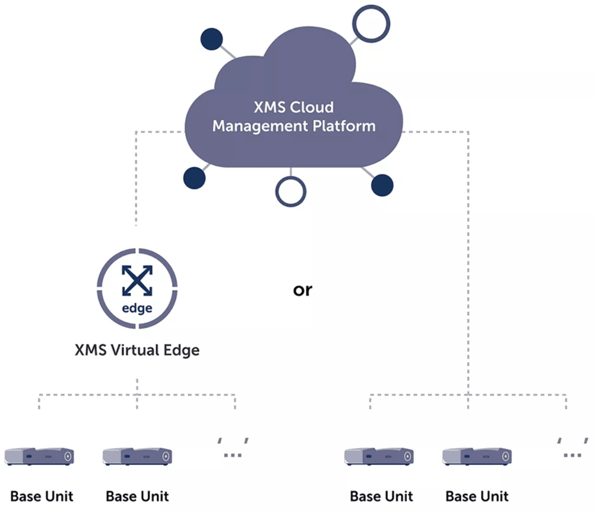
XMS (virtual) Edge

ClickShare



User guide

ENABLING BRIGHT OUTCOMES

Product revision

Software Revision: 2.13

Barco NV
Beneluxpark 21, 8500 Kortrijk, Belgium

Registered office: Barco NV
President Kennedypark 35, 8500 Kortrijk, Belgium

Copyright ©

Trademarks

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

1.1 About XMS

Overview

eXperience Management Suite (XMS) is an 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 Edge or on a virtual machine connected to the network. The functionality can be accessed by users via a web browser based application from anywhere within the network. A user/admin may inspect and/or change a large set of data about the ClickShare Base Units and Buttons without leaving their desk. This is especially useful in large corporations with many ClickShare Base Units installed across different sites. Before the application on the XMS (virtual) Edge 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 XMS Edge or virtual machine and the Base Units, typical ports should be activated. For an overview of these ports, see "Network requirements", page 102.

In order to diagnose connection problems between XMS and the Base Units please see "Diagnose connection issues", page 40.

Supported Base Units

XMS supports:

- CX-50 Gen2 with software version 2.13 or higher
- C-5 with software version 2.8 or higher
- C-10 with software version 2.8 or higher
- CX-50 with software version 2.5 or higher
- CX-30 with software version 2.5 or higher
- CX-20 with software version 2.5 or higher
- CSE-800 with software version 01.00 or higher
- CSE-200+ with software version 01.06 or higher
- CSE-200 with software version 01.01 or higher
- CS-100 (Huddle) with software version 01.06 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 83.

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

Functionality	IT admin	Support	Key user
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	-
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

XMS 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 XMS 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] only reboot jobs are shown.

1.3 From online to offline access

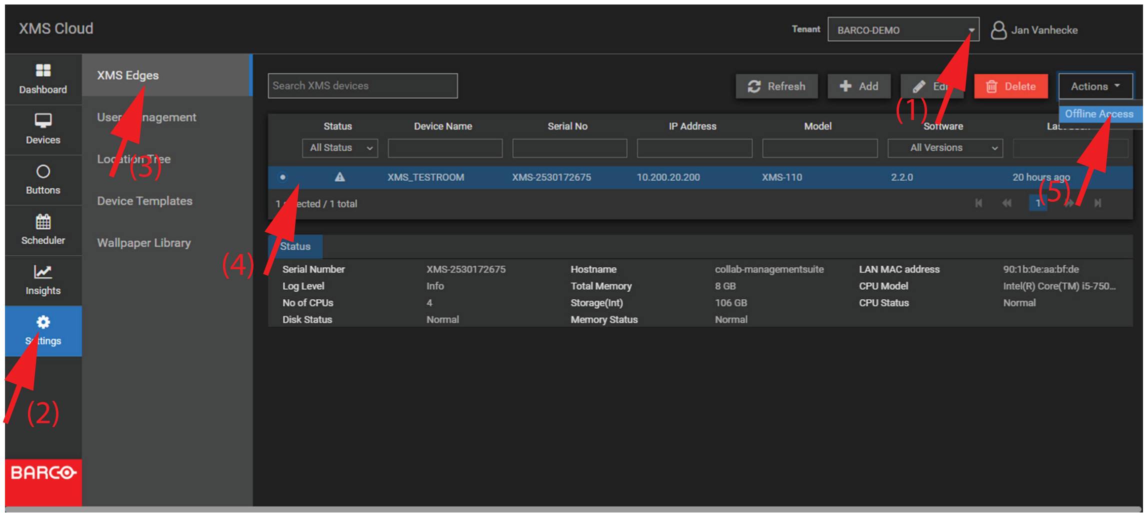
Switching to offline access

XMS (virtual) Edge can act both as a gateway between the Base Units and XMS Cloud, as well as an on-premise management solution for the ClickShare and wePresent Base Units. The device and software are both by default configured as a gateway and require to be manually switched to the offline mode for on-premise management.

Note that in order to switch to the offline mode, the XMS (virtual) Edge first needs to be added to an XMS Cloud tenant.

How to go offline

1. Open XMS cloud in browser environment. Enter the address https://xms.cloud.barco.com in your browser’s address line.
2. Select the correct *Tenant* (1).



	Status	Device Name	Serial No	IP Address	Model	Software	La
●	⚠	XMS_TESTROOM	XMS-2530172675	10.200.20.200	XMS-110	2.2.0	20 hours ago

1 selected / 1 total

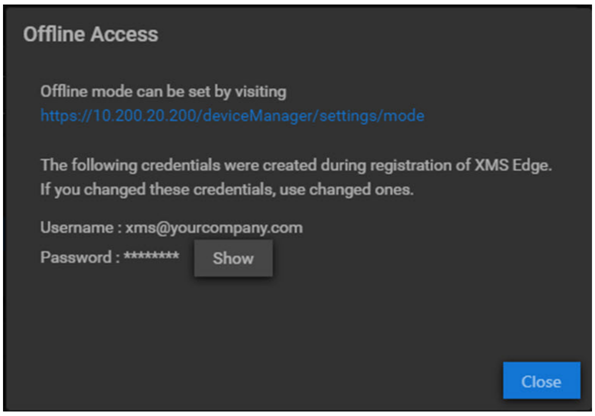
Status

Serial Number	XMS-2530172675	Hostname	collab-managementsuite	LAN MAC address	90:1b:0e:aa:bf:de
Log Level	Info	Total Memory	8 GB	CPU Model	Intel(R) Core(TM) i5-750...
No of CPUs	4	Storage(Int)	106 GB	CPU Status	Normal
Disk Status	Normal	Memory Status	Normal		

Image 1–1

3. Select the **Settings** button (2) and click on **XMS Edge** (3).
4. Select the desired XMS Edge (4).
5. Click on **Actions** and select *Offline access*.

   The offline access window opens with the link and login credentials.



Offline Access

Offline mode can be set by visiting
https://10.200.20.200/deviceManager/settings/mode

The following credentials were created during registration of XMS Edge.
If you changed these credentials, use changed ones.

Username : xms@yourcompany.com
Password : ********

Image 1–2

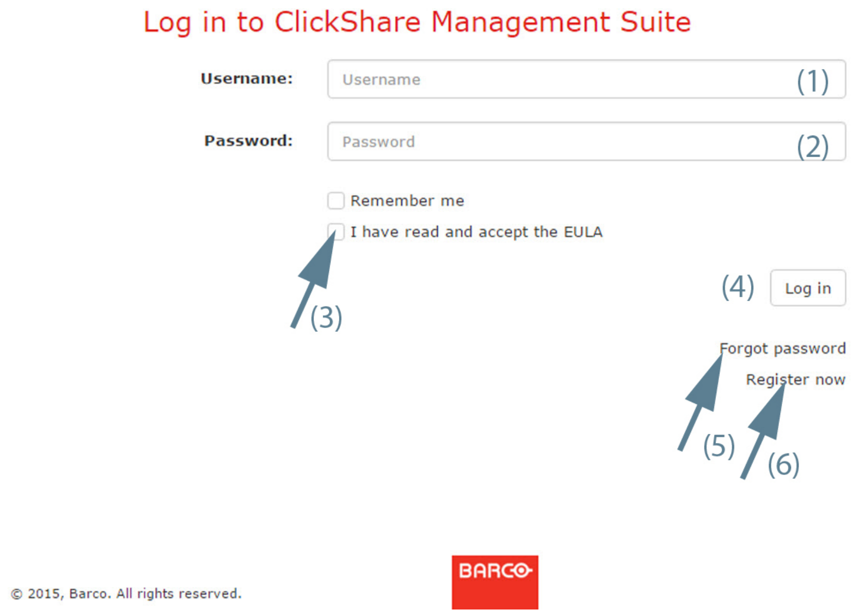
6. Click on the link or copy the link into a separate browser window.

   The login page opens.

1.4 Login in

How to start up

1. Enter your E-mail address (1) and password (2).



Log in to ClickShare Management Suite

Username: Username

Password: Password

□ Remember me

□ I have read and accept the EULA

Log in

Forgot password

Register now

© 2015, Barco. All rights reserved.

Image 1–3 Login

Note: Initial login credentials : user name = **xms@yourcompany.com** and password = **<indicated-on-XMS-Cloud-window>**

2. 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.

3. 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.

4. Click **Login** (4).

   Your login credentials are checked and when valid the *XMS mode* page is displayed.

   Check the checkbox next to *Use XMS in offline mode*. Click **Save changes**. The *Device manager application* is running.

   More information about the Device manager application can be found in "Device Manager Application", page 17

5. If you forgot your password, click on *Forgot password* (5).
6. 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).

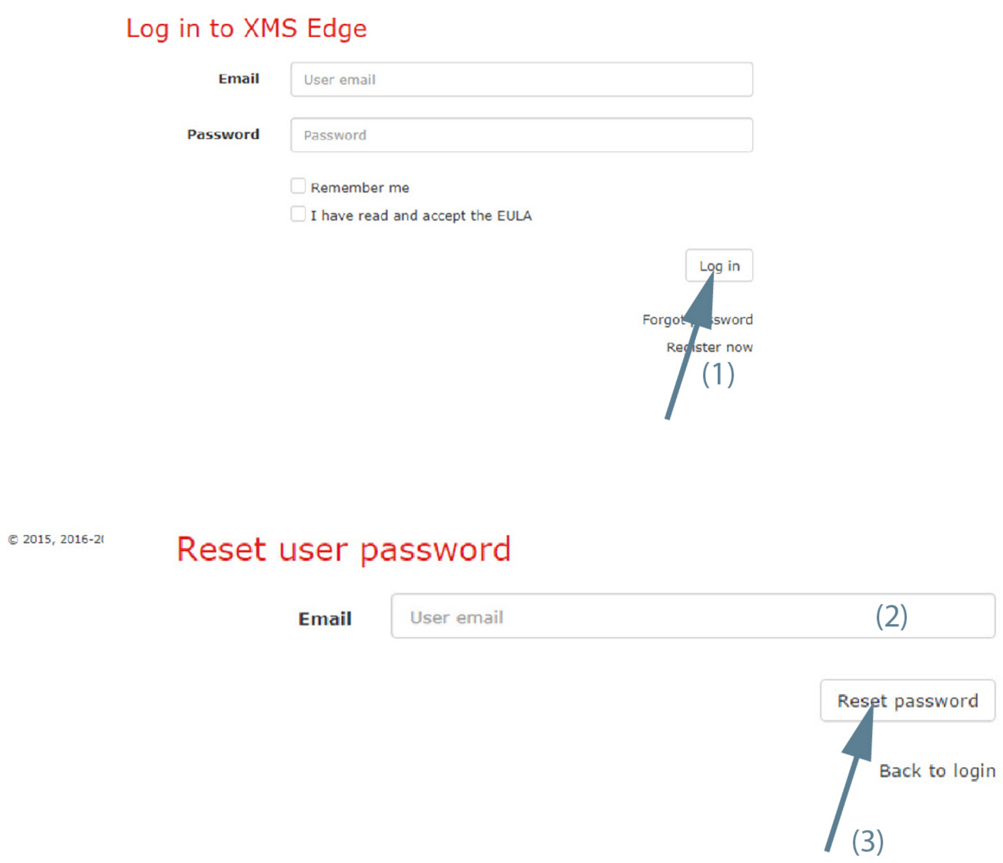


Image 1–4 Forgot password

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 XMS (virtual) Edge. If not, the XMS (virtual) Edge will not be able to send any E-mails to the users.

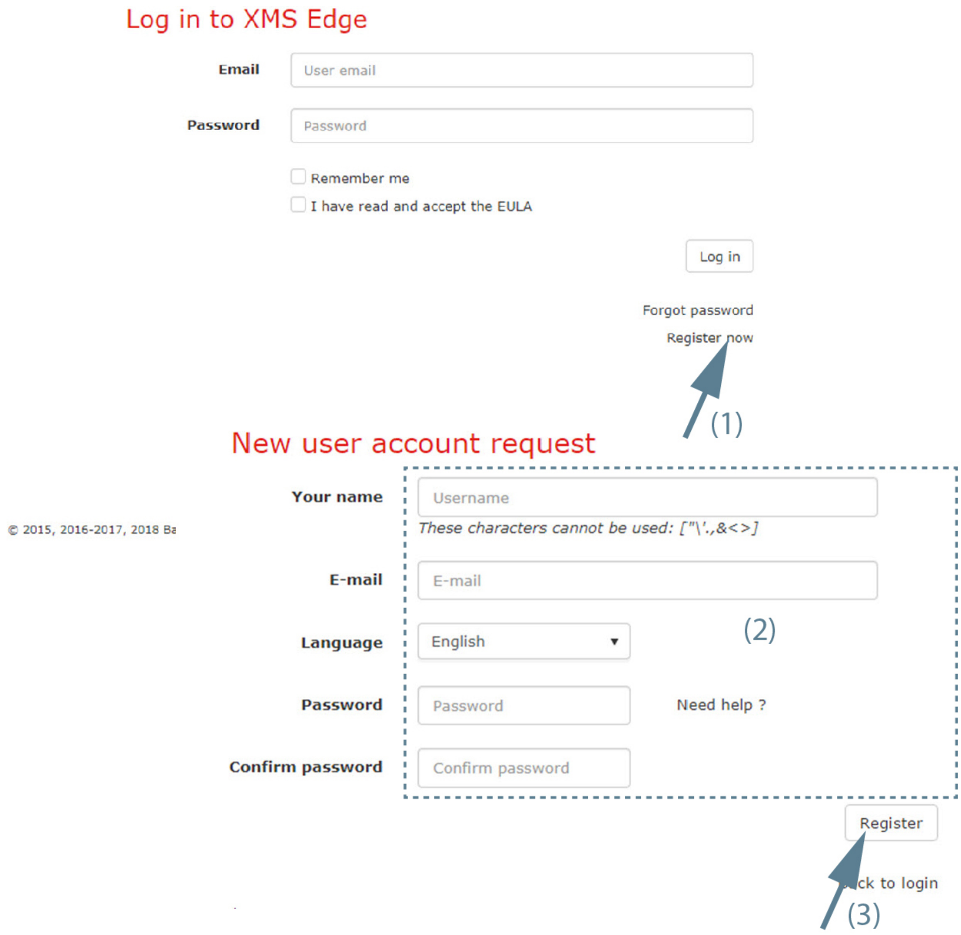
1.6 Register as new user

What can be done?

A new user can request access to XMS (virtual) Edge. 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).



Log in to XMS Edge

Email: User email

Password: Password

□ Remember me

□ I have read and accept the EULA

Log in

Forgot password

Register now

© 2015, 2016-2017, 2018 Ba

New user account request

Your name: Username

These characters cannot be used: ["\'.,&<>]

E-mail: E-mail

Language: English ▾

Password: Password

Need help ?

Confirm password: Confirm password

Register

...ck to login

Image 1–5

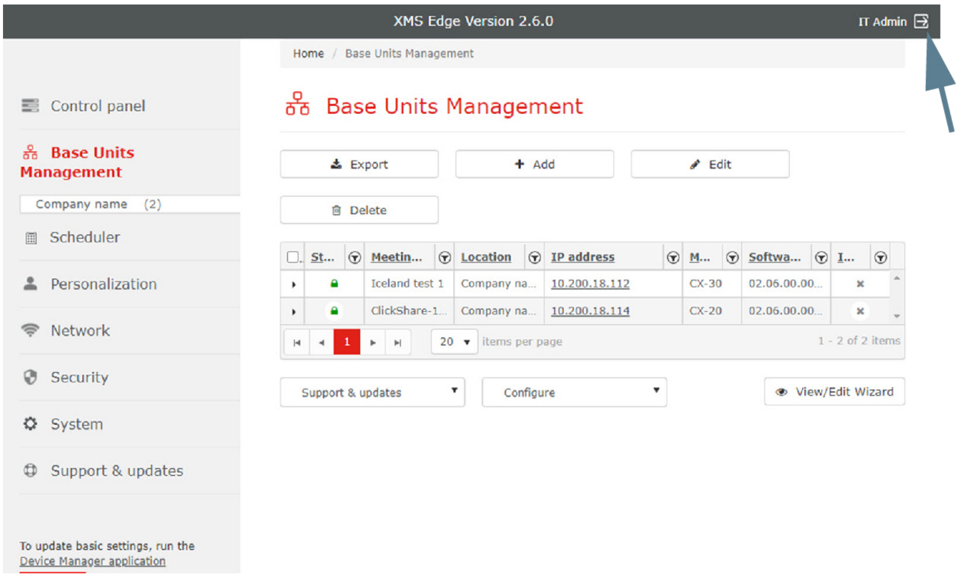
A registration page opens.

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 XMS (virtual) Edge

How to logout

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



□	St...	Meetin...	Location	IP address	M...	Softwa...	I...
▸	🔒	Iceland test 1	Company na...	10.200.18.112	CX-30	02.06.00.00...	✖
▸	🔒	ClickShare-1...	Company na...	10.200.18.114	CX-20	02.06.00.00...	✖

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

To update basic settings, run the Device Manager application

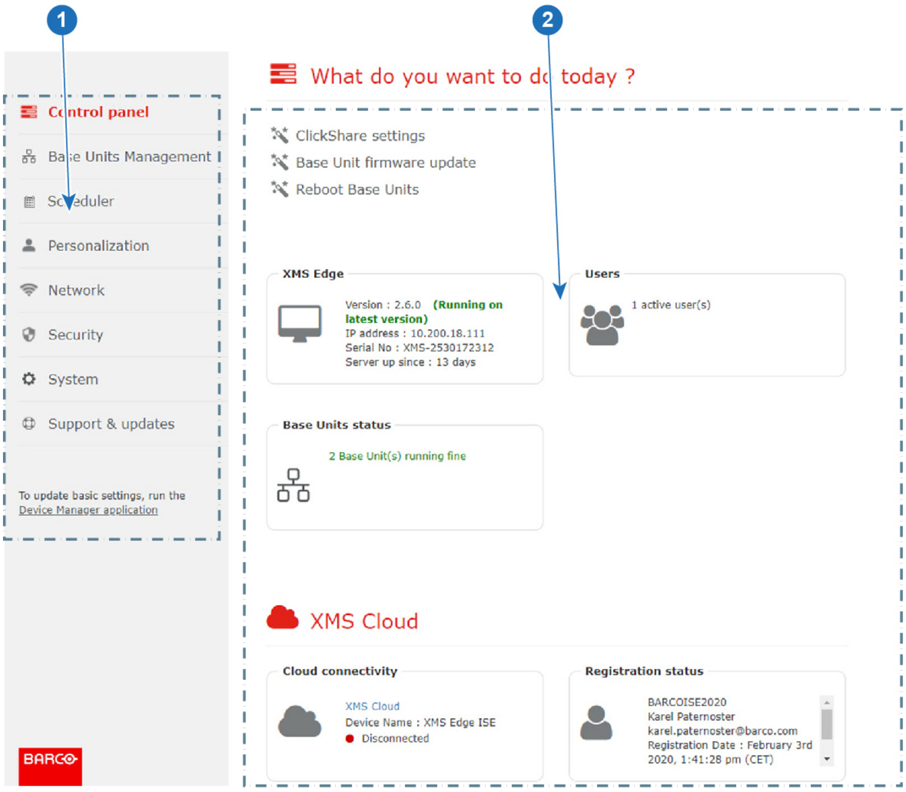
Image 1–6 Logout

Device Manager Application

2

2.1 About the Home page, control panel

Overview



To update basic settings, run the Device Manager application

XMS Edge
Version : 2.6.0 (Running on latest version)
IP address : 10.200.18.111
Serial No : XMS-2530172312
Server up since : 13 days

Users
1 active user(s)

Base Units status
2 Base Unit(s) running fine

Cloud connectivity
XMS Cloud
Device Name : XMS Edge ISE
● Disconnected

Registration status
BARCOISE2020
Karel Paternoster
karel.paternoster@barco.com
Registration Date : February 3rd 2020, 1:41:28 pm (CET)

Image 2–1 Home page overview

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

1 Menu pane.

The following main menus are available:

- Control panel
- Base Unit Management
- 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
- Reboot Base Units
- XMS (virtual) Edge overview
- Users overview
- Base Unit statuses
- New Base Units discovered (only for ClickShare (CSE range) and ClickShare Conference)

- New firmware(s) available
- XMS Cloud Registration status
- Cloud connectivity

Explanation of wizards

- Base Unit status will guide you to a Base Units overview, see “Base Units page”, page 28 to continue.
- Users will guide you to the users page. For more info, seeé“Users”, page 78 to continue.
- New firmware will start the firmware wizard, see “Firmwares”, page 85 to continue.
- Auto-discovered Base Units will guide you to the auto-discover wizard, see “Auto discovering of Base Units”, page 30 to continue.

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

2.2 Network, LAN settings

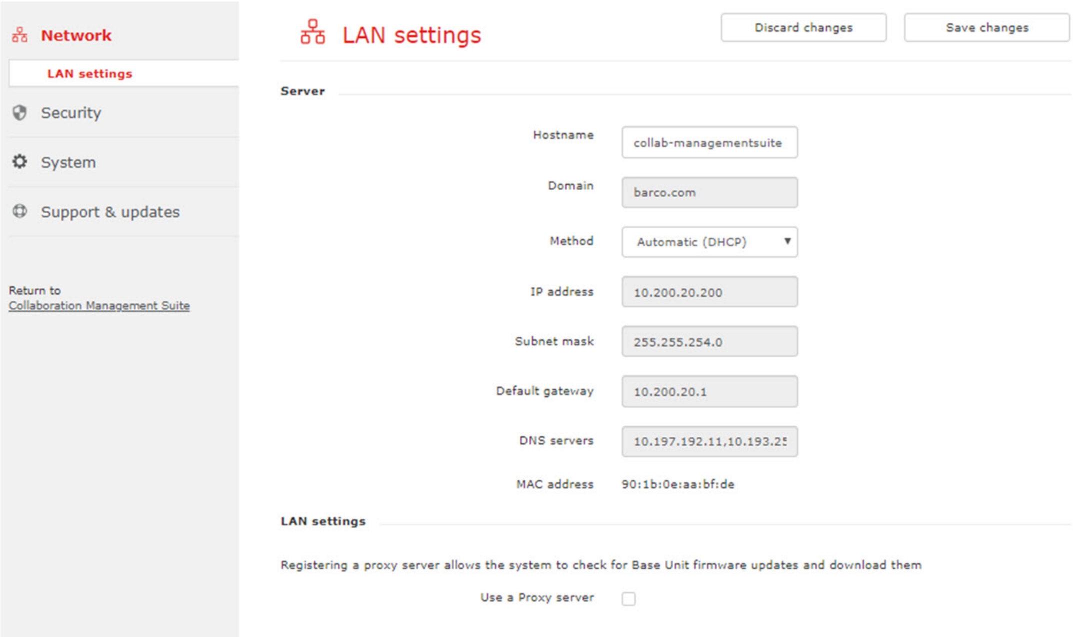
About LAN settings

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.



Hostname: collab-managementsuite

Domain: barco.com

Method: Automatic (DHCP)

IP address: 10.200.20.200

Subnet mask: 255.255.254.0

Default gateway: 10.200.20.1

DNS servers: 10.197.192.11,10.193.25

MAC address: 90:1b:0e:aa:bf:de

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

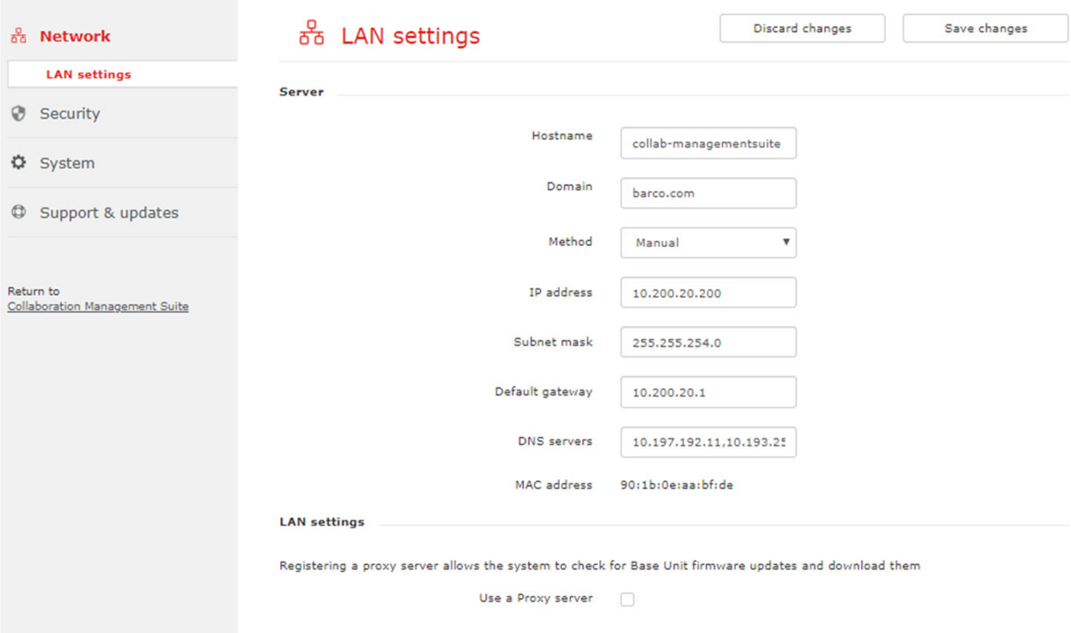
Use a Proxy server □

Image 2–2 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*.



LAN settings

Server

Hostname: collab-managementsuite

Domain: barco.com

Method: Manual

IP address: 10.200.20.200

Subnet mask: 255.255.254.0

Default gateway: 10.200.20.1

DNS servers: 10.197.192.11,10.193.2!

MAC address: 90:1b:0e:aa:bf:de

LAN settings

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

Use a Proxy server □

Image 2–3 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!).

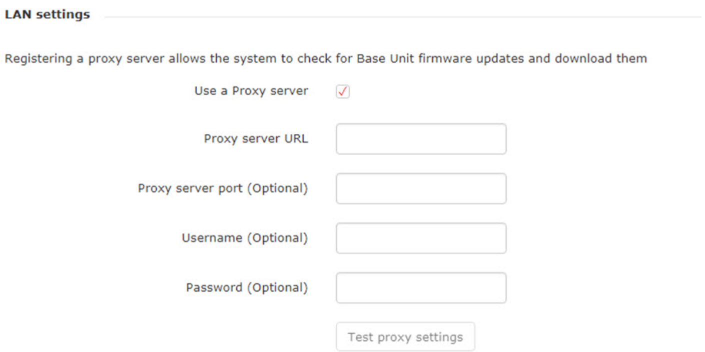
   Note: This must NOT be 0.0.0.0.
   If there is no router on the local subnet then just set this field to any IP-Address on the subnet.

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.



LAN settings

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

Use a Proxy server ☑

Proxy server URL:

Proxy server port (Optional):

Username (Optional):

Password (Optional):

Image 2–4 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.

2.3 Security, deploy SSL certificate

About SSL certificate

The SSL certificate is used for secure communication between the XMS (virtual) Edge 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 XMS (virtual) Edge as a secure site. With the current certificates from XMS (virtual) Edge, 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 XMS (virtual) Edge.

How to deploy

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

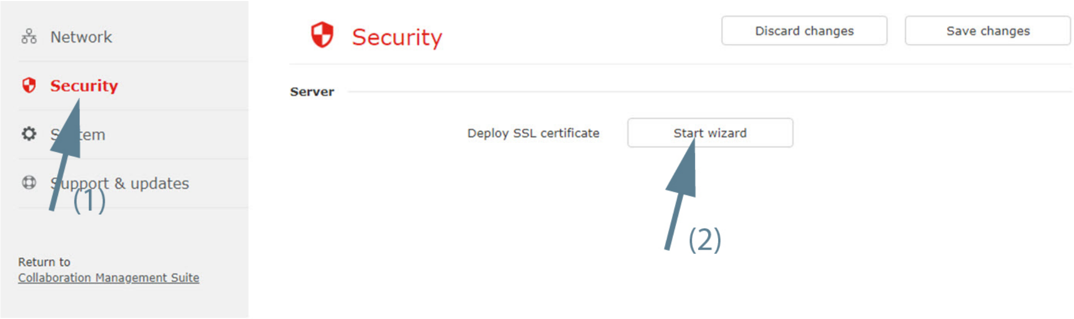
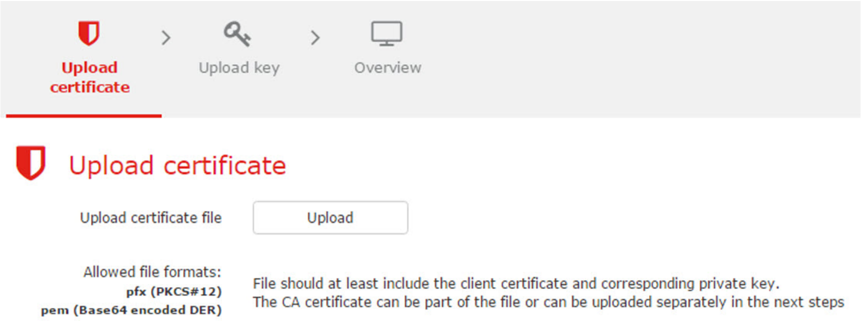


Image 2–5

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



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

Image 2–6 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.

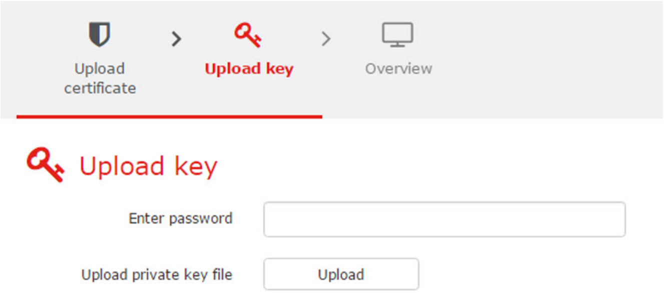


Image 2–7 Upload key

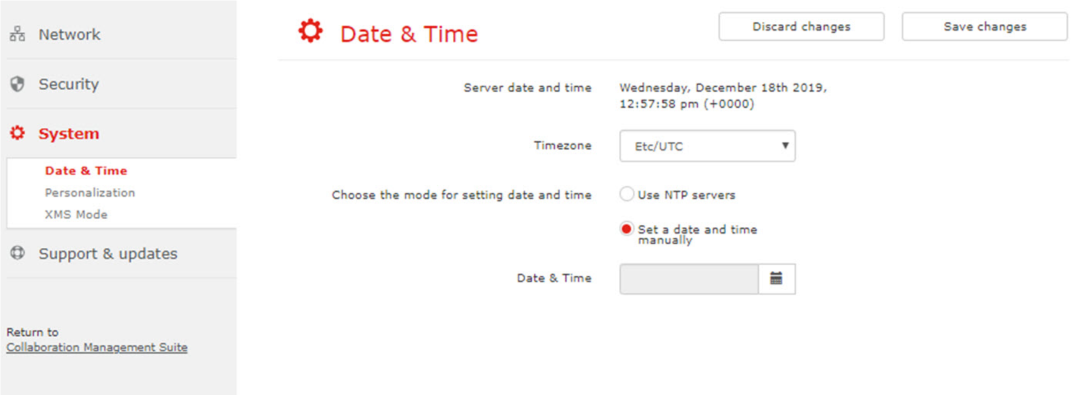
An *Overview* window is displayed.

5. Click **Finish**.

2.4 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



Server date and time: Wednesday, December 18th 2019, 12:57:58 pm (+0000)

Timezone: Etc/UTC

Choose the mode for setting date and time: ○ Use NTP servers ● Set a date and time manually

Date & Time:

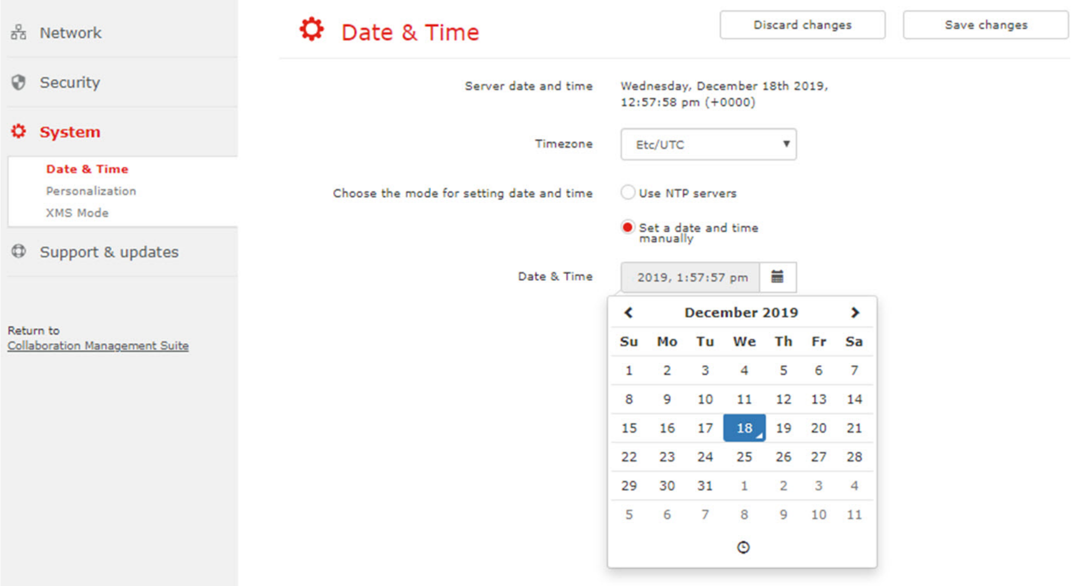
Image 2–8 Timezone and NTP server

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.



Date & Time

Server date and time: Wednesday, December 18th 2019, 12:57:58 pm (+0000)

Timezone: Etc/UTC

Choose the mode for setting date and time: ○ Use NTP servers ● Set a date and time manually

Date & Time: 2019, 1:57:57 pm

December 2019

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

Image 2–9 Date & time

6. Click **Save changes**.

2.5 Personalization

About personalization

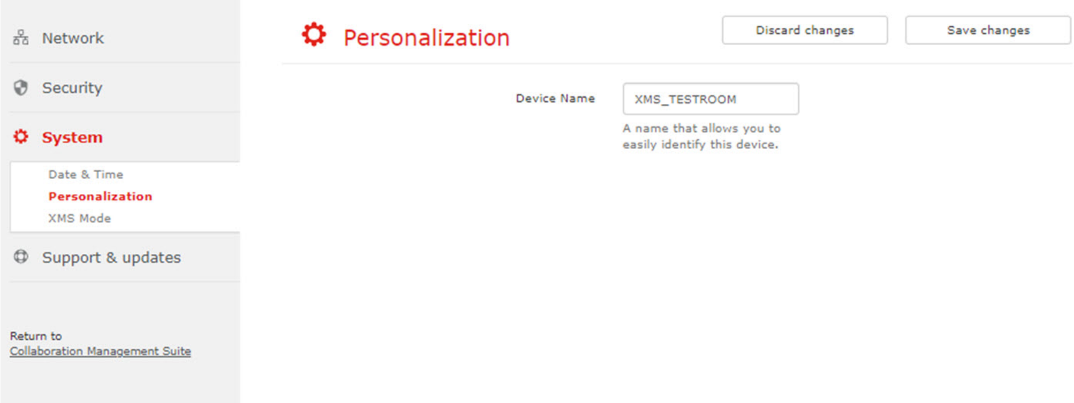
The current name of the XMS (virtual) Edge server can be changed to a new name.

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.



Personalization

Device Name: XMS_TESTROOM

A name that allows you to easily identify this device.

Image 2–10 Personalization of XMS

3. Click **Save changes**.

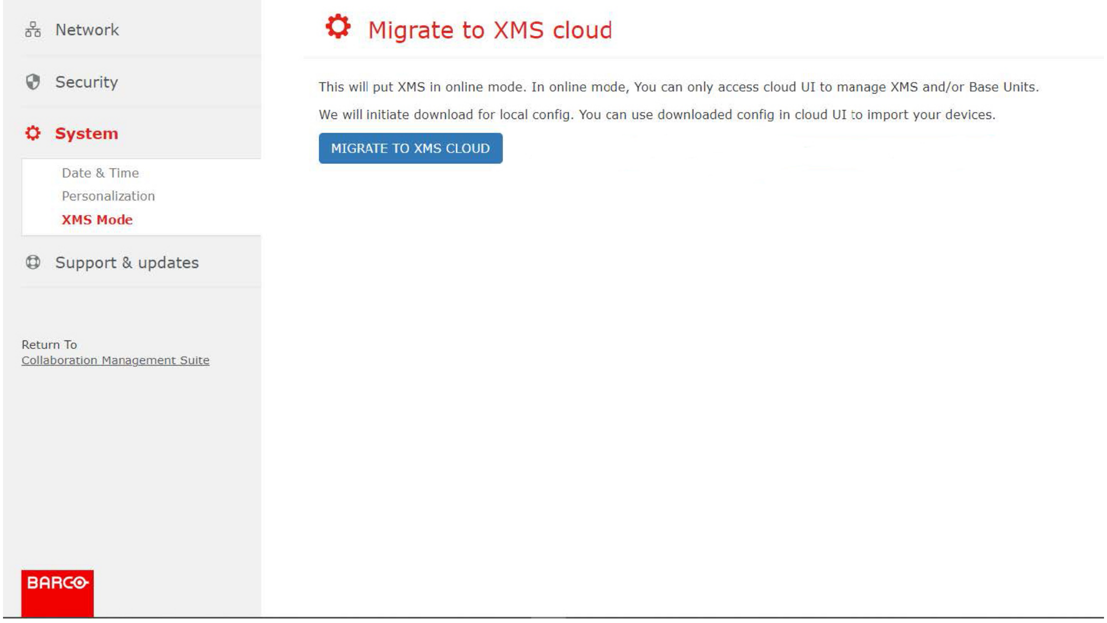
2.6 XMS Mode

What can be done?

The XMS mode can be switched between online and offline. When in online mode, you can only access cloud UI to manage XMS and/or Base Units.

How to change the mode

1. In the menu pane, select *System* → *XMS Mode*.



This will put XMS in online mode. In online mode, You can only access cloud UI to manage XMS and/or Base Units.

