

Network Integration Guide

How to integrate and configure ClickShare in your network

DATE 11/04/2019

AUTHORS **Karel Paternoster** | Product Manager ClickShare

Gauthier Renard | Product Manager ClickShare

Michaël Vanderheeren | Product Line Manager ClickShare

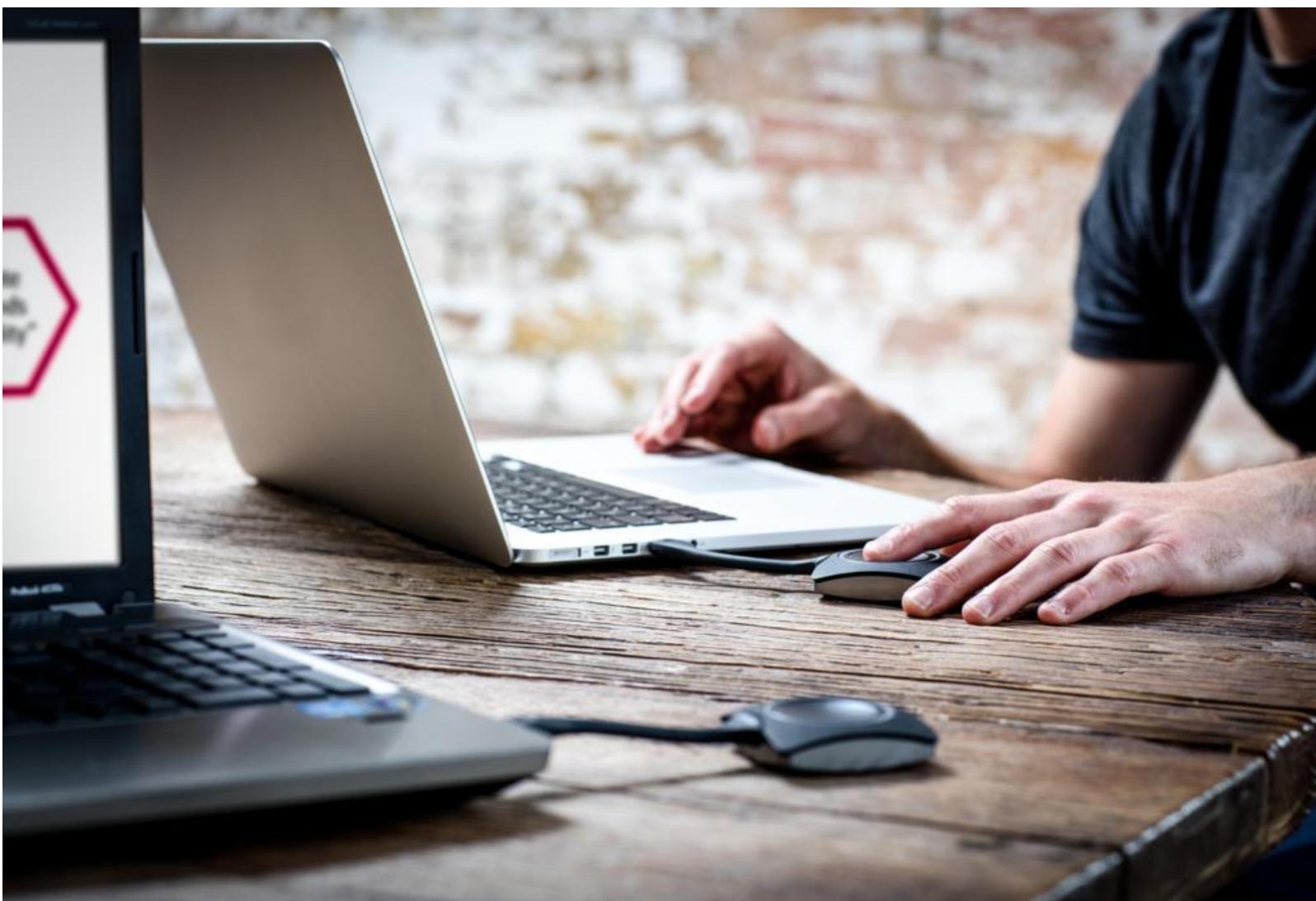


Table of content

About this Network Integration Whitepaper	5
Disclaimer	5
Limitations	5
Important notes on the ClickShare system installation	6
ClickShare : secure and easy enterprise-wide deployment	7
Network integration levels	8
Additional functionalities per integration level	9
Out-of-the-box use	10
Business requirements	10
Central Management	10
Out-of-the-box use with ethernet link	11
Business requirements	11
Central Management	11
Integration in the Enterprise network	12
Business requirements	12
Advantages	12
Prerequisites	13
Setup	13
Integration in a dedicated Enterprise network	14
Business requirements	14
Advantages	15
Prerequisites	15
Setup	15
Recommendations for network integration	16
Base Units	16
Buttons	17
ClickShare App	17
Airplay & Google Cast	17
VLAN	17
DNS	17

NTP	18
Dual Network Connection	18
SNMPv3	18
Firewall	19
Security modes for the Buttons	20
WPA2-Enterprise with 802.1x	20
WPA2-PSK or WPA2-Personal	20
Setting a Security Mode using the Network Integration wizard	21
Security mode EAP-TLS	21
Security mode EAP-TTLS	23
Security mode PEAP	24
Security mode WPA2-PSK	25
Post-setup	26
Apps	26
Quick-reference for the Network Integration wizard settings	27
Recommendations for Wi-Fi configuration	28
Buttons	28
Wi-Fi spectrum and channels organization	28
ClickShare Wi-Fi channel selection	30
Site survey	31
Generic configuration rules	31
Recommendations for using antenna extension cables with ClickShare Base Units	34
Scope for these recommendations	34
Situations that require antenna extension cables	34
Recommended cables	35
Communication range	35
Mounting the antennas	36
An example	36
Troubleshooting the ClickShare setup	40
The Button is unable to connect via the corporate network	40
Sharing using the ClickShare App, Airplay, and/or Google Cast is not working	40
The Button disconnects while sharing	41
The Base Unit does not accept the corporate network certificates	41
The sharing quality drops when enabling network integration mode	42

Troubleshooting the wireless setup	43
Check the RSSi from the connected clients	43
Measure the interference level	43
Effect of unauthorized rogue access point	43
Troubleshooting for support	44
Check the Button connection	44
Gathering in-depth network and system information	44
Troubleshooting for debug logs	48
ClickShare Client log (Button log)	48
Base Unit debug log	49
Acronyms	50

About this Network Integration Whitepaper

This guide helps you to get started with ClickShare and deploy the ClickShare Base Units either directly out of the box or by integrating them in your Enterprise network. It contains [an overview of the security modes](#) and offers you [recommendations for Wi-Fi configuration](#) and for [using antenna extension cables](#). Finally the [troubleshooting](#) sections provide you with an answer on the most common issues.

Note: Typically, all ClickShare network configurations are done only once, before use. The setup should not require any further modifications after installation.

Disclaimer

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

Take into account that the **ClickShare Base Unit and 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

Should you have any questions, please let us know via clickshare@barco.com.

Important notes on the ClickShare system installation

A correct installation of the ClickShare Base Unit is of critical importance to ensure optimal performance and a robust communication between the Base Unit and ClickShare Buttons, the ClickShare App and mobile devices. When installing ClickShare, take into account these recommendations:

- The credentials for network integration need to match the settings of the nearest Wi-Fi access point. Check whether the Button is connecting to your access point by verifying its presence in the MAC address table.

The Button has a MAC address starting with 00:23:A7 or 88:DA:1A.

The Base Units have MAC addresses starting with 00:04:A5 on the LAN ports.

- To use the auto-update function for ClickShare, ensure that cs-update.barco.com leads to cs-update-prod.elasticbeanstalk.com and whitelist these IP addresses: 52.201.38.187 and 52.5.31.207.

Specific recommendations for [Out-of-the-box use](#) and [Out-of-the-box use with Ethernet link](#):

- When setting the ClickShare up as out-of-the-box, the most favorable setup is a **direct line of sight between Base Unit and Buttons**. Any obstruction will cause the signal to follow a longer propagation path, possibly impacting performance.
- Due to the particular radiation pattern of the dipole antennas used with the ClickShare Base Unit, the antennas should not be placed above the ClickShare users. In case of a ceiling-mounted setup, **the advised position for the ClickShare Base Unit antennas is at the side of the meeting room**.
- **Do not use the ClickShare Base Unit without the shipped antennas**. Removing the antennas will cause severe degradation of the signal quality and may result in connection issues between the ClickShare Base Unit and clients. Note however that CS-100 and CSE-200+ models have internal antennas.
- **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. In case this setup cannot be avoided, please use a ClickShare rack-mounting kit or external antennas as explained in the ClickShare application note "[Recommendations for using antenna extension cables with ClickShare Base Units](#)".
- 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**.

For more information on the ClickShare setup, see: [Troubleshooting the ClickShare setup](#).

For more information on the wireless setup, see: [Troubleshooting the wireless setup](#).

ClickShare : secure and easy enterprise-wide deployment

ClickShare (CS) is Barco's wireless **presentation and collaboration system**. It allows any meeting participant to share content on the central meeting room screen **at the click of a button**. Connecting ClickShare does not alter the screen size or aspect ratio: what you see on your laptop or mobile device screen is replicated on the meeting room screen.

The ClickShare **CSE-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** and **Google Cast, Touch Back** support for interactivity and **multi-user on screen**. The CS-100 (Huddle) Base Units support the ClickShare App, but lack the other features.

The ClickShare Base Units come with **enterprise-strength security** that is configurable up to three levels for the CS100 (Huddle) and CSE-range. It can be controlled via the on-premise web configurator or via **a central asset management system** (CMGS or XMS) and be fully integrated into your corporate network. The Base Units also offer **a comprehensive API** for integration with other applications.

More ClickShare support documentation at <https://www.barco.com/en/support>

Network integration levels

This table shows the four network integration levels and the connection options between the ClickShare Base Unit, Button(s), laptops running the ClickShare App and mobile apps:

Integration level	Base Unit	Button	ClickShare App	Mobile apps
Out-of-the-box use	Completely disconnected (Base Unit Wi-Fi enabled)	Direct connection to the Base Unit	Direct connection to Base Unit	Direct connection to the Base Unit (1) + (2)
Out-of-the-box use with Ethernet link	Connected to Enterprise LAN via ethernet port (Base Unit Wi-Fi enabled)	Direct connection to the Base Unit	Direct connection to Base Unit / Connection via Enterprise Network	Direct connection to the Base Unit (1) + (2) or via Enterprise LAN (1)
Network Integrated	Integrated in Enterprise LAN via ethernet port (Base Unit Wi-Fi disabled)	Connection via Enterprise Network	Connection via Enterprise Network	Via Enterprise LAN (1)
Connected to a dedicated network (ClickShare vLAN) in the Enterprise network	Connected to ClickShare vLAN via ethernet port (Base Unit Wi-Fi disabled)	Connection via Enterprise Network	Connection via Enterprise Network	Connection via Enterprise Network (1) or via Guest Network (2)

Table: Overview Network integration levels

(1) For Mobile Devices Employees

(2) For Mobile Devices Guests

Note: For sharing over the corporate LAN from laptops running the ClickShare App and mobile devices using Airplay or Google Cast, the "Enable over LAN" option must be enabled, which can be controlled both via the Web Configuration page and the eXperience Management Suite (XMS).

Additional functionalities per integration level

The ClickShare Base Units can be configured to operate directly out of the box (default mode) or integrated in your network, depending on the functionalities required. The following table lists the additional functionalities per integration level.

