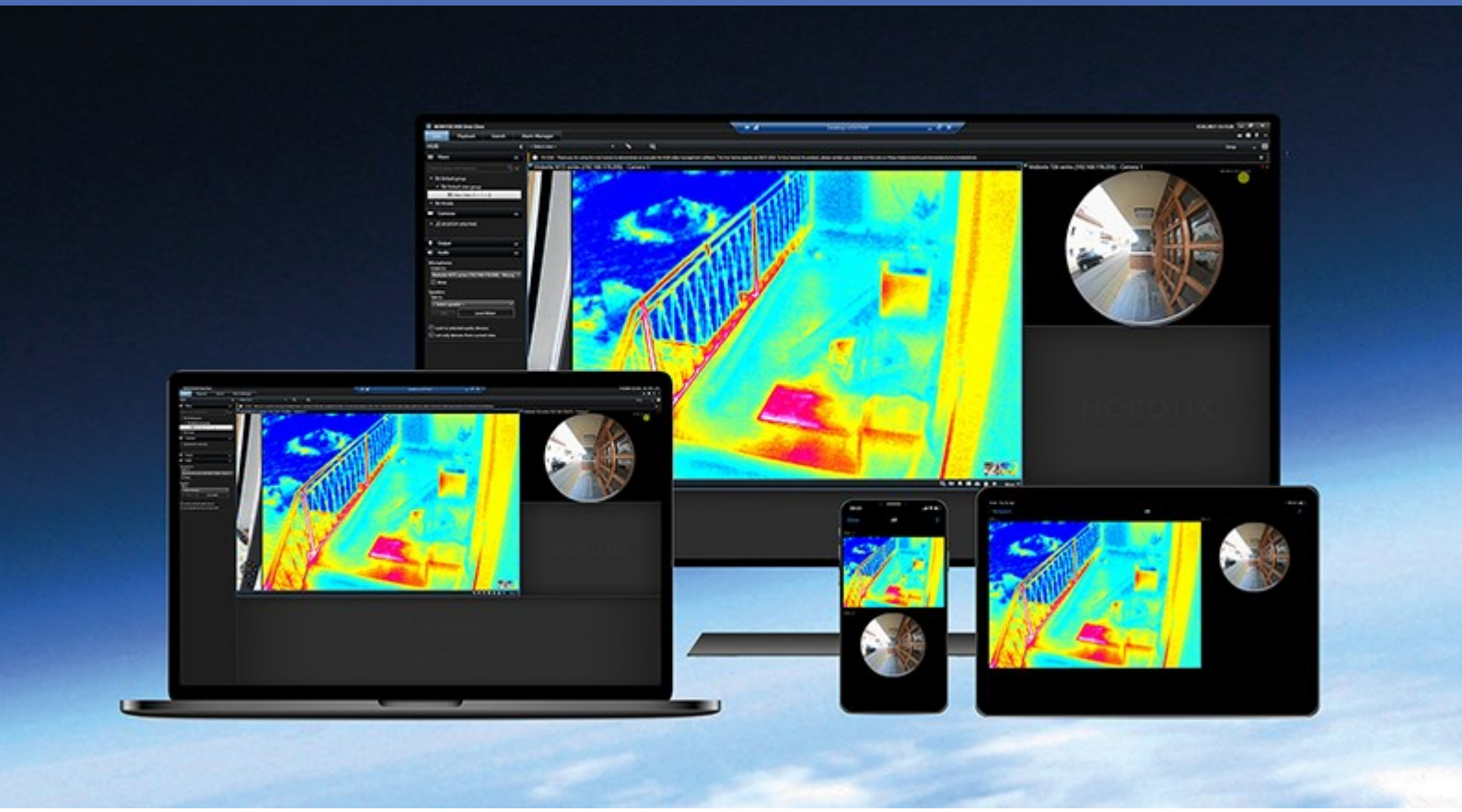
Administrator manual

MOBOTIX HUB Mobile server 2023 R2

© 2023 MOBOTIX AG



BeyondHumanVision

MOBOTIX

Contents

Copyright **5**

Overview **6**

What's new? 6

MOBOTIX HUB Mobile (explained) 6

MOBOTIX HUB Mobile server (explained) 7

Product comparison 7

Requirements and considerations **8**

MOBOTIX HUB Mobile system requirements 8

Before you install MOBOTIX HUB Mobile server 8

Prerequisites for using MOBOTIX HUB Mobile 8

Requirements for user's two-step verification setup 9

Requirements for Video Push setup 9

Requirements for direct streaming 9

Requirements for using Share 10

Installation **11**

Install MOBOTIX HUB Mobile server 11

Configuration **14**

Mobile server settings 14

General tab 14

Connectivity tab 16

Server Status tab 17

Performance tab 19

Investigations tab 21

Video Push tab 23

Two-step verification tab 24

Direct streaming (explained) 26

Adaptive streaming (explained) 27

Mobile server data encryption (explained) 27

Mobile server encryption requirements for clients 28

Enable encryption on the mobile server ... 29
MOBOTIX Federated Architecture and parent/child sites (explained) ... 30
Set up investigations ... 30
Using Video Push to stream video (explained) ... 32
Set up Video Push to stream video ... 32
Add a Video Push channel for streaming video ... 32
Edit a Video Push channel ... 33
Remove a Video Push channel ... 33
Change password ... 33
Add the Video Push Driver as a hardware device on the recording server ... 34
Add the Video Push Driver device to the channel for Video Push ... 35
Enable audio for existing video push channel ... 35
Set up users for two-step verification via email ... 36
Enter information about your SMTP server ... 36
Specify the verification code that will be sent to users ... 36
Assign verification method to users and Active Directory groups ... 37
Actions (explained) ... 37
Mobile device management (MDM) (explained) ... 37
Configure mobile server details on MDM platform (administrators) ... 38
Naming an output for use in MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client (explained) ... 39
External IDP and MOBOTIX HUB Mobile (explained) ... 40
Configure external IDP login for MOBOTIX HUB Web Client ... 40
Maintenance ... 41
Mobile Server Manager (explained) ... 41
Access MOBOTIX HUB Web Client ... 41
Start, stop and restart Mobile Server service ... 42
Change data protection password ... 42
Show/edit port numbers ... 43
Accessing logs and investigations (explained) ... 43
Change investigations folder ... 44
Show status (explained) ... 44

Troubleshooting **45**

Troubleshooting MOBOTIX HUB Mobile 45

Appendices **47**

Appendix A 47

Appendix B 49

Copyright

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816 0 • sales@mobotix.com • www.mobotix.com

MOBOTIX is a trademark of MOBOTIX AG registered in the European Union, the U.S.A., and in other countries. Subject to change without notice. MOBOTIX do not assume any liability for technical or editorial errors or omissions contained herein. All rights reserved. © MOBOTIX AG 2023

Overview

What's new?

In MOBOTIX HUB Mobile server 2023 R2

Bookmarks and live video sharing:

- To share bookmarks and live video in the MOBOTIX HUB Mobile client, you must enable encryption on the management server. See Requirements for using Share on page 10.

Notifications:

- You can remove device registration data from the VMS database. See Remove one or all registered devices from the Registered devices list.

In MOBOTIX HUB Mobile server 2022 R3

External IDP:

- You can now log in to MOBOTIX HUB Web Client and the MOBOTIX HUB Mobile client with an external IDP. See External IDP and MOBOTIX HUB Mobile (explained) on page 40

Mobile device management (MDM):

- The MOBOTIX HUB Mobile client now supports mobile device management (MDM). With MDM, you can manage and secure devices, apps, and data from a unified console. For more information, see Mobile device management (MDM) (explained) on page 37

In MOBOTIX HUB Mobile server 2022 R2

Installation:

- When installing Mobile Server, you can connect to the surveillance system with a basic user

MOBOTIX HUB Mobile (explained)

MOBOTIX HUB Mobile consists of five components:

- MOBOTIX HUB Mobile client

  The MOBOTIX HUB Mobile client is a mobile surveillance app that you can install and use on your Android or Apple device. You can use as many installations of MOBOTIX HUB Mobile client as you need.

- MOBOTIX HUB Web Client

  MOBOTIX HUB Web Client lets you view live video in your web browser and lets you download recordings. MOBOTIX HUB Web Client is installed automatically together with the installation of the MOBOTIX HUB Mobile server.

- MOBOTIX HUB Mobile server
- MOBOTIX HUB Mobile plug-in
- Mobile Server Manager

This manual covers the MOBOTIX HUB Mobile server, MOBOTIX HUB Mobile plug-in, and Mobile Server Manager.

MOBOTIX HUB Mobile server (explained)

The MOBOTIX HUB Mobile server handles logins to the system from the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client.