We will initiate download for local config. You can use downloaded config in cloud UI to import your devices.

Image 2–11

2. To use XMS in online mode, check the check box next to *XMS in online mode*.

2.7 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**.

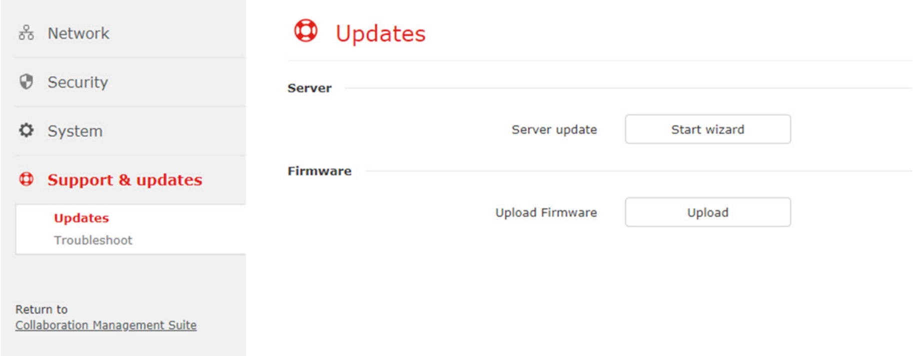
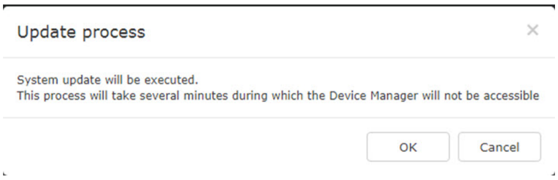


Image 2–12 Server Updates

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

   A message is diplayed.



System update will be executed.
This process will take several minutes during which the Device Manager will not be accessible

Image 2–13

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**.

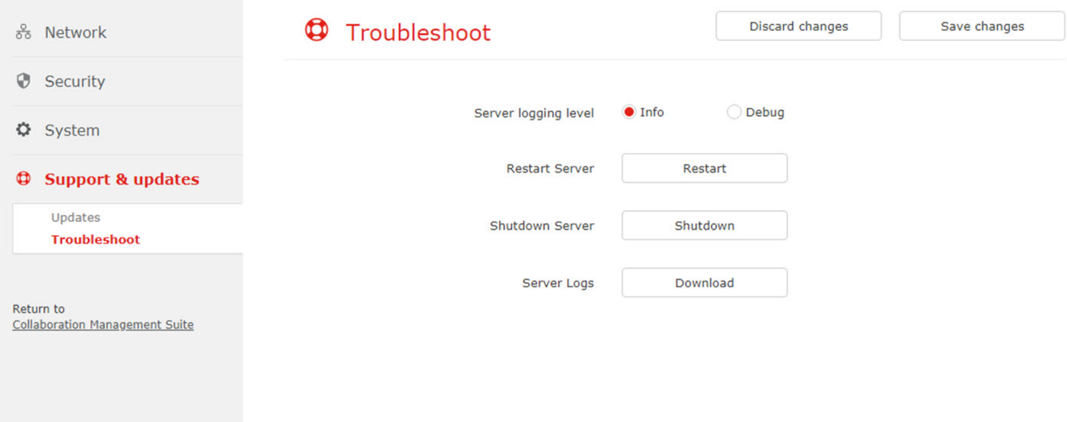
   The firmware will be uploaded.

2.8 Troubleshoot

Server logging level

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

Click on the desired radio button to select.



Server logging level ● Info ○ Debug

Restart Server

Shutdown Server

Server Logs

Image 2–14

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*.

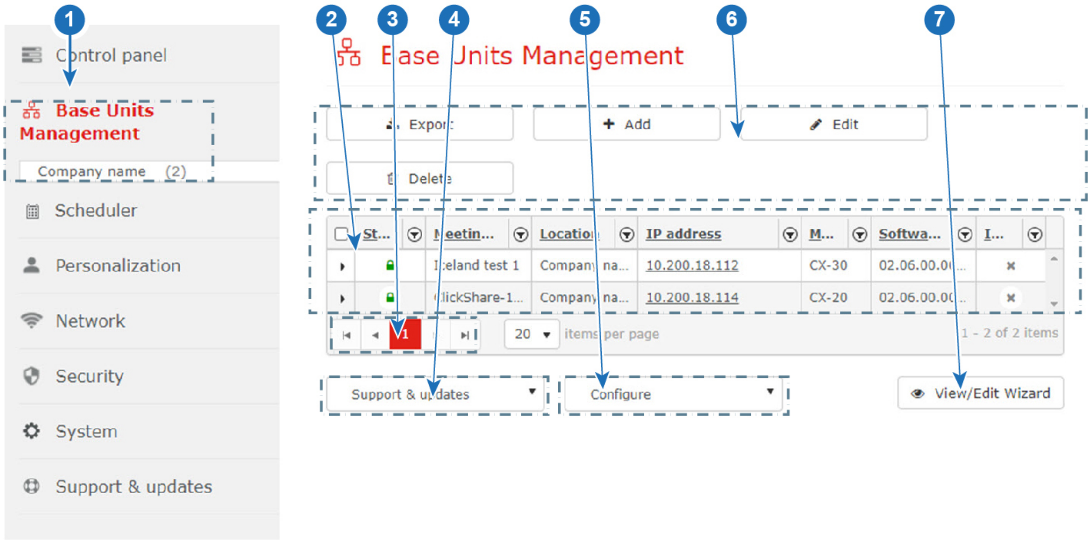
XMS (virtual) Edge 3

3.1 Base Units page

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

3.1.1 About the Base Units Management page

Overview



St...	Meetin...	Locatio...	IP address	M...	Softwa...	I...
🔒	Iceland test 1	Company na...	10.200.18.112	CX-30	02.06.00.0(...	×
🔒	ClickShare-1...	Company na...	10.200.18.114	CX-20	02.06.00.0(...	×

Image 3–1 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[2]:

- 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 XMS (virtual) Edge.
- 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.

[2] Views differ with every account type

- nothing (empty), for devices unknown by XMS.

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**.

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 theBase Units

6 Tool bar to export, add, edit or delete Base Units on the page.

7 To start up the view/edit wizard to configure the Base Units.

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

XMS (virtual) Edge 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

- XMS (virtual) Edge was not able to enforce the XMS user preference wrt. Base Unit HTTP/HTTPS communication
- XMS (virtual) Edge was not able to enforce the Base Unit password requested by the XMS user.
- Base Unit is running a very old firmware version that does not allow XMS 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
- XMS (virtual) Edge determined that the added device is not a Base Unit hence should be removed from XMS

Gray triangle

XMS (virtual) Edge 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 XMS and the Base Unit : user should use the Diagnostics page to find out more details.

3.1.2 Auto discovering of Base Units

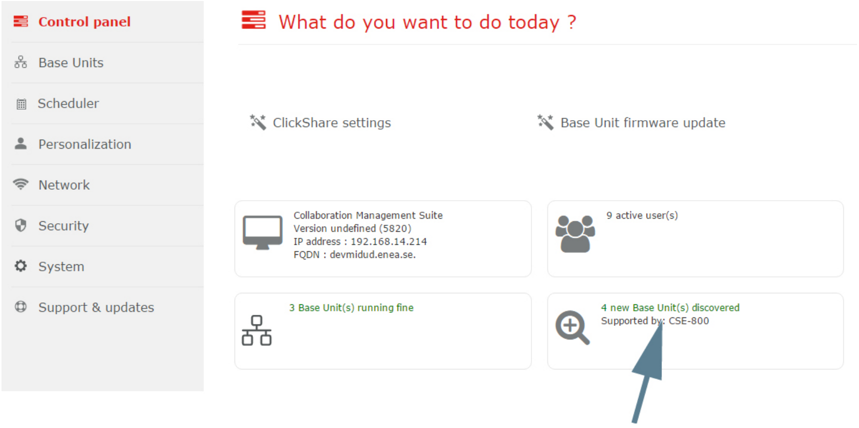
Only for CSE device range.

What can be done?

New CSE device Base Units on your network might be automatically detected if the XMS (virtual) Edge has the default hostname, or if the user entered the correct XMS (virtual) Edge 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 XMS (virtual) Edge list of available Base Units.

Auto discovery

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



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

9 active user(s)

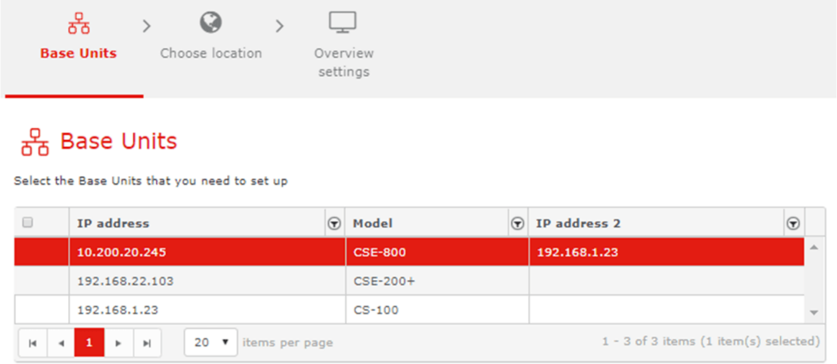
3 Base Unit(s) running fine

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

Image 3–2 Auto-discover Base Units

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

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



Base Units

Select the Base Units that you need to set up

□	IP address	Model	IP address 2
	10.200.20.245	CSE-800	192.168.1.23
	192.168.22.103	CSE-200+	
	192.168.1.23	CS-100	

Image 3–3 Select Base Units

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

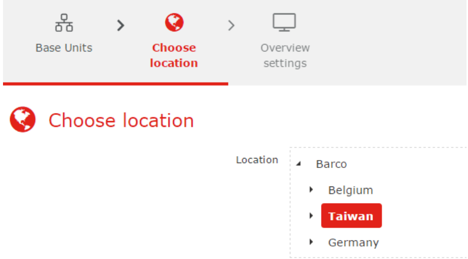
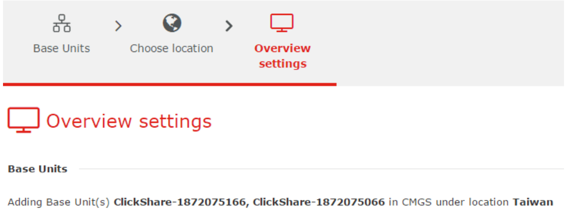


Image 3–4 Choose location

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

4. Click **OK** to continue.

An overview of the settings is displayed.



Base Units

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

Image 3–5 Overview settings

5. Click **Finish**.

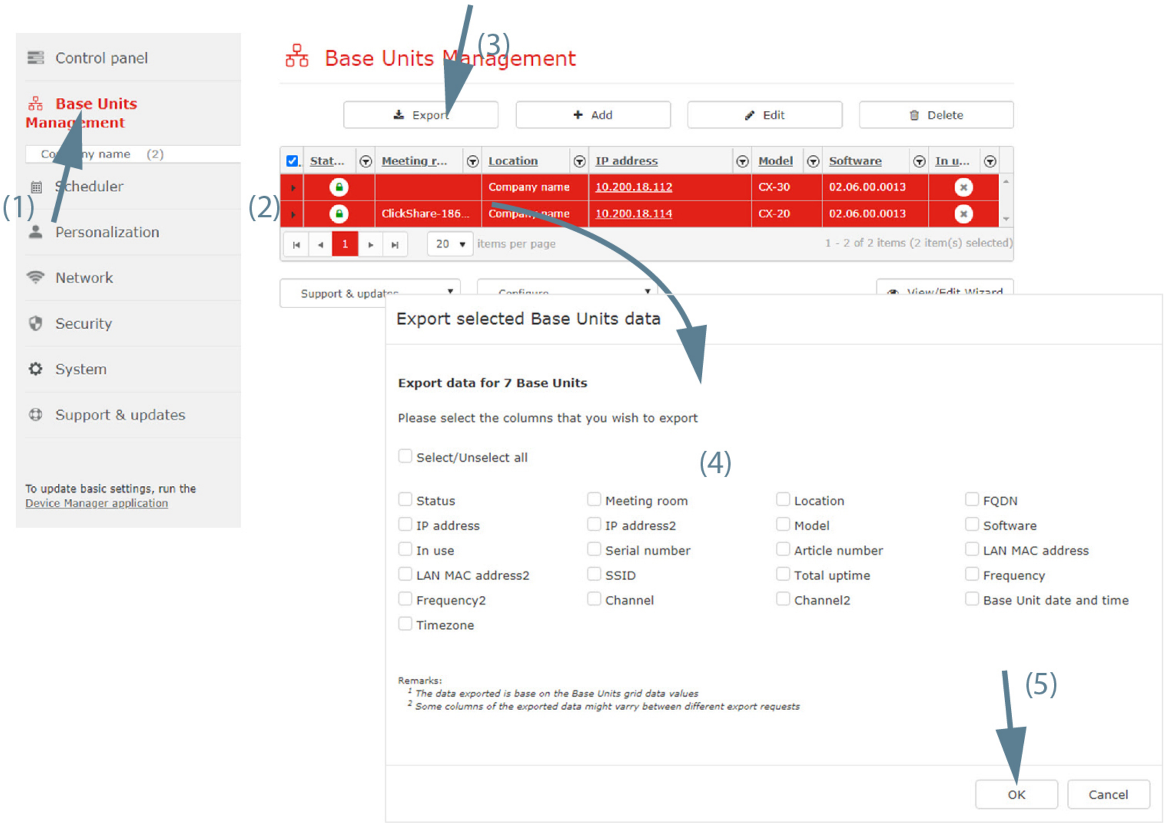
3.1.3 Export Base Unit list

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).



To update basic settings, run the Device Manager application

☑	Stat...	Meeting r...	Location	IP address	Model	Software	In u...
	🔒		Company name	10.200.18.112	CX-30	02.06.00.0013	✖
	🔒	ClickShare-186...	Company name	10.200.18.114	CX-20	02.06.00.0013	✖

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

Export selected Base Units data

Export data for 7 Base Units

Please select the columns that you wish to export

□ Select/Unselect all

□ Status
□ IP address
□ In use
□ LAN MAC address2
□ Frequency2
□ Timezone
□ Meeting room
□ IP address2
□ Serial number
□ SSID
□ Channel
□ Location
□ Model
□ Article number
□ Total uptime
□ Channel2
□ FQDN
□ Software
□ LAN MAC address
□ Frequency
□ Base Unit date and time

Remarks:
[1] *The data exported is base on the Base Units grid data values*
[2] *Some columns of the exported data might varry between different export requests*

Image 3–6 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.

3.1.4 Add new Base Unit(s)

About adding Base Units

New Base Units on the network can be added to the XMS (virtual) Edge.

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.

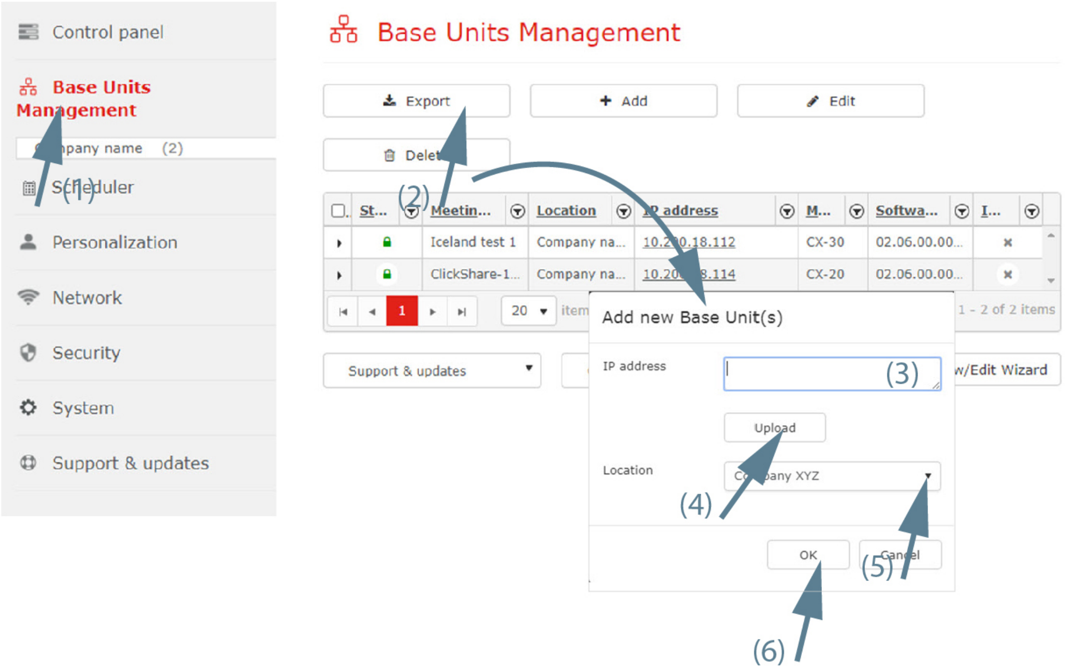


Image 3–7 Add Base Unit

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.

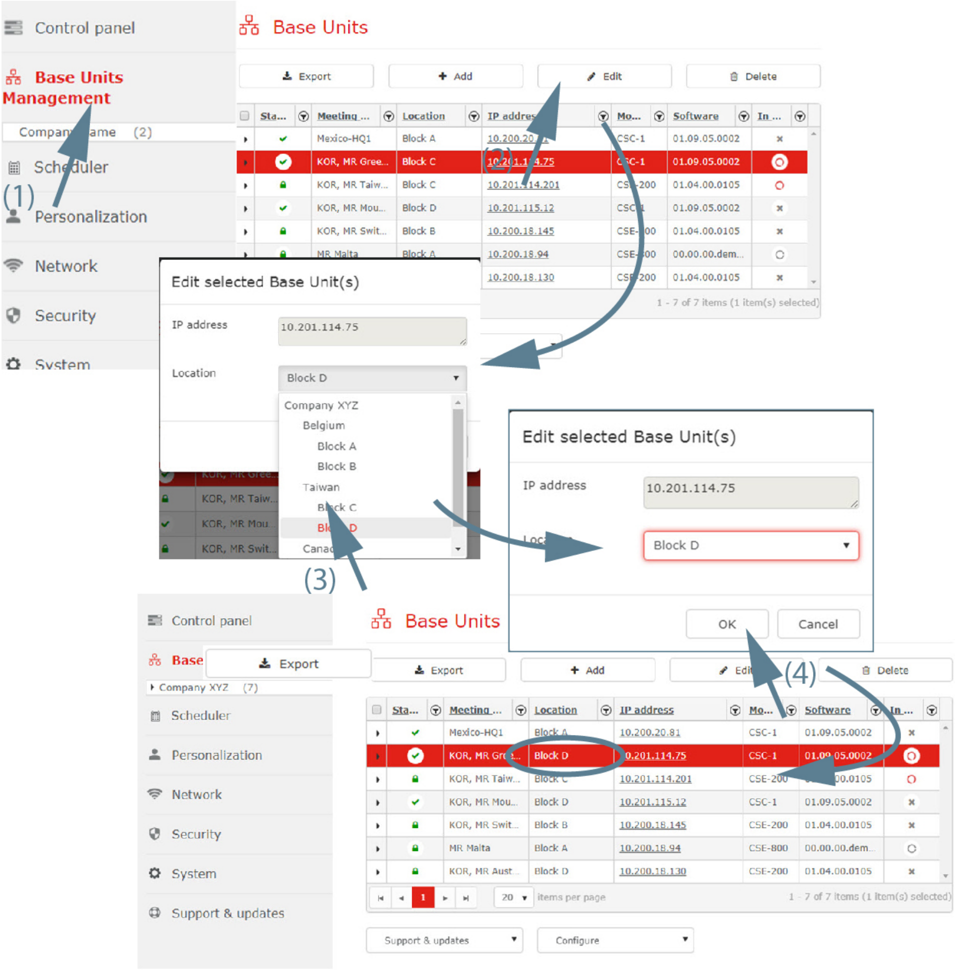
3.1.5 Edit selected Base Unit(s)

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).



Edit selected Base Unit(s)

IP address: 10.201.114.75

Location: Block D

	Sta...	Meeting ...	Location	IP address	Mo...	Software	In ...
▸	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
▸	✓	KOR, MR Gre...	Block D	10.201.114.75	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Taiw...	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
▸	✓	KOR, MR Mou...	Block D	10.201.115.12	CSC-1	01.09.05.0002	✖
▸	🔒	KOR, MR Swit...	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
▸	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.dem...	○
▸	🔒	KOR, MR Aust...	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

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

Image 3–8 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 XMS (virtual) Edge

How it works:

1. client manually adds Base Unit in XMS by IP Address or Hostname
2. XMS - 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 XMS database and it will be used from this moment on

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

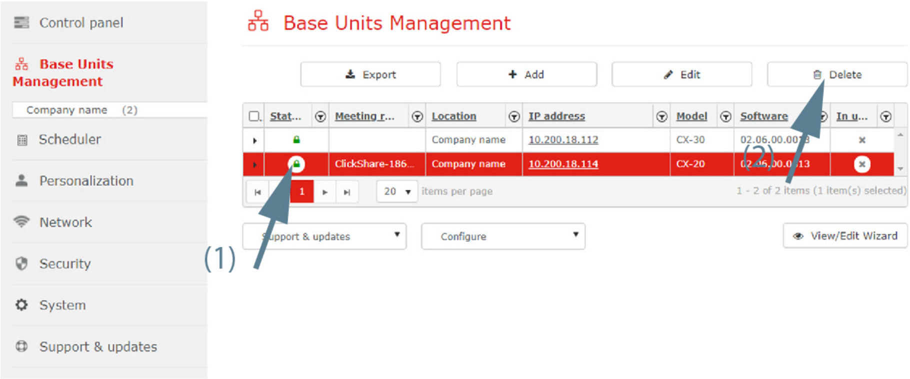
3.1.6 Delete selected Base Unit(s)

About deleting Base Units

Multiple Base Units can be removed from XMS (virtual) Edge at the same time.

How to delete

1. Select the Base Units to delete.



□	Stat...	Meeting r...	Location	IP address	Model	Software	In u...
▸	🔒		Company name	10.200.18.112	CX-30	02.06.00.0018	×
▸	🔒	ClickShare-186...	Company name	10.200.18.114	CX-20	02.06.00.0013	×

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

Image 3–9 Delete Base Unit

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

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

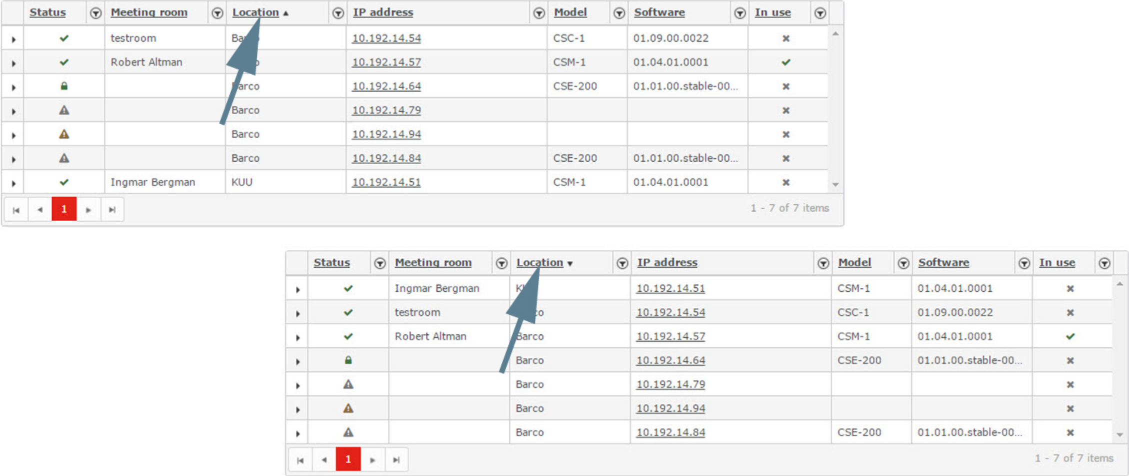
3. Press **OK** to delete the Base Unit(s).

3.1.7 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.



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

1 · 1 - 7 of 7 items

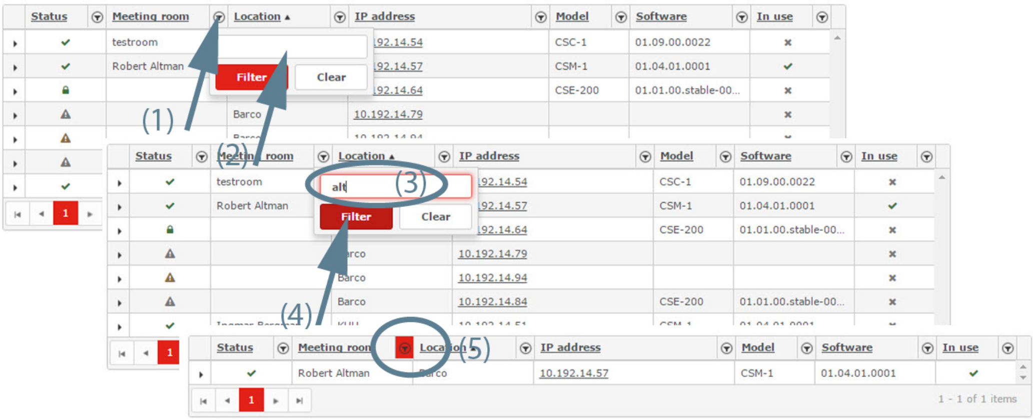
	Status	Meeting room	Location ▾	IP address	Model	Software	In use
▸	✓	Ingmar Bergman	KUU	10.192.14.51	CSM-1	01.04.01.0001	×
▸	✓	testroom	Barco	10.192.14.54	CSC-1	01.09.00.0022	×
▸	✓	Robert Altman	Barco	10.192.14.57	CSM-1	01.04.01.0001	✓
▸	🔒		Barco	10.192.14.64	CSE-200	01.01.00.stable-00...	×
▸	⚠		Barco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

1 · 1 - 7 of 7 items

Image 3–10 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.



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

1 - 1 of 1 items

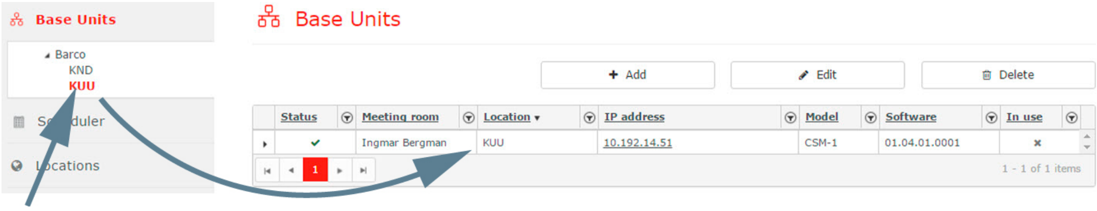
Image 3–11 Filtering overview

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'.



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

1 - 1 of 1 items

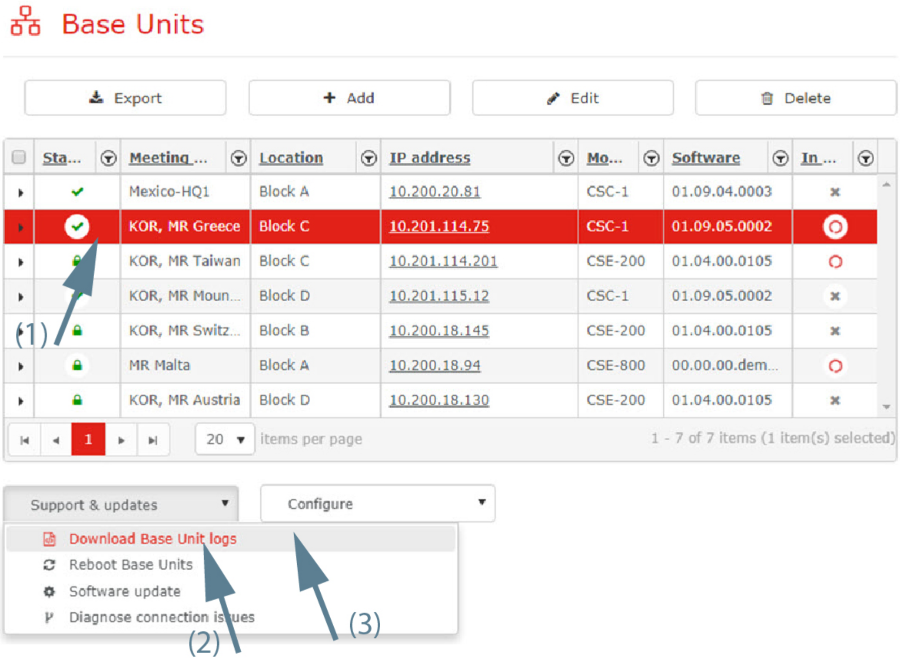
Image 3–12 Filtering via tree

3.1.8 Support and updates

3.1.8.1 Download Base Unit log

How to download

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



Sta...	Meeting ...	Location	IP address	Mo...	Software	In ...
✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.04.0003	✖
✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	○
	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	KOR, MR Moun...	Block D	10.201.115.12	CSC-1	01.09.05.0002	✖
🔒	KOR, MR Switz...	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.dem...	○
🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

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

Image 3–13 Download Bas Unit logs

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

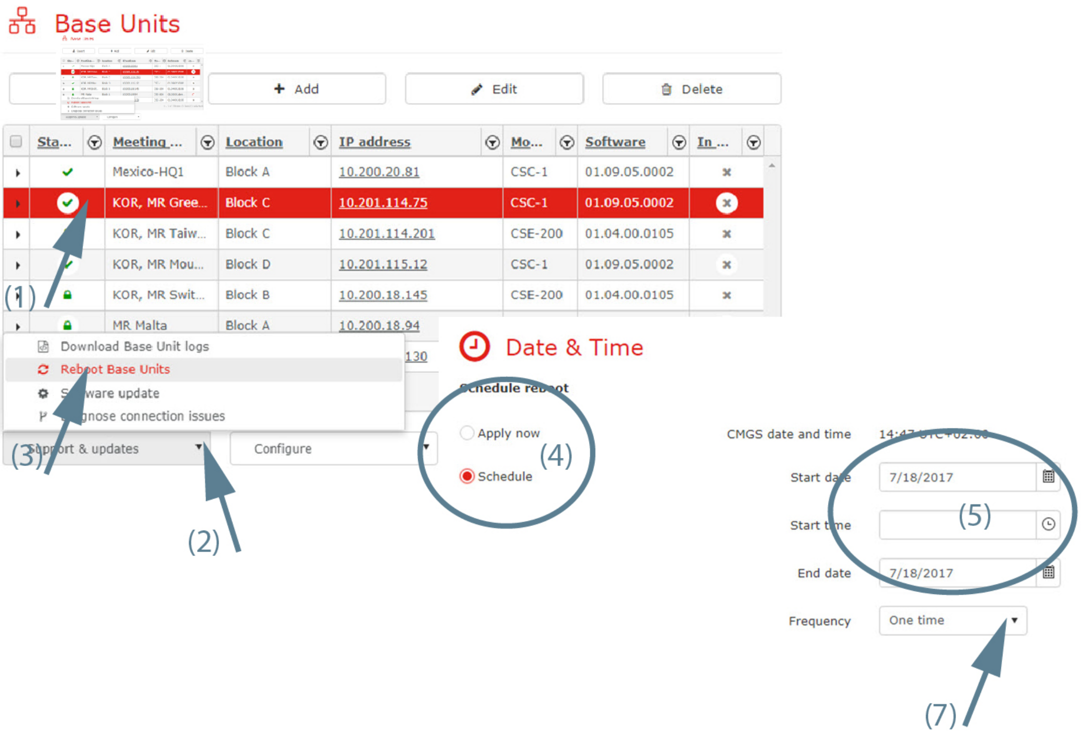
   A message is displayed: “Download Base Unit logs, please wait”.

   The logging file will be saved automatically on your PC.

3.1.8.2 Reboot Base Units

How to reboot

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



Sta...	Meeting ...	Location	IP address	Mo...	Software	In ...
✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
✓	KOR, MR Gree...	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
	KOR, MR Taiw...	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
✓	KOR, MR Mou...	Block D	10.201.115.12	CSC-1	01.09.05.0002	✖
🔒	KOR, MR Swit...	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
🔒	MR Malta	Block A	10.200.18.94			

Schedule reboot

○ Apply now

● Schedule

CMGS date and time 14:47 UTC+02:00

Start date 7/18/2017

Start time

End date 7/18/2017

Frequency One time

Image 3–14 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.

3.1.8.3 Software update

About software update

The firmware of a single Base Unit or of multiple Base Units can be updated with XMS (virtual) Edge. The update can be executed immediately or it can be scheduled.

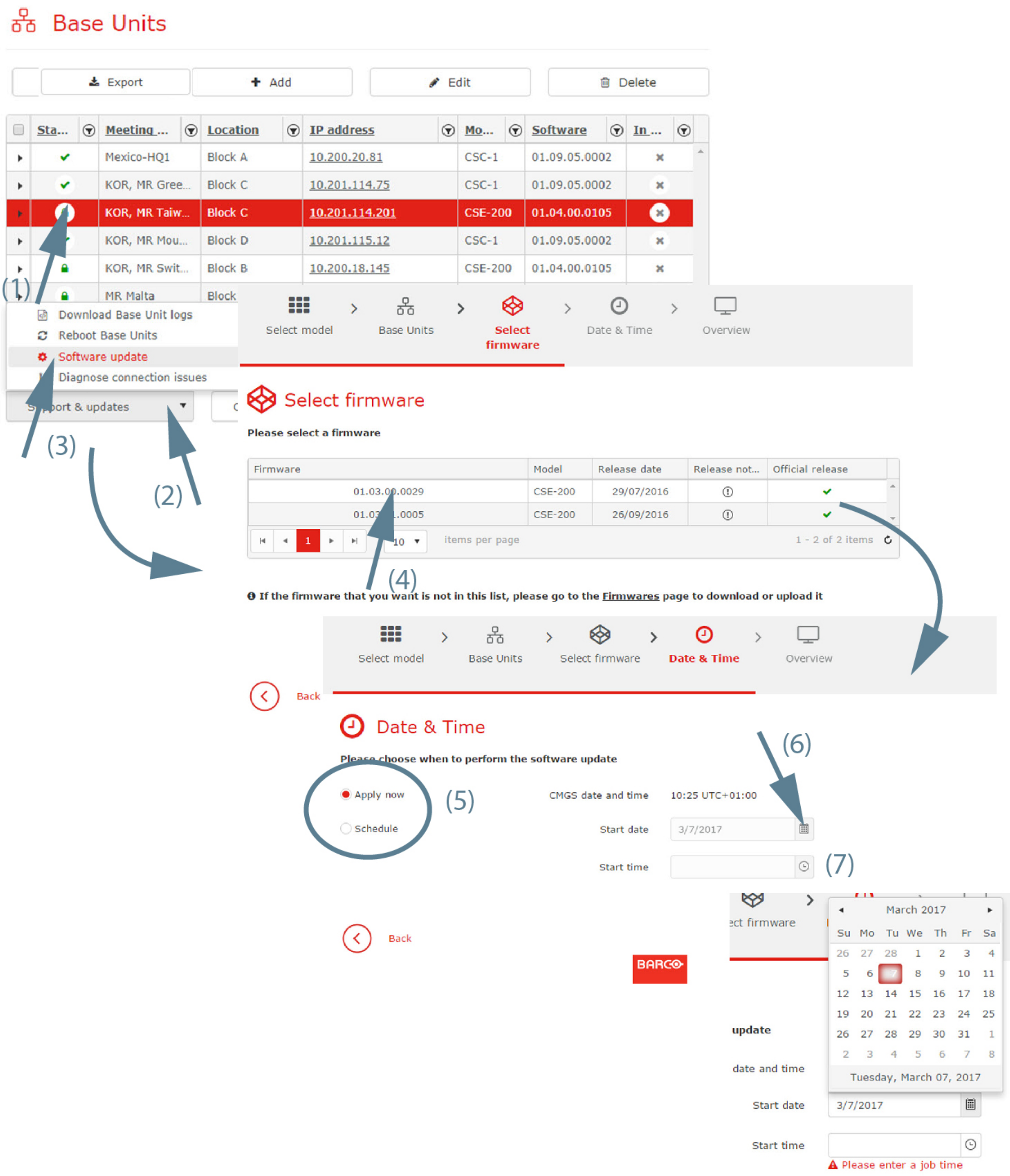
The Base Unit firmware must be loaded on the XMS (virtual) Edge, prior the update. XMS (virtual) Edge may directly download a firmware from Barco site, or the firmware may be uploaded to XMS (virtual) Edge.

Before a firmware update can take place, the firmware must be available on the XMS (virtual) Edge. For more info, see "Firmwares", page 85

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.



Sta...	Meeting ...	Location	IP address	Mo...	Software	In ...
✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	×
✓	KOR, MR Gree...	Block C	10.201.114.75	CSC-1	01.09.05.0002	×
	KOR, MR Taiw...	Block C	10.201.114.201	CSE-200	01.04.00.0105	×
	KOR, MR Mou...	Block D	10.201.115.12	CSC-1	01.09.05.0002	×
	KOR, MR Swit...	Block B	10.200.18.145	CSE-200	01.04.00.0105	×
	MR Malta	Block				

Please select a firmware

Firmware	Model	Release date	Release not...	Official release
01.03.00.0029	CSE-200	29/07/2016	ⓘ	✓
01.03.00.0005	CSE-200	26/09/2016	ⓘ	✓

1 · 10 items per page · 1 - 2 of 2 items

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

Please choose when to perform the software update

● Apply now

○ Schedule

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

Start date 3/7/2017

Start time

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

March 2017 · Tuesday, March 07, 2017

update

date and time

Start date 3/7/2017

Start time

Please enter a job time

Image 3–15 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 button in front of **Schedule**. To change the date, click on the calendar icon (6) and select the date (7). Enter the time (hh:mm) or click on the clock icon, then select a predefined time.

