

ClickShare Management Suite

Installation manual

Barco NV

President Kennedypark 35, 8500 Kortrijk, Belgium

Phone: +32 56.36.82.11

Fax: +32 56.36.883.86

Support: www.barco.com/en/support

Visit us at the web: www.barco.com

Copyright ©

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

Trademarks

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

TABLE OF CONTENTS

1. Installation	3
1.1 Set up requirements.....	3
1.2 Installation steps.....	4
1.2.1 Server installation.....	4
1.2.2 Server configuration.....	12
1.3 Administrator functions.....	14

1. INSTALLATION

Overview

- Set up requirements
- Installation steps
- Administrator functions

1.1 Set up requirements

Overview

The ClickShare Management Suite is a downloadable ISO file. The ISO file can be loaded into a Virtual Machine or burned on a CD-R in order to install on a new PC (without operating system) or formatted PC. Both must have a 64-bit supported processor.

About the virtual machine

VMware player and Oracle VM Virtualbox are the supported Virtual Machines for the ISO file. While creating the virtual machine on your server, select **Linux Debian 64bit** as operating system for your virtual machine. Refer to the Virtual Machine user manual for installation help.

System requirements

The minimum requirements for the computer are:

- AMD64 or Intel 64 processor (amd64 processor architecture).
- 2GB RAM.
- 32GB free Hard disk space.
- The video memory must be equal or greater than 4 MB, only one monitor output is needed.
- One network interface is sufficient, no additional interfaces for load-balancing are necessary.

Network configuration requirements

To use the full functionality of the ClickShare Management Suite there must be communication via typical ports between the ClickShare Management Suite server and the Base Units.

The following ports are used:

By ClickShare Management Suite server

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

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

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

- port 80 TCP outbound
- port 8080 TCP outbound

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

- port 53 UDP outbound
- port 53 TCP outbound

NTP: used for time synchronization

- port 123 UDP outbound
- port 123 TCP outbound

Ports used by the Base Unit's REST API

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

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

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

By the Base Units

1. Installation

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

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

REST API

- port 4000 TCP inbound
- port 4001 TCP inbound

Starting the installation

For a virtual machine, select the iso file stored on the same computer.

For new or formatted PC, insert the created CD and start up the PC.

1.2 Installation steps

The complete installation contains 2 steps:

- Server installation
- Server configuration

1.2.1 Server installation



Server installation will typically be executed by IT department who will install the server on the corporate network.

Preparations

1. Download the latest version from www.barco.com/clickshare.

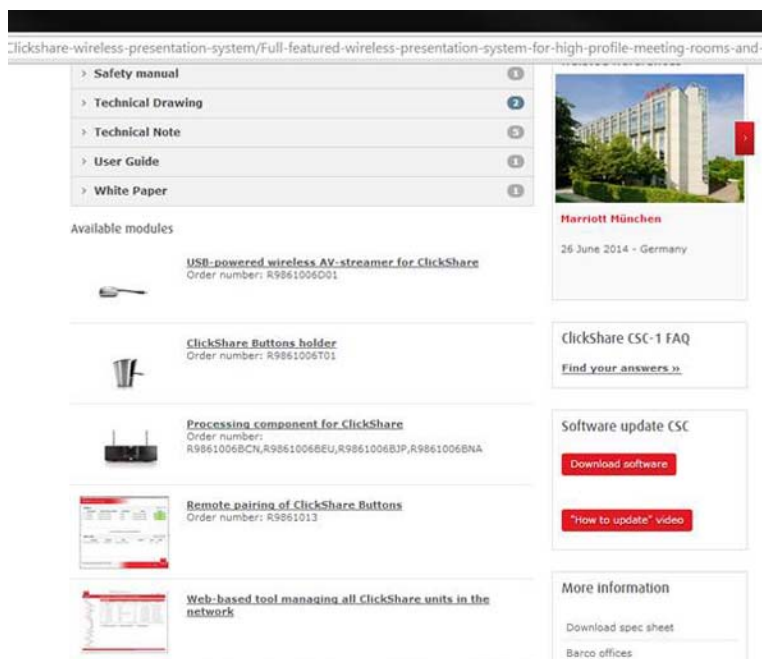


Image 1-1

2. Burn the downloaded ISO file on a CD-R or copy it to the Virtual Machine server to load it in the virtual machine.

The main installation menu window opens.

