Collaboration Management Suite

User guide

R5900020/03
30/03/2017

Visibly yours

Product revision

Software version: 1.3

Barco NV
Beneluxpark 21, 8500 Kortrijk, Belgium
Phone: +32 56.23.32.11
Fax: +32 56.26.22.62
Support: www.barco.com/en/support
Visit us at the web: www.barco.com

Registered address: Barco NV
President Kennedypark 35, 8500 Kortrijk, Belgium
Phone: +32 56.23.32.11
Fax: +32 56.26.22.62
Support: www.barco.com/en/support
Visit us at the web: www.barco.com

Printed in Belgium

Copyright ©

Trademarks

Barco ClickShare End-User License Agreement (EULA/Software License)

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE OPENING OR DOWNLOADING AND USING SOFTWARE OR HARDWARE PROVIDED TO YOU BY BARCO AS IT CONTAINS THE TERMS AND CONDITIONS BY WHICH BARCO OFFERS TO LICENSE THE SOFTWARE. BY OPENING THE SOFTWARE PACKAGE, OR USING THE HARDWARE IN WHICH THE SOFTWARE IS EMBEDDED, YOU AGREE TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT.

The Software as supplied by BARCO is licensed, not sold to you, on a non-exclusive basis for use only under the terms of this license, and BARCO 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.

By installing, executing and/or using the Software, either as initial version or as an upgrade, update, patch or enhancement of a prior release, this Software License shall supersede any terms and conditions previously agreed upon (whether or not in writing) between Barco and you with respect to the subject matter of this Software License and such previous terms shall from the date hereof cease to have any force or effect; provided, however that this Software License shall not be construed as a renunciation, discharge or waiver of any right or remedy provided in any terms and conditions previously agreed upon with respect to a failure of either party to perform any of its obligations under any terms and conditions previously agreed upon.

Software Specifications

The Software contains the following software products: ClickShare

Software License Terms

1. This Software License is between you and BARCO NV, a corporation organized and existing under the laws of Belgium registered under number BE 0473.191.041, Commercial Companies' Register of Kortrijk, having its registered office President Kennedypark, 35 at B-8500 Kortrijk, Belgium ("Barco") for the use of the Software.
   You hereby undertake to inform all users authorized by you to make use of the computing device on which the Software is loaded/installed ("Authorized Users") of the terms of this Software License and to bind all Authorized Users to accept all such terms of this Software License as applies to them.
2. Barco grants you a limited, non-exclusive, non-assignable, non-transferable user license (without the right to grant sublicenses). Unless specifically agreed upon otherwise between you and Barco or unless specifically allowed by the Software (or its DRM management) itself, i) the license under this Software License applies to one (1) copy of the Software to be used on one single computing device and ii) 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 active user connected to a computing device on which the Software is being used.
   You and Authorized Users are entitled to use the Software for the purposes and in the manner set out in this Software License (and documentation), but neither you nor any Authorized User are entitled to: (i) sell or grant a security interest in the Software to other parties in any way, or to rent, lease or sub-license the Software to others without the express prior written consent of Barco; or (ii) exploit the Software or any of its component parts for any commercial purpose, other than use by you and/or Authorized Users of the Software.
   Neither you nor any Authorized User may, whether in whole or in part, copy, translate, reverse engineer, derive source code from, modify, disassemble, decompile, create derivative works based on the Software, or remove any proprietary notices or labels on the Software, save as may be permitted by law or this Software License, without the prior consent, in writing, of Barco.
3. Barco (and Barco's licensors, as appropriate) retain ownership of all intellectual property rights in the Software and any copies you or any Authorized User may make of such Software. The Software is protected by national copyright laws, international copyright treaties and conventions, and other applicable laws. All rights not expressly licensed to you in this Software License are reserved to Barco and Barco's licensors, as appropriate. The Software contains certain other licensed materials and Barco's licensors may protect their rights in the event of any violation of this Software License.

4. Barco shall hold you harmless, defend and indemnify you from and against direct damages, losses and expenses arising from infringement or alleged infringement of any patent, trademark or copyright of such third party by the license and the right to install the Software as permitted by this Software License and settle at its sole expense any amounts awarded in a final judgment or settlement resulting therefrom, under the condition that (i) you promptly notify Barco in writing after a claim has been asserted against you or the commencement of any claim, action, suit or proceeding (whichever is the earlier), and (ii) Barco shall be allowed to assume sole control of the defense and any settlement negotiations related to any claim, action, suit or proceeding, and (iii) you shall not negotiate, settle or compromise any claim, action, suit or proceeding without the prior written consent of Barco and (iv) you, at your cost, shall cooperate with Barco and provide assistance and support, as may reasonably be required by Barco, in connection with the defense and any settlement negotiations related to any claim, action, suit or proceeding. Barco shall have no indemnity obligation for any Software, or any portion thereof, (i) that is based on specifications, drawings, models or other data furnished by you or, (ii) that is not provided by Barco or, (iii) that is modified, in spite of the prohibition for you to modify the software or, (iv) to the extent that you continue allegedly infringing activity after having been provided modifications that avoid the alleged infringement, or (v) where the use of the Software, or the combination or thereof with other Software, processes or materials or the distribution thereof rather than the Software itself is the primary cause of an alleged infringement. In case it has been determined by a finally awarded judgment that Barco infringed or misappropriated such third party rights or earlier, at Barco's discretion, it may, at its option and cost, (i) modify the Software in such a way that it shall not infringe upon or misappropriate the rights of the third party or (ii) obtain for you a license or other right to use the rights allegedly infringed or (iii) replace the Software in question with non-infringing Software. The remedies set forth in this paragraph shall constitute your sole and exclusive remedy and Barco's sole and exclusive liability for a third party claim that the Software infringes or misappropriates any intellectual property right of a third party.

5. The duration of this Software License 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), with no termination date, unless otherwise specified. You may terminate this Software License at any time by destroying all copies of the Software then in your possession and returning all associated materials and documentation, to Barco or the appointed Barco reseller that sold or provided these to you. Barco may terminate this Software License forthwith by informing you at any time if you and/or any Authorized User are in breach of any of the Software License's terms.

6. 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 SUCH ERRORS WILL BE CORRECTED BY BARCO AND YOU ARE SOLELY RESPONSIBLE FOR ALL COSTS AND EXPENSES ASSOCIATED WITH RECTIFICATION, REPAIR OR DAMAGE CAUSED BY SUCH ERRORS.
   YOU ALSO ACKNOWLEDGE AND AGREE THAT:
   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 AN AMOUNT OF 250 EURO IN THE AGREGATE (OR TO THE MAXIMUM EXTENT PERMITTED BY LAW WHERE NO FURTHER EXCLUSION IS LEGALLY ALLOWED).
   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.
   YOU HEREBY AGREE TO INDEMNIFY, KEEP INDEMNIFIED, DEFEND AND HOLD HARMLESS BARCO AND BARCO'S AFFILIATES AND SUBSIDIARIES FROM AND AGAINST ANY AND ALL ACTIONS, PROCEEDINGS, LIABILITY, LOSS, DAMAGES, FEES AND COSTS (INCLUDING ATTORNEYS" 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. You shall treat as confidential all information obtained from the other pursuant to this Software License which is marked "confidential" or the equivalent or has the necessary quality of confidence about it and shall not divulge such information to any persons without Barco's prior written consent provided that this Paragraph 7 shall not extend to information which was rightfully in the possession of you prior to the commencement of the negotiations leading to this Software License, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this paragraph 7), is required to be disclosed by law or which is trivial or obvious. You are aware of and ensure to comply with the provisions of this paragraph 7. The foregoing obligations as to confidentiality shall survive any termination of this Software License.

8. You will remain responsible for the maintenance of your hardware, operating system, the functioning of your network and in keeping your systems 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 specific requirements and expectations and the selection of the Software by you is entirely your own choice and decision. For the avoidance of doubt, nothing in this Software License shall impose any obligation on Barco to provide support services (on the Software or any other hardware or software product).

9. This Software License is the only understanding and agreement between you and Barco for use of the Software by you and/or Authorized Users. The Software License supersedes all other communications, understandings or agreements we had prior to this Software License (with the exception of any continuing confidentiality agreement) although nothing in this Software License purports to exclude liability for fraudulent misrepresentation. You may not export or re-export the Software or any copy or adaptation in violation of any applicable laws or regulations. This Software License shall not be altered, amended or varied. If any provision of this Software License is determined to be illegal, void or unenforceable, or if any court of competent jurisdiction in any final decision so determines, this Software License 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 Software License a close as possible.
10. You acknowledge that this Software may be subject to U.S. or other governments Export Jurisdiction. 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. Barco shall be entitled to sub-contract all or any of Barco's obligations hereunder to a third party and/or any of Barco's affiliated companies.
12. The construction, validity and performance of this Software License 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 Software License shall be subject to the exclusive jurisdiction of the courts of Kortrijk, 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 Software License, however, if the Convention is deemed by a court of competent jurisdiction to apply to this Software License, Barco shall not be liable for any claimed non-conformance of the Software under Article 35(2) of the Convention.

Trademarks Software License Terms

Brand and product names mentioned in relation to the Software may be trademarks, registered trademarks or copyrights of their respective (third party) holders. All such brand and product names mentioned in relation to the Software serve as comments or examples and are not to be understood as advertising for the products or their manufacturers.

Privacy Policy

You acknowledge and agree that the Software is gathering technical information about the functionality of the products which are connected through the Software ("Functional Information") and that Barco may make use of such Functional Information (with the exclusion of any personal data) for any reason Barco sees fit, including but not limited to providing services to you / your organization, allowing third party to access to such Functional Information and/or to provide services to you / your organization .

You hereby explicitly give consent that Barco may gather, access, preserve, and/or disclose the personal data you provide to us (e.g. connected with your account allowing for the gathering of Functional Information as well as any content associated with that account) as well as personal information we receive from you through the use of the Software:

- For the benefit of the business purposes of Barco and/or its affiliates;
- In order to provide, maintain, protect and/or improve the Software and to develop new software;
- For administration of the relationship between you, your organization and Barco and/or its affiliates ;
- For any other legitimate purpose (including i) direct marketing purposes from Barco, its affiliates or selected third parties, and ii) allowing third parties to provide services to you related to the Software);
- if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to:
    - Satisfy any applicable law, regulation, legal process or enforceable governmental request;
    - Enforce this Software License, including investigation of potential violations hereof;
    - Detect, prevent, or otherwise address fraud, security or technical issues (including, without limitation, the filtering of spam);
    - Protect against imminent harm to the rights, property or safety of Barco, its users or the public as required or permitted by law.

Barco shall not process any "sensitive information" whatsoever, including but not limited to medical information.

You understand that the technical processing and transmission of or by the Software, including your content, may involve:

- Transmissions over various networks;
- Changes to conform and adapt to technical requirements of connecting networks, devices and/or services.

You hereby explicitly give consent that Barco may export your personal data to any country worldwide, especially to any country where Barco and/or its affiliates have infrastructure, or where a third party is making available infrastructure to Barco and/or its affiliates, to process personal data.

Barco fully adheres to the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, as implemented in the local EU member states. In accordance with these regulations, you have a right of access to, and rectification of, your personal data. You may exercise these rights by contacting 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 (an updated list may be made available through the (customer section of the) Barco website or other (online) means):

Open source component	Open source license
node	https://raw.githubusercontent.com/nodejs/node/master/LICENSE
async	https://raw.githubusercontent.com/caolan/async/master/LICENSE
bcrypt	https://raw.githubusercontent.com/ncb000gt/node.bcrypt.js/master/LICENSE
compression	https://raw.githubusercontent.com/expressjs/compression/master/LICENSE
connect-mongo	http://www.opensource.org/licenses/mit-license.php
connect-multiparty	http://www.opensource.org/licenses/mit-license.php
cookie-parser	https://raw.githubusercontent.com/expressjs/cookie-parser/master/LICENSE
cron	http://www.opensource.org/licenses/mit-license.php
DejaVu	http://dejavu-fonts.org/wiki/License
ejs	http://www.apache.org/licenses/LICENSE-2.0
ejs-locals	http://www.opensource.org/licenses/mit-license.php
express	https://raw.githubusercontent.com/strongloop/express/master/LICENSE
express-brute	https://raw.githubusercontent.com/AdamPflug/express-brute/master/LICENSE
express-session	https://raw.githubusercontent.com/expressjs/session/master/LICENSE
gm	http://opensource.org/licenses/MIT
i18n	https://raw.githubusercontent.com/mashpie/i18n-node/master/LICENSE
js-base64	https://github.com/dankogai/js-base64/blob/master/LICENSE.md
jsonschema	http://en.wikipedia.org/wiki/MIT_License
lodash	https://lodash.com/license
md5	https://github.com/pvorb/node-md5/blob/master/LICENSE
moment	https://raw.githubusercontent.com/moment/moment/develop/LICENSE
mongodb	https://raw.githubusercontent.com/mongodb/node-mongodb-native/2.1/LICENSE
mongoose	http://www.opensource.org/licenses/mit-license.php
multer	https://raw.githubusercontent.com/expressjs/multer/master/LICENSE
nodemailer	https://raw.githubusercontent.com/nodemailer/nodemailer/master/LICENSE
passport	https://raw.githubusercontent.com/jaredhanson/passport/master/LICENSE
passport-local	https://raw.githubusercontent.com/jaredhanson/passport-local/master/LICENSE
python-shell	http://www.opensource.org/licenses/mit-license.php
q	https://github.com/kriskowal/q
request	https://raw.githubusercontent.com/request/request/master/LICENSE

Open source component	Open source license
serve-favicon	https://raw.githubusercontent.com/expressjs/serve-favicon/master/LICENSE
tar.gz	https://raw.githubusercontent.com/alanhoff/node-tar.gz/master/LICENSE
time	https://raw.githubusercontent.com/TooTallNate/node-time/master/LICENSE
urijs	https://raw.githubusercontent.com/medialize/URI.js/gh-pages/LICENSE.txt
winston	https://raw.githubusercontent.com/winstonjs/winston/master/LICENSE
graphicsmagick	http://en.wikipedia.org/wiki/MIT_License
jQuery	jquery.org/license
jQuery Form Plugin	https://github.com/malsup/form#copyright-and-license
Bootstrap	https://github.com/twbs/bootstrap/blob/master/LICENSE
Kendo UI	http://www.telerik.com/purchase/license-agreement/kendo-ui-complete
Jasny Bootstrap	https://github.com/jasny/bootstrap/blob/master/LICENSE
Respond.js	https://github.com/scottjehl/Respond/blob/master/LICENSE-MIT
HTML5 Shiv	MIT/GPL2 Licensed
Font Awesome	http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
jQuery Upload File	https://github.com/hayageek/jquery-upload-file/blob/master/MIT-License.txt
jQuery Validate	http://en.wikipedia.org/wiki/MIT_License
js-cookie	https://github.com/js-cookie/js-cookie/blob/master/MIT-LICENSE.txt

TABLE OF CONTENTS

1. INTRODUCTION

Overview

- About Collaboration Management Suite
- Before you start
- Starting up Collaboration Management Suite
- Forgot password
- Register as new user
- Logout from Collaboration Management Suite
- First start up
- About the Home page, control panel

1.1 About Collaboration Management Suite

Overview

Collaboration Management Suite (CMGS) is a software application that gives an overview of all ClickShare Base Units installed within the company network. It is a server installed application on a physical PC or it runs as virtual machine connected to the network. The functionality can be accessed by users via a web browser based application from anywhere within the network. A user/admin may inspect and/or change a large set of data about the ClickShare Base units and Buttons without leaving their desk. This is especially useful in large corporations with many ClickShare Base Units installed across different sites.

The information provided includes:

- Health and status monitoring
- Schedule software updates and reboots
- User management and user notifications
- Device parameters management

An administrator can define different roles for different users. Depending on these roles, access to some function can be limited.

To realize the communication between the Collaboration Management Suite server and the Base Units, typical ports should be activated. For an overview of these ports, see "Used ports", page 75.

In order to diagnose connection problems between CMGS and the Base Units please see "Diagnose connection issues", page 24.

Supported Base Units

CMGS supports:

- CSE-800 with software version 01.00 or higher
- CSE-200 with software version 01.01 or higher
- CSM-1 with software version 01.02.00.0144 or higher
- CSC-1 with software version 01.05.00.0032 or higher

About user roles

Functionality	IT admin	Support	Key user
Base Units			
Grid	RW	RW	R
Add/remove/edit	RW	RW	-
Link to local webUI	R	R	R
Support & updates			
Buttons	R	R	R
Base Unit debug logging	RW	RW	RW
Download Base Unit logs	RW	RW	RW
Reboot Base Unit	RW	RW	RW
Software updates	RW	RW	-
Diagnose connection issues	RW	RW	RW
Configure			

Functionality	IT admin	Support	Key user
Clone configuration	RW	RW	-
Network integration	RW	RW	-
Wallpaper	RW	RW	RW
WebUI access via WiFi	RW	RW	-
Deploy Base Unit certificates	RW	RW	-
Users			
Grid	RW	R	-
Locations	RW	-	-
Scheduler	RW	RW	-
Scheduled jobs	RW	RW	R[1]
User preferences	RW	RW	RW
System settings	RW	-	-
System administration	RW	-	-
Logout	R	R	R

Collaboration Management Suite supports only one user with IT admin rights!

About the screenshots

The screenshots in this manual are given as an example. The CMGS version may be different, but the indicated functions on the screenshots are correct.

1.2 Before you start

Requirements

The Collaboration Management Suite application provides a browser-based user interface to the data and tools of the system. Before you start using the application, you need the following info:

- The URL of the Collaboration Management Suite application.
- The user name and password assigned to you.

The Recommended browsers are:

- Internet Explorer | 11.0.10240.17184 | Windows 10 Enterprise, v.10.0 (Build 10240)
- Google Chrome | 57.0.2987.98 | Windows 10 Enterprise, v.10.0 (Build 10240)
- Mozilla Firefox | 49.0.2 | Windows 10 Enterprise, v.10.0 (Build 10240)
- Safari on Mac | 9.1.1 (116016.17) | OS X El Capitan v. 10.11.5

1.3 Starting up Collaboration Management Suite

How to start up

1. Type the URL in the address line of your browser.

[1] only reboot jobs are shown.

The login page is displayed.

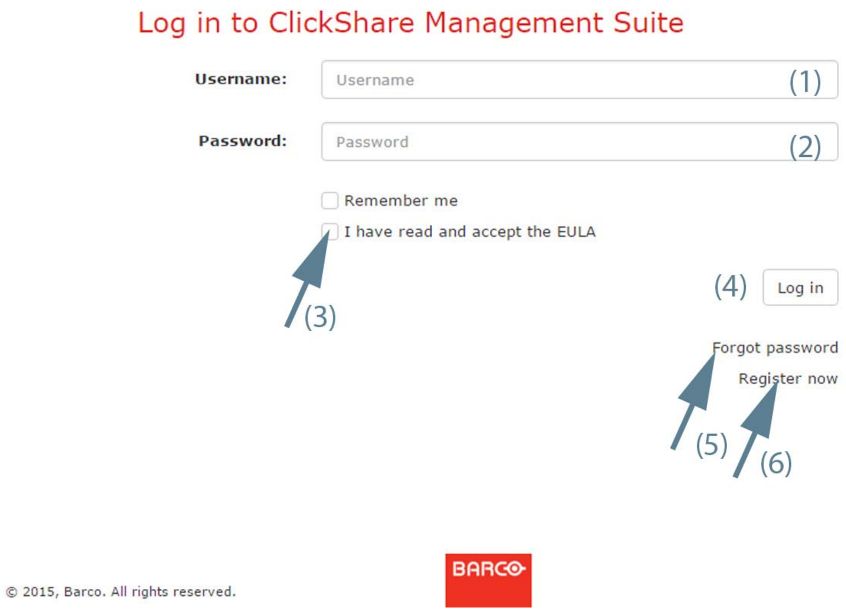

Log in to ClickShare Management Suite
Username:
Username
(1)
Password:
Password
(2)
□ Remember me
□ I have read and accept the EULA
(3)
(4)
Log in
Forgot password
Register now
(5)
(6)
© 2015, Barco. All rights reserved.
BARCO

Image 1-1
Login

2. Enter your E-mail address (1) and password (2).
   Note: *Initial login credentials : user name =* ***admin@yourcompany.com*** *and password =* ***admin****.*
3. If you want to stay logged in, check the checkbox in front of *Remember me* (3).
   Note: *Cookies has to be enabled before you can use this function.*
4. Read and accept the EULA by checking the check box in front of *I have read and accept the EULA*.
   Note: *To read the EULA, click on the word EULA to open the link.*
5. Click **Login** (4).

   Your login credentials are checked and if valid the home page opens.
6. If you forgot your password, click on *Forgot password* (5).
7. If you are a new user who wants access, click on *Register now* (6)

1.4 Forgot password

What to do when you forgot your password

1. Click on *Forgot password* (1).

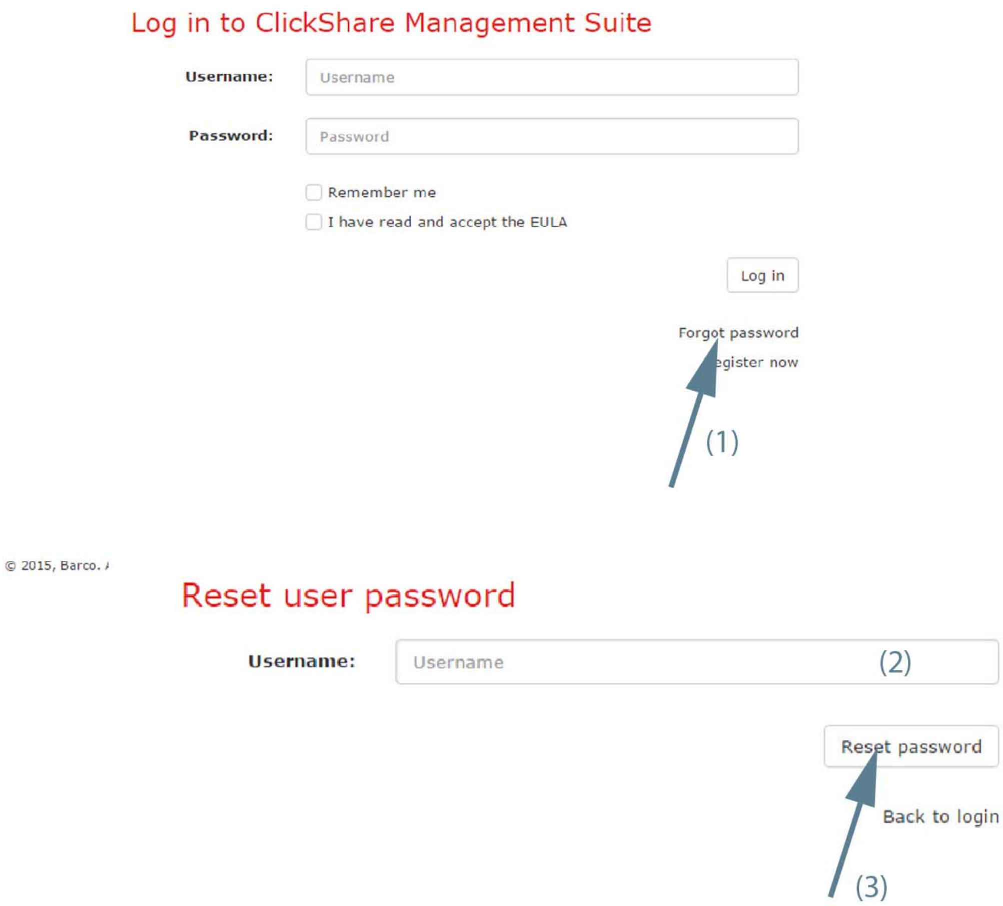


Image 1-2
Forgot password

2. Enter your E-mail address (2).
3. Click on **Reset password** (3).
4. Check your E-mail address (4).

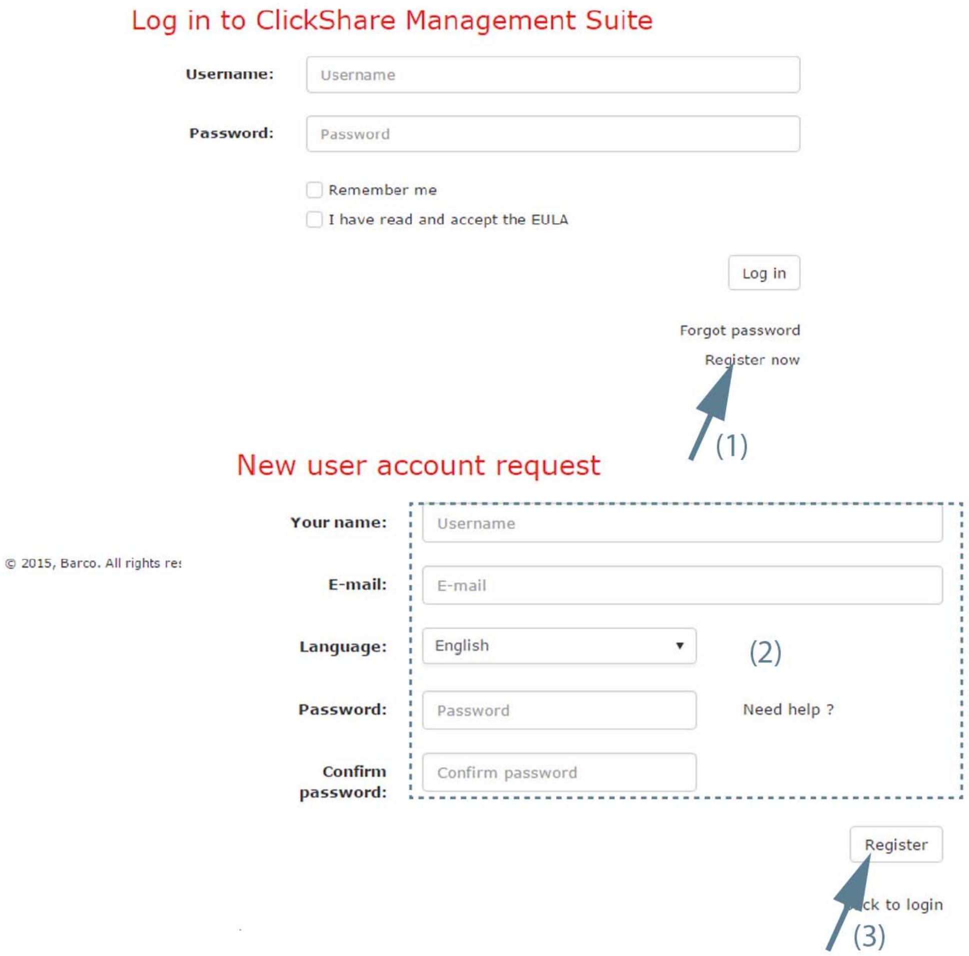
1.5 Register as new user

What can be done?

A new user can request access to Collaboration Management Suite. This request will be sent to the system administrator who can confirm or reject the request. The user will be informed via E-mail.

How to register

1. On the login-logout page, click on *Register now* (1).



Log in to ClickShare Management Suite

Username: Username

Password: Password

□ Remember me

□ I have read and accept the EULA

New user account request

Your name: Username

E-mail: E-mail

Language: English

Password: Password

Confirm password: Confirm password

© 2015, Barco. All rights re:

Image 1-3

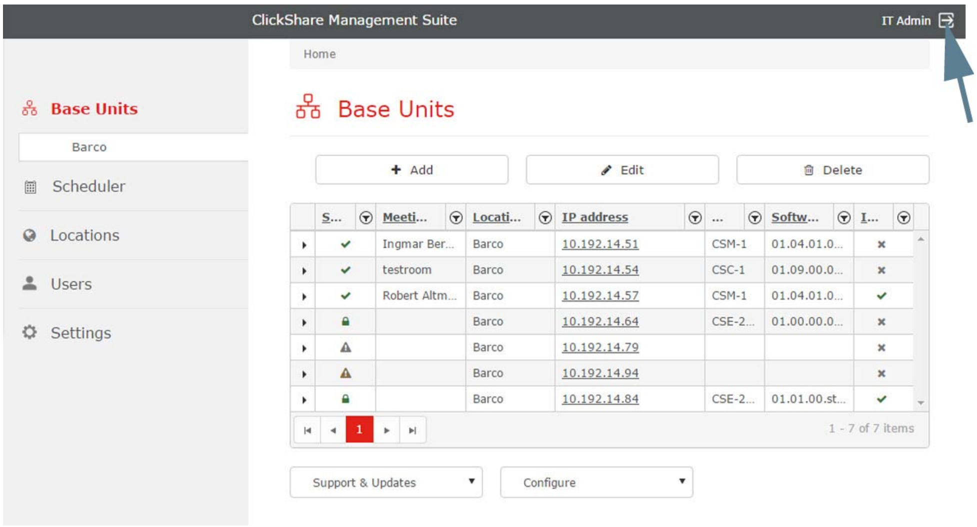
A registration page opens.

2. Enter the following data (2):
   - user name
   - E-mail address
   - Select your language by clicking on the drop down box and selecting the language out of the list.
   - Enter a password.
   - Renterer the password.
3. Click on **Register** (3).

1.6 Logout from Collaboration Management Suite

How to logout

1. Click on the logout symbol (upper right corner) next to the login name.



Base Units

S...	Meeti...	Locati...	IP address	...	Softw...	I...
✓	Ingmar Ber...	Barco	10.192.14.51	CSM-1	01.04.01.0...	✗
✓	testroom	Barco	10.192.14.54	CSC-1	01.09.00.0...	✗
✓	Robert Altm...	Barco	10.192.14.57	CSM-1	01.04.01.0...	✓
🔒		Barco	10.192.14.64	CSE-2...	01.00.00.0...	✗
⚠		Barco	10.192.14.79			✗
⚠		Barco	10.192.14.94			✗
🔒		Barco	10.192.14.84	CSE-2...	01.01.00.st...	✓

1 - 7 of 7 items

Image 1-4
Logout

1.7 First start up

About the setup wizard

When starting up the Collaboration Management Suite for the first time a *Setup wizard* will guide you trough the setup process.

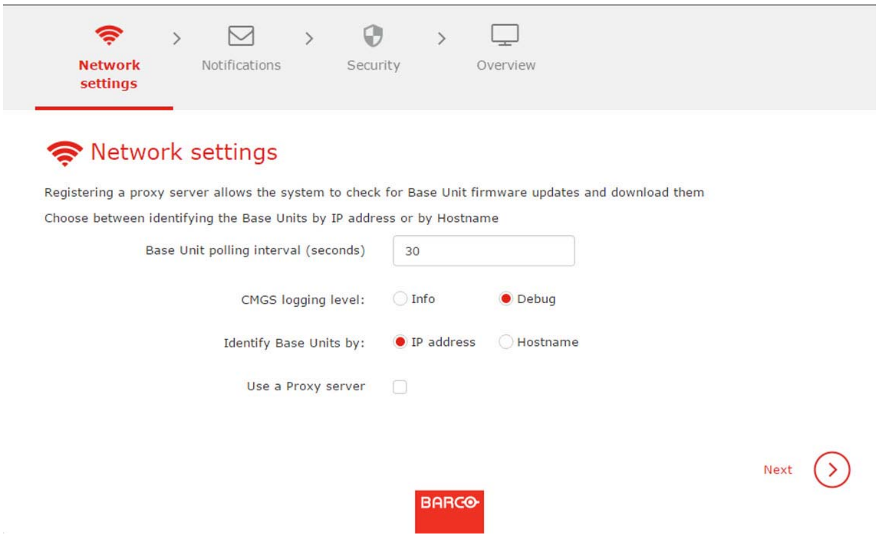
The following setup points are included:

- Network settings
- Notifications
- Security
- Overview

Once the wizard is started, fill out the necessary items and click **Next** to continue. Use the Back button to return one step.

Network settings

1. Fill out the Network settings.



Network settings

Registering a proxy server allows the system to check for Base Unit firmware updates and download them

Choose between identifying the Base Units by IP address or by Hostname

Base Unit polling interval (seconds) 30

CMGS logging level: ○ Info ● Debug

Identify Base Units by: ● IP address ○ Hostname

Use a Proxy server □

Image 1-5
Start wizard, network settings

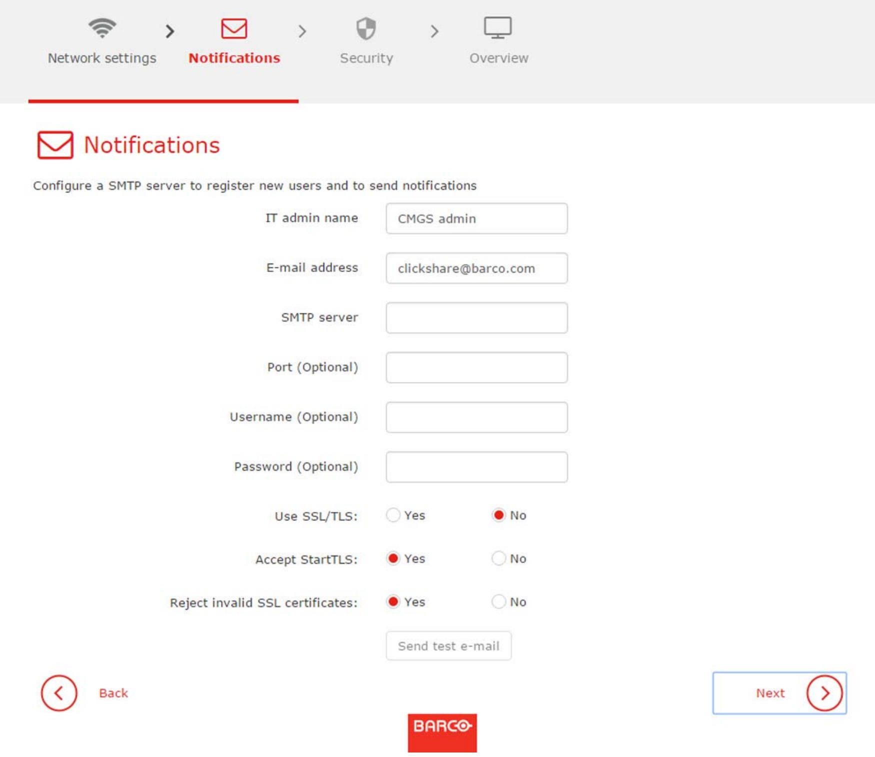
The following settings can be filled out:

- The base unit polling interval in seconds
- CMGS logging level, Info or Debug
- The way to identify the Base Unit, IP address or Hostname
- The use of a Proxy server.

