Collaboration Management Suite

User guide

ENABLING BRIGHT OUTCOMES

BARCO

Product revision

Software Revision: 1.5

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

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

Product Security Incident Response

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

Table of contents

Introduction 1

Overview

- About Collaboration Management Suite
- Security Recommendation
- Before you start
- Starting up Collaboration Management Suite
- Forgot password
- Register as new user
- Logout from Collaboration Management Suite
- First start up (registration - settings)
- 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 Barco's XMS-110 box 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. Before the application on the XMS-110 can be used, it must be registered on Barco's website.

The information provided includes:

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

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 112.

In order to diagnose connection problems between CMGS and the Base Units please see "Diagnose connection issues", page 36.

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

It also supports wePresent devices however the configuration of those devices is part of the wePresent documentation set

About user roles

User roles settings can be found under *System*, *User roles*. For more info, see "User roles", page 86.

By default the user roles are:

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	RW	RW	RW
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			
Clone configuration	RW	RW	-

Functionality	IT admin	Support	Key user
Network integration	RW	RW	-
Wallpaper	RW	RW	RW
WebUI access via WiFi	RW	RW	-
Deploy Base Unit certificates	RW	RW	-
Users			
Add/Remove	RW	-	-
Grid	RW	R	-
Locations	RW	-	-
Scheduler	RW	RW	-
Scheduled jobs	RW	RW	RW[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! Multiple users could share the same account. However, these user roles can be adjusted.

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 Security Recommendation

Overview

To avoid unauthorized access and potential harmful operations to the server with consequences to the rest of your network, it is recommended to:

1. Install the server in an area with restricted/controlled access
2. Disable USB boot in the BIOS and protect the BIOS with a password to avoid installation of malicious software.
   The BIOS can be accessed by pressing the <F2> key during startup of the device.

> Make sure the BIOS password can be provided to the Barco Service personnel to facilitate the repair process. If the password is lost, the system will need to be wiped completely upon service intervention.

1.3 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.
- By default, this is
  - user name: admin@yourcompany.com

1: only reboot jobs are shown.

- password: admin

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

1.4 Starting up Collaboration Management Suite

How to start up

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

   The login page is displayed.

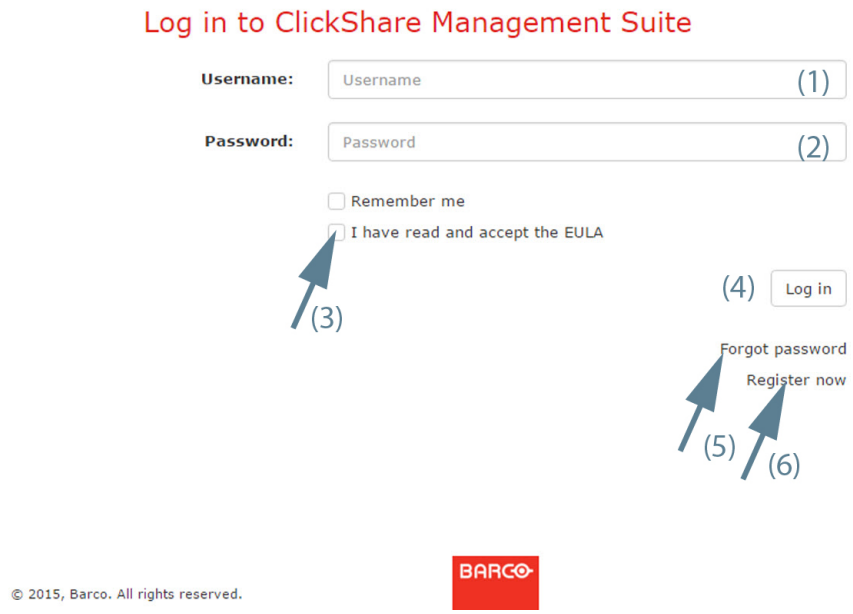

Image 1-1: Login

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 when 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)

1.5 Forgot password

What to do when you forgot your password

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

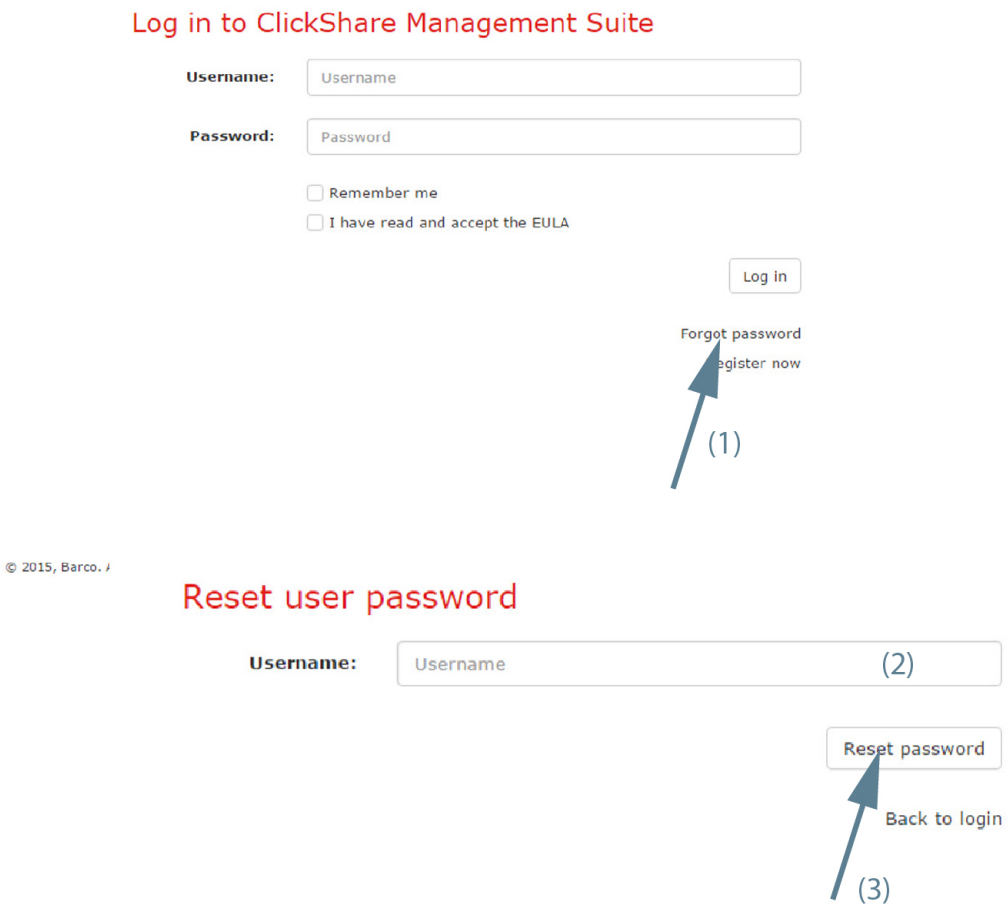

Image 1-2: Forgot password

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

> This E-mail service will only work if an email system was set up during the installation of Collaboration Management Suite. If not, the Collaboration Management Suite will not be able to send any E-mails to the users.

1.6 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 can be informed via E-mail.

How to register

1. On the logon page, click on *Register now* (1).

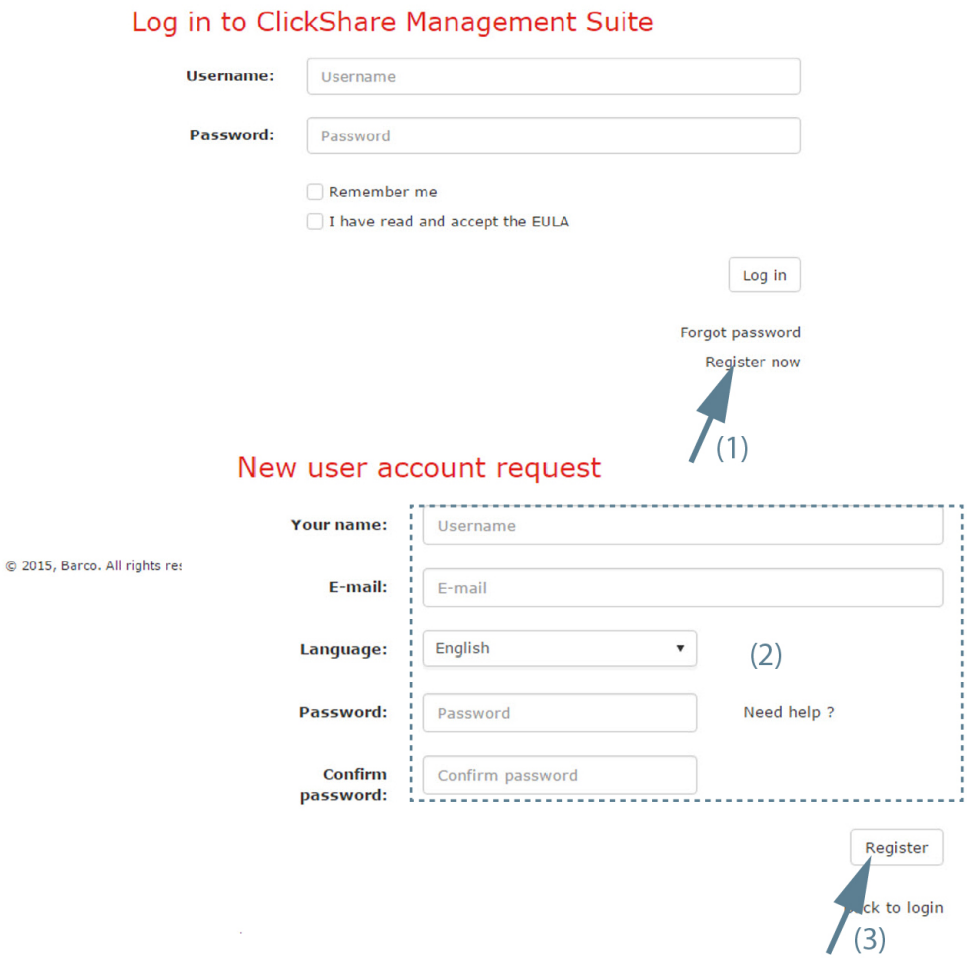

Image 1-3

A registration page opens.

2. Enter the following data (2):
   - Your 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.
   - Repeat your previous entered password.
3. Click on **Register** (3).

1.7 Logout from Collaboration Management Suite

How to logout

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

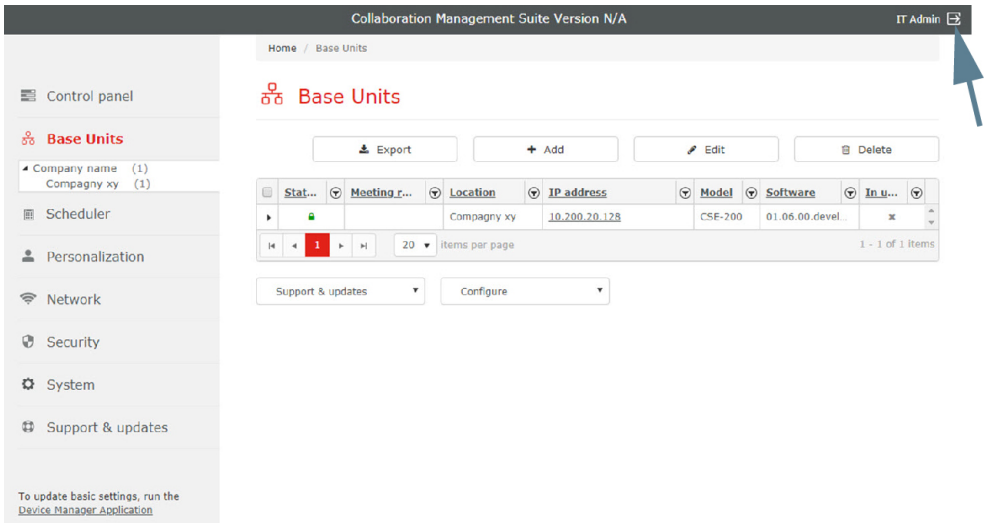

Image 1-4: Logout

1.8 First start up (registration - settings)

About the setup wizard

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

The following setup points are included:

- Personalization
- Registration
- System settings
- Network settings
- Overview

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

Personalization & registration

1. Enter a Device name that allow you to easily identify this device..

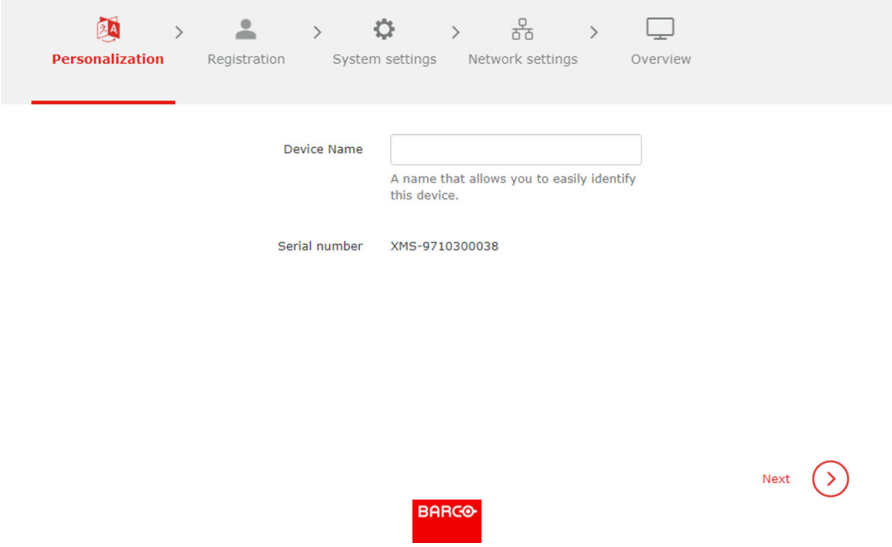

Image 1-5: Device name

2. Click **Next**.

3. Register your device.

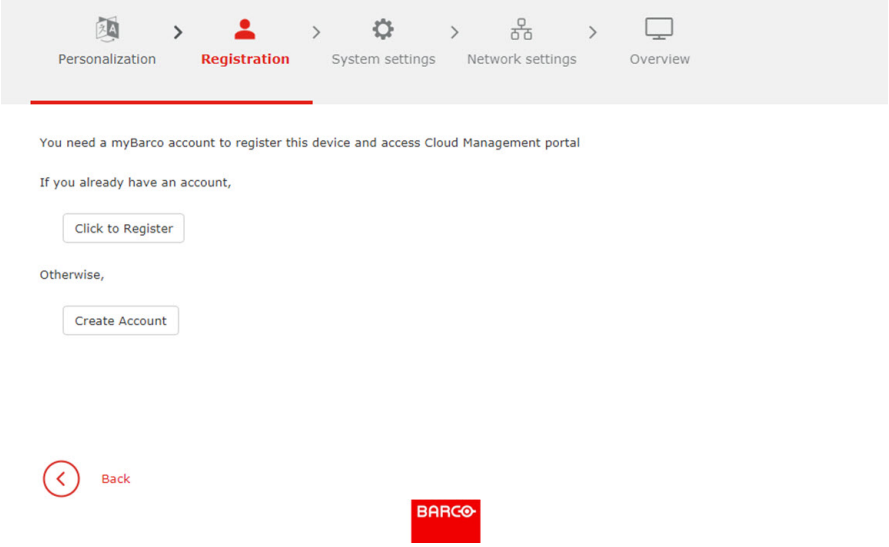

Image 1-6: Registration

If you already have an account to myBarco, click on **Click to Register**.

If do not have an account, click on **Create Account** and following the instructions on the Barco website. Return to the registration page when your receive your new account.

4. Enter your credentials and **Sign in**.

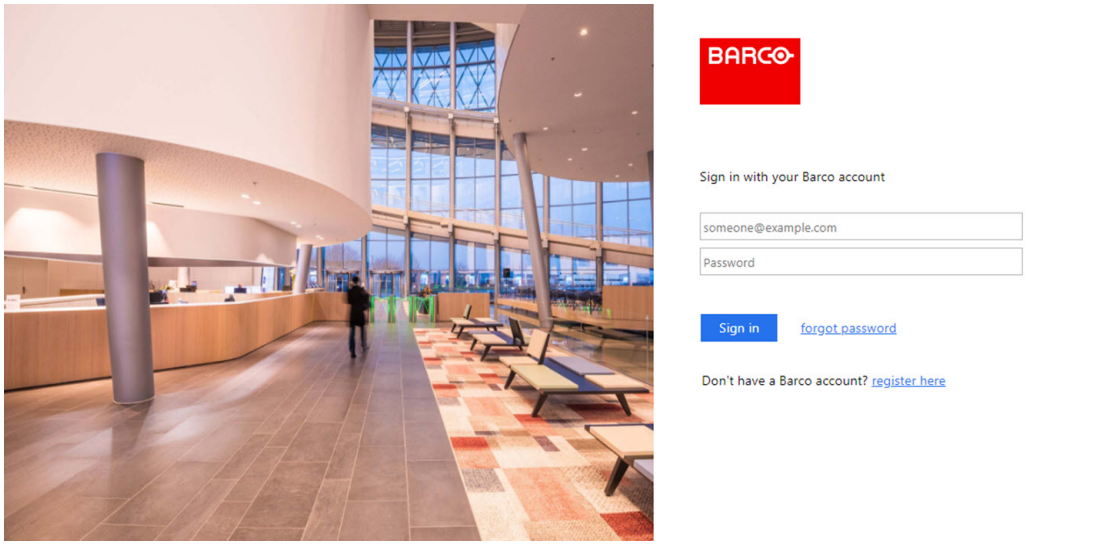

Image 1-7: myBarco login

The device activation page opens.

5. Fill out the activation page.

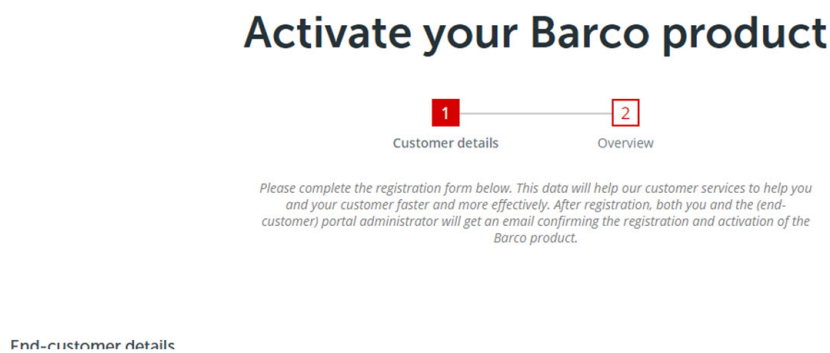

Image 1-8: Product activation

The following items should be filled out

- End-customers details
  - Contact name
  - phone number
  - Portal administrator email
- Installation address

Goto step 2 to get an overview. Check the data and read the EULA. Click **Confirm**.

An overview will be displayed in the registration page.

System settings

1. The current UTC time is indicated. Select you timezone. Click on the drop down box and select the corresponding zone.

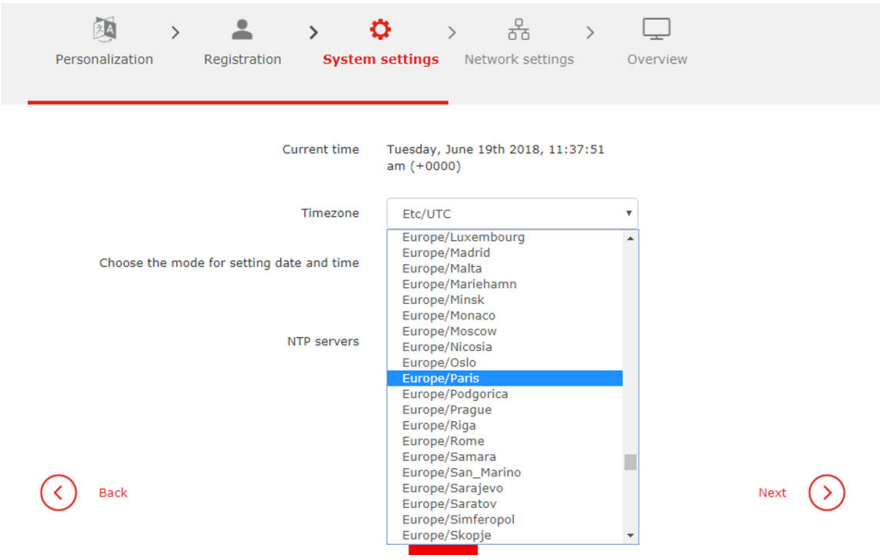

Image 1-9: Timezone setup

2. Select mode for setting date and time. Check the check box of your choice.
   - Use NTP server
   - Set a date and time manually

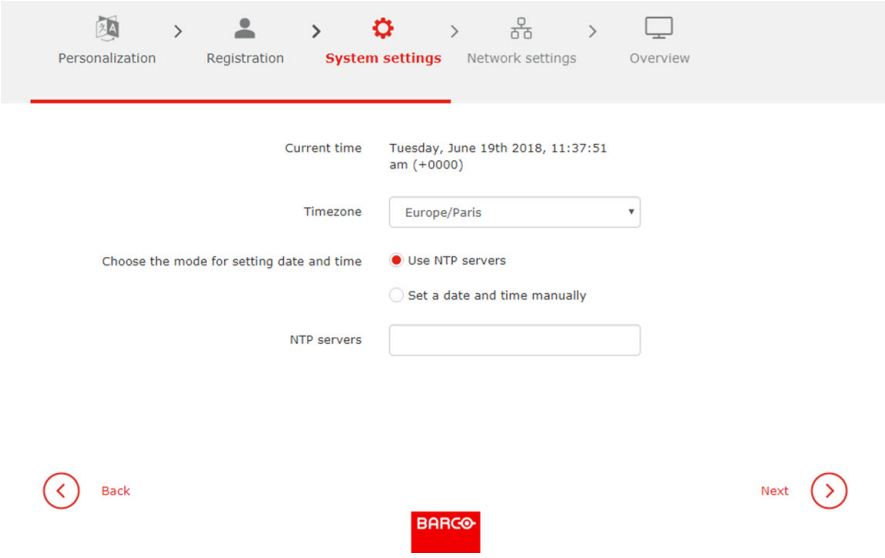

Image 1-10: Timezone and NTP server

3. To use an NTP server, fill out the NTP server IP address or host name next to *NTP servers*.

   Up to maximum 5 servers can be added, separated by a comma.

4. To set a time and date manually, select the radio button next to *Set a date and time manually*.

   Click on the date table icon and select the current date.

   To select the time, click on the clock icon. Click on the up down control to set the hours, minutes and second. Toggle the period between AM and PM just by clicking on AM or PM.

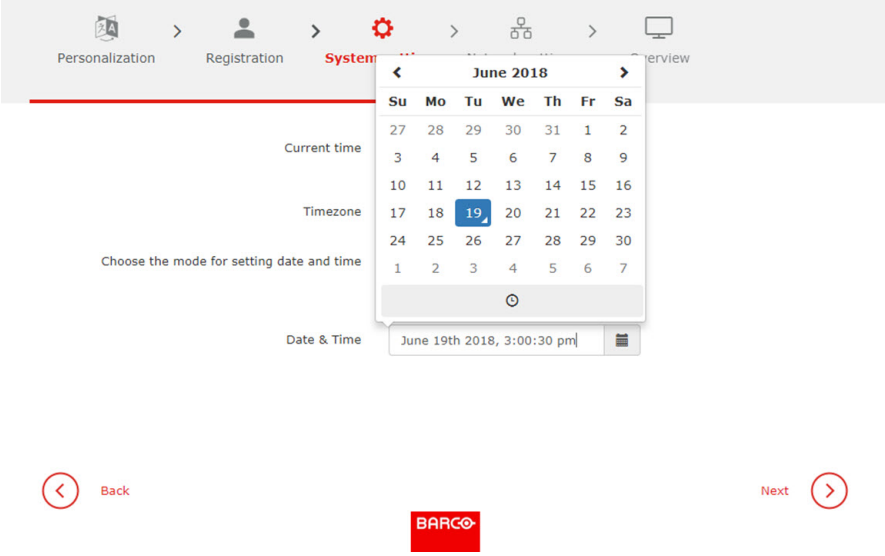

Image 1-11: Time and date setup

5. Click Next to continue to the Network settings.

Network settings

1. Fill out the Network settings.

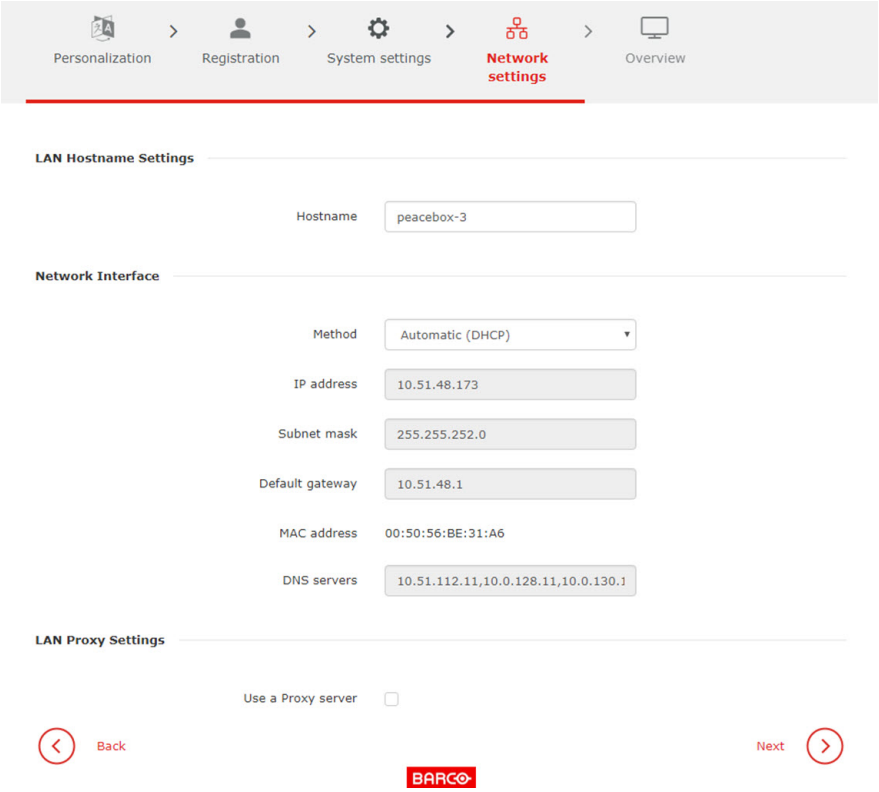

Image 1-12: Network settngs

The following settings can be filled out:

- LAN Hostname Settings, IP address or FQDN[2]
- Network interface, method, automatically or manually
- 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. Click **Next**.

   An overview page is displayed.

3. Click **Finish** to terminate the wizard.

   The check for updates starts.

Image 1-13: Check for updates

When new updates are found, these updates will be installed automatically. The XMS-100 will reboot.

2: Fully Qualified Domain Name

When finished the Home page is displayed.

1.9 About the Home page, control panel

Overview

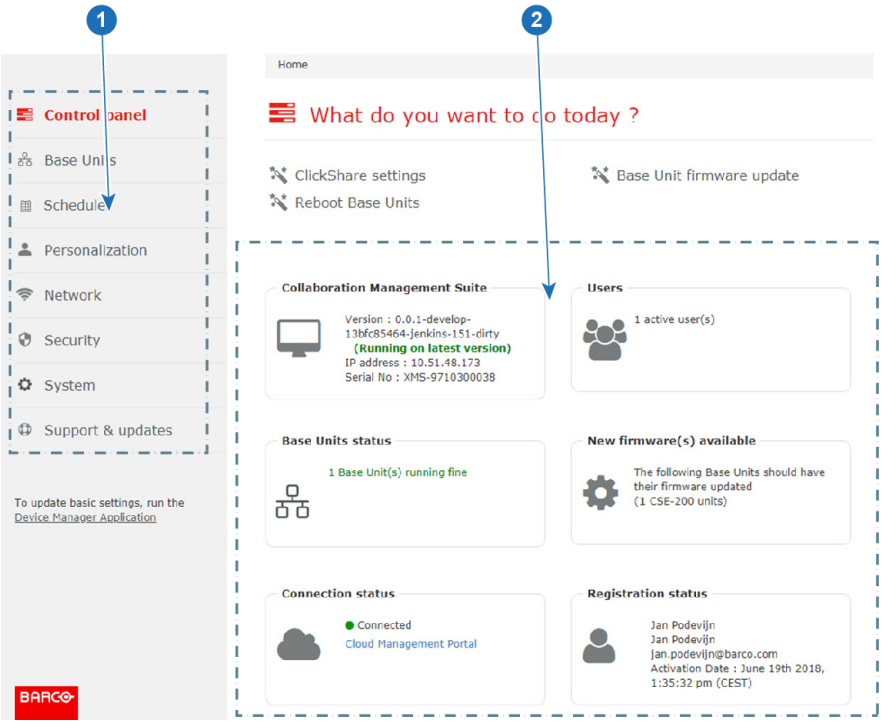

Image 1-14: Home page overview

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

1 Menu pane.
  The following main menus are available:
  - Control panel
  - Base Units
  - Scheduler
  - Personalization
  - Network
  - Security
  - System
  - Support & updates
  - Run Device Manager Application

2 Overview and selection pane.

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

The following items can be controlled or seen:

- ClickShare settings
- Base Unit firmware update
- Collaboration Management Suite overview
- Users overview
- Base Unit statuses
- New Base Units discovered (only for CSE devices)
- New firmware(s) available
- Registration status

- Connection status

Explanation of wizards

- Base Unit status will guide you to a Base Units overview, see “Base Units page”, page 23 to continue.
- Users will guide you to the users page. For more info, see “Users”, page 81 to continue.
- New firmware will start the firmware wizard, see “Firmwares”, page 90 to continue.
- Auto-discovered Base Units will guide you to the auto-discover wizard, see “Auto discovering of Base Units”, page 26 to continue.

When changing a setting in one of the menu pages, always click **Save changes** to apply the new settings.