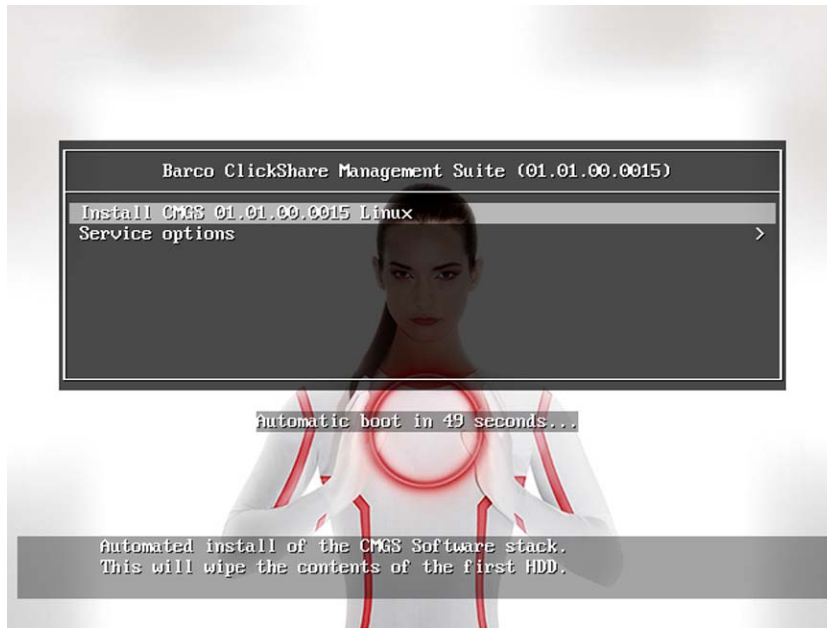


Image 1-2

3. Select *Install CMGS Linux* and press **ENTER**.

Note: *Service options* is for Barco purposes only. This part is password protected.



A mounted CD is automatically removed after installation from the Virtual Machine to avoid booting from CD upon reboot. It needs to be added each time one wants to initiate an update.

About the buttons on the installation windows

Screenshot – Screenshot button could be used to take the screenshot of the installation window. These screenshots can be downloaded with cmgs logs.

Go back – Go Back button takes the interface back to the debian installer main menu. User is advised to continue with default selected option in order to have head less installation.

Installation

1. Select your country.
Choose *Other* if not listed

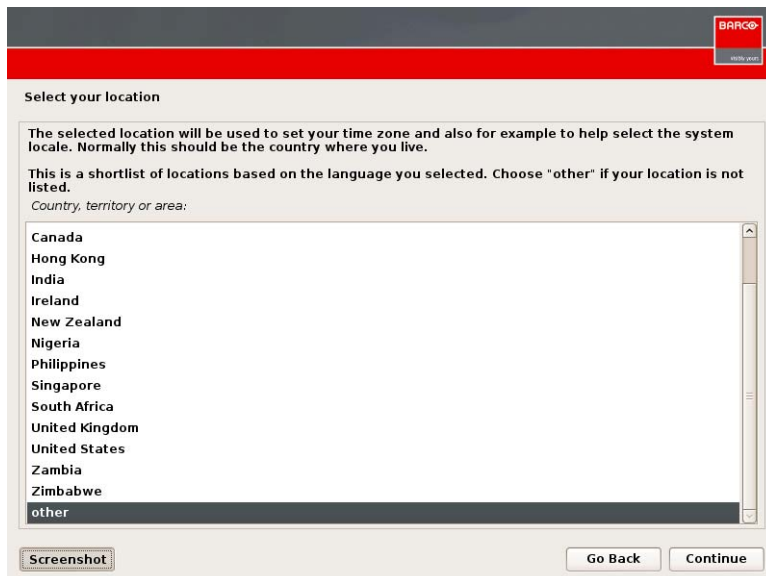


Image 1-3

2. If other is selected, select your *Region* and click **Continue**.

1. Installation

Then select your *Country* and click **Continue**.

