 to facilitate video streaming.

Configuration

Wireless Client: configuration

To configure the wireless client capabilities of the Base Unit, navigate to the “Wi-Fi Settings” pane under “Wi-Fi & Network”, where you will find an overview of the Wi-Fi settings for the device. Note in the images below that there is a difference in capabilities between the C-5, C-10, CX-20, CX-30, CB Core and Pro, and the CX-50 and CX-50 Gen2. The latter having concurrent connectivity support and can simultaneously connect to a wireless network and provide an access point for the Buttons to connect to directly. Enabling the wireless client capabilities on a C-5, C-10, CX-20 or CX-30, as well as the ClickShare Bar Core and Pro, will require to connect the Buttons to the corporate network as is explained here.



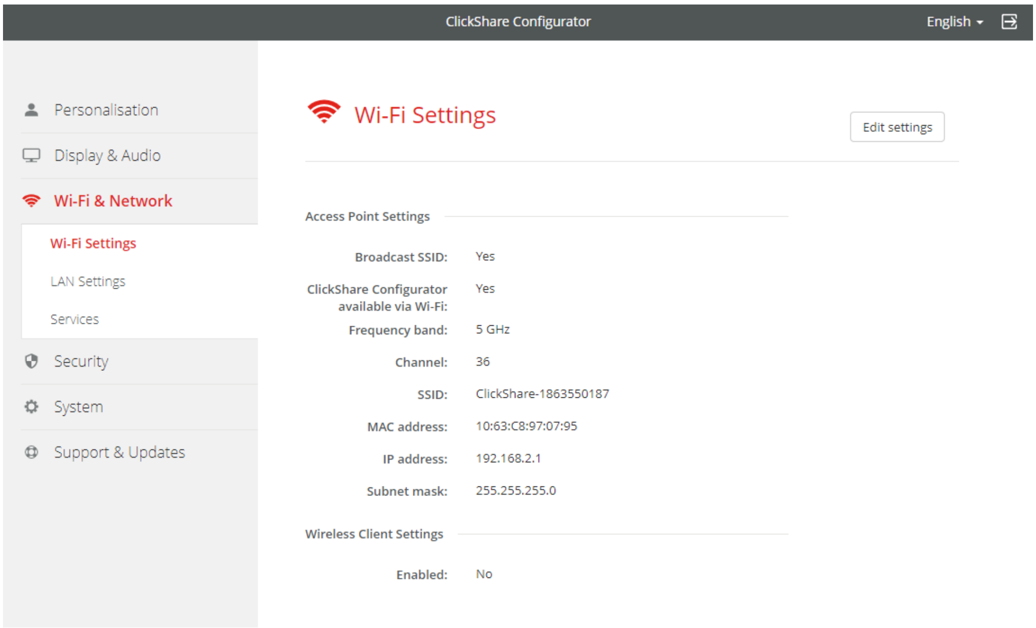
Wi-Fi Settings

Operation Mode: Access Point

Access Point Settings

Broadcast SSID: Yes
ClickShare Configurator available via Wi-Fi: Yes
Frequency band: 5 GHz
Channel: 36
SSID: CX-30 DEMO
MAC address: E8:D0:FC:BF:16:09
IP address: 192.168.2.1
Subnet mask: 255.255.255.0

Figure: Base Unit Wi-Fi settings for a C-5, C-10, CX-20 and CX-30, and ClickShare Bar Core and Pro