Base Units page

2

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

Overview

- About the Base Units page
- Auto discovering of Base Units
- Export Base Unit list
- Add new Base Unit(s)
- Edit selected Base Unit(s)
- Delete selected Base Unit(s)
- Sorting and filtering
- Support and updates
- Configure

2.1 About the Base Units page

Overview

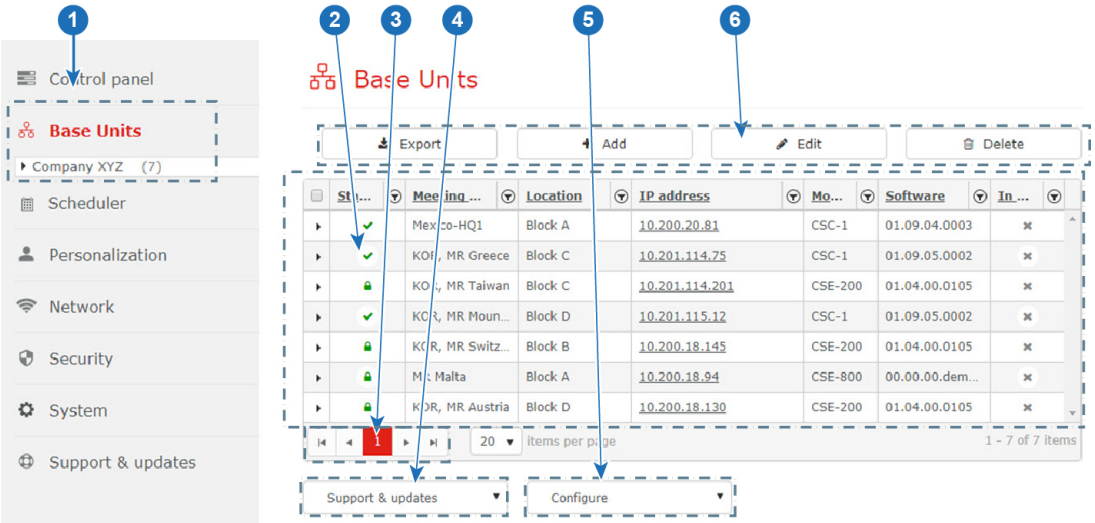

Image 2-1: Overview page

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 displayed[3]:

- The "Status" column of the Base Units grid contains an icon that shows if the device is working properly or not:
  - Green: both green check mark or green lock mean that the device is OK.
    - Green check mark: device works properly and communication protocol is HTTP.
    - Green hang lock: device works poperly and communication protocol is HTTPS
  - 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)
  - 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, buttons are connected, or device is connected with a source but nothing is sharing.
  - A red spinning circle, if the device is connected to a source or buttons are connected, 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, enter the desired page and click **ENTER**.

3: Views differ with every account type

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 export, add, edit or delete Base Units 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

- 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 device range.

What can be done?

New CSE device 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.

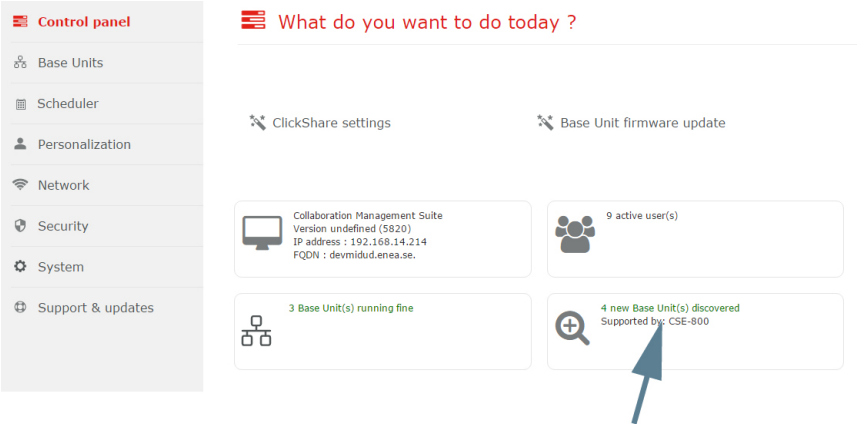

Image 2-2: Auto-discover Base Units

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**.

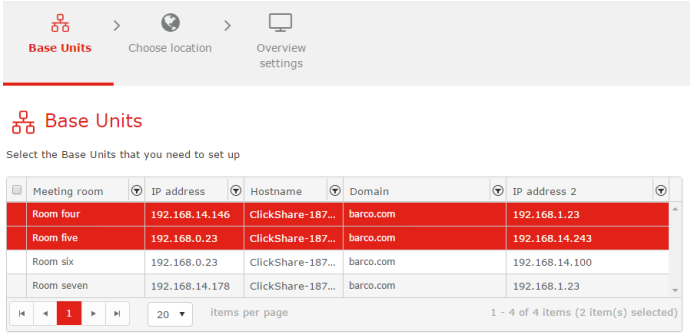

Image 2-3: Select Base Units

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

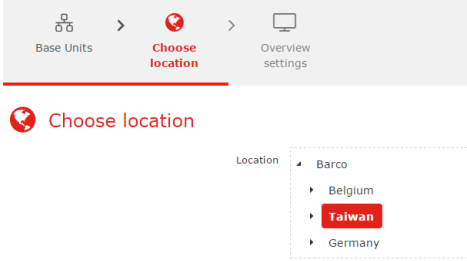

Image 2-4: Choose location

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

4. Click **OK** to continue.

An overview of the settings is displayed.

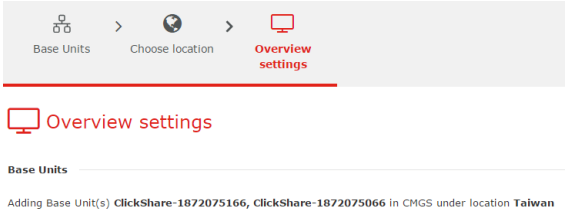

Image 2-5: Overview settings

5. Click **Finish**.

2.3 Export Base Unit list

About exporting Base Units

Selectable information about a Base Unit can be exported into an Excel file (.xls). The export can be done for one or multiple Base Units at the same time.

Export Base Unit(s)

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

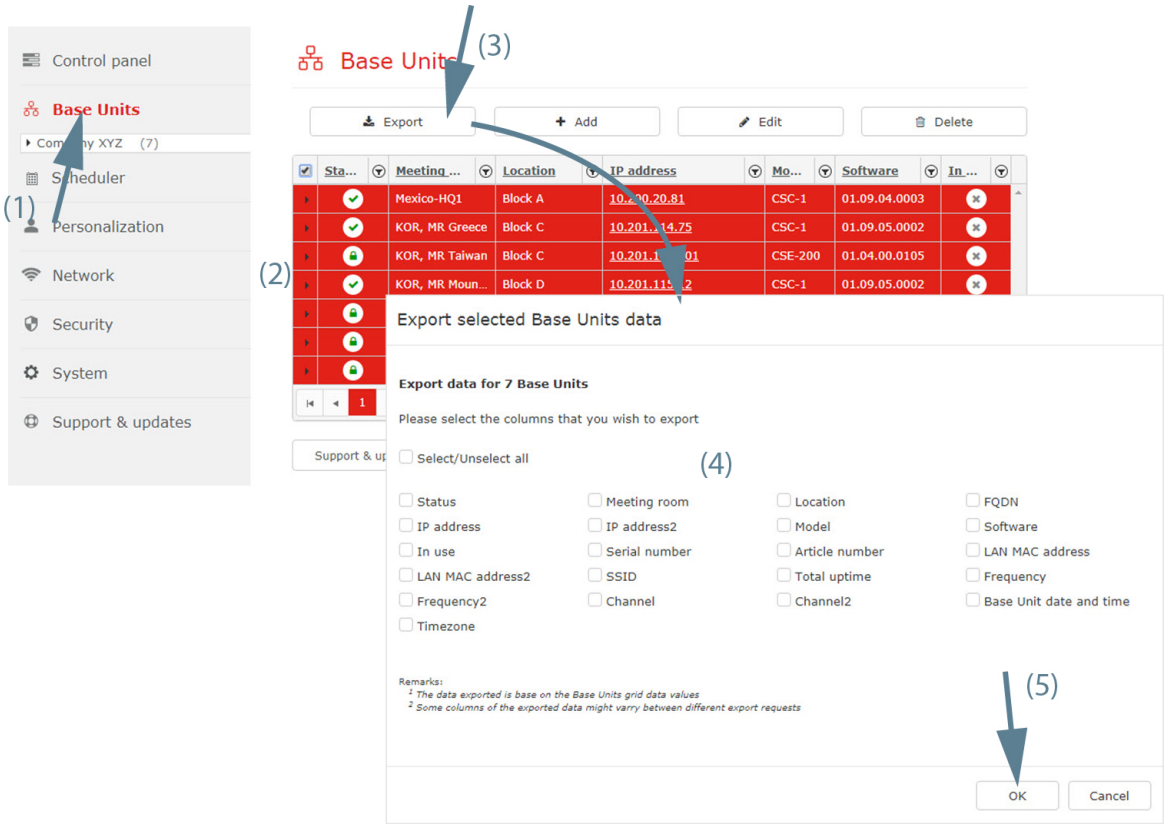

Image 2-6: Export Base Unit(s)

An overview of the current coupled Base Units is shown.

2. Select one or multiple Base Units (2). To select all Base Units, check the check box in the upper left corner.
3. Click on **Export** (3).

   The *Export selected Base Units* data window opens.
4. Select the items to be included in the list (4).

   To select all items at once, check the check box next to *Select/Unselect* all.
5. Click **OK** to start the export (5).

   An Excel file (.xlsx) is created and stored on your local machine.

2.4 Add new Base Unit(s)

About adding Base Units

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

Auto-discovering is supported for CSE devices.

Add via the Base Units window

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

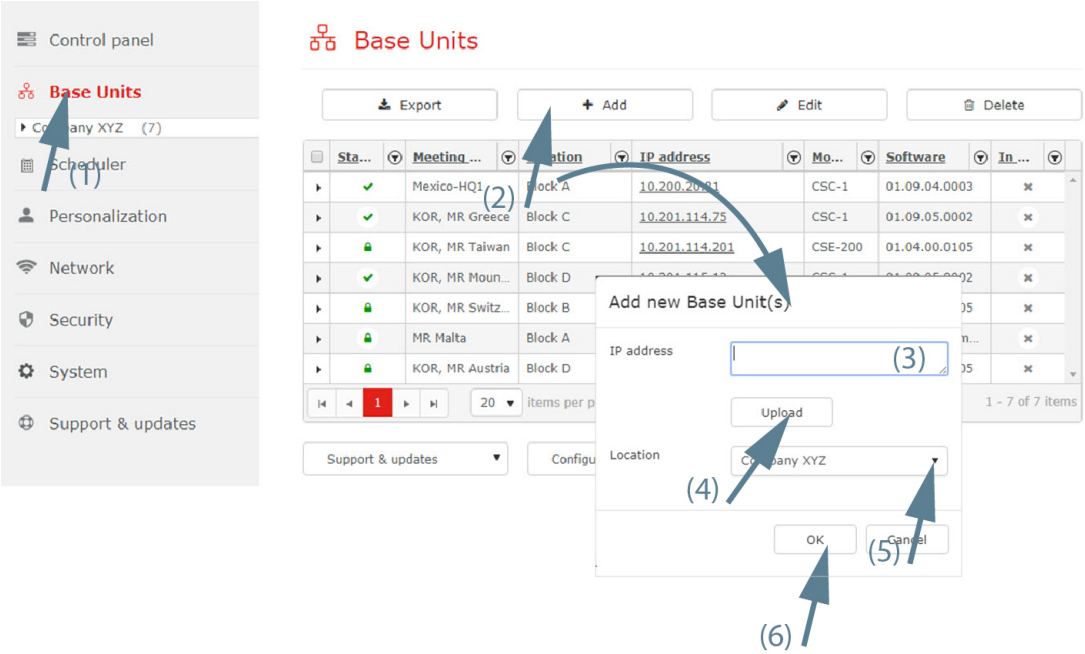

Image 2-7: Add Base Unit

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 *IP Address* (3) and enter the IP address or hostname 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 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 , click on **Upload** (4) and select this file and click on **Open**. After uploading information from file, Base Units must appear into IP address field (no limitation in the number of Base Units).

   Note: Hostnames can have up to maximum 63 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.

   It may take some time before all details of the base units are shown, since this data is acquired in the next polling cycle. The polling interval can be set by the IT admin

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

2.5 Edit selected Base Unit(s)

About editing a Base Unit(s)

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

How to edit

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

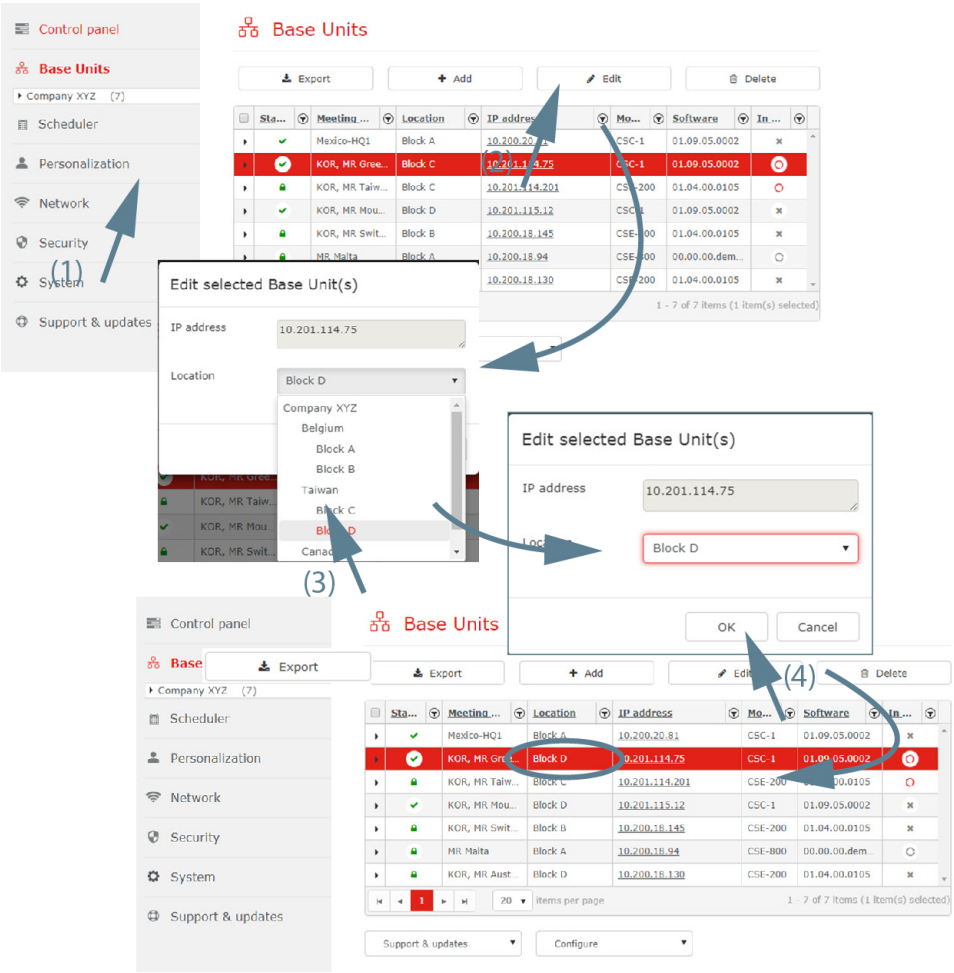

Image 2-8: Edit Base Unit

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 Units are 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
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.

2.6 Delete selected Base Unit(s)

About deleting Base Units

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

How to delete

1. Select the Base Units to delete.

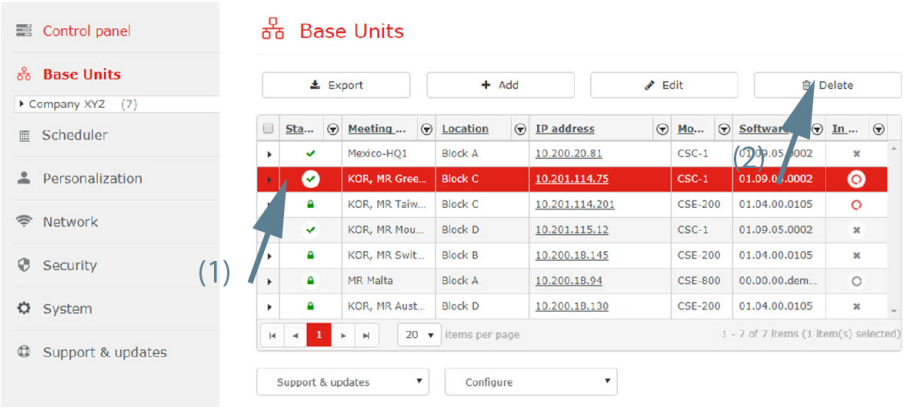

Image 2-9: Delete Base Unit

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).

2.7 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.

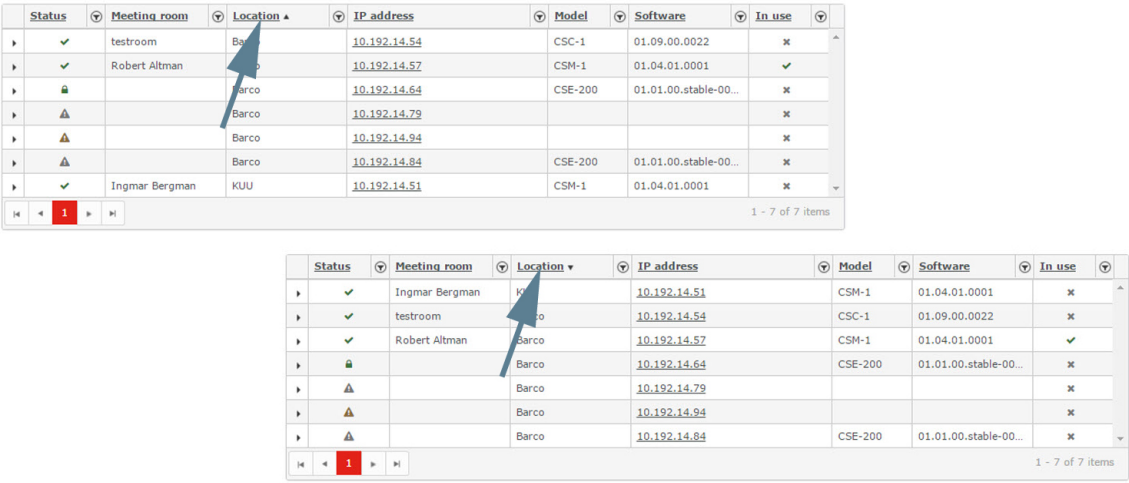

Image 2-10: Sorting overview

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.

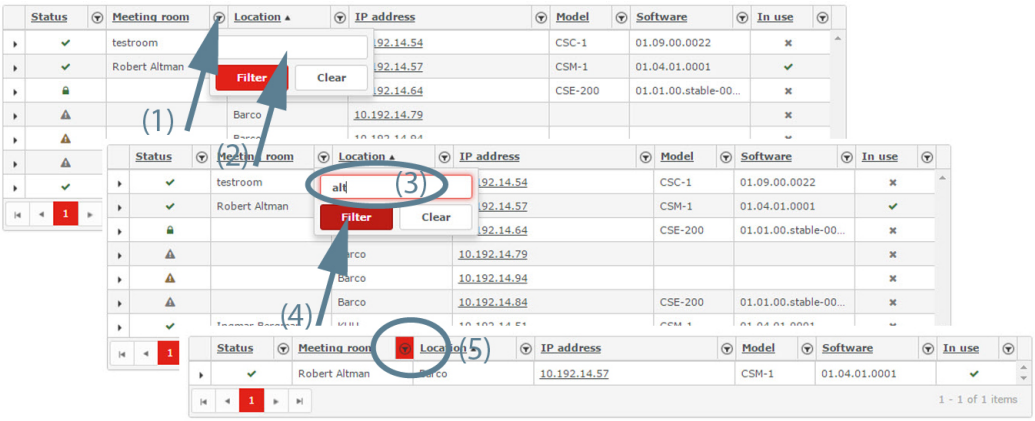

Image 2-11: Filtering overview

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'.

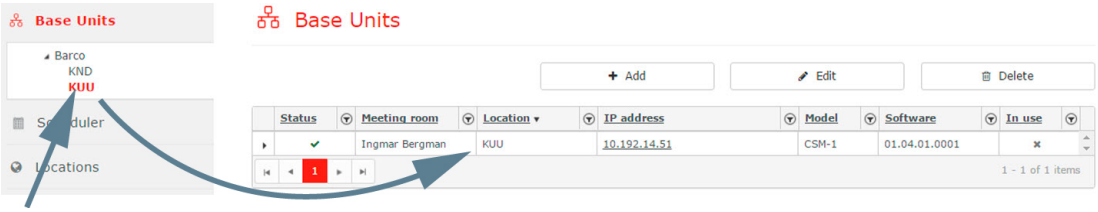

Image 2-12: Filtering via tree

2.8 Support and updates

Overview

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

2.8.1 Download Base Unit log

How to download

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

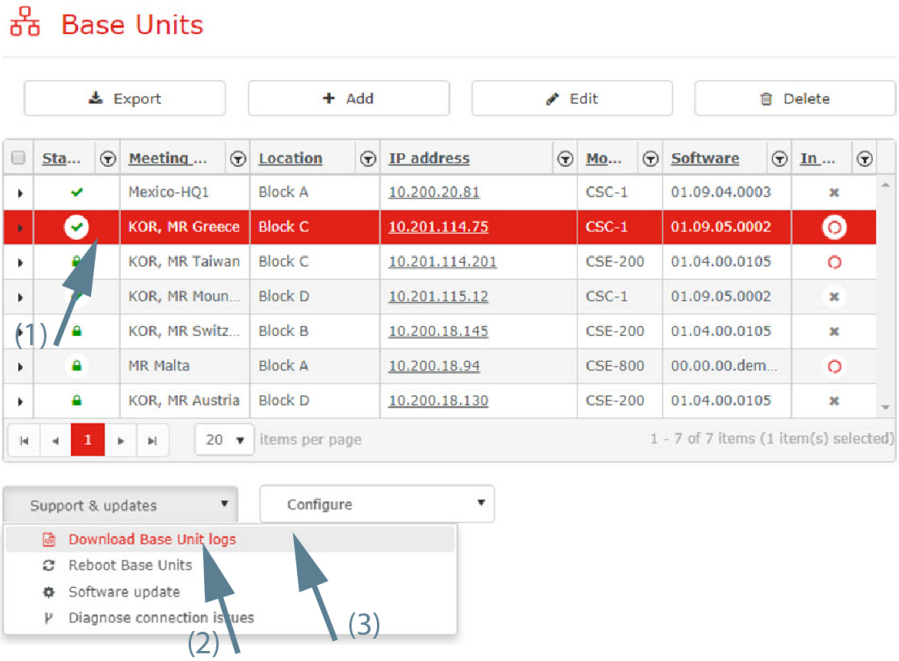

Image 2-13: Download Bas Unit logs

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 will be saved automatically on your PC.

2.8.2 Reboot Base Units

How to reboot

1. Select the Base Units to reboot (1).

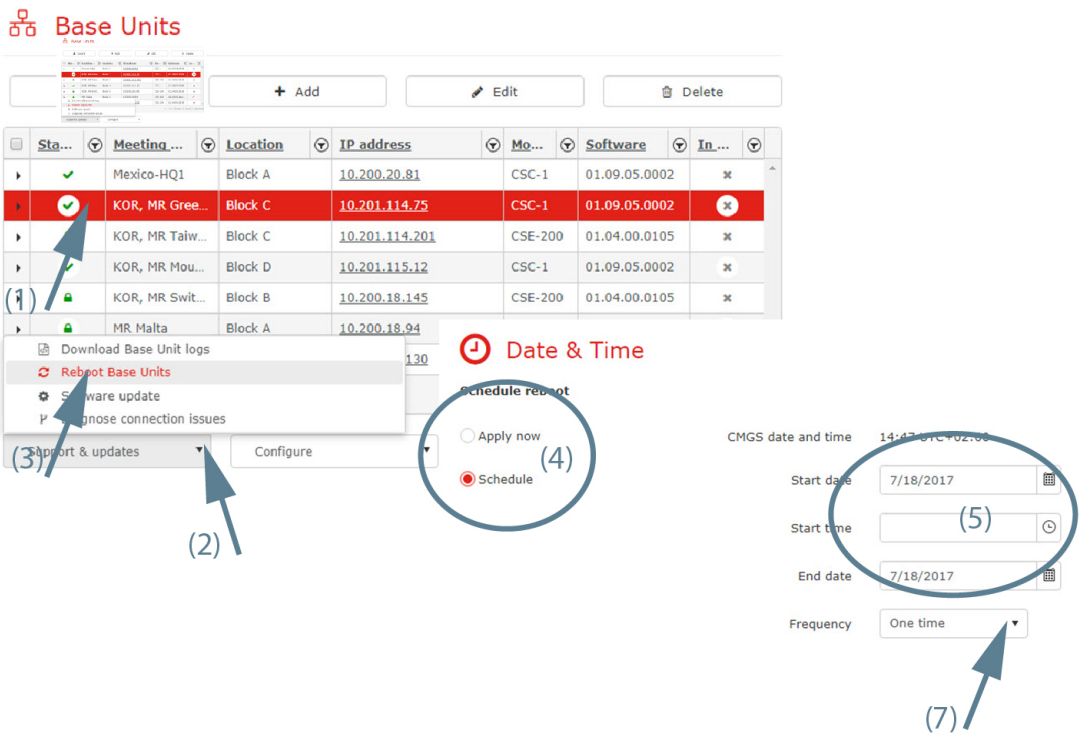

Image 2-14: Reboot Base Unit(s)

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

   A *Date & Time* page opens.

3. To reboot immediately, click **Apply now** (4).

   To reboot on a later date, click **Schedule** (4). Fill out a date and time (5)and click **Schedule** (7).

   Note: A schedule frequency can be entered. The following choices are possible: one time, daily, weekly, monthly or yearly.

2.8.3 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.

Before a firmware update can take place, the firmware must be available on the Collaboration Management Suite. For more info, see “Firmwares”, page 90

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.

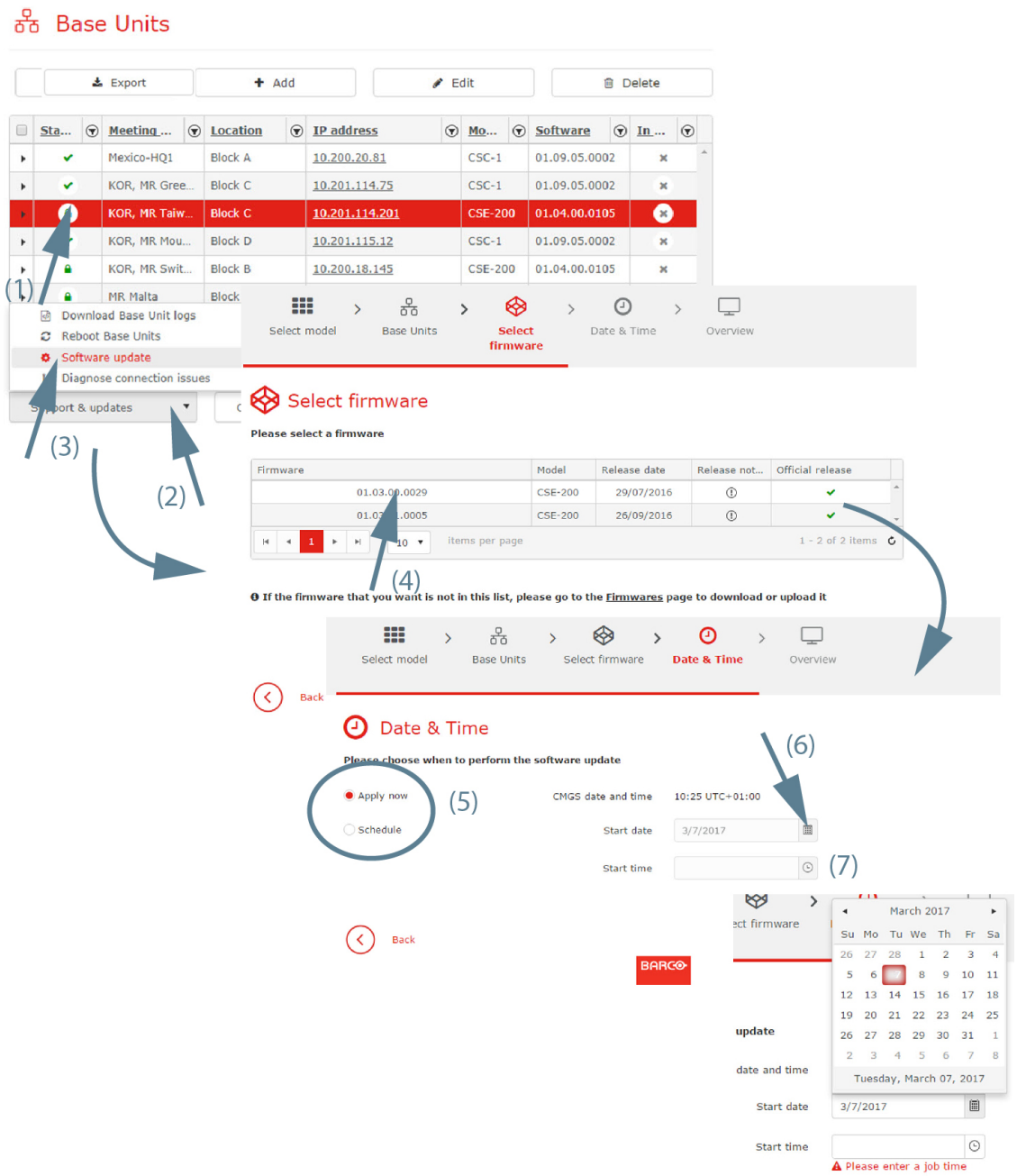

Image 2-15: Software updates

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.