Functionalities	Out-of-the box use	Out-of-the box use with Ethernet link	Network integrated	Connected to a dedicated Clickshare network
Central Management via eXperience Management Suite (XMS)	n/a	Via an Enterprise LAN	Via an Enterprise LAN	Via dedicated Enterprise LAN
Auto-update	n/a	Via an Enterprise LAN	Via an Enterprise LAN	Via dedicated Enterprise LAN
Configuring individual ClickShare Base Units	Via a direct connection to the Base Unit	Via an Enterprise LAN	Via an Enterprise LAN or wireless	Via dedicated Enterprise LAN or wireless
Remote pairing of ClickShare buttons	n/a	Via ClickShare Button Manager	Via ClickShare Button Manager	Via ClickShare Button Manager
Presence detection using the ClickShare App	Via Wi-Fi beacons	Via Wi-Fi beacons	Currently not available (1)	Currently not available (1)
SNMPv3 for monitoring hard- and software	n/a	Supported (2)	Supported (2)	Supported (2)
SSDP for advertisement & discovery of Base Units	n/a	Supported (2) (3)	Supported (2)	Supported (2)
Wired authentication via 802.1x	n/a	Supported (2)	Supported (2)	Supported (2)
Custom certificates for HTTPS	n/a	Supported (2)	Supported (2)	Supported (2)

Table: Overview of functionalities per integration level

- (1) In Network Integration mode, the ClickShare App does not support presence detection yet. This feature will be added as a firmware upgrade in the second half of 2019.
- (2) Supported from 1.7 firmware release onwards (March 2019).
- (3) Note that, in the out-of-the-box use with Ethernet connection, the ClickShare Base Unit will always respond to SSDP messages, independent of the 'enable over LAN' toggle state.

Out-of-the-box use

In this default mode, the ClickShare Base Unit and Button(s) operate directly out of the box, without any integration in the Enterprise network. **Users can connect directly to the Base Unit Wi-Fi via the ClickShare Buttons, using the ClickShare App or Windows Wireless Display (Miracast)¹ or with their mobile devices using Airplay or Google Cast.**

Note: Using a ClickShare Button allows you to stay connected to the internet. Using the ClickShare App, Miracast, Airplay or Google Cast will require connecting to the Base Unit directly and will only be able to access the internet if the device supports to use data (3G/4G) at the same time. For an improved user experience, it is highly recommended to [connect an Ethernet cable to the Base Unit](#). For detailed Wi-Fi information on the usage of this mode, see also [Recommendations for Wi-Fi Configuration](#).

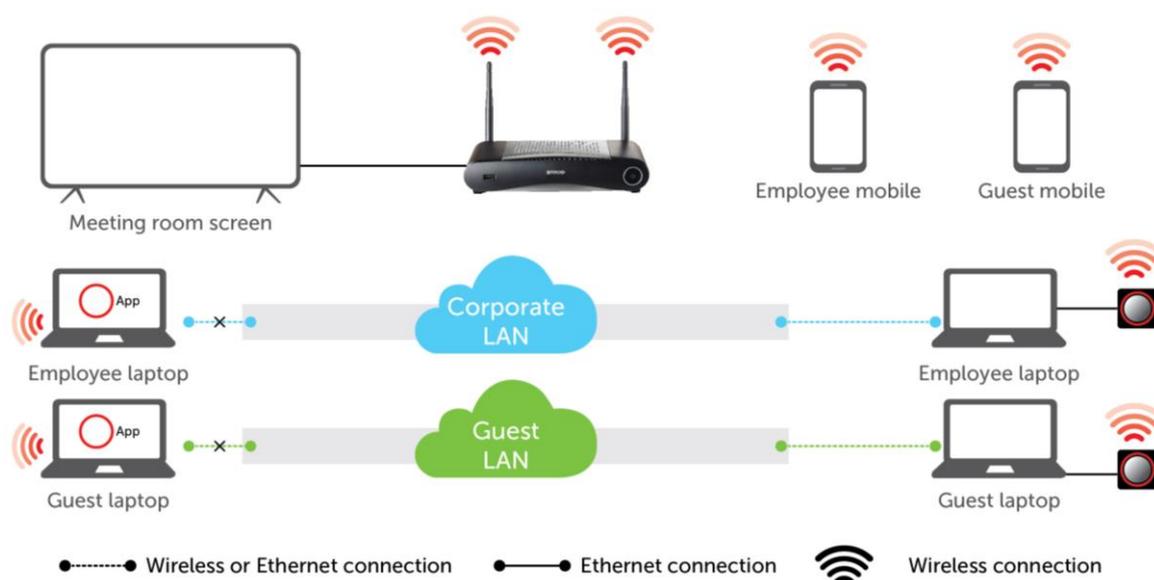


Figure: Out-of-the-box mode network topology diagram

Business requirements

Using the ClickShare Base Unit and Buttons directly out of the box is ideal for temporary setups, visitor centers and small to medium installations without network integration needs or possibilities. This setup requires the least installation effort and keeps any shared data completely separated from your Enterprise network. Updating and configuring the Base Units will need to be done manually.

Central Management

It is strongly recommended to also use the central asset management functionality for this out-of-the-box use. This means connecting the Base Unit to the Enterprise network via an Ethernet link in order to allow management using the eXperience Management Suite (XMS) and/or using the auto-update functionality. Refer to [Out-of-the-box use with Ethernet link](#).

¹ Miracast will be supported on the CSE-200+ with a firmware update in the second half of 2019.
P 10 / 51

Out-of-the-box use with ethernet link

In this extended out-of-the-box mode, an Ethernet connection is made between the ClickShare Base Unit and the corporate network. The ClickShare Base Unit Wi-Fi is kept enabled, ensuring users can still connect directly to the Base Unit Wi-Fi via the ClickShare Buttons, using the ClickShare App, Miracast, Airplay or Google Cast. **Employee computers running the ClickShare App or Miracast² and employee mobile devices using Airplay or Google Cast can connect via the corporate LAN if the "enable over LAN" option is enabled in the ClickShare Configurator or via XMS.**

Note: Using a ClickShare Button allows guests to stay connected to the Guest LAN and thus retain internet connectivity. Guest mobile devices will usually need to connect to the Base Unit directly and will only be able to access the internet if the device supports to use data (3G/4G) at the same time. For detailed Wi-Fi information on the usage of this mode, see also [Recommendations for Wi-Fi Configuration](#).

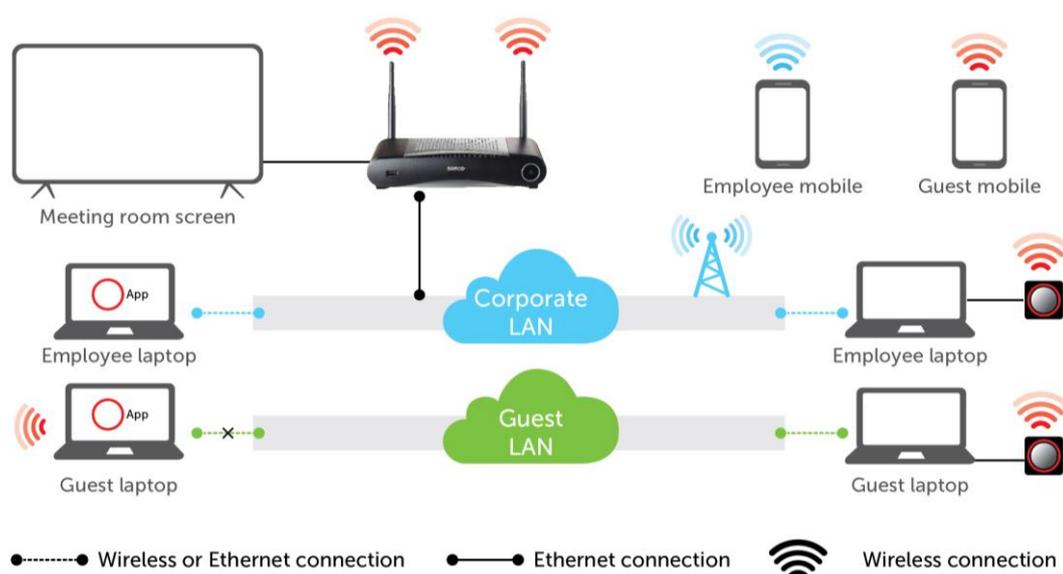


Figure: Out-of-the-box mode network topology diagram

Business requirements

Using the ClickShare Base Unit and Buttons directly out of the box is ideal for temporary setups, visitors' centers and small to medium installations without network integration needs. The Ethernet connection allows employees to use the ClickShare App without switching their Wi-Fi network, as well as central management via XMS and for auto-updates. Guest BYOD users will usually not be able to share with the ClickShare Base Unit unless they switch their Wi-Fi connection to the Base Unit SSID.

Central Management

Connecting the Base Unit to the Enterprise network via an Ethernet link opens the possibility for using the eXperience Management Suite (XMS) and/or using the auto-update functionality.

² Miracast will become available on the CSE-200+ with a firmware update in the second half of 2019.

Integration in the Enterprise network

In this full network integration mode, the ClickShare Base Unit is integrated into the corporate network or guest network via a cabled connection. The Base Unit's wireless access point is disabled and all traffic from the Button(s), the ClickShare App as well as Airplay and Google Cast travels via the Enterprise network to the Base Unit. **Employees and guests can share directly via the ClickShare Button or when connected with their mobile device to the same Enterprise network. Employees can also share using the ClickShare App if the "Enable over LAN" option is enabled in the Web Configurator/XMS** (for guest users, a bridge is required between the guest and corporate network).

Note: The ClickShare Buttons are wirelessly connected via the corporate access points (APs) to the corporate LAN. All sharing traffic travels through the LAN to the Base Unit. Please refer to [Recommendations for network integration](#) for further information.

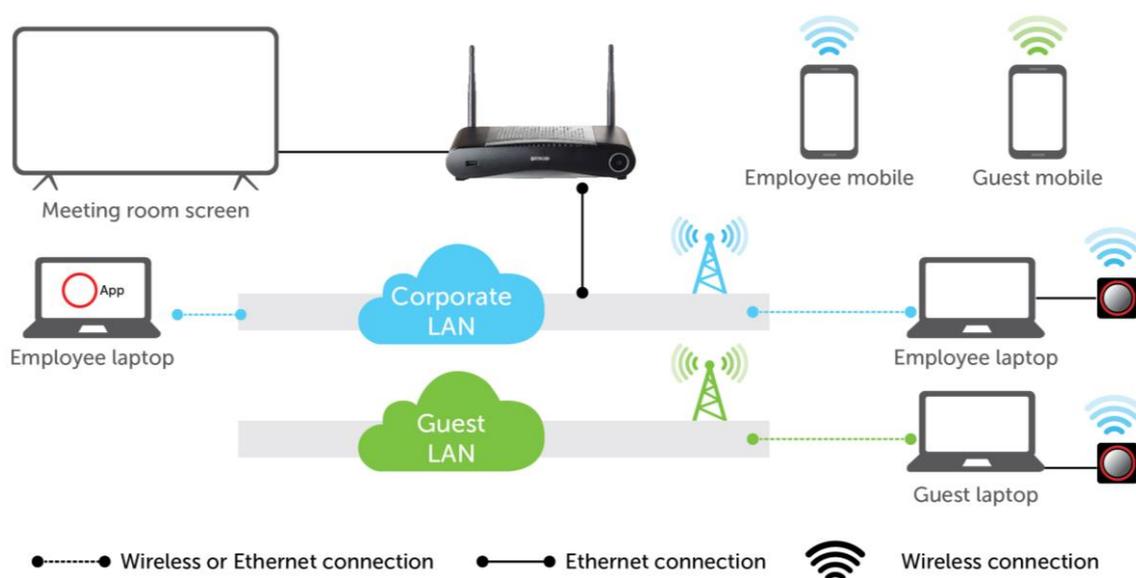


Figure: Enterprise network integration topology diagram, for this example the corporate LAN is used

Business requirements

This setup is used for large Enterprise installations where ClickShare Units are integrated into a single corporate network, which is used for all devices.

Advantages

- Less Wi-Fi access points allowing to better control the Wi-Fi spectrum.
- Easy installation in your Enterprise network via the built-in Wizard in the ClickShare configurator or via XMS.
- Improved Wi-Fi coverage for the Buttons and BYOD devices.
- Employees can keep using their mobile devices on the same Enterprise network while sharing via ClickShare.
- Employees can share using the ClickShare App without switching networks, keeping their internet access over Wi-Fi.
- Guests can share using the ClickShare Button, keeping their internet access over Wi-Fi.

Prerequisites

In order to configure the ClickShare devices for integration in the Enterprise network:

- Ensure you have all required access rights and credentials to allow the ClickShare Base Units and Buttons on the network.
- Check the network capacity with the IT administrator to guarantee an optimal ClickShare experience.

