

White Paper

ClickShare Network Deployment Guide

Authors:

Adrien Descotre, Jef Neefs,
Gilles Bonne, Michael Vanderheeren

BARCO

Visibly yours

Table of Contents

1.	Introduction	3
2.	Available network modes	4
3.	ClickShare Setup in your network	5
3.1.	Overview	5
3.2.	Stand-alone mode	6
3.3.	Network integration in the corporate network	7
3.4.	Network integration in dedicated network	9
3.5.	Network integration routing Enterprise network traffic in dedicated network	11
3.6.	Configure Network integration	13
4.	Troubleshooting	23
4.1.	Top problems & solutions	23
4.2.	Support	25
4.3.	How to retrieve debug logs	29
5.	Acronyms	31
6.	Disclaimer	32

1. Introduction

ClickShare (CS) is Barco's wireless presentation and collaboration system that makes sharing content on the central meeting room screen for any meeting participant only a matter of clicking a button. With the ClickShare's universal USB-powered Button and ClickShare App this avoids the unsightly jumble of cables often seen in meeting rooms. On top, connecting ClickShare does not alter your screen size or resolution, so what you see on your laptop screen is replicated on the big meeting room screen. In this way ClickShare transforms a meeting into a complete sharing experience with a single click.

The ClickShare CSE-range furthermore has a specific set of features to facilitate the deployment in Enterprise environments including full support for bring your own device (BYOD) users via Airplay and Google Cast. Next to that, the Units have Enterprise-strength security configurable with up to three levels, can be controlled via a browser-based central asset management system and can be fully integrated into your corporate network. They also offer a comprehensive API for integration with other applications.

In order to get the most out of your ClickShare, this guide helps you in deploying your Units in your Enterprise network by providing you an overview of the different deployment models and how to perform the setup and installation. Typically, this configuration is performed once, before use, and does not require any further modifications after installation.

2. Available network modes

The ClickShare Base Units can be configured to operate in different modes depending on the desired integration level in the Enterprise network. These different modes are described here.

Stand-alone mode

This is the default mode where the Unit operates directly out of the box and does not require any integration with the Enterprise network. In this configuration ClickShare functions as a stand-alone wireless access point (WAP) where users can directly connect to it via ClickShare Buttons or mobile devices in order to share media with the in-room display(s) and collaborate. This mode does not rule out the central asset management functionality. The Base Unit can still be connected to the Enterprise network via an Ethernet link for management by the ClickShare Management Suite (CMGS) and/or auto-update functionality. Detailed information on the usage of this mode is described in our “ClickShare recommendations for Wi-Fi configuration” Whitepaper.

Network integration mode

In this mode, the ClickShare Units operate completely via an existing network which can be the corporate network, a guest network, or a separate (virtual) LAN. This implies that the Base Unit’s WAP functionality is disabled and all traffic from the buttons travels via the Enterprise network to the Base Unit. In this integrated configuration, anyone who has access to the network wherein the ClickShare resides, can directly share and collaborate without changing network. In addition, mobile devices can concurrently use the corporate network and internet access while presenting on screen.

This mode is used in the following network deployment models:

- Enterprise network
- Dedicated network
- Routing into dedicated network

Depending on the network mode used to integrate the ClickShare Base Unit (BU) within your network Buttons, Apps, and other sharing services will connect in a different way. Table 1 gives a more detailed overview on the different connections.

Table 1: ClickShare available network modes

Connection	Stand-alone mode	Network integration mode
Base Unit Ethernet	Only for management purposes (CMGS)	Connected to corporate network as Client
Base Unit Wireless	Access point for Buttons and Clients	Disabled
Buttons sharing via	Via BU Wireless	Via Corporate Network Access Point
Clients (Apps) sharing via	Via BU Wireless	Via Corporate Network Access Point
Airplay / Google Cast	Via BU Wireless	Via Corporate Network Access Point
API / Management	Via BU Ethernet	Via BU Ethernet

3. ClickShare Setup in your network

This section describes the different ClickShare network integration configurations in more detail, covering what they are about, for which scenarios they are intended, and how to configure each deployment model.

3.1. Overview

Table 2 gives a brief overview of the different deployment models of ClickShare in your Enterprise network as elaborated in sections 3.2 to 3.5. A summary of the different connections used in the two different ClickShare network modes can be seen in Table 1.

Table 2: Overview of the different deployment models of ClickShare

	Deployment Model	Network Configuration	Business Scenario
Stand-alone mode	Stand-Alone	The ClickShare Base Unit does not have to be connected to a network and acts as a stand-alone WAP. Users can share using the Button or by connecting with their mobile device to the Base Unit Wi-Fi. This configuration does not rule out the ClickShare Management Suite (CMGS) functionality.	• Temporary setups • Visitors centers • Small to medium installations • With there are no network integration requirements or capabilities
Network integration mode	Enterprise Network	The ClickShare Base Unit is integrated in either the existing Enterprise or guest network using the Ethernet or Wireless controller. Anyone connected to the Enterprise or guest network can share.	• Large Enterprise installations • Where a single Enterprise network is used for all devices • Sharing from other networks is not required • Limiting the amount of WAP polluting the Wi-Fi space
	Dedicated Network	The ClickShare Base Unit resides in a separate physical or virtual LAN. Anyone who wants to share is required to join the dedicated wireless (V)LAN.	• E.g. Banks, Government, Defense Industry, ... • Large Enterprise installations • Where no physical or virtual access to an existing network is for security reasons • A connection to an existing network is not required/wanted
	Routing Enterprise Network traffic into Dedicated Network	The ClickShare Base Unit resides in a separate physical or virtual LAN. Anyone who wants to share is required to join the dedicated wireless (V)LAN. A network bridge is provided between the Enterprise and guest network into the ClickShare network to facilitate sharing from those networks.	• Large Enterprise installations • Where a dedicated network is preferred for the ClickShare Base Units • Sharing from an Enterprise or guest network is a requirement • Providing flexibility and reduce friction when sharing from mobile devices • Limiting the amount of WAP polluting the Wi-Fi space

3.2. Stand-alone mode

This is the default mode where the Unit operates directly out of the box and the ClickShare Base Unit functions as a stand-alone WAP and is not connected to a network. Both corporate users and guests can directly share via the Button or by connecting with their mobile device directly to the Base Unit Wi-Fi. Note that using a Button allows you to remain with your device connected to your existing network so you still have internet access. Devices which have the capability of using both Wi-Fi and 3G/4G at the same time can still access internet while sharing.

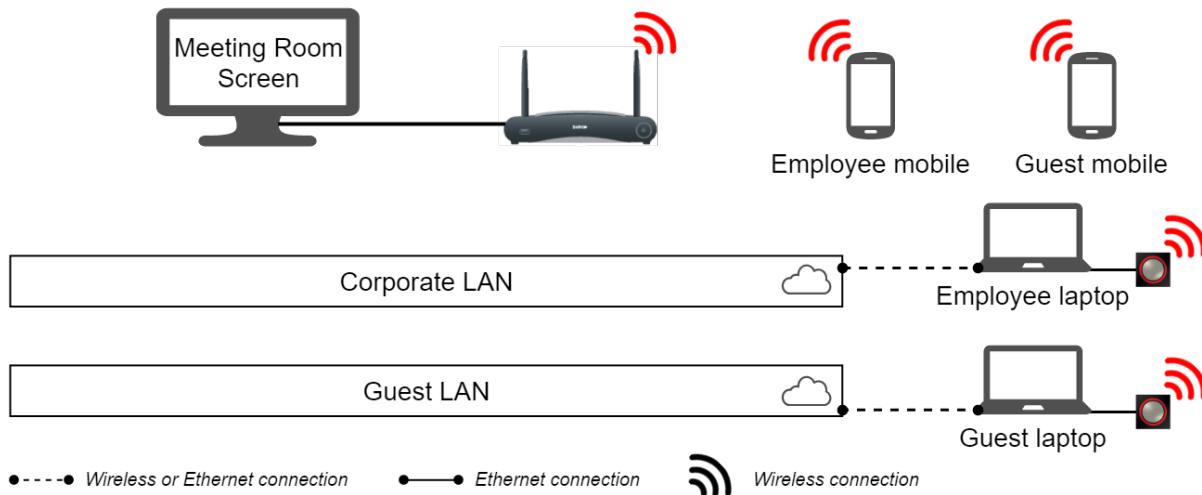


Figure 1: Stand-alone mode network topology diagram

Business scenario

The stand-alone mode is typically used in environments where there are no network integration requirements or capabilities present. This setup is often found in temporary setups, visitor centers, small to medium installations. In this configuration, ClickShare does not require any interaction with the Enterprise network. This allows to clearly separate the sharing traffic from the Enterprise network and requires the least installation effort.