Access Point Settings

Broadcast SSID: Yes

ClickShare Configurator available via Wi-Fi: Yes

Frequency band: 5 GHz

Channel: 36

SSID: ClickShare-1863550187

MAC address: 10:63:C8:97:07:95

IP address: 192.168.2.1

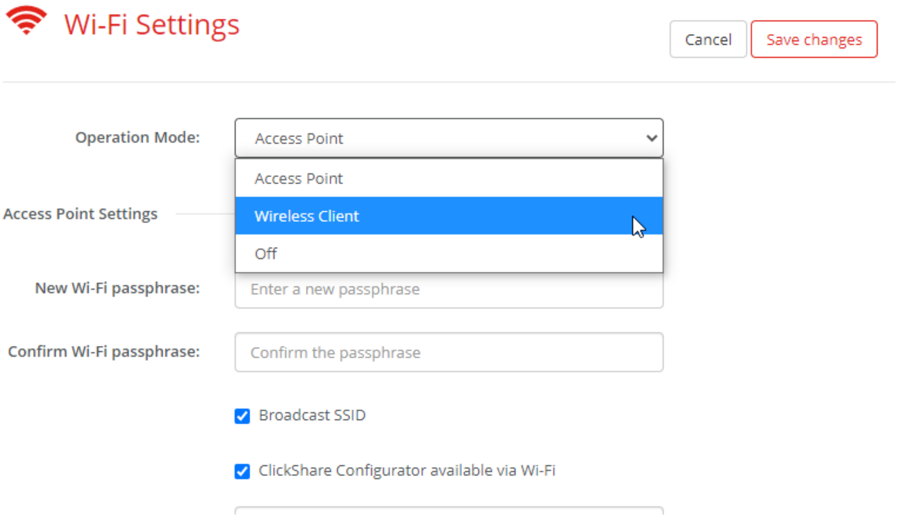
Subnet mask: 255.255.255.0

Wireless Client Settings

Enabled: No

Figure: Base Unit Wi-Fi settings for a CX-50/CX-50 Gen2. Note the separate Access Point and Wireless Client settings

To configure the wireless client capabilities of the Base Unit, click the "Edit settings" button on the top right. On the C-5, C-10, CX-20 and CX-30 as well as the ClickShare Bar Core and Pro, select the wireless client option in the dropdown on the top. For the CX-50/CX-50 Gen2, enable the wireless client checkbox at the bottom of the page.



Operation Mode: Access Point

Access Point Settings

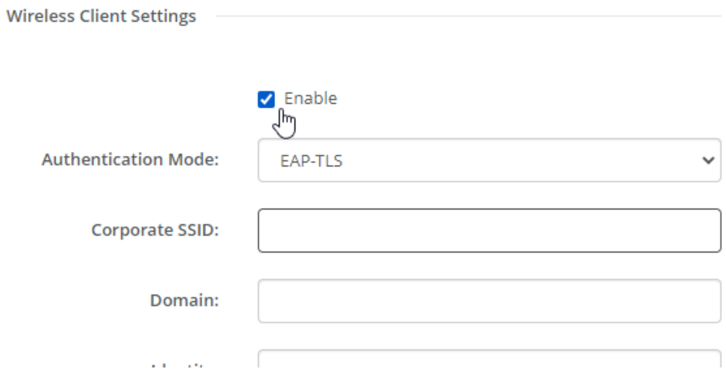
New Wi-Fi passphrase:

Confirm Wi-Fi passphrase:

☑ Broadcast SSID

☑ ClickShare Configurator available via Wi-Fi

Figure: On the CX-20, CX-30 and ClickShare Bar Core and Pro, select the Wireless Client option in the dropdown.



Wireless Client Settings

☑ Enable

Authentication Mode: EAP-TLS

Corporate SSID:

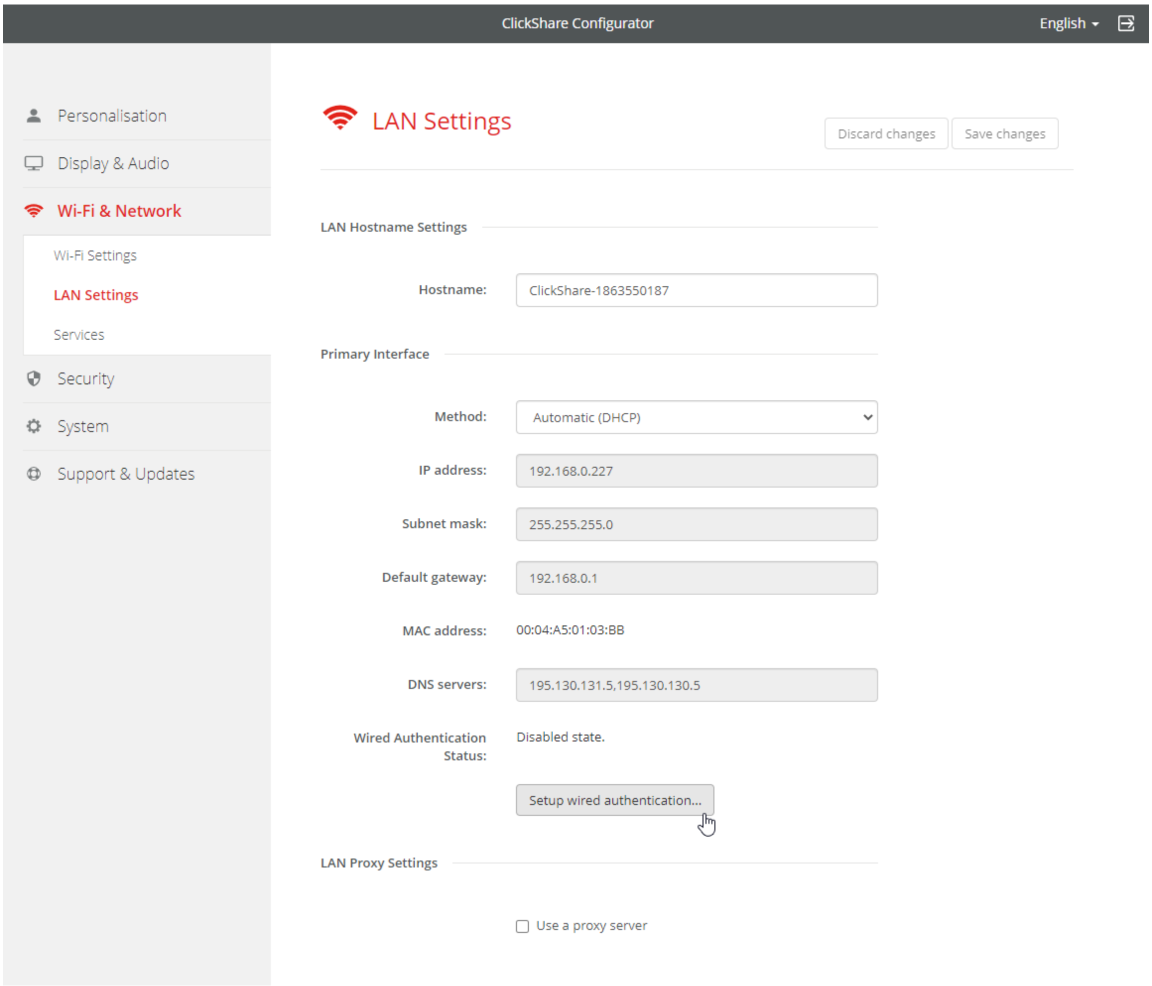
Domain:

Figure: On the CX-50/CX-50 Gen2, tick the "Enable" checkbox under the Wireless Client settings section.

Select the appropriate Authentication mode and fill in the required fields for each respective authentication mode. Once configured, click the "Save changes" Button on the top right on the page.

Wired network authentication: 802.1X

To enable and configure authentication on the wired network interface, navigate to the "LAN Settings" pane under "Wi-Fi & Network" and click the "Setup wired authentication" button near the bottom of the page. Upon clicking this button, a wizard will open to select the desired authentication method and to configure the required settings.



LAN Hostname Settings

Hostname: ClickShare-1863550187

Primary Interface

Method: Automatic (DHCP)

IP address: 192.168.0.227

Subnet mask: 255.255.255.0

Default gateway: 192.168.0.1

MAC address: 00:04:A5:01:03:BB

DNS servers: 195.130.131.5,195.130.130.5

Wired Authentication Status: Disabled state.