An MOBOTIX HUB Mobile server distributes video streams from recording servers to the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client. This offers a secure setup where recording servers are never connected to the internet. When an MOBOTIX HUB Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats, allowing the streaming of video on the mobile device.

You must install the MOBOTIX HUB Mobile server on any computer from which you want to access recording servers.

The MOBOTIX HUB Mobile server supports direct streaming and adaptive streaming in live mode (not available for MOBOTIX HUB L1).

Product comparison

MOBOTIX HUB VMS includes the following products:

- MOBOTIX HUB L5
- MOBOTIX HUB L4
- MOBOTIX HUB L3
- MOBOTIX HUB L2
- MOBOTIX HUB L1

See the complete feature list, which is available on the product overview page on the MOBOTIX website (https://www.mobotix.com/en/products/vms/mobotixhub).

Requirements and considerations

MOBOTIX HUB Mobile system requirements

For information about the system requirements for the various VMS applications and system components, go to the MOBOTIX website (https://www.mobotix.com/en/media/4821).

- To find requirements for the MOBOTIX HUB Mobile client, select the **MOBOTIX HUB Mobile** product icon
- To find requirements for MOBOTIX HUB Web Client, select the **MOBOTIX HUB Web Client** product icon
- To find requirements for the MOBOTIX HUB Mobile server, select the icon of the MOBOTIX HUB product that you have installed
- The requirements for MOBOTIX HUB Mobile plug-in are:
    - A running Management Client
    - The MOBOTIX plug-in is installed to integrate with your VMS

Before you install MOBOTIX HUB Mobile server

MOBOTIX recommends that you install the MOBOTIX HUB Mobile server on a separate computer. Before you begin the installation, make sure of the following:

- Ensure that the mobile server computer resolves the host names of the management server computer and the recording server computers
- Ensure that the management server computer resolves the host name of the mobile server computer
- To install the MOBOTIX HUB Mobile server, add a Windows user account to the Administrators role in MOBOTIX HUB Management Client. Use the same Windows account when you install the MOBOTIX HUB Mobile server. The MOBOTIX HUB Mobile server installer must be able to log in to the MOBOTIX HUB VMS during the installation

To connect to the surveillance system, you must select an existing VMS user. The role to which this user is added requires permissions for the management server:

- **Connect** - Enables you to connect to the management server
- **Read** - Enables you to access a wide range of functionality
- **Edit** - Eenables you to modify data in a wide range of functionality

To learn more about permissions, see the administrator manual for the MOBOTIX HUB VMS.

Prerequisites for using MOBOTIX HUB Mobile

Before you can start using MOBOTIX HUB Mobile, you must make sure that you have the following:

- A running VMS installed and configured with at least one user
- Cameras and views set up in MOBOTIX HUB Desk Client
- A mobile device running Android or iOS with access to Google Play or App Store℠ from which you can download the MOBOTIX HUB Mobile client application
- A web browser for running MOBOTIX HUB Web Client

To read more about requirements, see MOBOTIX HUB Mobile system requirements on page 8.

Requirements for user's two-step verification setup

- You have installed an SMTP server
- You have added users and groups to your MOBOTIX HUB system in the Management Client on the **Roles** node in the **Site Navigation** pane. On the relevant role, select the **Users and Groups** tab
- If you upgraded your system from a previous version of MOBOTIX HUB, you must restart the mobile server to enable the two-step verification feature

For more information, see:

Set up users for two-step verification via email on page 36

Two-step verification tab on page 24

Requirements for Video Push setup

- Each channel requires a device license
- To enable audio with video push:
    1. Download and install MOBOTIX HUB Device Pack 10.3a version or later from https://www.mobotix.com/en/software-downloads
    2. Download and install MOBOTIX HUB Mobile Server Installer.exe 13.2a or later from the Download Manager web page that is available at **http://[management server address]:[port]/installation/admin/**
    3. Restart the Recording Server service.

Requirements for direct streaming

MOBOTIX HUB Mobile supports direct streaming in live mode.

Camera configuration requirements for direct streaming

To use direct streaming in MOBOTIX HUB Web Client and MOBOTIX HUB Mobile client, you must have the following camera configuration:

- The cameras must support the H.264 codec (for all clients) or the H.265 codec (for the MOBOTIX HUB Mobile client only)
- It is recommended that you set the **GOP size** value to **1 second**, and the **FPS** setting must have a value that is higher than **10** FPS

Requirements for using Share

Users can share bookmarks and live video while using the MOBOTIX HUB Mobile client app. These functionalities are available after:

- You have enabled encryption on the management server.

Installation

Install MOBOTIX HUB Mobile server

Once you have installed the MOBOTIX HUB Mobile server, you can use MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client with your system. To reduce the overall use of system resources on the computer running the management server, install the MOBOTIX HUB Mobile server on a separate computer.

The management server has a built-in public installation webpage. From this webpage, administrators and end-users can download and install the required MOBOTIX HUB system components from the management server or any other computer in the system.

> MOBOTIX HUB Mobile server is automatically installed when you install the "single computer" option.

To install the MOBOTIX HUB Mobile server:

1. Enter the following URL in your browser: *http://[management server address]/installation/admin* where the [management server address] is the IP address or the host name of the management server.
2. Select **All Languages** for the MOBOTIX HUB Mobile server installer.
3. Run the downloaded file. Then, select **Yes** to all warnings. Then, unpacking starts.
4. Select a language for the installer. Then, select **Continue**.
5. Read and accept the license agreement. Then, select **Continue**.
6. Select the installation type:
   - Select **Typical** to install MOBOTIX HUB Mobile server and plug-in
   - Select **Custom** to install only the server or only the plug-in. For example, installing only the plug-in is useful if you want to use Management Client to manage MOBOTIX HUB Mobile servers but don't need an MOBOTIX HUB Mobile server on that computer

     > MOBOTIX HUB Mobile plug-in is required on the computer running Management Client to manage MOBOTIX HUB Mobile servers in Management Client.

7. For custom installation only: Select the components that you want to be installed. Then, select **Continue**.
8. Select the service account for the mobile server. Then, select **Continue**.

   > To change or edit the service account credentials at a later stage, you have to reinstall the mobile server.

9. For custom installation only: Log in with an existing VMS user account when connecting to the surveillance system:
   - **Service account** is the account you selected in step 8. To connect using this account, make sure that the service account is a member of a domain to which the management server has access
   - **Basic user.** Use a basic user when the service account is not a member of a domain to which the management server has access

   > To change or edit the service account or the basic user credentials at a later stage, you have to reinstall the mobile server.

   Select **Continue**.
10. In the **Server URL** field, fill in the primary management server address.
11. For custom installation only: Specify the connection ports for communication with the mobile server. Then, select **Continue**.

    > In a typical installation, the connection ports get the default port numbers (8081 for HTTP port and 8082 for HTTPS port).

12. On the **Assign a mobile server data protection password** page, enter a password to encrypt your investigations. As a system administrator, you will need to enter this password to access the mobile server data in case of system recovery or when expanding your system with additional mobile servers.

    > You must save this password and keep it safe. Failure to do so may compromise your ability to recover mobile server data.

    If you do not want your investigations to be password-protected, select **I choose not to use a mobile server data protection password, and I understand that investigations will not be encrypted**.

    Click **Continue**.
13. Specify the mobile server encryption. Then, select **Continue**.

    On the **Select encryption** page, you can secure the communication flows:
    - Between the mobile servers and the recording servers, data collectors, and the management server. To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate
    - Between the mobile servers and clients. To enable encryption between the mobile server and clients that retrieve data streams from the mobile server, in the **Streaming media certificate** section, select a certificate

> If you do not enable encryption, some features in some clients will not be available. For more information, see Mobile server encryption requirements for clients.

For more information about establishing secure communication in your system, see:

- Mobile server data encryption (explained)
- The MOBOTIX guide about certificates

You can also enable encryption after the installation completes from the Mobile Server Manager tray icon in the taskbar of your operating system. (see Enable encryption on the mobile server on page 29).

14. Select the file location and product language and then select **Install**.
15. When the installation is completed, a list of successfully installed components appears. Then, select **Close**.

You are ready for configuring MOBOTIX HUB Mobile (see Mobile server settings on page 14).

Configuration

Mobile server settings

In Management Client, you can configure and edit a list of MOBOTIX HUB Mobile server settings. You can access these settings on the bottom toolbar of the mobile server **Properties** section. From there, you can:

- Enable or disable server features general configuration (see General tab on page 14)
- Configure server connectivity settings (see Connectivity tab on page 16)
- See the current status of the server and the list of active users (see Server Status tab on page 17)
- Set up performance parameters to enable direct streaming and adaptive streaming, or to set transcoded video stream limitations (see Performance tab on page 19)
- Configure investigation settings (see Investigations tab on page 21)
- Configure Video Push settings (see Video Push tab on page 23)
- Enable and configure an additional login step for users (see Two-step verification tab on page 24)

General tab

The following table describes the settings on this tab.

