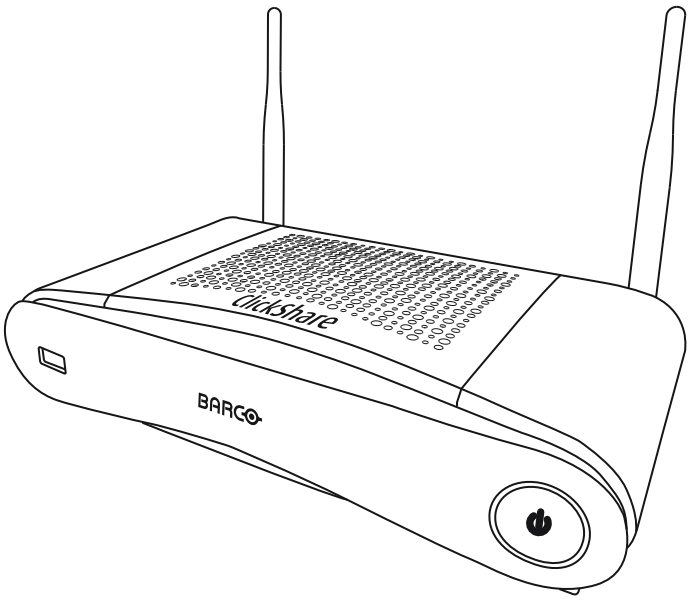
ClickShare CSE-200



Installation manual

Product revision

Software Revision: 1.10.x

Barco NV
Beneluxpark 21, 8500 Kortrijk, Belgium
www.barco.com/en/support
www.barco.com

Registered office: Barco NV
President Kennedypark 35, 8500 Kortrijk, Belgium
www.barco.com/en/support
www.barco.com

Changes

Barco provides this manual 'as is' without warranty of any kind, either expressed or implied, including but not limited to the implied warranties or merchantability and fitness for a particular purpose. Barco may make improvements and/or changes to the product(s) and/or the program(s) described in this publication at any time without notice.

This publication could contain technical inaccuracies or typographical errors. Changes are periodically made to the information in this publication; these changes are incorporated in new editions of this publication.

The latest edition of Barco manuals can be downloaded from the Barco web site *www.barco.com* or from the secured Barco web site *https://www.barco.com/en/signin*.

Copyright ©

All rights reserved. No part of this document may be copied, reproduced or translated. It shall not otherwise be recorded, transmitted or stored in a retrieval system without the prior written consent of Barco.

Trademarks

USB Type-C™ and USB-C™ are trademarks of USB Implementers Forum.

Trademarks

Brand and product names mentioned in this manual may be trademarks, registered trademarks or copyrights of their respective holders. All brand and product names mentioned in this manual serve as comments or examples and are not to be understood as advertising for the products or their manufacturers.

HDMI Trademark Notice

The terms HDMI, HDMI High Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

Product Security Incident Response

As a global technology leader, Barco is committed to deliver secure solutions and services to our customers, while protecting Barco's intellectual property. When product security concerns are received, the product security incident response process will be triggered immediately. To address specific security concerns or to report security issues with Barco products, please inform us via contact details mentioned on *https://www.barco.com/psirt*. To protect our customers, Barco does not publically disclose or confirm security vulnerabilities until Barco has conducted an analysis of the product and issued fixes and/or mitigations.

Patent protection

Please refer to *www.barco.com/about-barco/legal/patents*

Guarantee and Compensation

Barco provides a guarantee relating to perfect manufacturing as part of the legally stipulated terms of guarantee. On receipt, the purchaser must immediately inspect all delivered goods for damage incurred during transport, as well as for material and manufacturing faults Barco must be informed immediately in writing of any complaints.

The period of guarantee begins on the date of transfer of risks, in the case of special systems and software on the date of commissioning, at latest 30 days after the transfer of risks. In the event of justified notice of complaint, Barco can repair the fault or provide a replacement at its own discretion within an appropriate period. If this measure proves to be impossible or unsuccessful, the purchaser can demand a reduction in the purchase price or cancellation of the contract. All other claims, in particular those relating to compensation for direct or indirect damage, and also damage attributed to the operation of software as well as to other services provided by Barco, being a component of the system or independent service, will be deemed invalid provided the damage is not proven to be attributed to the absence of properties guaranteed in writing or due to the intent or gross negligence or part of Barco.

If the purchaser or a third party carries out modifications or repairs on goods delivered by Barco, or if the goods are handled incorrectly, in particular if the systems are operated incorrectly or if, after the transfer of risks, the goods are subject to influences not agreed upon in the contract, all guarantee claims of the purchaser will be rendered invalid. Not included in the guarantee coverage are system failures which are

attributed to programs or special electronic circuitry provided by the purchaser, e.g. interfaces. Normal wear as well as normal maintenance are not subject to the guarantee provided by Barco either.

The environmental conditions as well as the servicing and maintenance regulations specified in this manual must be complied with by the customer.

Barco ClickShare Product Specific End User License Agreement[1]

THIS PRODUCT SPECIFIC USER LICENSE AGREEMENT (EULA) TOGETHER WITH THE BARCO GENERAL EULA ATTACHED HERETO SET OUT THE TERMS OF USE OF THE SOFTWARE.

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE OPENING OR DOWNLOADING AND USING THE SOFTWARE.

DO NOT ACCEPT THE LICENSE, AND DO NOT INSTALL, DOWNLOAD, ACCESS, OR OTHERWISE COPY OR USE ALL OR ANY PORTION OF THE SOFTWARE UNLESS YOU CAN AGREE WITH ITS TERMS AS SET OUT IN THIS LICENSE AGREEMENT.

1. Entitlement

Barco ClickShare (the “Software”) offered as a wireless presentation solution that includes the respective software components as further detailed in the applicable Documentation.

The Software can be used upon purchase from, and subject to payment of the relating purchase price to, a Barco authorized distributor or reseller of the ClickShare base unit and button or download of the authorized ClickShare applications (each a “Barco ClickShare Product”).

- **Term**
  The Software can be used under the terms of this EULA from the date of first use of the Barco ClickShare Product, for as long as you operate such Barco ClickShare Product.
- **Deployment and Use**
  The Software shall be used solely in association with a Barco ClickShare Product in accordance with the Documentation issued by Barco for such Product.

2. Support

The Software is subject to the warranty conditions outlined in the Barco warranty rider. Maintenance, including the provision of upgrades and updates to the Software, and helpdesk support are available at your option on the terms of Barco’s then current warranty rider.

Higher maintenance and support levels can be obtained at the moment of product sale or during the Barco ClickShare Product and/or Software warranty term.

Higher maintenance and support levels may be included in the initial transaction if ordered and paid for additionally. It is strongly suggested to maintain the maintenance and support agreement without interruption. Barco reserves the right not to restart maintenance following an interruption by the customer.

3. Terms of Use

The Software can be used as set out in the Barco EULA attached hereto.

The provisions of this Product Specific EULA override the Barco generic EULA in case of conflicts or inconsistencies.

In case of (inadvertent or other) non-compliance (e.g. where the actual use overshoots the use authorized hereunder), Barco shall have the option to suspend access to the Software until the non-compliance is remedied, failing of which Barco may terminate the License Agreement as set out herein.

4. Privacy

You are controller for personal data which are being processed via the Software. Therefore, you remain solely responsible for complying with all applicable data protection laws and for implementing and maintaining privacy protection and security measures (especially for components that you provide or control). Barco disclaims any liability in this regard.

Barco created a specific privacy policy for the ClickShare software application for mobile devices, which describes the processing of personal data via this application (*http://www.barco.com/en/about-barco/legal/privacy-policy/clickshare-app*).

1: In the event of any differences or inconsistencies between translations of the EULA and the English text of the EULA, the English text will prevail.

5. Other Terms

- **Open Source components**
  The Software contains software components released under an Open Source license.
  A list of the third party components used is available in the Software's README files, through the "My Barco" section of the Barco website or through other (online) means. The applicable license terms, copyright notices and, as relevant, source code access conditions apply as set out in the Barco EULA attached hereto.
- **Retention of data**
  Barco right to use and retain Functional Information (section 10.2 of the EULA) shall survive the term of this EULA.

BARCO END USER LICENSE AGREEMENT[1]

By accepting these terms (through tick box or other mechanism designed to acknowledge agreement to the terms of an electronic copy of this License Agreement), or by installing, downloading, accessing, or otherwise copying or using all or any portion of the Software (as defined below), (i) you accept this License Agreement on behalf of the entity for which you are authorized to act (e.g., your employer) and you agree to act in a manner consistent with this License Agreement (or, if there is no such entity for which you are authorized to act, you accept this License Agreement on behalf of yourself as an individual and acknowledge that you are legally bound by this Agreement), and (ii) you represent and warrant that you are duly empowered by the end user in case you act on behalf of such entity.

These terms apply to your use of the Software as of and for the original Term of your license. When you renew or purchase an additional license, the then current version of this License Agreement shall apply and will remain unchanged during the term of that license and/or in respect of such changed elements. The other contract documents (Product Specific EULA; Maintenance and Support Agreement, if and when provided alongside with this document) applies in addition to these terms and constitute the entire License Agreement. You acknowledge that an electronic copy of this Agreement shall have the same proving value as a hard copy signed by the parties.

If you are unwilling to accept this License Agreement on these terms, or you do not have the right, power and authority to act on behalf of and bind such entity (or yourself as an individual if there is no such entity), DO NOT SELECT THE "I ACCEPT" BUTTON OR OTHERWISE CLICK ON ANY BUTTON OR OTHER MECHANISM DESIGNED TO ACKNOWLEDGE AGREEMENT, AND DO NOT INSTALL, DOWNLOAD, ACCESS, OR OTHERWISE COPY OR USE ALL OR ANY PORTION OF THE SOFTWARE.

1. Definitions

"Affiliate" means any corporation or other entity directly or indirectly, controlling, controlled by or under common control with such corporation or entity. For the purpose of the above, "control" shall mean (i) the ownership or control, directly or indirectly, of fifty percent (50%) or more of the equity capital or the shares or voting rights in the corporation or other entity in question or (ii) the control of the composition of the board of directors of the corporation or other entity in question.

"Barco" means Barco NV (company number 0473.191.041) with company address at Beneluxpark 21, 8500 Kortrijk, Belgium, or its designated Affiliate licensing to you the proprietary software which is the subject matter of this Agreement.

"Documentation" means all technical, reference and installation manuals, user guides, published performance specifications and other written documentation provided by Barco generally to its licensees with respect to the Software, along with any modifications and updates thereto;

"DRM" means Barco's digital rights management platform used to provide access to and access conditions of the Software.

"License Agreement" means this Barco End User License Agreement (EULA), incorporating the terms of the Product Specific EULA, and any modifications thereof as set out herein.

"Product Specific EULA" means the supplemental software terms applicable

"Software" means the computer software, released in object code only, which is being licensed hereunder, as described in the applicable purchase order and related Product Specific EULA.

"Term" means the period set out in article 9.1 hereof, as well as any agreed renewal period.

"you" means the entity on behalf of which these terms are accepted, and any of its representatives having access to the Software.

2. License Grant

2.1 '*License Scope*'. Subject to compliance with all license terms and payment of applicable fees, Barco grants you a limited, non-exclusive, non-assignable, non-transferable, non-sub-licensable license to use the Software exclusively in accordance with the conditions and parameters set forth herein. Save for the Product Specific EULA or any broader license terms confirmed through the DRM tool, the license under this License Agreement applies to one (1) copy of the Software to be used on one single computing device by one (1) single user. Installation on a computing device that may be concurrently accessed by more than one user shall not constitute a permitted use and a separate license is required for each user connecting at the same time to a computing device on which the Software is being deployed.

2.2 ' *License Type*'. The applicable license type, and your rights in time, deployment and usage, are further detailed in the Product Specific EULA (in the absence of which the scope shall be as set in article 2.1 hereof).

2.3 '*License restrictions*'.

Intended Use. You agree to use the Software solely as permitted by this License Agreement (and any Product Specific EULA made part of it), by any applicable laws and in a matter consistent with its design and Documentation.

No Transfer (License Agreement). You agree not to transfer, assign or sublicense your license rights to any other person or entity, unless Barco's prior written consent is obtained.

No Transfer (Software). If you deactivate or uninstall the Software from the computer device on which it was originally installed, this will terminate this License Agreement unless otherwise and specifically approved by Barco. You agree not to use the Software in association with other hardware or software that allows to pool connections, reroute information or in any other way enables to breach or circumvent the license restrictions by enabling the deployment and use of the Software by more than the authorized number of devices or users (e.g. multiplexing) or otherwise attempts to reduce the number of licenses actually required.

Authorized Users. The use of the Software is restricted to persons within your organization, or any third party representatives operating under your responsibility and control, provided any such persons have accepted the terms of this License Agreement. You agree not to use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the prior written authorization of Barco. You shall not lease, rent, sell or otherwise transfer or grant a security or other interest in the Software.

No Modifications. You shall not make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same.

No Reverse Engineering. You agree not to reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction, or except to the extent Barco is legally required to permit such specific activity pursuant to any applicable open source license.

Code required to ensure interoperability. To the extent required by law, and at your written request, Barco shall provide you with the interface information needed to achieve interoperability between the Software and another independently created programs used by you, on payment of Barco's applicable fee (if any). You shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with terms and conditions which Barco makes applicable.

No Unbundling. The Software may include various applications and components, may support multiple platforms and languages, and may be provided on multiple media or in multiple copies. Nonetheless, the Software is designed and provided to you as a single product to be used as a single product on devices as permitted herein. You agree not to unbundle the component parts of the Software for use on different computer devices.

Territory. You agree to use the Software solely in the territory or region where you obtained the Software from Barco or its authorized reseller or as otherwise stated in the Documentation. Any export if permitted shall comply with any applicable (export) laws and regulations.

2.4 '*Your Infrastructure*'. You remain responsible to procure and maintain hardware, operating system, network and other infrastructure (the "Infrastructure") required to operate the Software and to keep such Infrastructure functioning and virus-free. You acknowledge that the Software is a complex computer software application, and that the performance thereof may vary depending hardware platform, software interactions and configuration. You acknowledge that the Software is not designed and produced specifically to meet your requirements and expectations and the selection of the Software by you is entirely your own choice and decision.

3. Ownership. Intellectual Property Rights.

3.1 '*Ownership*'. Any Software is licensed, not sold to you, on a non-exclusive basis for use only under the terms of this License Agreement, and Barco and its suppliers reserve all rights not expressly granted to you. You may own the carrier on which the Software is provided, but the Software is owned and copyrighted by Barco or by third party suppliers. Your license confers no title or ownership and is not a sale of any rights in the Software or its Documentation.

3.2 '*Third Party Materials*'. The Software may contain or require the use of certain third party technology (whether proprietary or open source software), identified by Barco in the Documentation, readme file, third-party click-accept, on *www. barco. com* or elsewhere (the "Identified Components"). Identified Components may be subject to additional and/or different terms and you agree that the Identified Components are licensed under the terms, disclaimers and warranties of their respective licenses which in the forthcoming case shall override the provisions of this License Agreement.

3.3 '*Source Code Access*'. To the extent required under third party (open source) license terms, and for a period of 36 months following your acceptance of this License Agreement, Barco shall provide access to the source code controlled by a third party (open source) license, via email or download link. If the relevant license terms require so, you may require Barco (attn. its legal department, at the address stated above) to obtain such code on tangible medium against payment of the cost of media, shipping and handling.

3.4 '*Trademarks / Copyright*'. Any brand and product names mentioned in relation to the Software may be trademarks, registered trademarks or copyrights of their respective (third party) holders. In addition, the Software is protected by national and international laws and treaty provisions. Copyright on the Software components belongs to the respective initial copyright holder, each additional contributor and/or their respective assignee(s), as may be identified in the Software Documentation, source code, README file, or otherwise. You shall not remove or obscure or otherwise alter any trademark, copyright or other proprietary notices, legends or logo's placed on or contained within the Software.

3.5 '*Trade Secrets*'. You acknowledge that the Software embodies valuable trade secrets of Barco and its third party licensors and agree not to disclose, provide or otherwise make available such trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Barco. You shall implement all reasonable security measures to protect such trade secrets.

4. Support

4.1 '*Principle*'. Barco is under no obligation to provide support and maintenance in respect of the Software, except as included in a Product Specific EULA and/or to the extent you have entered into a separate maintenance and support agreement and paid applicable maintenance and support fees. Any unauthorized use of the Software, as specified in any maintenance and support agreement, may prohibit Barco from providing such support and maintenance.

4.2 '*Support policy*'. Maintenance releases updates or upgrades can be obtained under the terms of a separate maintenance and support agreement which is being offered to you. Such agreements, together with the support included in a Product Specific EULA, include Barco's sole liability and your sole remedy in respect of the support and maintenance of the Software. You agree to install any maintenance releases to address bugs or security issues in the Software if the same are being provided to you. Barco will keep you informed as of when earlier versions of the Software are no longer serviced.

4.3 '*Remote connectivity*'. Barco may require, as a material condition to provide maintenance or support, that the Software remains remotely connected with Barco over a network.

5. Warranty

EXCEPT FOR THE LIMITED WARRANTY THAT MAY APPLY AS PER THE PRODUCT SPECIFIC EULA, YOU UNDERSTAND THAT THE SOFTWARE IS BEING PROVIDED TO YOU "AS IS". BARCO DOES NOT MAKE NOR INTENDS TO MAKE ANY WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY AND DOES NOT WARRANT THAT THE SOFTWARE WILL BE FREE FROM ERRORS OR THAT YOU WILL BE ABLE TO OPERATE THE SOFTWARE WITHOUT INTERRUPTIONS OR THAT SUCH ERRORS WILL BE CORRECTED BY BARCO. EXCEPT FOR ANY MAINTENANCE AND SUPPORT OBLIGATIONS SEPARATELY AGREED, YOU ARE SOLELY RESPONSIBLE FOR ALL COSTS AND EXPENSES ASSOCIATED WITH RECTIFICATION, REPAIR OR DAMAGE CAUSED BY SUCH ERRORS. IN THE FORTHCOMING CASE, THE WARRANTY DISCLAIMER FOUND IN APPLICABLE OPEN SOURCE LICENSES SHALL OVERRIDE THE PROVISIONS OF THIS LICENSE AGREEMENT.

6. Compliance and Enforcement

6.1 '*Reporting and Audit*'. In addition to good practice record-keeping obligations, you agree to report the use of the Software and relating billing metrics in the DRM or otherwise as agreed. You grant to Barco and its

designated auditors, at Barco's expenses, the right to verify your deployment and use of the Software during your normal business hours so as to verify your compliance with the License Agreement. In the event such audit reveals non-compliance with your payment obligations hereunder, you shall promptly pay to Barco the appropriate license fees plus the reasonable cost of conducting the audit.

6.2 '*Fair Use Monitor*'. You are informed and acknowledge that the Software includes technology which allows to remotely decrease (in part or in full) the functionality of the Software (the "Fair Use Monitor"). Such technology is an enabling tool and a material condition precedent for Barco to enter into this License Agreement.

6.3 '*Enforcement*'. Upon breach of the License Agreement (including overdue payment), Barco shall inform the then known user, through the DRM or otherwise in writing, (i) which condition of the License Agreement (including payment terms) is violated; (ii) allow a period of 8 calendar days to cure such breach, if it can be cured at all; and (iii) inform which part of the functionality Barco intends to reduce (all Software or certain additionally licensed features only; in part or in full) if the breach is not remedied on time and in full.

6.4 '*Remedy*'. If the breach is not cured within the applicable remedy period (or cannot be cured at all), Barco shall have the option (i) to cause you to procure such additional licenses required as per the actual usage; (ii) to reduce the Software's functionality, including through the use of the Fair Use Monitor; or (iii) to terminate the License Agreement as set out herein, without prejudice to any other remedies available at law, under contract or in equity.

6.5 '*Indemnification*'. YOU HEREBY AGREE TO INDEMNIFY, DEFEND AND HOLD HARMLESS BARCO AND BARCO'S AFFILIATES FROM AND AGAINST ANY AND ALL ACTIONS, PROCEEDINGS, LIABILITY, LOSS, DAMAGES, FEES AND COSTS (INCLUDING ATTORNEY FEES), AND OTHER EXPENSES INCURRED OR SUFFERED BY BARCO ARISING OUT OF OR IN CONNECTION WITH ANY BREACH BY YOU OF THE TERMS OF THIS SOFTWARE LICENSE.

7. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW, BARCO ACCEPTS NO LIABILITY FOR ANY DAMAGES, LOSSES OR CLAIMS YOU OR ANY THIRD PARTY MAY SUFFER AS A RESULT OF YOUR USE OF THE SOFTWARE. IN JURISIDCTIONS WHERE BARCO'S LIABILITY CANNOT BE EXCLUDED, BARCO'S LIABILITY FOR DIRECT DAMAGES SHALL BE LIMITED TO THE LICENSE FEES ACTUALLY PAID FOR THE SOFTWARE DURING THE TWELVE MONTHS PRECEEDING THE CLAIM (OR AN AMOUNT OF 250 EURO IF NO FEE WOULD BE PAID) IN THE AGREGATE.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL BARCO BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS OR DAMAGES OF ANY KIND WHICH MAY ARISE OUT OF OR IN CONNECTION WITH THE SOFTWARE, THIS SOFTWARE LICENSE OR THE PERFORMANCE OR PURPORTED PERFORMANCE OF OR FAILURE IN THE PERFORMANCE OF BARCO'S OBLIGATIONS UNDER THIS SOFTWARE LICENSE OR FOR ANY ECONOMIC LOSS, LOSS OF BUSINESS, CONTRACTS, DATA, GOODWILL, PROFITS, TURNOVER, REVENUE, REPUTATION OR ANY LOSS ARISING FROM WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OF THE SOFTWARE AND ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES WHICH MAY ARISE IN RESPECT OF USE OF THE SOFTWARE, EVEN IF BARCO HAS BEEN ADVISED OF THE POSSIBILITY OF THEIR OCCURRENCE.

8. Confidentiality

8.1 '*Confidential Information*'. You will be receiving information which is proprietary and confidential to Barco during the procurement and Term of this License Agreement. "Confidential Information" shall include (i) the underlying logic, source code and concepts of the Software or other trade secrets (the access to which is strictly limited as expressly set out herein), (ii) any information designated as confidential by Barco or which has the necessary quality of confidence about it and (iii) any license key provided by Barco to you hereunder.

8.2 '*Non-Disclosure*'. You agree not to divulge any Confidential Information to any persons without Barco's prior written consent provided that this article 8 shall not extend to information which was rightfully in your possession prior to the commencement of this License Agreement, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this article 8), to the extent it is required to be disclosed by law or which is trivial or obvious. You agree not to use any Confidential Information except for the authorized purpose hereunder. The foregoing obligations as to confidentiality shall survive the Term of this License Agreement.

9. Term and Termination

9.1 '*Term*'. The duration of this License Agreement will be from the date of your acceptance (as set forth above) of the Software (whereby you acknowledge that use of the Software implies acceptance), until you de-activate the Software, discontinue the use of the device on which the Software was first installed for its

intended use or the expiration of the limited time period set out in the Product Specific EULA, whichever comes first.

9.2 '*Termination*'. You may terminate this License Agreement at any time by destroying all copies of the Software then in your possession and destroying all Documentation and associated materials, or returning the same to Barco or the appointed Barco reseller that sold or provided these to you. Barco may terminate this License Agreement, immediately or gradually in accordance with article 6 hereof, by informing you at any time if any user is in breach of any of the License Agreement's terms.

9.3 '*Consequences of Termination*'. All rights associated with the use of the Software and the acquisition of updates and upgrades cease once the License Agreement is terminated or expires. Termination or expiry of your license will not entitle you to any retroactive refund of current or past payments.

10. Other relevant terms

10.1 '*Personal Data*'. Whether or not Barco assumes the role of processor of personal data (as stated in the Product Specific EULA), you remain solely responsible for complying with all applicable data protection laws and for implementing and maintaining privacy protection and security measures (especially for components that you provide or control). Barco disclaims any liability for any data not provided by Barco, or any use of the Software outside the intended use as per this License Agreement or an applicable data processing annex.

10.2 '*Functional Information*'. Via the Software, Barco may gather technical information about (i) the functioning and the functionality of the products which are connected through the Software, and/or (ii) as provided by you or generated by your use of the Software ("Functional Information"). Barco may make use of such Functional Information for purposes of analytics, for developing and improving products and services, offering products and services to your organization and/or allowing third parties to access such Functional Information; based on the legitimate interest of Barco of evaluating the market, assessing and improving its products and conducting research and development. All knowhow, inventions and works derived by Barco from the Functional Information will be exclusively owned by Barco.

11. Final Clauses

11.1 '*Entire Agreement*'. This License Agreement is the only understanding and agreement between you and Barco for use of the Software. This License Agreement supersedes all other communications, understandings or agreements we had prior to this License Agreement (with the exception of any continuing confidentiality agreement).

11.2 '*Notices*'. Notices can be validly delivered through the DRM and alternatively or additionally to the parties' last known address.

11.3 '*Severability*'. This License Agreement shall not be altered, amended or varied, except by written agreement signed by its parties. If any provision of this License Agreement is determined to be illegal, void or unenforceable, or if any court of competent jurisdiction in any final decision so determines, this License Agreement shall continue in full force save that such provision shall be deemed to be deleted with effect from the date of such decision, or such earlier date, and shall be replaced by a provision which is acceptable by law and which embodies the intention of this License Agreement a close as possible.

11.4 '*Export*'. You acknowledge that this Software may be subject to U.S. or other governments' Export control laws and regulations. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use, and destination restrictions issued by the U.S. or other governments.

11.5 '*Survival*'. The provisions of articles 3, 5, 6, 7, 8, 10 and 11 will survive the termination of this License Agreement, howsoever caused, but this will not imply or create any continued right to use the Software after termination of this License Agreement.

11.6 '*Assignment*'. You are not allowed to assign this Agreement in part or in full to any third party without Barco's consent. Barco shall be entitled to assign all or any of Barco's obligations hereunder to a third party and/or any of Barco's Affiliates.

11.7 '*Law and Jurisdiction*'. The construction, validity and performance of this License Agreement shall be governed in all respects by the laws of Belgium, without recourse to its conflict of law principles. All disputes arising in any way out of or affecting this License Agreement shall be subject to the exclusive jurisdiction of the courts of Kortrijk (Belgium), without prejudice to enforcement of any judgment or order thereof in any other jurisdiction. The United Nations Convention on Contracts for the International Sale of Goods (the "Convention") shall not apply to this License Agreement, however, if the Convention is deemed by a court of competent jurisdiction to apply to this License Agreement, Barco shall not be liable for any claimed non-conformance of the Software under Article 35(2) of the Convention.

YOU HEREBY ACKNOWLEDGE TO HAVE READ, UNDERSTOOD AND ACCEPTED TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS LICENCE AGREEMENT AS INDICATED ABOVE

Barco ClickShare Product Specific Privacy policy

You are controller for personal data which are being processed via the Software. Therefore, you remain solely responsible for complying with all applicable data protection laws and for implementing and maintaining privacy protection and security measures (especially for components that you provide or control). Barco disclaims any liability in this regard. Barco created a specific privacy policy for the ClickShare software application for mobile devices, which describes the processing of personal data via this application (*http://www.barco.com/en/about-barco/legal/privacy-policy/clickshare-app*).

Via the Software, Barco may gather technical information about (i) the functioning and the functionality of the products which are connected through the Software, and/or (ii) as provided by you or generated by your use of the Software (“Functional Information”). Barco may make use of such Functional Information for purposes of analytics, for developing and improving products and services, offering products and services to your organization and/or allowing third parties to access such Functional Information; based on the legitimate interest of Barco of evaluating the market, assessing and improving its products and conducting research and development. All knowhow, inventions and works derived by Barco from the Functional Information will be exclusively owned by Barco.

Open Source Software provisions

This product contains software components released under an Open Source license. A copy of the source code is available on request by contacting your Barco customer support representative.

EACH SEPARATE OPEN SOURCE SOFTWARE COMPONENT AND ANY RELATED DOCUMENTATION ARE PROVIDED "AS IS"WITHOUT EXPRESS OR IMPLIED WARRANTY INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL THE COPYRIGHTHOLDER OR ANY OTHER CONTRIBUTOR BE LIABLE FOR DIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS OPEN SOURCE SOFTWARE. MORE INFORMATION/ DETAILS IS TO BE FOUND IN EACH SPECIFIC OPEN SOURCE LICENSE.

Copyright on each Open Source Software component belongs to the respective initial copyright holder, each additional contributor and/or their respective assignee (s), as may be identified in the respective documentation, source code, README file, or otherwise. You shall not remove or obscure or otherwise alter the respective copyrights.

You acknowledge living up to the conditions of each separate Open Source Software license.