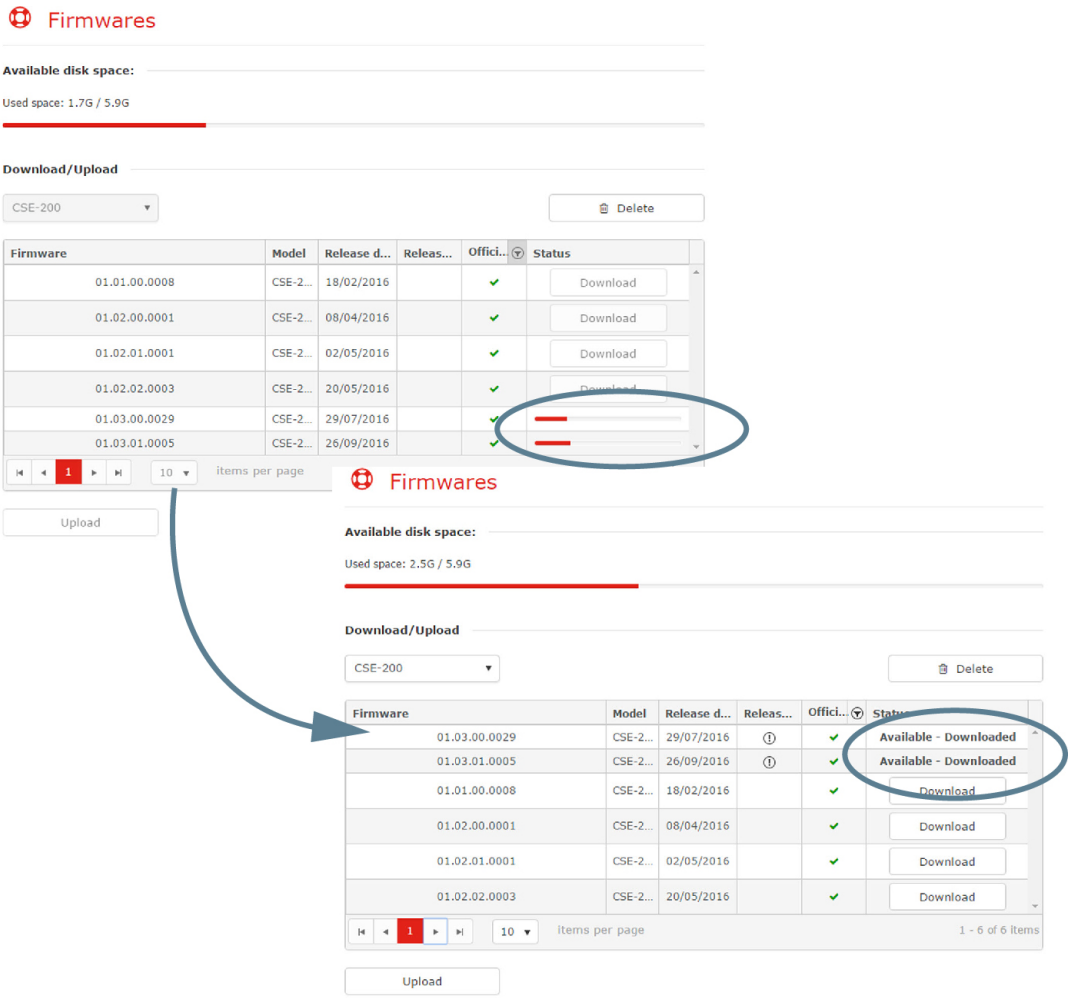

Image 2-16: Firmware download

The download starts.

2.8.4 Diagnose connection issues

How to start the diagnose

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

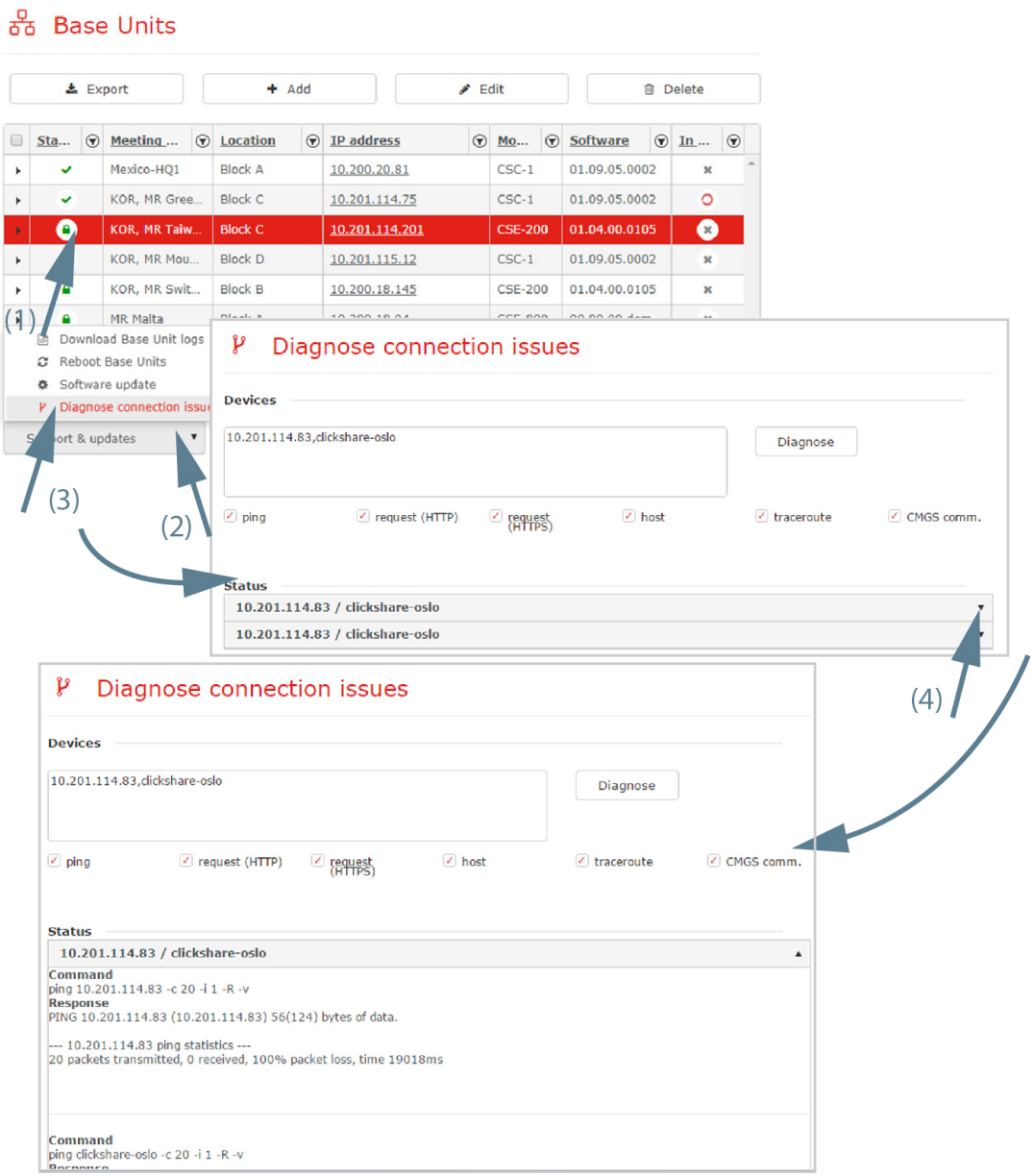

Image 2-17: Diagnosis connection issues

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. 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**.

2.9 Configure

Overview

- Clone Base Unit configuration

- Wallpaper

2.9.1 Clone Base Unit configuration

What can be done?

The current configuration of a Base Unit can be implemented on other Base Units of the same model.

How to clone

1. Select the Base Unit to clone (1). Select only a Base Unit with status OK.

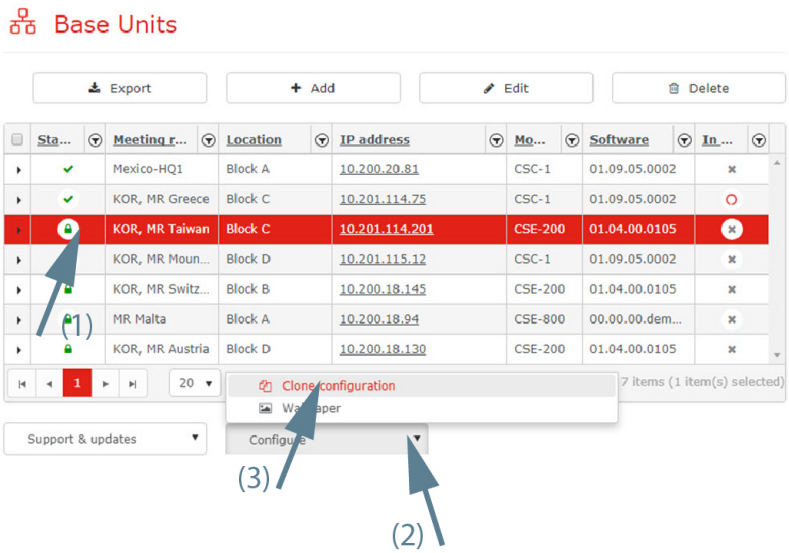

Image 2-18: Clone Base Unit configuration

2. Click on the drop down next to *Configure* (2) and select **Clone configuration** (3).

   The Customization window opens.

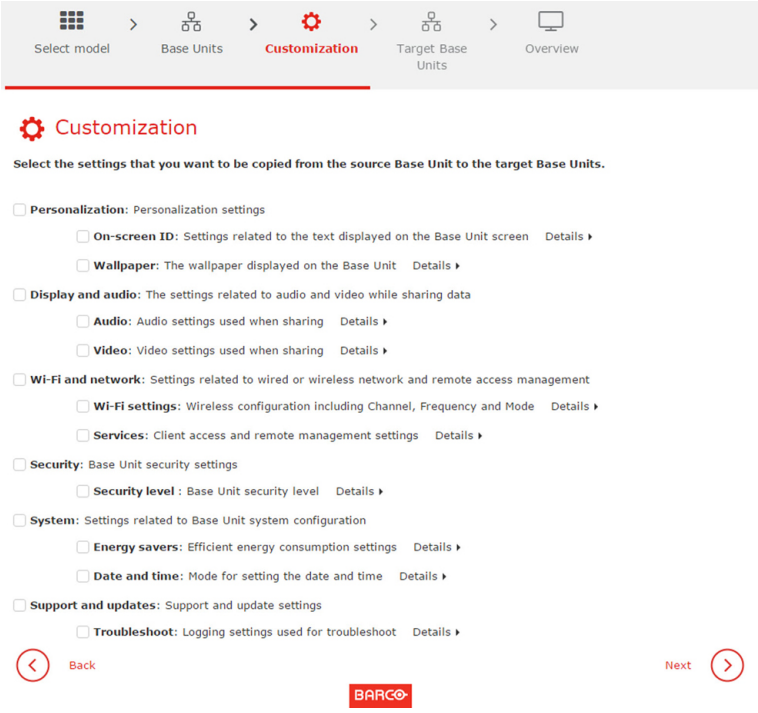

Image 2-19: Customization

3. Check the items to be cloned and click **Next**.

Download of configuration file from the selected Base Unit is started and it will take some time. After a successful download a window with the current possible target Base Units will open.

Image 2-20: Select Target Base Units

4. Select the Target Base Units and click **Next**.

   The configuration file previously downloaded is copied to the target Base Units. The Base Units will reboot after the configuration is copied onto them.

> Some changes will also require a re-pairing of the button. E.g. security level. A warning message will be displayed at the end of the wizard.

2.9.2 Wallpaper

About wallpaper

When a ClickShare device starts up, a background (wallpaper) is displayed. By default a general ClickShare and a quick start wallpaper are available. The possibility exists to upload personal backgrounds (wallpapers). A selected wallpaper is shown in the preview pane before it is applied.

Wallpaper setup

1. Select one or multiple Base Units (1).

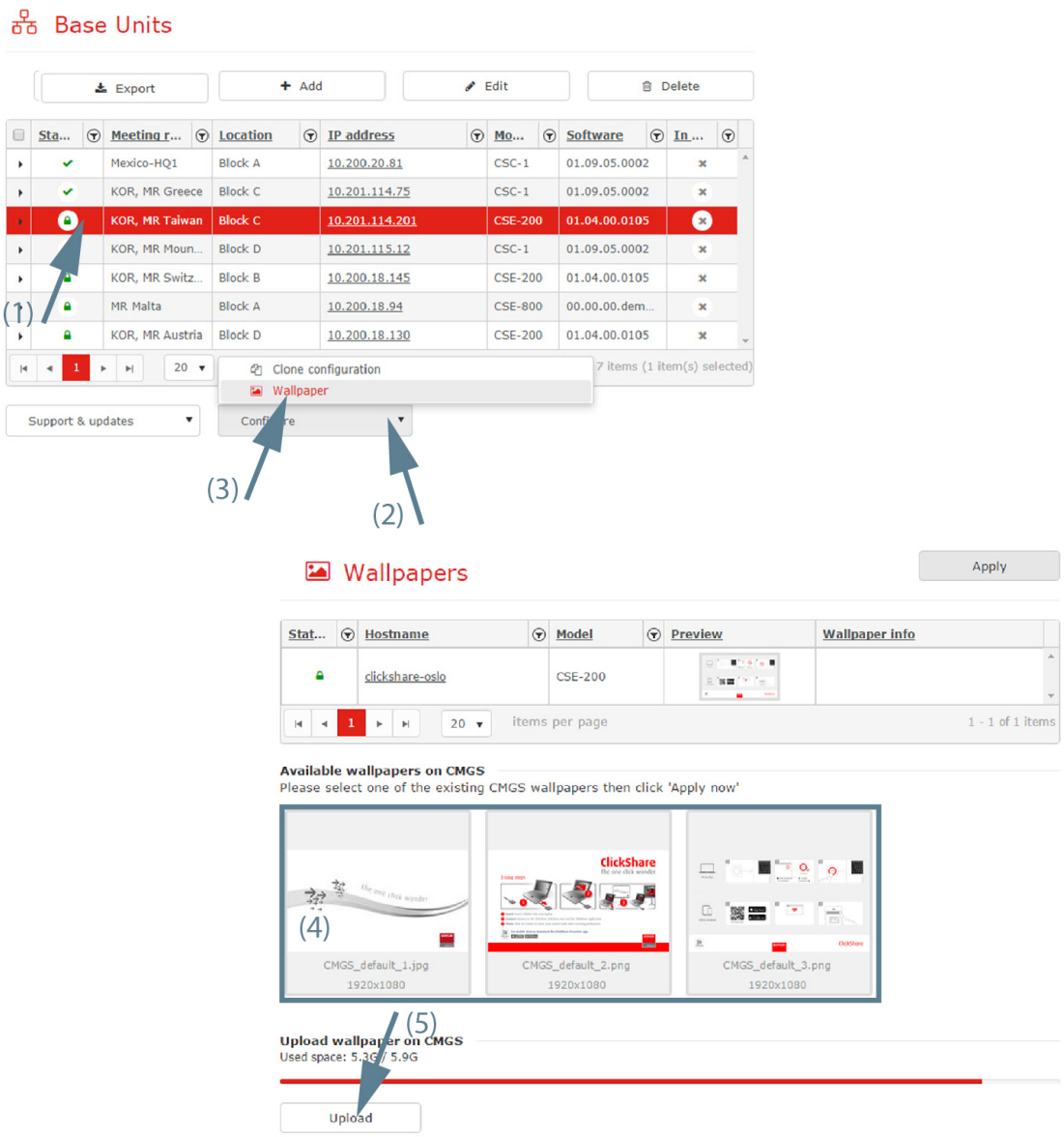

Image 2-21

2. Click on the drop down next to *Configure* (2) and select **Wallpaper** (3).

   The wallpaper selection window opens. The current available wallpapers in Collaboration Management Suite are displayed.

3. Select one of the available wallpapers and click on **Apply now**.

   The wallpaper file is sent to the Base Units.

   A message in the *Wallpaper info column* appears to inform user that the wallpaper is updating.

   CMGS also deletes all previously user uploaded wallpapers to the base unit.

Upload a new wallpaper on the Collaboration Management Suite

1. Click on **Upload** (1).

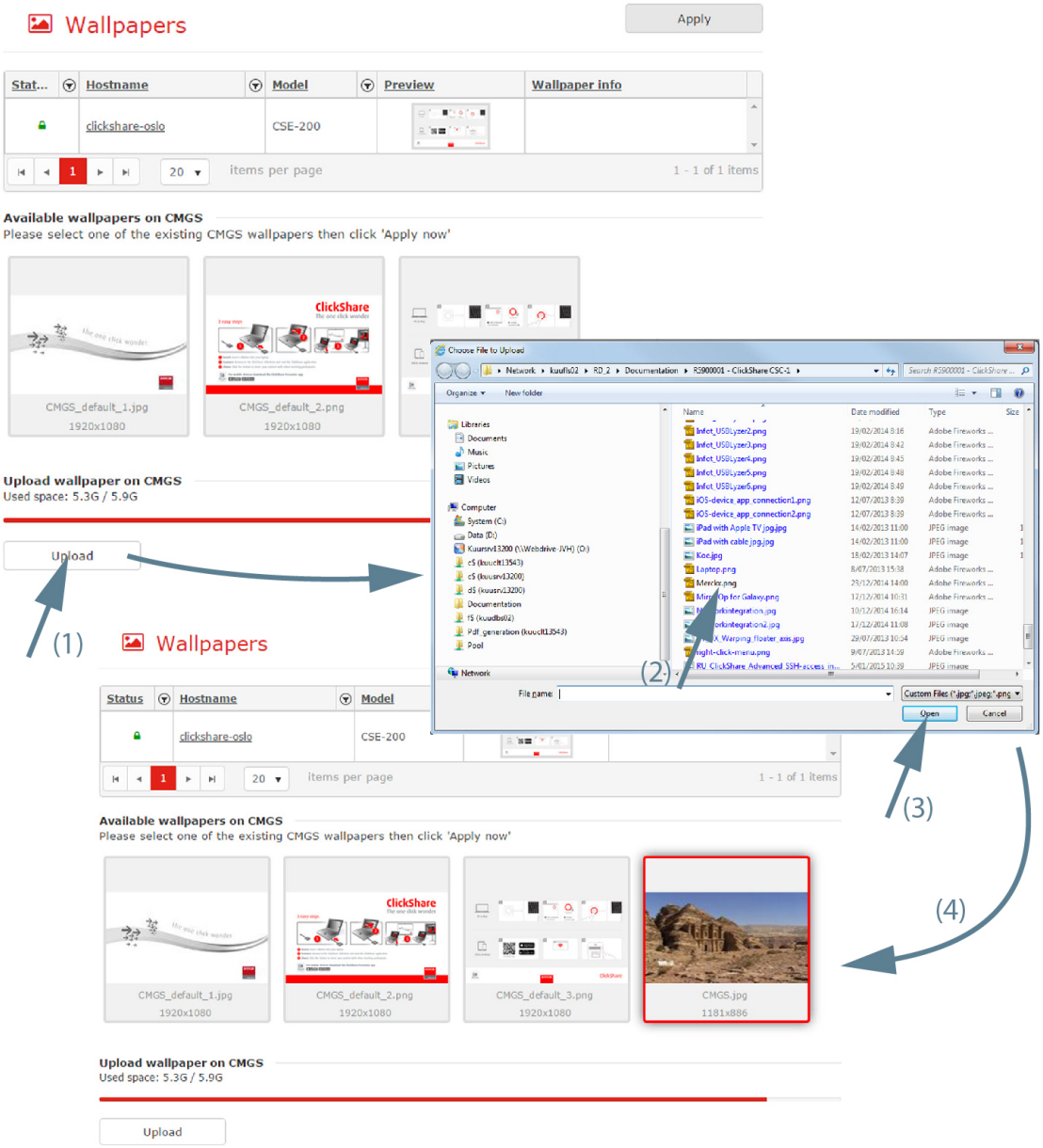

Image 2-22

A browser window opens.

2. Select the new wallpaper file (2) and click **Open** (3).

Note: The file type must be png, jpg or jpeg.

The new wallpaper file is added to the list of available files (4). This file can now be applied to a Base Unit.

The maximum allowed size for a wallpaper that can be uploaded on CMGS is 20 MB. Each base unit model may have different file size constraints. The maximum allowed resolution for a wallpaper applied to a

- CSE-200 : 1920x1200 px (2.50 MB)
- CSE-800 : 4096x2160 px (2.50 MB)
- CSM-1 : 1920 x 1080 px (2.50 MB)
- CSC-1 : 3840x2160 px (2.50 MB)

Custom uploaded wallpaper on the Collaboration Management Suite can be removed also.

Scheduler

3

Only for IT admin and 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** (1).

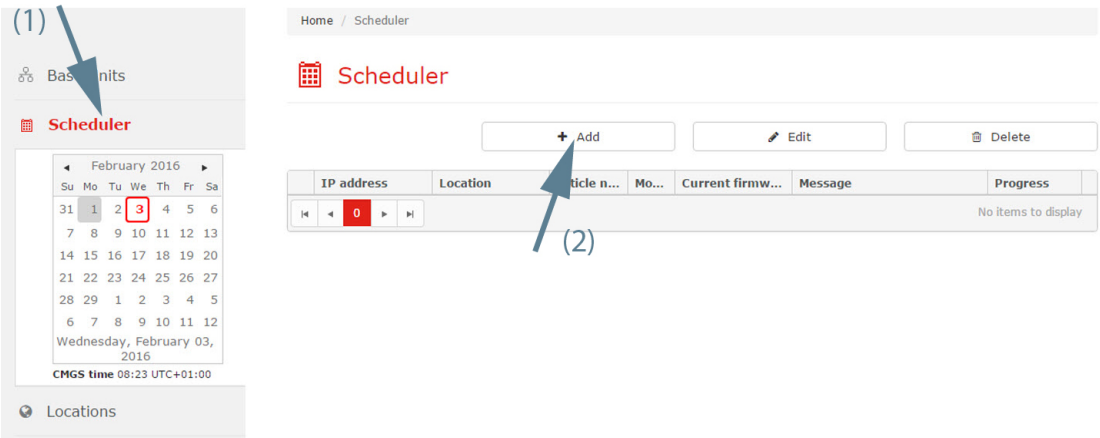

Image 3-1: Schedule new job

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. The user is able to change the month by clicking on the name of the current month. In order to view the daily calendar, the user should click on the name of the current date, located in the bottom of the calendar.

Gray highlighted number represents the current day. A red highlighted number represents the schedule date.

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

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

3. Follow the instructions as given in “Software update”, page 34 or “Reboot Base Units”, page 33. To finalize the procedure, check **Scheduler**.

4. To enter 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.

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

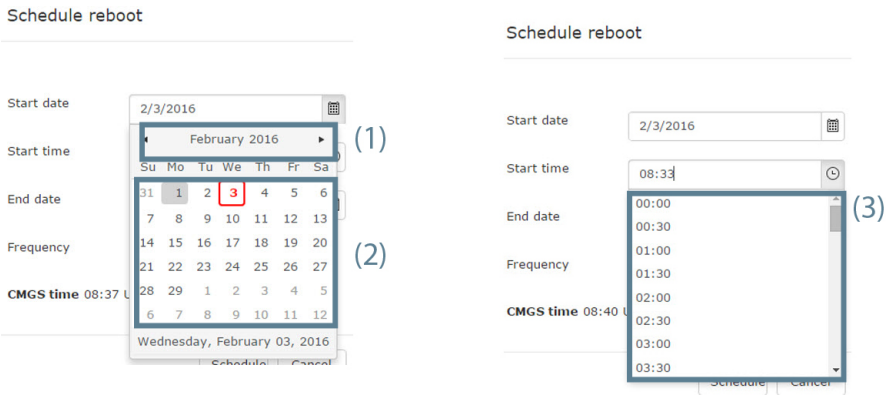

Image 3-2: Scheduler

   2. To change the day, click on the desired day in the calendar (2).
   3. To set the desired time comparing to the server time, click on the icon and select a predefined time (3).

   or
   enter the start & end date (mm/dd/yyyy) and time (hh:mm) by clicking in the input field and changing the values.

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.

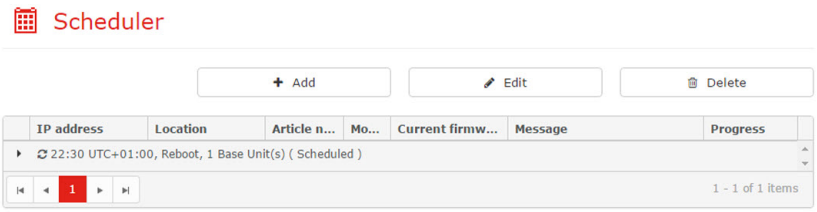

Image 3-3: Scheduler overview page

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 job can be rescheduled to a new time slot.

How to edit

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

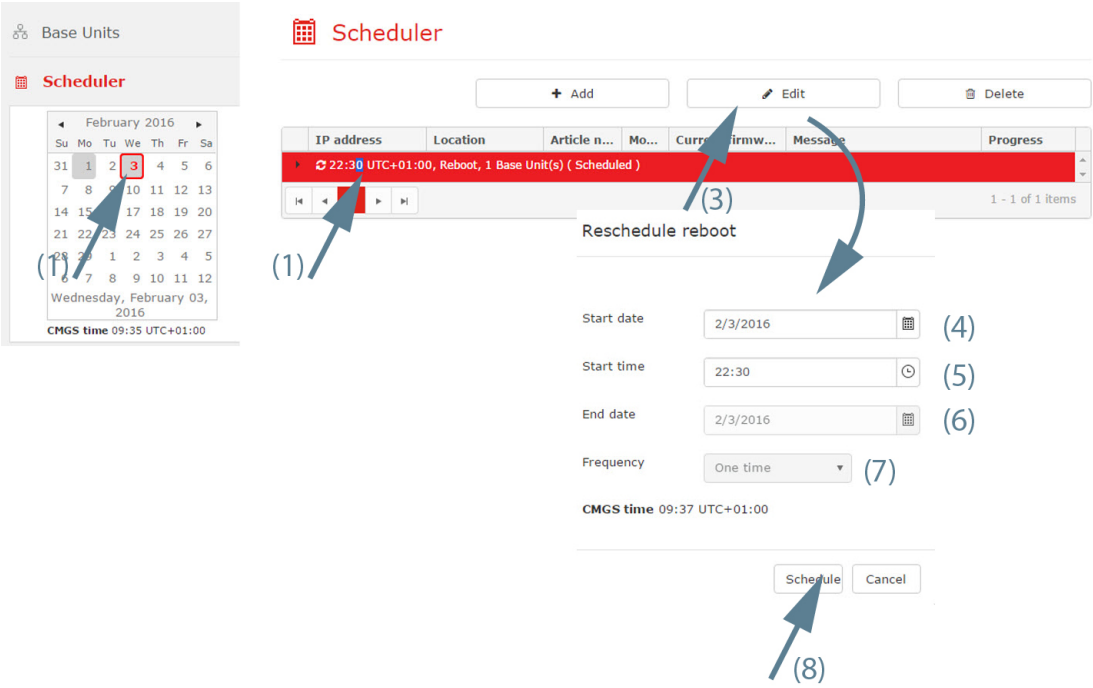

Image 3-4: Edit scheduled job

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 month and date where the job can be found (1) and select the job (2). (date means year/month/day)

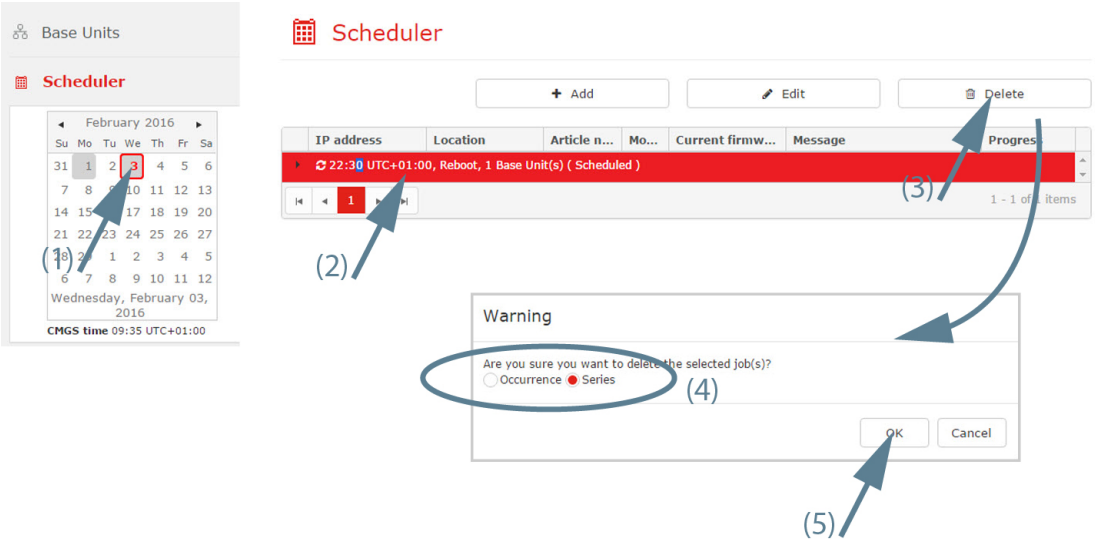

Image 3-5: Delete scheduled job

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).

Personalization

4

Overview

- User preferences
- Locations
- Configuration files

4.1 User preferences

How to setup

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

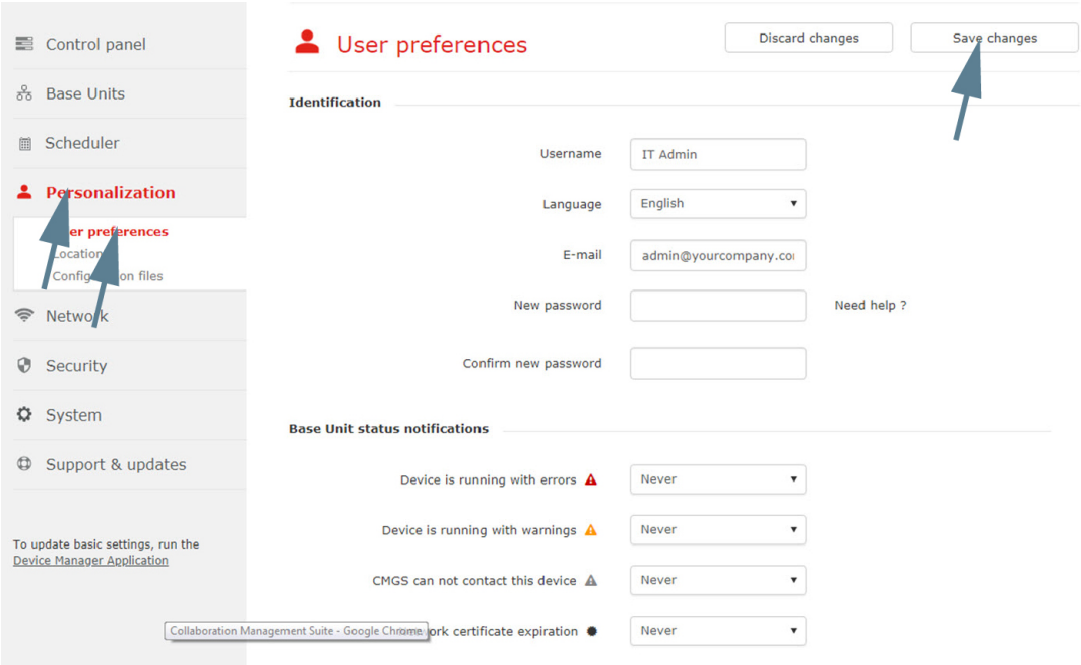

Image 4-1: User preferences

The current user preferences are displayed. Any changes can be made.

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.

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

4.2 Locations

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).