Setup

To activate this network integration mode on the Base Unit **without XMS**

1. Connect with the Base Unit, browse to the ClickShare Configurator and log in.
2. Open the **Network integration** tab, click **Setup Network Configuration**, select the preferred authentication mode and fill out the details. Click **Save Configuration** when finished.
3. Pair the ClickShare Buttons again with the Base Unit to apply the new configuration.

References: Detailed steps on how to open the ClickShare Configurator are described in the Installation manual.

To activate this network integration mode on the Base Unit **with CMGS/XMS**

1. Log in to CMGS or XMS and go to the **Base Units** tab.
2. In the **device list** select the Unit(s) for deploying network integration mode.
3. Open the **Configure** dropdown list and choose **Network integration**.
4. Select one of the authentication modes for network integration mode and fill out the details.
5. Re-pair the ClickShare Buttons with the updated Base Unit(s) to apply the new configuration

References: Detailed steps on how to use CMGS / XMS are described in the CMGS / XMS User Guide.

Integration in a dedicated Enterprise network

In this integration mode, the ClickShare Base Unit is connected to **a dedicated physical or virtual LAN via a cabled network**. The Base Unit's wireless access point function is disabled. Corporate users as well as guests share directly via the ClickShare Button, via the ClickShare App and with their mobile devices using Airplay or Google Cast³ if they are connected to the dedicated LAN or Enterprise network. This setup allows for more fine grained access control or to separate the ClickShare network traffic from all other IP traffic to ensure business requirements in terms of bandwidth and latency.

Note: The ClickShare Buttons are also connected to the dedicated LAN and all sharing traffic travels through that LAN to the Base Unit. When using a ClickShare Button or ClickShare App⁴ for sharing, all users can keep their computers connected to any of the other connected networks and still have corporate and internet access. Mobile users will be able to access the internet on the corporate LAN if the network configuration allows it. Please refer to [Recommendations for network integration](#) for further information.

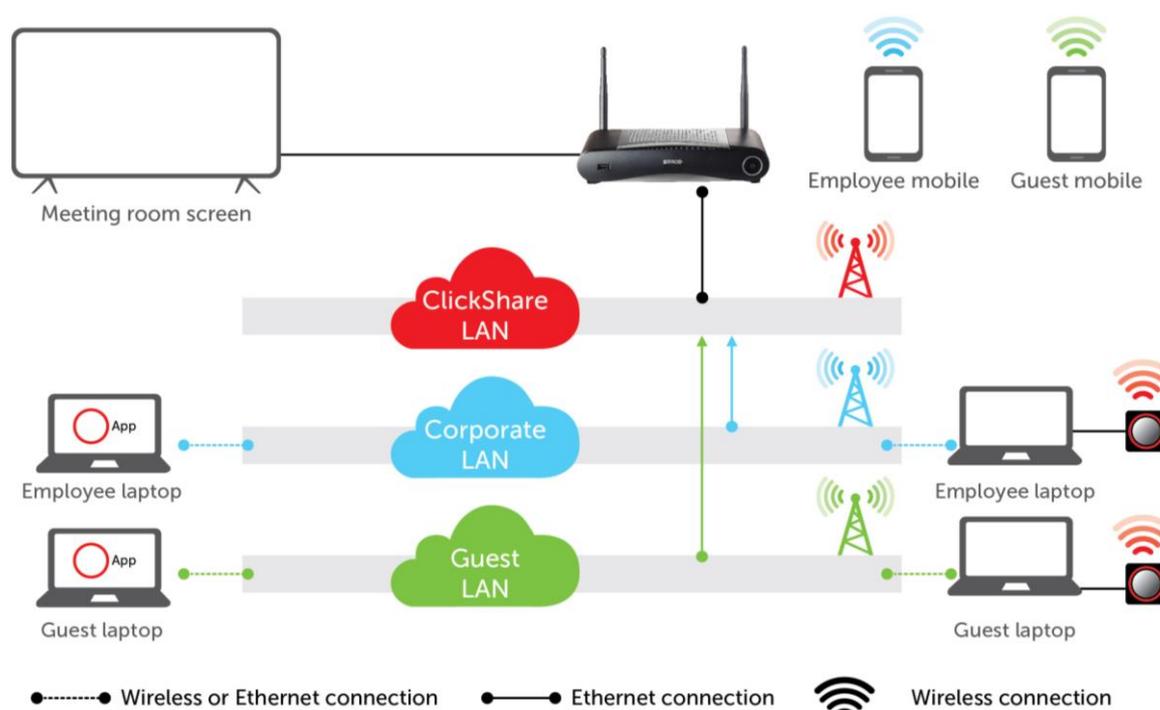


Figure: Network integration in dedicated network with routed Enterprise network topology diagram

Business requirements

This setup is used to integrate ClickShare into a dedicated network because a connection to an existing network is not required or wanted. It is preferred for large Enterprise installations where security constraints are strict, such as for Banks, Defense industry, Government, etc.

³ Service discovery and advertisement for Airplay and Google Cast devices is supported using the standard zeroconf multicast DNS (mDNS) protocol, called Apple's Bonjour protocol in the airplay case. This link-local multicast protocol is only forwarded to the local L2 network and thus aimed at a single subnet setup as it cannot be routed over multiple subnets. This inconvenience can be addressed by installing mDNS repeaters, often built-in into routers (eg. Cisco).

⁴ The March 2019 ClickShare firmware release introduced support for the SSDPv3 protocol, facilitating cross-network routing and easy connectivity, also in multiple subnet configurations. The ClickShare App makes use of this protocol for discovery, whereas Airplay and Google Cast only rely on mDNS.

Advantages

- Less Wi-Fi access points allowing to better control the Wi-Fi spectrum
- Eliminates any security risks via ClickShare because all Base Units are in an isolated and separate (virtual) LAN
- Easy management of all ClickShare Base Units in the separate (virtual) LAN, e.g. through their assigned IP addresses
- If the network configuration allows it, mobile users remain connected to their current network when sharing and have access to corporate environment and the internet. Enterprise network traffic is routed to the dedicated ClickShare network for content sharing purposes.

Prerequisites

In order to configure your devices for integration in a dedicated Enterprise network:

- Set up a dedicated network and ensure that you have all the access rights and credentials to allow the ClickShare Base Units and Buttons to connect to it and share on it.
- Ensure that the corporate wireless access points from which you want to share to a ClickShare Base Unit are connected to the dedicated ClickShare LAN.
- Install all the needed routing paths from the desired Enterprise networks to the dedicated LAN.
- Check the network capacity with the IT administrator to guarantee an optimal ClickShare experience.

Setup

To activate this network integration mode on the Base Unit **without XMS**

1. Connect with the Base Unit, browse to the ClickShare Configurator and log in.
2. Open the **Network integration** tab, click **Setup Network Configuration**, select the preferred authentication mode and fill out the details. **Save Configuration** when finished.
3. Pair the ClickShare Buttons again with the Base Unit to apply the new configuration.

References: Detailed steps on how to open the ClickShare Configurator are described in the Installation manual.

To activate this network integration mode on the Base Unit **with CMGS/XMS**

4. Log in to CMGS or XMS and go to the **Base Units** tab.
5. In the **device list** select the Unit(s) for deploying network integration mode.
6. Open the **Configure** dropdown list and choose **Network integration**.
7. Select one of the authentication modes for network integration mode and fill out the details.
8. Re-pair the ClickShare Buttons with the updated Base Unit(s) to apply the new configuration

References: Detailed steps on how to use CMGS / XMS are described in the CMGS / XMS User Guide.

Recommendations for network integration

This chapter contains all recommendations for integrating ClickShare into your Enterprise network. For integration of **wePresent** (WiPG/WiCS) devices, please refer to the [wePresent Network Deployment Guide](#).

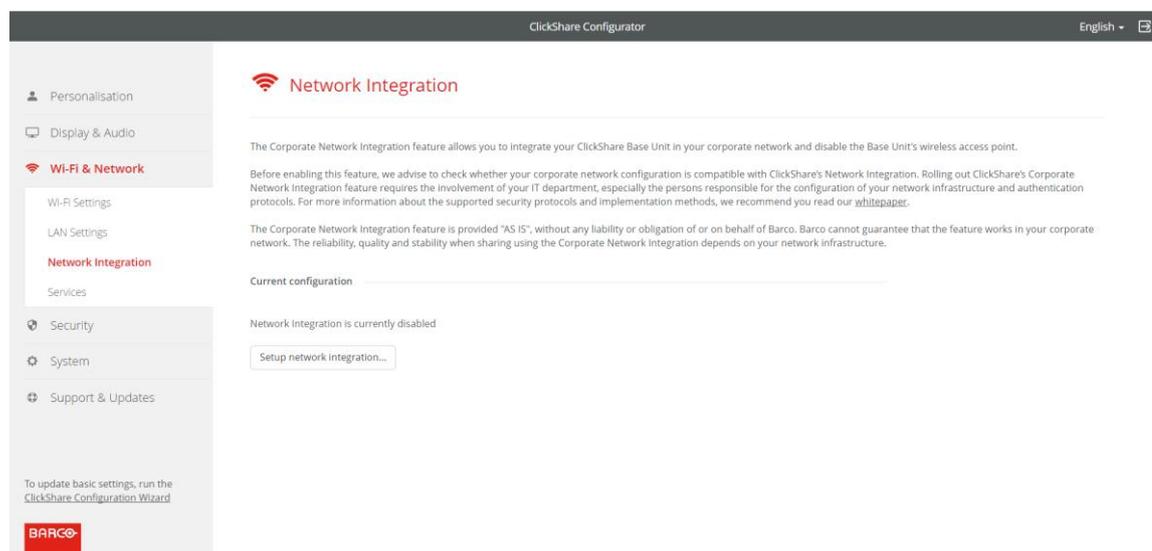


Figure: ClickShare Configurator Network Integration page

Base Units

- Ensure that all Base Units are connected to your network via a wired Ethernet interface⁵.
- The internal Wi-Fi access points on the ClickShare Base Units are disabled as soon as a ClickShare Button is paired with any of the Units over the corporate access points. The assigned IP-address of the Base Unit is displayed in the wallpaper.
- Provide sufficient bandwidth to prevent bottlenecks in your network (e.g. 100 Mbps switches), which could potentially degrade the ClickShare experience.
- Check whether the corporate wireless access points support the IEEE 802.11d standard.
- 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 Google Cast make use of the mDNS protocol. The ClickShare App makes use of SSDP for advertisement and discovery, a protocol which is easier to route in complex network setups.
- To use the auto-update function for ClickShare, ensure that cs-update.barco.com leads to cs-update-prod.elasticbeanstalk.com and whitelist these IP addresses: 52.201.38.187 and 52.5.31.207.

⁵ On the ClickShare CSE-800, network integration of the Buttons is currently only supported via the primary Ethernet interface. The secondary Ethernet interface can be used for all other functionalities, such as central management via the Collaboration Management Suite, control via the ClickShare API, remote Button pairing via the Button Manager and sharing for mobile devices via the "Enable over LAN" feature.

⁶ The CSE-200+ will receive a firmware update in the second half of 2019 which will allow to connect to a network over Wi-Fi (Wireless Client mode).

Buttons

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

- 2 Mbps bandwidth to present static content
- between 7 and 15 Mbps for optimal video performance

For more technical details, please refer to [Buttons](#).

ClickShare App

- The ClickShare desktop App uses SSDP for advertisement and discovery within the network, requiring to open UDP port 1900 in the network.
- Presence detection, which will sort the Base Units according to the measured signal strength, currently only works in [Out-of-the-box use](#) and [Out-of-the-box use with ethernet link](#). A firmware update in the second half of 2019 will make this functionality also available in network integration modes.
- The required bandwidth for sharing via the ClickShare desktop App is estimated around 2Mbps for static content and 5Mbps for video content.

Airplay & Google Cast

Note: Only for [Integration in the Enterprise network](#) and [Integration in a dedicated Enterprise network](#).

- AirPlay and Google Cast require multicast to make the ClickShare Base Unit discoverable within your network, requiring to open UDP port 5353.
- Both AirPlay and Google Cast are 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.