In the development of the Software, the following Open Source Software components have been used:

PACKAGE	VERSION	SOURCE SITE
alsa-lib	1.1.7	ftp://ftp.alsa-project.org/pub/lib
alsa-utils	1.1.7	ftp://ftp.alsa-project.org/pub/utils
libsamplerate	0.1.9	http://www.mega-nerd.com/SRC
libsndfile	1.0.28	http://www.mega-nerd.com/libsndfile/files
ncurses	6.1	http://ftpmirror.gnu.org/ncurses
avahi	0.7	https://github.com/lathiat/avahi/releases/download/v0.7
dbus	1.12.16	https://dbus.freedesktop.org/releases/dbus
expat	2.2.7	http://downloads.sourceforge.net/project/expat/expat/2.2.7
libdaemon	0.14	http://0pointer.de/lennart/projects/libdaemon
libglib2	2.56.4	http://ftp.gnome.org/pub/gnome/sources/glib/2.56
libffi	v3.3-rc0	https://github.com/libffi/libffi/archive/v3.3-rc0

PACKAGE	VERSION	SOURCE SITE
pcre	8.42	https://ftp.pcre.org/pub/pcre
util-linux	2.33	https://cdn.kernel.org/pub/linux/utils/util-linux/v2.33
readline	8.0	http://ftpmirror.gnu.org/readline
libzlib	1.2.11	http://www.zlib.net
bc	1.06.95	http://alpha.gnu.org/gnu/bc
bluez5_utils	5.50	https://cdn.kernel.org/pub/linux/bluetooth
eudev	3.2.7	http://dev.gentoo.org/~blueness/eudev
kmod	25	https://cdn.kernel.org/pub/linux/utils/kernel/kmod
busybox	1.29.3	http://www.busybox.net/downloads
e2fsprogs	1.44.5	https://cdn.kernel.org/pub/linux/kernel/people/tytso/e2fsprogs/v1.44.5
i2c-tools	4.1	https://www.kernel.org/pub/software/utils/i2c-tools
ntp	4.2.8p13	https://www.eecis.udel.edu/~ntp/ntp_spool/ntp4/ntp-4.2
libevent	2.1.8-stable	https://github.com/libevent/libevent/releases/download/release-2.1.8-stable
libopenssl	1.1.1c	https://www.openssl.org/source
c-ares	1.15.0	http://c-ares.haxx.se/download
ca-certificates	20190110	http://snapshot.debian.org/archive/debian/20190513T145054Z/pool/main/c/ca-certificates
crda	4.14	https://git.kernel.org/pub/scm/linux/kernel/git/mcgrof/crda.git/snapshot
libgcrypt	1.8.4	https://gnupg.org/ftp/gcrypt/libgcrypt
libgpg-error	1.33	https://www.gnupg.org/ftp/gcrypt/libgpg-error
libnl	3.4.0	https://github.com/thom311/libnl/releases/download/libnl3_4_0
cryptsetup	2.0.6	https://cdn.kernel.org/pub/linux/utils/cryptsetup/v2.0
json-c	0.13.1	https://s3.amazonaws.com/json-c_releases/releases
lvm2	2.02.183	ftp://sources.redhat.com/pub/lvm2
libaio	0.3.111	https://releases.pagure.org/libaio
popt	1.16	http://rpm5.org/files/popt
devmem2	1	http://bootlin.com/pub/mirror
dhcp	4.3.6	http://ftp.isc.org/isc/dhcp/4.3.6
dnsmasq	2.79	http://thekelleys.org.uk/dnsmasq
dropbear	2018.76	https://matt.ucc.asn.au/dropbear/releases
ethtool	4.19	https://cdn.kernel.org/pub/software/network/ethtool
faad2	2.8.8	http://downloads.sourceforge.net/project/faac/faad2-src/faad2-2.8.0
ffmpeg	3.4.6	http://ffmpeg.org/releases

PACKAGE	VERSION	SOURCE SITE
fontconfig	2.13.1	http://fontconfig.org/release
freetype	2.9.1	http://download.savannah.gnu.org/releases/freetype
libpng	1.6.37	http://downloads.sourceforge.net/project/libpng/libpng16/1.6.37
lame	3.100	http://downloads.sourceforge.net/project/lame/lame/3.100
libvorbis	1.3.6	http://downloads.xiph.org/releases/vorbis
libogg	1.3.3	http://downloads.xiph.org/releases/ogg
opus	1.3.1	https://downloads.xiph.org/releases/opus
speex	1.2.0	https://downloads.xiph.org/releases/speex
file	5.36	ftp://ftp.astron.com/pub/file
imx-lib	3f777974c0-c146817e2ff5c-b0340ca66a1-f99e57	https://source.codeaurora.org/external/imx/imx-lib
kernel-module-imx-gpu-viv	bfa78-b095a892705-a09afe9514fc5-d236b3124d2	https://github.com/Freescale/kernel-module-imx-gpu-viv/archive/bfa78b095a892705a09afe9514fc5d236b3124d2
gnupg2	2.2.17	https://gnupg.org/ftp/gcrypt/gnupg
libassuan	2.5.2	ftp://ftp.gnupg.org/gcrypt/libassuan
libksba	1.3.5	ftp://ftp.gnupg.org/gcrypt/libksba
libnpth	1.6	https://www.gnupg.org/ftp/gcrypt/npth
libusb	1.0.22	https://github.com/libusb/libusb/releases/download/v1.0.22
sqlite	3280000	https://www.sqlite.org/2019
gssdp	1.0.2	http://ftp.gnome.org/pub/gnome/sources/gssdp/1.0
libsoup	2.62.3	http://ftp.gnome.org/pub/gnome/sources/libsoup/2.62
libxml2	2.9.9	http://xmlsoft.org/sources
gst1-plugins-bad	1.14.4	https://gstreamer.freedesktop.org/src/gst-plugins-bad
gst1-plugins-base	1.14.4	https://gstreamer.freedesktop.org/src/gst-plugins-base
gstreamer1	1.14.4	https://gstreamer.freedesktop.org/src/gstreamer
gst1-plugins-good	1.14.4	https://gstreamer.freedesktop.org/src/gst-plugins-good
pulseaudio	12.2	http://freedesktop.org/software/pulseaudio/releases
libtool	2.4.6	http://ftpmirror.gnu.org/libtool
hostapd	2.7	http://w1.fi/releases
input-event-daemon	v0.1.3	https://github.com/gandro/input-event-daemon/archive/v0.1.3
iperf	2.0.13	http://downloads.sourceforge.net/project/iperf2
iptables	1.8.2	https://netfilter.org/projects/iptables/files
iw	4.14	https://cdn.kernel.org/pub/software/network/iw

PACKAGE	VERSION	SOURCE SITE
libjpeg	9c	http://www.ijg.org/files
libarchive	3.3.3	http://www.libarchive.org/downloads
libbsd	0.10.0	https://libbsd.freedesktop.org/releases
libcurl	7.65.3	https://curl.haxx.se/download
libestr	0.1.10	http://libestr.adiscon.com/files/download
libevdev	1.6.0	http://www.freedesktop.org/software/libevdev
libfastjson	v0.99.8	https://github.com/rsyslog/libfastjson/archive/v0.99.8
libhttpparser	v2.9.0	https://github.com/nodejs/http-parser/archive/v2.9.0
libical	1.0.1	https://github.com/libical/libical/releases/download/v1.0.1
libid3tag	0.15.1b	http://downloads.sourceforge.net/project/mad/libid3tag/0.15.1b
libimxvpuapi	0.10.3	https://github.com/Freescale/libimxvpuapi/archive/0.10.3
libinput	1.12.5	http://www.freedesktop.org/software/libinput
mtdev	1.1.4	http://bitmath.org/code/mtdev
liblogging	1.0.6	http://download.rsyslog.com/liblogging
libmad	0.15.1b	http://downloads.sourceforge.net/project/mad/libmad/0.15.1b
libmpeg2	0.5.1	http://libmpeg2.sourceforge.net/files
libpciaccess	0.14	http://xorg.freedesktop.org/releases/individual/lib
libpthread-stubs	0.4	http://xcb.freedesktop.org/dist
libqrencode	4.0.0	http://fukuchi.org/works/qrencode
libsha1	0.3	https://github.com/dottedmag/libsha1/archive/0.3
libuv	v1.25.0	https://github.com/libuv/libuv/archive/v1.25.0
libzip	1.5.1	http://www.nih.at/libzip
lighttpd	1.4.53	http://download.lighttpd.net/lighttpd/releases-1.4.x
lm-sensors	V3-5-0	https://github.com/lm-sensors/lm-sensors/archive/V3-5-0
logrotate	3.13.0	https://github.com/logrotate/logrotate/archive/3.13.0
memtester	4.3.0	http://pyropus.ca/software/memtester/old-versions
monit	5.25.3	http://mmonit.com/monit/dist
netsnmp	5.8	https://downloads.sourceforge.net/project/net-snmp/net-snmp/5.8
nodejs	8.15.1	http://nodejs.org/dist/v8.15.1
pcre2	10.32	https://ftp.pcre.org/pub/pcre
php	7.3.9	http://www.php.net/distributions
protobuf	v2.6.1	https://github.com/google/protobuf/archive/v2.6.1
qt5base	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5declarative	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules

PACKAGE	VERSION	SOURCE SITE
qt5xmlpatterns	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5imageformats	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5multimedia	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5quickcontrols	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5svg	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
qt5websockets	5.12.4	https://download.qt.io/archive/qt/5.12/5.12.4/submodules
rsyslog	8.22.0	http://rsyslog.com/files/download/rsyslog
tslib	1.20	https://github.com/libts/tslib/releases/download/1.20
tzdata	2018e	http://www.iana.org/time-zones/repository/releases
wireless-regdb	2019.06.03	https://cdn.kernel.org/pub/software/network/wireless-regdb
wireless_tools	30.pre9	https://hewlettpackard.github.io/wireless-tools
wpa_supplicant	2.7	http://w1.fi/releases
arphic-uming-fonts	20080216	http://archive.ubuntu.com/ubuntu/pool/main/t/ttf-arphic-uming
dejavu-fonts	2.34	http://downloads.sourceforge.net/project/dejavu/dejavu/2.34
sazanami-fonts	20040629	http://sourceforge.jp/projects/efont/downloads/10087
splashutils	1.5.4.4	http://dev.gentoo.org/~spock/projects/gensplash/archive
unfonts	1.0	http://kldp.net/frs/download.php/1425
uboot	2014.04	http://git.freescale.com/git/cgit.cgi/imx/uboot-imx.git
rockbox	v3.10	https://github.com/Rockbox/rockbox/tree/v3.10
gstreamer-imx	0.12.3	https://github.com/Freescale/gstreamer-imx/releases
libcap	2.25	https://www.kernel.org/pub/linux/libs/security/linux-privs/libcap2
mtd	1.5.2	ftp://ftp.infradead.org/pub/mtd-utils
procps-ng	3.3.12	http://downloads.sourceforge.net/project/procps-ng/Production
strace	4.15	http://downloads.sourceforge.net/project/strace/strace/4.15
hidapi	0.5.2	https://github.com/signal11/hidapi
linux	3.1.0	https://mirrors.edge.kernel.org/pub/linux/kernel/v3.x/
linux	4.1.15	https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/
rscode	1.3	https://sourceforge.net/projects/rscode/files/rscode/

EN55032-CISPR32 Class B ITE (Information Technology Equipment)

This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

If this equipment does cause interference to radio or television reception, the user may try to correct the interference by one or more of the following measures :

- Re-orientation of the receiving antenna for the radio or television.
- Relocate the equipment with respect to the receiver.

- Plug the equipment into a different outlet so that the equipment and receiver are on different branch circuits.
- Fasten cables connectors to the equipment by mounting screws.

Federal Communication Commission Interference Statement

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

You may also find helpful the following booklet, prepared by the FCC: "How to Identify and Resolve Radio-TV Interference Problems." This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402.

Changes and Modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commissions rules.

In order to maintain compliance with FCC regulations shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio & television reception.

FCC RF Radiation Exposure Statement: This device is capable of operating in 802.11a mode. For 802.11a devices operating in the frequency range of 5.15 - 5.25 GHz, they are restricted for indoor operations to reduce any potential harmful interference for Mobile Satellite Services (MSS) in the US. Wi-Fi Access Points that are capable of allowing your device to operate in 802.11a mode (5 .15 - 5.25 GHz band) are optimized for indoor use only. If your Wi-Fi network is capable of operating in this mode, please restrict your Wi-Fi use indoors to not violate federal regulations to protect Mobile Satellite Services.

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Base Unit FCC ID: 2AAED-R9861520

Button FCC ID (model R9861500D01): 2AAED-R9861500D01

Button FCC ID (model R9861500D01C): 2AAED-R9861500D01

ClickShare Button 2AAED-R9861500D01 has been tested and meets the FCC RF exposure guidelines. The maximum SAR value reported is 0.915W/kg.

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada licence-exempt RSS standard (s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the Barco Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Barco Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

Caution: Exposure to Radio Frequency Radiation.

1. To comply with the Canadian RF exposure compliance requirements, this device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.
2. To comply with RSS 102 RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Base Unit IC: IC: 9393B-R9861520

Button IC (model R9861500D01): 9393B-R9861500D01

Button IC (model R9861500D01C): 9393B-R9861500D01

IC Antenna statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter 9393B-R9861520 has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Type: Dipole

Maximum Peak Gain: 2 dBi

Impedance: 50

Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l'appareil de sans fil Barco est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l'appareil de sans fil Barco de façon à minimiser les contacts humains lors du fonctionnement normal.

Avertissement: L'exposition aux rayonnements fréquences radio

1. Pour se conformer aux exigences de conformité RF canadienne l'exposition, cet appareil et son antenne ne doivent pas être co-localisés ou fonctionnant en conjonction avec une autre antenne ou transmetteur.
2. Pour se conformer aux exigences de conformité CNR 102 RF exposition, une distance de séparation d'au moins 20 cm doit être maintenue entre l'antenne de cet appareil et toutes les personnes.

IC Unité de Base: 9393B-R9861520

IC Button (modèle R9861500D01): 9393B-R9861500D01

IC Button (model R9861500D01C): 9393B-R9861500D01

Déclaration d'antenne d'Industrie Canada (IC)

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p. i. r. e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio 9393B-R9861520 a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Type: Dipole

Gain maximum: 2 dBi

Impédance: 50

Table of contents

1 Introduction to the Installation Guide 19
1.1 Documentation 20
1.2 Symbols and fonts 20

2 CSE-200 Specifications 23
2.1 About the CSE-200 24
2.2 CSE-200 specifications 25
2.3 About the Base Unit 26
2.4 About the Button 29
2.5 Mobile Device Support 30
2.6 Ports used by the ClickShare Base Unit 31

3 Getting started 33
3.1 Environmental Condition Check 34
3.2 Basic Workflow 34

4 CSE-200 Installation 35
4.1 Installation methods for the Base Unit 36
4.2 Table mounting 36
4.3 Wall mounting 36
4.4 Recommendations about antenna placement and orientation 37
4.5 Video signal connections to the Base Unit 38
4.6 Audio connection 38
4.7 LAN connection 39
4.8 Out-of-the-box use 39
4.9 Out-of-the-box use with Ethernet link 40
4.10 Integration in the Enterprise network 41
4.11 Integration in a dedicated Enterprise network 42
4.12 Power connection 44

5 Preparing the Buttons 47
5.1 Pairing 48
5.2 ClickShare Extension Pack 49
5.3 ClickShare Extension Pack installer 49
5.4 ClickShare Windows Certified driver 50
5.5 ClickShare Desktop app 51

6 CSE-200 Configurator 53
6.1 Accessing the Configurator 55
6.2 ClickShare Configuration Wizard 58
6.3 On-Screen Language and Text Size 61
6.4 Meeting room information 63
6.5 Personalisation, wallpaper 64
6.6 Personalisation, Personalized wallpaper 65
6.7 Manage configuration files 67
6.8 Display setup 69
6.9 Audio settings 69
6.10 Wi-Fi settings 70
6.11 LAN settings 74
6.12 LAN Settings, Wired Authentication 76
6.13 LAN Settings, EAP-TLS security mode 77
6.14 LAN Settings, EAP-TTLS security mode 79
6.15 Services, mobile devices 80
6.16 Service, ClickShare API, remote control via API 82
6.17 XMS Server Integration 82
6.18 Services, SNMP 83
6.19 Services, Remote Button Pairing 84
6.20 Security, security level 84
6.21 Security, passwords 85
6.22 Security, HTTP Encryption 86
6.23 Status information Base Unit 89
6.24 Date & Time setup, manually 89
6.25 Date & Time setup, time server 91
6.26 Energy savers 92
6.27 Buttons 93
6.28 Buttons, External access point 93
6.29 Buttons, External access point, mode EAP-TLS 94
6.30 Buttons, External access point, mode EAP-TTLS 95
6.31 Buttons, External access point, mode PEAP 96
6.32 Buttons, External access point, mode WPA2-PSK 97
6.33 Firmware Update 98
6.34 Support & Updates, Troubleshoot, log settings 99
6.35 Factory defaults 100

7 Firmware updates 103
7.1 Firmware update 104

8 Troubleshooting 105
8.1 Troubleshooting list 106

9 Environmental information 109
9.1 Disposal information 110
9.2 Rohs compliance 110
9.3 Importers contact information 112

Introduction to the Installation Guide

1

1.1 Documentation 20
1.2 Symbols and fonts 20

1.1 Documentation

This guide

Partnumber	Description	Level
R5900023	Installation Guide	Installation engineer

This installation guide explains how to install your CSE-200 in a meeting room, It explains also how to make everything operational. It provides detailed information on how to configure your CSE-200.

Available System documentation

This guide is part of the documentation set describing the CSE-200 product.

Guide	Article number
User Guide	R5900025
Installation Guide	R5900023
Safety Guide	R5900032
Service Guide	R5900027
Button Guide	R5900007
Recycling Manual	R5900029
API Guide	R5900018

A printed copy of the Safety Guide is included in the CSE-200 box at purchase.

Always check for the latest version of the manual on *www.barco.com/clickshare*

Depending on the CSE-200 version, some graphics might be different to the ones used in this manual. This however does not have any effect on the functionality.

1.2 Symbols and fonts

Symbol overview

The following icons are used in the manual :

	Caution
	Warning
	Info, term definition. General info about the term
	Note: gives extra information about the described subject
	Tip: gives extra advice about the described subject

Font overview

- Buttons are indicated in bold, e.g. **OK**.
- Menu items are indicated in *italic*.
- Step related notes, tips, warnings or cautions are printed in *italic*.

- Procedure related notes, tips, warnings or cautions are printed in **bold** between 2 lines preceded by the corresponding icon.

CSE-200 Specifications

2

2.1 About the CSE-200

CSE-200 sets

CSE-200 makes connecting to the meeting room's video system a matter of clicking a Button.

This CSE-200 not only helps the presenter get the presentation on-screen in a second, but it also allows the other people in the meeting to participate more actively. The result is enhanced meeting efficiency and better decision-making.

At the moment 4 different sets are available on the market. Each set is sold in its specific region and it can only be used in that specific region because of Wi-Fi regulations.

Components CSE-200 set

A standard CSE-200 set consists of a Base Unit and 2 Buttons. Depending on the location where you buy the product, the software of the Base Unit is different. If needed, you can buy additional Buttons and a tray to store the Buttons.

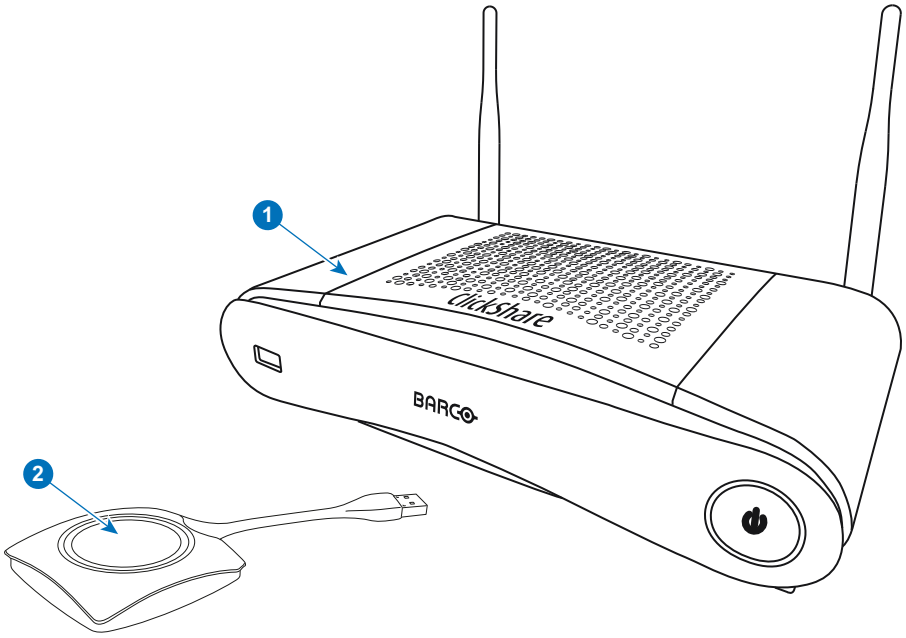


Image 2–1

1	Base Unit
2	Button

Accessories included

Depending on the country where you buy the product, the following regionalized accessories are also included in the CSE-200 box.

Products	Contains	Accessories included
R9861521xx[2]	• R9861521 • 1x R9861500D01	• DC adapter with AC clips type A, C, G, I[3] • Printed safety manual
R9861500D01	1x R9861500D01	
R9861500D01C	1x R9861500D01C	

Contact your local sales representative for the correct regional variant to be used in your country.

2: xx=EU, CN, NA, ZH,
3: Included AC clips can be different according to the region

2.2 CSE-200 specifications

Base Unit

Dimensions (HxWxD)	205mm x 115mm x 45mm (excl. antennas) / 8.1” x 4.5” x 1.8” 205mm x 150mm x 135mm (incl. antennas) / 8.1" x 5.9" x 5.3"
Power supply	Standard 110/220 V AC plug or Power over Ethernet (PoE Plus)
Power consumption	Operation: 6W (typical) / 18W (max) Standby: 2.6W (ECO standby) / 0.4W (Deep standby)
Weight	600g / 1.32lbs
Operating system	Windows 7/8/8.1/10 32 & 64 bit macOS 10.14/10.15 (Catalina) Android 9 & 10 (ClickShare app) iOS 11, 12 & 13 (ClickShare app)
Video outputs	1x HDMI 1.2
Output resolution	1920x1080 @60Hz
Audio	Via HDMI, analog via Audio Jack 3.5mm, S/PDIF
AirPlay Support	iOS 11, 12 & 13 / macOS 10.14, 10.15
Google Cast Support	Android 9, 10
Frame rate	Up to 30fps*
Number of sources simultaneous on screen	2
Number of simultaneous connections	16
iPad, iPhone and Android compatibility	Sharing of documents, browser, camera for both Android and iOS devices via ClickShare app or using AirPlay / Google Cast
Extended desktop	Available for Windows, requires ClickShare Extension Pack.
Authentication protocol	WPA2-PSK in stand-alone mode WPA2-PSK or IEEE 802.1X using the ClickShare Button in network integration mode
Wireless transmission protocol	IEEE 802.11 a/g/n
Reach	Adjustable with signal strength modulation; max. 30m (100 ft) between ClickShare Button and ClickShare Base Unit
Frequency band	2.4 GHZ and 5 GHz (DFS channels not supported)
Connections	1x Ethernet LAN 100Mbit 2x (back) + 1x (front) USB Audio analog line out on mini jack socket (3.5mm), digital S/PDIF
Noise Level	Fanless
Temperature range	Operating: 0°C to +40°C (+32°F to +104°F) Max: 35°C (95°F) at 3000m Storage: -20°C to +60°C (-4°F to +140°F)
Humidity	Storage: 0 to 90% relative humidity, non-condensing

	Operation: 0 to 85% relative humidity, non-condensing
Anti-theft system	Kensington lock
Certifications	FCC/CE
Warranty	3 years standard Possible to extend to 5 years
***Note**	*In optimal WiFi conditions with minimal WiFi interference and as measured during our quality validation. Check Network Deployment Guide for more info on WiFi optimisation and ideal configuration depending on your network environment.

Button

Weight	75 g/0.165 lb
Frequency band	2.4 GHZ and 5 GHz
Wireless transmission protocol	IEEE 802.11 a/b/g/n
Authentication protocol	WPA2-PSK in stand alone mode WPA2-PSK or IEEE 802.1X in network integration mode
Dimensions (HxWxD)	16.3 mm x 59.3 mm x 162.52 mm / 0.64” x 2.335” x 6.398”
Power consumption	Powered over USB-C 5V DC 350mA Typical 500mA Maximum

2.3 About the Base Unit

Base Unit
The Base Unit receives the wireless input from the Buttons and controls the content of the meeting room display and the sound of the meeting room's audio system.
The Base Unit can be installed in two different ways.

Front and Top layout of the Base Unit

At the front of the Base Unit you can find a power button and a USB Type-A port. Status LED ring is mounted around the standby button of the Base Unit.

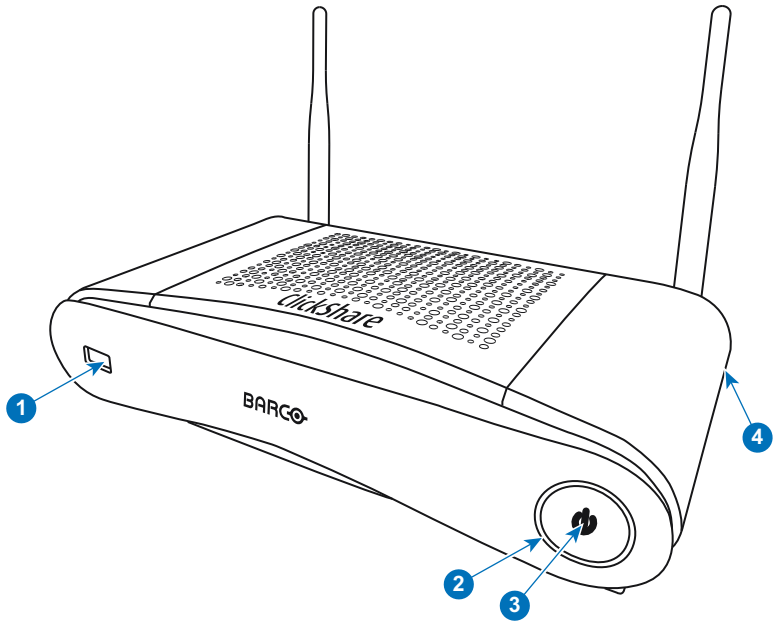


Image 2–2 Front panel Base Unit

1	USB Type-A port
2	Status LED ring
3	Standby Button
4	Kensington lock

USB port

The USB port is used to update the soft- and firmware of both the Base Unit and the Buttons. See also “Firmware update”, page 104.

When plugging in the Button into the Base Unit, the Button is paired to the Base Unit. The Base Unit checks whether the Button's software and firmware are up to date. If not, the Base Unit updates the software and/or firmware.

To update the Base Unit software, download the latest version of the software from the Barco website. Copy the file on a USB stick and plug it into the USB port of the Base Unit. Follow the progress and instructions on the display.

Status LED ring

The color of the LED at the front of the Base Unit give information on the status of the system.

LEDs behavior	Explanation
static red	• receiving content from the Buttons and streaming towards the display. • pairing and software update of the Button is done. You can now unplug the Button from the Base Unit. • during the first phase of the Base Unit boot process.
blinking white	• system is starting up (during the second phase) • Button pairing is in progress • software update of the Base Unit
breathing white	• ECO standby mode
static white	• awake and ready (i.e. showing the welcome message on the display) • pairing is done

LEDs behavior	Explanation
red blinking	• an error occurred
dark	• deep standby/off

Standby button

The button at the front of the Base Unit has a standby function once the Base Unit is powered

- When the system is in normal operational mode, a push makes the system goes to a pre-defined standby mode.
- When the system is in a standby mode, a push triggers the system to start up and to go to normal operational mode.

Back layout of the Base Unit

The connection panel is situated at the back of the Base Unit.

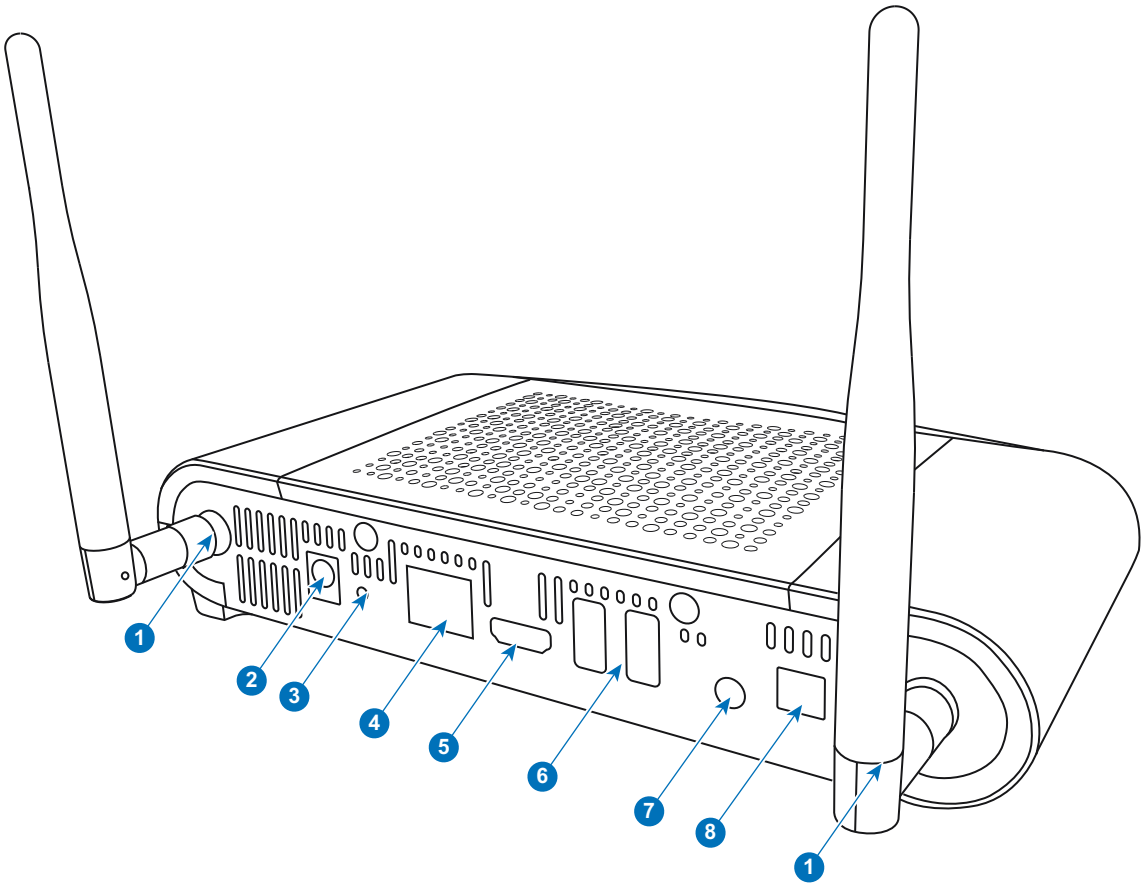


Image 2–3 Backside Base Unit

1	Fixture points for the antenna
2	Power connection
3	Reset
4	LAN Ethernet connection
5	HDMI connector
6	USB Type-A port
7	Analog Audio out
8	Digital Audio out

Mechanical fixture points

The mechanical fixture points are located at the bottom of the Base Unit

Antenna

Two antennas are included in the CSE-200 box. To avoid damage during transport, they are not pre-mounted.