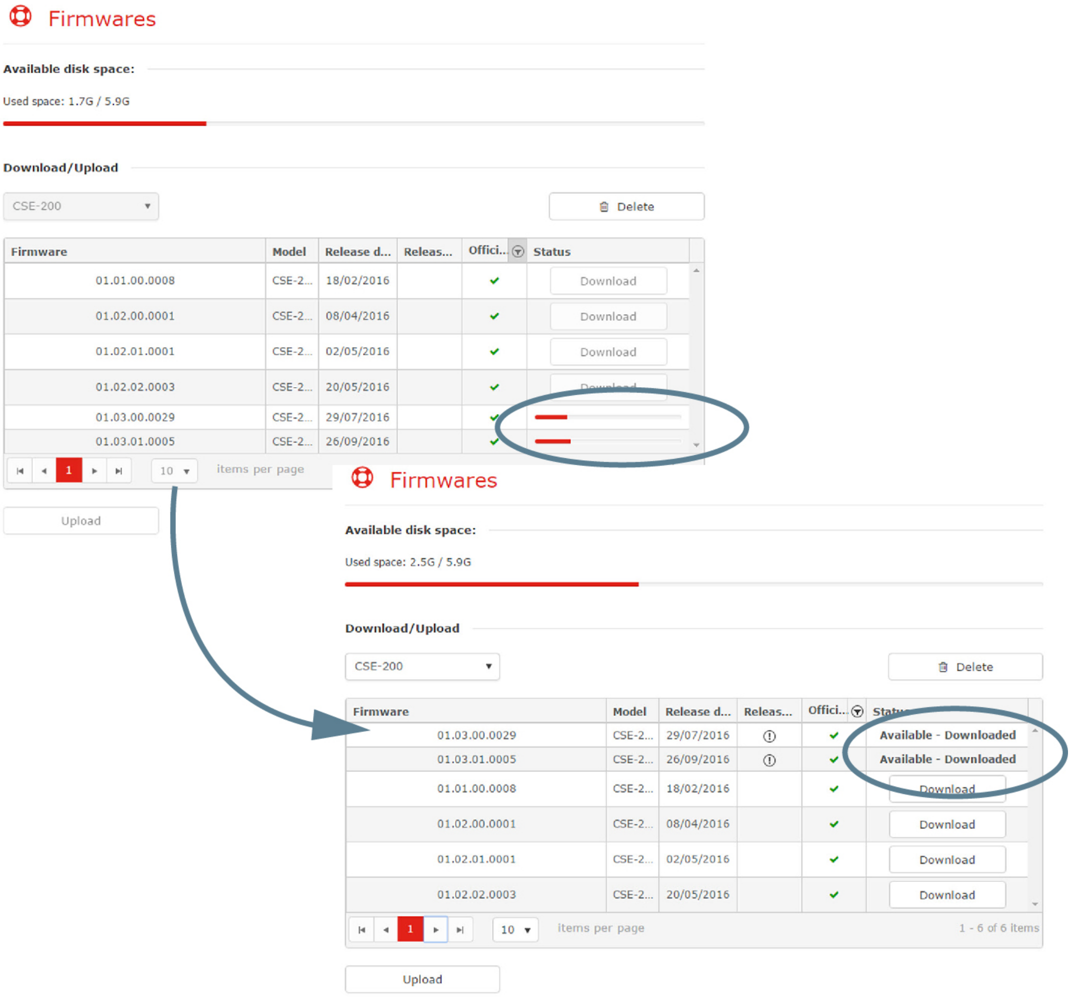
5. Click **OK**.

Download firmware

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

   The possible firmware for that model are displayed.

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



Firmwares

Available disk space:

Used space: 1.7G / 5.9G

Download/Upload

CSE-200 ▾ | Delete

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

1 | 10 ▾ items per page

Upload

Firmwares

Available disk space:

Used space: 2.5G / 5.9G

Download/Upload

CSE-200 ▾ | Delete

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

1 | 10 ▾ items per page | 1 - 6 of 6 items

Upload

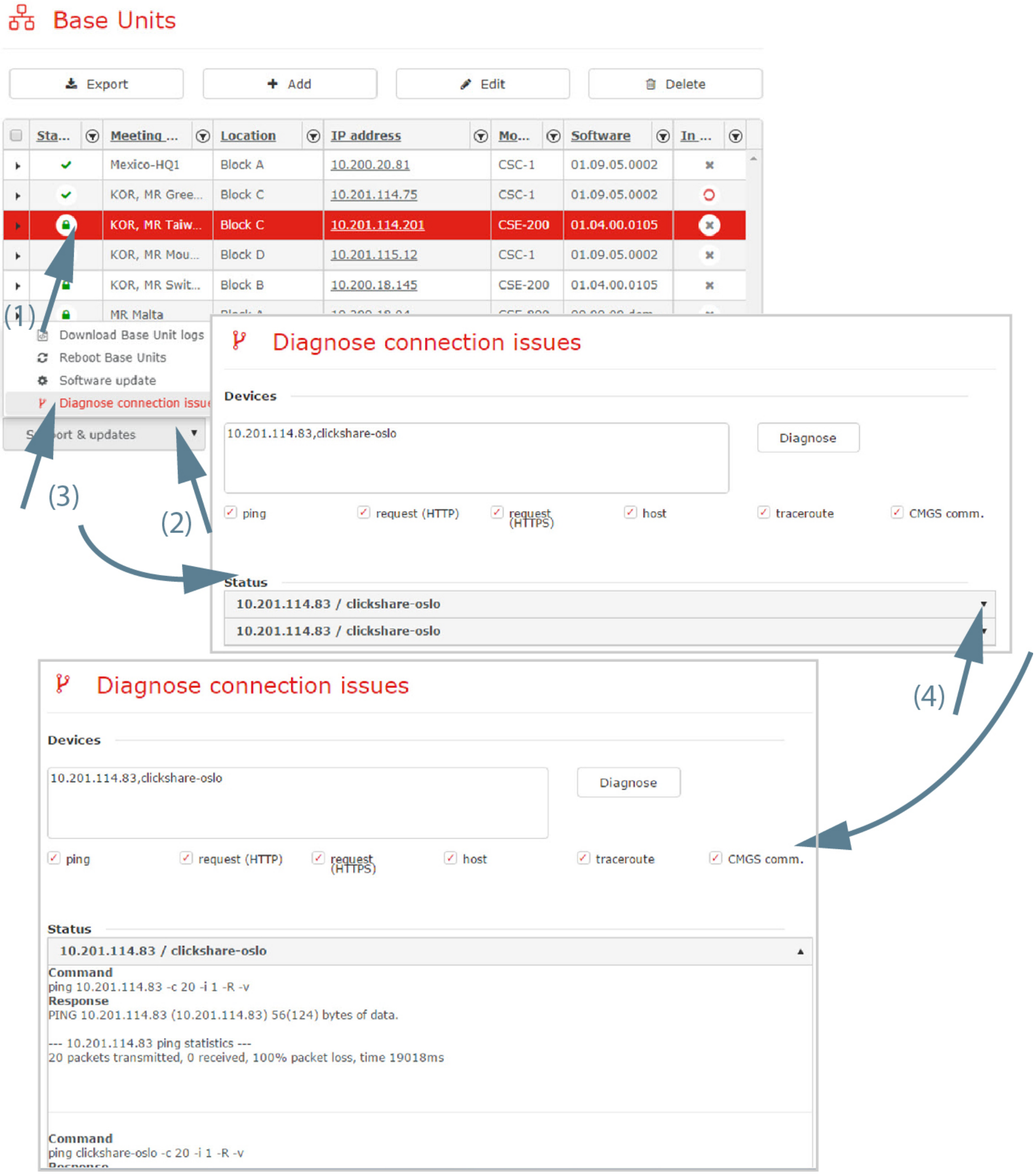
Image 3–16 Firmware download

The download starts.

3.1.8.4 Diagnose connection issues

How to start the diagnose

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



	Sta...	Meeting ...	Location	IP address	Mo...	Software	In ...
▸	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
▸	✓	KOR, MR Gree...	Block C	10.201.114.75	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Taiw...	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
▸		KOR, MR Mou...	Block D	10.201.115.12	CSC-1	01.09.05.0002	✖
▸	🔒	KOR, MR Swit...	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
▸	🔒	MR Malta					

Devices: 10.201.114.83,clickshare-oslo

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

Status

10.201.114.83 / clickshare-oslo

10.201.114.83 / clickshare-oslo

Devices: 10.201.114.83,clickshare-oslo

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

Status

10.201.114.83 / clickshare-oslo

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

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


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

Image 3–17 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**.

3.1.9 Configure

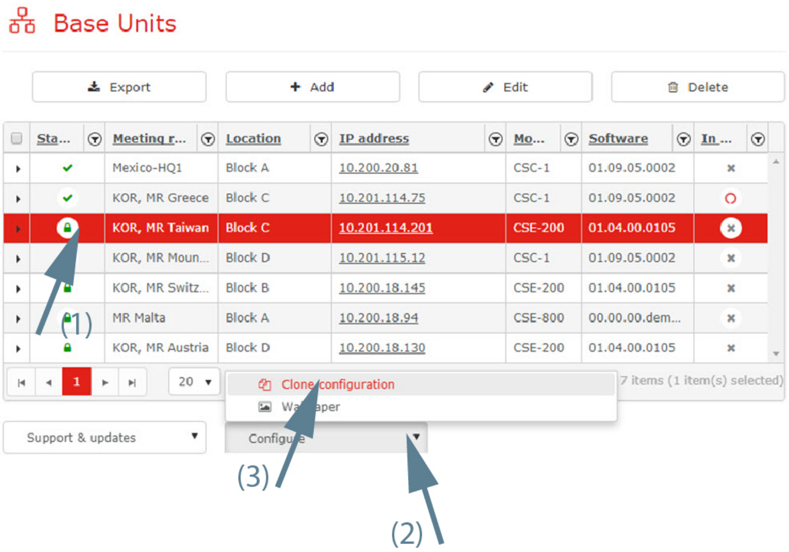
3.1.9.1 Clone Base Unit configuration

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.



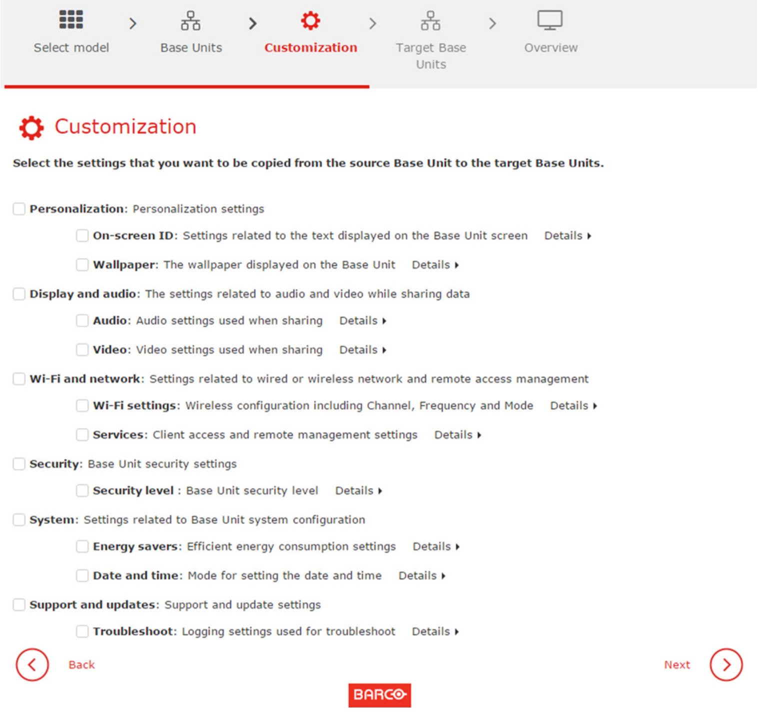
	Sta...	Meeting r...	Location	IP address	Mo...	Software	In ...
▸	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	×
▸	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	○
▸	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	×
▸		KOR, MR Moun...	Block D	10.201.115.12	CSC-1	01.09.05.0002	×
▸	🔒	KOR, MR Switz...	Block B	10.200.18.145	CSE-200	01.04.00.0105	×
▸	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.dem...	×
▸	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	×

7 items (1 item(s) selected)

Image 3–18 Clone Base Unit configuration

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

   The Customization window opens.



Customization

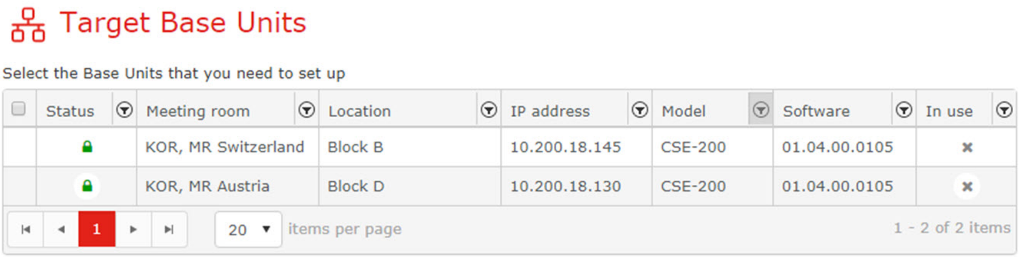
Select the settings that you want to be copied from the source Base Unit to the target Base Units.

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

Image 3–19 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.



Target Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

Image 3–20 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.

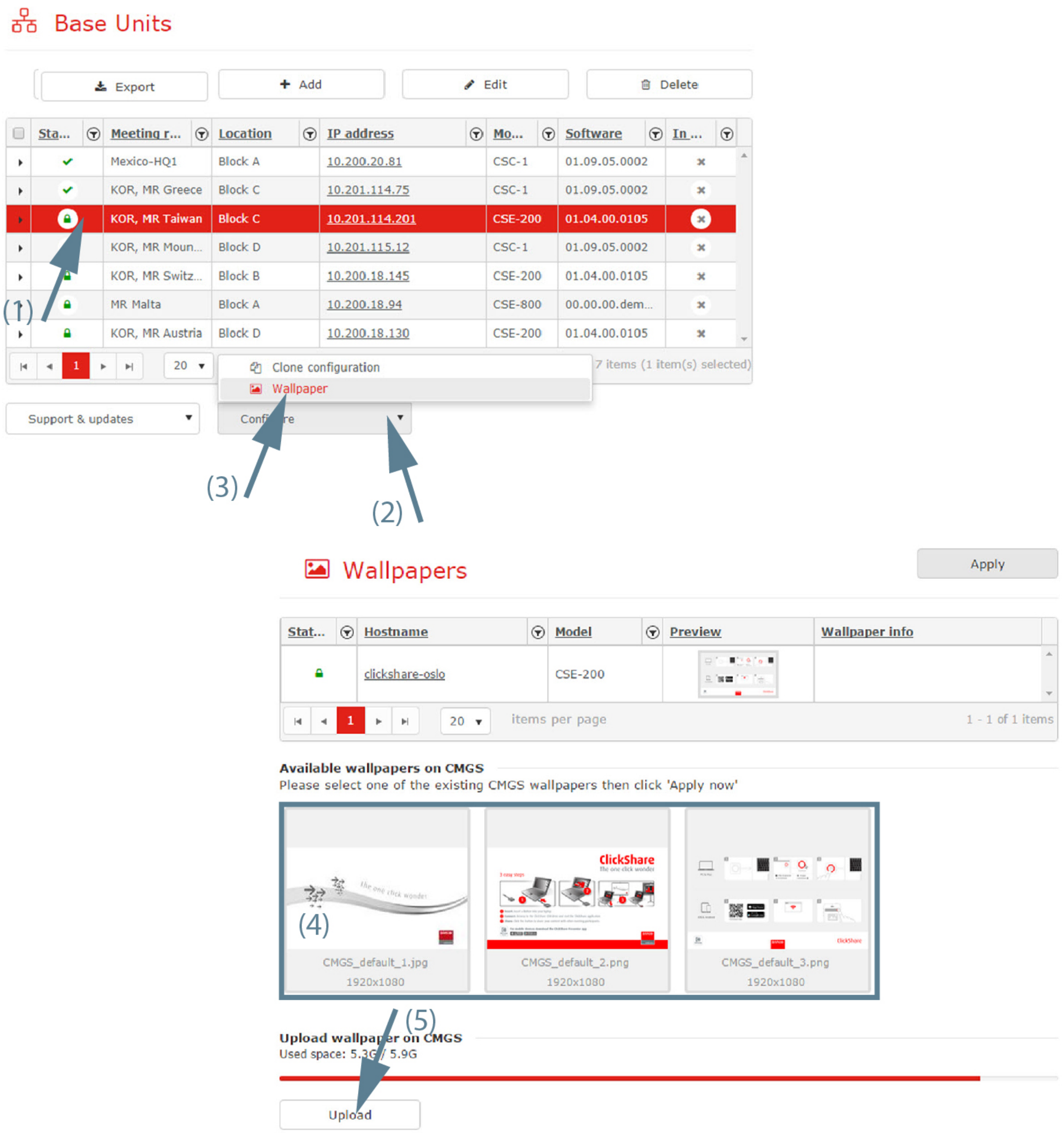
3.1.9.2 Wallpaper

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).



	Sta...	Meeting r...	Location	IP address	Mo...	Software	In ...
▸	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
▸	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
▸	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
▸		KOR, MR Moun...	Block D	10.201.115.12	CSC-1	01.09.05.0002	✖
▸	🔒	KOR, MR Switz...	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
▸	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.dem...	✖
▸	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

1 20 7 items (1 item(s) selected)

Stat...	Hostname	Model	Preview	Wallpaper info
🔒	clickshare-oslo	CSE-200		

1 20 items per page 1 - 1 of 1 items

Available wallpapers on CMGS

Please select one of the existing CMGS wallpapers then click 'Apply now'

CMGS_default_1.jpg
1920x1080

CMGS_default_2.png
1920x1080

CMGS_default_3.png
1920x1080

Upload wallpaper on CMGS

Used space: 5.3G / 5.9G

Image 3–21

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

   The wallpaper selection window opens. The current available wallpapers in XMS (virtual) Edge are displayed.

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

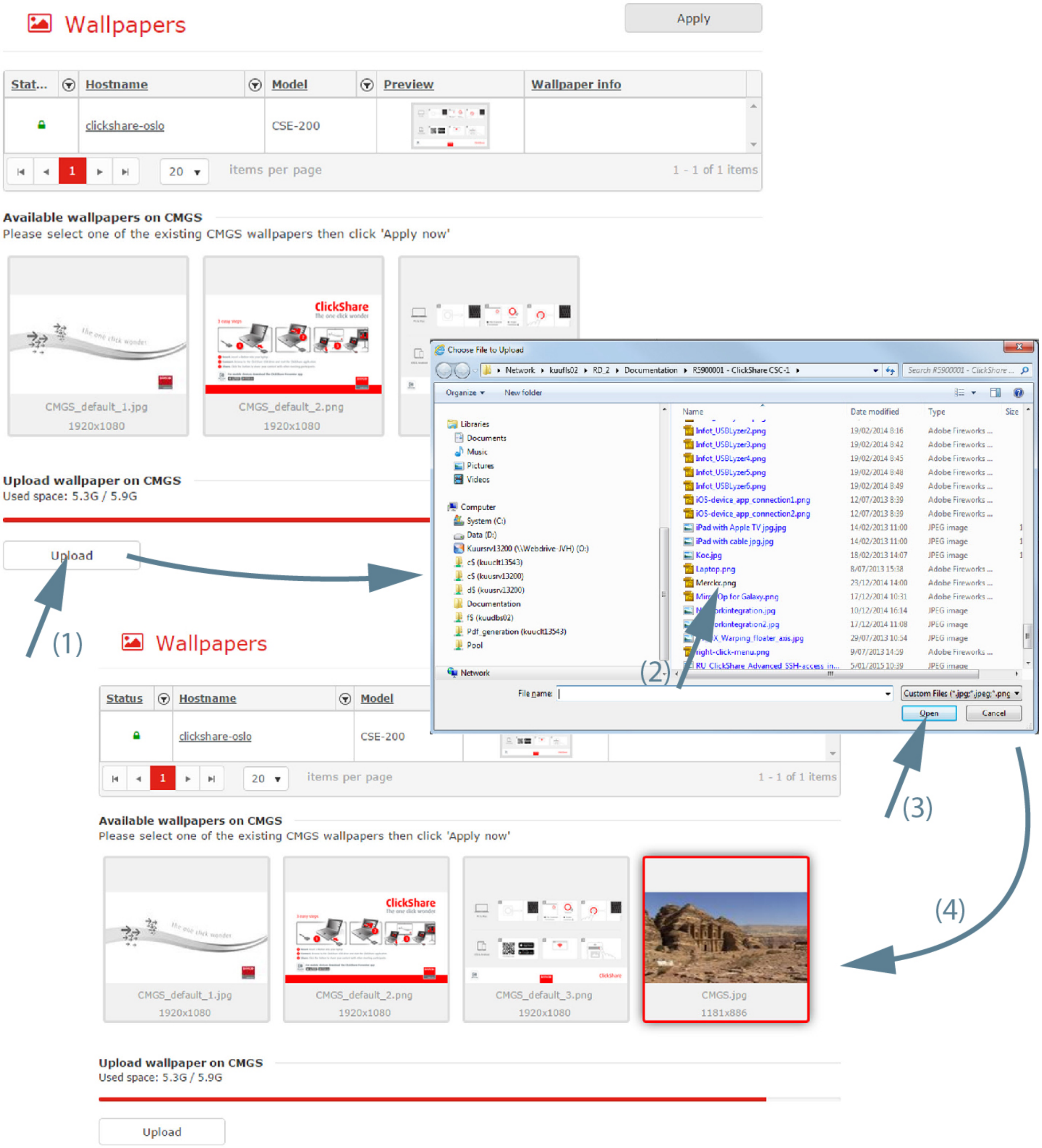
   The wallpaper file is sent to the Base Units.

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

   XMS (virtual) Edge also deletes all previously user uploaded wallpapers to the Base Unit.

Upload a new wallpaper on the XMS (virtual) Edge

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



Stat...	Hostname	Model	Preview	Wallpaper info
	clickshare-oslo	CSE-200		

20 items per page 1 - 1 of 1 items

Available wallpapers on CMGS

Please select one of the existing CMGS wallpapers then click 'Apply now'

CMGS_default_1.jpg 1920x1080

CMGS_default_2.png 1920x1080

CMGS_default_3.png 1920x1080

CMGS.jpg 1181x886

Upload wallpaper on CMGS

Used space: 5.3G / 5.9G

Image 3–22

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 XMS is 20 MB. Each base unit model may have different file size constraints. The maximum allowed resolution for a wallpaper applied to a

- CX-50 Gen2: 1920x1200 px (10 MB)
- C-5 :1920x1200 px (10 MB)
- C-10 :1920x1200 px (10 MB)
- CX-50 :1920x1200 px (10 MB)
- CX-30 :1920x1200 px (10 MB)
- CX-20 :1920x1200 px (10 MB)
- CS-100 & CS-100 Huddle : 1920x1200 px (2.50 MB)
- CSE-200+ : 1920x1200 px (2.50 MB)
- 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 XMS (virtual) Edge can be removed also.

3.2 Scheduler

Only for IT admin and support users.

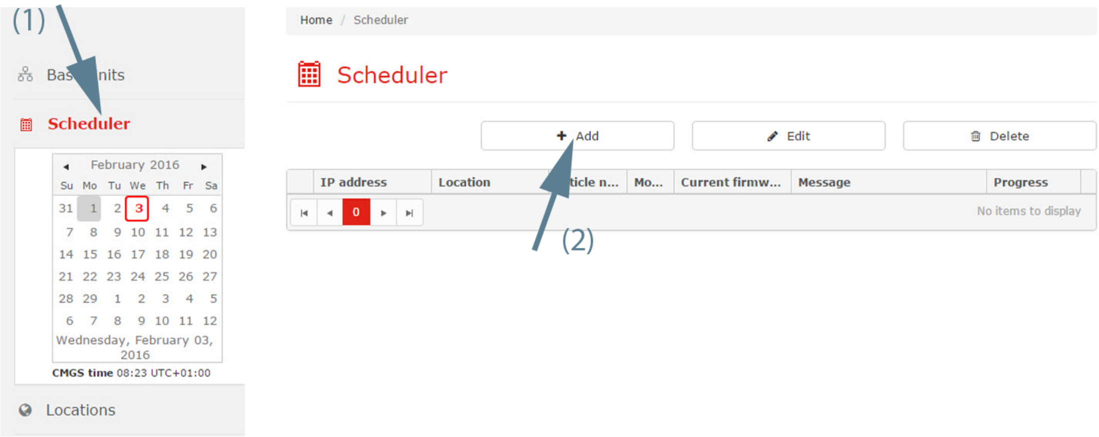
About the scheduler

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

3.2.1 Schedule a new job

How to schedule

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



February 2016

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

Wednesday, February 03, 2016

CMGS time 08:23 UTC+01:00

Image 3–23 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.

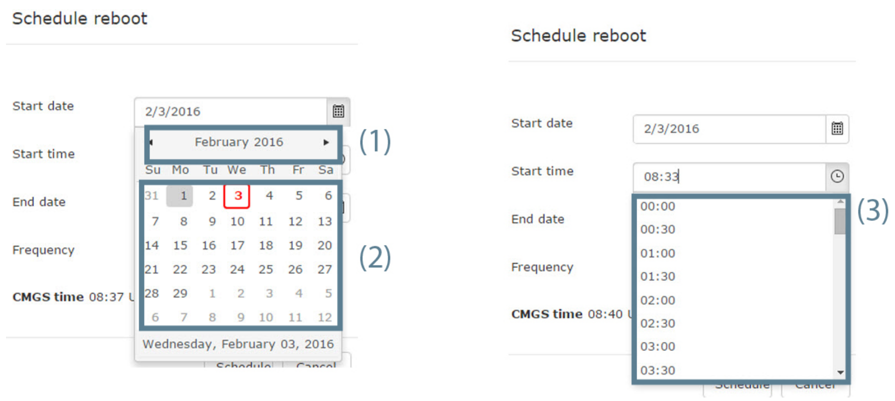
Gray highlighted number represents the current day. A red highlighted number represents the schedule date.

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 38 or "Reboot Base Units", page 37. 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).



Schedule reboot

Start date: 2/3/2016

Start time

End date

Frequency

CMGS time 08:37

Schedule reboot

Start date: 2/3/2016

Start time: 08:33

End date

Frequency

CMGS time 08:40

Image 3–24 Scheduler

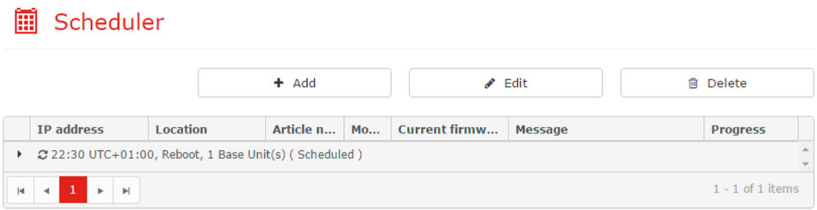
2. To change the day, click on the desired day in the calendar (2).
3. To set the desired time comparing to the server time, click on the icon and select a predefined time (3).

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.



Scheduler

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

Image 3–25 Scheduler overview page

The calendar highlights the days a job is created.

3.2.2 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).

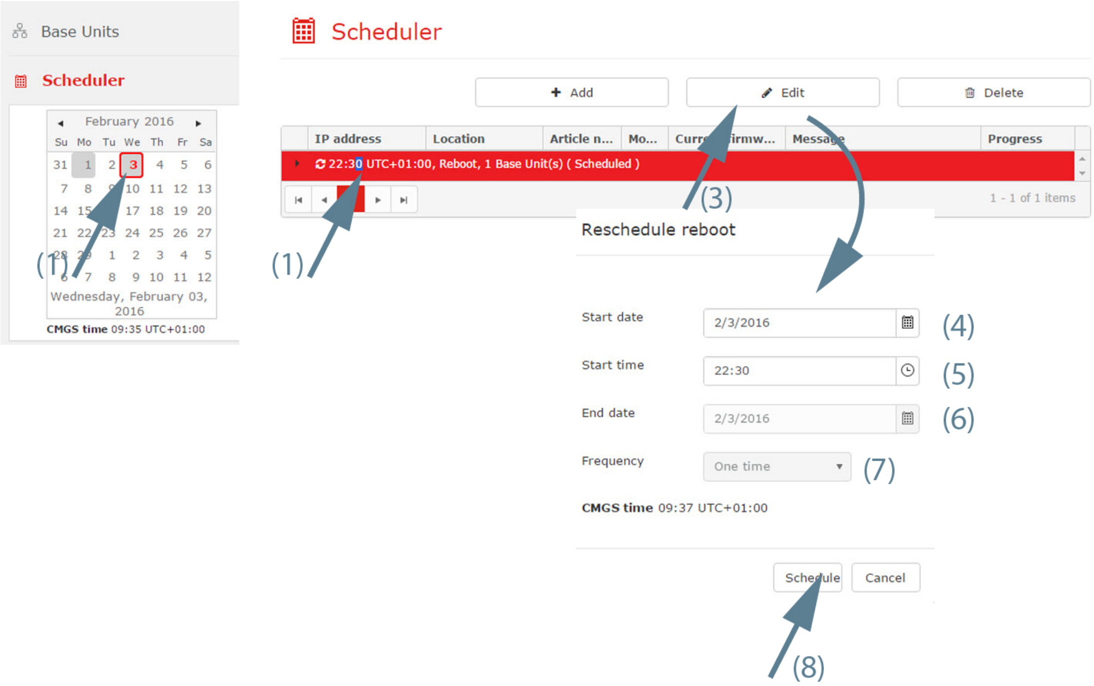


Image 3–26 Edit scheduled job

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).

3.2.3 Delete a job

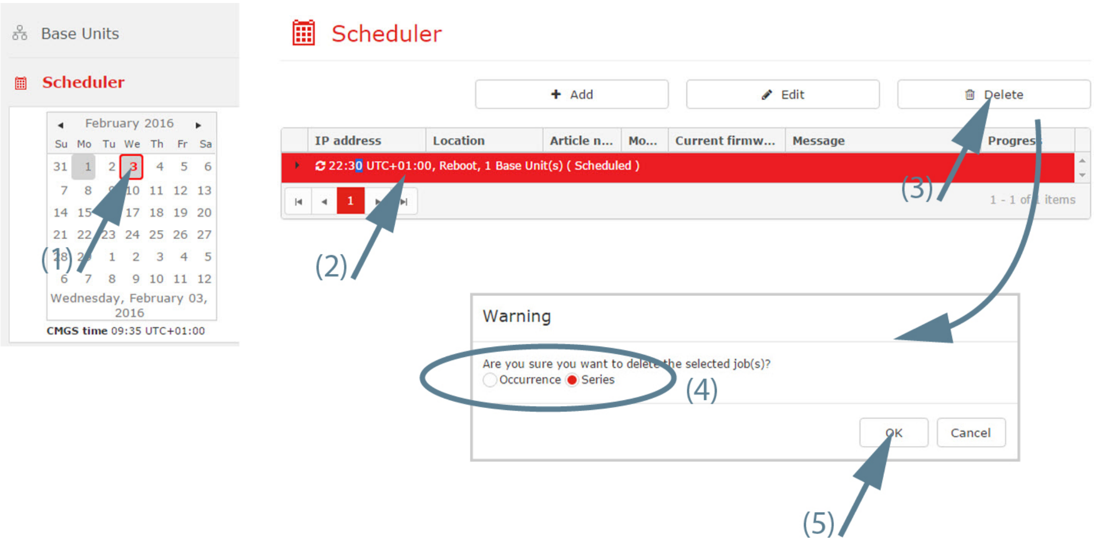
What can be done?

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)



CMGS time 09:35 UTC+01:00

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

Are you sure you want to delete the selected job(s)?
○ Occurrence ● Series

Image 3–27 Delete scheduled job

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

   A delete selection window is displayed.

3. Select *Occurence* or *Series* (4).

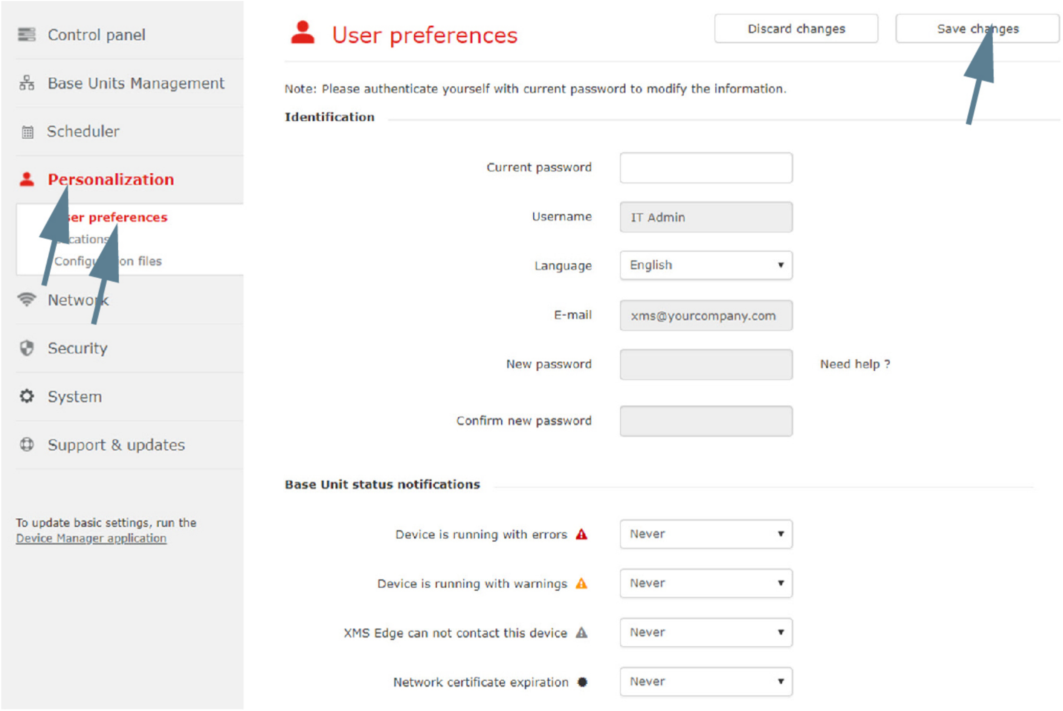
4. Click **OK** to confirm the deletion (5).

3.3 Personalization

3.3.1 User preferences

How to setup

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



To update basic settings, run the Device Manager application

Note: Please authenticate yourself with current password to modify the information.

Identification

Current password	
Username	IT Admin
Language	English
E-mail	xms@yourcompany.com
New password	
Confirm new password	

Base Unit status notifications

Device is running with errors	Never
Device is running with warnings	Never
XMS Edge can not contact this device	Never
Network certificate expiration	Never

Image 3–28 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.

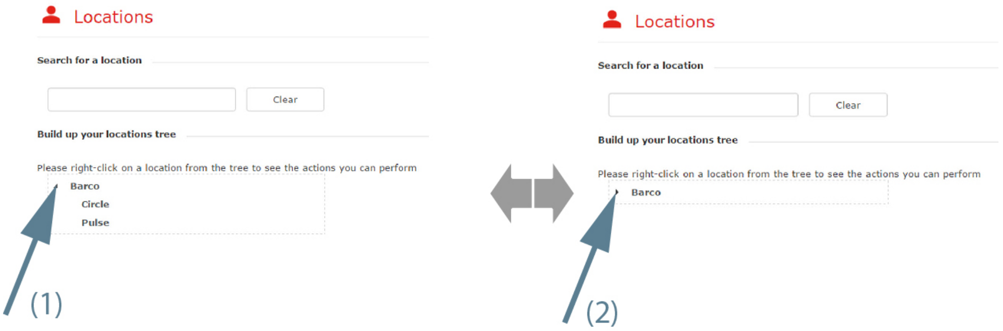
2. Click on **Save changes** to apply the changes.

3.3.2 Locations

3.3.2.1 Expand/collapse tree

How to collapse/expand

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



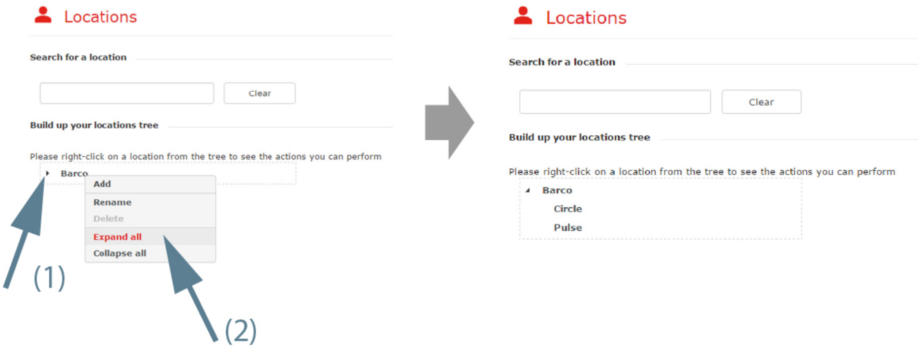
Please right-click on a location from the tree to see the actions you can perform

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

Image 3–29 Collapse/expand locations

Expand all

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



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

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

Image 3–30 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.

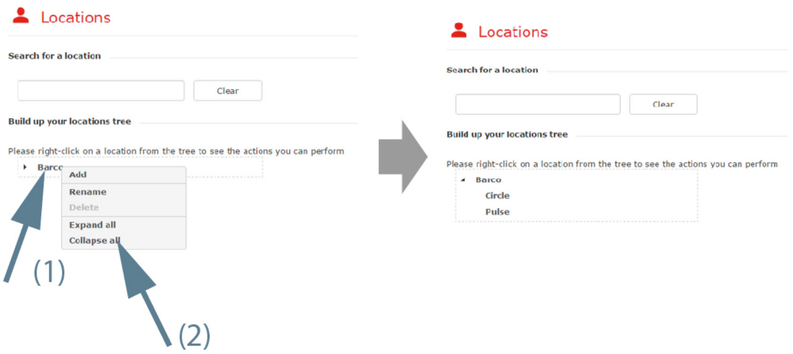

Locations
Search for a location
Clear
Build up your locations tree
Please right-click on a location from the tree to see the actions you can perform
Barco
Add
Rename
Delete
Expand all
Collapse all
(1)
(2)
Locations
Search for a location
Clear
Build up your locations tree
Please right-click on a location from the tree to see the actions you can perform
Barco
Circle
Pulse

Image 3–31 Collapse all

2. Select *Collapse all*.

   The branch with its sub branches is collapsed.

3.3.2.2 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).

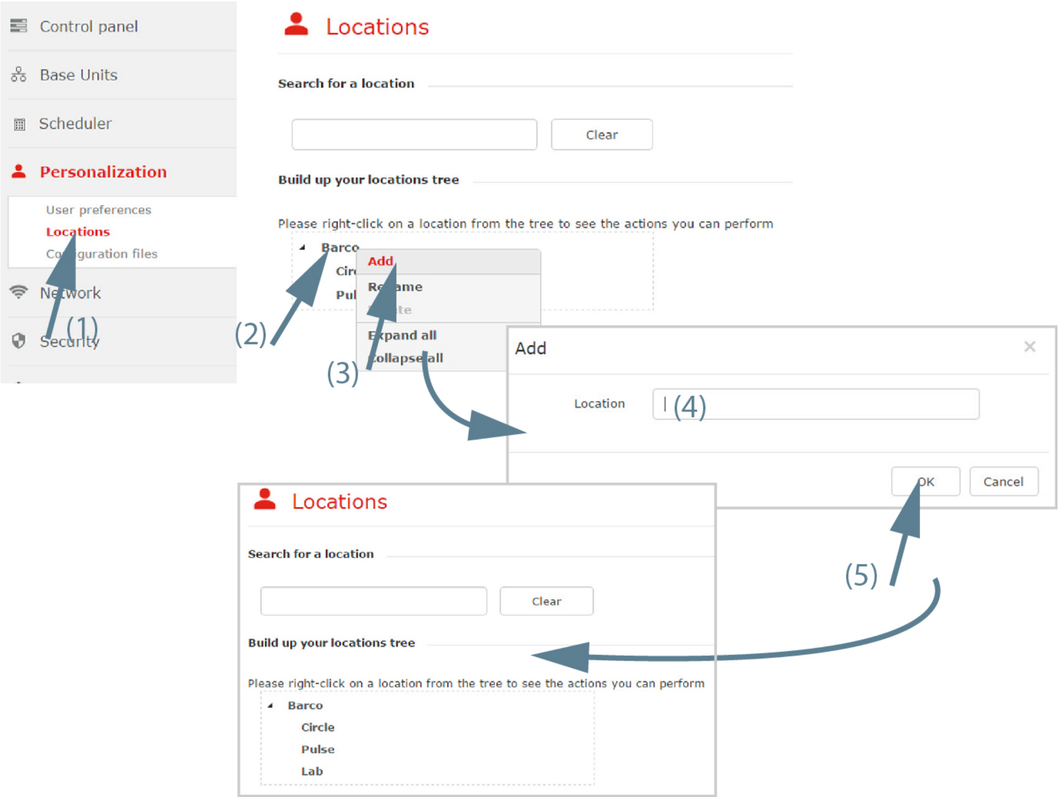


Image 3–32 Add new location

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.