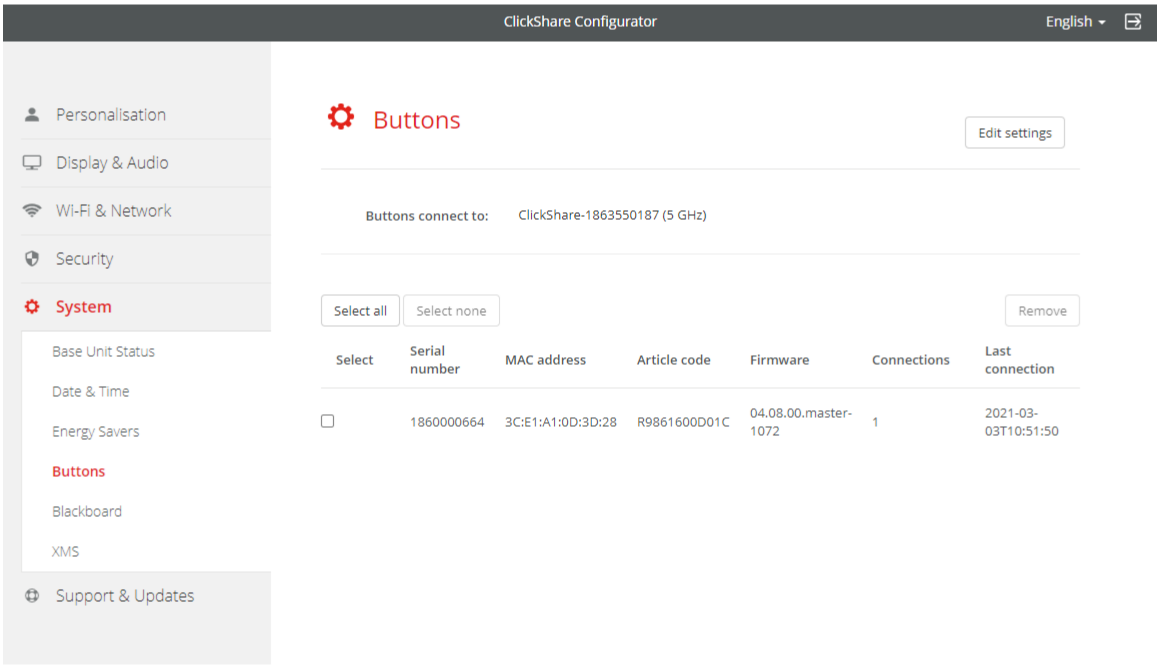
LAN Proxy Settings

☐ Use a proxy server

Figure: Base Unit LAN settings: where to set up wired authentication.

Button network integration

To enable and configure the ClickShare Button network integration, navigate to the Buttons pane under “System” in the Base Unit’s web interface.



Buttons connect to: ClickShare-1863550187 (5 GHz)

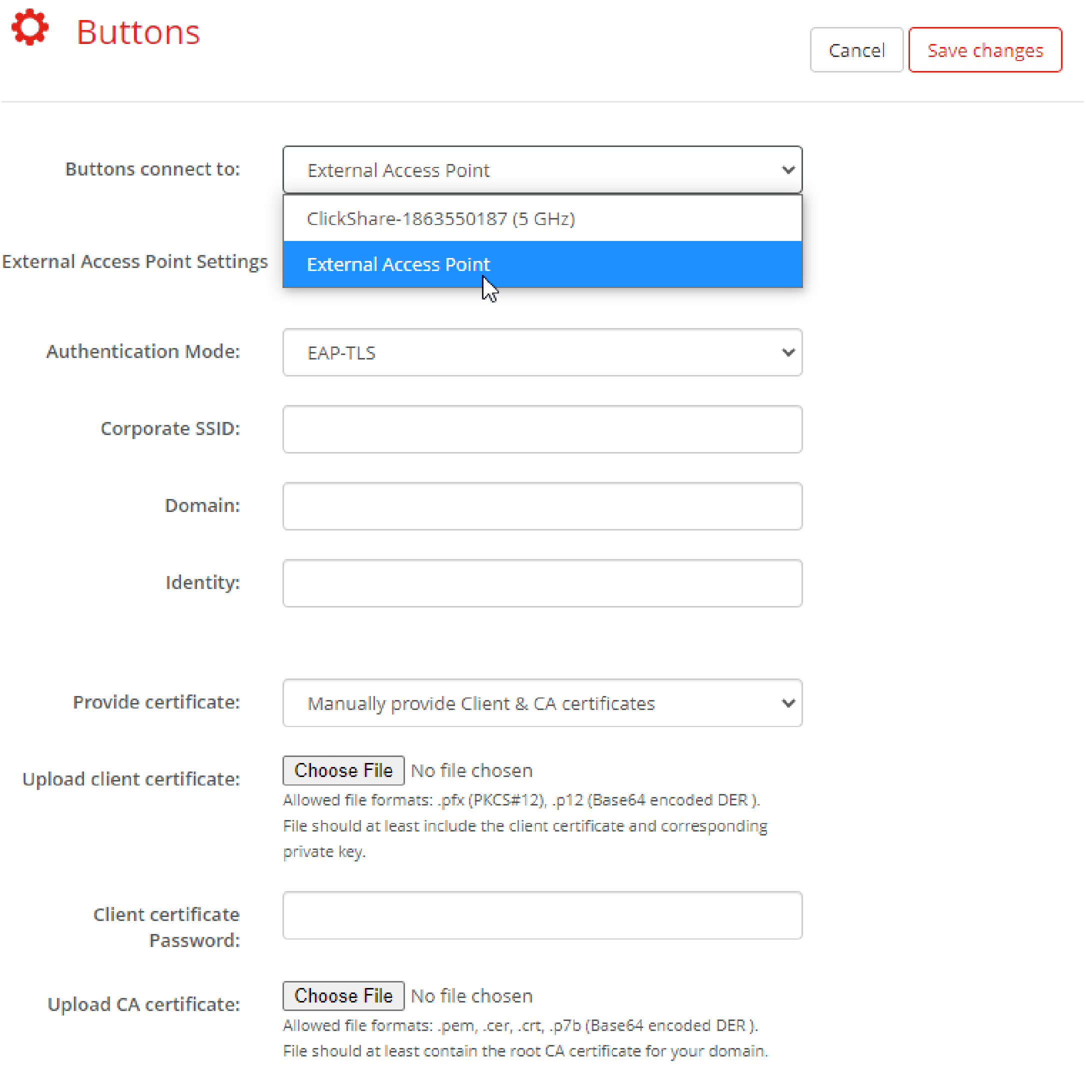
Select	Serial number	MAC address	Article code	Firmware	Connections	Last connection
□	1860000664	3C:E1:A1:0D:3D:28	R9861600D01C	04.08.00.master-1072	1	2021-03-03T10:51:50