The antennas can rotate for a better wireless connection.

Usage of antennas other than the ones provided with the unit are allowed within the restrictions on usage of other antennas defined by local regulations. Barco does not take responsibility for damage or disturbance of other devices that may be caused by using a different antenna. The use of an active power amplifier is not allowed.

Antenna type : Dipole

Gain : Maximum 2 dBi peak gain in 2.4GHz and 5Ghz band

Bottom layout of the Base Unit

The serial number label containing the Barco part number, the revision number, production date (week-year) and the serial number.

The product label with the applicable certification logos.

The product label contains:

- the Barco logo
- the product name
- the Barco part number
- the power rating
- markings for applicable standards (CE, CCC, UL, ...)
- markings for waste regulation
- “Made in ...”

Bluetooth

Bluetooth functionality is currently not available and Bluetooth signal is disabled.

2.4 About the Button

Button
A Button toggles the sharing of the individual PC or MAC screen on the meeting screen.

Button layout

A Button consists of three main components.

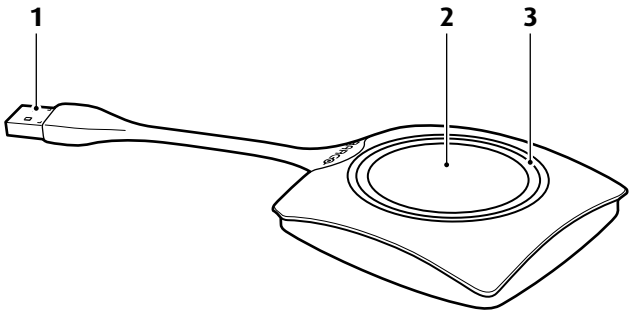


Image 2–4 Button layout

1	USB connector
2	Button
3	LED ring

USB connector

Using the USB connector the Button can be plugged into a laptop (for sharing your screen) or the Base Unit (for pairing the Button to the Base Unit or updating its software). Button R9861500D1 has a USB Type-A connector, Button R9861500D1C has a USB Type-C™ connector. Depending on the type of USB port on your laptop or on the Base Unit a convertor must be use.

Button

Click the Button to display the content of the laptop's screen on the meeting room display. Clicking the Button during the meeting will toggle the sharing of the screen.

LED ring

The LED ring indicates the current status of your ClickShare.

LEDs behavior	Explanation
white blinking	• the Button is plugged in the laptop and initializing or waiting for the user to start the ClickShare application. • pairing/software update of the Button in the Base Unit is in progress.
static white	• ClickShare is ready to start sharing your screen. • pairing is done. You can now unplug the Button from the Base Unit.
static red	• sharing your screen with the display[4]. • pairing and software update is done. You can now unplug the Button from the Base Unit.
red blinking	• an error occurred.
off (no light)	• the Button is not or not properly inserted into the USB port. • the Button might be defective. • the USB port or computer might be defective.

Button label

The label at the bottom of the Button contains:

- the Barco logo
- the Barco part number
- the serial number
- the revision number
- markings for applicable standards
- markings for waste regulation
- “Made in...”

Handle the Button cable with care. Rough handling might cause defects.

2.5 Mobile Device Support

Overview

The below list of Apps are supported by ClickShare and can be installed on your mobile device from Google Play or Apple App Store.

Before you can use your mobile device with ClickShare, you have to connect the mobile device Wi-Fi with the ClickShare Base Unit Wi-Fi. Follow the instructions as given in your mobile device user guide.

4: While sharing content, the laptop will not go to standby. Once sharing is stopped, the laptop will again be capable of going to standly.

App	Used on	Logo
ClickShare App	iOS Android	

2.6 Ports used by the ClickShare Base Unit

Overview

Sender		CSE-200 Base Unit
ClickShare Button	TCP	6541; 6542; 6543; 6544; 6545
	UDP	514
ClickShare Apps for Windows, MacOS, iOS and Android	TCP	6541; 6542; 6543; 6544; 6545
	UDP	5353
ClickShare Configurator	TCP	80; 443
ClickShare REST API & XMS	TCP	4000; 4001
Airplay	TCP	4100-4200; 7000; 7100; 47000
	UDP	4100-4200; 5353
Google Cast	TCP	8008; 8009; 9080
	UDP	1900; 32768:61000[5]
Auto-update	TCP	80; 443
Button Manager	TCP	6546

If Proxy settings are enabled in the Configurator for auto-update functionality, additional ports may be used.

5: Google Cast will pick a random UDP port above 32768 to facilitate video streaming

3 Getting started

3.1 Environmental Condition Check 34
3.2 Basic Workflow 34

3.1 Environmental Condition Check

Environment condition check

For installations in environments where the device is subject to excessive dust, then it is highly advisable and desirable to have this dust removed prior to it reaching the device clean air supply. Devices or structures to extract or shield excessive dust well away from the device are a prerequisite; if this is not a feasible solution then measures to relocate the device to a clean air environment should be considered.

It is the customer's responsibility to ensure at all times that the device is protected from the harmful effects of hostile airborne particles in the environment of the device. The manufacturer reserves the right to refuse repair if a device has been subject to negligence, abandon or improper use.

Ambient temperature conditions

Max. ambient temperature : +40°C or 104°F

Min. ambient temperature: +0°C or 32°F

Storage temperature: -10°C to +60°C (14°F to 140°F)

Humidity Conditions

Storage: 0 to 90% relative humidity, non-condensing

Operation: 0 to 85% relative humidity, non-condensing

Environment

Do not install the device in a site near heat sources such as radiators or air ducts, or in a place subject to direct sunlight, excessive dust or humidity. Be aware that room heat rises to the ceiling; check that temperature near the installation site is not excessive.

3.2 Basic Workflow

Before using CSE-200

1. Unpack the ClickShare components and accessories from the box.

   For a detailed overview of the content of the CSE-200 box, see “*About the CSE-200*”, page 24.
2. Install the Base Unit in the meeting room using one of the 2 possible installation methods.

   For more information on the installing procedures, see “*CSE-200 Installation*”, page 35
3. Connect the video signal between the Base Unit and the display.
4. Connect the audio from the Base Unit to the meeting room's sound system (only required for audio via jack or SPDIF).
5. If configuration via a network is needed, connect a network cable between the Base Unit and the local network (if not yet done to power the Base Unit).
6. Connect the Base Unit to the mains power (optional if Ethernet supports PoE+).

   For more information see “*Power connection*”, page 44,
7. If desired, configure CSE-200 via the Configurator.

   For more information on the different ways to configure CSE-200, see “*CSE-200 Configurator*”, page 53

For more information on using CSE-200, refer to the CSE-200 User Guide. This manual can be found on Barco's website www.barco.com/clickshare.

CSE-200 Installation 4

4.1 Installation methods for the Base Unit 36
4.2 Table mounting 36
4.3 Wall mounting 36
4.4 Recommendations about antenna placement and orientation 37
4.5 Video signal connections to the Base Unit 38
4.6 Audio connection 38
4.7 LAN connection 39
4.8 Out-of-the-box use 39
4.9 Out-of-the-box use with Ethernet link 40
4.10 Integration in the Enterprise network 41
4.11 Integration in a dedicated Enterprise network 42
4.12 Power connection 44

4.1 Installation methods for the Base Unit

For optimal performance, install the Base Unit close to the display and avoid obstacles between the Base Unit and the Buttons.

Make sure not to install the Base Unit in a metal enclosure.

Introduction to the installation methods

The Base Unit can be installed in different ways in a meeting room.

- Table mount
- Wall mount

A Kensington lock is foreseen on one side of the Base Unit.

WARNING: Ceiling mount is not allowed !

Standalone or network integration

The Base Unit can be use as standalone unit or integrated in a corporate network.

- Out-of-the-box use
- Out-of-the-box use with Ethernet link
- Integration in the Enterprise network
- Integration in a dedicated Enterprise network

4.2 Table mounting

Overview

Put the Base Unit directly on the meeting room table.

The total weight of the Base Unit is 600 g.

4.3 Wall mounting

About wall mounting

No mounting bracket is needed to install the Base Unit on the wall. The Base Unit can be mounted in any position on the wall, but it is preferred to mount it with the connections downwards.

The total weight of the Base Unit is 600 g.

Required tools

- a drill (type of drill depends on the type of wall)
- Screwdriver (depending on the used screws)

Required parts

- 2 mounting screws, maximum head diameter of 6.5 mm
- 2 plugs

How to install

1. Drill two holes in the wall or ceiling as indicated on the drawing.

   Horizontal distance : 162 mm,

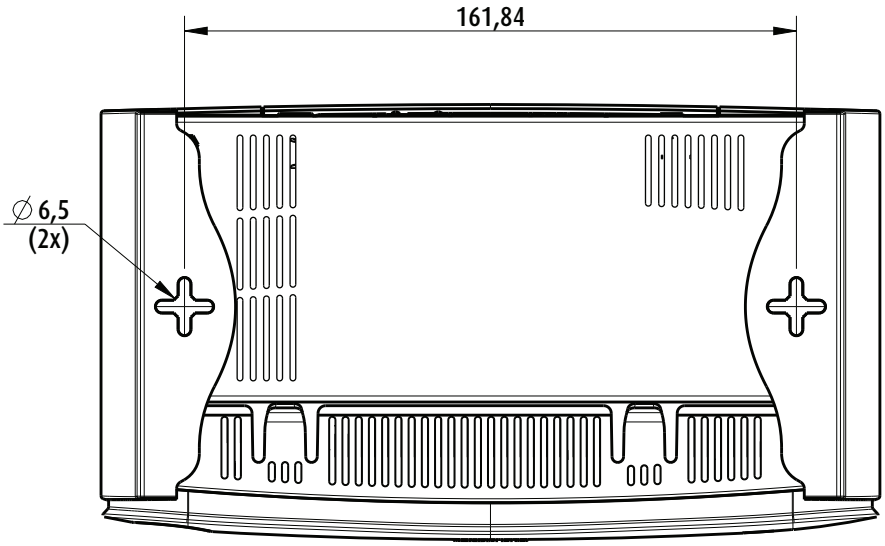


Image 4–1 Mounting holes

2. Insert a plug in each hole (if needed, depends on the wall or ceiling type) and drive in 2 screws. Do not drive in the screws completely.

   Note: Mounting screws and plugs are not included in the CSE-200 box . The type of screws and plugs depend on the type of wall (stone, wood, plasterboard, ...) you are mounting the Base Unit to. Make sure the head of the screw is not larger than the hole in the bottom plate of the Base Unit (< 6.5 mm).

3. Hook the Base Unit on both screw heads and slide the Base Unit downwards until it is fixed.

4.4 Recommendations about antenna placement and orientation

Antenna placement rules

- The antennas should be oriented vertically, so perpendicular to the ceiling and parallel to the walls.
- 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 15 cm (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 result in performance degradation.
- Due to the particular radio pattern of the dipole antennas, the antennas should not be placed just above potential positions of ClickShare users. As a result, the advised position for the antennas is at the side of the meeting room.

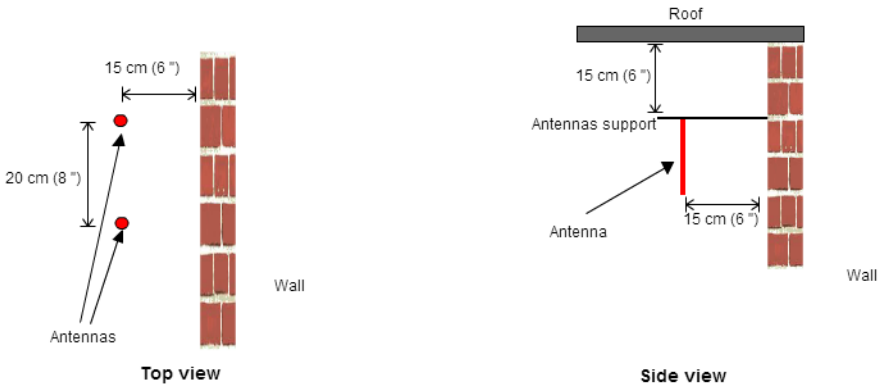


Image 4–2 Closer view of antennas installation in the meeting room

4.5 Video signal connections to the Base Unit

About Video signal connection

A single screen can be connected to the Base Unit.

To connect a display, an HDMI connection should be made between the Base Unit and the display.

To connect

1. Connect the Base Unit to the display using a display cable.

   Note: No display cables are included in the ClickShare box at purchase.

   When setting up a display configuration, connect the HDMI cable to the display. When necessary, use an adapter piece to connect to a display port or a DVI port on the display side.

Image 4–3 Display connection

4.6 Audio connection

About audio

The ClickShare Button captures the audio output of the user's laptop and sends it to the Base Unit together with the video signal. The audio will be output at line levels from the mini jack socket (3.5mm), TOSLINK socket and via the HDMI connector.

It is up to the user to decide whether or not to send the audio signal together with the video signal. The user can decide this by using the same tools as he would to control the laptop's speakers or a headphone: the audio controls of the operating system (eg for Windows: Control Panel > Sounds and audio devices) or the physical buttons on the keyboard of their laptop (mute/unmute, lower volume, higher volume).

There will be synchronization between the audio and video signal.

Audio via HDMI

When your display is connected via HDMI and it supports audio, a separate audio connection is not necessary. The audio signal is sent together with the video signal to the display.

How to connect separate audio

1. When using the analog output, connect an audio cable with mini jack (3.5mm) into the analog audio output of the Base Unit.

   When using the digital output, connect an fibre optical cable with TOSLINK connector into the digital audio output of the Base Unit.

2. Connect the other side to the meeting room's sound system.

Audio output needs to be selected in the Configurator, for more info, see "*Audio settings*", page 69.

Sound is not sent out

In some Windows environments sound is not sent out. This can be solved as follow:

1. Right click on the sound icon in the system tray and select *Playback devices*. The *Sound* window opens.
2. Select Speakers ClickShare, select *Set default* and click **Apply**.

4.7 LAN connection

About LAN connection

The Base Unit can be connected to a local network or directly to a laptop. For normal operation, a LAN connection is not necessary.

Maximum allowed LAN speed: 100 Mbit

The LAN connection can be used:

- to configure your CSE-200 unit
- to update the software
- for maintenance purposes
- for network integration of your CSE-200 unit

How to connect

1. Insert a network cable with RJ-45 connector into the LAN port.
2. Connect the other side to a LAN.

4.8 Out-of-the-box use

Overview

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 with their mobile devices using Airplay or Google Cast.

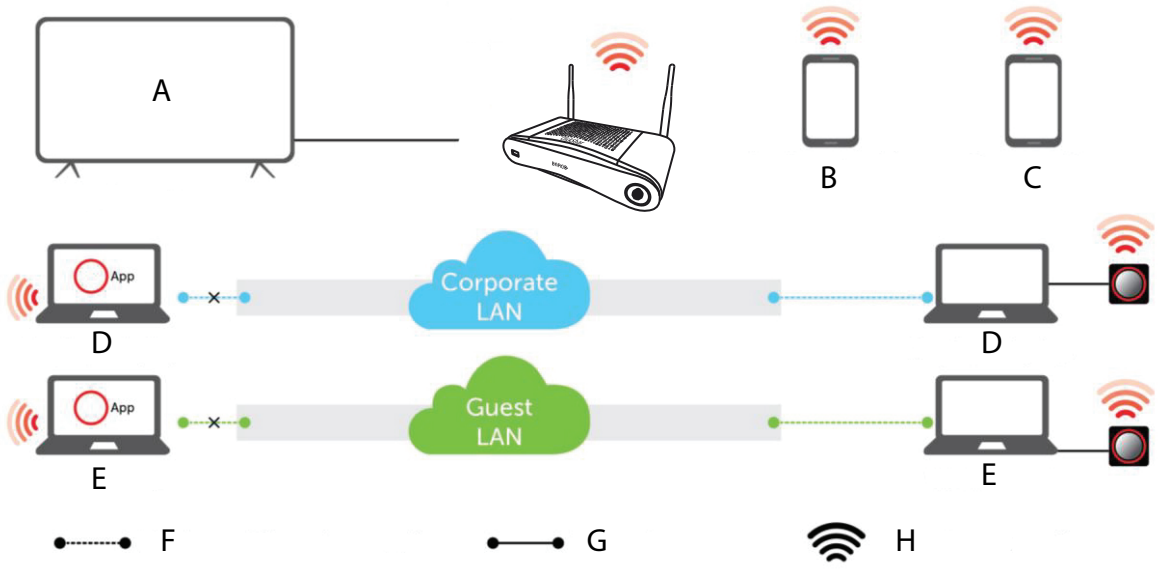


Image 4–4 Out-of-the-Box use

A Meeting room screen
B Employee mobile
C Guest mobile
D Employee laptop
E Guest laptop
F Wireless or Ethernet connection
G Ethernet connection
H Wireless connection

Note: Using a ClickShare Button allows you to stay connected to the internet. Using the ClickShare App, 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.

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.

4.9 Out-of-the-box use with Ethernet link

Overview

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 and employee mobile devices using Airplay or Google Cast can connect via the corporate LAN.

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.

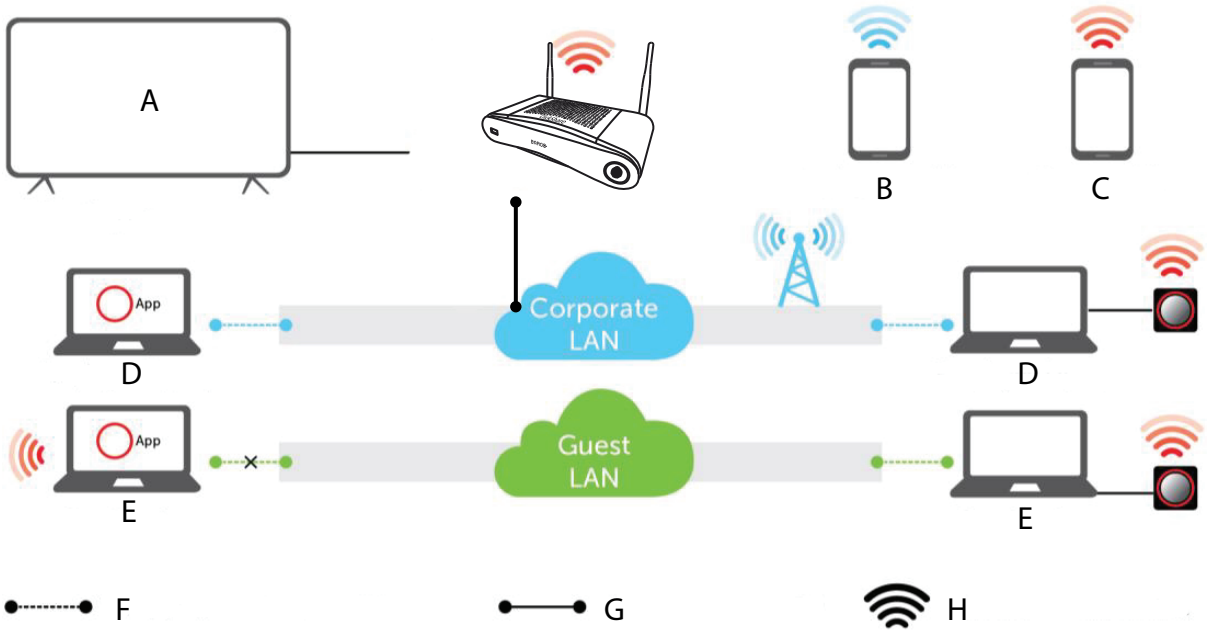


Image 4–5 Out-of-the-Box use with Ethernet link

A Meeting room screen
B Employee mobile
C Guest mobile
D Employee laptop
E Guest laptop
F Wireless or Ethernet connection
G Ethernet connection
H Wireless connection

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.

4.10 Integration in the Enterprise network

Overview

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 typically disabled and all traffic from the Button(s), the ClickShare App, Airplay, Google Cast and Miracast 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 (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.

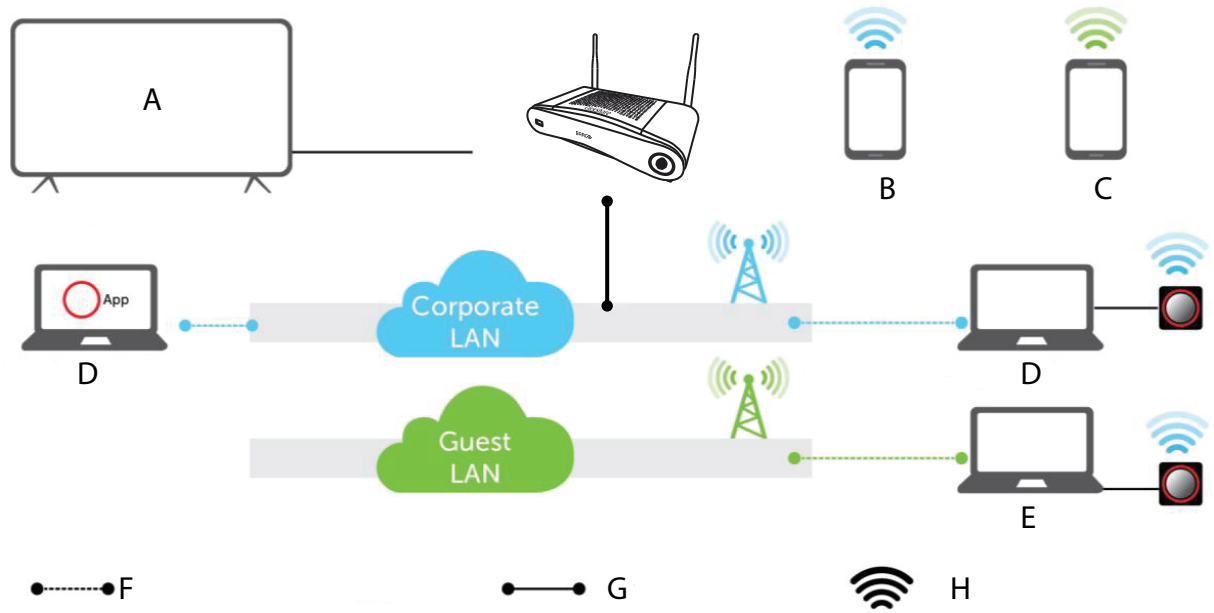


Image 4–6 Enterprise network integration

A Meeting room screen
B Employee mobile
C Guest mobile
D Employee laptop
E Guest laptop
F Wireless or Ethernet connection
G Ethernet connection
H Wireless connection

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 ClickShare configurator or via XMS.
- Improved Wi-Fi coverage for theButtons and BYOD[6] 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. When the Base Unit Wi-Fi is enabled, direct connections to the Base Unit are also possible.

How to setup via the Configurator

1. Connect the Base Unit and browse to the *ClickShare Configurator* and log in.
2. Select *Button* in the *System* menu and click **Edit settings**.

6: Bring your own device

Select *External Access Point* from the drop down menu and select the preferred authentication mode and fill out the details.

Click **Save Changes**. For more information, see “*Buttons*”, page 93

3. Pair the Buttons again with the Base Unit.
4. Optionally the Base Unit’s Wi-Fi can be set to Access Point or can be set to Off. For more info, “Wi-Fi settings”, page 70

Setup via XMS

1. Log in to XMS and go to the *Base Units* tab.
2. In the device list select the Unit(s) for deploying network integration mode and click **Edit** in the top right menu..
3. Browse to *System* > *Button Connects To* in the configurator.
4. Select *External Access Point* from the drop-down menu.
5. Select the preferred authentication mode and fill out the details.
6. Click **Save Changes** when finished.
7. Re-pair the ClickShare Buttons with the updated Base Unit(s) to apply the new configuration

   For more detailed information on how to use XMS, consult the XMS user guide.

4.11 Integration in a dedicated Enterprise network

Overview

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 typically disabled. Corporate users as well as guests share directly via the ClickShare Button, via the ClickShare App and with their mobile devices using Airplay, Google Cast or Miracast 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 App 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.

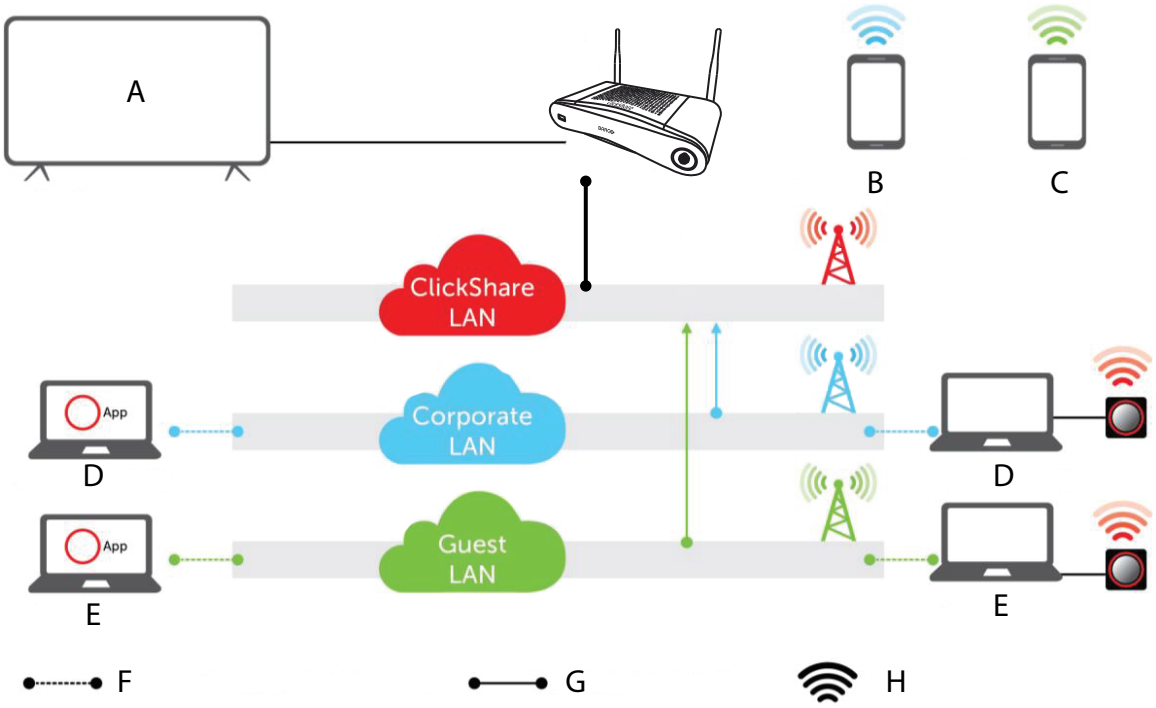


Image 4–7 Dedicated enterprise network

A Meeting room screen
B Employee mobile
C Guest mobile
D Employee laptop
E Guest laptop
F Wireless or Ethernet connection
G Ethernet connection
H Wireless connection

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.

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.

How to setup via the Configurator

1. Connect the Base Unit and browse to the *ClickShare Configurator* and log in.
2. Select *Button* in the *System* menu and click **Edit settings**.

   Select *External Access Point* from the drop down menu and select the preferred authentication mode and fill out the details.

   Click **Save Changes**. For more information, see “*Buttons*”, page 93
3. Pair the Buttons again with the Base Unit.
4. Optionally the Base Unit’s Wi-Fi can be set to Access Point or can be set to Off. For more info, “Wi-Fi settings”, page 70

Setup via XMS

1. Log in to XMS and go to the *Base Units* tab.

2. In the device list select the Unit(s) for deploying network integration mode and click **Edit** in the top right menu..
3. Browse to *System* > *Button Connects To* in the configurator.
4. Select *External Access Point* from the drop-down menu.
5. Select the preferred authentication mode and fill out the details.
6. Click **Save Changes** when finished.
7. Re-pair the ClickShare Buttons with the updated Base Unit(s) to apply the new configuration

   For more detailed information on how to use XMS, consult the XMS user guide.

4.12 Power connection

About power

This product is intended to be supplied by a UL Listed Power Unit marked “Class 2” or “LPS” or “Limited Power Source” with output rated 12 VDC 1.5A min or Power over Ethernet (PoE) Plus IEEE802.3at Type 2 compliant Power Sourcing Equipment (PSE) rated 42.5-57 VDC, 0.4-0.3A.

An external power adapter is delivered with the product.

Once the Base Unit is powered, it starts up. Then the power button can be used to switch on or off.

How to connect the external power adapter.

1. Plug the barrel connector of the power adapter into the power input of the Base Unit.
2. Slide a power input adaptor piece (US, CN, EU or UK) on the power adapter of the ClickShare . Use the one which is applicable in your country.
   1. Slide down the button on the adapter (1).
   2. Insert the latch (2) of the adapter piece into notch (3)

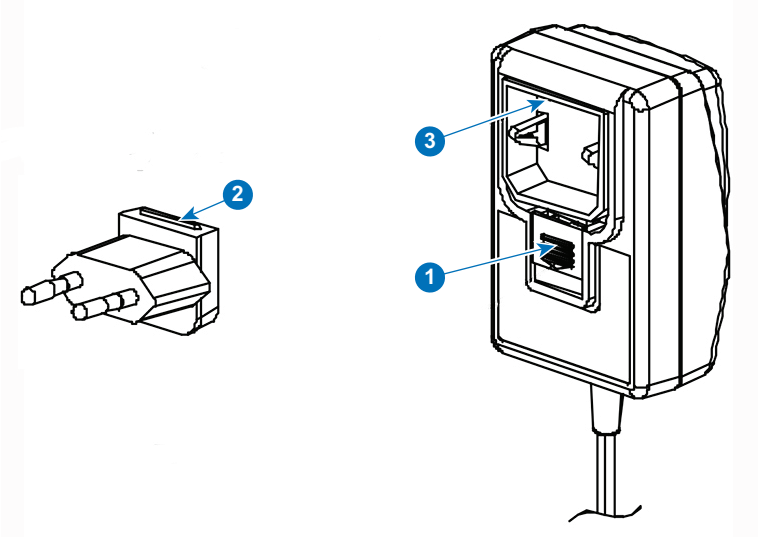


Image 4–8 Mounting adapter piece

Image 4–9 Type A

Image 4–10 Type A

Image 4–11 Type C

Image 4–12 Type G

Image 4–13 Type I

3. Connect the power cable to the wall outlet.

Preparing the Buttons

5

5.1 Pairing 48
5.2 ClickShare Extension Pack 49
5.3 ClickShare Extension Pack installer 49
5.4 ClickShare Windows Certified driver 50
5.5 ClickShare Desktop app 51

5.1 Pairing

Pairing of the Buttons with the Base Unit

To be able to use a Button it should be assigned to the Base Unit you are using. This process is called pairing. By default, the Button(s) delivered with the Base Unit are already paired to that specific Base Unit.