VLAN

In large installations, it is recommended to put all ClickShare Base Units in **a dedicated VLAN for easy management**, cf. [Integration in a dedicated Enterprise network](#).

Many corporate networks are divided into multiple virtual LANs, e.g. to separate BYOD (Bring Your Own Device) traffic from the "core" corporate network. When integrating ClickShare into your network, take into account that the ClickShare Buttons connecting to your wireless infrastructure, should be able to connect to the Base Units. Also, if you want to use the desktop and mobile Apps as well as Airplay and Google Cast, ensure that they can reach the Base Units.

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.

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.

Dual Network Connection

The two Ethernet interfaces on the CSE-800⁷ Base Unit allow to simultaneously connect the Base Unit to two separate networks on different subnets.

This allows for instance to connect simultaneously to the corporate and guest LAN, allowing both employees and guests to share content via the ClickShare App, Airplay or Google Cast to the ClickShare unit without changing their network connection. This 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.

SNMPv3

The 1.7 firmware release introduced the support of **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.

SNMPv3 is supported on the the entire CS(E)-xxx range 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.

⁷ A firmware update to the CSE-200+ in the second half of 2019 will allow dual network capabilities comparable to the CSE-800, with one physical Ethernet connection and one connection over Wi-Fi.

Firewall

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

Sender		CS-range	CSE-range	CSC-1	CSM-1
ClickShare Button	TCP	6541-6545	6541-6545	9870; 9876	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	514	514	514	1047-1049; 9870
ClickShare apps for Windows, MacOS, iOS and Android	TCP	6541-6545	6541-6545	389; 445; 515; 636; 1688; 1689; 3268; 8080	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	5353	5353	1047-1049; 9870	1047-1049; 9870
AirPlay	TCP	n/a	4100-4200; 7000; 7100; 47000	4100-4200; 7000; 7100; 47000	4100-4200; 7000; 7100; 47000
	UDP	n/a	4100-4200; 5353	4100-4200; 5353	4100-4200; 5353
Google Cast	TCP	n/a	8008; 8009; 9080	n/a	n/a
	UDP	n/a	1900; 5353; 32768:61000 ⁸	n/a	n/a
MirrorOp for ClickShare	TCP	6541-6545	6541-6545	389; 445; 515; 636; 1688; 1689; 3268; 8080	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	5353	5353	1047-1049; 9870	1047-1049; 9870
ClickShare Configurator	TCP	80; 443	80; 443	80	80
	UDP	n/a	n/a	n/a	n/a
ClickShare REST API & XMS	TCP	4000; 4001	4000; 4001	4000; 4001	4000; 4001
	UDP	n/a	n/a	n/a	n/a
Auto-update	TCP	80; 443	80; 443	80 (only via XMS)	80 (only via XMS)
	UDP	n/a	n/a	n/a	n/a
Button Manager	TCP	6546	6546	n/a	n/a

Table: Firewall recommendations

⁸ Google Cast will pick a random UDP port above 32768 to facilitate video streaming.
P 19 / 51

Security modes for the Buttons

The ClickShare Button supports **two security modes** to connect to the corporate network. Both modes are based on Wi-Fi Protected Access (WPA). WPA2 is an improved version of the original WPA standard, adding AES encryption for improved security.

- WPA2-Enterprise with 802.1x: for a typical corporate network setup
- WPA2-PSK or WPA2-Personal: for a more traditional Wi-Fi setup

WPA2-Enterprise with 802.1x

WPA2-Enterprise security relies on a server using RADIUS, to authenticate each client on the network. To do this, 802.1x authentication is used, also known as **port-based Network Access Control**.

802.1x encapsulates the Extensible Authentication Protocol (EAP) for use on Local Area Networks. This is also known as **EAP over LAN** or **EAPoL**. Using RADIUS, these EAPoL messages are routed over the network in order to authenticate the client device on the network. For ClickShare, these devices are the Buttons.

The 802.11i (WPA2) standard defines a number of required EAP methods. However, not all of them are used extensively in the field, and others, which are not in the standard, are used more often. Therefore, we have selected the most widely used EAP methods: **EAP-TLS**, **EAP-TTLS** and **PEAP**.

References: for more details on each EAP method and the setup instructions, please refer to the respective paragraphs on these security modes in following section:

- [Security mode EAP-TLS](#)
- [Security mode EAP-TTLS](#)
- [Security mode PEAP](#)

WPA2-PSK or WPA2-Personal

WPA2-PSK is short for Wi-Fi Protected Access 2 - Pre-Shared Key. This is also called **WPA** or **WPA2 Personal**. This is a method to secure mostly traditional Wi-Fi setups in a network using **WPA2** with the use of a username, a password and the optional Pre-Shared Key (**PSK**) authentication.

References: for more details on the WPA2-PSK method and the setup instructions, please refer to [Security mode WPA2-PSK](#).

Setting a Security Mode using the Network Integration wizard

To select a security mode and configure that mode for ClickShare, you can use the Network Integration Wizard in the ClickShare Configurator. The wizard will guide you through the integration process according to the security mode you select.

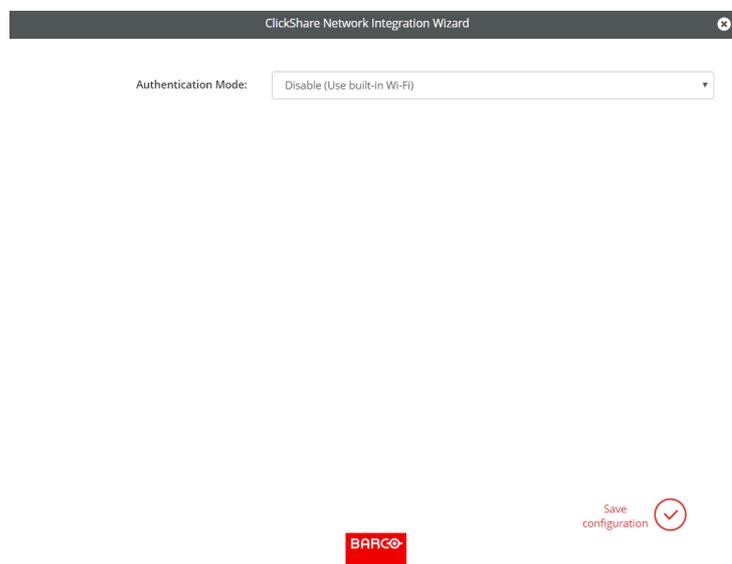


Figure: Start of the network integration wizard

Security mode EAP-TLS

EAP-TLS (Transport Layer Security) is an EAP method **based on certificates**, which allows mutual authentication between client and server. It **requires a PKI (Public Key Infrastructure)** to distribute server and client certificates⁹. EAP-TTLS and PEAP provide good alternatives to the EAP-TLS mode.

Even though **an X.509 client certificate** is not strictly required by the standard, it is **mandatory** in most implementations, including for ClickShare.

When implemented using client certificates, EAP-TLS is considered to be **one of the most secure EAP methods**. The only minor disadvantage, compared to PEAP and EAP-TTLS, is the transmission of the user's identity in the clear before the actual TLS handshake is performed. EAP-TLS is **supported via SCEP or manual certificate (.pem or .pfx format) upload**.

⁹ The 1.7 firmware release introduced the support for both custom certificates for HTTPS and multiroot certificates (certificate chaining). Custom certificates can be used instead of the self-signed ClickShare certificates, for instance to remove the privacy warning when navigating to the ClickShare Configuration page.
P 21 / 51

ClickShare Network Integration Wizard

Authentication Mode:

Corporate SSID:

Domain:

Identity:

Provide certificate:

Upload client certificate:
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: Geen bestand gekozen
Allowed file formats: .pem, .cer, .crt, .p7b (Base64 encoded DER). File should at least contain the root CA certificate for your domain.

Save configuration

Figure: Network integration via EAP-TLS

Auto-enrolment via SCEP

SCEP or Simple Certificate Enrolment Protocol enables issuing and revoking certificates in a scalable way. SCEP support is included to allow for quicker and smoother integration of the ClickShare Base Units and Buttons into the corporate network.

Because most companies use Microsoft Windows Server and its active directory (AD) to manage users and devices, our SCEP implementation is specifically targeted at the Network Device Enrolment Service (NDES), which is part of Windows Server 2008 R2 and 2012. At this time, **no other SCEP server implementations are supported.**

ClickShare Network Integration Wizard

Enter necessary data

Domain:

SCEP server:

SCEP username:

SCEP password:

Identity:

Corporate SSID:

< >

Figure: Network integration wizard via EAP-TLS – Authentication via SCEP

NDES

The Network Device Enrolment Service is Microsoft's server implementation of the SCEP protocol. If you want to enable EAP-TLS using SCEP, make sure **NDES is enabled, configured and running on your Windows Server**. For more details about setting up NDES, refer to the Microsoft website¹⁰.

SCEP uses a so-called "challenge password" to authenticate the enrolment request. For NDES, this challenge can be retrieved from your server at:

```
http(s)://[your-server-hostname]/CertSrv/mscep_admin.
```

Enter the necessary credentials in the setup wizard to allow the Base Unit to automatically retrieve this challenge from the web page and use it in the enrolment request. This automates the process.

For a detailed explanation of each setting, refer to the [Quick-reference for the Network Integration wizard settings](#).

Manually provide Client and CA certificates

If your current setup does not support SCEP, or if you prefer not to use it but still want to benefit from the mutual authentication EAP-TLS offers, upload the necessary certificates manually.

- **Client Certificate:** The client certificate should be signed by the authoritative root CA in your domain and linked to the user in the Identity field. Make sure the client certificate contains the private key, necessary to set up the TLS connection successfully. The client certificate should be a so-called device or machine certificate and not a user certificate.
- **CA Certificate:** The CA certificate is the certificate of the authoritative root CA in your domain that is used in setting up the EAP-TLS connection. During the wizard, the Base Unit ensures it can validate the chain of trust between the Client and the CA certificates.

Security mode EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) is an EAP implementation by Juniper¹¹ networks. It is designed to provide authentication that is as strong as for EAP-TLS, but does not require issuing a **certificate** to each user, **only to the authentication servers**.

User authentication is done by password, but the password credentials are transported in a securely encrypted tunnel based on the server certificates. User authentication is performed against the same security database that is already in use on the corporate LAN: for example, SQL or LDAP databases, or token systems.

Because EAP-TTLS is usually implemented in corporate environments without a client certificate, ClickShare does **not support for a scenario with client certificates**. If you prefer to use client certificates per user, it is recommended to use [Security mode EAP-TLS](#) instead.

¹⁰NDES White Paper: <http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs-en-us.aspx>

¹¹https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html

Figure 1: Network integration wizard via EAP-TTLS

For a detailed explanation of each setting, refer to the [Quick-reference for the Network Integration wizard settings](#).

Security mode PEAP

PEAP (Protected Extensible Authentication Protocol) is an EAP implementation co-developed by Cisco Systems, Microsoft and RSA Security. It sets up a secure TLS tunnel using the server's CA certificate. After that set-up, the actual user authentication takes place within the tunnel. This way of working enables using TLS security while authenticating the user, without the need for a PKI.

The standard does not mandate what method is to be used to authenticate within the tunnel. In this guide, however, we refer to **PEAPv0 with EAP-MSCHAPv2 as the inner authentication method**. This is one of the two certified PEAP implementations in the WPA and WPA2 standards – and the most common and widespread implementation of PEAP.

ClickShare Network Integration Wizard

Authentication Mode: PEAP

Corporate SSID:

Domain:

Identity:

Password:

Upload CA certificate (optional): Geen bestand gekozen
Allowed file formats: .pem, .cer, .crt, .p7b (Base64 encoded DER). File should at least contain the root CA certificate for your domain.

BARCO

Save configuration

Figure: Network integration wizard via PEAP

For a detailed explanation of each setting, refer to the [Quick-reference for the Network Integration wizard settings](#).

Security mode WPA2-PSK

WPA2-PSK does not distinguish between individual users. There is 1 password (PSK – Pre-Shared Key) for all clients connecting to the wireless infrastructure. This PSK is calculated based on the SSID and the passphrase. This makes set-up very straightforward. Once connected, all data transmitted between client and AP is encrypted using either a CCMP or TKIP 256-bit key.