Setup

By default, the ClickShare Units are configured in this mode.

To revert to this mode on the Base Unit without CMGS:

1. Connect with the Base Unit, browse to the CS Configurator WebUI and log in
2. Open the “Network integration” tab as shown in Figure 5 on page 13, and click on “Change configuration” to select the stand-alone mode
3. Pair the Buttons again with the Base Unit to effectuate the new configuration

Detailed steps on how to open the CS Configurator WebUI are described in the Installation Manual.

To activate this mode on the Base Unit with CMGS:

1. Log in on the ClickShare Management Suite and go to the “Base Units” tab
2. Within the device list select the Units to set in stand-alone mode
3. Click via the Configure dropdown list on “Network integration”
4. Select “disable” for stand-alone mode and follow the next steps of the wizard
5. Pair the Buttons again with the Base Units to effectuate the new configuration

Detailed steps on how to use the CMGS are described in the CMGS User Guide.

3.3. Network integration in the corporate network

In this configuration, the ClickShare Base Unit is connected to the corporate or guest network via an Ethernet link and its wireless access point function is disabled. Both corporate users and guests share directly via the Button or when connected with their mobile device in the same Enterprise network. Note that in this scenario the Buttons are also connected to the chosen Enterprise LAN and all sharing traffic travels through the LAN to the Base Unit.

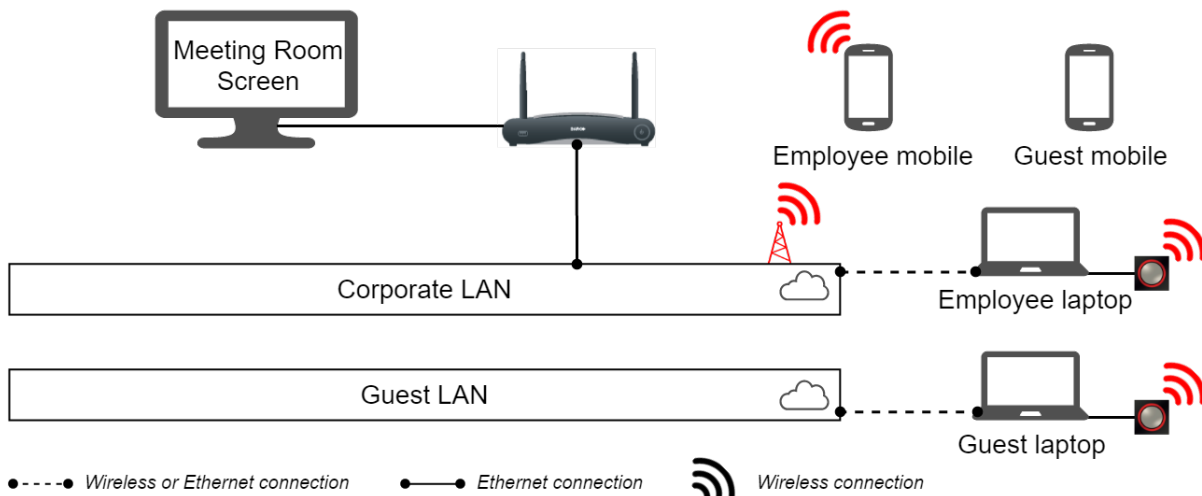


Figure 2: Network integration in Enterprise network topology diagram, as example the Corporate LAN is used.

Business scenario

The network integration in the Enterprise network is typically used in contexts where there is a desire to integrate the ClickShare Units in one network, because a single network is used for all devices or sharing from other networks is not required. Often this setup is preferred in large Enterprise installations.

Using this deployment model allows you to reduce the amount of Wi-Fi access points in order to control the Wi-Fi spectrum and associated security threats. Further, for the ease of installation in your Enterprise network you can choose to integrate ClickShare in one of your existing networks. This enables users with their mobile devices to remain on the same Enterprise network while being able to share via ClickShare. When using a Button, you can always remain with your device connected to your existing network so you still have internet access.

Setup

In order to configure your devices for integration in the Enterprise network, you need to have all the access rights and credentials to allow the ClickShare Base Units and Buttons on it. Also, check the capacity of the network with the IT responsible to guarantee the optimal ClickShare experience.

To activate this mode on the Base Unit without CMGS

1. Connect with the Base Unit, browse to the CS Configurator WebUI and log in
2. Open the "Network integration" tab as shown in Figure 5 on page 13, click on "Change configuration", and follow the wizard to select network integration mode
3. Pair the Buttons again with the Base Unit to effectuate the new configuration

Detailed steps on how to open the CS Configurator WebUI are described in the Installation manual.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

To activate this mode on the Base Unit with CMGS

1. Log in on the ClickShare Management Suite and go to the “Base Units” tab
2. Within the device list select the Units to set in network integration mode
3. Click via the Configure dropdown list on “Network integration”
4. Select one of the security modes for network integration mode and follow the next steps of the wizard
5. Pair the Buttons again with the changed Base Units to effectuate the new configuration

Detailed steps on how to use the CMGS are described in the CMGS User Guide.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

3.4. Network integration in dedicated network

In this configuration, the ClickShare Base Unit is connected to a dedicated physical or virtual LAN via an Ethernet link and its wireless access point function is disabled. Both corporate users and guests share directly via the Button or by connecting their mobile device to the dedicated LAN. Note that in this scenario the Buttons are also connected to the dedicated LAN and all sharing traffic travels through the LAN to the Base Unit. When using a Button, you can remain with your device connected to your existing network so you still have internet access.

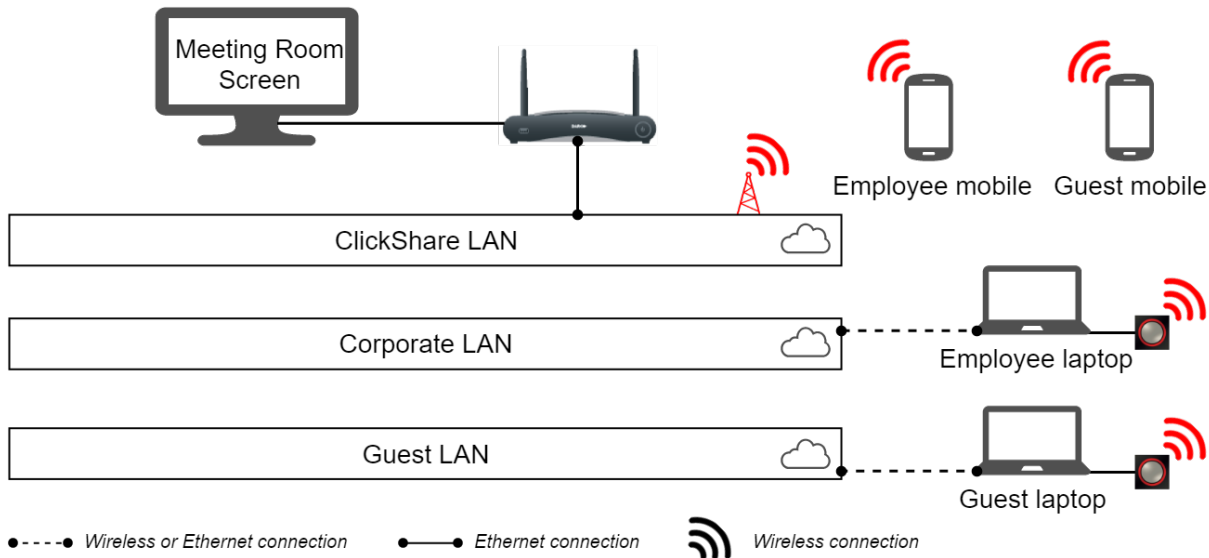


Figure 3: Network integration in dedicated network topology diagram

Business scenario

Integrating ClickShare into a dedicated network is typically used in settings where there is a desire to integrate the ClickShare Units but where a connection to an existing network is not required/wanted. Often this setup is preferred in large Enterprise installations and where security constraints are higher, such as in: Banks, Defense industry, Government.