General

Name	Description
Server name	Enter the name of the MOBOTIX HUB Mobile server.
Description	Enter an optional description of the MOBOTIX HUB Mobile server.
Mobile server	See the name of the currently selected MOBOTIX HUB Mobile server.

Features

The following table describes how you control the availability of MOBOTIX HUB Mobile features.

Name	Description
Enable MOBOTIX HUB Web Client	Enable access to MOBOTIX HUB Web Client. This feature is enabled by default.
Enable the All cameras view for MOBOTIX HUB Mobile client	This view displays all the cameras that a user is allowed to view on a recording server. This feature is enabled by default.
Enable bookmarks	Enable the bookmarks feature to quickly locate video sequences in MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client. This feature is enabled by default.
Enable actions (outputs and events)	Enable access to actions in MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client. This feature is enabled by default. If you disable this feature, the client users are not able to see output and events, even if these are configured correctly.
Enable incoming audio	Enable the incoming audio feature in MOBOTIX HUB Web Client and MOBOTIX HUB Mobile client. This feature is enabled by default.
Enable push-to-talk	Enable the push-to-talk (PTT) feature in MOBOTIX HUB Web Client and MOBOTIX HUB Mobile client. This feature is enabled by default.
Deny the built-in Administrator role access to the MOBOTIX HUB Mobile server	Enable this to prevent users assigned to the built-in administrator role from accessing video on MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client.

Log settings

You can see the log settings information.

Name	Description
Log file location	See where the system saves log files.
Keep logs for	See the number of days to keep logs for. The default is three days.

Configuration backup

If your system has multiple MOBOTIX HUB Mobile servers, you can use the backup function to export the current settings and import them on other MOBOTIX HUB Mobile servers.

Name	Description
Import	Import an XML file with a new MOBOTIX HUB Mobile server configuration.
Export	Export your MOBOTIX HUB Mobile server configuration. Your system stores the configuration in an XML file.

Connectivity tab

Settings on the **Connectivity** tab are used in the following tasks:

- Configure connection settings
- Send an email message to users
- Enable connections on complex network
- Enable Universal Plug and Play discoverability on your router

You can configure how the MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client users should connect to the MOBOTIX HUB Mobile server when you open the **Server Configurator** during installation or by right-clicking the Mobile Server Manager tray icon after installation. The connection type can either be HTTPS or HTTP. For more information, see Enable encryption on the mobile server on page 29.

General

Name	Description
Client timeout	Set a time frame for how often the MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client must indicate to the MOBOTIX HUB Mobile server that they are up and running. The default value is 30 seconds. MOBOTIX recommends that you do not increase the time frame.

Name	Description
Enable UPnP-discoverability	This makes the MOBOTIX HUB Mobile server discoverable on the network by means of the UPnP protocols. The MOBOTIX HUB Mobile client has scanning functionality for finding MOBOTIX HUB Mobile servers based on UPnP.
Enable automatic port mapping	When the MOBOTIX HUB Mobile server is installed behind the firewall, a port mapping is required in the router, so clients can still access the server from the internet. The **Enable automatic port mapping** option enables the MOBOTIX HUB Mobile server to do this port mapping by itself, provided that the router is configured for it.

Internet access

Name	Description
Configure custom internet access	Provide the **IP address or hostname** and the port number to use for the connection. For example, you might do this if your router does not support UPnP or if you have a chain of routers.
• **HTTP** • **HTTPS**	Select the type of connection.
Select to retrieve IP address dynamically	Select the check box, if your IP addresses often change.
Use the configured URL address only	Select the check box to connect to the mobile server with a custom-specified IP address or hostname only.
Server addresses	Lists all the URL addresses that are connected to the mobile server.

Server Status tab

See the status details for the MOBOTIX HUB Mobile server. The details are read-only:

Name	Description
Server active since	Shows the time and date when the MOBOTIX HUB Mobile server was last started.
CPU usage	Shows current CPU usage on the mobile server.
External bandwidth	Shows the current bandwidth in use between the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client and the mobile server.

Active users

See the status details of the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client currently connected to the MOBOTIX HUB Mobile server.

Name	Description
User Name	Shows the user name for each MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user connected to the mobile server.
State	Shows the current relation between the MOBOTIX HUB Mobile server and the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user in question. Possible states are: • **Connected**: An initial state when the clients and the server exchange keys and encrypting credentials • **Logged In**: The MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user is logged into the MOBOTIX HUB system
Video bandwidth usage (kB/s)	Shows the total bandwidth of the video streams that are currently open for each MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user.
Audio bandwidth usage (kB/s)	Shows the total bandwidth of the audio streams that are currently open for each MOBOTIX HUB Web Client user.
Transcoded video streams	Shows the total number of transcoded video streams that are currently open for each MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user.
Direct video streams	Shows the total number of direct video streams that are currently open for each MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client user (for MOBOTIX

Name	Description
	HUB L4 and MOBOTIX HUB L5 only).
Transcoded audio streams	Shows the total number of transcoded audio streams that are currently open for each MOBOTIX HUB Web Client user.

Performance tab

On the **Performance** tab, you can set the following settings and limitations on the MOBOTIX HUB Mobile server's performance:

Video streaming settings (for MOBOTIX HUB L4 and MOBOTIX HUB L5 only)

Name	Description
Enable direct streaming	Enable direct streaming in MOBOTIX HUB Web Client and MOBOTIX HUB Mobile client (for MOBOTIX HUB L4 and MOBOTIX HUB L5 only). This feature is enabled by default.
Enable adaptive streaming	Enable adaptive streaming in MOBOTIX HUB Web Client and MOBOTIX HUB Mobile client (for MOBOTIX HUB L4 and MOBOTIX HUB L5 only). This feature is enabled by default.
Streaming modes	After you enable the adaptive streaming feature, you can select the type of the streaming mode from the list: • **Optimize video quality (default)** - selects the stream with the lowest available resolution that is equal to or higher than the requested resolution • **Optimize server performance** - reduces the requested resolution and then selects the stream with the lowest available resolution that is equal to or higher than the reduced request • **Optimize resolution for low bandwidth** - selects the stream with the lowest available resolution (recommended if you use 3G or an unstable network)

Transcoded video stream limitations

Level 1

Level 1 is the default limitation placed on the MOBOTIX HUB Mobile server. Any limitations that you set here are always applied to the MOBOTIX HUB Mobile's transcoded video streams.

Name	Description
Level 1	Select the check box to enable the first level of limitations to MOBOTIX HUB Mobile server performance.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the MOBOTIX HUB Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the MOBOTIX HUB Mobile server to clients.

Level 2

If you want to enforce a different level of limitations than the default one in **Level 1**, select the **Level 2** check box. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to MOBOTIX HUB Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the MOBOTIX HUB Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the MOBOTIX HUB Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the MOBOTIX HUB Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the MOBOTIX HUB Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or less.

Name	Description
Level 3	Select the check box to enable the third level of limitations to MOBOTIX HUB Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the MOBOTIX HUB Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the MOBOTIX HUB Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the MOBOTIX HUB Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the MOBOTIX HUB Mobile server to clients.

The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Investigations tab

Investigations settings

You can enable investigations so that people can use the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client to:

- Access recorded video
- Investigate incidents
- Prepare and download video evidence

Name	Description
Enable investigations	Select this check box to allow users to create investigations.
Investigations folder	Shows where your video exports are saved on your hard drive.
View investigations made by other users	Select this check box to allow users to access investigations that they did not create.
Enable the size limit of investigations folder	Select this check box to set a size limit on the investigations folder and enter the maximum number of megabytes that the investigations folder can contain. The default size is 2000 MB.
Enable the investigation retention time	Select this check box to set a retention time for investigations. By default, the retention time is seven days.
Export formats	Select the check box of the export format that you want to use. The available export formats are: • **AVI format** • **MOBOTIX HUB format** • **MKV format** By default, the check boxes are cleared.
Include timestamps for AVI exports	Select this check box to include the date and time that the AVI file was downloaded.
Used codec for AVI exports	Select the compression format to use when preparing AVI packages for download. The codecs that you can choose from can differ depending on your operating system. If you do not see the codec you want, you can add it to the list by installing it on the computer where the MOBOTIX HUB Mobile server is running.
Used audio bit for AVI exports	Select from the list the appropriate audio bit rate when audio is included in your video export. The default is 160000 Hz.