When a Proxy server is used, fill out the following information:

- Proxy server URL
- Proxy server port (optional)
- Username (optional)
- Password (optional)

2. Fill out the Notifications settings



Notifications

Configure a SMTP server to register new users and to send notifications

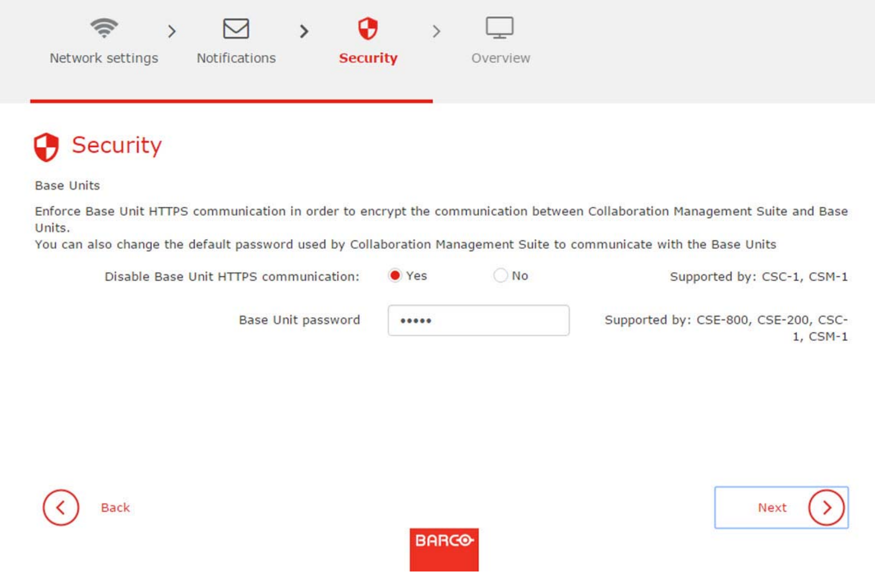
IT admin name	CMGS admin
E-mail address	clickshare@barco.com
SMTP server	
Port (Optional)	
Username (Optional)	
Password (Optional)	
Use SSL/TLS:	○ Yes ● No
Accept StartTLS:	● Yes ○ No
Reject invalid SSL certificates:	● Yes ○ No

Image 1-6
Start wizard, notifications

The following settings can be filled out:

- IT admin name.
- E-mail address used to send E-mails.
- SMTP server address to send E-mails.
- Port (optional)
- Username (optional)
- Password (optional)
- SSL/TLS usage
- Accept startTLS
- Reject invalid SSL certificates

3. Fill out the Security settings.



Security

Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

Disable Base Unit HTTPS communication: ● Yes ○ No Supported by: CSC-1, CSM-1

Base Unit password ••••• Supported by: CSE-800, CSE-200, CSC-1, CSM-1

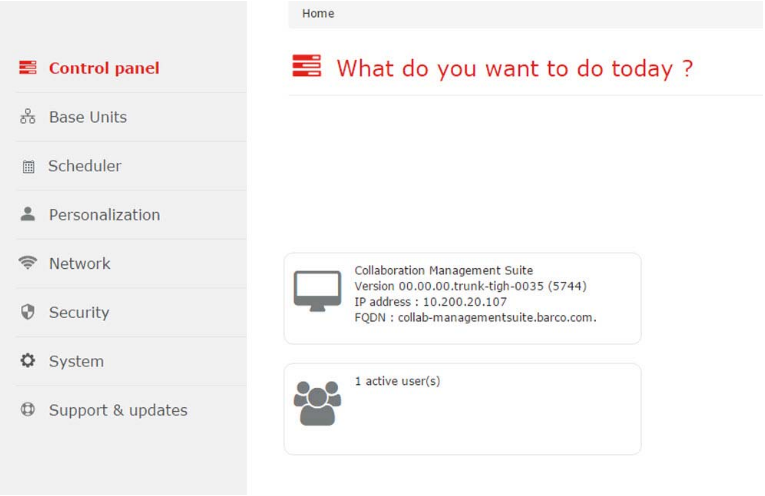
Image 1-7
Start wizard, security

The following settings can be set depending on the model type:

- Disabling the HTTPS communication.
- Base Unit password.

4. The overview page shows the settings which are set.
   Click **Finish** to finalize the start up wizard.

   The Home page is displayed. The Collaboration Management Suite is ready for use. The control panel contains basic information about the Collaboration Management Suite, Base Units and users.



What do you want to do today ?

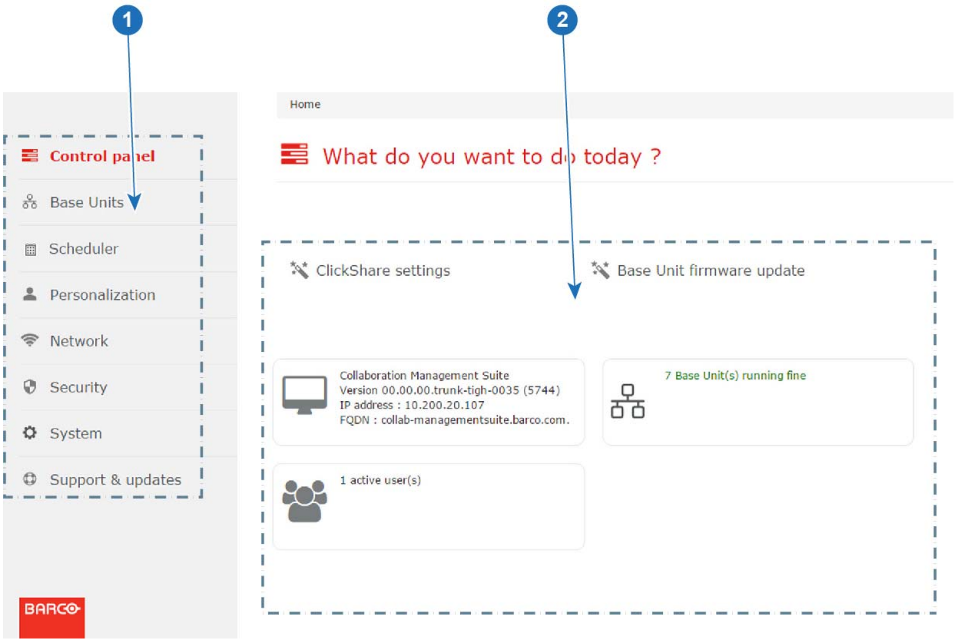
Collaboration Management Suite
Version 00.00.00.trunk-tigh-0035 (5744)
IP address : 10.200.20.107
FQDN : collab-managementsuite.barco.com.

1 active user(s)

Image 1-8
Home page, control panel

1.8 About the Home page, control panel

Overview



Collaboration Management Suite
Version 00.00.00.trunk-tigh-0035 (5744)
IP address : 10.200.20.107
FQDN : collab-managementsuite.barco.com.

7 Base Unit(s) running fine

1 active user(s)

Image 1-9
Home page overview

Note: the control panel might contain also some discovered CSE-800 devices.

1 Menu pane.

The following main menus are available:

- Control panel
- Base Units
- Scheduler
- Personalization
- Network
- Security
- System
- Support & updates

2 Overview and selection pane.

Frequently used actions can be started from the control panel. After clicking on an action, you will be redirected to the corresponding web page or wizard step.

The following items may be displayed:

- ClickShare settings
- Base Unit firmware update
- Collaboration Management Suite overview
- Users overview
- Base Unit statuses
- New Base Units discovered

2. BASE UNITS PAGE

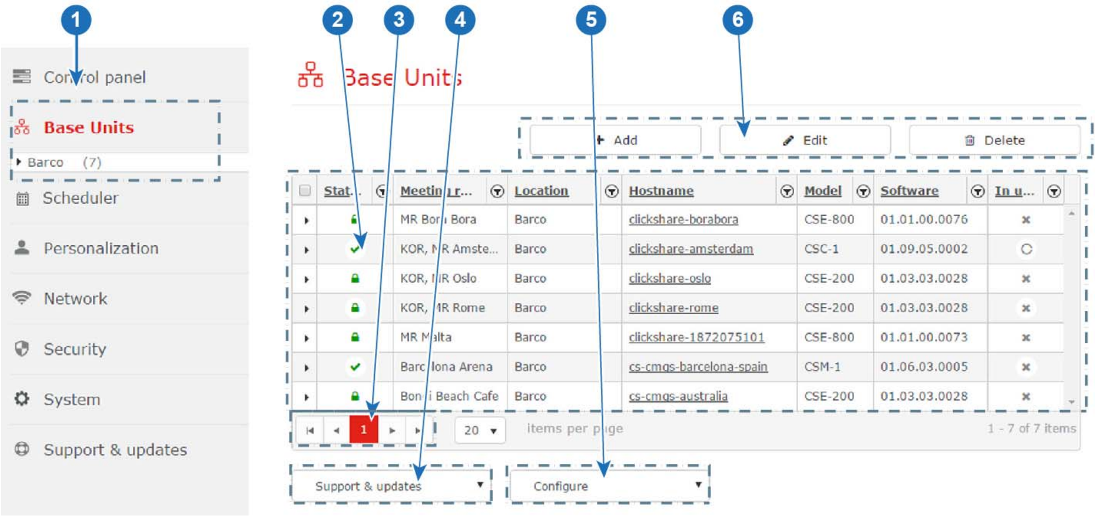
Depending on the user role, some may not be visible.

Overview

- About the Base Units page
- Auto discovering of Base Units
- Add new Base Unit
- Edit selected Base Unit
- Delete selected Base Unit
- Sorting and filtering
- Support and updates

2.1 About the Base Units page

Overview



	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✕
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✕
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✕
▸	🔒	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	✕
▸	✓	Barcelona Arena	Barco	cs-cmgs-barcelona-spain	CSM-1	01.06.03.0005	✕
▸	🔒	Bondi Beach Cafe	Barco	cs-cmgs-australia	CSE-200	01.03.03.0028	✕

Image 2-1
Overview page

1 Menu pane. Selected menu is expanded and menu title is displayed in red. When different location are sub-locations are available, a tree will be shown.

The number behind the location indicates the number of Base Units in that location or sub location.

2 Overview Base Units of selected location branch.

The following information is displayed2:

- The "Status" column of the Base Units grid contains an icon that shows if the device is working properly or not:
  - Green check mark, or green lock: Device is working properly - all processes are running fine
  - Blue check mark: Device is in Network Standby mode
  - Orange triangle with exclamation mark: Device is running with warnings (something is wrong with non-critical processes)
  - Red triangle with exclamation mark: Device is running with errors (something is wrong with critical processes)
  - Yellow triangle with exclamation mark: Device is running with warnings (non-critical processes may not run properly)
  - Grey triangle with exclamation mark: Device is not available or not responding
- Meeting room name, automatically added when connection is established.
- Location, filled out while adding the Base Unit in Collaboration Management Suite.
- Hostname, automatically added when connection is established.
- Model, automatically added when connection is established.
- Software, automatically added when connection is established.

- The column "In use", of the Base Units grid, contains one of the following icons:
  - A gray ’x’ for a Base Unit that is not connected to a source, not sharing, nor ready to share.
  - A gray circle, if the device is connected to a source, but not sharing.
  - A red spinning circle, if the device is connected to a source, and sharing.
  - nothing (empty), for devices unknown by CMGS, i.e. other than CSC-1, CSM-1, CSE-200, CSE-800

3 Page selection buttons. The added Base Units are displayed in pages.

To change a page, click on the arrow buttons next to the page indication or click in the page input field and select the desired page number.

4 Support and Update

- Download Base Unit logs: to download the logging from a selected Base Unit.
- Reboot Base Units: to reboot the selected Base Units.
- Software update: to update the software of the selected Base Units.
- Diagnose connection issues: to start the diagnostics of the selected Base Units.

5 Configure

- Clone configuration: to clone the configuration from a selected Base Unit to multiple other Base Units of the same type.
- Wallpaper: to change the wallpaper displayed by the Base Units

6 Tool bar to add, edit or delete a Base Unit on the page.

Base Unit details

The overview page contains a first column with arrows. Click on that arrow to view more details such as serial number, total uptime, hostname, SSID, frequency and channel. The details displayed depend on the current mode of the Base Unit. If a Base Unit is integrated into the Corporate Network (using EAP-TLS, EAP-TTLS, PEAP or WPA2-PSK) then specific details are displayed for each mode.

Base Unit selection

Click on a row to select the Base Unit. The row background turns into red. Multiple selection is possible by holding the CTRL button while selecting the desired rows. Or by clicking on the first row, holding down the SHIFT button and then clicking on the last one in the selection. All the Base Units in between the first selected and the last selected Base Unit are selected. Base Unit selection can also be done by clicking and holding down the left mouse button and dragging across the desired Base Units (this can also be done on mobile devices). All the Base Units can be selected by checking the check box from the top-left corner of the grid

About the status

CMGS can communicate with the Base Unit, the status can be either:

Green check mark

- Base Unit is OK. Communication protocol is HTTP.

Green lock

- Base Unit is OK. Communication protocol is HTTPS

Blue check mark

- Base Unit is in Network Standby mode (only for CSE-800)

Orange triangle

- Base Unit reports some problems with some processes that are not critical for sharing usage (meeting room usage)
  - WebUI Server not running
  - System Logging not running
  - Process Monitor not running
  - Job Scheduler not running
  - LED Control not running
  - Projector Control not running (only CSC-1, CSM-1)
  - Button Agent not running
  - DHCP Server not running
- CMGS was not able to enforce the CMGS user preference wrt. Base Unit HTTP/HTTPS communication
- CMGS was not able to enforce the Base Unit password requested by the CMGS user
- Base Unit is running a very old firmware version that does not allow CMGS communication; The user should update the firmware of the Base Unit manually.

Red triangle

[2] Views differ with every account type

- the Base Unit reports some problems that prevent sharing
  - ClickShare Server
  - Config Manager
  - Graphics Server (not on CSE-200, CSE-800)
  - Device Daemon
  - DBus Daemon
  - Wifi Access Point Daemon
- CMGS determined that the added device is not a Base Unit hence should be removed from CMGS

Gray triangle

CMGS can not communicate with the device.

- Base Unit not connected to the network infrastructure
- Base Unit shut down or performing a reboot procedure
- network configuration preventing the communication between CMGS and the Base Unit : user should use the Diagnostics page to find out more details.

2.2 Auto discovering of Base Units

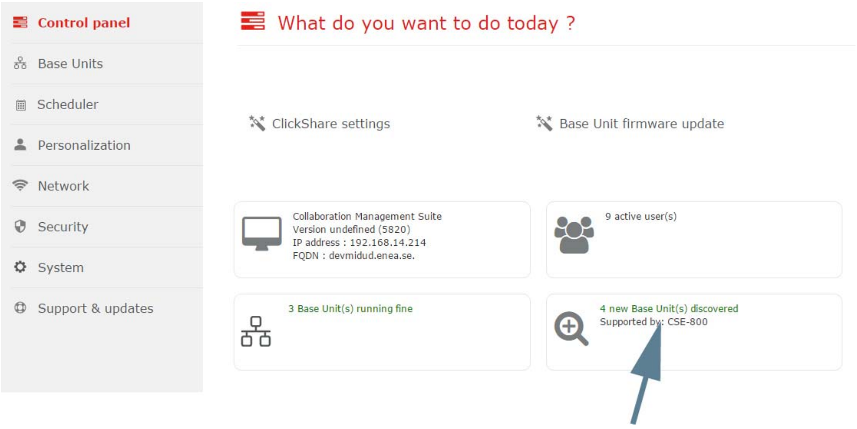
Only for CSE-800.

What can be done?

New CSE-800 Base Units on your network might be automatically detected if the Collaboration Management Suite has the default hostname, or if the user entered the correct Collaboration Management Suite hostname or IP address in the Base Unit Web UI, page *WiFi & Network → Services*. The Base Units are added to a discovered list and displayed on in the Control panel and then in the wizard that will add them in the Collaboration Management Suite list of available Base Units.

Auto discovery

1. On the *Control panel* page, click on the new Base Units message.



Collaboration Management Suite
Version undefined (5820)
IP address : 192.168.14.214
FQDN : devmidud.enea.se.

9 active user(s)

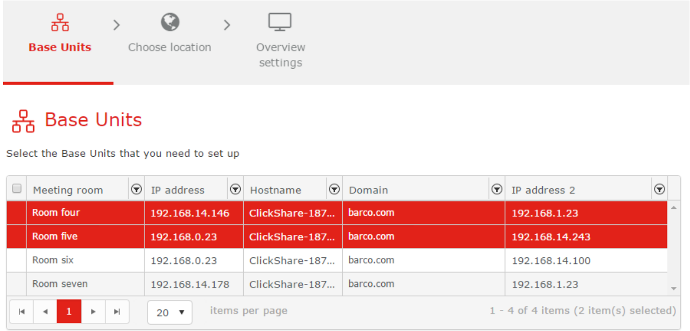
3 Base Unit(s) running fine

4 new Base Unit(s) discovered
Supported by: CSE-800

Image 2-2
Auto-discover Base Units

The Base Unit list is displayed and the Base units can be set up.

2. Select the Base Unit(s) to set up and click **Next**.



Base Units

Select the Base Units that you need to set up

□	Meeting room	IP address	Hostname	Domain	IP address 2
	Room four	192.168.14.146	ClickShare-187...	barco.com	192.168.1.23
	Room five	192.168.0.23	ClickShare-187...	barco.com	192.168.14.243
	Room six	192.168.0.23	ClickShare-187...	barco.com	192.168.14.100
	Room seven	192.168.14.178	ClickShare-187...	barco.com	192.168.1.23

1 | 20 items per page | 1 - 4 of 4 items (2 item(s) selected)

Image 2-3
Select Base Units

3. Select the *Location*. Click on the arrow to expand the list and select the desired location. Click **Next** to continue.

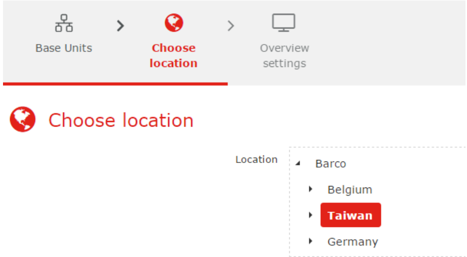
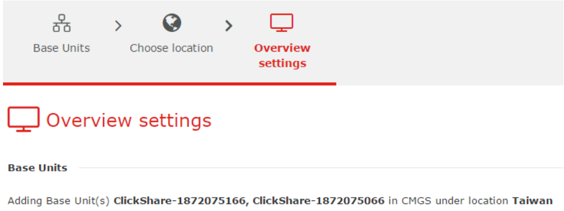


Image 2-4
Choose location

A confirmation message is displayed that x Base Units are added successfully.

4. Click **OK** to continue.

An overview of the settings is displayed.



Overview settings

Base Units

Adding Base Unit(s) **ClickShare-1872075166, ClickShare-1872075066** in CMGS under location **Taiwan**

Image 2-5
Overview settings

5. Click **Finish**.

2.3 Add new Base Unit

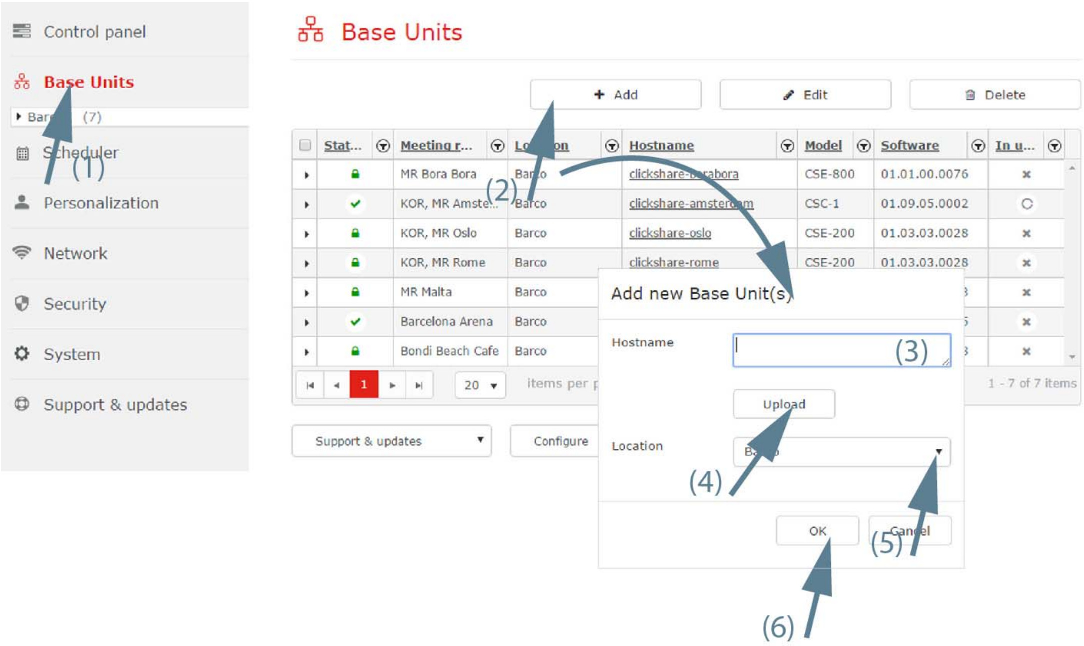
About adding Base Units

New Base Units on the network can be added to the Collaboration Management Suite.

Auto-discovering is supported for CSE-800.

Add via the Base Units window

1. When the overview window is not open yet, click on **Base Units** in the menu bar.



☐	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Malta	Barco				✖
▸	✓	Barcelona Arena	Barco				✖
▸	🔒	Bondi Beach Cafe	Barco				✖

Image 2-6
Add Base Unit

An overview of the current coupled Base Units is shown.

2. Click on the "**+ Add**" button to add a Base Unit.

   The *Add New Base Unit(s)* window opens.

3. Click in the input field next to *Hostname* (3) and enter the hostname or IP address or FQDNs (Fully Qualified Domain Names) of the Base Unit to be added. Multiple Base Units can be added at the same time by entering the different hostnames or IP addresses or FQDNs (Fully Qualified Domain Names) separated by a comma (there is no limitation in the number of Base Units).
   Or,
   if you have a text file where each line contains an IP address or hostname or FQDNs (Fully Qualified Domain Names) , click on **Upload** (4) and select this file and click on **Open**. After uploading information from file, Base Units must appear into Hostname field (no limitation in the number of Base Units).
   Note: *A hostname or FQDNs can have up to maximum 253 characters.*

4. Select a location in the location tree (5). Click on the drop down box and select a branch or sub branch.

5. Click **OK** (6) to add the Base Unit(s) to the overview list.

   Details of the added Base Unit(s) are acquired in about 30 seconds (only when the Base Unit polling interval and the CMGS database polling interval are not changed by the IT admin). The overview list will be updated.

   The IT admin can choose between identifying Base Units by *IP address* or *Hostname* in *Network* → *WiFi & LAN settings* page.

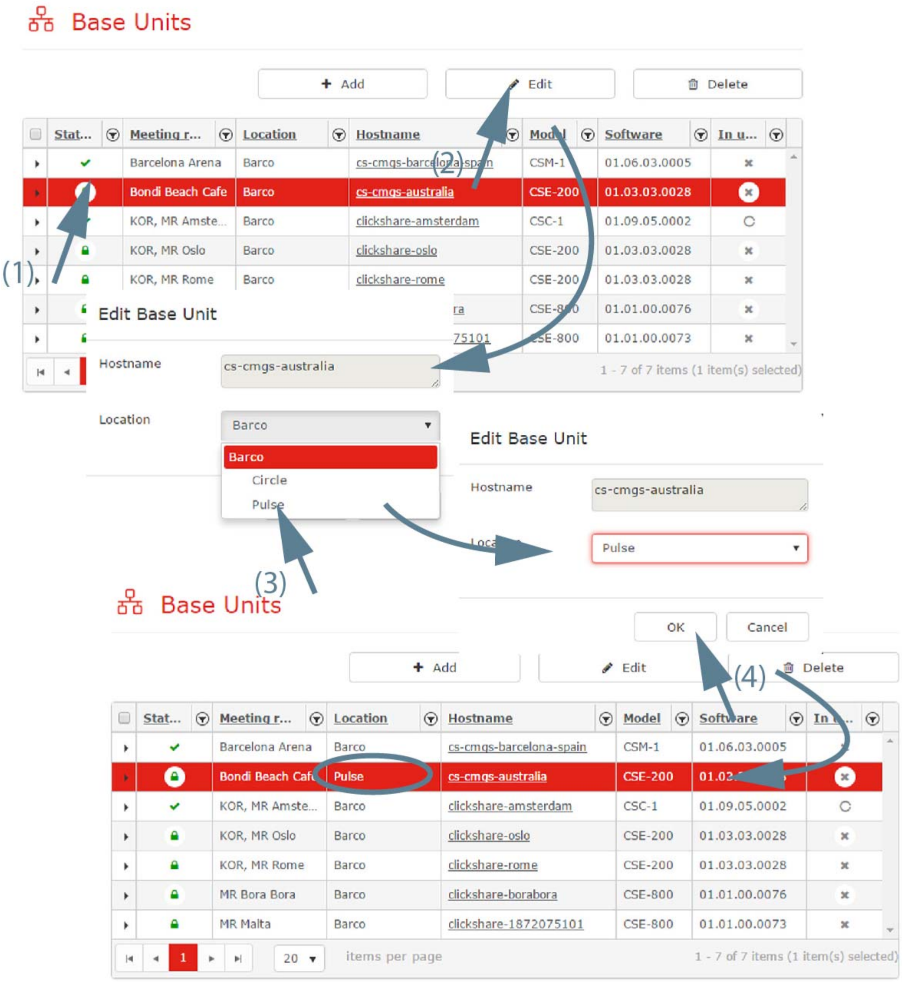
2.4 Edit selected Base Unit

About editing a Base Unit

The location of a Base Unit can be changed to any location in the location tree.

How to edit

1. Select the Base Unit to edit (1).



Edit Base Unit

Hostname: cs-cmgs-australia

Location: Barco

Barco
Circle
Pulse

Edit Base Unit

Hostname: cs-cmgs-australia

Location: Pulse

□	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	✓	Barcelona Arena	Barco	cs-cmgs-barcelona-spain	CSM-1	01.06.03.0005	✖
▸	🔒	Bondi Beach Cafe	Pulse	cs-cmgs-australia	CSE-200	01.03.03.0028	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	🔒	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	✖

1 | 20 items per page | 1 - 7 of 7 items (1 item(s) selected)

Image 2-7
Edit Base Unit

2. Click on the **Edit** button (2).

   The *Edit Base Unit* window opens. The current location is indicated.

3. Click on the new desired location (3).

4. Click on **OK** (4).

   The Base Unit is updated with the new location.

About changes in hostname or IP address

Changes can be made to the hostname or IP address directly on WebUI of the Base Unit. These changes are reflected in Collaboration Management Suite

How it works:

1. client manually adds Base Unit in CMGS by IP Address or Hostname or FQDN (no auto-discover support)
2. CMGS - Base Unit communication is done based on IP address and if this does not work, Hostname communication is tried.
3. If either communication is successful Base Unit information is updated in the CMGS database and it will be used from this moment on

Any change made to an IP address or hostname are automatically updated in CMGS.

2.5 Delete selected Base Unit

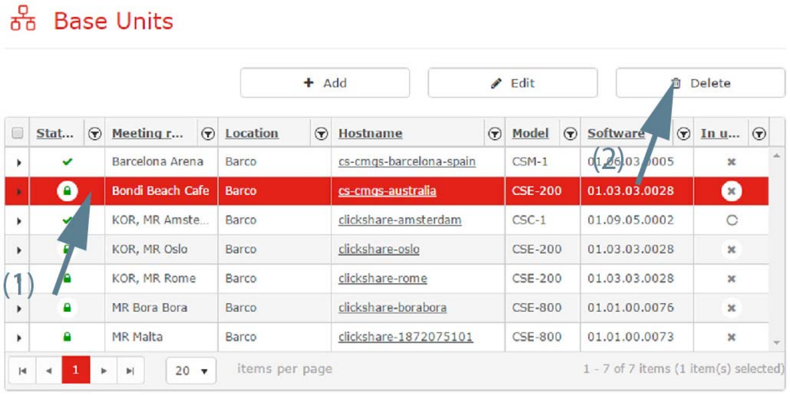
About deleting a Base Unit

Multiple Base Units can be removed from Collaboration Management Suite at the same time.

How to delete

1. Select the Base Unit to delete.

To select multiple Base Units, click and drag the mouse over them or click on the first one, hold down the CTRL button and click on the last one. All Base Units in between are selected.



☐	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	✓	Barcelona Arena	Barco	cs-cmqs-barcelona-spain	CSM-1	01.06.03.0005	✖
▸	🔒	Bondi Beach Cafe	Barco	cs-cmqs-australia	CSE-200	01.03.03.0028	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	🔒	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	✖

1 20 items per page 1 - 7 of 7 items (1 item(s) selected)

Image 2-8
Delete Base Unit

2. Click on the **Delete** button.

   A warning message appears to ask confirmation from the user: "*Delete x Base Unit(s)?*".

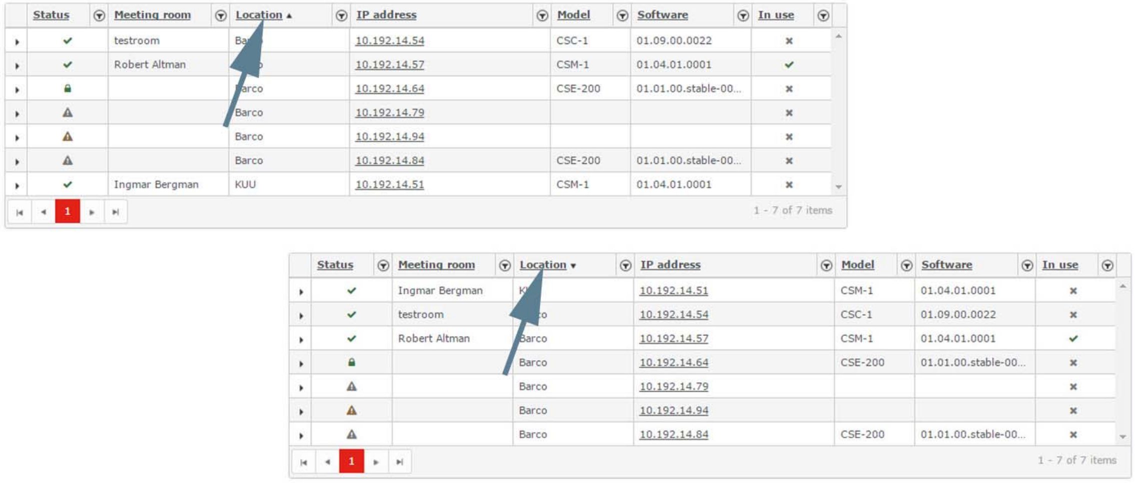
3. Press **OK** to delete the Base Unit(s).

2.6 Sorting and filtering

Do not use one of the following characters in a sorting or filtering field : [, (,), \, +, *, ?

About sorting

The overview page can be sorted using any header of the overview page. Click on the header to sort the overview page in descending or ascending order. Click again on the header to change the order.



	Status	Meeting room	Location ▲	IP address	Model	Software	In use
▸	✓	testroom	Ba	10.192.14.54	CSC-1	01.09.00.0022	✖
▸	✓	Robert Altman	o	10.192.14.57	CSM-1	01.04.01.0001	✓
▸	🔒		arco	10.192.14.64	CSE-200	01.01.00.stable-00...	✖
▸	⚠		Barco	10.192.14.79			✖
▸	⚠		Barco	10.192.14.94			✖
▸	⚠		Barco	10.192.14.84	CSE-200	01.01.00.stable-00...	✖
▸	✓	Ingmar Bergman	KUU	10.192.14.51	CSM-1	01.04.01.0001	✖

1 1 - 7 of 7 items

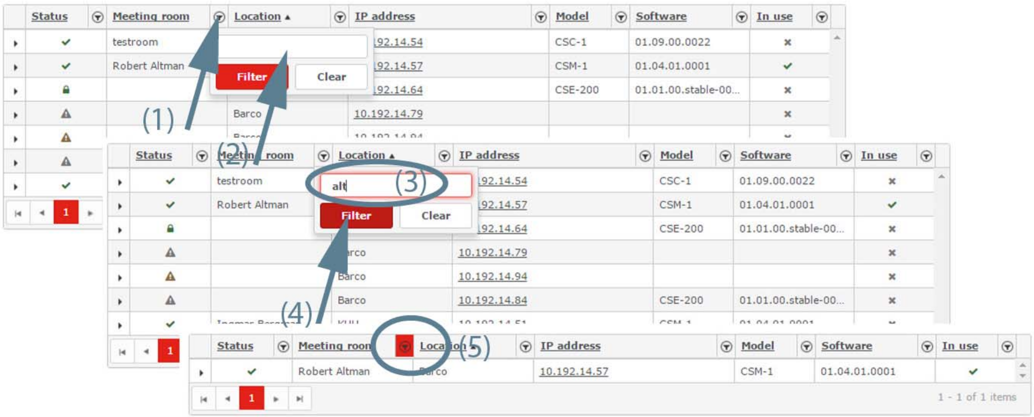
	Status	Meeting room	Location ▾	IP address	Model	Software	In use
▸	✓	Ingmar Bergman	K	10.192.14.51	CSM-1	01.04.01.0001	✖
▸	✓	testroom	o	10.192.14.54	CSC-1	01.09.00.0022	✖
▸	✓	Robert Altman	Barco	10.192.14.57	CSM-1	01.04.01.0001	✓
▸	🔒		Barco	10.192.14.64	CSE-200	01.01.00.stable-00...	✖
▸	⚠		Barco	10.192.14.79			✖
▸	⚠		Barco	10.192.14.94			✖
▸	⚠		Barco	10.192.14.84	CSE-200	01.01.00.stable-00...	✖

1 1 - 7 of 7 items

Image 2-9
Sorting overview

About filtering via the overview page

The overview page can be filtered using the filter arrow next to each item in the header (1). Click on that arrow to open the filter window. Enter a search criterion (2–3). A search criterion can be any part of the name. Click **Filter** (4) to update the overview page. The filter arrow in the header gets a red background.