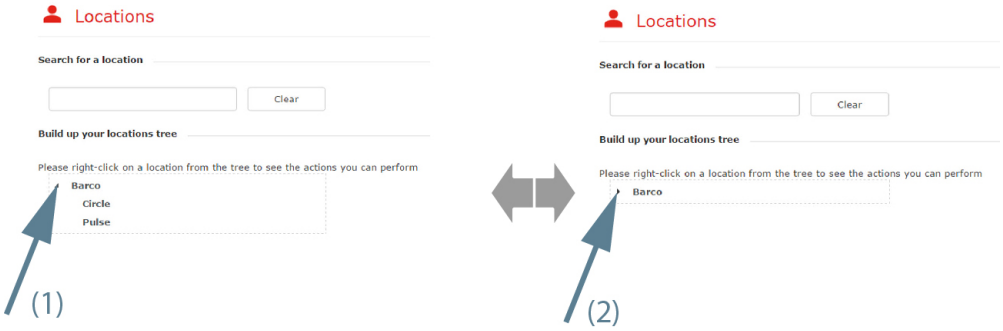

Image 4-2: Collapse/expand locations

Expand all

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

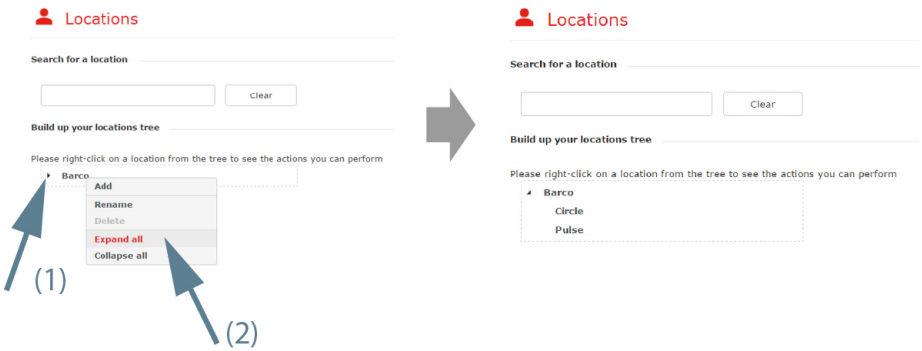

Image 4-3: Expand al

2. Select *Expand all*.

   The branch is expanded until its lowest level.

Collapse all

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

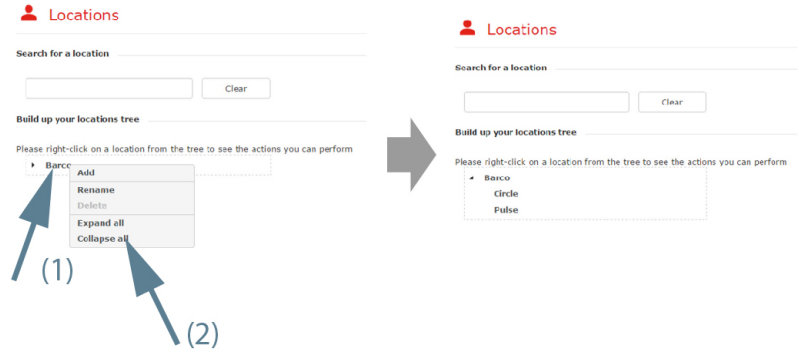

Image 4-4: Collapse all

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).

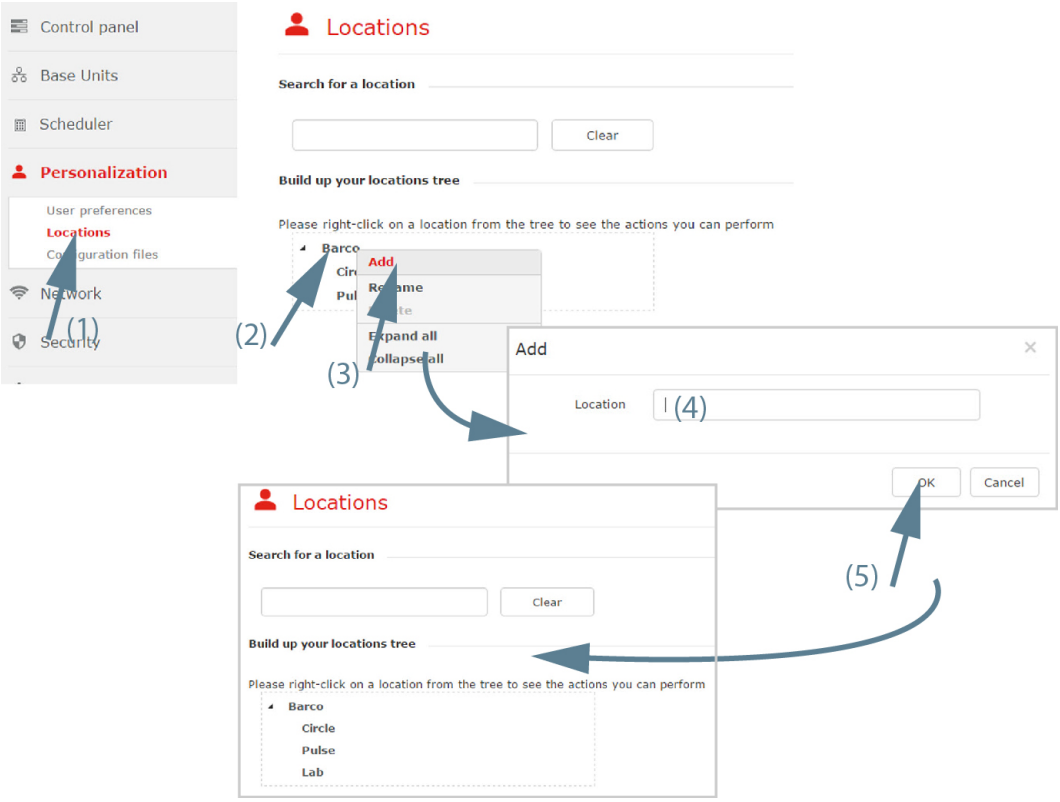

Image 4-5: Add new location

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).

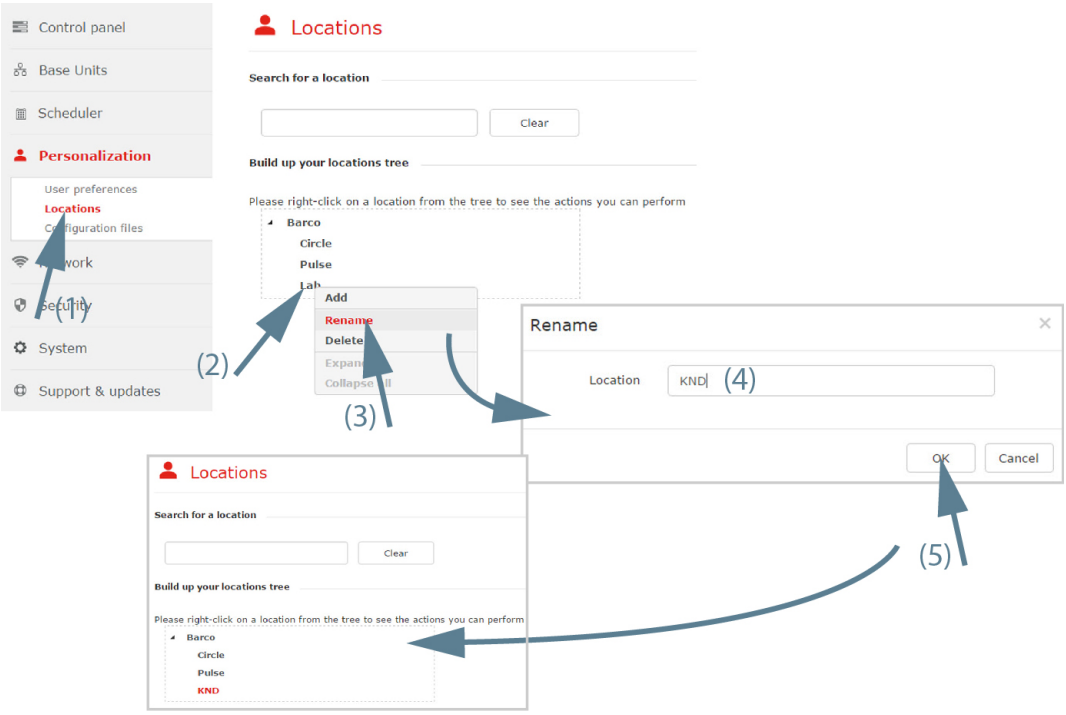

Image 4-6: Rename location

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

   A context menu opens.

3. Select *Rename* (3).

   The *Rename* window opens.

4. Edit the current displayed name for the location (4) and click **OK**.

   Note: It is not allowed to use the backslash character "\" in the location name.

The location tree and Base Units home are updated with the new name.

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).

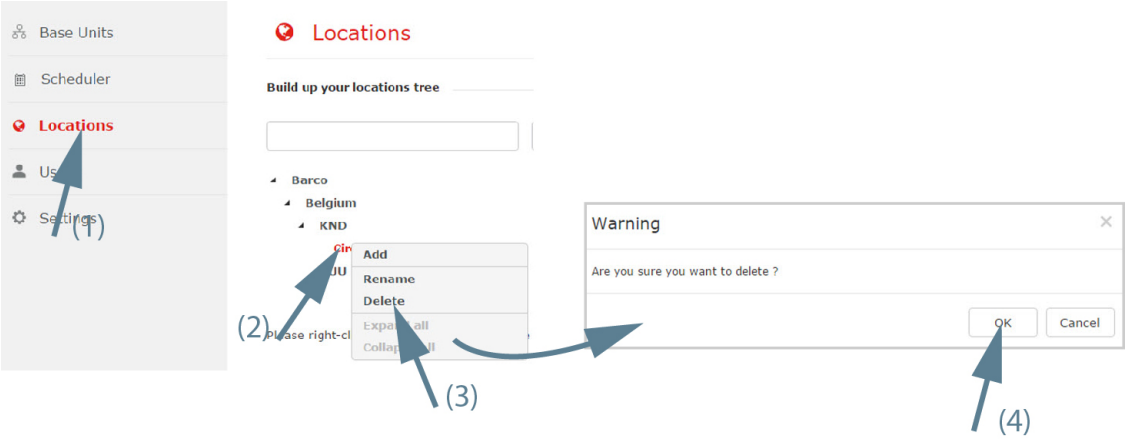

Image 4-7: Delete location

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).

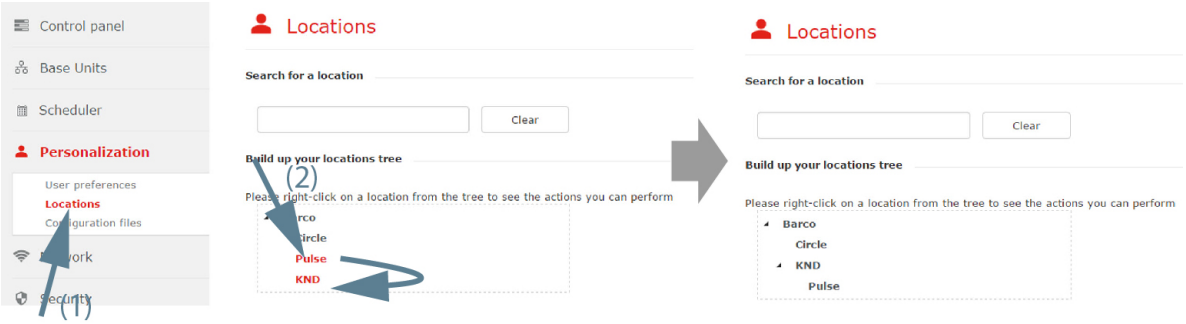

Image 4-8: Move location

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).

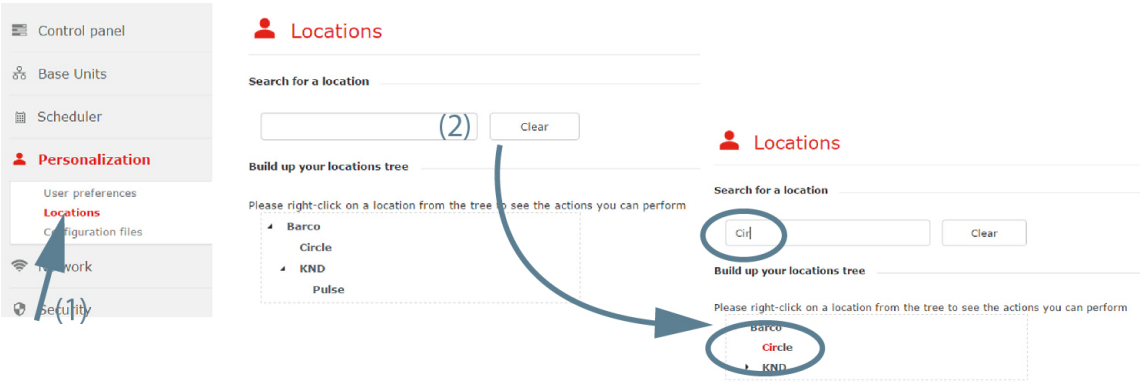

Image 4-9: Search for location

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 cloned (copied) 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**.

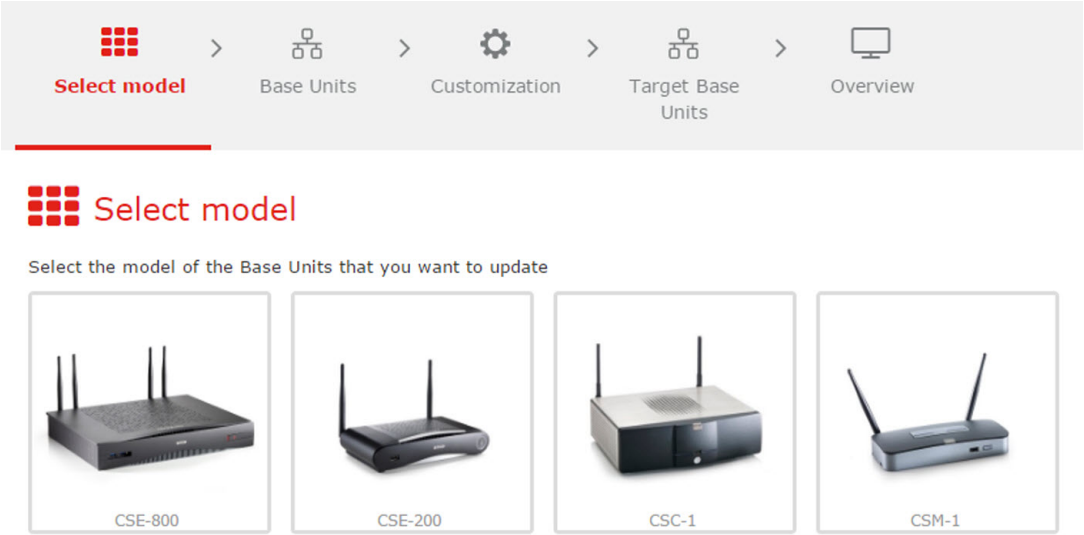

Image 4-10: Select model

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

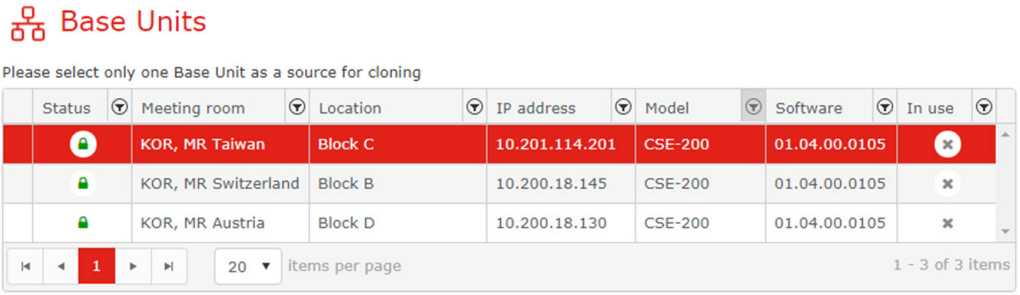

Image 4-11: Select Base Unit

5. Select the settings that you want to be copied from the Base Unit. Check the check boxes 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.

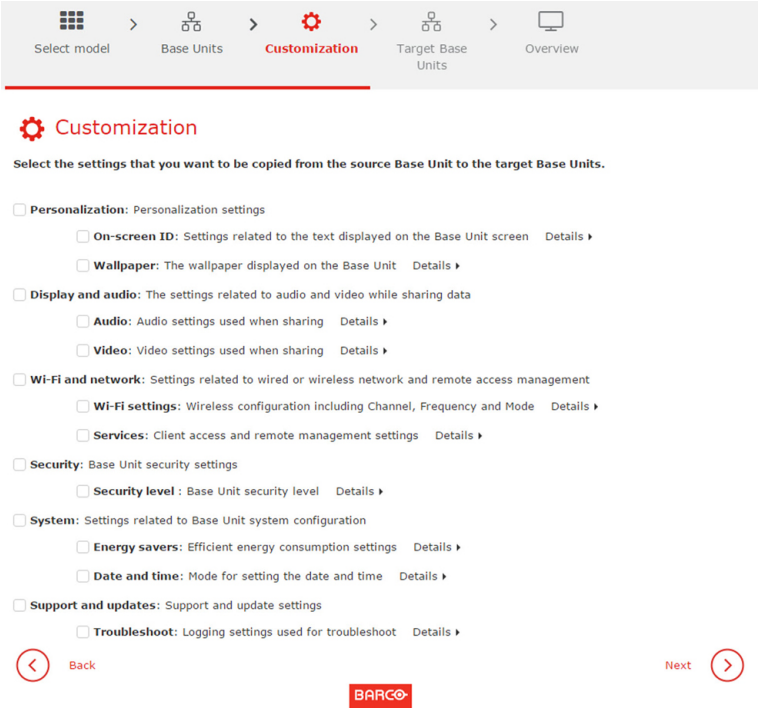

Image 4-12: Customization

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

Image 4-13: Select Target Base Units

Note: The target Base Units might 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.

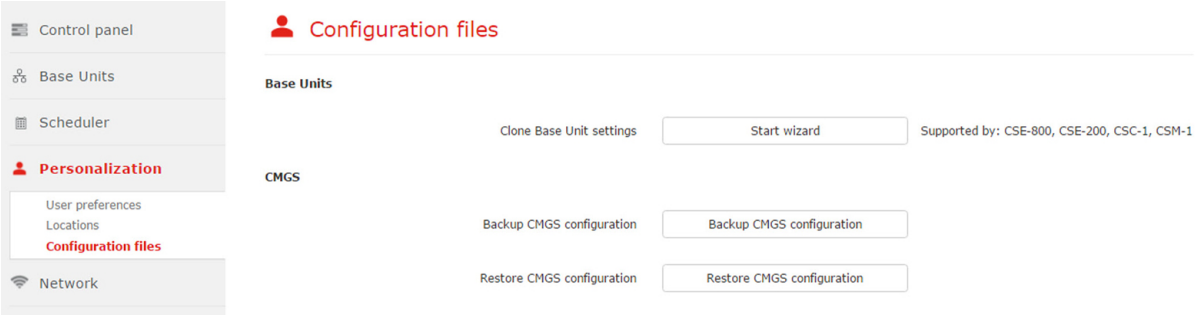

Image 4-14: Configuration files

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.

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.

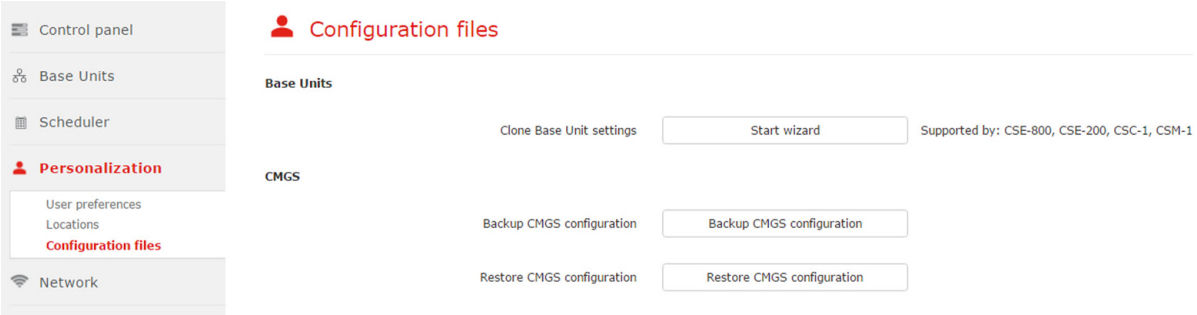

Image 4-15: Configuration files

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 (Base Units, users, roles, etc.). 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.

Network

5

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 webUI availability can be set via the WiFi.

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.

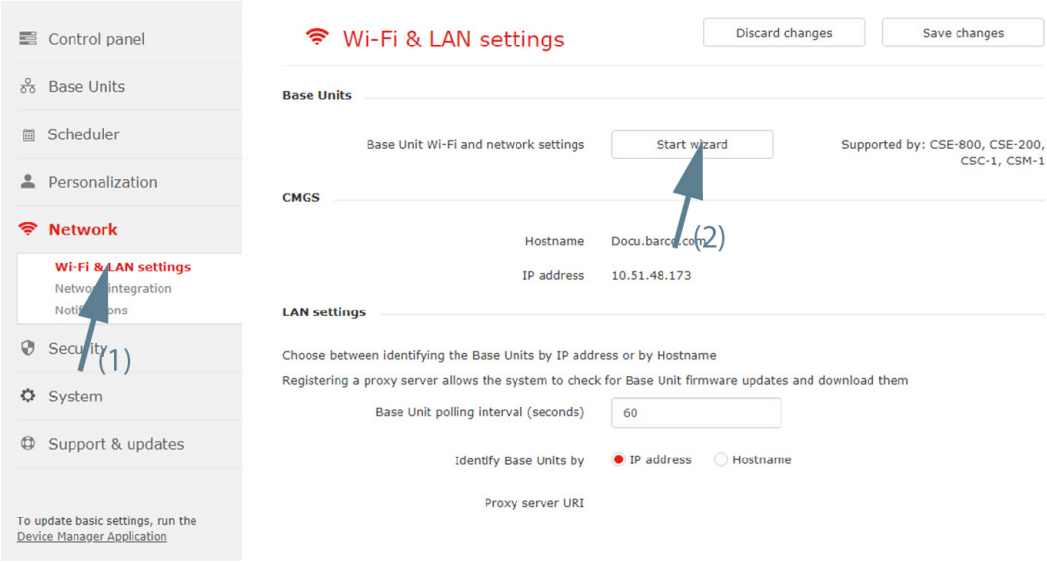

Image 5-1: Network, start wizard

2. Click on **Start wizard** next to *Base Unit Wi-Fi and network settings* to start.
3. Select the Base Units. Click **Next** to continue.

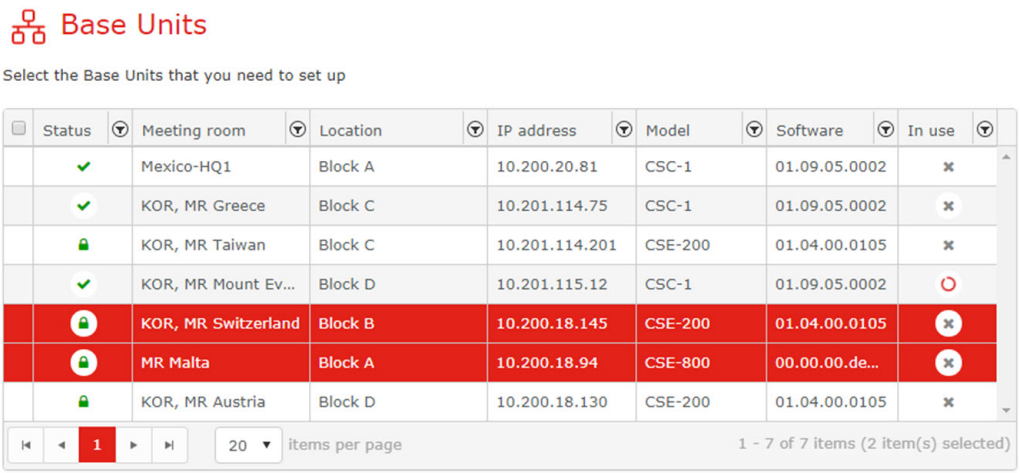

Image 5-2: Base units to setup

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.

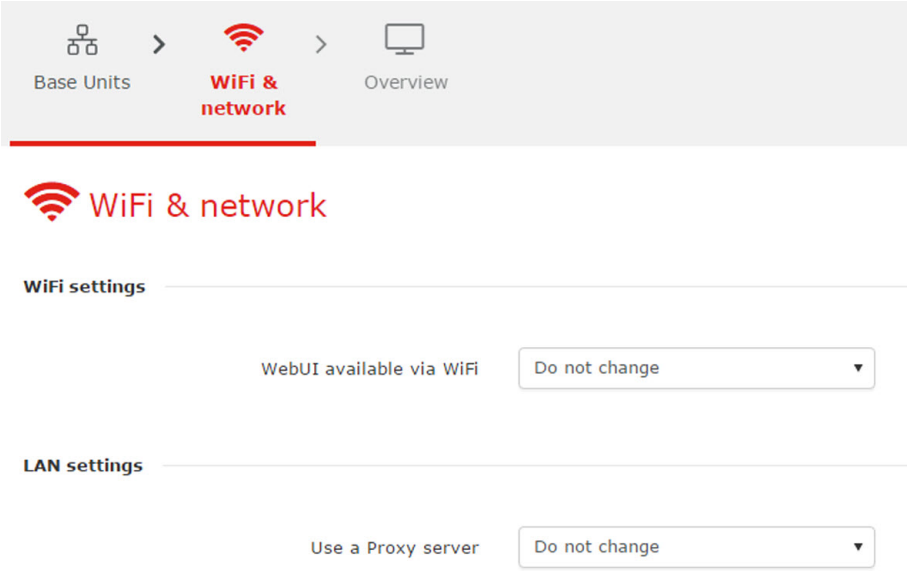

Image 5-3: Network, WiFi and LAN settings

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 proxy settings below. Proxy server uri

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

6. Enable or disable remote Button pairing.

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

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

5.2 LAN settings

How to set

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

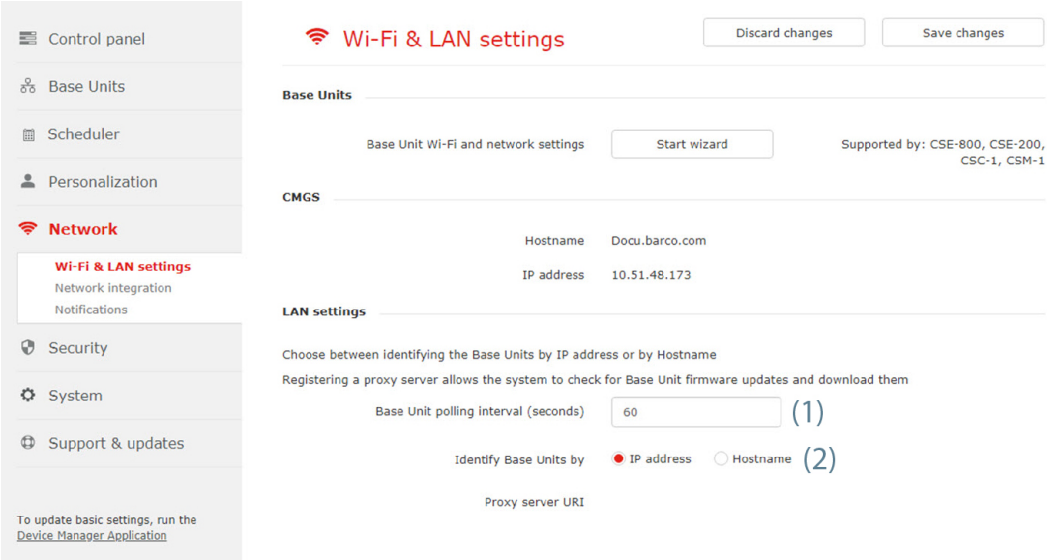

Image 5-4: Network, LAN settings

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 (limitation between 30s and 6h) (1).
3. To setup the identification of the Base Units, check the radio button of your choice (2).

   The following choices are possible:
   - IP address
   - hostname
4. 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. Additionally, 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 and removes TKIP 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 112 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).

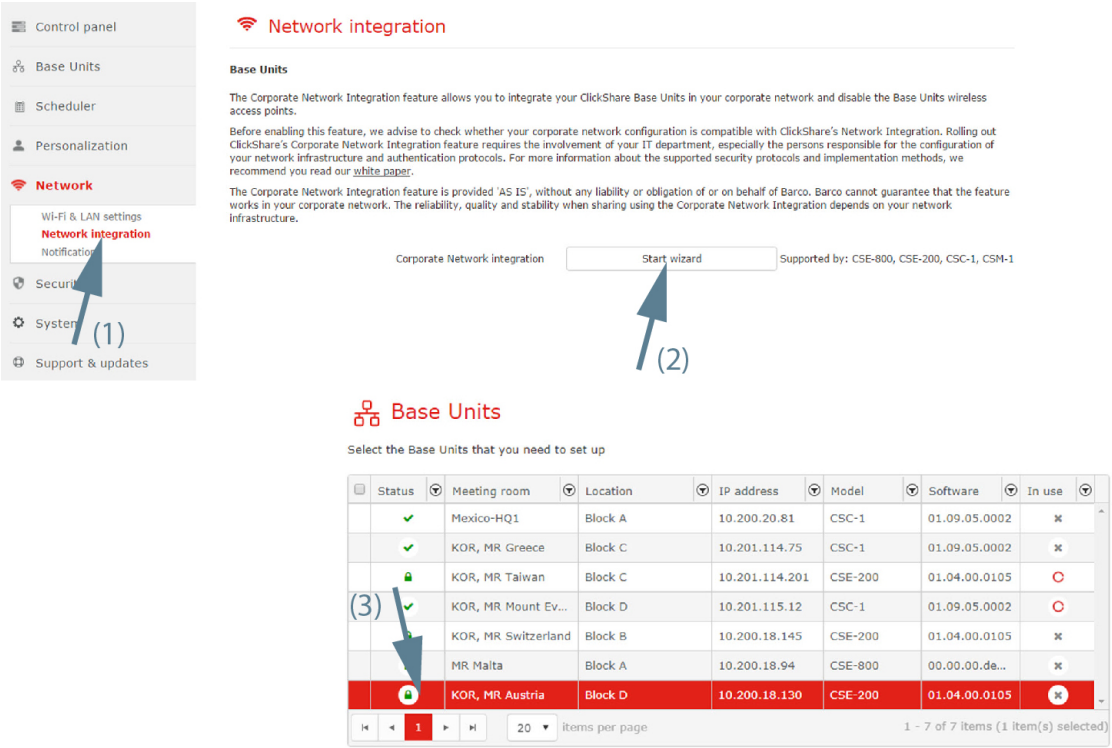

Image 5-5: Network integration, start wizard

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.