Investigations

Name	Description
Investigations	Lists the investigations that have been set up so far in the system. Use the **Delete** or **Delete all** buttons if you no longer want to keep an investigation. This can be useful if, for example, you want to make more disk space available on the server.
Investigation details	To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the **Investigation details** group, select the delete icon to the right of the **MOBOTIX HUB**, **AVI**, or **MKV** fields for exports.

Video Push tab

You can specify the following settings if you enable Video Push:

Name	Description
Video Push	Enable Video Push on the mobile server.
Number of channels	Shows the number of enabled Video Push channels in your MOBOTIX HUB system.
Channel	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video Push channel.
MAC Address	MAC address for the relevant Video Push channel.
User Name	Enter the user name associated with the relevant Video Push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see Set up Video Push to stream video on page 32), select **Find Cameras** to search for the relevant camera.

Two-step verification tab

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the MOBOTIX website (https://www.mobotix.com/en/products/vms/mobotixhub).

Use the **Two-step verification** tab to enable and specify an additional login step on users of:

- MOBOTIX HUB Mobile app on their iOS or Android mobile devices
- MOBOTIX HUB Web Client

The first type of verification is a password. The second type is a verification code, which you can configure to be sent to the user via email.

For more information, see Set up users for two-step verification via email on page 36.

The following tables describe the settings on this tab.

Provider settings > **Email**

Name	Description
SMTP server	Enter the IP address or host name of the simple mail transfer protocol (SMTP) server for two-step verification emails.
SMTP server port	Specify the port of the SMTP server for sending emails. The default port number is 25 without SSL and 465 with SSL.
Use SSL	Select this check box if your SMTP server supports SSL encryption.
User name	Specify the user name for logging in to the SMTP server.
Password	Specify the password for logging in to the SMTP server.
Use Secure Password Authentication (SPA)	Select this check box if your SMTP server supports SPA.
Sender's email address	Specify the email address for sending verification codes.

Name	Description
Email subject	Specify the subject title for the email. Example: Your two-step verification code.
Email text	Enter the message you want to send. Example: Your code is {0}. If you forget to include the {0} variable, the code is added at the end of the text by default.

Verification code settings

Name	Description
Reconnection timeout (0-30 minutes)	Specify the period within which MOBOTIX HUB Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes. This setting does not apply to MOBOTIX HUB Web Client.
Code expires after (1-10 minutes)	Specify the period within which the user can use the received verification code. After this period, the code is invalid, and the user has to request a new code. The default period is five minutes.
Code entry attempts (1-10 attempts)	Specify the maximum number of code entry attempts before the provided code becomes invalid. The default number is three.
Code length (4-6 characters)	Specify the number of characters for the code. The default length is six.
Code composition	Specify the complexity of the code that you want the system to generate. You can select among: • **Latin uppercase (A-Z)** • **Latin lowercase(a-z)** • **Digits (0-9)** • **Special characters (!@#...)**

User settings

Name	Description
Users and groups	Lists the users and groups added to the MOBOTIX HUB system. If a group is configured in Active Directory, the mobile server uses details, such as email addresses, from Active Directory. Windows groups do not support two-step verification.
Verification method	Select a verification setting for each user or group. You can select among: • **No login**: the user cannot log in • **No two-step verification**: the user must enter user name and password • **Email**: the user must enter a verification code in addition to the user name and password
User details	Enter the email address to which each user will receive codes.

Direct streaming (explained)

MOBOTIX HUB Mobile supports direct streaming in live mode.

Direct streaming is a video streaming technology that transfers video from an MOBOTIX HUB system to the clients directly in H.264 codec, which is supported by most modern IP cameras. Direct streaming does not require any transcoding and, therefore, removes some of the stress on the MOBOTIX HUB system.

The direct streaming technology is in contrast to the transcoding setting in MOBOTIX HUB, in which an MOBOTIX HUB system decodes video from the codec that is used on the camera into JPEG files. Enabling the feature results in reduced CPU usage for the same configuration of cameras and video streams. Direct streaming also increases streaming performance for the same hardware - up to five times as many concurrent video streams compared to transcoding.

You can also use the direct streaming feature to transfer video from cameras that support the H.265 codec directly to the MOBOTIX HUB Mobile client.

In Management Client, you can enable or disable direct streaming for clients (see Mobile server settings on page 14).

The video stream falls back from direct streaming to transcoding if:

- The direct streaming feature has been disabled in Management Client, or the requirements have not been fulfilled (see Requirements for direct streaming on page 9)
- The codec of the streaming camera is different than H.264 (for all clients) or H.265 (for the MOBOTIX HUB Mobile client only)
- The video cannot start playing for more than ten seconds

- The frame rate of the streaming camera is set to one frame per second (1 FPS)
- The connection with the server or with the camera has been lost
- You use the privacy masking feature during live video

Adaptive streaming (explained)

MOBOTIX HUB Mobile supports adaptive streaming in live mode.

Adaptive streaming is useful when you view multiple live video streams in the same view of cameras. The feature optimizes the performance of the MOBOTIX HUB Mobile server and improves the decoding capability and performance of devices that are running MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client.

To take advantage of adaptive streaming, your cameras must have multiple streams defined with different resolutions. In this case, the feature enables you to:

- Optimize video quality - selects the stream with the lowest available resolution that is equal to or higher than the requested resolution.
- Optimize server performance - reduces the requested resolution and then selects the stream with the lowest available resolution that is equal to or higher than the reduced request.
- Optimize resolution for low bandwidth - selects the stream with the lowest available resolution (recommended if you use 3G or an unstable network).

When zooming, the live video stream requested is always the one with the highest available resolution.

Bandwidth usage is often reduced when the resolution of the requested streams is reduced. Bandwidth usage also depends on other settings in the configurations of the defined streams.

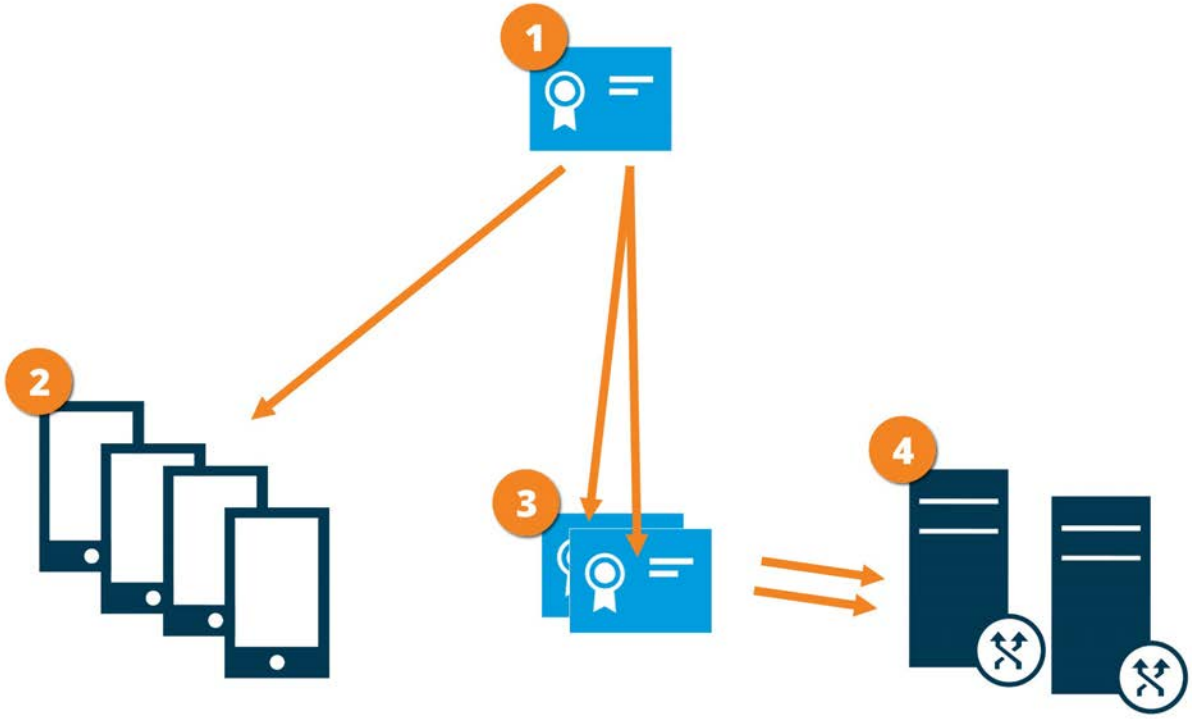
You can enable or disable adaptive streaming and set the preferred streaming mode of the feature on the **Performance tab** of the mobile server settings in Management Client (see Mobile server settings on page 14).