Status	Meeting room	Location ▲	IP address	Model	Software	In use
✓	testroom		192.14.54	CSC-1	01.09.00.0022	✗
✓	Robert Altman		192.14.57	CSM-1	01.04.01.0001	✓
🔒			192.14.64	CSE-200	01.01.00.stable-00...	✗
⚠		Barco	10.192.14.79			✗
⚠		Barco	10.192.14.94			✗
⚠		Barco	10.192.14.84	CSE-200	01.01.00.stable-00...	✗

Status	Meeting room	Location	IP address	Model	Software	In use
✓	Robert Altman	Barco	10.192.14.57	CSM-1	01.04.01.0001	✓

1 - 1 of 1 items

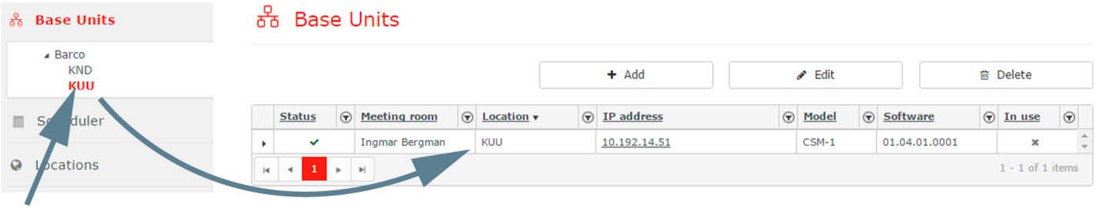
Image 2-10
Filtering overview

To clear the search filter, click on the filter arrow with red background to open the filter window and click on Clear.

About filtering via the location tree

Click on a branch of the location tree to filter the Base Units. Only those Base Unit located on that branch (and sub branches) are displayed.

Example: filter for *'KUU'*. Click on the branch *'KUU'* and the overview page displays only the Base Units located in 'KUU'.



Status	Meeting room	Location ▾	IP address	Model	Software	In use
✓	Ingmar Bergman	KUU	10.192.14.51	CSM-1	01.04.01.0001	✗

1 - 1 of 1 items

Image 2-11
Filtering via tree

2.7 Support and updates

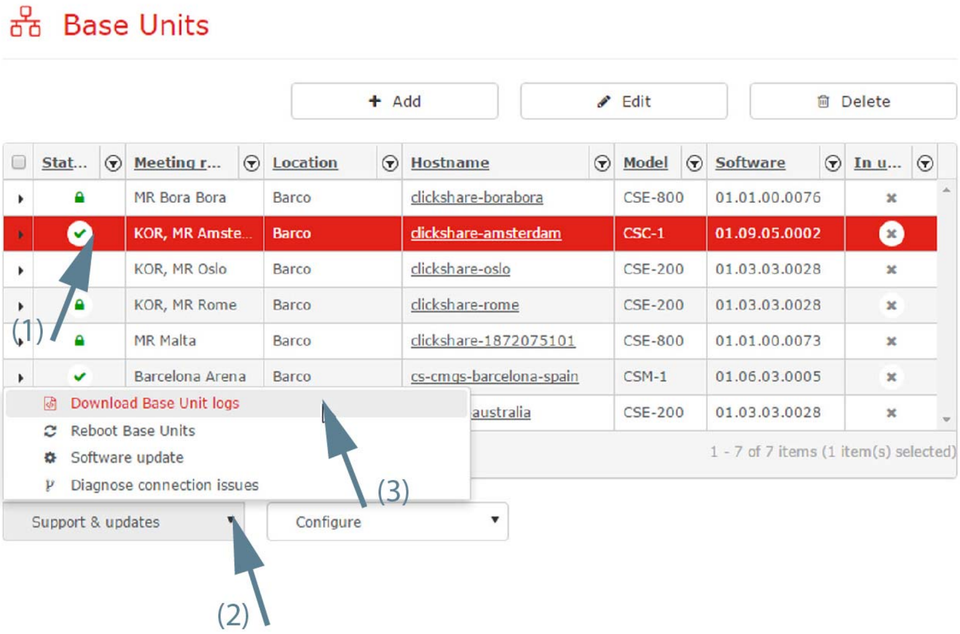
Overview

- Download Base Unit log
- Reboot Base Units
- Software update
- Diagnose connection issues

2.7.1 Download Base Unit log

How to download

1. Select the Base Unit to download the logging (1). Multiple Base Units can be selected.



Base Units

+ Add | ✎ Edit | 🗑 Delete

□	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	✖
▸		KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	✖
▸	✓	Barcelona Arena	Barco	cs-cmgs-barcelona-spain	CSM-1	01.06.03.0005	✖
				australia	CSE-200	01.03.03.0028	✖

1 - 7 of 7 items (1 item(s) selected)

Image 2-12
Download Bas Unit logs

2. Click on the drop down box *Support & Updates* (2) and select **Download Base Unit logs** (3).

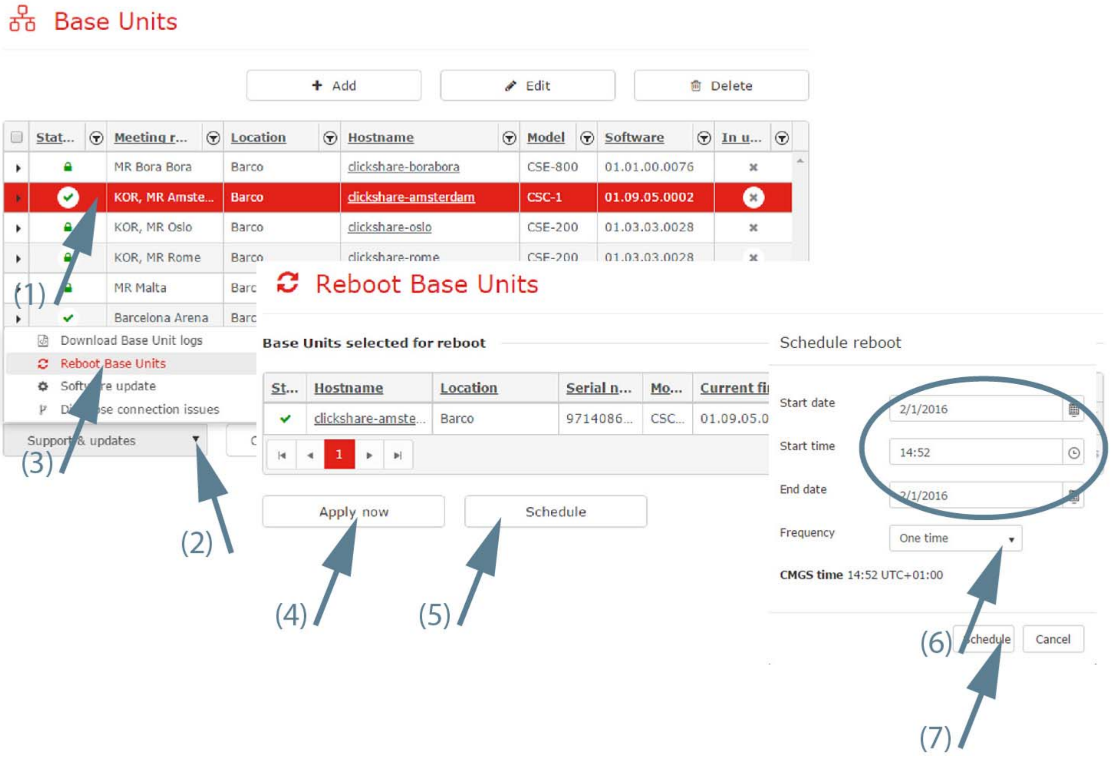
   A message is displayed: "Download Base Unit logs, please wait".

   The logging file can be saved on your hard disk.

2.7.2 Reboot Base Units

How to reboot

1. Select the Base Units to reboot.



Base Units

+ Add | ✎ Edit | 🗑 Delete

□	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	✖
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Malta	Barc				
▸	✓	Barcelona Arena	Barc				

Reboot Base Units

Base Units selected for reboot

St...	Hostname	Location	Serial n...	Mo...	Current fi
✓	clickshare-amste...	Barco	9714086...	CSC...	01.09.05.0

Schedule reboot

Start date: 2/1/2016

Start time: 14:52

End date: 2/1/2016

Frequency: One time

CMGS time 14:52 UTC+01:00

Image 2-13
Reboot Base Unit(s)

2. Click on the drop down box *Support & Updates* (2) and select **Reboot Base Units** (3).

   A *Reboot Base Unit* page opens with the overview of the selected Base Units.

3. To reboot immediately, click **Apply now** (4).
   To reboot on a later date, click **Schedule** (5). Fill out a date and time and click **Schedule** (7).
   Note: *A schedule frequency can be entered. The following choices are possible: one time, daily, weekly, monthly or yearly.*

2.7.3 Software update

About software update

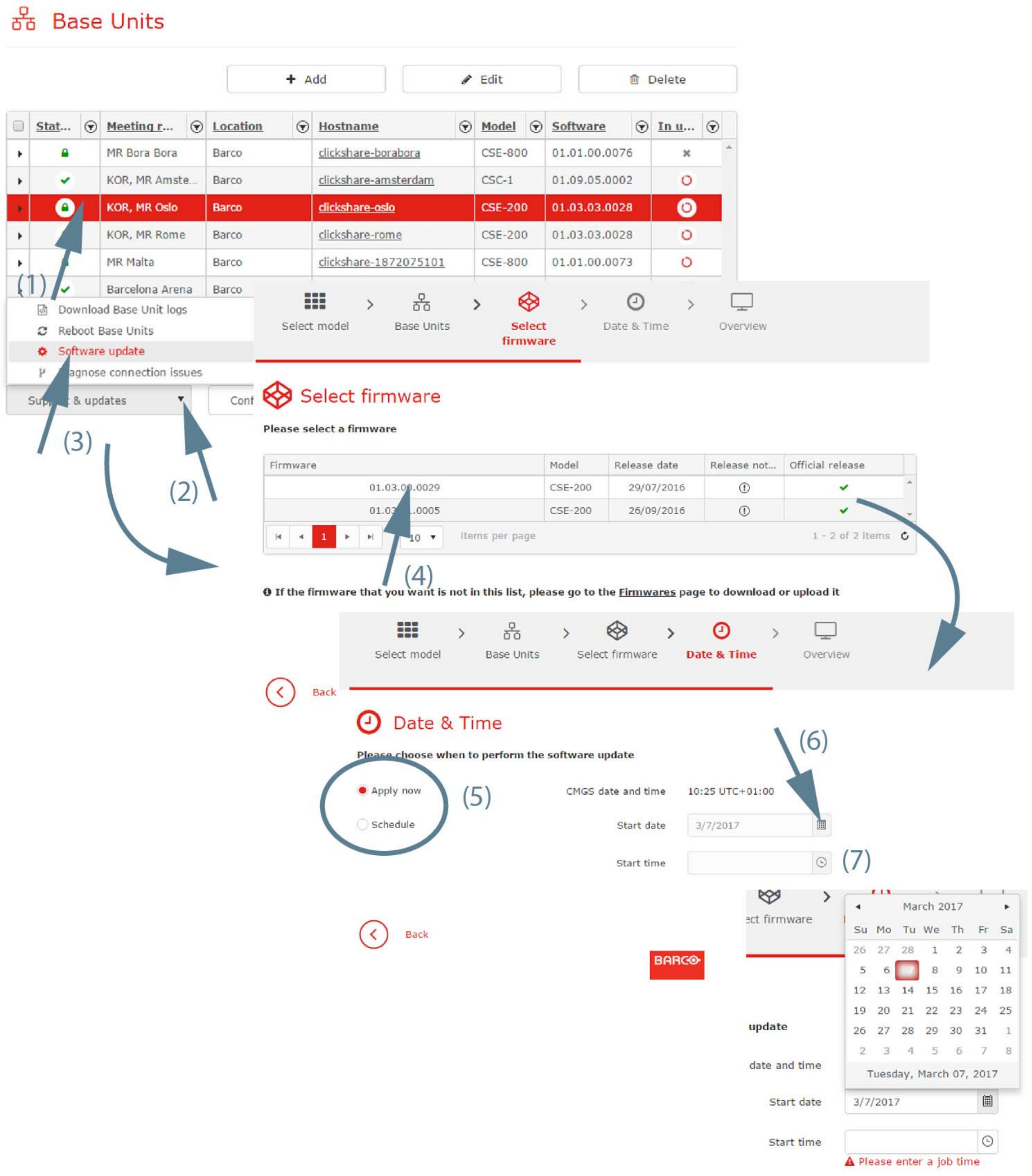
The firmware of a single Base Unit or of multiple Base Units can be updated with Collaboration Management Suite. The update can be executed immediately or it can be scheduled.

The Base Unit firmware must be loaded on the Collaboration Management Suite, prior the update. Collaboration Management Suite may directly download a firmware from Barco site, or the firmware may be uploaded to Collaboration Management Suite.

An update takes about 10 up to 20 minutes for a CSC-1, about 5 up to 10 minutes for a CSE-200/CSE-800 and 15 up to 30 minutes for a CSM-1.

How to update

1. Select the Base Unit(s) to update (1). All the selected Base Units must be of the same type.



Base Units

Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	○
	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	○
	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	○
✓	Barcelona Arena	Barco				

Select firmware

Please select a firmware

Firmware	Model	Release date	Release not...	Official release
01.03.00.0029	CSE-200	29/07/2016	ⓘ	✓
01.03...0005	CSE-200	26/09/2016	ⓘ	✓

1 - 2 of 2 items

ⓘ If the firmware that you want is not in this list, please go to the Firmwares page to download or upload it

Date & Time

Please choose when to perform the software update

● Apply now

○ Schedule

CMGS date and time: 10:25 UTC+01:00

Start date: 3/7/2017

Start time:

March 2017

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Tuesday, March 07, 2017

Start date: 3/7/2017

Start time:

⚠ Please enter a job time

Image 2-14
Software updates

2. Click on the drop down box *Support & Updates* (2) and click **Software Update** (3).

   The Select firmware window opens.

   The possible updates are displayed. If the firmware that you want is not in the list, click on **Firmwares** to go to the firmware page to download or upload this version. See Download firmware.

3. Select the firmware version (4) and click **Next** to continue.

4. To apply the firmware immediately, check the radio button in front of **Apply now** (5).
   To schedule the update in the future, check the radio buton in front of **Schedule**. To change the date, click on the calendar icon (6) and select the date (7). Enter the time (hh:mm) or click on the clock icon, then select a predefined time.

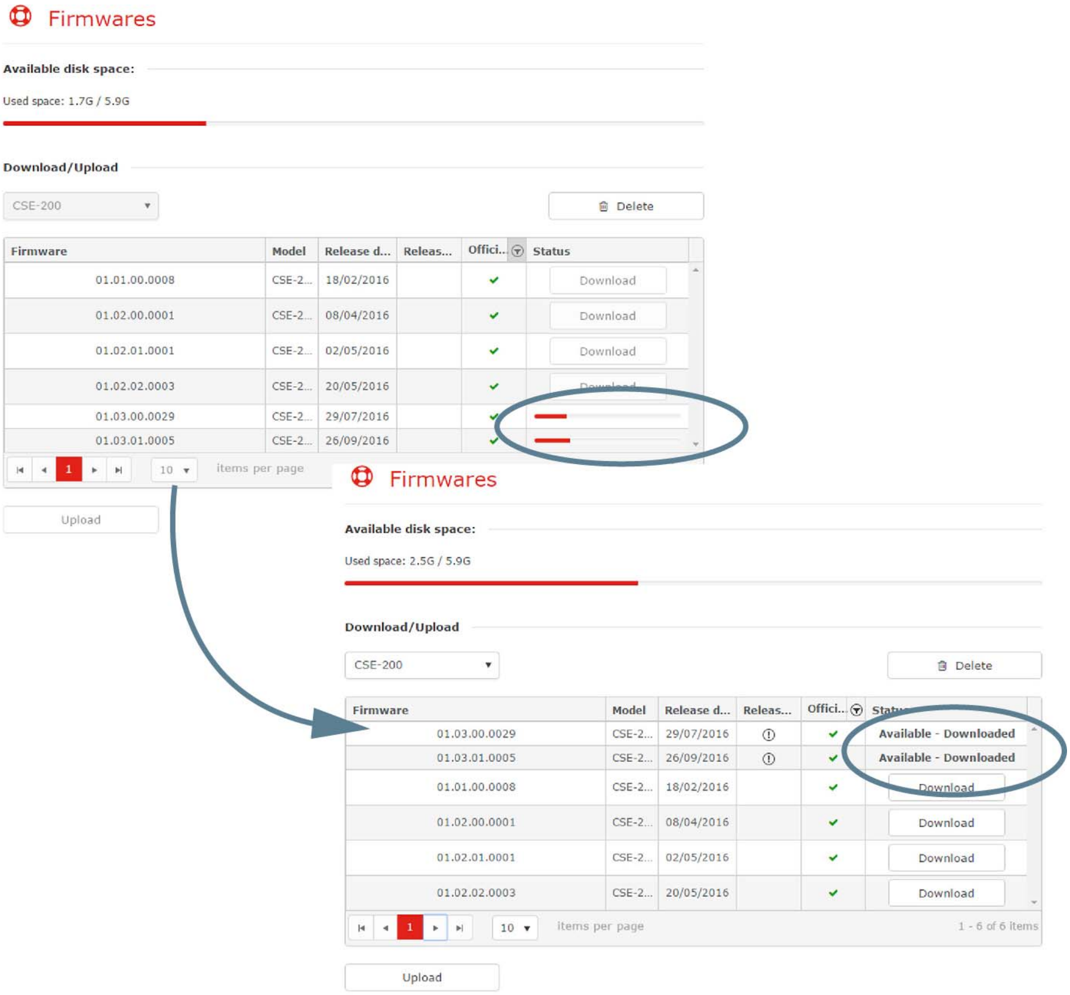
5. Click **OK**.

Download firmware

1. First select the desired device type from the drop down list before downloading or uploading a firmware.

   The possible firmware for that model are displayed.

2. On the firmware page, click on the download button next to the firmware you want to download.



Firmwares

Available disk space:

Used space: 1.7G / 5.9G

Download/Upload

CSE-200

Delete

Firmware	Model	Release d...	Releas...	Offici...	Status
01.01.00.0008	CSE-2...	18/02/2016		✓	Download
01.02.00.0001	CSE-2...	08/04/2016		✓	Download
01.02.01.0001	CSE-2...	02/05/2016		✓	Download
01.02.02.0003	CSE-2...	20/05/2016		✓	Download
01.03.00.0029	CSE-2...	29/07/2016		✓	
01.03.01.0005	CSE-2...	26/09/2016		✓	

1 10 items per page

Upload

Firmwares

Available disk space:

Used space: 2.5G / 5.9G

Download/Upload

CSE-200

Delete

Firmware	Model	Release d...	Releas...	Offici...	Status
01.03.00.0029	CSE-2...	29/07/2016	ⓘ	✓	Available - Downloaded
01.03.01.0005	CSE-2...	26/09/2016	ⓘ	✓	Available - Downloaded
01.01.00.0008	CSE-2...	18/02/2016		✓	Download
01.02.00.0001	CSE-2...	08/04/2016		✓	Download
01.02.01.0001	CSE-2...	02/05/2016		✓	Download
01.02.02.0003	CSE-2...	20/05/2016		✓	Download

1 10 items per page 1 - 6 of 6 items

Upload

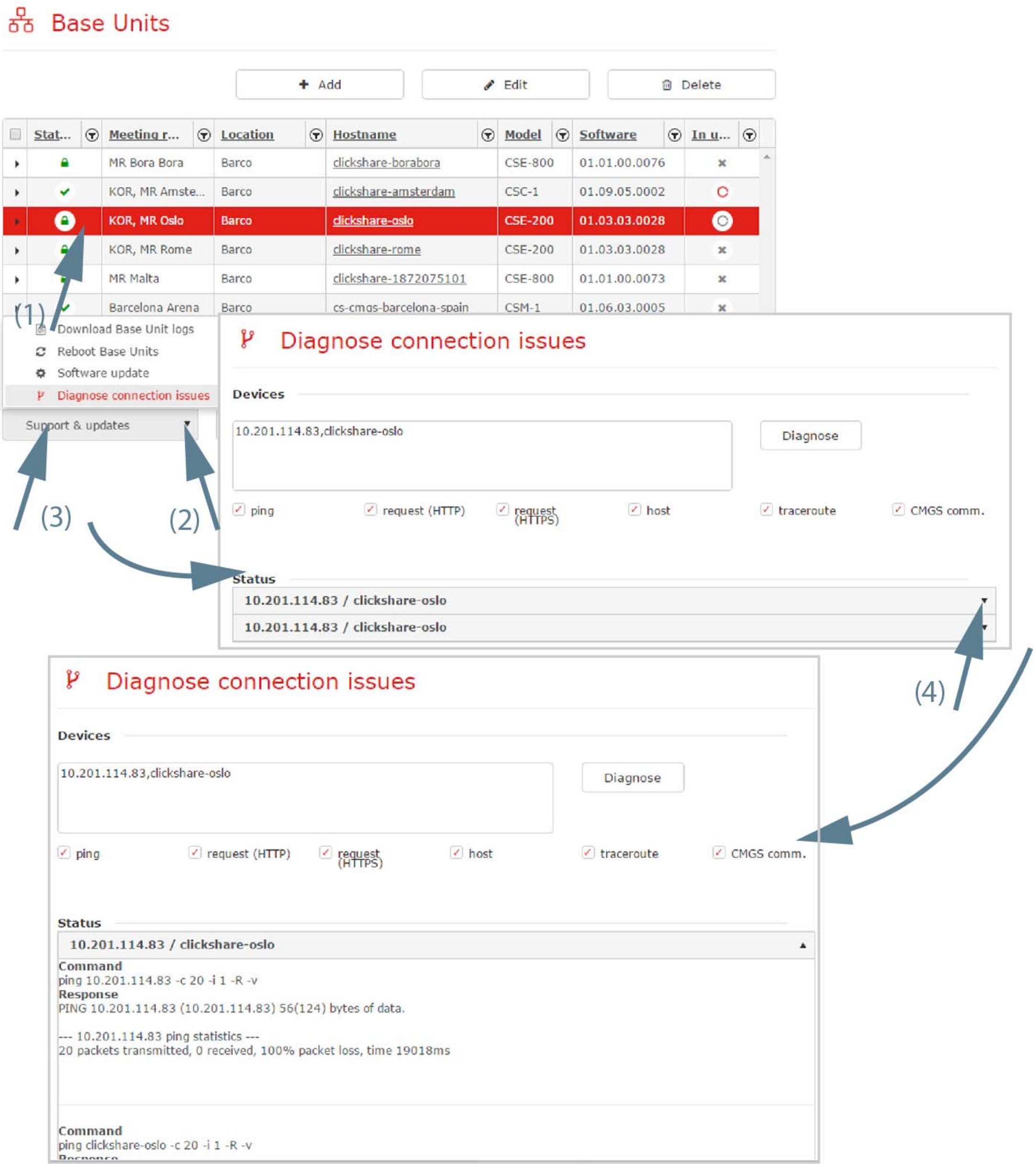
Image 2-15
Firmware download

The download starts.

2.7.4 Diagnose connection issues

How to start the diagnose

1. Select the Base Unit(s) to diagnose (1).



	Stat...	Meeting r...	Location	Hostname	Model	Software	In u...
▸	🔒	MR Bora Bora	Barco	clickshare-borabora	CSE-800	01.01.00.0076	✖
▸	✓	KOR, MR Amste...	Barco	clickshare-amsterdam	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	○
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	MR Malta	Barco	clickshare-1872075101	CSE-800	01.01.00.0073	✖
▸	✓	Barcelona Arena	Barco	cs-cmgs-barcelona-spain	CSM-1	01.06.03.0005	✖

10.201.114.83,clickshare-oslo

☑ ping ☑ request (HTTP) ☑ request (HTTPS) ☑ host ☑ traceroute ☑ CMGS comm.

10.201.114.83 / clickshare-oslo ▾

10.201.114.83 / clickshare-oslo ▾

10.201.114.83,clickshare-oslo

☑ ping ☑ request (HTTP) ☑ request (HTTPS) ☑ host ☑ traceroute ☑ CMGS comm.

10.201.114.83 / clickshare-oslo ▴

```
Command
ping 10.201.114.83 -c 20 -i 1 -R -v
Response
PING 10.201.114.83 (10.201.114.83) 56(124) bytes of data.

--- 10.201.114.83 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19018ms

Command
ping clickshare-oslo -c 20 -i 1 -R -v
Response
```

Image 2-16
Diagnosis connection issues

2. Click on the drop down box *Support & Updates* (2) and click **Diagnose connection issues** (3).

   The Diagnose connection issues window opens. The Device area gives an overview of the IP addresses of the selected Base Unit(s).

3. If the diagnosis is not started automatically, click on **Diagnose** to start the diagnose.

   The diagnosis is executed and displayed in the status pane as follow: IP address/hostname Base Unit.

4. To open the diagnosis log, click on the arrow next to the status line.
   To close the diagnosis log, click again on the arrow next to the status line.

5. To save the diagnosis log on your local drive, click on **Save**.

3. SCHEDULER

Only for IT admin and IT support users.

Overview

- Schedule a new job
- Edit a job
- Delete a job

About the scheduler

With the scheduler, software updates can be postponed until a certain time.

3.1 Schedule a new job

How to schedule

1. In the menu pane, click on **Scheduler** (a).

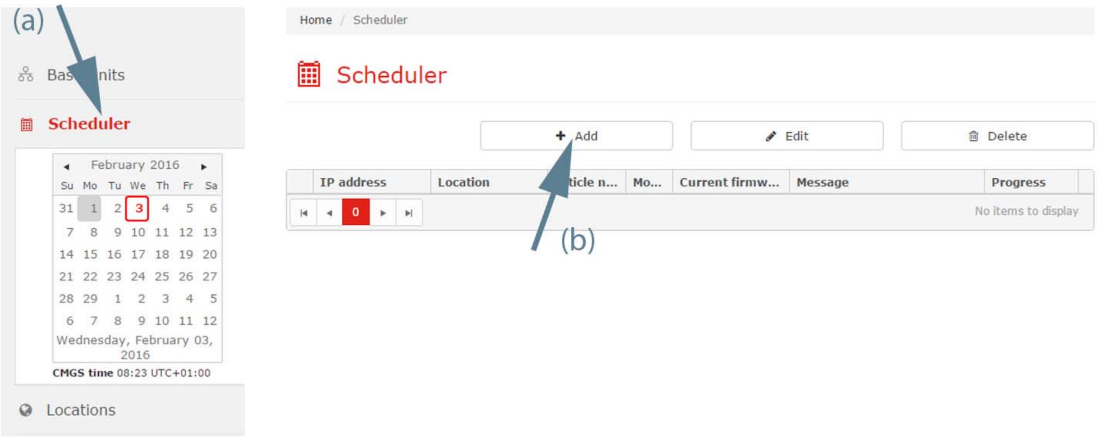


Image 3-1
Schedule new job

An overview of the scheduled jobs for the selected day is given. To see an overview for another day, click on a day in the calendar and if necessary, change the month. User is able to change month by clicking on the name of the current month. In order to view daily calendar user should click on the name of the current date, located in the bottom of the calendar.

Gray highlighted number represents the current day. Red surrounded number represents the schedule date.

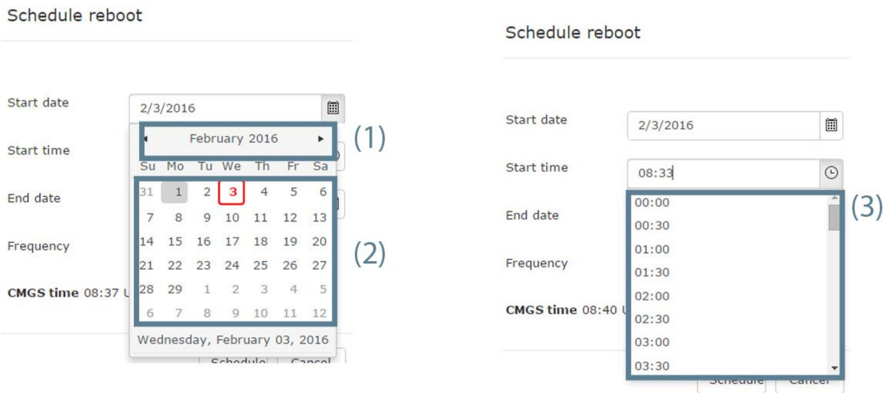
2. Click on **Add** (b).

An information message is displayed to announce that the Base Units overview page will be displayed. Select *Support & Updates* and then choose either *Updates*.

3. Follow the instruction as given in "Software update", page 22 or "Reboot Base Units", page 21. To finalize the procedure, select on **Scheduler** instead of **Apply now**.

4. To change the date, click on the calendar icon and select the date. Enter the time (hh:mm) or click on the clock icon and select a predefined time.

a) To change the year and month, click on the left or right arrow key next to the month-year name (1).



Schedule reboot

Start date 2/3/2016

Start time

End date

Frequency

CMGS time 08:37 U

February 2016

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	1	2	3	4	5
6	7	8	9	10	11	12

Wednesday, February 03, 2016

Schedule reboot

Start date 2/3/2016

Start time 08:33

End date

Frequency

CMGS time 08:40 U

00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30

Image 3-2
Scheduler

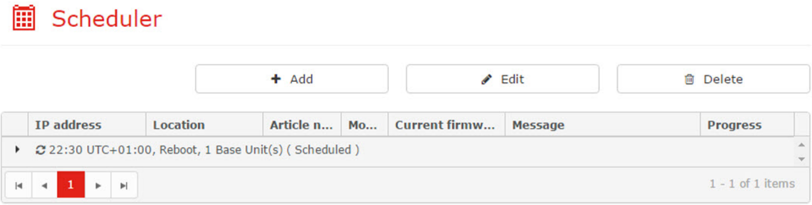
b) To change the day, click on the desired day in the calendar (2).

c) To set the desired time comparing to the server time, click on the icon and select a predefined time (3).

5. Set the frequency.

6. Click **Schedule**.

The Scheduler overview page is displayed again with the new job filled out. The status of the job is scheduled or pending.



Scheduler

IP address	Location	Article n...	Mo...	Current firmw...	Message	Progress
22:30 UTC+01:00, Reboot, 1 Base Unit(s) (Scheduled)						

1 - 1 of 1 items

Image 3-3
Scheduler overview page

The calendar highlights the days a job is created.

3.2 Edit a job

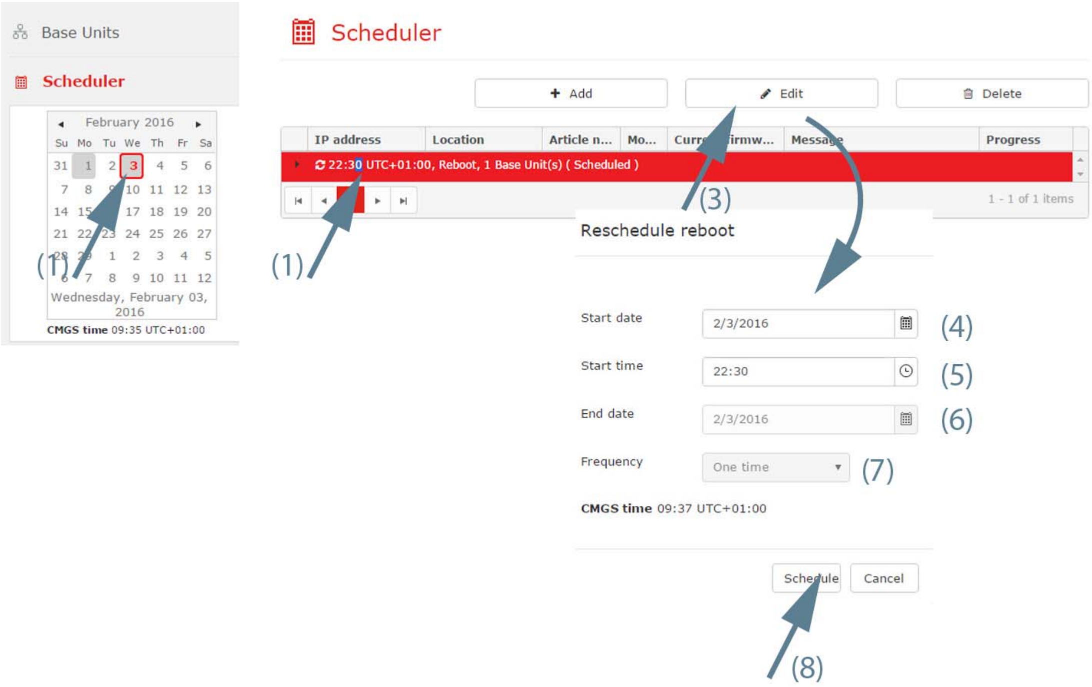
A scheduled job can only be edited if the user has access rights to the location of all Base Units in the scheduled job.

What can be done?

A scheduled job can be moved in time to a new time slot.

How to edit

1. Go to the month and date where the job can be found (1) and select the job to be edited (2).



22:30 UTC+01:00, Reboot, 1 Base Unit(s) (Scheduled)

Reschedule reboot

Start date 2/3/2016

Start time 22:30

End date 2/3/2016

Frequency One time

CMGS time 09:37 UTC+01:00

Image 3-4
Edit scheduled job

2. Click on **Edit** (3).

   The *Reschedule* window opens.

3. Change the start date. To change the date, click on the calendar icon and select the new date (4).
4. Set the new time. Click in the input field and enter the new time or click on the icon and select the new time (5).
5. Change the end date. To change the date, click on the calendar icon and select the new date (6).
6. Change the frequency if necessary (7).
7. Click **Schedule** to reschedule the job (8).

3.3 Delete a job

What can be done?

A scheduled job can be removed from the execution list. If a job consists of updates on multiple Base Units all will be removed from the calendar.

Deleting a recurrent Base Units job will offer the user the choice to remove the whole series or just the selected occurrence.