This deployment model allows you to reduce the amount of Wi-Fi access points in order to control the Wi-Fi spectrum and associated security threats. Furthermore, by isolating all Base Units in one separate (virtual) LAN you eliminate completely the possibility of having security risks via ClickShare in your Enterprise Network. Grouping all ClickShare Units in one separate LAN also facilitates the management of them, e.g. their assigned IP addresses.

Setup

In order to configure your devices in network integration mode in a dedicated network, you need to have the dedicated network available and have all the access rights and credentials to allow the ClickShare Base Units and Buttons on it. Note that the corporate wireless access points from which you want to share to a ClickShare Base Unit must also be connected to the dedicated ClickShare LAN. Also check the capacity of the network with the IT responsible to guarantee the optimal ClickShare experience.

To activate this mode on the Base Unit without CMGS

1. Connect with the Base Unit, browse to the CS Configurator WebUI and log in
2. Open the "Network integration" tab as shown in Figure 5 on page 13, click on "Change configuration", and follow the wizard to select network integration mode
3. Pair the Buttons again with the Base Unit to effectuate the new configuration

Detailed steps on how to open the CS Configurator WebUI are described in the Installation manual.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

To activate this mode on the Base Unit with CMGS

1. Log in on the ClickShare Management Suite and go to the “Base Units” tab
2. Within the device list select the Units to set in network integration mode
3. Click via the Configure dropdown list on “Network integration”
4. Select one of the security modes for network integration mode and follow the next steps of the wizard
5. Pair the Buttons again with the changed Base Units to effectuate the new configuration

Detailed steps on how to use the CMGS are described in the CMGS User Guide.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

3.5. Network integration routing Enterprise network traffic in dedicated network

In this configuration, the ClickShare Base Unit is connected to a dedicated physical or virtual LAN via an Ethernet link and its wireless access point function is disabled. Both corporate users and guests share directly via the Button or when connected with their mobile device to the dedicated LAN or Enterprise network. Note that in this scenario the Buttons are also connected to the dedicated LAN and all sharing traffic travels through the LAN to the Base Unit. When sharing, all users can remain with their device connected to their existing network so they still have all the needed corporate and internet access.

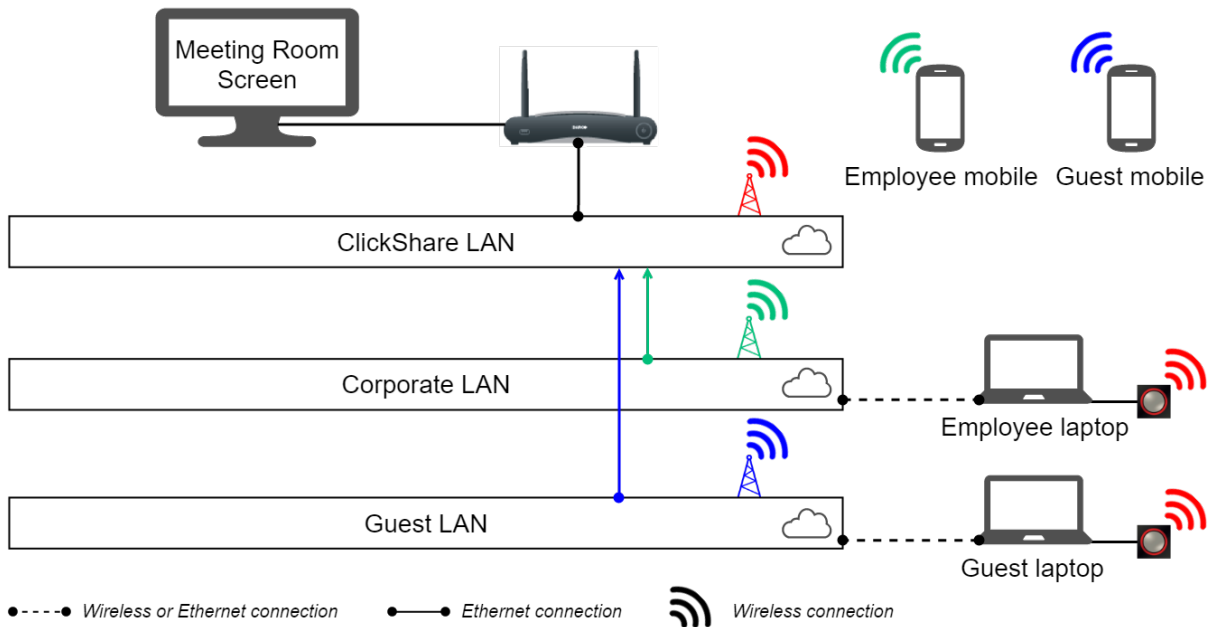


Figure 4: Network integration in dedicated network with routed Enterprise network topology diagram

Business scenario

The network integration with routing Enterprise traffic to a dedicated network is typically used in environments where there is a desire to integrate the ClickShare Units in one separate network with the requirement of being able to share directly from an Enterprise or guest network. Often this setup is preferred in large Enterprise installations.

Using this deployment model allows you to reduce the amount of Wi-Fi access points in order to control the Wi-Fi spectrum and associated security threats. Grouping all ClickShare Units in one separate LAN also facilitates the management of them, e.g. their assigned IP addresses. Furthermore, by isolating all Base Units in one separate (virtual) LAN you reduce¹ the possibility of having security risks via ClickShare in your Enterprise Network. In addition, for sharing you can still allow mobile users to remain connected to their current network with all related corporate and internet accessibility by routing Enterprise network traffic in the dedicated ClickShare network.

Setup

In order to configure your devices in this network integration mode, you need to have the dedicated network available and have all the access rights and credentials to allow the ClickShare Base Units and Buttons to connect and share. Furthermore, you need to have installed all the needed routing paths from the desired Enterprise networks into the dedicated LAN. Also check the capacity of the network with the IT responsible to guarantee the optimal ClickShare experience.

¹ The remaining security risks are only associated with the opened ports to route traffic between the dedicated LAN and the other Enterprise network(s). Table 3 on page 14 lists for which services what ports need to be opened between the networks.

To activate this mode on the Base Unit without CMGS

1. Connect with the Base Unit, browse to the CS Configurator WebUI and log in
2. Open the “Network integration” tab as shown in Figure 5 on page 13, click on “Change configuration”, and follow the wizard to select network integration mode
3. Pair the Buttons again with the Base Unit to effectuate the new configuration

Detailed steps on how to open the CS Configurator WebUI are described in the Installation manual.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

To activate this mode on the Base Unit with CMGS

1. Log in on the ClickShare Management Suite and go to the “Base Units” tab
2. Within the device list select the Units to set in network integration mode
3. Click via the Configure dropdown list on “Network integration”
4. Select one of the security modes for network integration mode and follow the next steps of the wizard
5. Pair the Buttons again with the changed Base Units to effectuate the new configuration

Detailed steps on how to use the CMGS are described in the CMGS User Guide.

The specifics on how to configure Network integration are listed in 3.6 Configure Network integration on page 13.

3.6. Configure Network integration

This section discusses the different aspects of configuring ClickShare for integration into the network in more detail. You will encounter these items in the network integration setup while following the wizard on the ClickShare Configurator WebUI or ClickShare Management Suite.

When you choose to integrate the ClickShare system into your corporate network, there are a few things to consider up front. Therefore, go first thoroughly through 0 Prerequisites.