Mobile server data encryption (explained)

In MOBOTIX HUB VMS, encryption is enabled or disabled per mobile server. When you enable encryption on a mobile server, you will have the option to use encrypted communication with all clients, services, and integrations that retrieve data streams.

Certificate distribution for mobile servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in MOBOTIX HUB VMS to secure the communication with the mobile server.



❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (mobile server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way, clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish a secure connection between the mobile server and clients and services

❹ The CA certificate must be installed on the computer on which the mobile server is running

Requirements for the CA certificate:

- The mobile server's host name must be included in the certificate, either as subject/owner or in the list of DNS names that the certificate is issued to
- The certificate must be trusted on all devices that are running services that retrieve data streams from the mobile server
- The service account that runs the mobile server must have access to the private key of the CA certificate

For more information, see the certificates guide about how to secure your MOBOTIX HUB VMS installations.

Mobile server encryption requirements for clients

For security reasons, MOBOTIX recommends that you use secure communication between the mobile server and clients when you manage user account settings.

If you do not enable encryption and use an HTTP connection, the push-to-talk feature in MOBOTIX HUB Web Client will not be available.

Enable encryption on the mobile server

To use an HTTPS protocol for establishing a secure connection between the mobile server and clients and services, you must apply a valid certificate on the server. The certificate confirms that the certificate holder is authorized to establish secure connections.

For more information, see the certificates guide about how to secure your MOBOTIX HUB VMS installations.

When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.

Certificates issued by CA (Certificate Authority) have a chain of certificates and on the root of that chain is the CA root certificate. When a device or browser sees this certificate, it compares its root certificate with pre-installed ones on the OS (Android, iOS, Windows, etc.). If the root certificate is listed in the pre-installed certificates list, then the OS ensures the user that the connection to the server is secure enough. These certificates are issued for a domain name and are not free of charge.

Steps:

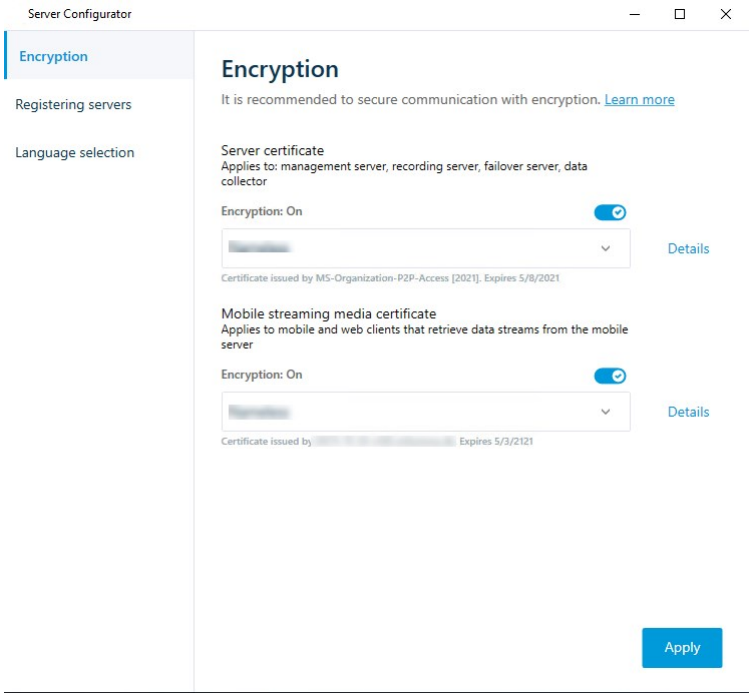
1. On a computer with a mobile server installed, open the **Server Configurator** from:
   - The Windows Start menu

   or
   - The Mobile Server Manager by right-clicking the Mobile Server Manager icon on the computer task bar
2. In the **Server Configurator**, under **Mobile streaming media certificate**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt the communication of MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client with the mobile server.

   Select **Details** to view Windows Certificate Store information about the selected certificate.

   The Mobile Server service user has been given access to the private key. It is required that this certificate be

trusted on all clients.



5. Click **Apply**.

When you apply certificates, the Mobile Server service restarts.

MOBOTIX Federated Architecture and parent/child sites (explained)

MOBOTIX Federated Architecture links multiple individual systems into a federated site hierarchy of parent/child sites.

To gain access to all sites with your MOBOTIX HUB Mobile or MOBOTIX HUB Web Client, install the MOBOTIX HUB Mobile server only on the parent site.

Users of MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client must connect to the management server on the parent site.

Set up investigations

Set up investigations so that people can use MOBOTIX HUB Web Client or MOBOTIX HUB Mobile to access recorded video and investigate incidents and to prepare and download video evidence.

To set up investigations, follow these steps:

1. In Management Client, click the mobile server, and then click the **Investigations** tab.
2. Select the **Enable investigations** check box. By default, the check box is selected.
3. In the **Investigations folder** field, specify where to store video for investigations.

4. Optional: To allow users to access investigations that other users create, select the **View investigations made by other users** check box. If you do not select this check box, users can see only their own investigations.
5. Select the **Enable the size limit of investigations folder** check box to set the maximum number of megabytes that the investigation folder can contain.
6. Select the **Enable the investigation retention time** check box to set a retention time for investigations. By default, the retention time is set to seven days.
7. Under **Export formats**, select the check box of the export format that you want to use. The available export formats are:
   - **AVI format**
   - **MOBOTIX HUB format**
   - **MKV format**

   By default, the check boxes are cleared.

8. (Optional) To include the date and time that a video was downloaded, select the **Include timestamps for AVI exports** check box.
9. In the **Used codec for AVI exports** field, select the compression format to use when preparing AVI packages for download.

   The codecs in the list can differ, depending on your operating system. If you do not see the codec you want to use, you can install it on the computer where Management Client is running, and it will display in this list.

   Additionally, codecs can use different compression rates, which can affect video quality. Higher compression rates reduce storage requirements but can also reduce quality. Lower compression rates require more storage and network capacity but can increase quality. It's a good idea to research the codecs before you select one.

10. From the **Used audio bit rate for AVI exports** list, select the appropriate audio bit rate when audio is included in your video export. The default is 160000 Hz.

    To enable users to save investigations, you must grant the **Export** permission to the security role assigned to the users.

Clean up investigations

If you have investigations or video exports that you no longer need to keep, you can delete them. For example, this can be useful if you want to make more disk space available on the server.

- To delete an investigation, and all of the video exports that were created for it, select the investigation in the list and then click **Delete**
- To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the **Investigation details** group, click the **Delete** icon to the right of the **MOBOTIX HUB**, **AVI**, or **MKV** fields for exports

Using Video Push to stream video (explained)

You can set up Video Push so that users can keep others informed about a situation or record a video to investigate it later by streaming video from their mobile device's camera to your MOBOTIX HUB surveillance system. The video stream may have audio as well.

See also Video Push tab on page 23 and Requirements for Video Push setup on page 9.

Set up Video Push to stream video

To let users stream video from their mobile devices to the MOBOTIX HUB system, set up Video Push on the MOBOTIX HUB Mobile server.

In Management Client, perform these steps in the following order:

1. On the **Video Push** tab, select the **Video Push** check box to enable the feature.
2. Add a Video Push channel for streaming video.
3. Add the Video Push Driver as a hardware device on the Recording Server. The driver simulates a camera device so that you can stream video to the Recording Server.
4. Add the Video Push Driver device to the channel for Video Push.

Add a Video Push channel for streaming video

To add a channel, follow these steps:

1. In the navigation pane, select **Mobile Servers**, then select the mobile server.
2. On the **Video Push** tab, select the **Video Push** check box.
3. Under **Channels mapping**, in the bottom-left corner, click **Add** to add a video push channel.
4. In the dialog box that appears, enter the user name of the user account (added under **Roles**) that will use the channel. This user account must be allowed to access the MOBOTIX HUB Mobile server and the recording server (on the **Overall Security** tab).

> To use Video Push, users must log in to MOBOTIX HUB Mobile on their mobile device using the user name and password for this account.

When you add a new Video Push channel on the mobile server, the system generates the port number and the MAC address of the channel that are used when the channel is added as a hardware device on the recording server. The system also generates the password that is used for connecting the Recording Server with the Mobile Server. The default password is **MOBOTIX**.

5. Make a note of the port number. You will need it when you add the Video Push driver as a hardware device on the recording server.
6. Click **OK** to close the Video Push Channel dialog box.
7. To save the channel, click **Save** in the upper-left corner of the navigation pane.

Edit a Video Push channel

You can edit the configuration details of a Video Push channel that you added:

1. Under **Channels mapping**, select the channel to edit, then click **Edit**.
2. When you are done with editing, click **OK** to close the Video Push Channel dialog box.
3. To save the edits, click **Save** in the upper-left corner of the navigation pane.