How to remove

1. Go to the date of the job to be deleted (1) and select the job (2). (date means year/month/day)

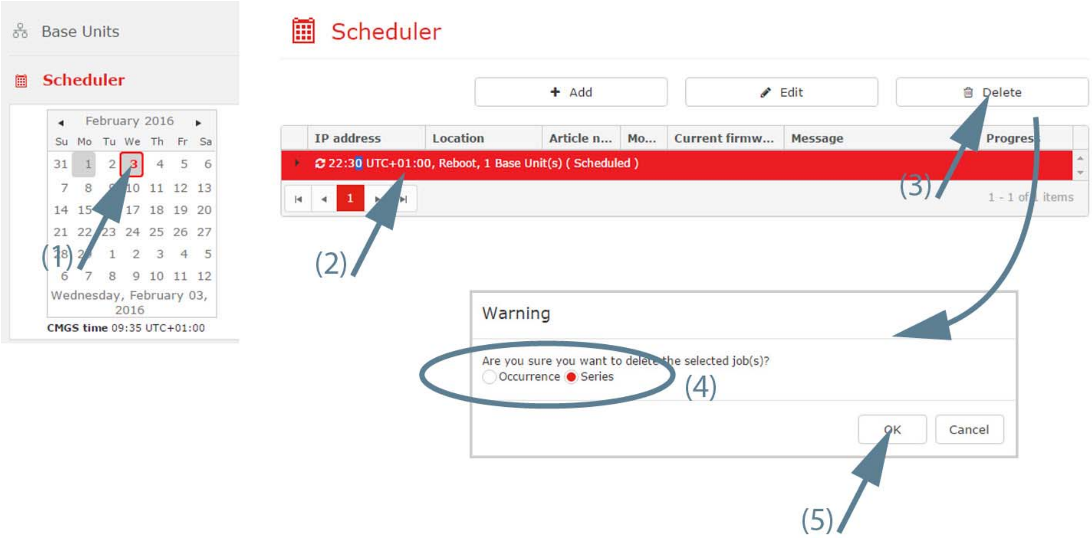


Image 3-5
Delete scheduled job

2. Click on the **Delete** button (3).

   A delete selection window is displayed.

3. Select *Occurence* or *Series* (4).
4. Click **OK** to confirm the deletion (5).

4. PERSONALIZATION

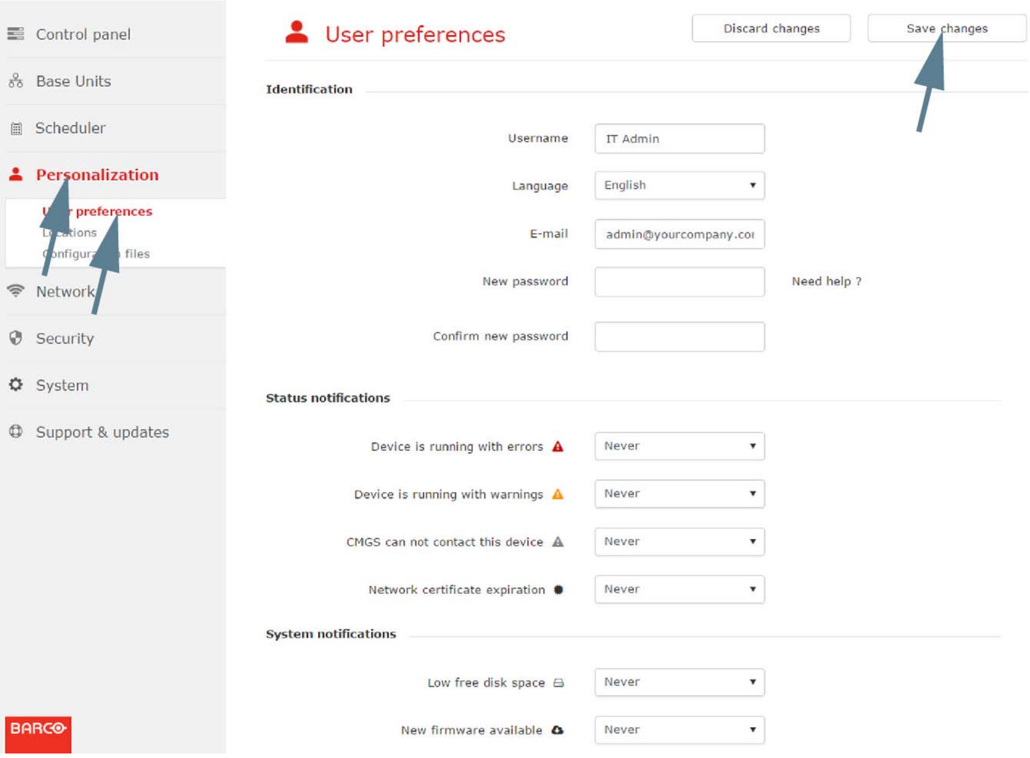
Overview

- User preferences
- Locations
- Configuration files

4.1 User preferences

How to setup

1. In the menu pane, click **Settings** and select *User preferences*.



Identification

Username: IT Admin

Language: English

E-mail: admin@yourcompany.coı

New password: Need help ?

Confirm new password:

Status notifications

Device is running with errors: Never

Device is running with warnings: Never

CMGS can not contact this device: Never

Network certificate expiration: Never

System notifications

Low free disk space: Never

New firmware available: Never

Image 4-1
User preferences

The current user preferences are displayed.

For the fields with a drop down box, click inside the field and select a new value out of the list. For text fields, click inside the field, select the current value and enter a new value with your keyboard.

2. Click on **Save changes** to apply the changes.

4.2 Locations

Only for IT admin user.

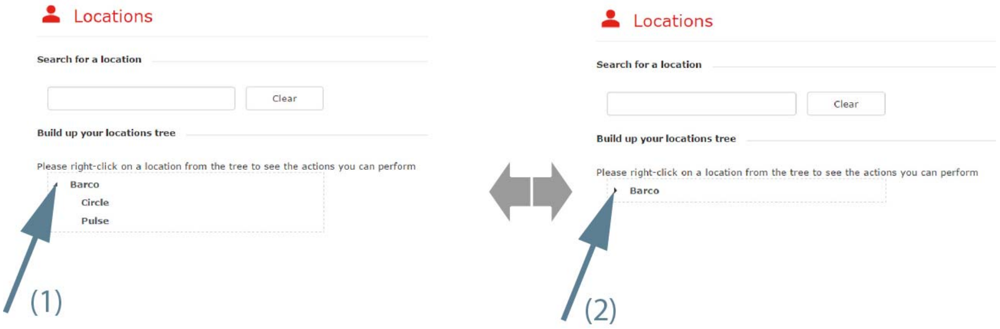
Overview

- Expand/collapse tree
- Add new location
- Rename location
- Delete location
- Move a location
- Search for a location

4.2.1 Expand/collapse tree

How to collapse/expand

1. To collapse a expanded branch, click on the arrow icon in front of a branch (1).
2. To expand a collapsed branch, click on the arrow icon in front of a branch (2).

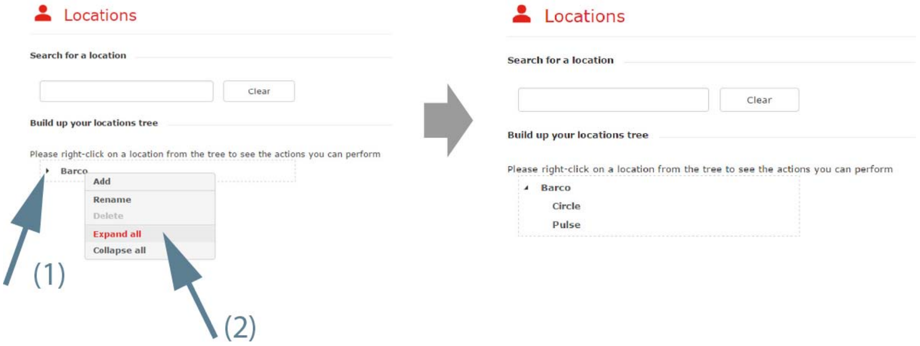


Please right-click on a location from the tree to see the actions you can perform

Image 4-2
Collapse/expand locations

Expand all

1. Right click on a collapsed branch with sub branches.



Please right-click on a location from the tree to see the actions you can perform

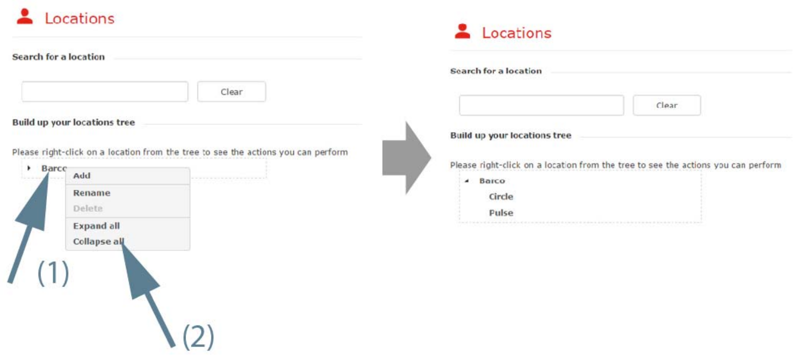
Image 4-3
Expand al

2. Select *Expand all*.

   The branch is expanded until its deepest level.

Collapse all

1. Right click on an expanded branch with sub branches.



Please right-click on a location from the tree to see the actions you can perform

Image 4-4
Collapse all

2. Select *Collapse all*.

   The branch with its sub branches is collapsed.

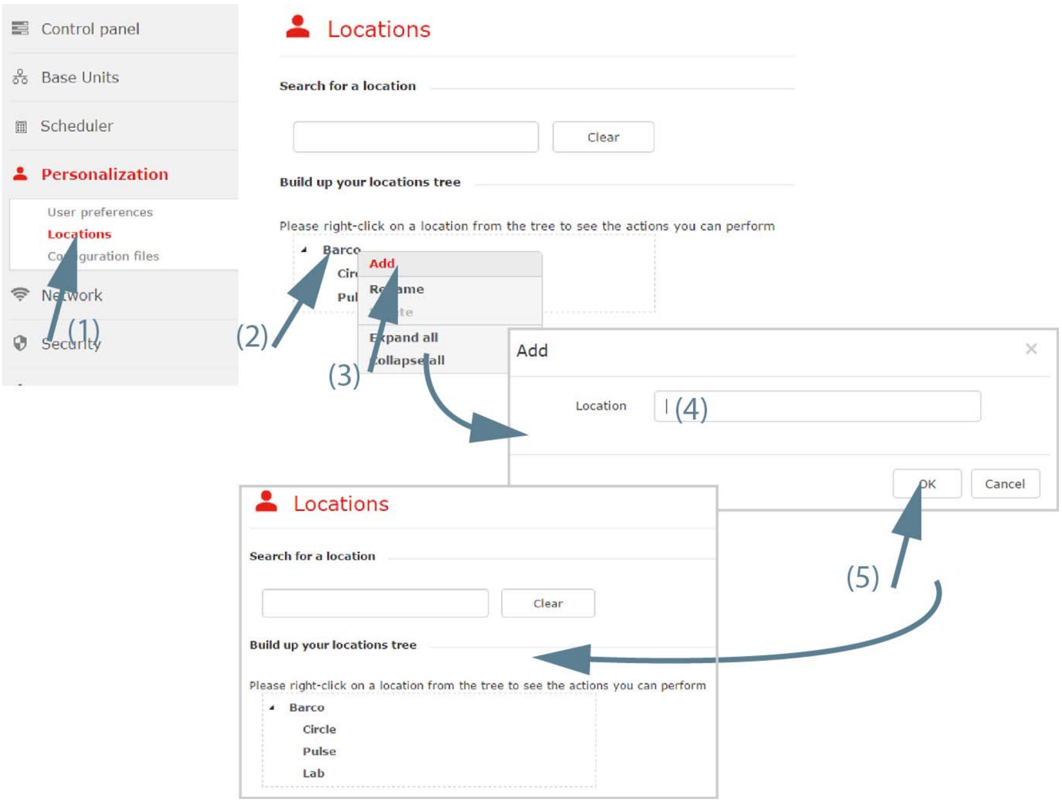
4.2.2 Add new location

What can be done?

A new location can be added to the location tree via the locations overview page

How to add

1. Select **Personalization** and click on **Locations** to display the locations page (1).



Please right-click on a location from the tree to see the actions you can perform

Image 4-5
Add new location

2. Right click on a location in the tree where to add a new location (2).

   A context menu opens.

3. Select *Add* (3).

   A *Add* window opens.

4. Enter a name for the location (4) and click **OK** (5).
   Note: *It is not allowed to use the backslash character "\" in the location name.*

   The new location is added to the selected branch.

4.2.3 Rename location

What can be done?

The name of any location in the tree can be changed.

How to rename

1. Select **Personalization** and click on **Locations** to display the locations page (1).

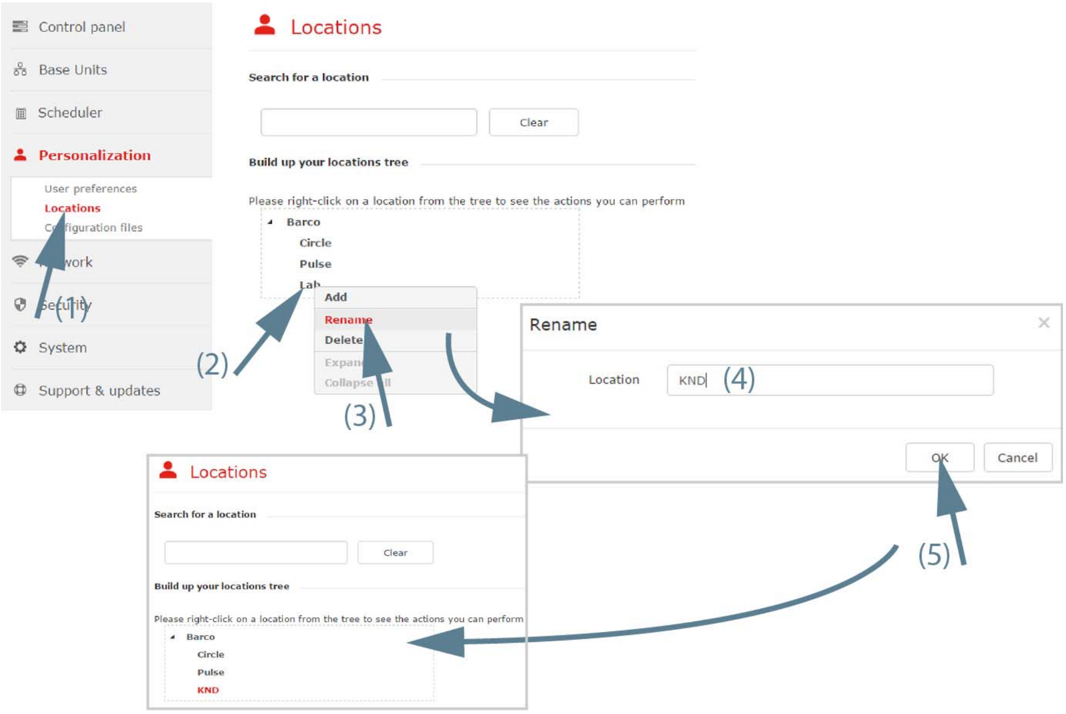


Image 4-6
Rename location

2. Right click on a location to rename (2).

   A context menu opens.

3. Select *Rename* (3).

   The *Rename* window opens

4. Edit the location name (4) and click **OK**.
   Note: *It is not allowed to use the backslash character "\" in the location name.*

   The location name is updated in the location tree.

4.2.4 Delete location

What can be done?

Any user added location in the locations tree can be removed from the tree.

Deleting a location is only possible when no Base Units are assigned to it or to one of its sub branches.

How to delete

1. Select **Personalization** and click on **Locations** to display the locations page (1).

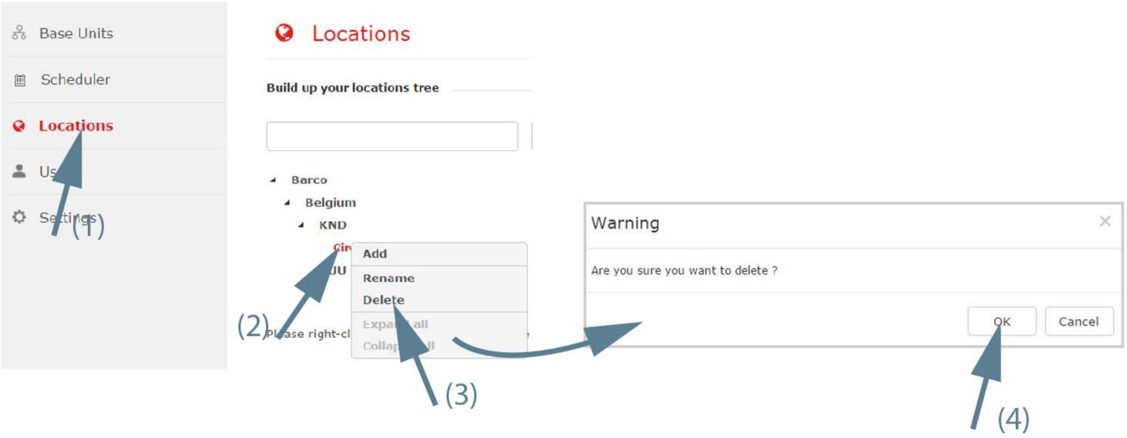


Image 4-7
Delete location

2. Right click on a location to remove (2).

   A context menu opens.

3. Select **Delete** (3) to remove the selected location.

   A warning message is displayed.

   If there are Base Units still connected to the selected branch or to one of its subbranches, the delete operation is not possible.

4. Click **OK** (4) to remove the selected location from the location tree. Also the sub-locations will be deleted.

4.2.5 Move a location

What can be done?

A location can be moved from one branch to another.

How to move

1. Select **Personalization** and click on **Locations** to display the locations page (1).

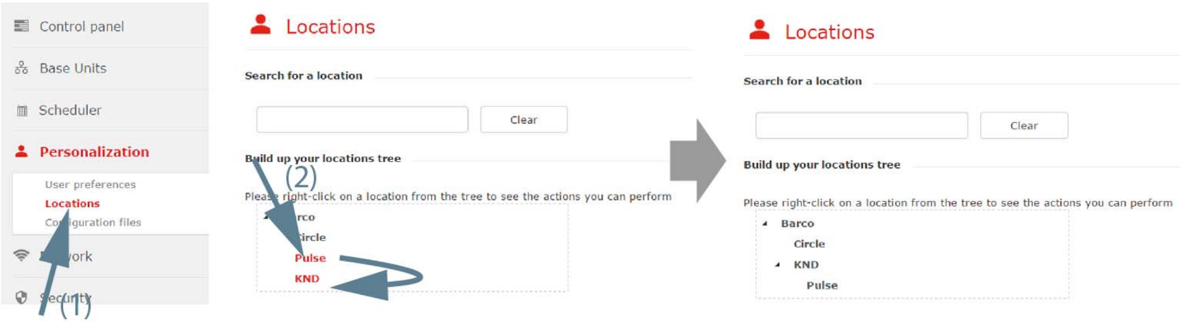


Image 4-8
Move location

2. Click on a location and drag to the desired place (2).

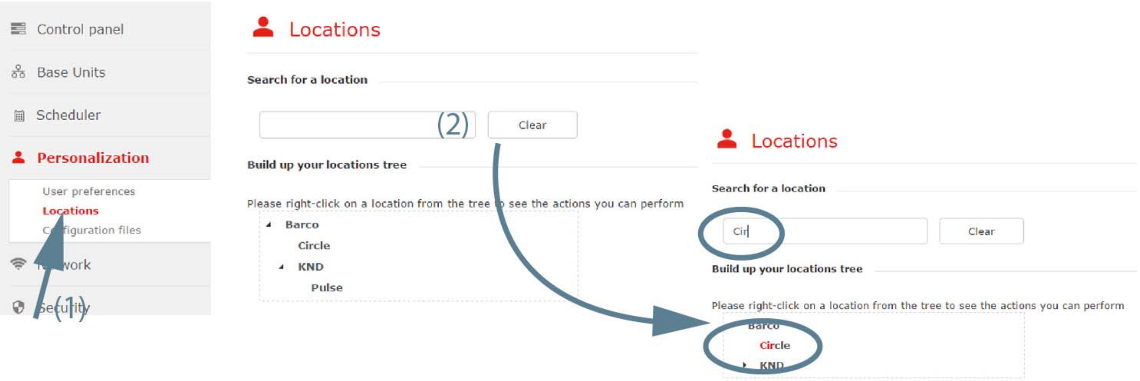
   While dragging a plus sign indicates that the dragged location can be dropped on that place.

   A cross sign indicates that the dragged location cannot be dropped on that place.

4.2.6 Search for a location

How to search

1. Select **Personalization** and click on **Locations** to display the locations page (1).



Please right-click on a location from the tree to see the actions you can perform

Image 4-9
Search for location

2. Click in the search criteria's input field and start entering your search criterion (2).

   The location tree is immediately updated while typing the search criterion.

   Click **Clear** to clear the search criteria.

4.3 Configuration files

Overview

- Clone Base Unit settings
- Backup CMGS configuration
- Restore CMGS configuration

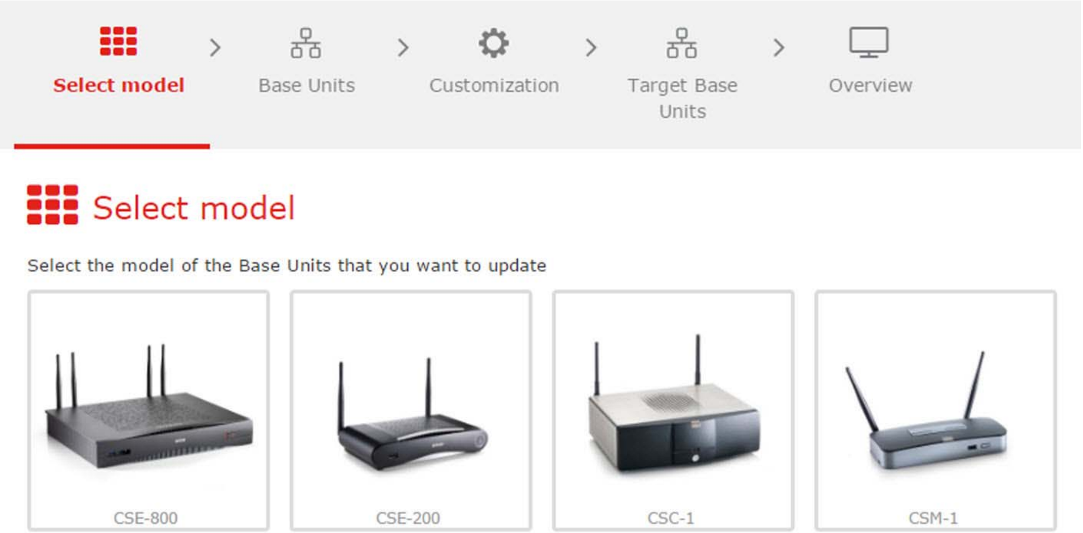
4.3.1 Clone Base Unit settings

About Base Unit settings

The current settings of a Base Unit can be implemented on other Base Units of the same model. A wizard will guide you through the process.

How to clone

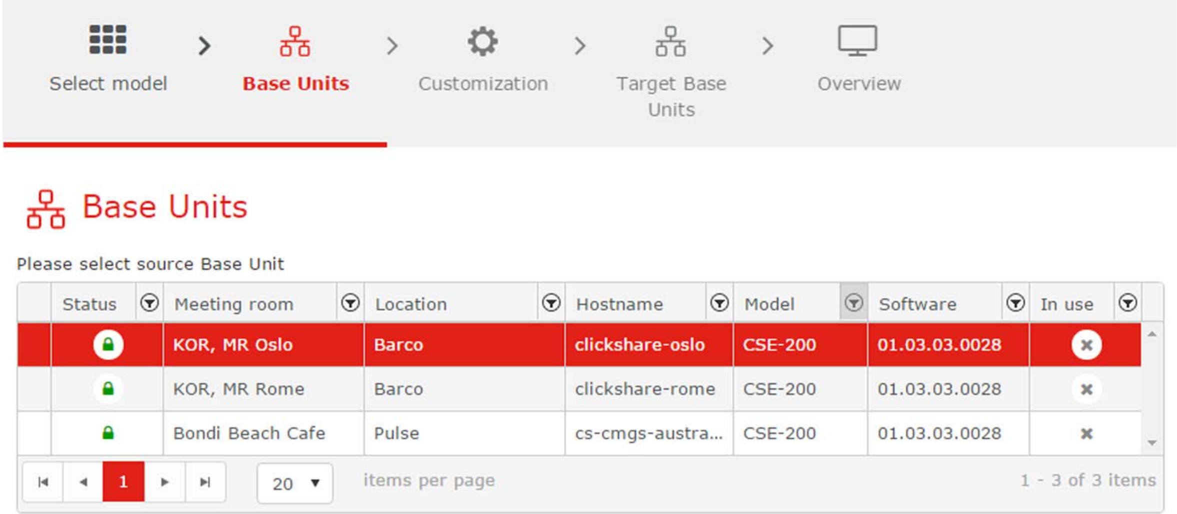
1. Select **Personalization** and click **Configuration files** to display the *Configuration files* page.
2. Click **Start wizard** next to *Clone Base Unit settings*.
3. Select your model of the Base Units you want to update and click **Next**.



Select the model of the Base Units that you want to update

Image 4-10
Select model

4. Select you source Base Unit and click **Next**.



Base Units

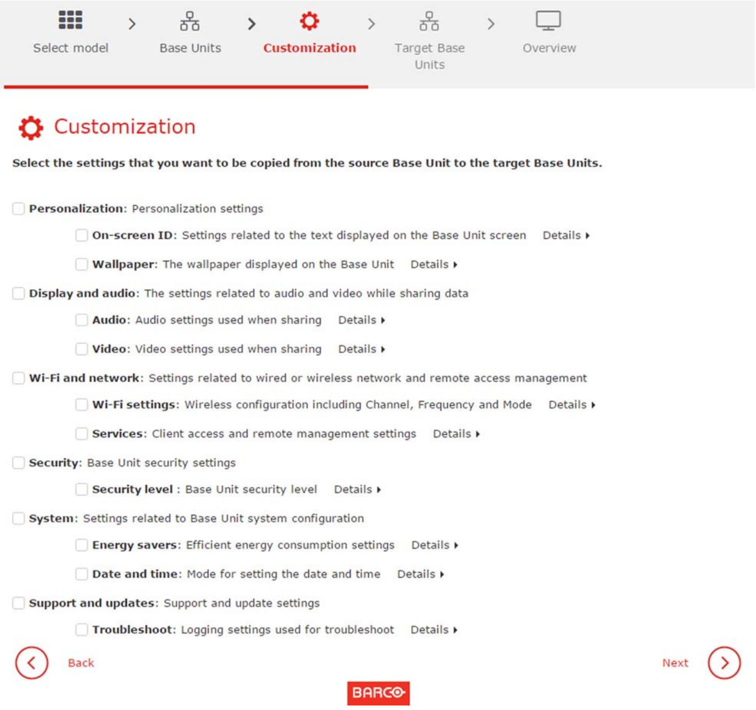
Please select source Base Unit

	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
	🔒	Bondi Beach Cafe	Pulse	cs-cmgs-austra...	CSE-200	01.03.03.0028	✖

1 | 20 items per page | 1 - 3 of 3 items

Image 4-11
Select Base Unit

5. Select the settings that you want to be copied from the Base Unit. Check the check box in front of the desired settings and click **Next**.
   To get more detailed information about a certain customization setting, click on **Details** next to the setting.



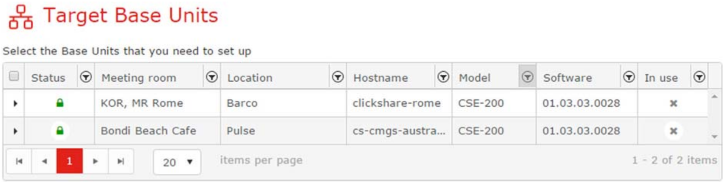
Customization

Select the settings that you want to be copied from the source Base Unit to the target Base Units.

- □ **Personalization**: Personalization settings
  - □ **On-screen ID**: Settings related to the text displayed on the Base Unit screen Details ▸
  - □ **Wallpaper**: The wallpaper displayed on the Base Unit Details ▸
- □ **Display and audio**: The settings related to audio and video while sharing data
  - □ **Audio**: Audio settings used when sharing Details ▸
  - □ **Video**: Video settings used when sharing Details ▸
- □ **Wi-Fi and network**: Settings related to wired or wireless network and remote access management
  - □ **Wi-Fi settings**: Wireless configuration including Channel, Frequency and Mode Details ▸
  - □ **Services**: Client access and remote management settings Details ▸
- □ **Security**: Base Unit security settings
  - □ **Security level** : Base Unit security level Details ▸
- □ **System**: Settings related to Base Unit system configuration
  - □ **Energy savers**: Efficient energy consumption settings Details ▸
  - □ **Date and time**: Mode for setting the date and time Details ▸
- □ **Support and updates**: Support and update settings
  - □ **Troubleshoot**: Logging settings used for troubleshoot Details ▸

Image 4-12
Customization

6. Select the target Base Units and click **Next**.



Target Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
▸	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
▸	🔒	Bondi Beach Cafe	Pulse	cs-cmgs-austra...	CSE-200	01.03.03.0028	✖

1 | 20 items per page | 1 - 2 of 2 items

Image 4-13
Select Target Base Units

Note: *The target Base Units may reboot after applying the settings.*

7. Click **Finish** on the *Overview settings* page to execute the cloning.

4.3.2 Backup CMGS configuration

How to backup

1. Select **Personalization** and click **Configuration files** to display the *Configuration files* page.

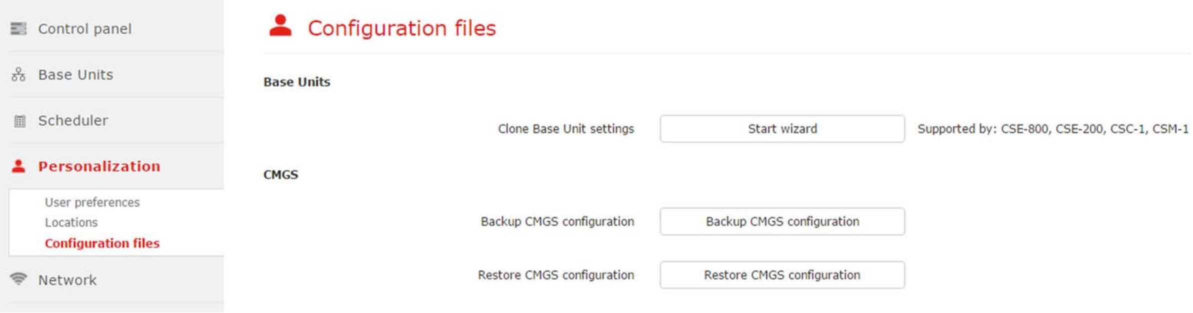


Image 4-14
Configuration files

2. Click on **Backup CMGS configuration** next to *Backup CMGS configuration*.

   A backup file is created and stored on the hard disk. The file has a tar.gz.gpg format.

   Restore will be executed. During this time the Collaboration Management Suite will not be accessible. This process will overwrite current settings. The firmware and scheduled software update jobs will not be restored. You will also be logged out of the application when the restore process ends.

3. To continue, click **OK**.

4.3.3 Restore CMGS configuration

How to restore

1. Select **Personalization** and click **Configuration files** to display the *Configuration files* page.

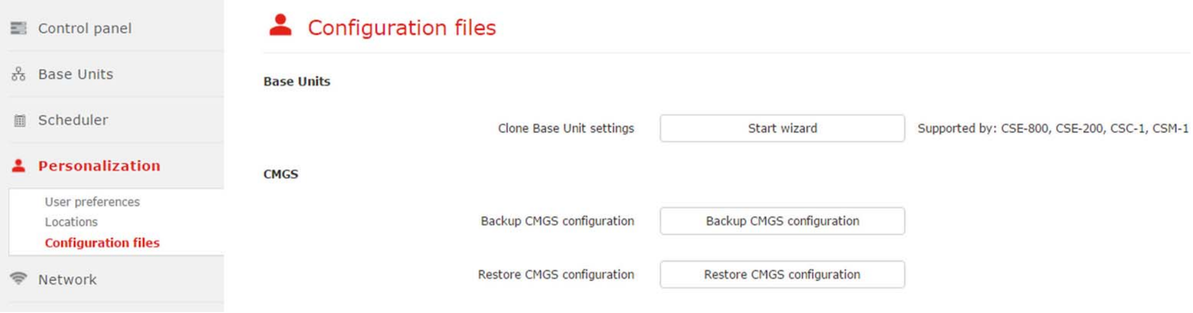


Image 4-15
Configuration files

2. Click on **Restore CMGS configuration** next to *Restore CMGS configuration*.

   Restore will be executed. During this time the Collaboration Management Suite will not be accessible. This process will overwrite current settings. The firmware and scheduled software update jobs will not be restored. You will also be logged out of the application when the restore process ends.

5. NETWORK

Overview

- Base Units WiFi and network settings
- LAN settings
- Network integration
- Notifications

5.1 Base Units WiFi and network settings

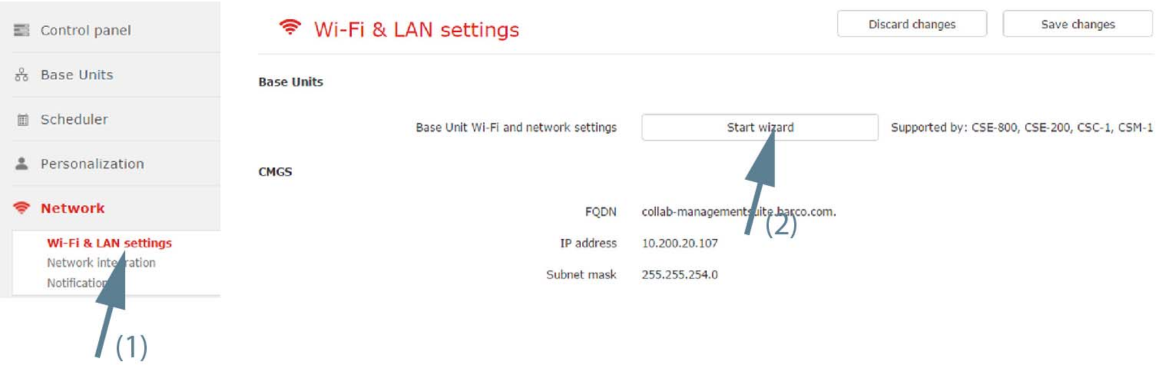
About Base Units WiFi and network settings

The availability of the webUI via WiFi can be set.

For the LAN settings, the use of the a proxy server can be set.

How to setup

1. Select **Network** and click **Wi-Fi & LAN settings** to display the *Wi-Fi & LAN settings* page.



Base Units

Base Unit Wi-Fi and network settings — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

CMGS

FQDN collab-managementsuite.barco.com.