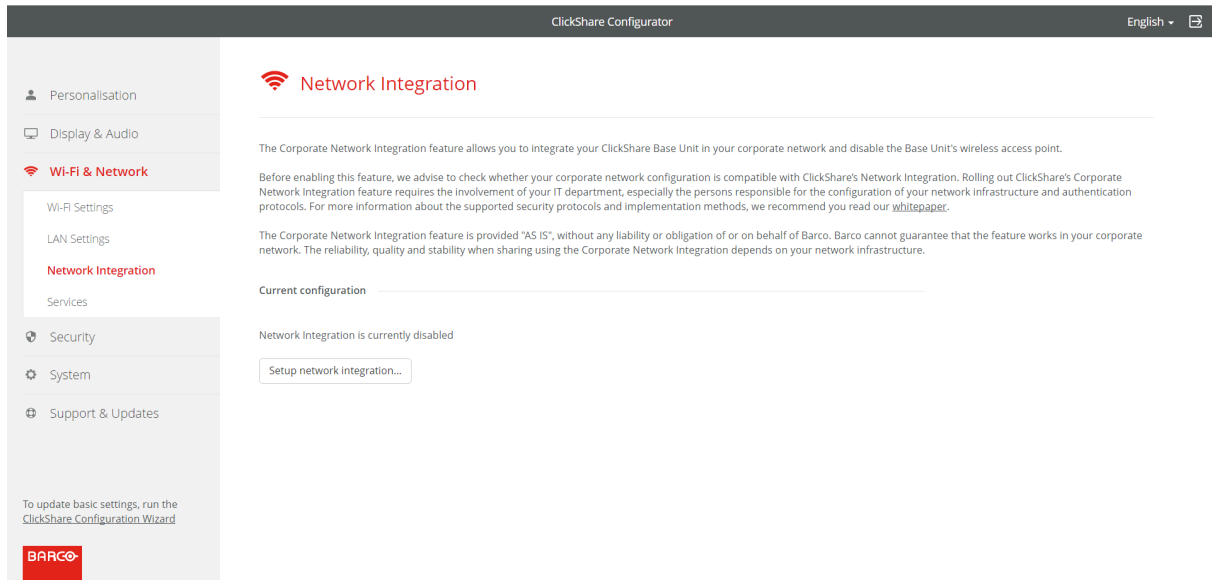


Figure 5: ClickShare Configurator WebUI Network integration page

Prerequisites

Before enabling network integration, we advise to check whether your corporate network configuration is compatible with ClickShare's Network integration. Deploying a ClickShare Base Unit within the network requires the involvement of your IT department, especially the persons responsible for the configuration of your network infrastructure and authentication protocols.

Network

First of all, make sure that all your Base Units can be connected to your network via the wired Ethernet interface². Once you enable the network integration, the internal Wi-Fi access point of the ClickShare Base Unit will be disabled from the moment you pair the first Button with it. The assigned IP-address to the Base Unit will be displayed on its wallpaper.

For normal operation of Buttons in network integration mode, the corporate wireless access points need to support the IEEE 802.11d standard. Further, the Buttons only can connect with Wi-Fi channels 1 to 13 in the 2.4 GHz band and channels 36 to 48 and 139 to 165 in the 5 GHz band, depending on the Base Unit's location specific restrictions. As of this writing, Buttons do not support roaming and dynamic channel assignment or DFS channels.

Also, take into account the amount of bandwidth that each Button needs to stream the captured content to the Base Unit –When presenting static content this is usually close to 2 Mbps. For optimal video performance, we advise to account for a data rate between **7 and 10 Mbps**. So, prevent bottlenecks in your network (e.g. 100 Mbps switches) that could potentially degrade your ClickShare experience due to a lack of bandwidth. Further, note that Buttons only use 20 MHz channel bands.

² On the ClickShare CSE-800, network integration is currently only supported via the primary Ethernet interface. The secondary Ethernet interface can be used to connect with the ClickShare Management Suite or control via the ClickShare API.

Airplay and Google cast, as well as the ClickShare App require multicast to make the ClickShare Base Unit discoverable within your network. Therefore, allowing multicast within the network is required to use Airplay and Google Cast. The Base Unit should be connected in the same subnet as the mobile device or a network connection should be available from the mobile device to the Base Unit.

Both Airplay and Google Cast are a proprietary protocol which does not allow filtering or sorting of the list of Base Units. In case your Enterprise network contains more than 10 Base Units we recommend to use a structured meeting room name. E.g. "Building A – Floor 2 – Meeting Room Rome" allowing users to quickly find the correct meeting room in a large list.

Firewall

Depending on the services you wish to use, you ensure that you can successfully share content via the ClickShare Button, or from mobile devices, to the Base Unit, by opening the following ports on your network:

Table 3: Network integration - required ports

Sender		CSE-200	CSC-1	CSM-1
ClickShare Button	TCP	6541-6545	9870; 9876	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	514	514	1047-1049; 9870
ClickShare Presenter	TCP	6541-6545	389; 445; 515; 636; 1688; 1689; 3268; 8080	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	5353	1047-1049; 9870	1047-1049; 9870
ClickShare Configurator WebUI	TCP	80; 443	80; 443	80; 443
	UDP			
ClickShare REST API	TCP	4000; 4001	4000; 4001	4000; 4001
	UDP			
Airplay	TCP	4100-4200; 7000; 7100; 47000	4100-4200; 7000; 7100; 47000	4100-4200; 7000; 7100; 47000
	UDP	4100-4200; 5353	4100-4200; 5353	4100-4200; 5353
Google Cast	TCP	8008; 8009; 9080	N/A	N/A
	UDP	1900; 5353; 32768:61000 ³	N/A	N/A
MirrorOp	TCP	6541-6545	389; 445; 515; 636; 1688; 1689; 3268; 8080	389; 445; 515; 636; 1688; 1689; 3268; 5566; 8080; 9876; 31865
	UDP	5353	1047-1049; 9870	1047-1049; 9870

VLAN

A lot of corporate networks are divided into multiple VLANs – for example, to separate BYOD (Bring Your Own Device) traffic from the "core" corporate network. Take this into consideration when integrating ClickShare into your network. ClickShare Buttons connecting to your wireless infrastructure should be able to connect to the Base Units. Furthermore, if you want to use the mobile Apps, these should also be able to reach the Base Units. It is advisable to put all ClickShare Units into a separate VLAN so they are easily manageable.

³ Google Cast will pick a random UDP port above 32768 to facilitate video streaming.

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. If no DNS is available Buttons will fall back to the IP of the Base Unit at the moment of USB pairing. Because of this we strongly advise to reserve IP addresses in your DHCP server for each Base Unit to prevent issues when the hostname is not resolvable or set a fixed IP address within the ClickShare Configurator WebUI. Further, Buttons need to be assigned an IP address on the network they are connect to by a DHCP server.

NTP

When using EAP-TLS, you must also configure NTP on the Base Unit. This can be done via the ClickShare Configurator WebUI. The Base Unit must have the correct time to handle the certificates required for EAP-TLS. Preferably, you should use an NTP server with high availability on the local corporate network. Be advised that, when using an NTP server on the internet, the Base Unit cannot connect through a proxy server.

Security Modes

There are 2 security modes supported by the Button to connect to the corporate network:

- The first one, which applies to a typical corporate network setup, is **WPA2-Enterprise with 802.1X**.
- For a more traditional Wi-Fi setup, there is also support for WPA2-PSK, also known as **WPA2-Personal**.

Both modes are based on Wi-Fi Protected Access (WPA). In this document, we talk about WPA2 – an improved version of the original WPA standard – which adds AES encryption to improve security.

WPA2-Enterprise with 802.1X

WPA2-Enterprise relies on a server (using RADIUS) to authenticate each individual client on the network. To do this, authentication 802.1x 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 through the network in order to authenticate the client device on the network – which, in the case of ClickShare, 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 some other ones (which are not in the standard) are used much more often. Therefore, we have selected the most widely used EAP methods. The list of EAP methods supported in the ClickShare system is:

- EAP-TLS
- PEAP
- EAP-TTLS

More details on each of them, plus setup instructions, can be found in the section on EAP-TLS, PEAP, or EAP-TTLS.

Setup

To facilitate the setup, we have opted for a wizard in the ClickShare Configurator WebUI. This wizard will guide you through the process according to the security mode you select. Further down, you will find an overview and explanation of each supported security mode and the input that is required to get everything integrated and working.

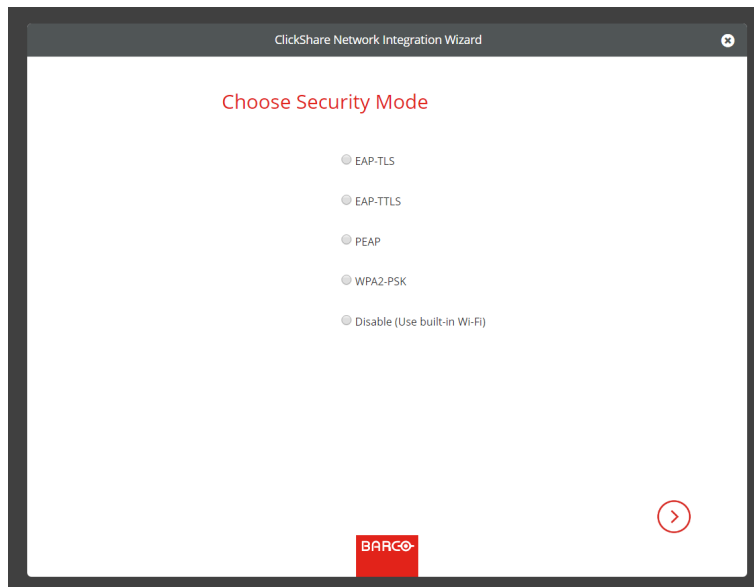


Figure 6: Start of the network integration wizard

Security modes

The next 4 sections describe each of the supported security methods in further detail. Please refer to the one that applies to your environment.