In case you buy additional Buttons or when a Button should be assigned to another Base Unit, the Button needs to be paired (again). The Button software update runs in the background and will not impact users while using the system. When downgrading or updating to an older version of the Base Unit software the Buttons need to paired manually to update their software and that only in case the Button update over Wi-Fi is disabled.

A Button can only be paired to one Base Unit at a time.
The Button will always make connection to the Base Unit it was last paired to.

Pairing a Button can be done in two ways:

- by plugging the Button to the Base Unit.
- by using the Button Manager application running on your laptop.

To pair a Button to the Base Unit by plugging in

1. Insert the Button in one of the USB port available on the Base Unit you are using (image is only given as example, all USB connectors can be used).

   Note: For some ports or Buttons, it can be necessary to use a convertor.

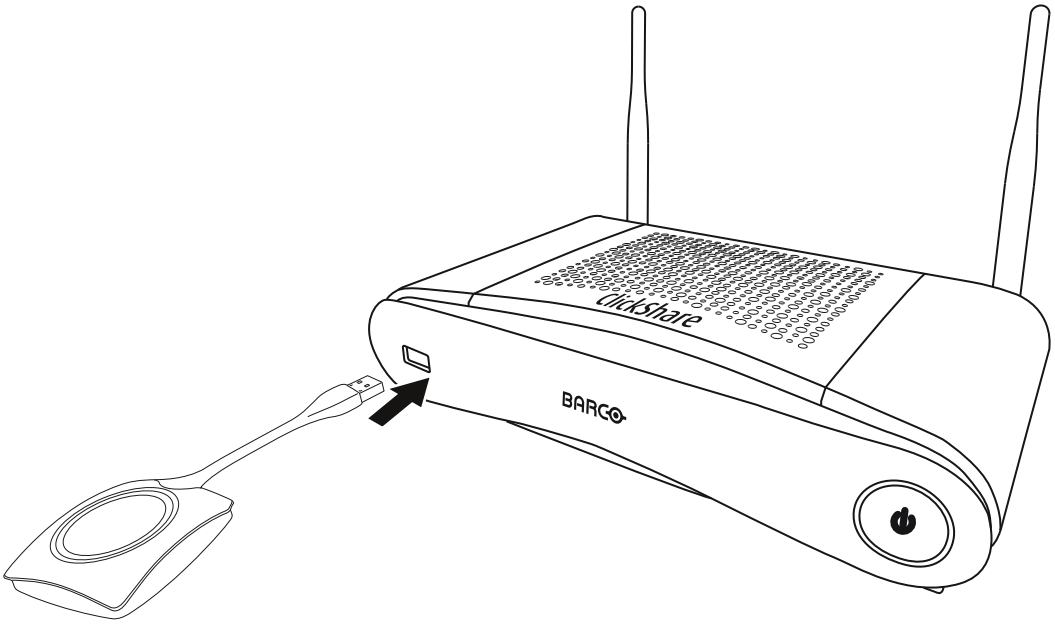


Image 5–1

Both the LEDs of the Button and the LEDs of the Base Unit are blinking white. This means pairing is in progress.

The Base Unit automatically checks whether the software of the Button is up to date. If not, the Base Unit updates the Button software. This may take more time.

During the pairing and update process, a small status bar is display.
The result of the pairing process can be as follows:

- When the LEDs become static white, the Button is paired to the Base Unit, but no software update was needed. You can unplug the Button from the Base Unit.
- When the LEDs become static red, the Button is paired to the Base Unit and the software update has finished. You can unplug the Button from the Base Unit.

2. Unplug the Button from the Base Unit.

The Button is now ready for use.

To pair a Button to the Base Unit using the Button Manager

Via the Button Manager client application running on your laptop, up to 4 Buttons can be paired simultaneously to a Base Unit without plugging the Buttons to the Base Unit. The Buttons are plugged in to your laptop. For more information about the Button Manager, consult the Button Manager's user guide which can be downloaded from Barco's website.

5.2 ClickShare Extension Pack

About

The ClickShare Extension Pack is a collection of tools to upgrade your ClickShare user experience. This Extension Pack contains the ClickShare Launcher service and a driver to enable the Extended Desktop functionality. Both tools will be installed by default. To change the default behavior of the installer, the installer will need to be executed with command line parameters.

The ClickShare Extension Pack can be installed by the end user manually, pre-installed on your company's laptop image or deployed company-wide with SCCM or other tools.

The ClickShare Extension Pack can be used in combination with a Button and/or with the ClickShare desktop app.

The latest extension pack can be downloaded via *http://www.barco.com/en/product/clickshare-extension-pack*

5.3 ClickShare Extension Pack installer

Interactive setup

In this setup, the user runs the installer which will install the ClickShare Extension Pack on his computer after the user accepts the EULA.

After the setup finished, the ClickShare launcher will be started automatically. The Extended desktop driver can only be used after the user reboots his computer.

Starting the setup

1. Download the ClickShare Extension Pack (download via *http://www.barco.com/en/product/clickshare-extension-pack*).
2. Unzip the downloaded file.
3. Click *ClickShare-Extension-Pack.msi* to start the installation.

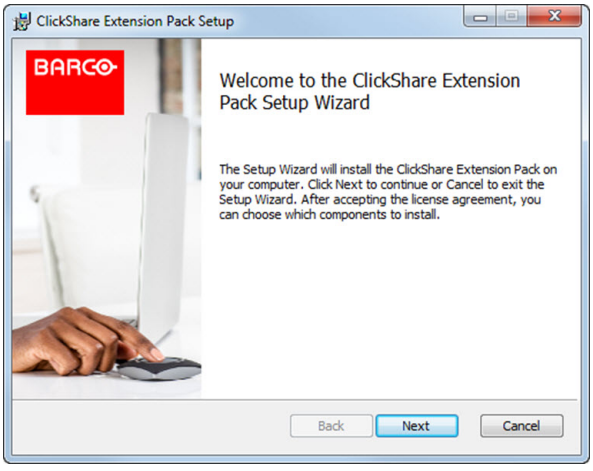


Image 5–2

4. Click **Next**, accept the License Agreement and click **Next** to continue.

If necessary, follow the on screen instructions.

Silent setup

In this setup, a user or an IT admin can install the ClickShare Extension pack using the Windows command prompt. Following is an example of a silent installation (version numbers are only given as example, always check Barco's web for the latest version):

Launcher only install:

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

Extended desktop only install :

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

Full install (laucher + extended desktop):

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

The computer will reboot. This can be suppressed with /norestart. A reboot will be needed afterwards for the extended desktop feature to be working. In case the end-user should decide if they want to reboot, /promptrestart /QB!+ can be used (basic UI, no cancel option, but prompt to reboot)

Parameter Description

ACCEPT_EULA	This parameter shows that the installer accepts the EULA text as is. This parameters must be set to YES in order to continue to the installation.
INSTALLFOLD-ER	This parameter specifies the installation directory for ClickShare launcher. If not specified, the default folder will be the Program Files folder.
LAUNCH_APP	The ClickShare launcher application will be started right after the installation finishes if this parameter is set to YES. Otherwise, the launcher application will not be started.
/qn	This parameter indicates that the installation will be done in silent mode, meaning that there will be no visible windows during the installation.
ADDLOCAL	This parameter indicated the type of the installation. No parameter added, installs only the launcher.

Windows environment variable

The variable to be used is CLICKSHARE_LAUNCHER_CLIENT_PATH. The value should be the path to the client software.

5.4 ClickShare Windows Certified driver

About

The ClickShare Windows Certified driver is auto-installed when plugging in a Button in a Window PC.

This Windows driver automatically lauches the executable on the Button.

Note that at least version **1.16.0** is required. In case an older version is installed on your PC, start windows update *check for updates* with a button inserted into your PC.

5.5 ClickShare Desktop app

About the

With the ClickShare desktop app installed on your computer you can enter a meeting room and get on the screen in a few seconds without the need to plug in a Button. The ClickShare app can be used in combination with a Button.

The ClickShare desktop app connects to the meeting room screen in order to share your content. Presence detection technology is used to do so. The ClickShare desktop app uses presence detection technics to determine which meeting room is closest to the user. Just click on your meeting room name. This means you will never have to enter IP addresses or scroll long lists of meeting rooms before being connected to your meeting room.

Installation

When the ClickShare desktop app is not pre-deployed in your IT environment, you can download and install the software without administrator rights from *www.clickshare.app* .

CSE-200 Configurator

6

6.1 Accessing the Configurator 55
6.2 ClickShare Configuration Wizard 58
6.3 On-Screen Language and Text Size 61
6.4 Meeting room information 63
6.5 Personalisation, wallpaper 64
6.6 Personalisation, Personalized wallpaper 65
6.7 Manage configuration files 67
6.8 Display setup 69
6.9 Audio settings 69
6.10 Wi-Fi settings 70
6.11 LAN settings 74
6.12 LAN Settings, Wired Authentication 76
6.13 LAN Settings, EAP-TLS security mode 77
6.14 LAN Settings, EAP-TTLS security mode 79
6.15 Services, mobile devices 80
6.16 Service, ClickShare API, remote control via API 82
6.17 XMS Server Integration 82
6.18 Services, SNMP 83
6.19 Services, Remote Button Pairing 84
6.20 Security, security level 84
6.21 Security, passwords 85
6.22 Security, HTTP Encryption 86
6.23 Status information Base Unit 89
6.24 Date & Time setup, manually 89
6.25 Date & Time setup, time server 91
6.26 Energy savers 92
6.27 Buttons 93
6.28 Buttons, External access point 93
6.29 Buttons, External access point, mode EAP-TLS 94
6.30 Buttons, External access point, mode EAP-TTLS 95
6.31 Buttons, External access point, mode PEAP 96
6.32 Buttons, External access point, mode WPA2-PSK 97
6.33 Firmware Update 98
6.34 Support & Updates, Troubleshoot, log settings 99
6.35 Factory defaults 100

Within some menus the *Configurator* is indicated as *WebUI*. E.g. WebUI password, that is the password to enter the Configurator.

6.1 Accessing the Configurator

Getting access to the Configurator

There are three ways to access the Configurator:

- Via the LAN
- Direct Ethernet connection between PC and Base Unit.
- Via the Base Unit's wireless network

When accessing the configurator for the first time, the ClickShare Configuration Wizard starts automatically.

This configuration wizard can be started at any moment to change your configuration instead of using the menus.

To access the Configurator via the LAN

1. Open a browser.

   Note: Supported browsers are Internet Explorer, Firefox, Google Chrome and Safari.

2. Browse to the IP address of your device.

   Note: If you do not know the IP address due to *Show network info* is disabled, connect via a direct connection or via a wireless connection to your device to discover the wired IP address.

   A login screen appears.

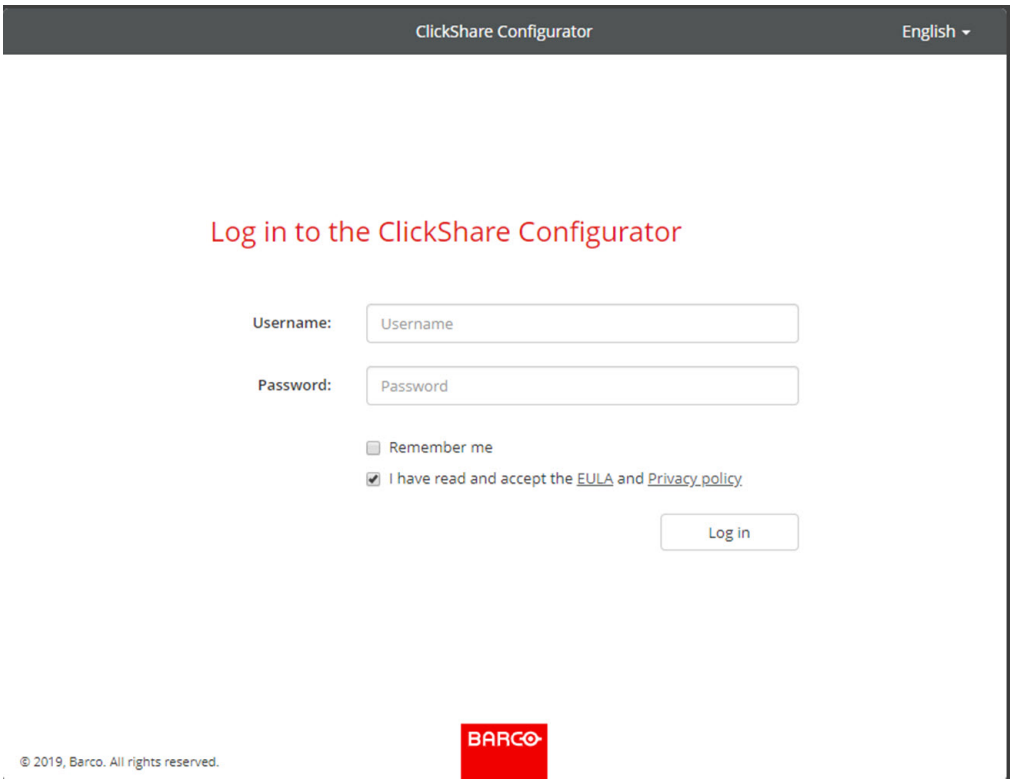


Image 6–1 Login screen

3. To change the language of the Configurator, click on the drop down next to the current selected language and select the desired language.

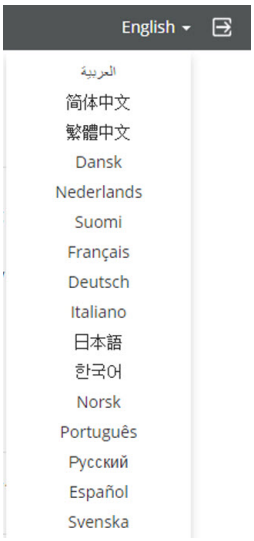


Image 6–2 Configurator lanuguages

The following languages are possible:

- Arabic
- Simplified Chinese
- Traditional Chinese
- Danish
- Dutch
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian
- Portuguese
- Russian
- Spanish
- Swedish

The Configurator language changes to the selected language.

4. Enter the user name 'admin' and the password, read and accept the EULA and the Privacy policy and click **OK**.

   By default, the password is set to 'admin'.

   Warning: It is strongly recommended to change the default password into a strong password on first use, to prevent that anyone else accessing the configurator can change the settings of the ClickShare Base Unit. See section “Security, passwords”.

   The Configurator opens.

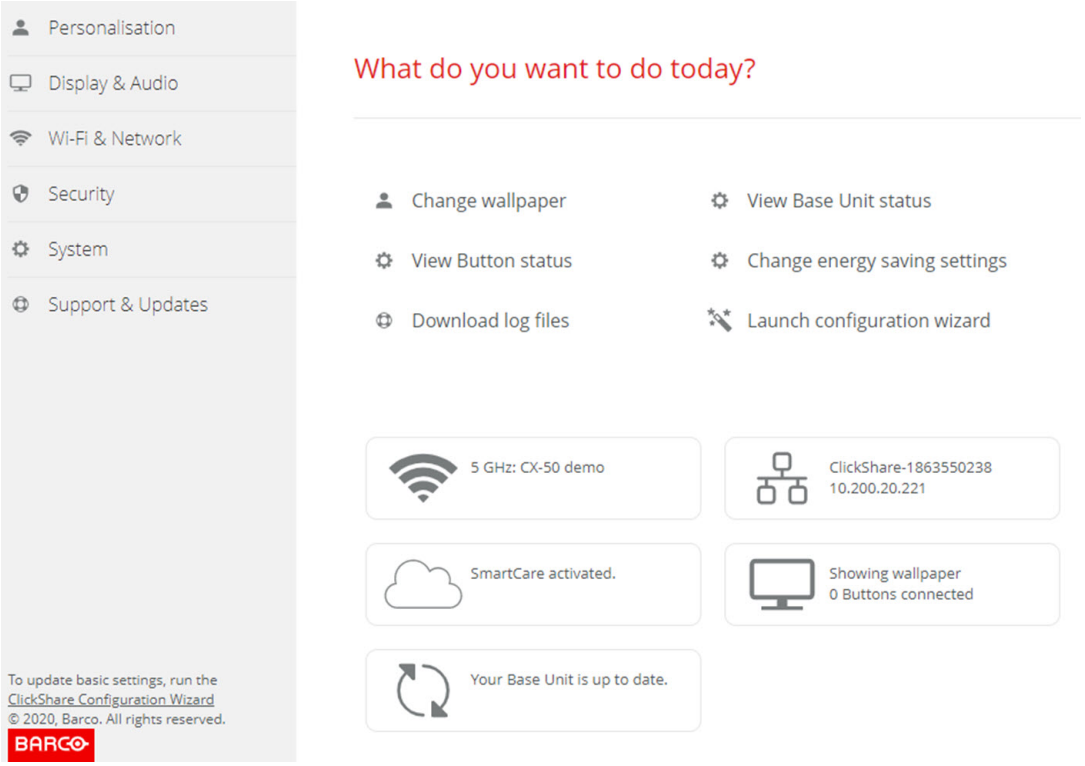


Image 6–3 Start screen

The language of the configurator can be changed on any page in the interface.

The screen is split up in 2 panes. Left pane with the selection buttons and a right pane to configure the selected function.

The startup screen itself shows:
- the wired IP address
- the wireless SSID
- the number of Buttons connected
- the system state

If you cannot find the IP address (e.g. there is no screen available) you should connect to the Base Unit directly with your laptop via an Ethernet crossover cable and access the web interface using the fixed IP address 192.168.1.23. Make sure your own LAN adapter is set in the 192.168.1.x range.

To access the Configurator via a direct connection.

1. Connect the Base Unit to your laptop using an Ethernet cable.
2. On your laptop, open a browser.

   Note: Supported browsers are Internet Explorer, Firefox and Safari.

3. Browse to *http://192.168.1.23*.

   A login screen appears.
4. Enter the user name 'admin' and the password, read and accept the EULA and click **OK**.

   By default the password is set to 'admin'.

   The configurator opens. The wired IP address is given on the startup page.

To access the Configurator via the Base Unit wireless network

1. On your laptop, connect to the Base Unit wireless network.

The default SSID and password to connect to the Base Unit are respectively 'ClickShare-<serial base number>' and 'clickshare'.

2. On your laptop, open a browser.

   Note: Supported browsers are Internet Explorer, Firefox and Safari.

3. Browse to *http://192.168.2.1*.

   A login screen appears.

4. Enter the user name 'admin' and the password, read and accept the EULA and click **OK**.

   By default the password is set to 'admin'.

   The configurator opens. The wired IP address is given on the startup page.

Older laptops might not support the 5 GHz Frequency Band. If your Base Unit is set to that frequency range, those devices will not be able to connect to the Base Unit via the wireless network.

Overview of functions

Group	Function
Personalization	On-Screen ID
	Wallpaper
	Configuration Files
Display & Audio	Display & Audio
Wi-Fi & Network	Wi-Fi Settings
	LAN Settings
	Services
Security	Security levels
	Passwords
System	Base Unit Status
	Date & Time
	Energy Savers
	Buttons
Support & Updates	Firmware
	Troubleshoot

When a setting is changed, always click **Save changes** to store the changes.

6.2 ClickShare Configuration Wizard

About the configuration wizard

During the first start up of the Base Unit, the configuration wizard starts up automatically.

All basic settings necessary to configure the Base Unit are covered by the configuration wizard. Once the configuration wizard is finished, the Base Unit is ready to be used.

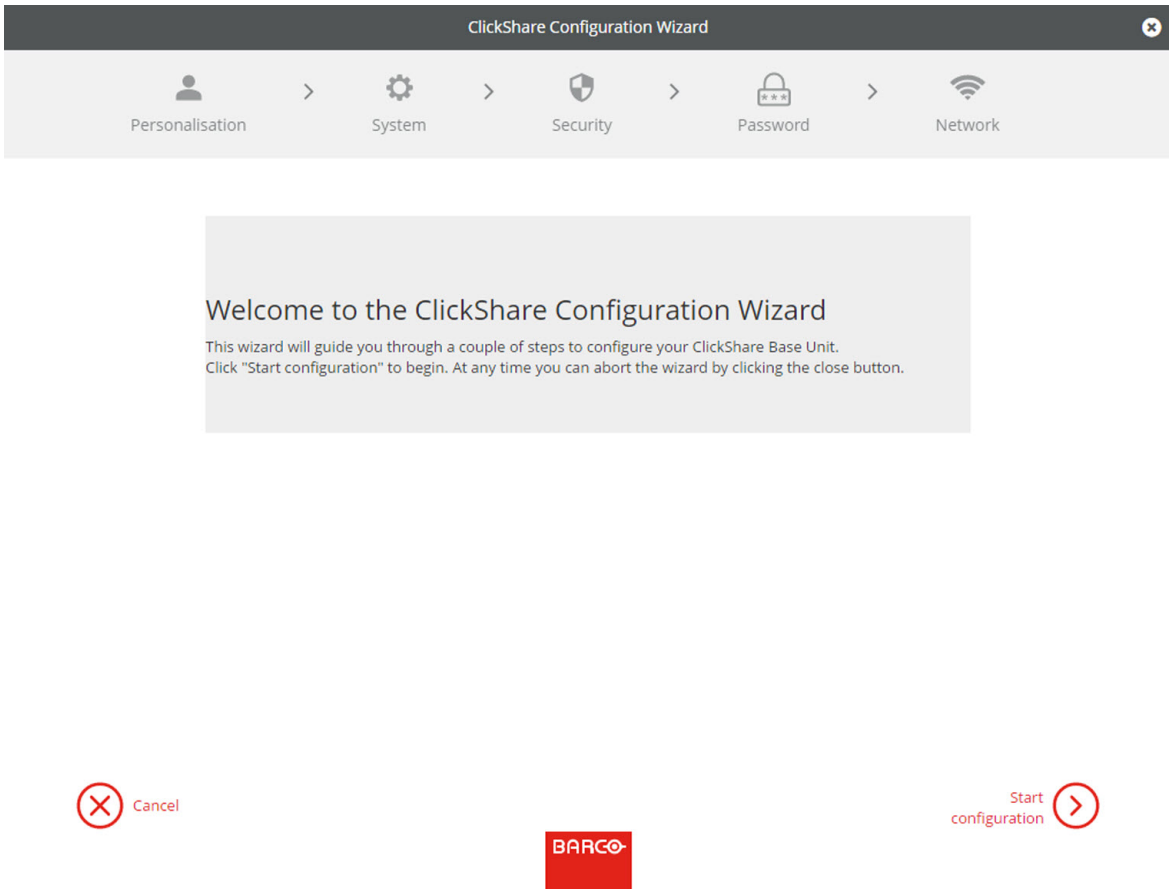


Image 6–4 Configuration wizard

To start the wizard, click on **Start Configuration**.

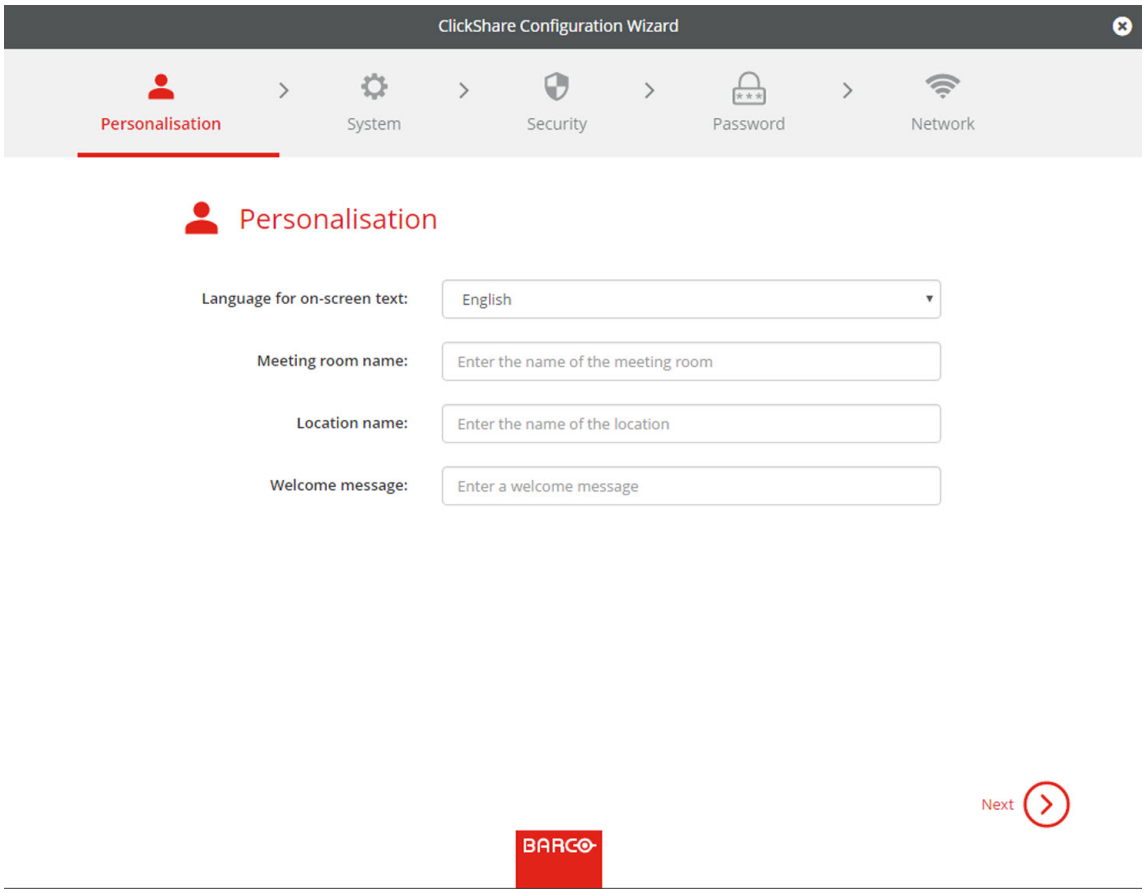


Image 6–5 Configuration wizard, Personalisation

Fill out the necessary field and click **Next** to continue.

To return to the previous step, click on **Back**.

For more information about a specific topic, see one of the following topics.

The ClickShare Configuration Wizard can be started at any time to change the configuration just by clicking on **ClickShare Configuration Wizard** at the left bottom of each screen.

Personalisation	Language on-screen text	See “On-Screen Language and Text Size”, page 61.
	Meeting room name, location name and welcome message	See “Meeting room information”, page 63.
System	Time zone, manual time setup	See “Date & Time setup, manually”, page 89.
	Use NTP	See “Date & Time setup, time server”, page 91.
Security	Level settings	See “Security, security level”, page 84.
Password	ClickShare Configurator (WebUI) password	See “Security, passwords”, page 85.
Network	Frequency band, channel Wi-Fi passphrase	See “Wi-Fi settings”, page 70.

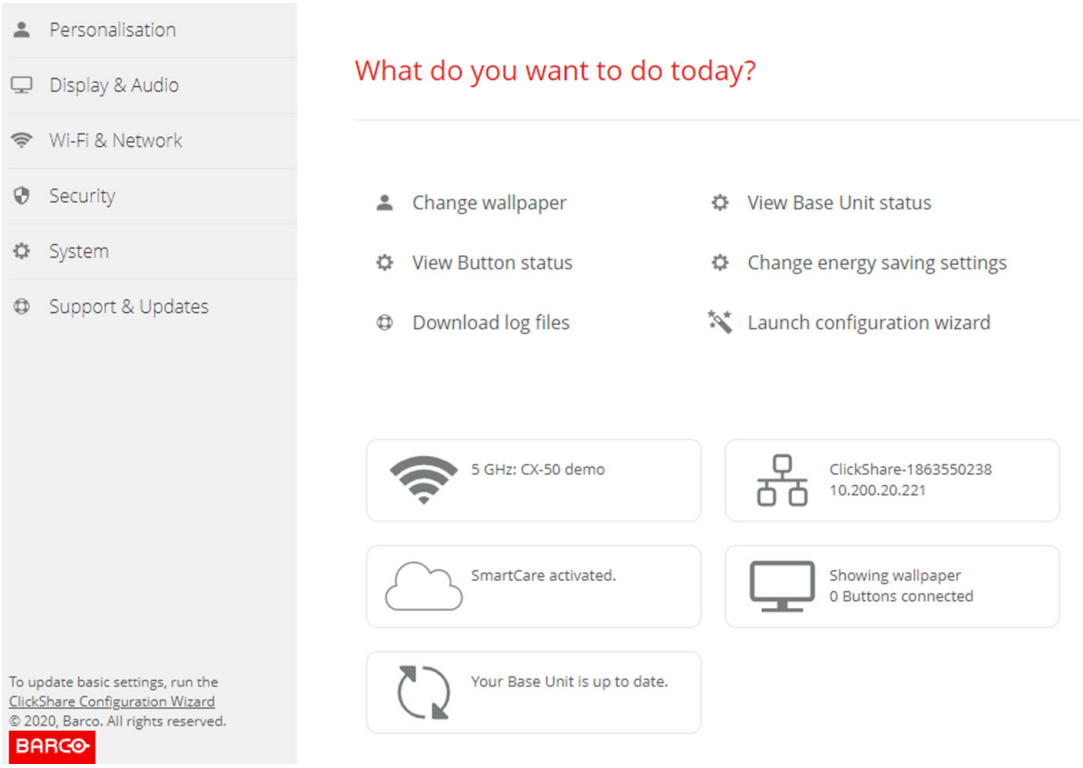


Image 6–6 Configuration Wizard start

6.3 On-Screen Language and Text Size

About the on-screen language.

The on-screen language can be set independent of the configurator language. The on-screen text size can be changed between small, medium or large.