3.3.2.3 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).

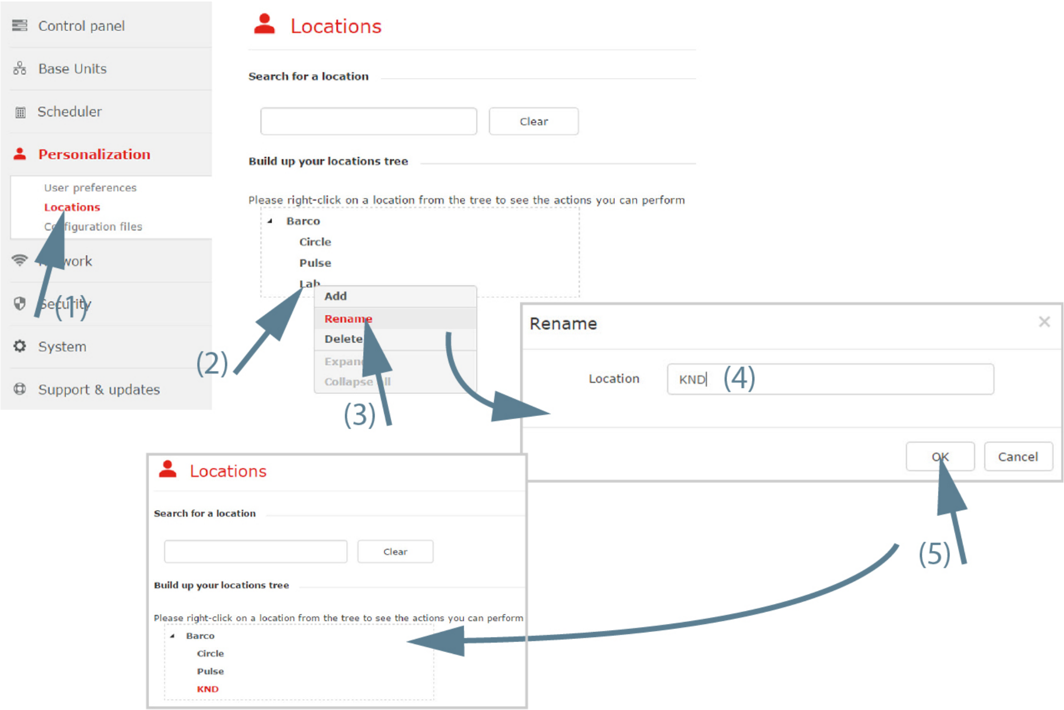


Image 3–33 Rename location

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.

3.3.2.4 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).

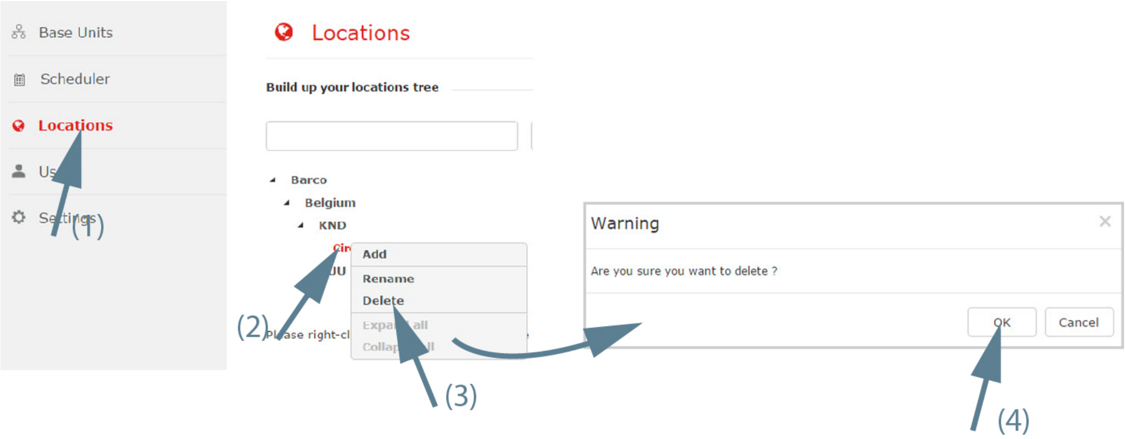


Image 3–34 Delete location

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.

3.3.2.5 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).

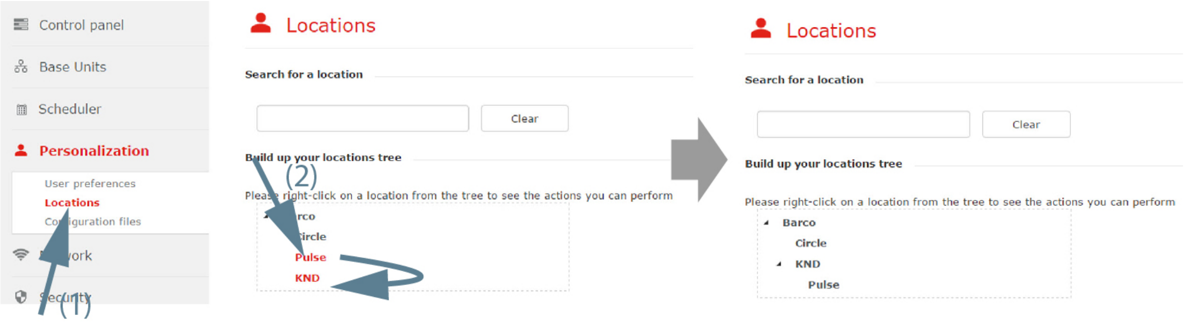


Image 3–35 Move location

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

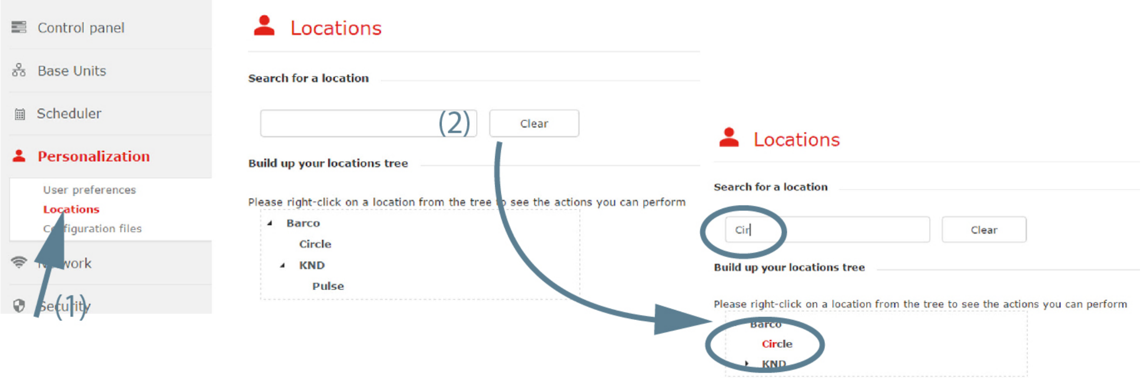
   While dragging a plus sign indicates that the dragged location can be dropped on that place.

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

3.3.2.6 Search for a location

How to search

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



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

Image 3–36 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.

3.3.3 Configuration files

3.3.3.1 Clone Base Unit settings

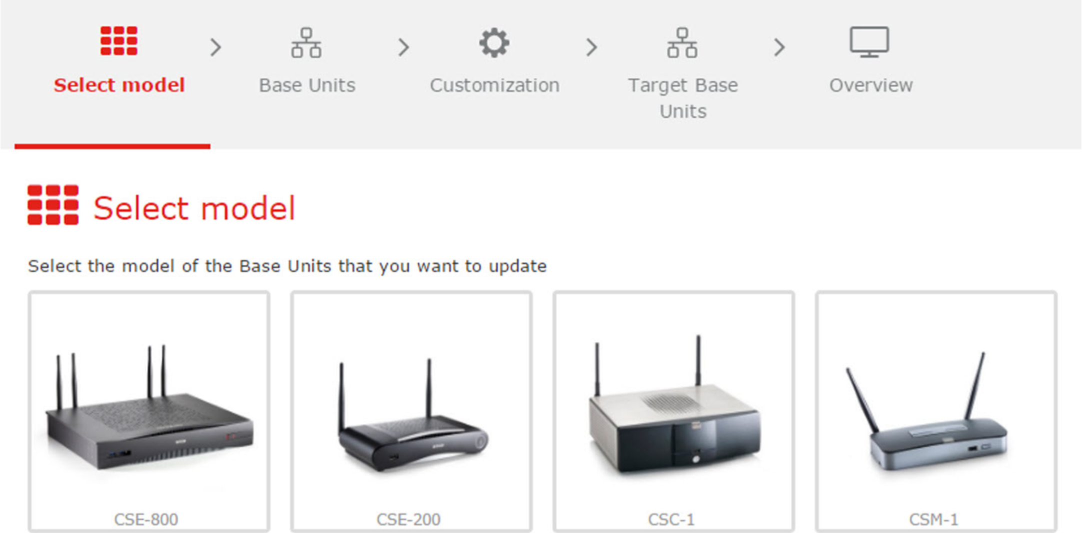
Only for CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1 devices.

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

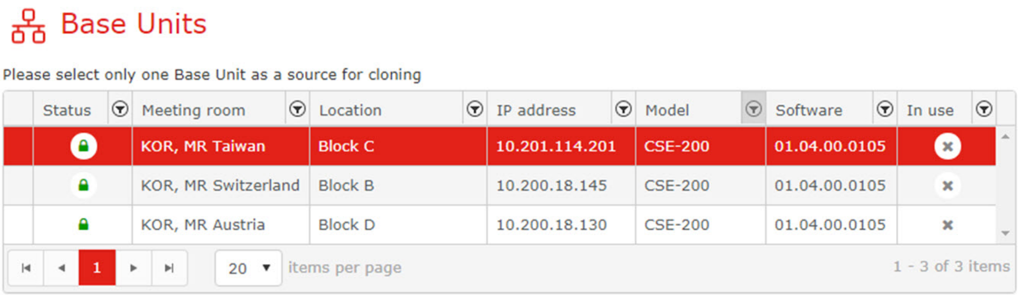
1. Select **Personalization** and click **Configuration files** to display the *Configuration files* page.
2. Click **Start wizard** next to *Clone Base Unit settings*.
3. Select your model of the Base Units you want to update and click **Next**.



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

Image 3–37 Select model

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



Base Units

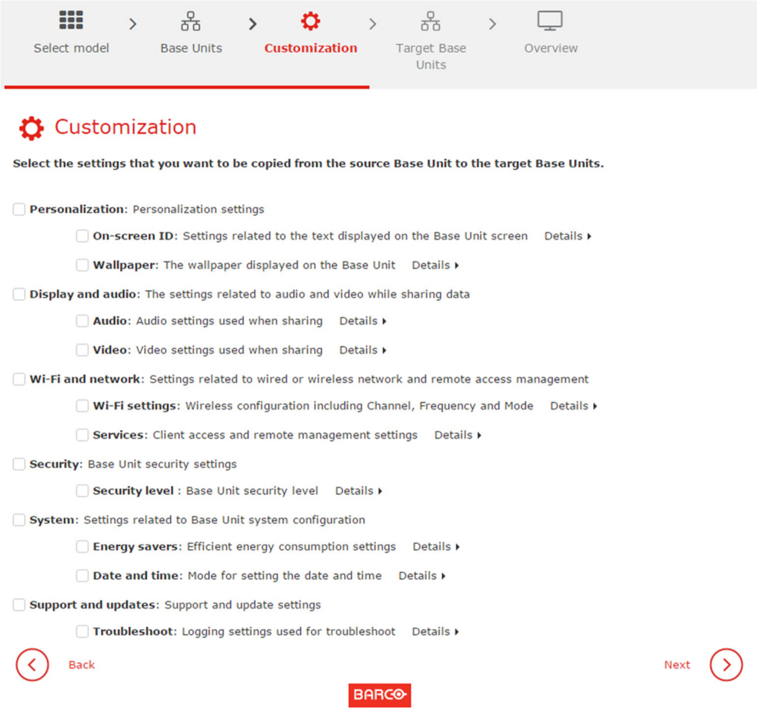
Please select only one Base Unit as a source for cloning

Status	Meeting room	Location	IP address	Model	Software	In use
🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

Image 3–38 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.



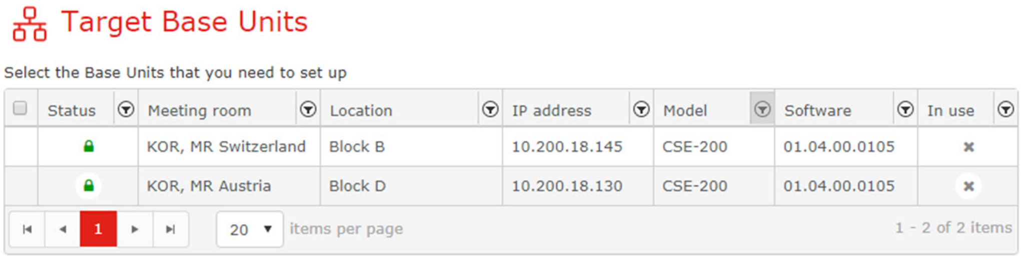
Customization

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

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

Image 3–39 Customization

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



Target Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

Image 3–40 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.

3.3.3.2 Backup XMS Edge configuration

How to backup

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

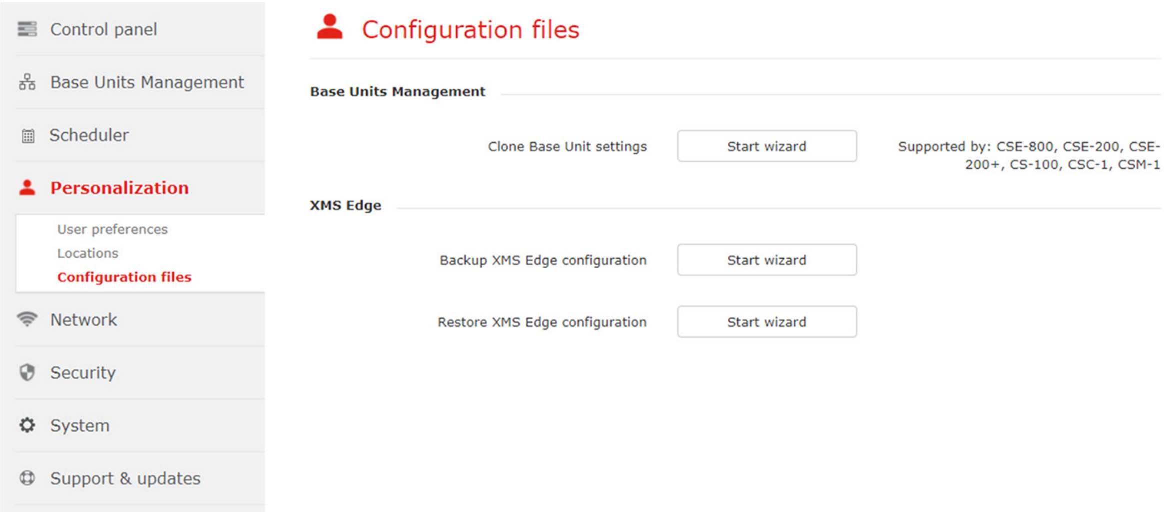


Image 3–41 Configuration files

2. Click on **Start wizard** next to *Backup XMS Edge 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**.

3.3.3.3 Restore XMS Edge configuration

How to restore

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

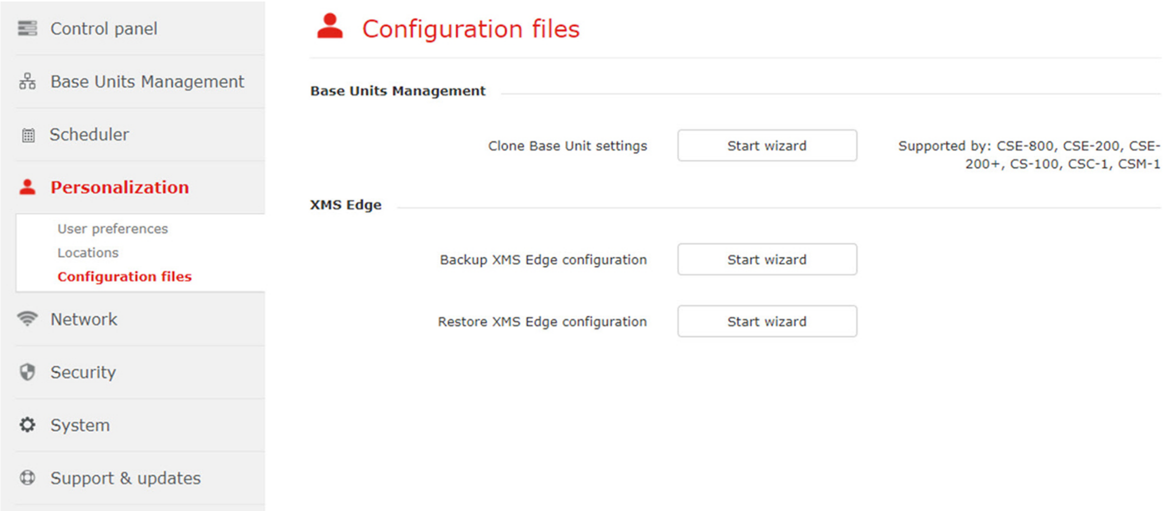


Image 3–42 Configuration files

2. Click on **Start wizard** next to *Restore XMS Edge configuration*.

   Restore will be executed. During this time the XMS (virtual) Edge 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.

3.4 Network

3.4.1 Base Units WiFi and network settings

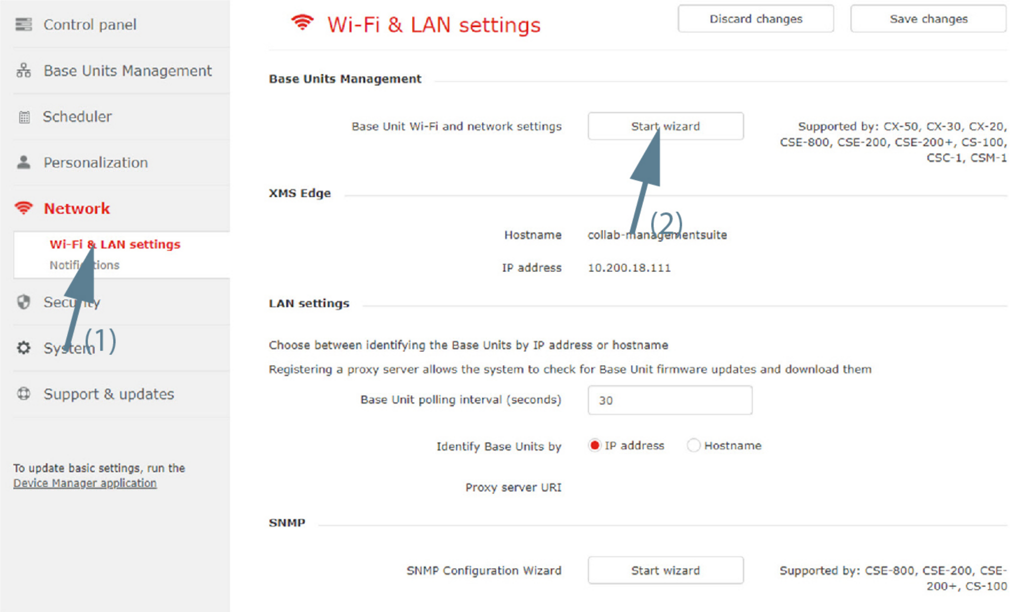
About Base Units WiFi and network settings

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.



To update basic settings, run the Device Manager application

Wi-Fi & LAN settings

Base Units Management

Base Unit Wi-Fi and network settings — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

XMS Edge

Hostname: collab-managementsuite

IP address: 10.200.18.111

LAN settings

Choose between identifying the Base Units by IP address or hostname

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

Base Unit polling interval (seconds): 30

Identify Base Units by: ● IP address ○ Hostname

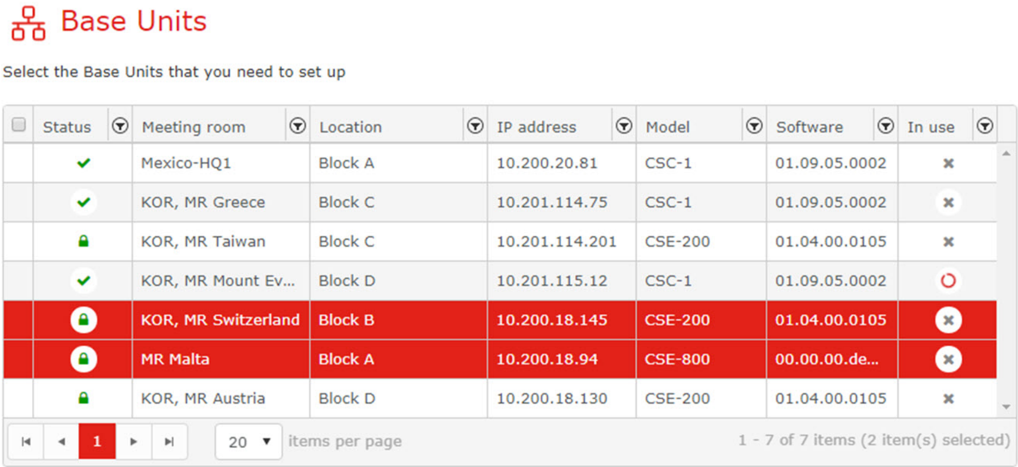
Proxy server URI

SNMP

SNMP Configuration Wizard — Start wizard — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Image 3–43 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.



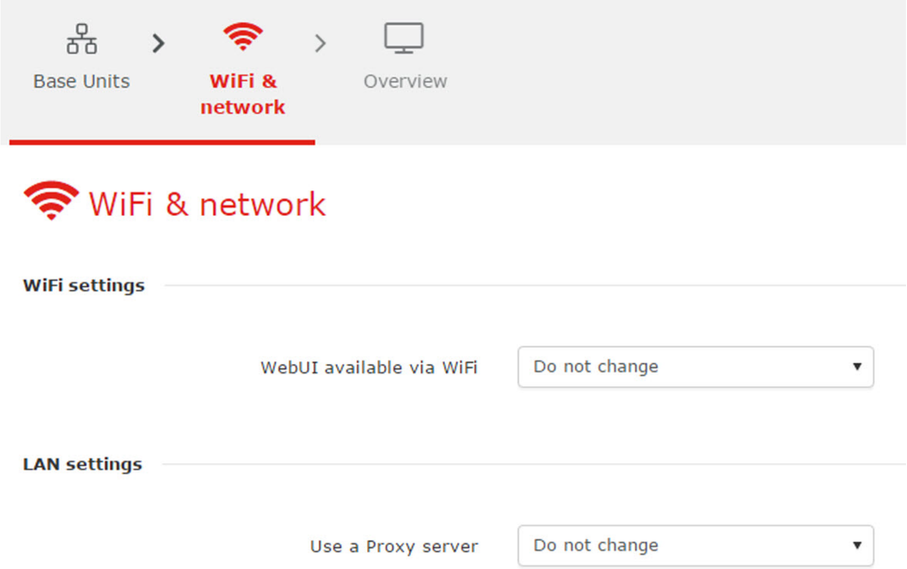
Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
	✓	KOR, MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	✖
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

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

Image 3–44 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.



WiFi & network

WiFi settings

WebUI available via WiFi: Do not change

LAN settings

Use a Proxy server: Do not change

Image 3–45 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.

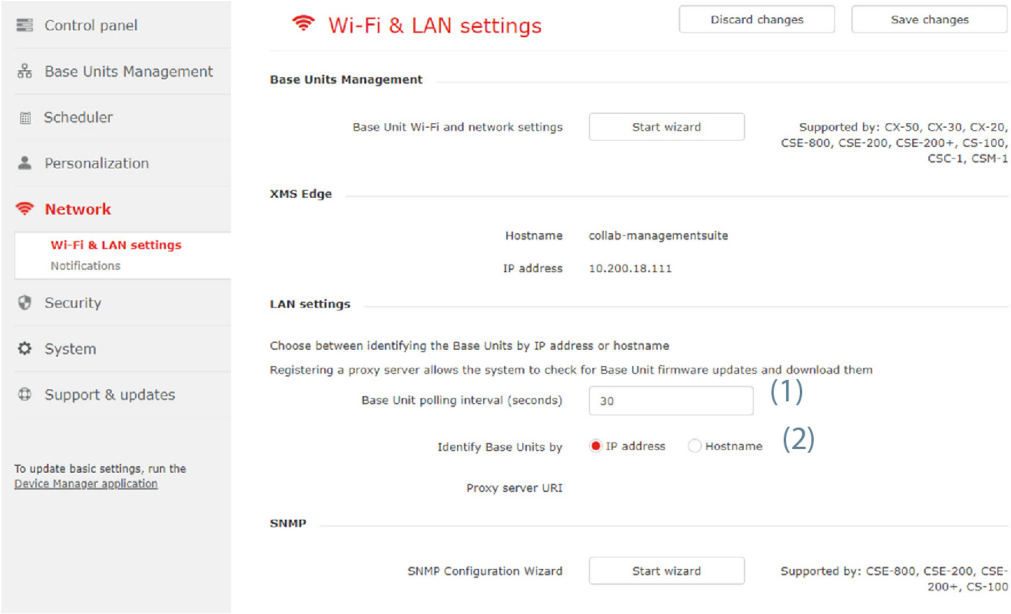
7. If you agree with the overview settings, click **Finish**.

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

3.4.2 LAN settings

How to set

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



To update basic settings, run the Device Manager application

Wi-Fi & LAN settings

Base Units Management

Base Unit Wi-Fi and network settings — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

XMS Edge

Hostname: collab-managementsuite

IP address: 10.200.18.111

LAN settings

Choose between identifying the Base Units by IP address or hostname

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

Base Unit polling interval (seconds): 30

Identify Base Units by: ● IP address ○ Hostname

Proxy server URI

SNMP

SNMP Configuration Wizard — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Image 3–46 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).

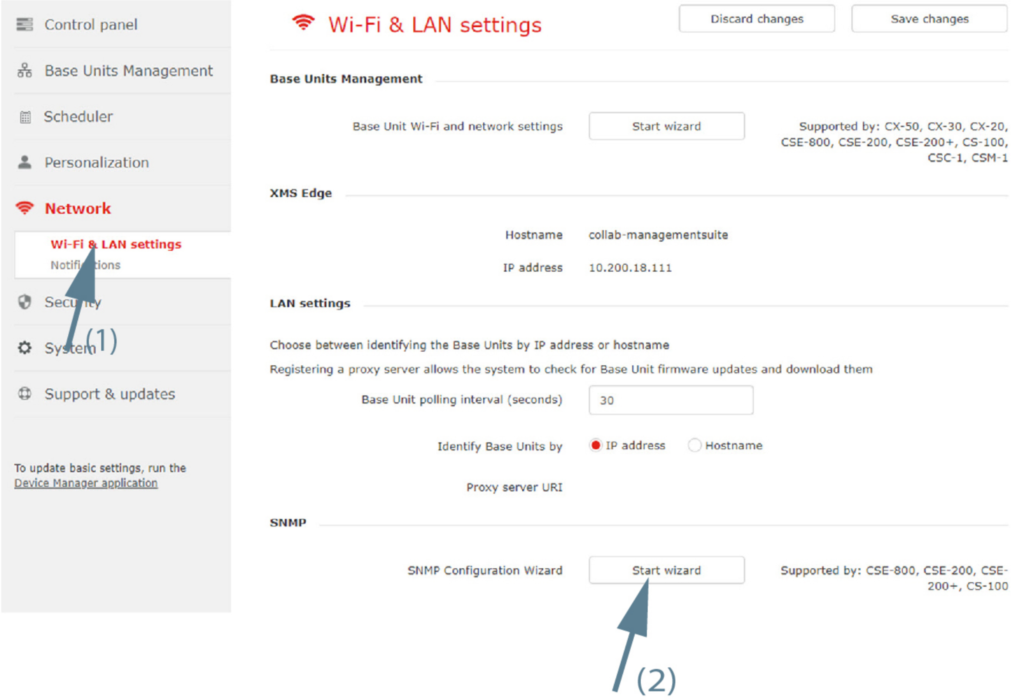
   The following choices are possible:

   - IP address
   - hostname
4. Click **Save changes** to apply the settings.

3.4.3 SNMP

How to setup

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



To update basic settings, run the Device Manager application

Wi-Fi & LAN settings

Base Units Management

Base Unit Wi-Fi and network settings — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

XMS Edge

Hostname: collab-managementsuite

IP address: 10.200.18.111

LAN settings

Choose between identifying the Base Units by IP address or hostname

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

Base Unit polling interval (seconds): 30

Identify Base Units by: ● IP address ○ Hostname

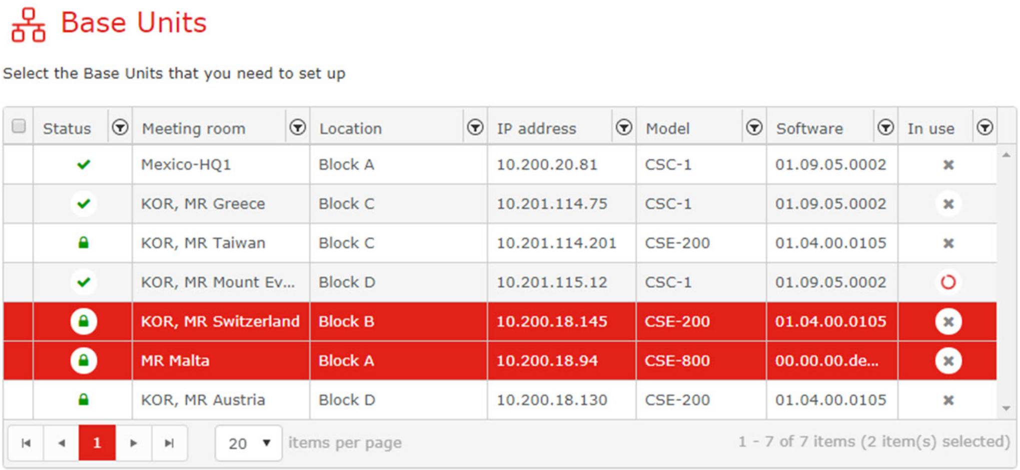
Proxy server URI

SNMP

SNMP Configuration Wizard — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Image 3–47 Network, SNMP

2. Click on **Start wizard** next to *SNMP Configuration Wizard* to start.
3. Select the Base Units. Click **Next** to continue.



Base Units

Select the Base Units that you need to set up

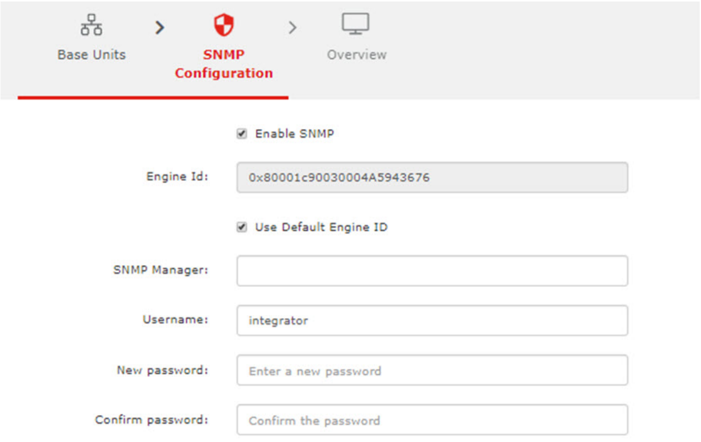
□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	✖
	✓	KOR, MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	✖
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

Image 3–48 Base units to setup

4. To enable SNMP, check the checkbox in front of *EnableSMNP*.
5. To use the default engine Id, check the checkbox in front of *Use Default Engine ID*.

   or

   fill out an engine Id.
6. Fill out the SNMP Manager address, Username and password (minimum 8 characters). Confirm the password.



☑ Enable SNMP

Engine Id: 0x80001c90030004A5943676

☑ Use Default Engine ID

SNMP Manager:

Username: integrator

New password: Enter a new password

Confirm password: Confirm the password

Image 3–49

3.4.4 Network integration

3.4.4.1 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 “Network requirements”, page 102 are open on your network.

VLAN

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

DNS

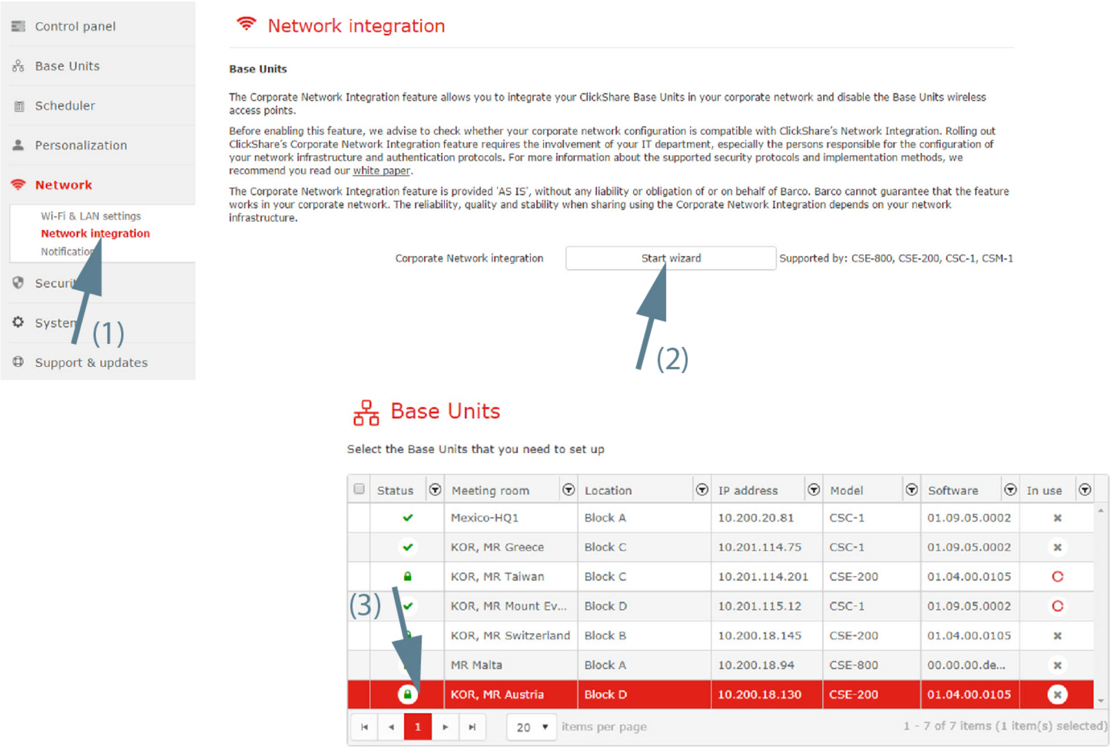
For the Buttons to be able to stream their content to the Base Unit, they must be able to resolve the Base Unit’s hostname within the network. If no DNS is available Buttons will fall back to the IP of the Base Unit at the moment of USB pairing. Because of this we strongly advise to reserve IP addresses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

NTP

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

Start up the wizard

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



Network integration

Base Units

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

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

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

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

Base Units

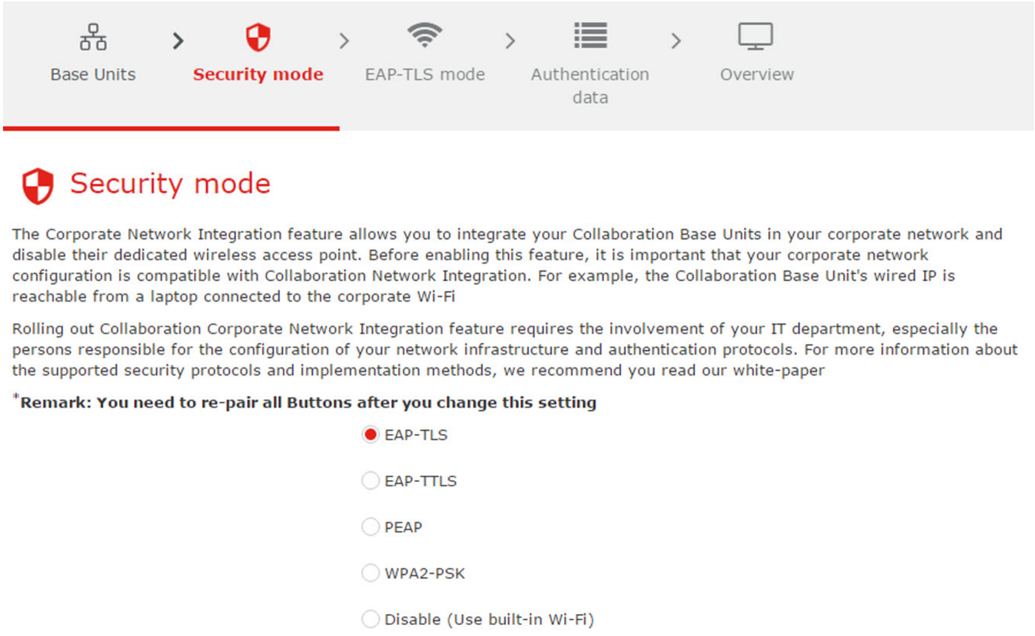
Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	✓	KOR, MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
		MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	✖
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

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

Image 3–50 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.



Security mode

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

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

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

● EAP-TLS

○ EAP-TTLS

○ PEAP

○ WPA2-PSK

○ Disable (Use built-in Wi-Fi)

Image 3–51 Network integration, security mode

The following modes are available:

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

3.4.4.2 Network integration, EAP-TLS security mode

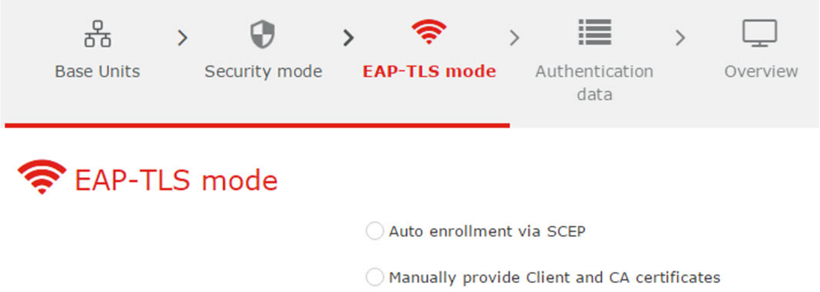
About EAP-TLS

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.