Figure: Buttons settings pane in the Base Unit’s web interface.

To connect the Buttons to another wireless network than the Base Unit’s built-in access point, click the “Edit settings” button on the top right and select “External Access Point” in the dropdown menu. Select the appropriate Authentication mode and fill in the required fields for each respective authentication mode. Once configured, click the “Save changes” Button on the top right on the page. Upon completion, pair the Buttons with the Base Unit to load the connection settings into the Buttons.

Note that this will not disable the access point of the Base Unit. Although we do not recommend turning off the access point as it reduces the PresentSense™ capabilities of the system (see PresentSense™ section in the guidelines), this can be done in the “Wi-Fi Settings” pane under “Wi-Fi & Network”.

When setting up the Base Unit in a dual network configuration, make sure to read the remarks in the dual network chapter in the requirements section.



Buttons connect to: External Access Point

ClickShare-1863550187 (5 GHz)
External Access Point

External Access Point Settings

Authentication Mode: EAP-TLS

Corporate SSID:

Domain:

Identity:

Provide certificate: Manually provide Client & CA certificates

Upload client certificate: No file chosen
Allowed file formats: .pfx (PKCS#12), .p12 (Base64 encoded DER). File should at least include the client certificate and corresponding private key.

Client certificate Password:

Upload CA certificate: No file chosen
Allowed file formats: .pem, .cer, .crt, .p7b (Base64 encoded DER). File should at least contain the root CA certificate for your domain.

Figure: configuration page when opting to connect the Buttons to an external access point.

Recommendations for Wi-Fi configuration

Important note

This section is applicable for direct connections between the Base Unit and the Button(s) or ClickShare Apps.

ClickShare relies on the **Wi-Fi standard (IEEE 802.11a/g/n/ac)** for the communication between the Base Unit access point and the clients: the ClickShare Buttons or ClickShare Apps.

Buttons

Consider the following recommendations for the Buttons:

- Buttons only use 20 MHz channel bands.
- Depending on the Base Unit’s location's specific restrictions, the Buttons can connect only to certain Wi-Fi channels. An overview is given in the tables below.
- When connected directly to the Base Unit, the Buttons do not support dynamic channel assignment or DFS channels. When connected to corporate access points, one can make use of most available DFS channels.
- Buttons do not support roaming. When Buttons change their connection to another access point or when channel hopping occurs on the corporate access point, the Button will lose its connection momentarily and a noticeable disruption in the stream can happen.
- Buttons apply QoS tagging on the conferencing audio. In this way, priority is always given on the audio in the conference to provide a good call experience, even in bad environments.

Wi-Fi spectrum and channels organization

The IEEE 802.11 a/g/n/ac standard uses part of the 2.4GHz ISM band and of the 5GHz U-NII bands. The 2.4GHz ISM band (industrial, scientific and medical) goes from 2.400 GHz to 2.500GHz and can be used freely by any radio device for industrial, scientific and medical application. This band is also used by several common telecommunications protocols or standards such as Wi-Fi, Bluetooth, ZigBee, RFID devices …

Reference: A more comprehensive list of systems authorized on this band can be found at https://efis.cept.org/sitecontent.jsp?sitecontent=ecatable for the European Union and at http://transition.fcc.gov/oet/spectrum/table/fcctable.pdf for the United States.