Language selection

1. Log in to the *Configurator*
2. Click *Personalisation* → *On-Screen ID*.

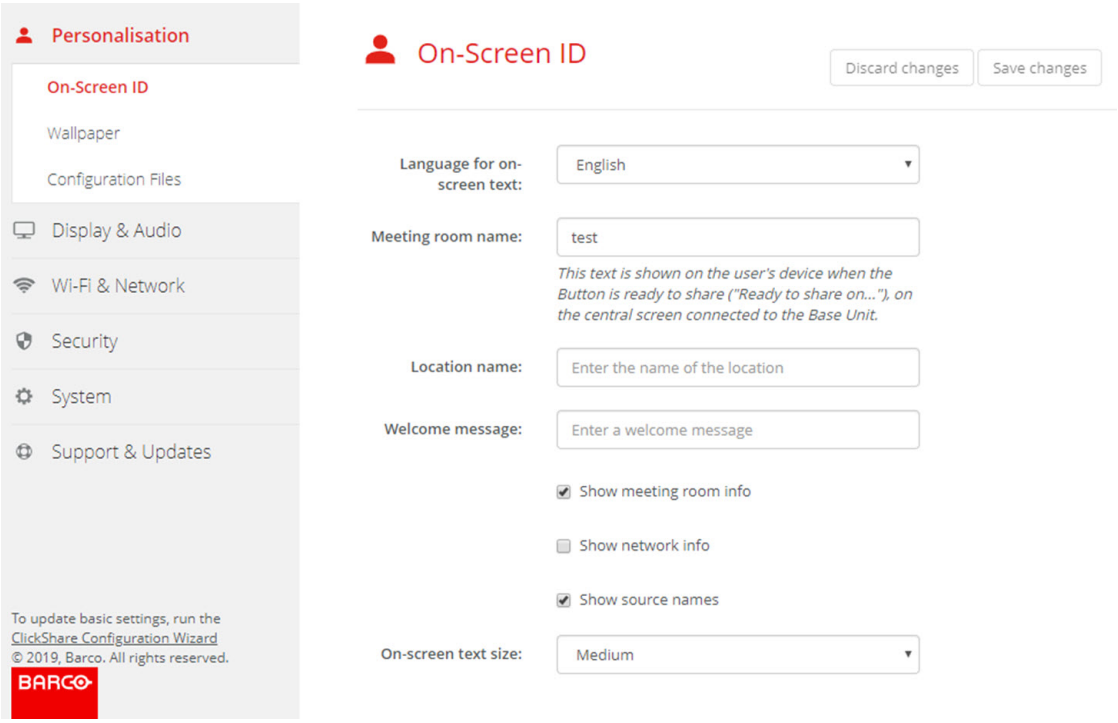


Image 6–7 Personalisation, On-Screen ID

3. Select the language of the on-screen text. Click on the drop down box next to *Language for on-screen text* and select the desired language.

   The following languages are possible:

   - Arabic
   - Simplified Chinese
   - Traditional Chinese
   - Danish
   - Dutch
   - English
   - Finnish
   - French
   - German
   - Italian
   - Japanese
   - Korean
   - Norwegian
   - Portuguese
   - Russian
   - Spanish
   - Swedish

Text size

1. Log in to the *Configurator*
2. Click *Personalisation* → *On-Screen ID*.
3. Click on the drop down box next to *On-screen text size* and select the desired font size.

   The following sizes are possible:

   - Small
   - Medium
   - Large

6.4 Meeting room information

About meeting room settings

The following settings are possible:

- Meeting room name
- Meeting room location
- Welcome message on the ClickShare screen
- Show meeting room info
- Show network info
- Show source names

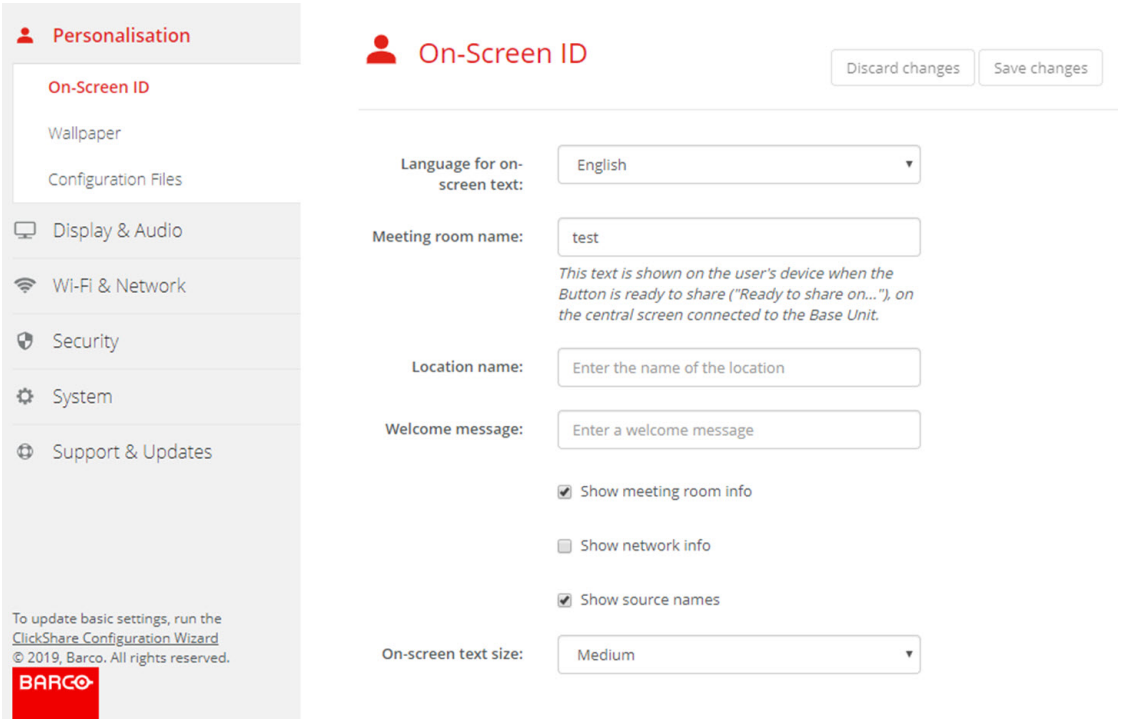


Image 6–8 Personalisation, On-Screen ID

Meeting room name, location and welcome message

1. Log in to the Configurator.
2. Click *Personalisation* → *On-screen ID*.
3. Click in the input field next to *Meeting room name* and enter a name for the meeting room.

   This text is shown on the user's device when the Button is ready to share ("Ready to share on..."), on the central screen connected to the Base Unit and in the list of AirPlay receivers on the user's iOS device.
4. Click in the input field next to *Location name* and enter the location.
5. Click in the input field next to *Welcome message* and enter the desired message.

Show on-screen information

1. Log in to the Configurator.
2. Click *Personalisation* → *On-screen ID*.
3. Check the check box in front of *Show meeting room info*.

   Checked: meeting room name, location and welcome message are displayed on-screen when nothing is shared.

   Not checked: nothing is shown on-screen.

4. Check the check box in front of *Show network info*.

   Checked: LAN information such as wired IP address, hostname are displayed. Also the Wi-Fi IP address and SSID are displayed.

   Not checked: no LAN nor Wi-Fi information is displayed.

5. Check the check box in front of *Show source names*.

   Checked: the source name of the shared content is displayed on the screen.

   Not checked: no source info displayed on the screen.

6.5 Personalisation, wallpaper

About wallpaper

When CSE-200 starts up, a background (wallpaper) is displayed. The display of this background wallpaper can be disabled.

By default a general ClickShare and a quick start wallpaper are available. The possibility exists to upload personal backgrounds (wallpapers). The default wallpapers cannot be removed from the system.

Wallpaper selection

1. Log in to the Configurator
2. Click *Personalisation* → *Wallpaper*.

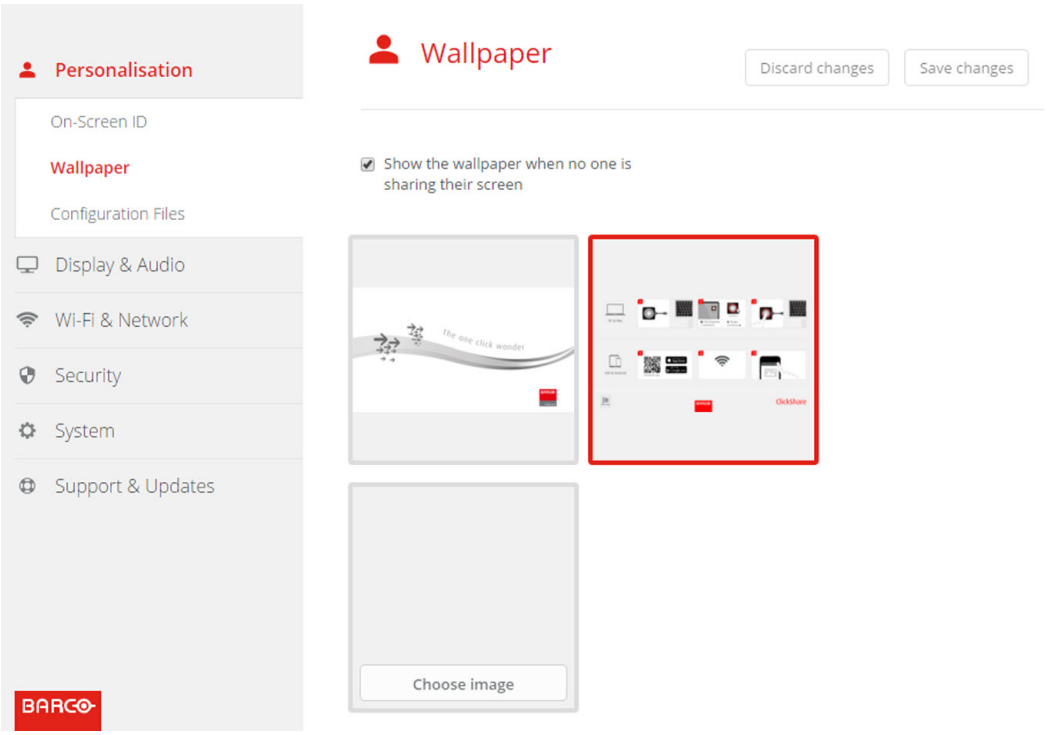


Image 6–9 Wallpaper selection

The *Wallpaper* selection pane is shown. The current selected wallpaper is shown with a red border.

3. Select one of the available wallpapers and click on **Save Changes**.

   Note: By default a general Barco CSE-200 wallpaper and a CSE-200 Quick Start Guide wallpapers are available.
   They are automatically resized to fit the aspect ratio of the screen.

   The selected wallpaper is indicated with a red border.

   The message **Successfully applied changes** appears on top of the wallpaper selection window.

You can also add a personal wallpaper, e.g. your company logo. For more information on adding a new wallpaper to the list, see “*Personalisation, Personalized wallpaper*”, page 65.

Download wallpaper

1. Hoover with your mouse over the wallpaper to download and click on the download symbol on the upper right corner.

Image 6–10 Download wallpaper

The wallpaper is downloaded to your PC.

Enable - disable Wallpaper

1. Within the Wallpaper pane, check the check box next to *Show the wallpaper when no one is sharing their screen*.

   Checked: wallpaper will be displayed when no one is sharing content.

   Not checked: no wallpaper will be displayed when no one is sharing content. The video output of the Base Unit is disabled when no content is shared. This feature is especially useful when the Base Unit is integrated in a larger AK system

6.6 Personalisation, Personalized wallpaper

About a personalized wallpaper

Via the Configurator it is possible to upload personalized backgrounds or wallpapers.

The upload file should be a JPEG, PNG, BMP or TIFF format with a maximum size of 2.5MB.

Maximum 5 wallpaper can be uploaded.

How to upload

1. Log in to the Configurator
2. Click *Personalisation* → *Wallpaper*.

   The *Wallpaper* selection pane is shown. The current selected wallpaper is shown with a red border.
3. Hoover your mouse over the free place and click on **Choose image**.

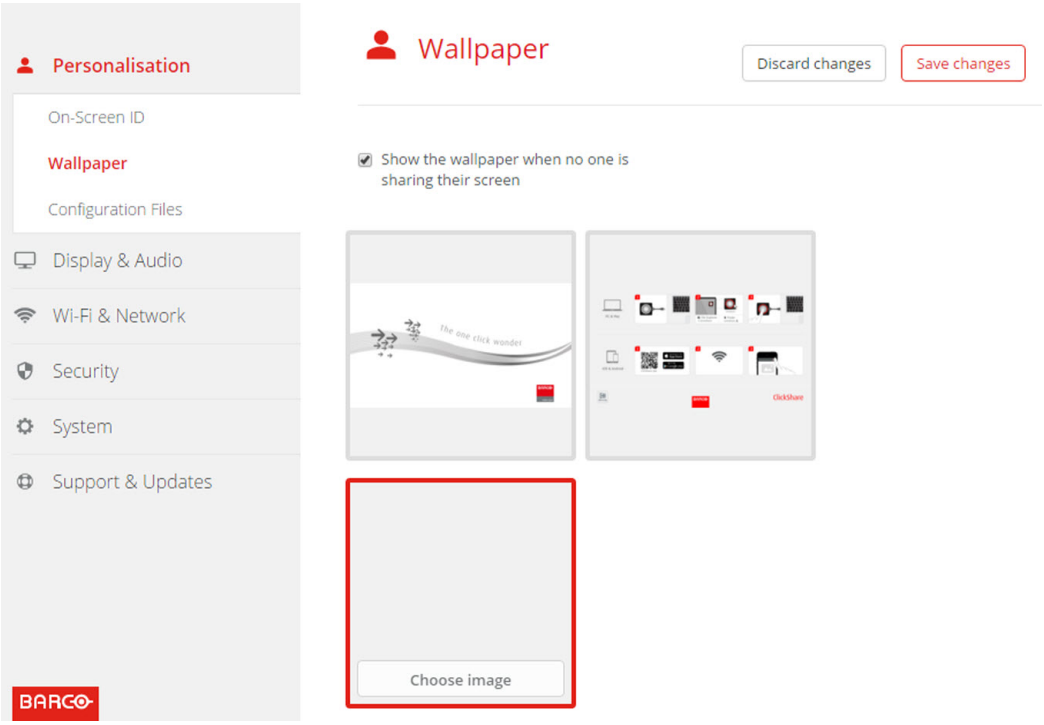


Image 6–11 Personalized wallpaper selection

A browser window opens.

4. Browse for the desired image, click Open to load the image.

   The content of the file is checked and when valid (format and size), the file is uploaded. The new wallpaper gets a red border.

5. Click on **Save changes** to apply the personalized wallpaper

   The message **Successfully applied changes** is displayed on top of the page.

Change personalized image

1. Click *Personalisation* → *Wallpaper*.
2. Hoover your mouse over the current personalized image and click **Change image**.

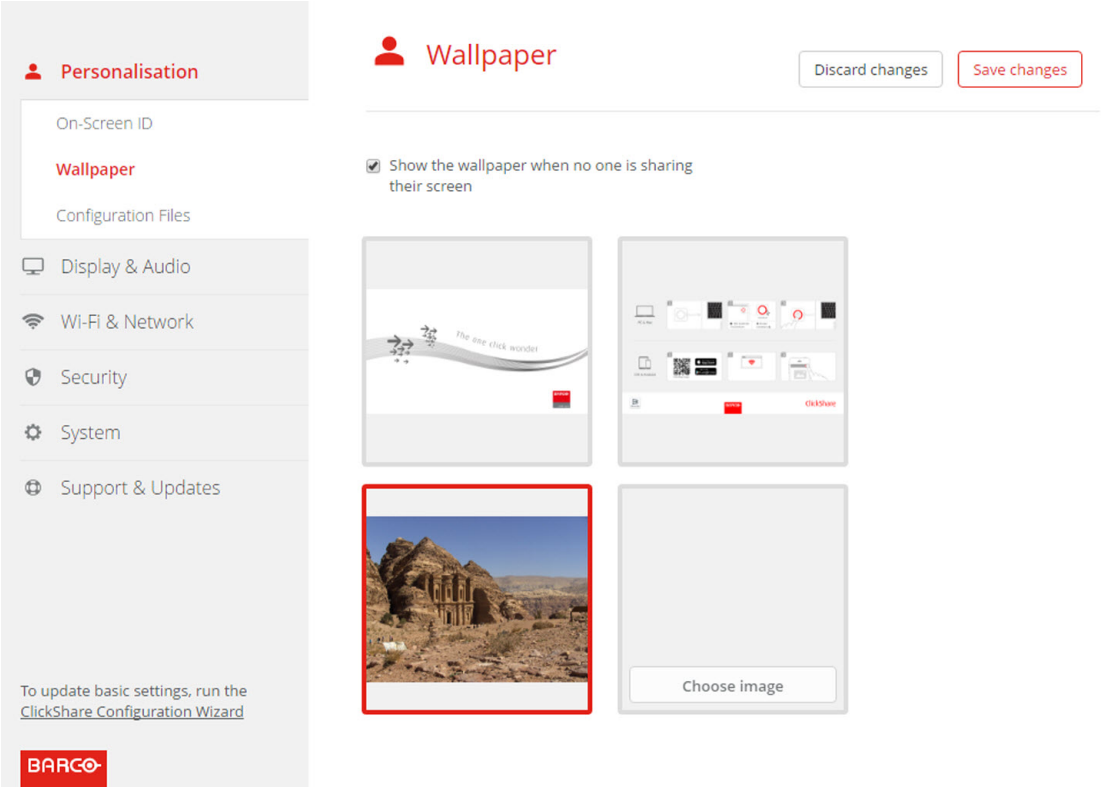


Image 6–12 Change image

3. Browse for the desired image, click Open to load the image.

   The content of the file is checked and when valid (format and size), the file is uploaded. The new wallpaper gets a red border.

4. Click on **Save changes** to apply the personalized wallpaper and replace the previous file.

   The message **Successfully applied changes** is displayed on top of the page.

Remove personalized wallpaper

1. Hoover your mouse over the current image and click on the trash bin to remove the image.

Image 6–13 Remove wallpaper

The personalized wallpaper is removed and the default wall paper is activated.

6.7 Manage configuration files

About Manage configuration files

A full backup can be downloaded but cannot be used to duplicate configuration settings to other Base Units. Therefore, it is possible to download a Portable version. This portable version can be uploaded via the upload

configuration button on other Base Units (same type). Via the same button, the full backup can be uploaded on the original Base Unit.

A portable backup contains:

- Wallpapers
- Wallpapers settings
- Logging settings
- All display settings
- OSD language
- Location
- Welcome message
- Wi-Fi channel
- Wi-Fi frequency

To manage the configuration files

1. Log in to the *Configurator*.
2. Click *Personalisation* → *Configuration Files*.

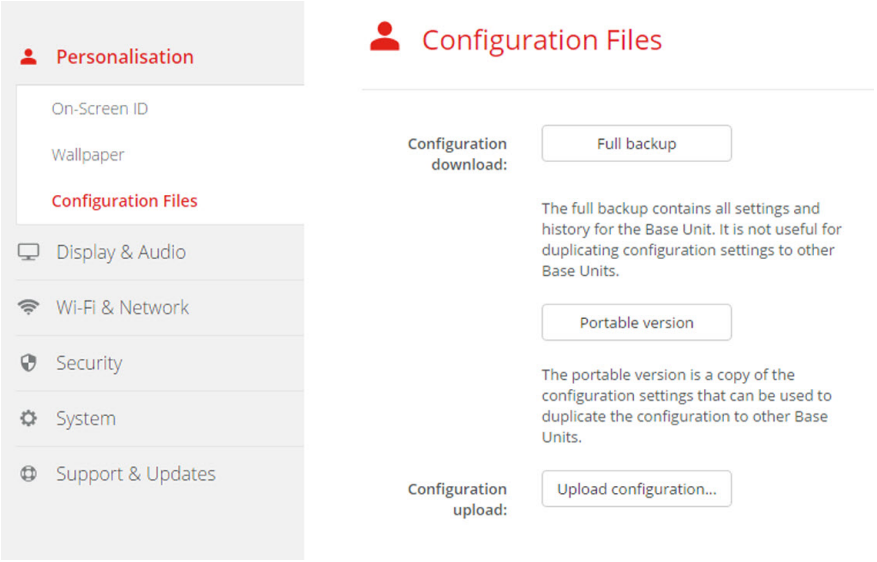


Image 6–14 Configuration files

3. To download a full backup, click on **Full Backup**.

   An xml file, containing all information and history will be downloaded. This file can be reused on the same Base Unit only.

4. To download a portable version, click on **Portable Version**.

   An xml file, containing portable information to duplicate settings on another Base Unit.

5. To upload a configuration, click on **Upload Configuration**.

   A browser window opens. Navigate to the upload file (xml file) and click **Open** to upload.

   A full backup can be uploaded on the Base Unit where the backup was created and a portable version can be uploaded on any other Base Unit of the same model.

When uploading a config file, the history of software updates and paired Buttons is lost. Paired Buttons will however remain functional if the Base Unit has not changed from SSID or wireless password.

6.8 Display setup

Resolution

The output resolution to the display is set on Auto. That means that the CSE-200 output resolution is automatically adapted to the resolution of the display. For HDMI displays, a hot plug detection is available.

Screen saver setup

1. Log in to the *Configurator*.
2. Click *Display & Audio* → *Display & Audio*.

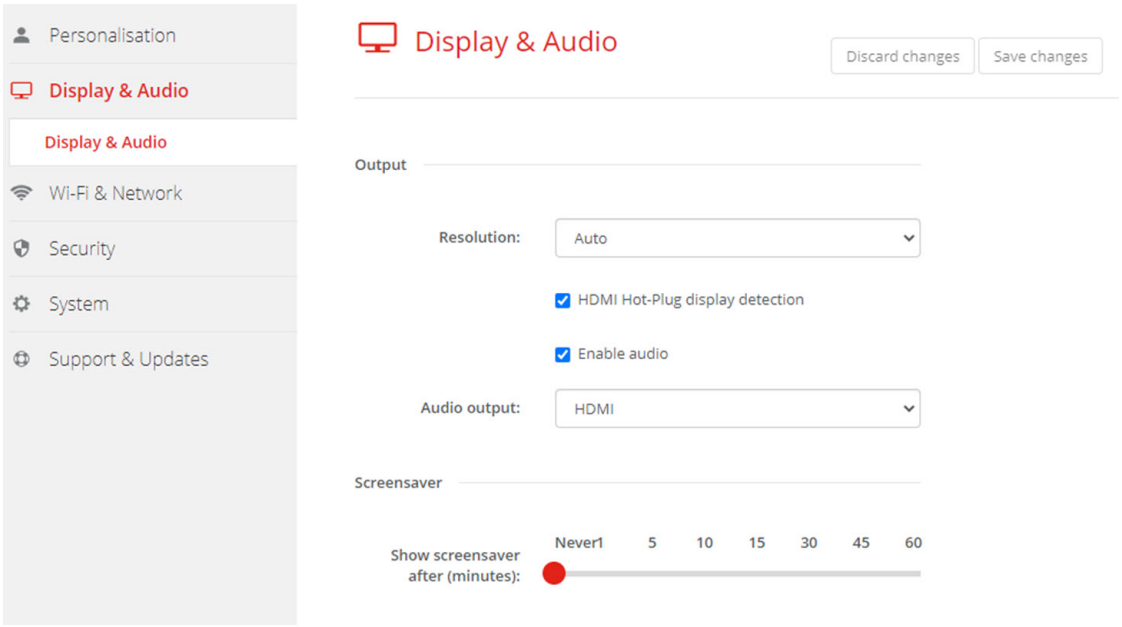


Image 6–15 Display settings

3. To activate the screen saver, drag the slider bar to the left or to the right until the desired delay time is reached.

   When the slider is set completely to the right, the screen saver will never be activated.

6.9 Audio settings

About the audio settings

The audio functionality can be disabled or enabled. When the enable and/or disable setting is changed, the Buttons must be re-paired before the setting becomes active.

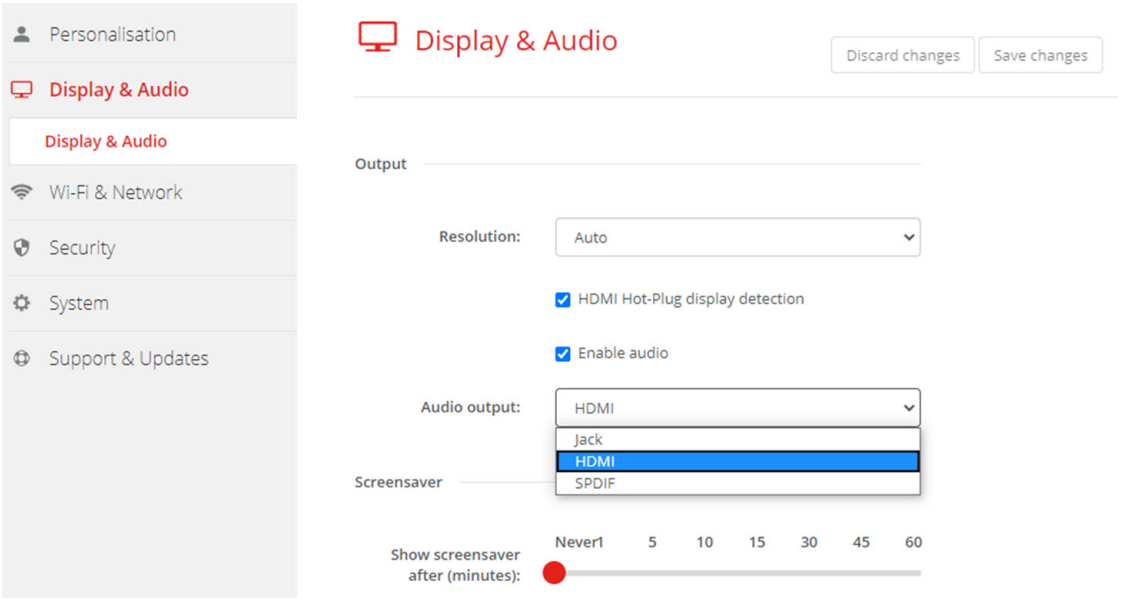


Image 6–16 Audio settings

How to change

1. Log in to the *Configurator*.
2. Click *Display & Audio* → *Display & Audio*.
3. Check or uncheck the check box next to Enable Audio.
   Checked: audio is enabled.
   Unchecked: audio is disabled.
4. To select the audio output, click on the drop down box and select the desired audio output.
   Jack: audio output via jack.
   HDMI: audio output via HDMI.
   SPDIF: digital audio ouput via TOSLINK
5. Click on **Save changes** to apply the new settings.

6.10 Wi-Fi settings

WARNING: It is not allowed to operate the Base Unit outside its intended geographical region.

About Wi-Fi

A connection with the Base Unit can be made via a wireless connection. A fixed wireless IP address is used to establish the connection.

The transmission power of the wireless signal can be reduced.

An overview of the current settings is given when *Wi-Fi Settings* is selected and operational mode is *Access Point*.

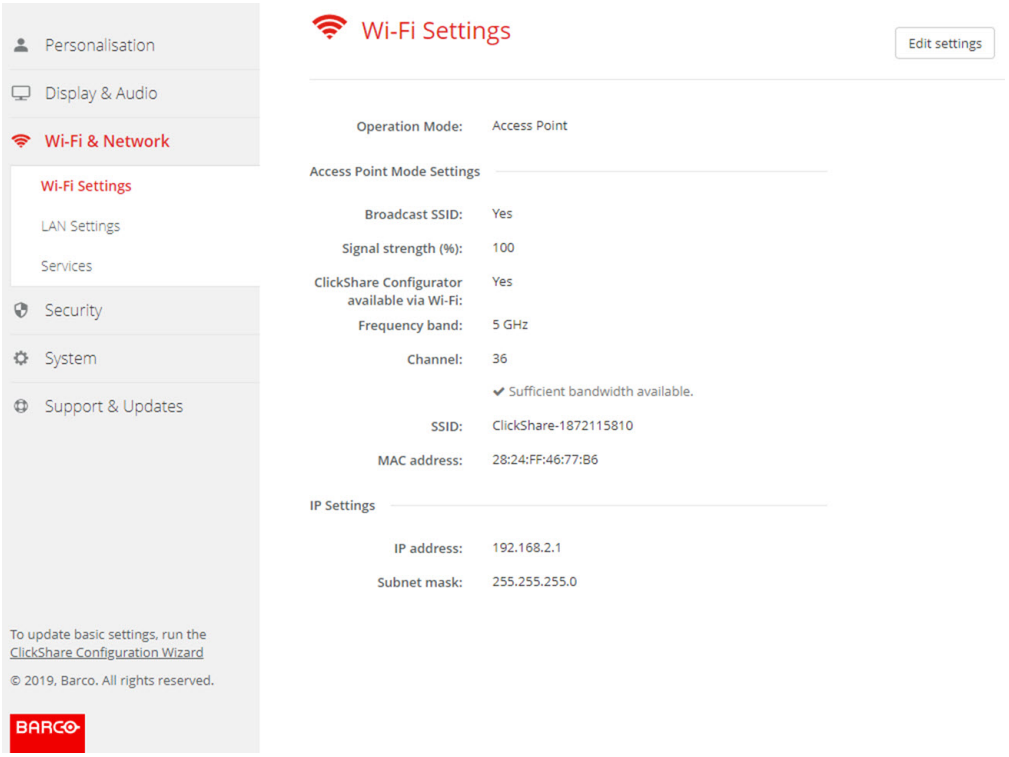


Image 6–17 Wi-Fi settings

When operational mode is set to *Off*. The following info is given: “The wireless interface is disabled. Buttons must be configured to connect to another Wi-Fi access point. Click *here* to go to the Button configuration page”.

Click on *here* to start the Button configuration. For more info, see “*Buttons*”, page 93.

To change any Wi-Fi-setting, click on **Edit settings**. The view depends on the previous selected operational mode. Here given with Access Point selected.