ClickShare Network Integration Wizard

Authentication Mode: WPA2-PSK

Corporate SSID:

Passphrase:

BARCO

Save configuration

Figure: Network integration wizard via WPA2-PSK

For a detailed explanation of each setting, refer to the [Quick-reference for the Network Integration wizard settings](#).

Post-setup

Note: after completing the steps in the Integration Wizard, **re-pair all ClickShare Buttons with the Base Unit**. Pairing the Buttons again is **mandatory** because the previously configured mode is still active on the Base Unit. Consequently, you cannot share until re-pairing is done.

Apps

Any mobile device connected to the corporate network will be able to share content with any Base Unit on the network. You can, however, prohibit sharing from mobile devices via the Base Unit's ClickShare Configurator.

It is recommended to **enable passcode authentication for mobile devices**. You can find this option in the **ClickShare Configurator>Wi-Fi & Network>Services** page or you can enforce this authentication by selecting security level 2 or 3.

Quick-reference for the Network Integration wizard settings

Before setting up ClickShare in your network using the setup wizard, it is recommended to consult the settings and details described in this section.

Setting	Details
SCEP Server URL / Hostname	<p>The IP or hostname of the Windows Server in your network running the NDES service.</p> <p>Since Internet Information Services (IIS) supports both HTTP and HTTPS, specify which of the two you want to use. If not specified, the default HTTP will be used.</p> <p>Examples: -http://myserver or https://10.192.5.1 -server.mycompany.com (will use http)</p>
SCEP Username	<p>A user in your Active Directory (AD), which has the required permission to access the NDES service and request the challenge password.</p> <p>To confirm this, the user should be part of the CA Administrators group (in the case of a stand-alone CA) or have enroll permissions on the configured certificate templates.</p>
SCEP Password	<p>The password of the User Account used as SCEP Username. The password is never stored on the Base Unit. It is kept in memory just long enough to request the Challenge Password from the server, and then it is immediately removed from memory.</p>
Domain	<p>The company domain for which you are enrolling, should match the one defined in your Active Directory (AD).</p>
Identity	<p>The identity of the user account in the Active Directory (AD), which the ClickShare Buttons use to connect to the corporate network.</p>
Password	<p>The corresponding password for the identity that you are using to authenticate on the corporate network. Per Base Unit, every Button uses the same identity and password to connect to the corporate network.</p>
Corporate SSID	<p>The SSID of your corporate wireless infrastructure to which the ClickShare Buttons connect.</p>
Client Certificate	<p>Client certificates are always the so-called device or machine certificates, never a user certificate. These 2 formats for uploading a client certificate are supported:</p> <ul style="list-style-type: none"> • PKCS#12 (.pfx) – An archive file format for storing multiple cryptography objects. • Privacy Enhanced Mail (.pem) – A Base64 encoded DER certificate stored between 2 tags: “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” <p>When the provided PKCS#12 file also contains the necessary CA certificate, the Base Unit extracts it and verifies the chain of trust, so that you do not have to provide the CA certificate separately. Support for client certificates is limited to PEM on the ClickShare CSM-1 and CSC-1.</p>
CA Certificate	<p>The common .crt file extension is supported, which can contain a Base64 encoded DER certificate.</p>
Passphrase	<p>The password used in WPA2-PSK to authenticate for the wireless infrastructure. This can be a string of 64 hexadecimal digits or a code of 8 to 63 printable ASCII characters.</p>

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)** for the communication between the Base Unit access point and the clients: the ClickShare Buttons or ClickShare apps.

Buttons

Take into account 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 these **Wi-Fi channels**:
 - 1 to 13 in the 2.4 GHz band
 - 36 to 48 and 149 to 165 in the 5 GHz band
- Buttons do **not support roaming** and **dynamic channel assignment** or DFS channels¹².

Wi-Fi spectrum and channels organization

The IEEE 802.11 a/g/n 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 <http://www.efis.dk/sitecontent.jsp?sitecontent=ecatable> for the European Union and at <http://transition.fcc.gov/oet/spectrum/table/fcctable.pdf> for the United States.

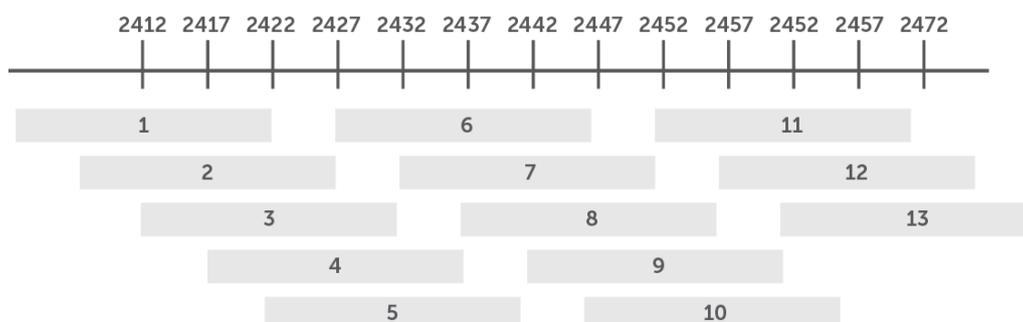


Figure: Wi-Fi channels in the 2.4GHz band

¹² The DFS channels will be made available for the Buttons when using the CSE-200+ in a firmware update in the second half of 2019.
P 28 / 51

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.

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

Table: ClickShare channels in the 2.4 GHz frequency band

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 13, 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.

¹³<http://www.fcc.gov/document/5-ghz-u-nii-ro>
P 29 / 51

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 standard¹⁴.

The list of the 5 GHz channels enabled for the different ClickShare regional variants is displayed in the following table.

Channel number	Frequency range (MHz)	Clickshare Regional Version			
		NA	EU	CN	ZH
36	5150 – 5170	X	X		X
40	5170 – 5190	X	X		X
44	5190 – 5210	X	X		X
48	5210 – 5230	X	X		X
149	5735 – 5755	X		X	X
153	5755 – 5775	X		X	X
157	5775 – 5795	X		X	X
161	5795 – 5815	X		X	X
165	5815 – 5835	X			

Table: ClickShare channels in the 5 GHz frequency bands

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 most often 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.

If you change the Wi-Fi channel for the Base Unit, the system will automatically check for sufficient bandwidth. If you see the message: "Intense use, change to another Wi-Fi channel", select another channel.

¹⁴ The DFS channels will be made available for the Buttons when using the CSE-200+ in a firmware update in the second half of 2019.
P 30 / 51

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, take into account 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.

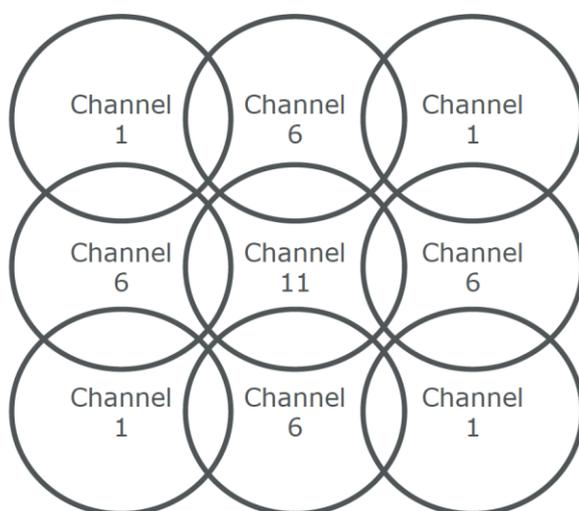


Figure: Theoretical Wi-Fi channel allocation map

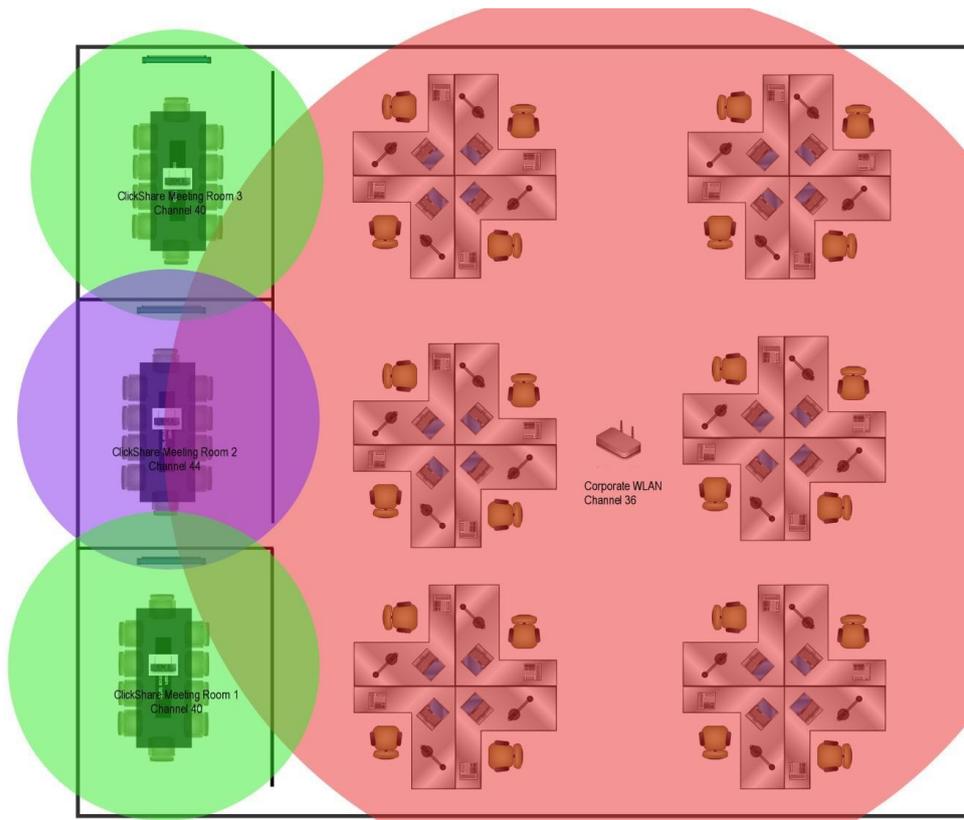


Figure: Example of ClickShare installation in a corporate environment with 3 meeting rooms

- In case there are not enough channels available, two or more ClickShare 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 sharing video	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

- To limit the effect of overlapping networks, it is highly recommended to **reduce the RF Tx Power** (standard range of about 30m) of the ClickShare Base Units. This can be adapted via the Base Unit ClickShare Configurator (Wi-Fi & network > Wi-Fi Settings > Signal strength). Reducing the Tx Power to its minimal value will reduce the actual range of the ClickShare to about 10m. By doing so, the size of coverage overlapping area will shrink and the risk for quality degradation on scenarios illustrated in the 2 tables above will decrease or even disappear.
- 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 units and on other WLAN users.



Recommendations for using antenna extension cables with ClickShare Base Units

Scope for these recommendations

This application note provides recommendations for the installation of antenna extension cables for the ClickShare wireless presentation system:

- The situations in which these extension cables can be used
- The types of cables that should be installed
- The way antennas should be mounted in the meeting room

Situations that require antenna extension cables

To ensure a good wireless connection, **obstacles** between the ClickShare Base Unit and the users **should be avoided**.

However, in some situations, the ClickShare Base Unit might be installed in a metallic rack or cabinet, or in a space external to the meeting room where the ClickShare users (ClickShare Buttons or ClickShare Apps for mobile devices) are located. The walls and metallic structures between the users and the Base Unit can attenuate the wireless signal, resulting in **poor signal quality, low transfer rate and, ultimately, lower system performance and less reliable behavior**.

When this is the case, **an antenna extension cable** can be a solution. Running antenna extension cables between the Base Unit and the antennas allows you to position the antennas in a more favorable location – where the obstacles blocking or attenuating the wireless signal can be avoided to achieve a more reliable connection and better performance.

ClickShare operates at Super High Frequencies (> 3 GHz). At such frequencies, the attenuation introduced by RF coax cables is considerable. Therefore, this type of solution is only advised up to a maximum length of 20 - 30 m (~65 – 100 ft), depending on the cable type used for the extension (see Table 1 for more details).