EAP-TLS mode

○ Auto enrollment via SCEP

○ Manually provide Client and CA certificates

Image 3–52 EAP-TLS mode

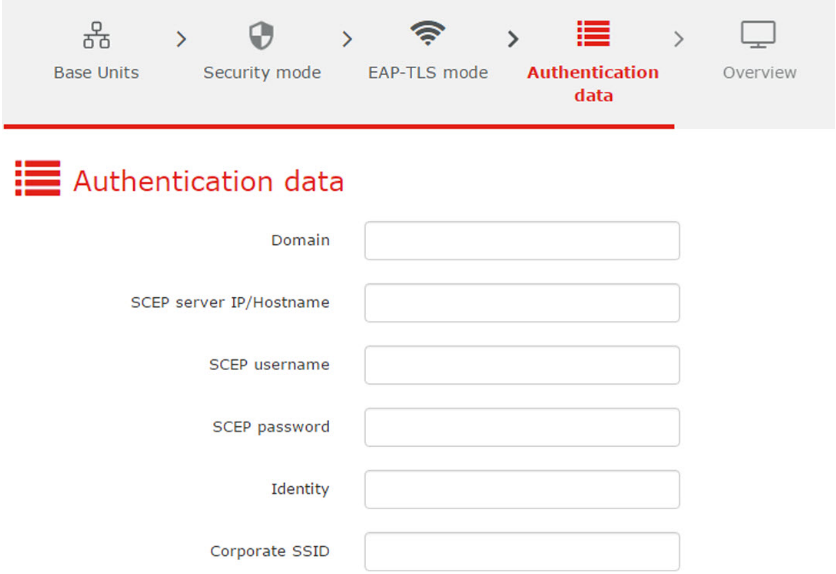
Two choices are possible:

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

Using SCEP

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

The Simple Certificate Enrolment Protocol (SCEP) is a protocol which enables issuing and revoking of certificates in a scalable way. SCEP support is included to allow a quicker and smoother integration of the ClickShare Base Unit and Buttons into the corporate network. Since most companies are using Microsoft Windows Server and its active directory (AD) to manage users and devices our SCEP implementation is specifically targeted at the Network Device Enrolment Service (NDES) which is part of Windows Server 2008 R2 and Windows Server 2012. No other SCEP server implementations are supported.



Authentication data

Domain

SCEP server IP/Hostname

SCEP username

SCEP password

Identity

Corporate SSID

Image 3–53 SCEP, authentication data

About NDES

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

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

Necessary Data to continue:

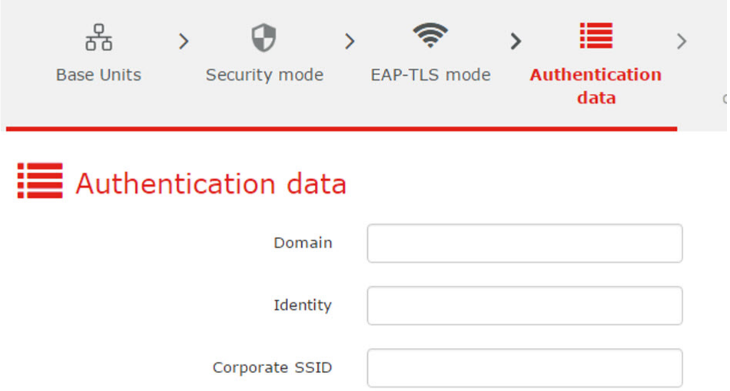
Domain	The company domain for which you are enrolling, should match with the one defined in your Active Directory.
SCEP ServerIP/ hostname	This is the IP or hostname of the Windows Server in your network running the NDES service. Since Internet Information Services (IIS) supports both HTTP and HTTPS, also include which of the two you want to use. If not provided it will be default set to HTTP. E.g.: http://myserver or https://10.192.5.1 or server.mycompany.com (will use http)
SCEP User name	This is a user in your Active Directory which has the required permission to access the NDES service and request the challenge password. To be sure of this, the user should be part of the CA Administrators group (in case of a stand-alone CA) or have enroll permissions on the configured certificate templates.
SCEP Password	The corresponding password for the identity that you are using to authenticate on the corporate network. Per Base Unit, every Button uses the same identity and password to connect to the corporate network.
Domain	The company domain for which you are enrolling should match the one defined in your Active Directory.
Identity	Identity of the user account in the Active Directory which will be used by the ClickShare Buttons to connect to the corporate network. When using EAP-TLS make sure that the necessary mapping exists between the Client Certificate issued by your CA and this user account.
Corporate SSID	The SSID of your corporate wireless infrastructure to which the ClickShare Buttons will connect.

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

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.



Domain

Identity

Corporate SSID

Image 3–54 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.

3.4.4.3 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.

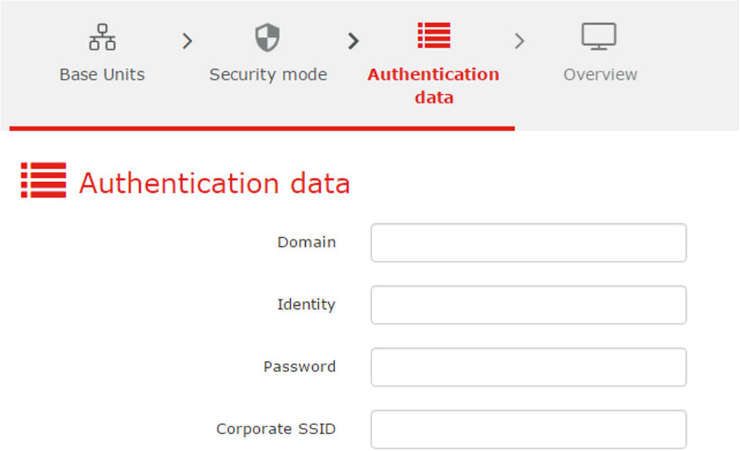


Image 3–55 EAP-TTLS

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.

3.4.4.4 Network integration, PEAP security mode

About PEAP

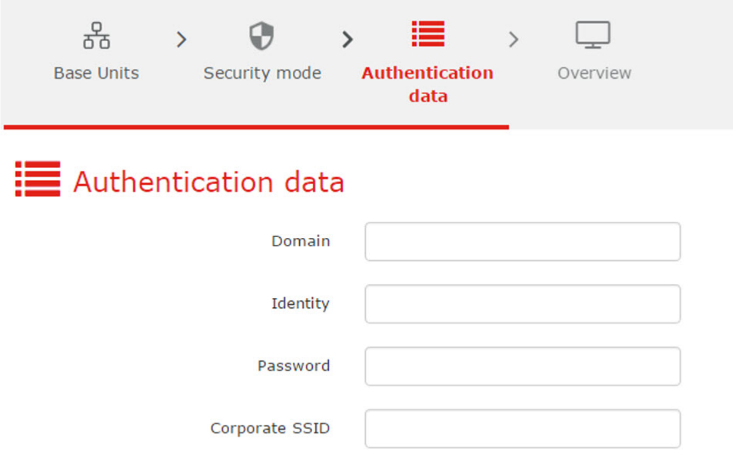
PEAP (Protected Extensible Authentication Protocol) is an EAP implementation co-developed by Cisco Systems, Microsoft and RSA Security. It sets up a secure TLS tunnel using the servers CA certificate after which actual user authentication takes place within the tunnel. This way of working enables it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

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

Start up for PEAP

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

   The PEAP window opens.



Authentication data

Domain

Identity

Password

Corporate SSID

Image 3–56 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.

3.4.4.5 Network integration, WPA2-PSK security mode

About WPA2-PSK

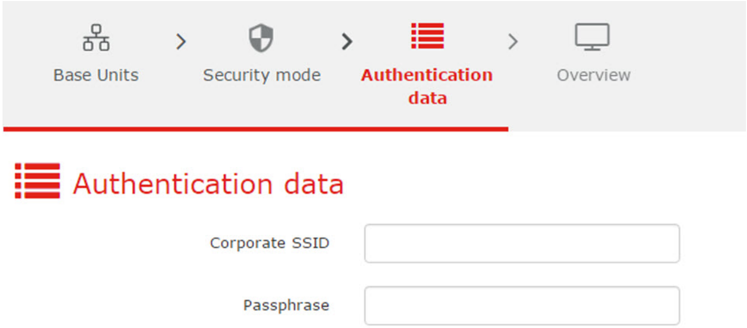
WPA2-PSK does not distinguish between individual users, there is 1 password (PSK – Pre-Shared Key) for all clients connecting to the wireless infrastructure. This makes setup very straightforward. Once connected, all data transmitted between client and AP (access point) is encrypted using a 256 bit key.

Start up for WPA2-PSK

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

   The WPA2-PSK mode window opens.

   Necessary Data to continue:

   Authentication data

   Corporate SSID

   Passphrase

   Image 3–57 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.

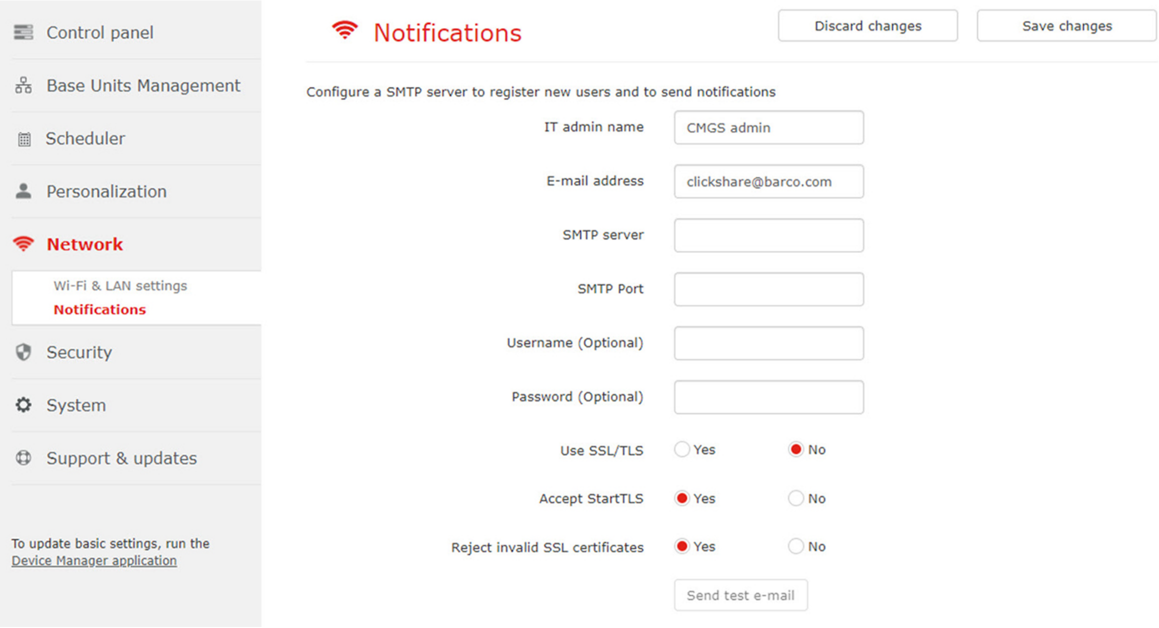
   The *Overview* window is displayed.

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.

3.4.5 Notifications

IT admin



To update basic settings, run the Device Manager application

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

IT admin name: CMGS admin

E-mail address: clickshare@barco.com

SMTP server:

SMTP Port:

Username (Optional):

Password (Optional):

Use SSL/TLS: ○ Yes ● No

Accept StartTLS: ● Yes ○ No

Reject invalid SSL certificates: ● Yes ○ No

Image 3–58 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.

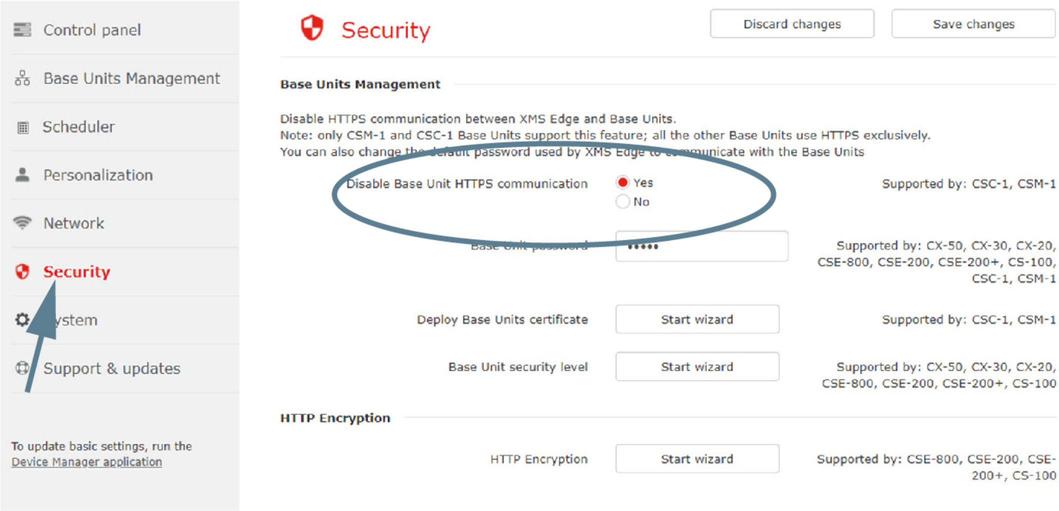
3.5 Security

3.5.1 Security, Base Unit HTTPS communication

Only for CSC-1 and CSM-1 devices.

HTTPS communication

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



Base Units Management

Disable HTTPS communication between XMS Edge and Base Units.
Note: only CSM-1 and CSC-1 Base Units support this feature; all the other Base Units use HTTPS exclusively.
You can also change the default password used by XMS Edge to communicate with the Base Units

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

Base Unit password ••••• — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

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

Base Unit security level — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

HTTP Encryption

HTTP Encryption — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Image 3–59 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.

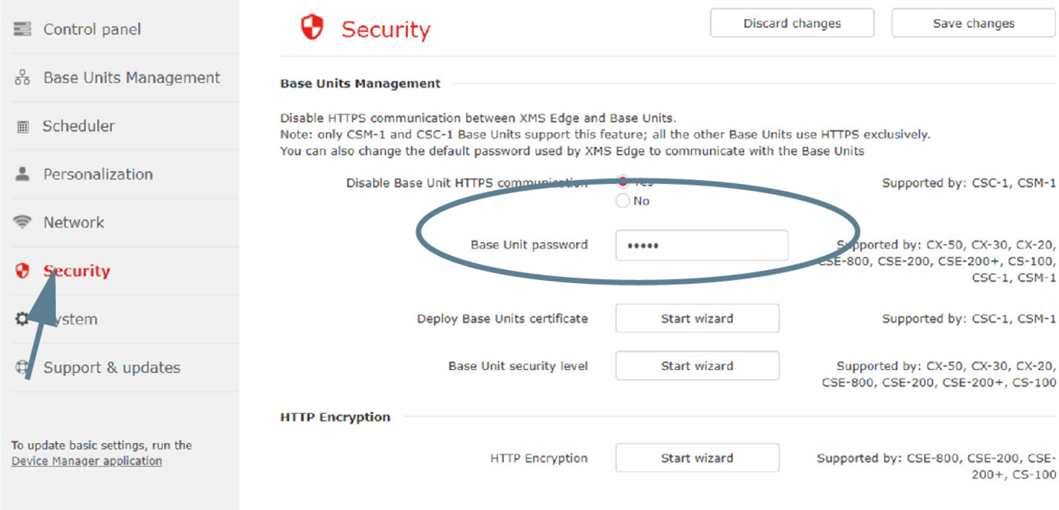
3.5.2 Security, Base Unit password

About Base Unit password

The Base Unit password field from the Security page is the password used for communication between the XMS (virtual) Edge 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 XMS (virtual) Edge will be the only application able to communicate and change settings on Base Units.

Set password

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



Base Units Management

Disable HTTPS communication between XMS Edge and Base Units.
Note: only CSM-1 and CSC-1 Base Units support this feature; all the other Base Units use HTTPS exclusively.
You can also change the default password used by XMS Edge to communicate with the Base Units

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

Base Unit password ••••• — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

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

Base Unit security level — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

HTTP Encryption

HTTP Encryption — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Image 3–60 Security, Base Unit password

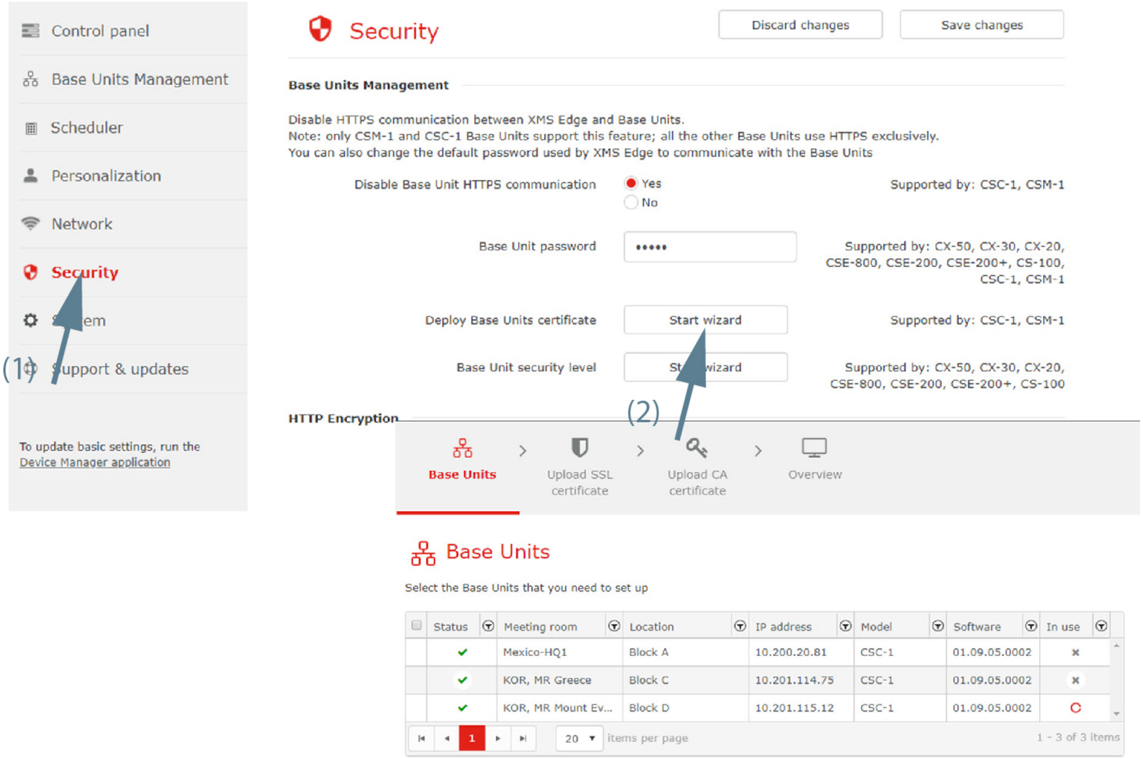
2. Enter the password used to access the Configurator of the Base Unit.

3.5.3 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).



To update basic settings, run the Device Manager application

Base Units Management

Disable HTTPS communication between XMS Edge and Base Units.
Note: only CSM-1 and CSC-1 Base Units support this feature; all the other Base Units use HTTPS exclusively.
You can also change the default password used by XMS Edge to communicate with the Base Units

Disable Base Unit HTTPS communication	● Yes ○ No	Supported by: CSC-1, CSM-1
Base Unit password	•••••	Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1
Deploy Base Units certificate	Start wizard	Supported by: CSC-1, CSM-1
Base Unit security level	Start wizard	Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

HTTP Encryption

Base Units

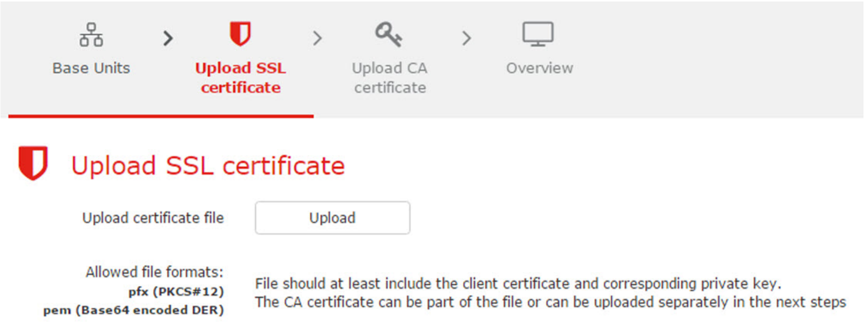
Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	×
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	×
	✓	KOR, MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○

1   20 items per page   1 - 3 of 3 items

Image 3–61 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.



Upload SSL certificate

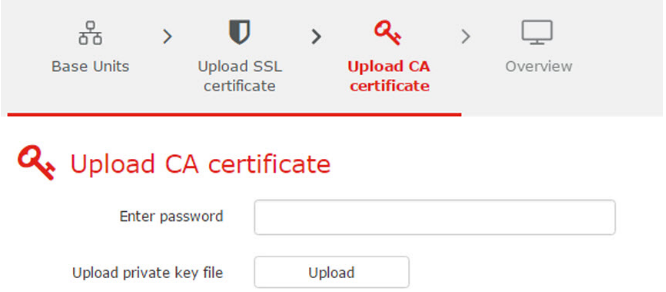
Upload certificate file

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

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

Image 3–62 Upload SSL certificate

5. Upload CA certificate. Enter password.



Upload CA certificate

Enter password

Upload private key file: Upload

Image 3–63 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**.

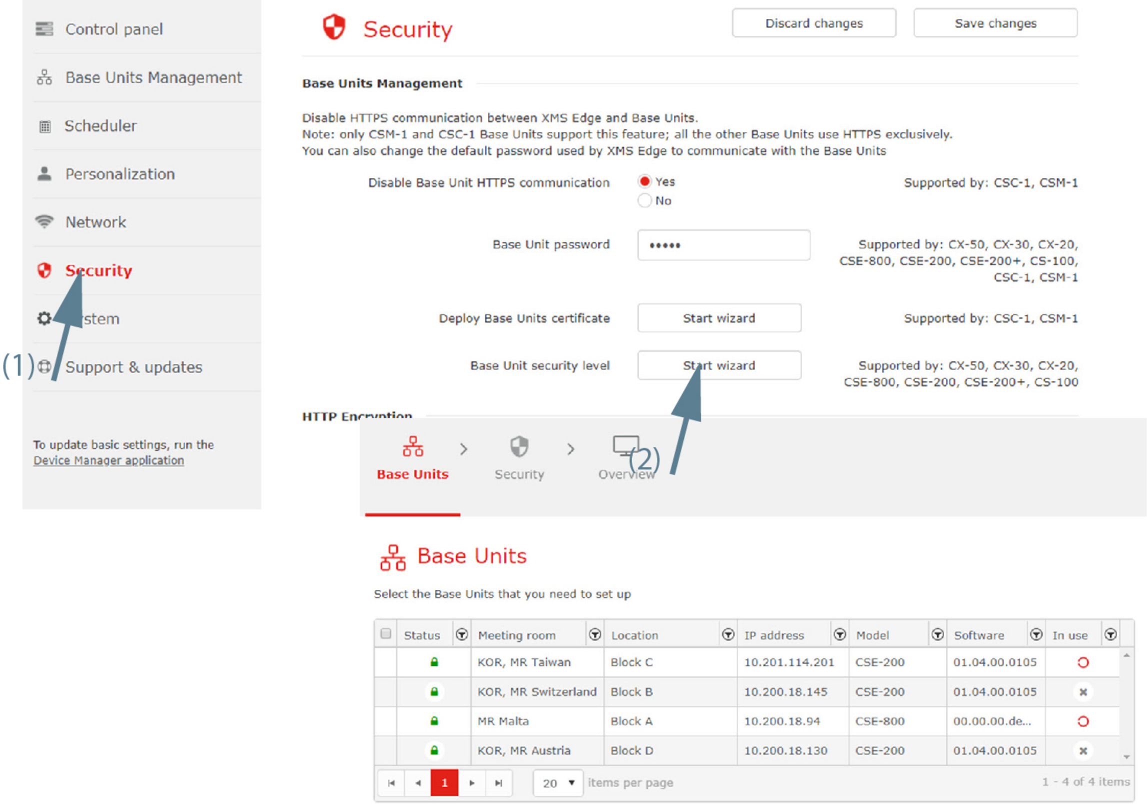
3.5.4 Security, Base Unit security level

Only for CSE-800, CSE-200, CSE-200+, CX-50, CX-50 Gen2, CX-30, CX-20, C-10 and C-5.

Changing the security level will require Button re-pairing.

How to set

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



To update basic settings, run the Device Manager application

Security

Base Units Management

Disable HTTPS communication between XMS Edge and Base Units.
Note: only CSM-1 and CSC-1 Base Units support this feature; all the other Base Units use HTTPS exclusively.
You can also change the default password used by XMS Edge to communicate with the Base Units

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

Base Unit password: ••••• — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

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

Base Unit security level: Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

HTTP Encryption

Base Units

Select the Base Units that you need to set up

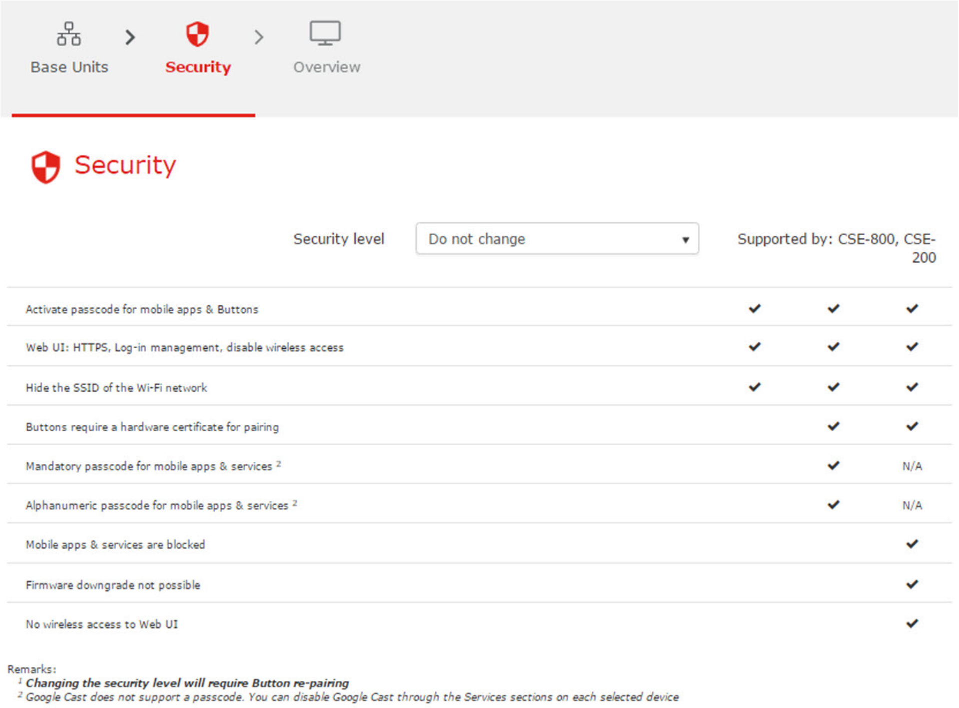
□	Status	Meeting room	Location	IP address	Model	Software	In use
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✖
	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	○
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✖

1 — 20 items per page — 1 - 4 of 4 items

Image 3–64 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).



Security level: Do not change

Supported by: CSE-800, CSE-200

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

Remarks:

[1] ***Changing the security level will require Button re-pairing***

[2] *Google Cast does not support a passcode. You can disable Google Cast through the Services sections on each selected device*

Image 3–65 Base Unit security

5. Click **Next** to continue.

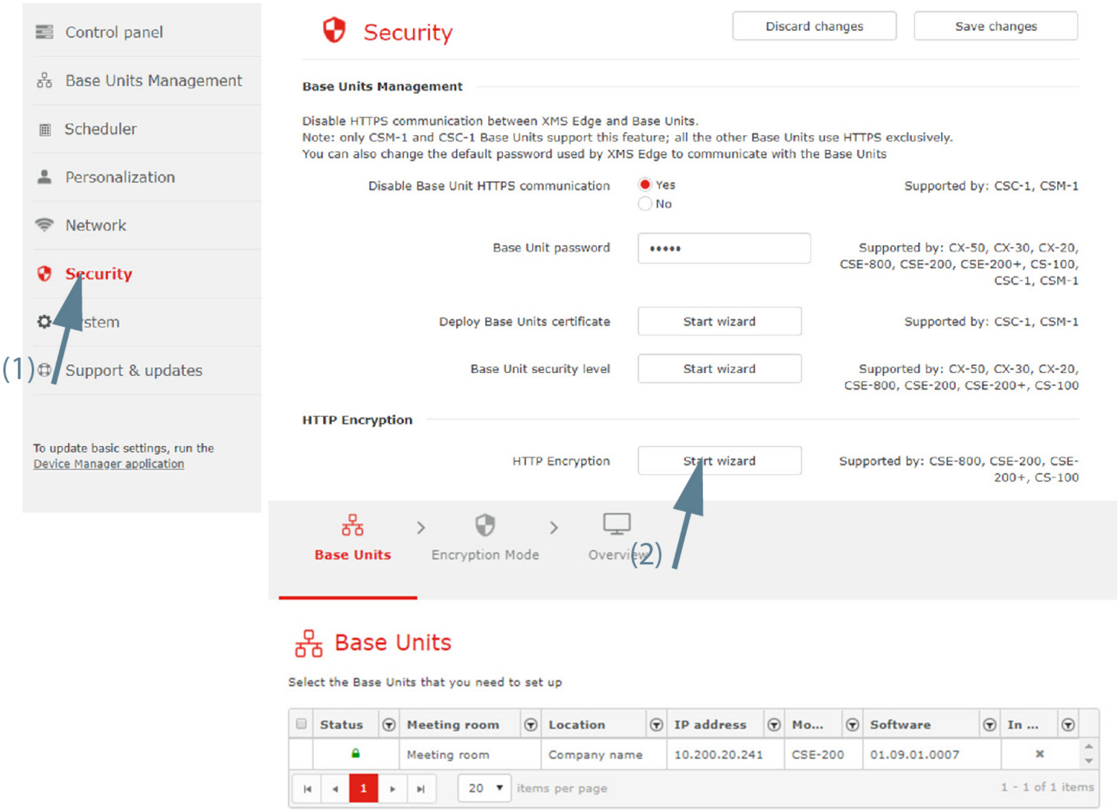
   An *Overview* window is displayed.

6. Click **Finish**.

3.5.5 HTTP Encryption

How to setup

1. In the menu pane, click on **Security** (1).
2. Click **Start wizard** next to *HTTP Encryption* (2).



To update basic settings, run the Device Manager application

Security

Base Units Management

Disable HTTPS communication between XMS Edge and Base Units.
Note: only CSM-1 and CSC-1 Base Units support this feature; all the other Base Units use HTTPS exclusively.
You can also change the default password used by XMS Edge to communicate with the Base Units

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

Base Unit password: ••••• — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

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

Base Unit security level: Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

HTTP Encryption

HTTP Encryption: Start wizard — Supported by: CSE-800, CSE-200, CSE-200+, CS-100

Base Units

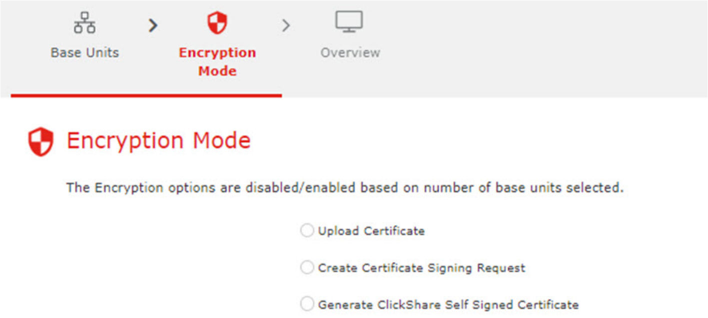
Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Mo...	Software	In ...
	🔒	Meeting room	Company name	10.200.20.241	CSE-200	01.09.01.0007	✖

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

Image 3–66

3. Select the Base Unit that you need to set up and click **Next**.
4. Select the desired encryption mode. Check the radio button of your choice.



Encryption Mode

The Encryption options are disabled/enabled based on number of base units selected.

○ Upload Certificate

○ Create Certificate Signing Request

○ Generate ClickShare Self Signed Certificate

Image 3–67

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

3.6 System

Only for IT admin user.

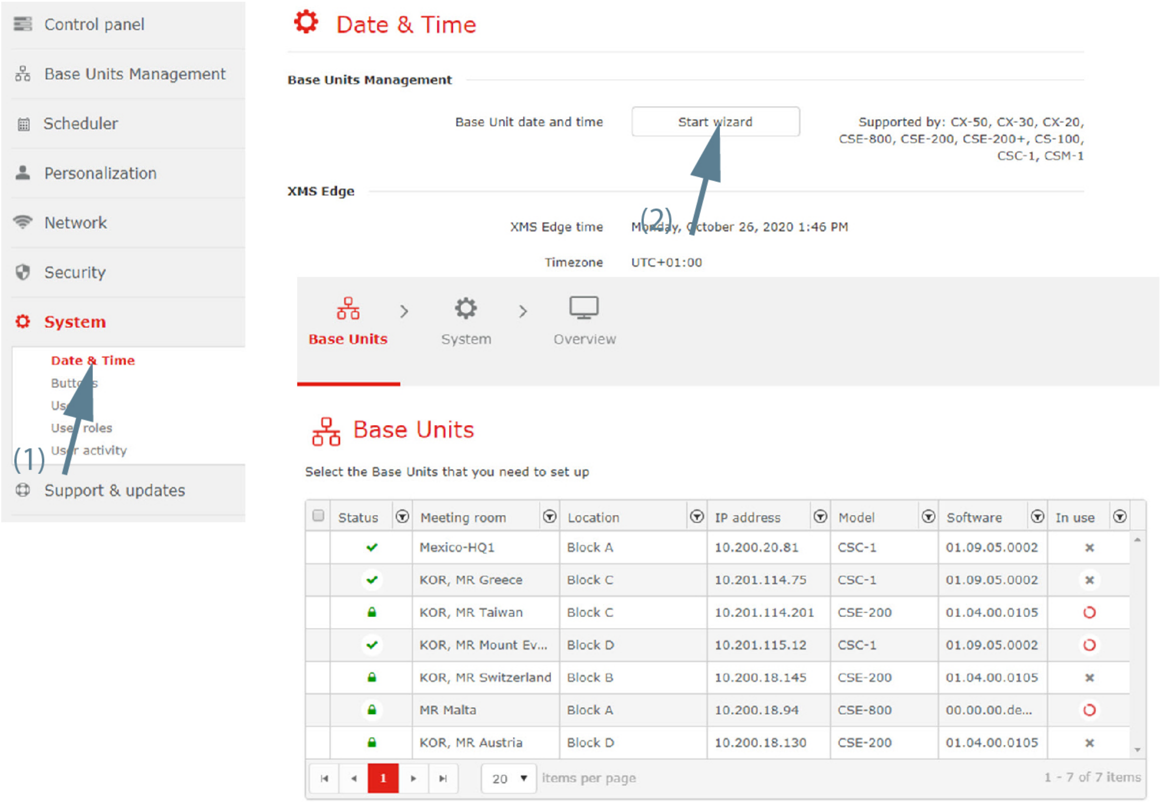
3.6.1 Date & Time

About date & time

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

How to set

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



Date & Time

Base Units Management

Base Unit date and time — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

XMS Edge

XMS Edge time: Monday, October 26, 2020 1:46 PM

Timezone: UTC+01:00

Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✗
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✗
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	✓	KOR, MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✗
	🔒	MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	○
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	✗

1 — 20 items per page — 1 - 7 of 7 items

Image 3–68 Date & time, start

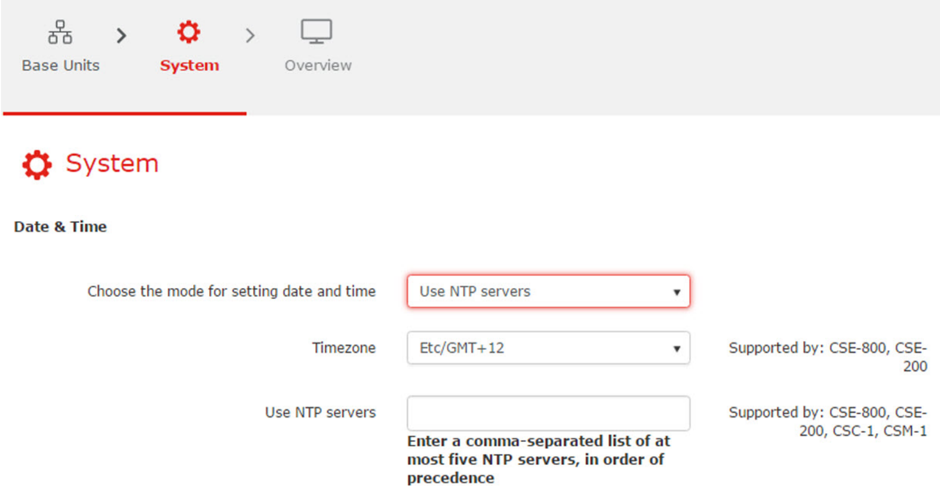
2. Click **Start wizard** next to *Base Unit date and time* (2).
3. Select the Base Unit(s) that you need to set up. Click **Next** to continue.
4. Choose the mode for setting date and time.

   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*.



Date & Time

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

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

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

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

Image 3–69 NTP server

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

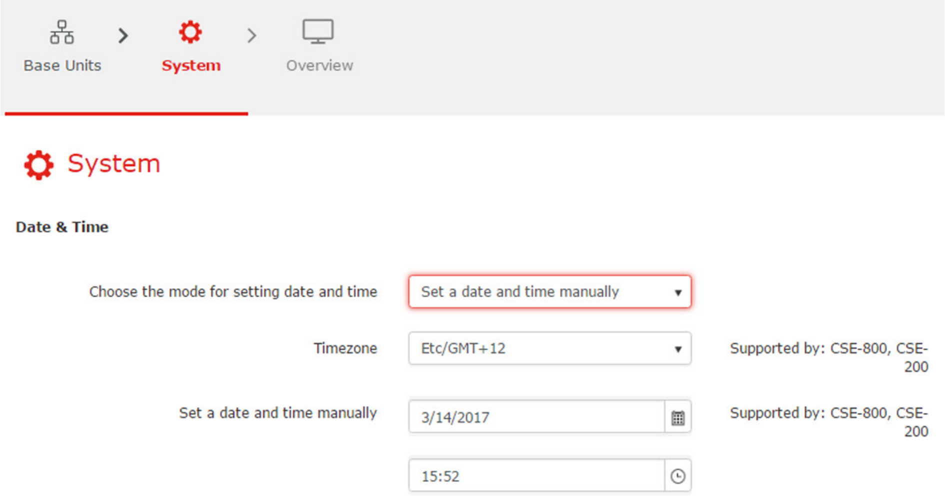
   Note: This is only for CSE-800, CSE-200, CSE-200+, CS-100, CS-100Huddle, C-5, C-10, CX-20, CX-30, CX-50 and CX-50 Gen2.