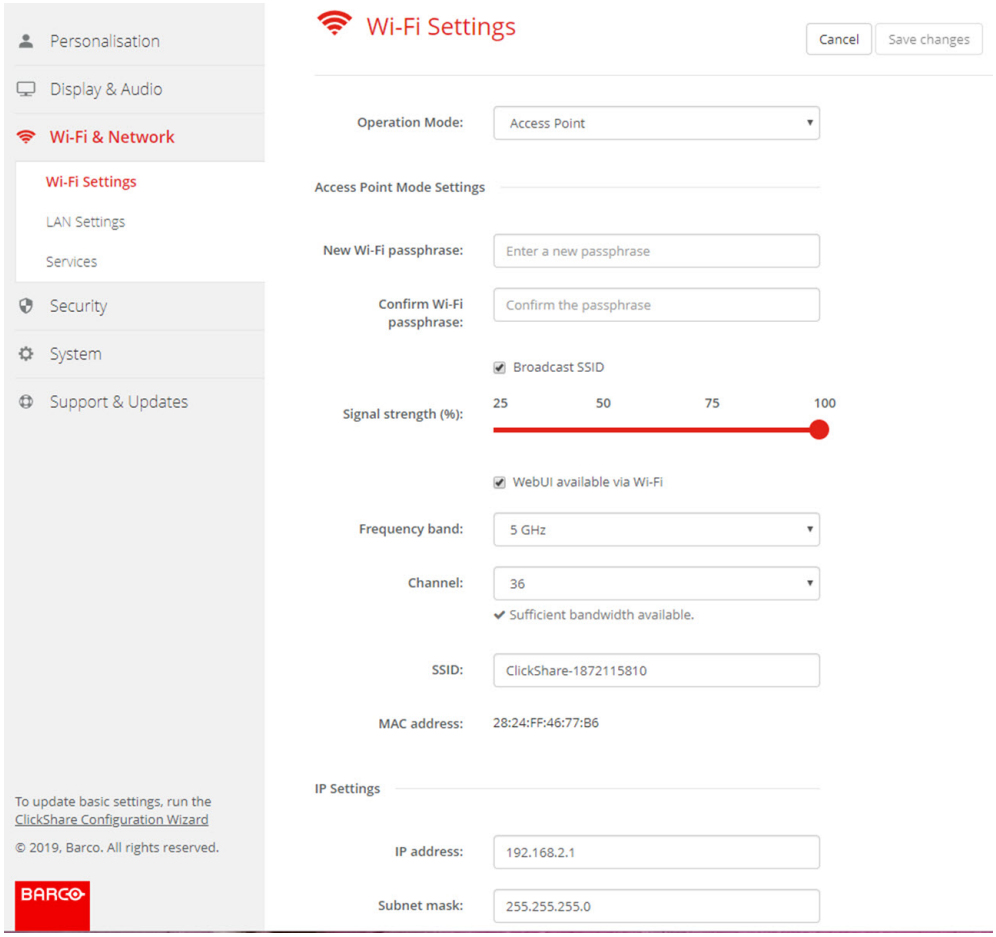


Image 6–18 Wi-Fi settings, edit

Changing the IP address will require a repairing of the Buttons used with this Base Unit.

Change operational mode

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Wi-Fi Settings*.
3. Click **Edit settings**.
4. Click on the drop down box next to *Operational Mode* and select the desired mode.

   The following options are possible:

   - Access Point: continue with the next blocks in this topic.
   - Wireless Client (only for CSE-200+)
   - Off

About frequency band & channel selection

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.

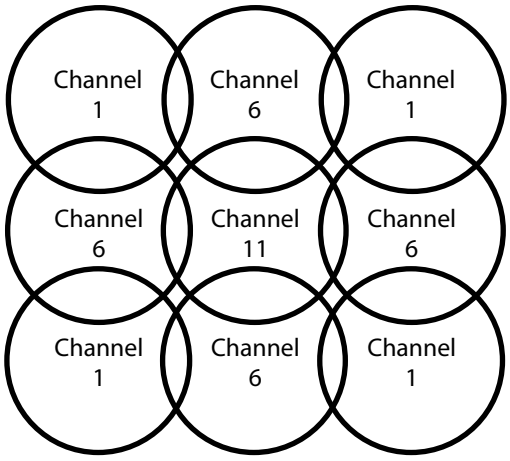


Image 6–19

To limit the effect of overlapping networks, it is highly recommended to reduce the signal strenght (standard range of about 30m) of the ClickShare Base Units. Reducing the signal strenght 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 will decrease or even disappear.

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.

Frequency band & channel selection

1. Select the wireless connection channel by clicking on the drop down box and selecting the desired channel.

   The channels available in the list vary according to the regional version of your Base Unit. Re-pairing the Buttons is not required when changing the frequency band or wireless connection channel.

   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.

2. Select the wireless connection frequency band: 2.4 GHz or 5 GHz by clicking on the drop down box and selecting the correct band.

   Below the channel selection pane, an indication is given of the available bandwidth of the current channel. To see if sufficient bandwidth is available in a different channel, select the channel in the drop down and save the changes. The page will reload with the new settings and an indication of the channel fit will be given after approximately 1 minute. There is no need to reload the page to see the result.

   The channels available in the list vary according to the regional version of your Base Unit. Re-pairing the Buttons is not required when changing the frequency band or wireless connection channel.

   When Intense use, change to another Wi-Fi channel is displayed, change to another channel. The page will reload after approximately 1 minute.

SSID & passphrase

1. Enter a public name (SSID) for the wireless network.

   The default SSID is *ClickShare-<serial number Base Unit>*.

2. If you want to broadcast this SSID, check the checkbox before *Enable SSID broadcast*.

3. Enter a new Wi-Fi passphrase and confirm that passphrase.

CAUTION: It is strongly recommended to change the Wi-Fi passphrase on first use to prevent anyone else accessing the Wi-Fi network.

Signal strength

1. Select the Signal Strength. Click on the slider and reduce the broadcasted power (signal strength) until the desired strength is obtained.

   Note: Too low power and interference by others might lead to connection issues. If so, increase again the signal strength until the issues are solved.

   By default the strength is set to 100%.

   Reducing the signal strength limits the effect of overlapping networks in the 2.4 GHz channels. Not necessary for the 5 GHz channels as their is no overlap.

ClickShare Configurator (WebUI) access via Wi-Fi

1. To allow access to the configurator via Wi-Fi, check the check box in front of *WebUI available via Wi-Fi*.

   Checked: Configurator accessible via Wi-Fi.

   Not checked: access to the configurator via Wi-Fi is blocked.

IP address & subnet mask

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Wi-Fi Settings*.
3. To change the IP address or subnet mask, click in the input field and enter the 4 octets of the new IP address or subnet mask.

   Note: This must NOT be 0.0.0.0 for static IP-Address assignment.

6.11 LAN settings

About LAN network settings

A network connection can be configured through DHCP or by manually entering a fixed IP address.

DHCP
Dynamic host configuration protocol. DHCP is a communications protocol that lets network administrators manage centrally and automate the assignment of IP addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

Hostname & method

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *LAN Settings*.

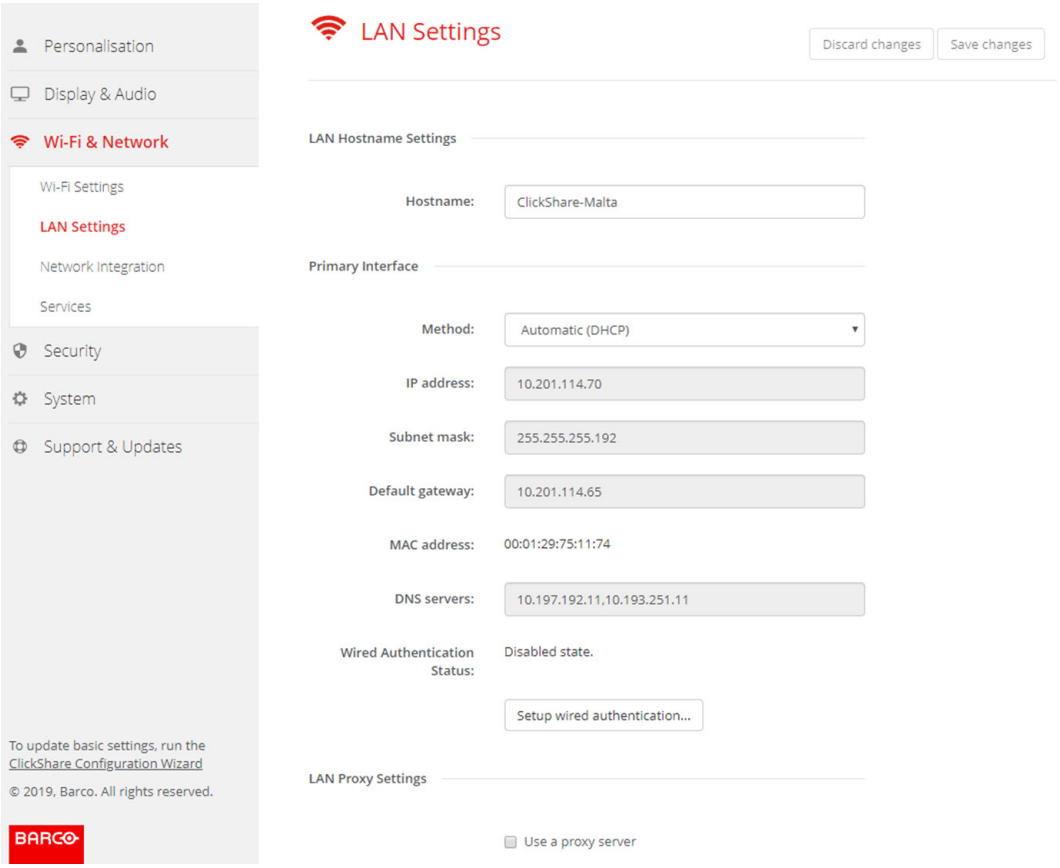


Image 6–20 LAN settings

3. Click in the input field next to *Hostname* and enter a host name for the Base Unit.

   The default host name is *ClickShare-<serial number Base Unit>*.

4. To select the method, click on the drop down box next to Method and select the *Automatic (DHCP)* or *Manual*.

   When Automatic (DHCP) is selected, the IP address, subnet mask and default gateway fields are grayed out but the currently used settings are filled out.

5. Click **Save changes** to apply the settings.

Manual (fixed) IP address

1. Click on the drop down box next to *Method* and select *Manual*.

   The IP address, subnet and gateway input fields are activated.

2. Click in the input field of the *IP address* and fill out the 4 octets.

   Note: An address contains 4 octets with a maximum value of 255.
   This must NOT be 0.0.0.0 for static IP-Address assignment

3. Click in the *Subnet mask* input fields and fill out the 4 octets as appropriate for the local subnet.

4. Click in the *Default Gateway* input fields and fill out the 4 octets. Set the Default-Gateway to the IP-Address of the router (MUST be on the local subnet!).

   Note: This must NOT be 0.0.0.0.
   If there is no router on the local subnet then just set this field to any IP-Address on the subnet.

5. Click in the DNS Servers input field and fill out the preferred DNS servers (maximum 5) in a comma separated list.

6. Click **Save changes** to apply the settings.

Do not use IP address 192.168.2.x for a Subnet mask 255.255.255.0 and IP address 192.168.x.x for a Subnet mask 255.255.0.0

Use a proxy server

This setting is important for the auto-update feature of the Base Unit, which require internet access.

1. Check the check box next to Use a proxy server.

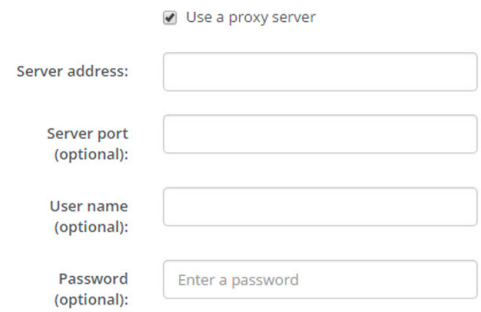


Image 6–21 Proxy settings

The proxy settings become available.

2. Enter the proxy server address. Enter the IP address or hostname.
   Some proxy servers need a port number, user name and password, for others is this optional.
3. Optionally, enter the used server port.
4. Optionally, enter the user name.
5. Optionally, enter the password.
6. Click **Save changes** to apply the settings.

6.12 LAN Settings, Wired Authentication

How to setup

1. Click on **Setup wired authentication...** .

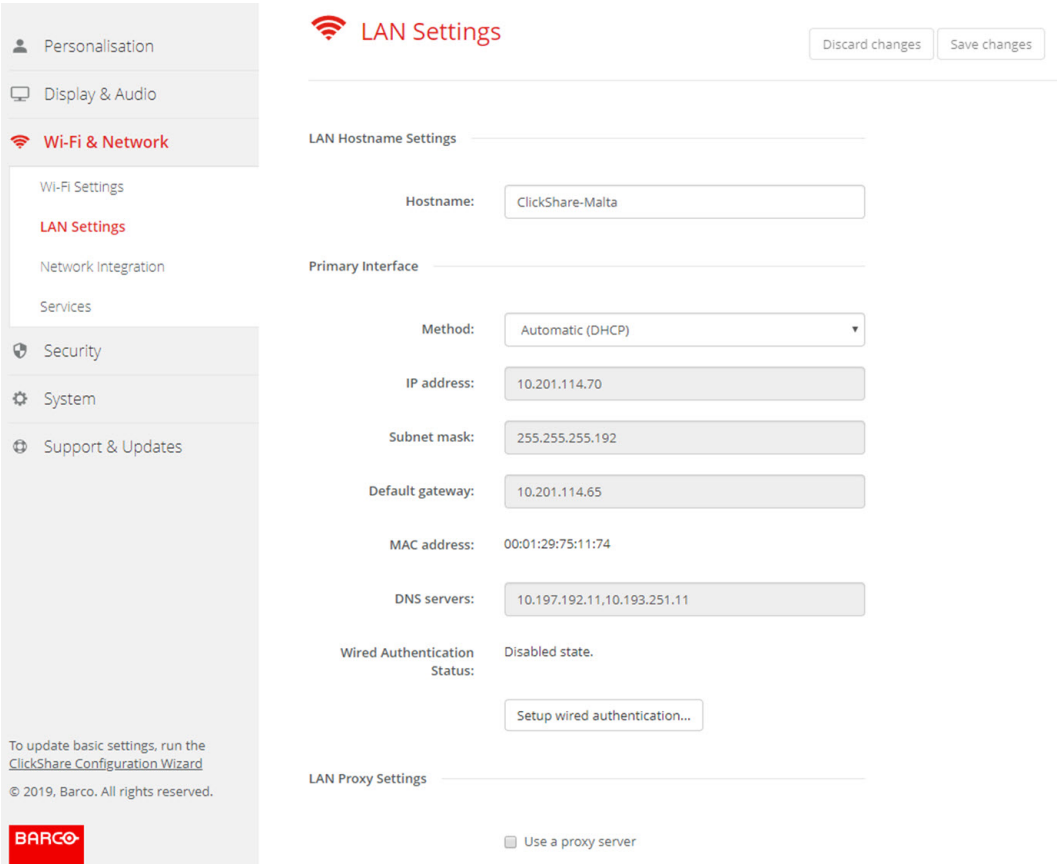


Image 6–22 Wired authentication

The setup wizard starts.

2. Select the authentication method. Click on the drop down and select the desired method.

   The following methods are available:

   - No authentication: no authentication mechanism will be applied to the wired interface.
   - EAP-TLS
   - EAP-TTLS
   - PEAP

6.13 LAN Settings, EAP-TLS security mode

About 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. For some organizations this might be too big of a hurdle, for those cases EAP-TTLS and PEAP provide good alternatives. Even though a 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 one of the most secure EAP methods. The only minor disadvantage, compared to PEAP and EAP-TTLS, is that the user identity is transmitted in the clear before the actual TLS handshake is performed. EAP-TLS is supported via SCEP or manual certificate upload.

How to setup EAP-TLS

1. Select Authentication Mode *EAP-TLS*.

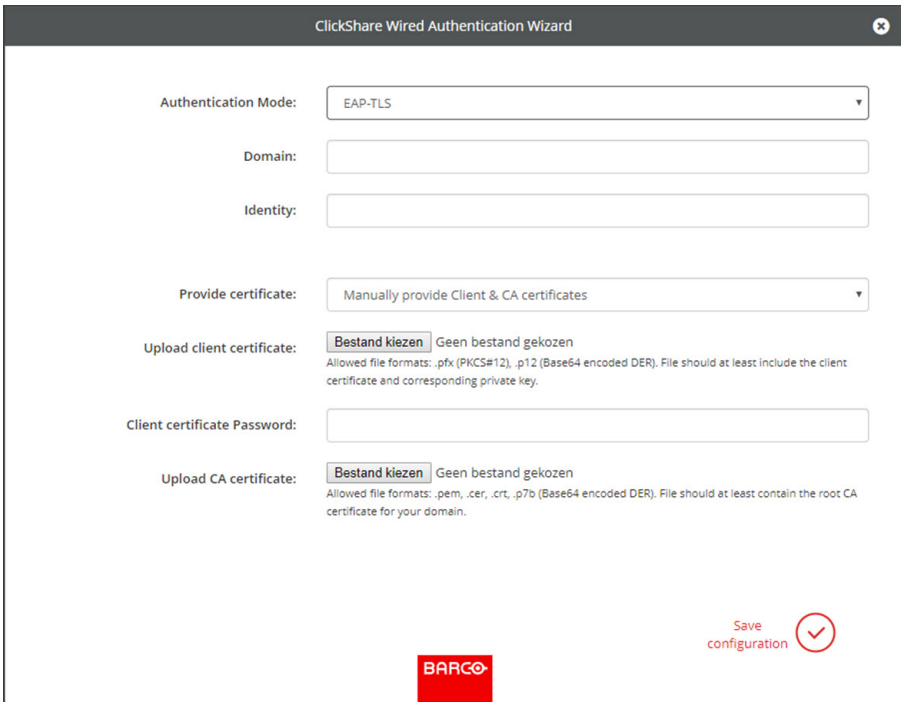


Image 6–23 EAP-TLS

2. Fill out the *Domain* and *Identity*.
3. Select the certification method. Click on the drop down box and select the desired method.
   - Manually provide Client & CA certificates
   - Auto enrollment via SCEP

Manually providing certificates

1. Upload client certificate. Click on Choose file and browse to the desired file.

   Allowed file formats:

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

   The should at least include the client certificate and corresponding private key.
2. Enter the Client certificate Password.
3. Upload CA certificate. Click on Choose file and browse to the desired file.

   The following formats are allowed:

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

   File should at least contain the root CA certificate for your domain.
4. Save configuration

Using SCEP

The Simple Certificate Enrolment Protocol (SCEP) is a protocol which enables issuing and revoking of certificates in a scalable way. SCEP support is included to allow a quicker and smoother integration of the ClickShare Base Unit and Buttons into the corporate network. Since most companies are using 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 Windows Server 2012. Initial support for other generic servers is available by extending the possible parameters to use for NDES/SCEP enrolment.

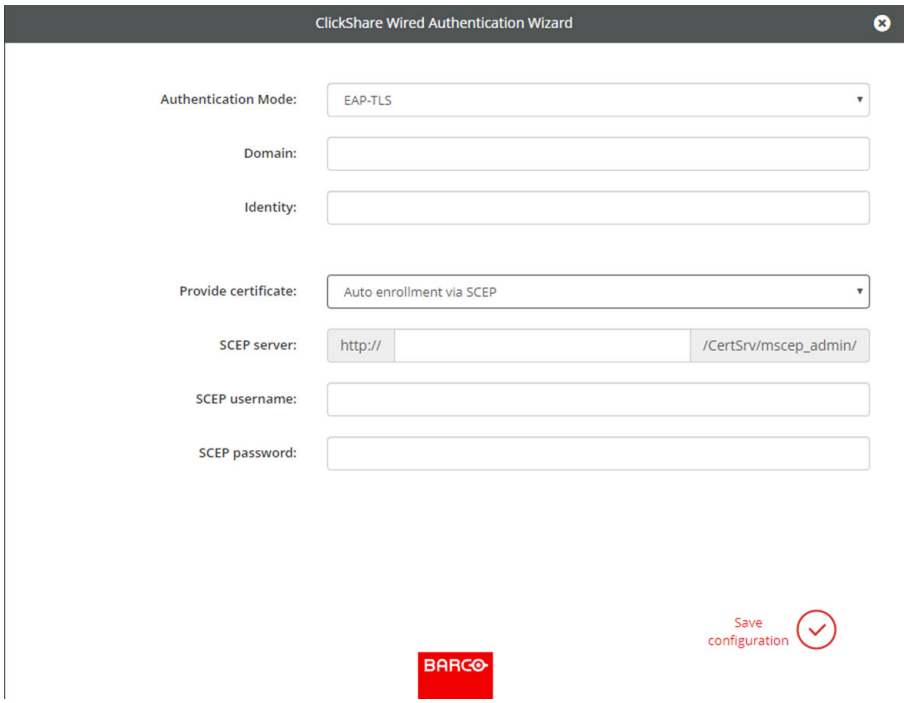


Image 6–24 EAP-TLS — SCEP

SCEP ServerIP/ hostname	This is the IP or hostname of the Windows Server in your network running the NDES service. By default HTTP is used. E.g.: http://myserver or http://10.192.5.1
SCEP User name	This is a user in your Active Directory which has the required permission to access the NDES service and request the challenge password. To be sure of this, the user should be part of the CA Administrators group (in case of a stand-alone CA) or have enroll permissions on the configured certificate templates.
SCEP 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.

Click on **Save configuration** to save the settings.

6.14 LAN Settings, EAP-TTLS security mode

About EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) is an EAP implementation by Juniper networks. It is designed to provide authentication that is as strong as EAP-TLS, but it does not require each user to be issued a certificate. 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 established based upon 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. Since EAP-TTLS is usually implemented in corporate environments without a client certificate we have not included support for this. If you prefer using client certificates per user we suggest using EAP-TLS.

How to setup EAP-TTLS

1. Select Authentication Mode *EAP-TTLS*.

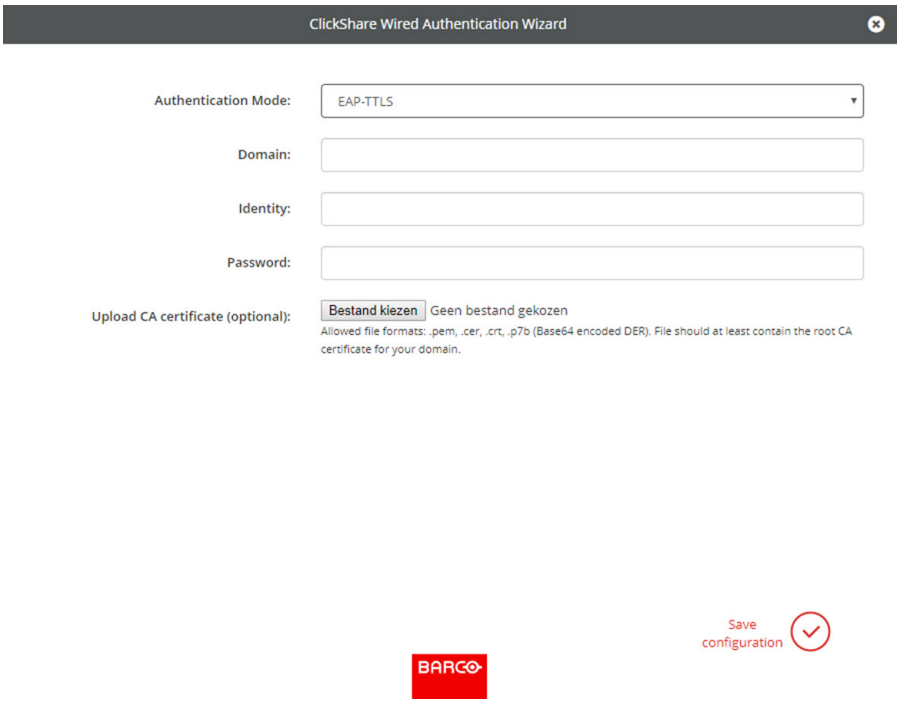


Image 6–25 EAP-TTLS

2. Fill out the *Domain* and *Identity*.

Domain	The company domain for which you are enrolling, should match with the one defined in your Active Directory.
Identity	Identity of the user account in the Active Directory which will be used by the ClickShare Buttons to connect to the corporate network.

3. Enter the *Password*.

   The corresponding password for the identity that you are using to authenticate on the LAN network. Per Base Unit each Button will use the same identity and password to connect to the corporate network.

4. Optionally, upload the CA certificate.

   The following formats are allowed:

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

   File should at least contain the root CA certificate for your domain.

5. Click **Save configuration**.

6.15 Services, mobile devices

ClickShare app

This function enables the possibility to connect with a mobile device using the ClickShare app to connect to the Base Unit.

It is enabled by default. When the Base Unit is integrated in the corporate network, it may be required to disable content sharing from the ClickShar app.

About streaming information via AirPlay

Before you can stream information and display it via ClickShare your device must be connected with the wireless network of the Base Unit. Then AirPlay must be activated on your device. For more information about activating AirPlay, consult the user guide of your device.

The supported versions of AirPlay can be found on Barco's website, *www.barco.com\clickshare*. The support of non-released version of these protocols cannot be guaranteed by Barco.

About streaming via Google Cast

Before you can mirror information and display it via ClickShare your device must be connected with the wireless network of the Base Unit. When activating Google Cast on your device an overview of the access points is given. For more information about using Google Cast, consult the user guide of your device.

The supported versions of Google Cast can be found on Barco's website, *www.barco.com\clickshare*. The support of non-released version of these protocols cannot be guaranteed by Barco.

Google Cast does not support a passcode.

Google Cast can only be used when the clock of the Base Unit is set correctly. If not Google Cast cannot make a connection with the Base Unit.

How to enable

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Services*.

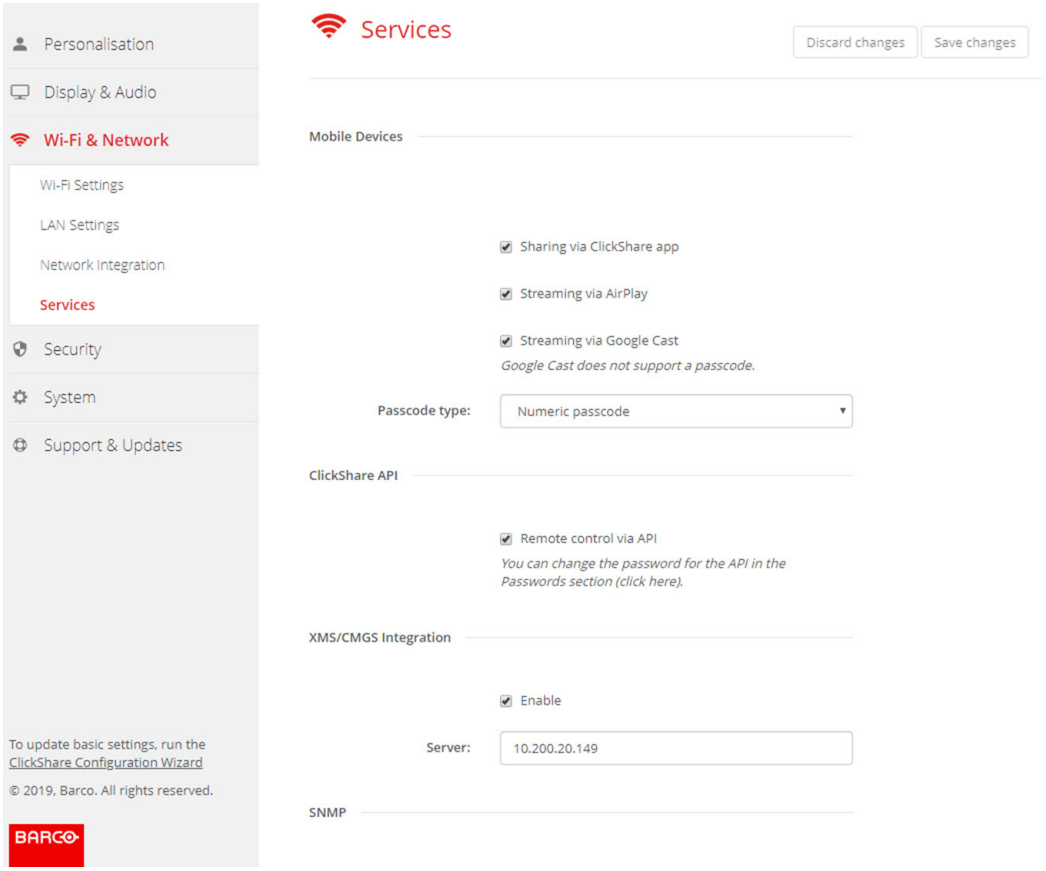


Image 6–26 Services, mobile devices

3. To allow sharing content via ClickShare app, check the check box in front of *Sharing via ClickShare app*.

   To allow streaming via AirPlay, check the check box in front of *Streaming via AirPlay*.

   To allow streaming (mirroring) via Google Cast, check the check box in front of *Streaming via Google Cast*.
4. To add a passcode, click on the drop down and select the desired passcode (not for Google Cast).

The following options are possible:

- No passcode
- Numeric passcode

5. Click **Save changes** to apply this setting.

   Access via mobile devices is activate.

6.16 Service, ClickShare API, remote control via API

About API settings

The API can be enabled or disabled, that means that the access to the unit from an external device can be allowed or can be blocked.

This functions in enabled by default.

How to enable

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Services*.

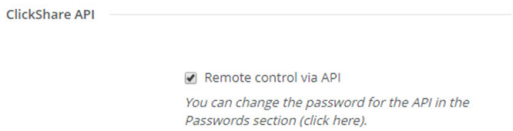


Image 6–27 ClickShare API setting

3. Check the check box in front of *Remote control via API* to enable this function.

   Checked: remote control via API is allowed. A password can be used to protect the access.

   Not checked: no remote control via API allowed.

6.17 XMS Server Integration

About the XMS Server integration

The CSE-200 Base Unit can be integrated within the company network and controlled via the XMS server application depending on the user rights.

How to integrate

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Services*.

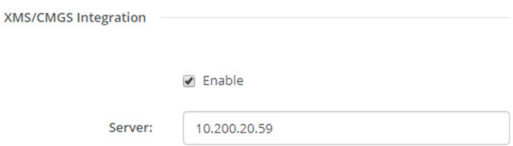


Image 6–28 XMS Server integration

3. Click in the XMS Server input field and enter the IP address or hostname of the XMS server.
4. Click **Save changes** to apply the settings.