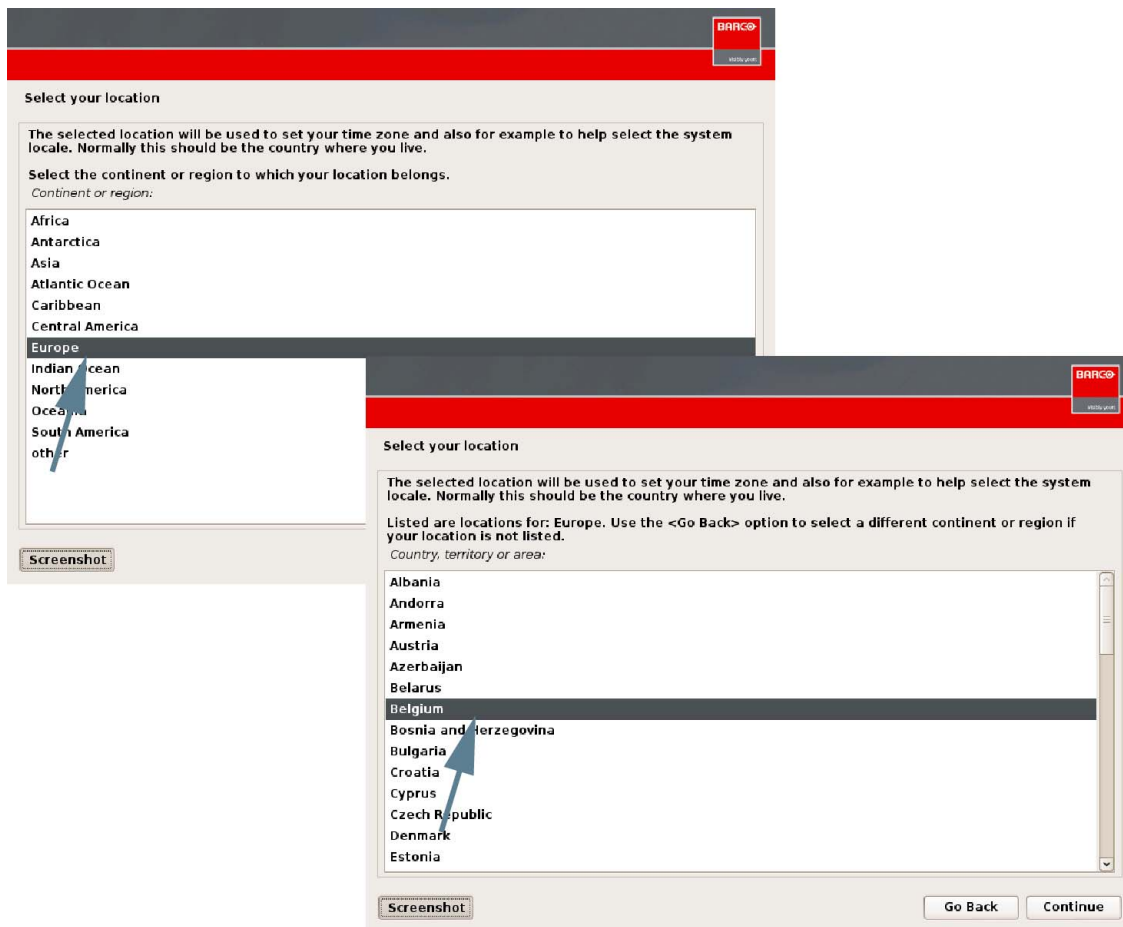


Image 1-4

3. Select your keyboard layout and click **Continue**.

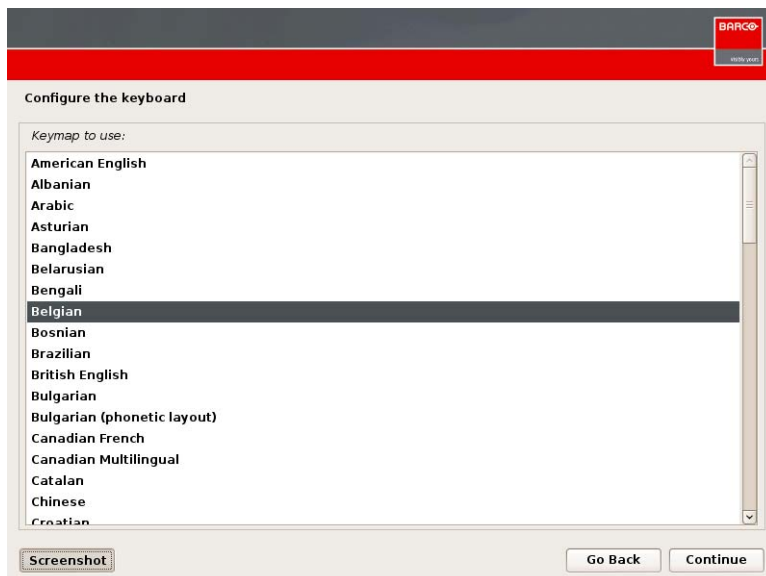


Image 1-5

4. Configure your network settings. Make the selection between automatic [Yes] or manual [No]. Select the corresponding radio button. Click **Continue**.



Image 1-6

5. If chosen for manual setup, enter the following addresses:

- IP address for your computer (unique address)
- the network mask
- the gateway
- the name server addresses