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*.



Date & Time

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

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

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

15:52

Image 3–70 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.

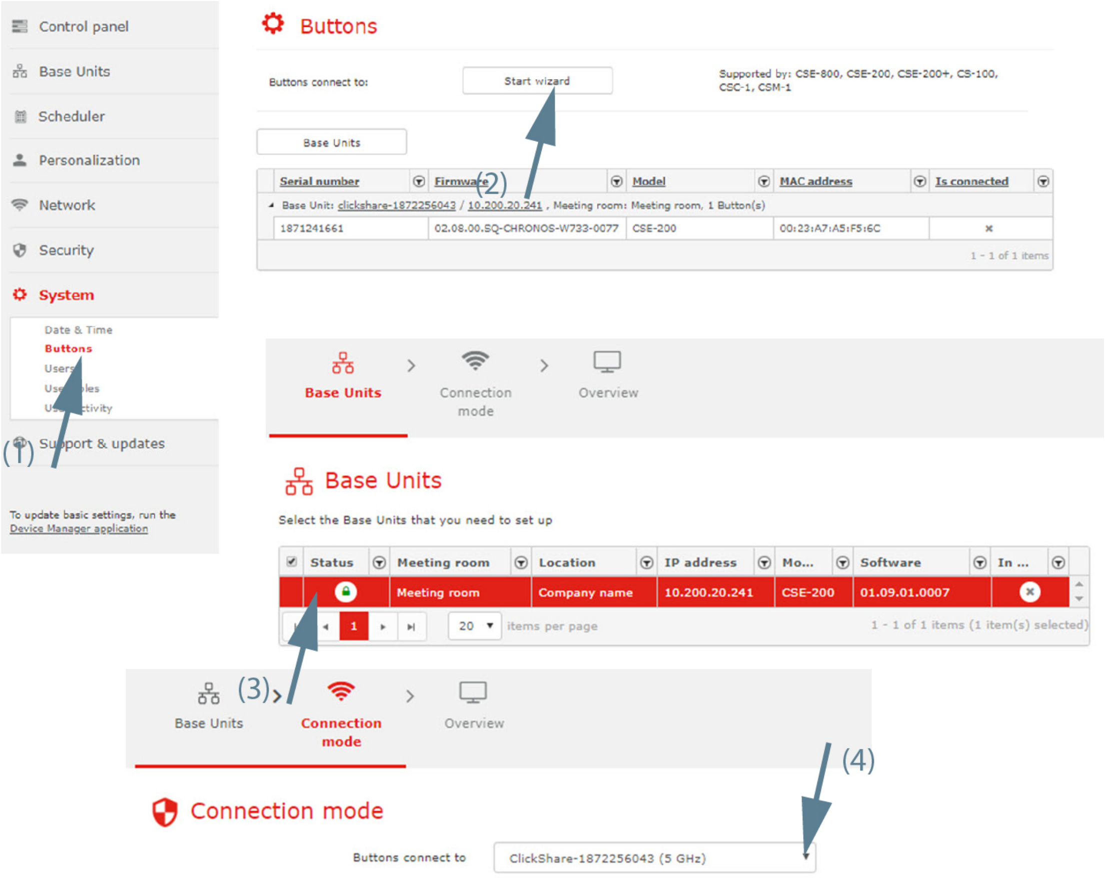
   An *Overview* window is displayed.

6. Click **Finish**.

3.6.2 Buttons

Buttons connection to Base Units

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



To update basic settings, run the Device Manager application

Buttons connect to: Start wizard

Supported by: CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Serial number	Firmware	Model	MAC address	Is connected
Base Unit: clickshare-1872256043 / 10.200.20.241 , Meeting room: Meeting room, 1 Button(s)				
1871241661	02.08.00.SQ-CHRONOS-W733-0077	CSE-200	00:23:A7:A5:F5:6C	✗

1 - 1 of 1 items

Base Units

Select the Base Units that you need to set up

☑	Status	Meeting room	Location	IP address	Mo...	Software	In ...
	🔒	Meeting room	Company name	10.200.20.241	CSE-200	01.09.01.0007	✗

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

Connection mode

Buttons connect to: ClickShare-1872256043 (5 GHz)

Image 3–71

2. Click on **Start wizard** next to *Buttons connect to*.
3. Select the Base Unit to connect to and click Next.

   The Connection mode window opens.

4. Select the way the Buttons are connecting with the Base Unit. Click on the drop down and select the desired setting.

   The following options are possible:

   - With the ClickShare Base Unit WiFi
   - External Access Point

About Buttons

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

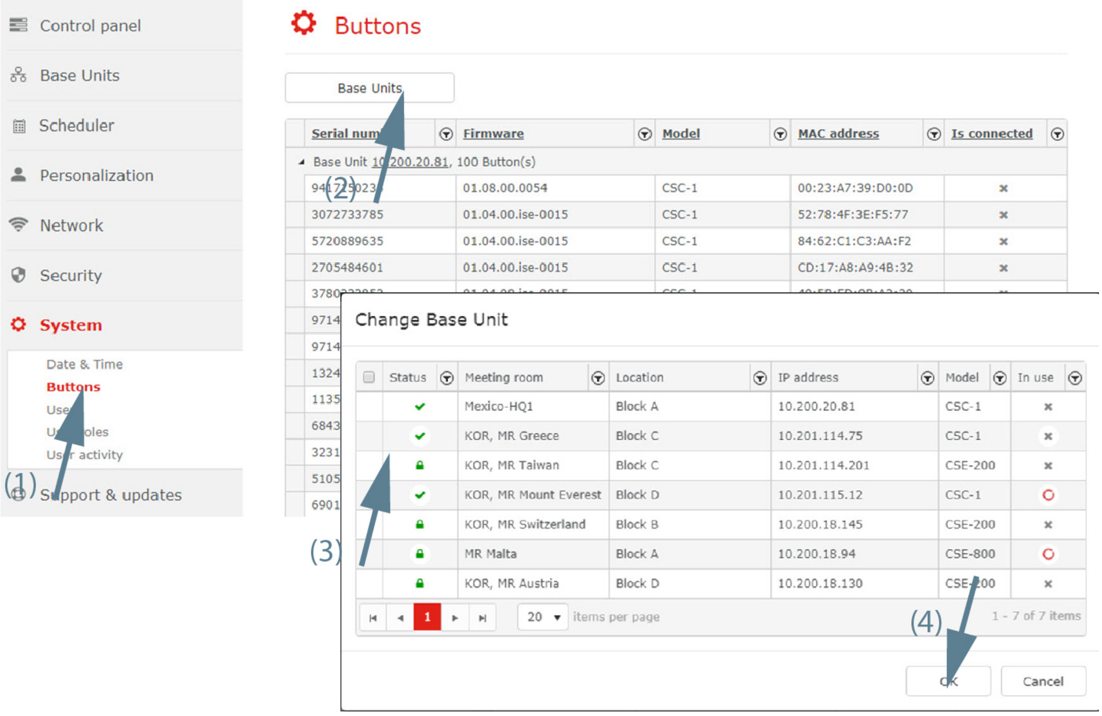
That overview contains the following information of a Button:

- 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).



Buttons

Base Units

Serial num[illegible]	Firmware	Model	MAC address	Is connected
Base Unit 10.200.20.81, 100 Button(s)				
941[illegible]023[illegible]	01.08.00.0054	CSC-1	00:23:A7:39:D0:0D	✗
3072733785	01.04.00.ise-0015	CSC-1	52:78:4F:3E:F5:77	✗
5720889635	01.04.00.ise-0015	CSC-1	84:62:C1:C3:AA:F2	✗
2705484601	01.04.00.ise-0015	CSC-1	CD:17:A8:A9:4B:32	✗
3780[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9714				
9714				
1324				
1135				
6843				
3231				
5105				
6901				

Change Base Unit

□	Status	Meeting room	Location	IP address	Model	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	✗
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	✗
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	✗
	✓	KOR, MR Mount Everest	Block D	10.201.115.12	CSC-1	○
	🔒	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	✗
	🔒	MR Malta	Block A	10.200.18.94	CSE-800	○
	🔒	KOR, MR Austria	Block D	10.200.18.130	CSE-200	✗

1 | 20 items per page | 1 - 7 of 7 items

OK | Cancel

Image 3–72 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.

3.6.3 Users

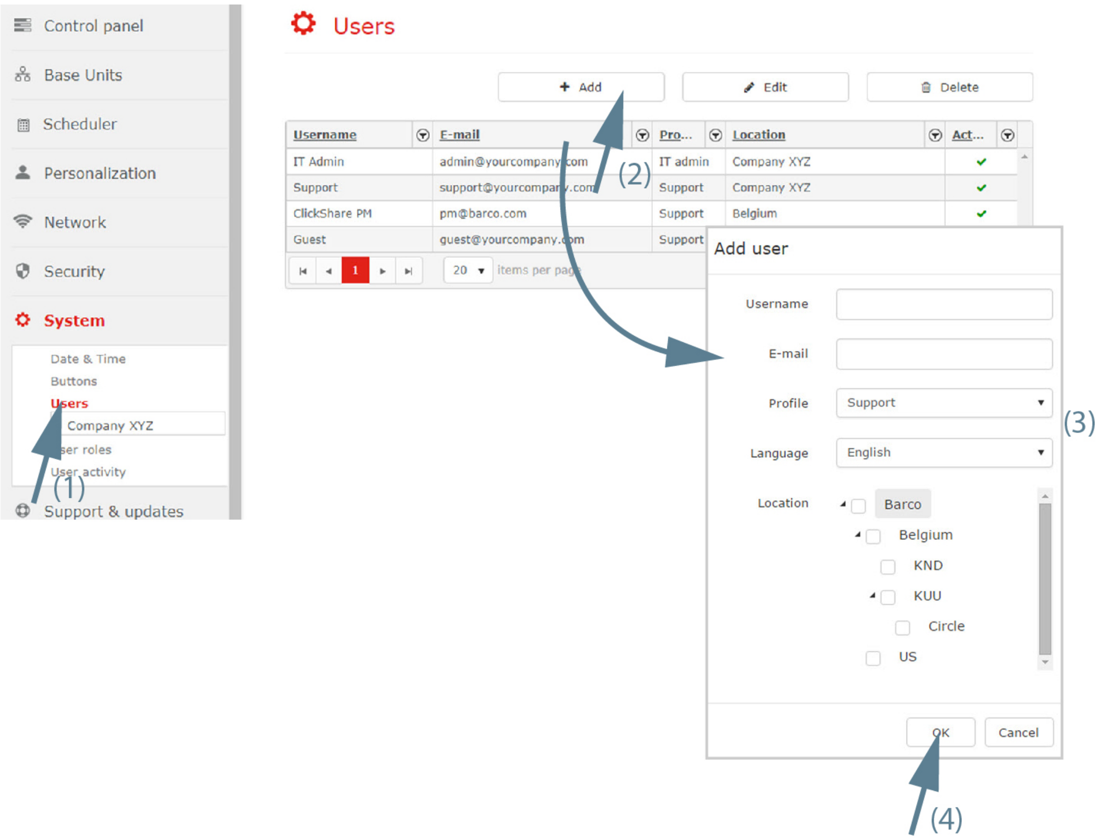
CAUTION: It is strongly recommended to change the password of the default IT admin account (admin@yourcompany.com) on first use and additionally create an IT admin account with a valid email address of the company for which XMS (virtual) Edge is installed.

Only for IT admin user.

3.6.3.1 Add new user

How to add

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



Username	E-mail	Pro...	Location	Act...
IT Admin	admin@yourcompany.com	IT admin	Company XYZ	✓
Support	support@yourcompany.com	Support	Company XYZ	✓
ClickShare PM	pm@barco.com	Support	Belgium	✓
Guest	guest@yourcompany.com	Support		

Username

E-mail

Profile: Support

Language: English

Location:
- □ Barco
  - □ Belgium
    - □ KND
    - □ KUU
      - □ Circle
  - □ US

Image 3–73 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).

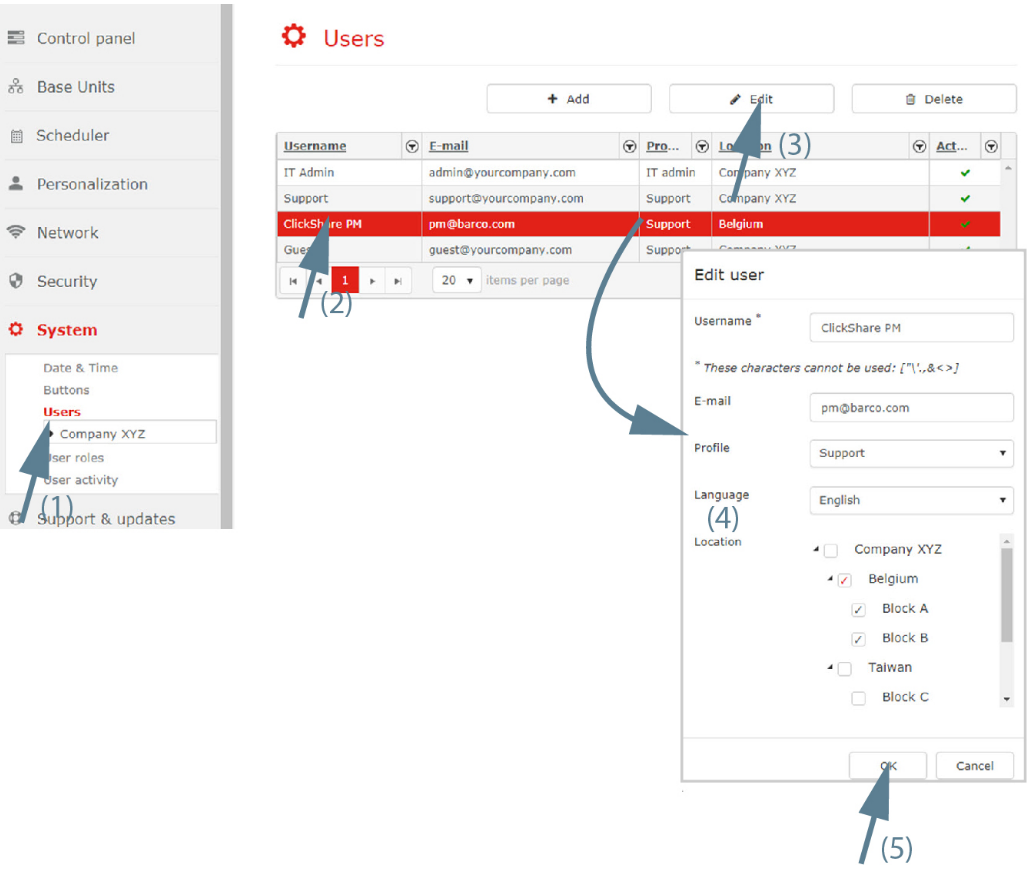
   The user is added to the list of active users.

   Users added by the IT admin using this method will receive an email with their password generated by the XMS. 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 82 in order to be able to populate the XMS with users without having the SMTP server set up.

3.6.3.2 Edit selected user

How to edit

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



Username	E-mail	Pro...	Location	Act...
IT Admin	admin@yourcompany.com	IT admin	Company XYZ	✓
Support	support@yourcompany.com	Support	Company XYZ	✓
ClickShare PM	pm@barco.com	Support	Belgium	✓
Guest	guest@yourcompany.com	Support	Company XYZ	✓

Username * ClickShare PM

* These characters cannot be used: ["\',&<>]

E-mail pm@barco.com

Profile Support

Language English

Location
- □ Company XYZ
  - ☑ Belgium
    - ☑ Block A
    - ☑ Block B
  - □ Taiwan
    - □ Block C

Image 3–74 Edit selected user

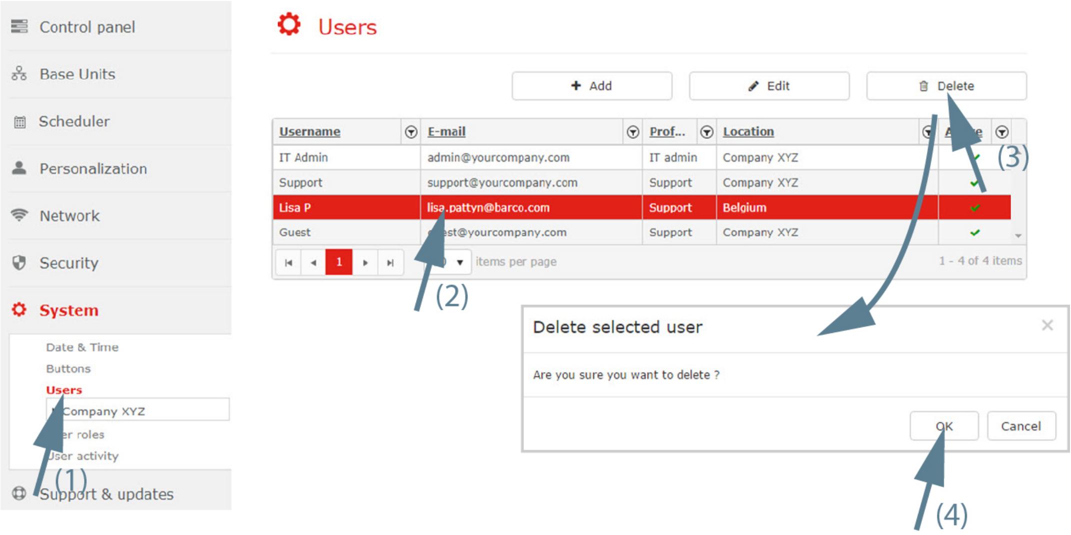
2. Select the user to edit (2).
3. Click on the **Edit** (3).

   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 XMS", 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).

3.6.3.3 Delete selected user

How to delete

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



Username	E-mail	Prof...	Location	A...e
IT Admin	admin@yourcompany.com	IT admin	Company XYZ	✓
Support	support@yourcompany.com	Support	Company XYZ	✓
Lisa P	lisa.pattyn@barco.com	Support	Belgium	✓
Guest	guest@yourcompany.com	Support	Company XYZ	✓

items per page 1 - 4 of 4 items

Delete selected user

Are you sure you want to delete ?

Image 3–75 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).

3.6.3.4 Filter users

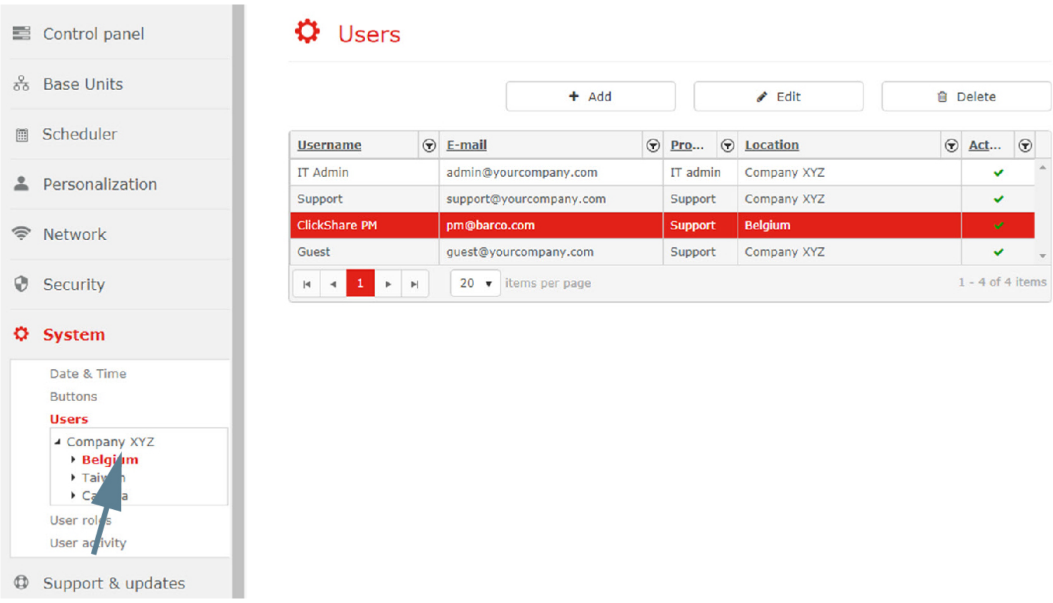
About filtering users

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

How to filter

1. Select **System** and click on the arrow before the main location to display a specific overview page (1).

   Click on the arrow to expand/collapse the tree and select the desired level.



Username	E-mail	Pro...	Location	Act...
IT Admin	admin@yourcompany.com	IT admin	Company XYZ	✓
Support	support@yourcompany.com	Support	Company XYZ	✓
ClickShare PM	pm@barco.com	Support	Belgium	✓
Guest	guest@yourcompany.com	Support	Company XYZ	✓

20 items per page 1 - 4 of 4 items

Image 3–76 Location filter on users

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

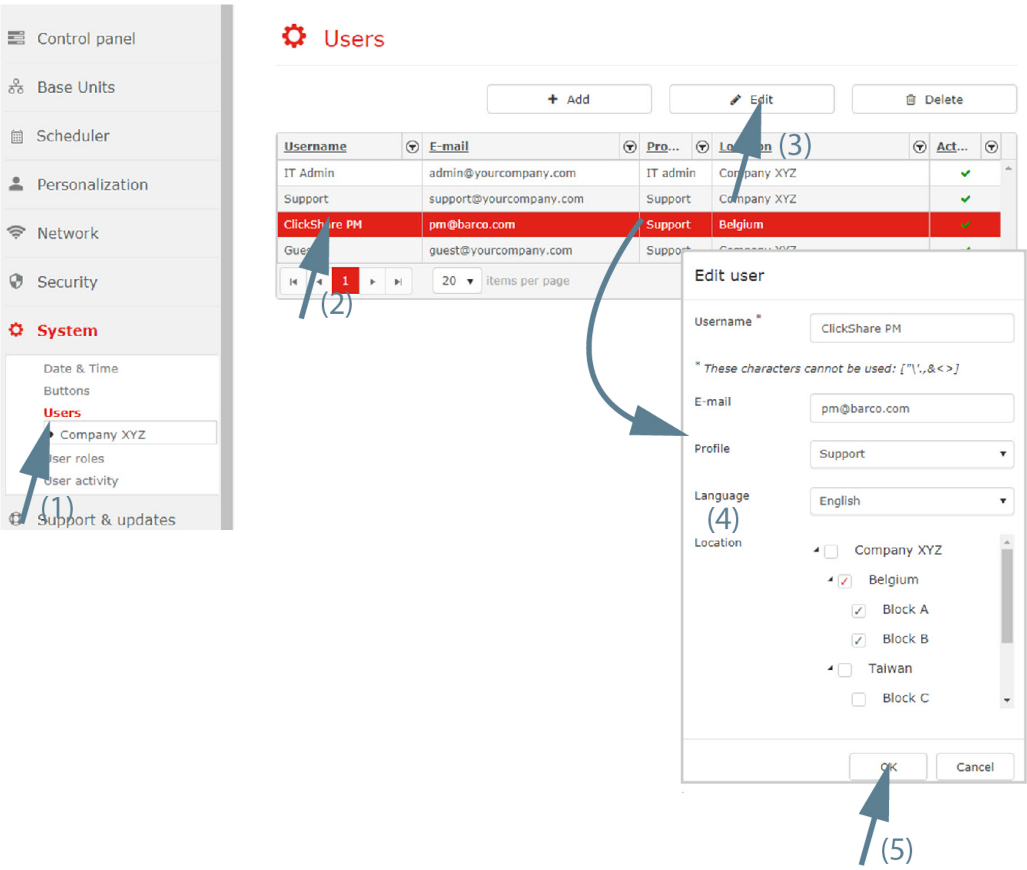
3.6.3.5 Accept/reject a registered user

What can be done?

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

How to accept a registered user

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



Username	E-mail	Pro...	Lo on	Act...
IT Admin	admin@yourcompany.com	IT admin	Co pany XYZ	✓
Support	support@yourcompany.com	Support	C mpany XYZ	✓
ClickSh re PM	pm@barco.com	Support	Belgium	✓
Gue	guest@yourcompany.com	Suppo		

20 items per page

Username * ClickShare PM

* These characters cannot be used: ["\',.&<>]

E-mail pm@barco.com

Profile Support

Language English

Location
- □ Company XYZ
  - ☑ Belgium
    - ☑ Block A
    - ☑ Block B
  - □ Taiwan
    - □ Block C

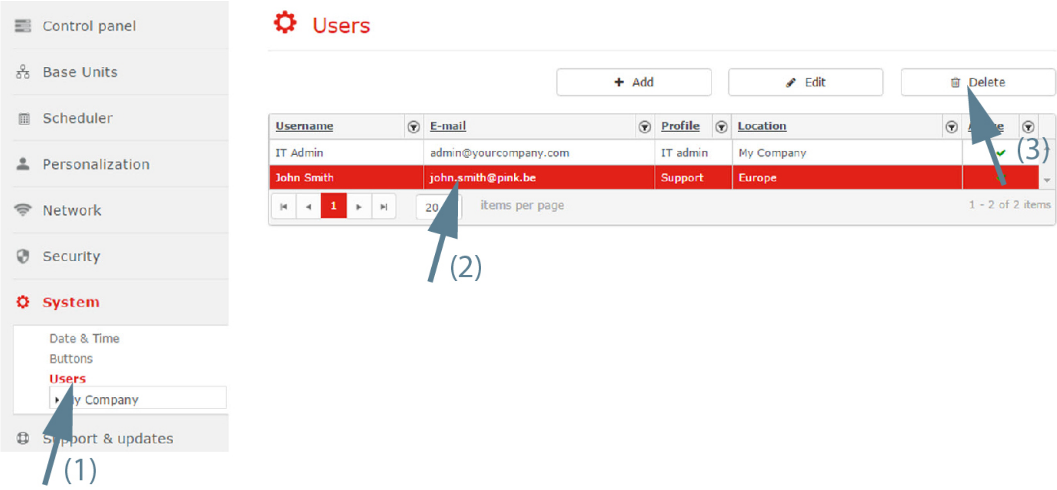
Image 3–77 Edit selected user

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 79 for more info.
5. Click **OK** (5).

   The registered user is activated and can login now.

How to reject a registered user

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



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

Image 3–78

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

   The registered user is removed.

3.6.4 User roles

3.6.4.1 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.

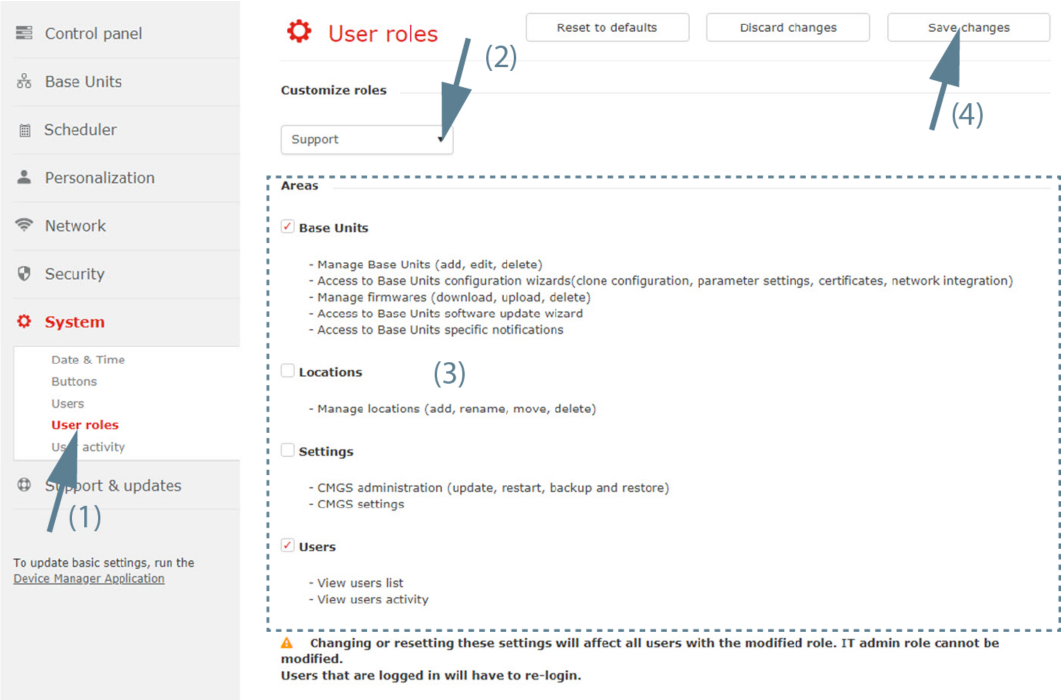
The customization can be done in different areas such as:

- 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).



To update basic settings, run the Device Manager Application

Customize roles

Support

Areas

☑ **Base Units**

- Manage Base Units (add, edit, delete)
- Access to Base Units configuration wizards(clone configuration, parameter settings, certificates, network integration)
- Manage firmwares (download, upload, delete)
- Access to Base Units software update wizard
- Access to Base Units specific notifications

□ **Locations**

- Manage locations (add, rename, move, delete)

□ **Settings**

- CMGS administration (update, restart, backup and restore)
- CMGS settings

☑ **Users**

- View users list
- View users activity

⚠ **Changing or resetting these settings will affect all users with the modified role. IT admin role cannot be modified.**
Users that are logged in will have to re-login.

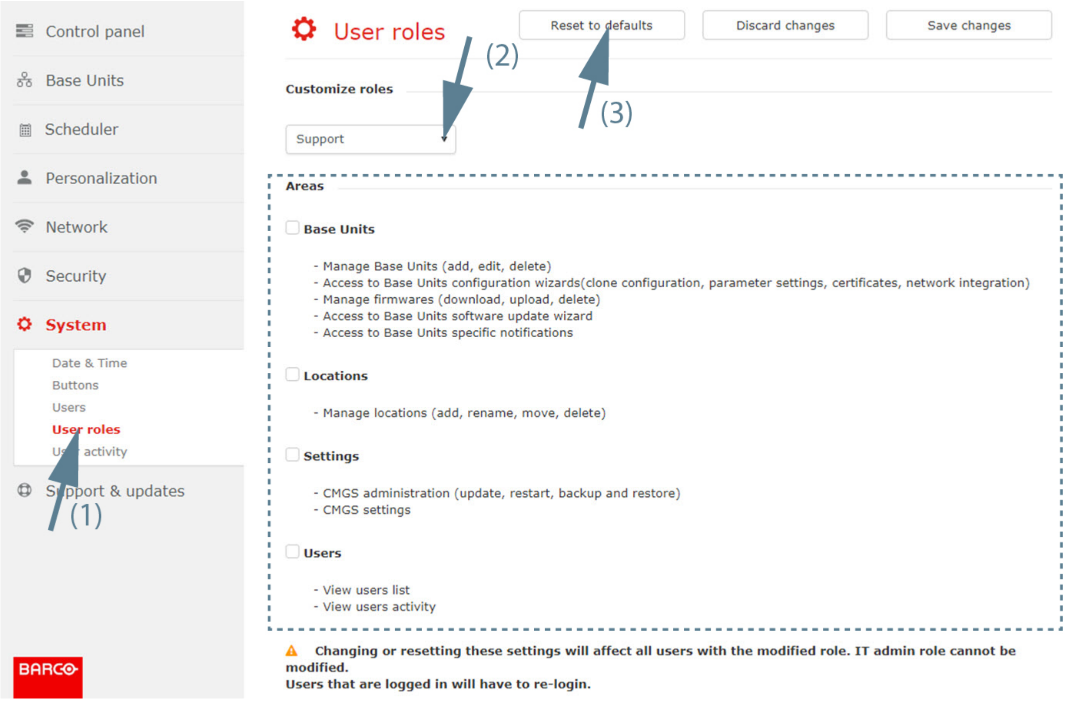
Image 3–79 Setup user roles

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).

3.6.4.2 Reset to default roles

How to return to default settings

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



Customize roles

Support

Areas

□ **Base Units**

- Manage Base Units (add, edit, delete)
- Access to Base Units configuration wizards(clone configuration, parameter settings, certificates, network integration)
- Manage firmwares (download, upload, delete)
- Access to Base Units software update wizard
- Access to Base Units specific notifications

□ **Locations**

- Manage locations (add, rename, move, delete)

□ **Settings**

- CMGS administration (update, restart, backup and restore)
- CMGS settings

□ **Users**

- View users list
- View users activity

⚠ **Changing or resetting these settings will affect all users with the modified role. IT admin role cannot be modified.**
Users that are logged in will have to re-login.

Image 3–80 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).

3.6.5 User activity

About user activity

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

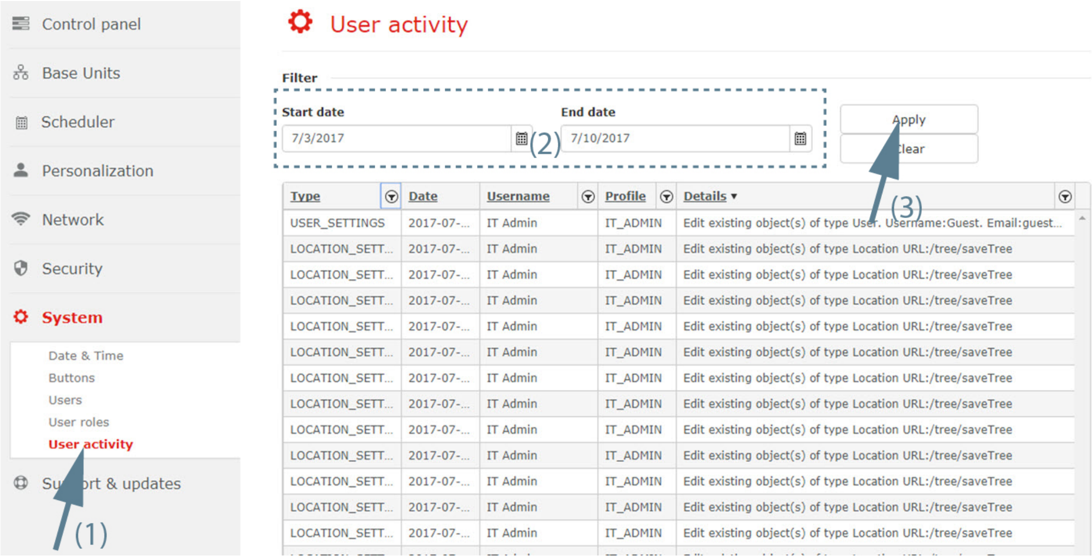
- Type of action
- Date
- Username
- Profile (role)
- Detail of the action

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).



Start date: 7/3/2017

End date: 7/10/2017

Type	Date	Username	Profile	Details ▾
USER_SETTINGS	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type User. Username:Guest. Email:guest...
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree
LOCATION_SETT...	2017-07-...	IT Admin	IT_ADMIN	Edit existing object(s) of type Location URL:/tree/saveTree

Image 3–81

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.

3.7 Support & updates

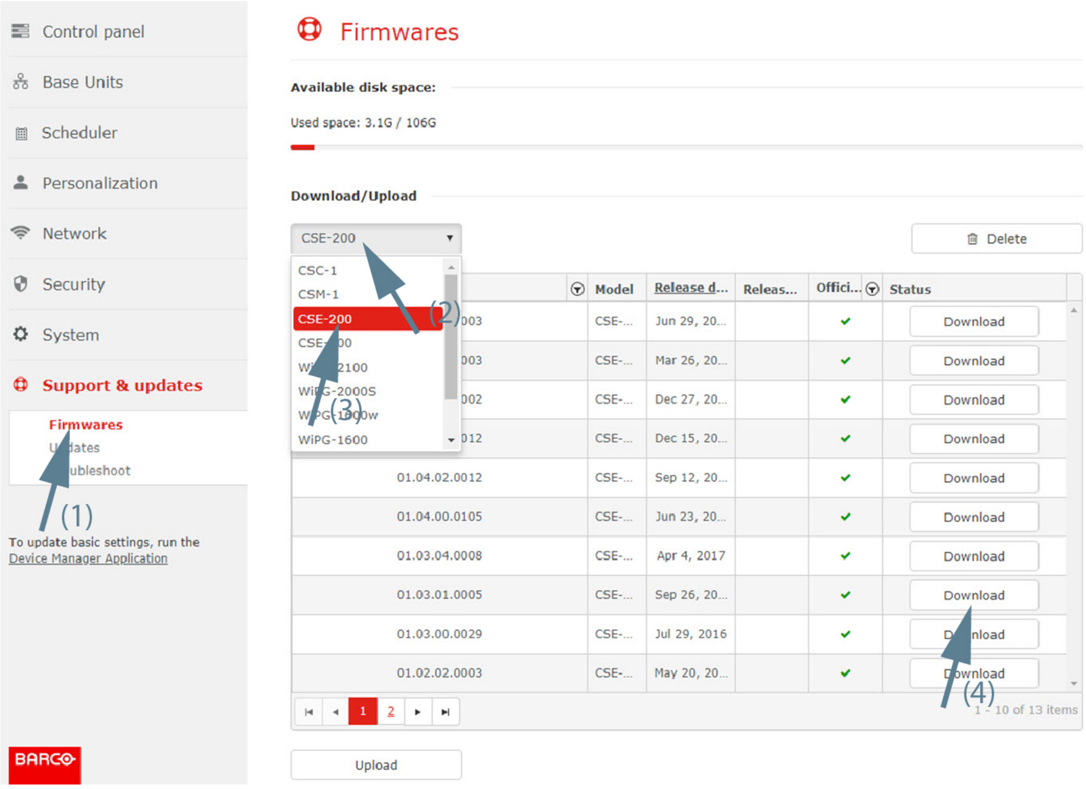
3.7.1 Firmwares

What should be done?

Before a firmware update can take place, the firmware must be available on the XMS (virtual) Edge. First, it should be downloaded.

Download/upload

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



To update basic settings, run the Device Manager Application

Available disk space:

Used space: 3.1G / 106G

Download/Upload

	Model	Release d...	Releas...	Offici...	Status
003	CSE-...	Jun 29, 20...		✓	Download
003	CSE-...	Mar 26, 20...		✓	Download
002	CSE-...	Dec 27, 20...		✓	Download
012	CSE-...	Dec 15, 20...		✓	Download
01.04.02.0012	CSE-...	Sep 12, 20...		✓	Download
01.04.00.0105	CSE-...	Jun 23, 20...		✓	Download
01.03.04.0008	CSE-...	Apr 4, 2017		✓	Download
01.03.01.0005	CSE-...	Sep 26, 20...		✓	Download
01.03.00.0029	CSE-...	Jul 29, 2016		✓	Download
01.02.02.0003	CSE-...	May 20, 20...		✓	Download

1 - 10 of 13 items

Image 3–82 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 XMS (virtual) Edge 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 XMS (virtual) Edge.

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**.