Post Setup

Please note that you must re-pair all of the ClickShare Buttons after completing the setup wizard. Before re-pairing, the previous configured mode is still active on the Base Unit and you will be unable to share.

Apps

Once integrated into the network, any mobile device connected to the corporate network will be able to share content with any Base Unit on the network. If desired, you can prohibit sharing from mobile devices via the Base Unit's ClickShare Configurator WebUI. We advise to enable passcode authentication for mobile devices. This option can be found on the 'Wi-Fi & Network > Services' page of the ClickShare Configurator WebUI or can be enforced by selecting security level 2.

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 certificates. (If this is too big of a hurdle for your organization, EAP-TTLS and PEAP provide good alternatives.) Even though an X.509 client certificate is not strictly required by the standard, it is mandatory in most implementations, including ours.

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 that the user's identity is transmitted in the clear before the actual TLS handshake is performed. EAP-TLS is supported via SCEP or manual certificate (.pem or .pfx format) upload.

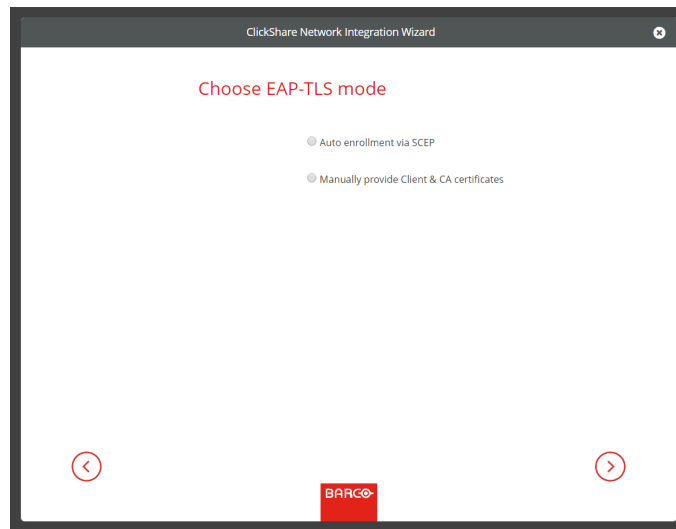


Figure 7: Network integration wizard via EAP-TLS – Choose authentication mode.

SCEP

The Simple Certificate Enrolment Protocol (SCEP) enables issuing and revoking certificates in a scalable way. We have included SCEP support to allow for quicker and smoother integration of the ClickShare Base Unit 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**.

Figure 8: 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, please visit the Microsoft website⁴.

⁴NDES 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>

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`. When you enter the necessary credentials into the setup wizard, the Base Unit automatically retrieves this challenge from the web page and uses it in the enrolment request – thereby fully automating the process.

Input

- SCEP Server IP / Hostname
- SCEP Username
- SCEP Password
- Domain
- Identity
- Corporate SSID

For a detailed explanation of each setting, please go to the Quick reference guide.

Provide certificates manually

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

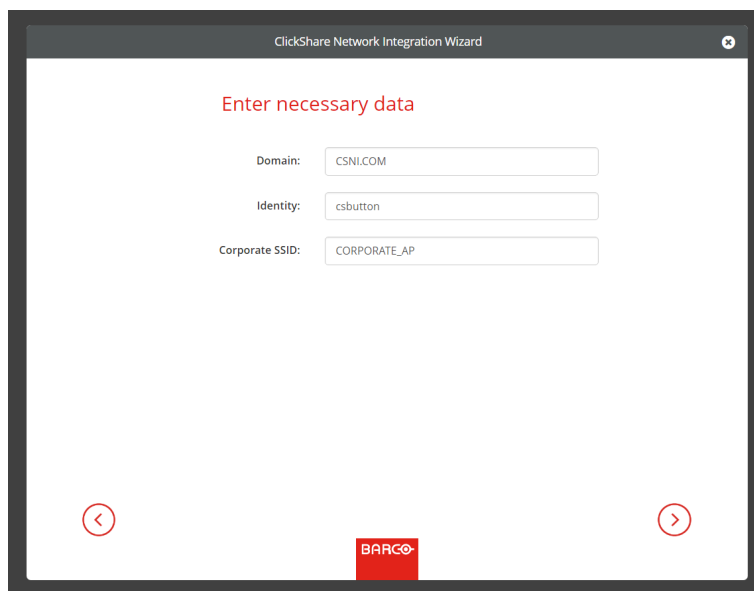
The image shows a screenshot of a web-based wizard titled "ClickShare Network Integration Wizard". The main heading inside the wizard is "Enter necessary data" in red. Below this heading are three input fields, each with a label to its left: "Domain:" with the value "CSNI.COM", "Identity:" with the value "csbutton", and "Corporate SSID:" with the value "CORPORATE_AP". At the bottom of the wizard window, there are two red circular buttons with white arrows pointing left and right, and a red rectangular button with the white text "BARCO".

Figure 9: Network integration wizard via EAP-TLS – Authentication via Client & CA certificates

Client Certificate

The client certificate you provide should be signed by the authoritative root CA in your domain and should be linked to the user you specify in the Identity field. Also, make sure that the client certificate you provide contains the private key – this is 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 that it can validate the chain of trust between the Client and the CA certificates you provide.

Input

To successfully set up an EAP-TLS configuration using SCEP, the following data is required:

- Client Certificate

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 which actual user authentication takes place within the tunnel. This way of working enables to use the security of TLS while authenticating the user, but without the need for a PKI.

The standard does not mandate which method is to be used to authenticate within the tunnel. But in this application note, with regard to PEAP, we are referring 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 by far the most common and widespread implementation of PEAP.

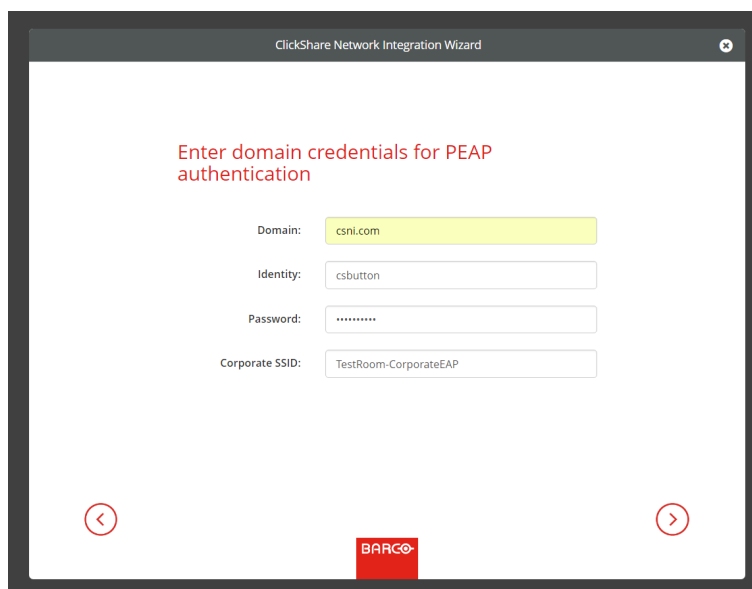


Figure 10: Network integration wizard via PEAP – Authentication data

Input

- Domain
- Identity
- Password
- Corporate SSID

For a detailed explanation of each setting, please go to the Quick reference guide.

EAP-TTLS

EAP-TTLS (Tunnelled Transport Layer Security) is an EAP implementation by Juniper⁵ networks. It is designed to provide authentication that is as strong as EAP-TLS, but it does not require issuing a certificate to each user. Instead, only the authentication servers are issued certificates. User authentication is performed 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

⁵ https://www.juniper.net/techpubs/software/aaa_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html

example, SQL or LDAP databases, or token systems.

Because EAP-TTLS is usually implemented in corporate environments without a client certificate, we have not included support for this. If you prefer to use client certificates per user, we suggest using EAP-TLS instead.