When you edit the port number and the MAC address of a Video Push channel, make sure to also replace the Video Push channel configuration details that you previously added on the recording server with the new information. Otherwise, the connection between the Recording Server and the Mobile Server will be broken.

Remove a Video Push channel

You can remove channels that you no longer use:

1. Under **Channels mapping**, select the channel to remove, then click **Remove**.
2. To save the change, click **Save** in the upper-left corner of the navigation pane.

Change password

You can change the automatically-generated password that is used to connect the Recording Server with the Mobile Server:

1. Under **Channels mapping**, in the bottom-right corner, click **Change password**.
2. In the **Change Video Push password** dialog box, type the new password in the first field, then repeat the new password in the second field, then click **OK**.
3. To save the change, click **Save** in the upper-left corner of the navigation pane.

When you change the Video Push channel password, the change will be applied to all Video Push channels that already exist in the list or will be added in the future. Even if you remove all existing Video Push channels from the list, the new password remains active and will be applied to future channels.

After the change is saved, all existing Video Push channels stop working because the connection between the Recording Server and the Mobile Server is broken. To restore this connection, in the navigation pane, by right-clicking the **Recording servers** tab, you must run the **Replace Hardware** wizard and enter the new password for the Video Push Driver that you added as a hardware device on the Recording Server.

Add the Video Push Driver as a hardware device on the recording server

1. In the navigation pane, click **Recording Servers**.
2. Right-click the server that you want to stream video to and click **Add Hardware** to open the **Add Hardware** wizard.
3. Select **Manual** as the hardware detection method and click **Next**.
4. Enter the login credentials for the Video Push Driver:
   - User name: Leave the filed blank to use the default user name.
   - Password: Enter **MOBOTIX** - the password that is generated by the system. If you have changed it when adding the Video Push channel on the mobile server, enter the password that you prefer using. Then click **Next**

   These credentials are for the hardware, not for the user. The credentials are not related to the user account that is used for accessing the Video Push channel.

5. In the list of drivers, expand **MOBOTIX**, select the **Video Push Driver** check box, and click **Next**.
6. In the **Address** field, enter the IP address of the computer where the MOBOTIX HUB Mobile server is installed.

   It is recommended that you use the MAC address generated by the system. Change it only if you experience problems with the Video Push Driver device or, for example, if you have edited the port number and the MAC address of the Video Push channel on the mobile server.

7. In the **Port** field, enter the port number for the channel that you created for streaming video. The port number was assigned when you created the channel.
8. In the **Hardware model** column, select **Video Push Driver**, and then click **Next**.

9. When the system detects the new hardware, click **Next**.
10. In the **Hardware name template** field, specify whether to display either the model of the hardware and the IP address or the model only.
11. Specify whether to enable related devices by selecting the **Enabled** check box. You can add related devices to the list for **Video Push Driver**, even though they are not enabled. You can enable them later.

    If you want to use location information when you stream video, you must enable the **Metadata** port.

    If you want to play audio when you stream video, you must enable the microphone related to the camera that you use for video streaming.

12. Select the default groups for the related devices on the left, or select a specific group in the **Add to Group** field. Adding devices to a group can make it easier to apply settings to all devices at the same time or replace devices.

Add the Video Push Driver device to the channel for Video Push

To add the Video Push Driver device to the channel for video push, follow these steps:

1. In the **Site navigation** pane, click **Mobile Servers**, and then click the **Video Push** tab.
2. Click **Find Cameras**. If successful, the name of the Video Push Driver camera displays in the **Camera Name** field.
3. Save your configuration.

Enable audio for existing video push channel

After you have fulfilled the requirements for enabling audio in video push (see Requirements for Video Push setup on page 9), in Management Client:

1. In the **Site Navigation** pane, expand the **Servers** node and click **Recording Servers**.
2. In the overview pane, select the relevant recording server folder, then expand the **Video Push Driver** folder and right-click the video push-related microphone.
3. Select **Enabled** to enable the microphone.
4. In the same folder, select the video push-related camera.
5. In the **Properties** pane, click the **Client** tab.
   For more information, see Client tab (devices).
6. On the right-hand side of the **Related microphone** field, click ••• . The **Selected device** dialog box opens.

7. On the **Recording Servers** tab, expand the recording server folder and select the video-push related microphone.
8. Click **OK**.

Set up users for two-step verification via email

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the MOBOTIX website (https://www.mobotix.com/en/products/vms/mobotixhub).

To impose an additional login step on users of the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client, set up two-step verification on the MOBOTIX HUB Mobile server. In addition to the standard user name and password, the user must enter a verification code received by email.

Two-step verification increases the protection level of your surveillance system.

In Management Client, perform these steps:

1. Enter information about your SMTP server on page 36.
2. Specify the verification code that will be sent to users on page 36.
3. Assign verification method to users and Active Directory groups on page 37.

See also Requirements for user's two-step verification setup on page 9 and Two-step verification tab on page 24.

Enter information about your SMTP server

The provider uses the information about the SMTP server:

1. In the navigation pane, select **Mobile Servers** and select the relevant mobile server.
2. On the **Two-step verification** tab, select the **Enable two-step verification** check box.
3. Below **Provider settings**, on the **Email** tab, enter information about your SMTP server and specify the email that the system will send to client users when they log in and are set up for a secondary login.

For more information, see Two-step verification tab on page 24.

Specify the verification code that will be sent to users

To specify the complexity of the verification code:

1. On the **Two-step verification** tab, in the **Verification code settings** section, specify the period within which MOBOTIX HUB Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes.
2. Specify the period within which the user can use the received verification code. After this period, the code is invalid, and the user must request a new code. The default period is five minutes.

3. Specify the maximum number of code entry attempts before the provided code becomes invalid. The default number is three.
4. Specify the number of characters for the code. The default length is six.
5. Specify the complexity of the code that you want the system to generate.

For more information, see Two-step verification tab on page 24.

Assign verification method to users and Active Directory groups

On the **Two-step verification** tab, in the **User settings** section, the list of users and groups added to your MOBOTIX HUB system appears.

1. In the **Verification method** column, select a verification method for each user or group.
2. In the **User details** field, add the delivery details, such as the email addresses of individual users. Next time the user logs into MOBOTIX HUB Web Client or the MOBOTIX HUB Mobile app, he or she is asked for a secondary login.
3. If a group is configured in Active Directory, the MOBOTIX HUB Mobile server uses details, such as email addresses, from Active Directory.

   Windows groups do not support two-step verification.

4. Save your configuration.

You have completed the steps for setting up your users for two-step verification via email.

For more information, see Two-step verification tab on page 24.

Actions (explained)

You can manage the availability of the **Actions** tab in the MOBOTIX HUB Mobile client or MOBOTIX HUB Web Client by enabling or disabling **Actions** on the **General** tab. **Actions** are by default enabled, and all available actions for the connected devices are shown here.

For more information, see General tab on page 14.

Mobile device management (MDM) (explained)

Mobile device management (MDM) is a software that secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers, and enterprises.

Typically, the MDM solutions include a server component, which sends out the management commands to the mobile devices, and a client component, which runs on the managed device and receives and implements the management commands.

You can distribute the MOBOTIX HUB Mobile client and add custom policies to the devices in your organization.

To use the MDM functionality on a mobile device, you must configure the mobile server details on the MDM software platform. The mobile server details include the server name, the server address, the server port, and the connection type protocol.

If you have updated the details of an already added mobile server, the operator must manually delete this server from the **Servers** list and restart the MOBOTIX HUB Mobile app.

Configure mobile server details on MDM platform (administrators)

To distribute and manage the MOBOTIX HUB Mobile client to mobile devices from an MDM platform, you need to add the server details. For more information about the configuration, check the documentation about your MDM software.

If you haven't typed in any of the mandatory server details or have provided incorrect details, the mobile server won't be added to the MOBOTIX HUB Mobile app.

For Android users

You can specify the server details in the user interface of your MDM platform. You have the option to upload a managed configuration file with the server details.

Server details:

- **Server name** - (Mandatory) Type in the server name
- **Server address** - (Mandatory) Type in the server address
- **Server port** - (Mandatory) Type in the server port number
- **Connection protocol type** - Enable when you use an HTTPS connection. Disable when you use an HTTP connection. By default, the HTTPS connection is enabled

To upload the file to your MDM platform:

1. At the back of this manual, in Appendix A, find the managed configuration template for Android devices. Copy the content.
2. Open a text editor of your choice and paste the content.
3. Specify the server details in the **android:description** fields.
4. Save the file as .XML.
5. Open your MDM platform and upload the managed configuration file.

For iOS users

To manage iOS devices from an MDM platform, you need to specify the connection details in the managed configuration file.