1. Installation

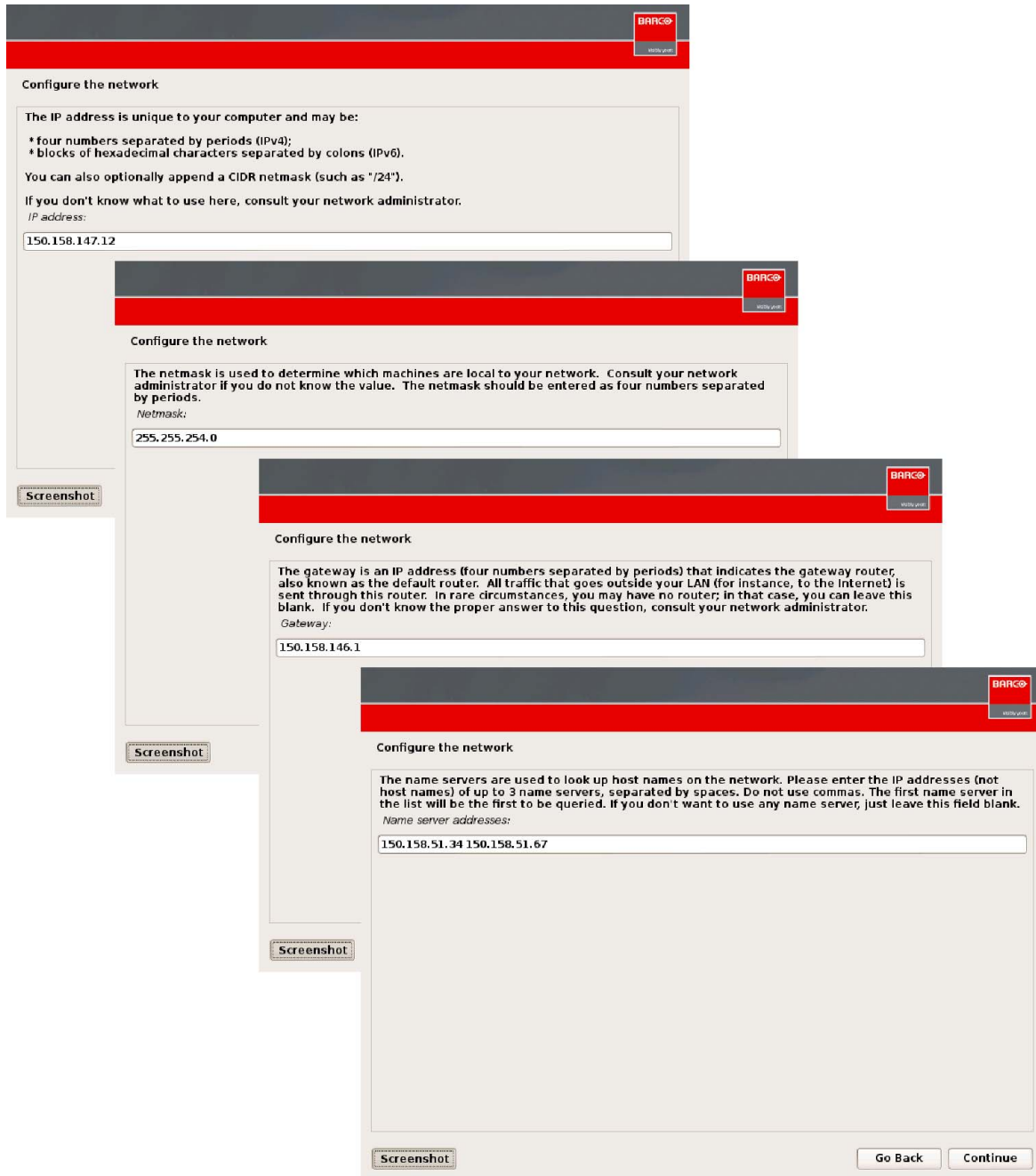


Image 1-7

6. Enter a hostname for the system.

Default hostname : cs-managementsuite

Note: A valid hostname may contain only the numbers 0-9, upper and lower case letters and the minus sign. It must be at most 63 characters long, and may not begin or end with a minus sign.

It is not allowed to use only numeric characters for the hostname.

Note: Contact your local IT administrator to create an entry in the name server to link the IP address with its hostname.



Image 1-8

7. Enter the domain name
Default domain name : barco.com



Image 1-9

8. Create an administrator password. First enter a password and then confirm that password by entering the password again.
The administrator password :
 - must be at least 8 characters in length
 - must contain at least one uppercase character
 - must contain at least one lowercase character
 - must contain at least one digit (0-9)
 - must contain at least one special characterClick **Continue**.

1. Installation



Set up users and passwords

The password must be at least 8 characters in length and is a mixture of uppercase alphabets, lowercase alphabets, digits, special characters and should be changed at regular intervals.
Choose a password for the new user:

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

Screenshot Go Back Continue

Image 1-10

9. During CMGS installation the admin user can synchronize the system clock with a network time server using the NTP protocol. This NTP server configuration will not be activated in the system after installation. Therefore, the admin user needs to explicitly configure it again using the administrator console in order to keep the system clock of the installed host continuously in sync with the configured NTP server. Configure the clock by entering a ntp server. If you do not have a ntp server within your company, you can use the pre-listed ntp server from Debian. Click **Continue**.



Configure the clock

The default NTP server is almost always a good choice, but if you prefer to use another NTP server, you can enter it here.
NTP server to use:

Screenshot Continue

Image 1-11

10. Select your time zone and click **Continue**.



Image 1-12

The installation will be finalized. The system reboots and shows the startup screen.