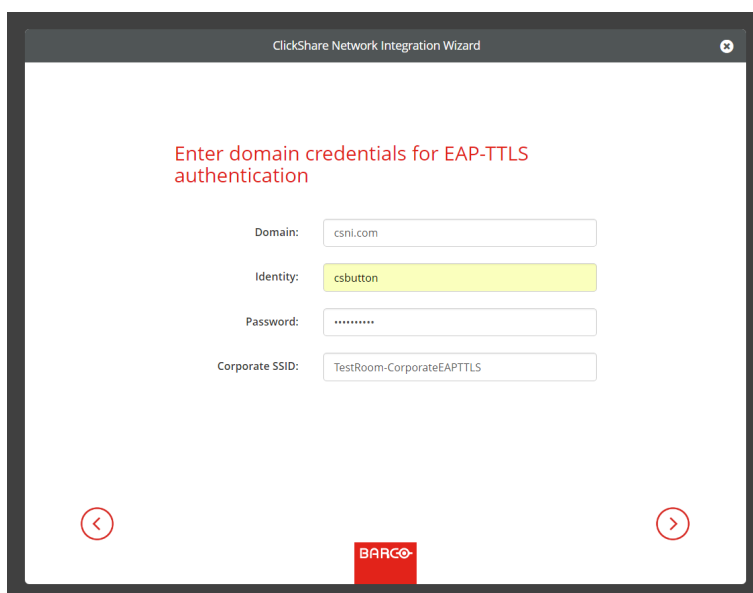
The image shows a screenshot of the 'ClickShare Network Integration Wizard' window. The title bar at the top reads 'ClickShare Network Integration Wizard'. The main content area has a red heading that says 'Enter domain credentials for EAP-TTLS authentication'. Below this heading are four input fields: 'Domain:' with the value 'csni.com', 'Identity:' with the value 'csbutton' (highlighted in yellow), 'Password:' with masked characters '*****', and 'Corporate SSID:' with the value 'TestRoom-CorporateEAPTTLS'. At the bottom of the window, there are two red circular navigation buttons with left and right arrows, and a red 'BARCO' logo in the center.

Figure 11: Network integration wizard via EAP-TTLS – Authentication data

Input

- Domain
- Identity
- Password
- Corporate SSID

For a detailed explanation of each setting, please go to the Quick reference guide.

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 setup very straightforward. Once connected, all data transmitted between client and AP is encrypted using either a CCMP or TKIP 256-bit key.

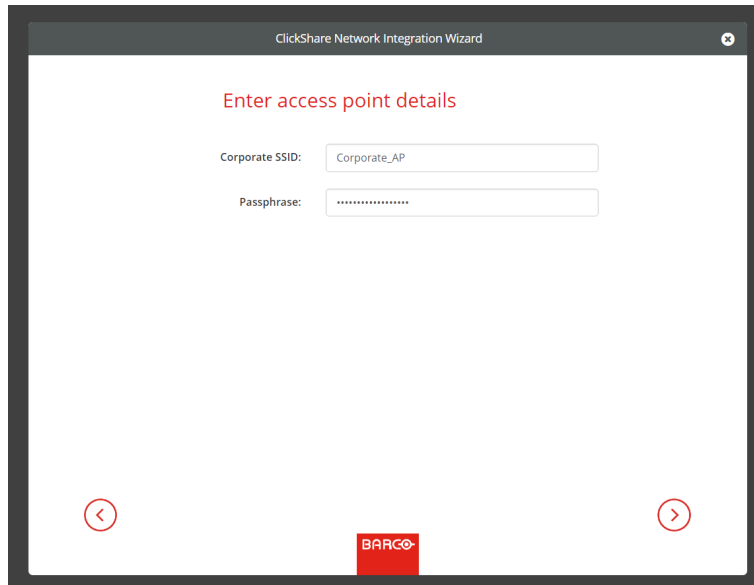


Figure 12: Network integration wizard via WPA2-PSK - Authentication data

Input

- Corporate SSID
- Passphrase

For a detailed explanation of each setting, please go to the Quick reference guide.

Quick reference guide

This section lists the configuration details, it describes the different settings you can encounter in the setup wizard in more detail.

SCEP Server URL / Hostname

This is the IP or hostname of the Windows Server in your network running the NDES service. Since Internet Information Services (IIS) supports both HTTP and HTTPS, specify which of the two you want to use. If not specified, we default to HTTP.

Examples: `http://myserver` or `https://10.192.5.1` or `server.mycompany.com` (will use http)

SCEP Username

This is a user in your Active Directory which has the required permission to access the NDES service and request the challenge password. To confirm this, the user should be part of the CA Administrators group (in the case of a stand-alone CA) or have enrol permissions on the configured certificate templates.

SCEP Password

This is 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.

Domain

The company domain for which you are enrolling should match the one defined in your Active Directory.

Identity

The identity of the user account in the Active Directory, which the ClickShare Buttons use to connect to the corporate network.

Password

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.

Corporate SSID

The SSID of your corporate wireless infrastructure to which the ClickShare Buttons connect.

Client Certificate

When we talk about client certificates we specifically mean the so called device or machine certificates not a user certificate. We support 2 formats for uploading a client certificate:

- 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-----"

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.

CA Certificate

We support the common .crt file extension, which can contain a Base64 encoded DER certificate.

Passphrase

The password used in WPA2-PSK to authenticate onto the wireless infrastructure. This can be a string of 64 hexadecimal digits or a code of 8 to 63 printable ASCII characters.

4. Troubleshooting

Here we list some most frequently occurring problems and their basic solution. Also detailed steps are given on how to troubleshoot your setup and request support in 4.2 Support, completed with a description on how to view the logs on your Button and Base Unit in 4.3 How to retrieve debug logs.

4.1. Top problems & solutions

Some most frequently occurring issues and a brief description of their solutions are listed here. If this does not solve the problem at hand, the advised methodology on how to get further support can be found section 4.2 Support.

The Button is unable to connect via the corporate network

Possible cause

The Button is unable to connect when the credentials set for network integration are incorrect and do not match the settings of the closest Wi-Fi access point.

Solution

Please verify the credentials and reconfigure network integration following the steps described in 3.6 Configure Network integration on page 13. Re-pair the Buttons after configuring network integration. Please 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”.

Possible cause

The Button is unable to find the Base Unit on the corporate network.

Solution

Please verify that the Base Unit is announced by its hostname and that its IP address can be resolved. In case you want to set a fixed IP for the Base Unit we advise to do so using a DHCP entry mapping the MAC address of the Base Unit to the IP address.

Possible cause

When ClickShare is configured in network integration mode using the “WPA2-PSK” security mode, it can be that the Buttons are unable to connect to an access point using a “WPA/WPA2 mixed” security mode.

Solution

Please change the access points’ security mode to “WPA2 only”.

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

Possible cause

The corporate network does not support traffic over a set of ports required for network integration or the Base Unit is not in the same network as the device you are sharing with.

Solution

Please check whether the ports mentioned in Table 3 on page 14 are open for traffic in your corporate network to use the ClickShare App, Airplay, and/or Google Cast. We advise to put the Base Unit in the same network as the mobile devices and Buttons. For example, Bonjour discovery (required for Airplay) requires the devices to be visible in the same subnet. In case the Base Unit is not in the same network as the mobile device, you can try to provide a bridge from one network into the other.

Note that for discovery of these services, multicasting must be enabled on your network.

The Button disconnects while sharing

The fact that the Button disconnects while sharing could be due to various reasons.

Possible cause

The distance between Button and Base Unit is too large or the Button is unable to connect to the nearest Wi-Fi access point.

Solution

Please check if the Base Unit is still accessible on your network. The IP address of the Unit should be displayed on the Wallpaper on screen. Not only should the Base Unit be accessible by its IP address, its hostname should also be resolvable. Therefore, make sure pinging the Base Unit's hostname is successful. Further you can verify that the Button is able to connect to the access point by checking both the Button log and reviewing the access point log.

Possible cause

There is interference between your access points in your Enterprise network, blocking a good usage of the Wi-Fi signal by the Button and other peripherals.

Solution

Please make sure that your access point is configured in a separate channel different from the surrounding access points. We advise to do a Wi-Fi spectrum analysis and plan assigned channels for each access point accordingly.

Possible cause

The ClickShare Button needs to switch during sharing between different access points as most frequently occurs while walking around.

Solution

The ClickShare Button does not support roaming between different access points. We advise to do a Wi-Fi spectrum analysis and plan Wi-Fi strength accordingly such that Buttons do not need to switch between access points while sharing. In case this is not an option within your Enterprise network and the ClickShare Buttons frequently switch between different access points which are close-by, the stand-alone mode is currently the advised way to allow sharing within a meeting room. Using the CS Configurator WebUI one can limit the signal strength of the Base Unit's internal Wi-Fi and hence limit interference with other access points.