1. At the back of this manual, in Appendix B, find the managed configuration template for iOS devices. Copy the content.
2. Open a text editor of your choice and paste the content.
3. Specify the server details:
   - **versionConfig** - (Mandatory) Type in the default version of the app configuration **1.0.0**
   - **serverNameConfig** - (Mandatory) Type in the server name
   - **serverAddressConfig** - (Mandatory) Type in the server address
   - **serverPortConfig** - (Mandatory) Type in the server port number
   - **serverConnectionProtocolTypeConfig** - The default connection type is **HTTPS**, to use a non-secure connection, type in **HTTP**
4. Save the file as .XML.
5. Open your MDM platform and upload the managed configuration file.

Naming an output for use in MOBOTIX HUB Mobile client and MOBOTIX HUB Web Client (explained)

To get actions to show correctly together with the current camera, you must create an output group that has the same name as the camera.

Example:

When you create an output group with outputs attached to a camera named "MOBOTIX M73 - 10.100.50.110 - Camera 1", you must enter the same name in the **Name** field (under the **Device group information**).

In the **Description** field, you can add a further description, for example, "MOBOTIX M73 - 10.100.50.110 - Camera 1 - Light switch".

If you do not follow these naming conventions, actions are not available in the action list for the associated camera's view. Instead, actions appear in the list of other actions on the **Actions** tab.

For more information, see Outputs.

External IDP and MOBOTIX HUB Mobile (explained)

IDP is an acronym for Identity Provider. An external IDP is an external application and service where you can store and manage user identity information and provide user authentication services to other systems. You can associate an external IDP with the MOBOTIX HUB VMS.

You can log in to MOBOTIX HUB Web Client or the MOBOTIX HUB Mobile client via an external IDP with MOBOTIX HUB 2022 R3 and later.

To log in with an external IDP to MOBOTIX HUB Web Client or the MOBOTIX HUB Mobile client, you must use an HTTPS connection.

Before you configure external an IDP login for MOBOTIX HUB Web Client and the MOBOTIX HUB Mobile client, make sure that you have:

- Configured an external IDP
- Registered claims
- Mapped claims to roles

For more information, see the administrator manual for MOBOTIX HUB VMS.For more information, see the administrator manual for MOBOTIX HUB VMS.

To log in to MOBOTIX HUB Web Client via an external IDP, you need additional configuration. See Configure external IDP login for MOBOTIX HUB Web Client on page 40.

Configure external IDP login for MOBOTIX HUB Web Client

The option to log in via an external IDP to MOBOTIX HUB Web Client is available for HTTPS connections only.

1. In Management Client, select **Tools** > **Options** and open the **External IDP** tab.
2. In the **Redirect URIs for web clients** section, select **Add**.
3. Enter the addresses for MOBOTIX HUB Web Client in the format **https://[address]:[port number]/index.html**:
    - For the address, enter the host name or the IP address of the computer on which the mobile server is running
    - For the port number, enter the port that MOBOTIX HUB Web Client uses to communicate with the mobile server. For HTTPS connections, the default port number is 8082

Maintenance

Mobile Server Manager (explained)

The Mobile Server Manager is a tray-controlled feature connected to the mobile server. Right-clicking the Mobile Server Manager tray icon in the notification area opens a menu from which you can access the mobile server functionalities.

You can:

- Access MOBOTIX HUB Web Client on page 41
- Start, stop and restart Mobile Server service on page 42
- Change data protection password on page 42
- Show/edit port numbers on page 43
- Enable encryption on the mobile server on page 29 using the **Server Configurator**
- Open today's log file (see Accessing logs and investigations (explained) on page 43)
- Open Log folder (see Accessing logs and investigations (explained) on page 43)
- Open investigations folder (see Accessing logs and investigations (explained) on page 43)
- Change investigations folder on page 44
- See MOBOTIX HUB Mobile Server status (see Show status (explained) on page 44)

Access MOBOTIX HUB Web Client

If you have an MOBOTIX HUB Mobile server installed on your computer, you can use the MOBOTIX HUB Web Client to access your cameras and views. Because you do not need to install MOBOTIX HUB Web Client, you can access it from the computer where you installed the MOBOTIX HUB Mobile server or any other computer you want to use for this purpose.

1. Set up the MOBOTIX HUB Mobile server in the Management Client.
2. If you are using the computer where an MOBOTIX HUB Mobile server is installed, you can right-click the Mobile Server Manager tray icon in the notification area and select **Open MOBOTIX HUB Web Client**.
3. If you are not using the computer where an MOBOTIX HUB Mobile server is installed, you can access it from a browser. Continue with step 4 in this process.
4. Open an Internet browser (Microsoft Edge, Mozilla Firefox, Google Chrome, or Safari).

5. Enter the external IP address, that is, the external address and port of the server on which the MOBOTIX HUB Mobile server is running.

   Example: The MOBOTIX HUB Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (default settings of the installer).

   In the address bar of your browser, enter **http://127.2.3.4:8081** if you want to use a standard HTTP connection or **https://127.2.3.4:8082** to use a secure HTTPS connection. You can now begin using MOBOTIX HUB Web Client.

6. Add the address as a bookmark in your browser for easy future access to MOBOTIX HUB Web Client. If you use MOBOTIX HUB Web Client on the local computer on which you installed the MOBOTIX HUB Mobile server, you can also use the desktop shortcut which the installer creates. Click the shortcut to launch your default browser and open MOBOTIX HUB Web Client.

You must clear the cache of Internet browsers running the MOBOTIX HUB Web Client before you can use a new version of the MOBOTIX HUB Web Client. System administrators must ask their MOBOTIX HUB Web Client users to clear their browser cache after upgrading or force this action remotely (you can do this action only in Internet Explorer in a domain).

Start, stop and restart Mobile Server service

If needed, you can start, stop and restart the Mobile Server service from the Mobile Server Manager.

- To perform any of these tasks, right-click the Mobile Server Manager icon and select **Start Mobile Server service**, **Stop Mobile Server service** or **Restart Mobile Server service**, respectively

Change data protection password

The mobile server data protection password is used to encrypt investigations. As a system administrator, you will need to enter this password to access the mobile server data in case of system recovery or when expanding your system with additional mobile servers.

To change the mobile server data protection password:

1. Right-click the Mobile Server Manager icon and select **Change data protection password settings**. A dialog box appears.
2. In the **New password** field, enter your new password.
3. Re-enter the new password in the **Confirm new password** field.
4. (Optional) If you do not want your investigations to be password protected, select **I choose not to use a mobile server data protection password, and I understand that investigations will not be encrypted**.
5. Click **OK**.

You must save this password and keep it safe. Failure to do so may compromise your ability to recover mobile server data.

Show/edit port numbers

1. Right-click the Mobile Server Manager icon and select **Show/edit port numbers**.
2. To edit the port numbers, enter the relevant port number. You can indicate a standard port number for HTTP connections or a secured port number for HTTPS connections, or both.
3. Click **OK**.

Accessing logs and investigations (explained)

The Mobile Server Manager lets you quickly access the log file of the day, open the folder where log files are saved, and open the folder where investigations are saved.

To open any one of these, right-click the Mobile Server Manager icon and select:

- **Open today's log file**
- **Open Log folder**
- **Open Investigation folder**

Audit logs are created for every action that is not already logged by the Management Server or the Recording Server.

The following actions are always logged (even when extended audit logging is not enabled):

- All administration (these audit log messages contain the old value and the new value)
- All actions regarding creating, editing or deleting investigations as well as preparation and download of exported material, changing relevant pieces of the configuration. The audit log contains details about what has been done.

Video push streaming is logged only when extended audit logging is enabled.

If you uninstall the MOBOTIX HUB Mobile server from your system, its log files are not deleted. Administrators with proper user permissions can access these log files at a later time or decide to delete them if they are not needed any longer. The default location of the log files is in the **ProgramData** folder. If you change the default location of log files, existing logs are not copied to the new location, nor are they deleted.

Change investigations folder

The default location of investigations is in the **ProgramData** folder. If you change the default location of the investigations folder, the existing investigations are not automatically copied to the new location, nor are they deleted. To change the location where you save the investigation exports on your hard disk:

1. Right-click the Mobile Server Manager icon and select **Change investigations folder**.

   The **Investigations location** window opens.

2. Next to the **Folder** field that shows the current location, click the folder icon to browse for an existing folder or create a new folder > Click **OK**.

3. From the **Old investigations** list, select the action that you want to apply to the existing investigations that are stored in the current location. The options are:

   - **Move**: Moves the existing investigations to the new folder

     If you do not move the existing investigations to the new folder, you will no longer be able to see them.