6.18 Services, SNMP

About SNMP

Simple Network Management Protocol (SNMP) is an internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour. In general a SNMP management suite (running on a server) communicates with an SNMP agent (running on the device). The SNMP agent collects and exposes device information in the form of variables according a MIB (Management Information Base). SNMP management suites will be able to approach ClickShare devices via SNMP protocol for requesting device information.

SNMPv3 is supported.

How to enable

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Services*.
3. Scroll to *SNMP*.

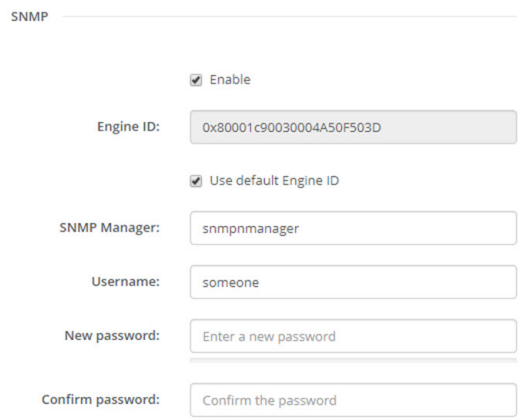


Image 6–29 Service, SNMP

4. Check the check box in front of *Enable*.

   The configuration fields become available.

How to configure

1. When using the default *Engine ID*, make sure the check box before *Use default Engine ID* is checked.

   The default engine ID is a combination of the Barco Enterprise Number with the MAC-address (eth0).

2. Fill out the *SNMP Manager* address.

   That is the host address which will receive the TRAP events/messages.
   Possible traps can be:

   - Alarm CPU temperature trap which indicates that CPU temperature exceeds the threshold.
   - Alarm Case Fan Speed trap which indicates the case fan is spinning too slow.
   - Alarm Process Not Running trap which indicates one of the monitored processes is not running.

3. Enter the *Username*.
4. Enter a new password and confirm that password.

6.19 Services, Remote Button Pairing

About remote Button pairing

When using ClickShare Button Manager, a stand alone software application on your computer, you can manage your Buttons on most of the types of ClickShare Base Units. Your computer can pair up to four Buttons at once with a known Base Unit. It is not necessary anymore to physically connect the Button with the Base Unit to pair it. This functionality makes it easy to use any Button with any Base Unit. Before you can use the ClickShare Button Manager a password must be configured on each Base Unit.

How to setup

1. Log in to the *Configurator*.
2. Click *Wi-Fi & Network* → *Services*.
3. Scroll to *Remote Button Pairing*.

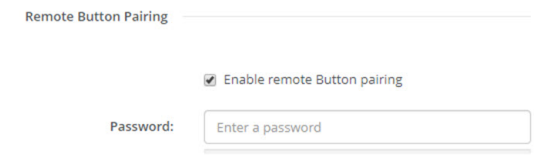


Image 6–30 Service, Remote Button pairing

4. Check the checkbox in front of *Enable remote Button pairing*.

   Checked: remote Button pairing is activated. A password should be entered to start the remote pairing from the Button Manager.

   Not checked: remote Button pairing is deactivated.
5. Click in the input field next to *Password* and enter a password.
6. Click **Save changes** to apply the settings.

6.20 Security, security level

About security levels

For the use of the ClickShare system, a security level can be set. By default, level 1 is activated. A security level is a predefined set of settings which are automatically set when a level is selected.

Level 1 : offers support for normal day-to-day operations in any organization.

Level 1 contains the standard security options and encryption of audio and video data.

The standard security options are:

- PIN code activation for mobile apps and Buttons,
- ClickShare Configurator (WebUI) access via HTTPS with login management,
- no wireless ClickShare Configurator (WebUI) access,
- SSID of Wi-Fi network is hidden.

Level 2 : this level offers a higher degree of security, fit for organizations that are more sensitive to security matters.

Level 2 contains the level 1 security and a mandatory PIN code for mobile devices. Alphanumeric PIN codes for mobile apps and Buttons and the Buttons require a certificate for pairing.

Level 3 : this level is used for organizations that have extremely strict requirements with regards to security.

Level 3 contains the level 2 security extended with blocking of mobile apps, downgrading firmware not possible and no wireless access to the Configurator (WebUI).

When a security level is set, the individual items included in that security level can be changed using the individual item in the Configurator. When changing an individual item the security level indication will be adapted accordingly, but no other settings will be changed automatically.

E.g. when level 3 is set and you change mobile app blocking to allowed, then the security level indication will change to level 2. But all other items initially in level 3 remains in the level 3 state.

To reset your individual changes, select the desired security level and click **Save changes**.

Changing the security level will require a re-pairing of the Buttons.
Changing the security level from 1 to a higher level will change the compatibility setting for Buttons with certificate (R9861006D01). They cannot re-pair as long as the security setting is higher than level 1.

How to set the security level

1. Log in to the *Configurator*.
2. Click *Security* → *Security Level*.

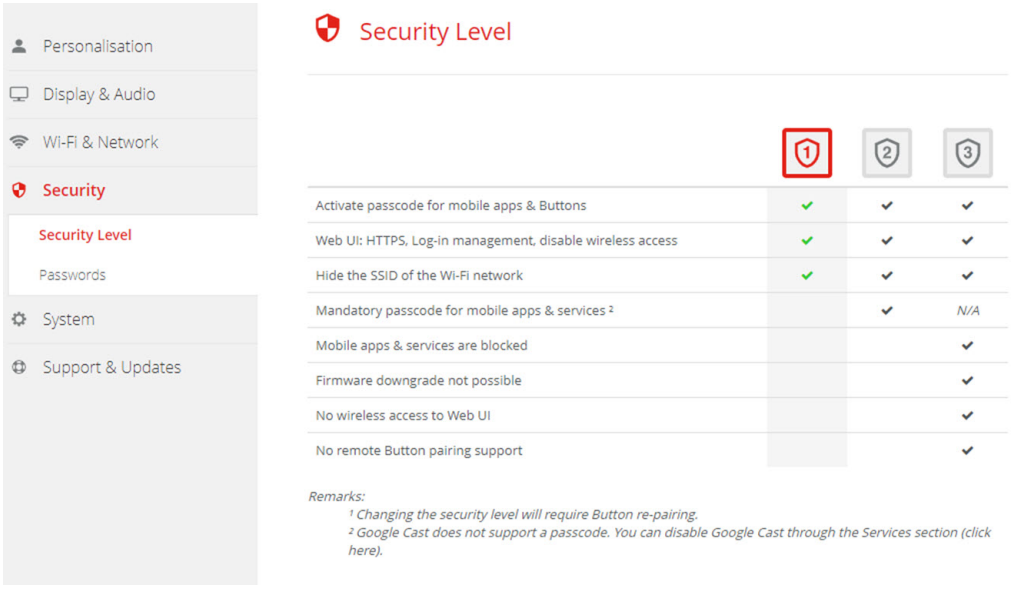


Image 6–31 Security levels

3. Select the desired security level icon.
4. Click **Save changes** to apply the setting.

6.21 Security, passwords

About passwords

To access the ClickShare Configurator (WebUI) a user name and password is needed. That password can be changed at any time to protect the *ClickShare Configuration* settings.

The ClickShare API access is password protected. That password can be changed in the ClickShare Configurator.

Changing the ClickShare Configurator password

1. Log in to the *Configurator*.
2. Click *Security* → *Passwords*.

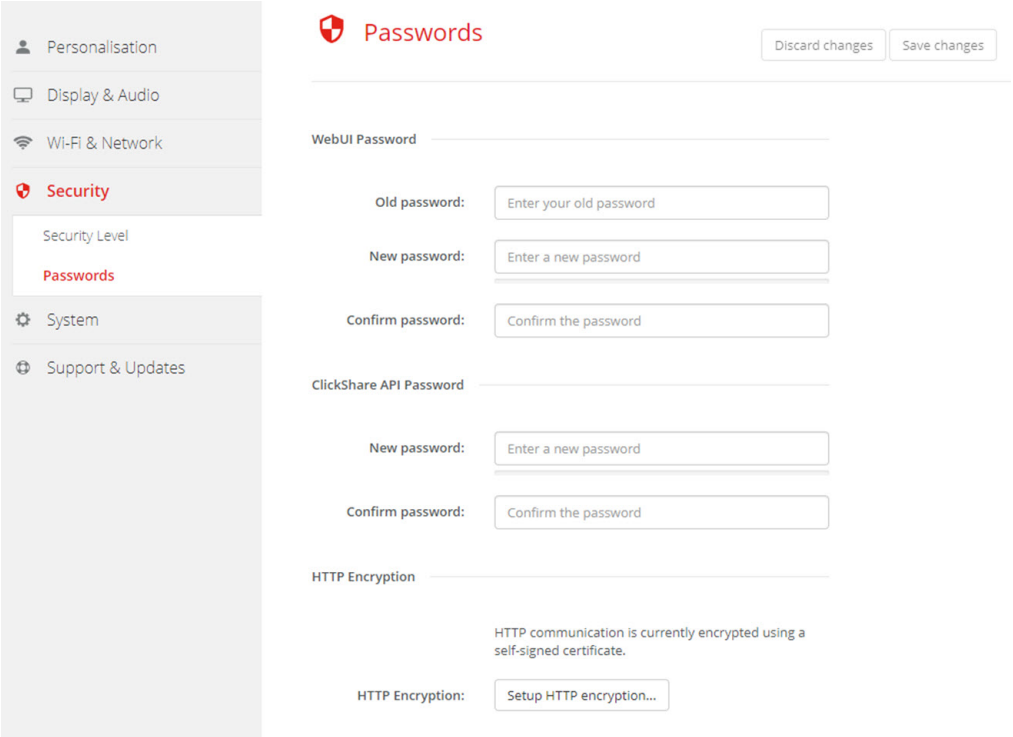


Image 6–32 Passwords

3. Click in the *WebUI Password* pane in the input field next to *Old password* and enter the old password.
4. Click in the input field next to *New password* and enter a new password.
5. Click in the input field next to *Confirm password* and enter the new password again.
6. Click **Save changes** to apply.

Changing the ClickShare API Password

1. Log in to the *Configurator*.
2. Click *Security* → *Passwords*.
3. Click in the *ClickShare API Password* pane in the input field next to *New password* and enter the new password.
4. Click in the input field next to *Confirm password* and enter the new password again.
5. Click **Save changes** to apply.

6.22 Security, HTTP Encryption

About HTTP encryption

Custom certificates for HTTPS can be uploaded to the ClickShare Base Unit. Custom certificates can as such replace the default self-signed ClickShare certificates for better compliance with company policies and have the advantage that privacy errors when browsing to the ClickShare Configurator can be avoided.

How to create a custom certificate

1. Log in to the *Configurator*.
2. Click *Security* → *Passwords* and scroll to *HTTP Encryption*.
3. Click **Setup HTTP encryption...** .

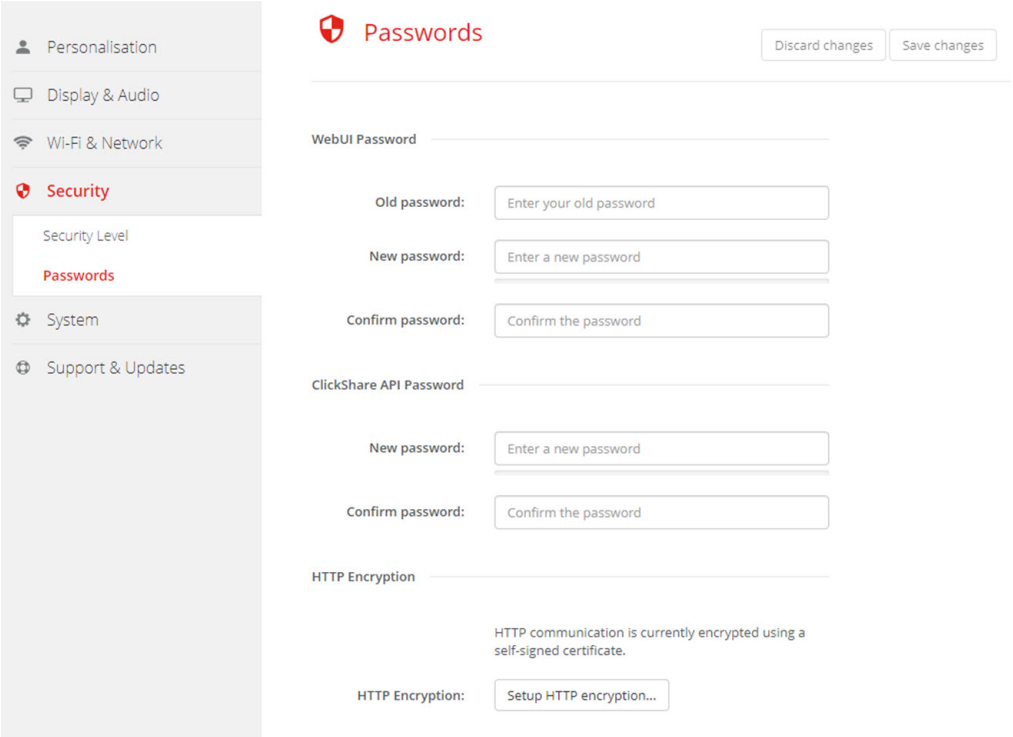


Image 6–33 HTTP Encryption

4. Choose the HTTP Encryption Mode. Check the corresponding radio button.

Image 6–34 HTTP encryption mode

The following modes are possible:

- Upload Certificates
- Create Certificate Signing Request
- Generate ClickShare Self Signed Certificate

5. To create a certificate signing request, check the corresponding radio button and click **Next** (right arrow).
6. Enter the necessary details to create a Certificate Signing Request.

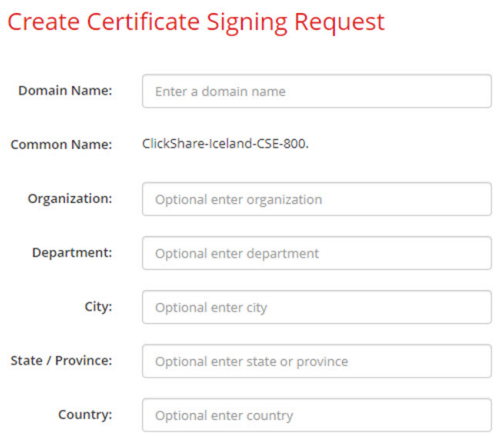


Image 6–35 Certificate signing request

The following items are possible:

- Domain name.
- Organization.
- Department.
- City.
- State / Province
- Country

7. Click **Next** (right arrow)

   A CRS is created and can be downloaded.

8. Click **Download CSR**.

Upload a certificate

1. Click *Security* → *Passwords* and scroll to *HTTP Encryption*.
2. Click **Setup HTTP encryption...** .
3. Choose Upload Certificate.

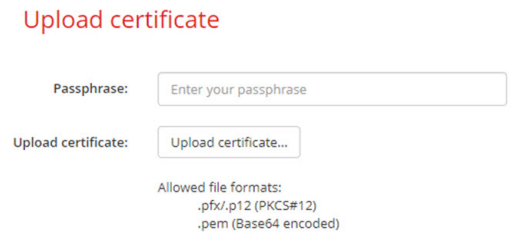


Image 6–36

The Upload certificate window opens.

4. Enter your passphrase and click **Upload certificate...** .

   A browse window opens.

5. Browse to the certificate file and click **Open**.

   A certificate can have the following formats:

   - .pfx/.p12 (PKC#12)
   - .pem (Base64 encoded)

6. Click **Finish configuration**.

6.23 Status information Base Unit

Status information

The following information can be found:

- Model information, name and part number
- Serial number
- Firmware version
- First used
- Last used
- Current uptime: time since last startup
- Lifetime uptime: time used since first startup
- Overall status

Base Unit restart

1. Log in to the *Configurator*.
2. Click *Support → Base Unit Status*.

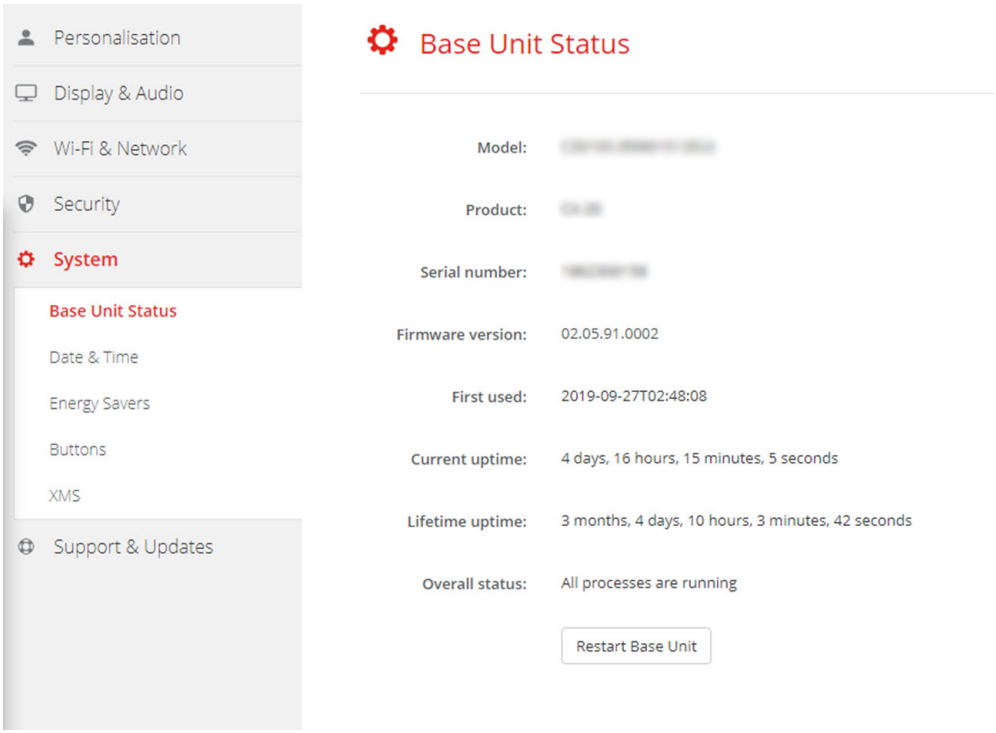


Image 6–37

3. To restart the Base Unit, click on **Restart Base Unit**.

   A ClickShare system reboot message with progress bar is displayed while rebooting takes place.

   When the reboot is finished, a re-login is necessary.

6.24 Date & Time setup, manually

About Date & Time setup

The date and time can be set manually using the time zone indication or using at least one NTP servers.

How to setup

1. Log in to the *Configurator*.
2. Click *System* → *Date & Time*.

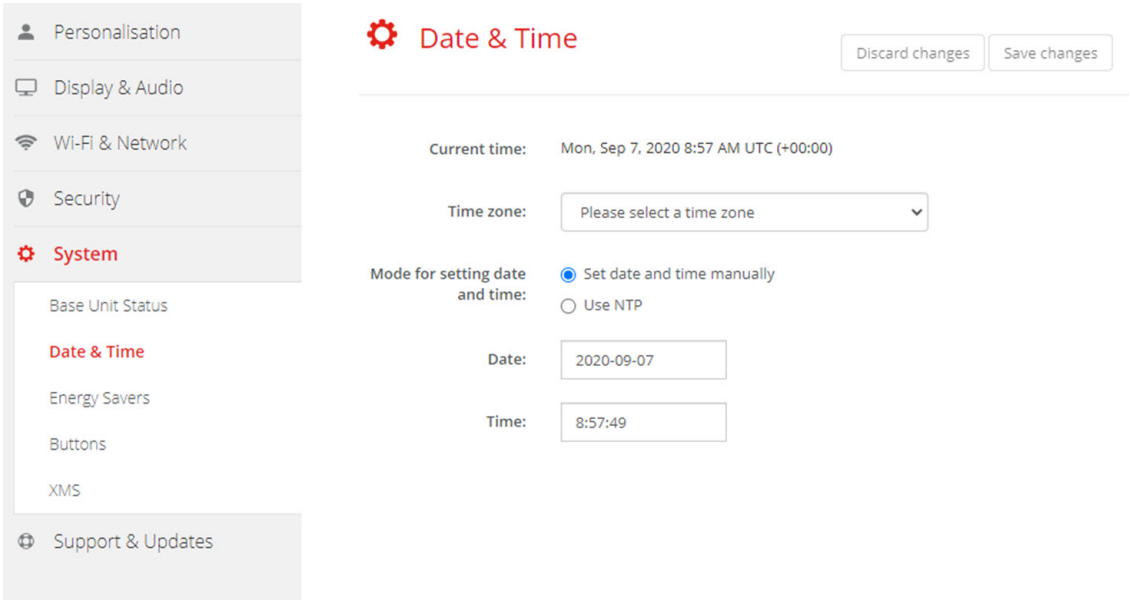


Image 6–38 Manual time & date update

The current time is indicated next to *Current time*.

3. Select your time zone. Click on the drop down box next to *Time zone* and select the corresponding time zone.
4. Check the radio button in front of *Set time and date manually*.
5. To change the date, click in the input field next to *Date*.

   A calendar window opens. The current date is indicated with a red background.

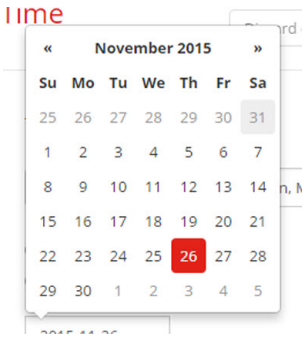


Image 6–39 Date selection

6. To change the month, click on the left or right arrows next the month name until the desired month and year are obtained.

   Click on a number in the number field to setup the day.
7. To change the time, click in the time field next to *Time*.

   A window with 3 scroll counters open.

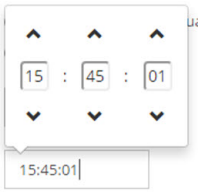


Image 6–40 Time setup

8. Click on the up down arrow of each scroll counter until the correct hour, minutes and seconds are obtained.
9. Click **Save changes** to apply.

6.25 Date & Time setup, time server

About using NTP server

The clock is continuously synchronized with an external time server and the deviation is in the order of milliseconds. Extra time servers can be added.

As long as there is no synchronization with a time server the status is indicated as disabled.

How to setup

1. Log in to the *Configurator*.
2. Click *System* → *Date & Time*.

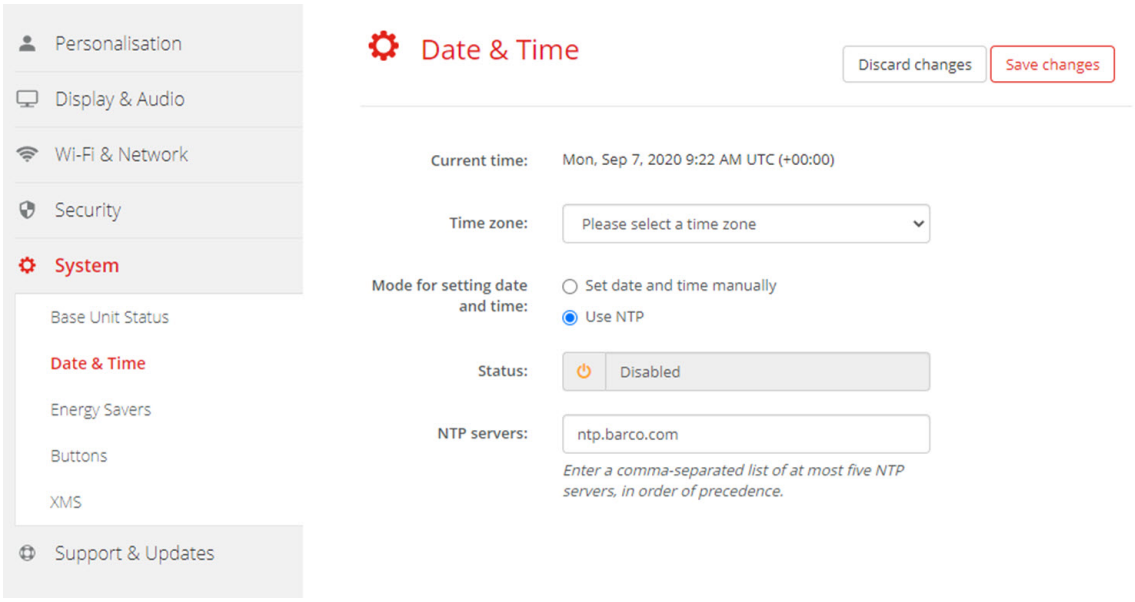


Image 6–41 Time server setup

The current time is indicated next to *Current time*.

3. Check the radio button next *Use NTP*.
4. Enter a NTP server address next to *NTP servers*. Enter the IP address or server name.

   Note: Multiple servers (maximum 5) can be added, separated by a comma.

5. Click **Save changes** to apply.

   A synchronization with the NTP server takes place. The status field indicates the progress.

6.26 Energy savers

About standby

Standby after (minutes): If there is no client connection detected during the standby timeout period, the Base Unit will enter the selected standby mode.

Default setting: Time to standby: 10 min, the Base Unit will enter the Eco standby mode.

Eco standby

When the Base Unit enters ECO standby mode, it will disable the HDMI output signal and go in low power mode. The Base Unit's LEDs will be breathing white to indicate the ECO standby mode.

Power consumption in Eco standby: 2.6W

The Base Unit will wake up with one of the following actions:

- Button or app connecting with the Base Unit
- Press the standby button on the Base Unit
- "Wake up" signal over the network
- Pairing a Button on the Base Unit's USB port
- Detection of display hot plug

Deep standby

When the Base Unit goes in Deep standby mode, it will shut down all processes, including the Wi-Fi access point and the (secondary) LAN connection.

For devices with two LAN interfaces (e.g. CSE-800), when there is an active network connected to the primary LAN connection and Corporate network is enabled, the primary LAN interface will remain active and the Base Unit's LEDs will be breathing white to indicate this standby mode. Otherwise, The Base Unit's LEDs will be dark.

Power consumption in Deep standby: 0.4W

The Base Unit will wake up when the standby button on the Base Unit is pressed, or

when the primary LAN interface remains active, a detection of HDMI input hot plug or Button or app connecting with the Base Unit's primary LAN interface.

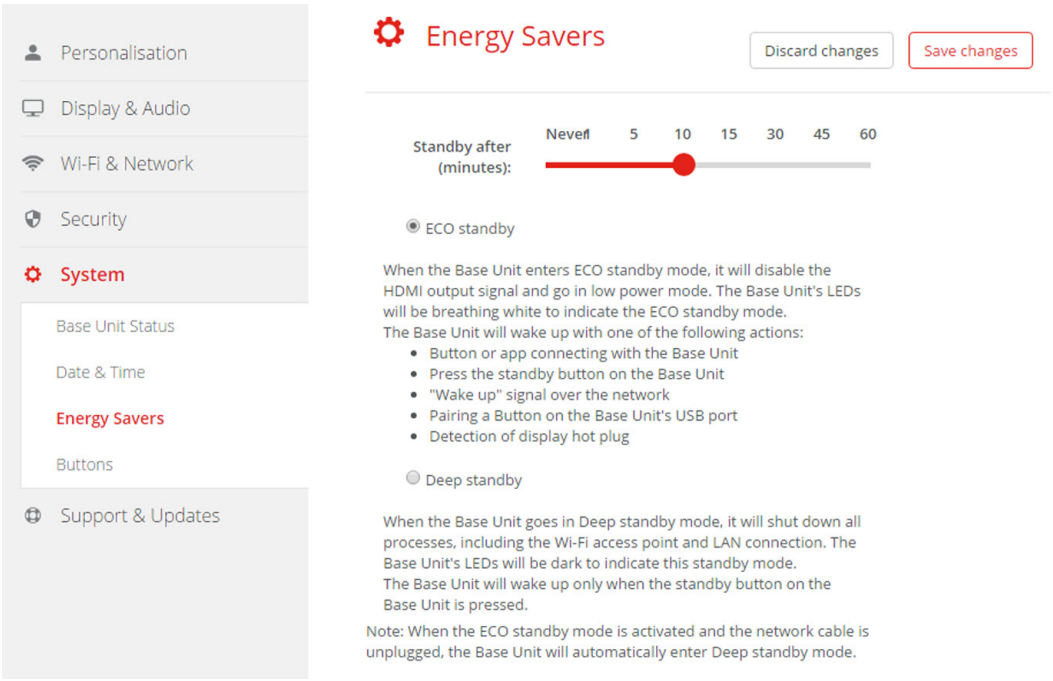


Image 6–42 Energy savers

How to change the display timeout and standby mode

1. Log in to the *Configurator*.

2. Click *System* → *Energy Savers*.
3. To set a display time out, move the slider to the left or to the right until the desired standby timeout is reached.
4. To select a standby mode, select the radio button before *Eco standby* or *Deep standby*.

6.27 Buttons

About Buttons

The Button page indicates to which Base Unit the Buttons are connected. It indicates also the current state.

All Buttons used with the Base Unit are indicated in the Buttons List. The list contains the state, the signal strength, the serial number, the firmware version, the number of connections and last connection.

It is possible to update the software of the Buttons over Wi-Fi.

To edit the settings

1. Log in to the *Configurator*.
2. Click *System* → *Buttons*.

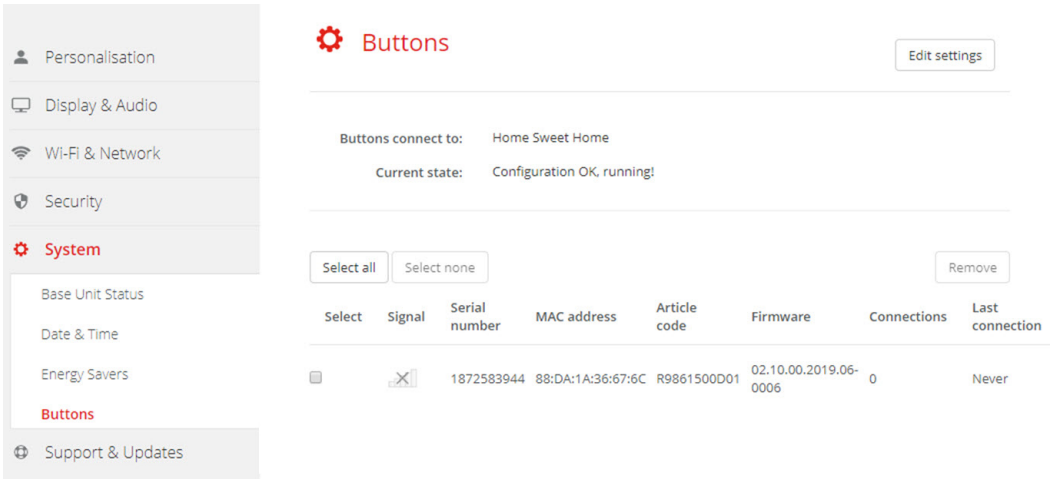


Image 6–43 Buttons overview

The current state is indicated and the list of Buttons is given.