Extension cable length	10 m	20 m	30 m
Cable type: RG-8X	~20 m (~65 ft)	~25 m (~85 ft)	~8 m (~25 ft)
Cable type LMR-400	~25 m (~85 ft)	~20 m (~65 ft)	~16 m (~55 ft)

Table: typical maximum communication range with antenna extension cables at 5.8 GHz in direct line of sight

Antenna extension cables are a short-distance solution for avoiding attenuation by local obstacles. To cover larger distances between Base Unit and Buttons, it is recommended to use ClickShare in combination with an external access point using the network integration.

Only the antennas provided with the ClickShare set and passive RF coax cables can be used. Active wireless signal amplifiers between Base Unit and antennas are not allowed.

Recommended cables

The ClickShare system follows the IEEE 802.11n standard for communication between the Buttons and the Base Unit. ClickShare operates in the 2.412 GHz - 2.482 GHz, 5.170 GHz - 5.250 GHz and 5.735 GHz - 5.835 GHz ranges. At these frequencies, material quality and properties are critical.

Because cable loss in these frequency ranges is typically very high, only a few RF coax cable types are suitable for this application. The following table lists the recommended types. LMR-400 cables are built with a different dielectric material than RG-8X cables and have a larger coax core, resulting in a lower loss of signal strength but at a (much) higher purchase cost.

Cable Type	2.4 GHz	5.8 GHz
RG-8X	39.5 dB	63.9 dB
LMR-400	22.2 dB	35.5 dB

Table: Typical cable loss dB/100 m (dB/330ft)

To avoid additional signal degradation, the overall cable quality is critical. Connectors must be soldered carefully to the cable coax core with the correct tooling. An incorrect connector type, or poor soldering quality, will reduce the signal quality and may result in poor performance or unreliable system behavior. Therefore, we strongly recommend the use of prefabricated cable assemblies provided by a specialized company, as shown in the following table.

Connector A	Reversed Polarized SMA (RP-SMA) Jack (Male/Pin)
Connector B	Reversed Polarized SMA (RP-SMA) Plug (Female/Socket)
Coax type	RG-8X / LMR-400

Table: Cable assembly specifications

When installing the antenna extension cables, be sure:

- not to bend the coax cable more than the bend radius specified in the supplier datasheet
- not to pull the coax cable

Not respecting the above precautions can result in deterioration of the cable characteristics, leading to additional attenuation and to poor or less reliable performance of the ClickShare system.

Communication range

In a typical meeting room environment without antenna extension cables, the communication range of ClickShare between the Base Unit and a Button is about 30m (~100ft) in the case of direct line of sight. If antenna extension cables are used, the maximum communication range in the air between antennas and Buttons will be reduced.

The following table provides an estimation of the maximum distances achieved at 5.8 GHz in line of sight conditions. It shows that, in order to achieve sufficient coverage, RG-8X cables longer than 20m (~65ft) and LMR-400 cables longer than 30m (~100 ft) should be avoided.

Cable Type	2.4 GHz	5.8 GHz
RG-8X	39.5 dB	63.9 dB
LMR-400	22.2 dB	35.5 dB

Table: Typical cable loss dB/100 m (dB/330ft)

Even at distances shorter than the ones mentioned above, the attenuation introduced by the antenna extension cables will decrease the robustness of the ClickShare system against external sources of interference. As the attenuation of the signal strength is proportional to the cable length, it is important to **keep the antenna extension cables as short as possible**.

Mounting the antennas

The ClickShare system uses MIMO algorithms to achieve a high data rate and a robust communication link between the Button or mobile device, and the Base Unit. As a result, the following **installation rules** must be respected when setting up the antennas with an extension cable:

- The spacing between the 2 dipole antennas must be between 10 cm and 25 cm (between 4 and 10 inches).
- Antennas mounted on the ceiling should point downward – thus, perpendicular to the ceiling and parallel to the walls.
- Antennas mounted on walls should be oriented parallel to the wall.
- The antennas should be installed far enough (at least 50cm/1.6ft) from metallic surfaces to avoid unwanted reflections and far enough (at least 1m/3.3ft) from other radio equipment that operates in the same frequency range (e.g. other Wi-Fi access points, cordless telephone, microwave ovens ...). It is also best to install antennas at least 15cm (6 inches) from concrete walls.
- The most favorable situation is a direct line of sight between antennas and Buttons. Any obstruction will cause the signal to follow a longer propagation path, which can degrade performance.
- Due to the particular radio pattern of the dipole antennas used with the ClickShare Base Unit, the antennas should not be placed just above potential positions of ClickShare users. Therefore, the advised position for the antennas is at the side of the meeting room.

An example

A practical example of antenna positioning is shown below. In this example, the Base Units are installed outside the meeting rooms, in a separate technical room. Antenna extension cables are used to increase the range between Base Unit and Buttons or mobile devices.

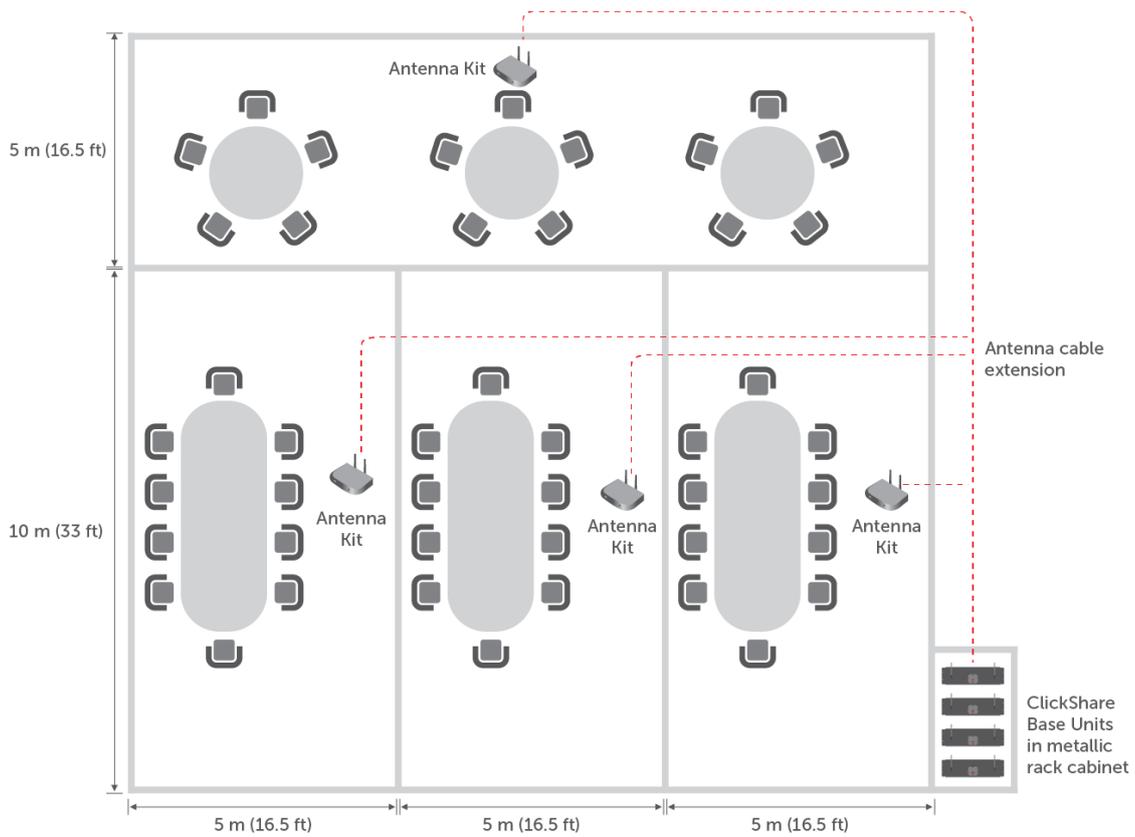


Figure: Example installation of antenna extension cables

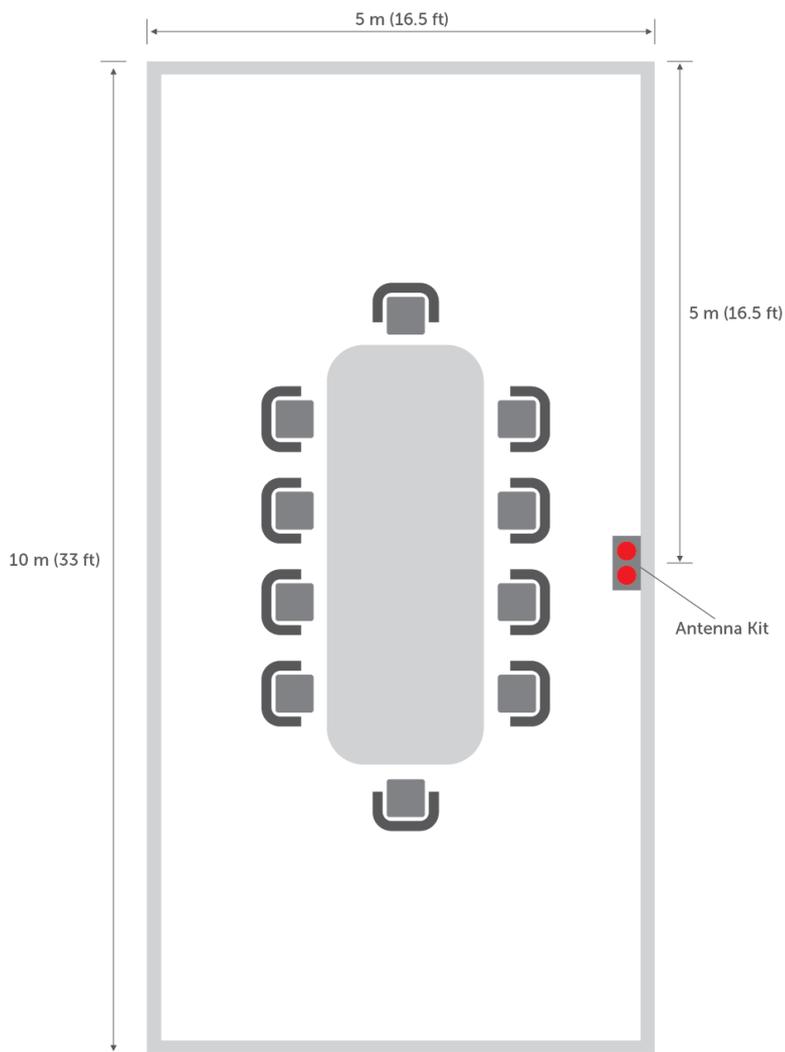


Figure: Example of antennas installed in a meeting room

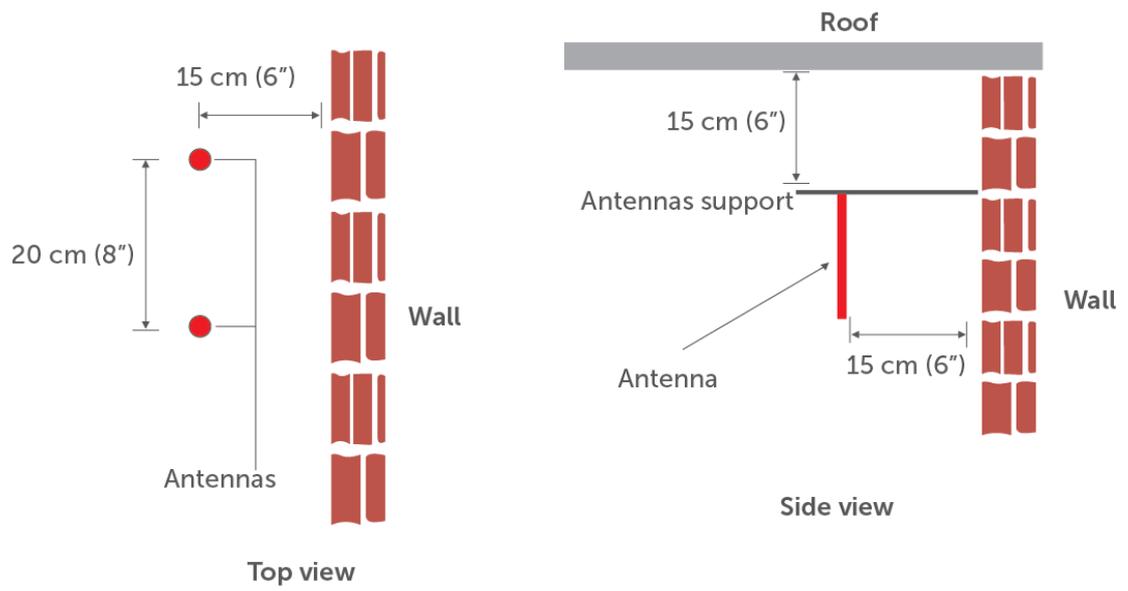


Figure: Closer view of antennas installed in the meeting room

Troubleshooting the ClickShare setup

In this section, you can find some of the most frequently occurring issues and a brief description of their solutions.