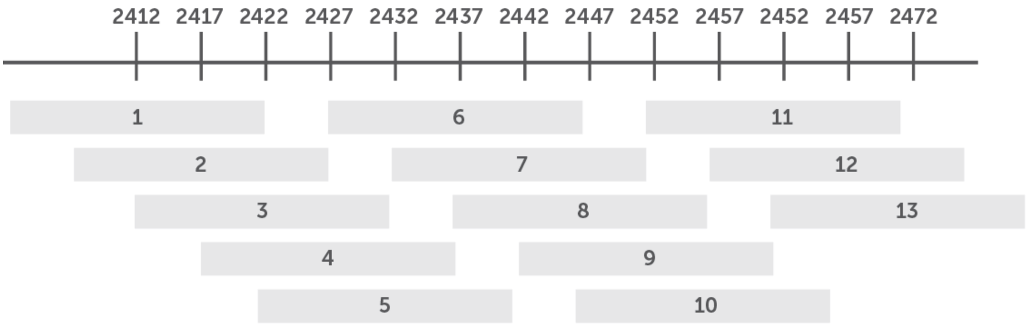


Figure: Wi-Fi channels in the 2.4GHz band

The 802.11 standard divides the **2.4GHz ISM band** into thirteen 22MHz wide channels, spaced 5MHz from each other. Consequently, these channels strongly overlap. The availability of these channels varies from country to country. ClickShare respects **local regulations**. The following table shows which channels are enabled for the regional versions of ClickShare, for both the Base Unit in client or access point mode, as the for the Buttons.

Channel number	Frequency range (MHz)	Clickshare Regional Version	
		RW / NA / US	EU / CN / ZH
1	2401 – 2423	X	X
2	2406 – 2428	X	X
3	2411 – 2433	X	X
4	2416 – 2438	X	X
5	2421 – 2443	X	X
6	2426 – 2448	X	X
7	2431 – 2453	X	X
8	2436 – 2458	X	X
9	2441 – 2463	X	X
10	2446 – 2468	X	X
11	2451 – 2473	X	X
12	2456 – 2478	(*)	X
13	2461 - 2483	(*)	X

Table: ClickShare channels in the 2.4 GHz frequency band
(*) Can be used when Base Unit or Buttons connected to a corporate access point only.

The **5GHz U-NII band** covers discontinued parts of the RF spectrum between 5.15GHz and 5.825GHz and allows the use of unlicensed wireless systems. The U-NII band is divided into 4 different sub-bands, which are subject to specific restriction, as is shown in the following table.

Band	Frequency range (MHz)	Number of Wi-Fi channels	Restriction
U-NII 1	5150 - 5250	4	Until recently only 7 channels were available, limited to indoor use only
U-NII 2	5250 – 5350	4	Requires use of radar detection (DFS Channels)
U-NII 2 extended	5470 – 5725	11	Requires use of radar detection (DFS Channels)
U-NII 3	5725 - 5825	4	

Table: U-NII organization

In contrast to the channels defined on the 2.4 GHz band, the channels defined on the 5 GHz band do not overlap.

As stated in the table with the U-NII bands, the U-NII 2 and U-NII 2 extended sub-bands are also used by several radar systems and can only be used by Wi-Fi access points using the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) algorithms. These 2 algorithms have been defined by the IEEE 802.11h standard. They specify a set of procedures to detect and to avoid interference with radar systems operating in the U-NII 2 and U-NII 2 extended sub-bands. Currently, the ClickShare access points do not support DFS and TPC as specified in the IEEE 802.11h standard.

The list of the 5 GHz channels enabled **between the Base Unit and the Button, when the Button connects to the access point of the Base Unit**, for the different ClickShare regional variants is displayed in the following table.