   - **Delete**: Deletes the existing investigations
   - **Do nothing**: The existing investigations remain in the current folder location. You will no longer be able to see them after you have changed the default location of the investigations folder

4. Click **Apply** > Click **OK**.

Show status (explained)

Right-click the Mobile Server Manager icon and select **Show Status** or double-click the Mobile Server Manager icon to open a window that shows the status of the MOBOTIX HUB Mobile server. You can see the following information:

Name	Description
Server running since	Time and date of the time when the MOBOTIX HUB Mobile server was last started.
Connected users	Number of users currently connected to the MOBOTIX HUB Mobile server.
Hardware decoding	Indicates if hardware accelerated decoding is in action on the MOBOTIX HUB Mobile server.
CPU usage	How many % of the CPU is currently being used by the MOBOTIX HUB Mobile server.
CPU usage history	A graph detailing the history of CPU usage by the MOBOTIX HUB Mobile server.

Troubleshooting

Troubleshooting MOBOTIX HUB Mobile

Connections

- **Why can't I connect from my MOBOTIX HUB Mobile client to my recordings/MOBOTIX HUB Mobile server**?

  In order to connect to your recordings, the MOBOTIX HUB Mobile server must be installed on the server that runs your MOBOTIX HUB system or, alternatively, on a dedicated server. The relevant MOBOTIX HUB Mobile settings are also needed in your MOBOTIX HUB video management setup. These are installed as plug-ins or as part of a product installation or upgrade. For details on how to get the MOBOTIX HUB Mobile server and how to integrate the MOBOTIX HUB Mobile client-related settings in your MOBOTIX HUB system, see the configuration section (see Mobile server settings on page 14).

  The server address field must contain a valid host name when applied in the iOS device. Valid host names can contain the ASCII letters 'a' through 'z' (case-insensitive), the digits '0' through '9', dot and the hyphen ('-').

- **I just turned on my firewall, and now I can't connect a mobile device to my server. Why not**?

  If your firewall was turned off while you installed the MOBOTIX HUB Mobile server, you must manually enable TCP and UDP communications.

- **How to avoid the security warning when I run MOBOTIX HUB Web Client through an HTTPS connection**?

  The warning appears because the server address information in the certificate is incorrect. The connection will still be encrypted.
  The self-signed certificate in the MOBOTIX HUB Mobile server needs to be replaced with your own certificate matching the server address used to connect to the MOBOTIX HUB Mobile server. These certificates are obtained through official certificate signing authorities such as Verisign. Consult the chosen signing authority for more details.
  MOBOTIX HUB Mobile server does not use Microsoft IIS. This means that instructions provided for generating certificate signing request (CSR) files by the signing authority using the IIS are not applicable for the MOBOTIX HUB Mobile server. You must manually create a CSR file using command line certificate tools or other similar third-party application. This process should be performed by system administrators and advanced users only.

Image quality

- **Why is the image quality sometimes poor when I view video in the MOBOTIX HUB Mobile client**?

  The MOBOTIX HUB Mobile server automatically adjusts image quality according to the available bandwidth between the server and client. If you experience lower image quality than in the MOBOTIX HUB Desk Client, you might have too little bandwidth to get full-resolution images through the MOBOTIX HUB Mobile client. The reason for this can either be too little upstream bandwidth from the server or too little downstream bandwidth on the client. For more information, see the user manual for MOBOTIX HUB Desk Client.

  If you are in an area with mixed wireless bandwidth, you may notice that the image quality improves when you enter an area with better bandwidth.

- **Why is the image quality poor when I connect to my MOBOTIX HUB video management system at home through Wi-Fi at my office**?

  Check your home internet bandwidth. Many private internet connections have different download and upload bandwidths, often described as, for example, 20 Mbit/2 Mbit. This is because home users rarely need to upload large amounts of data to the internet but consume a lot of data instead. The MOBOTIX HUB video management system needs to send video to the MOBOTIX HUB Mobile client and is limited by your connection's upload speed. If the low image quality is consistent on multiple locations where the download speed of the MOBOTIX HUB Mobile client's network is good, the problem might be solved by upgrading the upload speed of your home internet connection.

Hardware-accelerated decoding

- **Does my processor support hardware-accelerated decoding**?

  Only newer processors from Intel support hardware-accelerated decoding. Check the Intel website (https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&0_QuickSyncVideo=True) if your processor is supported.

  In the menu, make sure **Technologies** > **Intel Quick Sync Video** is set to **Yes**.

  If your processor is supported, hardware-accelerated decoding is enabled by default. You can see the current status in **Show status** in the Mobile Server Manager (see Show status (explained) on page 44).

- **Does my operating system support hardware-accelerated decoding**?

  All the operating systems that MOBOTIX HUB supports also support hardware acceleration.

  Make sure you install the newest graphic drivers on your system. These drivers are not available from Windows Update.

- **How do I disable hardware-accelerated decoding on the mobile server? (Advanced)**

  If the processor on the mobile server supports hardware accelerated decoding, it is by default enabled. To turn hardware-accelerated decoding off, do the following:

  1. Locate the file VideoOS.MobileServer.Service.exe.config. The path is typically: `C:\Program Files\MOBOTIX\MOBOTIX HUB Mobile Server\VideoOS.MobileServer.Service.exe.config`.
  2. Open the file in Notepad or a similar text editor. If necessary, associate the file type .config with Notepad.
  3. Locate the field `<add key="HardwareDecodingMode" value="Auto" />`.
  4. Replace the value "Auto" with "Off".
  5. Save and close the file.

Appendices

Appendix A

Managed configuration template for Android

```
<?xml version="1.0" encoding="utf-8"?>

<restrictions xmlns:android="http://schemas.android.com/apk/res/android">

    <restriction
        android:defaultValue="1.0.0"
        android:description="The current version of the app configuration"
        android:key="version_config"
        android:restrictionType="hidden"
        android:title="Version" />

    <restriction
        android:description="(Mandatory) Enter the server name."
```

```
        android:key="server_name_config"
        android:restrictionType="string"
        android:title="Server name" />

    <restriction
        android:description="(Mandatory) Enter the server address."
        android:key="server_address_config"
        android:restrictionType="string"
        android:title="Server address" />

    <restriction
        android:description="(Mandatory) Enter the server port."
        android:key="server_port_config"
        android:restrictionType="integer"
```

```
        android:title="Server port" />

    <restriction
        android:description="Enable when you use an HTTPS connection. Disable when
you use an HTTP connection."
        android:key="server_secure_connection_config"
        android:restrictionType="bool"
        android:title="Connection protocol type"
        android:defaultValue="true"/>

</restrictions>
```

Appendix B

Managed configuration template for iOS

```
<managedAppConfiguration>
```

```
    <version>1</version>
    <bundleId>com.mobotix.hubmobileclient</bundleId>
    <dict>
        <string keyName="versionConfig">
            <defaultValue>
                <value>1.0.0</value>
            </defaultValue>
        </string>
        <string keyName="serverNameConfig">
        </string>
        <string keyName="serverAddressConfig">
        </string>
        <string keyName="serverPortConfig">
        </string>
```

```
        <string keyName="serverConnectionProtocolTypeConfig">
            <defaultValue>
                <value>HTTPS</value>
            </defaultValue>
        </string>
    </dict>
    <presentation defaultLocale="en-US">
        <field keyName="versionConfig" type="input">
            <label>
                <language value="en-US">Version</language>
            </label>
            <description>
                <language value="en-US">The current version of the app
configuration</language>
            </description>
```

```
        </field>
    <fieldGroup>
        <name>
            <language value="en-US">Mobile server</language>
        </name>
        <field keyName="serverNameConfig" type="input">
            <label>
                <language value="en-US">Server name</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
name.</language>
            </description>
        </field>
        <field keyName="serverAddressConfig" type="input">
```

```
            <label>
                <language value="en-US">Server address</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
address.</language>
            </description>
        </field>
        <field keyName="serverPortConfig" type="input">
            <label>
                <language value="en-US">Server port</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
port.</language>
            </description>
```

```
        </field>

        <field keyName="serverConnectionProtocolTypeConfig" type="input">

            <label>

                <language value="en-US">Connection protocol type</language>

            </label>

            <description>

                <language value="en-US">To specify the connection protocol type,
enter HTTPS or HTTP.</language>

            </description>

        </field>

    </fieldGroup>

    </presentation>

</managedAppConfiguration>
```

MOBOTIX

BeyondHumanVision

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816 0 • sales@mobotix.com • www.mobotix.com

MOBOTIX is a trademark of MOBOTIX AG registered in the European Union, the U.S.A., and in other countries. Subject to change without notice. MOBOTIX do not assume any liability for technical or editorial errors or omissions contained herein. All rights reserved. © MOBOTIX AG 2023