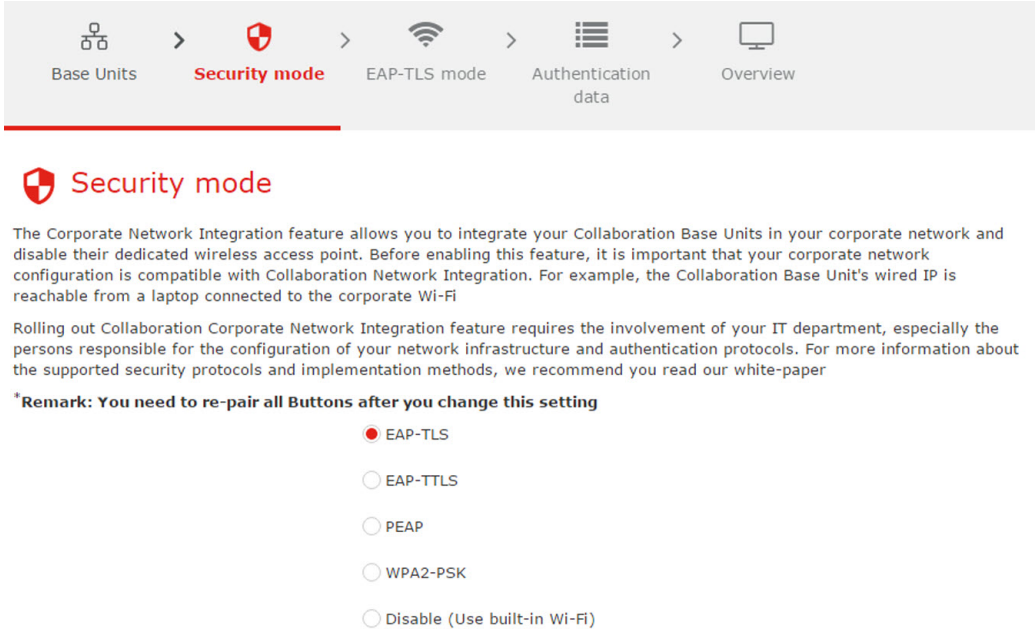

Image 5-6: Network integration, security mode

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.

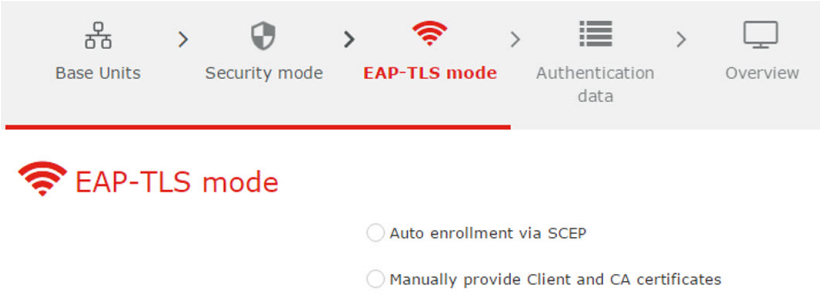

Image 5-7: EAP-TLS mode

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.

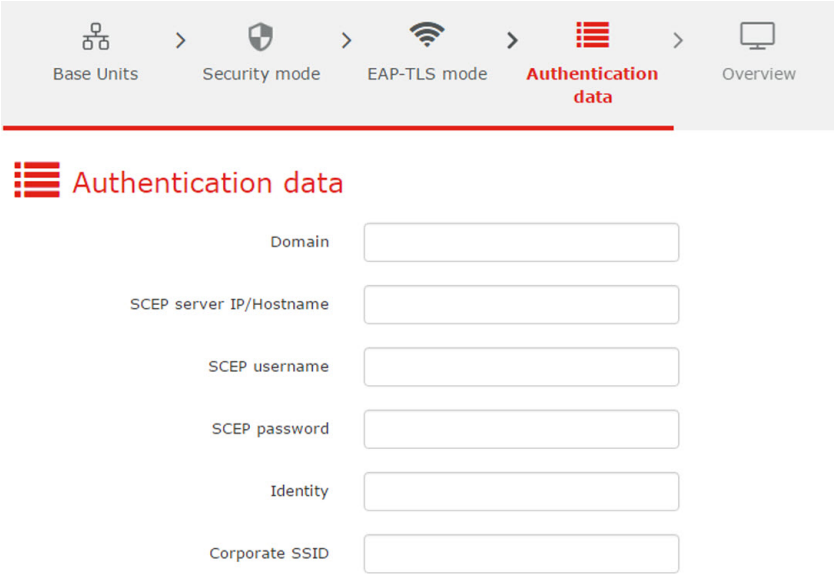

Image 5-8: SCEP, authentication data

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[4]. 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.

4: 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

Using manually upload of certificates

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

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.

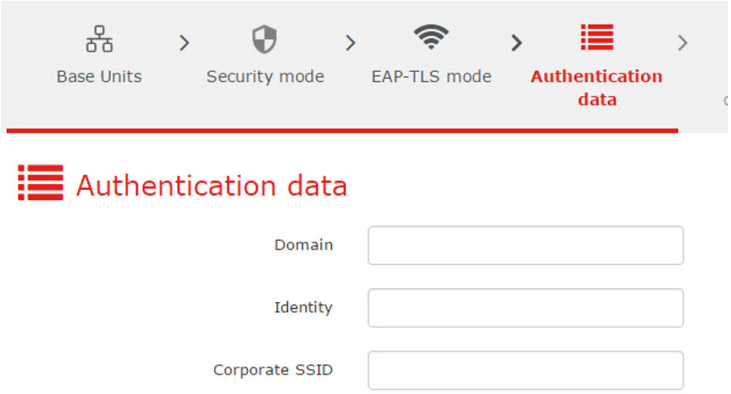

Image 5-9: Manually upload

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 format 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.

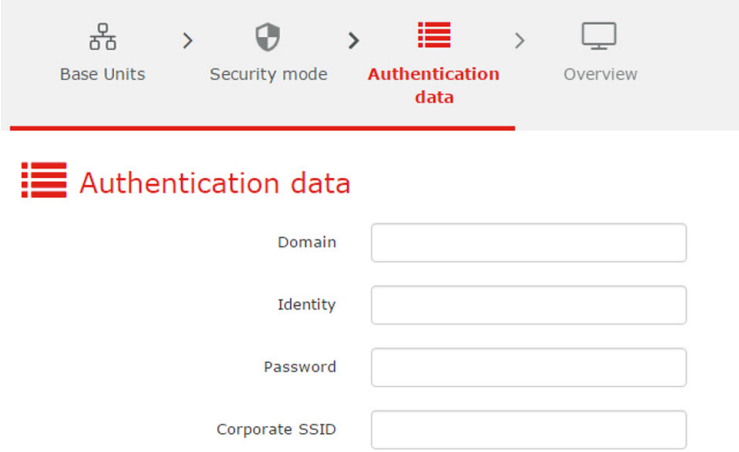

Image 5-10: EAP-TTLS

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.

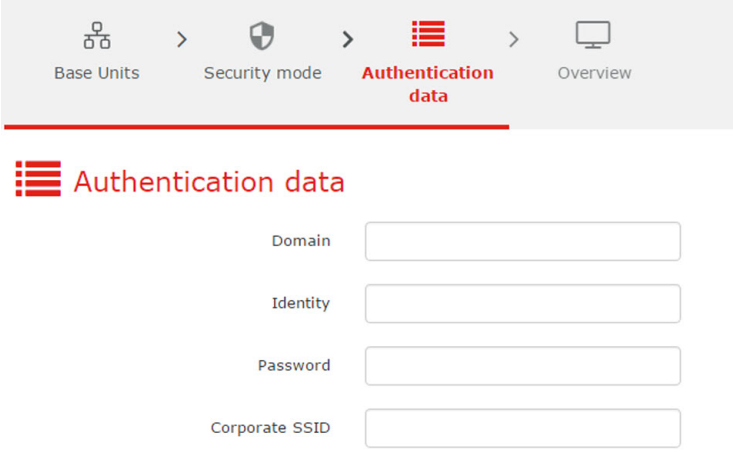

Image 5-11: PEAP, authentication data

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:

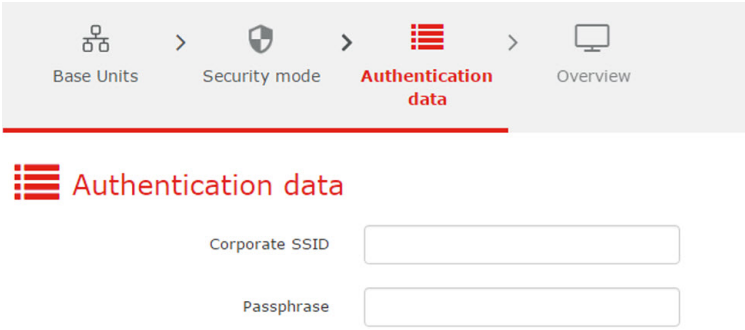

Image 5-12: WPA2–PSK, authentication data

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

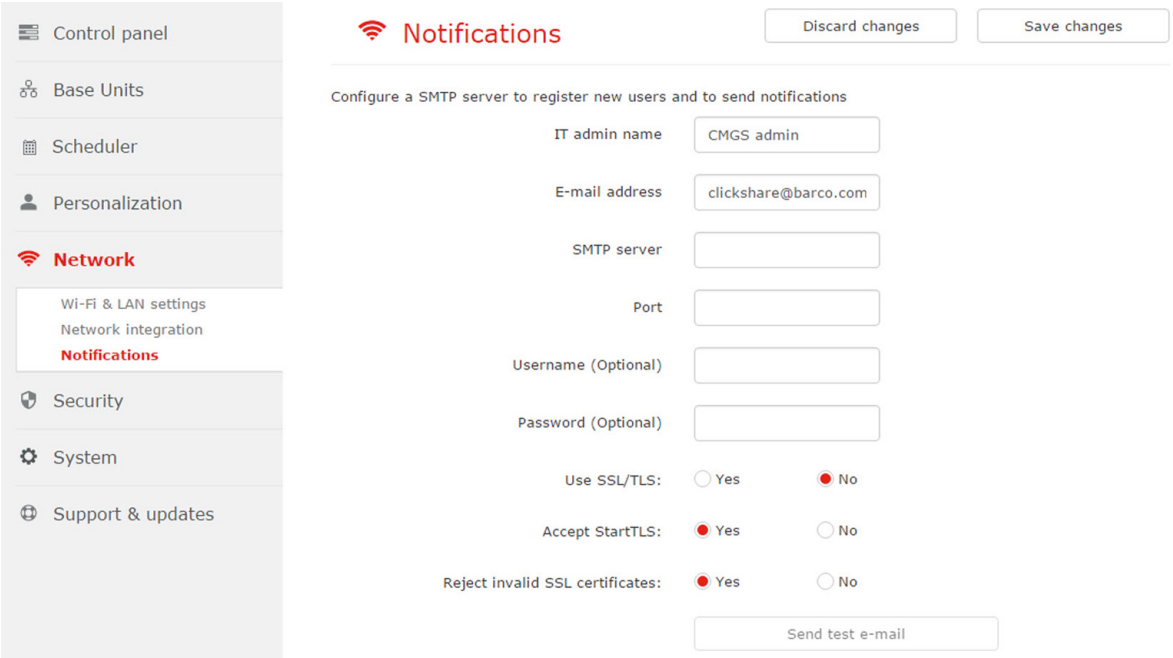

Image 5-13: Notifications

IT admin name: name used to send out notifications.

E-mail address: address used to send out notifications

SMTP parameters

SMTP server	Hostname or IP address 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.

Security

6

Overview

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

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**.

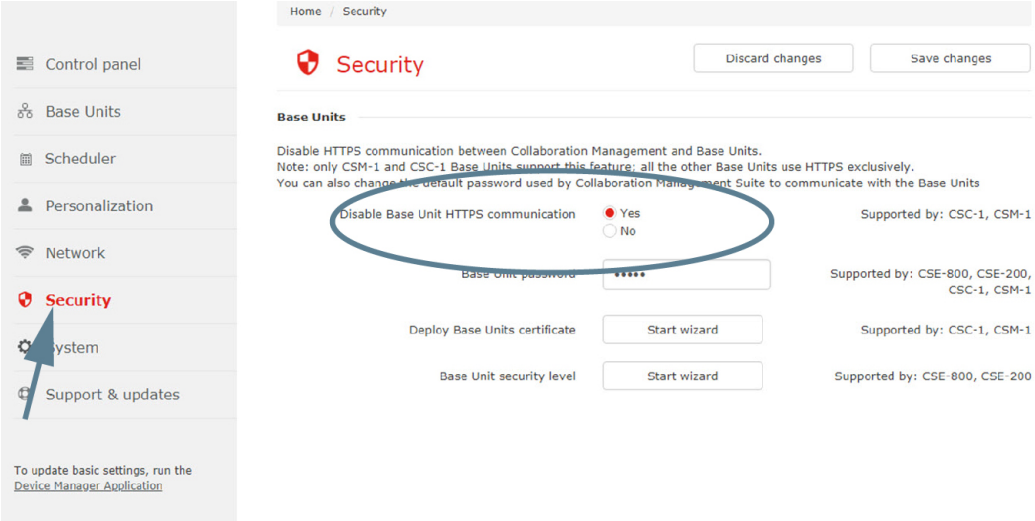

Image 6-1: Security, HTTPS communication

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

About Base Unit password

The Base Unit password field from the Security page is the password used for communication between the Collaboration Management Suite and the Base Unit. It is part of the REST API password. Changing this only changes the communication password. It does not change the base unit set password or ensure that the Collaboration Management Suite will be the only application able to communicate and change settings on Base Units.

Set password

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

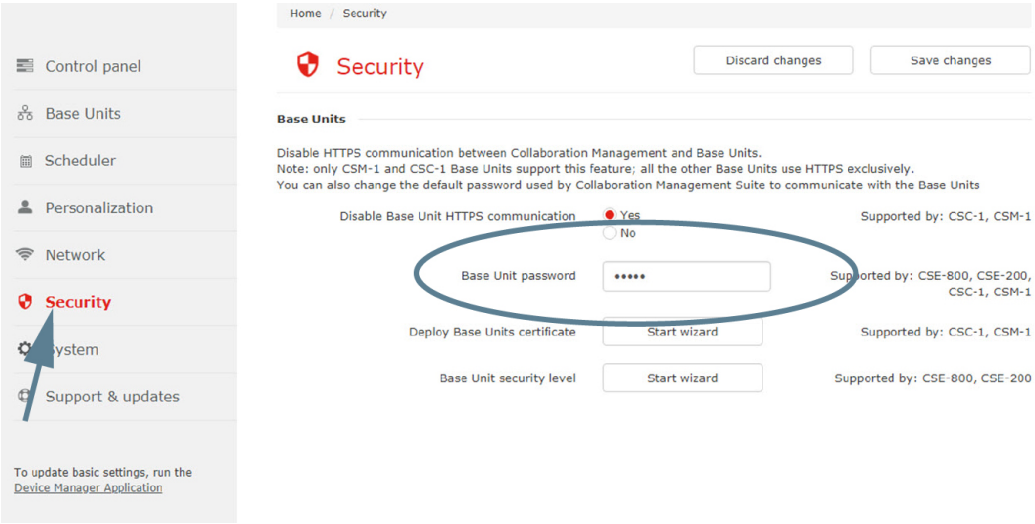

Image 6-2: Security, Base Unit password

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).

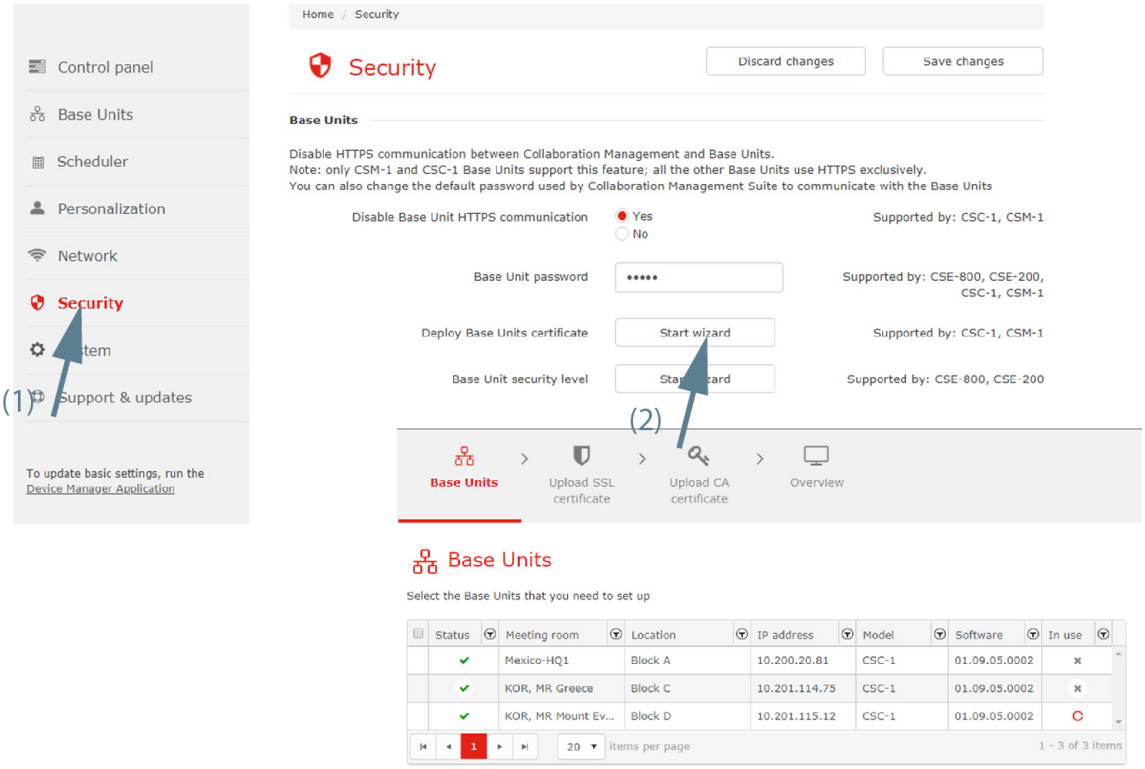

Image 6-3: Security, Base Unit certificate

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.

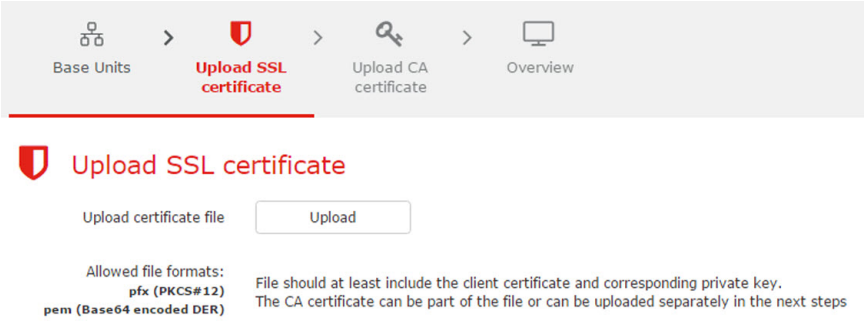

Image 6-4: Upload SSL certificate

5. Upload CA certificate. Enter password.

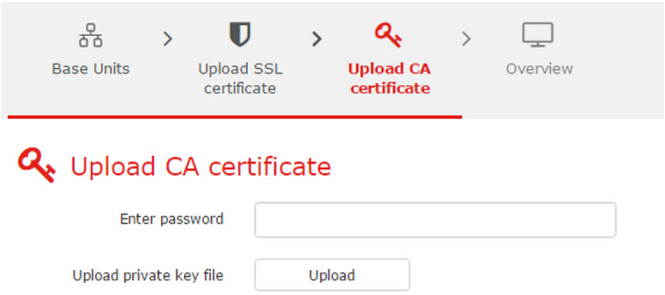

Image 6-5: Upload CA certificate

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).

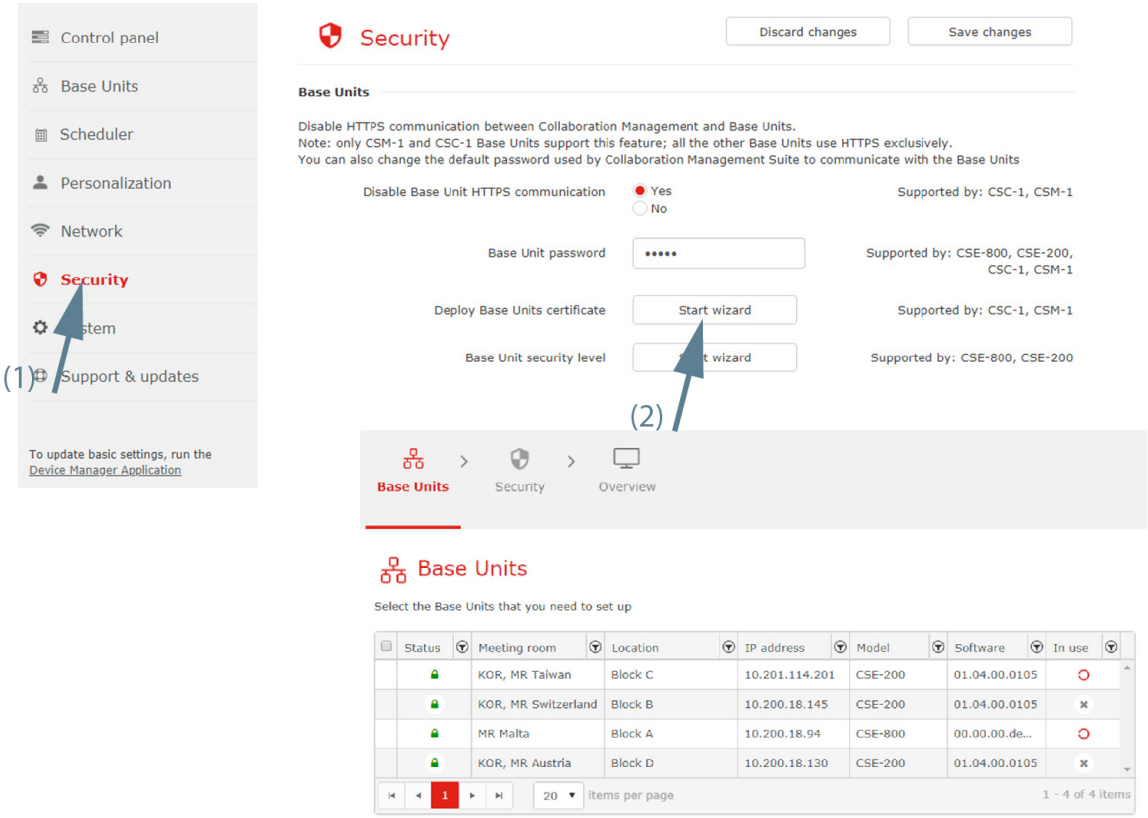

Image 6-6: Base Unit security level, start

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).

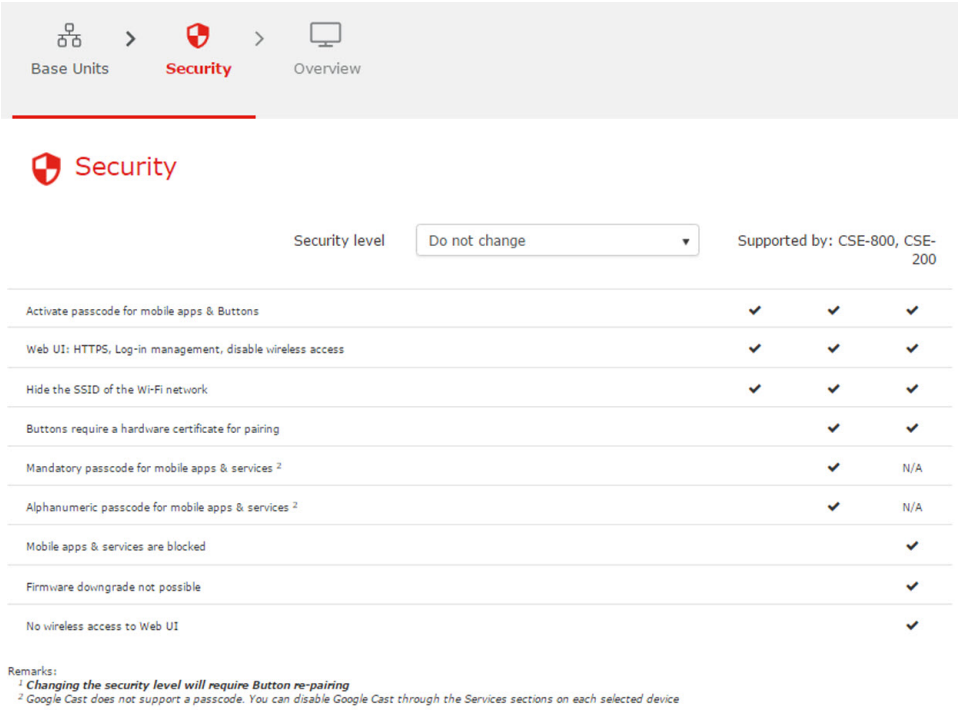

Image 6-7: Base Unit security

5. Click **Next** to continue.

An *Overview* window is displayed.

6. Click **Finish**.

System 7

Only for IT admin user.

Overview

- Date & Time
- Buttons
- Users
- User roles
- User activity

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).

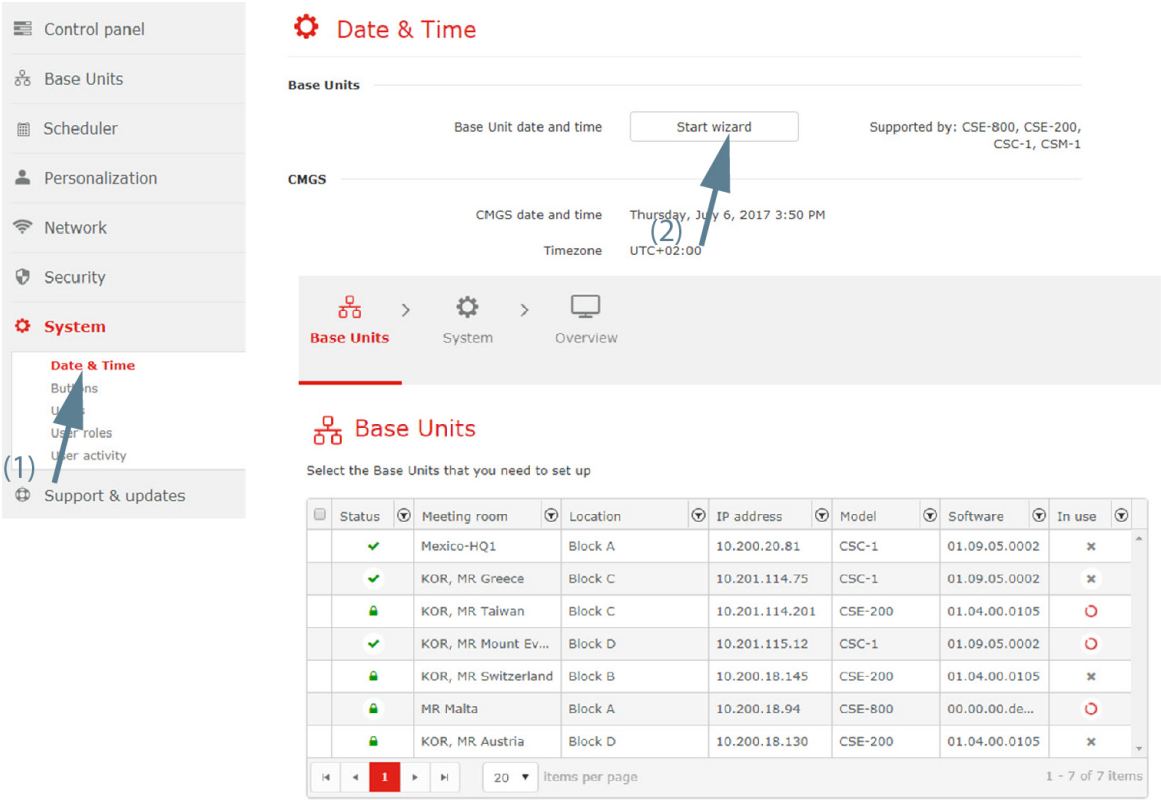

Image 7-1: Date & time, start

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*.

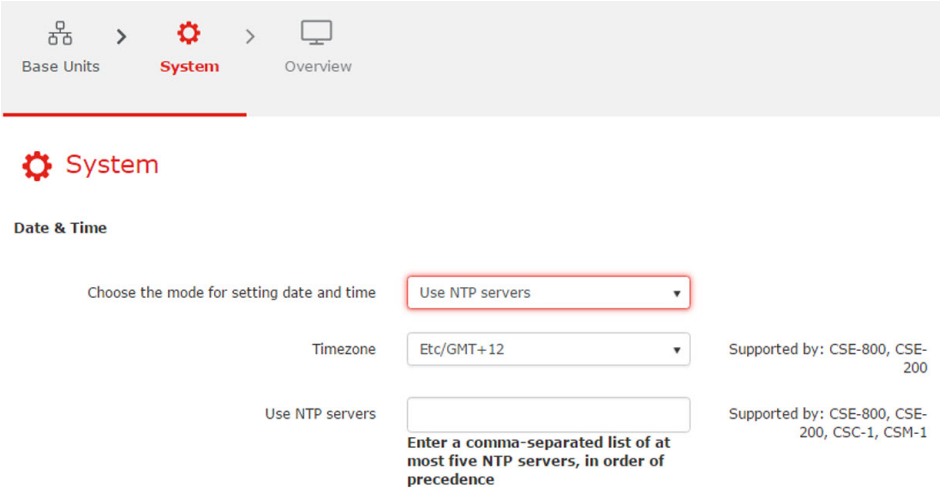

Image 7-2: NTP server

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*.

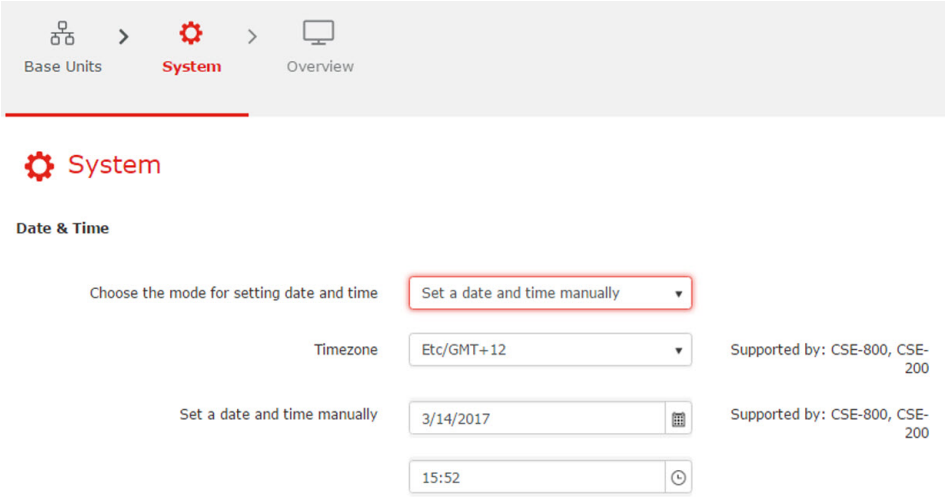

Image 7-3: Manually setup

2. Click on the drop down box next to Timezone and select the corresponding time zone.
3. Click in the date field, select the current value and enter a new value. Use the following mask *dd/mm/yyyy*.

   or

   click on the icon next to the input field and select a month and a day. The current date is indicated with a red background.