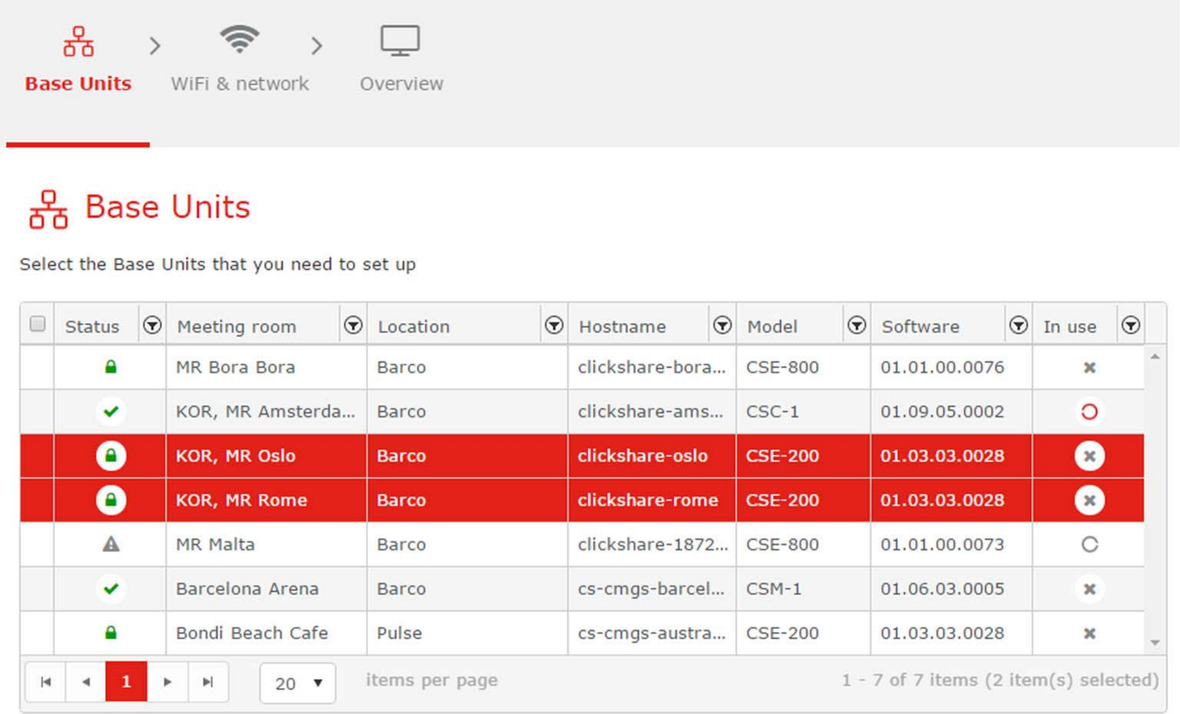
IP address 10.200.20.107

Subnet mask 255.255.254.0

Image 5-1
Network, start wizard

2. Click on **Start wizard** next to *Base Unit Wi-Fi and network settings* to start.

3. Select the Base Units that need to set up. Click **Next** to continue.



Base Units > WiFi & network > Overview

Base Units

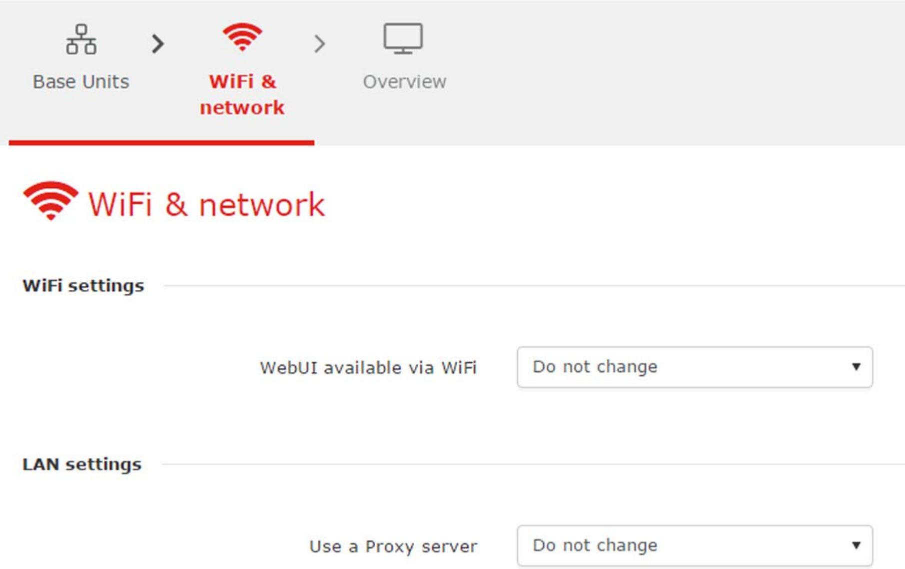
Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Barco	clickshare-bora...	CSE-800	01.01.00.0076	✖
	✓	KOR, MR Amsterda...	Barco	clickshare-ams...	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✖
	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✖
	⚠	MR Malta	Barco	clickshare-1872...	CSE-800	01.01.00.0073	○
	✓	Barcelona Arena	Barco	cs-cmgs-barcel...	CSM-1	01.06.03.0005	✖
	🔒	Bondi Beach Cafe	Pulse	cs-cmgs-austra...	CSE-200	01.03.03.0028	✖

1 | 20 ▾ items per page | 1 - 7 of 7 items (2 item(s) selected)

Image 5-2
Base units to setup

4. To change the setting for the WebUI availability via WiFi, click on the drop down box next to *WebUI available via WiFi* and select the desired setting.



Base Units > WiFi & network > Overview

WiFi & network

WiFi settings

WebUI available via WiFi: Do not change ▾

LAN settings

Use a Proxy server: Do not change ▾

Image 5-3
Network, WiFi and LAN settings

The following setting are possible:

- Do not change: keep the current setting as set in the WebUI of the Base Unit.
- Enable: WebUI access via WiFi is enabled.
- Disable: WebUI access via WiFi is disabled.

5. To change the Proxy server setting, click on the drop down box next to *Use a Proxy server* and select the desired setting.

The following setting are possible:

- Do not change: keep the current setting as set in the WebUI of the Base Unit.
- Disable proxy server: the use of the proxy server is disabled.
- Use proxy settings below: use the proxy setting as set on this page.
  - Fill out the Proxy server URL
  - (optional) fill out Proxy server port
  - (optional) fill out Username
  - (optional) fill out Password
- Note: Changes made to the proxy settings will also be reflected in the CMGS proxy settings.

Click **Next** to continue to get an overview.

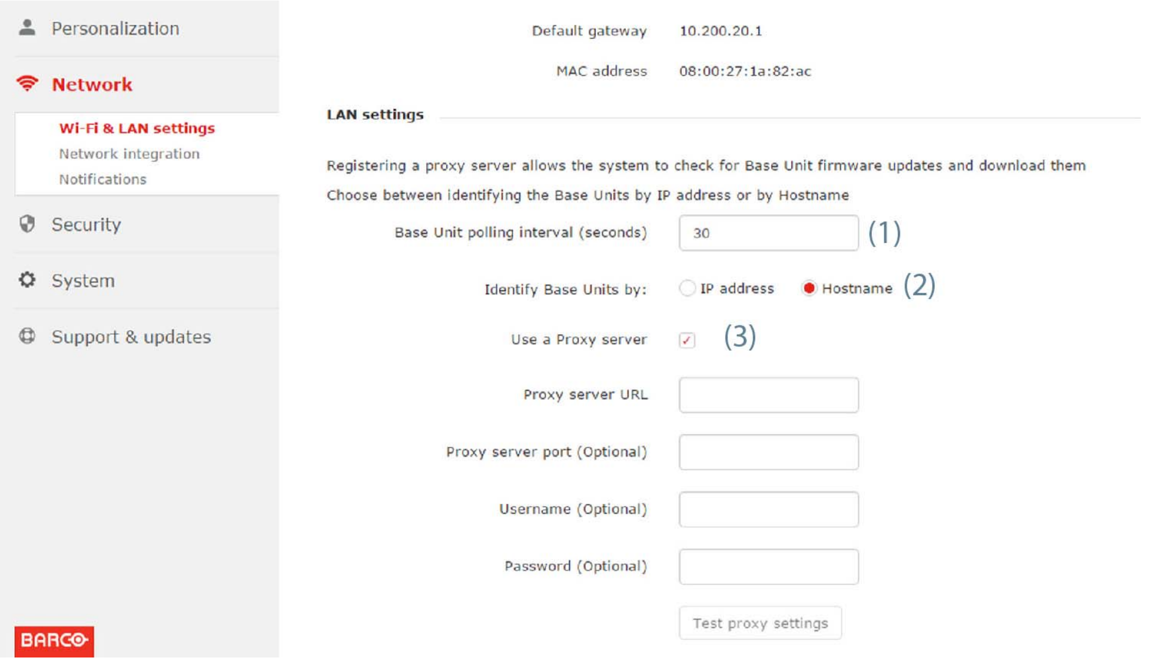
6. If you agree with the overview settings, click **Finish**.

   WiFi networks settings might affect (downgrade) previous Base Units security settings and need button repairing.

5.2 LAN settings

How to set

1. Select **Network** and click **Wi-Fi & LAN settings** to display the *Wi-Fi & LAN settings* page.



Default gateway 10.200.20.1

MAC address 08:00:27:1a:82:ac

LAN settings

Registering a proxy server allows the system to check for Base Unit firmware updates and download them

Choose between identifying the Base Units by IP address or by Hostname

Base Unit polling interval (seconds) 30

Identify Base Units by: ○ IP address ● Hostname

Use a Proxy server ☑

Proxy server URL

Proxy server port (Optional)

Username (Optional)

Password (Optional)

Image 5-4
Network, LAN settings

2. To set up the Base Unit polling interval in seconds, click in the input field, select the current value and enter the desired value.
3. To setup the identification of the Base Units, check the radio button of your choice.
   The following choices are possible:
   - IP address
   - Hostname
4. If you want to use a proxy server, check the check box behind *Use a Proxy server.*

   If checked, fill out the proxy settings.
   - Fill out the Proxy server URL
   - (optional) fill out Proxy server port
   - (optional) fill out Username
   - (optional) fill out Password
5. Click **Save changes** to apply the settings.

5.3 Network integration

Overview

- Network integration, wizard
- Network integration, EAP-TLS security mode
- Network integration, EAP-TTLS security mode
- Network integration, PEAP security mode
- Network integration, WPA2-PSK security mode

5.3.1 Network integration, wizard

Introduction

“Network Integration” aims at deploying the Base units in larger organizations without interfering with the existing wireless network infrastructure. In a default stand-alone setup, the ClickShare Base Unit creates its own wireless access point (AP) which the ClickShare Buttons use to connect. These so-called “rogue” APs can become a nuisance in larger installations. Next to that, meeting participants who are sharing content from mobile devices have to switch networks to connect with the ClickShare Base Unit.

This is where Network Integration comes in. Once fully configured and enabled, the built-in AP of the Base Unit is disabled. The Button or the mobile devices can then connect to a wireless access point that is part of the corporate network. At this point, the Base Unit needs to be connected to the corporate network via the wired Ethernet interface so that the Buttons and mobile devices can share their content on the Base Unit.

Security modes

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

- The first one, which applies to a typical corporate network setup, is WPA2-Enterprise with 802.1X.
- As we also want to support smaller organizations, which might have a more traditional Wi-Fi setup, there is also support for WPA2-PSK, also known as WPA2-Personal.

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

WPA2-Enterprise with 802.1X

WPA2-Enterprise relies on a server (using RADIUS) to authenticate each individual client on the network. To do this, authentication 802.1x is used (also known as port-based Network Access Control). 802.1x encapsulates the Extensible Authentication Protocol (EAP) for use on local area networks. This is also known as “EAP over LAN” or EAPoL. Using RADIUS, these EAPoL messages are routed through the network in order to authenticate the client device on the network – which, in the case of ClickShare, are the Buttons.

The 802.11i (WPA2) standard defines a number of required EAP methods. However, not all of them are used extensively in the field, and some other ones (which are not in the standard) are used much more often. Therefore, we have selected the most widely used EAP methods. The list of EAP methods supported in the ClickShare system is:

- EAP-TLS
- PEAP
- EAP-TTLS

Considerations

When you choose to integrate the ClickShare system into your corporate network, there are a few things to consider up front. First of all, make sure that all your Base Units can be connected to your network via the wired Ethernet interface. Also, take into account the amount of bandwidth that each Button needs to stream the captured screen content to the Base Unit – this is usually somewhere between 5 and 15 Mbps. So, prevent bottlenecks in your network (e.g. 100 Mbps switches) that could potentially degrade your ClickShare experience due to a lack of bandwidth.

Prerequisites

Before rolling out ClickShare Network Integration, make sure your infrastructure meets the following prerequisites.

Network

Once you enable the corporate network, the internal Wi-Fi access point of the ClickShare Base Unit is disabled. Make sure your Base Unit is connected to the corporate network via its wired Ethernet interface.

Firewall

To ensure that you can successfully share content via the ClickShare Button, or from mobile devices, to the Base Unit, make sure the ports mentioned in "Used ports", page 75 are open on your network.

VLAN

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

DNS

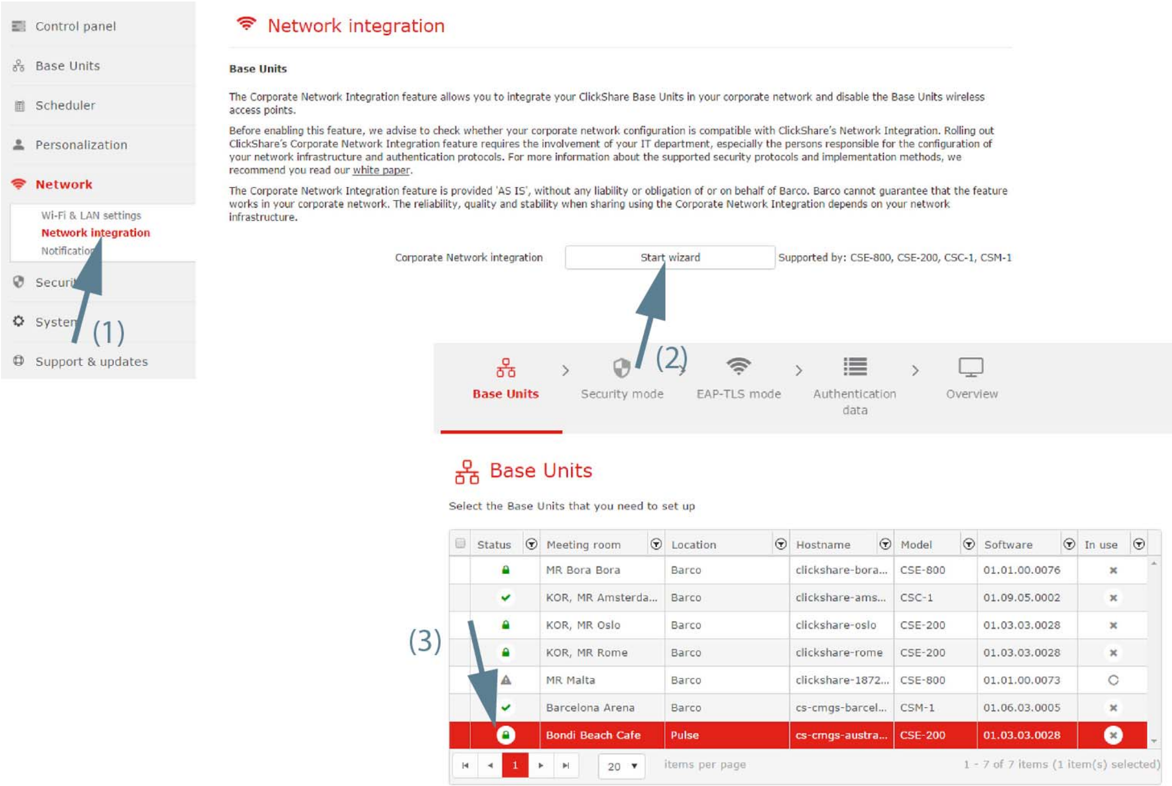
For the Buttons to be able to stream their content to the Base Unit, they must be able to resolve the Base Unit's hostname within the network. If no DNS is available Buttons will fall back to the IP of the Base Unit at the moment of USB pairing. Because of this we strongly advise to reserve IP addresses in your DHCP server for each Base Unit to prevent issues when the hostname is not resolvable.

NTP

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

Start up the wizard

1. Select **Network** and click **Network integration** to display the *Network integration* page (1).



Network integration

Base Units

The Corporate Network Integration feature allows you to integrate your ClickShare Base Units in your corporate network and disable the Base Units wireless access points.

Before enabling this feature, we advise to check whether your corporate network configuration is compatible with ClickShare's Network Integration. Rolling out ClickShare's Corporate Network Integration feature requires the involvement of your IT department, especially the persons responsible for the configuration of your network infrastructure and authentication protocols. For more information about the supported security protocols and implementation methods, we recommend you read our white paper.

The Corporate Network Integration feature is provided 'AS IS', without any liability or obligation of or on behalf of Barco. Barco cannot guarantee that the feature works in your corporate network. The reliability, quality and stability when sharing using the Corporate Network Integration depends on your network infrastructure.

Corporate Network integration [Start wizard] Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Barco	clickshare-bora...	CSE-800	01.01.00.0076	✕
	✓	KOR, MR Amsterda...	Barco	clickshare-ams...	CSC-1	01.09.05.0002	✕
	🔒	KOR, MR Oslo	Barco	clickshare-oslo	CSE-200	01.03.03.0028	✕
	🔒	KOR, MR Rome	Barco	clickshare-rome	CSE-200	01.03.03.0028	✕
	⚠	MR Malta	Barco	clickshare-1872...	CSE-800	01.01.00.0073	○
	✓	Barcelona Arena	Barco	cs-cmgs-barcel...	CSM-1	01.06.03.0005	✕
	🔒	Bondi Beach Cafe	Pulse	cs-cmgs-austra...	CSE-200	01.03.03.0028	✕

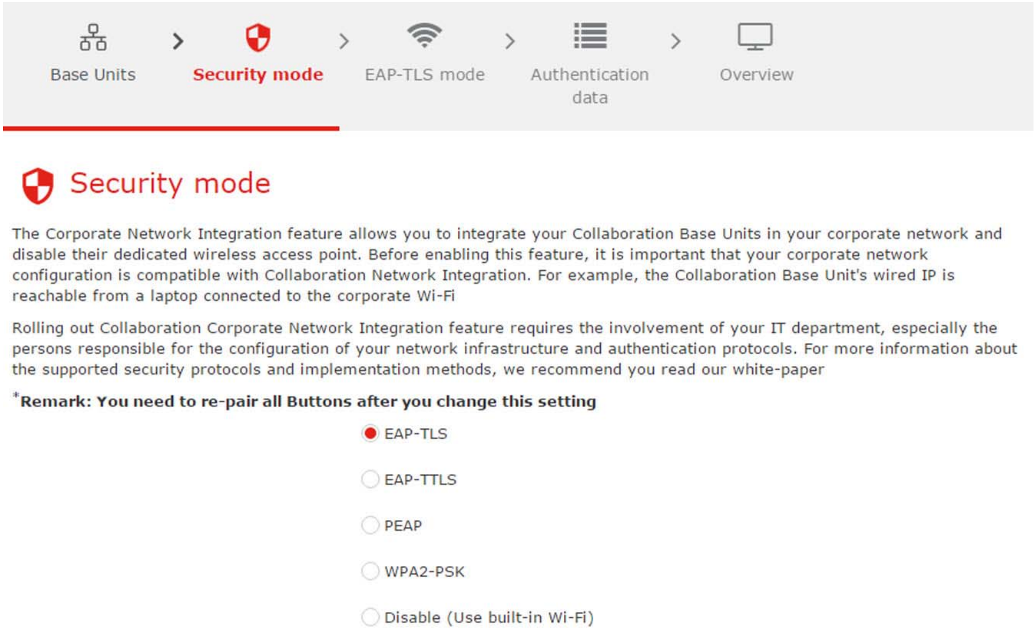
1 | 20 items per page | 1 - 7 of 7 items (1 item(s) selected)

Image 5-5
Network integration, start wizard

2. Click **Start wizard** (2).

3. Select the Base Units that you need to set up (3). Click **Next** to continue.

4. Select the Security mode. Click **Next** to continue.


Base Units > Security mode > EAP-TLS mode > Authentication data > Overview

Security mode

The Corporate Network Integration feature allows you to integrate your Collaboration Base Units in your corporate network and disable their dedicated wireless access point. Before enabling this feature, it is important that your corporate network configuration is compatible with Collaboration Network Integration. For example, the Collaboration Base Unit's wired IP is reachable from a laptop connected to the corporate Wi-Fi

Rolling out Collaboration Corporate Network Integration feature requires the involvement of your IT department, especially the persons responsible for the configuration of your network infrastructure and authentication protocols. For more information about the supported security protocols and implementation methods, we recommend you read our white-paper

*Remark: You need to re-pair all Buttons after you change this setting**

● EAP-TLS

○ EAP-TTLS

○ PEAP

○ WPA2-PSK

○ Disable (Use built-in Wi-Fi)

Image 5-6
Network integration, security mode

The following modes are available:

- EAP-TLS
- EAP-TTLS
- PEAP
- WPA2–PSK
- Disabled: use the built-in WiFi

5.3.2 Network integration, EAP-TLS security mode

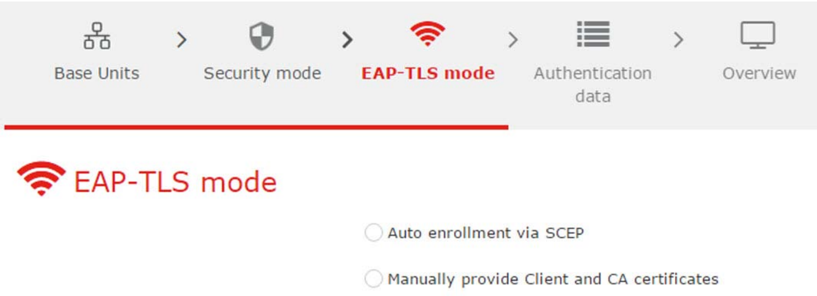
About EAP-TLS

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.

Start up for EAP-TLS

1. Select the radio button next to *EAP-TLS* and click **Next**.

   The EAP-TLS mode window opens.


Base Units > Security mode > EAP-TLS mode > Authentication data > Overview

EAP-TLS mode

○ Auto enrollment via SCEP

○ Manually provide Client and CA certificates

Image 5-7
EAP-TLS mode

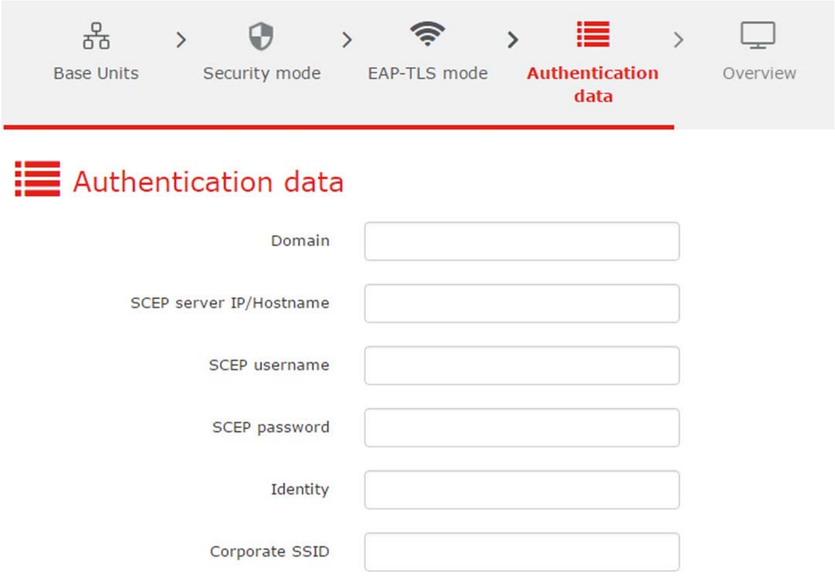
Two choices are possible:

- Auto alignment via SCEP
- Manually provide Client & CA certificates

Using SCEP

Select the radio button next to *Auto enrollment via SCEP* and click **Next**.

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. No other SCEP server implementations are supported.



Authentication data

Domain

SCEP server IP/Hostname

SCEP username

SCEP password

Identity

Corporate SSID

Image 5-8
SCEP, authentication data

About NDES

The Network Device Enrolment Service is Microsoft's server implementation of the SCEP protocol. If you want to enable EAP-TLS using SCEP make sure NDES is enabled, configured and running on your Windows Server. For more details about setting up NDES, please visit the Microsoft website[3]. SCEP uses a so called *"challenge password"* to authenticate the enrollment request. For NDES, this challenge can be retrieved from your server at: http(s)://[your-server-hostname]/CertSrv/mscep_admin.

After you enter the necessary credentials into the setup wizard, the Base Unit will automatically retrieve this challenge from the web page and use it in the enrollment request, thereby fully automating the process.

Necessary Data to continue:

Domain	The company domain for which you are enrolling, should match with the one defined in your Active Directory.
SCEP ServerIP/hostname	This is the IP or hostname of the Windows Server in your network running the NDES service. Since Internet Information Services (IIS) supports both HTTP and HTTPS, also include which of the two you want to use. If not provided it will be default set to HTTP. E.g.: http://myserver or https://10.192.5.1 or server.mycompany.com (will use http)
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.
Domain	The company domain for which you are enrolling should match 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. When using EAP-TLS make sure that the necessary mapping exists between the Client Certificate issued by your CA and this user account.
Corporate SSID	The SSID of your corporate wireless infrastructure to which the ClickShare Buttons will connect.

Using manually upload of certificates

Select the radio button next to *Provide certificates manually* and click **Next**.

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

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

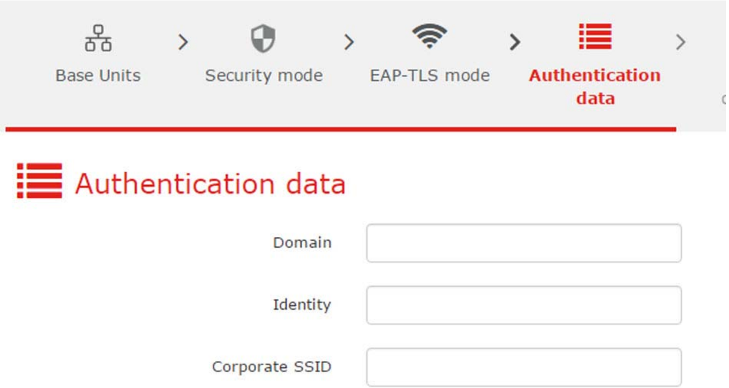


Image 5-9
Manually upload

Necessary Data to continue:

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. When using EAP-TLS make sure that the necessary mapping exists between the Client Certificate issued by your CA and this user account.

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

Click **Next** to continue with the upload of the client certificate.

Click **Upload Client Certificate**.

The client certificate you provide should be signed by the authoritative root CA in your domain and should be linked to the user you specify in the Identity field. Also, make sure that the client certificate you provide contains the private key – this is necessary to set up the TLS connection successfully.

ClickShare supports 2 formats for uploading a client certificate:

- *PKCS#12 (.pfx)* - An archive file format for storing multiple cryptography objects.
- *Privacy Enhanced Mail (.pem)* – A Base64 encoded DER certificate stored between 2 tags: `"-----BEGIN CERTIFICATE-----"` and `"-----END CERTIFICATE-----"`.

When the provided PKCS#12 file also contains the necessary CA certificate the Base Unit will extract it and verify the chain of trust to avoid that you have to separately provide the CA certificate.

CA certificate

The CA certificate is the certificate of the authoritative root CA in your domain and will be used in setting up the EAP-TLS connection. During the wizard the Base Unit will ensure that it can validate the chain of trust between the Client and CA certificates you provide.

ClickShare supports the common .crt file extension which can contain a Base64 encoded DER certificate.

When having problems connecting the Button to your corporate network, to get feedback from the Button please have a look at the ClickShare Client log. This log can be pressing the holding Shift key when starting the Client executable. Look for the lines *"EDSUSBDongleConnection::mpParseDongleMessages"*. An error code and a short summary of the issue should be logged.

5.3.3 Network integration, EAP-TTLS security mode

About EAP-TTLS

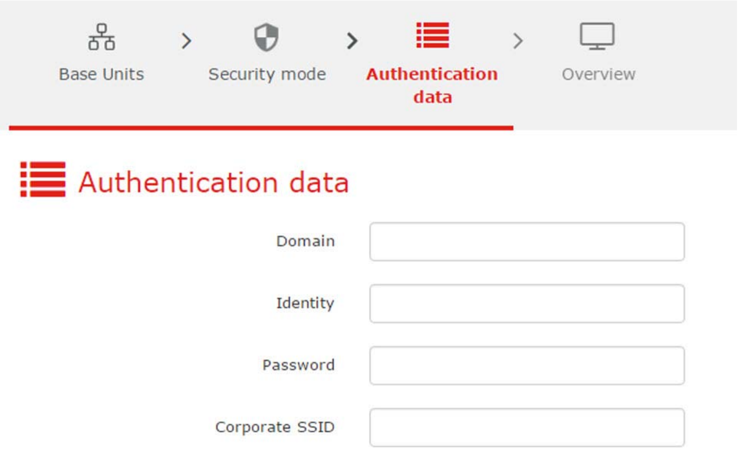
EAP-TTLS (Tunneled Transport Layer Security) is an EAP implementation by Juniper networks. It is designed to provide authentication that is as strong as EAP-TLS, but it does not require each user to be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication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

Start up of the EAP-TTLS

1. Select the radio button next to *EAP-TTLS* and click **Next**.

   The EAP-TTLS mode window opens.



Domain
Identity
Password
Corporate SSID

Image 5-10
EAP-TTLS

   Necessary Data to continue:

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.
Password	The corresponding password for the identity that you are using to authenticate on the corporate network. Per Base Unit each Button will use the same identity and password to connect to the corporate network.
Corporate SSID	The SSID of your corporate wireless infrastructure to which the ClickShare Buttons will connect.

2. Click **Next** to continue.

   The Overview window is displayed.

3. Click **Finish**.

   When having problems connecting the Button to your corporate network, to get feedback from the Button please have a look at the ClickShare Client log. This log can be enabled by holding shift when starting the Client executable. Look for the lines *“EDSUSBDongleConnection::mpParseDongleMessages”*. An error code and a short summary of the issue should be logged.

5.3.4 Network integration, PEAP security mode

About PEAP

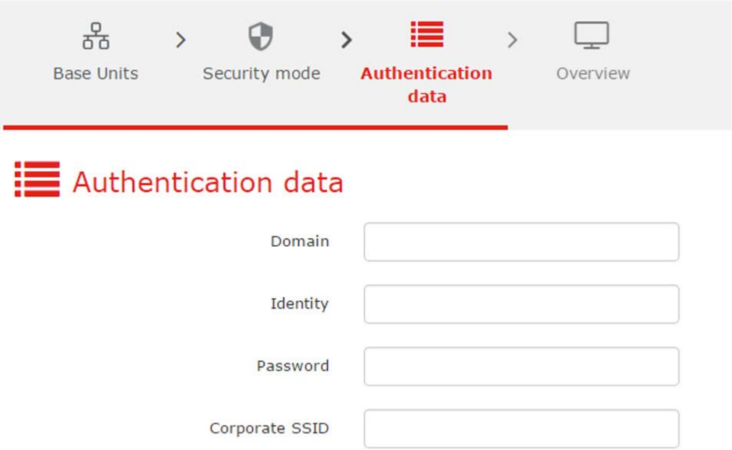
PEAP (Protected Extensible Authentication Protocol) is an EAP implementation co-developed by Cisco Systems, Microsoft and RSA Security. It sets up a secure TLS tunnel using the servers CA certificate after which actual user authentication takes place within the tunnel. This way of working enables it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

The standard does not mandate which method is to be used to authenticate within the tunnel. But in this application note, with regard to PEAP, we are referring to PEAPv0 with EAP-MSCHAPv2 as the inner authentication method. This is one of the two certified PEAP implementations in the WPA and WPA2 standards – and by far the most common and widespread implementation of PEAP.

Start up for PEAP

1. Select the radio button next to *PEAP* and click **Next**.

The PEAP window opens.



Authentication data

Domain

Identity

Password

Corporate SSID

Image 5-11
PEAP, authentication data

Necessary Data to continue:

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.

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

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

2. Click **Next** to continue.

   The *Overview* window is displayed.

3. Click **Finish**.

   When having problems connecting the Button to your corporate network, to get feedback from the Button please have a look at the ClickShare Client log. This log can be enabled by holding shift when starting the Client executable. Look for the lines *“EDSUSBDongleConnection::mpParseDongleMessages”*. An error code and a short summary of the issue should be logged.

5.3.5 Network integration, WPA2-PSK security mode

About WPA2-PSK

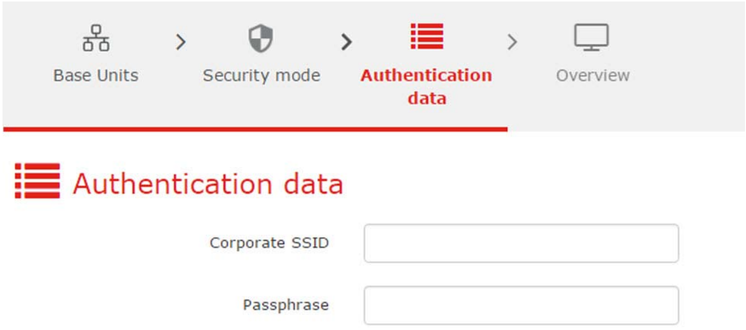
WPA2-PSK does not distinguish between individual users, there is 1 password (PSK – Pre-Shared Key) for all clients connecting to the wireless infrastructure. This makes setup very straightforward. Once connected, all data transmitted between client and AP (access point) is encrypted using a 256 bit key.

Start up for WPA2-PSK

1. Select the radio button next to *WPA2-PSK* and click **Next**.

   The WPA2-PSK mode window opens.

   Necessary Data to continue:



Authentication data

Corporate SSID	
Passphrase	

Image 5-12
WPA2–PSK, authentication data

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

Passphrase (Pre-shared key) — 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.