3.7.2 Updates

3.7.2.1 Base Unit firmware upgrade

About software update

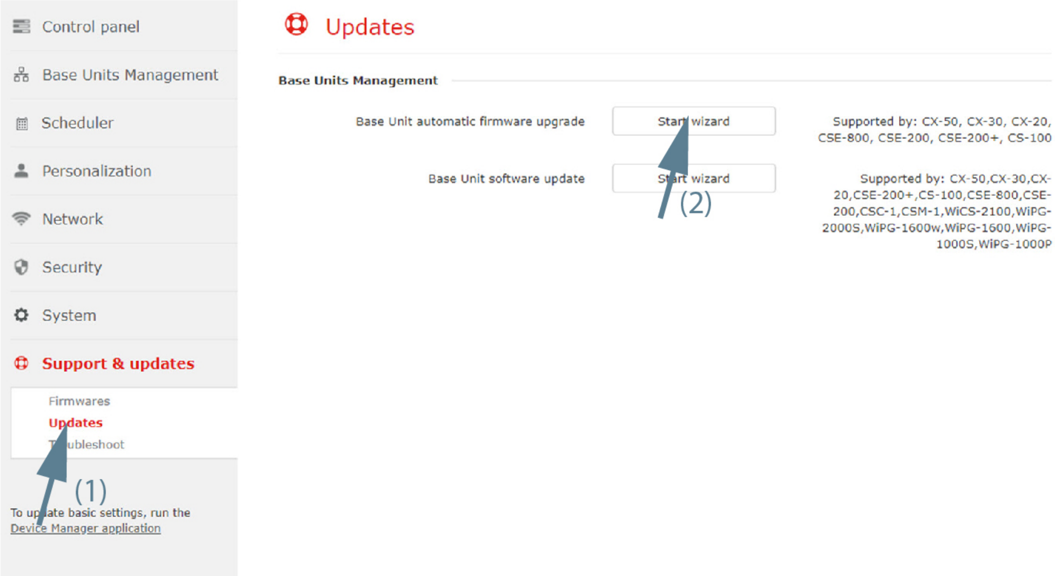
The firmware of a single Base Unit or of multiple Base Units can be updated with XMS (virtual) Edge. The update can be executed immediately or it can be scheduled.

The Base Unit firmware must be loaded on the XMS (virtual) Edge, prior the update. XMS (virtual) Edge may directly download a firmware from Barco site, or the firmware may be uploaded to XMS (virtual) Edge.

> An update takes between 10 and 20 minutes for a CSC-1/CSE-200/CSE-800/CSE-200+/C-5/C-10/CX-20/CX-30/CX-50/CX-50 Gen2 and 15 up to 30 minutes for a CSM-1.

Automatic firmware update[4]

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



Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100

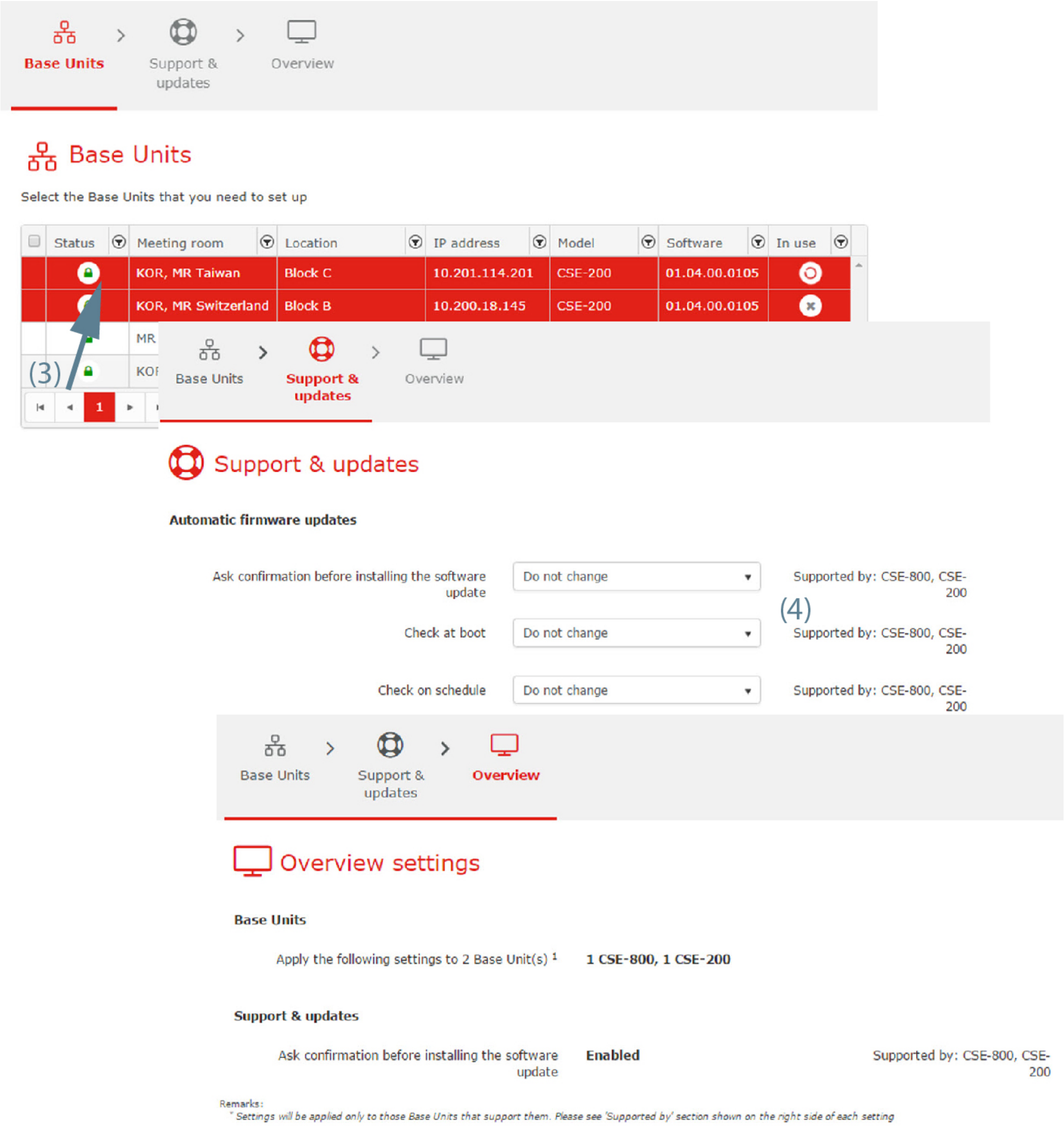
Supported by: CX-50,CX-30,CX-20,CSE-200+,CS-100,CSE-800,CSE-200,CSC-1,CSM-1,WiCS-2100,WiPG-2000S,WiPG-1600w,WiPG-1600,WiPG-1000S,WiPG-1000P

To update basic settings, run the Device Manager application

Image 3–83 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).

[4] only for CSE devices



Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	●	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	●	KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	☒
	●	MR					
	●	KOI					

Support & updates

Automatic firmware updates

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

Overview settings

Base Units

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

Support & updates

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

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

Image 3–84 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.

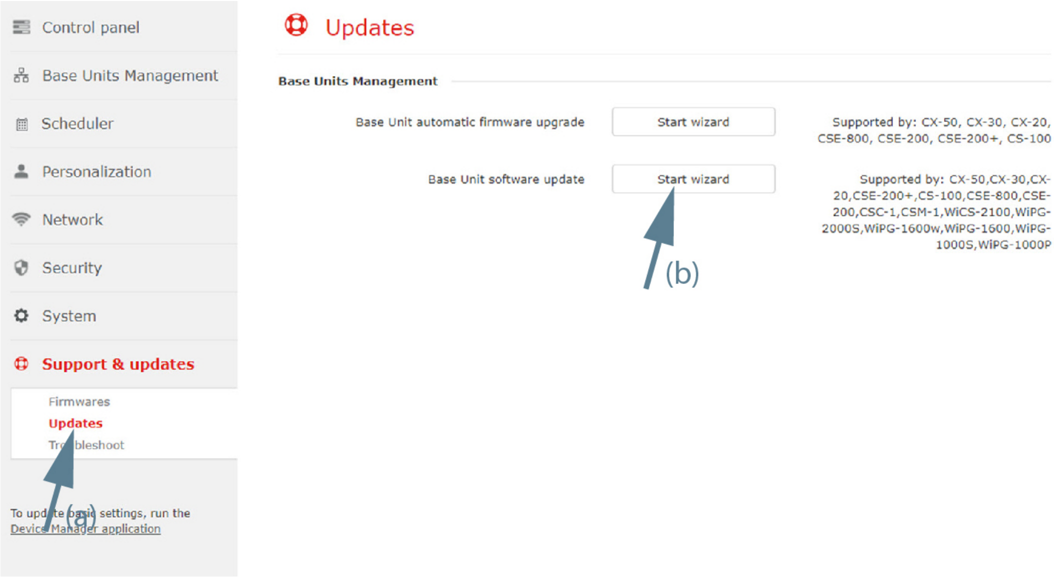
6. Click **Finish**.

Software update[5]

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

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

[5] all models

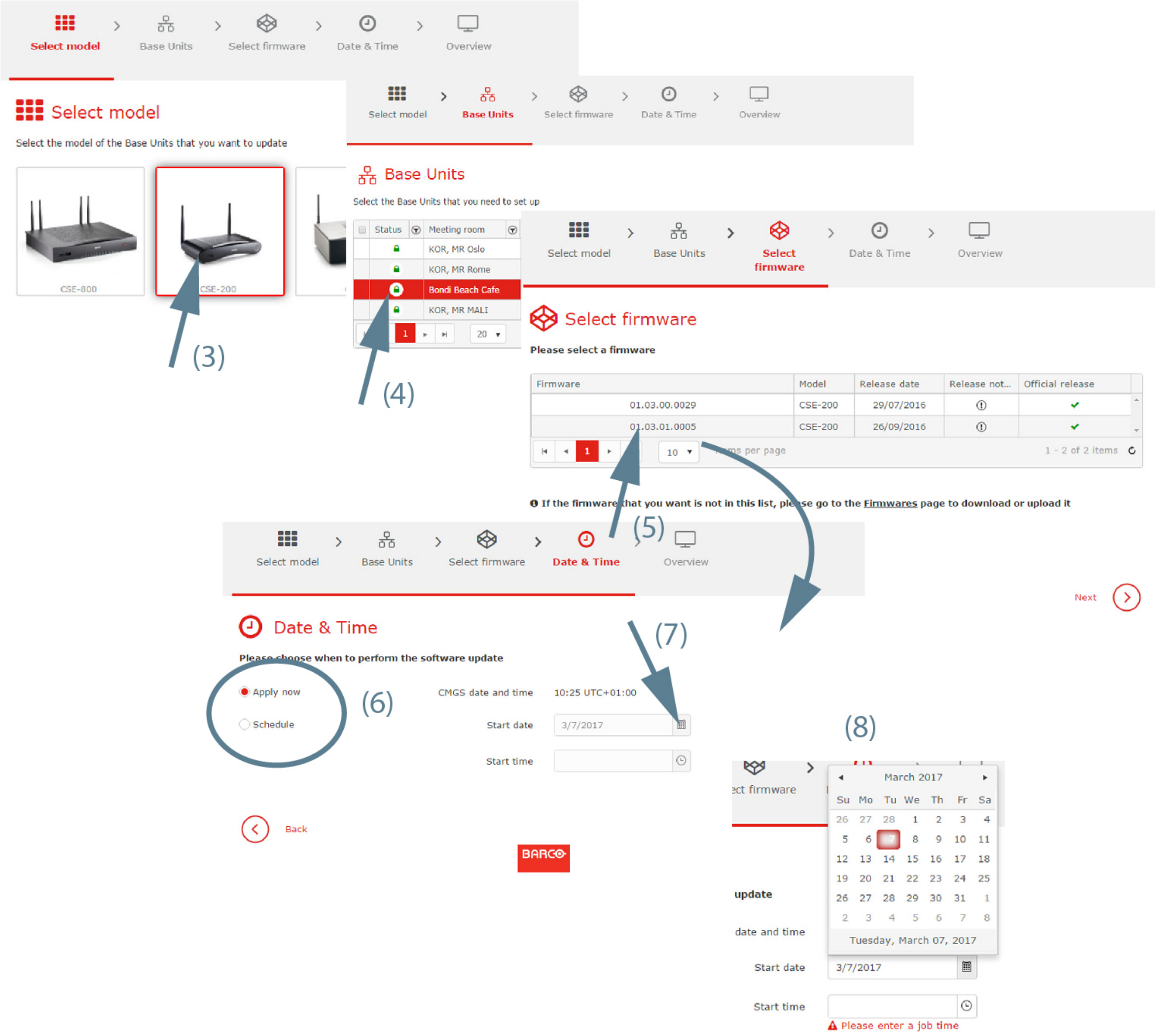


To update basic settings, run the Device Manager application

Base Unit automatic firmware upgrade	Start wizard	Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100
Base Unit software update	Start wizard	Supported by: CX-50,CX-30,CX-20,CSE-200+,CS-100,CSE-800,CSE-200,CSC-1,CSM-1,WiCS-2100,WiPG-2000S,WiPG-1600w,WiPG-1600,WiPG-1000S,WiPG-1000P

Image 3–85 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).



Select model

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

Base Units

Select the Base Units that you need to set up

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

Select firmware

Please select a firmware

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

10 items per page 1 - 2 of 2 items

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

Date & Time

Please choose when to perform the software update

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

Start date 3/7/2017

Start time

Please enter a job time

Image 3–86 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 step 6.
   - ▶ If no, go first to the *Firmwares* page. For more info, see "Firmwares", page 85.
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

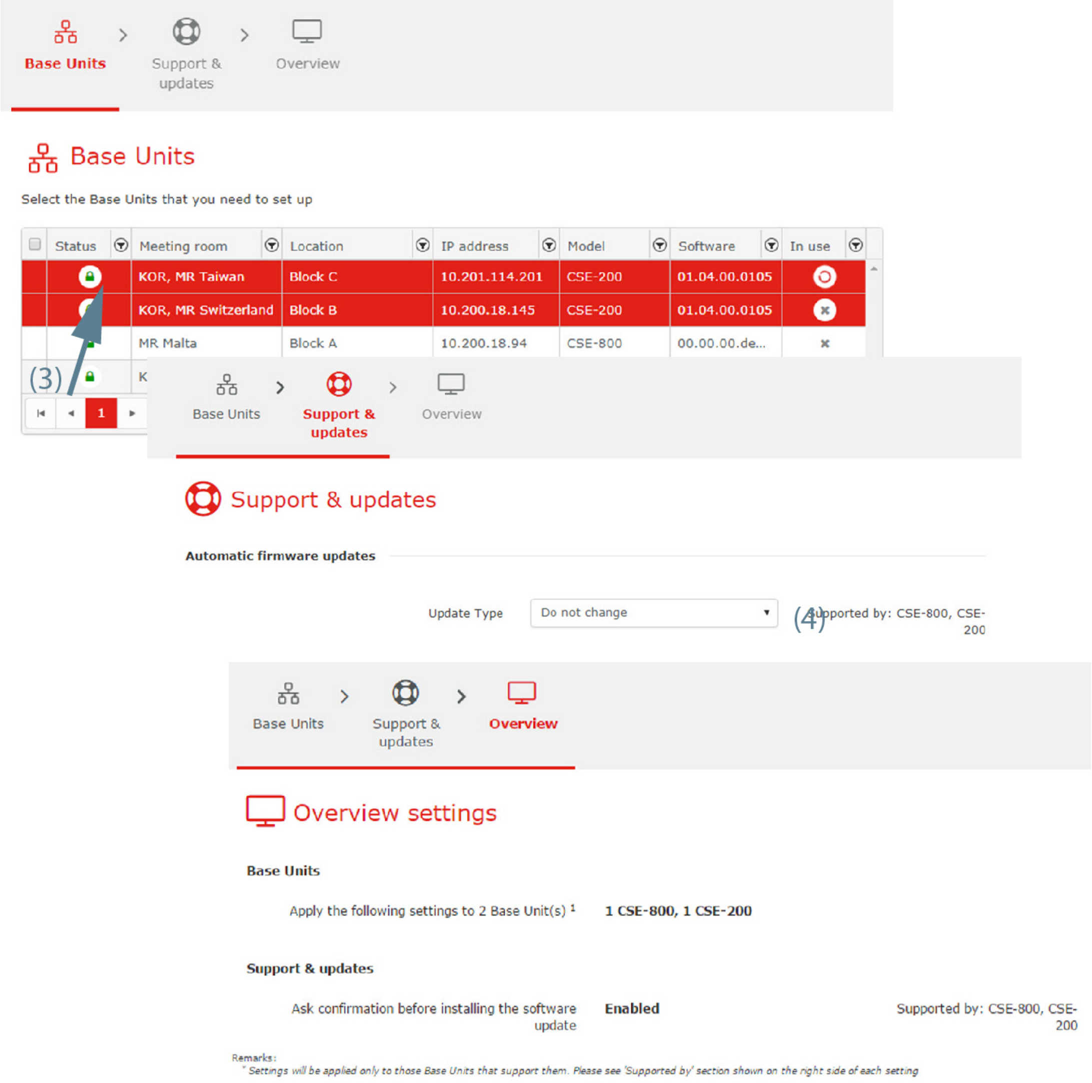
   click on the icon in the date field to open a calender and select a month and a day. To change the month, click on the right or left arrow next to month name until the desired month and year are obtained. Click on a number in the number field to setup the day.
8. When date and time is filled out, click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

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

3.7.2.2 XMS (virtual) Edge upgrade

How to upgrade

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



Base Units

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
		KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
		KOR, MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	✕
		MR Malta	Block A	10.200.18.94	CSE-800	00.00.00.de...	✕
		K					

Support & updates

Automatic firmware updates

Update Type: Do not change — Supported by: CSE-800, CSE-200

Overview settings

Base Units

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

Support & updates

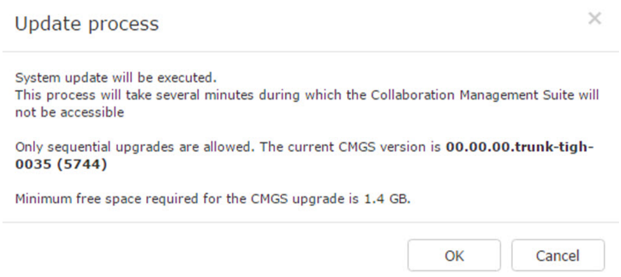
Ask confirmation before installing the software update — Enabled — Supported by: CSE-800, CSE-200

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

Image 3–87 CMGS upgrade wizard

2. Click on the **Upgrade CMGS** button next to *XMS (virtual) Edge upgrade* (b).

   An *Update process message* is displayed.



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

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

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

Image 3–88 Update process

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

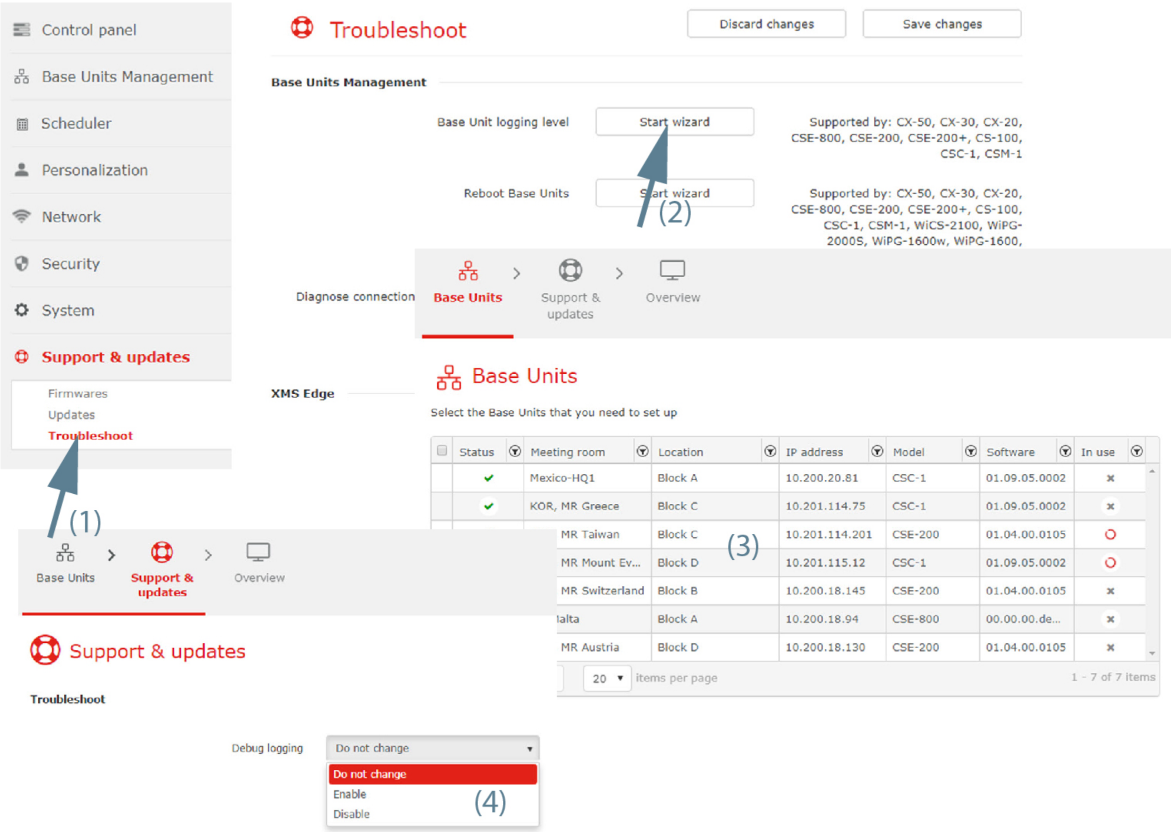
3. Click **OK** to continue.

3.7.3 Troubleshoot

3.7.3.1 Base Unit logging level

How to set

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



Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600,

Select the Base Units that you need to set up

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	×
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	×
		MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
		MR Mount Ev...	Block D	10.201.115.12	CSC-1	01.09.05.0002	○
		MR Switzerland	Block B	10.200.18.145	CSE-200	01.04.00.0105	×
		alta	Block A	10.200.18.94	CSE-800	00.00.00.de...	×
		MR Austria	Block D	10.200.18.130	CSE-200	01.04.00.0105	×

20 items per page 1 - 7 of 7 items

Debug logging: Do not change

Image 3–89 Troubleshoot, Base Unit logging level

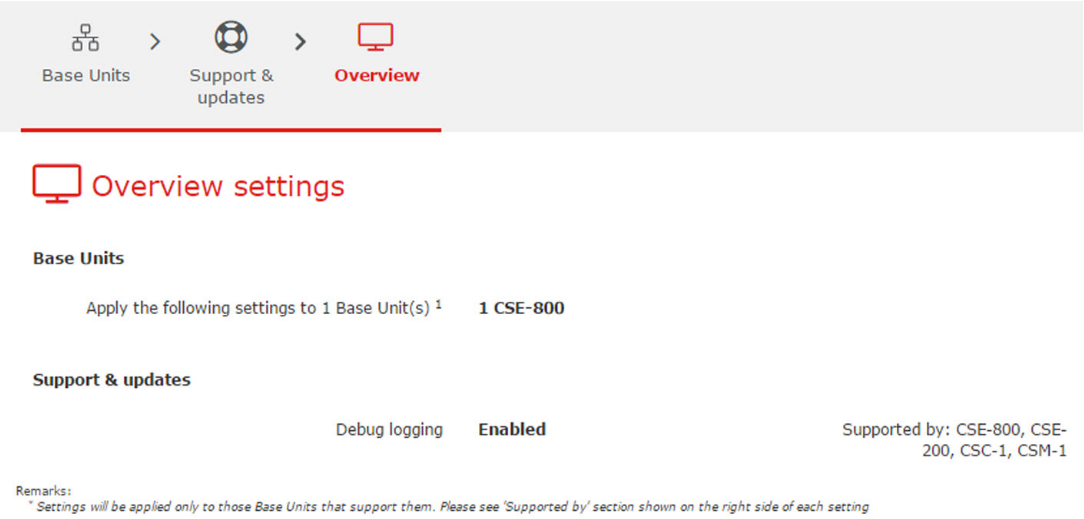
2. Click **Start wizard** next to *Base Unit logging level* (2).
3. Select Base Unit(s) (3) and click **Next**.
4. Click on the drop down next to *Debug logging* and select the desired setting (4).

The following settings are possible:

- Do not change: the current setting remains active.
- Enable: debug logging is enabled.
- Disable: debug logging is disabled.

5. Click **Next** to continue.

   An overview page is displayed.



Overview settings

Base Units

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

Support & updates

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

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

Image 3–90 Overview settings

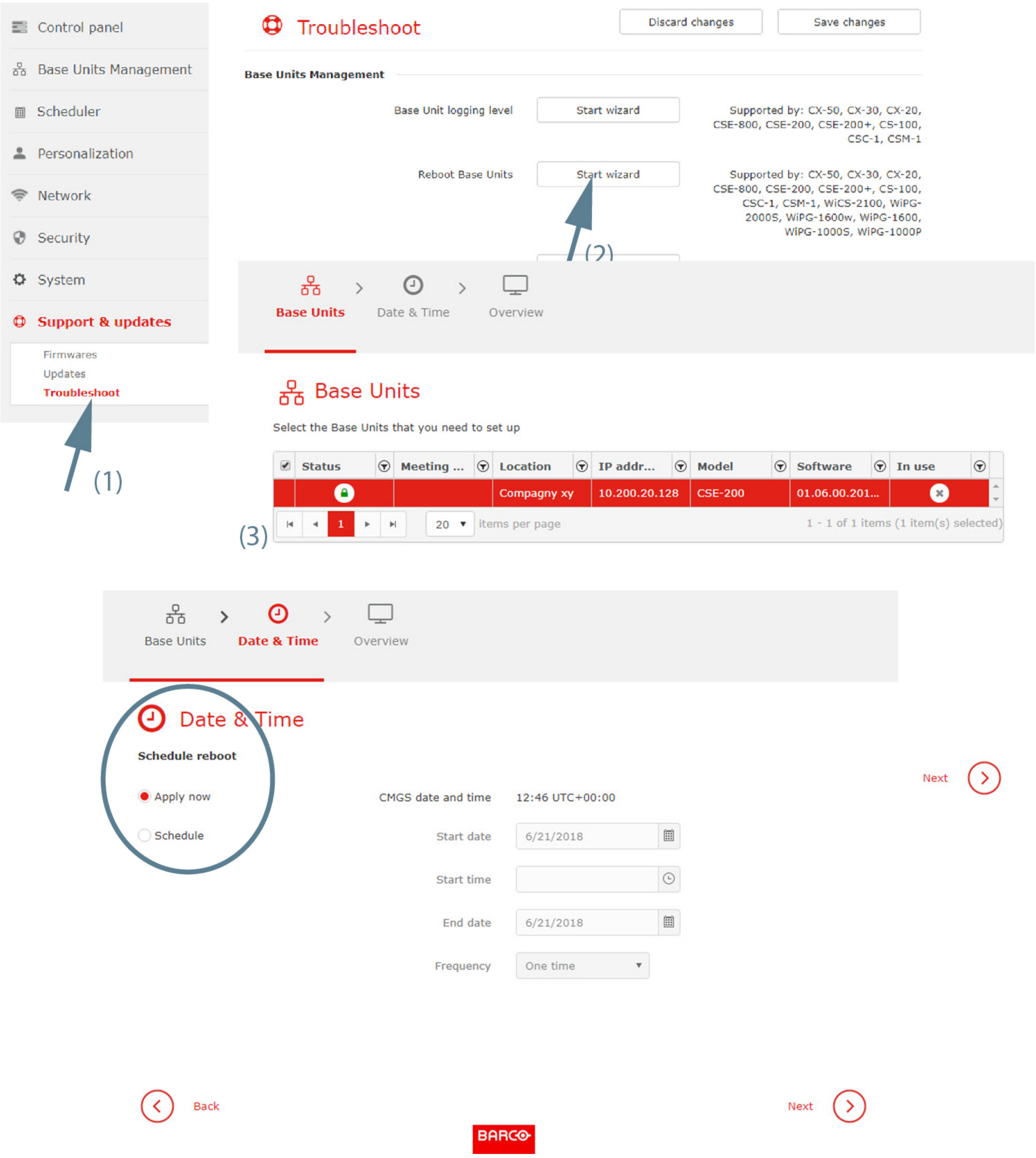
6. Click **Finish**.

3.7.3.2 Reboot Base Units

What can be done?

How to reboot

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



Troubleshoot

Discard changes | Save changes

Base Units Management

Base Unit logging level — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Reboot Base Units — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

Base Units > Date & Time > Overview

Base Units

Select the Base Units that you need to set up

☑	Status	Meeting ...	Location	IP addr...	Model	Software	In use
	🔒		Compagny xy	10.200.20.128	CSE-200	01.06.00.201...	☒

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

Base Units > Date & Time > Overview

Date & Time

Schedule reboot

● Apply now

○ Schedule

CMGS date and time: 12:46 UTC+00:00

Start date: 6/21/2018

Start time:

End date: 6/21/2018

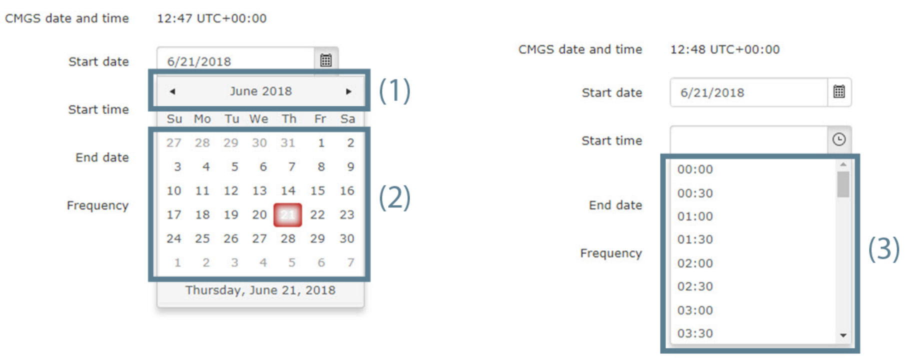
Frequency: One time

Back — Next

Image 3–91 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).



CMGS date and time 12:47 UTC+00:00

Start date 6/21/2018

CMGS date and time 12:48 UTC+00:00

Start date 6/21/2018

Image 3–92 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

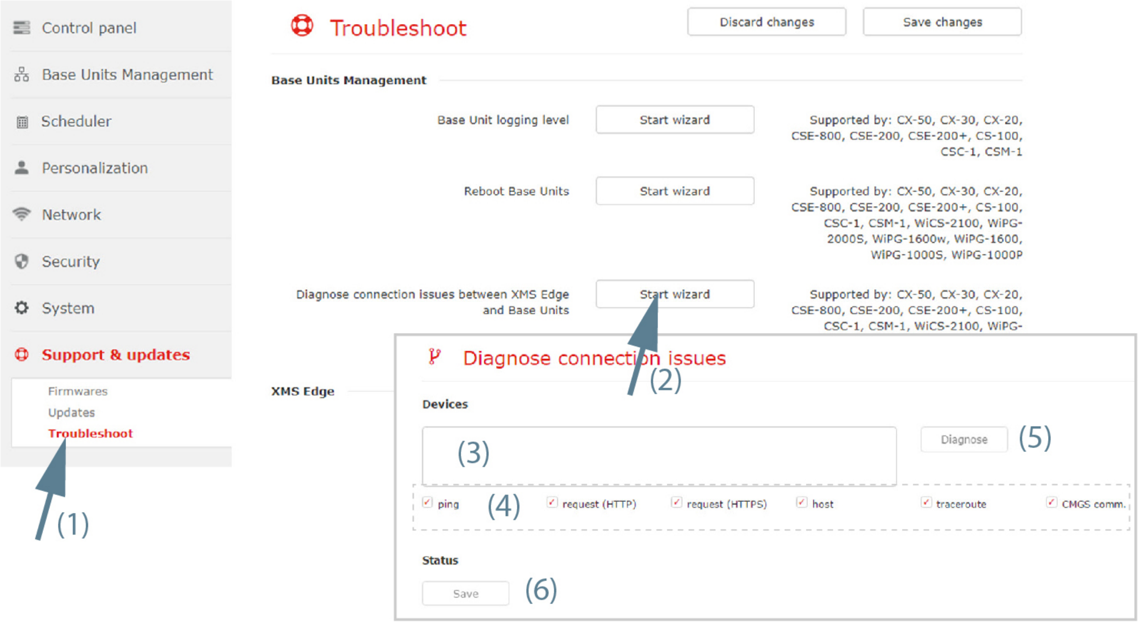
enter the start & end date (mm/dd/yyyy) and time (hh:mm) by clicking in the input field and changing the values.

6. Click **Next** to continue.

3.7.3.3 Diagnose connection issues XMS (virtual) Edge - Base Unit

How to setup

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



Base Unit logging level — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Reboot Base Units — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

Diagnose connection issues between XMS Edge and Base Units — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-

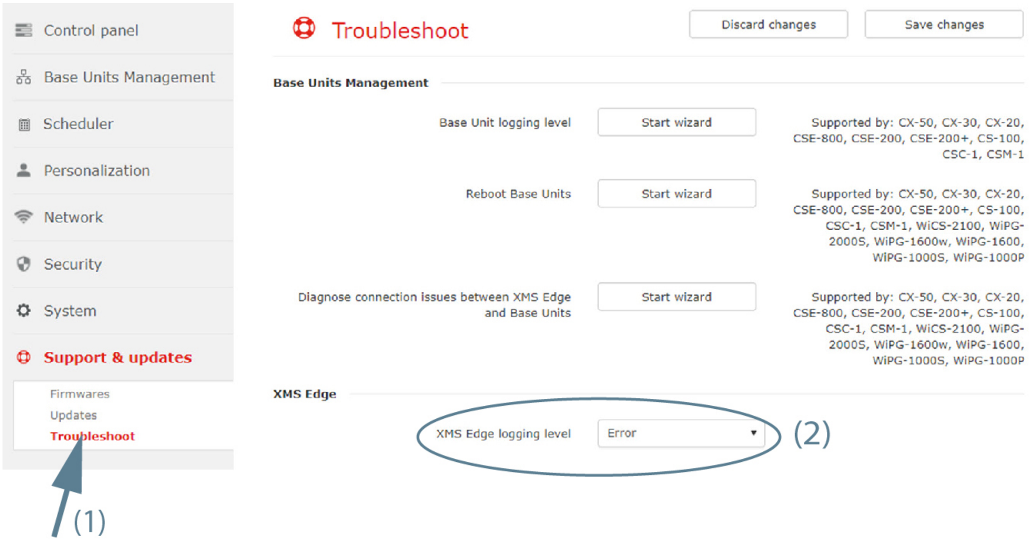
Image 3–93 Troubleshoot, diagnose connection issues

2. Click **Start wizard** next to *Diagnose connection issues between XMS Edge 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).

3.7.3.4 XMS Edge logging level

How to set

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



Base Unit logging level — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Reboot Base Units — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

Diagnose connection issues between XMS Edge and Base Units — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

XMS Edge logging level: Error

Image 3–94 Troubleshoot, XMS Edge logging level

2. Next to *XMS Edge logging level*, click on the drop down and select according your choice (2).

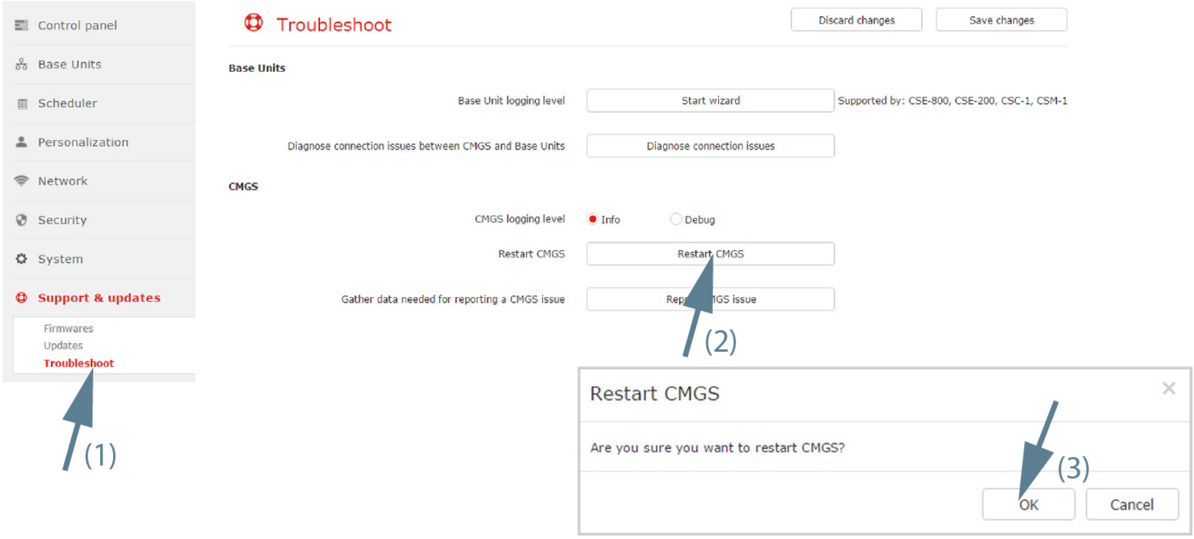
   The following choices are possible:

   - Debug
   - Info
   - Warning
   - Error

3.7.3.5 Restart CMGS

How to restart

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



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

Diagnose connection issues between CMGS and Base Units — Diagnose connection issues

CMGS logging level: ● Info ○ Debug

Restart CMGS — Restart CMGS

Gather data needed for reporting a CMGS issue — Report CMGS issue

Restart CMGS

Are you sure you want to restart CMGS?

Image 3–95

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

   A restart message is displayed.

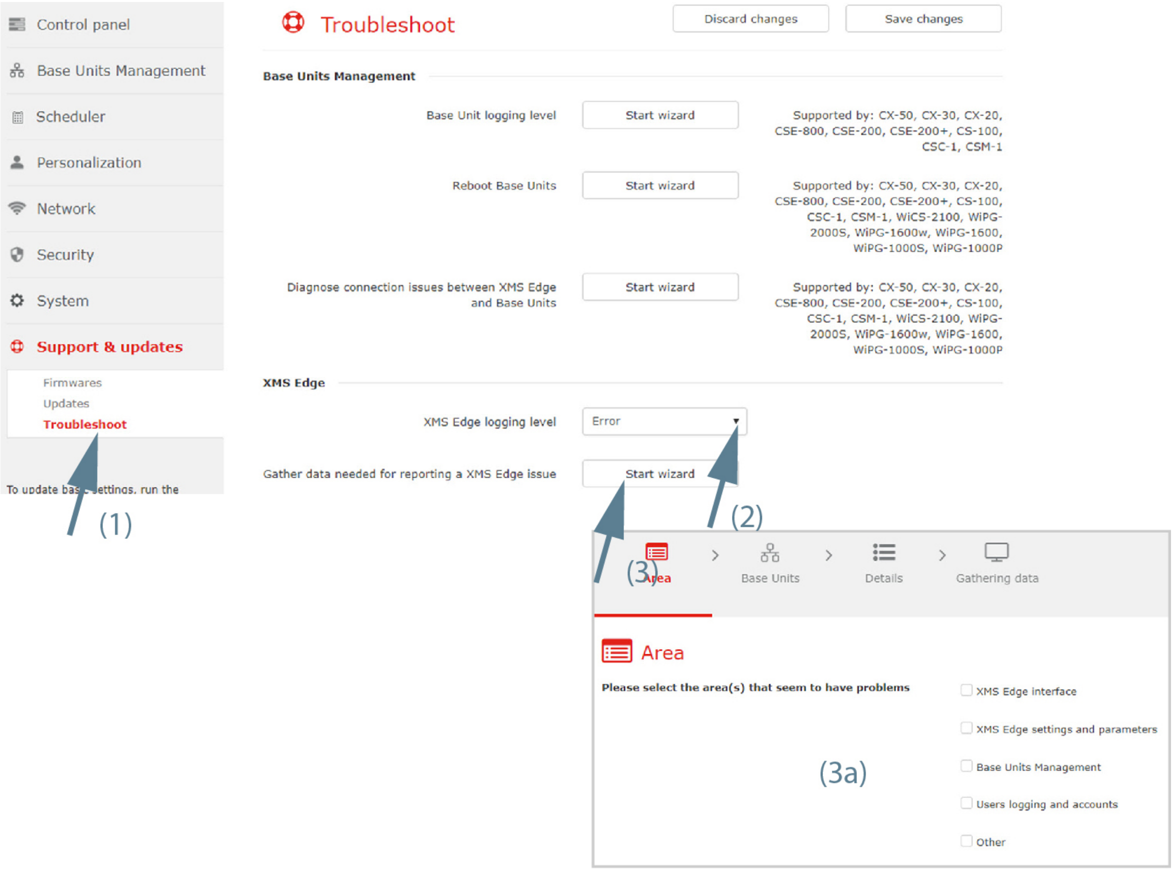
3. If you really want to restart, click **OK** (3).