Possible cause

The access point is changing channels dynamically to cope with interference from other signals within your Enterprise network.

Solution

The ClickShare Button is not capable of working with dynamically changing parameters of an access point including but not limited to changing Wi-Fi configurations and channel hopping, nor the use of DFS channels. Channel hopping and DFS channels are not supported by the Button. We advise to review close-by access points and force them to use a non-DFS and static channel.

The corporate network certificates are not accepted by the Base Unit

Possible cause

In some cases, the certificates uploaded on the Base Unit do not work as expected. The upload procedure fails or the connection is impossible or sometimes drops.

Solution

Please re-read the section on EAP-TLS on page 16 to learn how to configure your Base Unit with network certificates. Next, retry uploading the certificates through the wizard and repairing the Buttons with the Base Unit. Note that Base Unit and Button cannot handle three level certificates. Network integration is provided as an "AS IS" feature. Although it supports many setups and certificates we cannot guarantee that it works in all cases.

The sharing quality dropped when enabling network integration mode

Possible cause

The wireless signal from the access point to the Button could be limited or the available bandwidth on the network is limited by other traffic or network configuration.

Solution

Please check if the distance between Button and wireless access point is not too large and whether the signal is optimal. Further, please review the traffic on the network and try to reduce the amount of bandwidth used. Note that the communication between Base Unit and Button requires an available link with a data rate between 7 and 10 Mbps. If that is not possible we advise to review the setup and either revert to stand-alone mode or setup a separate (V)LAN.

4.2. Support

If you are experiencing problems, please go first through the next section "Check the button connection". If this does not resolve the issue at hand you need to create a report containing detailed information on the Enterprise environment wherein ClickShare operates, the problem, and the ClickShare installation as listed in the section "

Gather in-depth network and system information". With this report, you can contact your ClickShare installer or reseller for support (or the Barco helpdesk).

Check the button connection

The ClickShare Button receives the connection details for connecting to your corporate network via USB pairing, please verify these details:

- Make sure the Base Unit is configured properly
- Pair the Buttons again

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 doesn't 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 doesn't change IP (reserve a DHCP addresses or define a fixed IP addresses)

Gather in-depth network and system information

To be able to help you further to resolve the issue please collect the info mentioned in the following steps. It is of the utmost importance to provide all of the information requested below to make a full diagnose of your problem.

1. Contact your IT department and let them describe the Corporate Network connection methods next to answering 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)
 - Can you see the Buttons requesting an IP address?
 - (and can the button reach the Base Unit from that IP address)
2. Please provide a full description of the problem. Please explain the problem which you're experiencing. If possible please explain the steps needed to reproduce the problem. Some pictures or a video can explain more than a thousand words.
3. Please follow the steps below and provide the requested information on your ClickShare installation
 - Enable debug logging on the Base Unit as described in the section "Base Unit" on page 29.
 - Capture some logs from the ClickShare client trying to connect to the Base Unit. Therefore, insert the ClickShare dongle into your computer. Start "ClickShare_for_Windows" (or for Mac) with shift pressed to start logging and let the ClickShare client connect for a few minutes (3 should be enough). Retrieve the log files as described in the section "Button" on page 29. Compress them into a zip archive and add them to the report you are creating.
 - Ping the hostname of the Base Unit and take a print screen of the ping process.

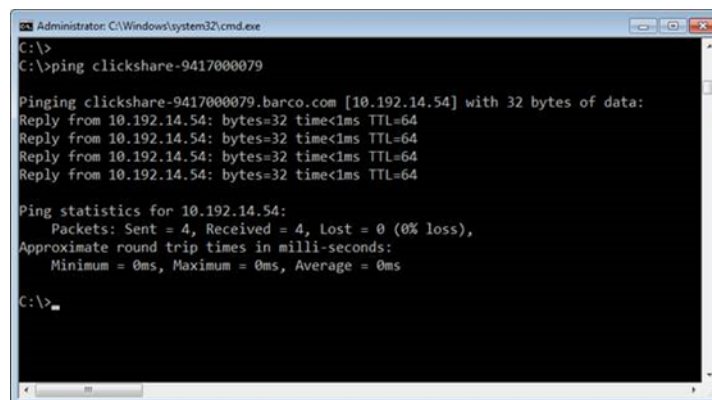


Figure 13: Screenshot ping process

- Retrieve the configuration file from the Base Unit in the ClickShare Configurator WebUI. You can download this configuration file by selecting on the Personalisation / Configuration Files tab and clicking on the “Full Backup” button.

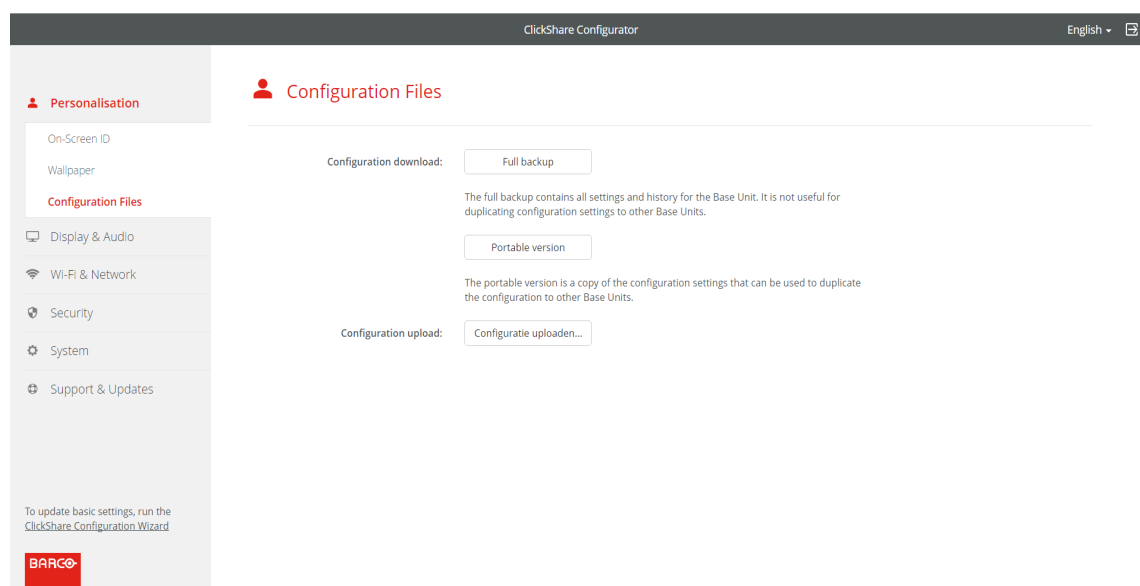


Figure 14: Screenshot on how to download a full backup of the Base Unit

- Capture a print screen of the Base Unit status page which can be found by clicking on the System / Base Unit Status tab.

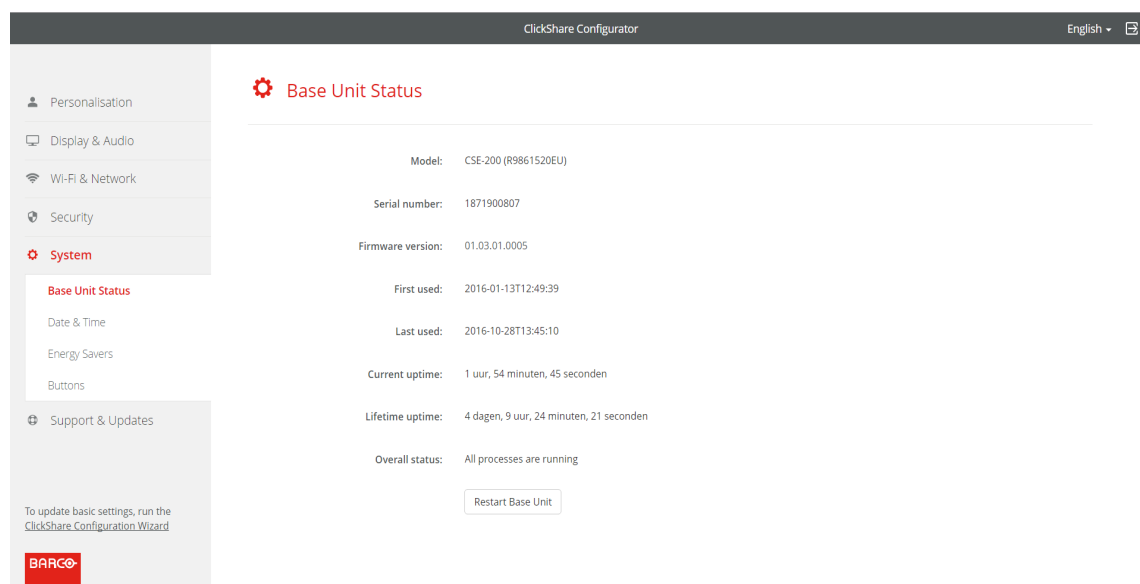


Figure 15: Screenshot of Base Unit status page

- Capture a print screen of the Base Unit Corporate Network configuration page, which can be found by clicking on the Wi-Fi & Network / Network integration tab.