3. Click **Edit settings**.
4. Select to which access point the Buttons are connected. Click on the drop down list next to *Buttons connect to* and select the desired point.

   Depending on the selection, internal access point or external access point, settings should be filed out.

   For an internal access point, no settings are needed.

6.28 Buttons, External access point

Overview

The selection of a security mode for the connection between the Buttons and the corporate access points can be done in the ClickShare Configurator. When configuring the Buttons to connect to an ‘External Access Point’ , the authentication mode can be selected:

- Security mode EAP-TLS, see “*Buttons, External access point, mode EAP-TLS*”, page 94.
- Security mode EAP-TTLS, “Buttons, External access point, mode EAP-TTLS”, page 95.
- Security mode PEAP, “Buttons, External access point, mode PEAP”, page 96.
- Security mode WPA2-PSK, “Buttons, External access point, mode WPA2-PSK”, page 97.

6.29 Buttons, External access point, mode EAP-TLS

How to fill out

1. Fill out a *Corporate SSID*.

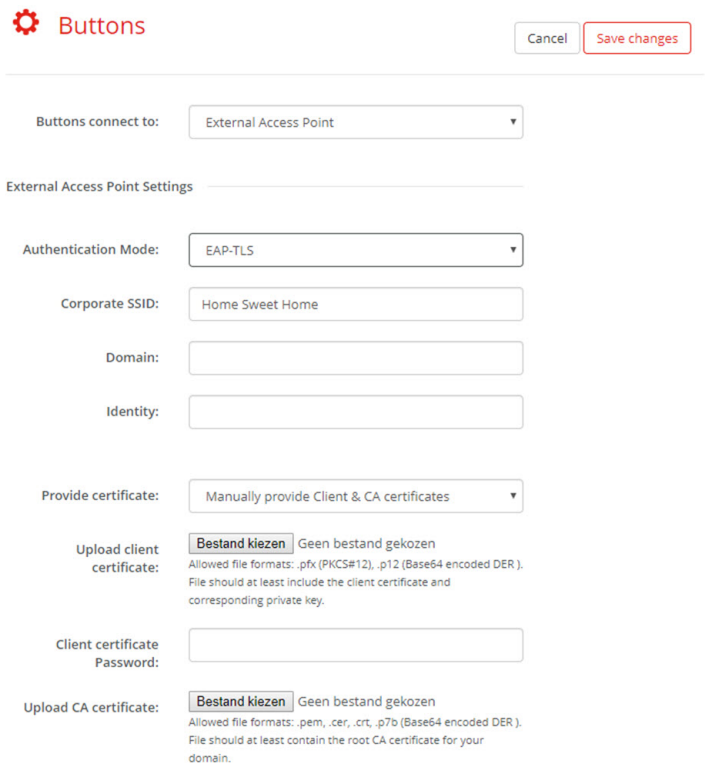


Image 6–44 Buttons, External access point, mode EAP-TLS

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

2. Fill out the *Domain* and *Identity*.
3. Select the certification method. Click on the drop down box and select the desired method.
   - Manually provide Client & CA certificates
   - Auto enrollment via SCEP

Manually providing certificates

1. Upload client certificate. Click on Choose file and browse to the desired file.

   Allowed file formats:

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

   The should at least include the client certificate and corresponding private key.
2. Enter the Client certificate Password.
3. Upload CA certificate. Click on Choose file and browse to the desired file.

   The following formats are allowed:

   - .pem
   - .cer
   - .crt

- .pb7 (Base64 encoded DER)

File should at least contain the root CA certificate for your domain.

4. Save Changes

Using SCEP

The Simple Certificate Enrolment Protocol (SCEP) is a protocol which enables issuing and revoking of certificates in a scalable way. SCEP support is included to allow a quicker and smoother integration of the ClickShare Base Unit and Buttons into the corporate network. Since most companies are using 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 Windows Server 2012. Initial support for other generic servers is available by extending the possible parameters to use for NDES/SCEP enrolment.

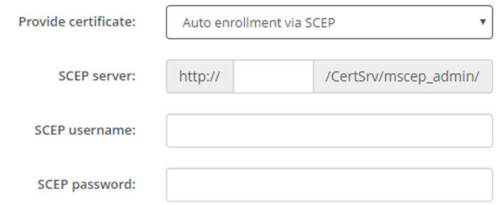


Image 6–45 Buttons, EAP-TLS, SCEP

SCEP ServerIP/ hostname	This is the IP or hostname of the Windows Server in your network running the NDES service. By default HTTP is used. E.g.: http://myserver or http://10.192.5.1
SCEP User name	This is a user in your Active Directory which has the required permission to access the NDES service and request the challenge password. To be sure of this, the user should be part of the CA Administrators group (in case of a stand-alone CA) or have enroll permissions on the configured certificate templates.
SCEP 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.

Click **Save Changes** to save the settings.

6.30 Buttons, External access point, mode EAP-TTLS

How to fill out the settings

1. Fill out a *Corporate SSID*.

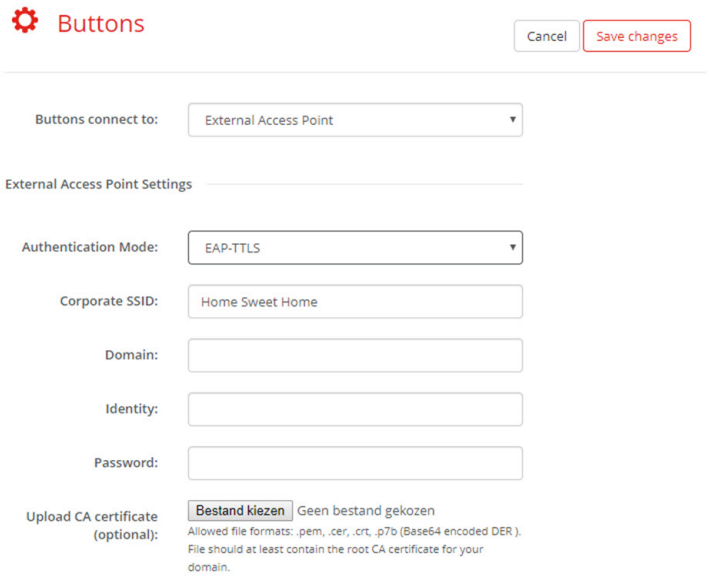


Image 6–46 Buttons, External access point, mode EAP-TTLS

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

2. Fill out the *Domain* and *Identity*.
3. Enter a *Password*.
4. Upload CA certificate. Click on Choose file and browse to the desired file.

   The following formats are allowed:

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

   File should at least contain the root CA certificate for your domain.
5. Click **Save Changes** to save the settings.

6.31 Buttons, External access point, mode PEAP

How to fill out the settings

1. Fill out a *Corporate SSID*.

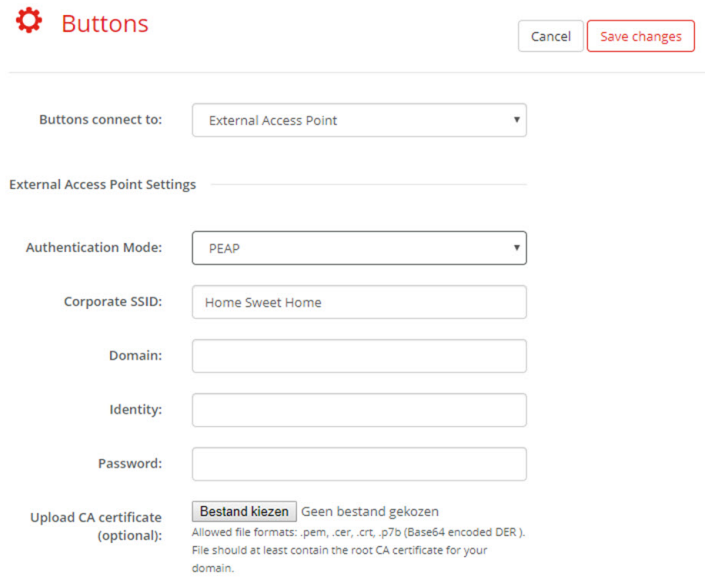


Image 6–47 Buttons, External access point, mode PEAP

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

2. Fill out the *Domain* and *Identity*.
3. Enter a *Password*.
4. Upload CA certificate. Click on Choose file and browse to the desired file.

   The following formats are allowed:

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

   File should at least contain the root CA certificate for your domain.
5. Click **Save Changes** to save the settings.

6.32 Buttons, External access point, mode WPA2-PSK

How to fill out the settings

1. Fill out a *Corporate SSID*.

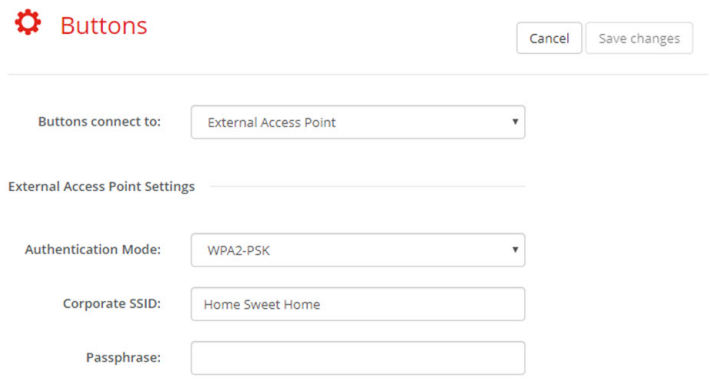


Image 6–48 Buttons, External access point, mode WPA2-PSK

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

2. Fill out Passphrase.

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

3. Click **Save changes** to save the settings.

6.33 Firmware Update

About Firmware update

The firmware of the Base Unit can be updated via the web interface. The latest version of the firmware is available on Barco's website.

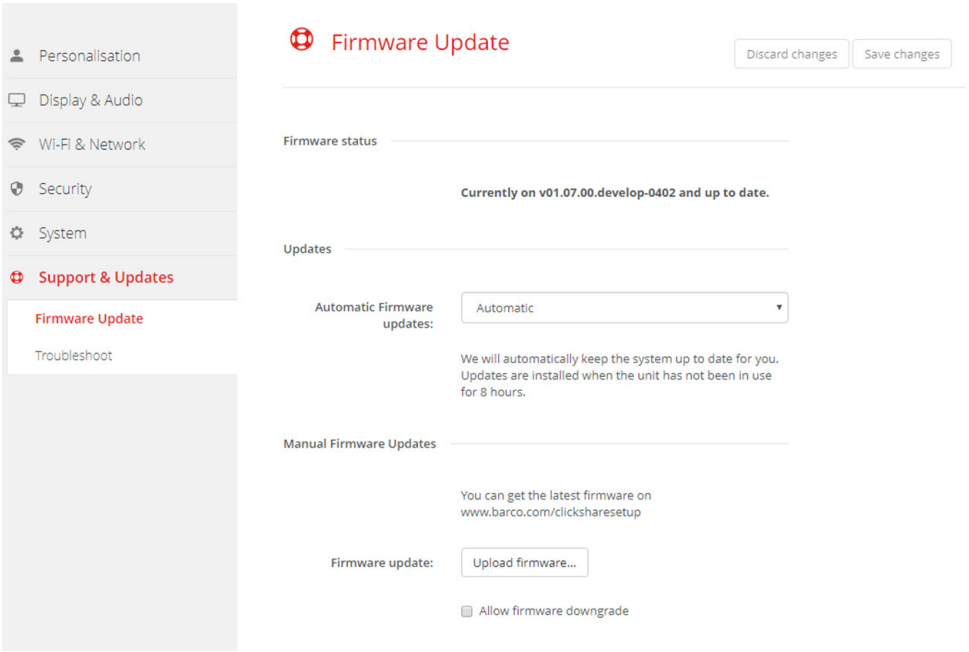


Image 6–49 Firmware update

About automatic firmware updates

There are 3 ways to configure automatic updates:

- Automatic: The system will automatically detect firmware updates and install them for you when it's not in use.
- Notify: The system will automatically detect firmware updates and notify you on the web interface dashboard and firmware page. The update can then be initiated via the *Support & Updates* > *Firmware* page
- Off: The system will not detect firmware updates and will not notify you.

Manual firmware update

1. Download the latest version of the firmware from Barco's website.
2. Log in to the *Configurator*.
3. Click *Support & Updates* → *Firmware*.
4. To upload a firmware version, click on **Upload firmware...**.

   A browser window opens.

5. Browse to the file with the new firmware and click **Open** to start the upload.

   Note: This should be an .enc file. You might have to unzip the file downloaded from Barco's website.

Note: Updating the software to the Base Unit takes several minutes. Progress can be followed on the meeting room display.

The Base Unit software is updated.

If a firmware downgrade is required on the Base Unit, check the check box in front of *Allow firmware downgrade*.

Firmware update without using the Configurator

Next to using the configurator to upgrade the firmware, the following ways are also possible:

- When your device is connected to a network and managed via the XMS (Cloud) management platform, the firmware can be upgrade via this Management solution. For more information on upgrading firmware in this way, consult Barco's web pages on XMS (https://www.barco.com/en/page/xms-cloud-management-platform).
- Download the firmware on a USB stick and plug in this USB in your device. For more information, see "*Firmware update*", page 104

6.34 Support & Updates, Troubleshoot, log settings

About logging

Both Button and Base Unit log data is saved in log files on the Base Unit. These log files can contain debugging information. They can be downloaded on a local computer and cleared on the Base Unit. Debug logging covers only a few hours before it will be overwritten. Therefore, it is important if you discover a problem with your system to download the logging immediately.

How to use

1. Log in to the *Configurator*.
2. Click *Support & Updates* → *Troubleshoot*.

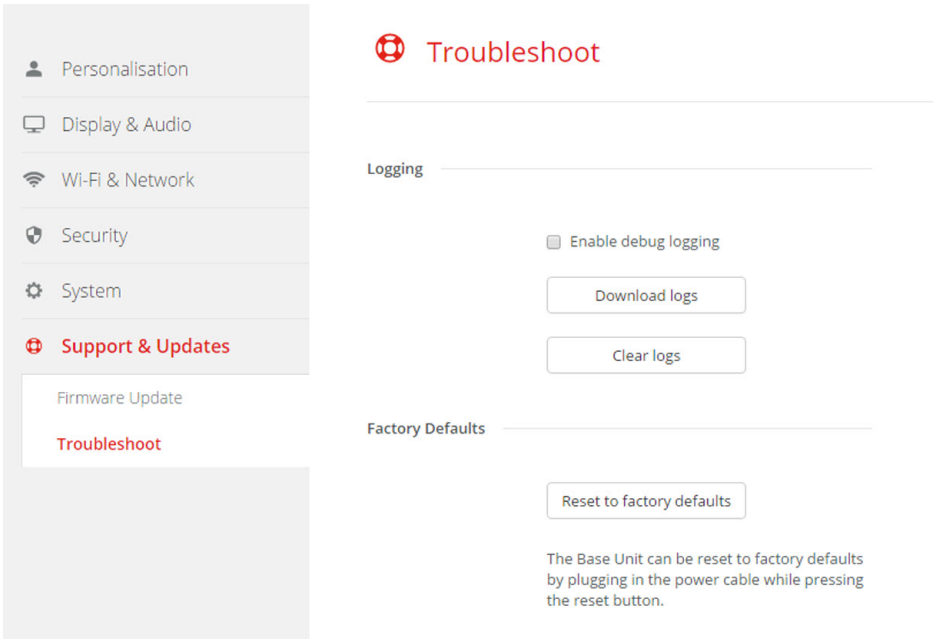


Image 6–50 Troubleshoot, logging

3. To create a debug log, check the check box next to *Enable debug logging*.
4. Reproduce the issue you want to report.
5. To download the current log file, click on **Download logs**.

6. To clear the current log file, click **Clear logs**.

6.35 Factory defaults

About default settings

The ClickShare Base Unit can return to the factory default settings.

The following settings are the defaults:

- Meeting room identification info is cleared.
- Language is set to English.
- Custom wallpapers are removed and the default wallpaper is restored.
- Standby timer is reset to 10 min.
- Hostname and SSID is set to *clickshare-serialnumber*.
- The SSID is broadcasted
- Wi-Fi password is reset to *clickshare*.
- The default Wi-Fi channel is set back to frequency 5 GHz, channel 36.
- The update history is cleared.
- The table with the associated Buttons is cleared.
- The admin password is reset to *admin*.
- Debug logging and remote logging are disabled.

Restoring to factory defaults will require a repairing of the Buttons used with this Base Unit and the setup flow has to be redone.

How to restore factory defaults

1. Log in to the *Configurator*.
2. Click *Support & Updates* → *Troubleshoot*.

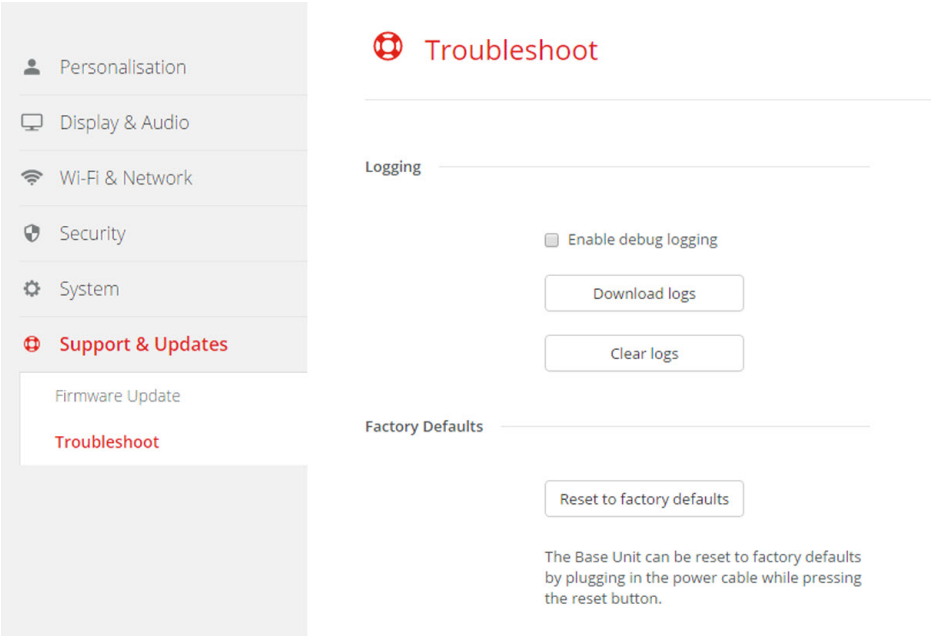


Image 6–51 Troubleshoot, factory defaults

3. Click **Reset to factory defaults**.

   The following message is displayed: “This action will remove all settings of the Base Unit and replace them with the default settings. Are you sure you want to continue?”

4. If you want to continue, click **Yes, remove all settings** otherwise click **No, I changed my mind**.

   When yes is clicked, the system starts a reboot.

Alternative way: The Base Unit can be reset to factory defaults by plugging in the power cable while pressing the reset button.

7 Firmware updates

7.1 Firmware update

During the first startup of the unit a typical wallpaper will be displayed which asks to update the unit.

Image 7–1

About Firmware updates

There are different ways to update the Base Unit software:

- via the Configurator, for more information, see “*Firmware Update*”, page 98.
- automatic update when connected to the network together with the central management via XMS solution.
- by copying the software on a USB stick.
- automatic update when connected in network together with the central management via XMS (only for CSE devices). For more information consult the XMS’s user guide which can be downloaded from Barco’s website (*www.barco.com/clickshare*).

To update the Base Unit software by copying the software on a USB stick

1. Download the latest version of the firmware from Barco's website, *www.barco.com/clickshare*. Click on **Support** and select the update firmware button of your device type.
2. Unzip the zip file.
3. Copy the ENC file to a USB stick.

   You can have multiple firmwares for multiple device types on the same stick.
4. Insert the USB stick into the USB port at the front of the Base Unit.
5. Follow the instructions on the meeting room screen.
6. When the on-screen message indicates that the process is finished, remove the USB stick.

   The Base Unit reboots.

8 Troubleshooting

8.1 Troubleshooting list

Problem solving

Problem	Cause	Solution
Quality of the image on the meeting room display is not satisfactory	The quality or length of the cable between the Base Unit and the display or the connection between these two.	• Replace the cable. • Use another cable.
	Bad resolution of the display The system can handle the average laptop resolution of 3 Megapixel. However, up or down scaling on the meeting room display can cause visible artefacts.	Change the resolution on the web interface and match it to the native resolution of the meeting room display.
Users have a bad wireless connection. The connection from the Button to the Base Unit keeps falling away.	Wireless congestion	• Use a Wi-Fi scanner to find a free wireless channel and select it via the web interface. You can use commercial as well as free online tools such as inSSIDer or Xirrus for this. Refer to “Wi-Fi settings”.
	Low signal strength	• Put the Base Unit closer to the meeting room table. • Change the orientation of the antennas at the back of the Base Unit. • Remove or limit as much as possible all obstructions between the Buttons and the Base Unit.
Web interface is not accessible	Browser	• Use another browser (version). • Check the browser settings.
	No connection	• There are three methods to access the web interface. Refer to the corresponding chapter of the documentation. • Check the proxy settings
Users do not get a CSE-200 drive when inserting the Button in their laptop.	• No automatic refresh of drives • Windows tries to assign the ClickShare drive to an already reserved drive letter	• Refresh your view on the laptop. • Use Microsoft Windows Disk Management to assign it to a free drive letter.
	Bad connection at USB port on the laptop	• Reconnect to the USB port. • Try another USB port. • Reboot the laptop.
	• Some types of USB devices might be blocked as a company policy. • USB port settings on the laptop might limit the usage of high power USB devices when on battery power.	If possible, change the USB port policy on the laptop.

Problem	Cause	Solution
Low video performance	Laptop performance	• Lower the screen resolution of the laptop. • Disable the hardware acceleration for video. • Use only a part of the display to show the video. • Right click ClickShare icon in system tray and click on Capture mode to toggle the current setting..
	Wireless connectivity	See “Users have bad connectivity”
Video is not shown on screen	Player uses overlays	Disable the usage of overlays in the preferences of the video player.
Some programs of Windows are not shown on the display	Use of overlays, 3D or hardware acceleration in the GPU	• Disable overlays or hardware acceleration in the GPU. • Disable AeroGlass in Windows 7 • Upgrade the Base Unit to the latest software version.
When using Windows 7 the following message about the Windows Aero color scheme appears: "Windows has detected your computer's performance is slow. This could be because there are not enough resources to run the Windows Aero color scheme. To improve...".	ClickShare uses resources from the GPU. In combination with other programs which do so, Windows 7 sometimes shows this message suggesting to disable Aero to improve the performance of your laptop.	It is safe to ignore this message and choose 'Keep the current color scheme'.
Your screen is not shown on the display when pressing the Button	You are the third person that wants to share content. Only two screens can appear simultaneously	Click and hold the button for 2 seconds to use the Show me full screen function.
	The ClickShare software is not running.	Go to the ClickShare drive and run the software.
Your content is removed from the display and the LEDs on the button are blinking white	Connection to the Base Unit is lost.	ClickShare tries to restore the connection automatically. If it fails, the LEDs on the Button start blinking red. Unplug the button from your laptop and try a new button.
Noting is shown on the displays at all.	The displays are switched off.	Switch on the displays.
	The display cable is not correctly connected	Insert the display cable to the display and the Base Unit.
	The display does not recognize or is not able to display the Base Unit output resolution.	Change the corresponding setting via the web interface.
	The Base Unit is in standby mode	Briefly push the standby button on the Base Unit or insert a button and run the ClickShare software.

Problem	Cause	Solution
Bad Wi-Fi connectivity	Congestion of the wireless channel	Use wireless network scan tools to look for free or the least congested channels.
	Metal cabinets, walls, construction elements, ... can cause reflections deteriorating the wireless signal.	Move the Base Unit to another place in the room.
	Obstructions between Buttons and Base Unit cause lowering of the wireless strength and quality.	Avoid placing it inside cabinets, false ceiling, below the table, behind a wall, in another room, ...
		Re-orient he Base Unit antennas
		Check out the ClickShare White paper on Wi-Fi See www.barco.com/clickshare.
Web Interface shows error in the processes “Wi-Fi Access Point Daemon” and/or “DHCP Server”	Configuration file is corrupted	Browse to the Configuration tab on the Web Interface and press “Load Default Settings”.
ClickShare Base Unit does not start up correctly	Configuration file is corrupted	Browse to the Configuration tab of the Web Interface and press “Load Default Settings”.
No LAN connection with the Base Unit	Wrong IP address	IP address is not within your LAN range.
		DHCP is not enabled.
No Wi-Fi connection with Base Unit	SSID not correct	Enter the correct SSID

Locate the problem you are experiencing in the table below and apply the solution.

Barco knowledge base and YouTube videos

Go to the product page on Barco’s website and select in the right column **Support**. You will get access to Barco’s *Knowledge base* and *Latest tutorial videos*. For more YouTube videos, consult https://www.youtube.com/user/barcoTV and select ClickShare.

Environmental information

9

9.1 Disposal information

Disposal Information

Waste Electrical and Electronic Equipment

This symbol on the product indicates that, under the European Directive 2012/19/EU governing waste from electrical and electronic equipment, this product must not be disposed of with other municipal waste. Please dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate these items from other types of waste and recycle them responsibly to promote the sustainable reuse of material resources.

For more information about recycling of this product, please contact your local city office or your municipal waste disposal service.

For details, please visit the Barco website at: *http://www.barco.com/AboutBarco/weee*

Disposal of batteries in the product

This product contains batteries covered by the Directive 2006/66/EC which must be collected and disposed of separately from municipal waste.

If the battery contains more than the specified values of lead (Pb), mercury (Hg) or cadmium (Cd), these chemical symbols will appear below the crossed-out wheeled bin symbol.

By participating in separate collection of batteries, you will help to ensure proper disposal and to prevent potential negative effects on the environment and human health.

9.2 Rohs compliance

Turkey RoHS compliance

Türkiye Cumhuriyeti: AEEE Yönetmeliğine Uygundur.

[Republic of Turkey: In conformity with the WEEE Regulation]

中国大陆 RoHS – Chinese Mainland RoHS

根据中国大陆《电器电子产品有害物质限制使用管理办法》（也称为中国大陆RoHS），以下部分列出了Barco产品中可能包含的有毒和/或有害物质的名称和含量。中国大陆RoHS指令包含在中国信息产业部MCV标准：“电子信息产品中有毒物质的限量要求”中。

According to the “Management Methods for the Restriction of the Use of Hazardous Substances in Electrical and Electronic Products” (Also called RoHS of Chinese Mainland), the table below lists the names and contents of toxic and/or hazardous substances that Barco’s product may contain. The RoHS of Chinese Mainland is included in the MCV standard of the Ministry of Information Industry of China, in the section “Limit Requirements of toxic substances in Electronic Information Products”.

零件项目(名称) Component Name	有毒有害物质或元素 Hazardous Substances or Elements					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr6+)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印制电路配件	x	0	x	0	0	0

Printed Circuit Assemblies 电(线)缆	x	0	x	0	0	0
Cables 底架	x	0	x	0	0	0
Chassis 电源供应器	x	0	x	0	0	0
Power Supply Unit 文件说明书	0	0	0	0	0	0
Paper Manuals						

本表格依据SJ/T 11364的规定编制

This table is prepared in accordance with the provisions of SJ/T 11364.

O: 表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下.

O: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in GB/T 26572.

X: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求.

X: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in GB/T 26572.

在中国大陆销售的相应电子信息产品（EIP）都必须遵照中国大陆《电子电气产品有害物质限制使用标识要求》标准贴上环保使用期限（EFUP）标签。Barco产品所采用的EFUP标签（请参阅实例，徽标内部的编号使用于指定产品）基于中国大陆的《电子信息产品环保使用期限通则》标准。

All Electronic Information Products (EIP) that are sold within Chinese Mainland must comply with the “Marking for the restriction of the use of hazardous substances in electrical and electronic product” of Chinese Mainland, marked with the Environmental Friendly Use Period (EFUP) logo. The number inside the EFUP logo that Barco uses (please refer to the photo) is based on the “General guidelines of environment-friendly use period of electronic information products” of Chinese Mainland.

Image 9–1

限用物質含有情況標示聲明書 (Declaration of the Presence Condition of the Restricted Substances Marking) — Taiwan RoHS compliance

設備名稱： 影音共享控制中心， 型號（型式）： CSE-200

Equipment name: wireless presentation system, Type designation: CSE-200

	限用物質及其化學符號 Restricted substances and its chemical symbols					
單元 Unit	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr6+)	多溴聯苯 Poly-brominat-ed biphenyld (PBB)	多溴二苯醚 Poly-brominated diphenyl ethers (PBDE)
電路板 Printed Circuit Assemblies	—	O	—	O	O	O

電（線）纜 Cables	—	O	—	O	O	O
機箱 Chassis	—	O	—	O	O	O
電源供應器 Power Supply Unit	—	O	O	O	O	O

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2：“○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝—〞係指該項限用物質為排除項目。

Note 3：The “—” indicates that the restricted substance corresponds to the exemption.

9.3 Importers contact information

Contact

To find your local importer, contact Barco directly or one of Barco's regional offices via the contact information given on Barco's web site, *www.barco.com*.

R5900023 /16 | 2020-09-16

Barco NV | Beneluxpark 21, 8500 Kortrijk, Belgium
Registered office: Barco NV | President Kennedypark 35, 8500 Kortrijk, Belgium
www.barco.com