Regional variants	Available 5 GHz channels								
	36	40	44	48	149	153	157	161	165
NA	x	x	x	x	x	x	x	x	x
US	x	x	x	x	x	x	x	x	x
EU	x	x	x	x					
CN	x	x	x	x					
ZH	x	x	x	x	x	x	x	x	x
RW					x	x			

Table: ClickShare channels in the 5 GHz frequency bands

[7] http://www.fcc.gov/document/5-ghz-u-nii-ro

When the Button or the Base Unit is connected to a corporate access point, it can connect to the 5GHz channels listed in the table above and to an additional subset of DFS channels which are made available by the corporate access point, depending on the regional variant of the Base Unit. The overview of additional DFS channels that each regional variant can connect to is given in the table below:

Regional variants	Available DFS channels when connected to a corporate access point															
	U-NII-2A				U-NII-2C											
	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144
NA	x	x	x	x	x	x	x	x					x	x	x	
US	x	x	x	x	x	x	x	x					x	x	x	
EU	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
CN	x	x	x	x												
ZH	x	x	x	x												
RW																

Table: DFS channels in the 5 GHz frequency bands to which the Button and/or Base Unit can connect to for each regional variant

The 5 GHz band is much less used by non-Wi-Fi devices than the 2.4 GHz band. In addition, many of the older Wi-Fi devices only support the 2.4 GHz channels, meaning that the 5 GHz band is less crowded. Moreover, 5 GHz channels do not overlap. **As a result, the 5 GHz channels are the preferred choice when installing a new ClickShare setup.**

ClickShare Wi-Fi channel selection

Wireless communication signals travel over the air. When two devices transmit at the same time, on the same frequency, and within range of one another, they are likely to disturb each other.

When the interference is too strong, the packets transmitted by the Wi-Fi transmitter get so distorted that they are no longer correctly understood by the receiver, and as a result these packets must be retransmitted. This causes a decrease in the actual data rate achieved between the transmitting and the receiving Wi-Fi devices.

Site survey

Ideally, the ClickShare channel is selected after conducting a wireless site survey. A site survey maps out the sources of interference and the active RF systems. There are several Wi-Fi survey tools available on the market. Based on the results from a site survey, the least occupied channel can be found and selected for each meeting room.

Generic configuration rules

In case no site survey can be made, consider the following rules of thumb:

- The ClickShare access point in a particular meeting room should not re-use a Wi-Fi channel that overlaps with one of the channels used in the corporate WLAN infrastructure. Ideally, at least two channels in the corporate WLAN should be reserved exclusively for ClickShare. In case many ClickShare systems are located closely to one another, more channels may be required. When installing ClickShare Base Units, it is recommended to check with the local IT department which channels are not used by the corporate WLAN infrastructure.

- In an ideal setup, overlapping channels should not be used for two ClickShare Base Units within range of each other. As the channels in the 2.4 GHz band overlap with each other, best practice is to use channels 1, 6 and 11 on a single floor. On floors above and below, the channel pattern will be shifted to avoid overlap between floors, e.g. by placing channel 6 at the center of the illustrated pattern.