2. Click **Next** to continue.

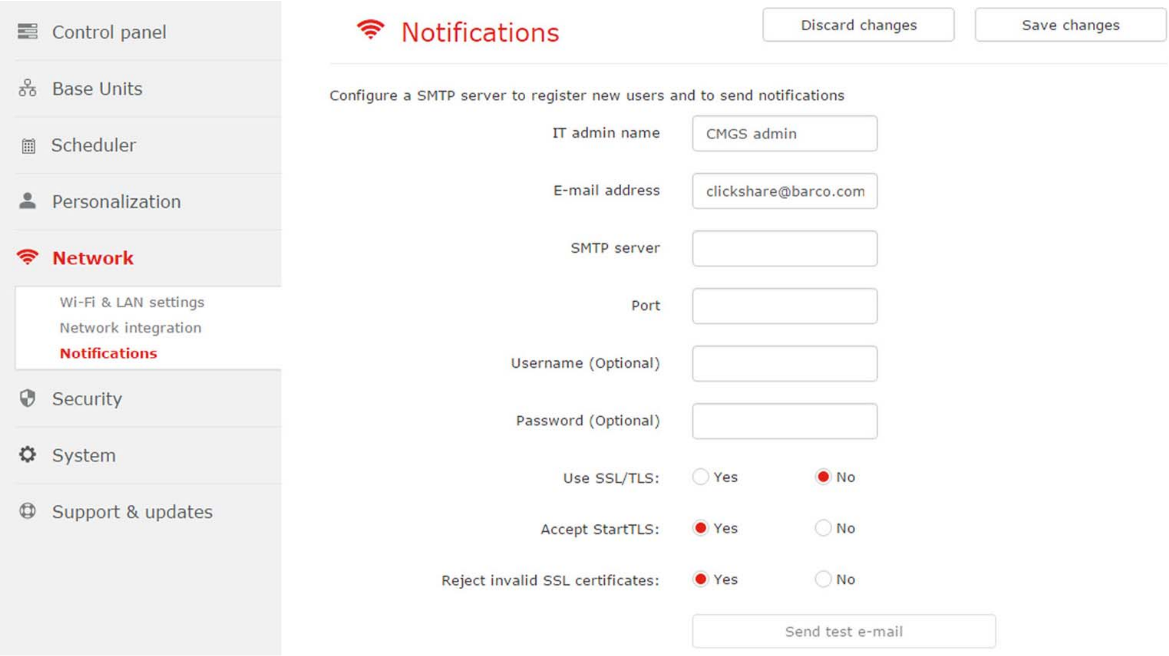
   The *Overview* window is displayed.

3. Click **Finish**.

   When having problems connecting the Button to your corporate network, to get feedback from the Button please have a look at the ClickShare Client log. This log can be enabled by holding shift when starting the Client executable. Look for the lines *“EDSUSBDongleConnection::mpParseDongleMessages”*. An error code and a short summary of the issue should be logged.

5.4 Notifications

IT admin



Notifications

Configure a SMTP server to register new users and to send notifications

IT admin name	CMGS admin	
E-mail address	clickshare@barco.com	
SMTP server		
Port		
Username (Optional)		
Password (Optional)		
Use SSL/TLS:	○ Yes	● No
Accept StartTLS:	● Yes	○ No
Reject invalid SSL certificates:	● Yes	○ No

Image 5-13
Notifications

IT admin name: name used to send out notifications.

E-mail address: address used to send out notifications

SMTP parameters

SMTP server — Host name of the outgoing mail server.

Port — Used port of the outgoing mail server.

User name (optional)	Name used to access the mail server.
Password (optional)	Password to access the mail server.
Use SSL/TLS	Use of secured sockets layer/transport layer security. Check the radio button of your choice.
Accept StartTLS	*"Yes"* will upgrade the existing unsecured connection to a secure connection using SSL/TLS.
Reject invalid SSL certificates	*"Yes"* will reject all invalid certificates.

Click on the button **Send test e-mail** to check the SMTP settings.

Click **Save changes** to activate the notification settings.

6. SECURITY

Overview

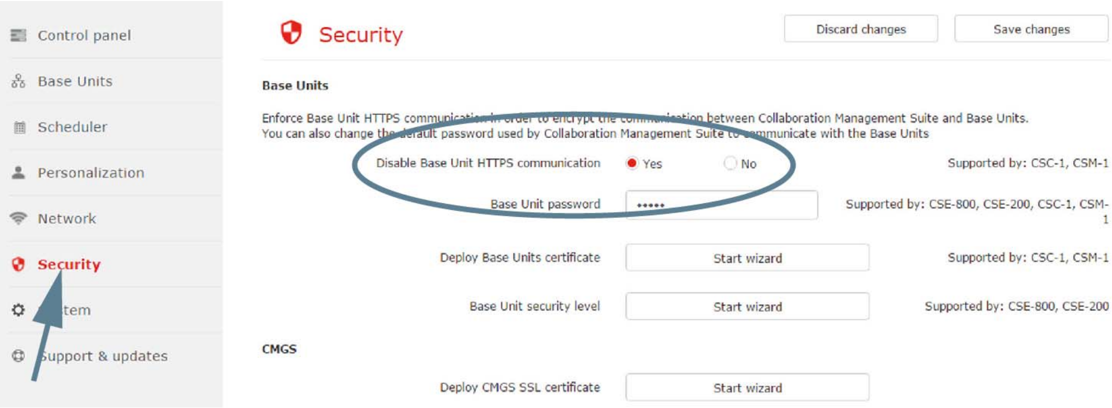
- Security, Base Unit HTTPS communication
- Security, Base Unit password
- Security, deploy Base Unit certificate
- Security, Base Unit security level
- Security, deploy CMGS SSL certificate

6.1 Security, Base Unit HTTPS communication

Only for CSC-1 and CSM-1 devices.

HTTPS communication

1. In the menu pane, click on **Security**.



Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

Disable Base Unit HTTPS communication ● Yes ○ No Supported by: CSC-1, CSM-1

Base Unit password ••••• Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Deploy Base Units certificate Supported by: CSC-1, CSM-1

Base Unit security level Supported by: CSE-800, CSE-200

CMGS

Deploy CMGS SSL certificate

Image 6-1
Security, HTTPS communication

2. To setup the HTTPS communication, check the radio button of your choice.

   Yes : Base Unit HTTPS communication is disabled.

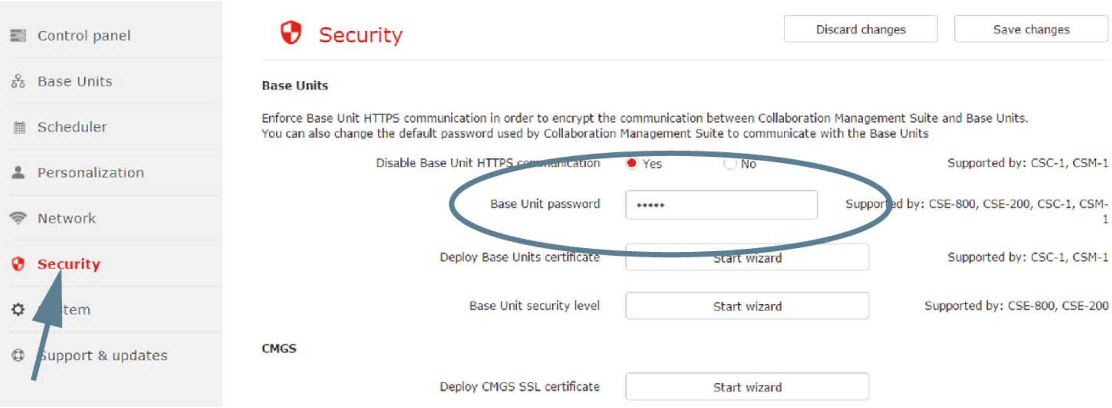
   No : HTTPS communication is used.

6.2 Security, Base Unit password

Supports in CSE-800, CSE-200, CSC-1 and CSM-1

Set password

1. In the menu pane, click on **Security**.



Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

Disable Base Unit HTTPS communication ● Yes ○ No — Supported by: CSC-1, CSM-1

Base Unit password ••••• — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Deploy Base Units certificate [Start wizard] — Supported by: CSC-1, CSM-1

Base Unit security level [Start wizard] — Supported by: CSE-800, CSE-200

CMGS

Deploy CMGS SSL certificate [Start wizard]

Image 6-2
Security, Base Unit password

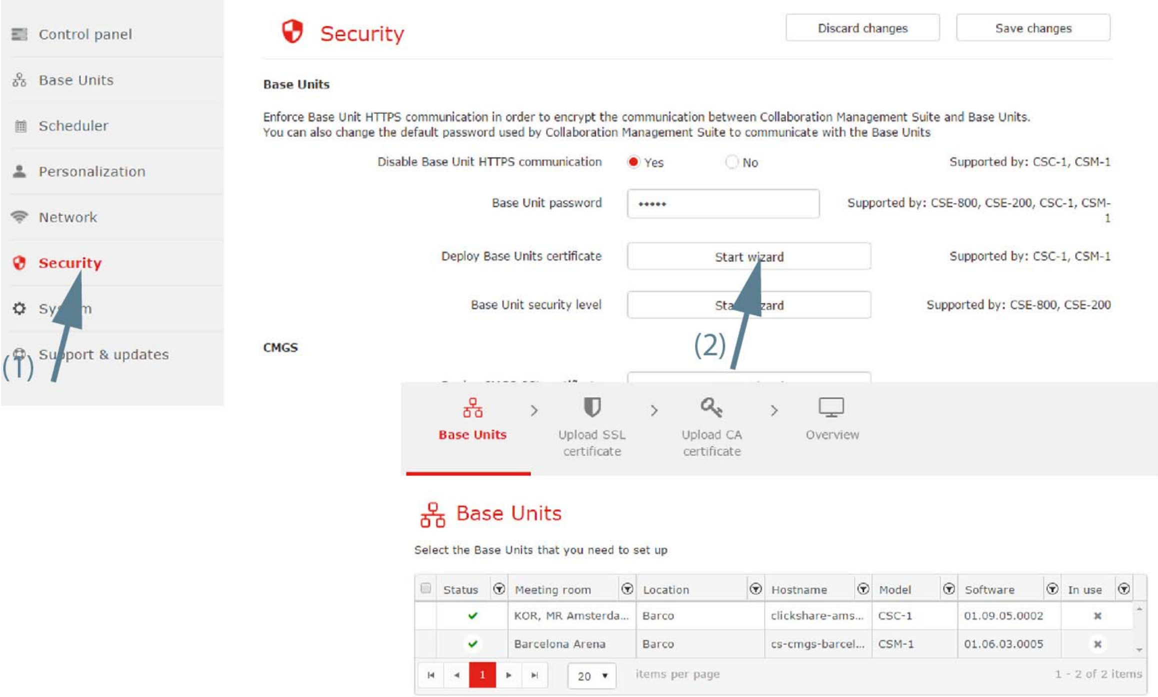
2. Enter the password used to access the Configurator of the Base Unit.

6.3 Security, deploy Base Unit certificate

Only for CSC-1 and CSM-1

How to deploy

1. In the menu pane, click on **Security** (1).
2. Click **Start wizard** next to *Deploy Base Unit certificate* (2).



Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

Disable Base Unit HTTPS communication ● Yes ○ No — Supported by: CSC-1, CSM-1

Base Unit password ••••• — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Deploy Base Units certificate [Start wizard] — Supported by: CSC-1, CSM-1

Base Unit security level [Start wizard] — Supported by: CSE-800, CSE-200

CMGS

Base Units

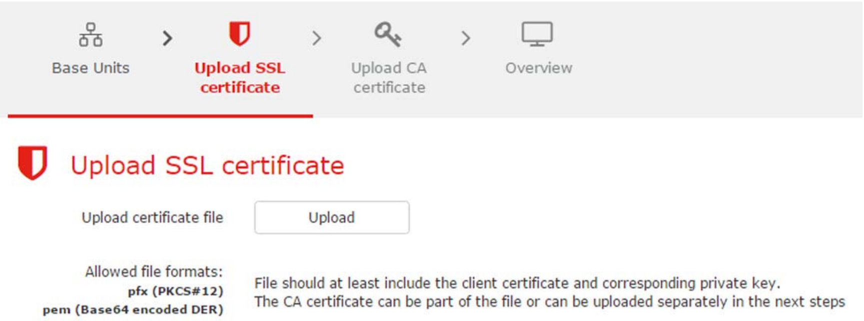
Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	✓	KOR, MR Amsterda...	Barco	clickshare-ams...	CSC-1	01.09.05.0002	✖
	✓	Barcelona Arena	Barco	cs-cmgs-barcel...	CSM-1	01.06.03.0005	✖

1 — 20 items per page — 1 - 2 of 2 items

Image 6-3
Security, Base Unit certificate

3. Select the Base Unit that you need to set up and click **Next**.
4. Upload SSL Certificate. Click on upload and browse to the location of certificate file. Click **Next** to continue.



File should at least include the client certificate and corresponding private key.
The CA certificate can be part of the file or can be uploaded separately in the next steps

Image 6-4
Upload SSL certificate

5. Upload CA certificate. Enter password.

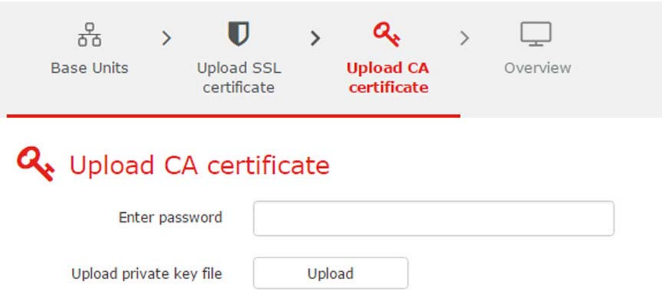


Image 6-5
Upload CA certificate

6. Upload private key file. Click on upload and select the private key file. Click **Next** to continue.

   An *Overview* window is displayed.

7. Click **Finish**.

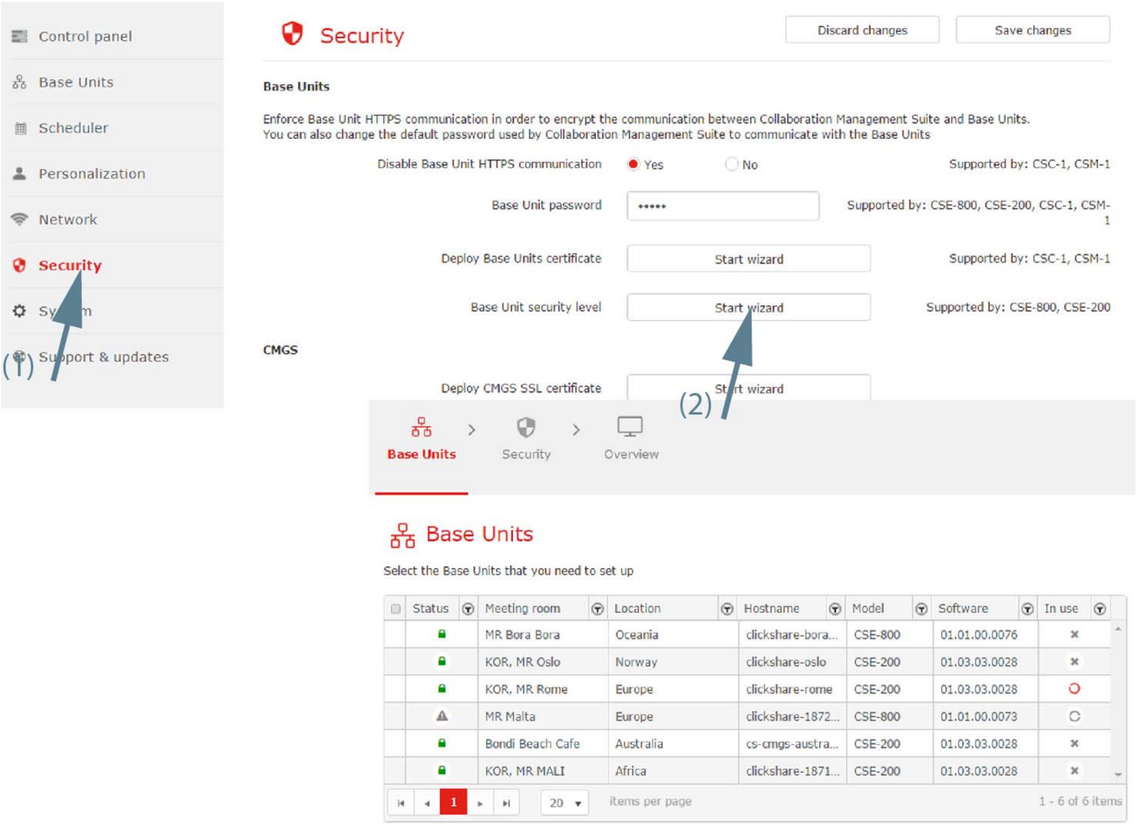
6.4 Security, Base Unit security level

Only for CSE-800 and CSE-200

Changing the security level will require Button re-pairing.

How to set

1. In the menu pane, click on **Security** (1).



Control panel
Base Units
Scheduler
Personalization
Network
Security
System
Support & updates

Security

Discard changes | Save changes

Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

Disable Base Unit HTTPS communication ● Yes ○ No — Supported by: CSC-1, CSM-1

Base Unit password ••••• — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Deploy Base Units certificate [Start wizard] — Supported by: CSC-1, CSM-1

Base Unit security level [Start wizard] — Supported by: CSE-800, CSE-200

CMGS

Deploy CMGS SSL certificate [Start wizard]

Base Units > Security > Overview

Base Units

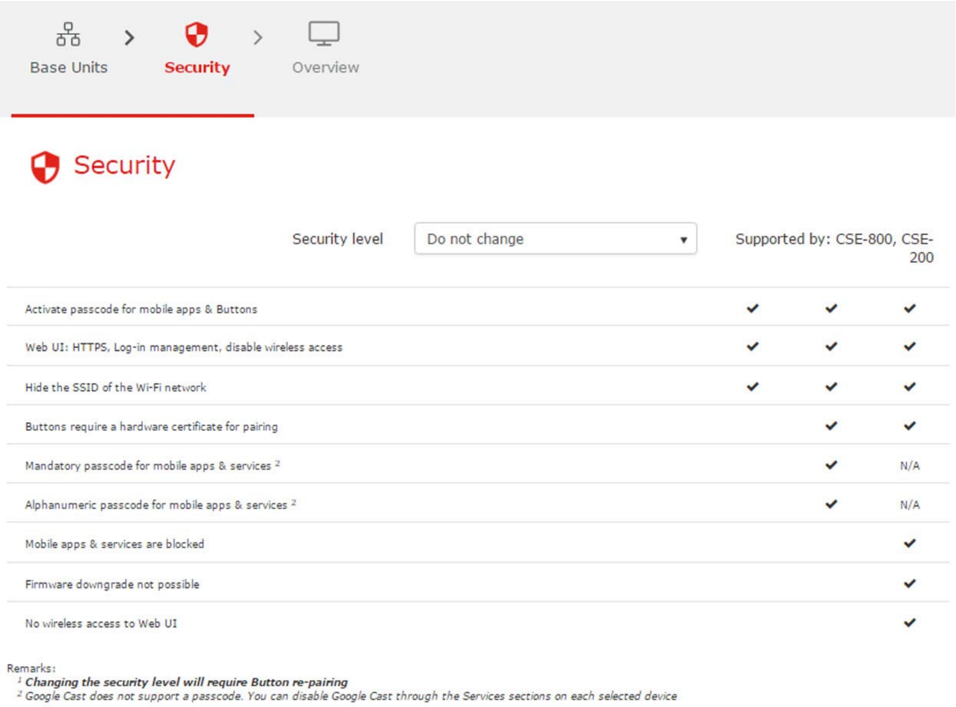
Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Oceania	clickshare-bora...	CSE-800	01.01.00.0076	×
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	01.03.03.0028	×
	🔒	KOR, MR Rome	Europe	clickshare-rome	CSE-200	01.03.03.0028	○
	⚠	MR Malta	Europe	clickshare-1872...	CSE-800	01.01.00.0073	○
	🔒	Bondi Beach Cafe	Australia	cs-cmgs-austra...	CSE-200	01.03.03.0028	×
	🔒	KOR, MR MALI	Africa	clickshare-1871...	CSE-200	01.03.03.0028	×

1 — 20 items per page — 1 - 6 of 6 items

Image 6-6
Base Unit security level, start

2. Click **Start wizard** next to *Base Unit security level* (2).
3. Select the Base unit(s) that need to set up. Click **Next** to continue.
4. Click on the drop down box next to *Security level* and select the desired level for the selected Base Unit(s).



Base Units > Security > Overview

Security

Security level [Do not change ▾] — Supported by: CSE-800, CSE-200

Activate passcode for mobile apps & Buttons	✓	✓	✓
Web UI: HTTPS, Log-in management, disable wireless access	✓	✓	✓
Hide the SSID of the Wi-Fi network	✓	✓	✓
Buttons require a hardware certificate for pairing		✓	✓
Mandatory passcode for mobile apps & services [2]		✓	N/A
Alphanumeric passcode for mobile apps & services [2]		✓	N/A
Mobile apps & services are blocked			✓
Firmware downgrade not possible			✓
No wireless access to Web UI			✓

Remarks:
[1] ***Changing the security level will require Button re-pairing***
[2] *Google Cast does not support a passcode. You can disable Google Cast through the Services sections on each selected device*

Image 6-7
Base Unit security

5. Click **Next** to continue.

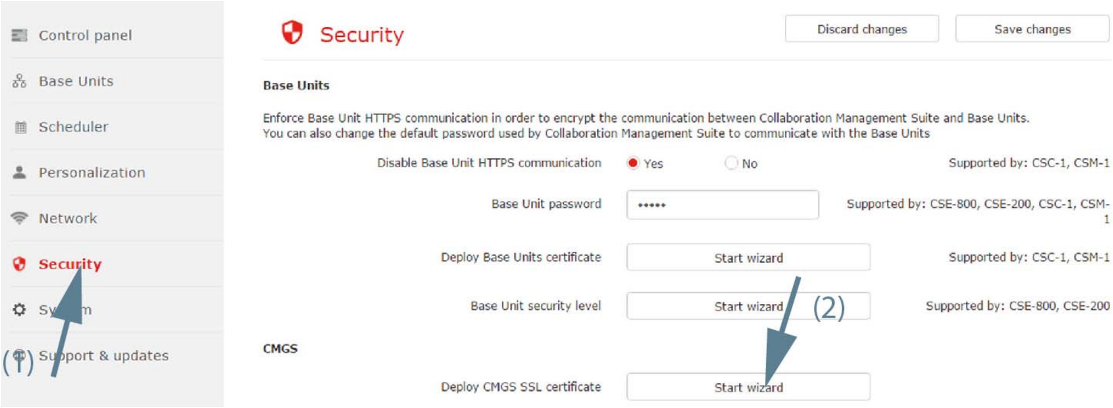
   An *Overview* window is displayed.

6. Click **Finish**.

6.5 Security, deploy CMGS SSL certificate

How to deploy

1. In the menu pane, click on **Security** (1).
2. Click **Start wizard** next to *Deploy CMGS SSL certificate* (2).



Security

Base Units

Enforce Base Unit HTTPS communication in order to encrypt the communication between Collaboration Management Suite and Base Units.
You can also change the default password used by Collaboration Management Suite to communicate with the Base Units

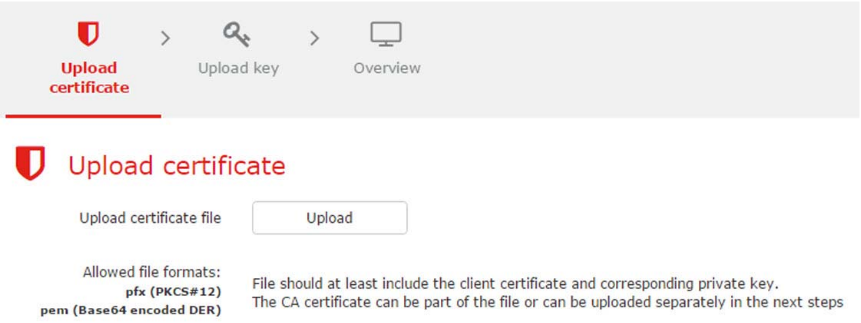
Disable Base Unit HTTPS communication	● Yes ○ No	Supported by: CSC-1, CSM-1
Base Unit password	•••••	Supported by: CSE-800, CSE-200, CSC-1, CSM-1
Deploy Base Units certificate	Start wizard	Supported by: CSC-1, CSM-1
Base Unit security level	Start wizard	Supported by: CSE-800, CSE-200

CMGS

Deploy CMGS SSL certificate	Start wizard

Image 6-8
CMGS SSL certificate

3. Upload certificate. Click on **Upload** and browse to the location of certificate file. Click **Next** to continue.



Upload certificate

Upload certificate file: Upload

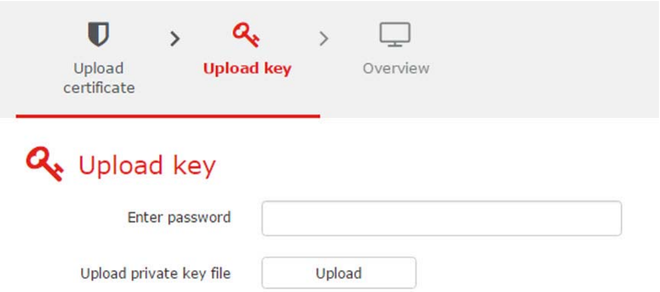
Allowed file formats:
pfx (PKCS#12)
pem (Base64 encoded DER)

File should at least include the client certificate and corresponding private key.
The CA certificate can be part of the file or can be uploaded separately in the next steps

Image 6-9
Upload certificate

The format of the certificate file must be a pdx or pem file

4. Enter the password and click on **Upload** to upload the private key file. Click **Next** to continue.



Upload key

Enter password

Upload private key file: Upload

Image 6-10
Upload key

An *Overview* window is displayed.

5. Click **Finish**.

7. SYSTEM

Only for IT admin user.

Overview

- Date & Time
- Buttons
- Users

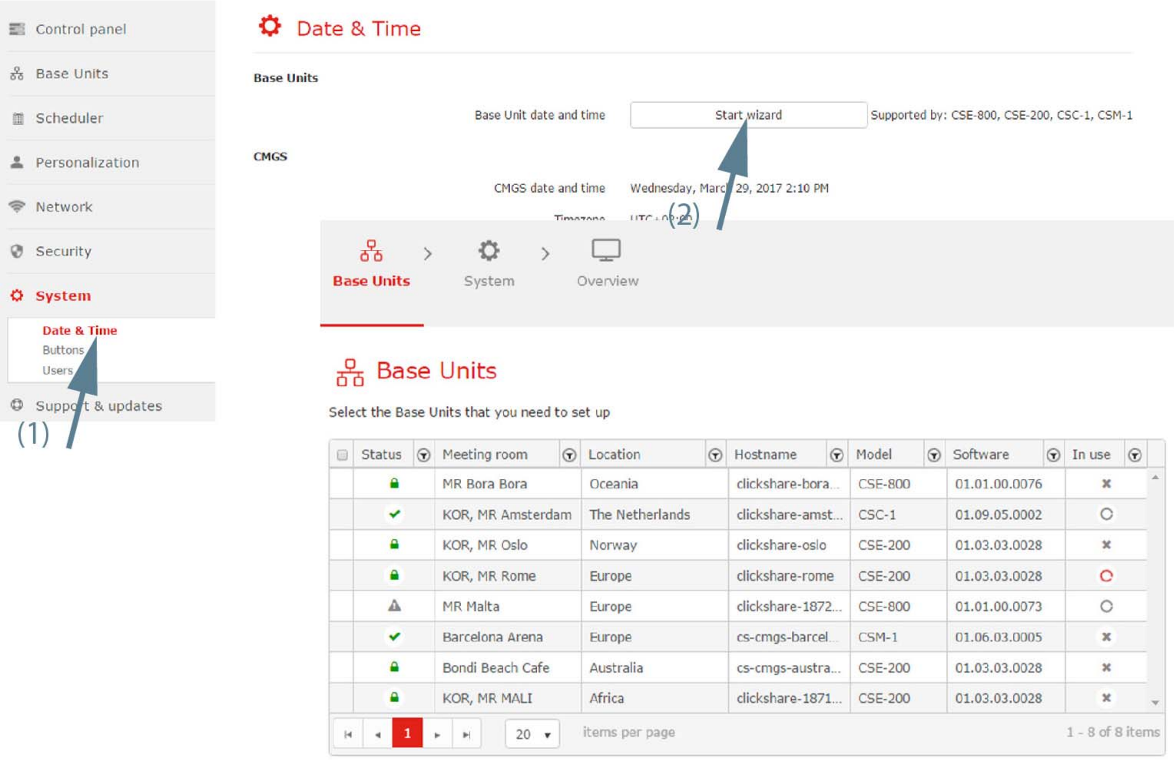
7.1 Date & Time

About date & time

The date & time of one of or multiple Base Units can be set.

How to set

1. In the menu pane, click on System and select **Date & Time** (1).



Date & Time

Base Units

Base Unit date and time [Start wizard] Supported by: CSE-800, CSE-200, CSC-1, CSM-1

CMGS

CMGS date and time Wednesday, March 29, 2017 2:10 PM

Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Oceania	clickshare-bora...	CSE-800	01.01.00.0076	✖
	✓	KOR, MR Amsterdam	The Netherlands	clickshare-amst...	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	01.03.03.0028	✖
	🔒	KOR, MR Rome	Europe	clickshare-rome	CSE-200	01.03.03.0028	○
	⚠	MR Malta	Europe	clickshare-1872...	CSE-800	01.01.00.0073	○
	✓	Barcelona Arena	Europe	cs-cmgs-barcel...	CSM-1	01.06.03.0005	✖
	🔒	Bondi Beach Cafe	Australia	cs-cmgs-austra...	CSE-200	01.03.03.0028	✖
	🔒	KOR, MR MALI	Africa	clickshare-1871...	CSE-200	01.03.03.0028	✖

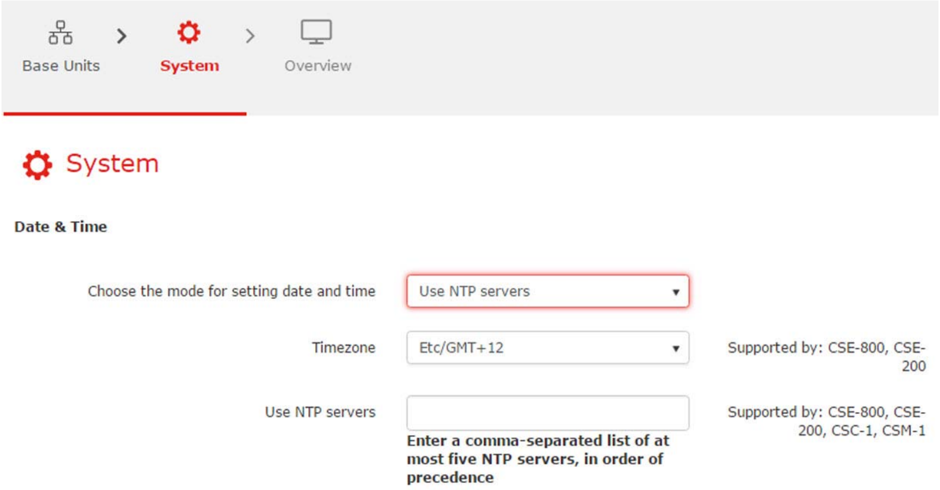
1 | 20 items per page | 1 - 8 of 8 items

Image 7-1
Date & time, start

2. Click **Start wizard** next to *Base Unit date and time* (2).
3. Select the Base Unit(s) that you need to set up. Click **Next** to continue.
4. Choose the mode for setting date and time.
   The following modes are available:
   - Use NTP servers
   - Set date and time manually

Use NTP server

1. Click on the drop down box next to *Choose the mode for setting date and time* and select *Use NTP servers*.



System

Date & Time

Choose the mode for setting date and time: Use NTP servers

Timezone: Etc/GMT+12 — Supported by: CSE-800, CSE-200

Use NTP servers: — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Enter a comma-separated list of at most five NTP servers, in order of precedence

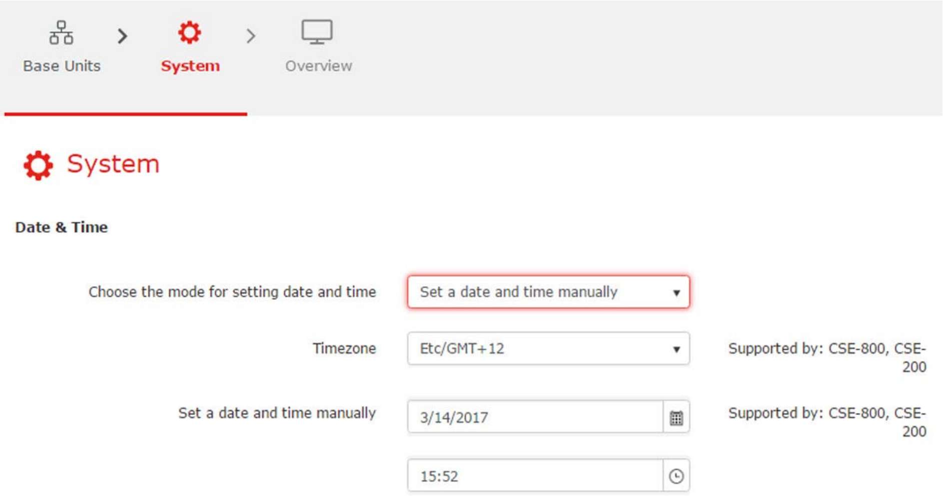
Image 7-2
NTP server

2. Click on the drop down box next to *Timezone* and select the corresponding time zone.
   Note: *This is only for CSE-800 and CSE-200.*

3. Enter the hostname or IP address of the NTP server.
   Up to maximum 5 server can be added, separated by a comma.

Set date and time manually

1. Click on the drop down box next to *Choose the mode for setting date and time* and select *Set date and time manually*.



System

Date & Time

Choose the mode for setting date and time: Set a date and time manually

Timezone: Etc/GMT+12 — Supported by: CSE-800, CSE-200

Set a date and time manually: 3/14/2017 — Supported by: CSE-800, CSE-200

15:52

Image 7-3
Manually setup

2. Click on the drop down box next to Timezone and select the corresponding time zone.

3. Select the date (it may be year, month and day)

4. Click in the time field, select the current value and enter a new value with you keyboard. Use the following format *hh:mm*.
   Or,
   click on the icon next to the input field and select a time from the drop down list.

5. Click **Next** to continue.

   An *Overview* window is displayed.

6. Click **Finish**.

7.2 Buttons

About Buttons

After selecting Buttons, on overview of the Base Units with its paired buttons is given together with the status, connected or not.