The Button is unable to connect via the corporate network

Causes	Solutions
The credentials set for network integration are incorrect and do not match the settings of the nearest Wi-Fi access point.	<p>Verify the credentials and reconfigure the network integration following the steps described in Setting a Security Mode using the Network Integration wizard</p> <p>Repair the Buttons after reconfiguring the network integration.</p> <p>Check whether the Button is connecting to your access point by verifying its presence in the MAC address table. The Button has a MAC address starting with 00:23:A7 or 88:DA:1A.</p>
The Button is unable to find the Base Unit on the corporate network.	<p>Verify that the Base Unit is announced by its hostname and that its IP address can be resolved.</p> <p>If you want to set a fixed IP address for the Base Unit, it is recommended to use a DHCP entry mapping the MAC address of the Base Unit to the IP address.</p>
When ClickShare is integrated in a network using the WPA2-PSK security mode, the Buttons can be unable to connect to an access point using a WPA/WPA2 mixed security mode.	Change the access points' security mode to WPA2 only .

Sharing using the ClickShare App, Airplay, and/or Google Cast is not working

Causes	Solutions
<p>The corporate network does not support traffic over a set of ports required for network integration.</p> <p>or</p> <p>The Base Unit is not in the same network as the device you are sharing with.</p>	<p>Check whether the ports as in Recommendations for network integration > Firewall are open for traffic in your corporate network to use the ClickShare App, Airplay, and/or Google Cast.</p> <p>It is recommended to put the Base Unit in the same network as the Buttons and mobile devices.</p> <p>An example: Bonjour discovery (required for Airplay) requires the devices to be visible in the same subnet. If the Base Unit is not in the same network as the mobile device, try to provide a bridge from one network to the other.</p> <p>For discovery of these services, multicasting must be enabled on your network.</p>

The Button disconnects while sharing

Causes	Solutions
<p>The distance between Button and the Base Unit is too large</p> <p>or</p> <p>The Button is unable to connect to the nearest Wi-Fi access point.</p>	<p>Check if the Base Unit is still accessible on your network. The IP address of the Unit should be displayed on the wallpaper on your screen.</p> <p>Check if the Base Unit's hostname is resolvable. Make sure pinging the Base Unit's hostname is successful.</p> <p>Verify whether the Button is able to connect to the access point by checking the Button log and reviewing the access point log.</p>
<p>There is interference between the access points in your Enterprise network, blocking a good usage of the Wi-Fi signal by the Button and other peripherals.</p>	<p>Make sure that your access point is configured in a separate channel that is different from the surrounding access points.</p> <p>It is recommended to do a Wi-Fi spectrum analysis and plan assigned channels for each access point accordingly.</p>
<p>During sharing, the ClickShare Button needs to switch between different access points as the most frequently access point varies while walking around.</p>	<p>The ClickShare Button does not support roaming between different access points.</p> <p>It is recommended to do a Wi-Fi spectrum analysis and plan Wi-Fi strength accordingly to ensure that Buttons do not need to switch between access points while sharing.</p> <p>If this is not an option within your Enterprise network and the ClickShare Buttons frequently switch between different access points which are close by, choose the out-of-the box mode to allow sharing within a meeting room.</p> <p>Limit the signal strength of the Base Unit's internal Wi-Fi and hence limit interference with other access points in the ClickShare Configurator.</p>
<p>The access point is changing channels dynamically to cope with interfering signals within your Enterprise network.</p>	<p>The Button does not support channel hopping or DFS channels. Review the close-by access points and force them to use a non-DFS and static channel.</p>

The Base Unit does not accept the corporate network certificates

Cause	Solution
<p>In some cases, the certificates uploaded on the Base Unit do not work as expected because the upload procedure fails, the connection is impossible or sometimes drops.</p>	<p>Check whether the ports as in Recommendations for network integration > Firewall are open for traffic in your corporate network to use the ClickShare App, Airplay, and/or Google Cast.</p> <p>It is recommended to put the Base Unit in the same network as the Buttons and mobile devices and.</p> <p>An example: Bonjour discovery (required for Airplay) requires the devices to be visible in the same subnet. If the Base Unit is not in the same network as the mobile device, try to provide a bridge from one network to the other.</p> <p>For discovery of these services, multicasting must be enabled on your network.</p>

The sharing quality drops when enabling network integration mode

Cause	Solution
<p>The wireless signal from the access point to the Button could be limited.</p> <p>or</p> <p>The available bandwidth on the network is limited by other traffic or network configuration.</p>	<p>Check if the distance between the Button and wireless access point is not too large and whether the signal is optimal.</p> <p>Review the traffic on the network and try to reduce the amount of bandwidth used.</p> <p>Note that the communication between the Base Unit and Button requires an available link with a data rate between 7 and 10 Mbps. If that is not possible, review the setup and either revert to the out-of-the-box mode or setup a separate (V)LAN.</p>

Troubleshooting the wireless setup

As the frequencies used by ClickShare are shared with other wireless systems (Wi-Fi, Bluetooth ...), interferences may occur and can cause connection or disconnection issues. If this type of issue occurs, it is recommended to check the following:

Check the RSSI from the connected clients

Even if the selected channel is free of any interference, a weak signal coming from the ClickShare client (Buttons or mobile devices) can result in an unstable link. In such cases:

- Measure the RSSI from the ClickShare Base Unit at various Button locations, by means of a free Wi-Fi survey tool. The RSSI should be at least -70dBm. See also: [Recommendations for Wi-Fi configuration](#).
- Check the signal state reported on the ClickShare Base Unit CGMS in the tab Maintenance > Buttons. If you see the message: "Intense use, change to another Wi-Fi channel", select another channel.

If the measured RSSI is too low, also refer to: [Important notes on the ClickShare system installation](#)

Measure the interference level

The easiest way to measure the interference level is to use a Wi-Fi survey tool. Most of these tools provide a measure of the channel usage. A high channel occupancy can cause a lot of packet collisions and retransmissions. In some extreme cases, it can lead to disconnection. If this is the case, change the Wi-Fi channel used by ClickShare.

See also: [Recommendations for Wi-Fi configuration](#)

Effect of unauthorized rogue access point

Some advanced corporate WLAN infrastructures use specific algorithms to detect and to neutralize unauthorized rogue access points. If such systems are not configured correctly, they will wrongly identify the ClickShare Base Unit as an unauthorized Wi-Fi access point and will cause an unwanted disconnection from ClickShare. To avoid this, ensure that you add the MAC address of the ClickShare Base Unit Wi-Fi access point to the list of authorized access points maintained by the central corporate Wi-Fi controller (**whitelisting**). The Base Unit MAC addresses start with **00:04:A5** on the LAN ports.

See also: [Recommendations for Wi-Fi configuration](#)

Troubleshooting for support

If you are experiencing problems with your ClickShare setup:

- Consult the section: [Check the Button connection](#).
- If this does not resolve the issue, create a report containing:
 - Detailed information on the Enterprise environment in which ClickShare operates
 - A description of the problem

With this report, contact your installer or reseller for support, or contact the Barco helpdesk.

Check the Button connection

The ClickShare Button receives connection details for connecting to your corporate network via USB pairing. Verify these details:

- Make sure the Base Unit is configured properly, as described in the ClickShare Installation Manual
- Pair the Button(s) with the Base Unit again, either by plugging them into the Base Unit's USB port¹⁵ or by making use of the ClickShare Button Manager for Windows, which allows to simultaneously pair up to four buttons from a pc/laptop.

When the ClickShare Button is connected to the corporate network it tries to find the ClickShare Base Unit via the Base Unit **hostname**. If the DNS server does not know the hostname of the Base Unit or there is no DNS server present, the Button will use a fallback mechanism to connect to the Wired IP of the Base Unit it had during USB pairing.

- Make sure the Button can resolve the Base Unit's hostname.
- If the Base Unit is not findable by hostname, make sure the ClickShare Base Unit does not change IP addresses. To this end, reserve a DHCP address or define a fixed IP address.

Gathering in-depth network and system information

To be able to help you resolve the issue, collect the information mentioned in the following steps. This will help to fully diagnose your problem.

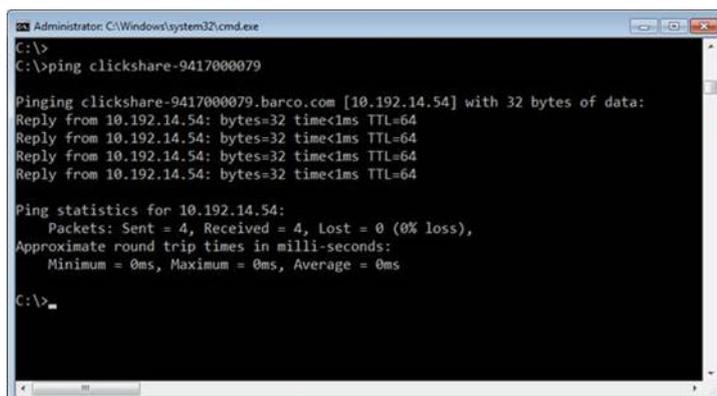
- Contact your IT department and ask them to answer the following questions:
 - Is there a DNS server in the network?
 - Is there a DHCP server in the network?
 - What is the DHCP lease length?
 - What is the protocol used to connect to the Corporate Wi-Fi: WPA2-PSK, PEAP, EAP-TLS, EAP-TTLS?
 - Can you see the Buttons requesting and failing to join the Network, on the Network Policy Server or equivalent RADIUS / AAA Server?

¹⁵ The Clickshare CS(E)-range ships with a number of USB-A buttons in the box, that can be paired directly to a Base Unit by plugging them into the USB-A port on the front panel or one of the USB-A ports on the back. Moreover, both USB-A and USB-C Buttons can be obtained separately. USB-C Buttons can be paired directly by making use of a USB-C/USB-A adaptor or with the Button Manager. The CSE-200+ has one USB-C port on the back which can be used for direct pairing of USB-C buttons.