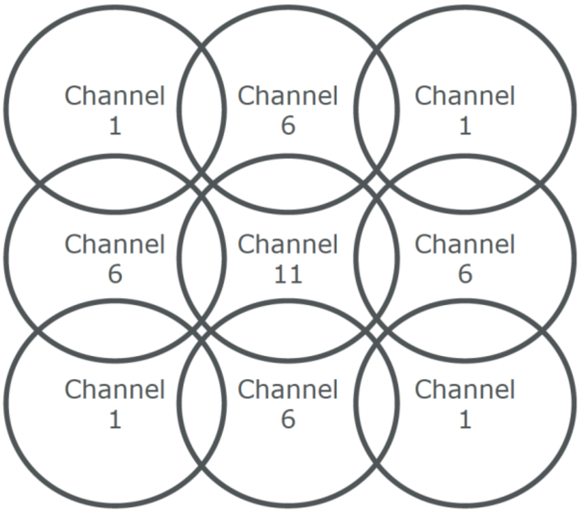


Figure: Theoretical Wi-Fi channel allocation map

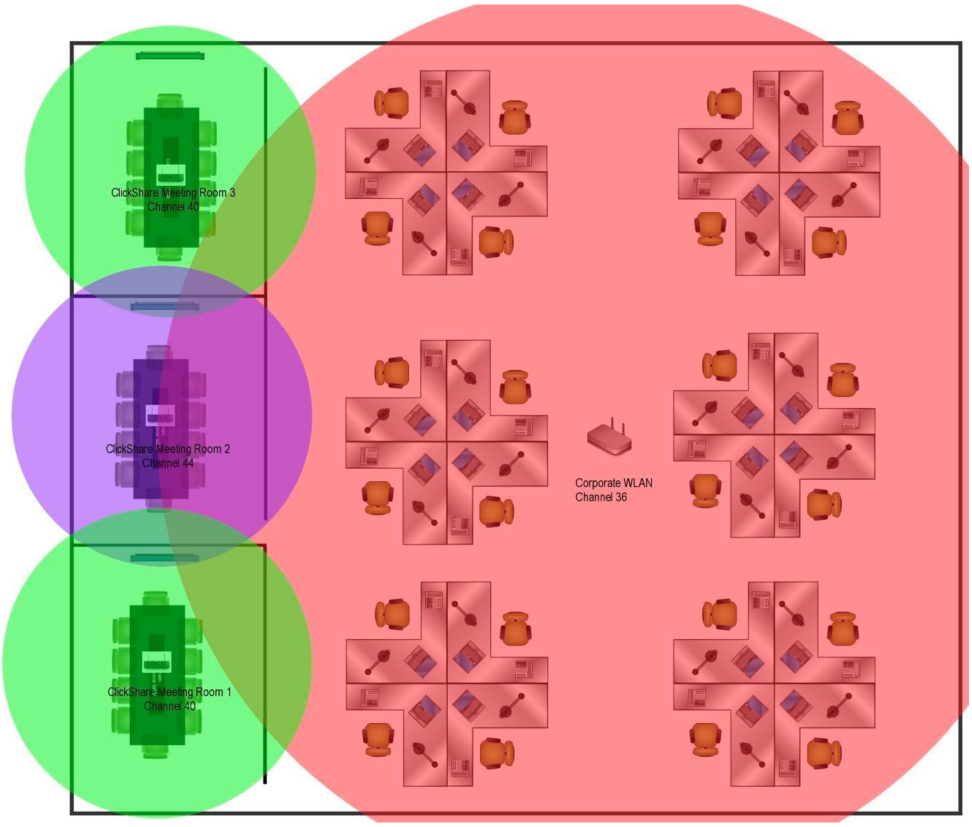

ClickShare Meeting Room 3
Channel 40
ClickShare Meeting Room 2
Channel 44
Corporate WLAN
Channel 36
ClickShare Meeting Room 1
Channel 40

Figure: Example of ClickShare installation in a corporate environment with 3 meeting rooms

- In case there are not enough channels available, two or more ClickShare Base Units can be placed on the same channel. This will of course have an impact on the quality of the link when several clients are sharing simultaneously. In a worst-case scenario, with three Base Units place on top of one another, this can result in performance issues, as illustrated in the following tables. The first table shows a scenario in which all clients are streaming video content, and the second table shows a standard office situation where clients share typical office documents or presentations.

Number of clients using conferencing functions	**Number of co-located Base Units sharing the same channel**		
	1	**2**	**3**
1	OK	OK	OK
2	OK	OK	Moderate risk of reduced quality
3	OK	Moderate risk of reduced quality	Strong risk of reduced quality
4	OK	Strong risk of reduced quality	Strong risk of reduced quality

Table: Connection quality matrix when multiple co-located Base Units use the same channel at the same time for video streaming

Number of clients sharing typical office documents	Number of co-located Base Units sharing the same channel		
	1	2	3
1	OK	OK	OK
2	OK	OK	OK
3	OK	OK	OK
4	OK	OK	Moderate risk of reduced quality

Table: Connection quality matrix when multiple co-located Base Units use the same channel at the same time for daily office work

- As stated above, the 5 GHz channels do not overlap with each other and are less used by non-Wi-Fi devices than the 2.4 GHz channels. Moreover, 5 GHz signals are more rapidly damped than 2.4 GHz signals. Therefore, the use of a 5 GHz channel is recommended. This will limit the impact of a ClickShare system on other installed ClickShare Base Units and on other WLAN users.

Acronyms

This is the list of acronyms used in this ClickShare Network Guide:

Acronym	In full
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
BU	Base Unit
BYOD	Bring Your Own Device
CA	Certification Authority
CCMP	Counter Mode Cipher Block Chaining Mesaage Authentication Code Protocol
CMGS	Collaboration Management Suite (renamed as XMS)
CS	ClickShare
DER	Distinguished Encoding Rules
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
IIS	Internet Information Services
LAN	Local Area Network
MAC	Media Access Control
NDES	Network Device Enrolment Service
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail

PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-in User Service
SCEP	Simple Certificate Enrolment Protocol
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
VLAN	Virtual Local Area Network
WAP	Wireless Access Point
WebUI	Web User Interface
WPA	Wi-Fi Protected Access
XMS	eXperience Management Suite