   To change the month, click on the right or left arrows next to the month name until the desired month and year are obtained. To select the day, click on a number in the number field.

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).

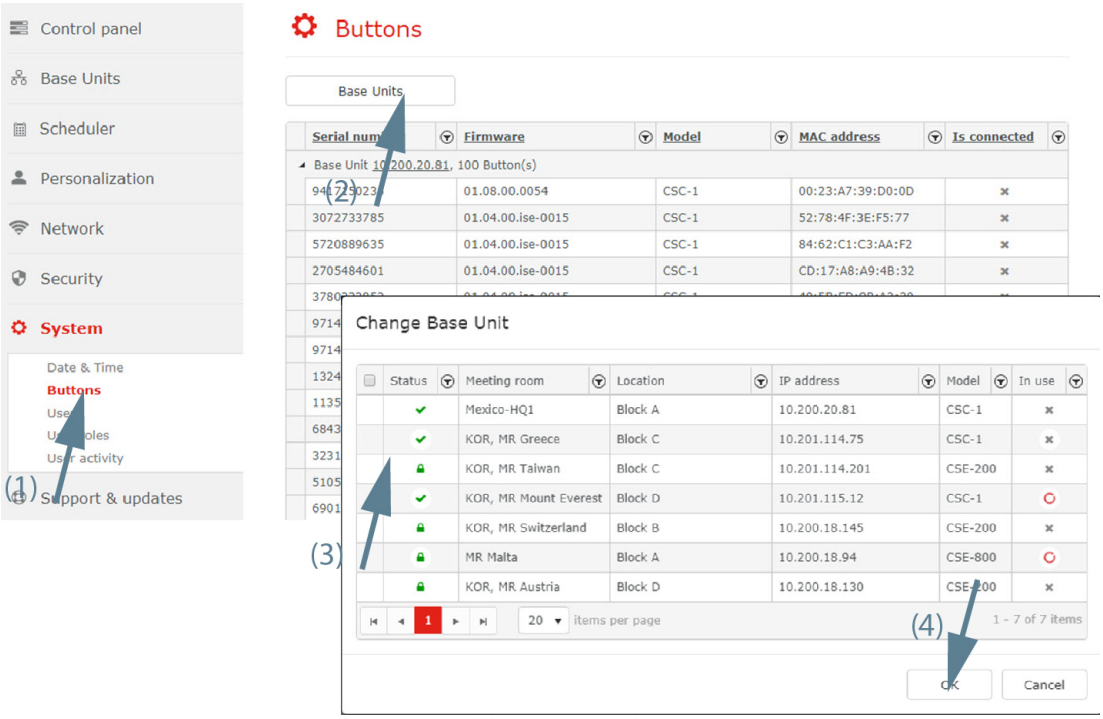

Image 7-4: Base Unit filter

2. Click on **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

CAUTION: It is strongly recommended to change the password of the default IT admin account (admin@yourcompany.com) on first use and additionally create an IT admin account with a valid email address of the company for which CMGS is installed.

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).

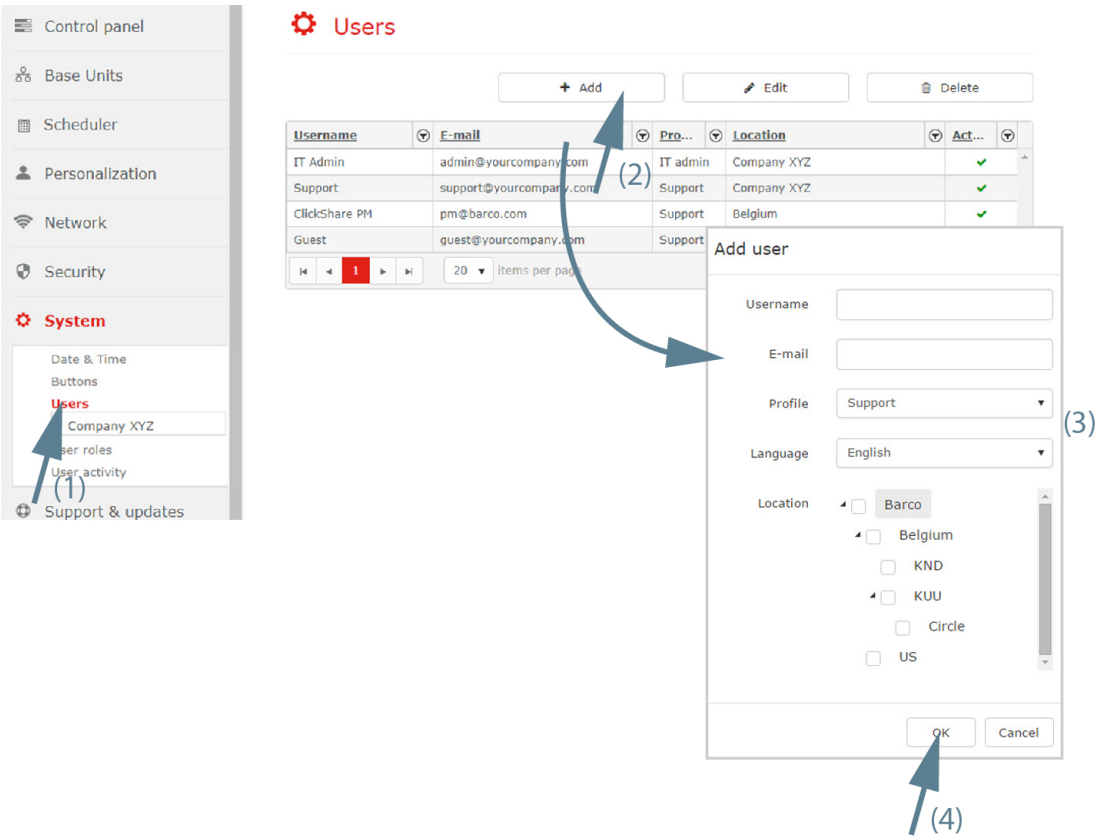

Image 7-5: Add new user

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 84 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).

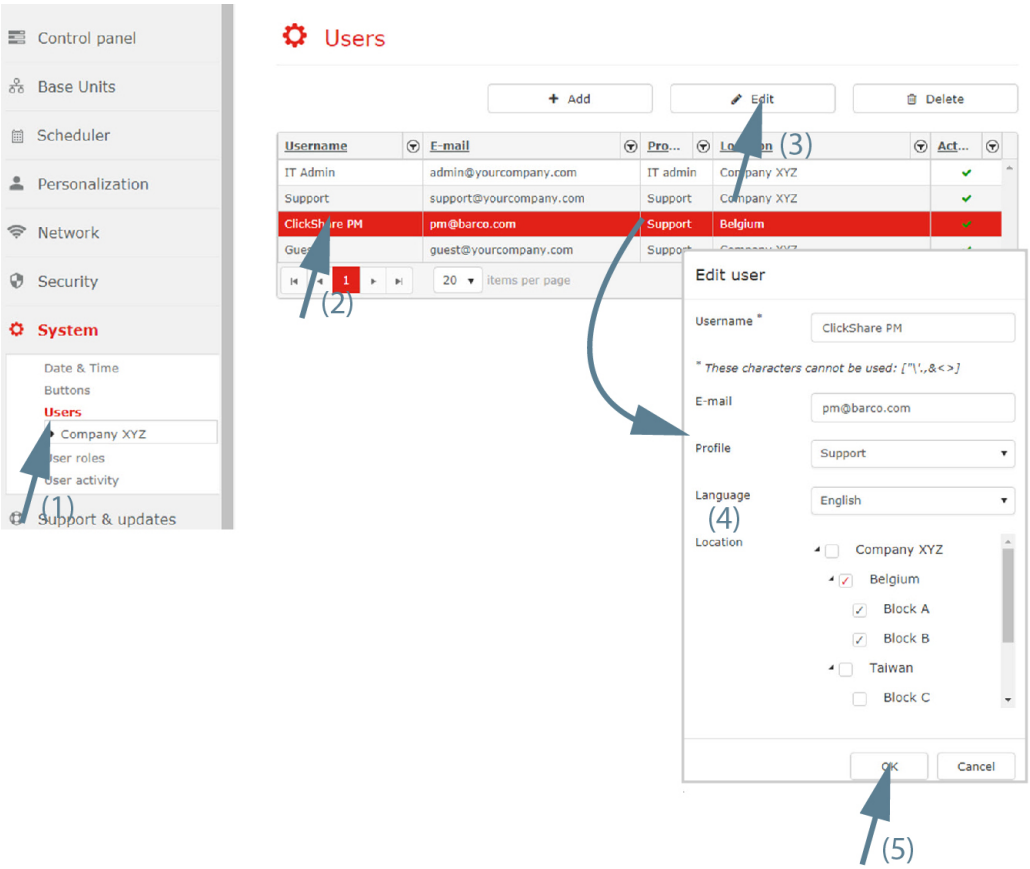

Image 7-6: Edit selected user

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*. See “About Collaboration Management Suite”, page 10 and look to “About user roles”.
   - *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).

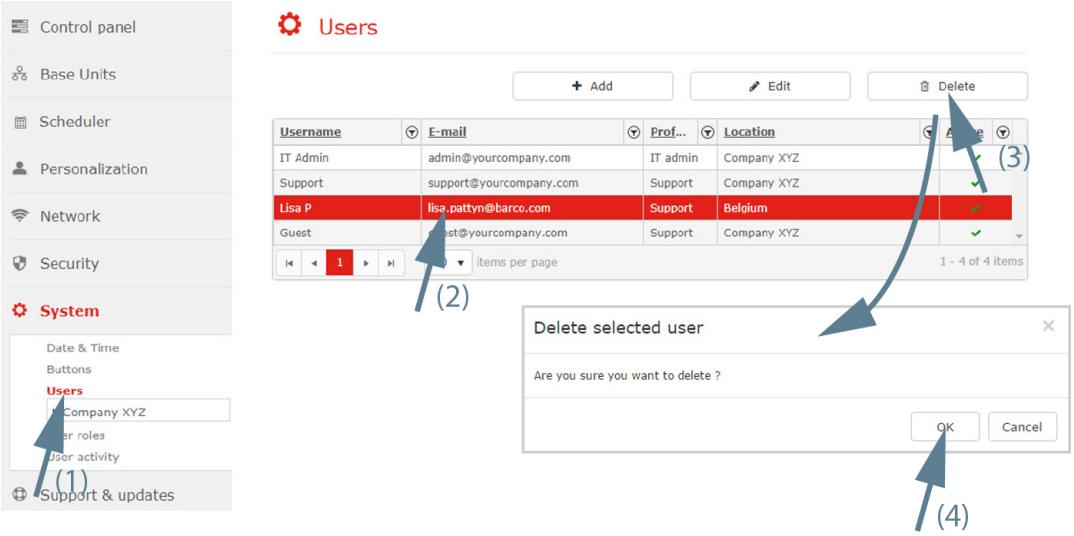

Image 7-7: Delete selected user

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.

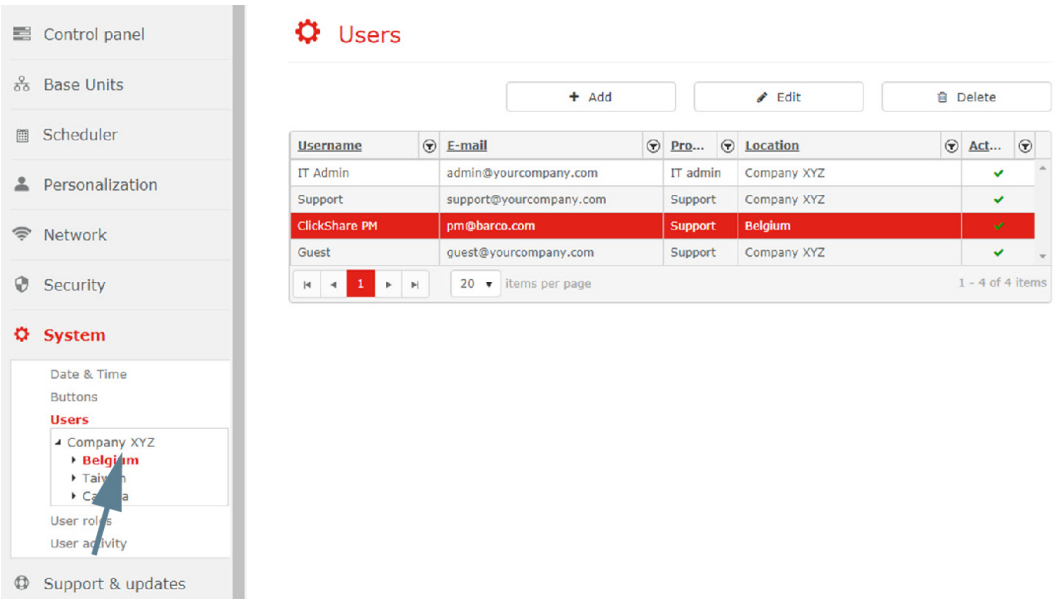

Image 7-8: Location filter on users

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).

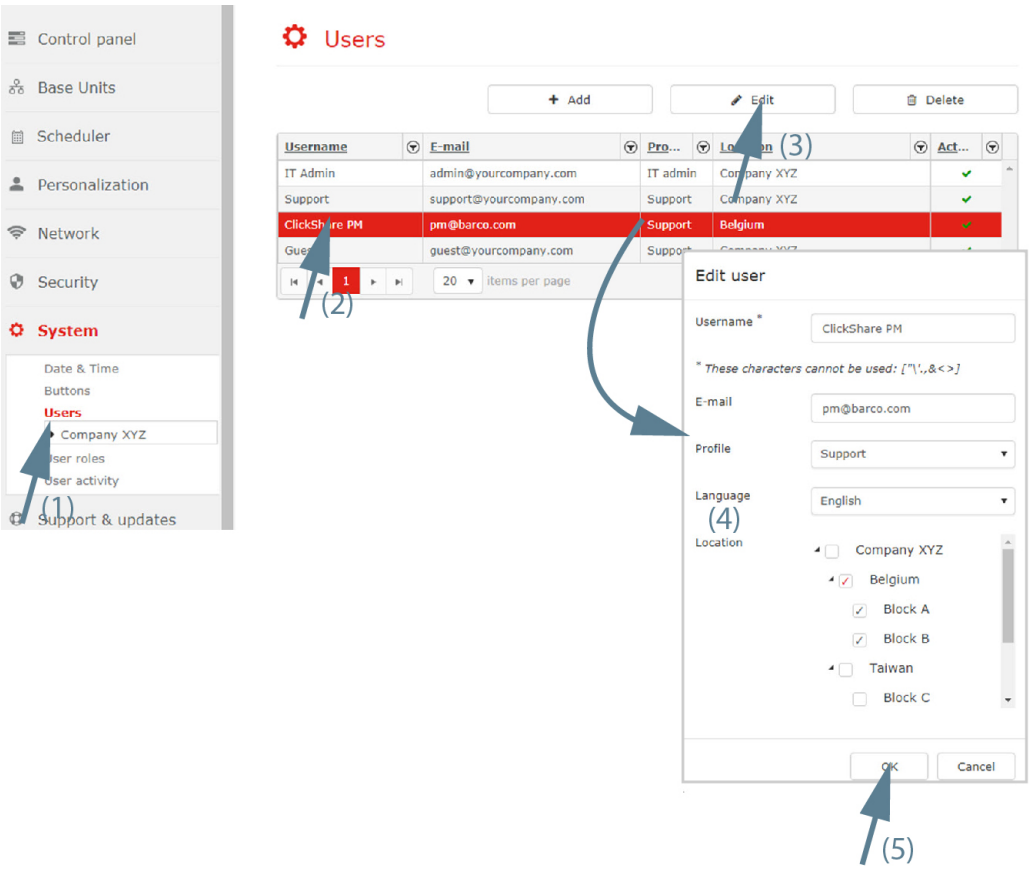

Image 7-9: Edit selected user

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 82 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).

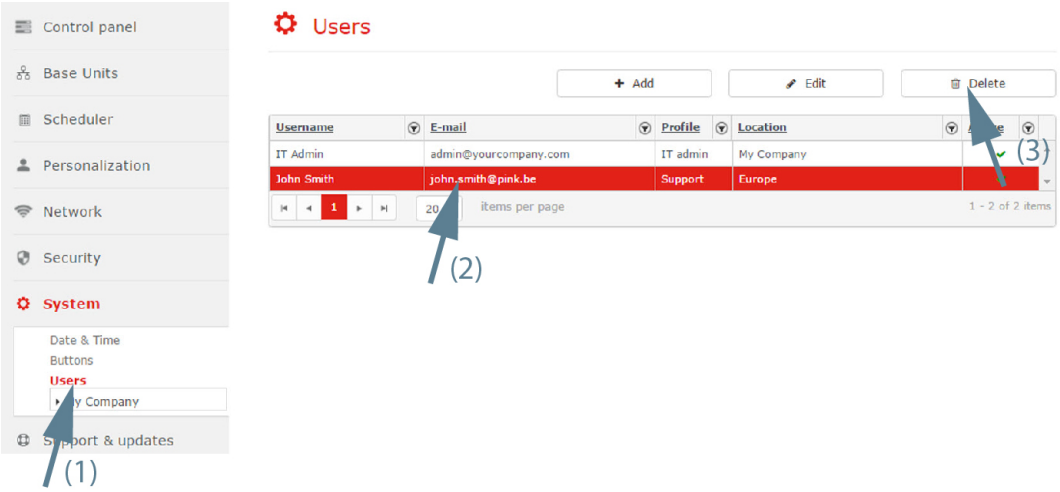

Image 7-10

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

The registered user is removed.

7.4 User roles

7.4.1 Setup user roles

About user roles

Customized roles can be created for a group of users. These roles are then valid for all user in the this group.

The customization can be done in different areas such as:

- Base units
- Locations
- Settings
- Users

Changing these settings will affect all users with the modified role. Users that are logged in will have to re-login.

How to setup a role

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

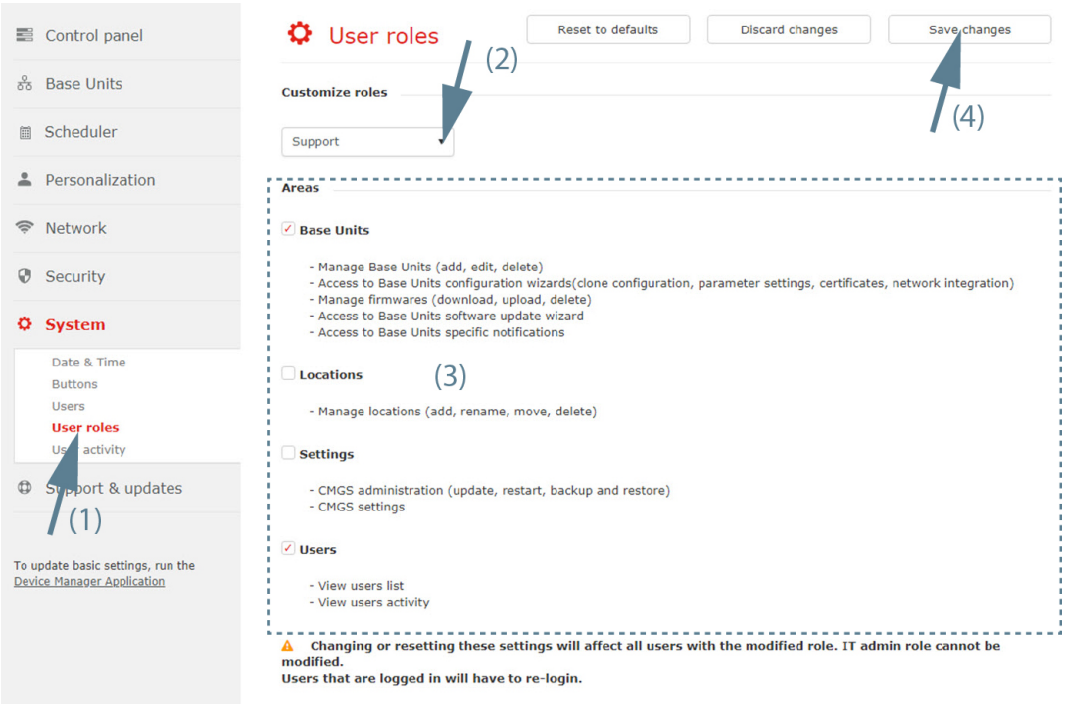

Image 7-11: Setup user roles

2. Select a customization role. Click on the drop down box and select the desired role (2).
3. Check the areas to include in the role (3).
4. Click **Save changes** (4).

7.4.2 Reset to default roles

How to return to default settings

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

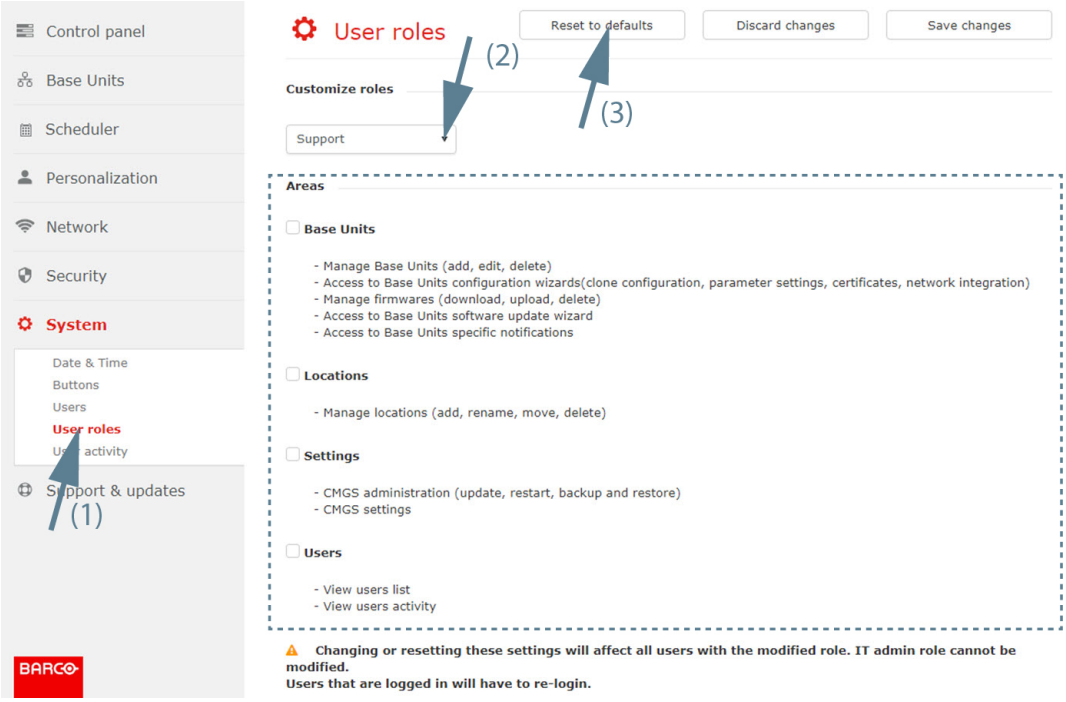

Image 7-12: Reset user role

2. Select a customization role. Click on the drop down box and select the desired role (2).
3. Click on **Reset to defaults** (3).

7.5 User activity

About user activity

All actions initiated by a user are logged in the user activity. The following items are stored:

- Type of action
- Date
- Username
- Profile (role)
- Detail of the action

The user activity list can be limited by setting up a time frame.

Within that time frame, a filter can be setup on column level. Click on the arrow button next to column title, fill out keyword and click Filter.

How to create a time frame

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

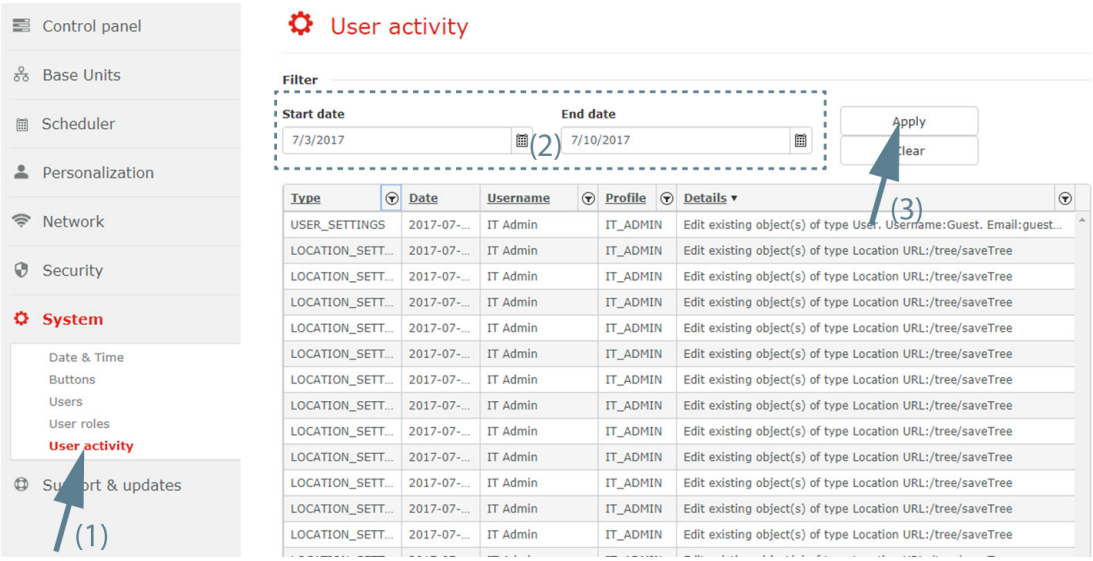

Image 7-13

2. Select the start date. Click if necessary on the calender and select the desired date or select the current date and enter a new date with the following mask mm/dd/yyyy (2).
3. Select the end date in the same way as the start date.
4. Click on **Apply** to apply the time frame (3).

   The list will be limited to the selected time frame.

Support & updates

8

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).

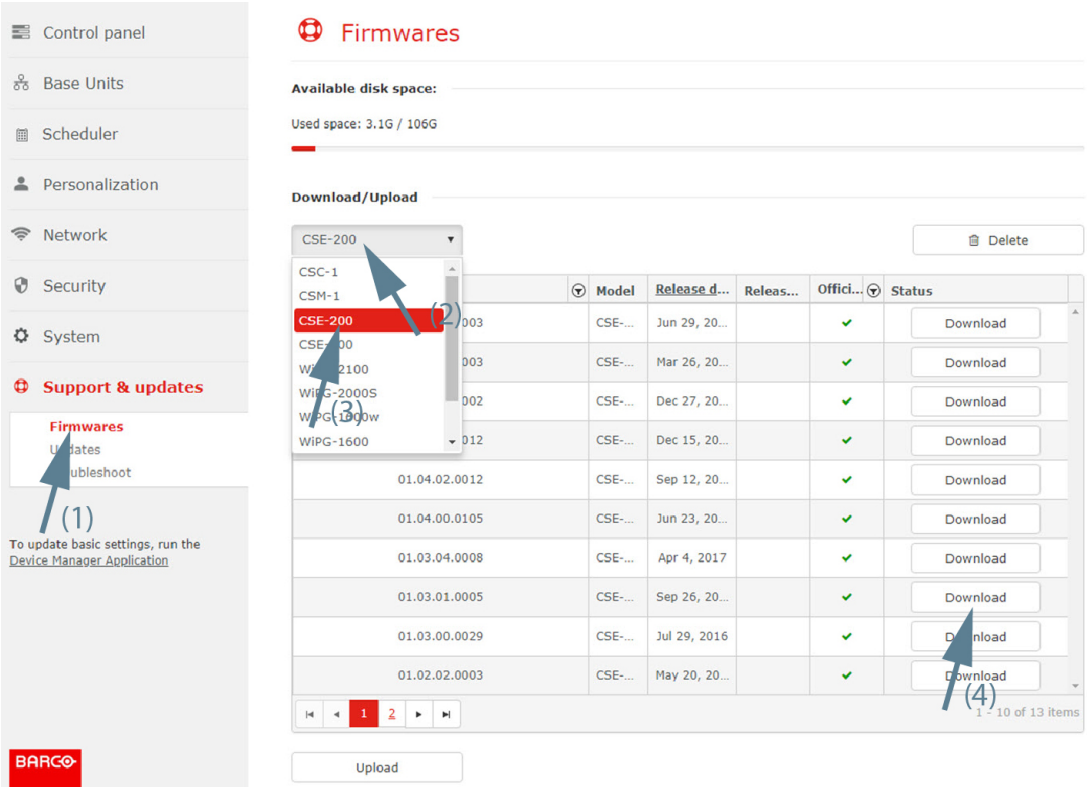

Image 8-1: Firmwares, download/upload

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 between 10 and 20 minutes for a CSC-1/CSE-200/CSE-800 and 15 up to 30 minutes for a CSM-1.