- Can you see the Buttons requesting an IP address, and can the button reach the Base Unit from that IP address?
- Provide a full description of the problem.
- Explain the steps needed to reproduce the problem.
- Add some pictures or a video to explain further

To gather in-depth information on your ClickShare installation:

1. Enable debug logging on the Base Unit as described in [Troubleshooting for debug logs](#).
2. Capture some logs from the ClickShare client trying to connect to the Base Unit.
 - Insert the ClickShare **Button** into your computer.
 - Start **ClickShare_for_Windows** (or for Mac) with shift pressed to start logging and let the ClickShare client connect for 3 minutes.
 - Retrieve the **log files** as described in [Troubleshooting for debug logs](#).
 - **Compress** them into a zip archive and add them to the report you are creating.
3. **Ping** the hostname of the Base Unit and take a print screen of the ping process.



```
Administrator: C:\Windows\system32\cmd.exe
C:\>
C:\>ping clickshare-9417000079

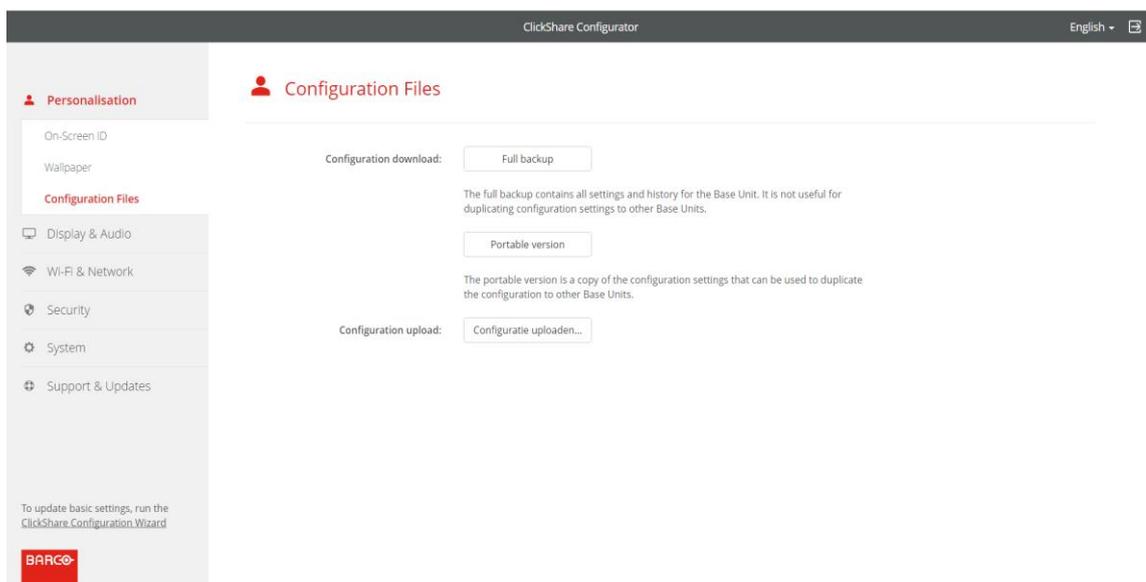
Pinging clickshare-9417000079.barco.com [10.192.14.54] with 32 bytes of data:
Reply from 10.192.14.54: bytes=32 time<1ms TTL=64

Ping statistics for 10.192.14.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

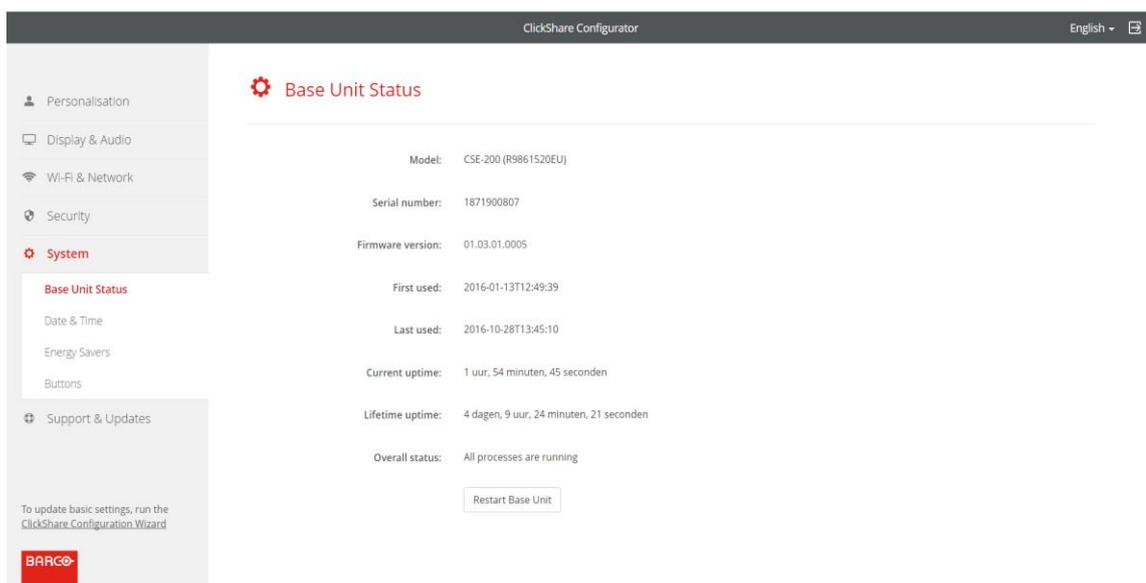
Screenshot ping process

4. Retrieve the configuration file from the Base Unit in the **ClickShare Configurator**. Download this configuration file by clicking the **Personalization / Configuration Files** tab and then clicking **Full Backup**.



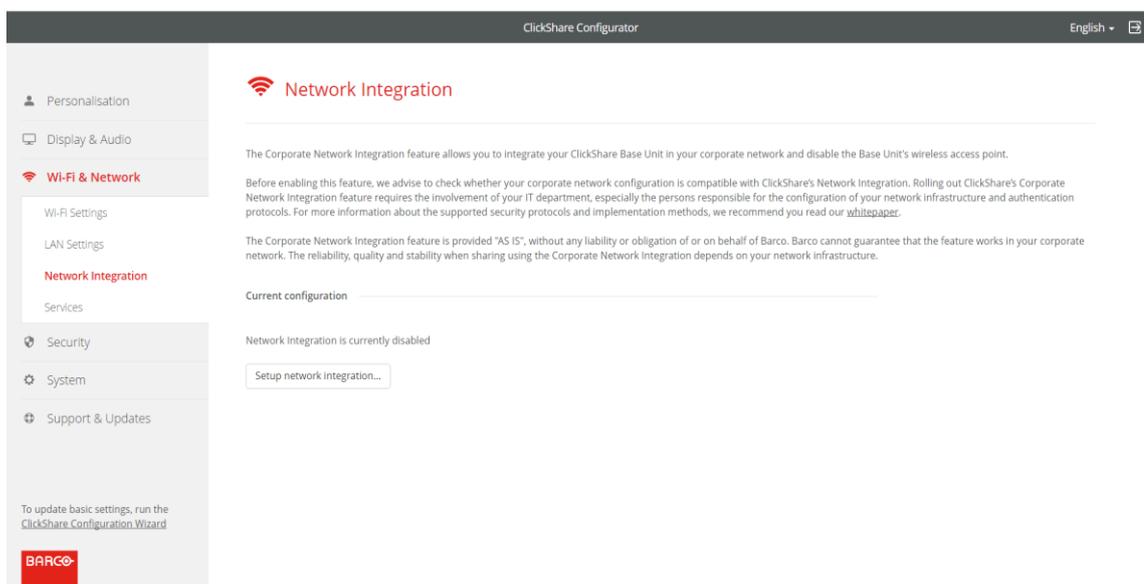
Screenshot on how to download a full backup of the Base Unit

5. Go the **System>Base Unit Status** tab and take a print screen of the Base Unit status page.



Screenshot of Base Unit status page

6. Go to the **Wi-Fi & Network>Network Integration** tab and take a print screen of **Network Integration** page.



Screenshot of the Base Unit Corporate Network configuration page

7. Get debug logs for the ClickShare Base Unit when trying to connect to the Base Unit with a Button. See also: Troubleshooting for debug logs.

Troubleshooting for debug logs

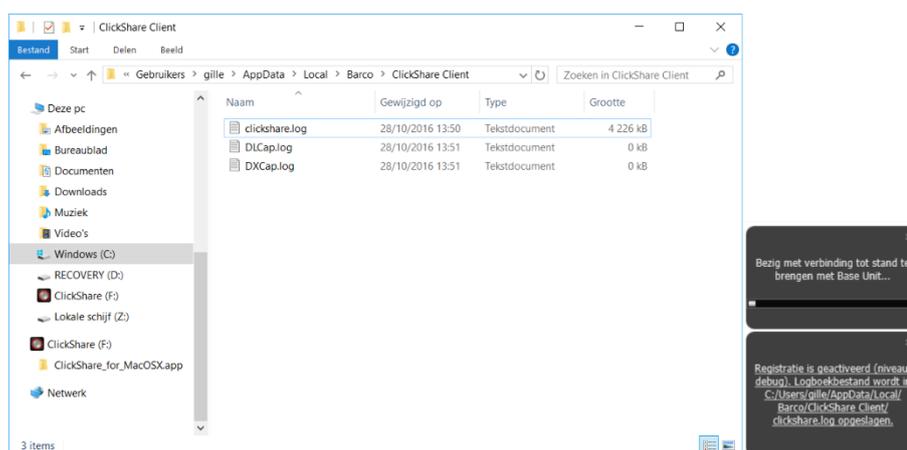
If the ClickShare Button cannot connect to your corporate network, there are several potential root causes for this. These include, but are not limited to: incorrect SSID, SSID not available, incorrect EAP Identity/Password, firewall settings, VLAN configuration ...

ClickShare Client log (Button log)

The ClickShare Client log contains all information from the Button when it is trying to connect to your corporate network.

To generate this log:

1. Press and hold the Shift-key when starting the **Client.exe** (ClickShare_for_Windows or for Mac).
2. Click the **logging pop up** to open the logging directory as shown in the following screenshot, to find the recorded log files.



Screenshot - logging pop up

3. In the log file, look for lines such as **EDSUSBDongleConnection::mpParseDongleMessages**. An error code and a short summary of the issue should be logged.

An example:

```
EDSUSBDongleConnection::mpParseDongleMessages - error message Selected interface
'wlan0';bssid=00:0e:8e:3a:a8:efssid=ClickShare-CorporateCSC-
1;id=0;mode=station;pairwise_cipher=CCMP;group_cipher=CCMP;key_mgmt=WPA2-
PSK;wpa_state=COMPLETED;ip_address=192.168.2.2;address=00:23:a7:3a:17:bd;#012
```

To check if a Button can reach the Base Unit:

1. **Connect** a pc to the Base Unit in the same way you would connect a Button to it, using the same user name, password, certificates, etc.
2. **Ping** the Base Unit's hostname. You can find the hostname in the Based Unit's ClickShare Configurator.
3. If the ping fails, try **pinging the IP address** and adjust your network setup to enable pinging the hostname.

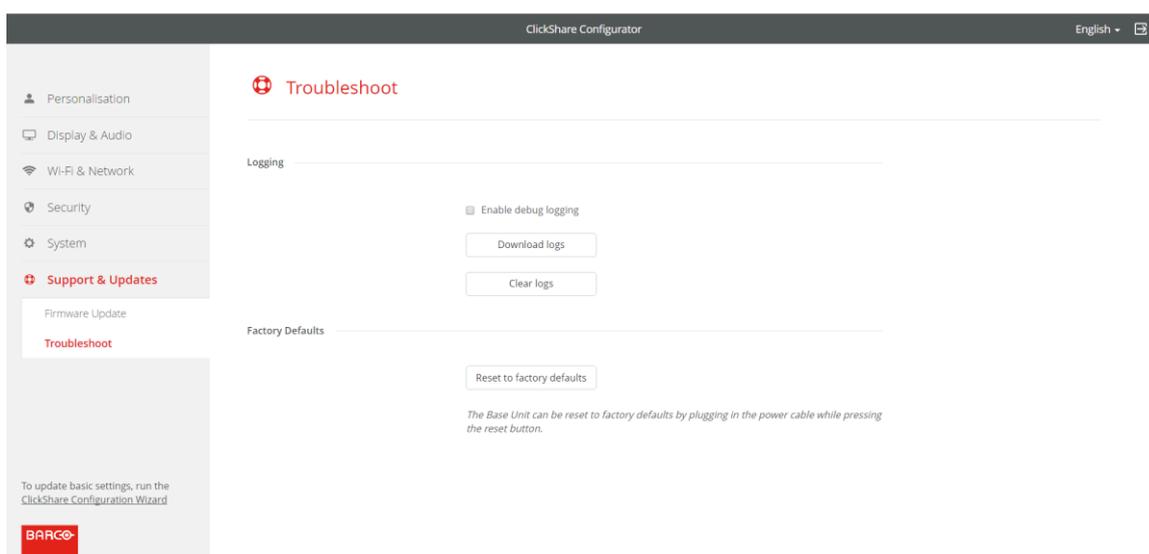
Key messages

We strongly recommend reserving dedicated IP addresses in your DHCP server for each Base Unit. This will prevent issues when the hostname is not resolvable.

Base Unit debug log

To locate Base Unit debug log:

1. In the **ClickShare Configurator** go to the **Support & Updates>Troubleshoot** tab.
2. To capture all system logging information, click the **Enable debug logging** option as shown in the following screenshot.



Screenshot on where to retrieve Base Unit debug logs

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 Message 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 Enrollment 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