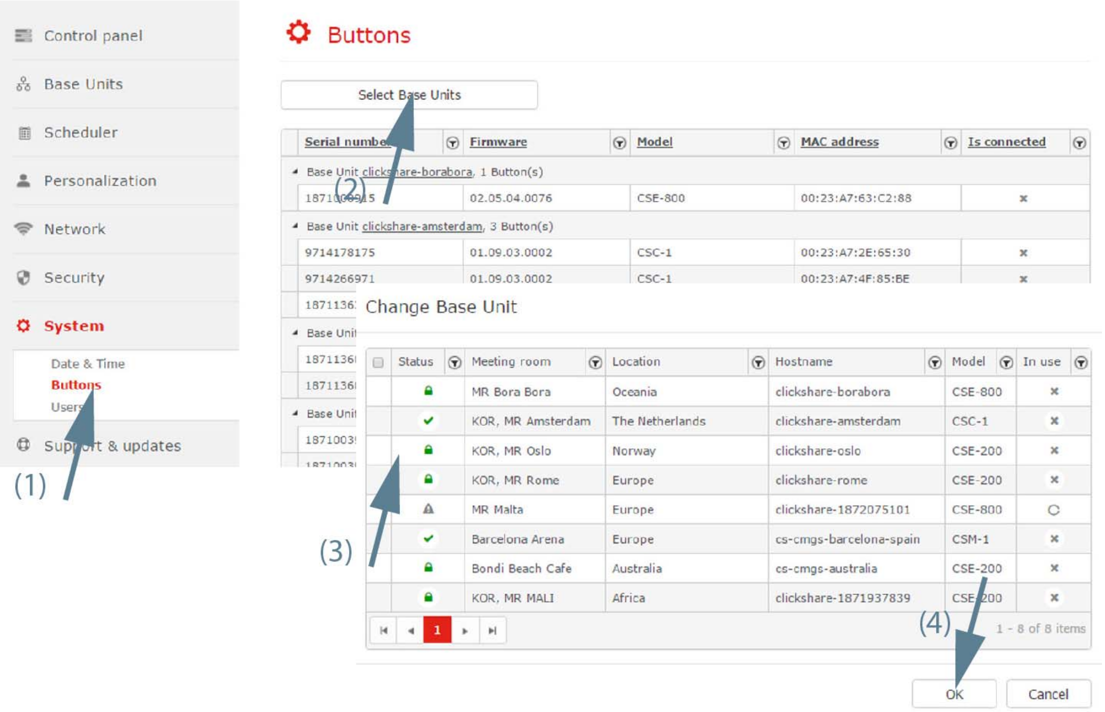
That overview contains the following information of a Button:

- Serial number
- Firmware version
- MAC address
- Connected status: Green check mark means connected or gray x means not connected.

The table can be sorted using the icons in the column header.

Setup a filter on Base Unit level

1. In the menu pane, click on **System** and select **Buttons** (1).



Serial number	Firmware	Model	MAC address	Is connected
Base Unit clickshare-borabora, 1 Button(s)				
1871000915	02.05.04.0076	CSE-800	00:23:A7:63:C2:88	✕
Base Unit clickshare-amsterdam, 3 Button(s)				
9714178175	01.09.03.0002	CSC-1	00:23:A7:2E:65:30	✕
9714266971	01.09.03.0002	CSC-1	00:23:A7:4F:85:BE	✕
1871136				
Base Unit				
1871136				
1871136				
Base Unit				
1871003				
1871003				

Change Base Unit

□	Status	Meeting room	Location	Hostname	Model	In use
	🔒	MR Bora Bora	Oceania	clickshare-borabora	CSE-800	✕
	✓	KOR, MR Amsterdam	The Netherlands	clickshare-amsterdam	CSC-1	✕
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	✕
	🔒	KOR, MR Rome	Europe	clickshare-rome	CSE-200	✕
	⚠	MR Malta	Europe	clickshare-1872075101	CSE-800	○
	✓	Barcelona Arena	Europe	cs-cmgs-barcelona-spain	CSM-1	✕
	🔒	Bondi Beach Cafe	Australia	cs-cmgs-australia	CSE-200	✕
	🔒	KOR, MR MALI	Africa	clickshare-1871937839	CSE-200	✕

Image 7-4
Base Unit filter

2. Click on **Select Base Units** (2).
3. Select the Base Unit(s) to display the paired buttons (3).
4. Click **OK** (4).

   An overview of the paired buttons for the selected Base Unit(s) is given.

7.3 Users

Only for IT admin user.

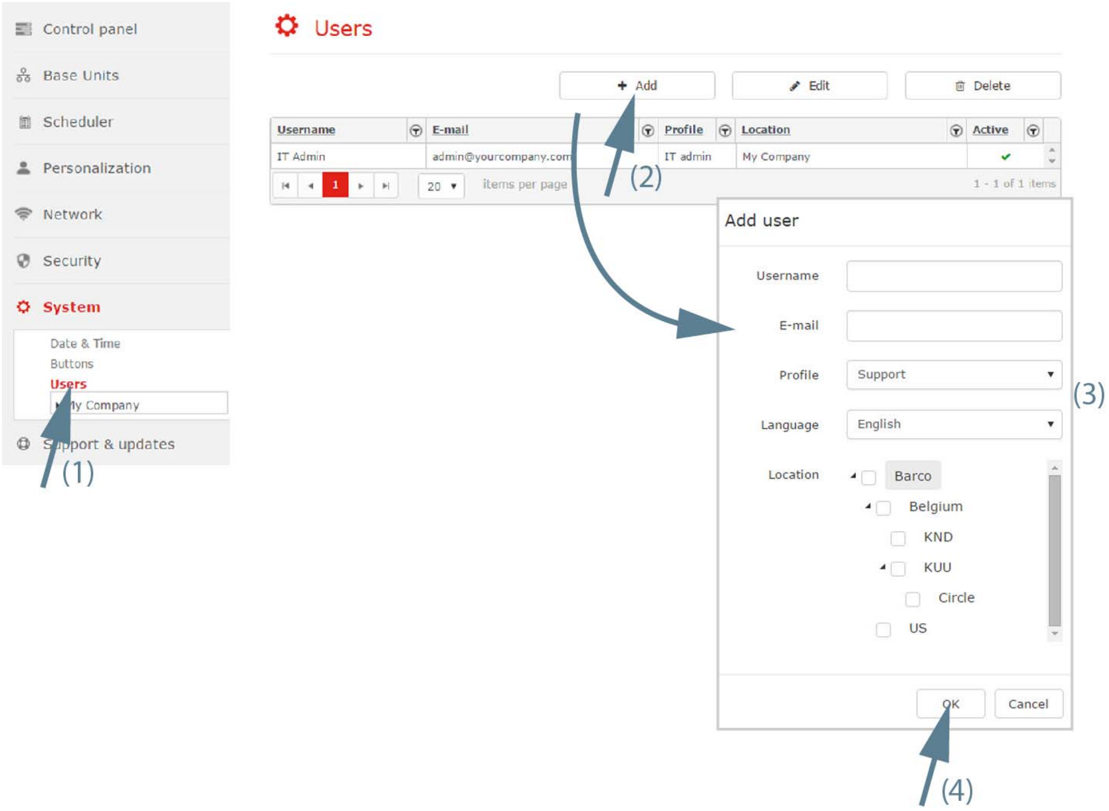
Overview

- Add new user
- Edit selected user
- Delete selected user
- Filter users
- Accept/reject a registered user

7.3.1 Add new user

How to add

1. Select System and click on **Users** to display the overview page (1).



Username	E-mail	Profile	Location	Active
IT Admin	admin@yourcompany.com	IT admin	My Company	✓

Username

E-mail

Profile: Support

Language: English

Location

Image 7-5
Add new user

2. Click on **Add** (2).

   The *Add user* window opens.

3. Fill out the user form (3).
   - enter a *User* name.
   - enter an *E-mail* address
   - select a *Profile*. This can be Support or Key User.
   - select a *Language*.
   - select a *Location* by checking the check box in front of the location. If the location has sub locations, then these sub locations are selected at the same time.

4. Click on **OK** (4).

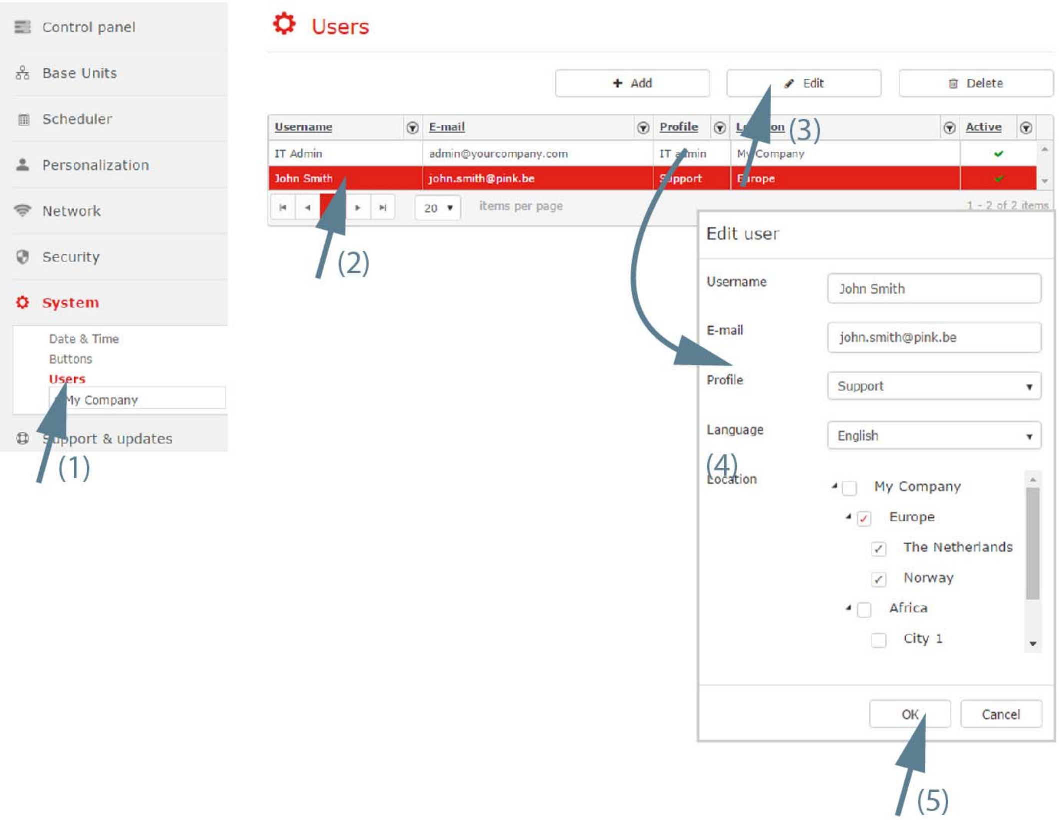
   The user is added to the list of active users.

   Users added by the IT admin using this method will receive an email with their password generated by the CMGS. If the SMTP settings are not added in the System Settings page then the users will not be able to login since they will not receive emails. See also "Accept/reject a registered user", page 62 in order to be able to populate the CMGS with users without having the SMTP server set up.

7.3.2 Edit selected user

How to edit

1. Select System and click on **Users** to display the overview page (1).



Username	E-mail	Profile	Location	Active
IT Admin	admin@yourcompany.com	IT admin	My Company	✓
John Smith	john.smith@pink.be	Support	Europe	✓

Username: John Smith

E-mail: john.smith@pink.be

Profile: Support

Language: English

Location:
- □ My Company
  - ☑ Europe
    - ☑ The Netherlands
    - ☑ Norway
  - □ Africa
    - □ City 1

Image 7-6
Edit selected user

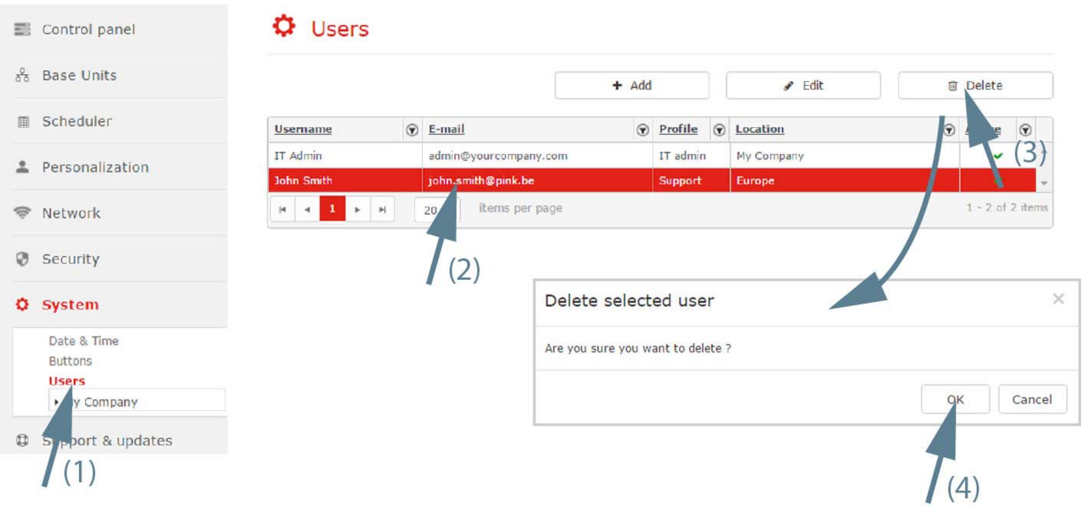
2. Select the user to edit (2).
3. Click on the **Edit** (3).

   The *Edit user* window opens.
4. Edit the user settings (4).
   - *Name*
   - *E-mail* address
   - *Profile*. This can be *Support* or *Key user*.
   - *Language*.
   - *Location*. Check the check box in front of the desired location. If the location has sub locations, then these sub locations are selected at the same time with gray selection marks. In order to explicitly assign the user to a sub-location it should be clicked to change the check-mark from gray into red. The user will have access on both the locations checked with gray or red check-marks. This could be useful only if the sub-location is planned to be moved later to another parent node and the user should still have access on it.
5. Click **OK** (5).

7.3.3 Delete selected user

How to delete

1. Select System and click on **Users** to display the overview page (1).



Username	E-mail	Profile	Location	Active
IT Admin	admin@yourcompany.com	IT admin	My Company	✓
John Smith	john.smith@pink.be	Support	Europe	

Delete selected user

Are you sure you want to delete ?

Image 7-7
Delete selected user

2. Select the user to delete (2).
3. Click **Delete** (3).

   A delete message is displayed, asking for confirmation to remove the record.
4. Click **OK** to delete the selected user (4).

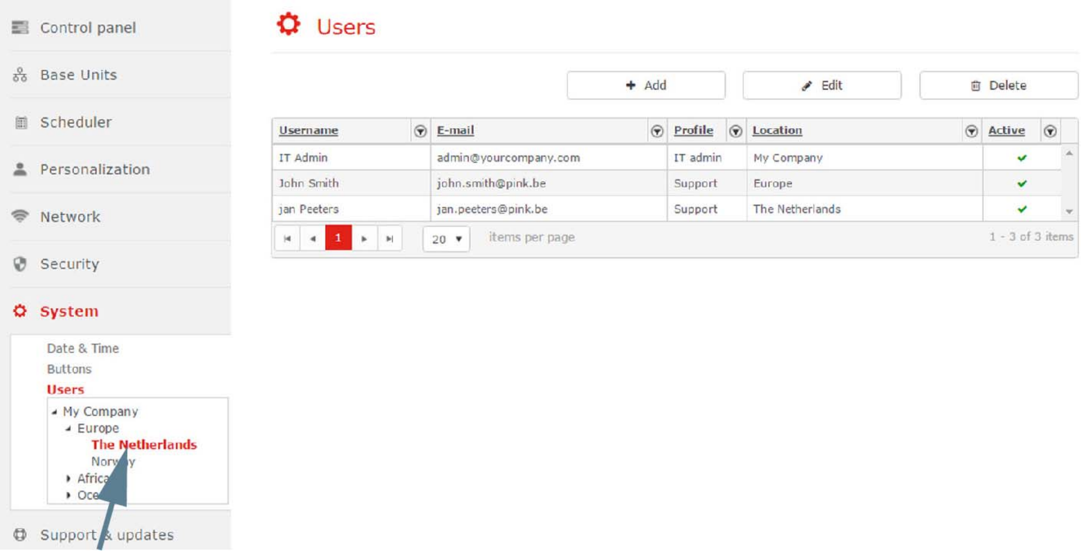
7.3.4 Filter users

About filtering users

All users of specific locations can be displayed in the list.

How to filter

1. Select **System** and click on the arrow before the main location to display a specific overview page (1).
   Click on the arrow to expand/collapse the tree and select the desired level.



Username	E-mail	Profile	Location	Active
IT Admin	admin@yourcompany.com	IT admin	My Company	✓
John Smith	john.smith@pink.be	Support	Europe	✓
jan Peeters	jan.peeters@pink.be	Support	The Netherlands	✓

Image 7-8
Location filter on users

All user of the selected level and the higher levels are displayed in the list.

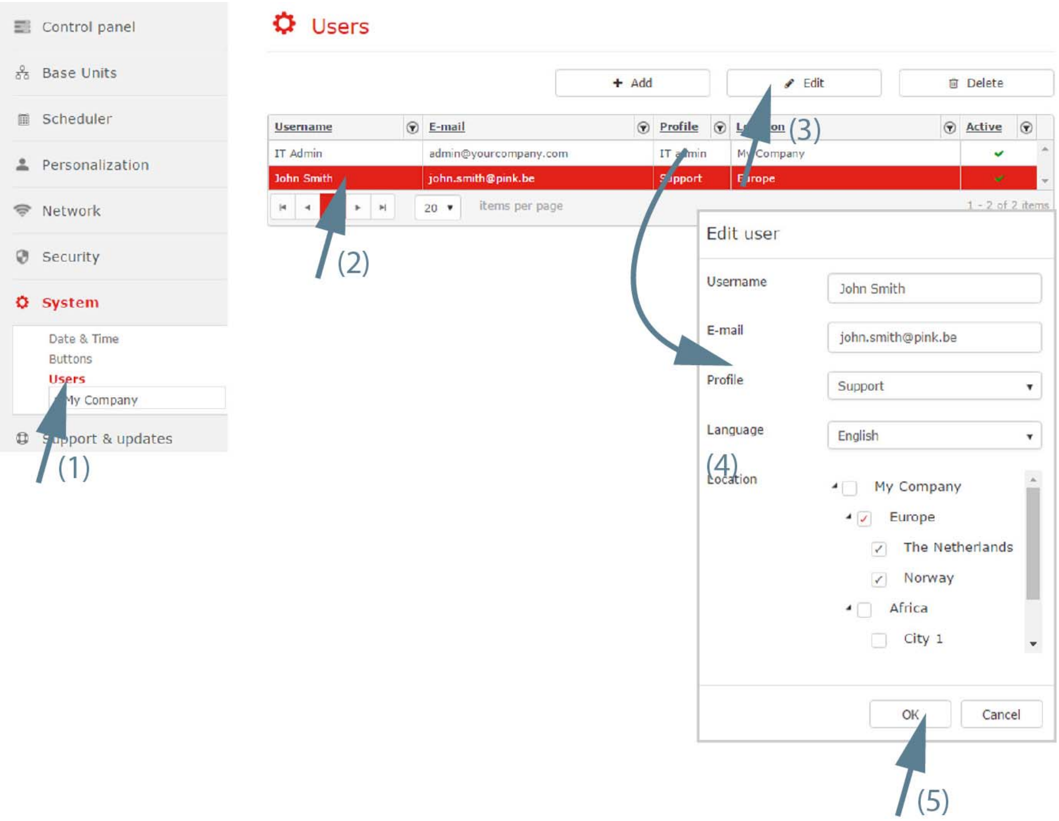
7.3.5 Accept/reject a registered user

What can be done?

If a new user has used the *Register now* page to register, this user will be displayed in the *Users* page but will not be able to login until the administrator accepts the registration. The administrator can edit the registered user, select a profile and assign a location in order to accept the registration. If the administrator simply deletes the user then the user registration will be considered as rejected. The users will define their own desired password when registering, so these users, if accepted by the IT admin, will be able to log in even if the SMTP server is not set up. However the IT admin will have to notify them that their account registration request has been accepted.

How to accept a registered user

1. Select System and click on **Users** to display the overview page (1).
2. Select the registered user (2).



Username	E-mail	Profile	Location	Active
IT Admin	admin@yourcompany.com	IT admin	My Company	✓
John Smith	john.smith@pink.be	Support	Europe	✓

Edit user

Username: John Smith

E-mail: john.smith@pink.be

Profile: Support

Language: English

Location:
- □ My Company
  - ☑ Europe
    - ☑ The Netherlands
    - ☑ Norway
  - □ Africa
    - □ City 1

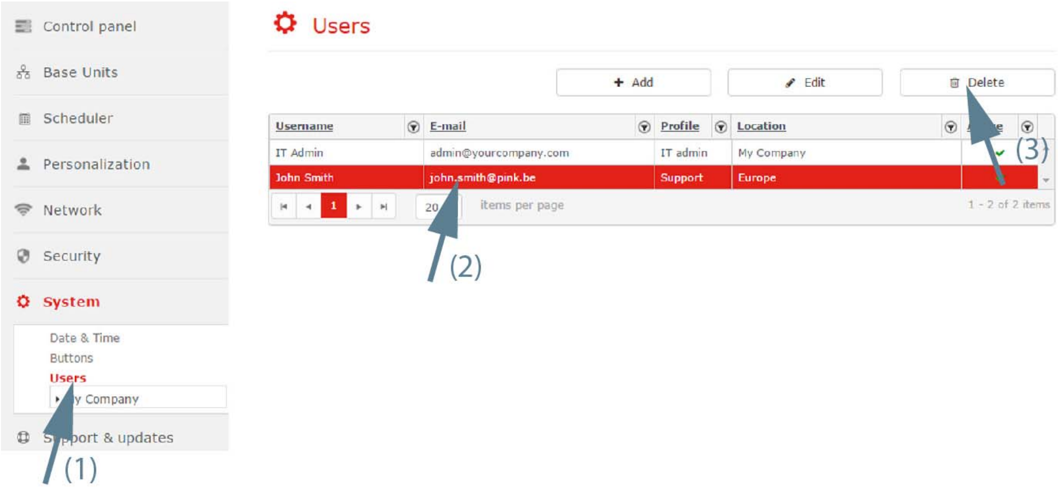
Image 7-9
Edit selected user

3. Click **Edit** to open the Edit user window (3).
4. Change the profile (4) and add a location (5). See "Edit selected user", page 60 for more info.
5. Click **OK** (5).

   The registered user is activated and can login now.

How to reject a registered user

1. Select System and click on **Users** to display the overview page (1).
2. Select the registered user (2).



Username	E-mail	Profile	Location	
IT Admin	admin@yourcompany.com	IT admin	My Company	✓
John Smith	john.smith@pink.be	Support	Europe	

Image 7-10

3. Click **Delete** (3).

   The registered user is removed.

8. SUPPORT & UPDATES

Overview

- Firmwares
- Updates
- Troubleshoot

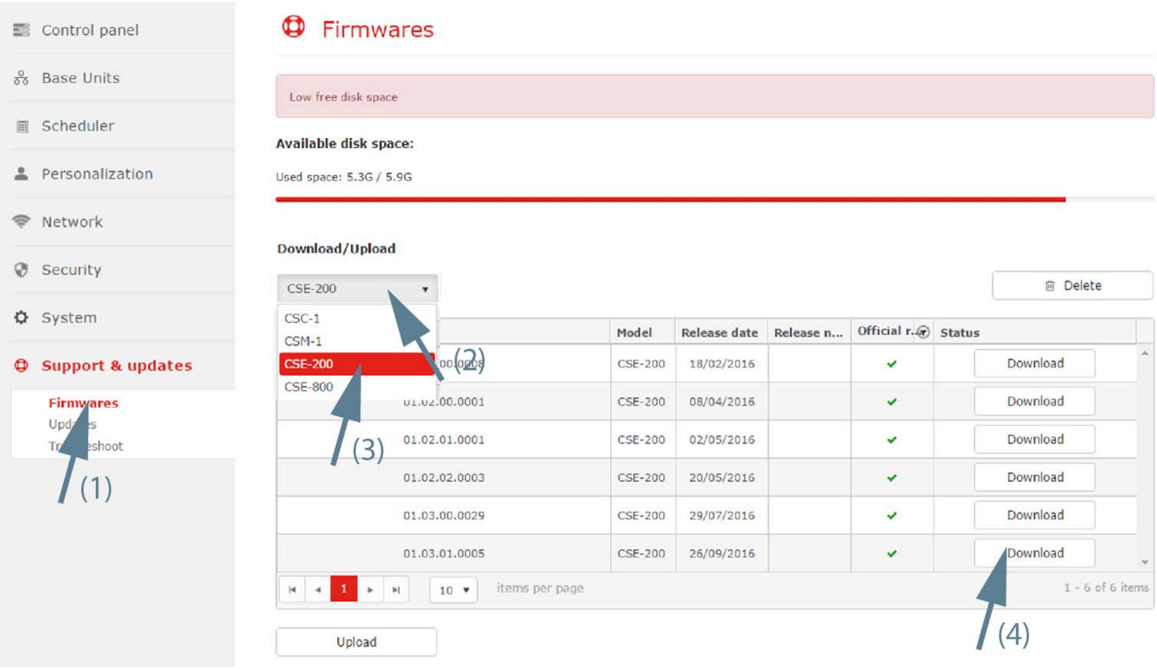
8.1 Firmwares

What should be done?

Before a firmware update can take place, the firmware must be available on the Collaboration Management Suite. First, it should be downloaded.

Download/upload

1. Select **Support & updates** and click on **Firmwares** to display the overview page (1).



Low free disk space

Available disk space:

Used space: 5.3G / 5.9G

	Model	Release date	Release n...	Official r...	Status
00.0008	CSE-200	18/02/2016		✓	Download
01.02.00.0001	CSE-200	08/04/2016		✓	Download
01.02.01.0001	CSE-200	02/05/2016		✓	Download
01.02.02.0003	CSE-200	20/05/2016		✓	Download
01.03.00.0029	CSE-200	29/07/2016		✓	Download
01.03.01.0005	CSE-200	26/09/2016		✓	Download

1 - 6 of 6 items

Image 8-1
Firmwares, download/upload

2. Click on the drop down list and select the Base Unit model.

   The current available firmwares are displayed.

3. Click on the **Download** button next to the firmware version you need.

   The download starts and a progress bar is displayed.

   When finished, the download button is replaced with the message Available.

With a low disk space on the Collaboration Management Suite server, a message is displayed on top of the Firmware page.

Upload firmware

If a firmware version is not available in the list, you may upload that firmware in the Collaboration Management Suite.

How to upload

1. While the *Firmwares* view is displayed, click on **Upload**.

   Browser window opens.

2. Browse to the desired firmware and click **Open**.

   The firmware is uploaded and becomes available in the list.

How to delete

1. While the *Firmwares* view is displayed, select the firmware to delete.
2. Click on **Delete**.

8.2 Updates

8.2.1 Base Unit firmware upgrade

About software update

The firmware of a single Base Unit or of multiple Base Units can be updated with Collaboration Management Suite. The update can be executed immediately or it can be scheduled.

The Base Unit firmware must be loaded on the Collaboration Management Suite, prior the update. Collaboration Management Suite may directly download a firmware from Barco site, or the firmware may be uploaded to Collaboration Management Suite.

An update takes more than 8 minutes for a CSC-1/CSE-200/CSE-800 and more than 10 minutes for a CSM-1, depending on the connection bandwidth, file size and Base Unit reboot duration.

Automatic firmware update[4]

1. Select **Support & updates** and click on **Updates** (a).

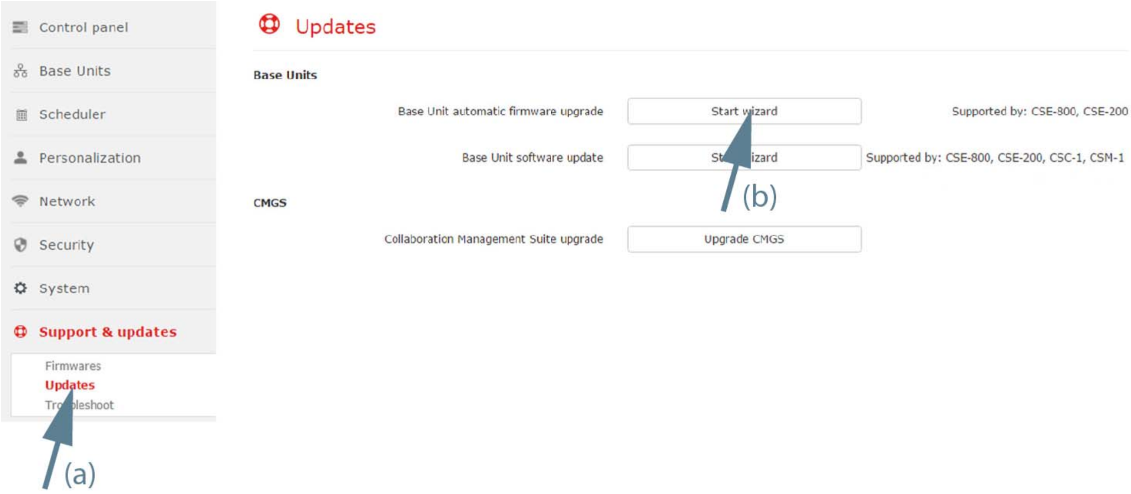
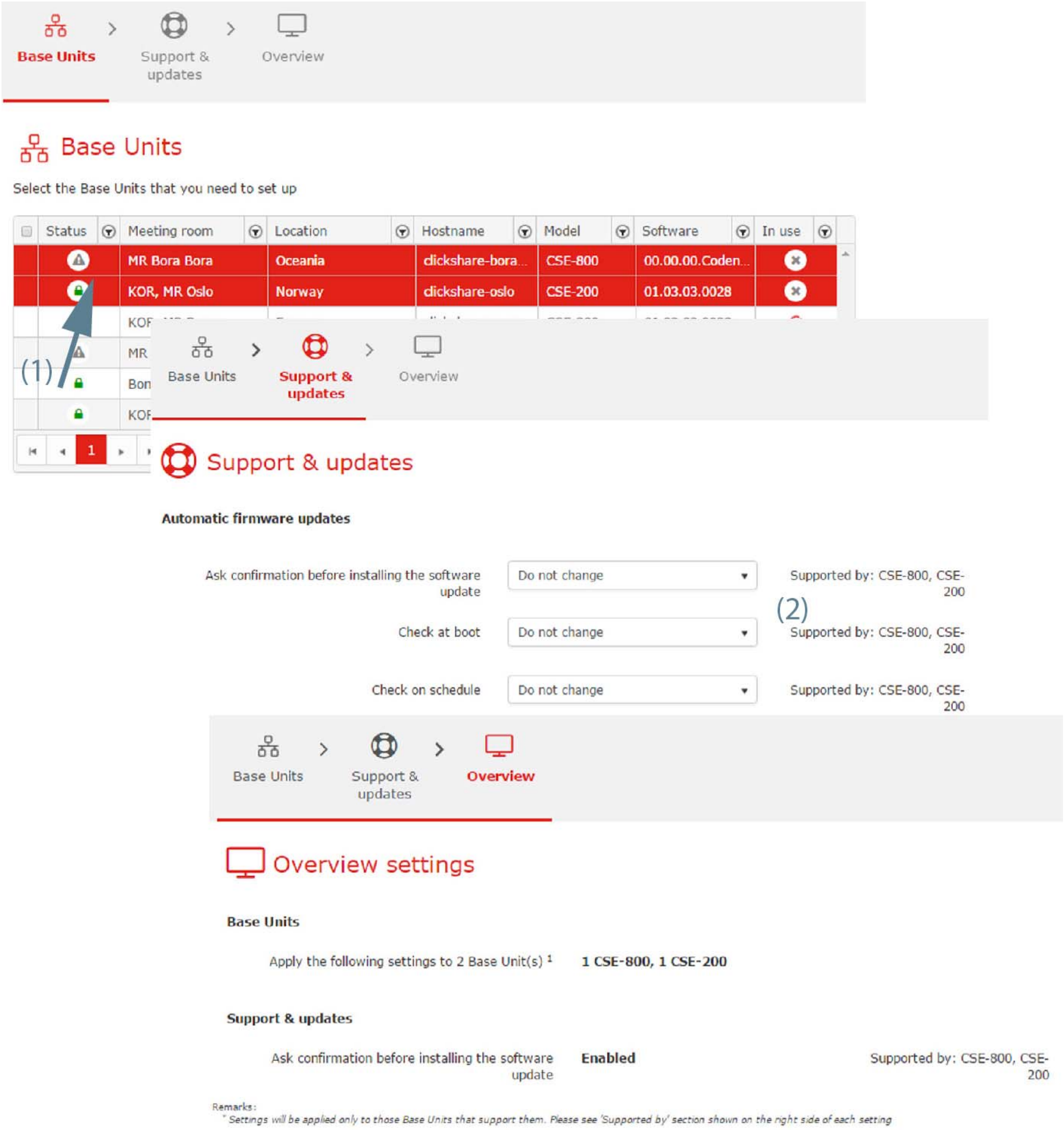


Image 8-2
Start firmware update wizard

2. Click on the **Start wizard** button next to *Base Unit automatic firmware upgrade* (b).
3. Select the Base Unit(s) to update (1).

[4] only for CSE-800 and CSE-200



Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	⚠	MR Bora Bora	Oceania	clickshare-bora...	CSE-800	00.00.00.Coden...	☒
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	01.03.03.0028	☒
		KOF					
	⚠	MR					
	🔒	Bon					
	🔒	KOF					

Support & updates

Automatic firmware updates

Ask confirmation before installing the software update	Do not change	Supported by: CSE-800, CSE-200
Check at boot	Do not change	Supported by: CSE-800, CSE-200
Check on schedule	Do not change	Supported by: CSE-800, CSE-200

Overview settings

Base Units

Apply the following settings to 2 Base Unit(s) ¹ **1 CSE-800, 1 CSE-200**

Support & updates

Ask confirmation before installing the software update **Enabled** Supported by: CSE-800, CSE-200

Remarks:
¹ Settings will be applied only to those Base Units that support them. Please see 'Supported by' section shown on the right side of each setting

Image 8-3
Automatic firmware updates

4. Check the settings and change is necessary (2). To change a setting, click on the drop down box and select the desired setting. The following can be changed:
   - Ask confirmation before installing the software update: enable or disable or do not change.
   - Check at boot: enable or disable or do not change
   - Check on schedule: enable or disable or do not change.
5. Click **Next** to continue.