Automatic firmware update[5]

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

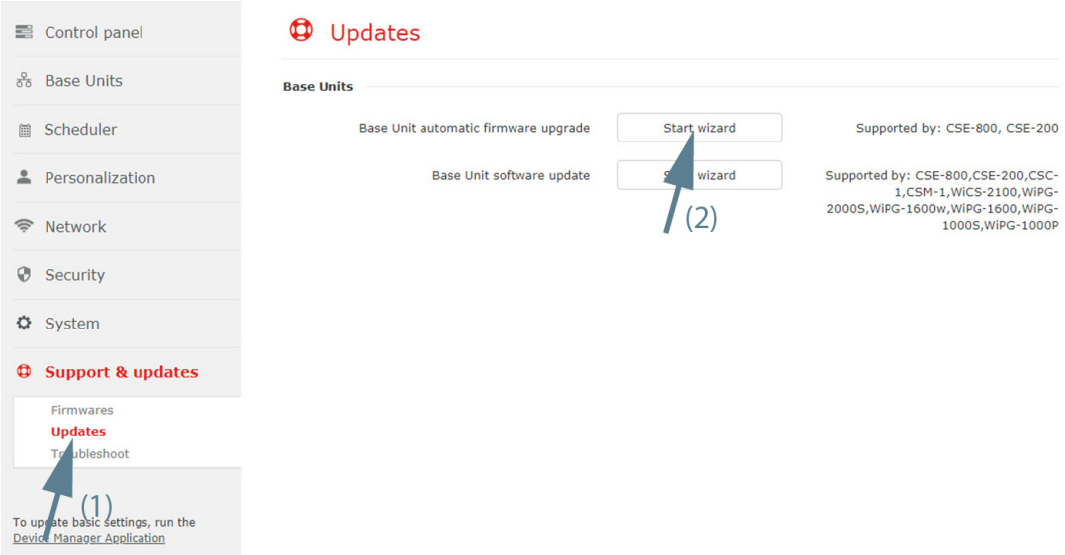

Image 8-2: Start firmware update wizard

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

5: only for CSE devices

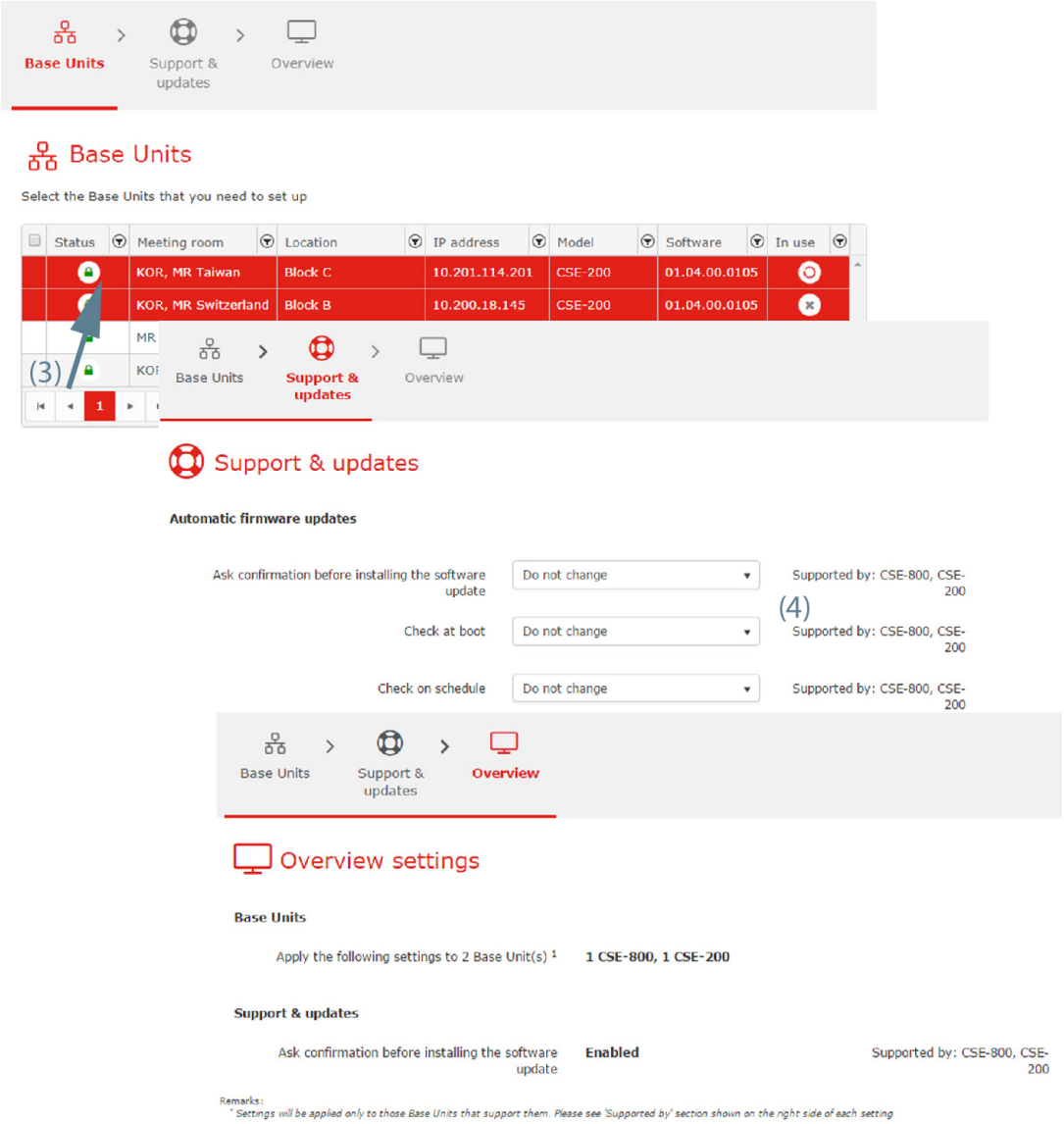

Image 8-3: Automatic firmware updates

4. Check the settings and change if necessary (4). 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[6]

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

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

6: all models

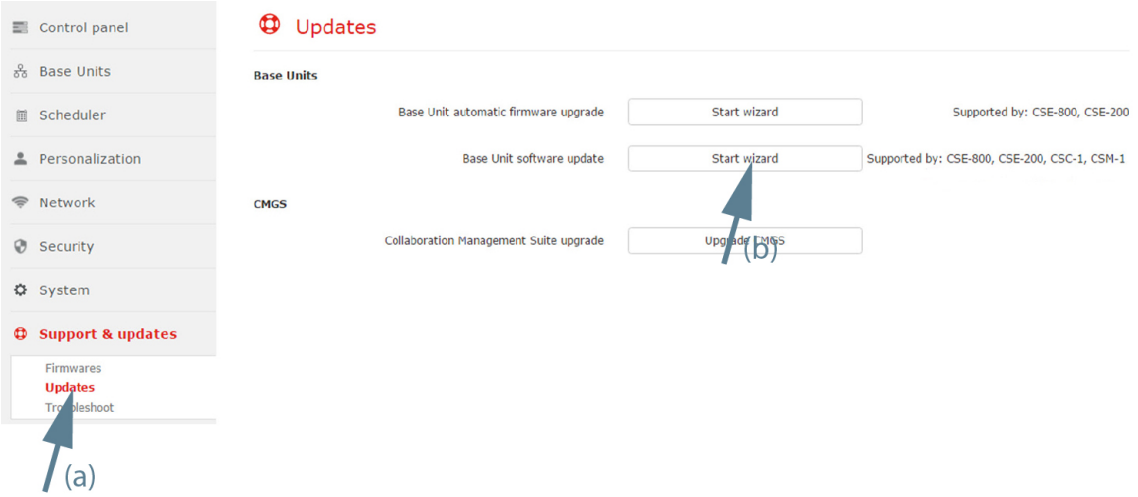

Image 8-4: Start software update wizard

2. Click on the **Start wizard** button next to *Base Unit software upgrade* (2).
3. Select your model and click **Next** to continue (3).

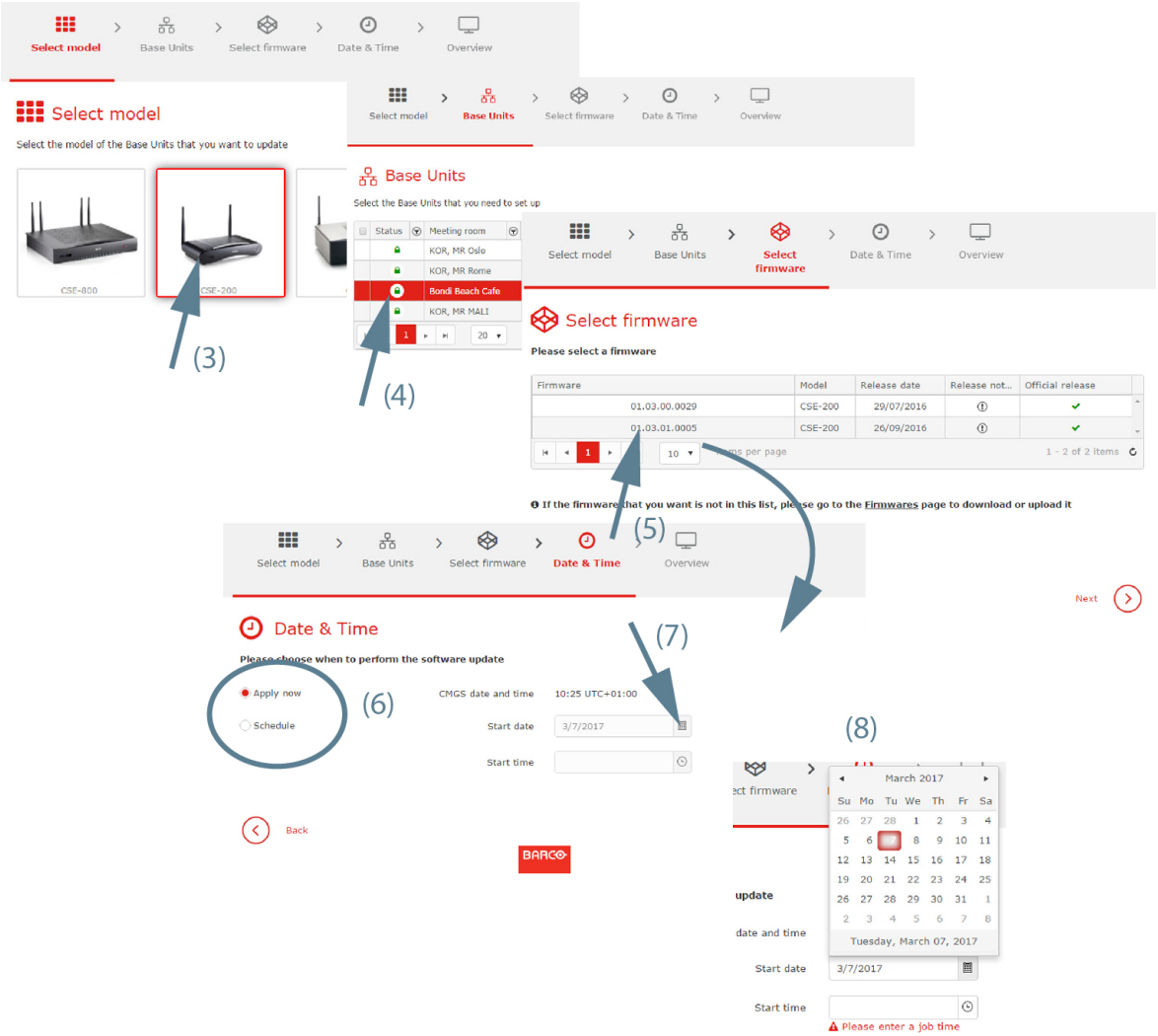

Image 8-5: Software updates

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

5. Is the firmware you want in the list?
   - If yes, Continue with .
   - If no, go first to the *Firmwares* page. For more info see “Firmwares”, page 90.
6. Select the firmware version and click **Next** to continue (5).
7. To apply the firmware immediately, check the radio button in front of **Apply now** (6).

   To schedule the update in the future, check the radio buton in front of **Schedule**. Fill out a day (mm/dd/yyyy) (7) and hour (hh:mm) (8) if necessary.

   or
   click on the icon in the date field to open a calender and select a month and a day. To change the month, click on the right or left arrow next to month name until the desired month and year are obtained. Click on a number in the number field to setup the day.
8. When date and time is filled out, click **Next**.

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

8.3 Troubleshoot

Overview

- Base Unit logging level
- Reboot Base Units
- Diagnose connection issues CMGS - Base Unit
- CMGS logging level
- Report CMGS issues
- Syslog server

8.3.1 Base Unit logging level

How to set

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

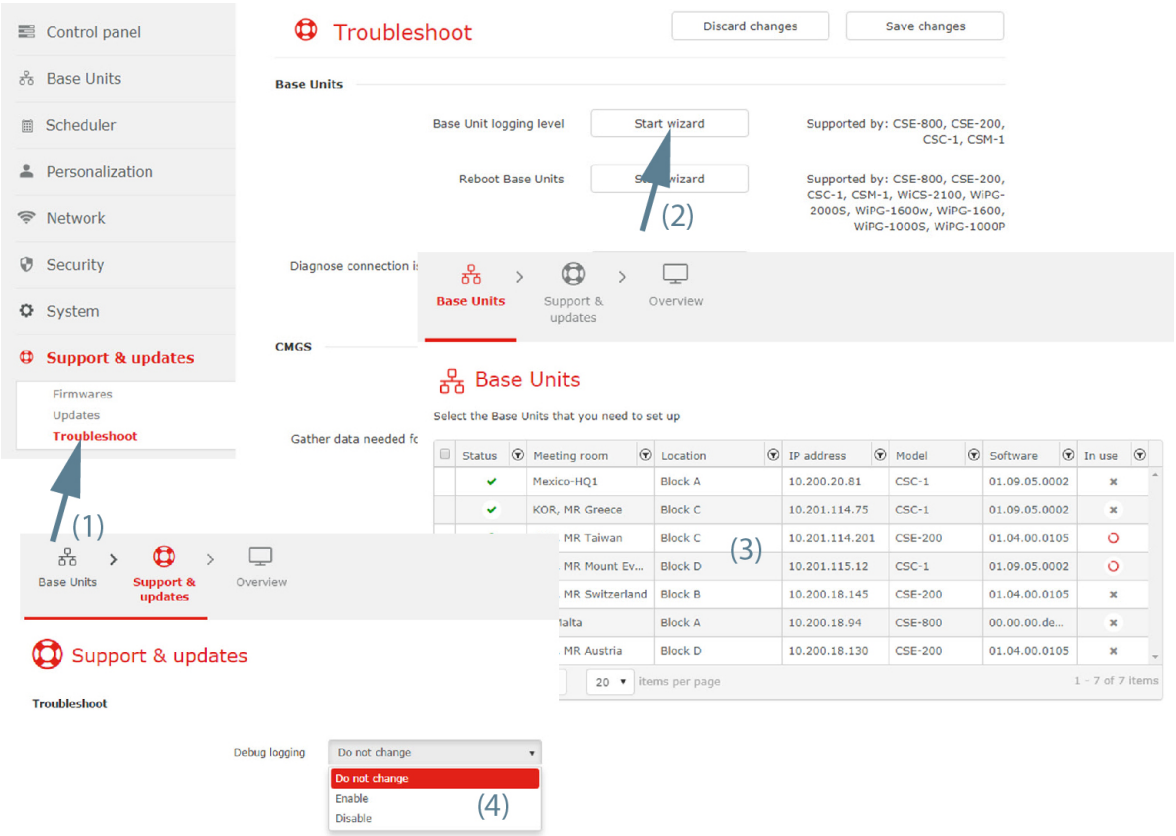

Image 8-6: Troubleshoot, Base Unit logging level

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.

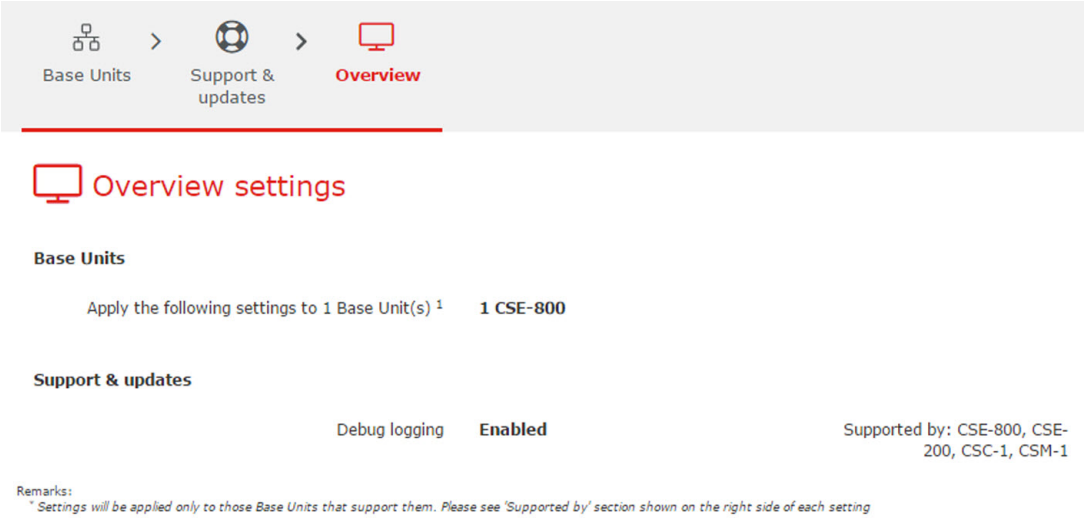

Image 8-7: Overview settings

6. Click **Finish**.

8.3.2 Reboot Base Units

What can be done?

How to reboot

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

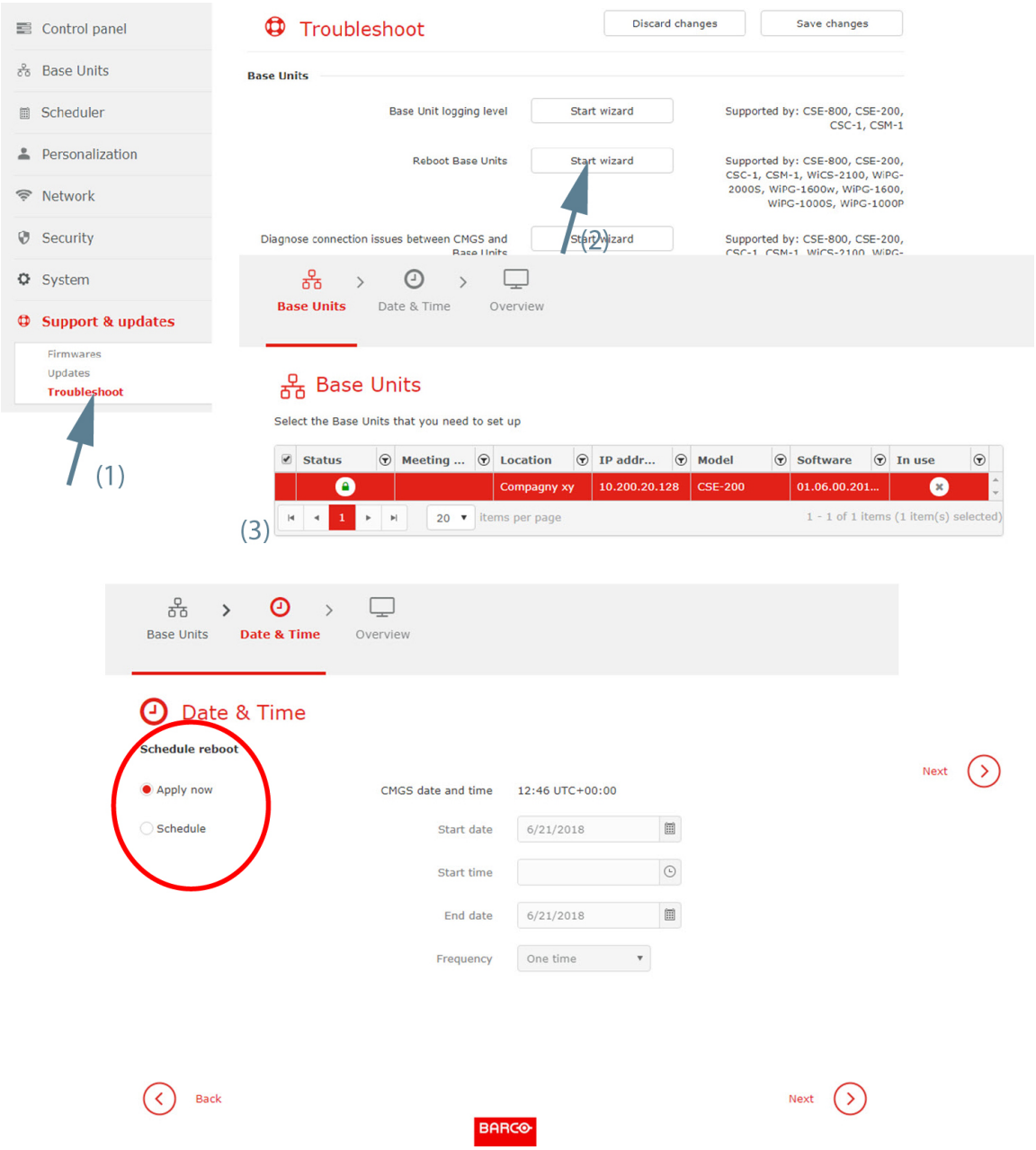

Image 8-8: Reboot Base Unit(s)

2. Click **Start wizard** next to *Reboot Base Unit* (2).
3. Select the Base Unit(s) (3) and click **Next**.
4. To reboot immediately, check the radio button next to *Apply now*.

   To reboot on a scheduled time, check the radio button next to *Schedule*. Continue with next step.
5. To enter 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.
   1. To change the year and month, click on the left or right arrow key next to the month-year name (1).

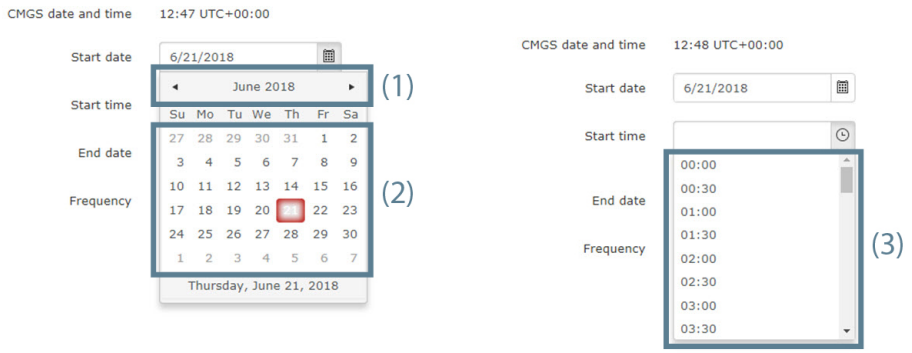

Image 8-9: Time and date setup

2. To change the day, click on the desired day in the calendar (2).
3. To set the desired time comparing to the server time, click on the icon and select a predefined time (3).

or
enter the start & end date (mm/dd/yyyy) and time (hh:mm) by clicking in the input field and changing the values.

6. Click **Next** to continue.

8.3.3 Diagnose connection issues CMGS - Base Unit

How to setup

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

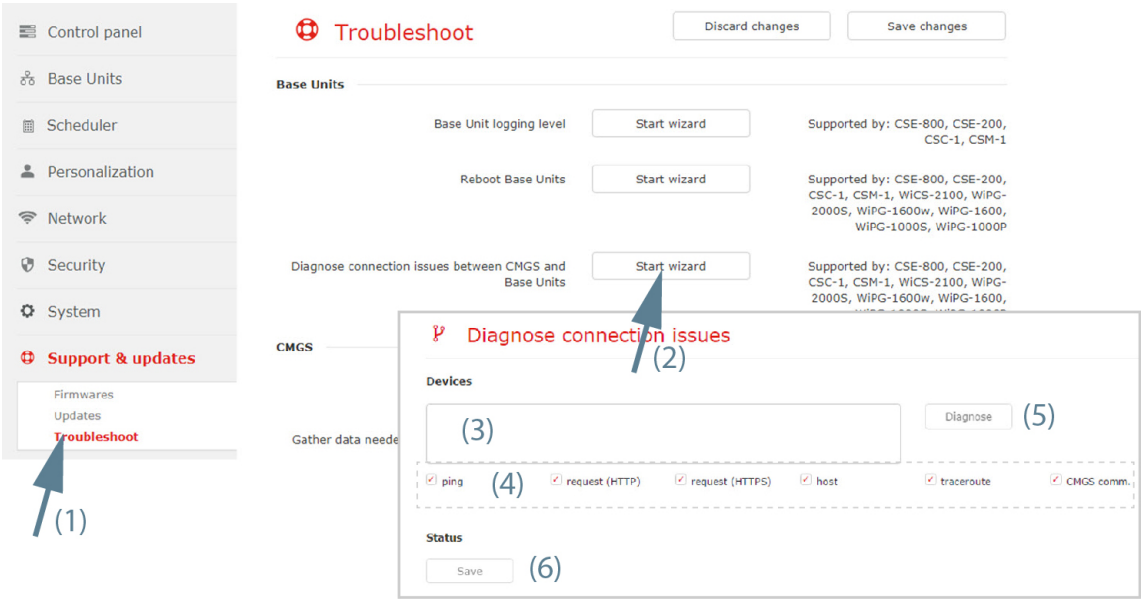

Image 8-10: Troubleshoot, diagnose connection issues

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).

8.3.4 CMGS logging level

How to set

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

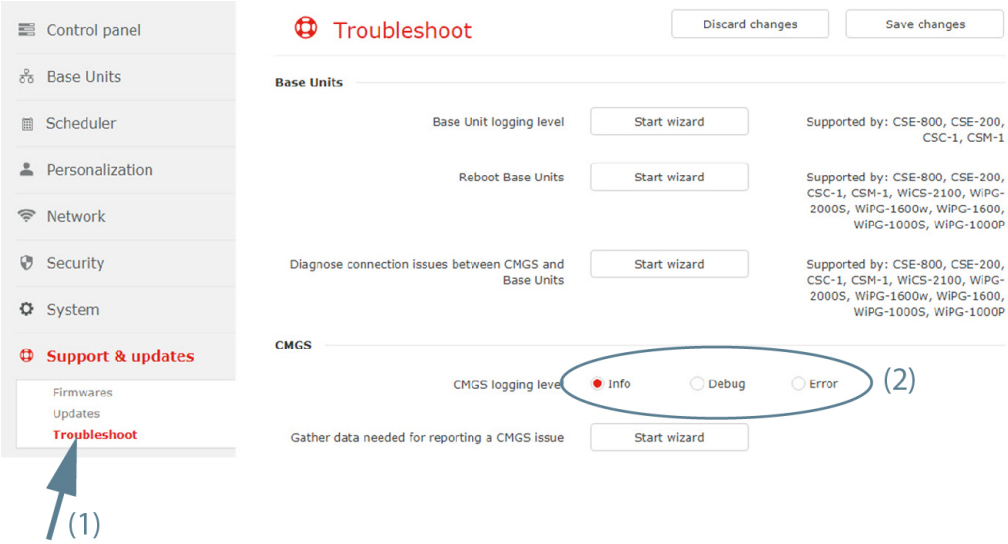

Image 8-11: Troubleshoot, CMGS logging level

2. Next to CMGS logging level, check the radio button of your choice (2).

   The following choices are possible:

   - Debug
   - Info
   - Warning
   - Error

8.3.5 Report CMGS issues

How to report issues

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

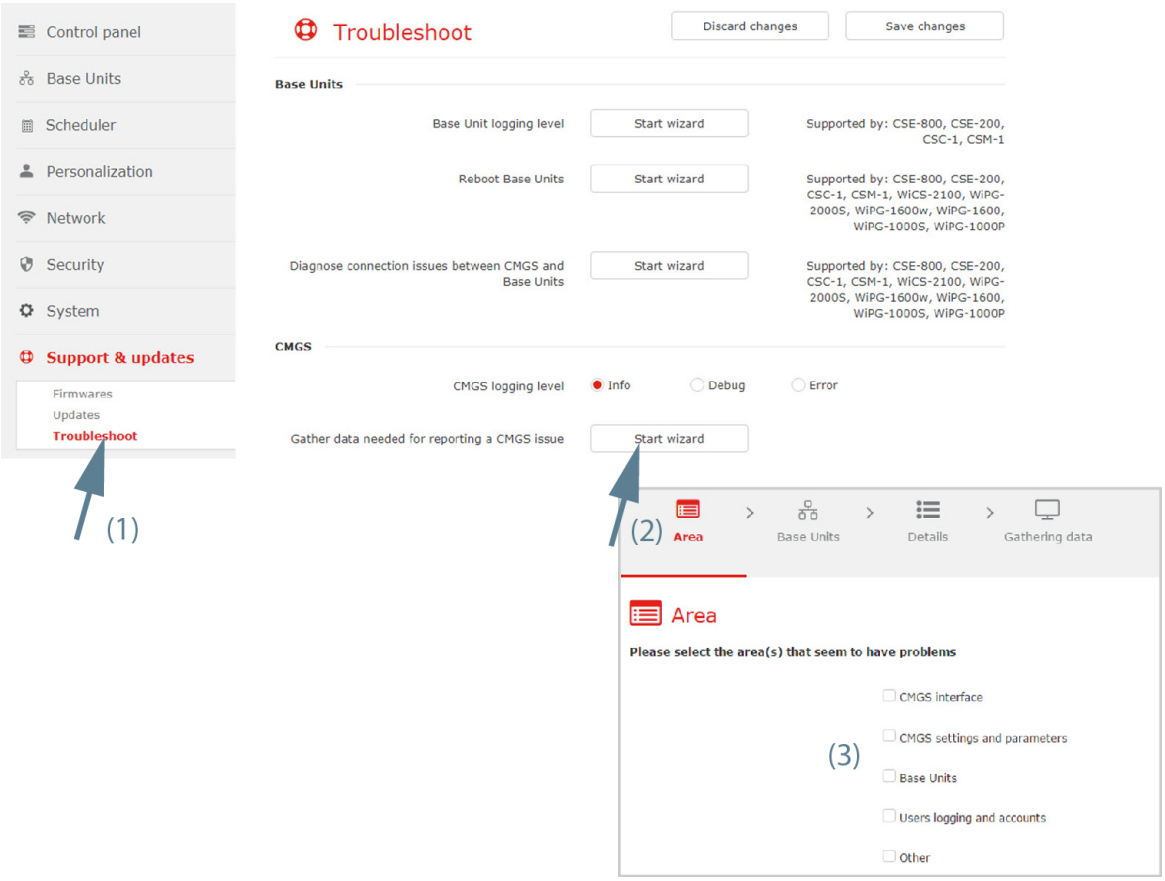

Image 8-12: Report CMGS issue

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).