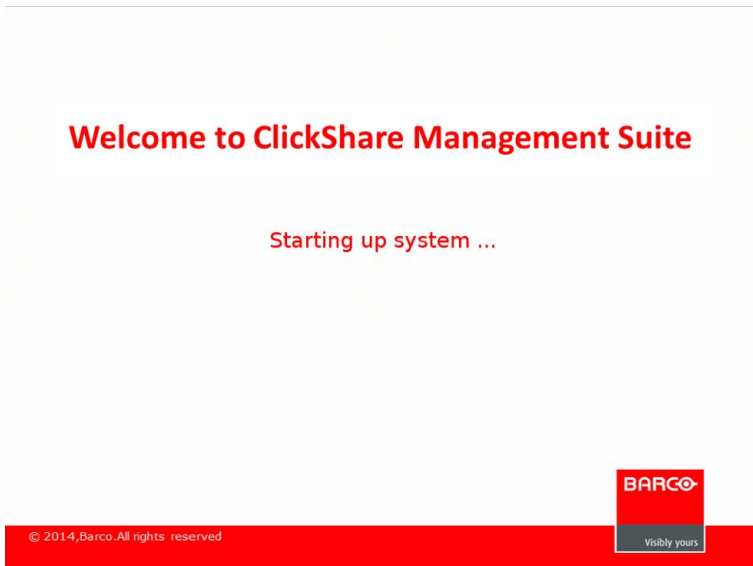


Image 1-13

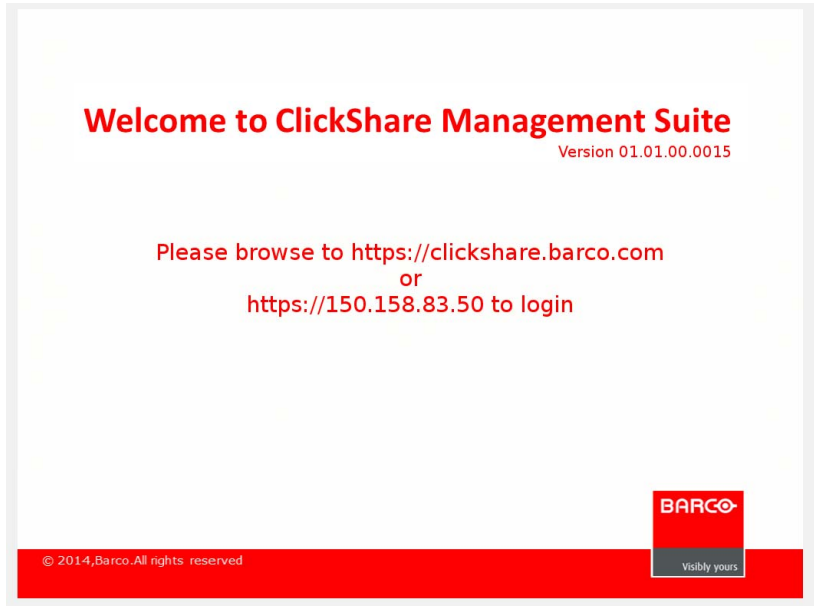


Image 1-14

1.2.2 Server configuration



Server configuration will typically be done by the IT admin of the system and is additionally required as 'initial' configuration to start working with the system. When logging in for the first time the setup wizard starts automatically.

Configuration

1. Browse to the CMGS web address and login with the default credentials.

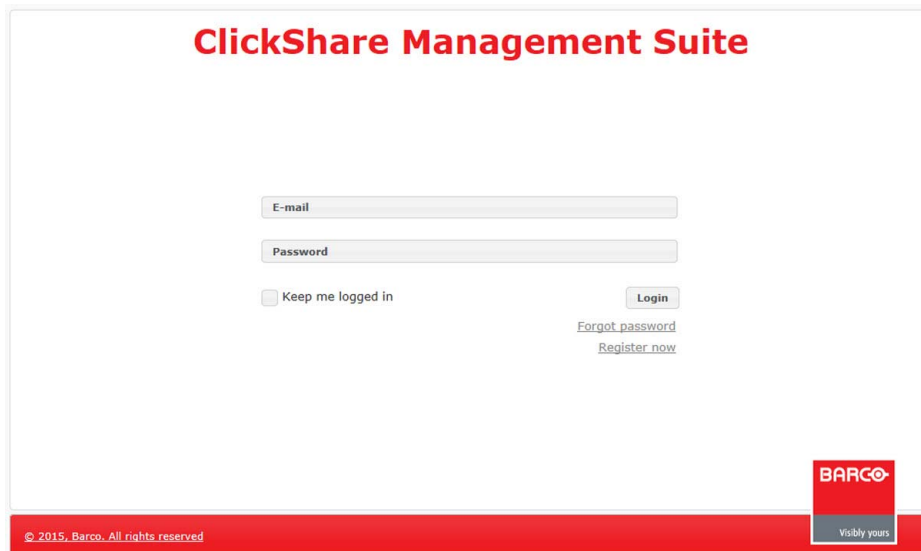


Image 1-15

User name: admin@yourcompany.com

Password: admin

A setup wizard starts up. This wizard contains all setup actions necessary to use the software correctly. These setup actions are spread over 3 tab pages, Network settings, Notifications and Security.

2. Fill out the Network settings according your local situation.

Image 1-16

Change or fill out the following settings:

- CMGS logging level: Info or Debug.
- Identify Base Units by: IP address or Hostname.
- Use a Proxy server: None or Manual
- Type: HTTP or HTTPS
- Proxy server: (only necessary when Manual is selected) fill out the address of the Proxy server.
- Port: used port to access the proxy server.
- Username: optional
- Password: optional

Click **Test Proxy settings** to test the settings.

3. Click **Next** to continue.

4. Fill out the *Notifications*.
Configure a SMPT server to register new users and to send notifications.

Image 1-17

1. Installation

- IT admin name: sender name used to send out notifications.
- E-mail address: E-mail address to send out notifications
- SMTP server: IP address or hostname of the outgoing mail server
- Port: port used on mail server to send out mail.
- Username: optional
- Password: optional
- 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

Click **Send test e-mail** to check the connection.