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

3.7.3.6 Report XMS (virtual) Edge issues

How to report issues

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



Base Units Management

Base Unit logging level — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Reboot Base Units — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

Diagnose connection issues between XMS Edge and Base Units — Start wizard — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

XMS Edge

XMS Edge logging level: Error

Gather data needed for reporting a XMS Edge issue — Start wizard

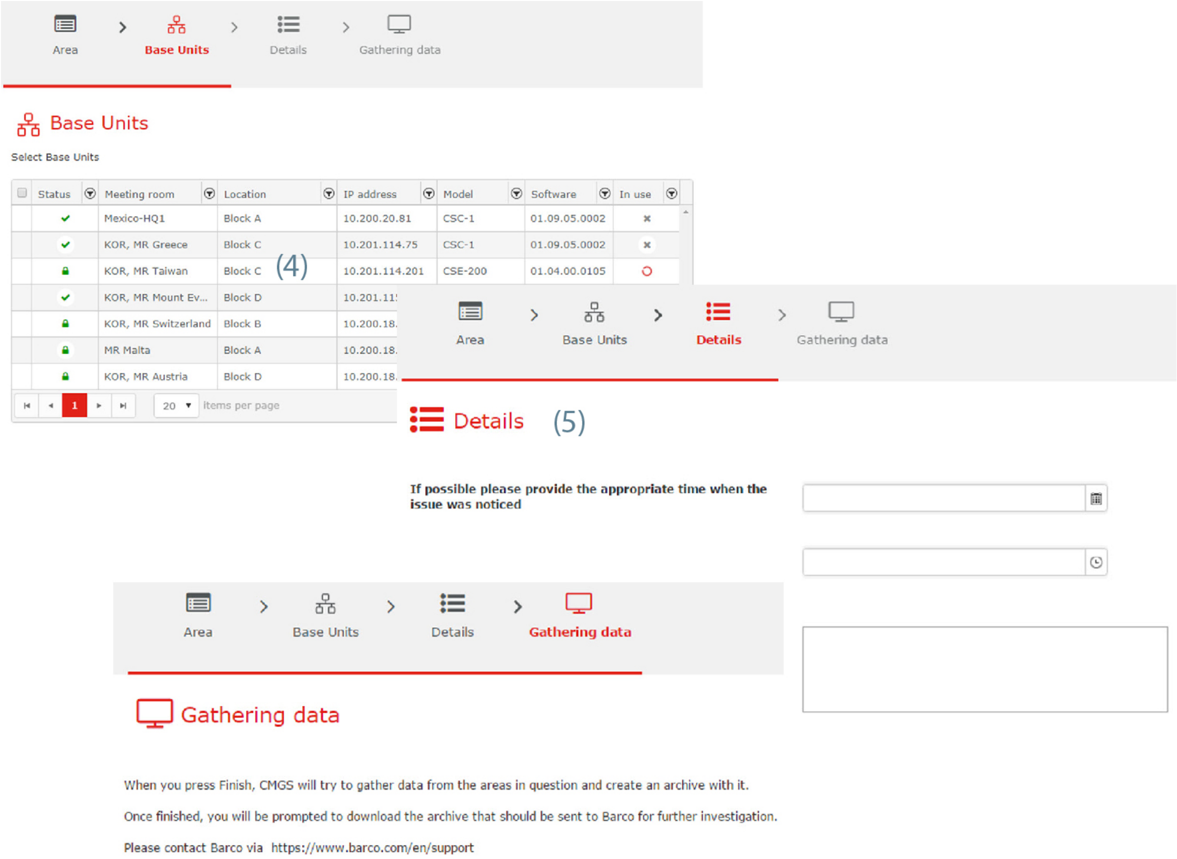
Area

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

- □ XMS Edge interface
- □ XMS Edge settings and parameters
- □ Base Units Management
- □ Users logging and accounts
- □ Other

Image 3–96 Report XMS issue

2. Next to *XMS Edge logging level*, click on the drop down and select according your choice (2).
3. Click **Report XMS Edge issue** next to *Gather data needed for reporting a XMS issue* (3).
4. Select the Area that seems to have problems (3a).
5. Select the Base Unit(s) where you discovered an issue (4).



Base Units

Select Base Units

□	Status	Meeting room	Location	IP address	Model	Software	In use
	✓	Mexico-HQ1	Block A	10.200.20.81	CSC-1	01.09.05.0002	✖
	✓	KOR, MR Greece	Block C	10.201.114.75	CSC-1	01.09.05.0002	✖
	🔒	KOR, MR Taiwan	Block C	10.201.114.201	CSE-200	01.04.00.0105	○
	✓	KOR, MR Mount Ev...	Block D	10.201.11			
	🔒	KOR, MR Switzerland	Block B	10.200.18.			
	🔒	MR Malta	Block A	10.200.18.			
	🔒	KOR, MR Austria	Block D	10.200.18.			

1 — 20 items per page

Details

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

Gathering data

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

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

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

Image 3–97 Report XMS issue

6. 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
7. Click Next to gather the data.

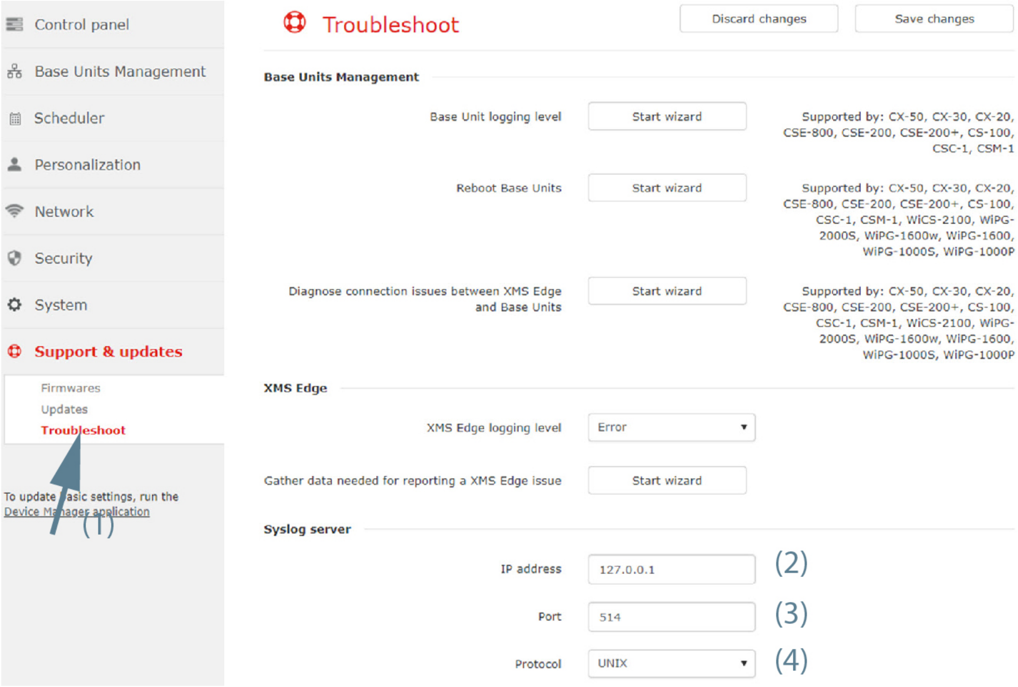
   An archive will be created and should be downloaded to be sent to Barco for further investigation.

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

3.7.3.7 Syslog server

How to setup

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



Base Units Management

Base Unit logging level — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1

Reboot Base Units — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

Diagnose connection issues between XMS Edge and Base Units — Supported by: CX-50, CX-30, CX-20, CSE-800, CSE-200, CSE-200+, CS-100, CSC-1, CSM-1, WiCS-2100, WiPG-2000S, WiPG-1600w, WiPG-1600, WiPG-1000S, WiPG-1000P

XMS Edge

XMS Edge logging level: Error

Gather data needed for reporting a XMS Edge issue

Syslog server

IP address: 127.0.0.1

Port: 514

Protocol: UNIX

To update basic settings, run the Device Manager application

Image 3–98

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

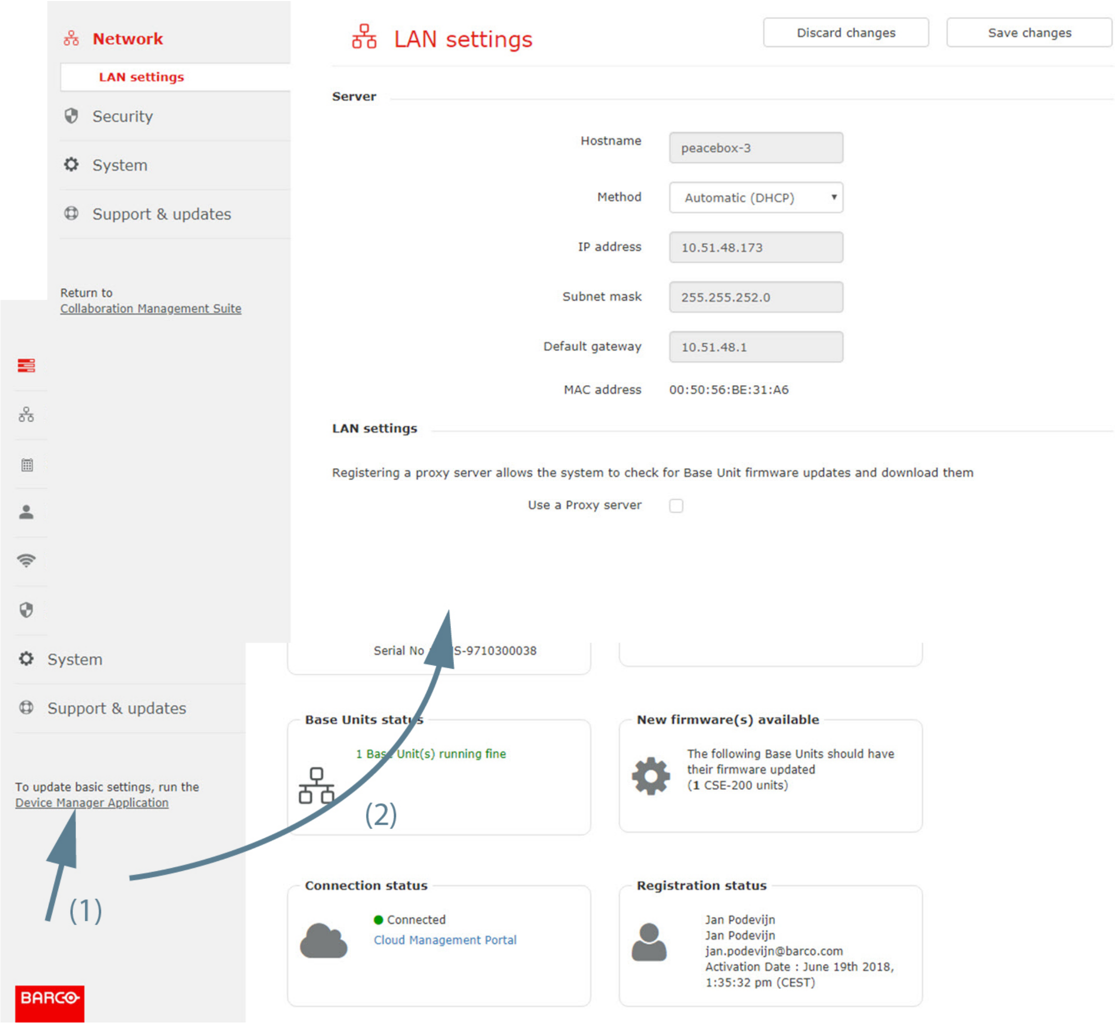
3.8 Starting the Device Manager application

About the device manager

The settings set during the first start up of the XMS (virtual) Edge 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.



LAN settings

Server

Hostname: peacebox-3

Method: Automatic (DHCP)

IP address: 10.51.48.173

Subnet mask: 255.255.252.0

Default gateway: 10.51.48.1

MAC address: 00:50:56:BE:31:A6

LAN settings

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

Use a Proxy server □

Return to Collaboration Management Suite

Serial No S-9710300038

Base Units status

1 Base Unit(s) running fine

New firmware(s) available

The following Base Units should have their firmware updated (1 CSE-200 units)

Connection status

● Connected

Cloud Management Portal

Registration status

Jan Podevijn
Jan Podevijn
jan.podevijn@barco.com
Activation Date : June 19th 2018, 1:35:32 pm (CEST)

To update basic settings, run the Device Manager Application

Image 3–99 Start up Device Manager

Software requirements & services

4

4.1 Network requirements

Ports used by ClickShare XMS (virtual) Edge

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 XMS 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
- port 4003TCP 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 XMS (virtual) Edge (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 XMS 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
- port 4003 TCP inbound

4.2 Services used by ClickShare XMS (virtual) Edge

Overview

- *Xms.cloud.barco.com* and sil-xms-prd01-iothub.azure-devices.net to connect your XMS (virtual) Edge to our XMS Cloud platform, allowing you to remotely monitor and manage different Base Units across different locations.
- *http://update.barco.com/ClickShare/releases.json* to retrieve the list of available firmware versions for the different ClickShare Base Units.
- barcoprdwebsitefs.azureedge.net & barco.com to retrieve the required firmware versions when updating the ClickShare Base Unit using XMS (virtual) Edge.

EULA and Open Source provisions A

A.1 End User Licence Agreement

Barco XMS (Virtual) Edge Product Specific End User License Agreement[6]

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. Metrics

XMS (Virtual) Edge is software to monitor and manage ClickShare and wePresent devices of Barco ("Software"). The Software is available in two models:

- XMS Edge appliance shall be invoiced and paid as per applicable prices and applicable purchase order acknowledged by Barco; or
- XMS Virtual Edge is offered as a free of charge virtual machine .OVA file.

The Software is available as a perpetual license.

A license is not bound to a single individual user, but grants usage rights to all users designated to operate the Software.

2. Enabling hardware

The Software must be used in combination with an on-premise XMS Edge instance (virtual machine or appliance).

3. Support

The provision of updates, upgrades and helpdesk support are included in the license for the applicable support period and the service levels purchased under the applicable license.

Barco will provide support for the last updates on the two (2) last minor upgrade branches of a major upgrade release version of the Software.

If a new major upgrade version of the Software is released by Barco, then Barco may send an End-Of-Life notification for the previous major upgrade version of the Software. This End-Of-Life notification will specify the end of the support period for the previous major upgrade release version.

Software patches are solely provided as part of a new release, and you shall upgrade your use of the Software to the latest release made available by Barco to implement any such patches.

As used above,

- **"Minor Upgrade"** shall mean all functional and/or feature enhancements that are incorporated and released at the discretion of Barco from time to time, to improve and/or otherwise enhance the product(s) functionality. Barco defines the Minor Upgrades for a specified software version as being those releases with the same software version number in the first position and a minor upgrade number increase as follows from x.y.z to x.y+1.z)
- **"Major Upgrade"** shall mean a significant change in the software functionality and/or architecture deemed by Barco to be so. Installation and use of Major Upgrades may require modification of existing projects and templates; such modifications are not included under this document. The release notes will explain the upgrade path; the services to implement Major Upgrade modifications including making required modifications to existing software, templates and integration and testing, are not covered by this document. Barco defines the Major Upgrades for a specified software version as follows e.g., major upgrade number increase from x.y.z to x+1.y.z).

4. 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.

[6] 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.

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 (i) cause you to procure such additional licenses required as per the actual usage and (ii) 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.

5. Privacy

You are the controller (as defined under applicable data protection law) for personal data which are being processed via the Software. Therefore, you remain responsible for complying with applicable data protection law and for implementing and maintaining privacy protection and security measures (especially for components that a system integrator provides or controls).

Your data (including the data of individuals you permit to use the Service) are treated in accordance with the Agreement. Any personal data are treated in accordance with the Exhibit DPA, attached hereto and accepted as part of this EULA, and the Product Privacy Policy is accessible on https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement.

Via the Software, Barco may gather (i) technical information about the functioning and the functionality of the products which are connected through the Software, and/or (ii) information 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 in accordance with Barco’s product privacy statement accessible on https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement.

6. Other Terms

- **Open Source components**
  The Software contains software components released under an Open Source license.
  A list of the third party software components used (open source and other) is available on the Barco website (www.barco.com/opensourcesoftware/xms/).The applicable license terms, copyright notices and, as relevant, source code access apply as set out in the Barco EULA attached hereto.
- **Safe and proper use of Devices**
  You remain solely responsible to operate any device which is controlled, monitored or analyzed by the Software in accordance with the operating instructions and safety guidelines as intended and/or recommended. Barco disclaims any liability resulting from an improper use of a device, even if such device is being controlled, monitored or analyzed by the Software.

BARCO END USER LICENSE AGREEMENT[6]

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 Barco proprietary software which is being licensed hereunder, released in object code only.

“Term” means the period set out in article 9.1 hereof.

“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 user license (without the right to grant sublicenses). Save for the Product Specific EULA or any broader license terms confirmed through the DRM tool, (i) the license under this License Agreement applies to one (1) copy of the Software to be used on one single computing device and (ii) installation on a computing device that may be concurrently accessed by more than one user shall not constitute a permitted use and a separate license is required for each active user connected to a computing device on which the Software is being used

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 article2.1 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) 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 (which consent shall be reasonably given, but may come with a fee).

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, reduce the number of devices or users that directly access or use the Software, or reduce the number of devices or users the Software directly manages (sometimes referred to as “multiplexing” or “pooling”) or otherwise attempt to reduce the number of licenses of any type that you need.

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, 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 program 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 specific 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 *'Copyright'*. 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 the respective copyrights.

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

3.6 *'Trade Secrets'*. You agree not to disclose, provide or otherwise make available 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 reasonable security measures to protect such trade secrets.

4. Support

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

4.2 *'Support policy'*. Barco may provide to you maintenance releases to address bugs or security issues in the Software and you agree to install the same. Any other updates or upgrades can be obtained under the terms of a separate software maintenance which is being offered to you. You may have a right to downgrade your licensed Software application to (only) such earlier version of the same Software application as agreed by Barco in the forthcoming case.

Additional functionality may be licensed to you with and subject to additional or different terms.

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 Software deployments and to examine your books, records and accounts during your normal business hours so as to verify your compliance with the License Agreement. In the event such audit discloses 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 *'Enforcement'*. Barco shall notify the then known user through the DRM (failing of which, otherwise in writing) of a substantial non-compliance, based on the triggers as per the Product Specific EULA. The non-compliance may result in an immediate or graduate denial of service (i. e. termination of the rights granted under the License Agreement), in part or in full, all based on the level of severity of the non-compliance [as per the Product Specific EULA].

6.3 *'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 AN AMOUNT OF 250 EURO IN THE AGREGATE (OR TO THE MAXIMUM EXTENT PERMITTED BY LAW WHERE NO FURTHER EXCLUSION IS LEGALLY ALLOWED).

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

8. Confidentiality

8.1 *'Confidential Information'*. You will be receiving information which is proprietary and confidential to Barco during the negotiation 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 the negotiations leading to 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 returning all Documentation and associated materials, 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 contract is terminated or expires. Cancelling your license will stop recurring fees going forward, but will not retroactively refund current or past payments.

10. Other relevant terms

10.1 *‘Data Protection’*. Barco may, without restriction, save, process, use and reuse any data obtained in connection with the sales or supply of the Services. Barco shall take suitable technical and organizational measures to protect personal data received against loss and unlawful processing.

10.2 *‘Functional Information’*. Via the Software, Barco may gather technical, aggregated and/or statistical 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 and its service providers may process and use such Functional Information for analytics purposes, for developing and improving products and services, offering products and services to Your organization, all based on the legitimate interest of Barco of evaluating the market, assessing and improving its products and conducting research and development. This Section shall survive the term of this Agreement.

10.3 **Return of Data**. Upon Your request made within 60 days after the termination or expiration of this Agreement, Barco will make User Data available to You for export or download as provided in the Documentation. After such 60-day period, Barco shall have no obligation to maintain or provide any User Data, and as provided in the Documentation will thereafter delete or destroy all copies of User Data in Barco’s systems or otherwise in Barco’s possession or control, unless legally prohibited.

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 to the parties’ last known address.

11.3 *‘Severability’*. This License Agreement shall not be altered, amended or varied. 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 Jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software, including the U. S. Export Administration Regulations, as well as end-user, end-use, and destination restrictions issued by the U.S. or other governments.

11.5 *‘Survival’*. The provisions of articles 3, 5, 6, 7 and 8 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’*. Barco shall be entitled to sub-contract all or any of Barco's obligations hereunder to a third party and/or any of Barco's 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, 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

Exhibit DPA — Data Processing Agreement

This Data Processing Agreement (“**Exhibit DPA**”) is an integral part of this End User License Agreement (the “**EULA**”) and applies to the extent your data includes personal data within the meaning of the GDPR.

WHEREAS under the Agreement, you procure identified software provided by Barco (which is referred to herein as the ”**Connected Services**”);

WHEREAS in rendering the Connected Services, Barco (acting as Data Processor) may from time to time be provided with, or have access to information of you (acting as Data Controller) and the individuals you permit to use the Connected Services, and this information may qualify as personal data within the meaning of the GDPR;

WHEREAS you (acting as Data Controller) engages Barco as a commissioned processor acting on your behalf as stipulated in art. 28 GDPR;

WHEREAS European data protection laws require data controllers in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries and such protection can be achieved by requiring processors to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (“**EC Standard Contractual Clauses**”) pursuant to Commission Decision 2010/87/EU of 5 February 2010 as set out in annex 3 1;

WHEREAS this DPA contains the terms and conditions applicable to the processing of such personal data by Data Processor as a commissioned data processor of Data Controller with the aim to ensure that the Parties comply with the Applicable Data Protection Laws.

1. **Definitions**

For the purpose of this DPA, the terminology and definitions as used in the GDPR shall apply. In addition to that,

“Affiliate” means any of Affiliate (s) of End User which (a) is subject to the data protection laws and regulations of the European Union, the EEA, the United Kingdom and Switzerland, and (b) is permitted to use the Connected Services.

“Applicable Data Processor law” means the Data Protection Laws that are applicable to Barco as the Data Processor.

“Applicable Data Protection Law” means the Data Protection Laws applicable to the Data Controller.

“Barco” means Barco NV, with registered office at President Kennedypark 35, 8500 Kortrijk Belgium and its subsidiaries.

“Customer” is defined in the Agreement.

“Data Controller” means, for the construction of this Exhibit, End User.

“Data Importer” means the Data Processor or Sub-Processor that is located in a Third Country.

“Data Exporter” means the Data Controller if (a) (i) the Data Controller is located in the EEA or (ii) is located outside of the EEA and is subject to GDPR, and (b) Data Controller transfers personal data to a Data Importer.

“Data Protection Law” means the GDPR and the laws and regulations containing rules for the protection of Data Subjects with regard to the Processing, including without limitation security requirements for and the free movement of Personal Data, implementing or completing the GDPR.

“EEA” means all member states of the European Union (excluding the United Kingdom), Norway, Iceland, Liechtenstein and, for the purposes of this DPA, the United Kingdom and Switzerland.

“Employee” means any employee, agent, contractor, work-for-hire or any other person working under the direct authority of Barco. However, “Employees” do not include “Sub-Processors”.

“End User” is defined in the Agreement, and shall mean a reference to you.

“End User Data” means Personal Data for which End User is the Data Controller under Applicable Data Protection law, which are being shared with Barco in the provision of the Connected Services.

“GDPR” means regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Non-Adequate Country” means a country that is deemed not to provide an adequate level of protection of Personal Data within the meaning of the articles 44-45 GDPR.

“Sub-Processor” means any Processor engaged by Barco that Processes End User Data.

“Third Party” means any party other than Barco, Sub-Processor, Customer or End User.

2. Instructions

2.1 To the extent Barco Processes End User Data necessary for the provision of the Connected Services it shall act as a Data Processor on behalf of End User, being the Data Controller.

2.2 Customer is obliged to ensure, and to make any due arrangements with End User, that any instruction given to Barco is in compliance with Applicable Data Protection Law and is endorsed by End User.

2.3 In the provision of the Connected Services, Barco shall Process the End User Data only on documented instructions from Data Controller (that is, End User or instructions given by Customer acting on behalf of End User), unless Barco is required to Process End User Data by Union or by a Member State law to which Barco is subject; in such case, Barco shall inform the End User of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

2.4 The Agreement and this DPA are Data Controller's complete and final Instructions to Barco with regard to the Processing.

2.5 Annex I to this DPA sets out certain information regarding the Processing of the End User Data as required by article 28 of the GDPR (and possibly, equivalent requirements of other Data Protection Laws).

2.6 If Barco thinks that an instruction of Data Controller infringes the Applicable Data Processor Law, Barco shall point this out to Data Controller without undue delay.

2.7 Any further instructions that go beyond the instructions contained in this DPA or the Agreement must be within the subject matter of this DPA and the Agreement. If the implementation of such further instructions results in costs for Barco, Barco shall inform Data Controller about such costs with an explanation of the costs before implementing the instruction. Data Controller shall give further instructions generally in writing, unless the urgency or other specific circumstances require another form. Instructions in another form shall be confirmed in writing by Data Controller without undue delay.

3. Applicable law

3.1 When performing this DPA, Data Controller shall comply with the Applicable Data Protection Law and Barco shall comply with the Applicable Data Processor Law.

3.2 Each party shall deal with reasonable requests for assistance of the other party (including of End User) to ensure that the Processing complies with Applicable Data Protection Law.

4. Obligations of Data Controller

4.1 Data Controller Personal Data are lawfully obtained from Data Subject and are lawfully provided to Barco under the Applicable Data Protection Law;

- it provides Barco with Personal Data that are up-to-date and relevant for the Processing activities;
- it has provided Data Subject all necessary and relevant information with regard to the Processing of the Personal Data as required under the Applicable Data Protection Law; and
- the End User Data does not infringe any third-party rights.

4.2 Data Controller, agrees that it remains the contact point for Data Subject and that it will inform Data Subject about this. Should a Data Subject contact Barco with regard to correction or deletion of its Personal Data, Barco will use commercially reasonable efforts to forward such requests to End User.

5. Obligations of Barco

5.1 Security. Barco shall implement appropriate technical, physical and organisational security measures as specified in Annex II taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons to ensure a level of security appropriate to the risk and to protect End User Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other forms of unlawful Processing including, but not limited to, unnecessary collection or further Processing.

5.2 Non-disclosure and confidentiality. Barco shall keep End User Data confidential and shall not disclose End User Data in any way to any Employee or Third Party without the prior approval of Data Controller, except where, (i) subject to this Section, the Disclosure is required for the performance of the Processing, or (ii) subject to Section 8.1 ii), where End User Data need to be disclosed to a competent public authority to comply with a legal obligation or as required for audit purposes. Barco shall provide the Employees access to End User Data only to the extent necessary to perform the Processing. Barco shall ensure that any Employee it authorises to have access to End User Data Processed on behalf of End User has committed himself to confidentiality or is under an appropriate statutory obligation of confidentiality.

6. Sub-Processors

6.1 Customer shall cause Data Controller to agree that Barco may use Sub-Processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services or hosting services. The Sub-Processors that are currently engaged by Barco to carry out Processing activities on End User Data on behalf of End User are mentioned in Barco's product privacy statement on *www.barco.com*.

6.2 Barco shall inform the Data Controller of any intended changes concerning the addition or replacement of Sub-Processors via Barco's usual email notification process. Data Controller shall not unreasonably object to such changes.

6.3 Where Barco subcontracts (part of) the Processing of End User Data on behalf of End User, it shall do so only by way of a written agreement with the Sub-Processor which imposes the same or essentially the same data protection obligations on the Sub-Processor as are imposed on Barco under this DPA and which shall restrict the Sub-Processor to use the End User Data for any other purpose than the provision of the Connected Services. Barco remains liable for the Sub-Processor's breach of its data protection obligations under such written agreement.

7. Audit and compliance

7.1 Barco shall, upon reasonable notice (no less than two (2) months) and not more than once every two years (unless there is a Personal Data Breach), allow its procedure and documentation to be inspected or audited by Data Controller (or the auditor of its choice, excluding any Barco competitor) during business hours in order to ascertain compliance with the obligations set forth in this DPA, in which case Barco shall make the processing systems, facilities and supporting documentation relevant to the Processing of End User Data available for an audit by End User. For the avoidance of doubt, the scope of such audit shall be limited to documents and records allowing the verification of Barco's compliance with the obligations set forth in this DPA and shall not include financial documents or records of Barco or any documents or records concerning other customers of Barco.

8. Notifications of Disclosures and Personal Data Breaches

8.1 Barco shall use reasonable efforts to inform Data Controller as soon as reasonably possible if:

- it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing, except where Barco is otherwise prohibited by law from making such disclosure;
- it intends to disclose Personal Data to any competent public authority; or
- it becomes aware of a Personal Data Breach.

8.2 In the event of a Personal Data Breach, Barco shall take reasonable remedial measures to preserve the confidentiality of the End User Data. Furthermore, Barco shall provide Data Controller the information reasonably requested by End User regarding the Personal Data Breach. This information will at least contain the following elements:

- a description of the nature of the Personal Data Breach, including the number and categories of Data Subject and personal data records affected;
- a description of the likely consequences of the Personal Data Breach; and
- a description how Barco proposes to address the Personal Data Breach, including any mitigation efforts.

8.3 Customer shall cause Data Controller to agree that an Unsuccessful Security Incident will not be subject to this Section 8. An “Unsuccessful Security Incident” is one that results in unauthorised access to End User Data or to any of Barco’s or Sub-Processor’s equipment or facilities storing End User Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents that did not result in an actual destruction, loss, alteration or unauthorised disclosure of Personal Data.

8.4. Barco’s obligation to report or respond to a Personal Data Breach under this Section 8 is not and will not be construed as an acknowledgement by Barco of any fault or liability of Barco with respect to the alleged Personal Data Breach.

9. Cooperation and assistance duty

9.1 Barco will assist Data Controller in the fulfilment of its obligation to respond to requests from Data Subjects, provided that (i) Data Controller has instructed Barco to do so by way of a written instruction and (ii) Data Controller reimburses Barco for the costs arising from this assistance.

9.2 Barco shall promptly inform Data Controller of any complaints, requests or enquiries received from a Data Subject, including but not limited to requests to rectify or erase End User Data or to object to the Processing of End User Data. Barco shall not respond directly to any complaints, requests or enquiries received from Data Subject without Data Controller’s prior written instruction, except where required by law.

9.3 Upon written request of Data Controller, Barco shall make available to the End User all information necessary to demonstrate compliance with the Applicable Data Protection Law.

9.4 Upon written request of Data Controller, Barco shall, taking into account the nature of the Processing and the information at its disposal, assist Data Controller in ensuring compliance with the obligations regarding security of the Processing, notification of Personal Data Breaches and mandatory data protection impact assessments (articles 32-36 GDPR).

9.5 Barco shall cooperate with the supervisory authorities in the performance of their duties.

10. Return and destruction of Personal Data

Upon termination of the provision of the Connected Services, Barco shall – at a reasonable fee - , at the option of Data Controller expressed in writing, return and/or delete the End User Data and copies thereof to End User, except to the extent applicable law provides otherwise. In that case, Barco shall no longer Process the End User Data, except to the extent required by applicable law.

11. Affiliates

11.1 The parties acknowledge and agree that, by providing the Connected Services, the Customer enters into the DPA on behalf of End User and, as applicable, in the name and on behalf of its or their Affiliates. Customer procures that End User and each Affiliate agree to be bound by the obligations under this DPA. All access to and use of the Connected Services by Affiliates must comply with the terms and conditions of the DPA and any violation of the terms and conditions of this DPA by an Affiliate shall be deemed a violation by End User.

11.2 Customer shall remain responsible for coordinating all communication with Barco under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of End User and any relevant Affiliates.

12. Liability

12.1 Barco indemnifies Customer and holds Customer harmless against all claims, losses or damages incurred by the End User and arising directly out of a breach by Barco of this DPA and/or the Applicable Data Processing Law provisions directed to Barco, unless Barco proves that it is not responsible for the event giving rise to the liability.

12.2 Customer indemnifies Barco and holds Barco harmless against all claims, losses or damages incurred by Barco and arising directly out of a breach of this DPA and/or the Applicable Data Protection Law by Customer or End User.

12.3 Each party’s liability will be limited to foreseeable, direct and personal damage suffered, excluding indirect, incidental, special or consequential damage and regulatory fines, even if advised of the possibility thereof. Indirect Damage shall mean damage or loss that do not directly and immediately result from an event giving rise to the liability, including but not limited to loss of earnings, business interruption, increase of personnel cost, failure to realize anticipated savings or benefits.

12.4 In any event and to the extent permitted by law, Barco's aggregated maximum liability under this DPA will be limited to the amounts received for the provision of the Connected Services in the twelve months preceding the incident giving rise to liability.

13. Data transfer

13.1 Barco shall not transfer End User Data to any Non-Adequate Country outside the EEA or make any End User Data accessible from any such Non-Adequate Country without adequate protection.

13.2 Any transfer of Personal Data to a Non-Adequate Country shall be governed by the terms of the EC Standard Contractual Clauses (annex III) or other model clauses that have been approved by the EU commission or another competent public authority in accordance with the Applicable Data Processing Law. Barco shall conclude these clauses on behalf of End User. The Appendices of these clauses will contain the same or essentially the same information as this DPA. Barco and End User shall work together to apply for and obtain any permit, authorization or consent that may be required under Applicable Data Processing Law in respect of the implementation of this Section.

14. Termination of the DPA

This DPA shall continue in force until the termination or expiration of the Agreement (the "Termination Date").

15. Entire Agreement

The following Annexes are attached hereto and made a part hereof:

- Annex I: Details of processing
- Annex II: Technical and organizational measures
- Annex III: EC Standard Contractual Clauses

Annex I — Details of Processing

This Annex 1 includes certain details of the Processing of End User Data as required by Article 28(3) GDPR. More specific details per Barco product are included in the product specific sections of Barco's product privacy statement.

Subject matter and duration of the Processing of End User Data

The subject matter of the Processing of the End User Data is set out in Barco's product privacy statement on *www.barco.com* and this DPA.

End User Data will be Processed for the duration of the provision of Connected Services for the benefit of the End User.

End User Data can be Processed outside the EEA by Barco Affiliates and/or Sub-Processors as indicated in Barco's Product Privacy Statement.

The nature and purpose of the Processing of End User Data

Barco is managing the hosting environment on behalf of the Data Controller to enable the provision of the Connected Services

The types of End User Data to be Processed is set out in Barco's product privacy statement

(*https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement*)

The categories of Data Subjects to whom the End User Data relates

- End User's employees (including End User's agents, advisors, freelancers and consultants) and End User's representatives (who are natural persons)
- Customers of the End User, its employees and representatives
- Customers of the End User's customers, its employees and representatives
- Users of the Barco Product authorized by the End User to use the products

Annex II — Technical and organisational measures

1. The pseudonymisation and encryption of personal data; (art. 32, par. 1, lit. a, GDPR)

based on a risk assessment (and if required an additional DPIA) Barco will ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. Pseudonymization
2. Encryption, conform Cryptographic Controls policy

2. Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (art. 32, par. 1, lit. b, GDPR)

1. Barco is verified under ISO/IEC 27001:2013 covering the business processes, infrastructure and tools related to software development, sales, deployment, and support of our ClickShare wireless collaboration product line in our Kortrijk, Noida and Taipei locations. https://www.barco.com/en/about-barco/legal/certificates
2. Security and privacy by design
3. Compliance with the security policies in place at Barco, covering
   a) Information Security Top Policy
   b) Code of Digital Conduct
   c) Acceptable Use
   d) Logical Access Control
   e) Third Party Security
   f) Backup and Recovery
   g) Password
   h) Info Sec Incident Management
   i) Anti Malware
   j) Network Protection
   k) Cryptographic Controls
   l) IT Operations
   m) Cloud Security
   n) Secure SDLC
   o) Disposal and Destruction
   p) Physical Environmental Security
   q) Secure Remote Support Policy

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (art. 32, par. 1, lit. c, GDPR)

Compliance with the security policies in place at Barco, covering

1. Backup and Recovery
2. IT Operations

4. Process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing (art. 32, par. 1, lit. d, GDPR)

1. Product Security Incident Response teams (psirt): https://www.barco.com/psirt
2. Barco Security Organization operates in three lines of defense, covering operations, governance and internal audit.
3. Regular evaluations by independent third parties (e.g. penetration testing, audit, …)
4. Integration of automated security scanning tools during the development process (Secure SDLC) and operations

Annex III — EC Standard Contractual Clauses

For the purposes of Article 26 (2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The entity identified as the “Data Controller” in the DPA (the “data exporter”) and the entity identified as the “Data Processor” in the DPA (the “data importer”).

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data

Clause 1
Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex I which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex II to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex II, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex II before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

1. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
2. any accidental or unauthorised access, and
3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex II which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Belgium

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1
to the Standard Contractual Clauses

Data exporter

The data exporter is using Connected Services of data importer as specified in the Agreement

Data importer

The data importer is rendering the Connected Services as specified in the Agreement

Data subjects

The personal data transferred concern the following categories of data subjects.

- Data exporter's employees (including data exporter's agents, advisors, freelancers and consultants) and Data exporter's representatives (who are natural persons)
- Customers of data exporter, its employees and representatives
- Customers of data exporter's customers, its employees and representatives
- Users of the Barco product authorized by the data exporter to use the products

Categories of data

The personal data transferred are specified in Barco's product privacy statement (*https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement*)

Special categories of data (if appropriate)

Data importer may, subject to the restriction set out in the Agreement, submit special catergories of Personal Data to the Connected Services, the extent of which is determined and controlled by data exporter in its sole discretion.

Processing operations

The objective of Processing of Personal Data by data importer is the performance of the Connected Services pursuant to the Agreement.

Appendix 2
to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are described in Annex II Technical and organisational measures.

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 XMS (virtual) Edge 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