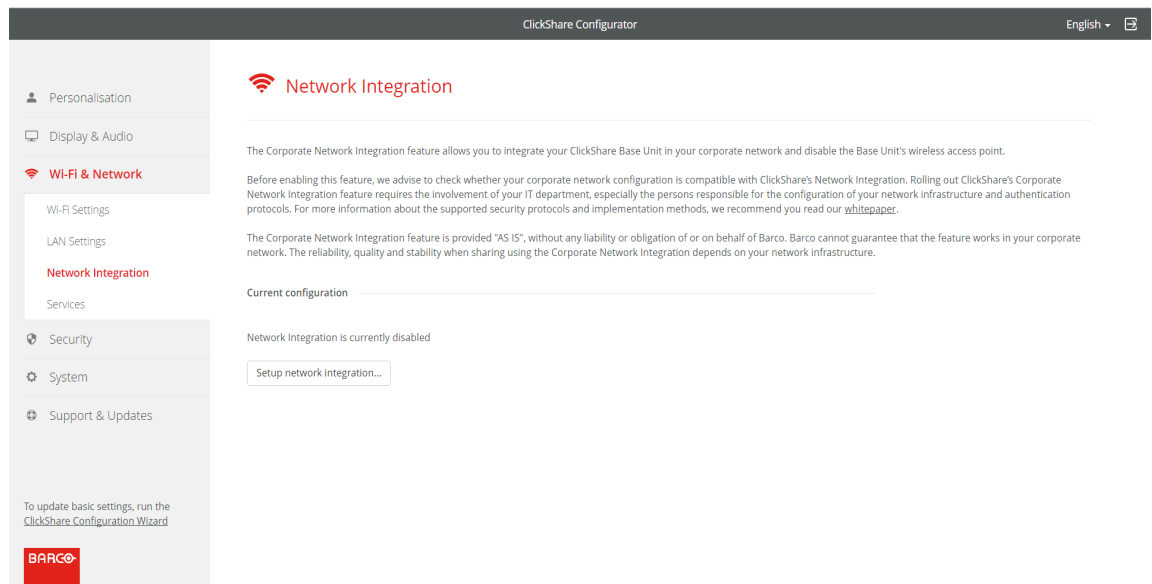


Figure 16: Screenshot of the Base Unit Corporate Network configuration page

- Get debug logs of the ClickShare Base Unit when trying to connect to the Base Unit with a Button. The method on how to retrieve these debug logs is described in the section “Base Unit” on page 29.

4.3. How to retrieve debug logs

Even though the Base Unit does its best to validate the provided configuration input, it is still possible that the Button will not be able to connect to your corporate network. There are several potential root causes for this, including but not limited to: incorrect SSID, SSID not available, incorrect EAP Identity / Password, firewall settings, VLAN configuration, ...

Button

To receive feedback from the Button when it is trying to connect to your corporate network, please look at the ClickShare Client log. This log can be enabled by pressing and holding the Shift key when starting the Client executable ("ClickShare_for_Windows" or for Mac).

Click on the logging pop up to open the logging directory as shown in Figure 17 where you can find the recorded log files.

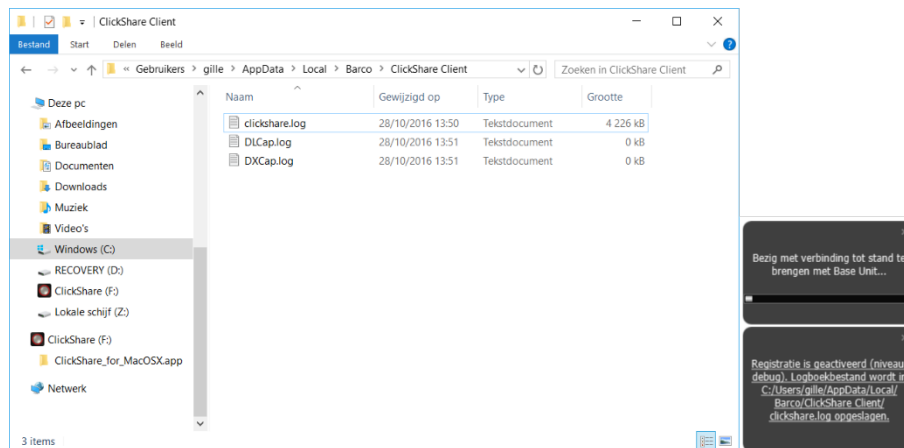


Figure 17: Screenshot - logging pop up

Look for lines like "EDSUSBDongleConnection::mpParseDongleMessages" in the log file.

An error code and a short summary of the issue should be logged. An example of this line could be the one below:

```
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 could reach the Base Unit please connect a PC in the same way a Button would connect (same user name, pw, certificates) and ping the Base Unit's hostname, you can find the hostname in the Based Unit's ClickShare Configurator WebUI. If the ping fails, try pinging the IP adjust your network setup so pinging the hostname is successful.

We strongly advise to reserve IP addresses in your DHCP server for each Base Unit to prevent issues when the hostname is not resolvable.

Base Unit

These debug logs can be found by browsing to the ClickShare Configurator WebUI and clicking onto the Support & Updates / Troubleshoot tab. To capture all system logging information, please enable "debug logging" as shown in Figure 18.

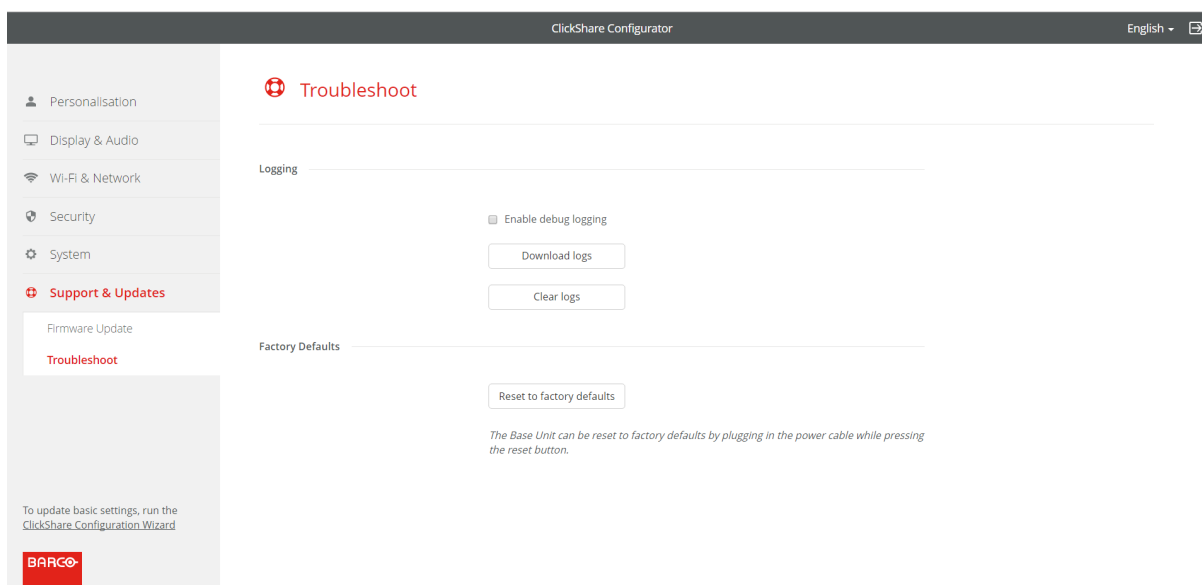


Figure 18: Screenshot where to retrieve Base Unit debug logs

5. Acronyms

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	ClickShare Management Suite
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
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

6. Disclaimer

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

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

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