5. Click **Next** to continue.
6. Fill out the *Security settings*.

ClickShare Management Suite

Verify your **Setup wizard**

1. Network settings | 2. Notifications | 3. Security

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

Enforce Base Unit HTTPS communication : Yes No

Base Unit password : *****

Previous Finish

Version 01.01.00.0139 (3556) End-user license agreement | © 2015, Barco. All rights reserved

Image 1-18

- Enforce Base Unit HTTPS communication: "Yes" will enforce a HTTPS communication.
 - Base Unit password: default password to communicate with the Base Units.
7. Click **Finish** to finalize the setup.

The ClickShare Management Suite is ready to be used. The home page opens.

1.3 Administrator functions

What can be done?

An administrator can login and change the configuration settings after the setup was finished. To start up the admin page, press **Ctrl+Alt+F1** on the host PC's keyboard.

```

88888888ba
88      "gb
88      ,BP
88aaaaaaP ,adPPYyba, 8b,dPPYba, ,adPPYba, ,adPPYba,
88""""""gb, ""  Y8 88P' "Y8 88' "" 88' "8a
88      8b ,adPPPP88 88      8b      8b      d8
88      a8P 88, ,88 88      "8a, ,aa "8a, ,88"
88888888P "" "8bbdP"Y8 88      "Ybbd8"" "" "YbbdP""

,ad8888ba, 88 88      88      ad8888ba 88
d8"""""" "8b 88 """" 88      d8"" "" "8b 88
d8'      88      88      Y8,      88
88      88 88 ,adPPYba, 88 ,d8 Y8aaaa, 88,dPPYba, ,adPPYyba, 8b,dPPYba, ,adPPYba,
88      88 88 a8' """" 88 ,d8' """"""""8b, 88P' "8a "" "" Y8 88P' "Y8 88P' "" 88
Y8,      88 88 8b      8888|      8b 88      88 ,adPPPP88 88      88P'""""""""
Y8a,      a8P 88 88 "8a, ,aa 88 "Yba, Y8a      a8P 88      88 88, ,88 88      "8b, ,aa
"Y8888y"" 88 88 "Ybbd8"" 88      Y8a "Y8888P" 88      88 "8bbdP"Y8 88      "Ybbd8""

Welcome to the administrator console of the ClickShare Management Suite.
Please login as "administrator" and use password set during installation or via administrator console.
Authorized use only, transactions may be monitored. By continuing past this point, you expressly consent to this
monitoring.

Barco CMS server with IP address 10.0.2.15

cms login:

```

Image 1-19

To login, the user name is *administrator* and the password is the one entered during the installation.

```

admin console
=====
1: NTP configuration
2: Name servers configuration
3: Network configuration
4: Host name
5: Domain name
6: Time zone
7: Password
8: System update
9: Reboot
10: Shutdown
11: Upload logs
q: Quit
>_

```

Image 1-20



To change the configuration, just enter the number of that item that should be changed and press ENTER to continue. Follow the instructions given on the different screens.

Use **q** to quit the administrator session.

Overview of the menu items on the admin console

After login, 10 different options can be chosen by typing the number behind the prompt ">" and hitting "Enter". "q" can always be used to return to the former configuration window.

1. Installation

1. **NTP configuration**
Configure the correct NTP servers and synchronize with them.
 Keep in mind that the NTP configuration set during installation is only for time synchronization during installation, NTP needs to be configured a second time after initial boot to correctly sync after installation.
2. **Name server configuration**
Configure the correct DNS name servers, if not automatically provided by DHCP.
3. **Network configuration**
Configure the network interface(s) statically or dynamically via DHCP.
4. **Host name**
Configure the host name.
5. **Domain name**
Configure the domain name in case it was not automatically configured via DHCP.
6. **Time Zone**
Configure the time zone if the originally configured time zone during installation should be changed.
 If changed, please reboot the machine to see the time zone change also reflected in the CMGS web application.
7. **Password**
Set new password for the admin console.
8. **System update**
Prior to system update the ISO from which the system will upgrade should be connected as CD/DVD source to the machine. Before starting update additional approval is requested.
9. **Reboot**
Reboot the system, before starting reboot additional approval is requested.
10. **Shutdown**
Shutdown the system gracefully, before starting shutdown additional approval is requested.
11. **Upload logs**
Logs to FTP server or to a network location
12. **q.Quit**