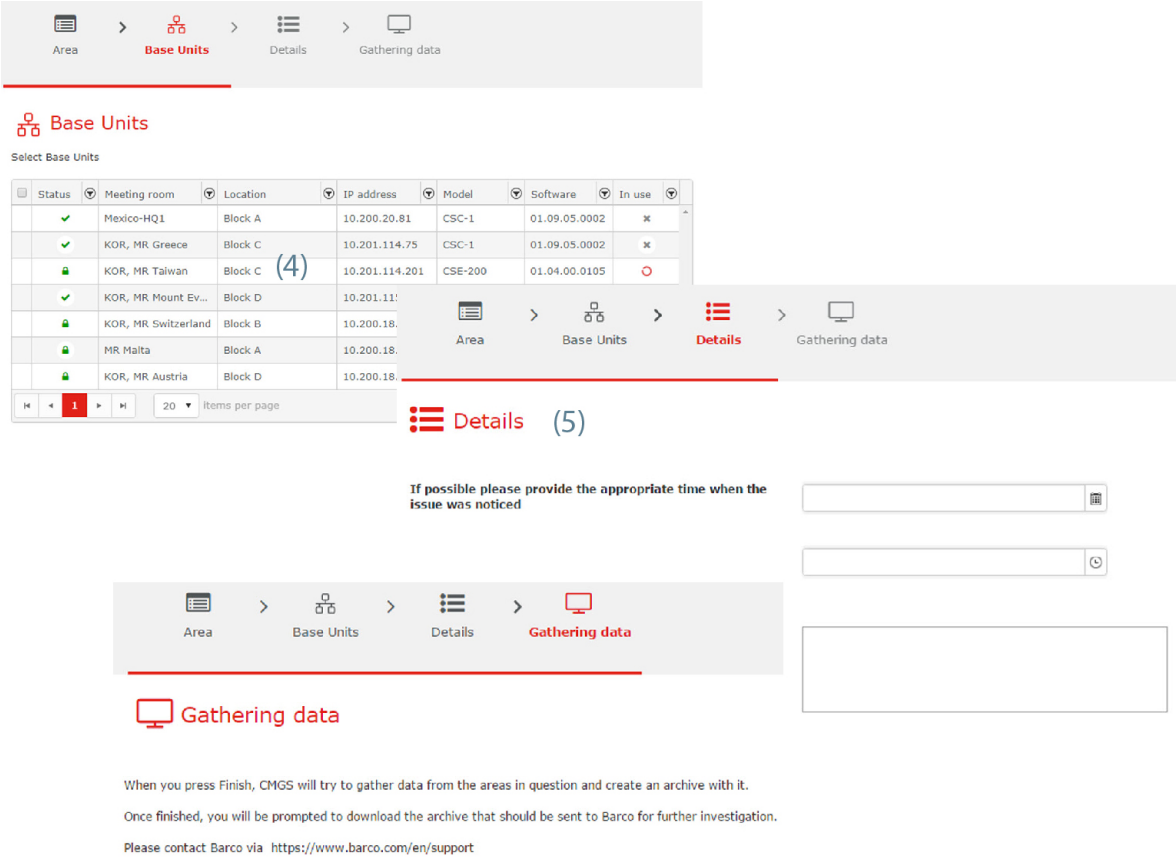

Image 8-13: Report CMGS issue

5. Enter more details (5).
   - Enter a date with mask *dd/mm/yyyy* or click on the calendar icon and select a month and day.
   - Enter a time with mask *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 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*

8.3.6 Syslog server

How to setup

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

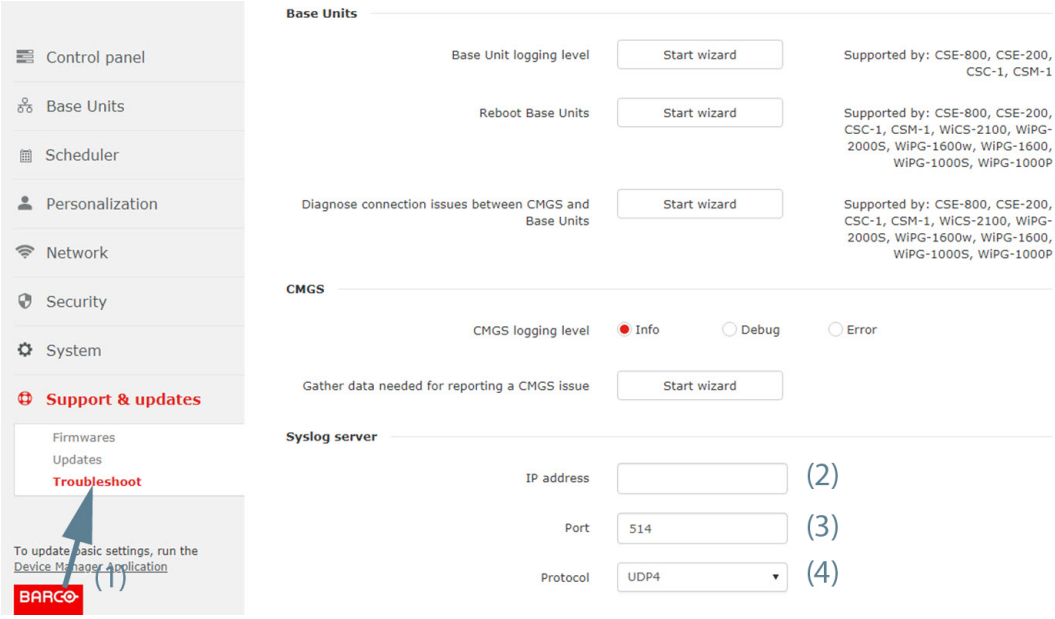

Image 8-14

2. In the *Syslog server* pane, enter the IP address or hostname (2).
3. The default port is 514. To change the port number, click in the input field and fill out a new port number (3).
4. To change the protocol, click on the drop down box and select the desired protocol (4).

   The following protocols are available:
   - TCP
   - UDP4
   - UDP6
   - UNIX

Device Manager Application

9

9.1 Starting the Device Manager application

About the device manager

The settings set during the first start up of the Collaboration Management Suite can be changed in the Device Manager.

Starting the Device Manager

The link to the Device Manager is indicated in the menu column of each page. Just click on that link to open the Device Settings.

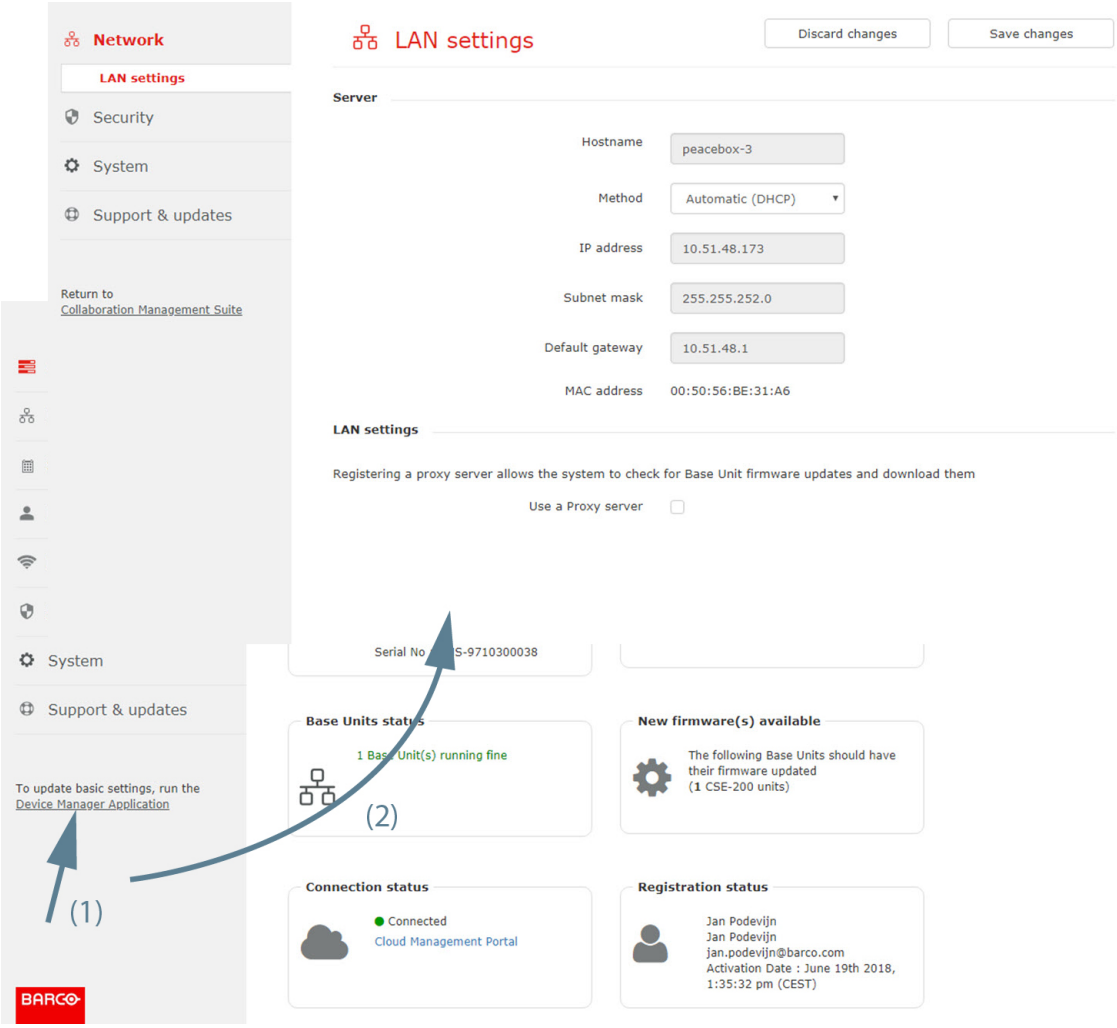

Image 9-1: Start up Device Manager

9.2 Network, LAN settings

About LAN settings

For the Server settings, only the method to obtain an IP address can be changed between Automatic and Manually.

For the LAN settings itself, the choice can be made to use a Proxy server.

Server settings, method

1. Click on the drop down next to Method and select Automatic (DHCP) or Manual.

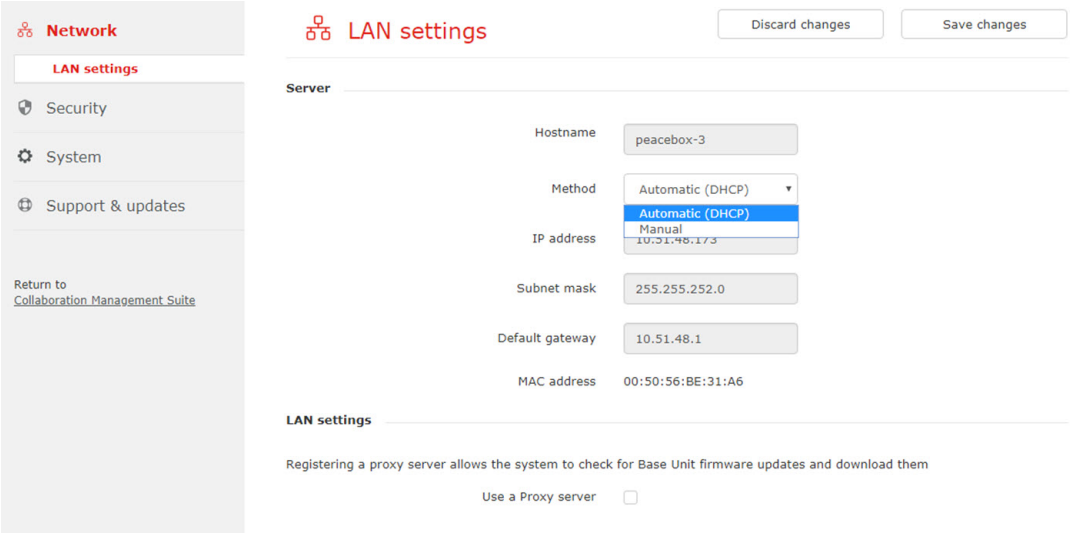

Image 9-2: Network, LAN settings, method

- Automatic (DHCP): an automatic IP address will be obtained.
- Manual: an manual IP address, subnet mask and gateway can be set. Continue with *Manual (fixed) IP address*.

Manual (fixed) IP address

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

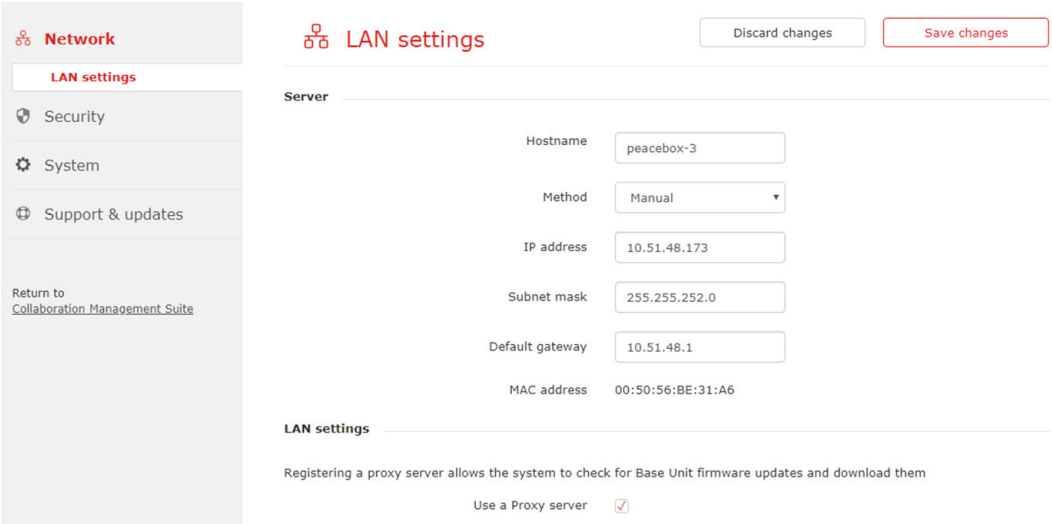

Image 9-3: Network, LAN settings, manual

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

The current IP addresses are filled out.

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

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

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

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

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

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

LAN settings, proxy server

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

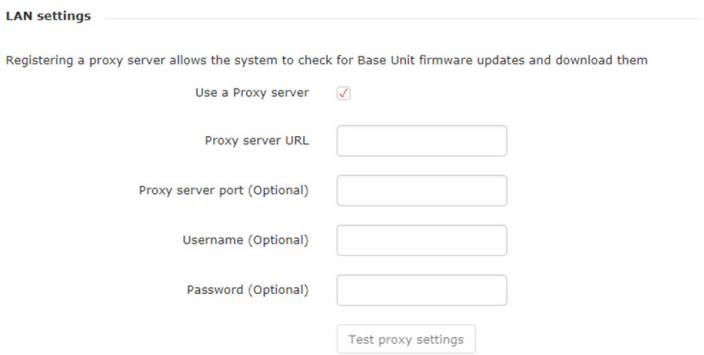

Image 9-4: Proxy settings

The proxy settings become available.

2. Enter the proxy server URL. Enter the IP address or hostname.

   Some proxy servers need a port number, user name and password, for others is this optional.

3. Optionally, enter the used server port.
4. Optionally, enter the user name.
5. Optionally, enter the password.
6. Click Test proxy settings to test the input.
7. Click **Save changes** to apply the settings.

9.3 Security, deploy SSL certificate

About SSL certificate

The SSL certificate is used for secure communication between the Collaboration Management Suite and the browser. The current certificate is a self-signed certificate. If you have a certificate signed by a Certificate Authority, then the browsers will consider Collaboration Management Suite as a secure site. With the current certificates from Collaboration Management Suite, some browsers might warn the users that the certificate is not signed by an authority and might not be secure to access the page, so the user has to explicitly accept the self-signed certificates when first accessing the Collaboration Management Suite.

How to deploy

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

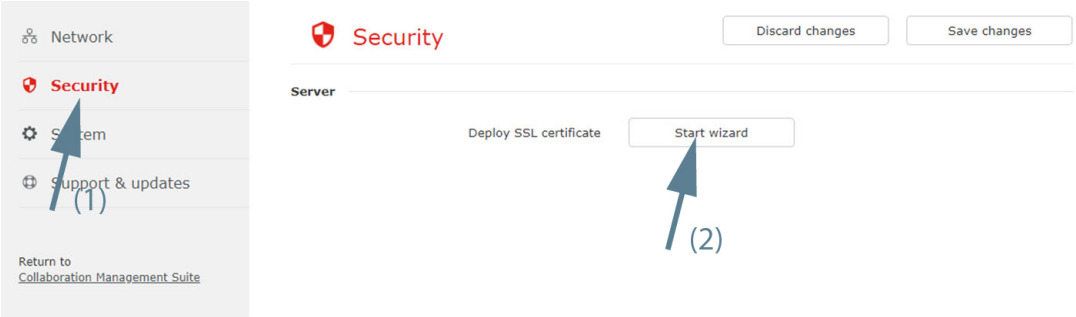

Image 9-5

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

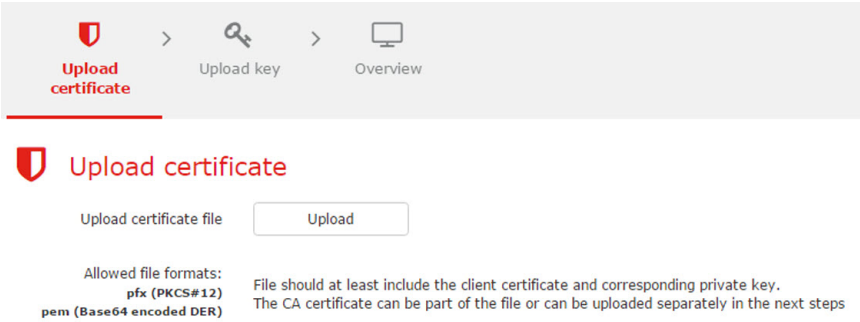

Image 9-6: Upload certificate

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.

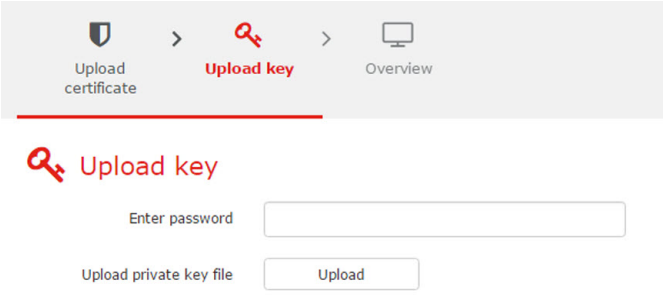

Image 9-7: Upload key

An *Overview* window is displayed.

5. Click **Finish**.

9.4 System, Date & Time setup

How to setup

1. In the menu pane, select **System** → **Date & Time**.
2. The current time and time zone are indicated. When necessary, select a new timezone. Click on the drop down box and select the corresponding zone.
3. Select mode for setting date and time. Check the check box of your choice.
   - Use NTP server
   - Set a date and time manually

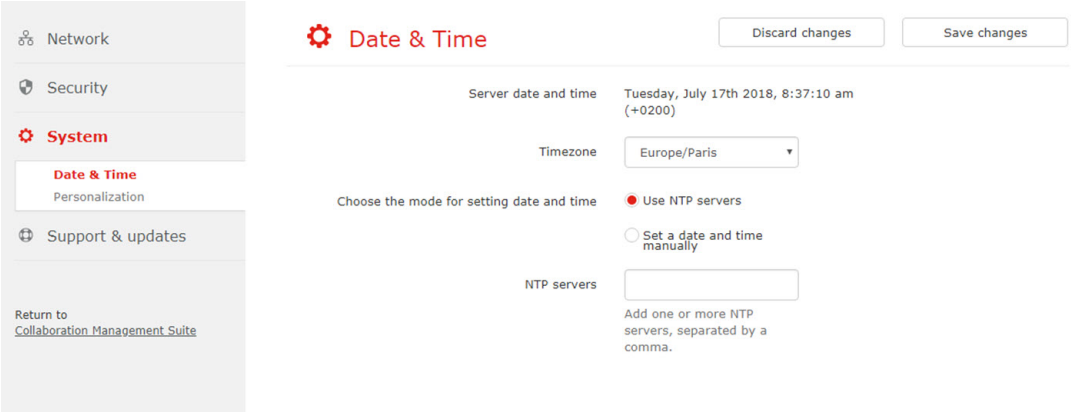

Image 9-8: Timezone and NTP server

4. To use an NTP server, fill out the NTP server IP address or host name next to *NTP servers*.

   Up to maximum 5 servers can be added, separated by a comma.

5. To set a time and date manually, select the radio button next to *Set a date and time manually*.

   Click on the date table icon and select the current date.

   To select the time, click on the clock icon. Click on the up down control to set the hours, minutes and second. Toggle the period between AM and PM just by clicking on AM or PM.

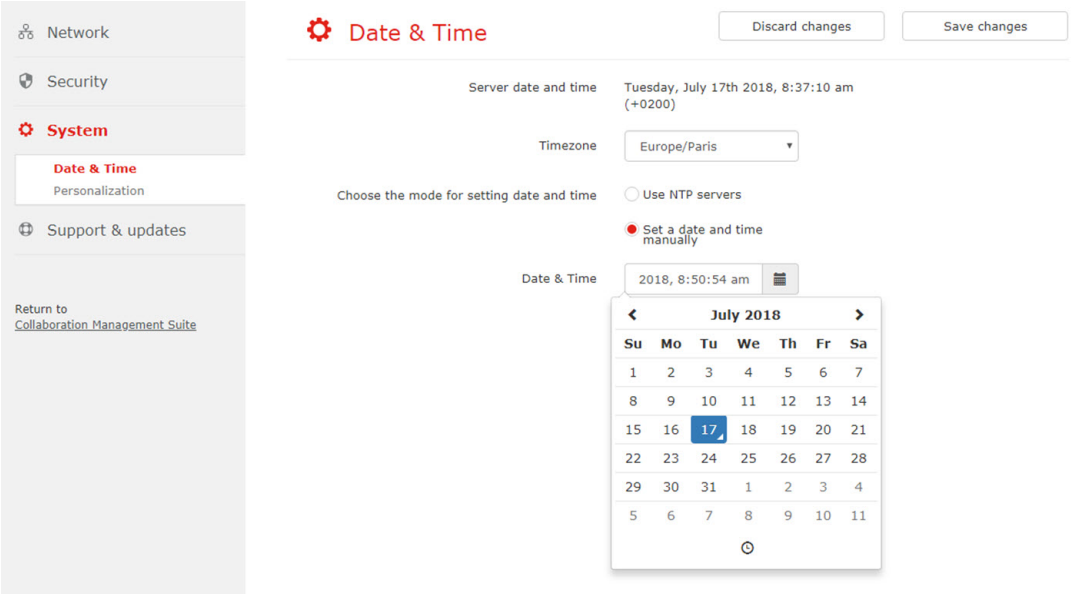

Image 9-9: Date & time

6. Click **Save changes**.

9.5 Personalization

About personalization

The current name of the Collaboration Management Suite server can be changed to a new name.

How to change

1. In the menu pane, select **System** → **Personalization**.

   The current device name is indicated next to *Device Name*.

2. Click in the input field and and enter a new name.

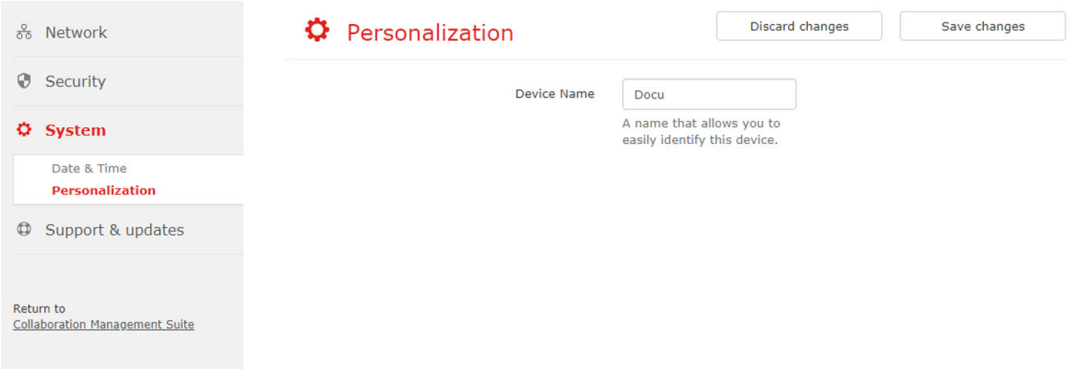

Image 9-10: Personalization of CMGS

3. Click **Save changes**.

9.6 Updates

About updates

Firmware can be uploaded and the server can be updated using a wizard.

Server update

1. In the menu pane, select **Support & updates** → **Updates**.

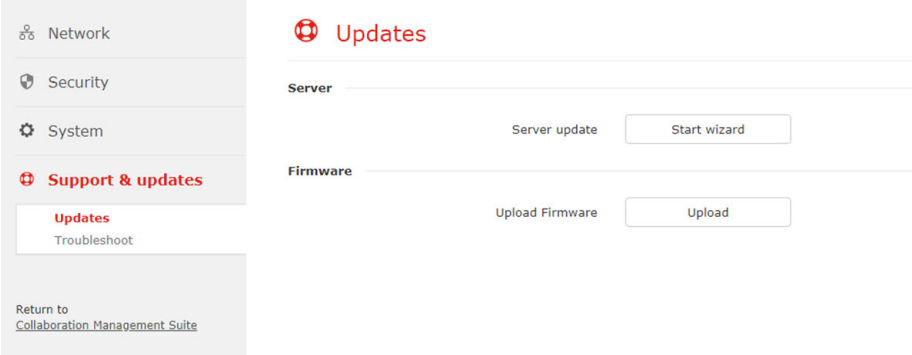

Image 9-11: Server Updates

2. Click on **Start wizard** next to *Server update*.

   A message is diplayed.

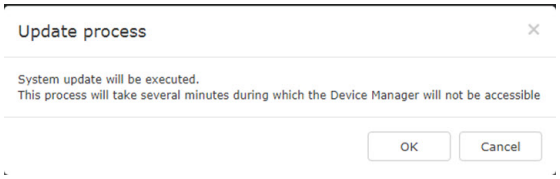

Image 9-12

3. Click **OK** and follow the instructions on the screen.

Firmware upload

1. In the menu pane, select **Support & updates** → **Updates**.
2. Click on **Upload** next to *Upload Firmware*.

   A browser window opens.
3. Select the firmware file and click **Open**.

The firmware will be uploaded.

9.7 Troubleshoot

Server logging level

The server logging level can be set on Info or Debug.

Click on the desired radio button to select.

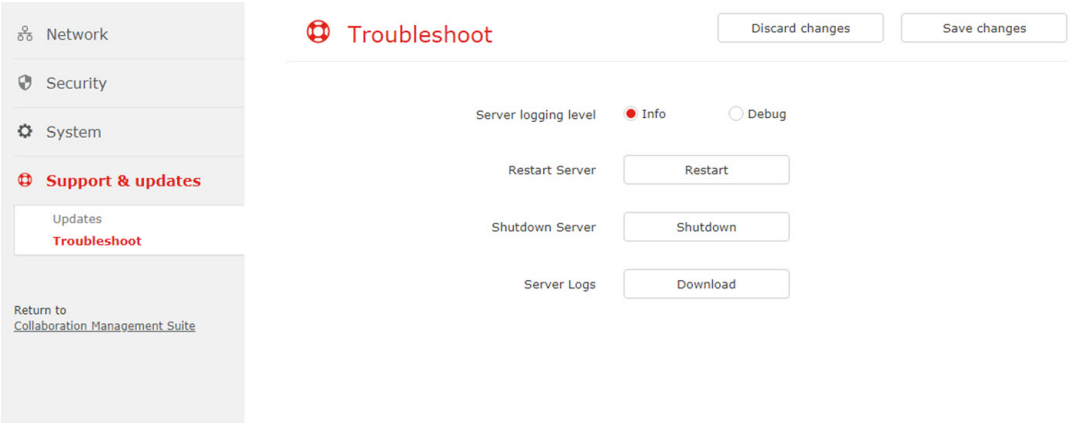

Image 9-13

Restart server

To restart the server, click **Restart** next to *Restart Server*.

Shutdown server

To shutdown the server, click **Shutdown** next to *Shutdown*.

Server logs

To download the server logging, press **Download** next to *Server Logs*.

10 Software ports

10.1 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) and for supporting the cloud portal.

- port 80 TCP inbound - for HTTP access
- port 443 TCP inbound & outbound - 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

EULA and Open Source provisions

A

Overview

- End User Licence Agreement
- Open Source Software provisions

A.1 End User Licence Agreement

Barco ClickShare Product Specific End User License Agreement[7]

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

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

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

1. Entitlement

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

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

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

2. Support

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

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

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

3. Terms of Use

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

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

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

4. Privacy

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

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

5. Other Terms

- **Open Source components**
  The Software contains software components released under an Open Source license.
  A list of the third party components used is available in the Software’s README files, through the “My Barco” section of the Barco website or through other (online) means. The applicable license terms,

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

copyright notices and, as relevant, source code access conditions apply as set out in the Barco EULA attached hereto.

- **Retention of data**
  Barco right to use and retain Functional Information (section 10.2 of the EULA) shall survive the term of this EULA.

BARCO END USER LICENSE AGREEMENT[7]

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

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

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

1. Definitions

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

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

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

“DRM” means Barco’s digital rights management platform used to provide access to and access conditions of the Software.

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

“Product Specific EULA” means the supplemental software terms applicable

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

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

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

2. License Grant

2.1 `License Scope`. Subject to compliance with all license terms and payment of applicable fees, Barco grants you a limited, non-exclusive, non-assignable, non-transferable, non-sub-licensable license to use the Software exclusively in accordance with the conditions and parameters set forth herein. Save for the Product Specific EULA or any broader license terms confirmed through the DRM tool, the license under this License Agreement applies to one (1) copy of the Software to be used on one single computing device by one (1) single user. Installation on a computing device that may be concurrently accessed by more than one user shall

not constitute a permitted use and a separate license is required for each user connecting at the same time to a computing device on which the Software is being deployed.

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

2.3 License restrictions.

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

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

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

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

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

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

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

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

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

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

3. Ownership. Intellectual Property Rights.

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

3.2 Third Party Materials. The Software may contain or require the use of certain third party technology (whether proprietary or open source software), identified by Barco in the Documentation, readme file, third-party click-accept, on www. barco. com or elsewhere (the "Identified Components"). Identified Components may be subject to additional and/or different terms and you agree that the Identified Components are licensed

under the terms, disclaimers and warranties of their respective licenses which in the forthcoming case shall override the provisions of this License Agreement.

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

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

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

4. Support

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

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

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

5. Warranty

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

6. Compliance and Enforcement

6.1 Reporting and Audit. In addition to good practice record-keeping obligations, you agree to report the use of the Software and relating billing metrics in the DRM or otherwise as agreed. You grant to Barco and its designated auditors, at Barco's expenses, the right to verify your deployment and use of the Software during your normal business hours so as to verify your compliance with the License Agreement. In the event such audit reveals non-compliance with your payment obligations hereunder, you shall promptly pay to Barco the appropriate license fees plus the reasonable cost of conducting the audit.

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

6.3 Enforcement. Upon breach of the License Agreement (including overdue payment), Barco shall inform the then known user, through the DRM or otherwise in writing, (i) which condition of the License Agreement (including payment terms) is violated; (ii) allow a period of 8 calendar days to cure such breach, if it can be

cured at all; and (iii) inform which part of the functionality Barco intends to reduce (all Software or certain additionally licensed features only; in part or in full) if the breach is not remedied on time and in full.

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

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

7. Limitation of Liability

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

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

8. Confidentiality

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

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

9. Term and Termination

9.1 Term. The duration of this License Agreement will be from the date of your acceptance (as set forth above) of the Software (whereby you acknowledge that use of the Software implies acceptance), until you de-activate the Software, discontinue the use of the device on which the Software was first installed for its intended use or the expiration of the limited time period set out in the Product Specific EULA, whichever comes first.

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

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

10. Other relevant terms

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

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

11. Final Clauses

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

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

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

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

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

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

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

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

Barco ClickShare Product Specific Privacy policy

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

Via the Software, Barco may gather technical information about (i) the functioning and the functionality of the products which are connected through the Software, and/or (ii) as provided by you or generated by your use of the Software ("Functional Information"). Barco may make use of such Functional Information for purposes of analytics, for developing and improving products and services, offering products and services to your organization and/or allowing third parties to access such Functional Information; based on the legitimate

interest of Barco of evaluating the market, assessing and improving its products and conducting research and development. All knowhow, inventions and works derived by Barco from the Functional Information will be exclusively owned by Barco.

A.2 Open Source Software provisions

For Collaboration Management Suite and XMS

A complete overview of all used Open Source Software components can be found on the Barco website.

Click on the following link to get this overview: *www.barco.com/opensourcesoftware/xms/*

Index

H

I

L

M

N

O

P

R

S

T

U

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