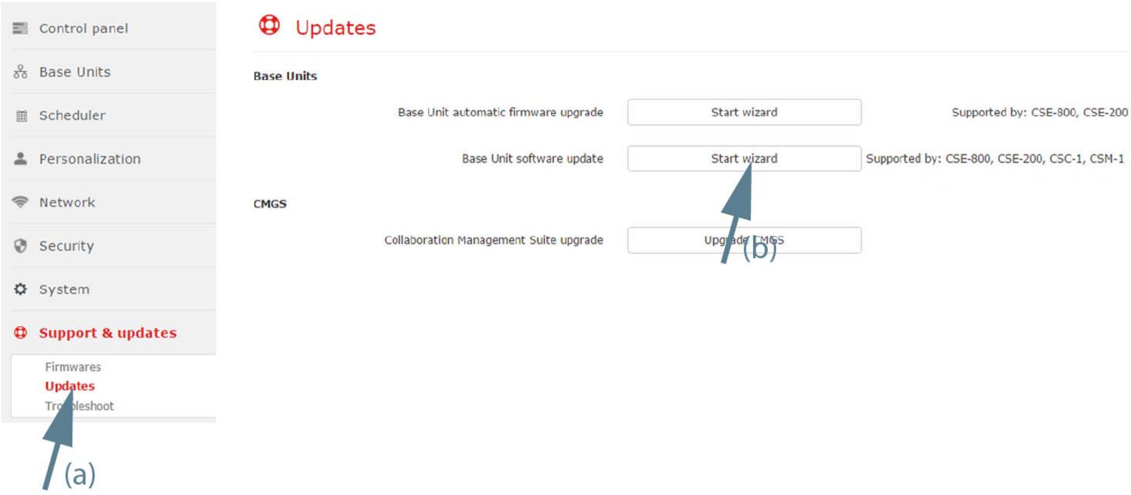
   The *Overview* page is displayed with changed settings.
6. Click **Finish**.

Software update[5]

This procedure is similar to the software update procedure in *Base Units - Support & updates - Software updates*.

1. Select **Support & updates** and click on **Updates** (a).

[5] all models



Base Units

Base Unit automatic firmware upgrade — Start wizard — Supported by: CSE-800, CSE-200

Base Unit software update — Start wizard — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

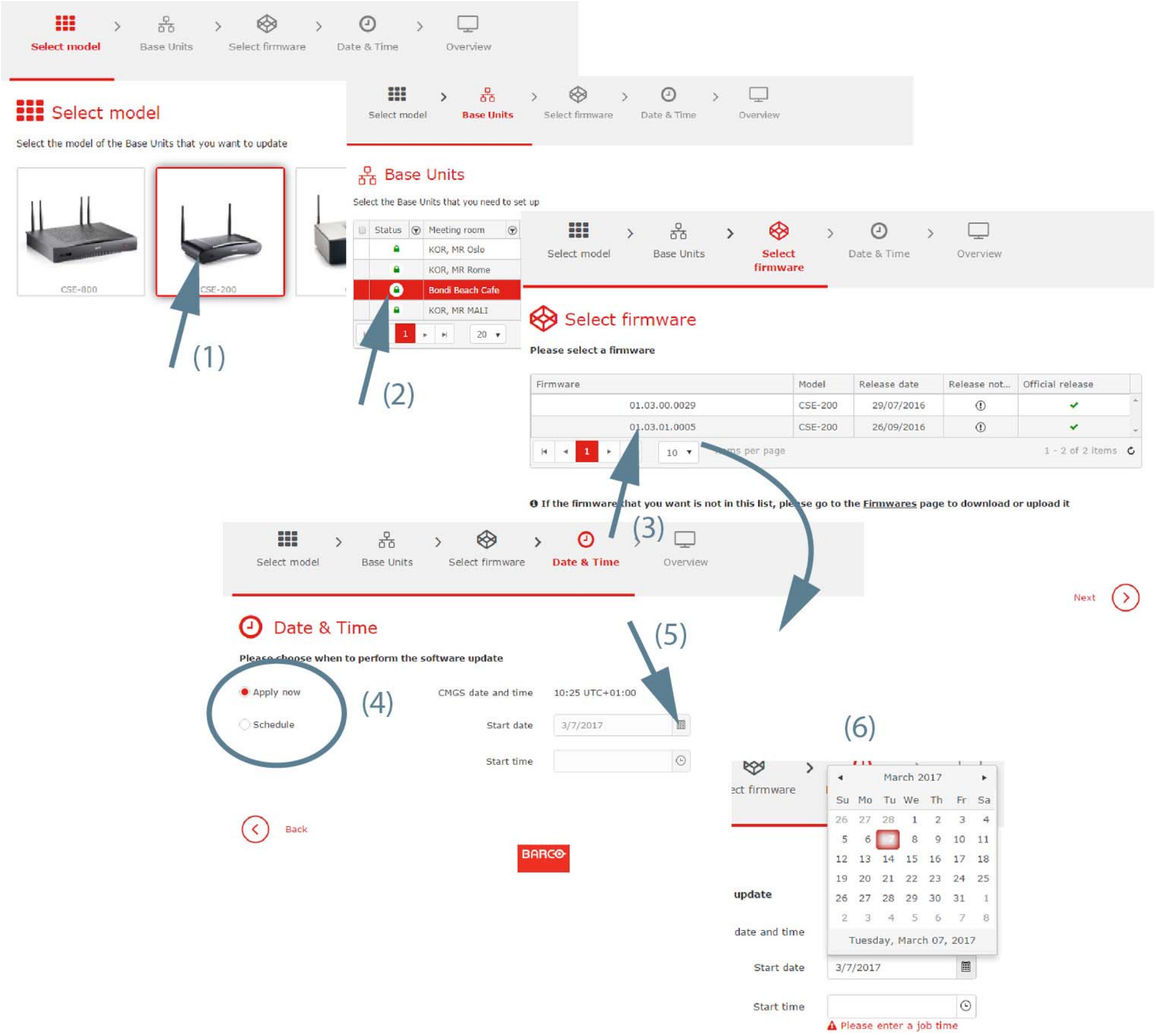
CMGS

Collaboration Management Suite upgrade — Upgrade CMGS

Image 8-4
Start software update wizard

2. Click on the **Start wizard** button next to *Base Unit software upgrade* (b).

3. Select your model and click **Next** to continue (1).



Select model

Select the model of the Base Units that you want to update

Base Units

Select the Base Units that you need to set up

Status	Meeting room
🔒	KOR, MR Oslo
🔒	KOR, MR Rome
🔒	Bondi Beach Cafe
🔒	KOR, MR MALI

Select firmware

Please select a firmware

Firmware	Model	Release date	Release not...	Official release
01.03.00.0029	CSE-200	29/07/2016	ⓘ	✓
01.03.01.0005	CSE-200	26/09/2016	ⓘ	✓

10 items per page — 1 - 2 of 2 items

If the firmware that you want is not in this list, please go to the Firmwares page to download or upload it

Date & Time

Please choose when to perform the software update

● Apply now
○ Schedule

CMGS date and time 10:25 UTC+01:00

Start date 3/7/2017

Start time

March 2017

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Tuesday, March 07, 2017

Start date 3/7/2017

Start time

Please enter a job time

Image 8-5
Software updates

4. Select the Base Unit(s) that need(s) to set up and click **Next** (2).

5. Is the firmware you want in the list?
If yes, Continue with step 6.
If no, go first to the *Firmwares* page. For more info see "Firmwares", page 65.

6. Select the firmware version and click **Next** to continue (3).
7. To apply the firmware immediately, check the radio button in front of **Apply now** (4).
   To schedule the update in the future, check the radio buton in front of **Schedule**. Click on the calendar to change the date (5). Click on the time drop down box and select a predefined time slot.
8. Click **OK**.

   The Overview page is displayed with the new scheduled settings.
9. Click **Finish**.

8.2.2 Collaboration Management Suite upgrade

How to upgrade

1. Select **Support & updates** and click on **Updates** (a).

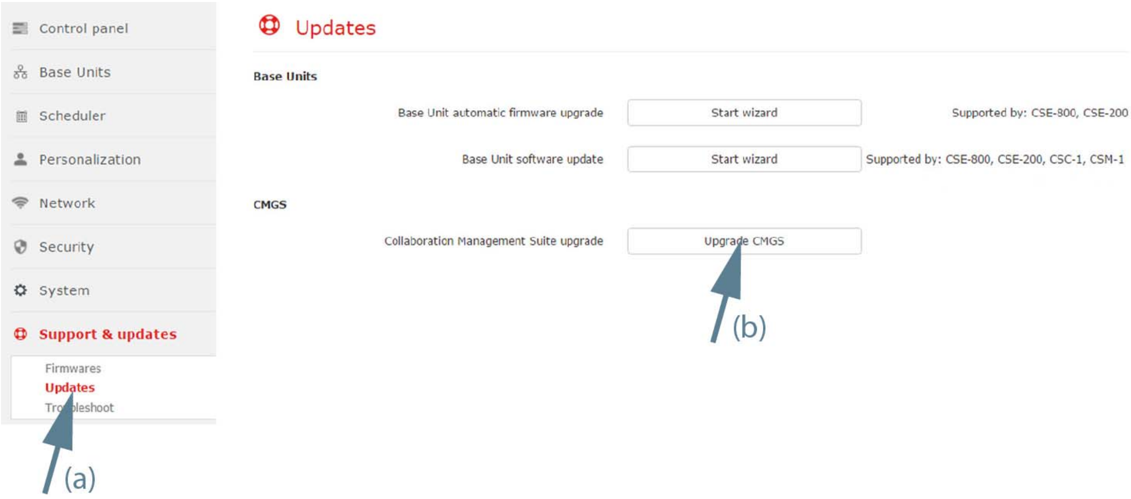
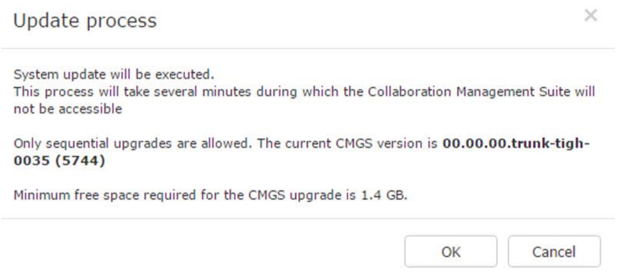


Image 8-6
CMGS upgrade wizard

2. Click on the **Upgrade CMGS** button next to *Collaboration Management Suite upgrade* (b).

   An *Update process message* is displayed.


Update process

System update will be executed.
This process will take several minutes during which the Collaboration Management Suite will not be accessible

Only sequential upgrades are allowed. The current CMGS version is **00.00.00.trunk-tigh-0035 (5744)**

Minimum free space required for the CMGS upgrade is 1.4 GB.

Image 8-7
Update process

This process will take several minutes during which the Collaboration Management Suite will not be accessible. Only sequential upgrades are allowed. That means that if your have to install all update version available between your version and the latest released version.

3. Click **OK** to continue.

8.3 Troubleshoot

Overview

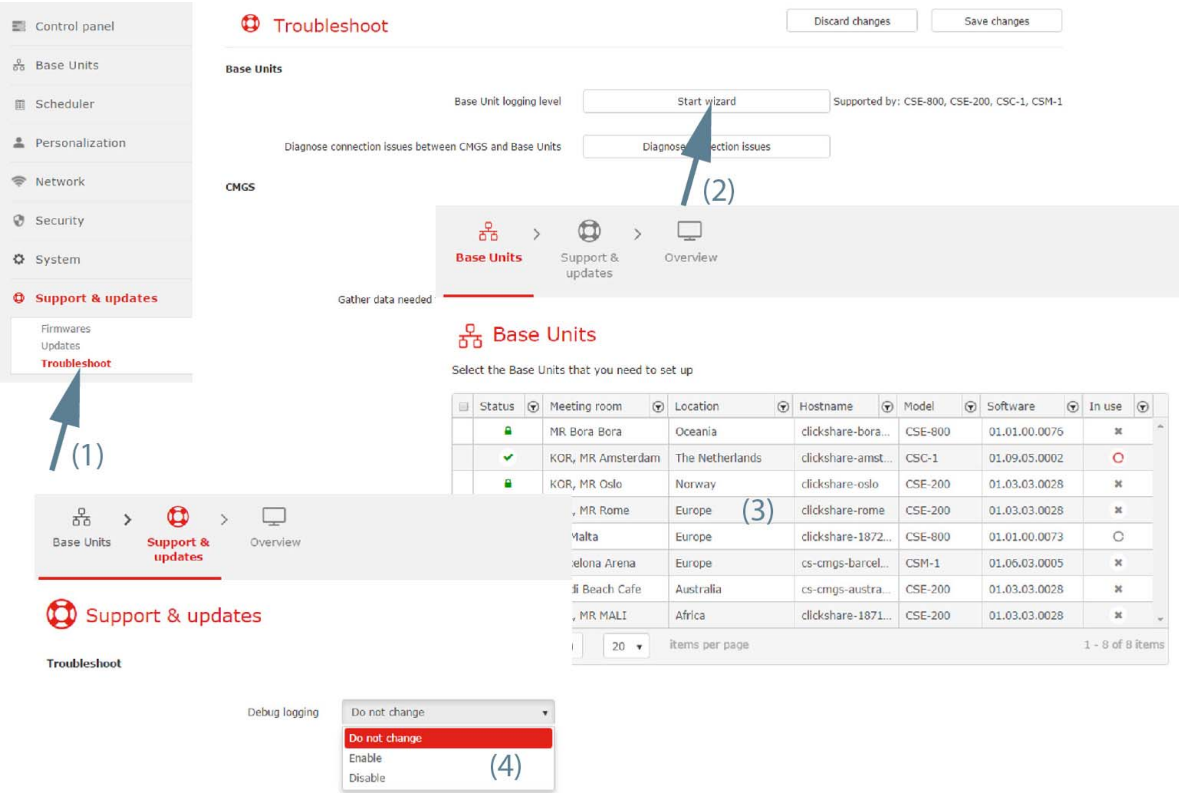
- Base Unit logging level
- Diagnose connection issues CMGS - Base Unit
- CMGS logging level
- Restart CMGS
- Report CMGS issues

After changing a setting in Troubleshoot, always click Save changes to apply the new settings.

8.3.1 Base Unit logging level

How to set

1. Select **Support & updates** and click on **Troubleshoot** (1).



Base Unit logging level: Start wizard — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Diagnose connection issues between CMGS and Base Units: Diagnose ection issues

Gather data needed

Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Oceania	clickshare-bora...	CSE-800	01.01.00.0076	✖
	✓	KOR, MR Amsterdam	The Netherlands	clickshare-amst...	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	01.03.03.0028	✖
		, MR Rome	Europe	clickshare-rome	CSE-200	01.03.03.0028	✖
		Malta	Europe	clickshare-1872...	CSE-800	01.01.00.0073	○
		elona Arena	Europe	cs-cmgs-barcel...	CSM-1	01.06.03.0005	✖
		i Beach Cafe	Australia	cs-cmgs-austra...	CSE-200	01.03.03.0028	✖
		, MR MALI	Africa	clickshare-1871...	CSE-200	01.03.03.0028	✖

20 ▾ items per page — 1 - 8 of 8 items

Debug logging: Do not change ▾ (Do not change / Enable / Disable)

Image 8-8
Troubleshoot, Base Unit logging level

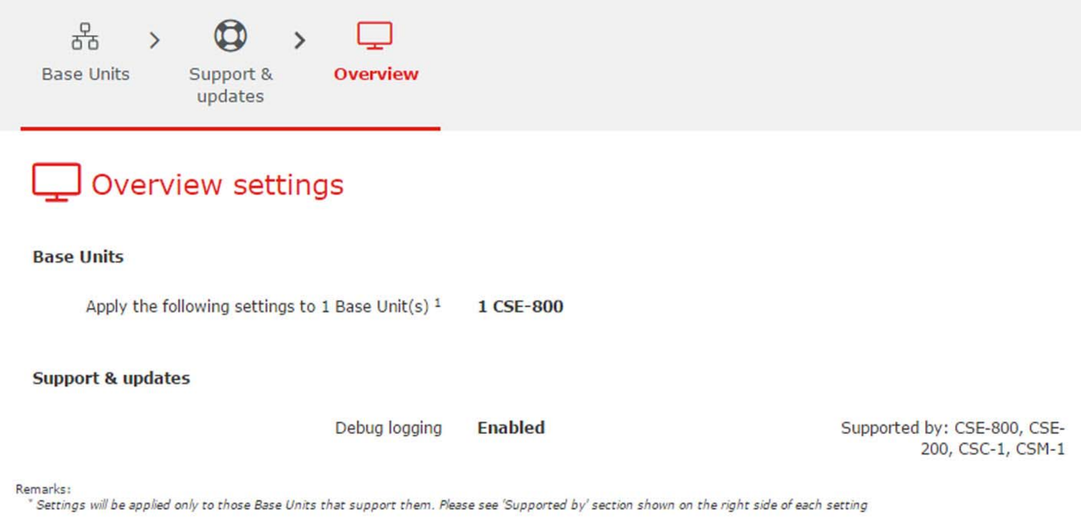
2. Click **Start wizard** next to *Base Unit logging level* (2).

3. Select Base Unit(s) (3) and click **Next**.

4. Click on the drop down next to *Debug logging* and select the desired setting (4).
   The following settings are possible:
   - Do not change: the current setting remains active.
   - Enable: debug logging is enabled.
   - Disable: debug logging is disabled.

5. Click **Next** to continue.

An overview page is displayed.



Overview settings

Base Units

Apply the following settings to 1 Base Unit(s) [1] 1 CSE-800

Support & updates

Debug logging Enabled Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Remarks:
[1] Settings will be applied only to those Base Units that support them. Please see 'Supported by' section shown on the right side of each setting

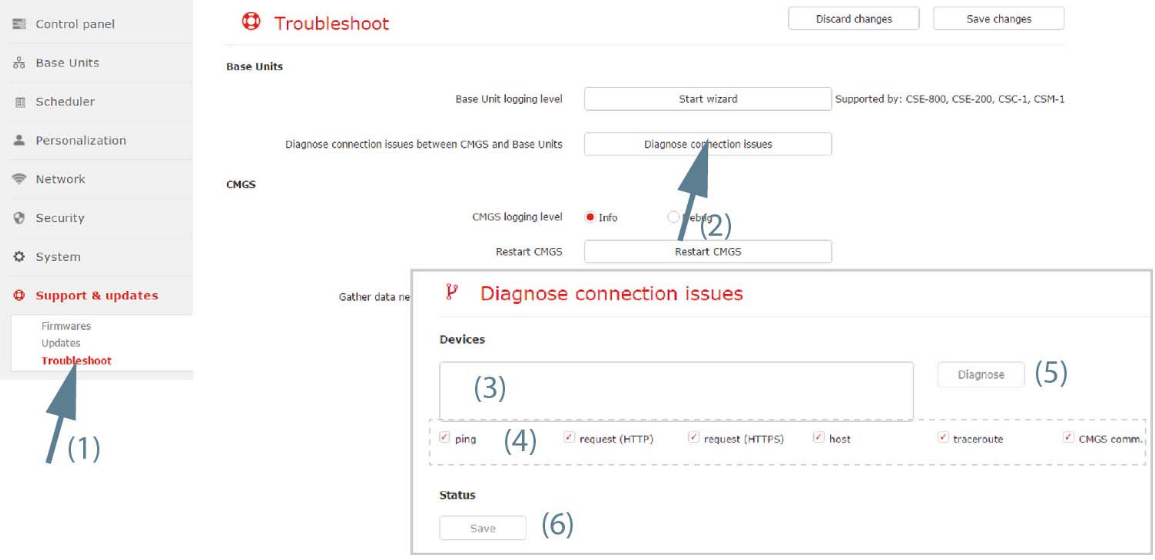
Image 8-9
Overview settings

6. Click **Finish**.

8.3.2 Diagnose connection issues CMGS - Base Unit

How to setup

1. Select **Support & updates** and click on **Troubleshoot** (1).



Base Units

Base Unit logging level Start wizard Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Diagnose connection issues between CMGS and Base Units Diagnose connection issues

CMGS

CMGS logging level ● Info ○ Debug

Restart CMGS Restart CMGS

Devices

☑ ping ☑ request (HTTP) ☑ request (HTTPS) ☑ host ☑ traceroute ☑ CMGS comm.

Status

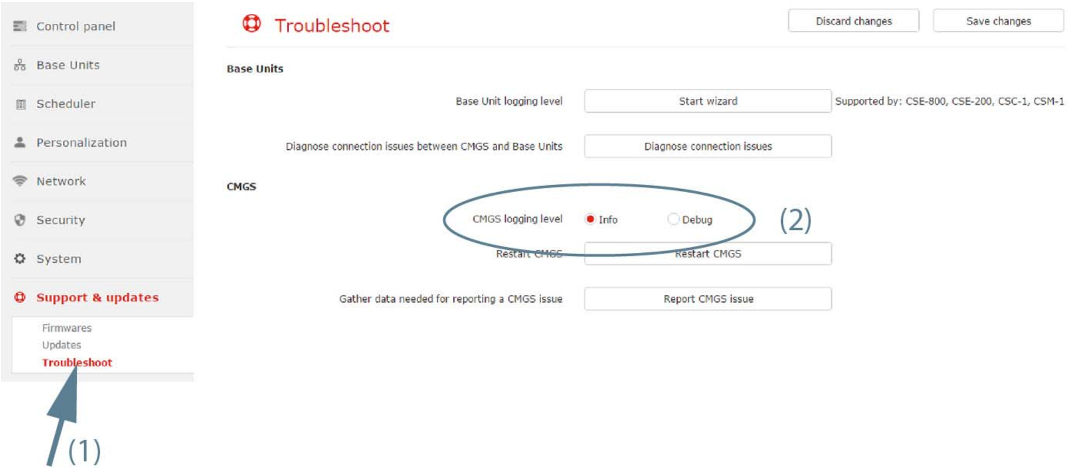
Image 8-10
Troubleshoot, diagnose connection issues

2. Click **Start wizard** next to *Diagnose connection issues between CMGS and Base Unit* (2).
3. Enter the hostnames or IP addresses, separated by a comme, of the Base Units to diagnose (3).
4. Check or uncheck the diagnose areas (4).
5. Click **Diagnose** (5).
6. To save the diagnose status, click on **Save** (6).

8.3.3 CMGS logging level

How to set

1. Select **Support & updates** and click on **Troubleshoot** (1).



CMGS logging level ● Info ○ Debug

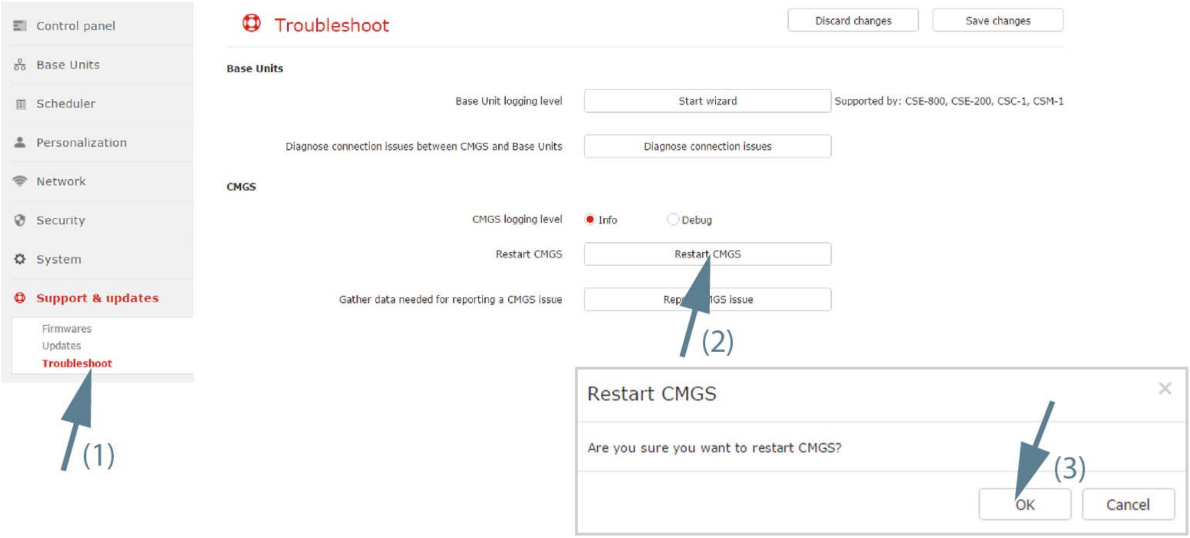
Image 8-11
Troubleshoot, CMGS logging level

2. Next to CMGS logging level, check the radio button of your choice (2).
   The following choices are possible:
   - Info
   - Debug

8.3.4 Restart CMGS

How to restart

1. Select **Support & updates** and click on **Troubleshoot** (1).



CMGS logging level ● Info ○ Debug

Are you sure you want to restart CMGS?

Image 8-12

2. Click on **Restart CMGS** next to *Restart CMGS* (2).

   A restart message is displayed.

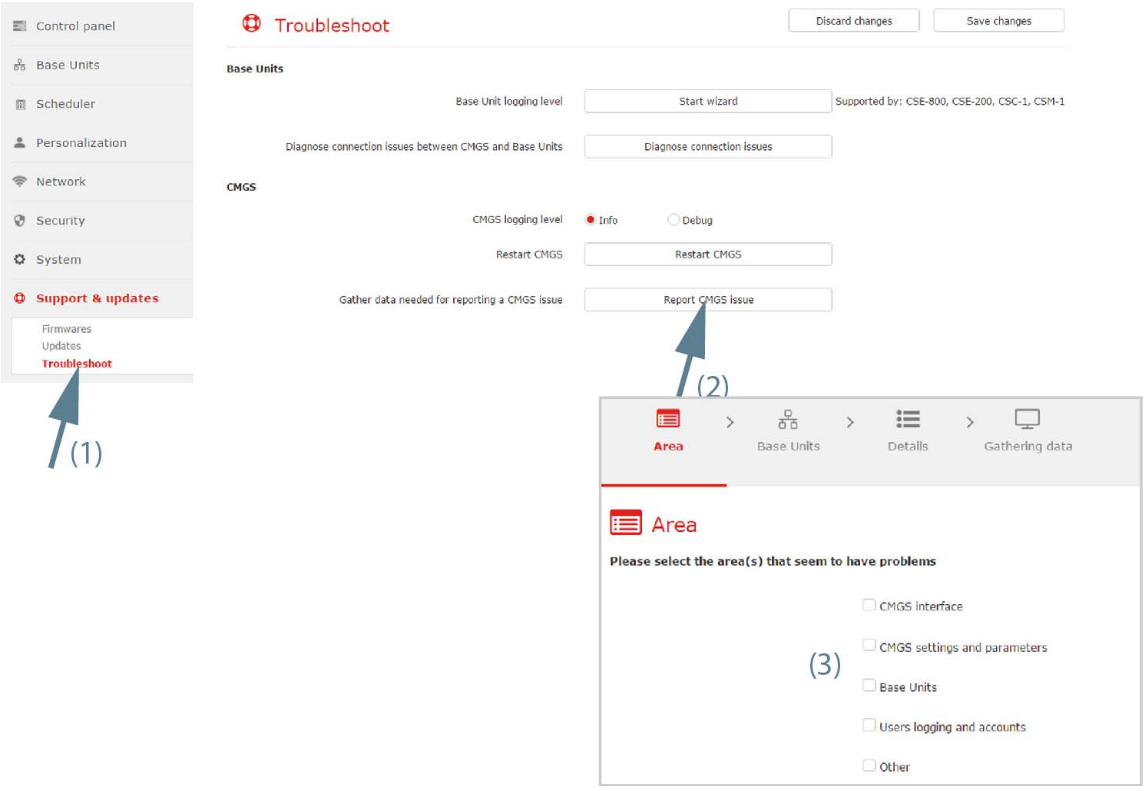
3. If you really want to restart, click **OK** (3).

   This will take several minutes. Re-login will be necessary.

8.3.5 Report CMGS issues

How to report issues

1. Select **Support & updates** and click on **Troubleshoot** (1).



Base Units

Base Unit logging level — Supported by: CSE-800, CSE-200, CSC-1, CSM-1

Diagnose connection issues between CMGS and Base Units

CMGS

CMGS logging level ● Info ○ Debug

Restart CMGS

Gather data needed for reporting a CMGS issue

Area

Please select the area(s) that seem to have problems

□ CMGS interface

□ CMGS settings and parameters

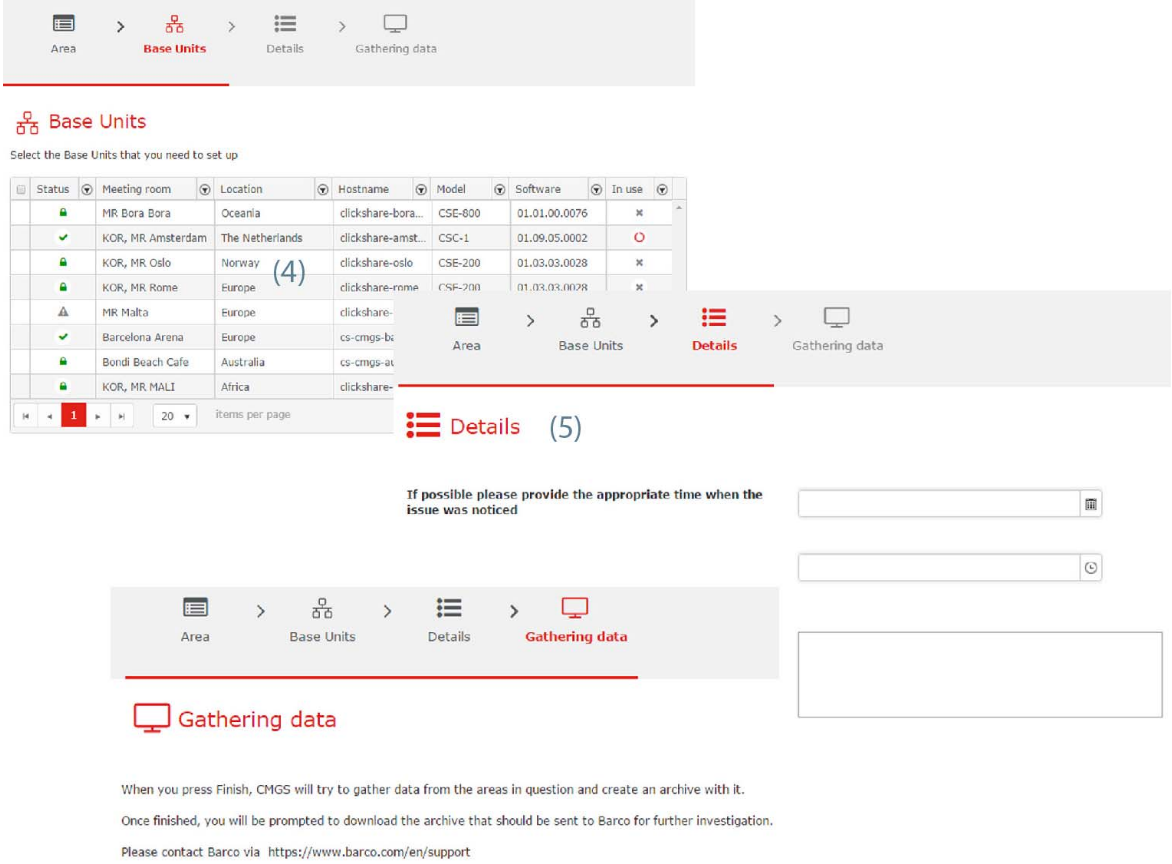
□ Base Units

□ Users logging and accounts

□ Other

Image 8-13
Report CMGS issue

2. Click **Report CMGS issue** next to *Gather data needed for reporting a CMGS issue* (2).
3. Select the Area that seems to have problems (3).
4. Select the Base Unit(s) where you discovered an issue (4).



Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	Hostname	Model	Software	In use
	🔒	MR Bora Bora	Oceania	clickshare-bora...	CSE-800	01.01.00.0076	✖
	✓	KOR, MR Amsterdam	The Netherlands	clickshare-amst...	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Oslo	Norway	clickshare-oslo	CSE-200	01.03.03.0028	✖
	🔒	KOR, MR Rome	Europe	clickshare-rome	CSE-200	01.03.03.0028	✖
	⚠	MR Malta	Europe	clickshare-			
	✓	Barcelona Arena	Europe	cs-cmgs-ba			
	🔒	Bondi Beach Cafe	Australia	cs-cmgs-au			
	🔒	KOR, MR MALI	Africa	clickshare-			

1 | 20 ▾ items per page

Details

If possible please provide the appropriate time when the issue was noticed

Gathering data

When you press Finish, CMGS will try to gather data from the areas in question and create an archive with it.

Once finished, you will be prompted to download the archive that should be sent to Barco for further investigation.

Please contact Barco via https://www.barco.com/en/support

Image 8-14
Report CMGS issue

5. Enter more details (5).
   - Click on the calendar icon and select the date.
   - Enter a time (hh:mm) or click on the icon and select a time out of the drop down list.
   - Enter a detailed description
6. Click Next to gather the data.

   An archive file will be created and should be downloaded to be sent to Barco for further investigation.

   Create a support ticket via https://www.barco.com/en/support

9. SOFTWARE PORTS

9.1 Used ports

Ports used by ClickShare Collaboration Management Suite

SMTP: depending on the settings of the SMTP server within the client's company the following ports are usually used:

- port 25 TCP/UDP outbound - this is needed for accessing SMTP server for sending E-mails.
- port 465 TCP/UDP outbound - this is needed for accessing SMTP over TLS/SSL (SMTPS) server for sending E-mails.

PROXY: if CMGS does not have direct access to the Internet and a Proxy server is needed to retrieve http://update.barco.com/ClickShare/releases.json then usually:

- port 80 TCP outbound
- port 8080 TCP outbound

DNS: if a DNS server exists in the client's company:

- port 53 UDP outbound
- port 53 TCP outbound

NTP: used for time synchronization

- port 123 UDP outbound
- port 123 TCP outbound

Ports used by the Base Unit's REST API

- port 4000 TCP outbound - for accessing Base Unit's REST API when HTTP is enabled on the Base Unit.
- port 4001 TCP outbound - for accessing Base Unit's REST API when HTTPS is enabled on the Base Unit

Browser access and Base Units access needed for retrieving files from CMGS (firmwares, Base units configuration files, wallpapers)

- port 80 TCP inbound - for HTTP access
- port 443 TCP inbound - for HTTPS access

Ports used by Base Units

Browser access and CMGS needs to retrieve certain files from the Base Units (Base Units configuration files)

- port 80 TCP inbound - for HTTP access
- port 443 TCP inbound - for HTTPS access

REST API

- port 4000 TCP inbound
- port 4001 TCP inbound

INDEX